A CONSTRUCTIVE APPROACH TO ZAUNER'S CONJECTURE VIA THE STARK CONJECTURES

MARCUS APPLEBY, STEVEN T. FLAMMIA, AND GENE S. KOPP

ABSTRACT. We propose a construction of d^2 complex equiangular lines in $\mathbb{C}^d$, also known as SICs or SIC-POVMs, which were conjectured by Zauner to exist for all d. The construction gives a putatively complete list of SICs with Weyl–Heisenberg symmetry in all dimensions $d > 3$. Specifically, we give an explicit expression for an object that we call a ghost SIC, which is constructed from the real multiplication values of a special function and which is Galois conjugate to a SIC. The special function, the Shintani–Faddeev modular cocycle, is more precisely a tuple of meromorphic functions indexed by a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We prove that our construction gives a valid SIC in every case assuming two conjectures: the order 1 abelian Stark conjecture for real quadratic fields and a special value identity for the Shintani–Faddeev modular cocycle. The former allows us to prove that the ghost and the SIC are Galois conjugate over an extension of $\mathbb{Q}(\sqrt{\Delta})$ where $\Delta = (d+1)(d-3)$, while the latter allows us to prove idempotency of the presumptive fiducial projector. We provide computational tests of our SIC construction by cross-validating it with known exact solutions, with the numerical work of Scott and Grassl, and by constructing four numerical examples of nonequivalent SICs in $d = 100$, three of which are new. We further consider rank-r generalizations called r-SICs given by equichordal configurations of r-dimensional complex subspaces. We give similar conditional constructions for r-SICs for all r, d such that $r(d-r)$ divides (d^2-1). Finally, we study the structure of the field extensions conjecturally generated by the r-SICs. If K is any real quadratic field, then either every abelian Galois extension of K, or else every abelian extension for which 2 is unramified, is generated by our construction; the former holds for a positive density of field discriminants.

CONTENTS

Date: January 7, 2025.

2020 *Mathematics Subject Classification.* 11R37, 11R42, 42C15, 81P15, 81R05.

Key words and phrases. SIC-POVM, complex equiangular lines, quantum measurement, equichordal tight fusion frame, Stark conjectures, Shintani–Faddeev modular cocycle, partial zeta function, class field theory, real quadratic field, Hilbert's twelfth problem, Weyl–Heisenberg group, Clifford group.

MA acknowledges the support of NSF PHY grant 2210495 and GSK acknowledges the support of NSF DMS grant 2302514.

1. Introduction

SICs (symmetric informationally complete positive operator valued measures, or SIC-POVMs) are complex equiangular tight frames for which the upper bound [29] of d^2 vectors in dimension d is achieved [109, Ch. 14]. They have applications to quantum information [23, 25, 26, 37, 42, 49, 61, 87, 88, 91, 102, 106, 114], compressed sensing in radar [54], classical phase retrieval [36], and the QBist approach to quantum foundations [28, 43]. The Stark conjectures [97–99, 101, 105], by contrast, concern the properties of special values of derivatives of zeta functions in algebraic number theory. They are closely related to Hilbert's twelfth problem [56]. It turns out that there are some connections between SICs and the Stark conjectures. Ref. [69] described a conjectured construction of SICs in terms of Stark units in prime dimensions congruent to $2 \pmod 3$ and greater than 4, while [10, 15] gave a different such construction for dimensions of the form $n^2 + 3$ which are either prime or 4 times a prime. In this paper we extend these observations to arbitrary dimensions greater than 3. In particular we show that the Stark conjectures together with a conjectural special function identity imply SIC existence in every finite dimension. We describe a practical method for constructing SICs numerically. We also describe a larger class of objects called r-SICs.

Let $\mathcal{L}(\mathbb{C}^d)$ denote the $\mathbb{C}$-algebra of linear operators on a d-dimensional complex vector space $\mathbb{C}^d$. We say $\Pi \in \mathcal{L}(\mathbb{C}^d)$ is a *projector* if $\Pi^2 = \Pi$. We will often need to contrast Hermitian and certain non-Hermitian projectors, so we introduce the following shorthand.

Definition 1.1 (H-projector)**.** An *H-projector* is a Hermitian projector.

A set of n distinct rank-1 H-projectors $\{\Pi_j\}_{j=1}^n$ is called *equiangular* if the Hilbert–Schmidt inner product is constant on all distinct pairs, $\mathrm{Tr}(\Pi_j \Pi_k) = \alpha$, for some α independent of $j \neq k$ but possibly depending on d and n. It can be shown [29] that $n \leq d^2$, with a SIC being the case when $n = d^2$. If we drop the the rank-1 requirement we obtain what we will call an r-SIC.

Definition 1.2 (r-SIC)**.** An *r-SIC* is a set of d^2 distinct rank-r H-projectors $\{\Pi_j\}_{j=1}^{d^2}$ in $\mathcal{L}(\mathbb{C}^d)$ such that for all $j \neq k$ and some fixed constant α we have $\mathrm{Tr}(\Pi_j \Pi_k) = \alpha$.

Remark. The terminology *r-SIC* is new, but related concepts have appeared in the literature in other contexts under different names; we review this below.

In 1999, Zauner [114] made the following conjecture regarding 1-SICs.

Conjecture 1.3 (Zauner's Conjecture)**.** *1-SICs exist for all d.*

Zauner further conjectured that 1-SICs should have certain symmetries related to a finite-order Weyl–Heisenberg group (see Definition 1.5), an important point to which we will return.

Prior work on Zauner's conjecture has proven the existence of 1-SICs in only a finite number of dimensions d. Prior authors have constructed 1-SICs exactly in every dimension ≤ 53 and in

many further dimensions up to a maximum of $5\,799$. High precision numerical solutions have been calculated in every dimension ≤ 193 and in many further dimensions up to a maximum of $39\,604$. These results are the work of many people obtained over a period of 25 years, starting with the original work of Hoggar [60] and Zauner [114]. For more on the current state of knowledge, and a review of the history, see [10,15,42,47,48]. In high dimensions the calculations are computationally intensive. The calculations reported in [10, 15] used two supercomputers, both on the TOP500 list [108] and each having $> 10^5$ cores.

As noted above, there seem to be some intimate connections between Conjecture 1.3 and an important open problem in number theory, related to Hilbert's twelfth problem, known as the Stark conjectures [97–99, 101]. The Stark conjectures posit the existence of special algebraic units, now called *Stark units*, arising from zeta functions. In a sequence of papers [7, 10, 13, 15, 69], it was shown that, in a variety of special cases of 1-SICs so far constructed, to very high precision, the expansion coefficients of the elements of a 1-SIC in a natural matrix basis are proportional to powers of Stark units.

This prior work raises the question whether Conjecture 1.3 might actually follow from the Stark conjectures, or perhaps a refinement thereof. In what follows, we partially answer that question, by showingthat Conjecture 1.3 (Zauner's Conjecture) follows from one of the Stark conjectures together with a related conjectural identity. We also show that the signed half-integral powers of the (generalized) Stark units that are needed to calculate r-SICs are naturally expressed in terms of a complex analytic function introduced in [70] and defined below (c.f. Definition 1.18), which we term the Shintani–Faddeev modular cocycle (a generalization of a function originally introduced by Shintani in the context of algebraic number theory [92, 94, 95], and rediscovered by Faddeev and Kashaev in the context of high energy physics [24, 31–35, 45, 64, 79, 111, 113]).

Specifically, we consider four conjectures to which we refer to by name throughout the paper. The *Stark Conjecture* (Conjecture 2.7) is a special case (for real quadratic base field and abelian L-functions vanishing to order 1 at $s = 0$) of the conjectures that can be extracted strictly from Stark's original series of papers [97–99, 101]. The *Stark–Tate Conjecture* (Conjecture 2.8) is a standard refinement of the Stark Conjecture due to Tate [105], stated in the special case we require.[1] The *Monoid Stark Conjecture* (Conjecture 2.9) is a further mild refinement, involving less-studied zeta functions attached to elements of a certain monoid, not known to follow from the Stark–Tate conjecture. The fourth conjecture is a new (and rather mysterious) identity involving special values of the Shintani–Faddeev modular cocycle that we call the *Twisted Convolution Conjecture* (Conjecture 1.35). Together, these conjectures give a remarkably precise refinement of the Stark conjectures as applied to real quadratic fields. We establish the following theorem.

Theorem 1.4. *The Stark Conjecture and the Twisted Convolution Conjecture together imply Zauner's conjecture.*

This result follows as a corollary of a much more precise and stronger theorem stated below, Theorem 1.47. To understand the ideas behind the proof and to see how it extends to certain families of r-SICs for $r > 1$, we need to establish a few more notions. The r-SICs we consider all carry a transitive action of the following Weyl–Heisenberg group.

[1] Tate himself attributes that special case to Stark, but the claim that the square root of the Stark unit is in an abelian extension does not appear as a conjecture in Stark's published work.

Definition 1.5 (Weyl–Heisenberg group, standard basis, ω_d, ξ_d, $\bar{d}$, displacement operators)**.** Let $|0\rangle, \ldots, |d-1\rangle$ be the orthonormal *standard basis* for $\mathbb{C}^d$. Let X, Z be unitary operators acting as

$$X|j\rangle = |j+1\rangle, \qquad Z|j\rangle = \omega_d|j\rangle, \qquad \omega_d = e^{\frac{2\pi i}{d}}, \tag{1.1}$$

where addition of indices in the first equation is performed modulo d. Also let $\xi_d = -e^{\frac{\pi i}{d}}$ and $\bar{d} = \frac{d}{2}\big(3 + (-1)^d\big)$, so that $\bar{d} = d$ when d is odd and $\bar{d} = 2d$ when d is even, and ξ_d is a $\bar{d}$-th root of unity. Then the *Weyl–Heisenberg group* in dimension d, denoted $\mathrm{WH}(d)$, is the set of $d^2\bar{d}$ operators

$$\{\xi_d^{p_0} X^{p_1} Z^{p_2} : 0 \le p_0 < \bar{d}, 0 \le p_1, p_2 < d\}. \tag{1.2}$$

The *displacement operators* are the d^2 distinct $\mathrm{WH}(d)$ group elements

$$D_{\mathbf{p}} = \xi_d^{p_1 p_2} X^{p_1} Z^{p_2}, \qquad \mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \in \mathbb{Z}^2. \tag{1.3}$$

Remark. In the SIC literature, the root of unity we are calling ξ_d is usually denoted τ. This conflicts with the way τ is used in the theory of modular forms, to which we make essential appeal.

Definition 1.6 (WH-covariant, fiducial)**.** An r-SIC is *WH-covariant* if it is of the form $\{\Pi_{\mathbf{p}} : 0 \le p_1, p_2 < d\}$, where

$$\Pi_{\mathbf{p}} = D_{\mathbf{p}} \Pi D_{\mathbf{p}}^\dagger \tag{1.4}$$

for some fixed H-projector Π, called the *fiducial* projector.

Remark. In this paper, we are exclusively concerned with WH-covariant r-SICs, and we further specialize to $d > 3$, henceforth without comment. The known 1-SICs thus excluded are all in some ways exceptional and are called *sporadic SICs* by Stacey [96]. It is open whether more such examples exist.

With the above restrictions, r-SICs split naturally into equivalence classes via an action of the *extended Clifford group* [4], defined later in Section 3.2. A long-standing problem has been to understand the structure of these classes for the case of 1-SICs. The classes exhibit rather complicated phenomenology, as can be seen from the data tables in, e.g., [11,89,90]. We summarize these empirical observations in Section 3.3. In Section 7 we show that Theorem 1.47 together with two additional conjectures implies that this phenomenology arises from the class structure of certain integral binary quadratic forms. The result is illustrated by the data tables in Appendix F. Also see the examples Section 7.3, where, among other things, we plot the number of SIC equivalence classes in each dimension up to $d = 10^6$. In Section 7 we give proofs for various other aspects of the currently observed phenomenology.

Our results also show that r-SICs can answer questions in number theory and explicit class field theory. For example, we show that, under conditional assumptions, every abelian Galois extension of $\mathbb{Q}(\sqrt{5})$ is contained in a field generated by the overlaps of an $\mathbf{r}$-SIC and roots of unity. The field $\mathbb{Q}(\sqrt{5})$ can be replaced by any real quadratic field with an odd trace unit (see Theorem 1.52), and such real quadratic fields make up a positive proportion of all real quadratic fields in the sense of asymptotic density (see Theorem 6.15).

Our classification scheme and conjectures suggest a new direction to approach the Stark conjectures and Hilbert's twelfth problem for real quadratic fields. Numerical evidence suggests that the polynomial equations defining a WH-covariant r-SIC (when $r < \frac{d-1}{2}$) define an algebraic variety of dimension zero. A proof of the Twisted Convolution Conjecture would reduce many cases of the Stark conjecture to a claim about the properties of the algebraic variety of WH-covariant r-SICs.

1.1. **Generalizing to r-SICs.** We wish to generalize prior work from 1-SICs to r-SICs, both because this is crucial for the construction of a large family of abelian extensions, and because the richness of the class of r-SICs for $r > 1$ has been heretofore unappreciated. Although general r-SICs have received much less attention, they have been studied in other contexts under different names. They are also called maximal equichordal tight fusion frames [22,38,67], maximal symmetric tight fusion frames [9], or regular quantum designs of degree 1 and cardinality d^2 [114]. They are instances of structures which have been variously described as SI-POVMs [5], general SIC-POVMs [46], and SIMs [50], and they are special cases of conical designs [50].

Unlike 1-SICs, there are some known cases where r-SICs are proven to exist in infinitely many dimensions. Firstly, it has been shown [5] that in every odd dimension d there exists an r-SIC with $r = (d-1)/2$. Secondly, it has been shown [9] that, to every 1-SIC in odd dimension d of the kind described in Definition 1.6 below, there is a corresponding r-SIC with $r = (d-1)/2$ (different from the one constructed in [5]). These constructions described in [5,9] are very different from the constructions in this paper, and we do not consider them further.

The connection to the Stark conjectures is via the so-called *normalized overlaps*, which we define below. To motivate their definition, we first see that the geometry of an r-SIC constrains the value of α in Definition 1.2 to certain specific values.

Theorem 1.7. *Let $\Pi_1, \ldots, \Pi_{d^2}$ be an r-SIC. Then for all j, k,*

$$\operatorname{Tr}(\Pi_j \Pi_k) = \left(\frac{rd(d-r)}{d^2-1}\right)\delta_{jk} + \frac{r(rd-1)}{d^2-1}. \tag{1.5}$$

Furthermore, the Π_j are a basis for $\mathcal{L}(\mathbb{C}^d)$, and up to a scale factor the Π_j form a resolution of the identity:

$$\sum_{j=1}^{d^2} \Pi_j = rdI. \tag{1.6}$$

Proof. This result can be proven without assuming WH-covariance or $d > 3$; see Section 3.4. □

Theorem 1.8. *Let Π be an H-projector in dimension d. Then Π is a fiducial projector for an r-SIC if and only if*

$$\left|\operatorname{Tr}\left(\Pi D_{\mathbf{p}}^{\dagger}\right)\right| = \sqrt{\frac{r(d-r)}{d^2-1}} \tag{1.7}$$

for all $\mathbf{p} \neq \mathbf{0} \pmod d$.

Proof. See Section 3.4. □

Definition 1.9 (overlaps; normalized overlaps)**.** Let Π be an r-SIC fiducial projector. The numbers $\mu_{\mathbf{p}} = \operatorname{Tr}\left(\Pi D_{\mathbf{p}}^{\dagger}\right)$ are called the *overlaps*. If $\mathbf{p} \not\equiv \mathbf{0} \pmod d$, from the polar decomposition $\mu_{\mathbf{p}} = |\mu_{\mathbf{p}}| e^{i\theta_{\mathbf{p}}}$ we define the *normalized overlaps* to be the phases $\nu_{\mathbf{p}} = e^{i\theta_{\mathbf{p}}}$.

It follows from Theorem 1.8 that

$$\nu_{\mathbf{p}} = \sqrt{\frac{d^2-1}{r(d-r)}}\mu_{\mathbf{p}} \tag{1.8}$$

for $\mathbf{p} \not\equiv \mathbf{0} \pmod d$. The fact that Π is Hermitian means

$$\nu_{\mathbf{p}}\nu_{-\mathbf{p}} = 1 \tag{1.9}$$

for all $\mathbf{p}$. Since the displacement operators form a basis for $\mathcal{L}(\mathbb{C}^d)$, a fiducial can be recovered from its normalized overlaps using the formula

$$\Pi = \frac{r}{d} I + \sqrt{\frac{r(d-r)}{d^2(d^2-1)}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \nu_{\mathbf{p}} D_{\mathbf{p}}, \tag{1.10}$$

where the sum is over any set of coset representatives of $\mathbb{Z}^2/d\mathbb{Z}^2$ with the representative of $d\mathbb{Z}^2$ excluded. This means one could equivalently define an r-SIC fiducial to be a $\Pi \in \mathcal{L}(\mathbb{C}^d)$ that is a rank-r H-projector where the $\nu_{\mathbf{p}}$ in the representation of (1.10) are unit complex numbers.

The overlaps and normalized overlaps of known 1-SIC solutions have been studied in great detail to extract insights that might lead to a resolution of Zauner's conjecture. It was realized quickly (see, e.g., [90]) that all known overlaps are algebraic numbers (excluding, as usual, the case of $d = 3$). We define a field generated by these numbers, adjoining a root of unity as well to ensure independence of the choice of fiducial.

Definition 1.10 (SIC field)**.** For a fiducial r-SIC projector Π, the *extended projector SIC field*, or simply the *SIC field*, is the field generated by the entries of Π and the $\bar{d}$-th root of unity ξ_d, or equivalently, the field generated by the overlaps along with ξ_d:

$$E = E_\Pi = \mathbb{Q}(\xi_d, \Pi_{ij} : 0 \leq i, j < d) = \mathbb{Q}(\xi_d, \operatorname{Tr}(\Pi D_{\mathbf{p}}) : \mathbf{p} \in (\mathbb{Z}/d\mathbb{Z})^2). \tag{1.11}$$

In [7] it was found (among other things) that, for known 1-SICs, the SIC field is an abelian extension of the real quadratic field $\mathbb{Q}\big(\sqrt{(d+1)(d-3)}\big)$. Refs. [12, 13] made an empirical study of the minimal SIC fields for a large number of dimensions where a full set of exact 1-SICs had been calculated. They showed (among other things) that for these examples:

(1) the minimal SIC field in dimension d is the ray class field over $\mathbb{Q}\big(\sqrt{(d+1)(d-3)}\big)$ with modulus $\bar{d}$ and ramification at both infinite places;
(2) the normalized overlaps $\nu_{\mathbf{p}} = e^{i\theta_{\mathbf{p}}}$ are in fact algebraic units.

The 1-SICs generating a ray class field have been explicitly related to Stark units in several examples. In [69], the normalized overlaps of the four lowest lying prime dimensions congruent to $5 \pmod 6$ were shown to be Galois conjugates of square roots of Stark units. In [10,15], a different construction was used, in which the components of the fiducial vector were directly related to Stark units for dimensions of the form $n^2 + 3$ which are either prime [10] or equal to 4 times a prime [15], thereby pushing up the highest dimension in which 1-SICs have been calculated by an order of magnitude.

The approach taken in this paper generalizes the method used in [69] to every r-SIC in every dimension. We hope to examine the connection with the method used in [10, 15] in a future publication.

SICs are constructed in [69] by taking Galois conjugates of half-integral powers of Stark units. This motivates mimicking the expression (1.10), but with *real* numbers that we hope to relate to Stark units in place of the normalized overlaps. Thus we define a *ghost r-SIC* in terms of certain *normalized ghost overlaps* which we expect to be algebraic units:

Definition 1.11 (Ghost fiducial, normalized ghost overlaps, ghost overlaps, twist)**.** A *ghost r-SIC fiducial*, or *ghost fiducial* for short, is a rank-r projector $\tilde{\Pi}$ given by

$$\tilde{\Pi} = \frac{r}{d} I + \sqrt{\frac{r(d-r)}{d^2(d^2-1)}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{G\mathbf{p}} D_{\mathbf{p}} \tag{1.12}$$

where the sum is over any set of coset representatives of $\mathbb{Z}^2/d\mathbb{Z}^2$ with the representative of $d\mathbb{Z}^2$ excluded, where G is a $\mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ matrix called the *twist*, and where the $\tilde{\nu}_{\mathbf{p}}$, called the *normalized ghost overlaps*, are real numbers satisfying

$$\tilde{\nu}_{\mathbf{p}}\tilde{\nu}_{-\mathbf{p}} = 1 \tag{1.13}$$

for all $\mathbf{p} \not\equiv \mathbf{0} \pmod{\bar{d}}$, and which are such that $\tilde{\nu}_{\mathbf{p}'} = \tilde{\nu}_{\mathbf{p}}$ whenever $\mathbf{p}' \equiv \mathbf{p} \not\equiv \mathbf{0} \pmod{\bar{d}}$. Paralleling (1.8) we also define the *ghost overlaps*

$$\tilde{\mu}_{\mathbf{p}} = \begin{cases} r & \mathbf{p} \equiv \mathbf{0} \pmod{d}, \\ \sqrt{\frac{r(d-r)}{d^2-1}}\tilde{\nu}_{\mathbf{p}} & \text{otherwise.} \end{cases} \tag{1.14}$$

(So $\mathrm{Tr}\big(\tilde{\Pi}D_{\mathbf{p}}^\dagger\big) = \tilde{\mu}_{G\mathbf{p}}$.)

Remark. A few observations are in order here. Firstly, we only introduce the matrix G at this stage for the sake of consistency with later discussion. When we subsequently give explicit formulae, it will be found that there is a natural way to define the $\tilde{\nu}_{\mathbf{p}}$ to which we want to give special prominence (see (1.46) below). Using this natural definition, we will be able to take $G = I$ when $r = 1$, but we will want to take $G \neq I$ for $r > 1$.

Secondly, in the case of r-SICs we start with a family of d^2 projectors, then introduce their overlaps, and finally define the corresponding normalized overlaps. In our definition of ghost fiducials we reverse that order and start with the normalized ghost overlaps. The reason is that the function of the ghost fiducial, at least for present purposes, is to make a bridge between r-SICs and the Stark conjectures. The normalized overlaps of the r-SICs considered in this paper are conjecturally units in an algebraic number field having absolute value 1 and satisfying (1.9). Conjecturally, they are are also Galois conjugates of a set of real units satisfying (1.13). It is these numbers, what we call the normalized ghost overlaps, which provide the connection with the Stark conjectures, and which are thus the objects of primary importance for the purposes of this paper. One can then use them in (1.12) to define a corresponding ghost fiducial. For present purposes the latter is only of secondary importance.

Note that, although one is free to define a family of d^2 projectors in analogy with (1.4), by defining $\tilde{\Pi}_{\mathbf{p}} = D_{\mathbf{p}}\tilde{\Pi}D_{\mathbf{p}}^\dagger$, the overlaps of this family are typically not real and do not have constant modulus. This construction will therefore play no role in this paper.

Conjecturally, there is a Galois automorphism g acting on a suitable number field such that (1.10) and (1.12) are related by $\tilde{\Pi} = g\big(\Pi\big)$. We therefore use a *tilde* to distinguish ghost objects from their "live" counterparts, though this notation does not presume any functional relationship between Π and $\tilde{\Pi}$. In view of (1.9), the condition (1.13) is implied by such a relationship.

Definition 1.12 (Live fiducial)**.** To contrast them with the ghost fiducials specified by Definition 1.11, r-SIC fiducials as specified by (1.10) will sometimes be referred to as *live* fiducials.

A ghost fiducial is typically not an H-projector. It is however a *P-projector*, short for parity-Hermitian projector, which we now define.

Definition 1.13 (Parity operator, parity-Hermitian, P-projector)**.** The *parity operator* is the unitary matrix U_P acting on the standard basis for $\mathbb{C}^d$ as $U_P|j\rangle = |-j\rangle$, where arithmetic inside the ket is modulo d (see also Definition 3.4). A matrix M is *parity-Hermitian* if it equals its Hermitian conjugate when conjugated by the parity operator:

$$M^\dagger = U_P M U_P^\dagger . \tag{1.15}$$

A *P-projector* is a parity-Hermitian projection operator.

Remark. The subscript P in the notation U_P stands for the 2×2 negative-identity matrix $P = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})$. The unitary matrix $U_P \in \mathrm{U}(d)$ comes from a certain function $(A \mapsto U_A) : \mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z}) \to \mathrm{U}(d)$ defining a projective representation $\mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z}) \to \mathrm{U}(d)/(\mathbb{C}^\times I)$. The representation is described in Section 3.2.

As examples, observe that the displacement operators are parity-Hermitian:

$$D_{\mathbf{p}}^\dagger = U_P D_{\mathbf{p}} U_P^\dagger \,. \tag{1.16}$$

The fact that the expansion coefficients on the RHS of (1.12) are all real means that a ghost fiducial $\widetilde{\Pi}$ is a P-projector.

1.2. **Refining Stark units.** Informally, the Stark conjectures give concrete formulas relating certain analytic functions with associated algebraic data. More specifically, they relate the values of the derivatives of certain partial zeta functions at $s = 0$ to the logarithms of absolute values of units in an algebraic number field.

Our goal is to construct r-SICs by first constructing the corresponding normalized ghost overlaps using (conjectural) Stark units. What we will actually need are not the Stark units themselves, but rather, certain *square roots* of generalized Stark units. This presents a difficulty in that the sign of the square root is *a priori* ambiguous. To get around this problem, instead of working with zeta functions as is done in [10, 15, 69], we work with a function we call the *Shintani–Faddeev modular cocycle*, introduced in [70] based on the approach pioneered by Shintani [92–95]. We will also need to resolve an ambiguity in roots of unity that arises in this process, and for this we also define the *Shintani–Faddeev phase*. We require some notation and several other definitions before we are ready to define these functions.

Let $\mathbb{H}$ be the *upper half plane*

$$\mathbb{H} = \{z \in \mathbb{C} \colon \operatorname{Im}(z) > 0\}. \tag{1.17}$$

We require two variants of the q-Pochhammer symbol, which in its usual variants is denoted $(a;q)_n$ or $(a;q)_\infty$. We will find it convenient to write $q = e^{2\pi i \tau}$ and $a = e^{2\pi i z}$ and to treat τ and z as the fundamental variables.

Definition 1.14 (variant q-Pochhammer symbols)**.** The *finite variant q-Pochhammer symbol* is defined by

$$\varpi_n(z,\tau) = \begin{cases} \prod_{j=0}^{n-1} \left(1 - e^{2\pi i(z+j\tau)}\right) & n > 0 \\ 1 & n = 0 \\ \prod_{j=n}^{-1} \left(1 - e^{2\pi i(z+j\tau)}\right)^{-1} & n < 0 \end{cases} \tag{1.18}$$

for $n \in \mathbb{Z}$, $z, \tau \in \mathbb{C}$. The (infinite) *variant q-Pochhammer symbol* is

$$\varpi(z,\tau) = \prod_{j=0}^{\infty} \left(1 - e^{2\pi i(z+j\tau)}\right) \tag{1.19}$$

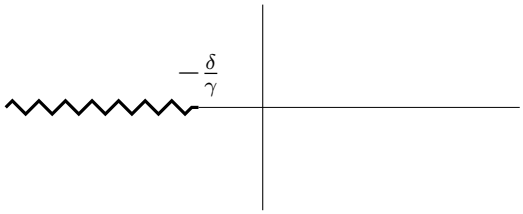
for $z \in \mathbb{C}$, $\tau \in \mathbb{H}$.

For $\tau \in \mathbb{C}$, $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, define the *fractional linear transform* $M \cdot \tau$ and denote the denominator $j_M(\tau)$ respectively by

$$M \cdot \tau = \frac{\alpha\tau + \beta}{\gamma\tau + \delta}\,, \qquad \text{and} \qquad j_M(\tau) = \gamma\tau + \delta\,. \tag{1.20}$$

We say τ is a *fixed point* of M if $M \cdot \tau = \tau$.

Definition 1.15 (The domain $\mathcal{D}_M$)**.** For $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ define $\mathcal{D}_M$ to be the set $\mathbb{C} \setminus \{\tau \in \mathbb{R} \colon \det(M) j_M(\tau) \leq 0\}$, illustrated in the complex plane below for the case $\gamma > 0$ and $\det(M) = 1$.



Remark. Note that for reasons of technical convenience we define $\mathcal{D}_M$ for an arbitrary matrix $M \in \mathrm{GL}_2(\mathbb{Z})$, although in its main application, to the definition of the Shintani–Faddeev modular cocycle (see below), we only need it for matrices $M \in \mathrm{SL}_2(\mathbb{Z})$.

Definition 1.16 (SF Jacobi cocycle)**.** For $M \in \mathrm{SL}_2(\mathbb{Z})$ the *Shintani–Faddeev (SF) Jacobi cocycle* is a meromorphic function σ_M on $\mathbb{C} \times \mathcal{D}_M$ whose restriction to $\mathbb{C} \times \mathbb{H}$ is given by

$$\sigma_M(z, \tau) = \frac{\varpi\left(\frac{z}{j_M(\tau)}, M \cdot \tau\right)}{\varpi(z, \tau)}. \tag{1.21}$$

Remark. See [70] and Appendix D for the continuation to $\mathbb{C} \times \mathcal{D}_M$.

It is shown in Appendix D that σ_M satisfies the cocycle condition

$$\sigma_{MM'}(z, \tau) = \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M' \cdot \tau\right) \sigma_{M'}(z, \tau)\,. \tag{1.22}$$

for all values of z, τ such that both sides of the equation are defined.

Up to a scale factor, $\sigma_S(z, \tau)$ with $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is the *double sine function* or *noncompact quantum dilogarithm*. The name Shintani–Faddeev acknowledges Shintani's original introduction of the double sine function in connection with his work on Kronecker-type limit formulas and the Stark conjectures [92–95], and its subsequent rediscovery under the name quantum dilogarithm by Faddeev in connection with his work on discrete Liouville theory [33, 34]. Subsequently it has also featured in quantum Teichmüller theory, three-dimensional supersymmetric gauge theory, complex Chern–Simons theory, quantum group theory, and quantum knot theory (see [24, 31, 32, 35, 44, 111] and references cited therein).

For $\mathbf{p} = \left(\begin{smallmatrix} p_1 \\ p_2 \end{smallmatrix}\right)$ and $\mathbf{q} = \left(\begin{smallmatrix} q_1 \\ q_2 \end{smallmatrix}\right) \in \mathbb{C}^2$, define the nondegenerate *symplectic form*

$$\langle \mathbf{p}, \mathbf{q} \rangle = -\det\left(\begin{smallmatrix} p_1 & q_1 \\ p_2 & q_2 \end{smallmatrix}\right) = p_2 q_1 - p_1 q_2\,. \tag{1.23}$$

When the second argument is a complex number $\tau \in \mathbb{C}$, we also use the notation

$$\langle\!\langle \mathbf{p}, \tau \rangle\!\rangle = \langle \mathbf{p}, \left(\begin{smallmatrix} \tau \\ 1 \end{smallmatrix}\right) \rangle = p_2 \tau - p_1\,. \tag{1.24}$$

It is easily verified that

$$\langle M\mathbf{p}, M\mathbf{q} \rangle = (\det M) \langle \mathbf{p}, \mathbf{q} \rangle, \qquad \langle\!\langle M\mathbf{p}, M \cdot \tau \rangle\!\rangle = \frac{(\det M)\, \langle\!\langle \mathbf{p}, \tau \rangle\!\rangle}{j_M(\tau)} \tag{1.25}$$

for all $L \in \mathrm{GL}_2(\mathbb{Z})$, $\mathbf{p}, \mathbf{q} \in \mathbb{Z}^2$, and $\tau \in \mathbb{C}$.

For $d \in \mathbb{N}$ define $\Gamma(d)$ to be the *principal congruence subgroup of level* d consisting of matrices $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $A \equiv I \pmod{d}$. We will also need a particular family of non-principal congruence subgroups, which we define now.

Definition 1.17 ($\Gamma_{\mathbf{r}}$)**.** For $\mathbf{r} \in \mathbb{Q}^2$, let $\Gamma_{\mathbf{r}}$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices A such that $(A - I)\mathbf{r} \in \mathbb{Z}^2$.

Remark. Note that if $\mathbf{r} \in \frac{1}{d}\mathbb{Z}^2$, then $\Gamma(d)$ is a subgroup of $\Gamma_{\mathbf{r}}$.

Definition 1.18 (SF modular cocycle)**.** If $\mathbf{r} \in \mathbb{Q}^2$ and $M \in \Gamma_{\mathbf{r}}$, then the *Shintani–Faddeev (SF) modular cocycle* is defined by

$$\mathfrak{w}_M^{\mathbf{r}}(\tau) = \frac{\sigma_M(\langle\langle \mathbf{r}, \tau \rangle\rangle, \tau)}{\varpi_{((I-M)\mathbf{r})_2}\left(\frac{\langle\langle \mathbf{r}, \tau \rangle\rangle}{j_M(\tau)}, M \cdot \tau\right)} \tag{1.26}$$

for all $\tau \in \mathcal{D}_M$. (This is equivalent to the definition given in [70, Defn. 4.18] by [70, Prop. 4.19].)

Remark. The symbol $\mathfrak{w}$ is the Hebrew letter "shin." For instructions on how to typeset this character in LaTeX, see [70, Sec. 9].

For $\tau \in \mathbb{H}$ and $\mathbf{r} \notin \mathbb{Z}^2$, a straightforward calculation shows that

$$\mathfrak{w}_M^{\mathbf{r}}(\tau) = \frac{\varpi(\langle\langle \mathbf{r}, M \cdot \tau \rangle\rangle, M \cdot \tau)}{\varpi(\langle\langle \mathbf{r}, \tau \rangle\rangle, \tau)}, \tag{1.27}$$

and thus that the multiplicative group-cohomological cocycle condition

$$\mathfrak{w}_{MN}^{\mathbf{r}}(\tau) = \mathfrak{w}_M^{\mathbf{r}}(N \cdot \tau)\, \mathfrak{w}_N^{\mathbf{r}}(\tau) \tag{1.28}$$

holds for $M, N \in \Gamma_{\mathbf{r}}$. By meromorphic continuation (see also Appendix D), the cocycle condition holds for $\tau \in \mathcal{D}_M$, while the "coboundary" expression (1.27) does not make sense outside the upper half plane (although a similar expression may be given on the lower half plane, but not on the real line). The map $M \mapsto \mathfrak{w}_M^{\mathbf{r}}$ from $\Gamma_{\mathbf{r}}$ to the multiplicative group of meromorphic functions defines a cohomologically nontrivial class in a certain cohomology group, which is somewhat tricky to define correctly and is discussed in more detail in [70, Sec. 4.1 and Sec. 5]. In this paper, we will primarily be concerned with $M \in \Gamma(d)$ rather than in the larger group $\Gamma_{\mathbf{r}}$, because we will be fixing d and varying $\mathbf{r}$. We abuse terminology slightly by referring to the meromorphic function $\mathfrak{w}_M^{\mathbf{r}}(\tau)$ itself (rather than the map from $\Gamma_{\mathbf{r}}$ or $\Gamma(d)$) as a "cocycle."

The importance of the function $\mathfrak{w}_M^{\mathbf{r}}(\tau)$ for us is that, as we will see, it provides a bridge between the geometric construct of an r-SIC with algebraic number theory. On the one hand we use special values of the function to construct ghost overlaps, while on the other hand these same special values are related to Stark units. In particular, under the assumption of the Stark Conjecture, (see Section 1.5), they are algebraic integers, and indeed units. For abelian extensions of a large set of real quadratic fields, they play an analogous role to the one that roots of unity play in connection with abelian extensions of $\mathbb{Q}$, and that elliptic functions and modular forms (more precisely, Siegel units [74]) play in connection with abelian extensions of imaginary quadratic fields. These algebraic properties are essential if we wish to take Galois conjugates of our constructed ghost overlaps, as we do to construct live r-SIC fiducials.

1.3. **Quadratic fields and quadratic forms.** We next briefly review some definitions associated to the theory of quadratic forms and quadratic fields, mainly to fix notation.

Let D be a square-free positive integer, and let $K = \mathbb{Q}(\sqrt{D})$ be the corresponding real quadratic field. Then the *discriminant* of K is

$$\Delta_0 = \begin{cases} D & \text{if } D \equiv 1 \pmod 4, \\ 4D & \text{otherwise.} \end{cases} \tag{1.29}$$

The *ring of integers* in K is denoted by $\mathcal{O}_K$ and the *unit group* by $\mathcal{O}_K^\times$.

A *binary quadratic form* is a bivariate polynomial $Q(x,y) = ax^2 + bxy + cy^2$. Unless stated explicitly to the contrary, we will simply say *form* to mean an integral, primitive, irreducible, and indefinite binary quadratic form. That is, a, b, c are coprime integers, the roots of $Q(x,1)$ are in $\mathbb{R}$ but not in $\mathbb{Q}$, and Q takes both positive and negative values. We will employ the shorthand $Q = \langle a, b, c\rangle$, and where there is no risk of confusion we will use the same symbol Q to denote the Hessian matrix of Q scaled by a factor of $\frac{1}{2}$:

$$Q = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}. \tag{1.30}$$

If $\mathbf{p}$ is the vector $\left(\begin{smallmatrix} p_1 \\ p_2 \end{smallmatrix}\right)$, we will also write $Q(\mathbf{p}) = Q(p_1, p_2)$.

Let Q be a form and let $M \in \mathrm{GL}_2(\mathbb{Z})$. Then we denote by Q_M the form

$$Q_M = \det(M) M^{\mathrm{T}} Q M. \tag{1.31}$$

We say two forms Q, Q' are *equivalent* and write $Q \sim Q'$ if

$$Q' = Q_M \tag{1.32}$$

for some $M \in \mathrm{GL}_2(\mathbb{Z})$.

Let $Q = \langle a, b, c\rangle$ be a form; then $\Delta = -4\det(Q) = b^2 - 4ac$ is its *discriminant*. Let D be the square-free part of Δ. Then the *fundamental discriminant* of Q is

$$\Delta_0 = \begin{cases} D & \text{if } D \equiv 1 \pmod 4 \\ 4D & \text{otherwise}, \end{cases} \tag{1.33}$$

and the *conductor* of Q is the integer

$$f = \sqrt{\frac{\Delta}{\Delta_0}}. \tag{1.34}$$

We say that the form Q is *associated* to the real quadratic field K if the discriminant of K is the fundamental discriminant of Q. We define the *roots* of Q to be

$$\rho_{Q,\pm} = \frac{-b \pm \sqrt{\Delta}}{2a}. \tag{1.35}$$

We will find it convenient to introduce a notion of sign to both forms and elements of $\mathrm{GL}_2(\mathbb{Z})$.

Definition 1.19 (Sign)**.** Let $Q = \langle a, b, c\rangle$ be a form, and let $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ be an element of $\mathrm{GL}_2(\mathbb{Z})$. We define:

(1) The *sign* of Q, denoted $\mathrm{sgn}(Q)$, to be the sign of a, $\mathrm{sgn}(a)$;
(2) The *sign* of M, denoted $\mathrm{sgn}(M)$, to be the sign of γ, with the convention that if $\gamma = 0$, then $\mathrm{sgn}(M) = \mathrm{sgn}(\delta)$.

We will also need the usual definition of the stability group of a form as well as one variant.

Definition 1.20 (Stability group of a quadratic form)**.** Let Q be a form and d a positive integer. We define:

(1) $\mathcal{S}(Q)$ to be the set of all $M \in \mathrm{GL}_2(\mathbb{Z})$ such that $Q_M = Q$;
(2) $\mathcal{S}_d(Q) = \mathcal{S}(Q) \cap \Gamma(d)$.

We refer to $\mathcal{S}(Q)$ as the *stability group* of Q.

1.4. **Admissible tuples, the Shintani–Faddeev phase, and normalized ghost overlaps.** We now introduce the data necessary to define the set of normalized ghost overlaps corresponding to a ghost fiducial. This is encapsulated in the notion of an *admissible tuple*.

It will turn out to be convenient to have two equivalent notions of admissible tuples: the first notion starts with the dimension and the rank and has a more geometric flavor; the second starts with the real quadratic field and has a more number-theoretic flavor. We will describe the geometric definition first and then describe the equivalence with the number-theoretic definition. The equivalence of these data is stated below in Theorem 1.25.

The dimension d and rank r of the r-SICs we consider in this paper must satisfy the following conditions.

Definition 1.21 (Admissible pair, associated field)**.** A pair of integers (d, r) is called *admissible* if there exists an integer $n > 4$ such that

$$0 < r < \frac{d-1}{2}\,, \qquad\qquad nr(d-r) = d^2 - 1\,. \tag{1.36}$$

For each such admissible pair, we define a real quadratic *associated field* $K = \mathbb{Q}\Big(\sqrt{n(n-4)}\Big)$.

The condition on r immediately implies $d > 3$. The reason for the requirement $n > 4$ is to ensure that K is real quadratic. The reasons for the restriction $r < (d-1)/2$ are: Firstly, the transformation $r \to d - r$ can be used to swap between a projector Π and its complement $I - \Pi$, and these give essentially equivalent objects; secondly, the cases[2] $r = d/2$ and $r = (d-1)/2$ are inconsistent with the requirement $n > 4$, and so with the requirement that K be real quadratic.

There are infinitely many admissible pairs (d, r). For example, for a given dimension d there is always the $r = 1$ solution $(d, 1)$ leading to a 1-SIC with associated field $\mathbb{Q}\big(\sqrt{(d+1)(d-3)}\big)$. There is also a solution for arbitrary $r > 2$ given by $(r^2 + r - 1, r)$ corresponding to an r-SIC with associated field $\mathbb{Q}\big(\sqrt{r^2-4}\big)$. However it is easily seen that there is no solution for $r = 2$. These are only a few of the possible solutions, as we discuss below.

Rather than starting with an admissible pair (d, r), the number-theoretic approach starts with a given field K and then characterizes the admissible pairs (d, r) associated to that field. One finds that they form two-index grids $d_{j,m}$, $r_{j,m}$ called the *dimension grid* and the *rank grid* respectively, defined below in Definition 1.24. The dimension and rank grids are defined in terms of powers of a unit ε defined as follows:

Definition 1.22 (Fundamental totally positive unit ε)**.** For K a real quadratic field, define ε to be the fundamental totally positive unit greater than 1 (equivalently, the smallest positive-norm unit greater than 1).

Remark. To avoid cluttering the notation, we do not indicate the field K explicitly. The field will always be clear from context.

Remark. As we will see, the properties of ε are intimately related to the Zauner symmetry of an r-SIC.

Before defining the dimension grid, we define the *sequence of conductors*, which is independently important, as it plays a central role in the classification of r-SICs.

[2]For the Diophantine equation $nr(d-r) = d^2-1$, the case $r = d/2$ reduces to the single solution $(d, r, n) = (2, 1, 3)$ in positive integers, whereas the case $r = (d-1)/2$ produces the family of solutions $(d, r, n) = (2k+1, k, 4)$. The former case leads to the 1-SIC in dimension $d = 2$, whereas the latter case leads to continuous families of r-SICs of a very different nature to those described herein, including examples with elementary descriptions.

Definition 1.23 (Sequence of conductors f_j)**.** Let K be a real quadratic field, let Δ_0 be its discriminant, and let ε be the unit from Definition 1.22. For positive integers j, define

$$f_j = \frac{\varepsilon^j - \varepsilon^{-j}}{\sqrt{\Delta_0}} \tag{1.37}$$

to be the *sequence of conductors*.

Remark. As with ε, we do not indicate the field K explicitly. This will always be clear from context.

We are now ready to define the dimension and rank grids.

Definition 1.24 (Dimension grid, rank grid, dimension tower, root dimension, admissible triple)**.** Let K be a real quadratic field and f_j its sequence of conductors. For all positive integers j, m, define

$$r_{j,m} = \frac{f_{jm}}{f_j}\,, \qquad d_{j,m} = r_{j,m+1} + r_{j,m}\,, \qquad d_j = d_{j,1}. \tag{1.38}$$

We define

(1) the two-index sequence $d_{j,m}$ as the *dimension grid* associated to K and $r_{j,m}$ as the *rank grid*,
(2) the sequence d_j as the *dimension tower* associated to K, and
(3) the integer d_1 as the *root dimension* of K.

For all real quadratic K and positive integers j, m we say (K, j, m) is an *admissible triple*.

Remark. As with ε and f_j, we do not indicate the field K explicitly in the definitions of $r_{j,m}$, $d_{j,m}$, d_j. This will always be clear from context.

The next theorem establishes a bijection between the set of admissible pairs and the set of admissible triples.

Theorem 1.25. *For each admissible triple (K, j, m), the pair $(d_{j,m}, r_{j,m})$ is admissible. Conversely, for each admissible pair, (d, r) there is a unique admissible triple (K, j, m) such that $(d_{j,m}, r_{j,m}) = (d, r)$.*

Proof. This is an immediate consequence of Theorem 4.21. □

Definition 1.26 (Admissible tuple equivalence $\sim$)**.** We write $(d, r) \sim (K, j, m)$ if (d, r) is associated to (K, j, m) under the bijection just described—that is, if $d = d_{j,m}$ and $r = r_{j,m}$.

The dimension grid $d_{j,m}$ consists of the dimensions in which, conditional on our conjectures, there exist r-SICs generating abelian extensions of the number field K, and the corresponding ranks of the r-SICs are $r_{j,m}$. When $m = 1$, the rank $r_{j,1}$ is always 1, and the sequence of dimensions $d_{j,1}$ is distinguished as the dimensions where there occur 1-SICs. From a physics and geometric point of view the 1-SICs have a special significance, which motivates picking out the dimensions in which they occur by defining $d_j = d_{j,1}$.

Example. Consider $K = \mathbb{Q}(\sqrt{5})$. The fundamental unit greater than 1 is $\frac{1}{2}\big(1 + \sqrt{5}\big)$, but this has norm -1. The unit ε is therefore the square of this unit, $\varepsilon = \frac{1}{2}\big(3 + \sqrt{5}\big)$. The sequence of conductors f_j begins $1, 3, 8, 21, 55, 144, 377, 987, \ldots$ and is given by the $(2n)^{\text{th}}$ Fibonacci number.

Consequently the dimension grid and rank grid for this case are

$$d_{j,m} = \begin{matrix} \vdots & \vdots & \vdots & \vdots & \\ 48 & 2\,255 & 105\,937 & 4\,976\,784 & \dots \\ 19 & 341 & 6\,119 & 109\,801 & \dots \\ 8 & 55 & 377 & 2\,584 & \dots \\ 4 & 11 & 29 & 76 & \dots \end{matrix}, \quad r_{j,m} = \begin{matrix} \vdots & \vdots & \vdots & \vdots & \\ 1 & 47 & 2\,208 & 103\,729 & \dots \\ 1 & 18 & 323 & 5\,796 & \dots \\ 1 & 7 & 48 & 329 & \dots \\ 1 & 3 & 8 & 21 & \dots \end{matrix} \tag{1.39}$$

In these grids the lower-left entries are $d_{1,1}$ and $r_{1,1}$ respectively; j increases from bottom to top and m increases from left to right. The left-hand column of the first grid gives d_j, the sequence of dimensions in which one finds 1-SICs associated to the field $\mathbb{Q}(\sqrt{5})$.

We now extend the notion of admissible to include a form as part of an admissible tuple.

Definition 1.27 (Admissible tuple with form)**.** Let Q be a form, and let $(d, r) \sim (K, j, m)$ be admissible tuples. We say that $(d, r, Q) \sim (K, j, m, Q)$ are *admissible* if the fundamental discriminant of Q is the discriminant of K and the conductor of Q is a divisor of f_j.

Example. Consider again $K = \mathbb{Q}(\sqrt{5})$. The form $Q = \langle 1, -3, 1\rangle$ has fundamental discriminant 5 and conductor 1, so (K, j, m, Q) is always admissible for positive integers j, m. When $j = 1, m = 1$, we see that $d_{1,1} = 4$ and $r_{1,1} = 1$, so $(K, 1, 1, Q) \sim (4, 1, Q)$ and $(4, 1, Q)$ is also admissible.

The form $Q' = \langle 5, -20, 4\rangle$ also has fundamental discriminant 5, but it has conductor 8. From the sequence of conductors $f_j = 1, 3, 8, 21, 55, 144, \dots$ we see that (K, j, m, Q') is only admissible for $j = 3, 6, \dots$ and in fact when $3 \,|\, j$. A corresponding admissible tuple for $j = 3, m = 1$ is given by $(K, 3, 1, Q') \sim (19, 1, Q')$.

Admissible tuples contain all of the data necessary to define a corresponding set of normalized ghost overlaps. However, before giving the explicit formula, it is convenient to introduce a few more definitions. Recall from Definition 1.20 that $\mathcal{S}(Q)$ is the stability group of Q and $\mathcal{S}_d(Q)$ is the intersection of $\mathcal{S}(Q)$ with $\Gamma(d)$.

Definition 1.28 (Associated stabilizers, L_t, A_t, $L_{+,t}, L_{\mathrm{z,t}}$)**.** Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, and let f be the conductor of Q. Define the *associated stabilizer* for $\mathcal{S}(Q)$, denoted L_t, to be the positive-trace generator of $\mathcal{S}(Q)$ with the same sign as Q, and the *associated stabilizer* for $\mathcal{S}_d(Q)$, denoted A_t, to be the generator of $\mathcal{S}_d(Q)$ with the same sign as Q.

Also define

$$L_{+,t} = \begin{cases} L_t & \det(L_t) = +1, \\ L_t^2 & \det(L_t) = -1, \end{cases} \tag{1.40}$$

$$L_{\mathrm{z,t}} = \frac{d_j - 1}{2} I + \frac{f_j}{f} SQ \tag{1.41}$$

where $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

Remark. We require that L_t is positive trace, and that L_t, A_t have the same sign as Q mainly for the sake of definiteness. Note, however, that other choices, though possible, might complicate the statements of some of our results.

In Theorem 4.53 we prove that $\mathcal{S}_d(Q)$ is infinite cyclic, so restricting the sign of A_t gives a unique choice of generator. However, $\mathcal{S}(Q)$ has nontrivial torsion, so we must also stipulate that it has positive trace to avoid any ambiguity.

The significance of the matrix $L_{+,t}$ is that $\mathcal{S}(Q) \cap \mathrm{SL}_2(\mathbb{Z})$ is generated by $L_{+,t}$ and $-I$ (see Theorem 4.53). The significance of the matrix $L_{\mathrm{z,t}}$ is that it is the unique element of $\mathcal{S}(Q)$ such that $L_{\mathrm{z,t}}^{2m+1} = A_t$ (see Theorem 4.53). In the case of a 1-SIC, it is related to the canonical order 3 symmetry which is a prominent feature of SIC phenomenology (see Theorem 7.21).

Example. Consider again $K = \mathbb{Q}(\sqrt{5})$. We have seen that the tuple $t = (d, r, Q) = (4, 1, \langle 1, -3, 1\rangle)$ is admissible. It is easily checked that the matrices $\pm \left(\begin{smallmatrix} 3 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\pm \left(\begin{smallmatrix} 0 & 1 \\ -1 & 3 \end{smallmatrix}\right)$ are in $\mathcal{S}(Q)$. In fact they are the generators, and accordingly we choose $L_t = + \left(\begin{smallmatrix} 3 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ as the associated stabilizer since this has the same sign as Q and positive trace. One then finds $L_{+,t} = L_{\mathrm{z,t}} = L_t$. The matrix $A_t = L_t^3$ is easily seen to be an element of $\mathcal{S}_d(Q)$ and is in fact a generator with the same sign as Q.

We have seen that the tuple $t = (19, 1, \langle 5, -20, 4\rangle)$ is another admissible tuple corresponding to the same field. The associated stabilizers are $L_t = L_{+,t} = L_{\mathrm{z,t}} = \left(\begin{smallmatrix} 19 & -4 \\ 5 & -1 \end{smallmatrix}\right)$ and $A_t = L_t^3$.

There are two more functions that we need to define. While the definitions are rather technical, the role these functions play is easy to motivate.

In general, the SF modular cocycle is complex, but the normalized ghost overlaps $\tilde{\nu}_{\mathbf{p}}$ are by definition real. The *Shintani–Faddeev (SF) phase*, defined below, is a complex unit which multiplies the SF modular cocycle so that the product is always a real number. This requirement alone could of course be achieved by simply multiplying by the complex unit having the conjugate argument, but for the result to be a ghost overlap requires certain additional structure in the pattern of signs as $\mathbf{p}$ varies. The SF phase achieves the desired sign structure. Moreover, it is simply a root of unity with a quadratic dependence on $\mathbf{p}$ in the exponent.

It is worth noting that the approach here, using the SF modular cocycle, has an important advantage over the L-function approach in [10, 15, 69] in that it provides a simple way to resolve the sign ambiguity in the definition of the normalized ghost overlaps. By contrast resolving the ambiguity using the approach in [10, 69] requires a demanding computation on a case-by-case basis.

The definition of the SF phase depends on a certain integral class function on $\mathrm{SL}_2(\mathbb{Z})$ known as the *Rademacher class invariant* [86].

Definition 1.29 (Rademacher class invariant)**.** For all $M \in \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ the *Rademacher class invariant* is given by

$$\Psi(M) = \begin{cases} \frac{\mathrm{Tr}(M)}{\gamma} - 3\,\mathrm{sgn}\big(\gamma\,\mathrm{Tr}(M)\big) - 12\,\mathrm{sgn}(\gamma)\mathfrak{s}(\alpha,\gamma) & \gamma \neq 0\,, \\ \frac{\beta}{\delta} & \gamma = 0\,, \end{cases} \tag{1.42}$$

where $\mathfrak{s}(a, b)$ with $a, b \in \mathbb{Z}$ and $b \neq 0$ is the Dedekind sum

$$\mathfrak{s}(a,b) = \sum_{n=1}^{|b|-1} \left(\!\!\left(\frac{n}{b}\right)\!\!\right)\left(\!\!\left(\frac{na}{b}\right)\!\!\right), \qquad \text{with } (\!(x)\!) = \begin{cases} 0 & x \in \mathbb{Z} \\ x - \lfloor x \rfloor - \frac{1}{2} & x \notin \mathbb{Z} \end{cases}, \tag{1.43}$$

and where we adopt the convention $\mathrm{sgn}(0) = 0$.

Definition 1.30 (SF phase)**.** Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, and let $\mathbf{p} \in \mathbb{Z}^2$. The *SF phase*, denoted $\phi_{\mathbf{p}}(t)$, is

$$\phi_{\mathbf{p}}(t) = (-1)^{s_d(\mathbf{p})} e^{-\frac{\pi i}{12}\Psi(A_t)} \xi_d^{-\frac{f_{jm}}{f} Q(\mathbf{p})}, \tag{1.44}$$

where $s_d(\mathbf{p}) = d + (1 + d)(1 + p_1)(1 + p_2)$ and f is the conductor of Q.

Remark. In the even dimensional case other choices for the sign $(-1)^{s_d(\mathbf{p})}$ are possible. However, it is shown in Appendix A that they do not lead to new equivalence classes of r-SICs.

Theorem 1.31. *Let $t = (d, r, Q)$ be an admissible tuple. Then*

$$\rho_{Q,\pm} \in \mathcal{D}_{A_t} \cap \mathcal{D}_{A_t^{-1}}. \tag{1.45}$$

Proof. See page 73 in Section 4.6. □

We now have all of the ingredients to state our formula for the normalized ghost overlaps.

Definition 1.32 (candidate normalized ghost overlaps corresponding to an admissible tuple)**.** Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, and let $\mathbf{p} \in \mathbb{Z}^2$. The corresponding *candidate normalized ghost overlaps* are defined by

$$\tilde{\nu}_{\mathbf{p}}(t) = \phi_{\mathbf{p}}(t)\, \mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho_t)\,. \tag{1.46}$$

for all $\mathbf{p}$, where the $\phi_{\mathbf{p}}(t)$ are defined by Definition 1.30 and $\rho_t = \rho_{Q,+}$. The corresponding *candidate ghost overlaps* are defined by

$$\tilde{\mu}_{\mathbf{p}}(t) = \begin{cases} r & \mathbf{p} \equiv \mathbf{0} \pmod{d}\,, \\ \sqrt{\frac{r(d-r)}{d^2-1}}\, \tilde{\nu}_{\mathbf{p}}(t) & \text{otherwise.} \end{cases} \tag{1.47}$$

Remark. Note that this definition relies on Theorem 1.31, since otherwise the RHS would not be well-defined. Note also that instead of defining $\rho_t = \rho_{Q,+}$, we could equally well define $\rho_t = \rho_{Q,-}$. Specifically, it is shown in Appendix A that ghost overlaps calculated using $\rho_{Q,-}$ with the form Q coincide with those calculated using $\rho_{Q',-}$ with a different form Q'. Finally, note that in Corollary 4.22 we derive a simpler expression for the scaling factor $\sqrt{\frac{r(d-r)}{d^2-1}}$ in (1.47).

1.5. **The main conjectures.** Our goal is to show that the candidate normalized ghost overlaps defined by (1.46), when inserted on the right hand side of (1.12) give, with a suitable choice of twist G, ghost fiducials from which live fiducials can then be constructed by applying a suitable Galois conjugation. The validity of the construction depends on the Twisted Convolution Conjecture and Stark Conjecture.

To motivate the Twisted Convolution Conjecture, observe that if the candidate normalized ghost overlaps $\tilde{\nu}_{\mathbf{p}}(t)$ specified by (1.46) are to give rise to a ghost fiducial when substituted into (1.12), then we must have

(1) The numbers $\tilde{\nu}_{\mathbf{p}}(t)$ are real for all $\mathbf{p} \not\equiv \mathbf{0} \pmod{d}$,
(2) $\tilde{\nu}_{\mathbf{p}}(t)\tilde{\nu}_{-\mathbf{p}}(t) = 1$ for all $\mathbf{p} \not\equiv \mathbf{0} \pmod{d}$),
(3) $\tilde{\Pi}^2 = \tilde{\Pi}$.

The first two conditions are proved in Theorem 5.8. However, we have so far been unable to prove the last condition, which must therefore be posited as an additional conjecture. Before stating it we need some definitions.

Definition 1.33. Let $\mathbf{p}, \mathbf{q} \in \mathbb{Q}^2$ and let n be a positive integer. Then we define

$$\delta_{\mathbf{p},\mathbf{q}}^{(n)} = \begin{cases} 1 & \mathbf{p} - \mathbf{q} \in n\mathbb{Z}^2, \\ 0 & \text{otherwise.} \end{cases} \tag{1.48}$$

Definition 1.34 (Shift)**.** Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple. We say that $\lambda \in \mathbb{Z}/d\mathbb{Z}$ is a *shift* for t if

(1) $2\lambda + d_j - 1$ is coprime to d,

(2) λ satisfies

$$\sum_{\mathbf{q}\in\mathcal{I}_{\mathbf{p}}} \omega_d^{r\langle \mathbf{p},(\lambda I+L_{\mathrm{z,t}})\mathbf{q}\rangle} \mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_t)\, \mathfrak{w}_{A_t^{-1}}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_t) = d^2\delta_{\mathbf{p},\mathbf{0}}^{(d)} \tag{1.49}$$

for all $\mathbf{p} \in \mathbb{Z}^2$, where the index set $\mathcal{I}_{\mathbf{p}}$ is any complete set of coset representatives for $\mathbb{Z}^2/d\mathbb{Z}^2$ containing $\mathbf{0}$ and $\mathbf{p}$. The set of all shifts for t is denoted $\mathcal{Z}_t$.

We are now ready to state our additional conjecture:

Conjecture 1.35 (Twisted Convolution Conjecture)**.** *For every admissible tuple the set of shifts $\mathcal{Z}_t$ includes the values $\lambda = 0, 1$. Moreover, if $t = (d, r, Q)$ and $t' = (d, r, Q')$ are admissible tuples such that Q and Q' have the same discriminant, then $\mathcal{Z}_t = \mathcal{Z}_{t'}$.*

As a matter of empirical observation it appears that $0, 1$ are the only shifts when $r = 1$, but that when $r > 1$ there are others.

The set of shifts for a given tuple $t = (d, r, Q) \sim (K, j, m, Q)$ also determines the possible choices of the twist in Definition 1.11. Specifically, it can be seen from the proof of Theorem 1.46 that if the Twisted Convolution Conjecture is valid, then a matrix G is a possible choice of twist if and only if

$$\det(G)r(2\lambda + d_j - 1 + d) \equiv 1 \pmod{\bar{d}} \tag{1.50}$$

for some $\lambda \in \mathcal{Z}_t$.

The Twisted Convolution Conjecture guarantees the existence of ghost fiducials in every dimension. To get from there to the existence of live fiducials in every dimension we need a guarantee that

(1) the matrix entries of the ghost fiducial are algebraic numbers,
(2) there exists a Galois automorphism with the properties needed to convert the ghost fiducial into a live fiducial.

These guarantees are provided directly by a conjectures about special values of the Shintani–Faddeev modular cocycle (called *real multiplication (RM) values* in [70]). We first state a "minimalist" such conjecture, which will be sufficient (together with the Twisted Convolution Conjecture) to prove SIC existence.

Conjecture 1.36 (Minimalist[3] Real Multiplication Values Conjecture)**.** *Let $\rho \in \mathbb{R}$ such that $a\rho^2 + b\rho + c = 0$ with $a, b, c \in \mathbb{Z}$ and $\Delta = b^2 - 4ac$ is not a square. Let $\mathbf{r} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ and $A \in \Gamma_{\mathbf{r}}$ such that $A \cdot \rho = \rho$. Then:*

(1) $\mathfrak{w}_A^{\mathbf{r}}(\rho)$ is an algebraic number.
(2) If $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $g(\sqrt{\Delta}) = -\sqrt{\Delta}$, then $|g(\mathfrak{w}_A^{\mathbf{r}}(\rho))| = 1$.

We also state here two stronger conjectures. These are identical except that the former is restricted to fundamental discriminants, while the latter is for non-square discriminants.

Conjecture 1.37 (Fundamental Real Multiplication Values Conjecture)**.** *Let $\rho \in \mathbb{R}$ such that $a\rho^2 + b\rho + c = 0$ with $a, b, c \in \mathbb{Z}$ and $\Delta = b^2 - 4ac$ is a fundamental discriminant. Let $\mathbf{r} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ and $A \in \Gamma_{\mathbf{r}}$ such that $A \cdot \rho = \rho$. Then:*

(1) $\mathfrak{w}_A^{\mathbf{r}}(\rho)$ is an algebraic unit in an abelian Galois extension of $\mathbb{Q}(\sqrt{\Delta})$.
(2) If $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $g(\sqrt{\Delta}) = -\sqrt{\Delta}$, then $|g(\mathfrak{w}_A^{\mathbf{r}}(\rho))| = 1$.

[3]Strictly, we could prove SIC existence from an even more "minimalist" conjecture by only assuming the existence of one Galois automorphism satisfying property (2).

Conjecture 1.38 (General Real Multiplication Values Conjecture)**.** *Let $\rho \in \mathbb{R}$ such that $a\rho^2 + b\rho + c = 0$ with $a, b, c \in \mathbb{Z}$ and $\Delta = b^2 - 4ac$ is not a square. Let $\mathbf{r} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ and $A \in \Gamma_{\mathbf{r}}$ such that $A \cdot \rho = \rho$. Then:*

(1) $\mathfrak{w}_A^{\mathbf{r}}(\rho)$ is an algebraic unit in an abelian Galois extension of $\mathbb{Q}(\sqrt{\Delta})$.
(2) If $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $g(\sqrt{\Delta}) = -\sqrt{\Delta}$, then $|g(\mathfrak{w}_A^{\mathbf{r}}(\rho))| = 1$.

Conjecture 1.36 is implied by the Stark Conjecture (Conjecture 2.7), that is, the version of Stark's conjecture on special values of derivatives of partial zeta functions attached to real quadratic fields that is conjectured in Stark's original work. Conjecture 1.36 is indeed considerably weaker than the Stark Conjecture.

Conjecture 1.37 is implied by the Stark–Tate Conjecture (Conjecture 2.8), which includes a small refinement of the Stark Conjecture due to Tate. Of course, Conjecture 1.37 is also implied by Conjecture 1.38.

Conjecture 1.38 is implied by the Monoid Stark Conjecture (Conjecture 2.9), a Stark-type conjecture for special values of derivatives of more general partial zeta functions attached to classes in ray class monoids. The MSC is technically due to the third author (as it is equivalent to [70, Conj. 1.4]) and is not currently known to follow from STC. The original form of the Stark Conjecture does imply that some integral power of $\mathfrak{w}_A^{\mathbf{r}}(\rho)$ is in an abelian extension of $\mathbb{Q}(\sqrt{\Delta})$; see Theorem 2.20.

The conditional implications between the Stark-type conjectures and the RM values conjectures are summarized in the following theorem.

Theorem 1.39. *The following implications hold.*

(1) Conjecture 2.7 (the Stark Conjecture) implies Conjecture 1.36.
(2) Conjecture 2.8 (the Stark–Tate Conjecture) implies Conjecture 1.37.
(3) Conjecture 2.9 (the Monoid Stark Conjecture) implies Conjecture 1.38.

Proof. See Section 2.7. □

1.6. **The main theorems: existence.** We now state the main theorems on the existence of ghost r-SICs and live r-SICs, conditional on the Twisted Convolution Conjecture and the Stark Conjecture. These theorems are proven in Section 5.

It will be helpful to attach a field E_t to an admissible tuple t in an unconditional manner independent of the connection to SICs. Conditionally, this field will be identical to the (extended projection) SIC field of any r-SIC fiducial associated to t.

Definition 1.40 (Fields associated to an admissible tuple)**.** Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple.

(1) We define the *field associated to* t, denoted E_t, to be the field generated over $\mathbb{Q}$ by the numbers $\{\tilde{\mu}_{\mathbf{p}}(t) \colon 0 \leq p_1, p_2 < d,\ \mathbf{p} \neq \mathbf{0}\}$ together with ξ_d.
(2) We define the *Galois-closed field associated to* t, denoted $\hat{E}_t$, to be the Galois closure (within $\mathbb{C}$) of the compositum of K and E_t.

The construction of r-SICs from admissible tuples requires some non-canonical choices. We bundle two additional pieces of data, a 2×2 matrix modulo $\bar{d}$ and a Galois automorphism, with an admissible tuple to form a *fiducial datum*, from which an r-SIC fiducial will be constructed.

Definition 1.41 (Fiducial datum)**.** A *fiducial datum* is a tuple $(d, r, Q, G, g) \sim (K, j, m, Q, G, g)$ such that $t = (d, r, Q) \sim (K, j, m, Q)$ is an admissible tuple, G is an element of $\mathrm{GL}_2(\mathbb{Z})$ whose

determinant satisfies

$$\det(G) r(2\lambda + d_j - 1 + d) \equiv 1 \pmod{\bar{d}} \tag{1.51}$$

for some $\lambda \in \mathcal{Z}_t$, and g is any element of $\mathrm{Gal}(\hat{E}_t/\mathbb{Q})$ such that $g(\sqrt{\Delta_0}) = -\sqrt{\Delta_0}$, where Δ_0 is the fundamental discriminant of Q.

We will sometimes write $s = (t, G, g)$, and say that the datum s *contains* the tuple t.

Remark 1.42. If E_t contains transcendentals, then we make sense of the above definitions as follows: The field $\hat{E}_t$ is all of $\mathbb{C}$, and $\mathrm{Gal}(\hat{E}_t/\mathbb{Q})$ is the full automorphism group of $\mathbb{C}$ over $\mathbb{Q}$. This will not matter in practice, because the Stark Conjecture will imply that E_t is a finite Galois extension of $\mathbb{Q}$ and $\hat{E}_t = E_t$.

It is not the case that $\tilde{\nu}_{\mathbf{p}}(t)$, $\tilde{\mu}_{\mathbf{p}}(t)$, considered as functions of $\mathbf{p}$, have period d. It is, however, true that the products $\tilde{\nu}_{\mathbf{p}}(t) D_{\mathbf{p}}$, $\tilde{\mu}_{\mathbf{p}}(t) D_{\mathbf{p}}$ have period d provided one excludes the case $\mathbf{p} \equiv 0 \pmod{d}$. More generally, we have the following result:

Lemma 1.43. *Let $s = (t, G, g)$ be a fiducial datum, and let $\mathbf{p}, \mathbf{p}' \in \mathbb{Z}^2/d\mathbb{Z}^2$ be such that $\mathbf{p}' \equiv \mathbf{p} \pmod{d}$ and $\mathbf{p}, \mathbf{p}' \notin d\mathbb{Z}^2$. Then*

$$\tilde{\nu}_{G\mathbf{p}'}(t) D_{\mathbf{p}'} = \tilde{\nu}_{G\mathbf{p}}(t) D_{\mathbf{p}}, \qquad \tilde{\mu}_{G\mathbf{p}'}(t) D_{\mathbf{p}'} = \tilde{\mu}_{G\mathbf{p}}(t) D_{\mathbf{p}}. \tag{1.52}$$

Proof. The proof is given in Section 5.3, following Lemma 5.7. □

Definition 1.44 (Candidate ghost r-SIC fiducial $\tilde{\Pi}_s$, Candidate r-SIC fiducial Π_s, candidate normalized overlap)**.** Let $s = (d, r, Q, G, g) \sim (K, j, m, Q, G, g)$ be a fiducial datum, and let t be the corresponding admissible tuple $(d, r, Q) \sim (K, j, m, Q)$. We define the corresponding candidate ghost r-SIC fiducial by

$$\tilde{\Pi}_s = \frac{1}{d} \sum_{\mathbf{p}} \tilde{\mu}_{G\mathbf{p}}(t) D_{\mathbf{p}} \tag{1.53}$$

where the sum is over any complete set of coset representatives for $\mathbb{Z}^2/d\mathbb{Z}^2$, and where $\tilde{\mu}_{\mathbf{p}}(t)$ is as defined in Definition 1.32.

We define the corresponding candidate r-SIC fiducial by

$$\Pi_s = g(\tilde{\Pi}_s), \tag{1.54}$$

the candidate overlaps by

$$\mu_{\mathbf{p}}(s) = \mathrm{Tr}\left(\Pi_s D^{\dagger}_{G^{-1}\mathbf{p}}\right), \tag{1.55}$$

and, for $\mathbf{p} \not\equiv \mathbf{0} \pmod{d}$, the normalized candidate overlaps by

$$\nu_{\mathbf{p}}(s) = \sqrt{\frac{d^2 - 1}{r(d - r)}} \mu_{\mathbf{p}}(s). \tag{1.56}$$

Remark. Note that this definition tacitly relies on Lemma 1.43, which shows that that the summand on the RHS of (1.53) is independent of the set of coset representatives chosen.

The candidate overlaps can be expressed directly in terms of their ghost counterparts via:

Lemma 1.45. *Let $s = (d, r, Q, G, g) \sim (K, j, m, Q, G, g)$ be a fiducial datum, and let t be the corresponding admissible tuple $(d, r, Q) \sim (K, j, m, Q)$. Then*

$$\mu_{\mathbf{p}}(s) = g\Big(\tilde{\mu}_{GH_g^{-1}G^{-1}\mathbf{p}}(t)\Big) \tag{1.57}$$

for all $\mathbf{p}$, where H_g is the matrix specified in Definition 3.6.

Remark. Note that, unlike $\tilde{\mu}_{\mathbf{p}}(t)$, the candidate overlaps $\mu_{\mathbf{p}}(s)$ depend on G and g as well as t.

Proof. See Section 3.2, following Theorem 3.7. □

Theorem 1.46. *Assume Conjecture 1.35 (the Twisted Convolution Conjecture). Then, for every fiducial datum s, the corresponding operator $\tilde{\Pi}_s$ given in Definition 1.44 is a ghost r-SIC fiducial.*

Proof. See Section 5.4. □

Theorem 1.47. *Assume Conjecture 1.35 (the Twisted Convolution Conjecture), and also assume Conjecture 1.36 (as implied by Conjecture 2.7, the Stark Conjecture). Let $s = (d, r, Q, G, g)$ be a fiducial datum. Then the operator Π_s given in Definition 1.44 is an r-SIC fiducial.*

Proof. See Section 5.6. □

1.7. **The main theorems: class fields attained.** We now state our main conditional results about the abelian extensions generated by SICs. These results are based on unconditional results in pure algebraic number theory giving containment of certain class fields. They are proven in Section 6.

We use the following notation for orders of real quadratic fields.

Definition 1.48. Given a real quadratic field K and positive integer f, we denote the order with conductor f in K by $\mathcal{O}_f$. That is,

$$\mathcal{O}_f = \left\{ m + nf\left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2}\right) : m, n \in \mathbb{Z} \right\}, \tag{1.58}$$

where Δ_0 is the discriminant of K.

Remark. Note that K will always be clear from context. In particular, the ring of integers $\mathcal{O}_K$ may alternatively be written $\mathcal{O}_1$.

The following two results give properties of the field E_t associated to an admissible tuple t within our framework of conjectures. Together, they show conditionally that E_t is an abelian extension of the real quadratic field K containing a particular ray class field. The latter theorem is restricted to the case when Q has conductor 1, i.e., $\mathrm{disc}(Q)$ is a fundamental discriminant.

Theorem 1.49. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple. Make the following conditional assumptions:*

- *If $\mathrm{disc}(Q)$ is fundamental, assume Conjecture 1.37 (as implied by Conjecture 2.8, the Stark–Tate Conjecture).*
- *If $\mathrm{disc}(Q)$ is not fundamental, assume Conjecture 1.38 (as implied by Conjecture 2.9, the Monoid Stark Conjecture).*

Then the field E_t is an abelian extension of K.

Proof. See Section 6.3. □

Theorem 1.50. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple for which $\mathrm{disc}(Q)$ is a fundamental, and let $d = d_{j,m}$. Assume Conjecture 2.8 (the Stark–Tate Conjecture). Let $E = H^{\mathcal{O}_1}_{\bar{d}\infty_1\infty_2}$ be the ray class field with level datum $(\mathcal{O}_1; \bar{d}\mathcal{O}_1, \{\infty_1, \infty_2\})$, as defined by Theorem 2.2. Then, E is equal to the field extension of K generated by the numbers $\{\tilde{\mu}_{\mathbf{p}}(t)^2 : 0 \leq p_1, p_2 < d, \mathbf{p} \neq \mathbf{0}\}$ together with ξ_d. The field $E_t \supseteq E \supseteq K$, the extension E_t/K is ramified at both infinite places of K, and field E_t depends only on the pair (d, r).*

Proof. See Section 6.3. □

Empirically, it seems that E_t is actually equal to the ray class field E in Theorem 1.50, and indeed a similar statement may be made when Q is not fundamental. As we do not know how to prove this from any form of the Stark conjectures in the literature, we state it as a separate conjecture.

Conjecture 1.51. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, let $d = d_{j,m}$, and let f be the conductor of Q. Let $E = H^{\mathcal{O}_f}_{\bar{d}\infty_1\infty_2}$ be the ray class field with level datum $(\mathcal{O}_f; \bar{d}\mathcal{O}_f, (\infty_1, \infty_2))$, as defined by Theorem 2.2. Then $\hat{E}_t = E_t = E$.*

Our results suggest that r-SICs provide a geometric interpretation of class field theory over a real quadratic field K. Thus, we'd like to realize arbitrary abelian extensions of K using r-SICs. We show conditionally that this is possible when the trace of the fundamental unit is odd.

Theorem 1.52. *Assume the Conjecture 2.8 (the Stark–Tate Conjecture). Let K be a real quadratic field of discriminant Δ_0, and let ε be a fundamental totally positive unit in K (as in Definition 1.22).*

(1) If $\mathrm{Tr}(\varepsilon)$ is odd, then every abelian extension of K is contained in E_t for some admissible tuple $t \sim (d, r, Q)$ with $\mathrm{disc}(Q) = \Delta_0$.
(2) If $\mathrm{Tr}(\varepsilon)$ is even, then every abelian extension of K that is unramified at the primes of K lying over 2 is contained in E_t for some admissible tuple $t \sim (d, r, Q)$ with $\mathrm{disc}(Q) = \Delta_0$.

Proof. See Section 6.4. □

The condition that $\mathrm{Tr}(\varepsilon)$ is odd is common among real quadratic fields. When ordered by discriminant, the condition holds for at least 7.4% of real quadratic K, in the sense of asymptotic density, by Theorem 6.15. (The true density looks empirically like 22.2%.) When ordered by root dimension d_1, $\mathrm{Tr}(\varepsilon)$ is odd if and only if d_1 is even, so instead 50% of real quadratic K satisfy the condition. For those real quadratic fields for which $\mathrm{Tr}(\varepsilon)$ is even, Theorem 1.52 still says that "many" abelian extensions are contained in some E_t.

Theorem 1.52 makes clear the relevance of r-SICs to Hilbert's twelfth problem of generating abelian extensions from special values of explicit complex-analytic functions. Specifically, a proof of the Stark–Tate Conjecture and the Twisted Convolution Conjecture would give a solution to Hilbert's twelfth problem that is both complex-analytic and geometric, for a positive proportion of real quadratic fields. Our construction is complex-analytic because the $\wp$-function is a complex analytic function. It is geometric both in the sense that r-SICs are described by sets of pairwise equichordal subspaces, and in the sense that the algebraic equations for a Weyl–Heisenberg r-SIC projector cut out an algebraic variety.

1.8. **Table of notation.** For the convenience of the reader we include the following summary of the notation and terminology used in this paper.

Notation	Terminology	Definition
$\mathcal{L}(\mathbb{C}^d)$	space of linear operators on $\mathbb{C}^d$	–
–	H-projector	1.1
–	P-projector	1.13
–	r-SIC	1.2
–	Zauner's Conjecture	conj. 1.3
$\mathrm{WH}(d)$	Weyl–Heisenberg group in dimension d	1.5
$\bar{d}$	d (resp. $2d$) if d is odd (resp. even)	1.5
ω_d	$e^{2\pi i/d}$	1.5
ξ_d	$-e^{\pi i/d}$	1.5
X, Z, $D_{\mathbf{p}}$	$\mathrm{WH}(d)$ displacement operators	1.5
U_P	parity operator	1.13, 3.4
P	parity matrix	3.4
–	WH covariant r-SIC	1.6
Π	fiducial H-projector	1.6
Π	live fiducial (alternative name for fiducial H-projector)	1.12
$\mu_{\mathbf{p}}$	overlap	1.9
$\nu_{\mathbf{p}}$	normalized overlap	1.9
$\tilde{\Pi}$	ghost fiducial P-projector	1.11
$\tilde{\mu}_{\mathbf{p}}$	ghost overlap	1.11
$\tilde{\mu}_{\mathbf{p}}(t)$	candidate ghost overlap for admissible tuple t	1.11
$\tilde{\nu}_{\mathbf{p}}$	normalized ghost overlap	1.11
$\tilde{\nu}_{\mathbf{p}}(t)$	candidate normalized ghost overlap for admissible tuple t	1.32
G	twist	1.11
$\mathbb{H}$	upper half-plane	(1.17)
ϖ, ϖ_n	variant q-Pochhammer symbols	1.14
$\langle \mathbf{p}, \mathbf{q} \rangle$	symplectic form	(1.23)
$\langle\!\langle \mathbf{p}, \tau \rangle\!\rangle$	fractional symplectic form	(1.24)
$\eta(\tau)$	Dedekind η-function	(2.33)
$M \cdot \tau$, $j_M(\tau)$	fractional linear transformation and its denominator	(1.20)
$\mathcal{D}_M$	domain of τ in SF Jacobi and SF modular cocycles	1.15
$\Gamma(d)$, $\Gamma_{\mathbf{r}}$	principal congruence subgroup and a variant	1.17
$\sigma_M(z, \tau)$	SF Jacobi cocycle	1.16
$\mathfrak{w}_A^{\mathbf{r}}(\tau)$	SF modular cocycle	1.18
K, Δ_0	real quadratic field and its discriminant	(1.29)
Q	integral, primitive, irreducible, indefinite quadratic form	sec. 1.3
Q_M	M-transform of Q	(1.31)
Δ_0, f	fundamental discriminant and conductor of a form	(1.34)
$\rho_{Q,\pm}$	roots of Q	eq. (1.35)
ρ_t	root corresponding to admissible tuple t	1.32
$\mathrm{sgn}(Q)$, $\mathrm{sgn}(M)$	signs of Q, M	1.19
$\mathcal{S}(Q)$, $\mathcal{S}_d(Q)$	stability group of Q, and a variant	1.20
ε	fundamental totally positive unit > 1	1.22

Notation	Terminology	Definition
f_j	sequence of conductors of a real quadratic field	1.23
$d_{j,m}$, $r_{j,m}$	dimension and rank grids of a real quadratic field	1.24
(d, r)	admissible pair	1.21
d_j, d_1	dimension tower, root dimension of a real quadratic field	1.24
(K, j, m)	admissible triple	1.24
$(d, r) \sim (K, j, m)$	admissible tuple equivalence	1.26
$\Psi(M)$	Rademacher class invariant	1.29
(d, r, Q)	admissible tuple with form	1.27
(K, j, m, Q)	admissible tuple with form	1.27
L_t, $L_{+,t}$, $L_{\mathrm{z,t}}$, A_t	stabilizers associated to admissible tuple t	1.28
$\phi_{\mathbf{p}}(t)$	SF phase for admissible tuple t	1.30
$\delta^{(n)}_{\mathbf{p},\mathbf{q}}$	modular δ-function	1.33
λ, $\mathcal{Z}_t$	shift and set of shifts for admissible tuple t	1.34
–	Stark–Tate conjecture	conj. 2.8
–	Twisted convolution conjecture	conj. 1.35
E_t, $\hat{E}_t$	Field & Galois closed field associated to t	1.40
$\mathcal{O}_f$	order with conductor f	1.48
g	standard notation for a Galois automorphism	
$s = (d, r, Q, G, g)$	fiducial datum	1.41
$s = (K, j, m, Q, G, g)$	fiducial datum	1.41
$s = (t, G, g)$	fiducial datum extending admissible tuple t	1.41
$\tilde{\Pi}_s$	ghost P-projector for fiducial datum s	1.44
Π_s	r-SIC H-projector for fiducial datum s	1.44
$\nu_{\mathbf{p}}(s)$	candidate normalized overlap for fiducial datum s	1.44
$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$	ray class group	2.1
$\overrightarrow{\mathrm{Clm}}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O})$	flat imprimitive ray class monoid	2.3
$\overrightarrow{\mathrm{ZClm}}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O})$	submonoid of zero classes	2.3
$\mathfrak{A}$	ray class in $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ or $\overrightarrow{\mathrm{Clm}}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O})$	2.4
$\zeta_{\mathfrak{m},\Sigma}(s, \mathfrak{A})$	ray class partial zeta function	2.4
$Z_{\mathfrak{m},\Sigma}(s, \mathfrak{A})$	differenced ray class partial zeta function	2.4
$u_{\mathfrak{A}}$	Stark unit	Sec. 2.3
$\mathrm{C}(d)$, $\mathrm{EC}(d)$	Clifford and extended Clifford groups	3.2
$\mathrm{PC}(d)$, $\mathrm{PEC}(d)$	projective Clifford and extended Clifford groups	3.2
$\mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$	symplectic group	3.3
$\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$	extended symplectic group	3.3
F	symplectic and anti-symplectic matrices	3.3
J	canonical anti-symplectic matrix	3.3
U_F	symplectic unitary	(3.10)
k_g	integer describing action of Galois conjugation g	3.6
H_g	matrix describing action of Galois conjugation g	3.6
U_F	anti-symplectic anti-unitary	(3.24)
$\mathrm{EC}_0(d)$	(anti-)symplectic subgroup of $\mathrm{EC}(d)$	3.8
$\mathcal{S}(\Pi)$	symmetry group of fiducial Π	3.9
–	canonical order 3 unitary	3.11
F_z, F_a, F'_a	Zauner and variant Zauner matrices	3.12
–	type-z, type-a, type-a' fiducials	3.15

Notation	Terminology	Definition
–	centred fiducial	3.16
$\mathcal{S}_{\mathrm{ESL}}(\Pi)$	symplectic symmetry group of fiducial Π	3.17
$\mathcal{S}_{\mathrm{OL}}(\Pi)$	overlap symmetry group of fiducial Π	3.17
–	Galois multiplet	3.18
–	strongly centred fiducial	3.19
φ	fundamental unit of K	4.1
Δ_j	discriminant at level j	4.2
$T_j^*(x)$, $U_j^*(x)$	variant Chebyshev polynomials	4.8
$\mathcal{U}_f$	unit group of $\mathcal{O}_f$	4.12
$\mathcal{U}_f^+$	positive norm subgroup of $\mathcal{U}_f$	4.12
$j_{\min}(f)$	minimum level of conductor f	4.14
ε_f	smallest unit greater than 1 in $\mathcal{U}_f^+$	4.14
φ_f	smallest unit greater than 1 in $\mathcal{U}_f$	4.17
$\mathcal{M}(R)$	ring of 2×2 matrices over R	4.27
$\mathcal{M}_{\mathrm{S}}(R)$	sub ring of symmetric matrices in $\mathcal{M}(R)$	4.27
$\mathcal{M}_0(R)$	sub ring of trace-zero matrices in $\mathcal{M}(R)$	4.27
$R\langle M_1, \ldots, M_n\rangle$	matrix sub-algebra generated by $M_1 \ldots, M_n$	4.28
S, T	generators of $\mathrm{SL}_2(\mathbb{Z})$	4.29
χ	canonical representation of field K	4.31
χ_Q	canonical representation of K associated to Q	4.33
$Q(M)$	form stabilized by M	thm. 4.39
$\mathcal{H}_+$	$M \in \mathrm{GL}_2(\mathbb{Z}) \setminus \{\pm I\}$ such that $(\mathrm{Tr}\, M)^2 - 4 \det M > 4$	4.43
$\mathcal{H}_-$	$M \in \mathrm{GL}_2(\mathbb{Z}) \setminus \{\pm I\}$ such that $(\mathrm{Tr}\, M)^2 - 4 \det M \leq 4$	4.43
$\mathcal{F}_+$	invariant, irreducible forms	4.43
$\mathcal{F}_-$	forms with discriminant $-4, -3, 0, 1$, or 4	4.43
n_t	level of admissible tuple t	4.52
Φ_t	function from $\mathbb{Z}/(d\mathbb{Z})$ to $\mathbb{Z}/(\bar{d}\mathbb{Z})$	5.10
$E_s^{(1)}$, $E_t^{(2)}$	Subfields of E_t generated by (ghost) overlaps	6.1
t_M	M-transformed admissible tuple	7.2
$t \sim t'$	equivalence of admissible tuples t and t'	7.2
s_M	M-transformed fiducial datum	7.2
π_s	homomorphism of $\mathrm{GL}_2(\mathbb{Z})$ onto $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$	7.3
$[t]$	equivalence class of tuples specifying an $\mathrm{EC}(d)$ orbit	7.11
$[\![t]\!]$	equivalence class of tuples specifying a Galois multiplet	7.11
H_t, $H_{K,f}$	ring class field for admissible tuple t	7.13
h_t, $h_{K,f}$	class number for admissible tuple t	7.13
$H_{[\![t]\!]}$	ring class field for equivalence class $[\![t]\!]$	7.13
$h_{[\![t]\!]}$	class number for equivalence class $[\![t]\!]$	7.13
R_s, $R_{+,s}$, $R_{\mathrm{z,s}}$	elements of overlap stabilizer group associated to s	7.17
–	tuples of unitary/anti-unitary type	7.18
–	canonical expansion	C.5
–	length of canonical expansion	C.5

2. Shintani–Faddeev cocycles and the Stark conjectures

This section summarizes some of the algebraic properties of the Shintani–Faddeev modular cocycle established in [70] as well as its relationship to the Stark conjectures, after first providing some necessary background. Proofs of theorems not proven here may be found in [71] and [70]. This section assumes some familiarity with algebraic number theory; for a standard text on the subject, see [81], or see [78] for a more elementary exposition.

2.1. Class field theory (for orders of number fields).

For a number field K, it is natural to ask for a characterization of the set of abelian Galois extensions

$$\{H/K : H \text{ is a number field and } \mathrm{Gal}(H/K) \text{ is abelian}\}. \tag{2.1}$$

Such fields are characterized abstractly by class field theory. Class field theory realizes every abelian extension of K as a subfield of a *ray class field*; ray class fields, proven to exist by Takagi, are parameterized by data intrinsic to the base field K.

It suits our purposes to give a broader definition of *ray class field* than is typical. Takagi's ray class fields are attached to the data of a *modulus*, which is a pair $(\mathfrak{m}, \Sigma)$ such that $\mathfrak{m}$ is a nonzero ideal of the ring of integers $\mathcal{O}_K$ and Σ is a subset of the set of *real embeddings* of K (that is, injective ring homomorphisms $K \to \mathbb{R}$). More general ray class field are used here in the sense defined by Kopp and Lagarias [71]. Each is attached to a *level datum*, which is a triple $(\mathcal{O}; \mathfrak{m}, \Sigma)$ such that $\mathcal{O}$ is an order[4] in the number field K, $\mathfrak{m}$ an ideal of $\mathcal{O}$, and Σ a subset of the set of real embeddings of K.

A level datum is used directly to define the *ray class group*, a finite abelian group, which will by the main theorems of class field theory be isomorphic to the Galois group over K of the corresponding ray class field. The definition of the ray class group uses *fractional ideals*, which may be defined for an order $\mathcal{O}$ in a number field K equivalently as either:

(1) a *fractional ideal* $\mathfrak{a}$ of $\mathcal{O}$ is a finitely-generated $\mathcal{O}$-submodule of K;
(2) a *fractional ideal* $\mathfrak{a}$ is an additive subgroup of K with the property that there is some $n \in \mathbb{N}$ such that $n\mathfrak{a}$ is an ideal of $\mathcal{O}$.

Ideals of $\mathcal{O}$ will be called *integral ideals* to distinguish them from more general fractional ideals. Fractional ideals may be multiplied together to give new fractional ideals, using the multiplication

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^{k} a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, k \in \mathbb{N} \right\}. \tag{2.2}$$

Nonzero fractional ideals form a group $\mathrm{J}^*(\mathcal{O})$.

The ray class group is defined as a quotient of a subgroup of $\mathrm{J}^*(\mathcal{O})$ by a smaller subgroup, so its elements are cosets consisting of fractional ideals. The following definition, given as [71, Defn. 5.4], generalizes the standard one by introducing a dependence on $\mathcal{O}$.

Definition 2.1 (Ray class group)**.** Let K be a number field and $(\mathcal{O}; \mathfrak{m}, \Sigma)$ be a level datum for K. The *ray class group of the order $\mathcal{O}$ modulo* $(\mathfrak{m}, \Sigma)$ is

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})}, \tag{2.3}$$

where

$$\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O}) = \{\text{invertible fractional ideals of } \mathcal{O} \text{ coprime to } \mathfrak{m}\}, \text{ and} \tag{2.4}$$

[4] An order $\mathcal{O}$ in a number field K is a subring of K having rank $[K : \mathbb{Q}]$ as an abelian group.

$$\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \{\alpha\mathcal{O} \text{ such that } \alpha \equiv 1 \pmod{\mathfrak{m}} \text{ and } \sigma(\alpha) > 0 \text{ for } \sigma \in \Sigma\}. \tag{2.5}$$

If the real embeddings of K are labelled $\sigma_1, \ldots, \sigma_r$ and $\Sigma = \{\sigma_{j_1}, \ldots, \sigma_{j_k}\}$, the pair $(\mathfrak{m}, \Sigma)$ may be abbreviated as $\mathfrak{m}\infty_{j_1} \cdots \infty_{j_k}$.

It is worth highlighting the meanings of the terms "invertible" and "coprime" in the above definition, as they involve features that do not appear in the maximal order case. A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is *invertible* if there is some fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$. (The order $\mathcal{O} = \mathcal{O}_K$ if and only if all nonzero ideals are invertible.) The fractional ideal $\mathfrak{a}$ is *coprime* to the integral ideal $\mathfrak{m}$ if it can be written as $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2^{-1}$ for an integral $\mathcal{O}$-ideal $\mathfrak{a}_1$ and an invertible integral $\mathcal{O}$-ideal $\mathfrak{a}_2$ satisfying $\mathfrak{a}_1 + \mathfrak{m} = \mathfrak{a}_2 + \mathfrak{m} = \mathcal{O}$. (Ideals of non-maximal orders do not always have prime factorizations.)

The following theorem defines ray class fields uniquely and asserts their existence. It is stated as [70, Thm. 3.4] and is a summary of [71, Thm. 1.1, Thm. 1.2, Thm. 1.3].

Theorem 2.2. *Let K be a number field and $(\mathcal{O}; \mathfrak{m}, \Sigma)$ be a level datum for K. Then there exists a unique abelian Galois extension $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K$ with the property that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that is coprime to the quotient ideal $(\mathfrak{m} : \mathcal{O}_K)$ splits completely in $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K$ if and only if $\mathfrak{p} \cap \mathcal{O} = \pi\mathcal{O}$, a principal prime $\mathcal{O}$-ideal having $\pi \in \mathcal{O}$ with $\pi \equiv 1 \pmod{\mathfrak{m}}$ and $\sigma(\pi) > 0$ for $\sigma \in \Sigma$.*

Additionally, these fields have the following properties:

- $H^{\mathcal{O}_K}_{\mathfrak{m}\mathcal{O}_K,\Sigma} \subseteq H^{\mathcal{O}}_{\mathfrak{m},\Sigma} \subseteq H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$.
- *There is a canonical isomorphism* $\mathrm{Art}_{\mathcal{O}} : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Gal}\big(H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K\big)$.

Another formal structure, the *flat imprimitive ray class monoid*, will be needed to define generalized zeta values that ultimately give rise to ghost r-SIC overlaps (by way of the $\mathfrak{w}$-function). This finite commutative monoid[5] contains the ray class group as a submonoid and is defined by weakening the "coprime to $\mathfrak{m}$" condition in Definition 2.1 and making other modifications. Further discussion and properties are given in [73, Sec. 4] and [70, Sec. 3.2].

Definition 2.3. The *flat imprimitive ray class monoid* is

$$\overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\overline{\mathrm{J}}^{\flat}_{\mathfrak{m}}(\mathcal{O})}{\sim_{\mathfrak{m},\Sigma}}, \tag{2.6}$$

where

$$\overline{\mathrm{J}}^{\flat}_{\mathfrak{m}}(\mathcal{O}) = \{\mathfrak{a} \in \mathrm{J}^*_{\mathcal{O}}(\mathcal{O}) : \mathfrak{a}\mathcal{O}[S_{\mathfrak{m}}^{-1}] \subseteq \mathcal{O}[S_{\mathfrak{m}}^{-1}]\} \text{ with} \tag{2.7}$$

$$S_{\mathfrak{m}} = \{\alpha \in \mathcal{O} : \alpha\mathcal{O} + \mathfrak{m} = \mathcal{O}\}, \tag{2.8}$$

and the equivalence relation $\sim_{\mathfrak{m},\Sigma}$ is defined by

$$\mathfrak{a} \sim_{\mathfrak{m},\Sigma} \mathfrak{b} \iff \begin{array}{l} \exists \mathfrak{c} \in \overline{\mathrm{J}}^{\flat}_{\mathfrak{m}}(\mathcal{O}) \text{ and } \alpha, \beta \in \mathcal{O}[S_{\mathfrak{m}}^{-1}] \text{ such that } \mathfrak{a} = \alpha\mathfrak{c}, \mathfrak{b} = \beta\mathfrak{c}, \\ \alpha - \beta \in \mathfrak{m}\mathcal{O}[S_{\mathfrak{m}}^{-1}], \mathrm{sgn}(\sigma(\alpha)) = \mathrm{sgn}(\sigma(\beta)) \text{ for all } \sigma \in \Sigma. \end{array} \tag{2.9}$$

The *submonoid of zero classes* is

$$\overline{\mathrm{ZClm}}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \{[\mathfrak{d}] \in \overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O}) : \mathfrak{d} \subseteq \mathfrak{m}\}. \tag{2.10}$$

[5] A monoid is a semigroup with identity, that is, a set with a binary operation satisfying associativity and having an identity element.

2.2. **Partial zeta functions.** The Stark conjectures relate the value at $s = 0$ of certain zeta functions to algebraic units in certain number fields. The zeta functions are *partial zeta functions*, meaning that they are defined by an infinite sum corresponding to "part" of a Dirichlet series used to define another zeta function. The Dedekind zeta function is written as a finite sum of partial zeta functions. Those partial zeta functions may be indexed either by ray classes in a ray class group (and more generally a ray class monoid) or by field automorphisms in a finite Galois extension.

In the simplest case, the Dedekind zeta function of $\mathbb{Q}$ is the Riemann zeta function

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} n^{-s}, \qquad \mathrm{Re}(s) > 1. \tag{2.11}$$

For any positive integer d, the Riemann zeta function may be written as a finite sum of Hurwitz zeta functions

$$\zeta_{\mathbb{Q}}(s) = \sum_{k=1}^{d} d^{-s}\zeta(s, \tfrac{k}{d}), \tag{2.12}$$

where the Hurwitz zeta function is defined as

$$\zeta(s, a) = \sum_{n=0}^{\infty}(n + a)^{-s}, \qquad \mathrm{Re}(s) > 1. \tag{2.13}$$

The Hurwitz zeta function may be understood as a partial zeta function associated to the congruence class of $k \pmod d$. Such k may be thought of as classes in a flat imprimitive ray class monoid,

$$\overrightarrow{\mathrm{Clm}}^{\flat}_{d\infty}(\mathbb{Z}) = \frac{\{r\mathbb{Z} : r = \frac{a}{b} \in \mathbb{Q}^{\times}, \gcd(b, d) = 1\}}{\left(r_1\mathbb{Z} \sim r_2\mathbb{Z} \text{ if } r_i = \pm\frac{\gamma_i c}{\delta_i d},\ \frac{\gamma_1}{\delta_1} - \frac{\gamma_2}{\delta_2} = \frac{\gamma_3}{\delta_3},\ m|\delta_3,\ \mathrm{sgn}(\frac{\gamma_1}{\delta_1}) = \mathrm{sgn}(\frac{\gamma_2}{\delta_2})\right)} \tag{2.14}$$

$$\cong (\mathbb{Z}/d\mathbb{Z}, \times), \tag{2.15}$$

where we stipulate that all fractions in (2.14) are in simplest form, and the notation in (2.15) indicates the set $\mathbb{Z}/d\mathbb{Z}$ thought of as a monoid with the binary operation of multiplication. When k is coprime to d, it may be thought of as either a class in the ray class group

$$\mathrm{Cl}_{d\infty}(\mathbb{Q}) = \frac{\{r\mathbb{Z} : r = \frac{a}{b} \in \mathbb{Q}^{\times}, \gcd(a, d) = \gcd(b, d) = 1\}}{\{r\mathbb{Z} : r = \frac{a}{b} \in \mathbb{Q}^{\times},\ \gcd(a, d) = \gcd(b, d) = 1,\ a \equiv b \pmod d,\ r > 0\}} \tag{2.16}$$

$$\cong (\mathbb{Z}/d\mathbb{Z})^{\times} \tag{2.17}$$

or to an element of the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\omega_d)/\mathbb{Q}) = \{\text{field automorphisms } g : \mathbb{Q}(\omega_d) \to \mathbb{Q}(\omega_d)\} \tag{2.18}$$

$$\cong (\mathbb{Z}/d\mathbb{Z})^{\times}. \tag{2.19}$$

The restriction that k is coprime to d is no great obstacle, as (2.12) may be rewritten as

$$\zeta_{\mathbb{Q}}(s) = \left(\prod_{\substack{p|d \\ p \text{ prime}}} (1 - p^{-s})^{-1}\right) \sum_{\substack{1\le k\le d \\ \gcd(k,d)=1}} d^{-s}\zeta(s, \tfrac{k}{d}). \tag{2.20}$$

The Dedekind zeta function

$$\zeta_K(s) = \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \mathrm{Nm}(\mathfrak{a})^{-s} \tag{2.21}$$

which generalizes the Riemann zeta function, can likewise be split up as a sum of finitely many ray class partial zeta functions.

Definition 2.4 (Ray class partial zeta function and differenced ray class partial zeta function)**.** Let K be a number field and $(\mathcal{O}; \mathfrak{m}, \Sigma)$ a level datum for K. Let $\mathfrak{A} \in \overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O})$, and let $\mathfrak{R}$ be the element of $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ defined by

$$\mathfrak{R} := \{\alpha\mathcal{O} : \alpha \equiv -1 \pmod{\mathfrak{m}} \text{ and } \sigma(\alpha) > 0 \text{ for all } \sigma \in \Sigma\}. \tag{2.22}$$

For $\mathrm{Re}(s) > 1$, define the *ray class partial zeta function* and the *differenced ray class partial zeta function*, respectively, by

$$\zeta_{\mathfrak{m},\Sigma}(s, \mathfrak{A}) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O} \\ \mathfrak{a} \in \mathfrak{A}}} \mathrm{Nm}(\mathfrak{a})^{-s}, \text{ and} \tag{2.23}$$

$$Z_{\mathfrak{m},\Sigma}(s, \mathfrak{A}) = \zeta_{\mathfrak{m},\Sigma}(s, \mathfrak{A}) - \zeta_{\mathfrak{m},\Sigma}(s, \mathfrak{R}\mathfrak{A}). \tag{2.24}$$

Ray class partial zeta functions are closely related (by Artin reciprocity) to partial zeta functions indexed by elements of a Galois group. We introduce different terminology and notation for Galois-thoeretic partial zeta functions, which are not always identical to ray class partial zeta functions, as they impose stricter coprimality conditions on the ideals indexing the summands.

Definition 2.5 (Galois-theoretic partial zeta function)**.** Let H/K be an abelian Galois extension of number fields. Let S be a finite set of places of K containing all the places that ramify in H as well as all the infinite places of K, and let $S = S_{\mathrm{fin}} \sqcup S_\infty$ for a set of finite places S_{fin} and a set of infinite places S_∞. For any $g \in \mathrm{Gal}(H/K)$ and $\mathrm{Re}(s) > 1$, define

$$\zeta_S^{\mathrm{Gal}}(g, s) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ (\forall \mathfrak{p} \in S_{\mathrm{fin}})\mathfrak{a}+\mathfrak{p}=\mathcal{O}_K \\ \mathrm{Art}([\mathfrak{a}])=g}} \mathrm{Nm}(\mathfrak{a})^{-s}, \tag{2.25}$$

where $\mathrm{Art} = \mathrm{Art}_{\mathcal{O}_K}$ is the Artin map of class field theory.

In the case when $\mathcal{O} = \mathcal{O}_K$ is the maximal order, each ray class partial zeta functions is equal to some Galois-theoretic partial zeta function times a factor of the form $\mathrm{Nm}(\mathfrak{d})^{-s}$, by [70, Prop. 6.2 and Thm. 6.7]. See [70, Sec. 6] for further results and discussion.

Often considered more fundamental that partial zeta functions are finite-order Hecke L-functions (associated to characters of a ray class group) and Artin L-functions (associated to characters, or more generally representations, of a Galois group). These L-functions have Euler products and are expected to satisfy the Riemann hypothesis. For abelian Galois extensions, Hecke and Artin L-functions are equal up to a finite number of Euler factors. One can state the Stark conjectures in terms of Hecke or Artin L-functions [105], but the formulas are more complicated. We stick to partial zeta functions here, as they are most closely linked to the Stark units.

2.3. **The Stark conjectures.** We will need a special case of Tate's refinement [105] of Stark's order 1 abelian L-values conjectures [97–101]. We first state Tate's refinement in general. The following statement is part (II)(a) of [105, Conj. 4.2] and is equivalent to the full statement of that conjecture. Tate notates this conjecture $\mathrm{St}(S, K/k)$, with his k taking the role of our K, and his K taking the role of our H.

Conjecture 2.6 (Stark–Tate Conjecture $\mathrm{ST}(H/K, S)$, general case)**.** *Let H/K be an abelian extension of number fields, and let W be the number of roots of unity in H. Let S be a finite set*

of places of K containing all the places that ramify in H as well as all the infinite places of K, satisfying $|S| \geq 2$. Suppose that S contains a place $\mathfrak{p}$ (finite or infinite) that splits completely in K, and let $T = S \setminus \{\mathfrak{p}\}$. Let $U_{S,H}^T$ denote the set of elements $\alpha \in H^\times$ such that its $\mathfrak{Q}$-adic valuations at places $\mathfrak{Q}$ of H satisfy

$$|\alpha|_{\mathfrak{Q}} = 1 \text{ for } \mathfrak{Q}|\mathfrak{q} \notin S, \tag{2.26}$$

$$|\alpha|_{\mathfrak{Q}} = 1 \text{ for } \mathfrak{Q}|\mathfrak{q} \in T, \qquad \text{if } |T| \geq 2, \text{ and} \tag{2.27}$$

$$|\alpha|_{\mathfrak{Q}} = a \text{ for } \mathfrak{Q}|\mathfrak{q} \text{ and } a \text{ constant}, \qquad \text{if } T = \{\mathfrak{q}\}. \tag{2.28}$$

Then, there is an element $u \in U_{S,H}^T$ such that

$$\log |g(u)|_{\mathfrak{P}} = -W\zeta_S'(g,0) \text{ for each } g \in \mathrm{Gal}(H/K) \text{ and } \mathfrak{P}|\mathfrak{p} \tag{2.29}$$

and such that $H(u^{1/W})$ is abelian over K.

We now state specialized consequences of the above conjecture in the case of interest to this paper. From now on, the field K will be real quadratic, and it will be considered to be a subfield of $\mathbb{R}$. The two real embeddings are $\sigma_1(x) = x$ and $\sigma_2(x) = x'$, where x' is the nontrivial Galois conjugate of x. We will also specialize the extension H to be a ray class field and state the conjecture in terms of ray class partial zeta functions. We state two versions, with the first being provable from conjectures in Stark's 1976 paper [99, Conj. 1 and Conj. 2], and the second containing the condition on the square root appearing in Tate's work [105].

Conjecture 2.7 (Stark Conjecture $\mathrm{S}(K,\mathfrak{m})$, real quadratic Archimedean ray class field case)**.** *Let $K \subset \mathbb{R}$ be a real quadratic number field embedded in $\mathbb{R}$, and let $\mathfrak{m}$ be a nonzero integral $\mathcal{O}_K$-ideal such that $\mathfrak{m} \neq \mathcal{O}_K$. Let $H = H_{\mathfrak{m}\infty_2}^{\mathcal{O}_K} \subset \mathbb{R}$. Then, for all $\mathfrak{A} \in \mathrm{Cl}_{\mathfrak{m}\infty_2}(\mathcal{O}_K)$, there are elements $u_{\mathfrak{A}} \in \mathcal{O}_H^\times$ such that*

$$u_{\mathfrak{A}} = \exp\left(-2\zeta_{\mathfrak{m}\infty_2}'(0,\mathfrak{A})\right), \tag{2.30}$$

$(\mathrm{Art}(\mathfrak{B}))(u_{\mathfrak{A}}) = u_{\mathfrak{A}\mathfrak{B}}$ *for $\mathfrak{B} \in \mathrm{Cl}_{\mathfrak{m}\infty_2}(\mathcal{O}_K)$, $|g(u_{\mathfrak{A}})| = 1$ for any $g \in \mathrm{Gal}(H/\mathbb{Q}) \setminus \mathrm{Gal}(H/K)$.*

Conjecture 2.8 (Stark–Tate Conjecture $\mathrm{ST}(K,\mathfrak{m})$, real quadratic Archimedean ray class field case)**.** *Let $K \subset \mathbb{R}$ be a real quadratic number field embedded in $\mathbb{R}$, and let $\mathfrak{m}$ be a nonzero integral $\mathcal{O}_K$-ideal such that $\mathfrak{m} \neq \mathcal{O}_K$. Then, $\mathrm{S}(K,\mathfrak{m})$ holds, and for all $\mathfrak{A} \in \mathrm{Cl}_{\mathfrak{m}\infty_2}(\mathcal{O}_K)$, the field $H(u_{\mathfrak{A}}^{1/2})$ is abelian over K.*

We also state a Stark-type conjecture for differenced ray class partial zeta functions attached to potentially imprimitive ray classes. This "Monoid Stark Conjecture" is not known to follow completely from the Stark (or Stark–Tate) conjectures, but it does follow in the case of the maximal order $\mathcal{O} = \mathcal{O}_K$.

Conjecture 2.9 (Monoid Stark Conjecture $\mathrm{MS}(\mathcal{O},\mathfrak{m})$)**.** *Let $K \subset \mathbb{R}$ be a real quadratic field, $\mathcal{O}$ an order in K, and $\mathfrak{m}$ a nonzero $\mathcal{O}$-ideal such that $\mathfrak{m} \neq \mathcal{O}$. Let $\{\infty_1, \infty_2\}$ be the two real places of K. Let $H = H_{\mathfrak{m}\infty_2}^{\mathcal{O}} \subset \mathbb{R}$. Then, for all $\mathfrak{A} \in \overline{\mathrm{Clm}}_{\mathfrak{m}\infty_2}^{\flat}(\mathcal{O})$, there are elements $u_{\mathfrak{A}} \in \mathcal{O}_H^\times$ such that*

$$u_{\mathfrak{A}} = \exp\left(-Z_{\mathfrak{m}\infty_2}'(0,\mathfrak{A})\right), \tag{2.31}$$

$(\mathrm{Art}(\mathfrak{B}))(u_{\mathfrak{A}}) = u_{\mathfrak{A}\mathfrak{B}}$ *for $\mathfrak{B} \in \mathrm{Cl}_{\mathfrak{m}\infty_2}(\mathcal{O})$, $|g(u_{\mathfrak{A}})| = 1$ for any $g \in \mathrm{Gal}(H/\mathbb{Q}) \setminus \mathrm{Gal}(H/K)$, and $H(u_{\mathfrak{A}}^{1/2})$ is abelian over K.*

Proposition 2.10. *We describe some nontrivial conditional implications between these Stark-type conjectures. Let $K \subset \mathbb{R}$ be a real quadratic field. Let $H = H_{\mathfrak{m},\Sigma}^{\mathcal{O}_K}$ for a modulus $(\mathfrak{m},\Sigma)$ for K. Let $S = \{\mathfrak{p}$ finite prime of $\mathcal{O}_K : \mathfrak{p}|\mathfrak{m}\} \cup \{\infty_1, \infty_2\}$.*

(1) $\mathrm{ST}(K, \mathfrak{m})$ *is equivalent to* $\mathrm{ST}(H/K, S)$.
(2) $\mathrm{MS}(\mathcal{O}_K, \mathfrak{m})$ *is equivalent to* $(\forall \mathfrak{m}' | \mathfrak{m})\, \mathrm{ST}(S, \mathfrak{m}')$.

Proof. Claim (1) is shown in [70, Prop. 6.10]. Claim (2) may be seen to follow from the proof of [70, Prop. 6.11]. □

The units $g(u)$ in Conjecture 2.6 and the units $u_{\mathfrak{A}}$ in Conjecture 2.7, Conjecture 2.8, and Conjecture 2.9 (at least for $\mathcal{O} = \mathcal{O}_K$) are generally called "Stark units" and are equal when the conjectures align, except in some trivial cases. Stark's original formulation of his conjecture in the rank 1 totally real case involved differenced ray class partial zeta functions (albeit only for primitive ray classes of the maximal order), denoted as $\zeta(s, \mathfrak{c})$ in [99], whereas most modern references follow Tate and state Stark's conjectures using Galois groups. We call the units $u_{\mathfrak{A}}$ *Stark units* (for $\mathcal{O} = \mathcal{O}_K$) or *generalized Stark units* (for non-maximal orders), without further comment.

2.4. **Eta-multipliers and theta-multipliers.** The relation between zeta functions and the Shintani–Faddeev modular cocycle involves a nontrivial root of unity factor that is best described as a value of a character $\psi^{-2}\chi_{\mathbf{r}}^{-1}$ at an element of congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, with the characters ψ and χ arising from multipliers of half-integral weight modular forms. We describe these characters here in terms of their relationships to modular forms.

Half-integral weight modular forms are best understood as modular forms for the *metaplectic group*, which is a double cover of SL_2. The real metaplectic group is defined to be

$$\mathrm{Mp}_2(\mathbb{R}) = \{(M, \epsilon) : M \in \mathrm{SL}_2(\mathbb{R}), \epsilon \text{ a continuous function on } \mathbb{H} \text{ with } \epsilon(\tau)^2 = j_M(\tau)\}, \quad (2.32)$$

having multiplication $(M_1, \epsilon_1)(M_2, \epsilon_2) = (M_1 M_2, \epsilon_3)$ with $\epsilon_3(\tau) = \epsilon_1(M_2 \cdot \tau)\epsilon_2(\tau)$. The integer metaplectic group is defined to be $\mathrm{Mp}_2(\mathbb{Z}) = \{(M, \epsilon) \in \mathrm{Mp}_2(\mathbb{R}) : M \in \mathrm{SL}_2(\mathbb{Z})\}$.

The *Dedekind eta function* is the function

$$\eta(\tau) = \prod_{k=1}^{\infty}(1 - e^{2\pi i k\tau}) \quad (2.33)$$

defined for $\tau \in \mathbb{H}$. For $M \in \mathrm{SL}_2(\mathbb{Z})$, it transforms under the fractional linear transformation $\tau \mapsto M \cdot \tau$ according to the equation

$$\eta(M \cdot \tau) = \psi(M, \epsilon)\epsilon(\tau)\eta(\tau), \quad (2.34)$$

where $(M, \epsilon) \in \mathrm{Mp}_2(\mathbb{Z})$.

An explicit formula for ψ is given by [70, Thm. 2.4]. Another explicit formula, in terms of the Rademacher function, is given as Proposition 5.2.

The *Jacobi theta function with characteristics* $\mathbf{r} = \left(\begin{smallmatrix} r_1 \\ r_2 \end{smallmatrix}\right) \in \mathbb{Q}^2$ is

$$\theta_{\mathbf{r}}(\tau) = \sum_{n=-\infty}^{\infty} e^{2\pi i\left(\frac{1}{2}\left(n+r_2+\frac{1}{2}\right)^2\tau+\left(n+r_2+\frac{1}{2}\right)\left(-r_1+\frac{1}{2}\right)\right)}. \quad (2.35)$$

Under the fractional linear transformation action of $(M, \epsilon) \in \mathrm{Mp}_2(\mathbb{Z})$ such that $M \in \Gamma_{\mathbf{r}}$, this theta function transforms by

$$\theta_{\mathbf{r}}(M \cdot \tau) = \psi(M, \epsilon)^3\, \chi_{\mathbf{r}}()\epsilon(\tau)\theta_{\mathbf{r}}(\tau). \quad (2.36)$$

The character $\chi_{\mathbf{r}} : \Gamma_{\mathbf{r}} \to \mathbb{C}^\times$ is given by the formula

$$\chi_{\mathbf{r}}(M) := (-1)^{1+\delta^{(2)}_{M\mathbf{r},\mathbf{r}}} e^{-\pi i\langle M\mathbf{r},\mathbf{r}\rangle}, \quad (2.37)$$

where $\delta^{(2)}_{M\mathbf{r},\mathbf{r}}$ is defined by Definition 1.33. For proofs of (2.36) and (2.36), see [70, Thm. 2.14 and Lem. 2.15].

In the sequel, we will often want to specify a standard choice of square root of $j_M(\tau)$ rather than using the metaplectic group. Define the choice of logarithm $(\log j_M)(\tau) := \log(j_M(\tau))$ according to the principal branch of the logarithm, with $\log(1) = 0$ and a branch cut along the negative real axis, along with the additional values $(\log j_M)(\tau) = \log|j_M(\tau)| + \pi i$ when $j_M(\tau)$ is on the negative real axis. Define the principal branch of the square root by $\sqrt{j_M(\tau)} := \exp\left(\frac{1}{2}(\log j_M)(\tau)\right)$.

This characters ψ and $\chi_{\mathbf{r}}$ are closely related to the SF phase $\phi_t(\mathbf{p})$, as defined in Definition 1.30. The exact relationship is proven in Section 5.1 and Section 5.2.

2.5. **The functional equations of the Shintani–Faddeev modular cocycle.** We now present several key identities satisfied by the Shintani–Faddeev modular cocycle $\boldsymbol{\omega}_M^{\mathbf{r}}(\tau)$, as defined in Definition 1.18. Most of these results are proven in [70].

The function $\boldsymbol{\omega}_M^{\mathbf{r}}(\tau)$ satisfies a particular symmetry under the involution $\mathbf{r} \mapsto -\mathbf{r}$. This symmetry derives from the modular properties of $\theta_{\mathbf{r}}(\tau)$ and $\eta(\tau)$ together with the Jacobi triple product identity.

Theorem 2.11. *Let $\mathbf{r} \in \mathbb{Q}^2$, $A \in \Gamma_{\mathbf{r}}$, and $\tau \in \mathcal{D}_A$. We have the identity*

$$\boldsymbol{\omega}_A^{\mathbf{r}}(\tau)\,\boldsymbol{\omega}_A^{-\mathbf{r}}(\tau) = \psi^2(M)\chi_{\mathbf{r}}(M)\, e^{2\pi i\left(\frac{r_2^2}{2}+\frac{1}{12}\right)(\tau - M\cdot\tau)} \cdot \frac{e^{\pi i(r_2(M\cdot\tau)-r_1)} - e^{\pi i(-r_2(M\cdot\tau)+r_1)}}{e^{\pi i(r_2\tau - r_1)} - e^{\pi i(-r_2\tau + r_1)}}. \tag{2.38}$$

Proof. See [70, Thm. 4.32]. □

An important special case is when τ is a fixed point of M under the fractional linear transformation, in which case the above transformation identity reduces to the following.

Corollary 2.12. *When $\tau = \rho$ satisfying $M \cdot \rho = \rho$, (2.38) reduces to*

$$\boldsymbol{\omega}_A^{\mathbf{r}}(\rho)\,\boldsymbol{\omega}_A^{-\mathbf{r}}(\rho) = \psi^2(M)\chi_{\mathbf{r}}(M). \tag{2.39}$$

Lemma 2.13. *For all $\mathbf{r} \in \mathbb{Q}^2$, $M \in \Gamma_{\mathbf{r}}$, and $\tau \in \mathcal{D}_{M^{-1}}$,*

$$\boldsymbol{\omega}_{M^{-1}}^{\mathbf{r}}(\tau)\,\boldsymbol{\omega}_M^{\mathbf{r}}\left(M^{-1}\tau\right) = 1. \tag{2.40}$$

Proof. Write the identity matrix $I = M^{-1}M$. The cocycle relation implies that

$$\boldsymbol{\omega}_I^{\mathbf{r}}(\tau) = \boldsymbol{\omega}_{M^{-1}}^{\mathbf{r}}(\tau)\,\boldsymbol{\omega}_M^{\mathbf{r}}\left(M^{-1}\cdot\tau\right). \tag{2.41}$$

Moreover, $\boldsymbol{\omega}_I^{\mathbf{r}}(\tau) = 1$, proving (2.40). □

We also give some further properties and identities that are useful. Recall that the function j_M was defined by $j_M(\tau) = \gamma\tau + \delta$ for $M = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$.

Lemma 2.14. *Let $\mathbf{r} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, $M \in \Gamma_{\mathbf{r}}$, and $\rho \in \mathcal{D}_M$ either of the fixed points of M. For all $\mathbf{s} \in \mathbb{Z}^2$,*

$$\boldsymbol{\omega}_M^{\mathbf{r}+\mathbf{s}}(\rho) = \boldsymbol{\omega}_M^{\mathbf{r}}(\rho). \tag{2.42}$$

Proof. See [70, Prop. 4.35]. □

Lemma 2.15. *Let ρ be either of the fixed points of $M \in \Gamma(d)$. Then*

$$\boldsymbol{\omega}_M^{\mathbf{r}}(\rho) = \begin{cases} \psi(M, \sqrt{j_M})\sqrt{j_M(\rho)} & \text{if } r_2 > 0, \\ \dfrac{\psi(M,\sqrt{j_M})}{\sqrt{j_M(\rho)}} & \text{if } r_2 \le 0, \end{cases} \tag{2.43}$$

with $\sqrt{j_M}$ denoting the standard branch, for all $\mathbf{r} = \left(\begin{smallmatrix} r_1 \\ r_2\end{smallmatrix}\right) \in \mathbb{Z}^2$.

Proof. See [70, Thm. 4.38]. □

Finally, we give some elementary properties of the function j_M and of the domains $\mathcal{D}_M$ that we will want to use frequently.

Lemma 2.16. *For all $M, N \in \mathrm{GL}_2(\mathbb{Z})$ and $\tau \in \mathbb{C}$,*

$$j_{MN}(\tau) = j_M(N \cdot \tau) j_N(\tau). \tag{2.44}$$

For all $M \in \mathrm{GL}_2(\mathbb{Z})$ and $\tau \in \mathbb{C}$,

$$j_M(M^{-1} \cdot \tau) = \frac{1}{j_{M^{-1}}(\tau)}. \tag{2.45}$$

Proof. Straightfoward consequences of the definition. □

Lemma 2.17. *For all $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$*

$$\mathcal{D}_{M^{-1}} = M \cdot \mathcal{D}_M, \tag{2.46}$$

$$\mathcal{D}_{JM} = -\mathcal{D}_{MJ} = \mathcal{D}_M \tag{2.47}$$

$$\mathcal{D}_M \cup \mathcal{D}_{-M} = \begin{cases} \mathbb{C} & \gamma = 0, \\ \mathbb{C} \setminus \{-\delta/\gamma\} & \gamma \neq 0, \end{cases} \tag{2.48}$$

$$\mathcal{D}_M \cap \mathcal{D}_{-M} = \mathbb{C} \setminus \mathbb{R}. \tag{2.49}$$

where

$$J = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \tag{2.50}$$

Proof. Straightforward consequences of the definition. □

Lemma 2.18. *Let $\rho \in \mathbb{R}$ be a fixed point of $M \in \mathrm{SL}_2(\mathbb{Z})$. Then $\rho \in \mathcal{D}_M$ if and only if $\mathrm{Tr}(M) > 0$.*

Proof. Write $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. We have $M \left(\begin{smallmatrix} \rho \\ 1 \end{smallmatrix}\right) = (\gamma\rho + \delta) \left(\begin{smallmatrix} M \cdot \rho \\ 1 \end{smallmatrix}\right) = (\gamma\rho + \delta) \left(\begin{smallmatrix} \rho \\ 1 \end{smallmatrix}\right)$ because ρ is a fixed point of M. Thus, $\gamma\rho + \delta$ is an eigenvalue of M. Hence,

$$\rho \in \mathcal{D}_M \iff \gamma\rho + \delta > 0 \iff M \text{ has a positive eigenvalue} \iff \mathrm{Tr}(M) > 0, \tag{2.51}$$

because $\det M = 1$, so the two eigenvalues must have the same sign. □

2.6. **The relation of the Shintani–Faddeev modular cocycle to Stark units.** We now present the main theorem of [70]. It expresses generalized Stark units, that is, $u_{\mathfrak{R}\mathfrak{A}} = u_{\mathfrak{A}}^{-1} = \exp(Z'_{\mathfrak{m}\infty_2}(0, \mathfrak{A}))$ for ray classes $\mathfrak{A}$ in a flat imprimitive ray class monoid, in terms of special values $\mathfrak{w}_A^{\mathbf{r}}(\rho)^2$ of the Shintani–Faddeev modular cocycle. The special values of interest are *real multiplication (RM) values*, that is, at they occur real quadratic ρ such that $A \cdot \rho = \rho$.

Theorem 2.19. *Let $\mathcal{O}$ be an order in a real quadratic field F, and let $\mathfrak{m}$ be a nonzero $\mathcal{O}$-ideal. Let $\mathfrak{A} \in \overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m}\infty_2}(\mathcal{O}) \setminus \overline{\mathrm{ZClm}}^{\flat}_{\mathfrak{m}\infty_2}(\mathcal{O})$, let $\mathfrak{A}_0$ be the class of $\mathfrak{A}$ in $\mathrm{Cl}(\mathcal{O})$, choose some $\mathfrak{b} \in \mathfrak{A}_0^{-1}$ coprime to $\mathfrak{m}$, and write $\mathfrak{b}\mathfrak{m} = \alpha(\rho\mathbb{Z} + \mathbb{Z})$ for some $\alpha, \rho \in K$ such that α is totally positive and $\rho > \rho'$. Choose $\mathbf{r} = \left(\begin{smallmatrix} r_1 \\ r_2 \end{smallmatrix}\right) \in \mathbb{Q}^2$ such that $(\alpha(r_2\rho - r_1))\mathfrak{b}^{-1} \in \mathfrak{A}$ and $r_2\rho' - r_1 > 0$. Write*

$$\{B \in \Gamma_{\mathbf{r}} : B \cdot \rho = \rho\} = \langle A \rangle \text{ or } \langle -I, A \rangle \tag{2.52}$$

such that $A \left(\begin{smallmatrix} \lambda \\ 1 \end{smallmatrix}\right) = \lambda \left(\begin{smallmatrix} \rho \\ 1 \end{smallmatrix}\right)$ for $\lambda > 1$. Let $n = \frac{2}{|\phi^{-1}(\mathfrak{A})|}$, where $\phi : \overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m}\infty_1\infty_2}(\mathcal{O}) \to \overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m}\infty_2}(\mathcal{O})$ is the natural quotient map. Then

$$\exp\bigl(nZ'_{\mathfrak{m}\infty_2}(0, \mathfrak{A})\bigr) = (\psi^{-2}\chi_{\mathbf{r}}^{-1})(A)\, \mathfrak{w}_A^{\mathbf{r}}(\rho)^2\,. \tag{2.53}$$

Proof. See [70, Thm. 1.1]. □

One may ask whether all real multiplication values of the Shintani–Faddeev cocycle captured by (2.53). This is answered in the affirmative by [70, Thm. 3.14], which proves certain properties of a function

$$\overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m}\infty_2}(\mathcal{O}) \xrightarrow{\Upsilon_{\mathfrak{m}}} \mathrm{GL}_2(\mathbb{Z})\backslash(\mathbb{Q}^2/\mathbb{Z}^2 \times K_{\mathrm{quad}}), \tag{2.54}$$

sending a ray class $\mathfrak{A}$ to $\Upsilon_{\mathfrak{m}}(\mathfrak{A}) = \mathrm{GL}_2(\mathbb{Z}) \cdot (\mathbf{r} + \mathbb{Z}^2, \rho)$ with $\mathbf{r}$ and ρ chosen in the manner described in Theorem 2.19. Here, $K_{\mathrm{quad}} = K \setminus \mathbb{Q}$, and the notation $\mathrm{GL}_2(\mathbb{Z})\backslash(\mathbb{Q}^2/\mathbb{Z}^2 \times K_{\mathrm{quad}})$ denotes the set of orbits by a certain left action of $\mathrm{GL}_2(\mathbb{Z})$; namely, $M \cdot (\mathbf{r}, \rho) = (\mathrm{sgn}(j_M(\rho))M\mathbf{r}, M \cdot \rho)$. In particular, it is proven that every orbit on the right-hand side is in the image of $\Upsilon_{\mathfrak{m}}$ for some choice of $\mathfrak{m}$. In the case $\mathfrak{m} = d\mathcal{O}$ for $d \in \mathbb{N}$, it is shown that

$$\mathrm{im}(\Upsilon_{\mathfrak{m}}) = \mathrm{GL}_2(\mathbb{Z})\backslash\left(\tfrac{1}{d}\mathbb{Z}^2/\mathbb{Z}^2 \times K_{\mathcal{O}}\right), \tag{2.55}$$

where $K_{\mathcal{O}} = \{\rho \in K \,:\, \lambda\rho\mathbb{Z} + \lambda\mathbb{Z} \subseteq \rho\mathbb{Z} + \mathbb{Z} \iff \lambda \in \mathcal{O}\}$.

2.7. **Conditional results on algebraicity of real multiplication values.** We now prove several results on the implication of the Stark conjectures for real multiplication values of the Shintani–Faddeev cocycle. These results are refined versions of [70, Thm. 1.3] allowing for additional control on the conjectural assumptions and giving some additional conclusions needed in this paper. We will conclude with a proof of Theorem 1.39.

We first examine the implications of our weakest Stark-type conjecture. This proof and the next are related to the proof of [70, Thm. 1.3] in [70, Sec. 8.2].

Theorem 2.20. *Assume Conjecture 2.7 (the Stark Conjecture). Let $\rho \in \mathbb{R}$ such that $a\rho^2 + b\rho + c = 0$ with $a, b, c \in \mathbb{Z}$, $\Delta := b^2 - 4ac$ not a square, and let $\mathbf{r} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$. Let $A \in \Gamma_{\mathbf{r}}$ such that $A \cdot \rho = \rho$.*

(1) There exists some $n \in \mathbb{N}$ such that $\mathfrak{w}^{\mathbf{r}}_A(\rho)^n$ is an algebraic unit in an abelian extension of $K = \mathbb{Q}(\rho)$.
(2) If $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $g(\sqrt{\Delta}) = -\sqrt{\Delta}$, then $|g(\mathfrak{w}^{\mathbf{r}}_A(\rho))| = 1$.

Proof. Let f be the conductor of β (that is, $b^2 - 4ac = f^2\Delta_0$ for a fundamental discriminant Δ_0 and a positive integer f). By [70, Lem. 4.42], there is some 2×2 integral matrix B of determinant f and some real quadratic number α of conductor 1 such that $\beta = B \cdot \alpha$. Choose $n \in \mathbb{N}$ so that

$$C := B^{-1}A^nB \in \bigcap_{\substack{\mathbf{s} \in \mathbb{Q}^2/\mathbb{Z}^2 \\ B\mathbf{s} - \mathbf{r} \in \mathbb{Z}^2}} \Gamma_{\mathbf{s}}. \tag{2.56}$$

Then, by [70, Thm. 4.46], we have

$$\mathfrak{w}^{\mathbf{r}}_A(\beta)^n = \mathfrak{w}^{\mathbf{r}}_{A^n}(\beta) = \mathfrak{w}^{\mathbf{r}}_{BCB^{-1}}(B \cdot \alpha) = \prod_{\substack{\mathbf{s} \in \mathbb{Q}^2/\mathbb{Z}^2 \\ B\mathbf{s} - \mathbf{r} \in \mathbb{Z}^2}} \mathfrak{w}^{\mathbf{s}}_C(\alpha)\,. \tag{2.57}$$

Note that, if (1) and (2) hold for the factors in the product (2.57), then they hold for $\mathfrak{w}^{\mathbf{r}}_A(\beta)^n$. For (1), any product of algebraic units in abelian extensions of K is an algebraic unit in an abelian extension of K (namely, the compositum of the fields generated by the factors over K). For (2), we would obtain

$$|\mathfrak{w}^{\mathbf{r}}_A(\beta)|^n = |\mathfrak{w}^{\mathbf{r}}_A(\beta)^n| = \prod_{\substack{\mathbf{s} \in \mathbb{Q}^2/\mathbb{Z}^2 \\ B\mathbf{s} - \mathbf{r} \in \mathbb{Z}^2}} |\mathfrak{w}^{\mathbf{s}}_C(\alpha)| = 1, \tag{2.58}$$

and thus, since the absolute value function returns a nonnegative real number, $|\mathfrak{w}_A^{\mathbf{r}}(\beta)| = 1$. It thus suffices to prove the theorem when $f = 1$, which we henceforth assume.

As in the statement of Theorem 2.19, write

$$\{B \in \Gamma_{\mathbf{r}} : B \cdot \beta = \beta\} = \langle A_0 \rangle \tag{2.59}$$

such that $A_0 \left(\begin{smallmatrix}\lambda\\1\end{smallmatrix}\right) = \lambda \left(\begin{smallmatrix}\beta\\1\end{smallmatrix}\right)$ for $\lambda > 1$. We have $A = A_0^k$ for some $k \in \mathbb{Z}$. Let $\mathfrak{m}$ be the largest $\mathcal{O}_K$-ideal such that $(\mathbf{r}, \rho) \in \mathrm{M}_{\mathcal{O},\mathfrak{m}}$ in the notation of [70, Thm. 3.12]. Since $\mathfrak{m}$ in $\mathcal{O}_K$-invertible (because $\mathcal{O}_K$ is the maximal order), there is some $\mathfrak{A} \in \overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m}\infty_2}(\mathcal{O})$ such that $\Upsilon_{\mathfrak{m}}(\mathfrak{A}) = (\mathbf{r}, \rho)$ in the notation of [70, Thm. 3.12] (as described at the end of Section 2.6), and moreover $\mathfrak{A} \in \mathrm{Cl}_{\mathfrak{m}\infty_2}(\mathcal{O})$ (because otherwise $\mathfrak{m}$ would not be the largest such $\mathcal{O}_K$-ideal). By Theorem 2.19, for some $n \in \{1, 2\}$,

$$\exp\bigl(nZ'_{\mathfrak{m}\infty_2}(0, \mathfrak{A})\bigr) = (\psi^{-2}\chi_{\mathbf{r}}^{-1})(A_0)\, \mathfrak{w}_{A_0}^{\mathbf{r}}(\rho)^2\,. \tag{2.60}$$

By the cocycle property, $\mathfrak{w}_{A_0^{t+1}}^{\mathbf{r}}(\rho) = \mathfrak{w}_{A_0^t}^{\mathbf{r}}(A_0 \cdot \rho)\, \mathfrak{w}_{A_0}^{\mathbf{r}}(\rho) = \mathfrak{w}_{A_0^t}^{\mathbf{r}}(\rho)\, \mathfrak{w}_{A_0}^{\mathbf{r}}(\rho)$ for any $t \in \mathbb{Z}$, so by induction $\mathfrak{w}_{A_0^k}^{\mathbf{r}}(\rho) = \mathfrak{w}_{A_0}^{\mathbf{r}}(\rho)^k$. Also using the fact that $\psi^2, \chi_{\mathbf{r}}$ are homomorphisms, we obtain

$$\exp\bigl(knZ'_{\mathfrak{m}\infty_2}(0, \mathfrak{A})\bigr) = (\psi^{-2}\chi_{\mathbf{r}}^{-1})(A_0^k)\, \mathfrak{w}_{A_0^k}^{\mathbf{r}}(\rho)^2 = (\psi^{-2}\chi_{\mathbf{r}}^{-1})(A)\, \mathfrak{w}_A^{\mathbf{r}}(\rho)^2\,. \tag{2.61}$$

Let $u_{\mathfrak{A}} = \exp\bigl(-Z'_{\mathfrak{m}\infty_2}(0, \mathfrak{A})\bigr)$, so

$$\mathfrak{w}_A^{\mathbf{r}}(\rho)^2 = (\psi^2\chi_{\mathbf{r}})(A)\, u_{\mathfrak{A}}^{-kn}. \tag{2.62}$$

We have $Z'_{\mathfrak{m}\infty_2}(0, \mathfrak{A}) = \zeta'_{\mathfrak{m}\infty_2}(0, \mathfrak{A}) - \zeta'_{\mathfrak{m}\infty_2}(0, \mathfrak{R}\mathfrak{A})$. By [103, Prop. 5], either $\mathfrak{R}$ is the identity class, in which case $Z'_{\mathfrak{m}\infty_2}(0, \mathfrak{A}) = 0$, or $\zeta'_{\mathfrak{m}\infty_2}(0, \mathfrak{R}\mathfrak{A}) = -\zeta'_{\mathfrak{m}\infty_2}(0, \mathfrak{R}\mathfrak{A})$, in which case $Z'_{\mathfrak{m}\infty_2}(0, \mathfrak{A}) = 2\zeta'_{\mathfrak{m}\infty_2}(0, \mathfrak{A})$. In the former case, $u_{\mathfrak{A}} = 1$, and in the latter case, $u_{\mathfrak{A}}$ is the Stark unit from Conjecture 2.7. In both cases, that conjecture implies that $u_{\mathfrak{A}}$ is an algebraic unit in an abelian extension of K, and thus so is $(\psi^2\chi_{\mathbf{r}})(A)\, u_{\mathfrak{A}}^{-kn}$ (since $(\psi^2\chi_{\mathbf{r}})(A)$ is a root of unity), proving (1). Additionally, in both cases, the conjecture implies that $|g(u_{\mathfrak{A}})| = 1$, and moreover, $g((\psi^2\chi_{\mathbf{r}})(A))$ must by a root of unity. Applying the Galois automorphism g followed by the absolute value function to (2.62) gives $|\mathfrak{w}_A^{\mathbf{r}}(\rho)|^2 = 1$, and thus $|g(\mathfrak{w}_A^{\mathbf{r}}(\rho))| = 1$. □

We now prove another conditional result with stronger assumptions. This time, we assume an appropriate case of the Monoid Stark Conjecture and include stronger conclusions.

Theorem 2.21. *Let $\rho \in \mathbb{R}$ such that $a\rho^2 + b\rho + c = 0$ with $a, b, c \in \mathbb{Z}$, $\Delta := b^2 - 4ac$ not a square, and let $\mathbf{r} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$. Let $\mathcal{O} = (\rho\mathbb{Z} + \mathbb{Z} : \rho\mathbb{Z} + \mathbb{Z}) = \mathbb{Z}[\frac{-b+\sqrt{\Delta}}{2}]$. Let $A \in \Gamma_{\mathbf{r}}$ such that $A \cdot \rho = \rho$. Suppose that $(\mathbf{r}, \rho) \in \mathrm{M}_{\mathcal{O},\mathfrak{m}}$ in the notation of [70, Thm. 3.12]. Assume $\mathrm{MS}(\mathcal{O}, \mathfrak{m})$ from Conjecture 2.9. Then:*

(1) $\mathfrak{w}_A^{\mathbf{r}}(\rho)$ is an algebraic unit in an abelian extension of $K = \mathbb{Q}(\rho)$.
(2) $(\psi^{-2}\chi_{\mathbf{r}}^{-1})(A)\, \mathfrak{w}_A^{\mathbf{r}}(\rho) \in \mathcal{O}_H^{\times}$ for $H = H^{\mathcal{O}}_{\mathfrak{m}\infty_2}$.
(3) In particular, if $d \in \mathbb{N}$ and $\mathbf{r} \in \frac{1}{d}\mathbb{Z}$, then $(\psi^{-2}\chi_{\mathbf{r}}^{-1})(A)\, \mathfrak{w}_A^{\mathbf{r}}(\rho) \in \mathcal{O}_H^{\times}$ for $H = H^{\mathcal{O}}_{d\infty_2}$.
(4) If $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $g(\sqrt{\Delta}) = -\sqrt{\Delta}$, then $|g(\mathfrak{w}_A^{\mathbf{r}}(\rho))| = 1$.

Proof. If $\mathbf{r} \in \frac{1}{2}\mathbb{Z}^2 \setminus \mathbb{Z}^2$, then $\mathfrak{w}_A^{\mathbf{r}}(\rho) = \pm 1$ unconditionally by [70, Thm. 4.38]. Henceforth, we assume $\mathbf{r} \notin \frac{1}{2}\mathbb{Z}^2$, so $-I \notin \Gamma_{\mathbf{r}}$. As in the statement of Theorem 2.19, write

$$\{B \in \Gamma_{\mathbf{r}} : B \cdot \beta = \beta\} = \langle A_0 \rangle \tag{2.63}$$

such that $A_0 \left(\begin{smallmatrix}\lambda\\1\end{smallmatrix}\right) = \lambda \left(\begin{smallmatrix}\beta\\1\end{smallmatrix}\right)$ for $\lambda > 1$. We have $A = A_0^k$ for some $k \in \mathbb{Z}$. By Theorem 2.19, for some $n \in \{1, 2\}$,

$$\exp\bigl(nZ'_{\mathfrak{m}\infty_2}(0, \mathfrak{A})\bigr) = (\psi^{-2}\chi_{\mathbf{r}}^{-1})(A_0)\, \mathfrak{w}_{A_0}^{\mathbf{r}}(\rho)^2\,. \tag{2.64}$$

By the cocycle property, $\mathfrak{w}^{\mathbf{r}}_{A_0^{t+1}}(\rho) = \mathfrak{w}^{\mathbf{r}}_{A_0^t}(A_0 \cdot \rho)\, \mathfrak{w}^{\mathbf{r}}_{A_0}(\rho) = \mathfrak{w}^{\mathbf{r}}_{A_0^t}(\rho)\, \mathfrak{w}^{\mathbf{r}}_{A_0}(\rho)$ for any $t \in \mathbb{Z}$, so by induction $\mathfrak{w}^{\mathbf{r}}_{A_0^k}(\rho) = \mathfrak{w}^{\mathbf{r}}_{A_0}(\rho)^k$. Also using the fact that $\psi^2, \chi_{\mathbf{r}}$ are homomorphisms, we obtain

$$\exp\bigl(knZ'_{\mathfrak{m}\infty_2}(0,\mathfrak{A})\bigr) = (\psi^{-2}\chi_{\mathbf{r}}^{-1})(A_0^k)\, \mathfrak{w}^{\mathbf{r}}_{A_0^k}(\rho)^2 = (\psi^{-2}\chi_{\mathbf{r}}^{-1})(A)\, \mathfrak{w}^{\mathbf{r}}_{A}(\rho)^2 . \tag{2.65}$$

Let $u_{\mathfrak{A}} = \exp\bigl(-Z'_{\mathfrak{m}\infty_2}(0,\mathfrak{A})\bigr)$, so $u_{\mathfrak{A}}^{-kn} = (\psi^{-2}\chi_{\mathbf{r}}^{-1})(A)\, \mathfrak{w}^{\mathbf{r}}_{A}(\rho)^2$.By the conjecture $\mathrm{MS}(\mathcal{O},\mathfrak{m})$, we have $u_{\mathfrak{A}} \in \mathcal{O}_H^\times$ for $H = H^{\mathcal{O}}_{\mathfrak{m}\infty_2}$; thus, $(\psi^{-2}\chi_{\mathbf{r}}^{-1})(A)\, \mathfrak{w}^{\mathbf{r}}_{A}(\rho)^2 \in \mathcal{O}_H^\times$, giving (2). If $\mathbf{r} \in \frac{1}{d}\mathbb{Z}^2$, then $(\mathbf{r},\rho) \in \mathrm{M}_{\mathcal{O},d\mathcal{O}}$ by [70, Thm. 3.12], so (3) follows from (2).

Conjecture $\mathrm{MS}(\mathcal{O},\mathfrak{m})$ also says that $u_{\mathfrak{A}}^{1/2}$ is an algebraic unit in an abelian extension of $K = \mathbb{Q}(\beta)$, and $\mathfrak{w}^{\mathbf{r}}_{A}(\rho) = \pm\sqrt{(\psi^2\chi_{\mathbf{r}})(A)}\, u_{\mathfrak{A}}^{-kn/2}$ (with the square root factor being a root of unity), so $\mathfrak{w}^{\mathbf{r}}_{A}(\rho)$ is an algebraic unit in an abelian extension of K, giving (1).

Finally, $\mathrm{MS}(\mathcal{O},\mathfrak{m})$ says that $|g(u_{\mathfrak{A}})| = 1$; since $g\Bigl(u_{\mathfrak{A}}^{1/2}\Bigr)^2 = g(u_{\mathfrak{A}})$, it follows that $\Bigl|g\Bigl(u_{\mathfrak{A}}^{1/2}\Bigr)\Bigr| = 1$. Since g is a homomorphism,

$$g(\mathfrak{w}^{\mathbf{r}}_{A}(\rho)) = \pm g\Bigl(\sqrt{(\psi^2\chi_{\mathbf{r}})(A)}\Bigr)\; g\Bigl(u_{\mathfrak{A}}^{1/2}\Bigr)^{-kn}, \tag{2.66}$$

and $g\Bigl(\sqrt{(\psi^2\chi_{\mathbf{r}})(A)}\Bigr)$ is a root of unity, so $|g(\mathfrak{w}^{\mathbf{r}}_{A}(\rho))| = 1$, giving (4). □

Proof of Theorem 1.39. Theorem 1.39(1) says that Conjecture 2.7 implies Conjecture 1.36. This follows from Theorem 2.20.

Theorem 1.39(3) says that Conjecture 2.9 implies Conjecture 1.38. Assume Conjecture 2.9. Then Conjecture 1.38(1) follows from Theorem 2.21(1), and Conjecture 1.38(2) follows from Theorem 2.21(4).

Theorem 1.39(2) says that Conjecture 2.8 implies Conjecture 1.37. Assume Conjecture 2.8. By Proposition 2.10, $\mathrm{MS}(\mathcal{O}_K,\mathfrak{m})$ holds for $K = \mathbb{Q}(\rho)$ and $\mathfrak{m}$ an ideal of the maximal order $\mathcal{O}_K$. Then Conjecture 1.38(1) follows from Theorem 2.21(1), and Conjecture 1.38(2) follows from Theorem 2.21(4). □

3. Weyl–Heisenberg group, extended Clifford group, and SIC phenomenology

The purpose of this section is, firstly, to review some relevant background material concerning the Weyl–Heisenberg group, the extended Clifford group, and r-SICs. For more details see refs. [4, 6]. We then go on to prove Theorems 1.7 and 1.8 from the introduction.

3.1. Weyl–Heisenberg group.

Definition 3.1. The discrete symplectic form is

$$\langle \mathbf{p},\mathbf{q}\rangle = \mathbf{p}^\top \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \mathbf{q} = p_2q_1 - p_1q_2, \qquad \mathbf{p},\mathbf{q} \in \mathbb{Z}^2. \tag{3.1}$$

The WH displacement operators (Definition 1.5) satisfy

$$D_{\mathbf{p}}^\dagger = D_{-\mathbf{p}}, \qquad \forall \mathbf{p} \in \mathbb{Z}^2 \tag{3.2}$$

$$D_{\mathbf{p}}D_{\mathbf{q}} = \xi_d^{\langle \mathbf{p},\mathbf{q}\rangle} D_{\mathbf{p}+\mathbf{q}}, \qquad \forall \mathbf{p},\mathbf{q} \in \mathbb{Z}^2. \tag{3.3}$$

The fact $(\xi_d)^d = (-1)^{d+1}$ means

$$D_{\mathbf{p}+d\mathbf{q}} = (-1)^{(d+1)\langle \mathbf{p},\mathbf{q}\rangle} D_{\mathbf{p}}. \tag{3.4}$$

for all $\mathbf{p}$, $\mathbf{q}$. So the displacement operators are d-periodic when d is odd, but not when d is even. It would be possible to define the displacement operators by $D_{\mathbf{p}} = X^{p_1}Z^{p_2}$, so that they were

d-periodic for all values of d. Defining them the way we do introduces major simplifications later on, at the cost of some additional complexity at the outset. To get an idea of the relative merits of the two definitions, see ref. [19].

One has

$$\mathrm{Tr}\big(D_{\mathbf{p}}D_{\mathbf{q}}^{\dagger}\big) = d(-1)^{\frac{d+1}{d}\langle \mathbf{p},\mathbf{q}\rangle}\delta_{\mathbf{p},\mathbf{q}}^{(d)}, \qquad \delta_{\mathbf{p},\mathbf{q}}^{(d)} = \begin{cases} 1 & \text{if } \mathbf{p} \equiv \mathbf{q} \pmod{d}, \\ 0 & \text{otherwise.} \end{cases} \tag{3.5}$$

It follows that the displacement operators are a basis for $\mathcal{L}(H_d)$. In particular, an arbitrary operator $W \in \mathcal{L}(H_d)$ can be expanded in terms of the $D_{\mathbf{p}}$ using

$$M = \frac{1}{d}\sum_{\mathbf{p}} \mathrm{Tr}\big(WD_{\mathbf{p}}^{\dagger}\big)\, D_{\mathbf{p}} \tag{3.6}$$

where the summation is over any transversal for the quotient group $\mathbb{Z}^2/(d\mathbb{Z}^2)$ (note that the product $\mathrm{Tr}\big(WD_{\mathbf{p}}^{\dagger}\big)\, D_{\mathbf{p}}$ is d-periodic, even though the two factors may not be).

3.2. **Clifford and extended Clifford groups.**

Definition 3.2 (Clifford Group; extended Clifford group;projective Clifford and extended Clifford groups)**.** The Clifford group in dimension d, denoted $\mathrm{C}(d)$, is the set of all unitaries U with the property

$$UD_{\mathbf{p}}U^{\dagger} = e^{i\varphi(\mathbf{p})}D_{f(\mathbf{p})} \tag{3.7}$$

for all $\mathbf{p}$ and some pair of functions $\varphi\colon \mathbb{Z}^2 \to \mathbb{R}$, $f\colon \mathbb{Z}^2 \to \mathbb{Z}^2$.

The extended Clifford group in dimension d, denoted $\mathrm{EC}(d)$, is the set of all unitaries and anti-unitaries with this property.

The projective groups $\mathrm{PC}(d)$ and $\mathrm{PEC}(d)$) are the quotients of $\mathrm{C}(d)$ and $\mathrm{EC}(d)$ by their centres:

$$\mathrm{PC}(d) = \mathrm{C}(d)/\langle I\rangle, \qquad \mathrm{PEC}(d) = \mathrm{EC}(d)/\langle I\rangle. \tag{3.8}$$

The importance of the groups $\mathrm{C}(d)$, $\mathrm{EC}(d)$ for us is that they preserve r-SIC fiduciality: if Π is a r-SIC fiducial, then so is $U\Pi U^{\dagger}$, for all $U \in \mathrm{EC}(d)$. Since the replacement $U \to e^{i\theta}U$ does not change $U\Pi U^{\dagger}$ we only need consider one representative of each coset in $\mathrm{PEC}(d)$.

Definition 3.3 (symplectic and extended symplectic groups; symplectic and anti-symplectic matrices)**.** We refer to the group $\mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ simply as "the symplectic group." Additionally, the extended symplectic group $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ is the set of all matrices in $\mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ with determinant equal to ± 1. An element of $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ is said to be *symplectic* (respectively *anti-symplectic*) if it has determinant equal to $+1$ (respectively -1). The *canonical anti-symplectic* matrix is defined to be

$$J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.9}$$

(Note that the $n \times n$ symplectic group $\mathrm{Sp}_n(R)$ and the $n \times n$ special linear group $\mathrm{SL}_n(R)$ for a ring R are not generally isomorphic, but for $n = 2$, they are isomorphic and equal inside $\mathrm{GL}_2(R)$.)

The significance of the canonical anti-symplectic matrix is that the map $F \mapsto JF$ converts symplectic matrices into anti-symplectic matrices, and conversely.

Trivially, $\mathrm{C}(d)$ contains $\mathrm{WH}(d)$. Less trivially, it contains [4] a representation of the symplectic group. Specifically, for each $F = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ there exists a unitary $U_F \in \mathcal{L}(H_d)$, unique up to multiplication by a number having absolute value equal to 1, such that

$$U_F D_{\mathbf{p}} U_F^\dagger = D_{F\mathbf{p}} \tag{3.10}$$

for all $\mathbf{p}$. We refer to U_F as a symplectic unitary. One has

$$U_{F^{-1}} \doteq U_F^\dagger \qquad \forall F \in \mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z}), \tag{3.11}$$

$$U_{F_1} U_{F_2} \doteq U_{F_1 F_2} \qquad \forall F_1, F_2 \in \mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z}). \tag{3.12}$$

where the symbol $\doteq$ signifies "equal up to multiplication by a number having absolute value equal to 1". So the map $F \mapsto U_F$ is a projective representation of $\mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$. It can be shown [4] that $\mathrm{C}(d)$ consists of all products of the form

$$e^{i\lambda} D_{\mathbf{p}} U_F \tag{3.13}$$

for $\lambda \in \mathbb{R}$, $\mathbf{p} \in \mathbb{Z}^2$, $F \in \mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$.

There exist [4, 6] explicit formulae for the U_F. We say that $F = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ is a *prime matrix* if β is coprime to $\bar{d}$. It can be shown that every matrix in $\mathrm{SL}_2(\mathbb{Z}/\bar{d}/\mathbb{Z})$ is a product of two prime matrices. It can also be shown that if F is a prime matrix then

$$U_F = \frac{e^{i\theta}}{\sqrt{d}} \sum_{j,k=0}^{d-1} \xi_d^{\beta^{-1}(\delta j^2 - 2jk + \alpha k^2)} |j\rangle\langle k| \tag{3.14}$$

where β^{-1} is the multiplicative inverse of β as an element of $\mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ and $e^{i\theta}$ is an arbitrary phase.

Definition 3.4 (Parity matrix)**.** We define the parity matrix by

$$P = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.15}$$

Using the decomposition

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.16}$$

together with (3.14) one finds, after a certain amount of algebra, that

$$U_P = \sum_{j=0}^{d-1} |-j\rangle\langle j| \tag{3.17}$$

in agreement with Definition 1.13.

If we choose the arbitrary phase in (3.14) according to

$$e^{i\theta} = \begin{cases} 1 & d \equiv 1 \pmod 4 \\ i & d \equiv 3 \pmod 4 \\ e^{\frac{\pi i}{4}} & d \equiv 0 \pmod 2 \end{cases} \tag{3.18}$$

then [6, 11] the components of U_F are all in the cyclotomic field $\mathbb{Q}(\xi_d)$. In the sequel we will always assume this choice has been made. On this assumption we have the following description of the action of a Galois automorphism.

We will need the fact

Theorem 3.5. *The homomorphism* $F \in \mathrm{SL}_2(\mathbb{Z}) \mapsto U_F\langle I\rangle \in \mathrm{PC}(d)$

(1) is injective if d *is odd*
(2) has kernel $\left\langle \left(\begin{smallmatrix} d+1 & 0 \\ 0 & d+1 \end{smallmatrix}\right) \right\rangle$ *if* d *is even.*

Proof. See Theorem 1 of ref. [4]. □

Definition 3.6. Let g be any Galois automorphism of $\mathbb{Q}(\xi_d)/\mathbb{Q}$. Define k_g to be the unique integer in the range $0 \leq k_g < \bar{d}$ such that $g(\xi_d) = \xi_d^{k_g}$, and define $H_g \in \mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ to be the matrix

$$H_g = \begin{pmatrix} 1 & 0 \\ 0 & k_g \end{pmatrix}. \tag{3.19}$$

Theorem 3.7. *Let* g *be any Galois automorphism of* $\mathbb{Q}(\xi_d)/\mathbb{Q}$*. Then*

$$g(D_{\mathbf{p}}) = D_{H_g\mathbf{p}} \tag{3.20}$$

$$g(U_F) \doteq U_{H_g F H_g^{-1}} \tag{3.21}$$

for all $\mathbf{p} \in \mathbb{Z}^2$*,* $F \in \mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$.

Remark. In particular, if g is complex conjugation, then $H_g = J$.

Proof. Theorem 2 in ref. [4], with the obvious modification to take account of Eq. (3.18) above. □

Proof of Lemma 1.45. It follows from Definition 1.44 and Theorem 3.7 that

$$\Pi_s = \frac{1}{d} \sum_{\mathbf{p}} g\left(\tilde{\mu}_{G\mathbf{p}}(t)\right) D_{H_g\mathbf{p}}. \tag{3.22}$$

Hence

$$\mu_{\mathbf{p}}(s) = \mathrm{Tr}\left(\Pi_s D^{\dagger}_{G^{-1}\mathbf{p}}\right) = g\left(\tilde{\mu}_{GH_g^{-1}G^{-1}\mathbf{p}}(t)\right) \tag{3.23}$$

□

Just as symplectic matrices F are associated to unitaries U_F satisfying Eq. (3.10), so anti-symplectic matrices F are associated to anti-unitaries U_F satisfying the same equation. Explicitly, such anti-unitaries act according to

$$U_F|\psi\rangle = \sum_{j=0}^{d-1} \langle j|\psi\rangle^* U_{FJ}|j\rangle. \tag{3.24}$$

In particular U_J acts by complex conjugation in the standard basis:

$$U_J|\psi\rangle = \sum_{j=0}^{d-1} \langle j|\psi\rangle^* |j\rangle. \tag{3.25}$$

One then finds that $\mathrm{EC}(d)$ consists of all products of the form (3.13), where now F is an arbitrary element of $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$.

Finally, we define

Definition 3.8 ((anti-)symplectic subgroup of $\mathrm{EC}(d)$)**.** We define the (anti-)symplectic subgroup of $\mathrm{EC}(d)$, denoted $\mathrm{EC}_0(d)$ to consist of all unitaries and anti-unitaries of the form

$$e^{i\theta} U_F \tag{3.26}$$

with $F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ and $e^{i\theta}$ a phase.

3.3. **SIC phenomenology.** Over the last 25 years, investigation of the large number of known 1-SICs has resulted in a large number of empirical observations. To reflect the fact that a lot of this material is unproven, we refer to it as *SIC phenomenology*. One of the aims of this paper is to show that many of these observations are consequences of the Twisted Convolution Conjecture together with the Stark Conjecture and its refinements.

The purpose of this subsection is to summarize this pre-existing body of empirical observations. Since it is concerned with previous results, we only discuss 1-SICs.

3.3.1. *Number of orbits.* The fact that the elements of $\mathrm{EC}(d)$ preserve r-SIC fiduciality suggests we group r-SICs into $\mathrm{EC}(d)$ orbits. The question then arises: how many orbits are there in each dimension? In the case of 1-SICs this question has been answered by brute-force numerical calculation in many low-lying dimensions (see refs. [47, 48, 89, 90] and references cited therein). One finds that for $d = 3$ there are infinitely many orbits. However, those are examples of sporadic 1-SICs [96], which are in various ways exceptional. In particular, 1-SICs in dimension 3 typically generate transcendental number fields. If we confine ourselves to non-sporadic 1-SICs (i.e. WH covariant 1-SICs in dimensions greater than 3) then explicit calculation suggests that the number of orbits is always finite. For the first 20 dimensions greater than 3 the number of orbits is given in Table 1. A long-standing puzzle has been to understand where these numbers are coming from. As

d	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
# orbits	1	1	1	2	2	2	1	3	2	2	2	4	2	3	2	5	2	5	1	6

TABLE 1. Number of $\mathrm{EC}(d)$ orbits of 1-SICs in dimensions 4–20.

will be shown in Section 7, the construction we describe answers that question.

3.3.2. *Symmetry group.*

Definition 3.9 (Symmetry group of a fiducial)**.** Let Π be a r-SIC fiducial in dimension d. Its symmetry group, denoted $\mathcal{S}(\Pi)$, is the set of cosets $U\langle I\rangle \in \mathrm{PEC}(d)$ such that

$$U\Pi U^\dagger = \Pi. \tag{3.27}$$

Brute-force numerical computation [4, 89, 90] suggests that in every case $\mathcal{S}(\Pi)$

(1) is non-trivial cyclic,
(2) contains a coset

$$D_{\mathbf{p}}U_F\langle I\rangle \tag{3.28}$$

for which $F \in \mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})$ is such that $\mathrm{Tr}(F) \equiv -1 \pmod d$. It can be shown that if $d > 3$ then such cosets are necessarily order 3.

Theorem 3.10. *Let $F \in \mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})$ be such that $\mathrm{Tr}(F) \equiv -1 \pmod d$. Assume $d > 3$. Then*

(1) The coset $D_{\mathbf{p}}U_F\langle I\rangle$ is order 3 for all $\mathbf{p} \in \left(\mathbb{Z}/d\mathbb{Z}\right)^2$.
(2) If d is odd then F is order 3.
(3) If d is even then F is order 3 if $\mathrm{Tr}(F) \equiv -1 \left(\mathrm{mod}\ \bar{d}\right)$ and order 6 if $\mathrm{Tr}(F) \equiv d - 1 \left(\mathrm{mod}\ \bar{d}\right)$.

Proof. The first statement is proved in ref. [4]. The other two are proved by repeated application of the identity

$$L^2 = \mathrm{Tr}(L)L - I. \tag{3.29}$$

valid for any $L \in \mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$. □

Note that we can switch between the two cases $\mathrm{Tr}(F) \equiv -1 \pmod{\bar{d}}$ and $\mathrm{Tr}(F) \equiv d-1 \pmod{\bar{d}}$ by multiplying by $d+1$: If $F' = (d+1)F$, then $\mathrm{Tr}(F') \equiv -1 \pmod{\bar{d}}$ if and only if $\mathrm{Tr}(F) \equiv d-1 \pmod{\bar{d}}$. Note also [4] that if $F' = (d+1)F$ then $D_{\mathbf{p}}U_{F'}\langle I\rangle = D_{\mathbf{p}}U_F\langle I\rangle$ for all $\mathbf{p}$. So if one is only interested in the corresponding elements of $\mathrm{PC}(d)$ there is no loss of generality in focusing on just one of the cases. Accordingly, in the following, if $D_{\mathbf{p}}U_F\langle I\rangle$ is a canonical order 3 unitary, it will always, unless the contrary is explicitly stated, be assumed that $\mathrm{Tr}(F) \equiv d-1 \pmod{\bar{d}}$. We thus define

Definition 3.11 (canonical Order 3 Unitary)**.** A coset $D_{\mathbf{p}}U_F\langle I\rangle$ in dimension $d > 3$ is said to be *canonical order 3* if $\det(F) = +1$ and $\mathrm{Tr}(F) \equiv d-1 \pmod{\bar{d}}$.

It is convenient to define the following standard trace $d-1$ matrices:

Definition 3.12 (F_z (Zauner), F_a, F'_a matrices)**.** For all d define the *Zauner* matrix to be

$$F_z = \begin{pmatrix} 0 & d-1 \\ d+1 & d-1 \end{pmatrix}. \tag{3.30}$$

If $d \equiv 3 \pmod 9$, also define the variant Zauner matrix

$$F_a = \begin{pmatrix} 1 & d+3 \\ \frac{4d-3}{3} & d-2 \end{pmatrix}, \tag{3.31}$$

while if $d \equiv 6 \pmod 9$, define the variant Zauner matrix

$$F'_a = \begin{pmatrix} 1 & d+3 \\ \frac{2d-3}{3} & d-2 \end{pmatrix}. \tag{3.32}$$

It turns out that every determinant $+1$, trace $d-1$ element of $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}/\mathbb{Z})$ is conjugate to one of these three matrices. Specifically:

Theorem 3.13. *The set of matrices in* $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ *having determinant equal to* $+1$ *and trace equal to* $d-1$ *consists of*

(1) The single conjugacy class $[F_z]$ *if* $d \not\equiv 3, 6 \pmod 9$,
(2) The two disjoint conjugacy classes $[F_z]$, $[F_a]$ *if* $d \equiv 3 \pmod 9$,
(3) The two disjoint conjugacy classes $[F_z]$, $[F'_a]$ *if* $d \equiv 6 \pmod 9$,

where the notation "$[F]$*" means "conjugacy class of* F *considered as an element of* $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$*".*

Remark. Although the matrices of interest are all in $\mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$, we consider conjugacy relative to $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$. This is essential. If instead we considered conjugacy relative to $\mathrm{SL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ the conjugacy classes would be smaller, and the description significantly more complicated.

Proof. See Appendix B. □

If $d \equiv 3 \pmod 9$ (respectively $d \equiv 6 \pmod 9$) we can use the following convenient criterion to tell if a given matrix is in $[F_a]$ or $[F_z]$ (respectively $[F'_a]$ or $[F_z]$).

Theorem 3.14. *Let $F \in \mathrm{ESL}_2(\mathbb{Z}/d\bar{\mathbb{Z}})$ have determinant equal to $+1$ and trace equal to $d-1$.*

(1) If $d \equiv 3 \pmod 9$ then $F \in [F_a]$ if and only if $F \equiv I \pmod 3$.
(2) If $d \equiv 6 \pmod 9$ then $F \in [F'_a]$ if and only if $F \equiv I \pmod 3$.

Remark. In particular $[F'_a] = [F_z]$ if $d \equiv 3 \pmod 9$, and $[F_a] = [F_z]$ if $d \equiv 6 \pmod 9$.

Proof. Immediate consequence of the fact

$$d \equiv 3 \pmod 9 \qquad \Longrightarrow \qquad F_z = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}, \; F_a \equiv I \pmod 3, \tag{3.33}$$

$$d \equiv 6 \pmod 9 \qquad \Longrightarrow \qquad F_z = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}, \; F'_a \equiv I \pmod 3. \tag{3.34}$$

□

It is observed empirically that if $d \equiv 3 \pmod 9$ (respectively $d \equiv 6 \pmod 9$) the symmetry group $\mathcal{S}(\Pi)$ never seems to contain two canonical order 3 unitaries $D_{\mathbf{p}}U_F$, $D_{\mathbf{q}}U_{F'}$ such that $F \in [F_z]$ and $F' \in [F_a]$ (respectively $F \in [F_z]$ and $F' \in [F_a]$. This suggests that we may classify fiducials by conjugacy class:

Definition 3.15 (type-z, type-a, type-a' fiducials)**.** A fiducial Π is said to be

(1) *type-z* if $\mathcal{S}(\Pi)$ contains a canonical order 3 fiducial $D_{\mathbf{p}}U_F$ with F conjugate to F_{z},
(2) *type- a* if $d \equiv 3 \pmod 9$ and $\mathcal{S}(\Pi)$ contains a canonical order 3 fiducial $D_{\mathbf{p}}U_F$ with F conjugate to F_{a},
(3) *type-a'* if $d \equiv 6 \pmod 9$ and $\mathcal{S}(\Pi)$ contains a canonical order 3 fiducial $D_{\mathbf{p}}U_F$ with F conjugate to $F_{\mathrm{a}'}$.

This is the source of four long-standing puzzles.

Question 1. One would like to understand why $\mathcal{S}(\Pi)$ always seems to contain a canonical order 3 unitary.

Question 2. One would like to understand why classification by conjugacy class works: why one seems never to find orbits which are simultaneously type-z and type-a (if $d \equiv 3 \pmod 9$), or simultaneously type-z and type-a' (if $d \equiv 6 \pmod 9$).

Question 3. It appears that when $d \equiv 3 \pmod 9$ there exist both type-z and type-a orbits. Specifically brute-force numerical computation [89] indicates that in the first nine such dimensions the numbers of type-z and type-a $\mathrm{EC}(d)$ orbits are

d:	12	21	30	39	48	57	66	75	84
# type-z orbits:	1	4	3	6	5	6	6	12	6
# type-a orbits:	1	1	1	4	2	2	3	3	4

One would like to know what determines these numbers.

Question 4. When $d \equiv 6 \pmod 9$, brute-force numerical computation [89] indicates that the number of type-a' orbits is zero, at least when $d \leq 87$. One would like to know the reason.

As we will see, our conjectures provide answers to all of these questions.

Definition 3.16 (centred fiducial)**.** A fiducial Π is said to be *centered* if $\mathcal{S}(\Pi)$ only contains cosets of the form $U_F\langle I\rangle$, $F \in \mathrm{ESL}_2(\mathbb{Z}/d\bar{\mathbb{Z}})$.

Numerical investigations suggest that every 1-SIC contains at least one centered fiducial.

Definition 3.17 (overlap symmetry group)**.** Suppose Π is centred, and let $\nu_{\mathbf{p}}$ be its normalized overlaps. Define the *symplectic symmetry group* by

$$\mathcal{S}_{\mathrm{ESL}}(\Pi) = \{F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})\colon U_F \in \mathcal{S}(\Pi)\}, \tag{3.35}$$

and the *overlap symmetry group* by

$$\mathcal{S}_{\mathrm{OL}}(\Pi) = \left\{F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})\colon \nu_{F\mathbf{p}} = \nu_{\mathbf{p}}\ \forall \mathbf{p} \in \mathbb{Z}^2\right\}. \tag{3.36}$$

It is easily seen [7] that if Π is centred then $\mathcal{S}_{\mathrm{OL}}(\Pi) = \{\det(F)F\colon F \in \mathcal{S}_{\mathrm{ESL}}(\Pi)\}$.

Inspection of the 1-SIC symmetry groups in low-lying dimensions [89] raises other questions. In the first place, one finds that in some cases, but not in others, the symmetry group contains anti-unitaries as well as unitaries. One would like to know why. One would also like to know, in dimensions where anti-unitary symmetries occur, on exactly how many $\mathrm{EC}(d)$ orbits this happens. Furthermore, one would like to know what determines the order of the symmetry group. As we will see, the Twisted Convolution Conjecture and the Stark Conjecture confirm and explain all the conjectures about the symmetry group in [89]. It also provides answers to the question marks in the Table in [89].

3.3.3. *Fields, multiplets, and ghosts.* The study [7, 10–13, 15, 69] of known exact 1-SICs has led to a number of conjectures regarding the field generated by a 1-SIC, and the associated Galois group.

Let Π be a 1-SIC fiducial in dimension $d > 3$, and let E be the field[6] generated by the matrix elements of Π together with the root of unity ξ_d. Then it was observed in ref. [7] that, in all the cases considered there, E is a finite degree abelian extension of $K = \mathbb{Q}(\sqrt{(d-3)(d+1)})$ which is normal over $\mathbb{Q}$. It was also observed that an important role is played by three subfields H, E_1, E_2 related to E and K as shown in Fig. 1.

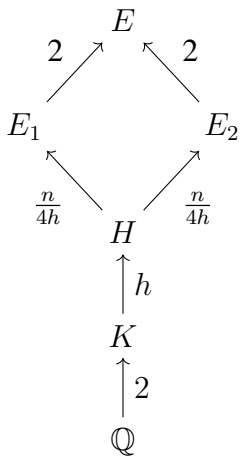


FIGURE 1. Structure of the field E. Arrows show field inclusions, and run from the smaller field to the larger. Numbers besides the arrows are the extension degrees, and $n = [E\colon \mathbb{Q}]$.

Specifically, let $\bar{g}_1$, $\bar{g}_2$ be the non-trivial automorphisms of the order 2 groups $\mathrm{Gal}(E/E_1)$, $\mathrm{Gal}(E/E_2)$. Then it was observed, in every case examined,

[6] If our conjectures are correct, and if Π is calculated from an admissible tuple t in the manner prescribed by Definition 1.44, then E is the SIC field E_t specified by Definition 1.40.

(1) $E_2 \subseteq \mathbb{R}$, and $\bar{g}_2$ is complex conjugation
(2) Let $\bar{g}_1$, $\bar{g}_2$ be the non-
(3) For all $g \in \mathrm{Gal}(E/\mathbb{Q})$,

$$g\bar{g}_1 = \bar{g}_1 g \qquad \Longleftrightarrow \qquad g\bar{g}_2 = \bar{g}_2 g \qquad \Longleftrightarrow \qquad g \in \mathrm{Gal}(E/K). \tag{3.37}$$

(4) For all $g \in \mathrm{Gal}(E/\mathbb{Q})$,

$$g(E_1) = E_1, \qquad g(E_2 = E_2, \qquad \text{if } g \in \mathrm{Gal}(E/K, \tag{3.38}$$

$$g(E_1) = E_2, \qquad g(E_2) = E_1, \qquad \text{if } g \notin \mathrm{Gal}(E/K). \tag{3.39}$$

(5) Let $g \in \mathrm{Gal}(E/\mathbb{Q})$ be arbitrary. Then
  (a) $g(\Pi)$ is a 1-SIC fiducial if and only if $g \in \mathrm{Gal}(E/K)$,
  (b) $g(\Pi)$ is a 1-SIC fiducial on the same $\mathrm{EC}(d)$ orbit as Π if and only if $g \in \mathrm{Gal}(E/H)$.

Definition 3.18 (Galois multiplet)**.** We refer to the set of $\mathrm{EC}(d)$ orbits obtained by acting on a fiducial Π by elements of $\mathrm{Gal}(E/K)$ and/or conjugating with an element of $\mathrm{EC}(d)$ as a *Galois multiplet*.

It follows from Item 5b in the above list that the Galois multiplet associated to Π has cardinality h.

In every case examined, the fields associated to the multiplets in a given dimension appear to form a bounded lattice under set inclusion. In particular, there is, in every case examined, a unique minimal field, and a unique maximal field. The dimension 35 fields and associated multiplets[7] are illustrated in Fig. 2.

Empirical investigation [10–13, 15, 69] indicates that the minimal multiplet in a given dimension d generates the ray class field over $\mathbb{Q}\big(\sqrt{D}\big)$ with modulus $\bar{d}$ and ramification at both infinite places. Empirical investigation also indicates that in the case of the minimal multiplet the field H is the Hilbert class field, meaning that the multiplicity of the minimal multiplet is equal to the class number of $\mathbb{Q}\big(\sqrt{D}\big)$. As we will see, it follows from our conjectures that these statements generalize to arbitrary multiplets of arbitrary rank r-SICs. Specifically, the fields E, E_1, E_2, H for an arbitrary multiplet of arbitrary rank are ray class fields of non-maximal orders, as defined in refs. [71, 72].

It follows from item 5b in the above list of properties that, for each $g \in \mathrm{Gal}(E/H)$ there is an associated $U^{(g)} \in \mathrm{EC}(d)$ such that

$$g(\Pi) = U^{(g)} \Pi U^{(g)\dagger} \tag{3.40}$$

To understand this action in more detail it helps to focus on the overlaps of strongly-centred fiducials:

Definition 3.19 (strongly centred fiducial)**.** A r-SIC fiducial Π is said to be strongly centred if it is centred, and if all its overlaps are in the field E_1.

Empirical investigation indicates that every 1-SIC contains at least one strongly centred fiducial.

Now let Π be a strongly centred fiducial, and let $\mu_{\mathbf{p}}$ be its overlaps. Then $\bar{g}_1(\mu_{\mathbf{p}}) = \mu_{\mathbf{p}}$ for all $\mathbf{p}$, so it is enough to consider the action of the subgroup $\mathrm{Gal}(E_1/H)$.

The empirical studies of 1-SIC fiducials reported in refs. [10–13, 15, 69] indicate that in the case of a type-z orbit there is a natural isomorphism

$$\mathrm{Gal}(E_1/H) \cong C/\mathcal{S}_{\mathrm{OL}}(\Pi) \tag{3.41}$$

[7] We are grateful to Markus Grassl for pointing out an error in the version of this diagram which appeared in ref. [11].

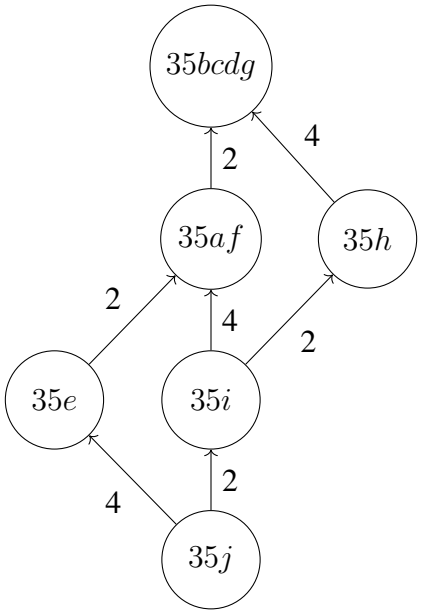


FIGURE 2. Fields and multiplets in dimension 35. The arrows indicate the field inclusions, and run from the smaller field to the larger. So $35j$ is the minimal multiplet and $35bcdg$ is the maximal multiplet. Numbers beside the arrows are the degrees of the extensions. In this diagram we use the Scott-Grassl convention [89,90], in which the $\mathrm{EC}(d)$ orbits for a given dimension are labelled by letters. For example $35bcdg$ denotes the Galois multiplet consisting of the 4 Scott–Grassl orbits $35b$, $35c$, $35d$, $35g$.

where $\mathcal{S}_{\mathrm{OL}}(\Pi)$ is as defined in Definition 3.17 and C is the centralizer of $\mathcal{S}_{\mathrm{OL}}(\Pi)$ considered as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$. The isomorphism associates to each $g \in \mathrm{Gal}(E_1/H)$ a coset $F\mathcal{S}_{\mathrm{OL}}(\Pi)$ with the property

$$g(\mu_{\mathbf{p}}) = \mu_{F'\mathbf{p}} \tag{3.42}$$

for all $\mathbf{p}$ and any $F' \in F\mathcal{S}_{\mathrm{OL}}(\Pi)$.

A similar statement holds for type a fiducials, except that C has to be replaced by one of three maximal abelian subgroups of $\mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ containing $\mathcal{S}_{\mathrm{OL}}(\Pi)$. For more details see ref. [11].

It is worth noting that this isomorphism gives us a geometrical interpretation of the Galois group which is very much in the spirit of Hilbert's original formulation of his 12^{th} problem.

In every case examined, the normalized overlaps $\nu_{\mathbf{p}}$ (as defined in Definition 1.9) are units. The subgroup of the full unit group which they generate has some interesting properties which are described in ref. [13].

Let Π be a strongly centred r-SIC fiducial, let $\mu_{\mathbf{p}}$ be its overlaps, and let $g \in \mathrm{Gal}(E/\mathbb{Q})$ be such that $g(\sqrt{D}) = -\sqrt{D}$. Then it follows from item 4 in the above list of properties that the numbers

$$\tilde{\mu}_{\mathbf{p}} = g\left(\mu_{\mathbf{p}}\right) \tag{3.43}$$

are all real. It will turn out that they are the ghost overlaps defined in Definition 1.11. Moreover, if E is a ray class field of a maximal order, then the normalized ghost overlaps $\tilde{\nu}_{\mathbf{p}}$ are half-integral powers of Stark units [70] (if the order is non-maximal then the situation is more complicated, and requires further investigation [70]).

3.3.4. *Dimension towers and 1-SIC alignment.* As we saw in Section 3.3.3, empirical investigations suggest that a 1-SIC in dimension d gives rise to an abelian extension of the real quadratic field $\mathbb{Q}(\sqrt{(d-3)(d+1)})$. It is natural to ask how many dimensions are associated in this way to a given real quadratic field. The following theorem answers that question.

Theorem 3.20. *Let K be a real quadratic field. Then $K = \mathbb{Q}(\sqrt{(d-3)(d+1)})$ if and only if d is in the dimension tower associated to K (see definition 1.24).*

Proof. See ref. [13, Lemma 4]. □

Theorem 3.21. *Let $j_1, j_2, \ldots$ be an increasing sequence of natural numbers such that, for all $n \in \mathbb{N}$,*

(1) j_n divides j_{n+1},
(2) j_{n+1}/j_n is coprime to 3.

Then d_{j_n} divides $d_{j_{n+1}}$ for all $n \in \mathbb{N}$.

Proof. See the proof of Proposition 7 in ref. [13]. In ref. [13] this result is stated with the unnecessarily strong condition that the individual terms of the sequence $j_1, j_2, \ldots$ are coprime to 3. However, the proof is easily seen to imply that the result continues to hold with the weaker condition we have stated here. □

It follows from this theorem that, if the various properties of the known 1-SICs described above generalize to every 1-SIC in every dimension, then for each subsequence $j_1, j_2, \ldots$ satisfying the conditions of the theorem, one has the field inclusions

$$E(d_{j_1}) \subseteq E(d_{j_2}) \subseteq \ldots \tag{3.44}$$

where $E(d)$ denotes the field associated to the minimal multiplet in dimension d. Given this relationship of the fields, it is natural to ask if there is a corresponding relationship of the 1-SICs themselves. This question was addressed in ref. [8] for a number of dimension pairs d_j, d_{2j} (also see refs. [3]). Denoting the normalized overlaps in dimensions d_j, d_{2j} by $e^{i\theta_{\mathrm{P}}}$, $e^{i\Theta_{\mathrm{P}}}$ respectively, it was found, in the cases examined, that

$$e^{i\Theta_{d_j\mathrm{P}}} = \begin{cases} 1 & d_j \text{ odd}, \\ -(-1)^{(p_1+1)(p_2+1)} & d_j \text{ even}, \end{cases} \tag{3.45}$$

$$e^{i\Theta_{(d_j-2)\mathrm{P}}} = \begin{cases} -e^{2i\theta_{F\mathrm{P}}} & d_j \text{ odd}, \\ (-1)^{(p_1+1)(p_2+1)} e^{2i\theta_{F\mathrm{P}}} & d_j \text{ even}. \end{cases} \tag{3.46}$$

Moreover, it was found that these properties generalize to other 1-SIC multiplets.

Definition 3.22. A pair of 1-SICs in dimensions d_j, d_{2j} whose normalized overlaps satisfy eqs. (3.45), (3.46) are said to be *aligned*.

In Section 7 a generalized property of 1-SIC-alignment will be defined and shown to be a consequence of our conjectures.

3.4. Proofs of Theorems 1.7 and 1.8 from the introduction.

Proof of Theorem 1.7. The result is well-known. However, existing discussions [5, 22, 38, 67] locate r-SICS in a larger context (symmetric POVMs, or fusion frames not assumed to be maximal), which obscures the fact that everything follows from maximality plus the equiangularity condition in Definition 1.2. We therefore give an independent proof.

Let $\mathcal{T}_0$ be the d^2-1 dimensional subspace of $\mathcal{L}(H_d)$ consisting of all operators A such that $\mathrm{Tr}(A)=0$. Define operators $B_j \in \mathcal{T}_0$ by

$$B_j = \sqrt{\frac{d}{r(d-r)}}\Pi_j - \sqrt{\frac{r}{d(d-r)}}I. \tag{3.47}$$

There must exist at least one set of numbers c_j, not all 0, such that

$$\sum_{j=1}^{d^2} c_j B_j = 0. \tag{3.48}$$

The c_j must satisfy, for all k

$$0 = \mathrm{Tr}\left(\left(\sum_{j=1}^{d^2} c_j B_j\right) B_k\right) = -\left(\frac{d(\alpha-r)}{r(d-r)}\right) c_k + \frac{\alpha d - r^2}{r(d-r)} \sum_{j=1}^{d^2} c_j \tag{3.49}$$

implying $c_1 = \cdots = c_{d^2} = \mu$ for some fixed, non-zero constant μ. It follows that the orthogonal complement of the B_j is 1-dimensional, implying that the B_j are a spanning set for $\mathcal{T}_0$. Substituting $c_j = \mu$ into Eq. (3.49) we deduce

$$\alpha = \frac{r(rd-1)}{d^2-1}, \tag{3.50}$$

from which Eq. (1.5) follows. We have incidentally shown that

$$\sum_{j=1}^{d^2} B_j = 0 \tag{3.51}$$

from which Eq. (1.6) follows.

Finally, let $\mathcal{S}$ be the span of the Π_j. It follows from Eq. (1.6) that $I \in \mathcal{S}$, which in turn implies the B_j are all in $\mathcal{S}$, and consequently that $\mathcal{T}_0 \subseteq \mathcal{S}$. Since every element of $\mathcal{L}(H_d)$ can be written as a linear combination of I and an element of $\mathcal{T}_0$, it follows that the Π_j are a basis for $\mathcal{L}(H_d)$. □

Proof of Theorem 1.8. Let Π be an H-projector in dimension d. It follows from Eq. (3.6) that

$$\Pi_{\mathbf{p}} = \frac{1}{d}\sum_{\mathbf{k}} \mathrm{Tr}\left(\Pi D_{\mathbf{k}}^\dagger\right) D_{\mathbf{p}} D_{\mathbf{k}} D_{\mathbf{p}}^\dagger = \frac{1}{d}\sum_{\mathbf{k}} \mathrm{Tr}\left(\Pi D_{\mathbf{k}}^\dagger\right) \omega_d^{\langle \mathbf{p},\mathbf{k}\rangle} D_{\mathbf{k}}. \tag{3.52}$$

Hence

$$\begin{aligned}\mathrm{Tr}\left(\Pi_{\mathbf{p}}\Pi_{\mathbf{q}}\right) &= \frac{1}{d}\sum_{\mathbf{k},\mathbf{k}'} \mathrm{Tr}\left(\Pi D_{\mathbf{k}}^\dagger\right) \mathrm{Tr}\left(\Pi D_{\mathbf{k}'}^\dagger\right) \omega_d^{\langle \mathbf{p},\mathbf{k}\rangle + \langle \mathbf{q},\mathbf{k}\rangle} (-1)^{\frac{d+1}{d}\langle \mathbf{k},\mathbf{k}'\rangle} \delta^{(d)}_{\mathbf{k},-\mathbf{k}'} \\ &= \frac{1}{d}\sum_{\mathbf{k}} \left|\mathrm{Tr}\left(\Pi D_{\mathbf{k}}^\dagger\right)\right|^2 \omega_d^{\langle \mathbf{p}-\mathbf{q},\mathbf{k}\rangle}\end{aligned} \tag{3.53}$$

So Π is an r-SIC fiducial if and only if

$$\begin{aligned}&\frac{1}{d}\sum_{\mathbf{k}} \left|\mathrm{Tr}\left(\Pi D_{\mathbf{k}}^\dagger\right)\right|^2 \omega_d^{\langle \mathbf{p},\mathbf{k}\rangle} = \left(\frac{rd(d-r)}{d^2-1}\right)\delta^{(d)}_{\mathbf{p},\mathbf{0}} + \frac{r(rd-1)}{d^2-1} \qquad \forall \mathbf{p} \\ \iff \qquad &\left|\mathrm{Tr}\left(\Pi D_{\mathbf{k}}^\dagger\right)\right|^2 = \frac{r(d-r)}{d^2-1} + \left(\frac{rd(rd-1)}{d^2-1}\right)\delta^{(d)}_{\mathbf{k},\mathbf{0}} \qquad \forall \mathbf{k}\end{aligned}$$

$$\iff \qquad \left|\mathrm{Tr}\left(\Pi D_{\mathbf{k}}^{\dagger}\right)\right|^2 = \frac{r(d-r)}{d^2-1} \qquad \forall \mathbf{k} \neq \mathbf{0}. \quad (3.54)$$

□

4. Units, dimensions, and binary quadratic forms

This section examines the unit group of a real quadratic field and its representations by matrices in $\mathrm{GL}_2(\mathbb{Z})$. We prove a number of results on these topics that will be needed in the sequel. We also prove some facts about the dimension towers and grids defined in Section 1.4.

In this section D will always be a fixed square free integer greater than 1, $K = \mathbb{Q}(\sqrt{D})$ the associated real quadratic field, Δ_0 the discriminant of K, and ε, d_j, f_j, $d_{j,m}$, $r_{j,m}$ the quantities specified in Definitions 1.22, 1.23, and 1.24. We will also use the following definitions.

Definition 4.1 (fundamental unit)**.** Define φ to be the smallest unit of K which is greater than 1.

Definition 4.2 (discriminant at level j)**.** The discriminant at level j of the tower is

$$\Delta_j = (d_j - 3)(d_j + 1). \quad (4.1)$$

In terms of φ one has

$$\varepsilon = \begin{cases} \varphi^2 & \text{if } \mathrm{Nm}(\varphi) = -1, \\ \varphi & \text{if } \mathrm{Nm}(\varphi) = 1, \end{cases} \quad (4.2)$$

where $\mathrm{Nm}(\varphi)$ denotes the norm of φ.

4.1. Dimension towers.

We now derive various useful relations between the between the quantities d_j and f_j as j varies. In particular, for every integer n, we will give (in Theorem 4.9) an expression for the pair (d_{nj}, r_{nj}) in terms of the pair (d_j, r_j). Our first lemma concerns that case $n = 2$.

Lemma 4.3. *For every positive integer j, the following relations hold.*

$$d_j, f_j \in \mathbb{Z} \quad (4.3)$$

$$d_j = \varepsilon^j + \varepsilon^{-j} + 1 \quad (4.4)$$

$$\Delta_j = f_j^2 \Delta_0 \quad (4.5)$$

$$d_{2j} + 1 = (d_j - 1)^2 \quad (4.6)$$

$$d_{2j} - 3 = f_j^2 \Delta_0 \quad (4.7)$$

$$\varepsilon^j = \frac{(d_j - 1) + f_j\sqrt{\Delta_0}}{2} = \frac{\sqrt{d_{2j}+1} + \sqrt{d_{2j}-3}}{2} \quad (4.8)$$

Proof. The fact that ε is an algebraic integer means

$$\varepsilon^j = n_1 + n_2\left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2}\right) \quad (4.9)$$

for some $n_1, n_2 \in \mathbb{Z}$. Hence $f_j = n_2 \in \mathbb{Z}$.

To prove (4.4), observe that it follows from Definition 1.24 that

$$d_j = \frac{\varepsilon^{2j} - \varepsilon^{-2j}}{\varepsilon^j - \varepsilon^{-j}} + 1 = \varepsilon^j + \varepsilon^{-j} + 1, \quad (4.10)$$

from which it also follows that $d_j \in \mathbb{Z}$. We then have

$$\frac{\Delta_j}{\Delta_0} = \frac{(\varepsilon^j + \varepsilon^{-j} - 2)(\varepsilon^j + \varepsilon^{-j} + 2)}{\Delta_0} = \frac{(\varepsilon^j - \varepsilon^{-j})^2}{\Delta_0} = f_j^2, \tag{4.11}$$

$$d_{2j} + 1 = \varepsilon^{2j} + \varepsilon^{-2j} + 2 = (\varepsilon^j + \varepsilon^{-j})^2 = (d_j - 1)^2, \tag{4.12}$$

$$d_{2j} - 3 = (d_j - 1)^2 - 4 = \Delta_j, \tag{4.13}$$

$$\varepsilon^j = \frac{(\varepsilon^j + \varepsilon^{-j}) + (\varepsilon^j - \varepsilon^{-j})}{2} = \frac{d_j - 1 + f_j\sqrt{\Delta_0}}{2} = \frac{\sqrt{d_{2j}+1} + \sqrt{d_{2j}-3}}{2}, \tag{4.14}$$

completing the proof. □

The next result is needed for the proof of Theorem 7.24.

Lemma 4.4. *For any pair of integers $j \geq 1$ $n > 1$,*

$$d_{nj} + 1 = \begin{cases} (d_{\frac{nj}{2}} - 1)^2 & n \equiv 0 \pmod 2, \\ (d_j + 1)\left(1 + \sum_{r=1}^{\frac{n-1}{2}} (-1)^r d_{rj}\right)^2 & n \equiv 1 \pmod 4, \\ (d_j + 1)\left(2 + \sum_{r=1}^{\frac{n-1}{2}} (-1)^r d_{rj}\right)^2 & n \equiv 3 \pmod 4. \end{cases} \tag{4.15}$$

Proof. If n is even, the result follows from (4.6). If $n = 2m + 1$, then (4.4) implies

$$\begin{aligned} \frac{d_{nj} + 1}{d_j + 1} &= \left(\frac{\varepsilon^{(m+\frac{1}{2})j} + \varepsilon^{-(m+\frac{1}{2})j}}{\varepsilon^{\frac{j}{2}} + \varepsilon^{-\frac{j}{2}}}\right)^2 \\ &= \left(\varepsilon^{mj} - \varepsilon^{(m-1)j} + \cdots - \varepsilon^{-(m-1)j} + \varepsilon^{-mj}\right)^2 \\ &= \left((-1)^m + \sum_{r=0}^{m-1} (-1)^r (d_{(m-r)j} - 1)\right)^2 \\ &= \begin{cases} \left(1 + \sum_{r=0}^{m-1} (-1)^r d_{(m-r)j}\right)^2 & m \text{ even}, \\ \left(-2 + \sum_{r=0}^{m-1} (-1)^r d_{(m-r)j}\right)^2 & m \text{ odd}, \end{cases} \\ &= \begin{cases} \left(1 + \sum_{r=1}^{m} (-1)^r d_{rj}\right)^2 & m \text{ even}, \\ \left(2 + \sum_{r=1}^{m} (-1)^r d_{rj}\right)^2 & m \text{ odd}, \end{cases} \end{aligned} \tag{4.16}$$

giving the last two cases of (4.15). □

The next result proves the monotoncity of the sequences of d_j and f_j.

Theorem 4.5. *The sequences of d_j and f_j satisfy*

$$4 \leq d_1 < d_2 < \cdots, \tag{4.17}$$

$$1 \leq f_1 < f_2 < \cdots. \tag{4.18}$$

Proof. The fact that $\varepsilon > 1$ means that, if $x > 0$, then

$$\frac{d}{dx}(\varepsilon^x + \varepsilon^{-x} + 1) = \log \varepsilon (\varepsilon^x - \varepsilon^{-x}) > 0, \tag{4.19}$$

and

$$\frac{d}{dx}\left(\frac{\varepsilon^x - \varepsilon^{-x}}{\sqrt{\Delta_0}}\right) = \log \varepsilon \left(\frac{\varepsilon^x + \varepsilon^{-x}}{\sqrt{\Delta_0}}\right) > 0. \tag{4.20}$$

Thus, the sequences $d_j = \varepsilon^j + \varepsilon^{-j} + 1$ and $f_j = \frac{\varepsilon^j - \varepsilon^{-j}}{\sqrt{\Delta_0}}$ are monotonically increasing. It is also clear that $d_1 > 3$ and $f_1 > 0$, so since they are integers, $d_1 \geq 4$ and $f_1 \geq 1$. □

We now give some special properties of the sequence of dimensions d_j associated to real quadratic fields with a unit of negative norm.

Theorem 4.6. *The following statements are equivalent:*

(1) $\mathrm{Nm}(\varphi) = -1$,
(2) $d_j - 3$ *is a perfect square for all odd values of* j,
(3) $d_j - 3$ *is a perfect square for one odd value of* j.

In that case

$$\varphi^j = \frac{\sqrt{d_j - 3} + \sqrt{d_j + 1}}{2} \tag{4.21}$$

for all $j \geq 1$. *One has,*

(a) If j *is odd, then* $d_j - 3$ *and* $\frac{d_j+1}{\Delta_0}$ *are perfect squares;*
(b) If j *is even, then* $\frac{d_j-3}{\Delta_0}$ *and* $d_j + 1$ *are perfect squares.*

Remark 4.7. As we will see, on the assumption that the Stark–Tate Conjecture and the Twisted Convolution Conjecture are both true, Theorem 4.6 explains the empirical observation [89] that, in every case calculated, the minimal multiplet in dimension d has an anti-unitary symmetry if and only if $d - 3$ is a perfect square, and that it contains a real r-SIC fiducial if in addition $d - 3$ is even.

Proof. For the equivalence of statements (1), (2), (3), see [112, Thm. 1]. If j is even, (4.21) is proved in Lemma 4.3. Suppose j is odd. Then

$$\varphi^j = m_1 + m_2 \left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2} \right) \tag{4.22}$$

for some pair of integers m_1, m_2 such that $2m_1 + m_2\Delta_0$, m_2 are both positive. The fact that $\mathrm{Nm}(\varphi^j) = -1$ means

$$\left(\frac{2m_1 + m_2\Delta_0}{2} \right)^2 - \left(\frac{m_2\sqrt{\Delta_0}}{2} \right)^2 = -1 \tag{4.23}$$

while the fact that $\varphi^{2j} + \varphi^{-2j} + 1 = d_j$ means

$$2\left(\frac{2m_1 + m_2\Delta_0}{2} \right)^2 + 2\left(\frac{m_2\sqrt{\Delta_0}}{2} \right)^2 = d_j - 1. \tag{4.24}$$

Hence

$$(2m_1 + m_2\Delta_0)^2 = d_j - 3; \tag{4.25}$$

$$\left(m_2\sqrt{\Delta_0} \right)^2 = d_j + 1. \tag{4.26}$$

Hence

$$\varphi^j = \frac{\sqrt{d_j - 3} + \sqrt{d_j + 1}}{2}. \tag{4.27}$$

This also shows that, if j is odd, then $d_j - 3$ and $\frac{d_j+1}{\Delta_0}$ are perfect squares. For the proof that $\frac{d_j-3}{\Delta_0}$ and $d_j + 1$ are perfect squares when j is even, see Lemma 4.3. □

We will now define *variant Chebyshev polynomials* and use them to express the pair (d_{nj}, f_{nj}) as a function of the pair (d_j, f_j) for any natural number n, as promised.

Definition 4.8 (variant Chebyshev polynomials)**.** For all $j \in \mathbb{N}$ define

$$T_j^*(x) = 1 + 2T_j\left(\frac{x-1}{2}\right), \tag{4.28}$$

$$U_j^*(x) = U_{j-1}\left(\frac{x-1}{2}\right) \tag{4.29}$$

where the T_j and U_j are respectively Chebyshev polynomials of the first and second kind.

Theorem 4.9. *For n, $j \in \mathbb{N}$*

$$d_{nj} = T_n^*(d_j), \tag{4.30}$$

$$f_{nj} = f_j U_n^*(d_j) \tag{4.31}$$

Proof. For the proof of (4.30), see [13, eq. (13)]. To prove (4.31), let $\theta = \log \varepsilon$. Then

$$f_{nj} = \frac{2\sinh(nj\theta)}{\sqrt{\Delta_0}} = \frac{2U_{n-1}(\cosh j\theta)\sinh j\theta}{\sqrt{\Delta_0}} = f_j U_n^*(d_j), \tag{4.32}$$

which is (4.31). □

Lemma 4.10. *$T_j^*(x)$, $U_j^*(x)$ satisfy the recursion relations*

$$T_1^*(x) = x, \quad T_2^*(x) = x(x-2), \quad T_j^*(x) = 3 - x + (x-1)T_{j-1}^*(x) - T_{j-2}^*(x), \tag{4.33}$$

$$U_1^*(x) = 1, \quad U_2^*(x) = x - 1, \quad U_j^*(x) = (x-1)U_{j-1}^*(x) - U_{j-2}^*(x). \tag{4.34}$$

For all $j \in \mathbb{N}$,

$$T_j^*(x) = \begin{cases} 3 + x^2\left(-\frac{j^2}{3} + \mathrm{O}(x)\right) & j \equiv 0 \pmod 3, \\ x\left(j + \frac{j(j-1)}{6}x + \mathrm{O}(x^2)\right) & j \equiv 1 \pmod 3, \\ x\left(-j + \frac{j(j+1)}{6}x + \mathrm{O}(x^2)\right) & j \equiv 2 \pmod 3, \end{cases} \tag{4.35}$$

$$U_j^*(x) = \begin{cases} x\left(-\frac{2j}{3} + \frac{j}{3}x + \mathrm{O}(x^2)\right) & j \equiv 0 \pmod 3, \\ 1 + x\left(\frac{j-1}{3} - \frac{(j-1)(j+2)}{6}x + \mathrm{O}(x^2)\right) & j \equiv 1 \pmod 3, \\ -1 + x\left(\frac{j+1}{3} + \frac{(j+1)(j-2)}{6}x + \mathrm{O}(x^2)\right) & j \equiv 2 \pmod 3. \end{cases} \tag{4.36}$$

Proof. Straightfoward consequence of the recursion relations for the Chebyshev polynomials. □

We are now in a position to prove some congruence and divisibility properties of the d_j and f_j.

Lemma 4.11. *Let $j, n \in \mathbb{N}$.*

(1) d_j is a divisor of d_{nj} if and only if $n \not\equiv 0 \pmod 3$.
(2) If d_j is odd, then
  (a) $\Delta_0 \equiv 0 \pmod 4$ if f_j is odd,
  (b) $\Delta_{nj} \equiv 0 \pmod 4$ for all n,
  (c) d_{nj} is odd for all n,
  (d) if f_j is even, then f_{nj} is even for all n,
  (e) if f_j is odd, then f_{nj} is odd if and only if n is odd.
(3) If d_j is even, then

(a) $\Delta_0 \equiv 1 \pmod 4$,
(b) $\Delta_{nj} \equiv 1 \pmod 4$ *if and only if* $n \not\equiv 0 \pmod 3$,
(c) d_{nj} *is even if and only if* $n \not\equiv 0 \pmod 3$,
(d) f_{nj} *is odd if and only if* $n \not\equiv 0 \pmod 3$.

Proof. Item 1 is a consequence of (4.35) and the fact that $d_j > 3$.

To prove item 2a, observe that the fact that Δ_0 is a discriminant means it is congruent to 0 or 1 modulo 4. The fact that

$$f_j^2 \Delta_0 = (d_j - 3)(d_j + 1) \tag{4.37}$$

is even, together with the fact that f_j is odd, then implies that $\Delta_0 \equiv 0 \pmod 4$.

To prove item 2b and item 2c, observe that it follows from (4.33) that, if d_j is odd, then

$$T_1^*(d_j) \equiv T_2^*(d_j) \equiv 1 \pmod 2, \tag{4.38}$$

$$\text{and } T_n^*(d_j) \equiv T_{n-2}^*(d_j) \pmod 2. \tag{4.39}$$

Consequently $d_{nj} = T_n^*(d_j)$ is odd for all n. It then follows that $\Delta_{nj} = (d_{nj} - 3)(d_{nj} + 1)$ is even for all n. Since Δ_{nj} is a discriminant, it follows that we must in fact have $\Delta_{nj} \equiv 0 \pmod 4$.

Item 2d is an immediate consequence of (4.31).

To prove item 2e observe that it follows from (4.34) that $U_n^*(d_j)$ is odd if and only if n is odd. Since f_j is odd, it follows from (4.31) that f_{nj} is odd if and only if n is odd.

To prove item 3a, observe that if d_j is even, then

$$f_j^2 \Delta_0 = \Delta_j = (d_j - 3)(d_j + 1) \equiv 1 \pmod 2, \tag{4.40}$$

implying that f_j, Δ_0, Δ_j are all odd. The statement follows from this and the fact that Δ_0 is a discriminant, which means Δ_0 is congruent to 0 or 1 modulo 4.

Item 3c is an immediate consequence of (4.35). It then follows that

$$\Delta_{nj} = (d_{nj} - 3)(d_{nj} + 1) \tag{4.41}$$

is odd if and only if $n \not\equiv 0 \pmod 3$. Item 3b is a consequence of this and the fact that Δ_{nj} is a discriminant (and thus congruent to 0 or 1 modulo 4).

Finally, (4.37) together with the fact that d_j is even means f_j is odd. In view of (4.36),

$$f_{nj} = f_j U_n^*(d_j) \equiv \begin{cases} 0 \pmod 2 & \text{if } n \equiv 0 \pmod 3, \\ 1 \pmod 2 & \text{if } n \not\equiv 0 \pmod 3. \end{cases} \tag{4.42}$$

This establishes item 3d and completes the proof. □

4.2. **Unit group of an order.** As we will see, under our conjectures, there is a natural correspondence between r-SIC multiplets and orders of the real quadratic field K. In this subsection we prove some facts about the unit group of an order which will be needed in the sequel.

Definition 4.12 (unit group, and positive norm unit group of conductor f)**.** Let $\mathcal{O}_f$ be the order of conductor f in the real quadratic field K (see Definition 1.48). Define

$$\mathcal{U}_f = \{w \in \mathcal{O}_f \colon \operatorname{Nm}(w) = \pm 1\} = \mathcal{O}_f^\times \tag{4.43}$$

to be the unit group of $\mathcal{O}_f$, and

$$\mathcal{U}_f^+ = \{w \in \mathcal{O}_f \colon \operatorname{Nm}(w) = 1\} \tag{4.44}$$

to be the subgroup of $\mathcal{U}_f$ consisting of all positive norm units.

Remark. To avoid cluttering the notation, we do not indicate the field K explicitly. It will always be clear from context.

Theorem 4.13. *Let K be a real quadratic field ,and let $f_1, f_2, \ldots$ be its associated sequence of conductors. Then, for each positive integer f, there exists a positive integer j such that $f \mid f_j$.*

Proof. It follows from the generalization of Dirichlet's unit theorem to an arbitrary order (see, for example, [68]) that

$$\mathcal{U}_f^+ = \{\pm w^n \colon n \in \mathbb{Z}\} \tag{4.45}$$

for some unit $w \neq \pm 1$. It can be assumed, without loss of generality, that $w > 1$. We then have

$$w = \varepsilon^j = \frac{d_j - 1 - f_j \Delta_0}{2} + f_j \left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2} \right) \tag{4.46}$$

for some $j \in \mathbb{N}$. The fact that $w \in \mathcal{O}_f$ implies $f \mid f_j$. □

This result motivates the following definition.

Definition 4.14 (minimum level; fundamental positive norm unit of an order)**.** Let K be a real quadratic field, and let $f_1, f_2, \ldots$ be its associated sequence of conductors. For each positive integer f, define

$$j_{\min}(f) = \min\{j \in \mathbb{N} \colon f | f_j\}, \tag{4.47}$$

and

$$\varepsilon_f = \varepsilon^{j_{\min}(f)}. \tag{4.48}$$

Remark. This definition depends on Theorem 4.13 for its validity. Note that $j_{\min}(f)$ and ε_f both depend on K as well as f, but to avoid cluttering the notation the K-dependence is not explicitly indicated. The identity of K will always be clear from context. It follows from the next theorem that ε_f is the smallest unit greater than 1 in $\mathcal{U}_f^+$.

Theorem 4.15. *Let K be a real quadratic field. Then:*

(1) For all $f \in \mathbb{N}$,

$$\mathcal{U}_f^+ = \{\pm \varepsilon_f^n \colon n \in \mathbb{Z}\}. \tag{4.49}$$

(2) For all $k \in \mathbb{N}$,

$$j_{\min}(f_k) = k. \tag{4.50}$$

(3) For all $f, j \in \mathbb{N}$,

$$f \mid f_j \iff j_{\min}(f) \mid j. \tag{4.51}$$

(4) For all $j, k \in \mathbb{N}$,

$$j \mid k \iff f_j \mid f_k \tag{4.52}$$

Proof. Statement (1). Let w, j be as in (4.45) and (4.46). The fact that $f \mid f_j$ implies $j_{\min}(f) \leq j$. On the other hand, the fact that $f \mid f_{j_{\min}(f)}$ implies

$$\varepsilon^{j_{\min}(f)} = \frac{d_{j_{\min}(f)} - 1 - f_{j_{\min}(f)} \Delta_0}{2} + f_{j_{\min}(f)} \left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2} \right) \tag{4.53}$$

is in $\mathcal{O}_f$ and consequently $\mathcal{U}_f^+$. Since $\varepsilon^{j_{\min}(f)} > 1$ we must have $\varepsilon^{j_{\min}(f)} = w^t = \varepsilon^{tj}$ for some $t \in \mathbb{N}$, implying $j_{\min}(f) \geq j$. We conclude $j_{\min}(f) = j$.

Statement (2). It follows from Theorem 4.5 that $j \geq k$ for all $j \in \{j \in \mathbb{N} \colon f_k | f_j\}$, implying $j_{\min}(f_k) \geq k$. Since k itself is in $\{j \in \mathbb{N} \colon f_k | f_j\}$, we must in fact have $j_{\min}(f_k) = k$.

Statement (3). Observe that $f \,|\, f_j$ if and only if

$$\varepsilon^j = \frac{d_j - 1 - f_j \Delta_0}{2} + f_j \left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2} \right) \tag{4.54}$$

is in $\mathcal{O}_f$, and consequently in $\mathcal{U}_f^+$. In view of Statement (1) this means $f \,|\, f_j$ if and only if $\varepsilon^j = \varepsilon_f^n$ for some $n \in \mathbb{N}$, which in turn is true if and only if $j_{\min}(f) \,|\, j$.

Statement (4). It follows from statements (2) and (3) that

$$j \,|\, k \iff j_{\min}(f_j) \,|\, k \iff f_j \,|\, f_k, \tag{4.55}$$

giving (4.52). □

We see from this that the conductor f is naturally associated to the infinite sequence of dimensions $d_{j_{\min}(f)}, d_{2j_{\min}(f)}, d_{3j_{\min}(f)}, \ldots$. As we will see, if the Stark Conjecture and Twisted Convolution Conjecture are correct, then the members of the corresponding sequence of 1-SIC multiplets are related. This is a generalization of the phenomenon of 1-SIC alignment (see [3, 8, 16] and Definition 3.22 above). As we will see, Theorem 4.6, combined with the our conjectures, tells us for which minimal multiplets (multiplets corresponding to $f = 1$) there is an anti-unitary symmetry. In the sequel we will also address the question of which non-minimal multiplets have such a symmetry. If $d_1 - 3$ is not a perfect square the question is easily answered, as it is then automatic that $\mathcal{U}_f = \mathcal{U}_f^+$ for all f. The next theorem determines for which values of f the unit group $\mathcal{U}_f$ contains a negative norm unit if $d_1 - 3$ is a perfect square.

Theorem 4.16. *Let f be any positive integer. Then the following statements are equivalent:*

(1) $\mathcal{U}_f$ contains a negative norm unit,

(2) $d_1 - 3$ is a perfect square, $j_{\min}(f)$ is odd, and the integer $\sqrt{\frac{d_{j_{\min}(f)}+1}{\Delta_0}} = \frac{f_{j_{\min}(f)}}{\sqrt{d_{j_{\min}(f)}-3}}$ is divisible by f.

In that case,

$$\mathcal{U}_f = \{\pm \varphi^{n j_{\min}(f)} \colon n \in \mathbb{Z}\}. \tag{4.56}$$

Proof. (1) $\implies$ (2). The fact that $\mathcal{U}_f$ contains a negative norm unit means φ must be negative norm. Theorem 4.6 then implies that $d_1 - 3$ is a perfect square. We may assume, without loss of generality, that the negative norm unit is greater than 1, and therefore equal to φ^j for some odd positive integer j. Since $\varepsilon^j = \varphi^{2j} \in \mathcal{U}_f^+$ we must have $j = \ell j_{\min}(f)$ for some $\ell \in \mathbb{N}$. The fact that j is odd means ℓ and $j_{\min}(f)$ are both odd. In particular $\ell = 2p + 1$ for some non-negative integer p. Since

$$\varphi^{2p j_{\min}(f)} = \varepsilon^{p j_{\min}(f)} \in \mathcal{U}_f \tag{4.57}$$

this means $\varphi^{j_{\min}(f)} \in \mathcal{U}_f$. It follows from Theorem 4.6 that

$$d_{j_{\min}(f)} - 3 = m_1^2, \tag{4.58}$$

$$d_{j_{\min}(f)} + 1 = m_2^2 \Delta_0, \tag{4.59}$$

$$f_{j_{\min}(f)}^2 = \frac{(d_{j_{\min}(f)} - 3)(d_{j_{\min}(f)} + 1)}{\Delta_0} = m_1^2 m_2^2, \tag{4.60}$$

and

$$\varphi^{j_{\min}(f)} = \frac{m_1 + m_2\Delta_0}{2} = \frac{m_1 - m_2\Delta_0}{2} + m_2\left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2}\right), \tag{4.61}$$

for some pair of positive integers m_1, m_2. The fact that $\varphi^{j_{\min}(f)} \in \mathcal{U}_f \subseteq \mathcal{O}_f$ then implies that f is a divisor of $m_2 = f_{j_{\min}(f)}/m_1$.

(2) $\implies$ (1). The fact that $d_1 - 3$ is a perfect square means, in view of Theorem 4.6, that φ is negative norm. Since $j_{\min}(f)$ is odd $\varphi^{j_{\min}(f)}$ is also negative norm. It follows from Theorem 4.6 that $\varphi^{j_{\min}(f)}$ can be written in the form of (4.61), with m_1, m_2 as given by (4.58) and (4.59). Since $f \,|\, m_2$, it follows that $\varphi^{j_{\min}(f)}$ is in $\mathcal{O}_f$, and therefore in $\mathcal{U}_f$.

To prove the last statement, suppose $\mathcal{U}_f$ contains a negative norm unit. Then it follows from the argument above that $\varphi^{j_{\min}(f)} \in \mathcal{U}_f$. So

$$\{\pm\varphi^{nj_{\min}(f)} \colon n \in \mathbb{Z}\} \subseteq \mathcal{U}_f. \tag{4.62}$$

Conversely, let w be any element of $\mathcal{U}_f$. Without loss of generality we may assume $w > 1$. Then $w = \varphi^\ell$ for some $\ell \in \mathbb{N}$. Since $\varepsilon^\ell = w^2 \in \mathcal{U}_f^+$, we must have $\ell = nj_{\min}(f)$ for some $n \in \mathbb{N}$. So $w \in \{\pm\varphi^{nj_{\min}(f)} \colon n \in \mathbb{Z}\}$. □

Definition 4.17 (fundamental unit of an order)**.** Given a real quadratic field K and positive integer f, define

$$\varphi_f = \begin{cases} \varepsilon^{j_{\min}(f)} & \text{if } \mathcal{U}_f = \mathcal{U}_f^+, \\ \varphi^{j_{\min}(f)} & \text{if } \mathcal{U}_f \supsetneq \mathcal{U}_f^+. \end{cases} \tag{4.63}$$

Corollary 4.18. *For all $f \in \mathbb{N}$*

$$\mathcal{U}_f = \{\pm\varphi_f^n \colon n \in \mathbb{N}\}. \tag{4.64}$$

Proof. Immediate consequence of Theorem 4.16. □

4.3. **Dimension grid.** So far we have been focusing on the dimension tower $d_1, d_2, \ldots$. In the sequel we will show that, if the Stark Conjecture and Twisted Convolution Conjecture are correct, these are the dimensions in which there exist 1-SICs with base field K. By contrast, it will turn out that r-SICs with base field K and $r > 1$ are found in dimensions $d_{j,m}$, with $m > 1$. The purpose of this subsection is to establish some properties of these dimensions which will be needed in the sequel.

Proposition 4.19. *Let $\theta = \log\varepsilon$. Then the following equalities hold for all $j, m \in \mathbb{N}$.*

$$r_{j,m} = \frac{\sinh mj\theta}{\sinh j\theta} \tag{4.65}$$

$$d_{j,m} = \frac{\sinh \frac{(2m+1)j\theta}{2}}{\sinh \frac{j\theta}{2}} \tag{4.66}$$

$$d_j = 1 + 2\cosh j\theta \tag{4.67}$$

Proof. Straightforward consequence of the definitions. □

Proposition 4.20. *Let K be a real quadratic field. Then the following holds for all $j \in \mathbb{N}$.*

$$1 = r_{j,1} < r_{j,2} < \cdots \tag{4.68}$$

$$3 < d_{j,1} < d_{j,2} < \cdots \tag{4.69}$$

Proof. Straightforward consequence of Proposition 4.19. □

We now characterize admissible pairs (d, r) (see Definition 1.21), which come from integer solutions (d, n, r) to the three-variable Diophantine equation $nr(d-r) = d^2 - 1$, in terms of rank and dimension grids.

Theorem 4.21. *This theorem has two parts.*

(A) Let K be a real quadratic field, and let $r_{j,m}$, $d_{j,m}$ be the associated rank and dimension grids. Then for all $j, m \in \mathbb{N}$,
(1) $0 < r_{j,m} < \frac{d_{j,m}-1}{2}$, and
(2) $(d_j + 1)r_{j,m}(d_{j,m} - r_{j,m}) = d_{j,m}^2 - 1$.

(B) Conversely, let r, d be any pair of integers such that
(1) $0 < r < \frac{d-1}{2}$, and
(2) $nr(d-r) = d^2 - 1$ for some integer $n > 4$.
Then there exists a unique real quadratic field K and unique natural numbers j, m such that $r = r_{j,m}$, $d = d_{j,m}$, and $n = d_j + 1$ where $r_{j,m}$, $d_{j,m}$ are the rank and dimension grids associated to K.

Proof. Part (A). To prove item 1, let $\theta = \log \varepsilon$. Then it follows from Proposition 4.19 that

$$\begin{aligned}
\frac{d_{j,m}-1}{2} - r_{j,m} &= \frac{\sinh \frac{(2m+1)j\theta}{2}}{2\sinh\frac{j\theta}{2}} - \frac{1}{2} - \frac{\sinh mj\theta}{\sinh j\theta} \\
&= \frac{\sinh mj\theta \cosh\frac{j\theta}{2} + \cosh mj\theta \sinh\frac{j\theta}{2}}{2\sinh\frac{j\theta}{2}} - \frac{1}{2} - \frac{\sinh mj\theta}{\sinh j\theta} \\
&= \frac{\sinh mj\theta}{\sinh j\theta}\left(\cosh^2\frac{j\theta}{2} - 1\right) + \frac{1}{2}\left(\cosh mj\theta - 1\right) \\
&> 0.
\end{aligned} \tag{4.70}$$

The fact that $0 < r_{j,m}$ is immediate. To prove item 2, observe Proposition 4.19 also implies

$$\begin{aligned}
(d_j + 1)r_{j,m}(d_{j,m} - 1) &= (d_j + 1)r_{j,m}r_{j,m+1} \\
&= \frac{2(1+\cosh j\theta)\sinh mj\theta \sinh(m+1)j\theta}{\sinh^2 j\theta} \\
&= \frac{\sinh mj\theta \sinh(m+1)j\theta}{\sinh^2\frac{j\theta}{2}} \\
&= \frac{\cosh(2m+1)j\theta - \cosh j\theta}{2\sinh^2\frac{j\theta}{2}} \\
&= \frac{\sinh^2\frac{(2m+1)j\theta}{2} - \sinh^2\frac{j\theta}{2}}{\sinh^2\frac{j\theta}{2}} \\
&= d_{j,m}^2 - 1.
\end{aligned} \tag{4.71}$$

Part (B). The fact that $nr(d-r) = d^2 - 1$ implies

$$d = \frac{nr \pm \sqrt{r^2 n(n-4) + 4}}{2} \tag{4.72}$$

The fact that $n > 4$ means $K = \mathbb{Q}\left(\sqrt{n(n-4)}\right)$ is a real quadratic field. Let Δ_0 be its discriminant, and f_j, d_j, $d_{j,m}$, $r_{j,m}$ the associated conductors, dimensions, and ranks. It then follows from Theorem 3.20 that $n = d_j + 1$ for some j. So

$$d = \frac{r(d_j+1) \pm \sqrt{r^2 f_j^2 \Delta_0 + 4}}{2} \tag{4.73}$$

Since d is an integer we must have

$$r^2 f_j^2 \Delta_0 + 4 = p^2 \tag{4.74}$$

for some $p \in \mathbb{N}$. Let

$$w_\pm = \frac{p \pm r f_j \sqrt{\Delta_0}}{2}. \tag{4.75}$$

Then $w_\pm$ are positive norm units in K, with $0 < w_- < 1 < w_+$. So $w_\pm = \varepsilon^{\pm k}$ for some positive integer k. We then have

$$p = \varepsilon^k + \varepsilon^{-k} = d_k - 1 \tag{4.76}$$

and

$$\begin{aligned} & r f_j \sqrt{\Delta_0} = \varepsilon^k - \varepsilon^{-k} \\ \Longrightarrow \qquad & r f_j = f_k \end{aligned} \tag{4.77}$$

In view of Theorem 4.15, this means $k = jm$ for some $m \in \mathbb{N}$. Consequently,

$$r = r_{j,m} \tag{4.78}$$

and

$$d = \frac{r_{j,m}(d_j+1) \pm (d_{jm} - 1)}{2}. \tag{4.79}$$

Setting $\theta = \log \varepsilon$ and using Proposition 4.19 the second expression becomes

$$\begin{aligned} d &= \frac{\sinh mj\theta\,(1 + \cosh j\theta)}{\sinh j\theta} \pm \cosh mj\theta \\ &= \frac{\sinh mj\theta + \sinh(m \pm 1)j\theta}{\sinh j\theta} \\ &= r_{j,m} + r_{j,m\pm 1}. \end{aligned} \tag{4.80}$$

The fact that $d \geq 2r$, together with Lemma 4.20, means we must in fact have

$$d = r_{j,m} + r_{j,m+1} = d_{j,m}. \tag{4.81}$$

It remains to prove uniqueness. Suppose $r = r'_{j',m'}$ and $d = d'_{j',m'}$, where $r'_{j',m'}$ and $d'_{j',m'}$ are in the rank and dimension towers associated to some other real quadratic field K'. Then it follows from Part (A) that

$$\begin{aligned} (d'_{j'}+1) r(d-r) &= (d'_j + 1) r'_{j',m'} (d'_{j',m'} - r'_{j',m'}) \\ &= d'^2_{j',m'} - 1 \\ &= d^2_{j,m} - 1 \\ &= (d_j + 1) r_{j,m}(d_{j,m} - r_{j,m}) \\ &= (d_j + 1) r(d-r), \end{aligned} \tag{4.82}$$

implying $d'_{j'} = d_j$. Hence

$$K' = \mathbb{Q}\left(\sqrt{(d'_{j'}+1)(d'_{j'}-3)}\right) = \mathbb{Q}\left(\sqrt{(d_j+1)(d_j-3)}\right) = K \tag{4.83}$$

and $j' = j$. Consequently $d_{j,m'} = d_{j,m}$ which, together with the fact that $d_{j,1}, d_{j,2}, \ldots$ is a monotonically increasing sequence (see Proposition 4.20), implies $m' = m$. □

This result implies the following expression for $\tilde{\mu}_{\mathbf{p}}(t)$, as an alternative to (1.47).

Corollary 4.22. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple. Then*

$$\tilde{\mu}_{\mathbf{p}}(t) = \frac{1}{\sqrt{d_j+1}}\,\tilde{\nu}_{\mathbf{p}}(t), \qquad \mu_{\mathbf{p}}(s) = \frac{1}{\sqrt{d_j+1}}\nu_{\mathbf{p}}(s) \tag{4.84}$$

for all $\mathbf{p} \not\equiv \mathbf{0} \pmod{d}$.

Proof. Immediate consequence of

$$(d_j+1)r_{j,m}(d_{j,m} - r_{j,m}) = d_{j,m}^2 - 1 \tag{4.85}$$

from Theorem 4.21(A)(2). □

Corollary 4.23. *$d_{j,m}$ is coprime to $r_{j,m}$ for all $j, m \in \mathbb{N}$.*

Proof. Immediate consequence of (4.85). □

The next lemma collects together various technical results which will be needed in the sequel.

Lemma 4.24. *The following inequalities and equations hold for all $j, m \in \mathbb{N}$.*

$$r_{j,m} < r_{j,m+1} - 1 \tag{4.86}$$

$$r_{j,m} < \frac{d_{j,m}-1}{2} \tag{4.87}$$

$$r_{j,m+1} - r_{j,m} = \sqrt{\frac{d_{(2m+1)j}+1}{d_j+1}} \tag{4.88}$$

$$r_{j,m+1}^2 - r_{j,m}^2 = r_{j,2m+1} \tag{4.89}$$

$$\varepsilon^{(2m+1)j} - 1 = d_{j,m}\varepsilon^{mj}(\varepsilon^j - 1) \tag{4.90}$$

$$d_{j,m+2} = (d_j - 1)d_{j,m+1} - d_{j,m} \tag{4.91}$$

If d_j is even, then

(1) $r_{j,m}$ is even if and only if $m \equiv 0 \pmod 3$;
(2) $d_{j,m}$ is even if and only if $m \equiv 1 \pmod 3$.

If d_j is odd, then

(1) $r_{j,m}$ is odd if and only if m is odd;
(2) $d_{j,m}$ is odd for all m.

If $d_{j,m}$ is even, then the following congruences hold.

$$d_{(m+1)j} - d_{mj} \equiv d_j \pmod 4 \tag{4.92}$$

$$d_{j,m} \equiv d_j \pmod 4 \tag{4.93}$$

$$r_{j,m+1} - r_{j,m} \equiv d_j + 2 \pmod 4 \tag{4.94}$$

$$f_{j(m+1)} - f_{jm} \equiv d_j + 2 \pmod 4 \tag{4.95}$$

Proof. It follows from Proposition 4.19 that

$$r_{j,m+1} = \frac{\sinh j(m+1)\theta}{\sinh j\theta} = \frac{\sinh jm\theta \cosh j\theta}{\sinh j\theta} + \cosh jm\theta > r_{j,m} + 1, \tag{4.96}$$

$$\frac{d_{j,m}-1}{2} = \frac{r_{j,m+1}+r_{j,m}-1}{2} > r_{j,m}, \tag{4.97}$$

$$\begin{aligned} r_{j,m+1} - r_{j,m} &= \frac{\sinh j(m+1)\theta - \sinh jm\theta}{\sinh j\theta} \\ &= \frac{\cosh \frac{(2m+1)j\theta}{2}}{\cosh \frac{j\theta}{2}} \\ &= \sqrt{\frac{\cosh(2m+1)j\theta + 1}{\cosh j\theta + 1}} \\ &= \sqrt{\frac{d_{(2m+1)j}+1}{d_j+1}}, \end{aligned} \tag{4.98}$$

$$\begin{aligned} r_{j,m+1}^2 - r_{j,m}^2 &= \frac{\sinh^2(m+1)j\theta - \sinh^2 mj\theta}{\sinh^2 j\theta} \\ &= \frac{\cosh 2(m+1)j\theta - \cosh 2mj\theta}{2\sinh^2 j\theta} \\ &= \frac{\cosh 2mj\theta \cosh 2j\theta + \sinh 2mj\theta \sinh 2j\theta - \cosh 2mj\theta}{2\sinh^2 j\theta} \\ &= \frac{\cosh 2mj\theta \sinh^2 j\theta + \sinh 2mj\theta \sinh j\theta \cosh j\theta}{\sinh^2 j\theta} \\ &= \frac{\sinh(2m+1)j\theta}{\sinh j\theta} \\ &= r_{j,2m+1}, \end{aligned} \tag{4.99}$$

$$\begin{aligned} d_{j,m}\varepsilon^{mj}(\varepsilon^j - 1) &= \frac{\sinh \frac{(2m+1)j\theta}{2} e^{mj\theta}\left(e^{j\theta}-1\right)}{\sinh \frac{j\theta}{2}} \\ &= e^{(2m+1)j\theta} - 1 \\ &= \varepsilon^{(2m+1)j} - 1. \end{aligned} \tag{4.100}$$

It follows from Theorem 4.9 and Lemma 4.10 that

$$\begin{aligned} d_{j,m+2} &= r_{j,m+3} + r_{j,m+2} \\ &= U_{m+3}^*(d_j) + U_{m+2}^*(d_j) \\ &= (d_j - 1)\left(U_{m+2}^*(d_j) + U_{m+1}^*(d_j)\right) - \left(U_{m+1}^*(d_j) + U_m^*(d_j)\right) \\ &= (d_j - 1)d_{j,m+1} - d_{j,m}. \end{aligned} \tag{4.101}$$

Suppose d_j is even. Then (4.31) and (4.36) imply

$$r_{j,m} = U_m^*(d_j) = \begin{cases} 0 & \text{if } m \equiv 0 \pmod 3, \\ 1 & \text{otherwise,} \end{cases} \tag{4.102}$$

from which it follows that $d_{j,m} = r_{j,m} + r_{j,m+1}$ is even if and only if $m \equiv 1 \pmod 3$.

Suppose d_j is odd. Then (4.34) implies $U^*_{j,1}$ is odd, $U^*_{j,2}$ is even, and $U^*_{j,m} \equiv U^*_{j,m-2} \pmod 2$ for all $m > 2$. Consequently $r_{j,m} = U^*_m(d_j)$ is odd if and only m is odd, and $d_{j,m} = U^*_{m+1}(d_j) + U^*_m(d_j)$ is odd for all m.

Suppose $d_{j,m}$ is even. Then it follows from results just proved that d_j is even and $m \equiv 1 \pmod 3$. Eq. (4.35) then implies

$$d_{(m+1)j} - d_{mj} = T^*_{m+1}(d_j) - T^*_m(d_j) \equiv -(2m+1)d_j \pmod{d_j^2} \tag{4.103}$$

$$\equiv d_j \pmod 4, \tag{4.104}$$

while (4.36) implies

$$\begin{aligned} d_{j,m} &= r_{j,m+1} + r_{j,m} \\ &= U^*_{m+1}(d_j) + U^*_m(d_j) \\ &\equiv \frac{(2m+1)d_j}{3} \pmod{d_j^2} \\ &\equiv d_j \pmod 4, \end{aligned} \tag{4.105}$$

$$\begin{aligned} r_{j,m+1} - r_{j,m} &= U^*_{m+1}(d_j) - U^*_m(d_j) \\ &\equiv -2 + d_j \pmod{d_j^2} \\ &\equiv d_j + 2 \pmod 4. \end{aligned} \tag{4.106}$$

Finally, it follows from Lemma 4.11 that f_j is odd, and thus

$$f_{(m+1)j} - f_{mj} = f_j\,(r_{j,m+1} - r_{j,m}) \equiv d_j + 2 \pmod 4, \tag{4.107}$$

completing the proof. □

Lemma 4.25. *Let $r^{-1}_{j,m}$ be the multiplicative inverse of $r_{j,m}$ modulo $\bar{d}_{j,m}$. Then*

$$r^{-1}_{j,m} \equiv r_{j,m}\,(1 + d_j + d_{j,m}) \pmod{\bar{d}_{j,m}}. \tag{4.108}$$

Proof. It follows from Theorem 4.21 that

$$(d_j + 1)r_{j,m}(r_{j,m} - d_{j,m}) \equiv 1 - d^2_{j,m} \equiv 1 \pmod{\bar{d}_{j,m}}. \tag{4.109}$$

If $d_{j,m}$ is even, then it follows from Corollary 4.23 and Lemma 4.24 that $d_j + 1$ and $r_{j,m}$ are both odd. So (4.109) implies

$$(d_j + 1)r^2_{j,m} + d_{j,m} \equiv 1 \pmod{\bar{d}_{j,m}}. \tag{4.110}$$

Consequently

$$r^{-1}_{j,m} \equiv (d_j + 1)r_{j,m} + d_{j,m}r^{-1}_{j,m} = (d_j + 1)r_{j,m} + d_{j,m} \pmod{\bar{d}_{j,m}}. \tag{4.111}$$

In view of Corollary 4.23 we can alternatively write

$$r^{-1}_{j,m} \equiv r_{j,m}(1 + d_j + d_{j,m}) \pmod{\bar{d}_{j,m}}. \tag{4.112}$$

□

Lemma 4.26. *$d_j \pm 1$ are coprime to $d_{j,m}$ for all $j, m \in \mathbb{N}$.*

Proof. The fact that $d_j + 1$ is coprime to $d_{j,m}$ is an immediate consequence of the relation

$$(d_j + 1)r_{j,m}(d_{j,m} - r_{j,m}) = d^2_{j,m} - 1 \tag{4.113}$$

proved in Theorem 4.21.

To prove that $d_j - 1$ is coprime to $d_{j,m}$ observe that it follows from Lemma 4.24 that

$$d_{j,m} \equiv -d_{j,m-2} \pmod{d_j - 1} \tag{4.114}$$

for all $m > 2$. Consequently

$$d_{j,m} \equiv \begin{cases} \pm d_{j,1} \pmod{(d_j - 1)} & \text{if } m \text{ odd} \\ \pm d_{j,2} \pmod{(d_j - 1)} & \text{if } m \text{ even} \end{cases} \tag{4.115}$$

Since

$$d_{j,1} \equiv d_j \equiv 1 \pmod{d_j - 1} \tag{4.116}$$

and

$$d_{j,2} = (d_j - 1)^2 + (d_j - 1) - 1 \equiv -1 \pmod{d_j - 1}, \tag{4.117}$$

it follows that $d_{j,m} \equiv \pm 1 \pmod{d_j - 1}$, and $d_{j,m}$ is thus coprime to $d_j - 1$, for all $j, m \in \mathbb{N}$. □

4.4. **Representations.** An important role in the following is played by what we refer to as *canonical representations* of the real quadratic base field K. These are faithful $\mathbb{Q}$-algebra representations of K by 2×2 matrices. All such representations are isomorphic, justifying the term *canonical*. However, up to equality, there are multiple canonical representations, and they are in natural bijective correspondence with the set of forms associated to K (recall the definition of *form* in Section 1.3). This correspondence in turn leads to a natural correspondence between extended Clifford group orbits of r-SICs and equivalence classes of forms.

The purpose of this subsection is to derive the results on canonical representations which will be needed in the sequel. We begin with some preliminary definitions and lemmas.

Definition 4.27 (matrices; symmetric matrices; trace-zero matrices)**.** Let R be a commutative ring with identity. Then

(1) $\mathcal{M}(R)$ is the ring of 2×2 matrices over R,
(2) $\mathcal{M}_{\mathrm{S}}(R) \subseteq \mathcal{M}(R)$ is the subring of symmetric matrices,
(3) $\mathcal{M}_0(R) \subseteq \mathcal{M}(R)$ is the additive subgroup of trace-zero matrices.

Definition 4.28 (matrix sub-algebra)**.** If R is a field and $M_1, \ldots, M_n \in \mathcal{M}(R)$, then $R\langle M_1, \ldots, M_n \rangle$ denotes the R-subalgebra of $\mathcal{M}(R)$ generated by the matrices M_j.

Definition 4.29 (generators of $\mathrm{SL}_2(\mathbb{Z})$)**.** Let

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{4.118}$$

be the usual generators of $\mathrm{SL}_2(\mathbb{Z})$.

Lemma 4.30. *Let R be a commutative ring with identity.*

(1) If $M \in \mathcal{M}_0(R)$, then $M^2 = -\det(M) I$.
(2) The map $M \mapsto SM$ is a bijection of $\mathcal{M}_{\mathrm{S}}(R)$ onto $\mathcal{M}_0(R)$.

Suppose further that R is a field.

(3) If $M, M' \in \mathcal{M}_0(R)$ are both non-zero, then $MM' = M'M$ if and only if $M' = \lambda M$ for some non-zero $\lambda \in R$.
(4) If $M \in \mathcal{M}_0(R)$, then

$$R\langle I, M \rangle = \{xI + yM : x, y \in R\}. \tag{4.119}$$

Proof. Statements (1), (2) are immediate consequences of the definitions. To prove (3) let $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & -\alpha \end{smallmatrix}\right)$, $M' = \left(\begin{smallmatrix} \alpha' & \beta' \\ \gamma' & -\alpha' \end{smallmatrix}\right)$. Then

$$MM' - M'M = \begin{pmatrix} (\beta\gamma' - \gamma\beta') & 2(\alpha\beta' - \beta\alpha') \\ 2(\gamma\alpha' - \alpha\gamma') & -(\beta\gamma' - \gamma\beta') \end{pmatrix}, \tag{4.120}$$

from which the statement follows. To prove (4), let $\mathcal{A} = \{xI + yM : x, y \in R\}$. In view of (1), $\mathcal{A}$ is closed under addition and multiplication, and is therefore a sub-algebra which contains I, M, and is contained in $R\langle I, M\rangle$. □

We now define canonical representations of K and prove a proposition giving their basic properties. The following definition and proposition would be exactly the same (with minor modifications to the proof) if K were replaced by an arbitrary degree n number field and $\mathcal{M}(\mathbb{Q})$ were replaced by the $\mathbb{Q}$-algebra of $n \times n$ matrices (where the n is the same on both sides).

Definition 4.31 (canonical representation)**.** A *canonical representation* of K is a map $\chi : K \to \mathcal{M}(\mathbb{Q})$ that is a $\mathbb{Q}$-algebra isomorphism of K onto a sub-algebra of $\mathcal{M}(\mathbb{Q})$.

Proposition 4.32. *Let $\chi : K \to \mathcal{M}(\mathbb{Q})$ be a canonical representation. Then χ enjoys the following properties.*

(1) The map χ is isomorphic to the "multiplication map" representation $\chi_0 : K \to \mathcal{L}_{\mathbb{Q}}(K)$ given by $(\chi_0(\kappa))(\kappa') = \kappa\kappa'$, where $\mathcal{L}_{\mathbb{Q}}(K)$ is the $\mathbb{Q}$-algebra of $\mathbb{Q}$-linear maps from K to K.
(2) The map χ turns norms into determinants, so that $\mathrm{Nm}(\kappa) = \det(\chi(\kappa))$ for all $\kappa \in K$.
(3) The map χ preserves traces in the sense that $\mathrm{Tr}(\kappa)$, the number field trace of κ, is equal to $\mathrm{Tr}(\chi(\kappa))$, the matrix trace of $\chi(\kappa)$, for all $\kappa \in K$.

Proof. Write $K = \kappa_1\mathbb{Q} + \kappa_2\mathbb{Q}$. Identify $\mathcal{L}_{\mathbb{Q}}(K)$ with $\mathcal{M}(\mathbb{Q})$, so that for any $\kappa \in K$, the linear transformation $\chi_0(\kappa)$ is represented by a matrix $M = \left(\begin{smallmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{smallmatrix}\right) \in \mathcal{M}(\mathbb{Q})$ such that $\kappa\kappa_i = m_{i1}\kappa_1 + m_{i2}\kappa_2$ for $i \in \{1, 2\}$.

Fix some $v_0 \in \mathcal{M}(\mathbb{Q})$ such that $v_1 := \chi(\kappa_1)v_0$ and $v_2 := \chi(\kappa_2)v_0$ are linearly independent. Then, for any $\kappa \in K$,

$$\chi(\kappa)v_i = \chi(\kappa)\chi(\kappa_i)v_0 = \chi(\kappa\kappa_i)v_0 = \chi(m_{i1}\kappa_1 + m_{i2}\kappa_2)v_0 = m_{i1}v_1 + m_{i2}v_2. \tag{4.121}$$

Thus, $\chi(\kappa)$ is represented by M in the basis $\{v_1, v_2\}$ of $\mathbb{Q}^2$. So χ is isomorphic to χ_0 as a $\mathbb{Q}$-algebra representation of K; that is, property (1) holds.

Property (2) and (3) follow, because the norm $\mathrm{Nm}(\kappa)$ is defined to be the determinant of $\chi_0(\kappa)$ (or, equivalently, the determinant of M), and the number field trace $\mathrm{Tr}(\kappa)$ is defined to be the trace of $\chi_0(\kappa)$ (or, equivalently, the trace of M). □

We will now use the fact that K is a quadratic field to parametrize all canonical representations up to equality by (binary quadratic) forms Q.

Definition 4.33 (canonical representation associated to a form)**.** Given a form Q associated to K with conductor f, define $\chi_Q : K \to \mathcal{M}(\mathbb{Q})$ to be the map specified by

$$\chi_Q\left(x + y\sqrt{\Delta_0}\right) = xI + \frac{2y}{f}SQ \tag{4.122}$$

for all $x, y \in \mathbb{Q}$.

Theorem 4.34. *For every form Q associated to K, the map χ_Q is a canonical representation of K. Conversely, if χ is a canonical representation of K, then there exists a form Q associated to K such that $\chi = \chi_Q$.*

Proof. Let Q be a form associated to K with conductor f. It is immediate that χ_Q is a $\mathbb{Q}$-linear monomorphism of K into $\mathcal{M}(\mathbb{Q})$. To show that it is a $\mathbb{Q}$-algebra monomorphism, observe that it follows from Lemma 4.30 that

$$(SQ)^2 = -\det(SQ)I = \frac{1}{4}f^2\Delta_0 I. \tag{4.123}$$

Hence

$$\begin{aligned}\chi_Q\left(x+y\sqrt{\Delta_0}\right)\chi_Q\left(x'+y'\sqrt{\Delta_0}\right) &= xx'I + \frac{4yy'}{f^2}(SQ)^2 + \frac{2(xy'+x'y)}{f}SQ \\ &= \chi_Q\left(\left(x+y\sqrt{\Delta_0}\right)\left(x'+y'\sqrt{\Delta_0}\right)\right)\end{aligned} \tag{4.124}$$

for all $x, y, x', y' \in \mathbb{Q}$. So χ_Q is a canonical representation of K.

Conversely, suppose χ is an arbitrary canonical representation of K. Define

$$L_1 = \chi(1), \qquad L_2 = \chi(\sqrt{\Delta_0}). \tag{4.125}$$

We have $\mathrm{Tr}(L_1) = 2$ and $L_1^2 = L_1$. Consequently $I - L_1 \in \mathcal{M}_0$ and $(I-L_1)^2 = I - L_1$. In view of Lemma 4.30 this means

$$I - L_1 = -\det(I - L_1)I. \tag{4.126}$$

So $L_1 = kI$ for some k. The fact that $\mathrm{Tr}(L_1) = 2$ means $k = 1$, implying $L_1 = I$.

Turning to L_2, the fact that $\mathrm{Tr}(L_2) = \mathrm{Tr}(\Delta_0)$ implies, by another application of Lemma 4.30, that

$$L_2 = SM \tag{4.127}$$

for some $M \in \mathcal{M}_{\mathrm{S}}(\mathbb{Q})$. We can write M in the form

$$M = qQ, \qquad Q = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \tag{4.128}$$

with $q \in \mathbb{Q}$ and a, b, c coprime integers. The fact that $\det(L_2) = \mathrm{Nm}(\sqrt{\Delta_0})$ means

$$\Delta_0 = \frac{q^2\Delta}{4} \tag{4.129}$$

where $\Delta = b^2 - 4ac$ is the discriminant of Q. Let D, D' be the square-free parts of Δ_0, Δ respectively. Then $n^2D = m^2D'$ for some $n, m \in \mathbb{Z}$, implying $D' = D$. So Q is associated to K, and $\Delta = f^2\Delta_0$ where f is the conductor of Q. It follows that $q = 2/f$ implying

$$L_2 = \frac{2}{f}SQ. \tag{4.130}$$

Hence $\chi = \chi_Q$. □

Theorem 4.35. *Let Q be a form associated to K and let f be its conductor. Let $\mathcal{O}_f, \mathcal{U}_f$ be the order and unit group with conductor f (see Definition 4.12). Then χ_Q restricts to*

(1) a ring isomorphism of $\mathcal{O}_f$ onto $\mathbb{Z}\langle I, SQ\rangle \cap \mathcal{M}(\mathbb{Z})$,
(2) a group isomorphism of $\mathcal{U}_f$ onto $\mathbb{Z}\langle I, SQ\rangle \cap \mathrm{GL}_2(\mathbb{Z})$.

Proof. Statement (1). Let $\kappa \in \mathcal{O}_f$ be arbitrary. Then

$$\kappa = x + yf\left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2}\right) \tag{4.131}$$

for some $x, y \in \mathbb{Z}$. Setting $Q = \left(\begin{smallmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{smallmatrix}\right)$, we have

$$\chi_Q(\kappa) = \left(x + \frac{yf\Delta_0}{2}\right) I + ySQ = \begin{pmatrix} x + \frac{y(f\Delta_0 - b)}{2} & -yc \\ ya & x + \frac{y(f\Delta_0 + b)}{2} \end{pmatrix}. \tag{4.132}$$

The fact that $f^2\Delta_0 = b^2 - 4ac$ means $f\Delta_0 \equiv b \pmod 2$. So $\chi_Q(\kappa) \in \langle I, SQ\rangle \cap \mathcal{M}(\mathbb{Z})$.

Conversely, suppose $L \in \mathbb{Z}\langle I, SQ\rangle \cap \mathcal{M}(\mathbb{Z})$. Then it follows from Lemma 4.30 that

$$L = xI + ySQ \tag{4.133}$$

for some $x, y \in \mathbb{Q}$. So

$$L = \chi_Q(\kappa), \qquad \kappa = \left(x - \frac{yf\Delta_0}{2}\right) + yf\left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2}\right). \tag{4.134}$$

Moreover, the fact that

$$L = \begin{pmatrix} x - \frac{yb}{2} & -yc \\ ya & x + \frac{yb}{2} \end{pmatrix} \in \mathcal{M}(\mathbb{Z}) \tag{4.135}$$

means ya, yc and $yb = (x + yb/2) - (x - yb/2)$ are all in $\mathbb{Z}$. Since a, b, c are coprime, it follows that $y \in \mathbb{Z}$. Also the fact that $x - yb/2 \in \mathbb{Z}$, together with the fact that $f\Delta_0 \equiv b \pmod 2$, means

$$x - \frac{yf\Delta_0}{2} = x - \frac{yb}{2} - \frac{y\,(f\Delta_0 - b)}{2} \in \mathbb{Z}. \tag{4.136}$$

So $\kappa \in \mathcal{O}_f$.

Statement (2). It follows from Statement (1) that χ_Q maps $\mathcal{U}_f$ into a multiplicative subgroup of $\mathbb{Z}\langle I, SQ\rangle \cap \mathcal{M}(\mathbb{Z})$. The fact that $\det(\chi_Q(\kappa)) = \mathrm{Nm}(\kappa)$ for all κ means that, if $\kappa \in \mathcal{U}_f$, then $\det(\chi_Q(\kappa)) = \pm 1$ implying $\chi_Q(\kappa) \in \mathbb{Z}\langle I, SQ\rangle \cap \mathrm{GL}_2(\mathbb{Z})$. It also means that, if $\chi_Q(\kappa) \in \mathbb{Z}\langle I, SQ\rangle \cap \mathrm{GL}_2(\mathbb{Z})$, then $\mathrm{Nm}(\kappa) = \pm 1$. Since Statement (1) implies $\kappa \in \mathcal{O}_f$ we must have $\kappa \in \mathcal{U}_f$. □

Corollary 4.36. *Let Q be a form associated to K, and let f be its conductor. Let $\kappa \in \mathcal{O}_f$ and $n \in \mathbb{N}$ be arbitrary. Then $\kappa \in n\mathcal{O}_f$ if and only if $\chi_Q(\kappa) \in n\mathcal{M}(\mathbb{Z})$.*

Proof. Necessity is immediate. Suppose, on the other hand, that $\chi_Q(\kappa) = nL$ for $L \in \mathcal{M}(\mathbb{Z})$. It follows from Theorem 4.35 that $nL \in \mathbb{Z}\langle I, SQ\rangle$. So L is also in $\mathbb{Z}\langle I, Q\rangle$. By another application of Theorem 4.35, $L = \chi_Q(a)$ for some $a \in \mathcal{O}_f$. Hence $\kappa = na \in n\mathcal{O}_f$. □

4.5. **Stability groups and maximal abelian subgroups of $\mathrm{GL}_2(\mathbb{Z})$.** The purpose of this subsection is to prove some results concerning the stability group of a form, which, as we will see, is the same thing as a maximal abelian subgroup of $\mathrm{GL}_2(\mathbb{Z})$.

In order to treat arbitrary maximal abelian subgroups of $\mathrm{GL}_2(\mathbb{Z})$ we need to temporarily relax the restrictions in Section 1.3 on the definition of *form*. We continue to assume without comment that the forms with which we deal are binary, quadratic, integral, and primitive. However, in this subsection (and nowhere else) we drop the assumption that they are irreducible and indefinite.

We now investigate the properties of $\mathcal{S}(Q)$, the stability group of Q as specified in Definition 1.20.

Lemma 4.37. *For all $M \in \mathrm{GL}_2(\mathbb{Z})$,*

$$\det(M) M^{\mathrm{T}} = -SM^{-1}S. \tag{4.137}$$

Proof. Write $M = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right)$. Then

$$SM^{-1}S = \frac{1}{\det M}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = -\frac{1}{\det M}\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix}, \tag{4.138}$$

as desired. □

Theorem 4.38. *Let Q be a form and $\mathcal{S}(Q)$ its stability group (as in Definition 1.20). Then:*

(1) $\mathcal{S}(Q)$ is the centralizer of SQ in $\mathrm{GL}_2(\mathbb{Z})$.
(2) $\mathcal{S}(Q) = \mathbb{Z}\langle I, SQ\rangle \cap \mathrm{GL}_2(\mathbb{Z})$.
(3) For all $M \in \mathcal{S}(Q)$, there exist unique integers t, n such that

$$M = \frac{t}{2}I + nSQ. \tag{4.139}$$

(4) $\mathcal{S}(Q)$ is abelian.

Proof. Statement (1). For all $M \in \mathrm{GL}_2(\mathbb{Z})$,

$$Q_M = Q \tag{4.140}$$
$$\iff \quad \det(M)M^{\mathrm{T}}QM = Q \tag{4.141}$$
$$\iff \quad -SM^{-1}SQM = Q \tag{4.142}$$
$$\iff \quad SQM = MSQ, \tag{4.143}$$

where Q_M is as defined in (1.31) and where we used Lemma 4.37 in the second step.

Statement (2). Let M be any element of the centralizer of SQ, and let

$$M_0 = M - \frac{1}{2}\operatorname{Tr}(M)I. \tag{4.144}$$

Then M_0 commutes with SQ. Since M_0 and SQ are both trace-zero, it follows from Lemma 4.30 that

$$M_0 = \lambda SQ \tag{4.145}$$

for some non-zero $\lambda \in \mathbb{Q}$. So M belongs to $\mathbb{Z}\langle I, SQ\rangle$ and therefore to $\mathbb{Z}\langle I, SQ\rangle \cap \mathrm{GL}_2(\mathbb{Z})$.

Conversely, if $M \in \mathbb{Z}\langle I, SQ\rangle \cap \mathrm{GL}_2(\mathbb{Z})$ then it follows from Lemma 4.30 that M is a linear combination of I and SQ and is therefore in the centralizer of SQ.

Statement (3). Let $Q = \langle a, b, c\rangle$, and let $M \in \mathcal{S}(Q)$. It follows from Statement (2) that

$$M = \begin{pmatrix}\frac{t-nb}{2} & -nc\\ na & \frac{t+nb}{2}\end{pmatrix} \tag{4.146}$$

for some $t, n \in \mathbb{Q}$. We must have $t, na, nb, nc \in \mathbb{Z}$. Since a, b, c are coprime, it follows that $n \in \mathbb{Z}$. Suppose that t', n' are any other pair of integers such that $M = (t'/2)I + n'SQ$. Then

$$t' = \operatorname{Tr}(M) = t \tag{4.147}$$

and, consequently, $n'Q = nQ$, implying $n' = n$.

Statement (4). Immediate consequence of Statement (2). □

Theorem 4.39. *For each $M = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}) \setminus \{\pm I\}$ there exists a unique form $Q(M)$ such that $M \in \mathcal{S}(Q(M))$ and $\operatorname{sgn}(M) = \operatorname{sgn}(Q(M))$. Explicitly,*

$$Q(M) = \frac{1}{n_M}\begin{pmatrix}\gamma & \frac{\delta-\alpha}{2}\\ \frac{\delta-\alpha}{2} & -\beta\end{pmatrix} \tag{4.148}$$

where

$$n_M = \gcd(\beta, \gamma, \alpha - \delta). \tag{4.149}$$

Setting

$$t_M = \mathrm{Tr}(M), \tag{4.150}$$

one then has

$$M = \frac{t_M}{2} I + n_M SQ(M). \tag{4.151}$$

Remark 4.40. When reading Theorem 4.39, one should keep in mind that, in this subsection, forms are not assumed to be irreducible or indefinite.

Proof. Let $Q(M), n_M, t_M$ be as defined in (4.148)–(4.150). The fact that $M \neq \pm I$ means n_M is non-zero, and $Q(M)$ is a well-defined form. We have $\mathrm{sgn}(M) = \mathrm{sgn}(\gamma) = \mathrm{sgn}\left(Q(M)\right)$. Moreover

$$\frac{t_M}{2} I + n_M SQ(M) = \frac{\alpha + \delta}{2} I + \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \gamma & \frac{\delta - \alpha}{2} \\ \frac{\delta - \alpha}{2} & -\beta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}. \tag{4.152}$$

In view of Theorem 4.38, this means $M \in \mathcal{S}\left(Q(M)\right)$.

Suppose Q is any other form such that $M \in \mathcal{S}(Q)$ and $\mathrm{sgn}(Q) = \mathrm{sgn}(M)$. In view of Theorem 4.38, this means

$$M = \frac{t}{2} I + nSQ \tag{4.153}$$

for some pair of integers t, n such that $n > 0$. It is immediate that $t = \mathrm{Tr}(M) = t_M$. Hence

$$nQ = n_M Q(M). \tag{4.154}$$

Consequently

$$na = n_M a_M \qquad nb = n_M b_M \qquad nc = n_M c_M \tag{4.155}$$

where we have set $Q(M) = \langle a_M, b_M, c_M \rangle$, $Q = \langle a, b, c \rangle$. Since Q, $Q(M)$ are primitive and n, n_M are both positive, it follows that $Q = Q(M)$. □

Corollary 4.41. *For any pair of distinct forms Q_1, Q_2,*

$$\mathcal{S}(Q_1) \cap \mathcal{S}(Q_2) = \{\pm I\}. \tag{4.156}$$

Proof. Immediate consequence of Theorem 4.39 and the fact that $\pm I \in \mathcal{S}(Q)$ for all Q. □

Lemma 4.42. *Let M, M' be any pair of elements of $\mathrm{GL}_2(\mathbb{Z}) \setminus \{\pm I\}$. Then M commutes with M' if and only if $Q(M) = Q(M')$, where $Q(M), Q(M')$ are as defined in (4.148).*

Proof. Suppose M, M' commute. Then $SQ(M') = n_{M'}^{-1}\left(M' - (t_{M'}/2)I\right)$ commutes with $SQ(M) = n_M^{-1}\left(M - (t_M/2)I\right)$. In view of Lemma 4.30, and the fact that $SQ(M')$, $SQ(M)$ are both trace-zero, this means

$$SQ(M') = \lambda SQ(M) \tag{4.157}$$

for some non-zero $\lambda \in \mathbb{Q}$, implying

$$m' Q(M') = m Q(M) \tag{4.158}$$

for some non-zero $m, m' \in \mathbb{Z}$. Because the forms are primitive, it follows that $Q(M') = Q(M)$.

The converse is immediate. □

Definition 4.43. Let

(1) $\mathcal{H}_+$ be the set of all $M \in \mathrm{GL}_2(\mathbb{Z}) \setminus \{\pm I\}$ such that $(\operatorname{Tr} M)^2 - 4 \det M > 4$,
(2) $\mathcal{H}_-$ be the set of all $M \in \mathrm{GL}_2(\mathbb{Z})$ such that $(\operatorname{Tr} M)^2 - 4 \det M \leq 4$,

and let

(1) $\mathcal{F}_+$ be the set of all forms which are indefinite and irreducible,
(2) $\mathcal{F}_-$ be the set of all forms whose discriminant equals $-4, -3, 0, 1$, or 4.

Theorem 4.44. *$M \in \mathcal{H}_\pm$ if and only if $Q(M) \in \mathcal{F}_\pm$.*

Proof. Write $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. Then

$$(\operatorname{Tr} M)^2 - 4 \det M = (\alpha + \delta)^2 - 4\alpha\delta + 4\beta\gamma = (\alpha - \delta)^2 + 4\beta\gamma = n_M^2 \Delta\big(Q(M)\big) \tag{4.159}$$

Now suppose $M \in \mathcal{H}_+$. Then (4.159) means $n_M^2 \Delta(Q(M)) > 4$. It follows that $Q(M)$ is indefinite. It also follows that $Q(M)$ is irreducible. Indeed, suppose that were not the case. Then $\Delta(Q(M)) = m^2$ for some $m \in \mathbb{N}$, implying

$$\big||\operatorname{Tr} M| - mn_M\big|\big(\,|\operatorname{Tr} M| + mn_M\big) = 4 \tag{4.160}$$

Since $|\operatorname{Tr} M| - mn_M \equiv |\operatorname{Tr} M| + mn_M \pmod 2$, this is only possible if

$$\big||\operatorname{Tr} M| - mn_M\big| = |\operatorname{Tr} M| + mn_M = 2. \tag{4.161}$$

Since $mn_M > 0$, this in turn implies $\operatorname{Tr} M = 0$, which is inconsistent with the assumption $M \in \mathcal{H}_+$. Conversely, if $Q(M) \in \mathcal{F}_+$, then $\Delta(Q(M)) > 4$, implying $(\operatorname{Tr} M)^2 - 4 \det M > 4$.

Suppose, on the other hand, that $M \in \mathcal{H}_-$. Then it follows from (4.159) that

$$n_M^2 \Delta(Q(M)) = \begin{cases} -4 & \text{if } \operatorname{Tr} M = 0,\ \det M = +1, \\ -3 & \text{if } \operatorname{Tr} M = \pm 1,\ \det M = +1, \\ 0 & \text{if } \operatorname{Tr} M = \pm 2,\ \det M = +1, \\ 4 & \text{if } \operatorname{Tr} M = 0,\ \det M = -1. \end{cases} \tag{4.162}$$

Since a discriminant must be 0 or 1 modulo 4, it follows that $\Delta(Q(M)) = -4, -3, 0, 1$, or 4. Conversely, if $Q(M) \in \mathcal{F}_-$, then it follows from the first part of the proof that M cannot belong $\mathcal{H}_+$, and so M must belong to $\mathcal{H}_-$. □

Theorem 4.45. *Let Q be any form.*

(1) If $Q \notin \mathcal{F}_+ \cup \mathcal{F}_-$, then

$$\mathcal{S}(Q) = \{\pm I\}. \tag{4.163}$$

(2) If $Q \in \mathcal{F}_+$, then

$$\mathcal{S}(Q) = \chi_Q\left(\mathcal{U}_Q\right) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}. \tag{4.164}$$

(3) If $Q \in \mathcal{F}_-$, then

$$\mathcal{S}(Q) = \begin{cases} \langle SQ \rangle \cong \mathbb{Z}/4\mathbb{Z} & \text{if } \Delta(Q) = -4, \\ \left\langle \frac{1}{2} I + SQ \right\rangle \cong \mathbb{Z}/6\mathbb{Z} & \text{if } \Delta(Q) = -3, \\ \langle -I, I + SQ \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z} & \text{if } \Delta(Q) = 0, \\ \langle -I, 2SQ \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) & \text{if } \Delta(Q) = 1, \\ \langle -I, SQ \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) & \text{if } \Delta(Q) = 4. \end{cases} \tag{4.165}$$

Proof. Suppose $Q \notin \mathcal{F}_+ \cup \mathcal{F}_-$, and let M be any element of $\mathcal{S}(Q)$. To show that $M = \pm I$, assume the contrary. It would then follow from Theorem 4.39 that $Q = Q(M)$, which is a contradiction since we know from Theorem 4.44 that $Q(M) \in \mathcal{F}_+ \cup \mathcal{F}_-$.

Suppose $Q \in \mathcal{F}_+$. Then it follows from Theorems 4.35 and 4.38 that

$$\mathcal{S}(Q) = \mathbb{Z}\langle I, SQ\rangle \cap \mathrm{GL}_2(\mathbb{Z}) = \chi_Q\left(\mathcal{U}_Q\right) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}. \tag{4.166}$$

Suppose $Q \in \mathcal{F}_-$, and let $\pm M \in \mathcal{S}(Q)$. Write $Q = \langle a, b, c\rangle$. It follows from Theorem 4.38 that there exist unique integers t, n such that

$$M = \frac{t}{2} I + nSQ = \begin{pmatrix} \frac{t-nb}{2} & -nc \\ na & \frac{t+nb}{2} \end{pmatrix}, \tag{4.167}$$

implying

$$t^2 - n^2 \Delta(Q) = 4 \det M. \tag{4.168}$$

If $\Delta(Q) = 0$, then it follows from (4.168) that $\det M = +1$ and $t = \pm 2$. It follows from Lemma 4.30 that $(SQ)^2 = 0$. Hence

$$(I + SQ)^n = I + nSQ \tag{4.169}$$

for all $n \in \mathbb{Z}$. Multiplying by $-I$ gives the elements with negative trace. We conclude that $I + SQ$ is infinite order and $\mathcal{S}(Q) = \langle -I, I + SQ\rangle$.

If $\Delta(Q) = -3$, then it follows from (4.168) that $\det M = +1$ and that either $M = \pm I$ or $|t| = |n| = 1$, implying $\mathcal{S}(Q)$ is order 6. It follows from Lemma 4.30 that $(SQ)^2 = -3/4I$. Putting these facts together, we deduce that $(1/2)I + SQ$ is order 6 and consequently that $\mathcal{S}(Q) = \langle (1/2)I + SQ\rangle$.

If $\Delta(Q) = -4$, then it follows from (4.168) that $\det M = +1$ and that either $M = \pm I$ or $t = 0, n = \pm 1$, implying $\mathcal{S}(Q)$ is order 4. It follows from Lemma 4.30 that $(SQ)^2 = -I$. Putting these facts together, we deduce that SQ is order 4 and consequently that $\mathcal{S}(Q) = \langle SQ\rangle$.

If $\Delta(Q) = 1$ (respectively $\Delta(Q) = 4$), then it follows from (4.168) that either $M = \pm I$ or $\det M = -1$, $t = 0$ and $n = \pm 2$ (respectively $n = \pm 1$), implying $\mathcal{S}(Q)$ is order 4. It follows from Lemma 4.30 that $(SQ)^2 = (1/4)I$ (respectively $(SQ)^2 = I$). Putting these facts together, we deduce that $2SQ$ (respectively SQ) is order 2 and consequently that $\mathcal{S}(Q) = \langle -I, 2SQ\rangle$ (respectively $\mathcal{S}(Q) = \langle -I, SQ\rangle$). □

Theorem 4.46. *Let $\mathcal{G}$ be any subgroup of $\mathrm{GL}_2(\mathbb{Z})$. Then $\mathcal{G}$ is maximal abelian if and only if $\mathcal{G} = \mathcal{S}(Q)$ for some $Q \in \mathcal{F}_+ \cup \mathcal{F}_-$.*

Proof. Let $\mathcal{G}$ be a maximal abelian subgroup of $\mathrm{GL}_2(\mathbb{Z})$. The fact that $\{\pm I\}$ is the centre of $\mathrm{GL}_2(\mathbb{Z})$ means that $\{\pm I\}$ is properly contained in $\mathcal{G}$. Choose $M \in \mathcal{G} \setminus \{\pm I\}$, and set $Q = Q(M)$. It follows from Theorem 4.44 that $Q \in \mathcal{F}_+ \cup \mathcal{F}_-$. If M' is any other element of $\mathcal{G} \setminus \{\pm I\}$, then it follows from Lemma 4.42 that $Q_{M'} = Q$. So $\mathcal{G} \subseteq \mathcal{S}(Q)$. Since $\mathcal{S}(Q)$ is abelian, it follows that $\mathcal{G} = \mathcal{S}(Q)$.

Conversely, let $Q \in \mathcal{F}_+ \cup \mathcal{F}_-$. Then $\mathcal{S}(Q)$ is an abelian group. It follows from Theorem 4.45 that we can choose $M \in \mathcal{S}(Q)$ such that $M \neq \pm I$. It then follows from Lemma 4.42 that if $M' \notin \mathcal{S}(Q)$, then M' does not commute with M. So $\mathcal{S}(Q)$ is maximal abelian. □

Theorem 4.47. *Let $M \in \mathcal{H}_+$ and let*

$$w_M = \frac{\mathrm{Tr}(M) + \sqrt{(\mathrm{Tr}\, M)^2 - 4 \det M}}{2}. \tag{4.170}$$

Then w_M is a unit in $\mathcal{U}_{Q(M)}$ and

$$M = \chi_{Q(M)}(w_M). \tag{4.171}$$

Proof. Write $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. Then we have from Theorem 4.39 the formula

$$Q(M) = \frac{1}{n_M} \begin{pmatrix} \gamma & \frac{\delta-\alpha}{2} \\ \frac{\delta-\alpha}{2} & -\beta \end{pmatrix}, \tag{4.172}$$

implying

$$\Delta(Q(M)) = \frac{(\operatorname{Tr} M)^2 - 4 \det M}{n_M^2}. \tag{4.173}$$

Let Δ_0 and f be the fundamental discriminant and conductor of Q. Then it follows that

$$w_M = \frac{\operatorname{Tr} M - f n_M \Delta_0}{2} + f n_M \left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2} \right). \tag{4.174}$$

The fact that $f^2 n_M^2 \Delta_0 = (\operatorname{Tr} M)^2 - 4 \det M$ means $(\operatorname{Tr} M - f n_M \Delta_0)/2 \in \mathbb{Z}$. Since $\operatorname{Nm}(w_M) = \det M$, it follows that w_M is a unit in $\mathcal{U}_{Q(M)}$. The fact that $\chi_{Q(M)}(w_M) = M$ is immediate. □

4.6. **Additional results.** We now revert to the convention explained in Section 1.3, according to which a form is always understood to be irreducible and indefinite unless the contrary is explicitly stated.

Lemma 4.48. *Let Q, Q' be any pair of forms. Then*

$$\rho_{Q,\pm} = \rho_{Q',\pm} \iff Q = Q' \tag{4.175}$$

Proof. Sufficiency is immediate. To prove necessity write $Q = \langle a, b, c \rangle$, $Q' = \langle a', b', c' \rangle$. Then $\rho_{Q,\pm} = \rho_{Q',\pm}$ implies

$$\frac{b}{a} = -(\rho_{Q,+} + \rho_{Q,-}) = -(\rho_{Q',+} + \rho_{Q',-}) = \frac{b'}{a'}, \tag{4.176}$$

$$\frac{c}{a} = \rho_{Q,+}\rho_{Q,-} = \rho_{Q',+}\rho_{Q',-} = \frac{c'}{a'}. \tag{4.177}$$

Also

$$\frac{\sqrt{b^2 - 4ac}}{a} = \rho_{Q,+} - \rho_{Q,-} = \rho_{Q',+} - \rho_{Q',-} = \frac{\sqrt{b'^2 - 4a'c'}}{a'}, \tag{4.178}$$

implying $\operatorname{sgn}(a) = \operatorname{sgn}(a')$. It follows that

$$nQ = n'Q' \tag{4.179}$$

for some pair of positive integers n, n'. Since Q, Q' are primitive, we must in fact have $n = n' = 1$ and $Q = Q'$. □

Lemma 4.49. *Let Q be an arbitrary form and let $M \in \mathcal{S}(Q)$ be such that $M \neq \pm I$. Then for all $\tau \in \mathbb{C}$*

$$M \cdot \tau = \tau \iff \tau = \rho_{Q,\pm}. \tag{4.180}$$

Remark 4.50. It can be shown that, if M and Q have the same (resp. opposite) sign, then $\rho_{Q,+}$ is the attractive (resp. repulsive) fixed point and $\rho_{Q,-}$ is the repulsive (resp. attractive) fixed point of M. We omit the proof, since the result is not actually needed for the purposes of this paper.

Proof. Straightforward consequence of the definitions. □

Lemma 4.51. *For any form Q and matrix $M \in \mathrm{GL}_2(\mathbb{Z})$*

$$M^{-1} \cdot \rho_{Q,\pm} = \rho_{Q_M,\pm}. \tag{4.181}$$

In particular

$$M \cdot \rho_{Q,\pm} = \rho_{Q,\pm} \iff M \in \mathcal{S}(Q). \tag{4.182}$$

Proof. Write $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, $Q = \langle a, b, c\rangle$, $Q_M = \langle a', b', c'\rangle$. Then

$$a' = (\det M)\left(a\alpha^2 + b\alpha\gamma + c\gamma^2\right), \tag{4.183}$$

$$b' = 2(\det M)\left(a\alpha\beta + b\left(\frac{\alpha\delta + \beta\gamma}{2}\right) + c\gamma\delta\right), \tag{4.184}$$

$$c' = (\det M)\left(a\beta^2 + b\beta\delta + c\delta^2\right). \tag{4.185}$$

Hence

$$b'^2 - 4a'c' = b^2 - 4ac \tag{4.186}$$

and

$$M^{-1} \cdot \rho_{Q,\pm} = \frac{-(2a\beta + b\delta) \pm \delta\sqrt{b^2 - 4ac}}{(2a\alpha + b\gamma) \mp \gamma\sqrt{b^2 - 4ac}} = \frac{-b' \pm \sqrt{b^2 - 4ac}}{2a'} = \rho_{Q_M,\pm}, \tag{4.187}$$

which is (4.181). Eq. (4.182) follows immediately. □

Definition 4.52 (Level of an admissible tuple)**.** We define the *level* of the admissible tuple $t = (d, r, Q) \sim (K, j, m, Q)$ to be the integer

$$n_t = \frac{j}{j_{\min}(f)}, \tag{4.188}$$

where f is the conductor of Q.

Theorem 4.53. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, and let f be the conductor of Q. Then the stabilizers L_t, $L_{+,t}$, A_t (see Definition 1.28) are given by*

$$L_t = \chi_Q(\varphi_f), \tag{4.189}$$

$$L_{+,t} = \chi_Q(\varepsilon_f), \tag{4.190}$$

$$L_{\mathrm{z,t}} = L_{+,t}^{n_t} = \chi_Q(\varepsilon^j), \tag{4.191}$$

$$A_t = L_{+,t}^{n_t(2m+1)} = \chi_Q(\varepsilon^{j(2m+1)}). \tag{4.192}$$

The stability groups $\mathcal{S}(Q)$, $\mathcal{S}_d(Q)$ (see Definition 1.20) are then given by

$$\mathcal{S}(Q) = \langle -I, L_t\rangle, \tag{4.193}$$

$$\mathcal{S}_d(Q) = \langle A_t\rangle. \tag{4.194}$$

In particular, $\mathcal{S}_d(Q)$ is a cyclic group, and every element has positive determinant and trace. Moreover, if d is even, then

$$A_t \equiv (d+1)\, I \pmod{2d}. \tag{4.195}$$

Remark 4.54. The fact that $\mathcal{S}_d(Q)$ contains no negative determinant matrices might at first sight seem to be an artifact of our decision to define $\Gamma(d)$ to be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. However, it is easily seen that, if $d > 2$, then there are no matrices in $\mathrm{GL}_2(\mathbb{Z})$ but outside $\mathrm{SL}_2(\mathbb{Z})$ that are congruent to I modulo d. Indeed, suppose $L = I + d\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ were such a matrix. Then we would have $-1 = \det L = 1 + d(\alpha + \delta + d(\alpha\delta - \beta\gamma))$ implying $d \,|\, 2$).

Proof. To prove (4.189) and (4.193), observe that it follows from Theorem 4.45 and Corollary 4.18 that

$$\mathcal{S}(Q) = \chi_Q(\mathcal{U}_Q) = \langle -I, \chi_Q(\varphi_f)\rangle. \tag{4.196}$$

Consequently, L_t must be one of the four matrices $\pm\chi_Q(\varphi_f)$, $\pm\chi_Q(\varphi_f^{-1})$. The requirement that $\mathrm{Tr}(L_t)$ is positive and $\mathrm{sgn}(L_t) = \mathrm{sgn}(Q)$ means we must in fact have $L_t = \chi_Q(\varphi_f)$.

If $\mathrm{Nm}(\varphi_f) = 1$, then $\varepsilon_f = \varphi_f$ and $\det(L_t) = +1$, implying $L_{+,t} = L_t = \chi_Q(\varepsilon_f)$. If, on the other hand, $\mathrm{Nm}(\varphi_f) = -1$, then $\varepsilon_f = \varphi_f^2$ and $\det(L_t) = -1$, implying $L_{+,t} = L_t^2 = \chi_Q(\varphi_f^2)$, so that we again have $L_{+,t} = \chi(\varepsilon_f)$.

Equation (4.191) is an immediate consequence of the definition of $L_{\mathrm{z,t}}$.

Now consider (4.192) and (4.194). The fact that $\mathcal{S}_d(Q)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ means every element is of the form $\pm L_{+,t}^l$, where $l \in \mathbb{Z}$. Let q be the multiplicative order of $L_{+,t}$ modulo d. We claim that $q = (2m+1)n$. Indeed, Lemma 4.24 implies

$$\varepsilon_f^{(2m+1)n} - 1 = \varepsilon^{(2m+1)j} - 1 = zd \tag{4.197}$$

where $n = j/j_{\min}(f)$ and $z = \varepsilon^{mj}(\varepsilon^j - 1) = \varepsilon_f^{mn}(\varepsilon_f^n - 1) \in \mathcal{O}_f$. It then follows from Corollary 4.36 that $L_{+,t}^{(2m+1)n} \equiv I \pmod d$. So $q \,|\, (2m+1)n$. To show that in fact $q = (2m+1)n$ assume the contrary. Then $q \le (2m+1)n/2$. The fact that $L_{+,t}^q \equiv I \pmod d$ means, in view of Corollary 4.36, that

$$\varepsilon_f^q - 1 = z'd \tag{4.198}$$

for some $z' \in \mathcal{O}_f$. It follows from Lemma 4.24

$$d = \frac{\varepsilon_f^{(2m+1)n} - 1}{\varepsilon_f^{mn}(\varepsilon_f^n - 1)}. \tag{4.199}$$

So

$$z' = \frac{\varepsilon_f^{mn}\left(\varepsilon_f^n - 1\right)\left(\varepsilon_f^q - 1\right)}{\varepsilon_f^{(2m+1)n} - 1}. \tag{4.200}$$

Taking norms on both sides, we deduce

$$\mathrm{Nm}(z') = \frac{\left(2 - \varepsilon_f^n - \varepsilon_f^{-n}\right)\left(2 - \varepsilon_f^q - \varepsilon_f^{-q}\right)}{2 - \varepsilon_f^{(2m+1)n} - \varepsilon_f^{-(2m+1)n}}. \tag{4.201}$$

Setting $\varepsilon_f^n = e^\theta$ this becomes

$$\mathrm{Nm}(z') = -\frac{4\sinh^2\frac{\theta}{2}\sinh^2\frac{q\theta}{2n}}{\sinh^2\frac{(2m+1)\theta}{2}} \tag{4.202}$$

In view of the assumption that $q \le (2m+1)n/2$, this means

$$|\mathrm{Nm}(z')| \le \frac{4\sinh^4\frac{(2m+1)\theta}{4}}{\sinh^2\frac{(2m+1)\theta}{2}} = \tanh^2\frac{(2m+1)\theta}{4} < 1, \tag{4.203}$$

contradicting the fact that $|\mathrm{Nm}(z')|$ is a positive integer.

We have thus shown that $\langle L_{+,t}^{(2m+1)n}\rangle \subseteq \mathcal{S}_d(Q)$. To show that in fact $\langle L_{+,t}^{(2m+1)n}\rangle = \mathcal{S}_d(Q)$, assume the contrary. Then there would exist a positive integer s such that

$$L_{+,t}^s \equiv -I \pmod d \tag{4.204}$$

It would follow that $L_{+,t}^{2s} \equiv I \pmod{d}$, implying $2s$ is a multiple of $(2m+1)n$. If it were an even multiple, it would follow that s is a multiple of $(2m+1)n$, implying $L_{+,t}^{s} \equiv I \pmod{d}$, contrary the assumption. So $2s = (2k+1)(2m+1)n$ for some non-negative integer k. In particular n would be even. We would then have

$$L_{+,t}^{\frac{(2m+1)n}{2}} = L_{+,t}^{k(2m+1)n} L_{+,t}^{\frac{(2m+1)n}{2}} = L_{+,t}^{\frac{(2k+1)(2m+1)n}{2}} = L_{+,t}^{s} = -I \pmod{d}. \tag{4.205}$$

In view of Corollary 4.36, this would mean

$$\varepsilon_f^{\frac{(2m+1)n}{2}} + 1 = z''d \tag{4.206}$$

for some $z'' \in \mathcal{O}_f$. By a suitably modified version of the argument leading to inequality (4.203), it would follow that

$$|\mathrm{Nm}(z'')| = \frac{\sinh^2 \frac{\theta}{2}}{\sinh^2 \frac{(2m+1)\theta}{4}} < 1, \tag{4.207}$$

contradicting the fact that $\mathrm{Nm}(z'')$ is a non-zero integer. We have thus shown $\mathcal{S}_d(Q) = \langle L_{+,t}^{(2m+1)n} \rangle$, implying $A_t = L_{+,t}^{\pm(2m+1)n}$. The requirement that $\mathrm{sgn}(A_t) = \mathrm{sgn}(Q)$ means we must in fact have $A_t = L_{+,t}^{(2m+1)n}$. Eqs. (4.192), (4.194) now follow.

The fact that the elements of $\mathcal{S}_d(Q)$ all have positive determinant follows from

$$\det\left(L_{+,t}^k\right) = \mathrm{Nm}(\varepsilon_f^k) = 1. \tag{4.208}$$

The fact that they all have positive trace follows from

$$\mathrm{Tr}\left(L_{+,t}^k\right) = \mathrm{Tr}(\varepsilon_f^k) = \begin{cases} d_{|k|j_{\min(\mathrm{f})}} - 1 & \text{if} k \neq 0, \\ 2 & \text{if} k = 0. \end{cases} \tag{4.209}$$

It remains to prove (4.195). The fact that $A_t = \chi_Q\left(\varepsilon_f^{(2m+1)n}\right)$ together with Corollary 4.36 means

$$A_t - (d+1)I \equiv 0 \pmod{2d} \tag{4.210}$$

if and only if

$$z = \frac{\varepsilon_f^{(2m+1)n} - d - 1}{2d} \in \mathcal{O}_f. \tag{4.211}$$

The fact that d is even means, in view of Lemmas 4.11 and 4.24, that $\Delta_0 \equiv 1 \pmod{4}$. So we need to show

$$z = n_1 + n_2 f\left(\frac{1+\sqrt{\Delta_0}}{2}\right) \tag{4.212}$$

for some $n_1, n_2 \in \mathbb{Z}$. It follows from Lemma 4.24 that

$$z = \frac{\varepsilon^{mj}(\varepsilon^j - 1) - 1}{2} = \frac{d_{(m+1)j} - d_{mj} - 2 + (f_{(m+1)j} - f_{mj})\sqrt{\Delta_0}}{4}. \tag{4.213}$$

That is,

$$z = \alpha_1 + \alpha_2 f\left(\frac{1+\sqrt{\Delta_0}}{2}\right) \tag{4.214}$$

where

$$\alpha_1 = \frac{\left(d_{(m+1)j} - d_{mj} - 2\right) - \left(f_{(m+1)j} - f_{mj}\right)}{4}, \qquad \alpha_2 = \frac{f_{(m+1)j} - f_{mj}}{2f}. \tag{4.215}$$

We need to show that α_1, α_2 are both in $\mathbb{Z}$. The fact that $\alpha_1 \in \mathbb{Z}$ is an immediate consequence of Lemma 4.24. Moreover,

$$\alpha_2 = \left(\frac{f_j}{f}\right)\left(\frac{r_{j,m+1} - r_{j,m}}{2}\right). \tag{4.216}$$

It follows from Lemma 4.24 that $r_{j,m+1} - r_{j,m}$ is even. Since $f \mid f_j$, this means $\alpha_2 \in \mathbb{Z}$. □

Proof of Theorem 1.31. It follows from Theorem 4.53 that $\mathrm{Tr}(A_t)$ and $\mathrm{Tr}(A_t^{-1})$ are both positive which, in view of Lemmas 2.18 and 4.51, means $\rho_{Q,\pm} \in \mathcal{D}_{A_t} \cap \mathcal{D}_{A_t^{-1}}$. □

5. Proof of main theorems (1): Existence

In this section, we show that the correctness of our construction of r-SICs follows from several number-theoretic conjectures. Specifically, we prove Theorem 1.46, which asserts that for every fiducial datum s, the matrix $\tilde{\Pi}_s$ defined in Definition 1.44 is a ghost r-SIC fiducial under the assumption of the Twisted Convolution Conjecture (Conjecture 1.35). Furthermore, we show Theorem 1.47, which asserts that the matrix Π_s defined in Definition 1.44 is an r-SICs fiducial under the assumption of the Twisted Convolution Conjecture and the Stark Conjecture (Conjecture 2.7).

This section first establishes the relationship of the Shintani–Faddeev modular cocycle $\mathfrak{w}^{d^{-1}\mathbf{p}}$ to the Shintani–Faddeev phase $\phi_{\mathbf{p}}(t)$, then uses that relationship in conjunction with the conjectures to prove the theorems on ghost r-SIC and "live" r-SIC existence. Section 5.1 and Section 5.2 proves some properties of the $\phi_{\mathbf{p}}(t)$, in order to connect it to the eta-multiplier character ψ and the theta-multiplier character $\chi_{d^{-1}\mathbf{p}}$. In Section 5.3, we use the properties of the SF phase to establish properties of our candidate ghost overlaps, including the crucial property that they are real numbers. The latter relies of results of [70] relating the SF cocycle to zeta values. In Section 5.4, we complete the proof of Theorem 1.46. In Section 5.5, we give some remarks on the "shift" appearing in our construction. Finally, in Section 5.6, we complete the proof of Theorem 1.47.

5.1. Properties of the Rademacher invariant.

We prove some properties of the Rademacher class invariant that we require. We provide references to proofs of some properties, but we provide a proof for others where a reference to the exact statement we needed could not be found.

Lemma 5.1. *Let Ψ be the Rademacher class invariant as defined in Definition 1.29, and let $\eta(\tau)$ be the Dedekind η-function. Then for all $M = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, $N \in \mathrm{GL}_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$ we have*

$$\Psi(-M) = \Psi(M), \tag{5.1}$$

$$\Psi(M^{-1}) = -\Psi(M), \tag{5.2}$$

$$\Psi(NMN^{-1}) = (\det N)\Psi(M) \tag{5.3}$$

$$\eta(M\cdot\tau) = \begin{cases} e^{\frac{\pi i}{12}\Psi(M)}\sqrt{\mathrm{sgn}(\mathrm{Tr}(M))j_M(\tau)}\eta(\tau) & \gamma \neq 0,\ \mathrm{Tr}(M) \neq 0\,, \\ e^{\frac{\pi i}{12}\Psi(M)}\sqrt{-i\,\mathrm{sgn}(\gamma)j_M(\tau)}\eta(\tau) & \gamma \neq 0,\ \mathrm{Tr}(M) = 0\,, \\ e^{\frac{\pi i}{12}\Psi(M)}\eta(\tau) & \gamma = 0\,. \end{cases} \tag{5.4}$$

where in (5.4) the principal branch of the square root is taken.

If $\mathrm{Tr}(M) \neq \pm 1$*, then*

$$e^{\frac{\pi i}{12}\psi(M^n)} = e^{\frac{\pi i}{12}n\psi(M)} \tag{5.5}$$

for all $n \in \mathbb{Z}$.

Proof. Equations (5.1) and (5.2) are proved in [84,86]. If $\det N = 1$, then (5.3) follows from the fact that Ψ is a class function, as also proven in [84]. It follows from (1.42) that $\Psi(JMJ^{-1}) = -\Psi(M)$, where $J = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. If N is any other element of $\mathrm{GL}_2(\mathbb{Z})$ such that $\det(N) = -1$ let $N' = NJ$. Then $\Psi(NMN^{-1}) = \Psi(JMJ^{-1}) = -\Psi(M)$. Equation (5.4) is a straightforward consequence of results proved in [85].

To prove (5.5), observe that if $\gamma = 0$, then

$$M = \begin{pmatrix} \pm 1 & \beta \\ 0 & \pm 1 \end{pmatrix}, \qquad M^n = \begin{pmatrix} (\pm 1)^n & n(\pm 1)^{n-1}\beta \\ 0 & (\pm 1)^n \end{pmatrix}, \tag{5.6}$$

implying $\Psi(M^n) = \pm n\beta = n\Psi(M)$. Suppose, next, that $\gamma \neq 0$ and $\mathrm{Tr}(M) = 0$. Then we use the easily verified identity

$$M^2 = \mathrm{Tr}(M)M - I. \tag{5.7}$$

to deduce that $M^2 = -I$, implying

$$M^n = \begin{cases} (-1)^{\frac{n}{2}} I & n \text{ even}, \\ (-1)^{\frac{n-1}{2}} M & n \text{ odd}. \end{cases} \tag{5.8}$$

The fact that $M^{-1} = -M$ means $\psi(M) = -\psi(M^{-1}) = -\psi(-M) = -\psi(M)$. So $\psi(M) = 0$. It is immediate that $\psi(I) = 0$. The claim now follows.

Next, suppose, $\gamma \neq 0$, $\mathrm{Tr}(M) \geq 2$. Using (5.7) it is straightforward to confirm that for every positive integer n,

$$M^n = P_n M - P_{n-1} I, \tag{5.9}$$

where

$$P_0 = 0, \qquad P_1 = 1, \qquad P_{n+1} = \mathrm{Tr}(M)P_n - P_{n-1} \quad \forall n \geq 1, \tag{5.10}$$

and

$$0 = P_0 < P_1 < \cdots < P_n < \ldots. \tag{5.11}$$

It follows that

$$\mathrm{Tr}(M^n) = P_n \,\mathrm{Tr}(M) - 2P_{n-1} \geq 2\,(P_n - P_{n-1}) > 0 \tag{5.12}$$

for all $n \geq 1$. Also, if we write

$$M^n = \begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix}, \tag{5.13}$$

then $\gamma_n = P_n\gamma_1$ has the same sign as γ_1 for all $n \geq 1$.

It now follows from Eq. (5.4) that for all $n \geq 1$ and $\tau \in \mathbb{H}$,

$$\begin{aligned} e^{\frac{\pi i}{12}\Psi(M^{n+1})} &= \frac{\eta(M^{n+1}\cdot\tau)}{\sqrt{j_{M^{n+1}}(\tau)}\eta(\tau)} \\ &= \frac{1}{\sqrt{j_{M^{n+1}}(\tau)}} \left(\frac{\eta(M^{n+1}\cdot\tau)}{\eta(M^n\cdot\tau)}\right)\left(\frac{\eta(M^n\cdot\tau)}{\eta(\tau)}\right) \end{aligned}$$

$$= \frac{1}{\sqrt{j_{M^{n+1}}(\tau)}} \left(e^{\frac{\pi i}{12}\Psi(M)} \sqrt{j_M(M^n \cdot \tau)} \right) \left(e^{\frac{\pi i}{12}\Psi(M^n)} \sqrt{j_{M^n}(\tau)} \right). \tag{5.14}$$

It follows from Lemma 2.16 that

$$j_{M^{n+1}}(\tau) = j_M(M^n \cdot \tau) j_{M^n}(\tau). \tag{5.15}$$

The fact that γ_{n+1}, γ_n, γ_1 have the same sign means the imaginary parts of $j_{M^{n+1}}(\tau)$, $j_M(M^n \cdot \tau)$, $j_{M^n}(\tau)$ have the same sign. Consequently

$$\sqrt{j_{M^{n+1}}(\tau)} = \sqrt{j_M(M^n \cdot \tau)} \sqrt{j_{M^n}(\tau)}, \tag{5.16}$$

implying

$$e^{\frac{\pi i}{12}\Psi(M^{n+1})} = e^{\frac{\pi i}{12}\Psi(M)} e^{\frac{\pi i}{12}\Psi(M^n)}. \tag{5.17}$$

It follows that $e^{\frac{\pi i}{12}\Psi(M^n)} = e^{\frac{\pi i}{12} n \Psi(M)}$ for all $n \geq 1$. The statement is immediate for $n = 0$, while if $n < 0$ we can use (5.2) together with the result just proved to deduce

$$e^{\frac{\pi i}{12}\Psi(M^n)} = e^{\frac{\pi i}{12}\Psi((M^{|n|})^{-1})} = e^{-\frac{\pi i}{12}\Psi(M^{|n|})} = e^{-\frac{\pi i}{12}|n|\Psi(M)} = e^{\frac{\pi i}{12} n \Psi(M)}. \tag{5.18}$$

Finally, if $\gamma \neq 0$ and $\mathrm{Tr}(M) \leq -2$ we can use (5.1) together with the result for $\mathrm{Tr}(M) \geq 2$ to deduce

$$e^{\frac{\pi i}{12}\Psi(M^n)} = e^{\frac{\pi i}{12}\Psi((-M)^n)} = e^{\frac{\pi i}{12} n \Psi(-M)} = e^{\frac{\pi i}{12} n \Psi(M)}, \tag{5.19}$$

completing the proof. □

We now explicitly relate the metaplectic character ψ to the Rademacher invariant Ψ.

Proposition 5.2. *Let* $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ *such that* $\gamma \neq 0$ *and* $\mathrm{Tr}(M) > 0$. *Then, taking* $\sqrt{j_M(\tau)}$ *to be the principal branch,*

$$\psi(M, \sqrt{j_M}) = e^{\frac{\pi i}{12}\Psi(M)}. \tag{5.20}$$

Proof. By (2.34), for any choice of $\tau \in \mathbb{H}$, we have

$$\eta(M \cdot \tau) = \psi(M, \sqrt{j_M}) \sqrt{j_M(\tau)} \eta(\tau). \tag{5.21}$$

By (5.4) in Lemma 5.1, we also have

$$\eta(M \cdot \tau) = e^{\frac{\pi i}{12}\Psi(M)} \sqrt{j_M(\tau)} \eta(\tau). \tag{5.22}$$

Therefore,

$$\psi(M, \sqrt{j_M}) = \frac{\eta(M \cdot \tau)}{\sqrt{j_M(\tau)} \eta(\tau)} = e^{\frac{\pi i}{12}\Psi(M)}, \tag{5.23}$$

completing the proof. □

5.2. **Properties of the Shintani–Faddeev phase.** The phase $(\psi^{-2}\chi_{\mathbf{r}}^{-1})(A)$ involves only A, whereas the phase $\phi_{\mathbf{p}}(t)$ involves both A_t and Q. In order the establish a relation, we require some technical lemmas about the quadratic form Q.

Lemma 5.3. *Let* (K, j, m, Q) *be an admissible tuple, let* f *be the conductor of* Q, *and define*

$$\langle a, b, c \rangle = \frac{f_j}{f} Q. \tag{5.24}$$

(1) If d_j *is even, then* a, b, c *are all odd.*

(2) If $d_j \equiv 1 \pmod 4$*, then*

$$\begin{aligned} &\textit{either} && b \equiv 0 \pmod 4\,,\ ac \equiv 1 \pmod 2\,,\\ &\textit{or} && b \equiv 2 \pmod 4\,,\ ac \equiv 0 \pmod 2\,. \end{aligned} \tag{5.25}$$

(3) If $d_j \equiv 3 \pmod 4$*, then*

$$\begin{aligned} &\textit{either} && b \equiv 0 \pmod 4\,,\ ac \equiv 0 \pmod 2\,,\\ &\textit{or} && b \equiv 2 \pmod 4\,,\ ac \equiv 1 \pmod 2\,. \end{aligned} \tag{5.26}$$

Proof. We have

$$b^2 - 4ac = \Delta_j = (d_j - 1)^2 - 4. \tag{5.27}$$

It follows that if d_j is even, then b is odd. Suppose ac is not also odd. Then

$$b^2 \equiv (d_j - 1)^2 + 4 \pmod 8\,, \tag{5.28}$$

which is impossible, because $n^2 \equiv 1 \pmod 8$ for every odd integer n.

Next, suppose $d_j \equiv 1 \pmod 4$. Then $d_j = 4n + 1$ for some integer n. Consequently

$$b^2 - 4ac = 16n^2 - 4. \tag{5.29}$$

It follows that b is even, and

$$(b/2)^2 - ac = 4n^2 - 1. \tag{5.30}$$

implying one of the pair $(b/2, ac)$ is even and the other odd.

Finally, suppose $d_j \equiv 3 \pmod 4$. Then $d_j = 4n + 3$ for some integer n. Consequently

$$b^2 - 4ac = 16n(n + 1). \tag{5.31}$$

It follows that b is even and

$$(b/2)^2 - ac = 4n(n + 1), \tag{5.32}$$

implying that the numbers $b/2$, ac are either both even or both odd. □

Corollary 5.4. *Let* (K, j, m, Q) *be an admissible tuple, let* f *be the conductor of* Q*, and let*

$$\langle a, b, c\rangle = \frac{f_{jm}}{f} Q. \tag{5.33}$$

Suppose $d_{j,m}$ *is even. Then* a, b, c *are all odd.*

Proof. It follows from Lemma 4.24 that d_j is even, $m \equiv 1 \pmod 3$, and $r_{j,m}$ is odd. We have

$$\tfrac{f_{jm}}{f} Q = r_{j,m} \tfrac{f_j}{f} Q \tag{5.34}$$

It follows from Lemma 5.3 that the coefficients of $\frac{f_j}{f} Q$ are all odd. Since $r_{j,m}$ is odd, the same must be true of the coefficients of $\frac{f_{jm}}{f} Q$. □

The next result is the main technical lemma needed to relate the two phases by showing an agreement of signs.

Lemma 5.5. *Let* $t = (d, r, Q) \sim (K, j, m, Q)$ *be an admissible tuple and let* f *be the conductor of* Q*. Then*

$$(-1)^{\frac{f_j}{f} Q(\mathbf{p})} = (-1)^{1 + \delta^{(2d)}_{A_t \mathbf{p}, \mathbf{p}}} \tag{5.35}$$

for all $\mathbf{p} \in \mathbb{Z}^2$*. (See Definition 1.28 for the definition of* A_t*).*

Proof. We begin by finding an expression for $A_t - I$. Using Theorem 4.53 together with Definition 4.33, Lemma 4.3, and Definition 1.24, we have

$$\begin{aligned} A_t - I &= \chi_Q(\varepsilon^{j(2m+1)}) - I \\ &= \left(\frac{d_{j(2m+1)} - 3}{2}\right) I + \frac{f_{j(2m+1)}}{f} SQ \\ &= \left(\frac{d_{j(2m+1)} - 3}{2}\right) I + r_{j,2m+1} S\bar{Q} \end{aligned} \tag{5.36}$$

where

$$\bar{Q} = \tfrac{f_j}{f} Q. \tag{5.37}$$

It follows from Proposition 4.19 that

$$\begin{aligned} \frac{d_{j(2m+1)} - 3}{2} &= \cosh(2m+1)j\theta - 1 \\ &= 2\sinh^2 \frac{(2m+1)j\theta}{2} \\ &= 2d^2 \sinh^2 \frac{j\theta}{2} \\ &= d^2(\cosh j\theta - 1) \\ &= d^2 \left(\frac{d_j - 3}{2}\right), \end{aligned} \tag{5.38}$$

while Lemma 4.24 implies $r_{j,2m+1} = r_{j,m+1}^2 - r_{j,m}^2 = (r_{j,m+1} - r_{j,m})d$. Hence

$$A_t - I = dH, \tag{5.39}$$

where

$$H = d\left(\frac{d_j - 3}{2}\right) I + (r_{j,m+1} - r_{j,m}) S\bar{Q}. \tag{5.40}$$

So the problem is to show that, for all $\mathbf{p}$,

$$\bar{Q}(\mathbf{p}) \equiv 0 \pmod 2 \qquad \Longleftrightarrow \qquad H\mathbf{p} \equiv \mathbf{0} \pmod 2 \tag{5.41}$$

Set $\bar{Q} = \langle a, b, c\rangle$. There are four cases to consider.

Case 1. d_j even, $m \equiv 1 \pmod 3$. It follows from Lemma 5.3 that a, b, c are all odd. So

$$\bar{Q}(\mathbf{p}) \equiv p_1 + p_1p_2 + p_2 \pmod 2, \tag{5.42}$$

implying $Q(\mathbf{p}) \equiv 0 \pmod 2$ if and only if $p_1 \equiv p_2 \equiv 0 \pmod 2$. On the other hand it follows from Lemma 4.24 that d is even, which in view of Theorem 4.53, means $H \equiv I \pmod 2$. So $H\mathbf{p} \equiv \mathbf{0} \pmod 2$ if and only if $p_1 = p_2 \equiv 0 \pmod 2$.

Case 2. d_j even, $m \not\equiv 1 \pmod 3$. As before a, b, c all odd, implying $\bar{Q}(\mathbf{p}) \equiv 0 \pmod 2$ if and only if $p_1 \equiv p_2 \equiv 0 \pmod 2$. On the other hand it follows from Lemma 4.24 that d and $r_{j,m+1} - r_{j,m} = d - 2r_{j,m}$ are odd. So

$$H \equiv \begin{pmatrix} \frac{d(d_j-3)-(r_{j,m+1}-r_{j,m})b}{2} & 1 \\ 1 & \frac{d(d_j-3)+(r_{j,m+1}-r_{j,m})b}{2} \end{pmatrix} \pmod 2. \tag{5.43}$$

Since

$$\frac{d(d_j-3)-(r_{j,m+1}-r_{j,m})b}{2}+\frac{d(d_j-3)+(r_{j,m+1}-r_{j,m})b}{2}\equiv 1 \pmod 2, \tag{5.44}$$

$H \equiv \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right) \pmod 2$. Consequently $H\mathbf{p}\equiv\mathbf{0} \pmod 2$ if and only if $p_1\equiv p_2\equiv 0 \pmod 2$.

Case 3. $d_j \equiv 1 \pmod 4$. Then $(d_j-3)/2$ is odd. It follows from Lemma 4.24 that d and $r_{j,m+1}-r_{j,m}=d-2r_{j,m}$ are also odd. So

$$H \equiv I + S\bar{Q} \pmod 2. \tag{5.45}$$

In view of Lemma 5.3 there are four possibilities:

(1) $b\equiv 0 \pmod 4$ and $a\equiv c\equiv 1 \pmod 2$. We have

$$Q(\mathbf{p})\equiv p_1+p_2 \pmod 2, \qquad H\equiv\begin{pmatrix}1&1\\1&1\end{pmatrix} \pmod 2. \tag{5.46}$$

So $\bar{Q}(\mathbf{p})\equiv 0 \pmod 2 \iff p_1+p_2\equiv 0 \pmod 2 \iff H\mathbf{p}\equiv\mathbf{0} \pmod 2$.

(2) $b\equiv 2 \pmod 4$, $a\equiv 1 \pmod 2$, $c\equiv 0 \pmod 2$.

$$\bar{Q}(\mathbf{p})\equiv p_1 \pmod 2, \qquad H=\begin{pmatrix}0&0\\1&0\end{pmatrix} \pmod 2. \tag{5.47}$$

So $\bar{Q}(\mathbf{p})\equiv 0 \pmod 2 \iff p_1\equiv 0 \pmod 2 \iff H\mathbf{p}\equiv\mathbf{0} \pmod 2$.

(3) $b\equiv 2 \pmod 4$, $a\equiv 0 \pmod 2$, $c\equiv 1 \pmod 2$.

$$\bar{Q}(\mathbf{p})\equiv p_2 \pmod 2, \qquad H\equiv\begin{pmatrix}0&1\\0&0\end{pmatrix} \pmod 2. \tag{5.48}$$

So $\bar{Q}(\mathbf{p})\equiv 0 \pmod 2 \iff p_2\equiv 0 \pmod 2 \iff H\mathbf{p}\equiv\mathbf{0} \pmod 2$.

(4) $b\equiv 2 \pmod 4$ and $a\equiv c\equiv 0 \pmod 2$. We have

$$\bar{Q}(\mathbf{p})\equiv 0 \pmod 2, \qquad H\equiv\begin{pmatrix}0&0\\0&0\end{pmatrix} \pmod 2. \tag{5.49}$$

So $\bar{Q}(\mathbf{p})\equiv 0 \pmod 2$ and $H\mathbf{p}\equiv\mathbf{0} \pmod 2$ for all $\mathbf{p}$.

Case 4. $d_j \equiv 3 \pmod 4$. Then $(d_j-3)/2$ is even. It follows from Lemma 4.24 that d and $r_{j,m+1}-r_{j,m}=d-2r_{j,m}$ are odd. So

$$H \equiv S\bar{Q} \pmod 2. \tag{5.50}$$

In view of Lemma 5.3 there are four possibilities:

(1) $b\equiv 0 \pmod 4$, $a\equiv 1 \pmod 2$, $c\equiv 0 \pmod 2$. We have

$$\bar{Q}(\mathbf{p})\equiv p_1 \pmod 2, \qquad H\equiv\begin{pmatrix}0&0\\1&0\end{pmatrix} \pmod 2. \tag{5.51}$$

So $\bar{Q}(\mathbf{p})\equiv 0 \pmod 2 \iff p_1=0 \pmod 2 \iff H\mathbf{p}=\mathbf{0} \pmod 2$.

(2) $b\equiv 0 \pmod 4$, $a\equiv 0 \pmod 2$, $c\equiv 1 \pmod 2$.

$$\bar{Q}(\mathbf{p})\equiv p_2 \pmod 2, \qquad H\equiv\begin{pmatrix}0&1\\0&0\end{pmatrix} \pmod 2. \tag{5.52}$$

So $\bar{Q}(\mathbf{p})\equiv 0 \pmod 2 \iff p_2\equiv 0 \pmod 2 \iff H\mathbf{p}\equiv\mathbf{0} \pmod 2$.

(3) $b \equiv 0 \pmod 4$, $a \equiv c \equiv 0 \pmod 2$.

$$\bar{Q}(\mathbf{p}) \equiv 0 \pmod 2, \qquad H \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \pmod 2. \tag{5.53}$$

So $\bar{Q}(\mathbf{p}) \equiv 0 \pmod 2$ and $H\mathbf{p} \equiv \mathbf{0} \pmod 2$ for all $\mathbf{p}$.

(4) $b \equiv 2 \pmod 4$ and $a \equiv c \equiv 1 \pmod 2$. We have

$$\bar{Q}(\mathbf{p}) \equiv p_1 + p_2 \pmod 2, \qquad H \equiv \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \pmod 2. \tag{5.54}$$

So $\bar{Q}(\mathbf{p}) \equiv 0 \pmod 2 \iff p_1 + p_2 \equiv 0 \pmod 2 \iff H\mathbf{p} \equiv \mathbf{0} \pmod 2$.

This completes the proof of Equation (5.40) in all four cases and thus proves the lemma. □

The sign calculation we have just finished allows us to establish an equality between the square of the SF phase and a product of eta-multiplier and theta-multiplier values.

Theorem 5.6 (Phase relation)**.** *Let $t = (d, r, Q)$ be an admissible tuple, and let $\mathbf{p} \in \mathbb{Z}^2/d\mathbb{Z}^2$. Then,*

$$\phi_{\mathbf{p}}(t)^2 = (\psi^{-2}\chi_{d^{-1}\mathbf{p}}^{-1})(A_t). \tag{5.55}$$

Proof. Let f be the conductor of Q. By Definition 1.30, the square of the SF-phase is

$$\phi_{\mathbf{p}}(t)^2 = \left((-1)^{s_d(\mathbf{p})} e^{-\frac{\pi i}{12}\Psi(A_t)} \xi_d^{-\frac{f_{jm}}{f}Q(\mathbf{p})}\right)^2 = e^{-\frac{\pi i}{6}\Psi(A_t)} \omega_d^{-\frac{f_{jm}}{f}Q(\mathbf{p})}. \tag{5.56}$$

The matrix $A_t = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ satisfies the conditions $\gamma \neq 0$ and $\mathrm{Tr}(A_t) > 0$. By Proposition 5.2, we have

$$\psi^{-2}(A_t) = \left(e^{\frac{\pi i}{12}\Psi(A_t)}\right)^{-2} = e^{-\frac{\pi i}{6}\Psi(A_t)} \tag{5.57}$$

It follows from (5.39), (5.40), and (5.37) that

$$\begin{aligned} \langle A_t\mathbf{p}, \mathbf{p}\rangle = -\langle \mathbf{p}, A_t\mathbf{p}\rangle &= -\frac{df_j(r_{j,m+1} - r_{j,m})}{f}\langle \mathbf{p}, SQ\mathbf{p}\rangle \\ &= \frac{df_j(d - 2r_{j,m})}{f} Q(\mathbf{p}) \\ &= \left(\frac{d^2 f_j}{f} - \frac{2df_{jm}}{f}\right) Q(\mathbf{p}). \end{aligned} \tag{5.58}$$

Hence the character value $\chi_{d^{-1}\mathbf{p}}(A_t)$ can therefore be written as

$$\begin{aligned} \chi_{d^{-1}\mathbf{p}}^{-1}(A_t) &= (-1)^{1+\delta^{(2)}_{A_t(d^{-1}\mathbf{p}),d^{-1}\mathbf{p}}} e^{\frac{\pi i}{d^2}\langle A_t\mathbf{p},\mathbf{p}\rangle} \\ &= (-1)^{1+\delta^{(2d)}_{A_t\mathbf{p},\mathbf{p}}} e^{\frac{\pi i}{d^2}\left(\frac{d^2 f_j}{f} - \frac{2df_{jm}}{f}\right)Q(\mathbf{p})} \\ &= (-1)^{1+\delta^{(2d)}_{A_t\mathbf{p},\mathbf{p}} + \frac{f_j}{f}} \omega_d^{-\frac{f_{jm}}{f}Q(\mathbf{p})} \\ &= \omega_d^{-\frac{f_{jm}}{f}Q(\mathbf{p})}, \end{aligned} \tag{5.59}$$

where we have used Lemma 5.5 in the last step. Thus, plugging (5.57) and (5.59) into (5.56),

$$\phi_{\mathbf{p}}(t)^2 = \psi^{-2}(A_t)\chi_{d^{-1}\mathbf{p}}^{-1}(A_t) = (\psi^{-2}\chi_{d^{-1}\mathbf{p}}^{-1})(A_t), \tag{5.60}$$

completing the proof. □

5.3. **Properties of the ghost overlaps.** We now apply the results on the SF phase, which appears in the definition of the candidate ghost overlaps $\tilde{\nu}_{\mathbf{p}}(t)$, to establish some relations satisfied by the $\tilde{\nu}_{\mathbf{p}}(t)$.

Lemma 5.7. *Let $t = (d, r, Q)$ be an admissible tuple. Then for all $\mathbf{p}, \mathbf{p}' \in \mathbb{Z}^2$ such that $\mathbf{p}' \equiv \mathbf{p} \pmod d$ and $\mathbf{p}', \mathbf{p} \not\equiv \mathbf{0} \pmod d$,*

$$\tilde{\nu}_{\mathbf{p}'}(t) = \xi_d^{\langle \mathbf{p}', \mathbf{p} \rangle} \tilde{\nu}_{\mathbf{p}}(t). \tag{5.61}$$

Proof. We have

$$\begin{aligned} \phi_{\mathbf{p}'}(t) &= (-1)^{s_d(\mathbf{p}') - s_d(\mathbf{p})} \xi_d^{-\frac{f_{jm}}{f}(Q(\mathbf{p}') - Q(\mathbf{p}))} \phi_{\mathbf{p}}(t) \\ &= (-1)^{s_d(\mathbf{p}') - s_d(\mathbf{p})} \xi_d^{-a(p_1'^2 - p_1^2) - b(p_1'p_2' - p_1p_2) - c(p_2'^2 - p_2^2)} \phi_{\mathbf{p}}(t) \end{aligned} \tag{5.62}$$

where we have set $\frac{f_{jm}}{f} Q = \langle a, b, c \rangle$. If d is odd, then

$$(-1)^{s_d(\mathbf{p}') - s_d(\mathbf{p})} \xi_d^{-a(p_1'^2 - p_1^2) - b(p_1'p_2' - p_1p_2) - c(p_2'^2 - p_2^2)} = 1 = \xi_d^{\langle \mathbf{p}', \mathbf{p} \rangle}. \tag{5.63}$$

Suppose, on the other hand, that d is even. Then $\mathbf{p}' \equiv \mathbf{p} \pmod 2$, implying

$$(-1)^{s_d(\mathbf{p}') - s_d(\mathbf{p})} = 1 \tag{5.64}$$

Also, it follows from Lemma 5.4 that b is odd. So, setting $\mathbf{p}' = \mathbf{p} + d\mathbf{q}$,

$$\begin{aligned} \xi_d^{-a(p_1'^2 - p_1^2) - b(p_1'p_2' - p_1p_2) - c(p_2'^2 - p_2^2)} &= \xi_d^{-ad(p_1' + p_1)q_1 - ((p_1 + dq_1)(p_2 + dq_2) - p_1p_2) - cd(p_2' + p_2)q_2} \\ &= (-1)^{q_1p_2 + q_2p_1} \\ &= \xi_d^{\langle \mathbf{p}', \mathbf{p} \rangle}. \end{aligned} \tag{5.65}$$

We conclude that

$$\phi_{\mathbf{p}'}(t) = \xi_d^{\langle \mathbf{p}', \mathbf{p} \rangle} \phi_{\mathbf{p}}(t) \tag{5.66}$$

irrespective of the value of d. Lastly, it follows from Lemma 2.14 that

$$\mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}'}(\rho_{Q,+}) = \mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho_{Q,+}). \tag{5.67}$$

Hence $\tilde{\nu}_{\mathbf{p}'}(t) = \xi_d^{\langle \mathbf{p}', \mathbf{p} \rangle} \tilde{\nu}_{\mathbf{p}}(t)$. □

Proof of Lemma 1.43. Let

$$f(\mathbf{p}) = \tilde{\nu}_{G\mathbf{p}}(t) D_{\mathbf{p}}, \tag{5.68}$$

and let $\mathbf{p}, \mathbf{p}' \in \mathbb{Z}^2$ be such that $\mathbf{p}' \equiv \mathbf{p} \pmod d$ and $\mathbf{p}', \mathbf{p} \not\equiv \mathbf{0} \pmod d$. Setting $\mathbf{p}' \equiv \mathbf{p} + d\mathbf{q}$, it follows from (3.4) and Lemma 5.7 that

$$\begin{aligned} f(\mathbf{p}') &= (-1)^{(d+1)\langle \mathbf{p}, \mathbf{q} \rangle} \xi_d^{\langle G\mathbf{p}', G\mathbf{p} \rangle} f(\mathbf{p}) \\ &= (-1)^{(d+1)\langle \mathbf{p}, \mathbf{q} \rangle} \xi_d^{d \det G \langle \mathbf{p}, \mathbf{q} \rangle} f(\mathbf{p}) \\ &= (-1)^{(d+1)(1 + \det G)\langle \mathbf{p}, \mathbf{q} \rangle} f(\mathbf{p}) \\ &= f(\mathbf{p}), \end{aligned} \tag{5.69}$$

where in the last step we used the fact that $\det G$ is coprime to d, as follows from Eq. (1.51). The second statement is an immediate consequence of this. □

Theorem 5.8. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, and let $\mathbf{p} \in \mathbb{Z}^2$. If $\mathbf{p} \not\equiv \mathbf{0} \pmod{d}$, then the numbers $\tilde{\nu}_{\mathbf{p}}(t)$ are real and satisfy*

$$\tilde{\nu}_{\mathbf{p}}(t)\tilde{\nu}_{-\mathbf{p}}(t) = 1. \tag{5.70}$$

Remark. This theorem establishes two of the requirements which must be satisfied if the expression on the right-hand side of (1.53) in Definition 1.44 is to be a ghost fiducial.

Proof. Let $\mathfrak{A}$ be the unique class in $\overline{\mathrm{Clm}}^{\flat}_{d\infty_2}(\mathcal{O}_f)$ that maps to the $\mathrm{SL}_2(\mathbb{Z})$-orbit of $(d^{-1}\mathbf{p}, \rho_t)$ under the map $\Upsilon_{d\mathcal{O}_f}$ described in [70, Thm. 3.12] and at the end of Section 2.6. Theorem 2.19 then gives the formula

$$(\psi^{-2}\chi^{-1}_{d^{-1}\mathbf{p}})(A_t)\, \mathfrak{w}_A^{d^{-1}\mathbf{p}}(\rho_t)^2 = \exp\bigl(nZ'_{d\infty_2}(0, \mathfrak{A})\bigr)\,, \tag{5.71}$$

where $Z_{d\infty_2}(s, \mathfrak{A})$ is the differenced ray class partial zeta function defined in Definition 2.4. By Definition 1.32 and Theorem 5.6, we have

$$(\tilde{\nu}_{\mathbf{p}}(t))^2 = \phi_{\mathbf{p}}(t)^2\, \mathfrak{w}_A^{d^{-1}\mathbf{p}}(\rho_t)^2 = (\psi^{-2}\chi^{-1}_{d^{-1}\mathbf{p}})(A_t)\, \mathfrak{w}_A^{d^{-1}\mathbf{p}}(\rho_t)^2\,, \tag{5.72}$$

and thus

$$(\tilde{\nu}_{\mathbf{p}}(t))^2 = \exp\bigl(nZ'_{d\infty_2}(0, \mathfrak{A})\bigr)\,. \tag{5.73}$$

The partial zeta function $Z_{d\infty_2}(s, \mathfrak{A})$ is a complex analytic function defined by a Dirichet series with real coefficients for $\mathrm{Re}(s) > 1$ and by analytic continuation to all $s \in \mathbb{C}$. The equation $(Z_{d\infty_2}(s, \mathfrak{A}))^* = Z_{d\infty_2}(s^*, \mathfrak{A})$ holds for $\mathrm{Re}(s) > 1$ and thus for all $s \in \mathbb{C}$ (where * denotes complex conjugation). Therefore, $Z'_{d\infty_2}(0, \mathfrak{A})$ is real, so $\exp\bigl(nZ'_{d\infty_2}(0, \mathfrak{A})\bigr)$ is real and positive, and thus $\tilde{\nu}_{\mathbf{p}}(t)$ is real.

We now compute $\tilde{\nu}_{\mathbf{p}}(t)\tilde{\nu}_{-\mathbf{p}}(t)$. Using the definition of $\tilde{\nu}_{\pm\mathbf{p}}(t)$ (Definition 1.32), we have

$$\tilde{\nu}_{\mathbf{p}}(t)\tilde{\nu}_{-\mathbf{p}}(t) = (\phi_{\mathbf{p}}(t)\phi_{-\mathbf{p}}(t)) \left(\mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho_t)\, \mathfrak{w}_{A_t}^{-d^{-1}\mathbf{p}}(\rho_t)\right). \tag{5.74}$$

Using Definition 1.30, the SF phase satisfies

$$\phi_{-\mathbf{p}}(t) = (-1)^{s_d(-\mathbf{p})} e^{-\frac{\pi i}{12}\Psi(A_t)} \xi_d^{-\frac{fjm}{f}Q(-\mathbf{p})} = (-1)^{s_d(\mathbf{p})} e^{-\frac{\pi i}{12}\Psi(A_t)} \xi_d^{-\frac{fjm}{f}Q(\mathbf{p})} = \phi_{\mathbf{p}}(t). \tag{5.75}$$

Corollary 2.12 and Theorem 5.6 imply

$$\mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho_t)\, \mathfrak{w}_{A_t}^{-d^{-1}\mathbf{p}}(\rho_t) = (\psi^2\chi_{\mathbf{r}})(A_t) = \phi_{\mathbf{p}}(t)^{-2}. \tag{5.76}$$

Consequently $\tilde{\nu}_{\mathbf{p}}(t)\tilde{\nu}_{-\mathbf{p}}(t) = \phi_{\mathbf{p}}(t)^2\phi_{\mathbf{p}}(t)^{-2} = 1$. □

Lemma 5.9. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple. Then*

$$\tilde{\nu}_{\mathbf{0}}(t) + \frac{1}{\tilde{\nu}_{\mathbf{0}}(t)} = -(d - 2r)\sqrt{d_j + 1}. \tag{5.77}$$

Proof. It follows from Lemma 2.15 that

$$\tilde{\nu}_{\mathbf{0}}(t) = \phi_{\mathbf{0}}(t)\mathfrak{w}^{\mathbf{0}}_{A_t}(\rho_{Q,+}) = -\frac{1}{\sqrt{j_{A_t}(\rho_{Q,+})}} \tag{5.78}$$

Write $A_t = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. It follows from Lemma 4.49 that $A_t\rho_{Q,+} = \rho_{Q,+}$. Hence

$$\gamma\rho_{Q,+}^2 + (\delta - \alpha)\rho_{Q,+} - \beta = 0. \tag{5.79}$$

Consequently

$$\rho_{Q,+} = \frac{\alpha - \delta \pm \sqrt{(\alpha + \delta)^2 - 4}}{2\gamma} \qquad \Longrightarrow \qquad j_A(\rho_{Q,+}) = \frac{\mathrm{Tr}(A) \pm \sqrt{\mathrm{Tr}(A)^2 - 4}}{2}. \tag{5.80}$$

It follows from Theorem 4.53 that $\mathrm{Tr}(A_t)$ and consequently $j_{A_t}(\rho_{Q,+})$ are positive. So

$$\left(\sqrt{j_{A_t}(\rho_{Q,+})} + \frac{1}{\sqrt{j_{A_t}(\rho_{Q,+})}}\right)^2 = \mathrm{Tr}(A_t) + 2 \tag{5.81}$$

implying

$$\tilde{\nu}_{\mathbf{0}}(t) + \frac{1}{\tilde{\nu}_{\mathbf{0}}(t)} = -\sqrt{\mathrm{Tr}(A_t) + 2}. \tag{5.82}$$

It follows from Theorem 4.53 that $A_t = \chi_Q(\varepsilon^{j(2m+1)})$, which in view of Lemma 4.3 means $\mathrm{Tr}(A) = \mathrm{Tr}(\varepsilon^{j(2m+1)}) = d_{j(2m+1)} - 1$. Lemma 4.24 then implies

$$\sqrt{\mathrm{Tr}(A) + 2} = (r_{j,m+1} - r_{j,m})\sqrt{d_j + 1} = (d - 2r_{j,m})\sqrt{d_j + 1}. \tag{5.83}$$

Together, (5.82) and (5.83) imply (5.78). □

Definition 5.10 (function Φ_t)**.** Given an admissible tuple $t = (d, r, Q) \sim (K, j, m, Q)$, define $\Phi_t \colon \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/\bar{d}\mathbb{Z}$ by

$$\Phi_t(x) = r(2x + d + d_j - 1). \tag{5.84}$$

Lemma 5.11. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple.*

(1) If d is odd, then Φ_t is a bijection of $\mathbb{Z}/d\mathbb{Z}$ onto itself.

(2) If d is even, then Φ_t is a bijection of $\mathbb{Z}/d\mathbb{Z}$ onto the set of odd elements in $\mathbb{Z}/\bar{d}\mathbb{Z}$.

The inverse function is given by

$$\Phi_t^{-1}(x) = \frac{(d+1)\big((d_j+1)rx - (d_j-1)\big)}{2}. \tag{5.85}$$

For all $x \in \mathbb{Z}$, $\Phi_t(x)$ is coprime to $\bar{d}$ if and only if $2x + d_j - 1$ is coprime to d.

Proof. Suppose d is odd. If $\Phi_t(x) = \Phi_t(x')$, then $2rx \equiv 2rx' \pmod{d}$, which in view of Corollary 4.23 means $x \equiv x' \pmod{\bar{d}}$. So Φ_t is injective. Since the domain and codomain have the same cardinality, it follows that it is also surjective. To calculate the inverse, observe that it follows from Lemma 4.25 that, if $y = \Phi_t(x)$, then

$$x = 2^{-1}\left(r^{-1}y - (d_j - 1)\right) = \tfrac{d+1}{2}\left((d_j+1)ry - (d_j-1)\right), \tag{5.86}$$

where 2^{-1} is the multiplicative inverse of $2 \pmod{d}$.

Suppose, on the other hand, that d is even. Then it follows from Corollary 4.23 that r is odd and from Lemma 4.24 that d_j is even. So $\Phi_t(x)$ is odd for all $x \in \mathbb{Z}/d\mathbb{Z}$. If $\Phi_t(x) \equiv \Phi_t(x') \pmod{\bar{d}}$, then $2rx \equiv 2rx' \pmod{2d}$. Since r is odd, it follows that $x \equiv x' \pmod{d}$. So Φ_t is injective. Since the domain and the set of odd elements in $\mathbb{Z}/\bar{d}\mathbb{Z}$ have the same cardinality, Φ_t must in fact be a bijection onto the set of odd elements in $\mathbb{Z}/\bar{d}\mathbb{Z}$. To calculate the inverse, suppose $y = \Phi_t(x)$ for some $x \in \mathbb{Z}/d\mathbb{Z}$. Then it follows from Lemma 4.25 that

$$\begin{aligned} 2x &\equiv yr^{-1} - (d_j - 1) - d \pmod{2d} \\ &\equiv yr(1 + d_j + d) - (d_j - 1) - d \pmod{2d} \\ &\equiv (d_j+1)ry - (d_j - 1) + d(yr - 1) \pmod{2d}. \end{aligned} \tag{5.87}$$

Since $yr - 1$ is even, this means

$$2x = (d_j+1)ry + 1 - d_j \pmod{2d}. \tag{5.88}$$

The fact that yr and $d_j \pm 1$ are odd means the right-hand side is even. So

$$x \equiv \frac{(d_j+1)r_{j,m}y - (d_j-1)}{2} \pmod{d} \tag{5.89}$$

or, equivalently,

$$x \equiv (d+1)\left(\frac{(d_j+1)ry - (d_j-1)}{2}\right) \pmod{d}. \tag{5.90}$$

Finally, $\Phi_t(x)$ is coprime to $\bar{d}$ if and only if it is coprime to d. Since r is coprime to d, this is true if and only if $2x - 1 + d_j$ is coprime to d. □

5.4. **Ghost existence under the Twisted Convolution Conjecture.** We now turn to the proof of Theorem 1.46, asserting that, under the assumption of Conjecture 1.35, the $d \times d$ matrix $\tilde{\Pi}_s$ constructed from a fiducial datum is a ghost r-SIC fiducial projector.

Proof of Theorem 1.46. To prove that $\tilde{\Pi}_s$ is a ghost projector, we need to show:

(1) The expression on the RHS of (1.53) is well-defined, in that the sum is independent of the set of coset representatives chosen,
(2) $\tilde{\nu}_{\mathbf{p}}(t)$ is real for all $\mathbf{p} \not\equiv \mathbf{0} \pmod{d}$,
(3) $\tilde{\nu}_{\mathbf{p}}(t)\tilde{\nu}_{-\mathbf{p}}(t) = 1$ for all $\mathbf{p} \not\equiv \mathbf{0} \pmod{d}$,
(4) $\tilde{\Pi}_s^2 = \tilde{\Pi}_s$.

The first proposition is proved in Lemma 1.43, and the second and third in Theorem 5.8. It remains to prove the last. We have

$$\tilde{\Pi}_s = \frac{r}{d}I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{\mathbf{p}}(t) D_{G^{-1}\mathbf{p}} \tag{5.91}$$

where the sum is over any set of coset representatives of $\mathbb{Z}^2/d\mathbb{Z}^2$ with the representative of $d\mathbb{Z}^2$ excluded. Hence

$$\begin{aligned}
\tilde{\Pi}_s^2 - \tilde{\Pi}_s &= \frac{r(r-d)}{d^2}I + \frac{2r-d}{d^2\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{\mathbf{p}}(t) D_{G^{-1}\mathbf{p}} \\
&\quad + \frac{1}{d^2(d_j+1)} \sum_{\mathbf{p},\mathbf{q} \notin d\mathbb{Z}^2} \xi_d^{\langle G^{-1}\mathbf{p}, G^{-1}\mathbf{q}\rangle} \tilde{\nu}_{\mathbf{p}}(t)\tilde{\nu}_{\mathbf{q}}(t) D_{G^{-1}(\mathbf{p}+\mathbf{q})} \\
&= \frac{r(r-d)}{d^2}I + \frac{2r-d}{d^2\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{\mathbf{p}}(t) D_{G^{-1}\mathbf{p}} \\
&\quad + \frac{1}{d^2(d_j+1)} \sum_{\mathbf{p}} \left(\sum_{\substack{\mathbf{q} \notin d\mathbb{Z}^2, \\ \mathbf{q} \notin \mathbf{p}+d\mathbb{Z}^2}} \xi_d^{\det(G^{-1})\langle \mathbf{p}, \mathbf{q}\rangle} \tilde{\nu}_{\mathbf{p}-\mathbf{q}}(t)\tilde{\nu}_{\mathbf{q}}(t) \right) D_{G^{-1}\mathbf{p}},
\end{aligned} \tag{5.92}$$

where $\mathbf{p}$ is summed over a complete set of cosets for $\mathbb{Z}^2/d\mathbb{Z}^2$, and $\mathbf{q}$ is summed over such a set with $d\mathbb{Z}^2$ and $\mathbf{p} + d\mathbb{Z}^2$ removed. Comparing (1.51) to (5.84), we see that

$$\det(G^{-1}) = (\det(G))^{-1} = \Phi_t(\lambda) \tag{5.93}$$

for some $\lambda \in \mathcal{Z}_t$, while it follows from Theorem 4.21 that

$$\frac{r(r-d)}{d^2} = -\frac{(d^2-1)}{d^2(d_j+1)}. \tag{5.94}$$

Inserting these expressions into Equation (5.92) gives

$$\tilde{\Pi}_s^2 - \tilde{\Pi}_s = \frac{1}{d^2(d_j+1)} \left(-(d^2-1)I - (d-2r)\sqrt{d_j+1} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{\mathbf{p}}(t) D_{G^{-1}\mathbf{p}} + \sum_{\mathbf{p}} \left(\sum_{\substack{\mathbf{q} \notin d\mathbb{Z}^2, \\ \mathbf{q} \notin \mathbf{p} + d\mathbb{Z}^2}} \xi_d^{\Phi_t(\lambda)\langle \mathbf{p}, \mathbf{q} \rangle} \tilde{\nu}_{\mathbf{p}-\mathbf{q}}(t) \tilde{\nu}_{\mathbf{q}}(t) \right) D_{G^{-1}\mathbf{p}} \right). \tag{5.95}$$

Theorem 5.8 and Lemma 5.9 imply

$$\begin{aligned}
&\sum_{\mathbf{p}} \left(\sum_{\substack{\mathbf{q} \notin d\mathbb{Z}^2, \\ \mathbf{q} \notin \mathbf{p} + d\mathbb{Z}^2}} \xi_d^{\Phi_t(\lambda)\langle \mathbf{p}, \mathbf{q} \rangle} \tilde{\nu}_{\mathbf{p}-\mathbf{q}}(t) \tilde{\nu}_{\mathbf{q}}(t) \right) D_{G^{-1}\mathbf{p}} \\
&\quad = (d^2-1)I + \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \left(\sum_{\substack{\mathbf{q} \notin d\mathbb{Z}^2, \\ \mathbf{q} \notin \mathbf{p} + d\mathbb{Z}^2}} \xi_d^{\Phi_t(\lambda)\langle \mathbf{p}, \mathbf{q} \rangle} \tilde{\nu}_{\mathbf{p}-\mathbf{q}}(t) \tilde{\nu}_{\mathbf{q}}(t) \right) D_{G^{-1}\mathbf{p}} \\
&\quad = (d^2-1)I + \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \left(\sum_{\substack{\mathbf{q} \notin d\mathbb{Z}^2, \\ \mathbf{q} \notin \mathbf{p} + d\mathbb{Z}^2}} \xi_d^{\Phi_t(\lambda)\langle \mathbf{p}, \mathbf{q} \rangle} \frac{\tilde{\nu}_{\mathbf{q}}(t)}{\tilde{\nu}_{\mathbf{q}-\mathbf{p}}(t)} \right) D_{G^{-1}\mathbf{p}} \\
&\quad = (d^2-1)I + (d-2r)\sqrt{d_j+1} \sum_{\mathbf{p} \notin d_{j,m}\mathbb{Z}^2} \tilde{\nu}_{\mathbf{p}}(t) D_{G^{-1}\mathbf{p}} \\
&\qquad + \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \left(\sum_{\mathbf{q} \in \mathcal{I}_{\mathbf{p}}} \xi_d^{\Phi_t(\lambda)\langle \mathbf{p}, \mathbf{q} \rangle} \frac{\tilde{\nu}_{\mathbf{q}}(t)}{\tilde{\nu}_{\mathbf{q}-\mathbf{p}}(t)} \right) D_{G^{-1}\mathbf{p}}
\end{aligned} \tag{5.96}$$

where $\mathcal{I}_{\mathbf{p}}$ is a complete set of coset representatives for $\mathbb{Z}^2/d_{j,m}\mathbb{Z}^2$ which includes $\mathbf{0}$ and $\mathbf{p}$. Hence

$$\begin{aligned}
\tilde{\Pi}_s^2 - \tilde{\Pi}_s &= \frac{1}{d^2(d_j+1)} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \left(\sum_{\mathbf{q} \in \mathcal{I}_{\mathbf{p}}} \xi_d^{\Phi_t(\lambda)\langle \mathbf{p}, \mathbf{q} \rangle} \frac{\tilde{\nu}_{\mathbf{q}}(t)}{\tilde{\nu}_{\mathbf{q}-\mathbf{p}}(t)} \right) D_{G^{-1}\mathbf{p}} \\
&= \frac{1}{d^2(d_j+1)} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \left(\sum_{\mathbf{q} \in \mathcal{I}_{\mathbf{p}}} \xi_d^{\Phi_t(\lambda)\langle \mathbf{p}, \mathbf{q} \rangle} \left(\frac{\phi_{\mathbf{q}}(t)}{\phi_{\mathbf{q}-\mathbf{p}}(t)} \right) \left(\frac{\mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_{Q,+})}{\mathfrak{w}_{A_t}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_{Q,+})} \right) \right) D_{G^{-1}\mathbf{p}}
\end{aligned} \tag{5.97}$$

where we used Definition 1.32 in the second line. It follows from Definition 1.30 that

$$\frac{\phi_{\mathbf{q}}(t)}{\phi_{\mathbf{q}-\mathbf{p}}(t)} = (-1)^{s_d(\mathbf{q})+s_d(\mathbf{q}-\mathbf{p})} \xi_d^{\frac{f_{jm}}{f}(Q(\mathbf{q}-\mathbf{p})-Q(\mathbf{q}))}. \tag{5.98}$$

We have

$$\begin{aligned}(-1)^{s_d(\mathbf{q})+s_d(\mathbf{q}-\mathbf{p})} &= (-1)^{(1+d)((1+q_1)(1+q_2)+(1+q_1+p_1)(1+q_2+p_2)} \\ &= (-1)^{(1+d)(p_1(1+q_2)+p_2(1+q_1)+p_1p_2} \\ &= (-1)^{(1+d)(p_1+p_2+p_1p_2)+(1+d)\langle\mathbf{p},\mathbf{q}\rangle} \\ &= (-1)^{1+d+(1+d)(1+p_1)(1+p_2)}\xi_d^{d\langle\mathbf{p},\mathbf{q}\rangle} \\ &= (-1)^{1+s_d(\mathbf{p})}\xi_d^{d\langle\mathbf{p},\mathbf{q}\rangle}. \end{aligned} \tag{5.99}$$

Also, referring to Definition 1.28, we see that

$$\frac{2f_j}{f}\mathbf{p}^{\mathrm{T}}Q\mathbf{q} = -\frac{2f_j}{f}\langle\mathbf{p}, SQ\mathbf{q}\rangle = \langle\mathbf{p}, (d_j - 1 - 2L_{\mathrm{z,t}})\mathbf{q}\rangle, \tag{5.100}$$

implying

$$\begin{aligned}\frac{f_{jm}}{f}\left(Q(\mathbf{q}-\mathbf{p}) - Q(\mathbf{q})\right) &= \frac{rf_j}{f}\left(Q(\mathbf{p}) - 2\mathbf{p}^{\mathrm{T}}Q\mathbf{q}\right) \\ &= \frac{rf_j}{f}Q(\mathbf{p}) - r(d_j-1)\langle\mathbf{p},\mathbf{q}\rangle + 2r\langle\mathbf{p}, L_{\mathrm{z,t}}\mathbf{q}\rangle. \end{aligned} \tag{5.101}$$

Hence

$$\frac{\phi_{\mathbf{q}}(t)}{\phi_{\mathbf{q}-\mathbf{p}}(t)} = (-1)^{1+s_d(\mathbf{p})}\xi_d^{\frac{rf_j}{f}Q(\mathbf{p})}\xi_d^{(d-r(d_j-1))\langle\mathbf{p},\mathbf{q}\rangle}\omega_d^{r\langle\mathbf{p},L_{\mathrm{z,t}}\mathbf{q}\rangle}. \tag{5.102}$$

It follows from Lemma 2.13 that

$$\frac{\mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_{Q,+})}{\mathfrak{w}_{A_t}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_{Q,+})} = \mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_{Q,+})\,\mathfrak{w}_{A_t^{-1}}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_{Q,+})\,. \tag{5.103}$$

Substituting (5.102) and (5.103) into (5.97) gives

$$\begin{aligned}\tilde{\Pi}_s^2 - \tilde{\Pi}_s = \frac{1}{d^2(d_j+1)}\sum_{\mathbf{p}\notin d\mathbb{Z}^2}(-1)^{1+s_d(\mathbf{p})}\xi_d^{\frac{rf_j}{f}Q(\mathbf{p})}\Bigg(\sum_{\mathbf{q}\in\mathcal{I}_{\mathbf{p}}}\xi_d^{(\Phi_t(\lambda)+d-r(d_j-1))\langle\mathbf{p},\mathbf{q}\rangle} \\ \times\,\omega_d^{r\langle\mathbf{p},L_{\mathrm{z,t}}\mathbf{q}\rangle}\mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_{Q,+})\,\mathfrak{w}_{A_t^{-1}}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_{Q,+})\Bigg)\,D_{G^{-1}\mathbf{p}}. \end{aligned} \tag{5.104}$$

It follows from Definition 1.34 that $2\lambda + d_j - 1$ is coprime to d. In view of Lemma 5.11 this means $\Phi_t(\lambda)$ is coprime to $\bar{d}$. Consequently

$$\Phi_t(\lambda) + d \equiv (d+1)\Phi_t(\lambda) \pmod{\bar{d}}\,. \tag{5.105}$$

Also, it follows from Lemma 4.24 that d_j is even if d is even. So

$$dd_j \equiv 0 \pmod{\bar{d}} \tag{5.106}$$

irrespective of whether d is odd or even. Putting these two facts together we conclude

$$\begin{aligned}\xi_d^{(\Phi_t(\lambda)+d-r(d_j-1))\langle\mathbf{p},\mathbf{q}\rangle} &= \xi_d^{((d+1)\Phi_t(\lambda)-r(d_j-1))\langle\mathbf{p},\mathbf{q}\rangle} \\ &= \xi_d^{((d+1)r(2z+d+d_j-1)-r(d_j-1))\langle\mathbf{p},\mathbf{q}\rangle} \\ &= \xi_d^{r(2(d+1)\lambda+d(d+1)+d(d_j-1)))\langle\mathbf{p},\mathbf{q}\rangle} \\ &= \omega_d^{rz\langle\mathbf{p},\mathbf{q}\rangle}. \end{aligned} \tag{5.107}$$

Substituting back into (5.104) we deduce

$$\tilde{\Pi}_s^2 - \tilde{\Pi}_s = \sum_{\mathbf{p}\notin d\mathbb{Z}^2} \frac{(-1)^{1+s_d(\mathbf{p})}\xi_d^{\frac{rf_j}{f}Q(\mathbf{p})}}{d^2(d_j+1)} \left(\sum_{\mathbf{q}\in\mathcal{I}_\mathbf{p}} \omega_d^{r\langle \mathbf{p},(zI+L_{\mathrm{z,t}})\mathbf{q}\rangle} \mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_{Q,+})\, \mathfrak{w}_{A_t^{-1}}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_{Q,+}) \right) D_{G^{-1}\mathbf{p}}. \tag{5.108}$$

It follows that $\tilde{\Pi}_s^2 = \tilde{\Pi}_s$ if and only if

$$\sum_{\mathbf{q}\in\mathcal{I}_\mathbf{p}} \omega_d^{r\langle \mathbf{p},(zI+L_{\mathrm{z,t}})\mathbf{q}\rangle} \mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_{Q,+})\, \mathfrak{w}_{A_t^{-1}}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_{Q,+}) = 0 \tag{5.109}$$

for all $\mathbf{p} \not\equiv \mathbf{0} \pmod d$. If $\mathbf{p} \equiv \mathbf{0} \pmod d$, it follows from Lemma 2.13 that

$$\sum_{\mathbf{q}\in\mathcal{I}_\mathbf{p}} \omega_d^{r\langle \mathbf{p},(zI+L_{\mathrm{z,t}})\mathbf{q}\rangle} \mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_{Q,+})\, \mathfrak{w}_{A_t^{-1}}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_{Q,+}) = \sum_{\mathbf{q}\in\mathcal{I}_\mathbf{0}} \mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_{Q,+})\, \mathfrak{w}_{A_t^{-1}}^{d^{-1}(\mathbf{q})}(\rho_{Q,+}) = d^2 \tag{5.110}$$

irrespective of whether $\tilde{\Pi}_s$ is a ghost fiducial. So it is in fact the case that $\tilde{\Pi}_s^2 = \tilde{\Pi}_s$ if and only if

$$\sum_{\mathbf{q}\in\mathcal{I}_\mathbf{p}} \omega_d^{r\langle \mathbf{p},(zI+L_{\mathrm{z,t}})\mathbf{q}\rangle} \mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_{Q,+})\, \mathfrak{w}_{A_t^{-1}}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_{Q,+}) = d^2\delta^{(d)}_{\mathbf{p},\mathbf{0}} \tag{5.111}$$

for all $\mathbf{p}$. □

5.5. **Remarks concerning the set of shifts.** In this subsection we make some observations concerning the set of shifts $\mathcal{Z}_t$ for a given admissible tuple t.

The argument in Section 5.4 actually shows a little more than was required for the proof of Theorem 1.46. Specifically, let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, and let λ be an element of $\mathcal{Z}_t$. Then $2z + d_j - 1$ is coprime to d, which in view of Lemma 5.11 means $\Phi_t(\lambda)$ is coprime to $\bar{d}$. So if we define $G = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \Phi_t(\lambda)^{-1} \end{smallmatrix}\right)$ (where $\Phi_t(\lambda)^{-1}$ is the inverse of $\Phi_t(\lambda)$ modulo $\bar{d}$), then $G \in \mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$, and $s = (d, r, Q, G, g) \sim (K, j, m, Q, G, g)$ is a fiducial datum for any appropriate choice of g. Consequently

$$\tilde{\Pi}_s = \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p}\notin d\mathbb{Z}^2} \tilde{\nu}_{G\mathbf{p}}(t) D_\mathbf{p} \tag{5.112}$$

is a ghost fiducial. Consider its complex conjugate

$$\begin{aligned} \tilde{\Pi}_s^* &= \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p}\notin d\mathbb{Z}^2} \tilde{\nu}_{G\mathbf{p}}(t) D_{J\mathbf{p}} \\ &= \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p}\notin d\mathbb{Z}^2} \tilde{\nu}_{JG\mathbf{p}}(t) D_\mathbf{p} \end{aligned} \tag{5.113}$$

(where J is defined in Definition 3.3). It is easily seen that $\tilde{\Pi}_s^*$ is also a ghost fiducial. The fact that $\det(JG) = -\det(G)$ means that $\det(JG)$ is coprime to $\bar{d}$, implying that $\bar{\lambda} = \Phi_t^{-1}(\det(JG)^{-1})$ is well-defined. Since $\Phi_t(\bar{\lambda}) = \det(JG)^{-1}$ is coprime to $\bar{d}$ it follows from Lemma 5.11 that $2\bar{\lambda}+d_j-1$. The argument in Section 5.4 shows that the fact that $\tilde{\Pi}_s^{*2} = \tilde{\Pi}_s^*$ implies that $\bar{\lambda}$ satisfies (1.49). It follows that $\bar{\lambda} \in \mathcal{Z}_t$.

We have

$$\bar{\lambda} = \Phi_t^{-1}(-\det G^{-1}) = \Phi_t^{-1}(-\Phi_t(\lambda)). \tag{5.114}$$

This expression leads to a simple, fully explicit expression for $\bar{\lambda}$ in terms of λ:

Lemma 5.12. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, let $\lambda \in \mathcal{Z}_t$, and let $\bar{\lambda} = \Phi_t^{-1}(-\Phi_t(\lambda))$. Then*

$$\bar{\lambda} = -(\lambda + d_j - 1) \tag{5.115}$$

Proof. Definition 5.10 and Lemma 5.11 imply

$$\begin{aligned}\bar{\lambda} &= \Phi_t^{-1}(-\det G^{-1}) \\ &= \Phi_t^{-1}(-\Phi_t(\lambda)) \\ &= \frac{(d+1)\left(-(d_j+1)r^2(2z+d+d_j-1)-(d_j-1)\right)}{2}.\end{aligned} \tag{5.116}$$

It follows from (4.110) that

$$-(d_j+1)r^2 = d - 1 + k\bar{d} \tag{5.117}$$

for some integer k. So

$$\begin{aligned}\bar{\lambda} &= \frac{(d+1)\left((d-1+k\bar{d})(2z+d+d_j-1)-(d_j-1)\right)}{2} \\ &= (d+1)(d-1+k\bar{d})\lambda + \frac{(d+1)\left((d-1+k\bar{d})(d+d_j-1)-(d_j-1)\right)}{2} \\ &= -\lambda + \frac{(d+1)\left((d-1+k\bar{d})(d+d_j-1)-(d_j-1)\right)}{2}.\end{aligned} \tag{5.118}$$

Suppose d is odd. Then $d+1 = 2m$ for some integer m, and

$$\begin{aligned}\bar{\lambda} &= -\lambda + m\left((d-1+k\bar{d})(d+d_j-1)-(d_j-1)\right) \\ &= -\lambda - 2m(d_j-1) \\ &= -\lambda - (d+1)(d_j-1) \\ &= -\lambda - (d_j-1).\end{aligned} \tag{5.119}$$

Suppose, on the other hand, d is even. Then $d = 2m$ for some integer m, and

$$\begin{aligned}\bar{\lambda} &= -\lambda + \frac{(d+1)\left((2m+4km-1)(2m+d_j-1)-(d_j-1)\right)}{2} \\ &= -\lambda + \frac{(d+1)\left(2m(1+2k)(2m+d_j-1)-2m-2(d_j-1)\right)}{2} \\ &= -\lambda + (d+1)\left(m(1+2k)(2m+d_j-1)-m-(d_j-1)\right) \\ &= -\lambda + m(1+2k)(d_j-1) - m - (d_j-1) \\ &= -\lambda + md_j - (d_j-1).\end{aligned} \tag{5.120}$$

The fact that d is even means, in view of Lemma 4.24, that d_j is even. Consequently $md_j \equiv 0 \pmod{d}$, and $\bar{\lambda} = -\lambda - (d_j - 1)$ in this case too. □

It follows from Lemma 5.12 that possible shifts come in pairs $(\lambda, \bar{\lambda})$. The question then arises how many such pairs there are. Observe that it follows from Lemma 4.26 that $\lambda = 0$ and $\lambda = 1$ both satisfy the requirement that $2z + d_j - 1$ be coprime to d. In every case examined it appears, as a matter of empirical observation, that they also satisfy (1.49). The corresponding values of $\bar{\lambda}$ are $\bar{\lambda} = d - d_j + 1$ and $\bar{\lambda} = d - d_j$, respectively. The values of $\det G$ are as given in the table

λ	$\det G$
0	$r^{-1}(d+d_j-1)^{-1}$
1	$r^{-1}(d+d_j+1)^{-1}=r$
$d-d_j$	$-r^{-1}(d+d_j+1)^{-1}=-r$
$d-d_j+1$	$-r^{-1}(d+d_j-1)^{-1}$

where the symbols r^{-1}, $(d+d_j\pm 1)^{-1}$ denote multiplicative inverses modulo $\bar{d}$, and where the alternative expressions for $\det G$ in the second and third rows are obtained using (4.110). Note that if $m=1$ these four values for λ reduce to the two values 0, 1 with the corresponding values of $\det G$ being -1, $+1$ respectively.

It appears (again as a matter of empirical observation) that, if $m\leq 2$, these are the only elements of $\mathcal{Z}_t$. However, if $m>2$, there seem to be others. Specifically, in the cases we examined we found three pairs for $m=3$ and $m=4$, and five pairs for $m=5$. However, we were not able to discern any obvious pattern to the additional λ-values. This is a question requiring further investigation.

5.6. **Conditional SIC existence.** We now turn to the proof of Theorem 1.47, which asserts that Zauner's conjecture follows from the conditional assumptions of the Twisted Convolution Conjectural and the Stark Conjecture, and more precisely, that those conditional assumptions imply that the $d\times d$ matrix Π_s constructed from a fiducial datum s is an r-SIC fiducial projector.

Proof of Theorem 1.47. We have

$$\tilde{\Pi}_s=\frac{r}{d}I+\frac{1}{d}\sum_{\mathbf{p}\notin d\mathbb{Z}^2}\tilde{\mu}_{\mathbf{p}}(t)D_{G^{-1}\mathbf{p}}. \tag{5.121}$$

Set $\mu_{\mathbf{p}}(t)=g(\tilde{\mu}_p(t))$, and apply the Galois automorphism g to obtain

$$\Pi_s=g(\tilde{\Pi}_s)=\frac{r}{d}I+\frac{1}{d}\sum_{\mathbf{p}\notin d\mathbb{Z}^2}\mu_{\mathbf{p}}(t)g(D_{G^{-1}\mathbf{p}})=\frac{r}{d}I+\frac{1}{d}\sum_{\mathbf{p}\notin d\mathbb{Z}^2}\mu_{\mathbf{p}}(t)D_{H_g\mathbf{p}}, \tag{5.122}$$

where $H_g=\left(\begin{smallmatrix}1&0\\0&k_g\end{smallmatrix}\right)$ and we have used Theorem 3.7 in the last line. To show that Π_s is a Weyl–Heisenberg r-SIC fiducial projector, we must show that:

(1) $\Pi_s^2=\Pi_s$,
(2) $\mu_p(t)\mu_{-p}(t)=\frac{1}{d_j+1}$ for $\mathbf{p}\notin d\mathbb{Z}^2$, and
(3) $|\mu_p(t)|=\frac{1}{\sqrt{d_j+1}}$ for $\mathbf{p}\notin d\mathbb{Z}^2$.

By Theorem 1.46 (using the assumption of Conjecture 1.35), $\tilde{\Pi}_s$ is a ghost r-SIC fiducial, so $\tilde{\Pi}_s^2=\tilde{\Pi}_s$. Applying the Galois automorphism g (which commutes with matrix multiplication) shows that $\Pi_s^2=\Pi_s$, giving (1). Now suppose $\mathbf{p}\notin d\mathbb{Z}^2$, and rewrite Theorem 5.8 in terms of the unnormalized overlaps:

$$\tilde{\mu}_p(t)\tilde{\mu}_{-p}(t)=\tfrac{1}{d_j+1}. \tag{5.123}$$

Applying g gives $\mu_p(t)\mu_{-p}(t)=\frac{1}{d_j+1}$, which is (2). As in (6.21), we have

$$\tilde{\mu}_{\mathbf{p}}(t)=\tfrac{1}{\sqrt{d_j+1}}\,\phi_{\mathbf{p}}(t)\mathfrak{w}_A^{d^{-1}\mathbf{p}}(\rho_t)\ \text{ for } \mathbf{p}\not\equiv\mathbf{0}\ (\mathrm{mod}\ d)\,. \tag{5.124}$$

By the assumption of Conjecture 1.36, we have

$$\left|g(\mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho_t))\right|=1. \tag{5.125}$$

Therefore, writing $g(\sqrt{d_j+1}) = \pm\sqrt{d_j+1}$ and using the fact that $\phi_{\mathbf{p}}(t)$ is a root of unity and indeed a power of ξ_d, we have

$$\mu_{\mathbf{p}}(t) = \pm\tfrac{1}{\sqrt{d_j+1}}\,\phi_{\mathbf{p}}(t)^{k_g} g(\mathfrak{w}_A^{d^{-1}\mathbf{p}}(\rho_t)). \tag{5.126}$$

Taking absolute values, we obtain $|\mu_{\mathbf{p}}(t)| = \frac{1}{\sqrt{d_j+1}}$, which is (3). □

6. Proof of main theorems (2): Class fields attained

We now prove results about which abelian extensions are generated by r-SICs according to our conjectural framework.

In Section 6.3, we prove results about realizing the field E_t associated to an admissible tuple t as a particular abelian extension of the associated field K. We prove Theorem 1.49, showing that E_t is an abelian extension of K. We also prove Theorem 1.50, relating E_t to a particular ray class field. Theorem 6.7 provides a strengthening of Theorem 1.50, and Conjecture 6.8 provides a strengthening of Conjecture 1.51.

In Section 6.4, we prove results on obtaining arbitrary abelian extensions of a real quadratic field K from r-SICs. Theorem 6.14 is an unconditional number-theoretic result on the containment of certain abelian extensions in certain ray class fields, based primarily on a technical elementary number theory result given as Theorem 6.13. As a corollary, we obtain Theorem 1.52, asserting under Stark–Tate that, when the trace of the fundamental unit of K is odd, the fields E_t are cofinal in the set of all abelian extensions.

We need some preliminary material to set the stage for the proofs of our main theorems on SIC-generated class fields. Section 6.1 defines three important fields, $E_s^{(1)}$, $E_t^{(2)}$, and E_t, attached to a fiducial datum $s = (t, g, G)$. Section 6.2 proves some key lemmas showing nontriviality of certain extensions of ray class fields.

6.1. Discussion of SIC fields.

Recall that for an r-SIC projector Π, the *SIC field* E_Π was defined in Definition 1.10 to be the field generated over $\mathbb{Q}$ by the overlaps $\mathrm{Tr}(\Pi D_{\mathbf{p}})$ and the $\bar{d}$-th root of unity ξ_d. This field is called the *extended projector SIC field* in [72, Defn. 3.1]; in that paper, it is compared to several other fields that can be associated to a SIC. The literature on SICs contains multiple definitions of fields associated to a SIC, many of which are conjecturally equal but not proven to be so; see [72, Sec. 3] for further discussion. In this paper, the *SIC field* is always E_Π as defined in Definition 1.10.

We also describe fields associated to an admissible tuple t or a fiducial datum s. Unlike the definition of the SIC field, the formal definition of these fields is in terms of (quantities defined from) special values of the Shintani–Faddeev modular cocycle, not in terms of a SIC.

For an admissible tuple t, an associated field E_t was defined in Definition 1.40. We expand that definition to give three fields associated to a fiducial datum s or an admissible tuple t.

Definition 6.1. Let $s = (d, r, Q, g, G) \sim (K, j, m, Q, g, G)$ be a fiducial datum, and let $t = (d, r, Q) \sim (K, j, m, Q)$ be the corresponding admissible tuple. Define the following fields.

(1) $E_s^{(1)}$ is the field generated over $\mathbb{Q}$ by the numbers $\{\mu_{\mathbf{p}}(t) \colon 0 \le p_1, p_2 < d,\ \mathbf{p} \neq \mathbf{0}\}$.
(2) $E_t^{(2)}$ is the field generated over $\mathbb{Q}$ by the numbers $\{\tilde{\mu}_{\mathbf{p}}(t) \colon 0 \le p_1, p_2 < d,\ \mathbf{p} \neq \mathbf{0}\}$.
(3) E_t is the field generated over $\mathbb{Q}$ by the numbers $\{\tilde{\mu}_{\mathbf{p}}(t) \colon 0 \le p_1, p_2 < d,\ \mathbf{p} \neq \mathbf{0}\}$ together with ξ_d.
(4) $\hat{E}_t$ is the Galois closure (within $\mathbb{C}$) of the compositum of K and E_t.

Recall that for $\mathbf{p} \not\equiv \mathbf{0} \pmod{d}$ we have by Lemma 1.45 the formula

$$\mu_{\mathbf{p}}(s) = g\Big(\tilde{\mu}_{GH_g^{-1}G^{-1}\mathbf{p}}(t)\Big) \tag{6.1}$$

relating the live and ghost overlaps, with $GH_g^{-1}G^{-1} \in \mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$. It follows that $E_s^{(1)} = g(E_t^{(2)})$.

We have defined three types of fields—SIC fields, fields associated to fiducial data, and ray class fields of orders (the latter in Section 2.1)—with no unconditional relationship between them. The remainder of this section concerns the strong conditional relationships and the strong empirical relationships between these three types of fields.

6.2. **Lemmas about class fields.** We now turn our attention to ray class fields of orders. For comparable level data $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}', \Sigma')$, with $\mathcal{O} \subseteq \mathcal{O}'$, $\mathfrak{m}\mathcal{O}' \subseteq \mathfrak{m}'$, and $\Sigma \supseteq \Sigma'$, there is a quotient map $\phi : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \twoheadrightarrow \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')$ and a corresponding field extension $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/H^{\mathcal{O}'}_{\mathfrak{m}',\Sigma'}$ with $\mathrm{Gal}(H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/H^{\mathcal{O}'}_{\mathfrak{m}',\Sigma'}) \cong \ker(\phi)$. In order to describe the structure of this kernel, we introduce the U-group notation from [71] for unit groups with congruence and "ray" restrictions.

Definition 6.2. For a commutative ring with unity R and an ideal I of R, define the group

$$\mathrm{U}_I(R) := \{\alpha \in R^\times : \alpha \equiv 1 \pmod{I}\} = (1 + I) \cap R^\times. \tag{6.2}$$

If R has real embeddings, and Σ is a subset of the real embeddings of R, define

$$\mathrm{U}_{I,\Sigma}(R) := \{\alpha \in R^\times : \alpha \equiv 1 \pmod{I} \text{ and } \rho(\alpha) > 0 \text{ for } \rho \in \Sigma\}. \tag{6.3}$$

The following exact sequence resolves the map $\phi : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \twoheadrightarrow \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')$, describing $\ker(\phi) \cong \mathrm{coker}(\lambda)$ for a reduction map λ from a certain global unit group to a certain $\pmod{\mathfrak{m}'}$ unit group.

Theorem 6.3. *Let K be a number field, and consider level data $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}', \Sigma')$ for K such that $\mathcal{O} \subseteq \mathcal{O}'$, $\mathfrak{m}\mathcal{O}' \subseteq \mathfrak{m}'$, and $\Sigma \supseteq \Sigma'$. Let $\mathfrak{d}$ be any $\mathcal{O}'$-ideal such that $\mathfrak{d} \subseteq (\mathfrak{m} : \mathcal{O}')$. We have the following exact sequence.*

$$1 \to \frac{\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} \xrightarrow{\lambda} \frac{\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d})}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})} \times \{\pm 1\}^{|\Sigma \setminus \Sigma'|} \xrightarrow{\psi} \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \xrightarrow{\phi} \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}') \to 1. \tag{6.4}$$

Proof. See [71, Thm. 6.5]. □

The exact sequence (6.4) gives us the most concrete description of $\mathrm{Gal}(H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/H^{\mathcal{O}'}_{\mathfrak{m}',\Sigma'})$ when the "global units" term $\frac{\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})}$ is the trivial group. More generally, we need to know something about the global units to use (6.4) effectively.

We now turn our attention to real quadratic fields and connect the U-groups to stability groups of 2×2 matrices by way of the canonical representations χ_Q from Section 4.

Lemma 6.4. *Fix a real quadratic field K of discriminant Δ_0, and consider any integers $d \geq 3$ and $f \geq 1$. Let Q be any primitive binary quadratic form of discriminant $f^2\Delta_0$, and consider the canonical ring homomorphism χ_Q defined by Definition 4.33. Then*

$$\chi_Q(d\mathcal{O}_f) = \chi_Q(\mathcal{O}_f) \cap d\mathcal{M}(\mathbb{Z}), \tag{6.5}$$

where, following Definition 4.27, $\mathcal{M}(\mathbb{Z})$ is the ring of 2×2 matrices with integer entries. Moreover, we have the following equalities of subgroups of $\mathrm{GL}_2(\mathbb{Z})$.

$$\chi_Q(\mathcal{O}_f^\times) = \mathcal{S}(Q). \tag{6.6}$$

$$\chi_Q(\mathrm{U}_{d\mathcal{O}_f,\emptyset}(\mathcal{O}_f)) = \mathcal{S}_d(Q). \tag{6.7}$$

Proof. We first prove (6.5). The inclusion $\chi_Q(\mathcal{O}_f) \subseteq \mathcal{M}(\mathbb{Z})$ holds by Theorem 4.35; thus, $\chi_Q(d\mathcal{O}_f) \subseteq \chi_Q(\mathcal{O}_f) \cap d\mathcal{M}(\mathbb{Z})$. To prove the reverse inclusion, suppose $M \in \chi_Q(\mathcal{O}_f) \cap d\mathcal{M}(\mathbb{Z})$, write $Q = \langle a, b, c\rangle$, and write

$$M = \chi_Q(x + y\sqrt{\Delta_0}) = xI + \frac{2y}{f}SQ = \begin{pmatrix} x - \frac{by}{f} & -\frac{2cy}{f} \\ \frac{2ay}{f} & x + \frac{by}{f} \end{pmatrix} \tag{6.8}$$

for $x, y \in \mathbb{Q}$. It follows that $\frac{2ay}{f} \in d\mathbb{Z}$, $\frac{2cy}{f} \in d\mathbb{Z}$, and $\frac{2by}{f} = (x + \frac{by}{f}) - (x - \frac{by}{f}) \in d\mathbb{Z}$. Because Q is primitive, $\gcd(a, b, c) = 1$, so $\frac{2y}{f} \in d\mathbb{Z}$; that is, $y \in \frac{df}{2}\mathbb{Z}$. We complete the proof of (6.5) by cases.

Case 1: Suppose $2 \,|\, f^2\Delta_0$. Then, since $b^2 - 4ac = f^2\Delta_0$, it follows that b is even. Thus, $\frac{by}{f} \in d\mathbb{Z}$. It follows from (6.8) that $x - \frac{by}{f} \in d\mathbb{Z}$, and thus, $x = (x - \frac{by}{f}) + b\frac{y}{f} \in d\mathbb{Z}$. In this case,

$$d\mathcal{O}_f = \left\{ x + y\sqrt{\Delta_0} : x \in d\mathbb{Z}, y \in \tfrac{df}{2}\mathbb{Z} \right\}, \tag{6.9}$$

and so $x + y\sqrt{\Delta_0} \in d\mathcal{O}_f$.

Case 2: Suppose $2 \nmid f^2\Delta_0$. Since $b^2 - 4ac = f^2\Delta_0$, it follows that b is odd; also, f is odd. It follows from (6.8) that $x - \frac{by}{f} \in d\mathbb{Z}$. Thus, $x = (x - \frac{by}{f}) + b\frac{y}{f} \in \frac{d}{2}\mathbb{Z}$, and $x - y = (x - \frac{by}{f}) + (f - b)\frac{y}{f} \in d\mathbb{Z}$. In this case,

$$d\mathcal{O}_f = \left\{ x + y\sqrt{\Delta_0} : x \in \tfrac{d}{2}\mathbb{Z}, y \in \tfrac{df}{2}\mathbb{Z}, x - y \in d\mathbb{Z} \right\}, \tag{6.10}$$

and so $x + y\sqrt{\Delta_0} \in d\mathcal{O}_f$.

Both case being proven, the proof of (6.5) is complete. Eq. (6.6) is a restatement of Theorem 4.45(2), which we have already proven. It remains to prove (6.7).

We first show that $\chi_Q(\mathrm{U}_{d\mathcal{O}_f,\emptyset}(\mathcal{O}_f))$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Consider any $\eta \in \mathrm{U}_{d\mathcal{O}_f,\emptyset}(\mathcal{O}_f)$. If η' is the nontrivial Galois conjugate of η, then $\eta \equiv 1 \pmod{d\mathcal{O}_1}$ and $\eta' \equiv 1 \pmod{d\mathcal{O}_1}$, so $\mathrm{Nm}(\eta) = \eta\eta' \equiv 1 \pmod{d\mathcal{O}_1}$. But $\mathrm{Nm}(\eta) = \pm 1$ because η is a unit, and $d \geq 3$, so $\mathrm{Nm}(\eta) = 1$. Thus, $\det(\chi_Q(\eta)) = \mathrm{Nm}(\eta) = 1$. So $\chi_Q(\mathrm{U}_{d\mathcal{O}_f,\emptyset}(\mathcal{O}_f))$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

We have $\mathrm{U}_{d\mathcal{O}_f,\emptyset}(\mathcal{O}_f) = \mathcal{O}_f^\times \cap (1 + d\mathcal{O}_f)$. Because χ_Q is an injective homomorphism, it follows that $\chi_Q(\mathrm{U}_{d\mathcal{O}_f,\emptyset}(\mathcal{O}_f)) = \chi_Q(\mathcal{O}_f^\times) \cap (I + \chi_Q(d\mathcal{O}_f))$. Thus, by (6.5) and (6.6), $\chi_Q(\mathrm{U}_{d\mathcal{O}_f,\emptyset}(\mathcal{O}_f)) = \mathcal{S}(Q) \cap d\mathcal{M}(\mathbb{Z})$. But since $\chi_Q(\mathrm{U}_{d\mathcal{O}_f,\emptyset}(\mathcal{O}_f))$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$, in fact $\chi_Q(\mathrm{U}_{d\mathcal{O}_f,\emptyset}(\mathcal{O}_f)) = \mathcal{S}(Q) \cap \Gamma(d) = \mathcal{S}_d(Q)$. □

The focus now narrows to the ray class fields of interest for the our construction of r-SICs. We will fix a real quadratic field K and associate to it the sequence of conductors f_j from Definition 1.23 and the dimension grid $d_{j,m}$ and rank grid $r_{j,m}$ from Definition 1.24.

The following lemma is the key technical result on global units that will allow us some control over the behavior of the ray class groups and ray class fields of interest for r-SICs. It generalizes [69, Lem. 5.3] and [72, Lem. B.2] by using Lemma 6.4 together with results proven in Section 4.

Lemma 6.5. *Fix a real quadratic field K of discriminant Δ_0. Let $j, m \in \mathbb{N}$. Let $d = d_{j,m}$ and $f \,|\, f_j$. Let Σ be a subset of the real embeddings of K. Then*

$$\mathrm{U}_{d\mathcal{O}_f,\Sigma}(\mathcal{O}_f) = \langle \varepsilon_{d_j}^{2m+1} \rangle. \tag{6.11}$$

Proof. Write $\varepsilon_{d_j} = \varepsilon^j$, where ε is the smallest totally positive unit of K with $\varepsilon > 1$. By (4.90) of Lemma 4.24,

$$\varepsilon_{d_j}^{2m+1} - 1 = \varepsilon^{(2m+1)j} - 1 = d_{j,m}\varepsilon^{mj}(\varepsilon^j - 1). \tag{6.12}$$

Also, $\varepsilon_{d_j} \in \mathcal{O}_{f_j}$. Thus, $\varepsilon_{d_j}^{2m+1} \equiv 1 \pmod{d_{j,m}\mathcal{O}_{f_j}}$, so

$$\varepsilon_{d_j}^{2m+1} \in \mathrm{U}_{d\mathcal{O}_f,\{\infty_1,\infty_2\}}(\mathcal{O}_f). \tag{6.13}$$

It follows that $\varepsilon_{d_j}^{2m+1} \in \mathrm{U}_{d\mathcal{O}_{f_j},\Sigma}(\mathcal{O}_{f_j})$, because $\mathrm{U}_{d\mathcal{O}_f,\{\infty_1,\infty_2\}}(\mathcal{O}_f) \subseteq \mathrm{U}_{d\mathcal{O}_{f_j},\Sigma}(\mathcal{O}_{f_j})$.

Since $\mathrm{U}_{d\mathcal{O}_{f_j},\Sigma}(\mathcal{O}_{f_j}) \subseteq \mathrm{U}_{d\mathcal{O}_1,\emptyset}(\mathcal{O}_1)$, It suffices to show that ε_{d_j} generates $\mathrm{U}_{d\mathcal{O}_1,\emptyset}(\mathcal{O}_1)$, which we will now do.

Let Q be any primitive binary quadratic form of discriminant Δ_0, and consider the canonical ring homomorphism χ_Q defined by Definition 4.33. By (6.7) of Lemma 6.4,

$$\chi_Q(\mathrm{U}_{d\mathcal{O}_1,\emptyset}(\mathcal{O}_1)) = \mathcal{S}_d(Q). \tag{6.14}$$

By (4.194) of Theorem 4.53,

$$\mathcal{S}_d(Q) = \langle A_t \rangle = \left\langle \chi_Q(\varepsilon_{d_j}^{2m+1}) \right\rangle = \chi_Q\left(\langle \varepsilon_{d_j}^{2m+1} \rangle \right). \tag{6.15}$$

It follows from (6.14) and (6.15), and the fact that χ_Q is an injective homomorphism, that $\mathrm{U}_{d\mathcal{O}_1,\emptyset}(\mathcal{O}_1) = \langle \varepsilon_{d_j}^{2m+1} \rangle$. □

As a consequence, we deduce the following lemma showing that varying the set of infinite primes in the ray class modulus produces distinct ray class groups and ray class fields.

Lemma 6.6. *Fix a real quadratic field K. Let $j, m \in \mathbb{N}$. Let $d = d_{j,m}$, $f \,|\, f_j$, and $d' \in \{d, \bar{d}\}$. The all the group homomorphism shown in the following diagram are 2-to-1 surjections.*

$$\begin{array}{ccccc} & & \mathrm{Cl}_{d'\infty_1\infty_2}(\mathcal{O}_f) & & \\ & \swarrow & & \searrow & \\ \mathrm{Cl}_{d'\infty_1}(\mathcal{O}_f) & & & & \mathrm{Cl}_{d'\infty_2}(\mathcal{O}_f) \\ & \searrow & & \swarrow & \\ & & \mathrm{Cl}_{d'}(\mathcal{O}_f) & & \end{array} \tag{6.16}$$

In the following field diagram, all of the extensions have degree 2.

$$\begin{array}{ccccc} & & H_{d'\infty_1,\infty_2}^{\mathcal{O}_f} & & \\ & \swarrow & & \searrow & \\ H_{d'\infty_1}^{\mathcal{O}_f} & & & & H_{d'\infty_2}^{\mathcal{O}_f} \\ & \searrow & & \swarrow & \\ & & H_{d'\mathcal{O}}^{\mathcal{O}_f} & & \end{array} \tag{6.17}$$

Proof. We first prove the claim in the case $d' = d$. Let $\mathcal{O} = \mathcal{O}_f$. Let Σ', Σ be subsets of the set of real embeddings of K. We apply the exact sequence of [71, Thm. 6.5] with level data $\mathcal{L} = (\mathcal{O}; d'\mathcal{O}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}; d'\mathcal{O}, \emptyset)$ and with $\mathfrak{d} = d\mathcal{O}$:

$$1 \to \frac{\mathrm{U}_{d\mathcal{O},\Sigma'}(\mathcal{O})}{\mathrm{U}_{d\mathcal{O},\Sigma}(\mathcal{O})} \to \frac{\mathrm{U}_{d\mathcal{O}}(\mathcal{O}/d\mathcal{O})}{\mathrm{U}_{d\mathcal{O}}(\mathcal{O}/d\mathcal{O})} \times \{\pm 1\}^{|\Sigma \setminus \Sigma'|} \to \mathrm{Cl}_{d\mathcal{O},\Sigma}(\mathcal{O}) \to \mathrm{Cl}_{d\mathcal{O},\Sigma'}(\mathcal{O}) \to 1. \tag{6.18}$$

By Lemma 6.5, the "global units" term is

$$\frac{\mathrm{U}_{d\mathcal{O},\Sigma'}(\mathcal{O})}{\mathrm{U}_{d\mathcal{O},\Sigma}(\mathcal{O})} = \frac{\langle \varepsilon_{d_j}^{2m+1} \rangle}{\langle \varepsilon_{d_j}^{2m+1} \rangle} = 1. \tag{6.19}$$

We may thus rewrite Equation (6.18) as the short exact sequence

$$1 \to \{\pm 1\}^{|\Sigma \setminus \Sigma'|} \to \mathrm{Cl}_{d\mathcal{O},\Sigma}(\mathcal{O}) \to \mathrm{Cl}_{d\mathcal{O},\Sigma'}(\mathcal{O}) \to 1. \tag{6.20}$$

It follows that the ray class groups $\mathrm{Cl}_d(\mathcal{O}) = \mathrm{Cl}_{d\mathcal{O},\emptyset}(\mathcal{O})$, $\mathrm{Cl}_{d\infty_1}(\mathcal{O}) = \mathrm{Cl}_{d\mathcal{O},\{\infty_1\}}(\mathcal{O})$, $\mathrm{Cl}_{d\infty_2}(\mathcal{O}) = \mathrm{Cl}_{d\mathcal{O},\{\infty_2\}}(\mathcal{O})$, $\mathrm{Cl}_{d\infty_1\infty_2}(\mathcal{O}) = \mathrm{Cl}_{d\mathcal{O},\{\infty_1,\infty_2\}}(\mathcal{O})$ are all distinct and have the 2-to-1 surjections shown in (6.16). The fact that the field extensions in the ray class field diamond (6.17) have degree 2 follows by Theorem 2.2.

In the case $d' = \bar{d}$, note that since $\mathrm{U}_{d\mathcal{O},\Sigma'}(\mathcal{O}) = \mathrm{U}_{d\mathcal{O},\Sigma}(\mathcal{O})$, it follows that $\mathrm{U}_{\bar{d}\mathcal{O},\Sigma'}(\mathcal{O}) = \mathrm{U}_{\bar{d}\mathcal{O},\Sigma}(\mathcal{O})$, because the latter two groups are subgroups of the former obtained by imposing the condition $u \equiv 1 \pmod{\bar{d}}$. Therefore, the same proof applies. □

6.3. **SIC fields as class fields.** Theorem 1.49 is a straightforward consequence of our conjectures about the RM values of the Shintani–Faddeev cocycle.

Proof of Theorem 1.49. Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple. We wish to show that E_t is an abelian extension of K.

The field E_t is defined to be the field generated over $\mathbb{Q}$ by the candidate ghost overlaps $\tilde{\mu}_{\mathbf{p}}(t)$ together with ξ_d. The candidate ghost overlaps are $\tilde{\mu}_{\mathbf{0}}(t) = 1$ and

$$\tilde{\mu}_{\mathbf{p}}(t) = \frac{1}{\sqrt{d_j + 1}} \tilde{\nu}_{\mathbf{p}}(t) = \frac{1}{\sqrt{d_j + 1}} \phi_{\mathbf{p}}(t) \mathfrak{w}_A^{d^{-1}\mathbf{p}}(\rho_t) \text{ for } \mathbf{p} \not\equiv \mathbf{0} \pmod{d}. \tag{6.21}$$

Note that $\sqrt{d_j + 1}$ and $\phi_{\mathbf{p}}(t)$ (a root of unity) are both contained in abelian extensions of $\mathbb{Q}$, so in particular they are both are contained in an abelian extension of K. By the conditional assumption (of Conjecture 1.37 when Q is fundamental and Conjecture 1.38 when Q is not fundamental), $\mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho_t)$ is also in an abelian extension of K. We have

$$E_t \subseteq K\left(\sqrt{d_j + 1}, \xi_d, \phi_{\mathbf{p}}(t), \mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho_t) : 0 \le p_1, p_2 < d\right), \tag{6.22}$$

and the right-hand field is abelian over K, so E_t is abelian over K. □

We prove the following theorem, which implies Theorem 1.50.

Theorem 6.7. *Assume Conjecture 2.8 (the Stark–Tate Conjecture). Let $s = (d, r, Q, G, g) \sim (K, j, m, Q, G, g)$ be a fiducial datum, let $t = (d, r, Q) \sim (K, j, m, Q)$, and let $d = d_{j,m}$. Suppose that $\mathrm{disc}(Q)$ is fundamental. Choose $\mathbf{p}_1 = \left(\begin{smallmatrix} p_{11} \\ p_{12} \end{smallmatrix}\right)$ such that $(p_{12}\rho_t - p_{11})\mathcal{O}_1$ is coprime to $d\mathcal{O}_1$ as $\mathcal{O}_1$-ideals. (For example, one may take $\mathbf{p}_1 = \left(\begin{smallmatrix} -1 \\ 0 \end{smallmatrix}\right)$.)*

(1) The ray class field $H_{d\infty_1}^{\mathcal{O}_1}$ is equal to the field extension of K generated by the numbers $\{\mu_{\mathbf{p}}(t) : 0 \le p_1, p_2 < d, \mathbf{p} \neq \mathbf{0}\}$ and is also equal to $\mathbb{Q}(\mu_{\mathbf{p}_1}(t)^2)$. The field $E_s^{(1)} \supseteq H_{d\infty_1}^{\mathcal{O}_1} \supseteq K$, the extension $E_s^{(1)}/K$ is ramified at ∞_1 and unramified ∞_2, and field $E_s^{(1)}$ depends only on the pair (d, r).

(2) The ray class field $H_{d\infty_2}^{\mathcal{O}_1}$ is equal to the field extension of K generated by the numbers $\{\tilde{\mu}_{\mathbf{p}}(t)^2 : 0 \le p_1, p_2 < d, \mathbf{p} \neq \mathbf{0}\}$ and is also equal to $\mathbb{Q}(\tilde{\mu}_{\mathbf{p}_1}(t)^2)$. The field $E_t^{(2)} \supseteq H_{d\infty_2}^{\mathcal{O}_1} \supseteq K$, the extension $E_t^{(2)}/K$ is unramified at ∞_1 and ramified ∞_2, and field $E_t^{(2)}$ depends only on the pair (d, r).

(3) *The ray class field* $H^{\mathcal{O}_1}_{\bar{d}\infty_1\infty_2}$ *is equal to the field extension of* K *generated by the numbers* $\{\tilde{\mu}_{\mathbf{p}}(t)^2 \colon 0 \leq p_1, p_2 < d,\ \mathbf{p} \neq \mathbf{0}\}$ *together with* ξ_d*, and it is also equal to* $K(\tilde{\mu}_{\mathbf{p_1}}(t)^2, \xi_d)$*. The field* $E_t \supseteq H^{\mathcal{O}_1}_{\bar{d}\infty_1\infty_2} \supseteq K$*, the extension* E_t/K *is ramified at both infinite places of* K*, and field* E_t *depends only on the pair* (d, r)*.*

(4) *Assume Conjecture 1.35. Then the SIC field* $E_{\Pi_s} = E^{(1)}_s(\xi_d) \supseteq H^{\mathcal{O}_1}_{\bar{d}\infty_1\infty_2} \supseteq K$*.*

Proof. We will prove (2) first, and the others will follow.

Consider $\mathbf{p} \in (\mathbb{Z}/d\mathbb{Z})^2$. As in the proof of Theorem 5.8, let $\mathfrak{A}_{\mathbf{p}}$ be the unique class in $\overline{\mathrm{Clm}}^{\flat}_{d\infty_2}(\mathcal{O}_1)$ that maps to the $\mathrm{SL}_2(\mathbb{Z})$-orbit of $(d^{-1}\mathbf{p}, \rho_t)$ under the map $\Upsilon_{d\mathcal{O}_1}$ described in [70, Thm. 3.12] and at the end of Section 2.6. By Equation (5.73), we have for

$$(d_j + 1)\,(\tilde{\mu}_{\mathbf{p}}(t))^2 = (\tilde{\nu}_{\mathbf{p}}(t))^2 = \exp\bigl(nZ'_{d\infty_2}(0, \mathfrak{A}_{\mathbf{p}})\bigr) = u^{-n_{\mathbf{p}}}_{\mathfrak{A}_{\mathbf{p}}} \tag{6.23}$$

for some $n_{\mathbf{p}} \in \{1, 2\}$ and $u_{\mathfrak{A}_{\mathbf{p}}} = \exp\bigl(-Z'_{d\infty_2}(0, \mathfrak{A}_{\mathbf{p}})\bigr)$. By Proposition 2.10, our conditional assumptions imply $\mathrm{MS}(\mathcal{O}_1, \mathfrak{m})$ (Conjecture 2.9) for all nonzero $\mathcal{O}_1$-ideals $\mathfrak{m}$ such that $\mathfrak{m} \neq \mathcal{O}_1$. In particular, they imply that $u_{\mathfrak{A}_{\mathbf{p}}} \in H^{\mathcal{O}_1}_{d\infty_2}$. It follows that $(\tilde{\nu}_{\mathbf{p}}(t))^2 \in H^{\mathcal{O}_1}_{d\infty_2}$, or equivalently $(\tilde{\mu}_{\mathbf{p}}(t))^2 \in H^{\mathcal{O}_1}_{d\infty_2}$.

Now restrict to the special case of $\mathbf{p} = \mathbf{p}_1 := \left(\begin{smallmatrix}-1\\0\end{smallmatrix}\right)$. Let $u := u_{\mathfrak{A}_{\mathbf{p}_1}}$. By definition, $n_{\mathbf{p}_1} = \frac{2}{|\phi^{-1}(\mathfrak{A}_{\mathbf{p}_1})|}$, where $\phi : \overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m}\infty_1\infty_2}(\mathcal{O}_1) \to \overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m}\infty_2}(\mathcal{O}_1)$ is the natural quotient map. The class $\mathfrak{A}_{\mathbf{p}_1}$ is primitive, so $|\phi^{-1}(\mathfrak{A}_{\mathbf{p}_1})|$ is equal to the cardinality of the kernel of the map $\mathrm{Cl}_{\mathfrak{m}\infty_1\infty_2}(\mathcal{O}_1) \to \mathrm{Cl}_{\mathfrak{m}\infty_2}(\mathcal{O}_1)$, which by Lemma 6.6 is 2. Thus $n_{\mathbf{p}_1} = \frac{2}{2} = 1$, and (6.23) becomes $(\tilde{\nu}_{\mathbf{p}_1}(t))^2 = \varepsilon^{-1}$. Because $f = 1$ and $\mathfrak{A}_{\mathbf{p}_1}$ is primitive, the number ε is a Stark unit in the original sense of [99]. The nontriviality of the maps between the ray class groups with different ramification at infinite places shown in Lemma 6.6 implies the non-vanishing condition in the hypotheses of [99, Thm. 1]. Applying that theorem, which says that the Stark unit generates the ray class field over the rational numbers, we obtain $\mathbb{Q}((\tilde{\nu}_{\mathbf{p}_1}(t))^2) = \mathbb{Q}(\varepsilon) = H^{\mathcal{O}_1}_{d\infty_2}$.

The claim that $E^{(2)}_t \supseteq H^{\mathcal{O}_1}_{d\infty_2}$ follows by the definition of $E^{(2)}_t$. The field $H^{\mathcal{O}_1}_{d\infty_2}$ is always unramified at ∞_1, and it is ramified at ∞_2 if and only if it is a nontrivial extension of $H^{\mathcal{O}_1}_d$, which is true by Lemma 6.6. The field $E^{(2)}_t$ is obtained from $H^{\mathcal{O}_1}_{d\infty_2}$ by adjoining square roots of numbers $(\tilde{\nu}_{\mathbf{p}}(t))^2$ that are positive in the first real embedding, so it remains unramified at ∞_1. It also follows from the "Artin map action" part of Conjecture 2.9, together with (6.23), that $\mathrm{Gal}(H^{\mathcal{O}_1}_{d\infty_2}/K)$ permutes the $(\tilde{\mu}_{\mathbf{p}}(t))^2$ with the ghost overlaps $(\tilde{\mu}_{\mathbf{p}}(t'))^2$ of all $t' = (d, r, Q')$ such that $\mathrm{disc}(Q')$ is fundamental. Thus $E^{(2)}_t$ depends only on the pair (d, r).

Claim (1) follows from (2), because $H^{\mathcal{O}_1}_{d\infty_1} = g(H^{\mathcal{O}_1}_{d\infty_2})$ and $E^{(1)}_s = g(E^{(2)}_t)$, and using Lemma 1.45; independence from g follows from the fact (given by Theorem 1.49) that $E^{(2)}_t/K$ is abelian, so $E^{(2)}_t$ can have no more that two conjugate fields over $\mathbb{Q}$, those being $E^{(1)}_s$ and $E^{(2))}_t$. Claim (3) also follows, because $H^{\mathcal{O}_1}_{\bar{d}\infty_1\infty_2} = H^{\mathcal{O}_1}_{d\infty_1}(\xi_d) = H^{\mathcal{O}_1}_{d\infty_2}(\xi_d)$ and $E_t = E^{(2)}_t(\xi_d)$.

Additionally, if one assumes Conjecture 1.35, then Π_s is a SIC fiducial projector by Theorem 1.47, so E_{Π_s} is well-defined. Then it follows from the definition of each that $E_{\Pi_s} = E^{(1)}_s(\xi_d)$, and so claim (4) follows from (1). □

Proof of Theorem 1.50. This is Theorem 6.7(3). □

Theorem 6.7 does not pin down the fields $E^{(1)}_s$, $E^{(2)}_t$, and E_t precisely but only says that they are abelian extensions containing certain ray class fields. This is because the Stark–Tate Conjecture

does not provide a precise description of the field generated by the square root of a Stark unit as a particular subfield of a ray class field. Theorem 6.7 also applies only in the case of fundamental discriminants, because the theory of ray class partial zeta functions for non-maximal orders is insufficiently developed at present to provide the analogue of [99, Thm. 1].

Nevertheless, the numerical data (discussed further in Sections 7 and 8 as well as in [72]) supports a precise prediction about the structure of the fields $E_s^{(1)}$, $E_t^{(2)}$, and E_t; this prediction includes the forms of non-fundamental discriminant. We presented the prediction as a conjecture. We note that this conjecture implies Conjecture 1.51 and also predicts the shape of the fields $\hat{E}_t$ and E_{Π_s}.

Conjecture 6.8. *Let $s = (d, r, Q, G, g) \sim (K, j, m, Q, G, g)$ be a fiducial datum, let $t = (d, r, Q) \sim (K, j, m, Q)$, let $d = d_{j,m}$, and let f be the conductor of Q. Then:*

(1) $E_s^{(1)} = H_{\bar{d}\infty_1}^{\mathcal{O}_f}$.

(2) $E_t^{(2)} = H_{\bar{d}\infty_2}^{\mathcal{O}_f}$.

(3) $E_t = H_{\bar{d}\infty_1\infty_2}^{\mathcal{O}_f}$.

Proposition 6.9. *Let $s = (d, r, Q, G, g) \sim (K, j, m, Q, G, g)$ be a fiducial datum, and let $t = (d, r, Q) \sim (K, j, m, Q)$.*

(1) Assuming Conjecture 6.8, one has $\hat{E}_t = E_t$, and Conjecture 1.51 follows.

(2) Assuming Conjecture 6.8 and Conjecture 1.35, one has $E_{\Pi_s} = E_t$.

Proof. The field $H_{\bar{d}\infty_1\infty_2}^{\mathcal{O}_f}$ contains K and is Galois over $\mathbb{Q}$; thus, by Conjecture 6.8, $\hat{E}_t = E_t$. It is then clear that Conjecture 1.51 follows by Conjecture 6.8(3). Additionally, if one assumes Conjecture 1.35, then Π_s is a SIC fiducial projector by Theorem 1.47, so E_{Π_s} is well-defined. Then it follows from the definition of each that $E_{\Pi_s} = E_s^{(1)}(\xi_d)$, and so by Conjecture 6.8, the SIC field $E_{\Pi_s} = H_{\bar{d}\infty_1}^{\mathcal{O}_f}(\xi_d) = H_{\bar{d}\infty_1\infty_2}^{\mathcal{O}_f} = E_t$. □

6.4. **The set of SIC-generated abelian extensions.** We now examine the implications of our conjectural framework for the generation of arbitrary abelian extensions of real quadratic fields. We begin with two preliminary results.

Definition 6.10. For any prime number p and any $r \in \mathbb{Q}^\times$, denote by $v_p(r)$ the *p-adic valuation* of r; that is, if $r = p^e \frac{a}{b}$ with $p \nmid a$ and $p \nmid b$, then $v_p(r) = e$.

Lemma 6.11. *Let $p, r, e \in \mathbb{N}$ be such that p is prime and $1 \leq r \leq p^e$. Then the following statements of about the p-adic valuations of binomial coefficients hold:*

$$v_p\left(\binom{p^e}{r}\right) = e - v_p(r), \tag{6.24}$$

$$v_p\left(p^r \binom{p^e}{r}\right) \geq e + 1. \tag{6.25}$$

Proof. We prove (6.24) by induction. The statement is immediate if $r = 1$. Suppose it is true for arbitrary $1 \leq r < p^e$. Then

$$v_p\left(\binom{p^e}{r+1}\right) = v_p\left(\frac{p^e - r}{r+1}\binom{p^e}{r}\right) = e - v_p(r) + v_p(p^e - r) - v_p(r+1). \tag{6.26}$$

Since $v_p(p^e - r) = v_p(r)$, it follows that

$$v_p\left(\binom{p^e}{r+1}\right) = e - v_p(r+1). \tag{6.27}$$

Eq. (6.25) follows from (6.24) and the fact that $r - v_p(r) \geq 1$. □

Lemma 6.12. *Let ε be the totally positive fundamental unit of the quadratic field K and $d_1 = \frac{\varepsilon+\varepsilon^{-1}}{2} + 1$ the associated root dimension. The order of $\varepsilon + 2\mathcal{O}_K$ as an element of $(\mathcal{O}_K/2\mathcal{O}_K)^\times$ is*

$$\#\langle \varepsilon + 2\mathcal{O}_K \rangle = \begin{cases} 1, & \text{if } d_1 \equiv 3 \pmod 4, \\ 2, & \text{if } d_1 \equiv 1 \pmod 4, \\ 3, & \text{if } d_1 \text{ is even}. \end{cases} \tag{6.28}$$

Proof. Suppose $d_1 = 4n + 3$ for $n \in \mathbb{N}$. Then

$$\varepsilon + 2\mathcal{O}_K = \frac{4n + 2 + 4\sqrt{n(n+1)}}{2} + 2\mathcal{O}_K = 1 + 2\mathcal{O}_K. \tag{6.29}$$

Suppose $d_1 = 4n + 1$ for $n \in \mathbb{N}$. Then

$$\begin{aligned} \varepsilon + 2\mathcal{O}_K &= \frac{4n + \sqrt{(4n-2)(4n+2)}}{2} + 2\mathcal{O}_K \\ &= \sqrt{4n^2 - 1} + 2\mathcal{O}_K \\ \implies \qquad \varepsilon^2 + 2\mathcal{O}_K &= 4n^2 - 1 + 2\mathcal{O}_K \\ &= 1 + 2\mathcal{O}_K. \end{aligned} \tag{6.30}$$

Finally, suppose d_1 is even. Then

$$\varepsilon^j - 1 = \frac{d_j - 3 - f_j\Delta_0}{2} + f_j\left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2}\right). \tag{6.31}$$

So $\varepsilon^j \equiv 1 \pmod{2\mathcal{O}_K}$ if and only if $(d_j - 3 - f_j\Delta_0)/2$ and f_j are both even. It follows from Lemma 4.11 that f_1, f_2 are both odd, implying that the order is greater than 2. It also follows that f_3 is even and $\Delta_0 \equiv 1 \pmod 4$. Using Lemma 4.10 we have

$$d_3 - 3 - f_3\Delta_0 = d_1^2(d_1 - 3) + f_1 d_1(d_1 - 2)\Delta_0 \equiv 0 \pmod 4. \tag{6.32}$$

Hence $\varepsilon^3 \in 1 + 2\mathcal{O}_K$. □

Theorem 6.13. *Let d be any positive integer, and let r be the order of $\varepsilon + d\mathcal{O}_K$ as an element of $(\mathcal{O}_K/d\mathcal{O}_K)^\times$, where ε is the totally positive fundamental unit of the quadratic field K. Write d, r in the form*

$$d = 2^{\ell_1}(2a + 1), \qquad\qquad r = 2^{\ell_2}(2b + 1), \tag{6.33}$$

for suitable non-negative integers ℓ_1, ℓ_2, a, b. Let $\ell = \max\{\ell_1, \ell_2\}$, and let $j, m \in \mathbb{N}$ be such that

$$2^\ell \,|\, j, \qquad\qquad (2a + 1)(2b + 1) \,|\, (2m + 1). \tag{6.34}$$

If d is even assume in addition that j is coprime to 3 and $2m + 1$ is a multiple of 3. Then

(1) If d_1 is even, then $d \,|\, d_{j,m}$,
(2) If d_1 is odd, then $d \,|\, d_{j,m}$ if and only if d is odd.

Proof. Let p^e be any element in the prime decomposition of $2a + 1$. Since $j(2b + 1) \,|\, r$

$$\varepsilon^{j(2b+1)} = 1 + dz \tag{6.35}$$

for some $z \in \mathcal{O}_K$. It then follows from Lemma 6.11 that

$$\varepsilon^{jp^e(2b+1)} = 1 + \sum_{t=1}^{p^e} (dz)^t \binom{p^e}{t} = 1 + p^e dzz' = 1 + p^e(\varepsilon^{j(2b+1)} - 1)z' \tag{6.36}$$

for some $z' \in \mathcal{O}_K$. In view of Lemma 4.24 this means

$$\varepsilon^{jp^e(2b+1)} = 1 + p^e d_{b,j}\varepsilon^{bj}(\varepsilon^j - 1)z' = 1 + p^e(\varepsilon^j - 1)z'' \tag{6.37}$$

for some $z'' \in \mathcal{O}_K$. Since $p^e(2b+1) \,|\, (2m+1)$ it follows that

$$\varepsilon^{j(2m+1)} = 1 + p^e(\varepsilon^j - 1)z''' \tag{6.38}$$

for some $z''' \in \mathcal{O}_K$. By another application of Lemma 4.24 we deduce

$$\begin{aligned} & d_{j,m}\varepsilon^{mj}(\varepsilon^j - 1) = p^e(\varepsilon^j - 1)z''' \\ \implies \qquad & d_{j,m} = p^e w \end{aligned} \tag{6.39}$$

for some $w \in \mathcal{O}_K$. We conclude that p^e, and consequently $(2a+1)$ divides $d_{j,m}$. If d is odd this proves $d \,|\, d_{j,m}$.

Suppose, on the other hand, that d is even. Suppose, first, that d_1 is also even. By assumption $3 \,|\, (2m+1)$, so it follows from Lemma 6.12 that

$$\varepsilon^{2m+1} = 1 + 2z \tag{6.40}$$

for some $z \in \mathcal{O}_K$. In view of Lemma 6.11 this means

$$\varepsilon^{(2m+1)2^\ell} = 1 + \sum_{t=1}^{2^\ell} (2z)^t \binom{2^\ell}{t} = 1 + 2^{\ell+1} zz' = 1 + 2^\ell(\varepsilon^{2m+1} - 1)z' \tag{6.41}$$

for some $z' \in \mathcal{O}_K$. Since $2^\ell \,|\, j$ it follows that

$$\varepsilon^{(2m+1)j} = 1 + 2^\ell(\varepsilon^{2m+1} - 1)z'' \tag{6.42}$$

for some $z'' \in \mathcal{O}_K$. Using Lemma 4.24 we deduce

$$\begin{aligned} & d_{j,m}\varepsilon^{mj}(\varepsilon^j - 1) = 2^\ell d_{1,m}\varepsilon^m(\varepsilon - 1)z'' \\ \implies \qquad & d_{j,m}(\varepsilon^j - 1) = 2^\ell w \end{aligned} \tag{6.43}$$

for some $w \in \mathcal{O}_K$. Since j is coprime to 3,

$$\varepsilon^j - 1 = c_1 + c_2\left(\frac{\Delta_0 + \sqrt{\Delta_0}}{2}\right) \tag{6.44}$$

for $c_1, c_2 \in \mathbb{Z}$ not both even. Since 2^ℓ divides both $c_1 d_{j,m}$ and $c_2 d_{j,m}$ it follows that it must divide $d_{j,m}$, which proves statement (1).

Suppose, on the other hand, that d_1 is odd. Then it follows from Lemmas 4.11 and 4.24 that $d_{j,m}$ is odd. So $d \nmid d_{j,m}$, which proves statement (2). □

Theorem 6.14. *Let K be a real quadratic field of discriminant Δ_0, let ε be a fundamental totally positive unit in K (as in Definition 1.22), and let f_j be as defined in Definition 1.23. Then*

(1) If $\mathrm{Tr}(\varepsilon)$ is odd, then every abelian extension of K is contained in $H^{\mathcal{O}_1}_{d_{j,m}\infty_1\infty_2}$ for some $j, m \in \mathbb{N}$.

(2) If $\mathrm{Tr}(\varepsilon)$ is even, d is a positive odd integer, and $f \,|\, f_{j_0}$ for some positive integer j_0 such that $3 \nmid j_0$, then there exists some $j, m \in \mathbb{N}$ such that $H^{\mathcal{O}_f}_{d\infty_1\infty_2} \subseteq H^{\mathcal{O}_f}_{d_{j,m}\infty_1\infty_2}$.

(2') *If* $\mathrm{Tr}(\varepsilon)$ *is even, then every abelian extension of* K *that is unramified at the primes of* K *lying over* 2 *is contained in* $H^{\mathcal{O}_1}_{d_{j,m}\infty_1\infty_2}$ *for some* $j, m \in \mathbb{N}$.

Proof. We prove (1) first. If $\mathrm{Tr}(\varepsilon)$ is odd, then the root dimension d_1 is even. Let E be any abelian extension of K. By the Takagi Existence Theorem, there is some $d \in \mathbb{N}$ such that $E \subseteq H^{\mathcal{O}_1}_{d\infty_1\infty_2}$. It follows from Theorem 6.13(1) that there are some $j, m \in \mathbb{N}$ such that $d \,|\, d_{j,m}$. Thus, $E \subseteq H^{\mathcal{O}_1}_{d_{j,m}\infty_1\infty_2}$.

Now we prove (2). If $\mathrm{Tr}(\varepsilon)$ is even, then the root dimension d_1 is odd. Let $r, \ell_1, \ell_2, \ell, a, b \in \mathbb{N}$ be as in the statement of Theorem 6.13. Set $j := 2^\ell j_0$ and $2m + 1 := (2a + 1)(2b + 1)$. Then by Theorem 6.13(2) we have $d \,|\, d_{j,m}$. Thus, $H^{\mathcal{O}_f}_{d\infty_1\infty_2} \subseteq H^{\mathcal{O}_f}_{d_{j,m}\infty_1\infty_2}$.

Finally, we prove (2'). Let E be any abelian extension of K that is unramified at the primes of K lying over 2. By the Takagi Existence Theorem, there is some odd $d \in \mathbb{N}$ such that $E \subseteq H^{\mathcal{O}_1}_{d\infty_1\infty_2}$. Choosing $f = 1$ in (2), the condition $f \,|\, f_{j_0}$ holds for any choice of j_0, so we obtain $E \subseteq H^{\mathcal{O}_1}_{d\infty_1\infty_2} \subseteq H^{\mathcal{O}_1}_{d_{j,m}\infty_1\infty_2}$ for some $j, m \in \mathbb{N}$. □

Proof of Theorem 1.52. By Theorem 1.50, our conditional assumptions imply that, for any admissible tuple $t = (d, r, Q) \sim (K, j, m, Q)$, one has the field containments

$$E_t \supseteq H^{\mathcal{O}_1}_{\bar{d}_{j,m}\infty_1\infty_2} \supseteq H^{\mathcal{O}_1}_{d_{j,m}\infty_1\infty_2}. \tag{6.45}$$

Theorem 1.52 thus follows from Theorem 6.14. □

For real quadratic fields K satisfying the hypothesis of Theorem 6.14(1), namely that $\mathrm{Tr}(\varepsilon)$ is odd, r-SICs have the potential to provide a full solution to Hilbert's twelfth problem. The fields $H^{\mathcal{O}_1}_{d_{j,m}\infty_1\infty_2}$ contain every abelian extension of K. By Theorem 6.7(4), these fields "SIC-generated" in the sense that they are contained in the SIC field E_{Π_s} of a SIC fiducial Π_s, under the assumptions of Conjecture 2.8 and Conjecture 1.35. Proofs of Conjecture 2.8 and Conjecture 1.35 could thus be considered a geometric, complex-analytic solution to Hilbert's twelfth problem for real quadratic fields with a unit of odd trace.

We provide a result of the natural density of such fields in the family of all real quadratic fields ordered by discriminant.

Theorem 6.15. *When ordered by discriminant, at least 7.4% and at most 33.4% of real quadratic fields* K *have a fundamental unit* ε_K *of odd trace (or equivalently, have a totally positive fundamental unit of odd trace, or have any unit of odd trace). Specifically, as* $X \to \infty$*, there is an asymptotic inequality*

$$\frac{2}{27} + o(1) \leq \frac{\#\{K : [K:\mathbb{Q}] = 2, 0 < \Delta_K < X, 2 \nmid \mathrm{Tr}(\varepsilon_K)\}}{\#\{K : [K:\mathbb{Q}] = 2, 0 < \Delta_K < X\}} \leq \frac{1}{3} + O(X^{-1/2}), \tag{6.46}$$

where $\Delta_K := \mathrm{disc}\, K$.

Proof. See Appendix E. □

7. SIC PHENOMENOLOGY

The purpose of this section is to show how the conjectures and results presented in previous sections explain many of the features of the calculated SIC fiducials that were described in Section 3.3.

We begin, in Section 7.1, by showing how the action of $\mathrm{GL}_2(\mathbb{Z})$ on quadratic forms translates into an action of $\mathrm{EC}_0(d)$ on the corresponding fiducials.

In Section 7.2 we discuss the classification of r-SIC fiducials. We restrict our attention to what we refer to as *standard fiducials*, by which we mean fiducials corresponding to fiducial data sets (d, r, Q, G, g) for which $\det(G) = \pm 1$. We show that if Conjectures 1.35, 1.36, and 1.51 are all true, then one gets the complete set of standard fiducials if one restricts to data sets having some fixed, but arbitrary choice of G and g. Given two such data sets (d, r, Q, G, g), (d, r, Q', G, g) we show that the corresponding fiducials are

(1) on the same $\mathrm{EC}(d)$ orbit if Q and Q' are equivalent,
(2) on the same Galois multiplelt if Q and Q' have the same discriminant.

In Section 7.3 we describe some illustrative examples. We also describe how, on the assumption that Conjectures 1.35, 1.36, and 1.51 are all true, the number of $\mathrm{EC}(d)$ orbits, and the number of Galois multiplets of standard 1-SIC fiducials varies with dimension d. Finally, we describe how the number of standard r-SICs with $r > 1$ varies with dimension.

In Section 7.4 we investigate the symmetry group for an r-SIC fiducial. We show that if Π_s is the fiducial corresponding to the datum $s = (d, r, Q, G, g)$, then $\mathcal{S}(Q)$, the stabilizer group for Q (see Definition 1.20), gives rise to a cyclic subgroup of $\mathcal{S}_{\mathrm{ESL}}(\Pi_s)$. In every case where it has been checked one finds in fact that the cyclic group corresponding to $\mathcal{S}(Q)$ coincides with $\mathcal{S}_{\mathrm{ESL}}(\Pi_s)$. If that is generally true then, given a fiducial data set $s = (d, r, Q, G, g)$,

(1) we have a criterion for when the symmetry group $\mathcal{S}(\Pi_s)$ has an anti-unitary symmetry,
(2) an expression for the order of $\mathcal{S}(\Pi_s)$.

In the rank-1 case we can also

(1) explain why every fiducial has a canonical order 3 symmetry (see Definition 3.11),
(2) explain why one only gets type z $\mathrm{EC}(d)$ orbits when $d \not\equiv 3 \pmod 9$ (see Definition 3.15),
(3) explain why one gets both type z and type a orbits when $d \equiv 3 \pmod 9$,
(4) give a criterion for identifying the type a orbits when $d \equiv 3 \pmod 9$.

Finally, in Section 7.5 we consider the phenomenon of SIC alignment. As discussed in Section 3.3.4, it is observed in the empirically calculated solutions [3, 8] that, up to a sign, the squares of the normalized overlaps for a 1-SIC at position d_j in a dimension tower reappear among the normalized overlaps at position d_{2j}. We show that this phenomenon is a consequence of our results. We also show that the phenomenon generalizes to a relation between the normalized overlaps for a 1-SIC at positions d_j and d_{nj} in a tower, for any positive integer n coprime to 3.

7.1. **Transformations of forms and fiducials.** Consider the map $s \mapsto \Pi_s$, where s is a fiducial datum and Π_s is an r-SIC fiducial. We have

(1) a natural action of $\mathrm{GL}_2(\mathbb{Z})$ on the domain of this map, in which $M \in \mathrm{GL}_2(\mathbb{Z})$ takes $s = (d, r, Q, G, g)$ to $s_M = (d, r, Q_M, G, g)$,
(2) a natural action of $\mathrm{EC}_0(d)$ on the range of the map, in which $U \in \mathrm{EC}_0(d)$ takes Π_s to $U\Pi_s U^\dagger$.

The purpose of this subsection is to show how these two actions are related. Its importance, among other things, is that it leads to the classification of r-SICs described in Section 7.3. In particular, it explains the numbers in Table 1 of Section 3.3.1.

Although we do not prove it in this paper, it appears that live fiducials of the form Π_s, with s a fiducial datum, are always strongly centred (see Definition 3.19). It also appears that every r-SIC contains at least one strongly centred fiducial. Conjugating with elements of $\mathrm{EC}_0(d)$ takes strongly centred fiducials to strongly centred fiducials. To obtain the full set of r-SICs we then conjugate the strongly centred fiducials with elements of $\mathrm{WH}(d)$.

We begin with a statement of the main results of this subsection.

It is an immediate consequence of the definition that if (d, r, Q) is an admissible tuple, then (d, r, Q_M) is another admissible tuple, for all $M \in \mathrm{GL}_2(\mathbb{Z})$. Our first result says that the corresponding fields are the same, and that a similar statement holds for a fiducial datum:

Theorem 7.1. *Assume Conjecture 1.35. Let (d, r, Q, G, g) be a fiducial datum and M any element of $\mathrm{GL}_2(\mathbb{Z})$. Define $t = (d, r, Q)$, $t_M = (d, r, Q_M)$. Then*

(1) $E_{t_M} = E_t$

(2) (d, r, Q_M, G, g) is another fiducial datum.

This motivates the following definition.

Definition 7.2 (M-transformed tuple and fiducial datum, equivalent tuples and data sets)**.** Let $t = (d, r, Q)$ be an admissible tuple, $s = (d, r, Q, G, g)$ a fiducial datum, and M an element of $\mathrm{GL}_2(\mathbb{Z})$. We define t_M to be the M-transformed admissible tuple (d, r, Q_M), and s_M to be the M-transformed fiducial datum (d, r, Q_M, G, g).

We say that two admissible tuples $t = (d, r, Q)$, $t' = (d, r, Q')$ are *equivalent*, and write $t \sim t'$, if and only if the forms Q, Q' are equivalent.

Similarly, we say two fiducial datums $s = (d, r, Q, G, g)$, $s' = (d, r, Q', G, g)$ are equivalent, and write $s \sim s'$, if and only if the forms Q, Q' are equivalent.

The following homomorphism describes the relation between transformations of s, and transformations of Π_s which is the focus of this subsection:

Definition 7.3. Let $s = (d, r, Q, G, g)$ a fiducial datum. We define π_s to be the map of $\mathrm{GL}_2(\mathbb{Z})$ to $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ defined by

$$\pi_s \colon M \mapsto \mathrm{sgn}(j_{M^{-1}}(\rho_t))\, H_g G^{-1} [M]_{\bar{d}} G H_g^{-1} \tag{7.1}$$

where t is the admissible tuple (d, r, Q) and $[M]_{\bar{d}}$ is the image of M under the canonical homomorphism of $\mathrm{GL}_2(\mathbb{Z})$ to $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$.

Remark. The factor $\mathrm{sgn}\,(j_{M^{-1}}(\rho_t))$ means π_s is not a homomorphism. It is, however, "almost" a homomorphism, in the sense that $\pi_s(M_1 M_2) = \pm \pi_s(M_1)\pi_s(M_2)$ for all $M_1, M_2 \in \mathrm{GL}_2(\mathbb{Z})$.

We need the following fact.

Theorem 7.4. *The map π_s is surjective for every fiducial datum s.*

Proof. We defer the proof to page 104, at the end of this subsection. □

We are now able to state the central result of this subsection:

Theorem 7.5. *Let $s = (d, r, Q, G, g)$ be a fiducial datum, and let $M \in \mathrm{GL}_2(\mathbb{Z})$ be arbitrary. Then*

$$\Pi_{s_M} = U_F^\dagger \Pi_s U_F, \tag{7.2}$$

where $F = \pi_s(M)$.

Remark. The fact that π_s is surjective means that the converse is also true: given arbitrary $F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ there exists $M \in \mathrm{GL}_2(\mathbb{Z})$ for which (7.2) holds.

Note, however, that this correspondence between $\mathrm{GL}_2(\mathbb{Z})$ transformations of s and (anti-)symplectic transformations of Π_s cannot be a function in either direction. Indeed, $\mathrm{GL}_2(\mathbb{Z})$ is an infinite group, whereas $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ is finite. So there must be infinitely many matrices M corresponding to a given matrix F. Conversely, the existence of the symmetries described in Section 3.3.2 and

Section 7.4 below means that there is more than one matrix F corresponding to a given matrix M. This incidentally means that infinitely many different sets of fiducial data s must give rise to the same fiducial Π_s.

Proof. We defer the proof to page 105, at the end of this subsection. □

Before proving Theorems 7.4, and 7.5 we need to establish some preliminary results.

Theorem 7.6. *Let t be an admissible tuple and M an element of $\mathrm{GL}_2(\mathbb{Z})$. Then*

$$L_{t_M} = M^{-1} L_t M, \tag{7.3}$$

$$L_{+,t_M} = M^{-1} L_{+,t} M, \tag{7.4}$$

$$L_{\mathrm{z},\mathrm{t_M}} = M^{-1} L_{\mathrm{z},\mathrm{t}} M, \tag{7.5}$$

$$A_{t_M} = M^{-1} A_t M, \tag{7.6}$$

and

$$\rho_{t_M} = M^{-1} \rho_t \tag{7.7}$$

(see Definitions 1.28, 1.32 for definitions of $L_t, L_{+,t}, L_{\mathrm{z},\mathrm{t}}, A_t, \rho_t$).

Proof. Let $t = (d, r, Q) \sim (K, j, m, Q)$. It follows from Theorem 4.53 that

$$L_{+,t} = \chi_Q(\varepsilon^{j_{\min}(f)}) = \left(\frac{d_{j_{\min}(f)} - 1}{2}\right) I + \frac{f_{j_{\min}}(f)}{f} SQ \tag{7.8}$$

and

$$L_{+,t_M} = \chi_Q(\varepsilon^{j_{\min}(f)}) = \left(\frac{d_{j_{\min}(f)} - 1}{2}\right) I + \frac{f_{j_{\min}}(f)}{f} SQ_M. \tag{7.9}$$

It follows from (1.31) and Lemma 4.37 that

$$SQ_M = \det(M) S M^{\mathrm{T}} Q M = M^{-1} S Q M, \tag{7.10}$$

implying

$$L_{+,t_M} = M^{-1} L_{+,t} M \tag{7.11}$$

Equation (7.5) and (7.6) follow from this and the fact that

$$L_{\mathrm{z},\mathrm{t}} = L_{+,t}^n, \qquad L_{\mathrm{z},\mathrm{t_M}} = L_{+,t_M}^n, \tag{7.12}$$

$$A_t = L_{+,t}^{n(2m+1)}, \qquad A_{t_M} = L_{+,t_M}^{n(2m+1)}, \tag{7.13}$$

where $n = j/j_{\min}(f)$. If $\varphi_f = \varepsilon_f$ then $L_t = L_{+,t}$, $L_{t_M} = L_{+,t_M}$, from which (7.3) follows. Otherwise it follows from Theorems 4.6 and 4.16 that $j_{\min}(f)$ is odd, $d_{j_{\min}(f)} - 3$ is a perfect square, $f_{j_{\min}(f)}$ is divisible by $f\sqrt{d_{j_{\min}(f)} - 3}$, and

$$L_t = \chi_Q(\varphi^{j_{\min}(f)}) = \frac{\sqrt{d_{j_{\min}(f)} - 3}}{2} I + \frac{f_{j_{\min}(f)}}{f\sqrt{d_{j_{\min}(f)} - 3}} SQ, \tag{7.14}$$

$$L_{t_M} = \chi_Q(\varphi^{j_{\min}(f)}) = \frac{\sqrt{d_{j_{\min}(f)} - 3}}{2} I + \frac{f_{j_{\min}(f)}}{f\sqrt{d_{j_{\min}(f)} - 3}} SQ_M. \tag{7.15}$$

Equation (7.3) is then a consequence of this together with (7.10).

Finally, it follows from Definition 1.32 and Lemma 4.51 that

$$\rho_{t_M} = \rho_{Q_M,+} = M^{-1}\rho_{Q,+} = M^{-1}\rho_t. \tag{7.16}$$

□

Theorem 7.7. *Let $t = (d, r, Q)$ be an admissible tuple, and let $M \in \mathrm{GL}_2(\mathbb{Z})$. Then*

$$\mathfrak{w}_{B_{t_M}}^{d^{-1}\mathbf{p}}(\rho_{t_M}) = \begin{cases} \mathfrak{w}_{B_t}^{d^{-1}lM\mathbf{p}}(\rho_t) & \det M = 1, \\ \left(\mathfrak{w}_{B_t}^{d^{-1}lM\mathbf{p}}(\rho_t)\right)^* & \det M = -1, \end{cases} \tag{7.17}$$

where either $\mathbf{p} \in \mathbb{Z}^2 \setminus d\mathbb{Z}^2$ or $\mathbf{p} = \mathbf{0}$, where either $B_t = A_t$, $B_{t_M} = A_{t_M}$ or $B_t = A_t^{-1}$, $B_{t_M} = A_{t_M}^{-1}$, and where $l = \operatorname{sgn}(j_{M^{-1}}(\rho_t))$.

Proof. Proved in [70, Thm. 4.37].

□

Theorem 7.8 tells us how the candidate normalized ghost overlaps transform under the action of an element of $\mathrm{GL}_2(\mathbb{Z})$:

Theorem 7.8. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, and let $M \in \mathrm{GL}_2(\mathbb{Z})$. Then*

$$\tilde{\nu}_{\mathbf{p}}(t_M) = \tilde{\nu}_{lM\mathbf{p}}(t) \tag{7.18}$$

for all $\mathbf{p} \notin d\mathbb{Z}^2$, where $l = \operatorname{sgn}(j_{M^{-1}}(\rho_t))$

Proof. Let f be the conductor of Q. Then f is also the conductor of Q_M. It follows from Definition 1.30 and Lemma 5.1 that

$$\begin{aligned} \phi_{\mathbf{p}}(t_M) &= (-1)^{s_d(\mathbf{p})} e^{-\frac{\pi i}{12}\Psi(A_{t_M})} \xi_d^{-\frac{fjm}{f} Q_M(\mathbf{p})} \\ &= (-1)^{s_d(\mathbf{p})} e^{-\frac{\pi i}{12}(\det M)\Psi(A_t)} \xi_d^{-\frac{fjm}{f}(\det M) Q(M\mathbf{p})} \end{aligned} \tag{7.19}$$

Let $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. Then

$$\begin{aligned} &s_d(lM\mathbf{p}) \\ &\quad = d + (1+d)(1 + l(\alpha p_1 + \beta p_2))(1 + l(\gamma p_1 + \delta p_2)) \\ &\quad \equiv d + (1+d)(1 + (\alpha + \gamma + \alpha\gamma)p_1 + p_1 p_2 + (\beta + \delta + \beta\delta)p_2) && \pmod 2 \\ &\quad \equiv d + (1+d)\left(((1+p_1)(1+p_2) + (1+\alpha)(1+\gamma)p_1 + (1+\beta)(1+\delta)p_2\right) && \pmod 2 \end{aligned} \tag{7.20}$$

The fact that α is coprime to γ and β is coprime to δ means $(1+\alpha)(1+\gamma)$ and $(1+\beta)(1+\delta)$ are both even. So

$$s_d(lM\mathbf{p}) \equiv s_d(\mathbf{p}) \pmod 2. \tag{7.21}$$

Also

$$Q(lM\mathbf{p}) = Q(M\mathbf{p}). \tag{7.22}$$

Hence

$$\phi_{\mathbf{p}}(t_M) = \begin{cases} \phi_{lM\mathbf{p}}(t) & \det M = +1, \\ (\phi_{lM\mathbf{p}}(t))^* & \det M = -1. \end{cases} \tag{7.23}$$

It follows from Theorem 7.7 that

$$\mathfrak{w}_{A_{t_M}}^{d^{-1}\mathbf{p}}(\rho_{t_M}) = \begin{cases} \mathfrak{w}_{A_t}^{d^{-1}lM\mathbf{p}}(\rho_t) & \det M = +1, \\ \left(\mathfrak{w}_{A_t}^{d^{-1}lM\mathbf{p}}(\rho_t)\right)^* & \det M = -1. \end{cases} \tag{7.24}$$

Combining these results gives

$$\tilde{\nu}_{\mathbf{p}}(t_M) = \phi_{\mathbf{p}}(t_M)\mathfrak{w}_{A_{t_M}}^{d^{-1}\mathbf{p}}(\rho_{t_M}) = \begin{cases} \tilde{\nu}_{lM\mathbf{p}}(t) & \det M = +1, \\ (\tilde{\nu}_{lM\mathbf{p}}(t))^* & \det M = -1. \end{cases} \tag{7.25}$$

Taking account of the fact that $\tilde{\nu}_{lM\mathbf{p}}(t)$ is real we conclude

$$\tilde{\nu}_{\mathbf{p}}(t_M) = \tilde{\nu}_{lM\mathbf{p}}(t) \tag{7.26}$$

irrespective of the sign of $\det M$. □

We are now able to prove the first of our main results:

Proof of Theorem 7.1. It follows from Theorem 7.8 that the elements of the sets $\{\tilde{\mu}_{\mathbf{p}}(t)\colon 0 \leq p_1, p_2 < d,\ \mathbf{p} \neq \mathbf{0}\}$ and $\{\tilde{\mu}_{\mathbf{p}}(t_M)\colon 0 \leq p_1, p_2 < d,\ \mathbf{p} \neq \mathbf{0}\}$ are equal up to a sign, implying $E_t = E_{t_M}$.

Turning to the second statement, by assumption

$$\det(G)r(2\lambda + d_j - 1 + d) \equiv 1 \pmod{\bar{d}} \tag{7.27}$$

for some for some $\lambda \in \mathcal{Z}_t$. To show $\lambda \in \mathcal{Z}_{t_M}$, let $\mathbf{p} \in \mathbb{Z}^2$ be arbitrary, and let $\mathcal{I}_{\mathbf{p}}$ be any complete set of coset representatives for $\mathbb{Z}^2/d\mathbb{Z}^2$ containing $\mathbf{0}$ and $\mathbf{p}$. Suppose, first of all, that $\det M = +1$. Then it follows from Theorem 7.6 and Theorem 7.7 that

$$\begin{aligned} &\sum_{\mathbf{q}\in\mathcal{I}_{\mathbf{p}}} \omega_d^{r\langle \mathbf{p}, (\lambda I + L_{\mathrm{z,t_M}})\mathbf{q}\rangle} \mathfrak{w}_{A_{t_M}}^{d^{-1}\mathbf{q}}(\rho_{t_M})\, \mathfrak{w}_{A_{t_M}^{-1}}^{d^{-1}(\mathbf{q}-\mathbf{p})}(\rho_{t_M}) \\ &\qquad = \sum_{\mathbf{q}\in\mathcal{I}_{\mathbf{p}}} \omega_d^{r\langle \mathbf{p}, M^{-1}(\lambda I + L_{\mathrm{z,t}})M\mathbf{q}\rangle} \mathfrak{w}_{A_t}^{d^{-1}lM\mathbf{q}}(\rho_t)\, \mathfrak{w}_{A_t^{-1}}^{d^{-1}lM(\mathbf{q}-\mathbf{p})}(\rho_t) \\ &\qquad = \sum_{\mathbf{q}\in\mathcal{I}'_{lM\mathbf{p}}} \omega_d^{r\langle M\mathbf{p}, (\lambda I + L_{\mathrm{z,t}})\mathbf{q}\rangle} \mathfrak{w}_{A_t}^{d^{-1}\mathbf{q}}(\rho_t)\, \mathfrak{w}_{A_t^{-1}}^{d^{-1}(\mathbf{q}-lM\mathbf{p})}(\rho_t) \\ &\qquad = d^2\delta_{\mathbf{p},\mathbf{0}}^{(d)} \end{aligned} \tag{7.28}$$

where $l = \operatorname{sgn}(j_{M^{-1}}(\rho_t))$ and $\mathcal{I}'_{lM\mathbf{p}} = lM\mathcal{I}_{\mathbf{p}}$. It follows that $\lambda \in \mathcal{Z}_{t_M}$ if $\det M = +1$. The fact that this is also true of $\det M = -1$ is proved similarly. It follows from the first statement that $\hat{E}_{t_M} = \hat{E}_t$. So (d, r, Q_M, G, g) is a fiducial datum. □

We next prove the following analogue of Theorem 7.5, applying to ghost fiducials.

Lemma 7.9. *Let $s = (t, G, g)$ be a fiducial datum containing the admissible tuple $t = (d, r, Q)$, and let M be any element of $\mathrm{GL}_2(\mathbb{Z})$. Let*

$$F = \operatorname{sgn}(j_{M^{-1}}(\rho_t))G^{-1}[M]_{\bar{d}}G \tag{7.29}$$

where $[M]_{\bar{d}}$ is the image of of M under the canonical homomorphism of $\mathrm{GL}_2(\mathbb{Z})$ into $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$. Then $F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ and

$$\tilde{\Pi}_{s_M} = U_F^\dagger \tilde{\Pi}_s U_F. \tag{7.30}$$

Proof. The fact that $F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ is immediate. It follows from Definition 1.44, Corollary 4.22 and Theorem 7.8 that

$$\begin{aligned}
\tilde{\Pi}_{s_M} &= \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{G\mathbf{p}}(t_M) D_{\mathbf{p}} \\
&= \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{lMG\mathbf{p}}(t) D_{\mathbf{p}} \\
&= \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{\mathbf{p}}(t) D_{lG^{-1}[M]_{\bar{d}}^{-1}\mathbf{p}} \\
&= \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{\mathbf{p}}(t) U_F^\dagger D_{G^{-1}\mathbf{p}} U_F \\
&= U_F^\dagger \tilde{\Pi}_s U_F, \qquad (7.31)
\end{aligned}$$

where $l = \mathrm{sgn}(j_{M^{-1}}(\rho_t))$. □

Before applying this result to the proof of the main theorem of this subsection we need to establish two technical results.

Lemma 7.10. *Let M be any element of $\mathrm{GL}_2(\mathbb{Z})$, x any irrational element of $\mathbb{R}$ and d any dimension greater than 1. Then there exists a matrix $M' \in \mathrm{GL}_2(\mathbb{Z})$ such that*

(1) $M' \equiv M \pmod{\bar{d}}$,
(2) $j_M(x) j_{M'}(x) < 0$.

Proof. The fact that $x \notin \mathbb{Q}$ means $j_M(x) \neq 0$. Define

$$F_{\pm 1} = \begin{pmatrix} -1-\bar{d} & \pm\bar{d} \\ \mp\bar{d} & -1+\bar{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}). \qquad (7.32)$$

We have

$$j_{F_+}(-Lx) + j_{F_-}(-Lx) = 2(\bar{d}-1) > 0. \qquad (7.33)$$

Consequently we can choose $\theta = \pm 1$ such that $j_{F_\theta}(-Lx)$ is positive. Define $M' = -F_\theta L$. Then $M' \equiv M \pmod{\bar{d}}$. Moreover, it follows from Lemma 2.16 that

$$j_{M'}(x) = j_{F_\theta}(-Lx) j_{-L}(x) = -j_{F_\theta}(-Lx) j_L(x) \qquad (7.34)$$

implying

$$\mathrm{sgn}(j_{M'}(x)) = -\mathrm{sgn}(j_M(x)). \qquad (7.35)$$

□

We next use this result to show that the map π_s is surjective:

Proof of Theorem 7.4. Let $F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}/\mathbb{Z})$ be arbitrary. The fact that the canonical homomorphism $\mathrm{GL}_2(\mathbb{Z}) \to \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ is surjective (see, e.g., ref. [30]) means that there exists $M \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$[M]_{\bar{d}} = G H_g^{-1} F H_g G^{-1} \qquad (7.36)$$

In view of Lemma 7.10 we may assume, without loss of generality, that $j_{M^{-1}}(\rho_t)$ is positive. We then have $\pi_s(M) = F$.

□

We are now ready to prove the main result of this subsection.

Proof of Theorem 7.5. Let $M \in \mathrm{GL}_2(\mathbb{Z})$. It follows from Lemma 7.9 that

$$\tilde{\Pi}_{s_M} = U_{\tilde{F}}^{\dagger} \tilde{\Pi}_s U_{\tilde{F}} \tag{7.37}$$

where

$$\tilde{F} = \mathrm{sgn}\left(j_{M^{-1}}(\rho_t)\right) G^{-1}[M]_{\bar{d}} G. \tag{7.38}$$

Applying g to both sides and using Definitions 1.44, 3.6 and Theorem 3.7 we find

$$\Pi_{s_M} = U_F^{\dagger} \Pi_s U_F \tag{7.39}$$

where

$$F = H_g \tilde{F} H_g^{-1} = \pi_s(M), \tag{7.40}$$

completing the proof. □

7.2. **Classification.** In this subsection we show that, subject to certain assumptions, 1-SICs can be classified in terms of equivalence classes of quadratic forms. We will need the following

Definition 7.11 (equivalence classes of admissible tuples)**.** For each admissible tuple $t = (d, r, Q)$ define

(1) $[t] = [d, r, Q]$ to be set of all admissible tuples (d, r, Q'), where Q' is equivalent to Q,
(2) $[\![t]\!] = [\![d, r, Q]\!]$ to be the set of all tuples (d, r, Q'), where Q' has the same conductor as Q.

We will sometimes write $[\![d, r, f]\!]$ in place of $[\![d, r, Q]\!]$, where f is the conductor of Q.

We will show that in the rank 1 case, subject to Conjectures 1.35, 1.51 and 2.9, and the three assumptions listed below,the equivalence classes $[t]$ are in bijective correspondence with the set of all $\mathrm{EC}(d)$ orbits of 1-SICs, and that the equivalence classes $[\![t]\!]$ are in bijective correspondence with the set of all Galois multiplets of 1-SICs. In Appendix F we illustrate this statement by listing the classes $[t]$, $[\![t]\!]$ along with salient details for the corresponding 1-SICs for dimensions 4–100.

Assumption 1. *Let Π, Π' be any pair of 1-SIC fiducials in dimension d. Then*

$$\mathrm{Tr}(\Pi D_{\mathbf{p}}) = \pm \mathrm{Tr}(\Pi' D_{\mathbf{p}}) \qquad \forall \mathbf{p} \tag{7.41}$$

if and only if $\Pi = \Pi'$.

Assumption 2. *Let $s = (d, 1, Q, G, g)$, $s' = (d, 1, Q', G', g')$ be admissible data such that Q and Q' have different discriminants. Then Π_s and $\Pi_{s'}$ are $\mathrm{EC}(d)$-inequivalent.*

Assumption 3. *In the rank 1 case the only shifts are 0 and 1.*

These statements have a different status from the ones we label "conjectures" in that they are only needed for the classification problem. Moreover, even if one or more of them were to fail it would not necessarily mean that 1-SICs could not be classified using quadratic forms; only that the classification would be more complicated.

Assumption 2 is worth singling out for special mention, in that it is shown in ref. [72], Theorem 8.2 that equivalence classes $[\![d, 1, f]\!]$, $[\![d, 1, f']\!]$ can give rise to the same field, even though $f \neq f'$. This happens, for instance, with the pairs $[\![47, 1, 1]\!]$, $[\![47, 1, 2]\!]$; $[\![67, 1, 1]\!]$, $[\![67, 1, 2]\!]$; and $[\![83, 1, 1]\!]$, $[\![83, 1, 2]\!]$. Although, there is no known instance, it is natural to wonder if there are cases where the corresponding SICs are $\mathrm{EC}(d)$-equivalent.

We confine our analysis to the rank 1 case due to uncertainties concerning the set of shifts when $r > 1$, as discussed in Section 5.5. In the following it will accordingly be assumed, without comment, that $r = 1$. In accordance with assumption 3 it will also be assumed without comment that $\det G = \pm 1$ for every twist G.

It is immediate that Π_s, $\Pi_{s'}$ cannot be be equal unless the dimensions are the same. So the classification problem reduces to the question of what can be said of the 1-SICs corresponding to two sets of fiducial data $s = (d, 1, Q, G, g)$, $s' = (d, 1, Q', G', g')$ when (Q, G, g) and (Q', G', g') are not assumed to be the same. We begin with the following result.

Theorem 7.12. *Let $s = (d, 1, Q, G, g)$, $s' = (d, 1, Q', G', g)$ be a pair of fiducial datums for which $Q' \sim Q$. If Assumption 3 is true there exists $F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ such that*

$$\Pi_{s'} = U_F \Pi_s U_F^\dagger \tag{7.42}$$

Proof. It follows from Lemma 7.9 that there exists $F' \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ such that

$$\tilde{\Pi}_{s''} = U_{F'} \tilde{\Pi}_s U_{F'}^\dagger \tag{7.43}$$

where $s'' = (d, 1, Q', G, g)$. Let F'' be the image of $G^{-1}G'$ under the canonical homomorphism $\mathrm{GL}_2(\mathbb{Z}) \to \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$. Writing $t' = (d, 1, Q')$ and referring to Definition 1.44 we see that

$$\begin{aligned}
\tilde{\Pi}_{s''} &= \frac{1}{d} I + \frac{1}{d\sqrt{d+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{\mathbf{p}}(t') D_{G^{-1}\mathbf{p}} \\
&= \frac{1}{d} I + \frac{1}{d\sqrt{d+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{\mathbf{p}}(t') U_{F''} D_{G'^{-1}\mathbf{p}} U_{F''}^\dagger \\
&= U_{F''} \tilde{\Pi}_{s'} U_{F''}^\dagger .
\end{aligned} \tag{7.44}$$

Hence

$$\tilde{\Pi}_{s'} = U_{F''}^\dagger U_{F'} \tilde{\Pi}_s U_{F'}^\dagger U_{F''} . \tag{7.45}$$

Applying g to both sides we find, in view of Definitions 1.44, 3.6 and Theorem 3.7,

$$\Pi_{s'} = U_F \Pi_s U_F^\dagger \tag{7.46}$$

with $F = H_g F''^{-1} F' H_g^{-1}$. □

We also need to consider the effect of varying the Galois conjugation, g. Let $t = (d, r, Q)$ be an admissible tuple, let f be the conductor of Q, and let E_t be the field associated to t (as specified in Definition 1.40). Then it is easily seen that for every fiducial datum $s = (t, G, g)$ extending t the matrix elements of $\tilde{\Pi}_s$, Π_s are in E_t. Also if Conjecture 1.51 is true then E_t is the ray class field (in the generalized sense of Kopp and Lagarias [71]) with datum $(\mathcal{O}_f, \bar{d}\mathcal{O}_f, (\infty_1, \infty_2))$. In particular, if Conjecture 1.51 is true, and if $t' = (d, r, Q')$ is any other element of $[\![t]\!]$, then $E_{t'} = E_t$. We accordingly define $E_{[\![t]\!]} = E_t$.

We also need the following subfield of E_t:

Definition 7.13 (ring class field, class number)**.** Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple, and let f be the conductor of Q. We define the *ring class field* for t, denoted H_t, to be the ray class field (in the generalized sense of Kopp and Lagarias [71]) with datum $(\mathcal{O}_f, \mathcal{O}_f, \emptyset)$. We define the *class number* for t, denoted h_t, to be the class number of $\mathcal{O}_f$ (or, equivalently, the degree of the extension H_t/K).

Since H_t and h_t only depend on the equivalence class $[\![t]\!]$, we may define $H_{[\![t]\!]} = H_t$, $h_{[\![t]\!]} = h_t$.

Remark. Note that if $f = 1$, so that $\mathcal{O}_f$ is the maximal order, then H_t is the Hilbert class field.

Also define

Definition 7.14. On the assumption that Conjecture 1.51 is true, for each equivalence class $[\![d, 1, Q]\!]$ make a once-and-for-all choice of automorphism $g_{[\![d,1,Q]\!]} \in \mathrm{Gal}(E_{[\![d,1,Q]\!]}/\mathbb{Q})$ which does not fix K.

We will also need the following result

Theorem 7.15. *Assume Conjecture 1.51. Let $s = (t, G, g)$ be a fiducial datum containing the admissible tuple $t = (d, 1, Q)$, and let f be the conductor of Q. Let $Q_1, \ldots, Q_{h_t}$ be a set of representatives of the h_t distinct equivalence classes of forms having the same discriminant as Q. Then for each $g' \in \mathrm{Gal}(E_t/K)$ there exists a form $Q(g')$ having the same discriminant as Q and such that*

$$g'(\Pi_s) = \Pi_{s(g')}, \qquad s(g') = (d, 1, Q(g'), G, g). \tag{7.47}$$

Moreover

(1) For each integer $n = 1, \ldots, h_t$ there exists $g' \in \mathrm{Gal}(E_t/K)$ such that $Q(g') \sim Q_n$.
(2) $Q(g') \sim Q$ if and only if $g' \in \mathrm{Gal}(E_t/H_t)$.

Proof. To appear in a subsequent publication [14]. □

We then have

Theorem 7.16. *Assume Conjectures 1.35, 1.51 and Assumptions 1, 2, 3 are true. Let $s = (d, 1, Q, G, g)$ be a fiducial datum. There exists a form Q', having the same discriminant as Q, such that*

$$\Pi_s = \Pi_{s'}, \qquad s' = (d, 1, Q', I, g_{[\![d,1,Q]\!]}). \tag{7.48}$$

Proof. Let $s'' = (d, 1, Q, G, g_{[\![d,1,Q]\!]})$. It follows from Theorem 7.15 that

$$\Pi_s = g g^{-1}_{[\![d,1,Q]\!]}(\Pi_{s''}) = \Pi_{s'''}, \qquad s''' = (d, 1, Q'', G, g_{[\![d,1,Q]\!]}) \tag{7.49}$$

for some Q'' having the same discriminant as Q. It then follows from Theorem 7.12 that

$$\Pi_{s'''} = U_F \Pi_{s''''} U_F^\dagger, \qquad s'''' = (d, 1, Q'', I, g_{[\![d,1,Q]\!]}) \tag{7.50}$$

for some $F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$. In view of Theorems 7.4 and 7.5 this means

$$\Pi_{s'''} = \Pi_{s''''_M}, \qquad s''''_M = (d, 1, Q''_M, I, g_{[\![d,1,Q]\!]}) \tag{7.51}$$

for some $M \in \mathrm{GL}_2(\mathbb{Z})$. Setting $Q''_M = Q'$, $s''''_M = s'$ the claim now follows. □

It follows from this result together with Definition 3.18 and Theorems 7.5, 7.15 that, if we assume Conjectures 1.35, 1.51 and 2.9 and Assumptions 1, 2, 3, , and if we confine ourselves to 1-SICs of the kind specified by Definition 1.44, then there are bijective maps associating

(1) to each equivalence class $[t]$ a corresponding $\mathrm{EC}(d)$ orbit of 1-SICs,
(2) to each equivalence class $[\![t]\!]$ a corresponding Galois multiplet of 1-SICs.

The procedure for finding all the 1-SICs corresponding to a given admissible $(d, 1) \sim (K, j, m)$ is then as follows:

Step 1 Find the set of divisors of f_j. Each such divisor corresponds to a distinct Galois multiplet of the specified rank and dimension,

Step 2 For each $f \,|\, f_j$ calculate the corresponding class number $h_{[\![d,1,f]\!]}$ (see Definitions 7.11 7.13). This is the number of distinct $\mathrm{EC}(d)$ orbits in the multiplet $[\![d, 1, f]\!]$.

Step 3 Find $h_{[\![d,1,f]\!]}$ inequivalent quadratic forms Q_j having discriminant $f^2\Delta_0$, where Δ_0 is the discriminant of K. The 1-SICs corresponding to the admissible tuples $t_j = (d, 1, Q_j)$ give us a full set of representatives for the distinct $\mathrm{EC}(d)$ orbits in $[\![d, 1, f]\!]$.

Step 4 Conjugate the fiducials corresponding to the tuples $t_1, \ldots, t_{h_{[\![d,1,f]\!]}}$ with the elements of $\mathrm{EC}(d)$ to obtain the full set of 1-SICs in the Galois multiplet $[\![d, 1, f]\!]$.

Notice that equivalence of forms is defined relative to the group $\mathrm{GL}_2(\mathbb{Z})$ rather than $\mathrm{SL}_2(\mathbb{Z})$. So it is the wide class number that is relevant here.

This construction is illustrated in the data tables in Appendix F, which gives a complete listing of 1-SICs and corresponding equivalence classes $[t]$, $[\![t]\!]$ for $d \leq 100$.

7.3. **Illustrative examples.** In this subsection we illustrate the discussion in Section 7.2 with some examples, on the assumption that Conjectures 1.35, 1.36, and 1.51 are all true.

Consider the dimension grid corresponding to the field $K = \mathbb{Q}(\sqrt{5})$, illustrated in Equation (1.39). Consider first the admissible tuple $(4, 1) \sim (K, 1, 1)$. We have $f_1 = 1$ so there is only one Galois multiplet. The class number is 1, so the multiplet consists of a single $\mathrm{EC}(4)$ orbit. A choice of form which is calculationally optimal is $Q = \langle 1, -3, 1\rangle$. Comparing with the tables in refs. [89, 90] we see that this agrees with what was previously found by a brute force computational approach, and that Scott–Grassl orbit $4a$ is, in our notation, the orbit $[4, 1, \langle 1, -3, 1\rangle]$.

Moving up the left hand column of the grid we come to the admissible tuple $(8, 1) \sim (K, 2, 1)$. We have $f_2 = 3$, so there are two Galois multiplets corresponding to the choices $f = 1, 3$. The class numbers are both 1, so each multiplet consists of a single $\mathrm{EC}(8)$ orbit. Calculationally optimal choices of Q are $\langle 1, -3, 1\rangle$, $\langle 1, -7, 1\rangle$ respectively. Again, this is consistent with what was previously found. Comparing with the tables in refs. [89, 90] one finds that Scott–Grassl orbit $8a$ is $[8, 3, \langle 1, -7, 1\rangle]$ in our notation, and orbit $8b$ is $[8, 1, \langle 1, -3, 1\rangle]$. Finally, the fact that $1 \,|\, 3$ implies $E_{[\![8,1,1]\!]} \subseteq E_{[\![8,1,3]\!]}$, while the fact that $3 \nmid 2 \times 1$ and $\Delta_0 \not\equiv 1 \pmod 8$ means that $E_{[\![8,1,3]\!]} \not\subseteq E_{[\![8,1,1]\!]}$. So $E_{[\![8,1,1]\!]}$ is a proper subfield of $E_{[\![8,1,3]\!]}$

Since they only depend on the divisors of f_j and the class numbers $h_{K,f}$, and since these quantities are constant along the rows of the dimension grid, it follows that the number of Galois multiplets, and the number of $\mathrm{EC}(d)$ orbits within each multiplet are constant along each row. Thus, moving along the bottom row one finds that each of the sequence of admissible pairs $(4, 1), (11, 3), (29, 8), \ldots$ gives rise to one Galois multiplet, comprising one $\mathrm{EC}(d)$ orbit. Similarly, moving along the next-to-bottom row one finds that each of the sequence of admissble pairs $(8, 1), (55, 7), (377, 48), \ldots$ gives rise to two Galois multiplets, each comprising one $\mathrm{EC}(d)$ orbit.

In Appendix F we give, on the assumption that Conjectures 1.35, 1.36, and 1.51 are true, a complete listing of Galois multiplets and $\mathrm{EC}(d)$ orbits of 1-SICs for $d \leq 100$. Using this table one can also find the number of Galois multiplets and $\mathrm{EC}(d)$ orbits for any admissible tuple $(d, r) \sim (K, j, m)$ such that $d_j \leq 100$.

In this way, assuming our conjectures, one can quickly compute the number of multiplets and orbits for much larger dimensions. For instance when $d = 10^6$ one finds that there is a single Galois multiplet with class number $14\,800$. By contrast, when $d = 10^6 + 3$ one finds that there are 40 Galois multiplets with conductors and class numbers as in Table 2. The number of multiplets as a function of dimension is plotted in Figure 3 while the number of $\mathrm{EC}(d)$ orbits is plotted in Figure 4.

f	$h_{K,f}$	f	$h_{K,f}$	f	$h_{K,f}$	f	$h_{K,f}$	f	$h_{K,f}$
1	1	2	1	4	1	5	2	8	2
10	2	16	4	20	4	25	10	40	8
50	10	53	52	80	16	100	20	106	52
125	50	200	40	212	52	250	50	265	104
400	80	424	104	500	100	530	104	848	208
1 000	200	1 060	208	1 325	520	2 000	400	2 120	416
2 650	520	4 240	832	5 300	1 040	6 625	2 600	10 600	2 080
13 250	2 600	21 200	4 160	26 500	5 200	53 000	10 400	106 000	20 800

TABLE 2. Conductors and class numbers for 1-SICs in dimension 10^6+3, assuming Conjectures 1.35, 1.36, and 1.51 are true.

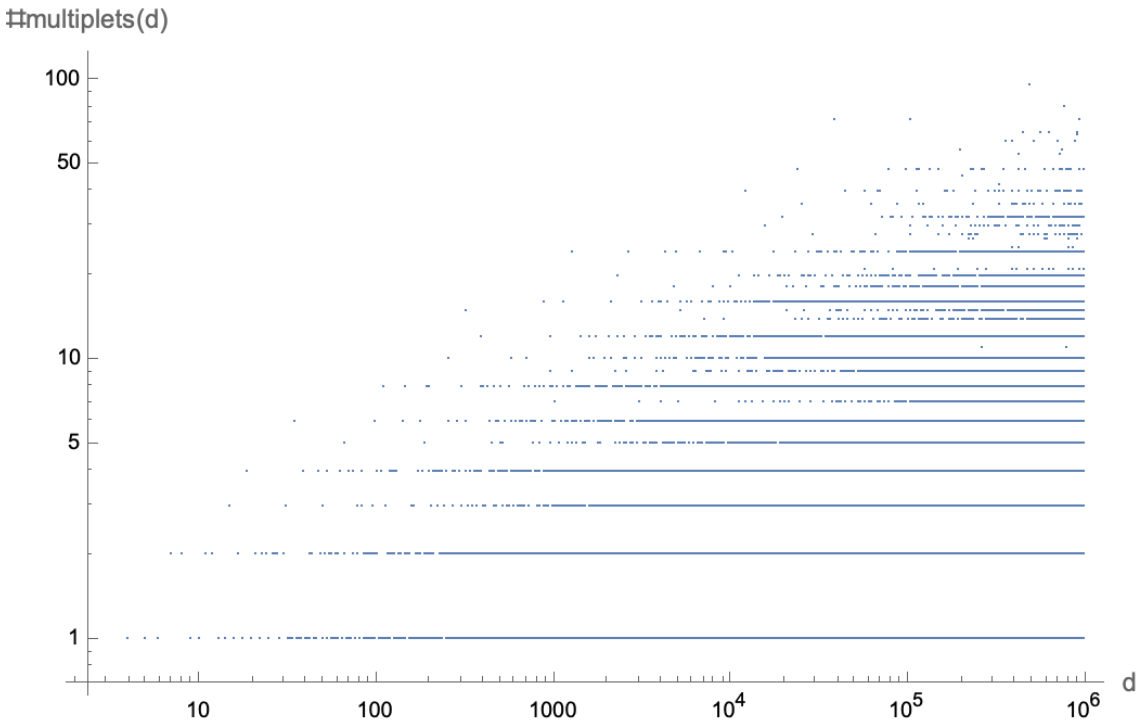


FIGURE 3. Number of Galois multiplets of 1-SICs as a function of dimension, assuming Conjectures 1.35, 1.36, and 1.51 are true.

We conclude with a few observations concerning the distribution of r-SICs with $r>1$. A pair (d,r) is admissible if and only if $0<r<(d-1)/2$ and

$$nr(d-r)=d^2-1 \tag{7.52}$$

for some integer $n>4$ (see Definition 1.21 and discussion following). If $r=1$ then solutions to (7.52) exist for every $d>3$. This is far from being the case when $r>1$. Thus, one finds that there are only 1 153 dimensions d less than 10^6 for which there exist admissible pairs (d,r) with $r>1$. Moreover, in almost of all of these cases there is only one pair with $r>1$, the only exceptions for $d\leq 10^6$ being the five dimensions 29, 71, 239, 3 191, 60 761 where there are exactly two pairs. See

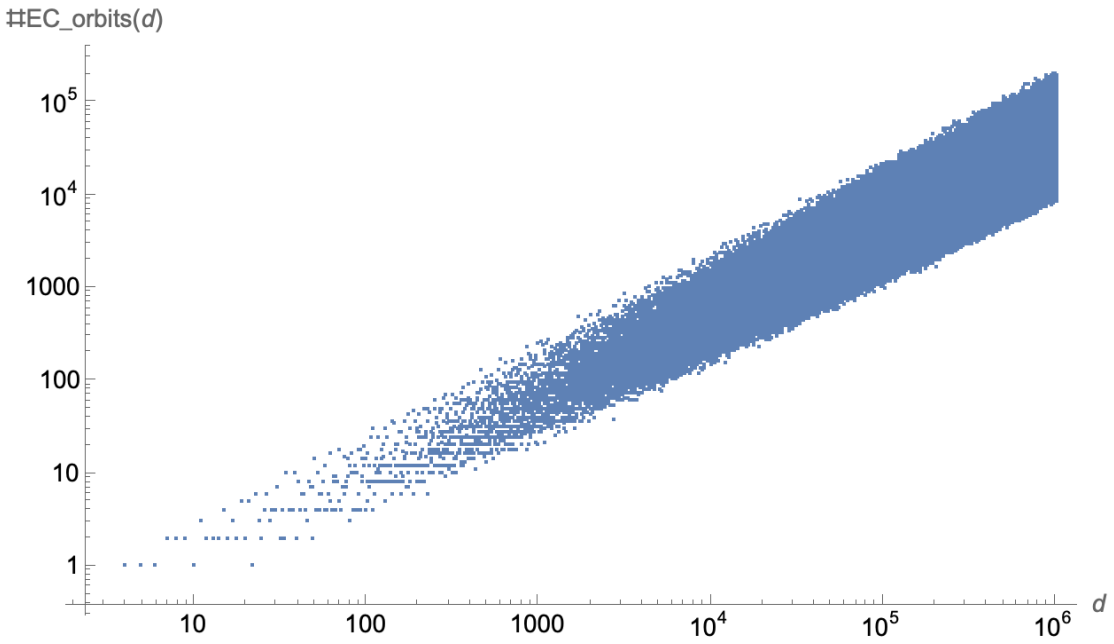


FIGURE 4. Number of $\mathrm{EC}(d)$ orbits of 1-SICs as a function of dimension, assuming Conjectures 1.35, 1.36, and 1.51 are true.

Figs. 5, 6 for the distribution of dimensions up to $d = 10^6$, and Table 3 for the first 30 solutions to Eq. (7.52) with $r > 1$.

d	r	K	j	m	d	r	K	j	m	d	r	K	j	m
11	3	$\mathbb{Q}(\sqrt{5})$	1	2	109	10	$\mathbb{Q}(\sqrt{6})$	1	2	271	16	$\mathbb{Q}(\sqrt{7})$	1	2
19	4	$\mathbb{Q}(\sqrt{3})$	1	2	131	11	$\mathbb{Q}(\sqrt{13})$	1	2	305	17	$\mathbb{Q}(\sqrt{285})$	1	2
29	5	$\mathbb{Q}(\sqrt{21})$	1	2	139	24	$\mathbb{Q}(\sqrt{21})$	1	3	341	18	$\mathbb{Q}(\sqrt{5})$	3	2
	8	$\mathbb{Q}(\sqrt{5})$	1	3	155	12	$\mathbb{Q}(\sqrt{35})$	1	2	377	48	$\mathbb{Q}(\sqrt{5})$	2	3
41	6	$\mathbb{Q}(\sqrt{2})$	1	2	181	13	$\mathbb{Q}(\sqrt{165})$	1	2	379	19	$\mathbb{Q}(\sqrt{357})$	1	2
55	7	$\mathbb{Q}(\sqrt{5})$	2	2	199	55	$\mathbb{Q}(\sqrt{5})$	1	5	419	20	$\mathbb{Q}(\sqrt{11})$	1	2
71	8	$\mathbb{Q}(\sqrt{15})$	1	2	209	14	$\mathbb{Q}(\sqrt{3})$	2	2	461	21	$\mathbb{Q}(\sqrt{437})$	1	2
	15	$\mathbb{Q}(\sqrt{3})$	1	3	239	15	$\mathbb{Q}(\sqrt{221})$	1	2	505	22	$\mathbb{Q}(\sqrt{30})$	1	2
76	21	$\mathbb{Q}(\sqrt{5})$	1	4		35	$\mathbb{Q}(\sqrt{2})$	1	3	521	144	$\mathbb{Q}(\sqrt{5})$	1	6
89	9	$\mathbb{Q}(\sqrt{77})$	1	2	265	56	$\mathbb{Q}(\sqrt{3})$	1	4	551	23	$\mathbb{Q}(\sqrt{21})$	2	2

TABLE 3. The first 30 solutions to Eq. (7.52) with $r > 1$.

7.4. **Symmetries.** The purpose of this subsection is to prove some of the empirical observations in Section 3.3.2, regarding the symmetry group of a 1-SIC, and to generalize them to an arbitrary r-SIC. We begin with a summary of our main results.

Definition 7.17 (R_s, $R_{+,s}$, $R_{\mathrm{z,s}}$)**.** Let $s = (t, G, g)$ be a fiducial datum containing the admissible tuple $t = (d, r, Q) \sim (K, j, m, Q)$. We define

$$R_s = \pi_s(L_t), \tag{7.53}$$

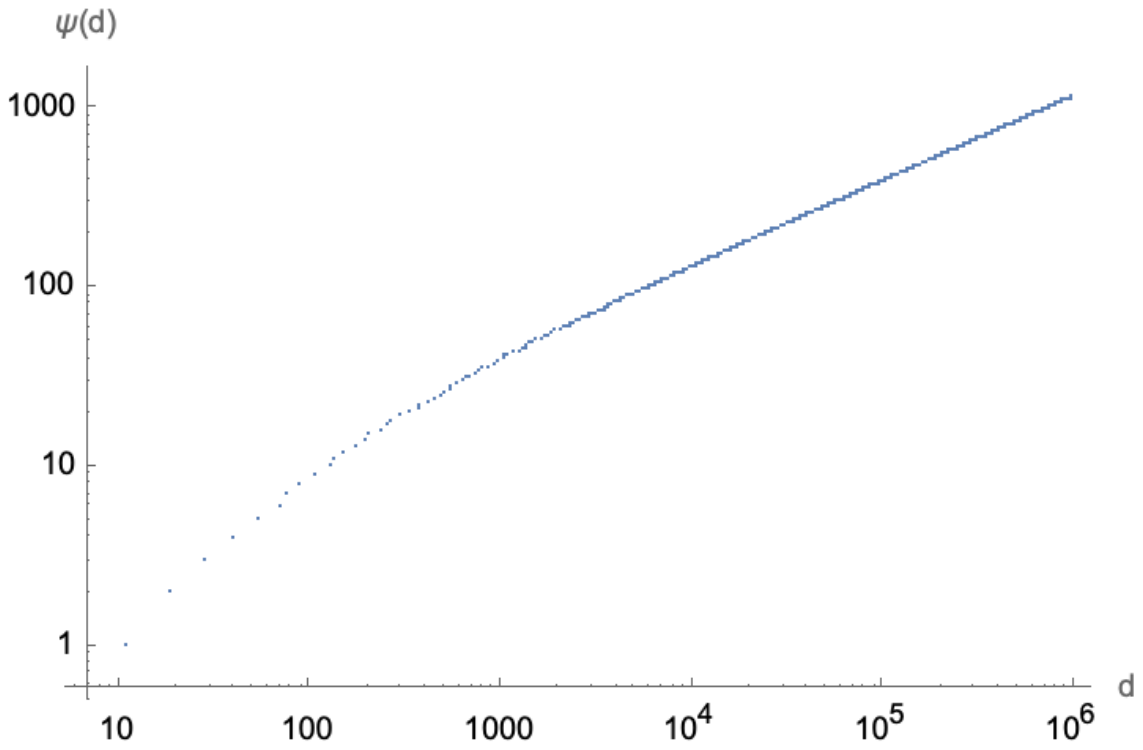


FIGURE 5. Plot of $\psi(d)$ against d, where $\psi(d)$ is the number of dimensions less than or equal to d in which there occur r-SICs with $r > 1$, assuming Conjectures 1.35, and 1.36 are true.

$$R_{+,s} = \pi_s(L_{+,t}), \tag{7.54}$$

$$R_{\mathrm{z,s}} = \pi_s(L_{\mathrm{z,t}}) \tag{7.55}$$

(see Definitions 1.28, 7.3 for definitions of L_t, $L_{+,t}$, $L_{\mathrm{z,t}}$, π_s).

Definition 7.18 (unitary/anti-unitary type)**.** Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple. Let f the conductor of Q. We say the tuple t is of *anti-unitary type* if all three of the following conditions are satisfied:

(1) $d_1 - 3$ is a perfect square,
(2) $j_{\min}(f)$ is odd,
(3) $f\sqrt{d_{j_{\min}}(f) - 3}$ divides $f_{j_{\min}(f)}$.

Otherwise, we say it is of *unitary type*.

Remark. Note that it follows from Theorem 4.6 that if $d_1 - 3$ is a perfect square and $j_{\min}(f)$ is odd then $d_{j_{\min}}(f) - 3$ is also a perfect square.

Our first result says that π_s maps stabilizers of forms into stabilizers of fiducials:

Theorem 7.19. *Let $s = (t, G, g)$ be a fiducial datum containing the admissible tuple $t = (d, r, Q) \sim (K, j, m, Q)$. The restriction of π_s to $\mathcal{S}(Q)$ is a homomorphism of $\mathcal{S}(Q)$ onto $\langle R_s \rangle$. Moreover, $\langle R_s \rangle \subseteq \mathcal{S}_{\mathrm{ESL}}(\Pi_s)$.*

Remark. See Definition 3.17 for definition of $\mathcal{S}_{\mathrm{ESL}}(\Pi_s)$. In every case where the groups have been calculated one finds in fact $\langle R_s \rangle = \mathcal{S}_{\mathrm{ESL}}(\Pi_s)$.

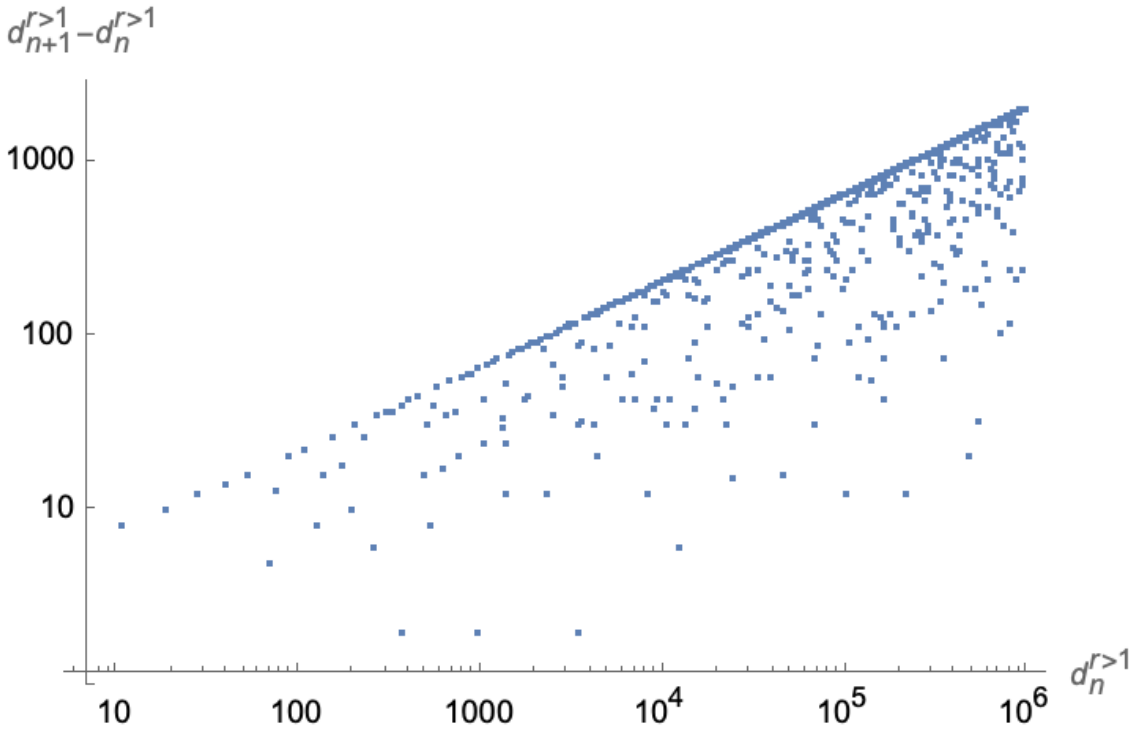


FIGURE 6. Plot of $d_{n+1}^{r>1} - d_n^{r>1}$ against $d_n^{r>1}$, where $d_1^{r>1}, d_2^{r>1}, \ldots$ is the increasing sequence of dimensions in which there occur r-SICs with $r > 1$, assuming Conjectures 1.35, and 1.36 are true.

Proof. See below. □

Our second result establishes some basic properties of the matrices R_s, $R_{\mathrm{z,s}}$.

Theorem 7.20. *Let $s = (t, G, g)$ be a fiducial datum containing the admissible tuple $t = (d, r, Q) \sim (K, j, m, Q)$. Then*

(1) R_s has the properties

Type of t	d	$\det(R_s)$	$Tr(R_s)$	*order of* R_s	*order of* $U_{R_s}\langle I\rangle$
unitary	*odd*	*1*	$d_{j_{\min}(f)} - 1$	$n_t(2m+1)$	$n_t(2m+1)$
unitary	*even*	*1*	$d_{j_{\min}(f)} - 1$	$2n_t(2m+1)$	$n_t(2m+1)$
anti-unitary	*odd*	*-1*	$-\sqrt{d_{j_{\min}(f)} - 3}$	$2n_t(2m+1)$	$2n_t(2m+1)$
anti-unitary	*even*	*-1*	$-\sqrt{d_{j_{\min}(f)} - 3}$	$4n_t(2m+1)$	$2n_t(2m+1)$

(2) $R_{\mathrm{z,s}}$ has the properties

Type of t	d	$R_{\mathrm{z,s}}$	$\det(R_{\mathrm{z,s}})$	$Tr(R_{\mathrm{z,s}})$	*order of* $R_{\mathrm{z,s}}$	*order of* $U_{R_{\mathrm{z,s}}}\langle I\rangle$
unitary	*odd*	$R_s^{n_t}$	*1*	$d_j - 1$	$2m+1$	$2m+1$
unitary	*even*	$R_s^{n_t}$	*1*	$d_j - 1$	$2(2m+1)$	$2m+1$
anti-unitary	*odd*	$R_s^{2n_t}$	*1*	$d_j - 1$	$2m+1$	$2m+1$
anti-unitary	*even*	$R_s^{2n_t}$	*1*	$d_j - 1$	$2(2m+1)$	$2m+1$

(see Definition 4.52 for the level, n_t).

Remark. If it is true that $\langle U_{R_s}\langle I\rangle\rangle = \mathcal{S}_{\mathrm{ESL}}(\Pi_s)$, as the empirical observations suggest, then this result means

(1) $\mathcal{S}(\Pi_s)$ contains a projective anti-unitary if and only if t is of anti-unitary type,
(2) $\mathcal{S}(\Pi_s)$ is cyclic order $n_t(2m+1)$ if t is of unitary type, and cyclic order $2n_t(2m+1)$ if t is of anti-unitary type.

It follows from the above that if $m = 1$ then $U_{R_{\mathrm{z,s}}}\langle I\rangle$ is a canonical order 3 projective unitary (see Definition 3.11). Our third main result establishes criteria for type-z and type-a orbits.

Theorem 7.21. *Let $s = (t, G, g)$ be a fiducial datum containing the admissible tuple $t = (d, 1, Q) \sim (K, j, 1, Q)$. Then*

(1) if $d \not\equiv 3 \pmod 9$ then $R_{\mathrm{z,s}}$ is conjugate to F_{z},
(2) if $d \equiv 3 \pmod 9$ there exist both type-a and type-z orbits. Specifically:
  (a) if $f_j/f \equiv 0 \pmod 3$ then $R_{\mathrm{z,s}}$ is conjugate to F_{a},
  (b) if $f_j/f \not\equiv 0 \pmod 3$ then $R_{\mathrm{z,s}}$ is conjugate to F_{z}.

Remark. This result explains why one gets both type-z and type-a orbits when $d \equiv 3 \pmod 9$. If one makes the additional assumption that $\langle R_s\rangle = \mathcal{S}_{\mathrm{OL}}(\Pi)$ (as is the case in every instance where the groups have been explicitly calculated) then it also explains why one never finds type-a' orbits when $d \equiv 6 \pmod 9$.

Proof. See below. □

Proof of Theorem 7.19. Suppose M_1, $M_2 \in \mathcal{S}(Q)$. Then it follows from Lemmas 2.16 and 4.51 that

$$j_{(M_1M_2)^{-1}}(\rho_t) = j_{M_2^{-1}}(M_1^{-1}\rho_t)j_{M_1^{-1}}(\rho_t) = j_{M_2^{-1}}(\rho_t)j_{M_1^{-1}}(\rho_t), \tag{7.56}$$

implying

$$\pi_s(M_1M_2) = \operatorname{sgn}\left(j_{(M_1M_2)^{-1}}(\rho_t)\right) H_gG^{-1}[M_1M_2]_{\bar{d}}GH_g^{-1} = \pi_s(M_1)\pi_s(M_2). \tag{7.57}$$

So the restriction of π_s to $\mathcal{S}(Q)$ is a homomorphism. It follows from Theorem 4.53 that $\mathcal{S}(Q) = \langle -I, L_t\rangle$. The fact that $j_{-I}(\rho_t) = -1$ implies $\pi_s(-I) = I$. So $\pi_s(\mathcal{S}(Q)) = \langle R_s\rangle$. Finally, it follows from Theorem 7.5 that

$$U_{R_s}^{\dagger}\Pi_s U_{R_s} = \Pi_{s_{L_t}} = \Pi_s \tag{7.58}$$

implying $R_s \in \mathcal{S}_{\mathrm{ESL}}(\Pi_s)$. □

Before proving Theorem 7.20 we need

Lemma 7.22. *Let $s = (t, G, g)$ be a fiducial datum containing the admissible tuple $t = (d, r, Q) \sim (K, j, m, Q)$. Then*

$$R_s = \pi_s(L_t) = \begin{cases} H_gG^{-1}[L_t]_{\bar{d}}GH_g^{-1} & \text{if } t \text{ is of unitary type,} \\ -H_gG^{-1}[L_t]_{\bar{d}}GH_g^{-1} & \text{if } t \text{ is of anti-unitary type.} \end{cases} \tag{7.59}$$

Proof. Let f be the conductor of Q. It follows from theorems 4.16, 4.34 and 4.53 that $\det(L_t) = \mathrm{Nm}(\varphi_f) = -1$ if and only if the tuple t is of anti-unitary type. Also, by assumption $\mathrm{Tr}(L_t^{-1}) > 0$ (see Definition 1.28). In view of Lemma 2.18 this means $\rho_t \in \mathcal{D}_{L_t^{-1}}$. Referring to Definition 1.15 we deduce that $\operatorname{sgn}(j_{L_t^{-1}}(\rho_t)) = \det(L_t^{-1})$. Equation (7.59) follows from this and definitions 7.3, 7.17. □

Proof of Theorem 7.20. Proof of statement 1. It follows from Lemma 7.22 that

$$\det(R_s) = \det\left([L_t]_{\bar{d}}\right) = \begin{cases} 1 & \text{if } t \text{ is of unitary type,} \\ -1 & \text{if } t \text{ is of anti-unitary type.} \end{cases} \tag{7.60}$$

Taking account of Lemma 4.3 and theorems 4.6, 4.34 and 4.53 it also follows that

$$\begin{aligned} \mathrm{Tr}(R_s) &= \begin{cases} \mathrm{Tr}\left(L_t\right) & \text{if } t \text{ is of unitary type,} \\ -\mathrm{Tr}\left(L_t\right) & \text{if } t \text{ is of anti-unitary type,} \end{cases} \\ &= \begin{cases} \mathrm{Tr}\left(\varepsilon_f\right) & \text{if } t \text{ is of unitary type,} \\ -\mathrm{Tr}\left(\varphi_f\right) & \text{if } t \text{ is of anti-unitary type,} \end{cases} \\ &= \begin{cases} d_{j_{\min}(f)} - 1 & \text{if } t \text{ is of unitary type,} \\ -\sqrt{d_{j_{\min}(f)} - 3} & \text{if } t \text{ is of anti-unitary type,} \end{cases} \end{aligned} \tag{7.61}$$

It remains to calculate the orders of R_s, $U_{R_s}\langle I\rangle$. We consider the four cases separately.

Case 1: t is of unitary type and d is odd. It follows from Lemma 7.22 and Theorem 4.53 that

$$\begin{aligned} R_s^l = I \quad &\iff \quad L_t^l \equiv I \pmod{d} \\ &\iff \quad L_t^l \in \mathcal{S}_d(Q) \\ &\iff \quad L_t^l \in \langle A_t \rangle \\ &\iff \quad l n_t(2m+1) \mid l. \end{aligned} \tag{7.62}$$

So R_s is order $n_t(2m+1)$. In view of Theorem 3.5 this is also the order of $U_{R_s}\langle I\rangle$.

Case 2: t is of unitary type and d is even. Let l be the order of R_s. It follows from (7.59) and Theorem 4.53 that

$$\begin{aligned} R_s^l = I \quad &\iff \quad L_t^l \equiv I \pmod{\bar{d}} \\ &\implies \quad L_t^l \equiv I \pmod{d} \\ &\iff \quad L_t^l \in \langle A_t \rangle \end{aligned} \tag{7.63}$$

implying L_t^l is a power of A_t. Since $A_t \equiv (d+1)I \pmod{\bar{d}}$ we must in fact have $L_t^l = A_t^2 = L_t^{2n_t(2m+1)}$. So $l = 2n_t(2m+1)$. Since $L_t^{n_t(2m+1)} = (d+1)I$ it follows from Theorem 3.5 that the order of $U_{R_s}\langle I\rangle$ is $n_t(2m+1)$.

Case 3: t is of anti-unitary type and d is odd. As in case 1 we have $R_s^l = I \iff L_t^l \in \langle A_t\rangle$. The fact that t is of anti-unitary type means $\varepsilon = \varphi^2$. In view of Theorem 4.53 this means $A_t = L_t^{2n_t(2m+1)}$. So R_s is order $2n_t(2m+1)$. In view of Theorem 3.5 this is also the order of $U_{R_s}\langle I\rangle$.

Case 4: t is of anti-unitary type and d is even. Let l be the order of R_s. As in case 2 we must have $L_t^l = A_t^2$. As in case 3 we have $A_t = L_t^{2n_t(2m+1)}$. So L_s is order $4n_t(2m+1)$. Since $L_t^{n_t(2m+1)} = (d+1)I$ it follows from Theorem 3.5 that the order of $U_{R_s}\langle I\rangle$ is $2n_t(2m+1)$.

Proof of statement 2. It follows from Lemma 7.22 and Theorem 4.53 that

$$\begin{aligned} R_{\mathrm{z,s}} &= \pi_s(L_{\mathrm{z,t}}) \\ &= \begin{cases} \pi_s(L_t^{n_t}) & t \text{ is of unitary type,} \\ \pi_s(L_t^{2n_t}) & t \text{ is of anti-unitary type,} \end{cases} \end{aligned}$$

$$= \begin{cases} H_g G^{-1} [L_t^{n_t}]_{\bar{d}} G H_g^{-1} & t \text{ is of unitary type,} \\ H_g G^{-1} [L_t^{2n_t}]_{\bar{d}} G H_g^{-1} & t \text{ is of anti-unitary type.} \end{cases} \tag{7.64}$$

It follows that

$$R_{\mathrm{z,s}} = \begin{cases} R_s^{n_t} & t \text{ is of unitary type,} \\ R_s^{2n_t} & t \text{ is of anti-unitary type,} \end{cases} \tag{7.65}$$

and that $\det(R_s) = 1$ irrespective of whether t is of unitary or anti-unitary type. It also follows that

$$\begin{aligned} \mathrm{Tr}(R_s) &= \begin{cases} \mathrm{Tr}(L_t^{n_t}) & t \text{ is of unitary type,} \\ \mathrm{Tr}(L_t^{2n_t}) & t \text{ is of anti-unitary type,} \end{cases} \\ &= \mathrm{Tr}(\varepsilon_f^{n_t}) \\ &= \mathrm{Tr}(\varepsilon^j) \\ &= d_j - 1. \end{aligned} \tag{7.66}$$

Finally, Equation (7.65) in conjunction with statement 1 implies, firstly, that the order of $R_{\mathrm{z,s}}$ is $2m+1$ if d is odd and $2(2m+1)$ if d is even; and, secondly, that the order of $U_{R_{\mathrm{z,s}}}$ is $2m+1$ irrespective of the values of d, t. □

Before proving Theorem 7.21 we need

Lemma 7.23. *Let $t = (d, r, Q) \sim (K, j, m, Q)$ be an admissible tuple. Then*

$$\gcd(f_j, d_j) \equiv \begin{cases} 1 & d_j \not\equiv 3 \pmod 9, \\ 3 & d_j \equiv 3 \pmod 9. \end{cases} \tag{7.67}$$

Proof. Suppose p is a prime divisor of $\gcd(f_j, d_j)$. Then p divides both d_j and $(d_j - 3)(d_j + 1) = f_j^2 \Delta_0$ where Δ_0 is the discriminant of K. Since d_j is coprime to $d_j + 1$ it must in fact be the case that p divides both d_j and $d_j + 3$. It follows that $p = 3$ and d_j is a multiple of 3. We have thus shown that $\gcd(f_j, d_j)$ is a power of 3. In particular, if d_j is not a multiple of 3 then f_j is coprime to d.

Suppose d_j is a multiple of 3. We can write $d_j = 3t$ for some integer $t > 1$. Then $f_j^2 \Delta_0 = 3(t-1)(3t+1)$, from which it can be seen that f_j is a multiple of 3 if and only if $t - 1$ is a multiple of 3. Equivalently, f_j is a multiple of 3 if and only if $d_j \equiv 3 \pmod 9$. Combined with the result proved in the last paragraph this means (a) if $d_j \not\equiv 3 \pmod 9$, then $\gcd(f_j, d_j) = 1$ and (b) if $d_j \equiv 3 \pmod 9$, then $\gcd(f_j, d_j) = 3$. □

Proof of Theorem 7.21. It follows from Theorem 7.20 that $\det(R_{\mathrm{z,s}}) = 1$ and $\mathrm{Tr}(R_{\mathrm{z,s}}) = d - 1$. In view of Theorem 3.13 this means that $R_{\mathrm{z,s}}$ is conjugate to F_z if $d \not\equiv 3$ or $6 \pmod 9$.

Suppose, on the other hand, that $d \equiv 3 \pmod 9$ (respectively, $d \equiv 6 \pmod 9$). Then it follows from theorems 3.13 and 3.14 that $R_{\mathrm{z,s}}$ is conjugate to F_a (respectively F_a') if $R_{\mathrm{z,s}} \equiv I \pmod 3$, and to F_z otherwise. To find the condition for this to be so, observe that theorems 4.53, 7.20, and Lemma 7.22 imply

$$\begin{aligned} R_{\mathrm{z,s}} &= \begin{cases} R_s^{n_t} & t \text{ is of unitary type,} \\ R_s^{2n_t} & t \text{ is of anti-unitary type,} \end{cases} \\ &= \begin{cases} H_g G^{-1} [L_t^{n_t}]_{\bar{d}} G H_g^{-1} & t \text{ is of unitary type,} \\ H_g G^{-1} [L_t^{2n_t}]_{\bar{d}} G H_g^{-1} & t \text{ is of anti-unitary type,} \end{cases} \end{aligned}$$

$$
\begin{aligned}
&= \begin{cases} H_g G^{-1}[\chi_Q(\varphi_f^{n_t}]_{\bar{d}} G H_g^{-1} & t \text{ is of unitary type,} \\ H_g G^{-1}[\chi_Q(\varphi_f^{2n_t})]_{\bar{d}} G H_g^{-1} & t \text{ is of anti-unitary type,} \end{cases} \\
&= H_g G^{-1}[\chi_Q(\varepsilon_f^{n_t}]_{\bar{d}} G H_g^{-1} \\
&= H_g G^{-1}[\chi_Q(\varepsilon^j]_{\bar{d}} G H_g^{-1}. \qquad (7.68)
\end{aligned}
$$

Taking account of Corollary 4.36 and the fact that $\bar{d}$ is divisible by 3 this means

$$
\begin{aligned}
& R_{\mathrm{z,s}} \equiv I \pmod 3 \\
\iff \quad & [\chi_Q(\varepsilon^j)]_{\bar{d}} \equiv I \pmod 3 \\
\iff \quad & \chi_Q(\varepsilon^j) \equiv I \pmod 3 \\
\iff \quad & \varepsilon^j - 1 \in 3\mathcal{O}_f \\
\iff \quad & \frac{d-3-f_j\Delta_0}{2} + f_j\left(\frac{\Delta_0+\sqrt{\Delta_0}}{2}\right) = 3\left(p_1 + p_2 f\left(\frac{\Delta_0+\sqrt{\Delta_0}}{2}\right)\right) \qquad (7.69)
\end{aligned}
$$

for some $p_1, p_2 \in \mathbb{Z}$. The fact that $f_j^2\Delta_0 = (d-3)(d+1)$ means $f_j\Delta_0 \equiv d-3 \pmod 6$. We conclude that $R_{\mathrm{z,s}} \equiv I \pmod 3$ if and only if $f_j/f \equiv 0 \pmod 3$. Since $d \equiv 0 \pmod 3$ it follows from Lemma 7.23 that f_j/f is coprime to 3 if $d \equiv 6 \pmod 9$, but divisible by 3 if $d \equiv 3 \pmod 9$. So $R_{\mathrm{z,s}}$ is necessarily conjugate to F_z if $d \equiv 6 \pmod 9$. On the other hand, if $d \equiv 3 \pmod 9$ then there are values of f such that $f_j/f \equiv 0 \pmod 9$, implying $R_{\mathrm{z,s}}$ is conjugate to F_a, and others such that $f_j/f \not\equiv 0 \pmod 9$, implying $R_{\mathrm{z,s}}$ is conjugate to F_z. □

7.5. **Alignment.** We now come to the phenomenon of *SIC alignment* [3, 8]. In the rank 1 case it is empirically observed, in every case examined, that, up to a sign, the squares of the normalized overlaps at position d_j in a dimension tower reappear among the normalized overlaps at position d_{2j}. We will show that this phenomenon is a consequence of our results. Moreover, we will show that it generalizes to a relation between the normalized overlaps at positions d_j and d_{nj} in the tower, for any integer n coprime to 3.

We first state the main result of this subsection.

Theorem 7.24. *Let $s = (t, G, g)$ be a fiducial datum containing the rank 1 admissible tuple $t = (d_j, 1, Q) \sim (K, j, 1, Q)$. Let n an a positive integer coprime to 3. Define $t' = (d_{nj}, 1, Q) \sim (K, nj, 1, Q)$, $s' = (t', G, g)$, and $\kappa = d_{nj}/d_j$. Then t' is an admissible tuple and κ is an integer. If s' is also a fiducial datum then*

$$\nu_{\kappa\mathbf{p}}(s') = (-1)^{l(\mathbf{p})}\nu_{\mathbf{p}}(s)^n \qquad (7.70)$$

for all $\mathbf{p} \not\equiv \mathbf{0} \pmod{d_j}$, where

$$l(\mathbf{p}) = \begin{cases} n + (1+p_1)(1+p_2) & \text{if } d_j \text{ is even and } n \equiv \pm 2 \text{ or } \pm 5 \pmod{12}, \\ n+1 & \text{otherwise}. \end{cases} \qquad (7.71)$$

Remark. In the rank 1 case the empirical observations suggest that if t is an admissible tuple then (t, G, g) is a fiducial datum if and only if $\det(G) = \pm 1$ and $g(\sqrt{\Delta_0}) = -\sqrt{\Delta_0}$. If that is true then s' is automatically a fiducial datum, so this requirement does not need to be imposed as an additional assumption.

Before proving it we need to establish the following technical result:

Lemma 7.25. *Let $t = (d, 1, Q) \sim (K, j, 1, Q)$ be an admissible tuple, and let n be a positive integer coprime to 3. Then d_{nj} is divisible by $d_j = d$ and*

$$\frac{f_{nj}d_{nj}(1+d_{nj})}{f_j d_j} \equiv \begin{cases} n(1+d_j)+d_j \pmod{2d_j} & \text{if } d_j \text{ is even and } n \equiv \pm 2 \text{ or } \pm 5 \pmod{12} \\ n(1+d_j) \pmod{2d_j} & \text{otherwise}\,. \end{cases} \tag{7.72}$$

Proof. The fact that d_{nj} is divisible by d_j follows from Theorem 4.9 and Lemma 4.10.

Suppose d_j is odd. It follows from Lemma 4.11 that d_{nj} is odd. So d_{nj}/d_j is odd. Theorem 4.9 and Lemma 4.10 imply

$$\frac{d_{nj}}{d_j} = \frac{T_n^*(d_j)}{d_j} \equiv \begin{cases} n \pmod{d_j} & \text{if } n \equiv 1 \pmod 3, \\ -n \pmod{d_j} & \text{if } n \equiv 2 \pmod 3, \end{cases} \tag{7.73}$$

The fact that d_{nj}/d_j is odd means that if n is also odd we must have $d_{nj}/d_j \equiv \pm n \pmod{2d_j}$, while if n is even we must have $d_{nj}/d_j \equiv \pm n + d_j \pmod{2d_j}$. In other words:

$$\frac{d_{nj}}{d_j} \equiv \begin{cases} n \pmod{2d_j} & \text{if } n \equiv 1 \pmod 6, \\ -n + d_j \pmod{2d_j} & \text{if } n \equiv 2 \pmod 6\,, \\ n + d_j \pmod{2d_j} & \text{if } n \equiv 4 \pmod 6, \\ -n \pmod{2d_j} & \text{if } n \equiv 5 \pmod 6, \end{cases} \tag{7.74}$$

Turning to the ratio f_{nj}/f_j, Theorem 4.9 and Lemma 4.10 imply

$$\frac{f_{nj}}{f_j} = U_n^*(d_j) \equiv \begin{cases} 1 \pmod{d_j} & \text{if } n \equiv 1 \pmod 3\,, \\ -1 \pmod{d_j} & \text{if } n \equiv 2 \pmod 3\,. \end{cases} \tag{7.75}$$

It follows fromLemma 4.10 that $U_1^*(d_j)$ is odd, $U_2^*(d_j)$ is even, and $U_n^*(d_j) \equiv U_{n-2}^*(d_j) \pmod 2$ for all $n > 2$. Consequently $U_n^*(d_j) \equiv n \pmod 2$ for every positive integer n. In conjunction with (7.75) this means that if n is odd we must have $f_{nj}/f_j \equiv \pm 1 \pmod{2d_j}$, while if n is even we must have $f_{nj}/f_j \equiv \pm 1 + d_j \pmod{2d_j}$. In other words:

$$\frac{f_{nj}}{f_j} \equiv \begin{cases} 1 \pmod{2d_j} & \text{if } n \equiv 1 \pmod 6\ , \\ -1 + d_j \pmod{2d_j} & \text{if } n \equiv 2 \pmod 6\ , \\ 1 + d_j \pmod{2d_j} & \text{if } n \equiv 4 \pmod 6\ , \\ -1 \pmod{2d_j} & \text{if } n \equiv 5 \pmod 6\,,. \end{cases} \tag{7.76}$$

Putting these results together we conclude

$$\begin{aligned} \frac{f_{nj}d_{nj}(1+d_{nj})}{f_j d_j} &\equiv \begin{cases} n(1+nd_j) \pmod{2d_j} & \text{if } n \equiv 1 \pmod 6\ , \\ (-1+d_j)(-n+d_j)(1+d_j(-n+d_j)) \pmod{2d_j} & \text{if } n \equiv 2 \pmod 6\ , \\ (1+d_j)(n+d_j)(1+d_j(n+d_j)) \pmod{2d_j} & \text{if } n \equiv 4 \pmod 6\ , \\ n(1-nd_j)) \pmod{2d_j} & \text{if } n \equiv 5 \pmod 6\,, \end{cases} \\ &\equiv n(1+d_j) \pmod{2d_j}\ . \end{aligned} \tag{7.77}$$

Suppose, on the other hand, that d_j is even. Then it follows from Theorem 4.9 and Lemma 4.10 that

$$\frac{d_{nj}}{d_j} = \frac{T_n^*(d_j)}{d_j} \equiv \begin{cases} n + \left(\frac{n(n-1)}{6}\right) d_j \pmod{2d_j} & \text{if } n \equiv 1 \pmod 3\,, \\ -n + \left(\frac{n(n+1)}{6}\right) d_j \pmod{2d_j} & \text{if } n \equiv 2 \pmod 3\ , \end{cases}$$

$$\equiv \begin{cases} n \pmod{2d_j} & \text{if } n \equiv 1,4 \pmod{12}\ , \\ -n + d_j \pmod{2d_j} & \text{if } n \equiv 2,5 \pmod{12}\ , \\ n + d_j \pmod{2d_j} & \text{if } n \equiv 7,10 \pmod{12}\ , \\ -n \pmod{2d_j} & \text{if } n \equiv 8,11 \pmod{12}\ , \end{cases} \tag{7.78}$$

and

$$\begin{aligned} \frac{f_{nj}}{f_j} = U_n^*(d_j) &\equiv \begin{cases} 1 + \left(\frac{n-1}{3}\right) d_j \pmod{2d_j} & \text{if } n \equiv 1 \pmod 3\,, \\ -1 + \left(\frac{n+1}{3}\right) d_j \pmod{2d_j} & \text{if } n \equiv 2 \pmod 3\,, \end{cases} \\ &\equiv \begin{cases} 1 \pmod{2d_j} & \text{if } n \equiv 1,7 \pmod{12}\ , \\ -1 + d_j \pmod{2d_j} & \text{if } n \equiv 2,8 \pmod{12}\ , \\ 1 + d_j \pmod{2d_j} & \text{if } n \equiv 4,10 \pmod{12}\ , \\ -1 \pmod{2d_j} & \text{if } n \equiv 5,11 \pmod{12}\,. \end{cases} \end{aligned} \tag{7.79}$$

Combining these results we find

$$\begin{aligned} \frac{f_{nj} d_{nj}(1+d_{nj})}{f_j d_j} &\equiv \begin{cases} n(1+nd_j) \pmod{2d_j} & \text{if } n \equiv 1 \pmod{12}\,, \\ (-n+d_j)(-1+d_j)(1+d_j(-n+d_j)) \pmod{2d_j} & \text{if } n \equiv 2 \pmod{12}\ , \\ n(1+d_j)(1+nd_j) \pmod{2d_j} & \text{if } n \equiv 4 \pmod{12}\ , \\ (n-d_j)(1+d_j(-n+d_j)) \pmod{2d_j} & \text{if } n \equiv 5 \pmod{12}\ , \\ (n+d_j)(1+d_j(n+d_j)) \pmod{2d_j} & \text{if } n \equiv 7 \pmod{12}\ , \\ n(1-d_j)(1-nd_j) \pmod{2d_j} & \text{if } n \equiv 8 \pmod{12}\ , \\ (n+d_j)(1+d_j)(1+d_j(n+d_j)) \pmod{2d_j} & \text{if } n \equiv 10 \pmod{12}\ , \\ n(1-nd_j) \pmod{2d_j} & \text{if } n \equiv 11 \pmod{12}\,, \end{cases} \\ &\equiv \begin{cases} n(1+d_j) \pmod{2d_j} & \text{if } n \equiv \pm 1, \pm 4 \pmod{12}\ , \\ n(1+d_j) + d_j \pmod{2d_j} & \text{if } n \equiv \pm 2, \pm 5 \pmod{12}\ , \end{cases} \end{aligned} \tag{7.80}$$

□

Proof of Theorem 7.24. The fact that t' is admissible is immediate. Referring to Definition 1.30 we see

$$\phi_{\kappa\mathbf{p}}(t') = (-1)^{s_{d_{nj}}(\kappa\mathbf{p})} e^{-\frac{\pi i}{12}\Psi(A_{t'})} \xi_{d_{nj}}^{-\frac{f_{nj}}{f} Q(\kappa\mathbf{p})} \tag{7.81}$$

where f is the conductor of Q. We first show

$$(-1)^{s_{d_{nj}}(\kappa\mathbf{p})} = (-1)^{n+1}(-1)^{n s_{d_j}(\mathbf{p})}. \tag{7.82}$$

Indeed, if d_j is odd then it follows from Lemma 4.11 that d_{nj} is odd, implying

$$(-1)^{s_{d_{nj}}(\kappa\mathbf{p})} = -1 = (-1)^{n+1}(-1)^{n s_{d_j}(\mathbf{p})}. \tag{7.83}$$

On the other hand if d_j is even then it follows from lemmas 4.10 and 4.11 that d_{nj} is even and $\kappa = T_n^*(d_j)/d_j \equiv n \pmod 2$, implying

$$(-1)^{s_{d_{nj}}(\kappa\mathbf{p})} = (-1)^{(1+np_1)(1+np_2)} = (-1)^{n+1}(-1)^{n(1+p_1)(1+p_2)} = (-1)^{n+1}(-1)^{n s_{d_j}(\mathbf{p})}. \tag{7.84}$$

Turning to the second factor on the right hand side of (7.81), observe that it follows from Theorem 4.53 that

$$A_{t'} = \chi_Q(\varepsilon^{3nj}) = A_t^n \tag{7.85}$$

and

$$\mathrm{Tr}(A_t) = \mathrm{Tr}(\varepsilon^{3j}) = d_{3j} - 1 > 1. \tag{7.86}$$

Lemma 5.1 consequently implies

$$e^{-\frac{\pi i}{12}\Psi(A_{t'})} = e^{-\frac{\pi i}{12}\Psi(A_t^n)} = e^{-\frac{n\pi i}{12}\Psi(A_t)}. \tag{7.87}$$

Finally, using Lemma 7.25, the last factor on the right hand side of (7.81) becomes

$$\begin{aligned}
\xi_{d_{nj}}^{-\frac{f_{nj}}{f}Q(\kappa\mathbf{p})} &= e^{-\left(\frac{\pi i}{d_j}\right)\left(\frac{f_{nj}d_{nj}(1+d_{nj})}{d_j f_j}\right)\left(\frac{f_j}{f}Q(\mathbf{p})\right)} \\
&= \begin{cases} e^{-\left(\frac{\pi i}{d_j}\right)(n(1+d_j)+d_j)\left(\frac{f_j}{f}Q(\mathbf{p})\right)} & \text{if } d_j \text{ is even and } n \equiv \pm 2 \text{ or } \pm 5 \pmod{12} \\ e^{-\left(\frac{\pi i}{d_j}\right)(n(1+d_j))\left(\frac{f_j}{f}Q(\mathbf{p})\right)} & \text{otherwise} \end{cases} \\
&= \begin{cases} (-1)^{\frac{f_j}{f}Q(\mathbf{p})}\xi_{d_j}^{-\frac{nf_j}{f}Q(\mathbf{p}} & \text{if } d_j \text{ is even and } n \equiv \pm 2 \text{ or } \pm 5 \pmod{12} \\ \xi_{d_j}^{-\frac{nf_j}{f}Q(\mathbf{p}} & \text{otherwise} \end{cases}
\end{aligned} \tag{7.88}$$

It follows from Lemma 5.3 that if d_j is even then

$$(-1)^{\frac{f_j}{f}Q(\mathbf{p})} = (-1)^{p_1^2+p_1p_2+p_2^2} = (-1)^{n+1}(-1)^{n+(1+p_1)(1+p_2)}, \tag{7.89}$$

Hence

$$\xi_{d_{nj}}^{-\frac{f_{nj}}{f}Q(\kappa\mathbf{p})} = (-1)^{n+1}(-1)^{l(\mathbf{p})}\xi_{d_j}^{-\frac{nf_j}{f}Q(\mathbf{p})}. \tag{7.90}$$

Combining these results we deduce

$$\phi_{\kappa\mathbf{p}}(t') = (-1)^{l(\mathbf{p})}(-1)^{ns_d(\mathbf{p})}e^{-\frac{n\pi i}{12}\Psi(A_t)}\xi_{d_j}^{-\frac{nf_j}{f}Q(\mathbf{p})} = (-1)^{l(\mathbf{p})}\left(\phi_{\mathbf{p}}(t)\right)^n. \tag{7.91}$$

Using (7.85), together with the fact that $\rho_{t'} = \rho_{Q,+} = \rho_t$ (see Definition 1.32) we also find

$$\mathfrak{w}_{A_{t'}}^{d_{nj}^{-1}\kappa\mathbf{p}}(\rho_{t'}) = \mathfrak{w}_{A_t^n}^{d_j^{-1}\mathbf{p}}(\rho_t) \tag{7.92}$$

It follows from (1.27) that, for all $\tau \in \mathbb{H}$,

$$\begin{aligned}
\mathfrak{w}_{A_t^n}^{d_j^{-1}\mathbf{p}}(\tau) &= \frac{\varpi\left(\left\langle\left\langle d_j^{-1}\mathbf{p}, A_t^n\tau\right\rangle\right\rangle, A_t^n\tau\right)}{\varpi\left(\left\langle\left\langle d_j^{-1}\mathbf{p}, \tau\right\rangle\right\rangle, \tau\right)} \\
&= \frac{\varpi\left(\left\langle\left\langle d_j^{-1}\mathbf{p}, A_t^n\tau\right\rangle\right\rangle, A_t^n\tau\right)}{\varpi\left(\left\langle\left\langle d_j^{-1}\mathbf{p}, A_t^{n-1}\tau\right\rangle\right\rangle, A_t^{n-1}\tau\right)} \times \cdots \times \frac{\varpi\left(\left\langle\left\langle d_j^{-1}\mathbf{p}, A_t\tau\right\rangle\right\rangle, A_t\tau\right)}{\varpi\left(\left\langle\left\langle d_j^{-1}\mathbf{p}, \tau\right\rangle\right\rangle, \tau\right)}
\end{aligned} \tag{7.93}$$

Taking the limit as $\tau \to \rho_t$ and using the fact that ρ_t is a fixed point of A_t we deduce

$$\mathfrak{w}_{A_{t'}}^{d_{nj}^{-1}\kappa\mathbf{p}}(\rho_{t'}) = \left(\mathfrak{w}_{A_t}^{d_j^{-1}\mathbf{p}}(\rho_t)\right)^n. \tag{7.94}$$

Hence

$$\tilde{\nu}_{\kappa\mathbf{p}}(t') = \phi_{\kappa\mathbf{p}}(t')\mathfrak{w}_{A_{t'}}^{d_{nj}^{-1}\kappa\mathbf{p}}(\rho_{t'}) = (-1)^{l(\mathbf{p})}\left(\phi_{\mathbf{p}}(t)\right)^n\left(\mathfrak{w}_{A_t}^{d_j^{-1}\mathbf{p}}(\rho_t)\right)^n = (-1)^{l(\mathbf{p})}\left(\tilde{\nu}_{\mathbf{p}}(t)\right)^n \tag{7.95}$$

It follows from Corollary 4.22 and Lemma 4.4 that

$$\frac{\tilde{\mu}_{\kappa\mathbf{p}}(t')}{(\tilde{\mu}_{\mathbf{p}}(t))^n} = q\left(\frac{\tilde{\nu}_{\kappa\mathbf{p}}(t')}{(\tilde{\nu}_{\mathbf{p}}(t))^n}\right), \qquad \frac{\mu_{\kappa\mathbf{p}}(s')}{(\mu_{\mathbf{p}}(s))^n} = q\left(\frac{\nu_{\kappa\mathbf{p}}(s')}{(\nu_{\mathbf{p}}(s))^n}\right), \tag{7.96}$$

where

$$q = \begin{cases} \frac{(d_j+1)^{\frac{n}{2}}}{d_{\frac{nj}{2}}-1} & n \equiv 0 \pmod 2, \\ \frac{(d_j+1)^{\frac{n-1}{2}}}{1+\sum_{r=1}^{\frac{n-1}{2}}(-1)^r d_{rj}} & n \equiv 1 \pmod 4, \\ \frac{(d_j+1)^{\frac{n-1}{2}}}{2+\sum_{r=1}^{\frac{n-1}{2}}(-1)^r d_{rj}} & n \equiv 1 \pmod 4. \end{cases} \tag{7.97}$$

The fact that $q \in \mathbb{Q}$ means we can use Lemma 1.45 in conjunction with Eqs. (7.95) and (7.96) to deduce

$$\frac{\nu_{\kappa\mathbf{p}}(s')}{(\nu_{\mathbf{p}}(s))^n} = q^{-1} g\left(\frac{\tilde{\mu}_{\kappa GH_g^{-1}G^{-1}\mathbf{p}}(t')}{\left(\tilde{\mu}_{GH_g^{-1}G^{-1}\mathbf{p}}(t)\right)^n}\right) = g\left(\frac{\tilde{\nu}_{\kappa GH_g^{-1}G^{-1}\mathbf{p}}(t')}{\left(\tilde{\nu}_{GH_g^{-1}G^{-1}\mathbf{p}}(t)\right)^n}\right) = (-1)^{l(GH_g^{-1}G^{-1}\mathbf{p})} \tag{7.98}$$

It remains to show

$$(-1)^{l(GH_g^{-1}G^{-1}\mathbf{p})} = (-1)^{l(\mathbf{p})} \tag{7.99}$$

The statement is immediate if d_j is odd, since then $l(\mathbf{p}) = n+1$ independently of $\mathbf{p}$. Suppose, on the other hand, that d_j is even. Let

$$M = GH_g^{-1}G^{-1} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}. \tag{7.100}$$

The fact that $M \in \mathrm{GL}_2(\mathbb{Z}/2d_j\mathbb{Z})$ means $\det M$ is odd. It also means that at least one of α, γ, and at least one of β, δ must be odd, implying $(1+\alpha)(1+\gamma)$ and $(1+\beta)(1+\delta)$ are both even. Hence

$$\begin{aligned} (-1)^{(1+(M\mathbf{p})_1)(1+(M\mathbf{p})_2)} &= (-1)^{1+(\alpha p_1+\beta p_2)+(\gamma p_1+\delta p_2)+(\alpha p_1+\beta p_2)(\gamma p_1+\delta p_2)} \\ &= (-1)^{1+(\alpha+\gamma+\alpha\gamma)p_1+(\beta+\delta+\beta\delta)p_2+(\alpha\delta+\beta\gamma)p_1p_2} \\ &= (-1)^{1+p_1+p_2+(1+\alpha)(1+\gamma)p_1+(1+\beta)(1+\delta)p_2+\det(M)p_1p_2} \\ &= (-1)^{(1+p_1)(1+p_2)}. \end{aligned} \tag{7.101}$$

Equation (7.99) now follows. Hence

$$\nu_{\kappa\mathbf{p}}(s') = (-1)^{l(\mathbf{p})}\,(\nu_{\mathbf{p}}(s))^n. \tag{7.102}$$

□

8. Necromancy and numerical computation

Suppose one wishes to use the preceding conjectures for constructing ghosts to compute an *explicit* r-SIC fiducial, either exactly or just a numerical approximation. We call any procedure for doing so *necromancy*, so-named because it "reanimates" the ghost fiducial as a r-SIC fiducial. In this section, we describe a method for necromancy specialized to 1-SICs.

There is a straightforward brute-force algorithm to achieve necromancy. Using (1.46), we first compute a ghost fiducial to arbitrary precision. We wish to round this numerical approximation into the closest point in a candidate number field to identify an exact representation of the ghost fiducial. Powerful tools with polynomial runtimes such as the Lenstra-–Lenstra—Lovász (LLL) lattice basis

reduction algorithm or other integer relation algorithms can be employed here, though we note that finding a closest vector in a lattice is not believed to be efficient in general. A conjecture for the specific number field is provided by the existing conjectures [13, 71, 72]. Then a Galois automorphism that flips the sign of $\sqrt{\Delta_0}$ can be applied to compute the 1-SIC fiducial. If the conjectures are correct, then with enough starting precision and patience for finding the exact representation, the result should be an exact expression for a 1-SIC fiducial. This exact expression can then be evaluated to any precision that one likes for numerical approximation.

Unfortunately this approach is impractical for two reasons. The first difficulty is that the relevant number field typically has very high degree, and the precision required to round into this field would therefore be impractically large for even storing a 1-SIC fiducial for modestly large d. Second, the convergence of LLL or similar algorithms is either far too slow in practice with such high-degree number fields or yields too weak a guarantee on accuracy with the "true" closest point to allow a direct computation of a ghost in this fashion.

To circumvent these difficulties, we now describe an alternative heuristic approach to necromancy that avoids the complexity bottleneck by working entirely in a (typically much lower degree) ring class field. One still requires very high precision already for moderately large dimensions. For example, we required $\sim 10^5$ digit precision in dimension $d = 100$ to implement this approach in detail. However, this is not impractically large for a modern laptop. The price for this reduced complexity is that the method itself is more involved.

We stress that the procedure for necromancy discussed in this section is at present only a heuristic, even assuming our conjectures. However, we believe it should be possible to specify a complete algorithm which provably converges to a 1-SIC assuming only our conjectures. It is likely that the methods here extend to r-SICs for $r > 1$, but we have not attempted to systematically approach numerical computation for $r > 1$, so we leave this case to future work and focus on 1-SICs for the rest of this section.

Let us first provide a high-level overview of our method of necromancy. The first step is to calculate a numerical estimate of a ghost fiducial associated to an admissible tuple $t = (d, 1, Q)$. In Section 8.2 we show how this can be done using the integral representation of the double sine function [70, 93]. It is not practical to use numerical integration to achieve the high precision required by the subsequent steps. We therefore use it to calculate an initial, low precision fiducial, and then amplify its precision using Newton's method, as described in Section 8.3. We then describe in Section 8.4 how to (numerically) compute a set of invariants that we call *ghost invariants*. The exact versions of these ghost invariants conjecturally live in the ring class field H_t associated to t (recall Definition 7.13). Since this is a field extension with substantially lower degree than the field containing the ghost overlaps, we can find an exact representation of the ghost invariants without too much difficulty using an integer relation algorithm. Importantly, the ghost invariants contain enough information about the original ghost overlaps to reconstruct them up to an action of the Galois group. Thus, as we show in Section 8.5, we can find exact Galois conjugates for the ghost invariants and from them obtain the subsequent "SIC invariants". The SIC invariants are at this point specified as exact numbers in a number field, but to make the remaining steps computationally tractable, we again resort to numerical approximations after the conversion step of passing from ghost to SIC. Notably, we no longer need the ultra-high precision required in the initial rounding step. From the SIC invariants, we can numerically reconstruct the SIC overlaps, again up to an action of the Galois group. While in principle we can do this on each separate Galois orbit and then combine the results, we can apply an additional heuristic to avoid having to match Galois actions across multiple orbits. In Section 8.6 we describe how a convex optimization on a single

maximal orbit, in every case tried, avoids the need to search for the unknown Galois action across multiple orbits. The output of this procedure is a 1-SIC fiducial vector of moderate precision; to gain confidence that this is a true 1-SIC fiducial vector, one can again use Newton's method to enhance the precision to any desired level.

8.1. **Numerical calculations.** We have implemented the necromancy method described here in Julia [40]. Using this implementation, we have calculated numerical approximations to all of the 1-SICs in every dimension up to $d = 20$ with the exception of the 1-SIC in $d = 12$ which has F_a symmetry. We have not yet implemented necromancy for the F_a-symmetric case because of how the Galois group structure is presently computed in our software. However, including F_a orbits should be a relatively straightforward extension that we hope to implement soon.

To see if we could achieve a moderately large dimension with our approach, we also used this algorithm to compute four numerical 1-SICs in dimension $d = 100$, three of which are new. This was somewhat challenging computationally, and it seems likely that our current ideas will need refinement to allow computation of a 1-SIC in, say, $d = 1000$.

The only required input to the `necromancy` function is an admissible tuple $(d, 1, Q)$, and in principle this function requires no fine-tuning to output a 1-SIC. As a practical matter however, the bottleneck in extending our current implementation to more dimensions is the convergence of the integer relation algorithm. The efficacy of the method hinges on convergence to the correct element of the ring class field for every ghost invariant. We find in practice that this is challenging to achieve within our current heuristics. We hope to improve the speed, convergence, and generality of this code (in particular to F_a orbits and $r > 1$) in future versions.

Throughout the remainder of this section, we are implicitly working with a fixed admissible tuple $t = (d, 1, Q)$. We further assume that the twist $G = I$, so that the fiducial datum is $(d, 1, Q, I, g)$ for some g. To ease notation, nowhere in this section do we explicitly label the dependence on t or s.

8.2. **Calculating the Shintani–Faddeev modular cocycle.** The first step in our necromancy method is to compute a ghost fiducial vector. In Definitions 1.32, 1.44 a ghost fiducial corresponding to the admissible tuple $t = (d, r, Q)$ is expressed in terms of the SF modular cocycle $\mathfrak{w}_{A_t}^{d^{-1}\mathbf{P}}(\rho_t)$. This in turn is expressed in terms of the SF Jacobi cocycle $\sigma_A(z, \tau)$ via (1.26). For $\tau \in \mathbb{H}$ the latter is given by a ratio of q-Pochhammer symbols via (1.21). However, we need its values for $\tau \in \mathbb{R}$. Although these can be obtained by taking a limit, it is numerically more efficient to calculate them directly, via an integral representation, using a procedure we now describe.

Let $L = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ be arbitrary. If $\gamma = 0$ then either $L = T^k$, in which case $\sigma_L(z, \tau) = 1$ for all z, τ, or $L = -T^k$, in which case the function is singular for all $\tau \in \mathbb{R}$. If $\gamma < 0$ we can express σ_L in terms of $\sigma_{L^{-1}}$. It is therefore sufficient to give a procedure for calculating the function when $\gamma > 0$. For this we use Theorem C.4 to deduce the existence of a sequence of integers $r_1, \ldots, r_{n+1}$ such that

$$L = T^{r_1} S \ldots S T^{r_{n+1}} \tag{8.1}$$

where $r_j \geq 2$ for $1 < j < n + 1$. The theorem also shows that if $L_j = T^{r_j} S \ldots S T^{r_{n+1}}$ then $\mathcal{D}_L = \mathcal{D}_{L_1} \subset \mathcal{D}_{L_2} \cdots \subset \mathcal{D}_{L_{n+1}}$. Consequently

$$\sigma_L(z, \tau) = \sigma_{T^{r_1} S}\left(\frac{z}{j_{L_2}(\tau)}, L_2 \tau\right) \ldots \sigma_{T^{r_n} S}\left(\frac{z}{j_{L_{n+1}}(\tau)}, L_{n+1} \tau\right) \sigma_{L_{n+1}}(z, \tau) \tag{8.2}$$

for all $\tau \in \mathcal{D}_L$. Using

$$\sigma_{L_{n+1}}(\tau, z) = \sigma_{T^{r_{n+1}}}(z, \tau) = 1 \tag{8.3}$$

and

$$\sigma_{T^m S}(z,\tau) = \sigma_{T^m}\left(\frac{z}{j_S(\tau)}, S\tau\right)\sigma_S(z,\tau) = \sigma_S(z,\tau) \tag{8.4}$$

this becomes

$$\sigma_L(z,\tau) = \sigma_S\left(\frac{z}{j_{L_2}(\tau)}, L_2\tau\right)\ldots\sigma_S\left(\frac{z}{j_{L_{n+1}}(\tau)}, L_{n+1}\tau\right). \tag{8.5}$$

for all $\tau \in \mathcal{D}_L$. The problem thus reduces to calculating $\sigma_S(z,\tau)$. This can be done using the formula [70, 93]

$$\sigma_S(z,\tau) = \frac{e^{\frac{\pi i}{12\tau}\left(6z^2+6(1-\tau)z+\tau^2-3\tau+1\right)}}{\mathrm{Sin}_2(z+1,\tau)} \tag{8.6}$$

where $\mathrm{Sin}_2(z+1,\tau)$ is the double sine function. Note that the double sine function as usually defined has three arguments; we are employing the shorthand [70] $\mathrm{Sin}_2(z,\tau,1) = \mathrm{Sin}_2(z,\tau)$. Note also that we are using the definition of Shintani [93] and Kurokawa and Koyama [75] which is prevalent in the mathematics literature, as opposed to the definition of Ponsot [82] which is more prevalent in the physics literature. We can calculate $\mathrm{Sin}_2(z+1,\tau)$ explicitly using the integral representation [70, 82],

$$\mathrm{Sin}_2(z+1,\tau) = \exp\left(-\int_0^\infty\left(\frac{\sinh\left(\frac{\tau-1-2z}{2}\right)t}{2\sinh\left(\frac{t}{2}\right)\sinh\left(\frac{\tau t}{2}\right)} - \frac{\tau-1-2z}{\tau t}\right)\frac{dt}{t}\right) \tag{8.7}$$

valid for $\mathrm{Re}(\tau) > 0$ and $-1 < \mathrm{Re}(z) < \mathrm{Re}(\tau)$. To use this in Eq. (8.5) one needs, firstly, that $\mathrm{Re}(L_r\tau) > 0$ for $r = 2, \ldots, n+1$. A sufficient condition for that to be true is that $\mathrm{Re}(j_L(\tau)) > 0$. In particular, it is true for the case that interests us, $\tau \in \mathcal{D}_L \cap \mathbb{R}$. Indeed, let $\tau = x + iy$ with x, $y \in \mathbb{R}$. Then, in the notation of Theorem C.4, $\mathrm{Re}(j_L(\tau)) > 0$ implies $x + m_r/l_r > 0$ for $r = 2,$, $n+1$ and, consequently,

$$\begin{aligned}\mathrm{Re}\left(L_r\tau\right) &= \begin{cases}\frac{\gamma_r}{\gamma_{r+1}}\left(\frac{\left(x+\frac{\delta_r}{\gamma_r}\right)\left(x+\frac{\delta_{r+1}}{\gamma_{r+1}}\right)+y^2}{\left(x+\frac{\delta_{r+1}}{\gamma_{r+1}}\right)^2+y^2}\right) & r = 2,\ldots,n\\ \gamma_{n+1}\left(x+\frac{\delta_{n+1}}{\gamma_{n+1}}\right) & r = n+1\end{cases}\\ &> 0\end{aligned} \tag{8.8}$$

To deal with the problem that $\mathrm{Re}\left(z/j_{L_r}(\tau)\right)$ may not be in the required interval we may use the fact

$$\sigma_S(z+m_1\tau+m_2,\tau) = \frac{\varpi_{m_1}(z,\tau)}{\varpi_{-m_2}\left(\frac{z}{\tau},-\frac{1}{\tau}\right)}\sigma_S(z,\tau) \tag{8.9}$$

for all m_1, $m_2 \in \mathbb{Z}$ and all $\tau \in \mathcal{D}_S$.

If we can calculate one 1-SIC on a given extended Clifford group orbit we can easily calculate all the others by applying the appropriate unitary or anti-unitary. To make the most efficient use of available resources one should choose the quadratic form Q appearing in the admissible tuple $t = (d, 1, Q)$ in such a way as to minimize the length of the expansion in Eq. (8.1). It follows from Theorem C.7 that to do this we need to choose Q to be HJ-reduced and such that the HJ-continued fraction expansion of $\beta_{Q,+}$ has minimal period. The HJ-reduced continued fraction then tells us the integers $r_1, \ldots, r_{n+1}$ in the expansion in Eq. (8.1) (see Appendix C for the definitions and a summary of the relevant properties of HJ-reduced forms and HJ-continued fractions). Appropriate choices of Q are tabulated in Appendix F for $d = 4$ to 100.

8.3. **Precision enhancement with Newton's method.** The method described below does not require us to calculate the full set of d^2 ghost overlaps. It does, however, require us to calculate a subset of size $\gg d\log(d)^c$ for some absolute constant c. To convert this subset into the corresponding subset of SIC overlaps requires the ghost overlaps to be calculated to very high precision (10^5 digit precision in dimension 100). Doing this using Eq. (8.7) would be prohibitively slow. We therefore use the alternative method we now describe.

Lemma 8.1. *Let $\tilde{\Pi}$ be a ghost 1-SIC fiducial. Then there exists $|\psi\rangle \in \mathcal{L}(\mathbb{C}^d)$ such that*

$$\tilde{\Pi} = \lambda|\psi\rangle\langle\psi|U_P \tag{8.10}$$

where $\lambda = \langle\psi|U_P|\psi\rangle = \pm 1$.

Remark. We will refer to $|\psi\rangle$ as the ghost SIC fiducial vector.

Proof. The fact that $\tilde{\Pi}$ is rank 1 means we can write it in the form

$$\tilde{\Pi} = |\psi\rangle\langle\phi| \tag{8.11}$$

for some pair of vectors satisfying $\langle\phi|\psi\rangle = 1$. The fact that $\tilde{\Pi}_s$ is a P-projector (see Definition 1.13 and discussion following) means

$$|\phi\rangle\langle\psi| = (|\psi\rangle\langle\phi|)^\dagger = U_P|\psi\rangle\langle\phi|U_P \qquad \Longrightarrow \qquad |\phi\rangle = \left(\frac{\langle\phi|U_P|\psi\rangle}{\langle\psi|\psi\rangle}\right) U_P|\psi\rangle. \tag{8.12}$$

So

$$\tilde{\Pi} = \lambda|\psi\rangle\langle\psi|U_P \tag{8.13}$$

for some λ. The fact that $\mathrm{Tr}(\tilde{\Pi}) = 1$ means $\lambda\langle\psi|U_P|\psi\rangle = 1$. Our freedom to make the replacements $|\psi\rangle \to \sqrt{|\lambda|}|\psi\rangle$ and $\lambda \to \lambda/|\lambda|$ means we can choose λ, $|\psi\rangle$ so that $\lambda = \langle\psi|U_P|\psi\rangle = \pm 1$. □

Expressed in terms of the ghost SIC fiducial vector Eq. (1.53) becomes

$$\lambda|\psi\rangle\langle\psi|U_P = \frac{1}{d}\sum_{\mathbf{p}} \tilde{\mu}_{\mathbf{p}} D_{\mathbf{p}}. \tag{8.14}$$

(setting $G = I$, and dropping the t-label). The simplest case is when none of the components of $|\psi\rangle$ is zero. In that case, in order to calculate the $2d-2$ real numbers determining the complex vector $|\psi\rangle$ (up to an overall constant) it suffices to know $2d$ of the numbers $\tilde{\mu}_{\mathbf{p}}$. Specifically, let

$$\chi_{0,j} = \frac{1}{d}\sum_{k=0}^{d-1} \omega_d^{jk}\tilde{\mu}_{0,k}, \qquad\qquad \chi_{1,j} = \frac{1}{d}\sum_{k=0}^{d-1} \xi_d^k\omega_d^{jk}\tilde{\mu}_{1,k}. \tag{8.15}$$

The vector $|\psi\rangle$ is only determined up to an arbitrary phase. We may therefore assume, without loss of generality, that $\langle 0|\psi\rangle$ is positive real. We then have

$$\langle j|\psi\rangle = \sqrt{|\chi_{0,0}|}\prod_{k=0}^{j-1}\left(\frac{\chi_{1,k}}{\chi_{0,k}}\right), \tag{8.16}$$

with the convention that $\prod_{k=0}^{-1} f(k) = 1$. Our strategy is therefore to calculate low precision approximations to the $2d$ numbers $\tilde{\mu}_{0,k}$, $\tilde{\mu}_{1,k}$ using the integral representation and then use these to

calculate a low precision approximation to the vector $|\psi\rangle$. We then apply Newton's method to the system of equations

$$\langle\psi|U_P D_{\mathbf{p}}|\psi\rangle\langle\psi|U_P D_{-\mathbf{p}}|\psi\rangle = \frac{d\delta^{(d)}_{\mathbf{p},\mathbf{0}} + 1}{d+1} \tag{8.17}$$

to calculate a high precision approximation to $|\psi\rangle$ which in turn can be used to calculate high precision approximations to the numbers $\tilde{\mu}_{\mathrm{p}}$. If it should happen that one or more of the components of $|\psi\rangle$ is zero then it may be necessary to calculate more than $2d$ low precision ghost overlaps. However in no case is it necessary to calculate the numerical integral to high precision.

8.4. **Ghost invariants.** We next describe our method for constructing a set of numbers in the ring class field $H := H_t$ which fully specify the ghost overlaps defined from the admissible tuple t on a maximal Galois orbit.

The method relies on the following empirical observation[8]:

Empirical Observation 8.2. *If $\tilde{E}$ is the field generated by the ghost overlaps, and if H is the ring class field, then there is an isomorphism of $\mathrm{Gal}(\tilde{E}/H)$ onto $\mathcal{M}/\mathcal{S}$, where $\mathcal{S}$ is the symmetry group (i.e. the set of $G \in \mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ such that $\tilde{\mu}_{G\mathbf{p}} = \tilde{\mu}_{\mathbf{p}}$ for all $\mathbf{p}$) and $\mathcal{M}$ is a maximal abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ containing $\mathcal{S}$. If $h \in \mathrm{Gal}(\tilde{E}/H)$ and $F_h\mathcal{S}$ is the corresponding element of $\mathrm{GL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ then*

$$h(\tilde{\mu}_{\mathbf{p}}) = \tilde{\mu}_{F_h\mathbf{p}}. \tag{8.18}$$

for all $\mathbf{p}$.

Remark. This isomorphism was originally noted empirically by studying the known examples of 1-SICs [7, 11]. For a type z orbit there is only one maximal subgroup containing $\mathcal{S}$ (namely, the centralizer of $\mathcal{S}$). The characterization of $\mathcal{M}$ in the case of a type a orbits will appear in future work.

The key to our method is that using this isomorphism one can calculate the action of $\mathrm{Gal}(\tilde{E}/H)$ on the ghost overlaps without knowing them exactly.

Let $\tilde{\mu}_{\mathbf{p}_1}, \ldots, \tilde{\mu}_{\mathbf{p}_n}$ be a maximal orbit of ghost overlaps under the action of $\mathrm{Gal}(E/H)$. Suppose that each element of the maximal orbit generates the full field $\tilde{E}$, and therefore is not stabilized by a non-identity element of $\mathrm{Gal}(\tilde{E}/H)$. In the case of a maximal order, this provably follows from the Stark Conjectures (see Subsection 2.3); for non-maximal orders we heuristically assume it holds. Choose $L_1, \ldots, L_m \in \mathcal{M}$ such that

(1) Each $L_j\mathcal{S}$ is order $n_j = q_j^{r_j}$ in $\mathcal{M}/\mathcal{S}$ with q_j prime and r_j a positive integer,
(2) $\mathcal{M}/\mathcal{S}$ is isomorphic to the direct product $\langle L_1\mathcal{S}\rangle \times \cdots \times \langle L_m\mathcal{S}\rangle$.

Let $\tilde{h}_j$ be the element of $\mathrm{Gal}(\tilde{E}/H)$ such that

$$\tilde{h}_j(\tilde{\mu}_{\mathbf{p}}) = \tilde{\mu}_{L_j\mathbf{p}} \tag{8.19}$$

for all $\mathbf{p}$, and let $\tilde{E}_j = \{c \in \tilde{E} \colon \tilde{h}_k(c) = c \text{ for all } k \neq j\}$. Finally choose some fixed element of the orbit, say $\tilde{\mu}_{\mathbf{p}_1}$, and define

$$\tilde{\mu}_{s_1,\ldots,s_m} = \tilde{\mu}_{L_1^{s_1}\ldots L_m^{s_m}\mathbf{p}_1}. \tag{8.20}$$

[8]While we do not have a proof of this observation at present, we believe it can be proven from our broader framework of conjectures and hope to show this in an upcoming paper.

Then the map $(s_1, \ldots, s_m) \to \tilde{\mu}_{s_1,\ldots,s_m}$ is a bijective correspondence between $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$ and the orbit. If follows that if we define sets

$$\tilde{K}_{j,t} = \{\tilde{\mu}_{s_1,\ldots,s_m} : s_j = t\} \tag{8.21}$$

then their intersection is the single-element set

$$\bigcap_{j=1}^{m} \tilde{K}_{j,t_j} = \{\tilde{\mu}_{t_1,\ldots,t_m}\}. \tag{8.22}$$

Let

$$\tilde{P}_{j,t}(x) = \prod_{\tilde{\mu} \in K_{j,t}} (x - \tilde{\mu}) = \sum_{l=0}^{n/n_j} \tilde{c}_{j,t,l} x^l. \tag{8.23}$$

Then the coefficients $\tilde{c}_{j,t,l}$ are all in $\tilde{E}_j$.[9] So one approach to the problem of calculating the SIC overlaps would be to calculate exact versions of the coefficients $\tilde{c}_{j,t,l}$ using an integer-relation algorithm, transform them using a $\sqrt{\Delta_0}$–sign switching automorphism, find the roots of the transformed polynomial, and then find the SIC overlaps using the transformed version of Eq. (8.22). Provided $m > 1$ this method would be more efficient than using an integer relation algorithm to calculate exact expressions for the $\tilde{\mu}_{\mathbf{p}}$ since $\tilde{E}_j$ is then lower degree than $\tilde{E}$. However, we can do better than that, by defining a set of numbers which are all in H, instead of $\tilde{E}_j$, and which are therefore easier to calculate from their numerical counterparts using an integer relation algorithm. We refer to these numbers as *ghost invariants*.

Our method relies on the fact

Lemma 8.3. *For each j there exists at least one index l such that the numbers $\{\tilde{c}_{j,t,l} : t = 0, 1, \ldots, n_j - 1\}$ are distinct non-zero. If l is such an index then $\tilde{E}_j = H(\tilde{c}_{j,0,l})$.*

Proof. Suppose there were no such index l. Since $\mathrm{Gal}(\tilde{E}_j/H) = \langle \tilde{h}_j \rangle$ is cyclic order n_j, where n_j is a power of a prime, and since $\tilde{c}_{j,t,l} = \tilde{h}_j^t(\tilde{c}_{j,0,l})$, it would follow that there existed a positive integer $r < n_j$ such that

$$\tilde{h}_j^r(\tilde{c}_{j,t,l}) = \tilde{c}_{j,t,l} \tag{8.24}$$

for all t, l. This in turn would mean $\tilde{K}_{j,t+r} = \tilde{K}_{j,t}$ for all t, contradicting the fact that these sets are disjoint.

To prove the second statement suppose $H(\tilde{c}_{j,0,l})$ was a proper subfield of $\tilde{E}_j$. Then it would be fixed by $\tilde{h}_j^r$, for some positive integer $r < n_j$. But that would mean $\tilde{c}_{j,r,l} = \tilde{c}_{j,0,l}$, contradicting the fact that the the coefficients are distinct. □

In view of Lemma 8.3 we can choose for each j an index l_j such that $\tilde{E}_j = H(\tilde{c}_{j,0,l_j})$. We then have, for each l a set of numbers $\tilde{a}_{j,r,l} \in H$ such that

$$\tilde{c}_{j,0,l} = \sum_{r=0}^{n_j-1} \tilde{a}_{j,r,l} \tilde{c}_{j,0,l_j}^r. \tag{8.25}$$

[9] In what follows we define $\tilde{c}_{j,t,l}$ to be (essentially) the elementary symmetric polynomials of the ghost overlaps. However, any basis of symmetric polynomials would suffice, and in our numerical calculations we have used power sums instead. Using power sums offers some computational advantages, but adds extra steps of changing bases to an already lengthy procedure, so we omit these details.

Repeatedly applying $\tilde{h}_j$ to both sides it follows

$$\begin{pmatrix} \tilde{c}_{j,0,l} \\ \vdots \\ \tilde{c}_{j,n_j-1,l} \end{pmatrix} = \tilde{V}_j \begin{pmatrix} \tilde{a}_{j,0,l} \\ \vdots \\ \tilde{a}_{j,n_j-1,l} \end{pmatrix} \tag{8.26}$$

where $\tilde{V}_j$ is the Vandermonde matrix

$$\tilde{V}_j = \begin{pmatrix} 1 & \tilde{c}_{j,0,l_j} & \cdots & \tilde{c}_{j,0,l_j}^{n_j-1} \\ \vdots & \vdots & & \vdots \\ 1 & \tilde{c}_{j,n_j-1,l_j} & \cdots & \tilde{c}_{j,n_j-1,l_j}^{n_j-1} \end{pmatrix} \tag{8.27}$$

In the case $l = l_j$ we also have

$$\tilde{c}_{j,1,l_j} = \sum_{r=0}^{n_j-1} \tilde{b}_{j,r} \tilde{c}_{j,0,l_j}^{r} \tag{8.28}$$

for some $\tilde{b}_{j,r} \in H$, from which it follows that

$$\begin{pmatrix} \tilde{c}_{j,1,l_j} \\ \vdots \\ \tilde{c}_{j,n_j-1,l_j} \\ \tilde{c}_{j,0,l_j} \end{pmatrix} = \tilde{V}_j \begin{pmatrix} \tilde{b}_{j,0} \\ \vdots \\ \tilde{b}_{j,n_j-1} \end{pmatrix} \tag{8.29}$$

Eq. (8.29) implies

$$\tilde{h}_j\big(\tilde{c}_{j,t,l_j}\big) = \tilde{Q}_j\big(\tilde{c}_{j,t,l_j}\big) \tag{8.30}$$

for all t, where

$$\tilde{Q}_j(x) = \sum_{u=0}^{n_j-1} \tilde{b}_{j,u} x^u \tag{8.31}$$

Following the terminology of ref. [10] we refer to the $\tilde{Q}_j(x)$ as *Galois polynomials*.

Numerical approximations to the numbers $\tilde{a}_{j,t,l}$, $\tilde{b}_{j,t}$ can be obtained from Eqs. (8.26), (8.29) by solving the linear system. Stable solution of Vandermonde linear systems can be done with only $O(n_j^2)$ operations [17,55].

Finally, define numbers $\tilde{e}_{j,t}$ by

$$\tilde{e}_{j,0} + \tilde{e}_{j,1} x + \cdots + \tilde{e}_{j,n_j-1} x^{n_j-1} + x^{n_j} = \prod_{t=0}^{n_j-1} (x - \tilde{c}_{j,t,l_j}) \tag{8.32}$$

The numbers $\tilde{a}_{j,t,l}$, $\tilde{b}_{j,t}$, $\tilde{e}_{j,t}$ are the ghost invariants we introduced earlier. They are all in the ring class field H, and exact versions can be calculated using an integer relation algorithm starting from high precision numerical approximations.

8.5. **Constructing the SIC overlaps.** Now let E be the field generated by the SIC overlaps, and let g be any automorphism which switches the sign of $\sqrt{\Delta_0}$. For the sake of simplicity assume $g(\omega_d) = \omega_d$ (although it is straightforward to construct a modified version of the argument which works when this condition is not satisfied). We have that g maps $\tilde{E}$ onto E, and that the map $h \mapsto ghg^{-1}$ is an isomorphism of $\mathrm{Gal}(\tilde{E}/H)$ onto $\mathrm{Gal}(E/H)$. Define

$$\Pi = g(\tilde{\Pi}), \quad \mu_{\mathbf{p}} = g(\tilde{\mu}_{\mathbf{p}}), \quad \mu_{s_1,\ldots,s_m} = g(\tilde{\mu}_{s_1,\ldots,s_m}) \quad c_{j,t,l} = g(\tilde{c}_{j,t,l}) \quad h_j = g\tilde{h}_j g^{-1} \tag{8.33}$$

where $\tilde{\Pi}$ is the ghost projector with which we started. Then Π is a 1-SIC projector, and $\mu_{\mathbf{p}} = \mathrm{Tr}(\Pi D^\dagger_{\mathbf{p}})$ are the corresponding SIC overlaps. Furthermore, it follows from Eqs. (8.19), (8.20) that

$$h_j(\mu_{\mathbf{p}}) = \mu_{L_j\mathbf{p}} \tag{8.34}$$

for all j, $\mathbf{p}$, and

$$\mu_{s_1,\ldots,s_m} = h_1^{s_1} \ldots h_m^{s_m}(\mu_{\mathbf{p}_1}) = \mu_{L_1^{s_1}\ldots L_m^{s_m}\mathbf{p}_1} \tag{8.35}$$

for all $s_1, \ldots, s_m$. Also define $K_{j,t}$ to be the set of roots of the equation

$$\sum_{l=0}^{n/n_j} c_{j,t,l} x^l = 0. \tag{8.36}$$

Then it follows from Eqs. (8.22) and (8.23) that

$$\bigcap_{j=1}^{m} K_{j,t_j} = \{\mu_{t_1,\ldots,t_m}\}. \tag{8.37}$$

Of course, the fact that we only have numerical approximations for $\tilde{\Pi}$, $\tilde{\mu}_{\mathbf{p}}$, and $c_{j,t,l}$ means that we cannot calculate Π, $\mu_{\mathbf{p}}$, $c_{j,t,l}$ directly. However, we do have exact expressions for the ghost invariants. Moreover, the fact that the ghost invariants are all in H means it is straightforward to calculate the corresponding *SIC invariants*

$$a_{j,t,l} = g(\tilde{a}_{j,t,l}), \qquad b_{j,t} = g(\tilde{b}_{j,t}), \qquad e_{j,t} = g(\tilde{e}_{j,t}). \tag{8.38}$$

The fact that one loses some information in going from the ghost fiducial to the ghost invariants means the SIC invariants do not specify Π unambiguously. However, they do contain enough information to enable us to construct a set of candidate operators, from which a set of 1-SIC fiducial projectors which includes Π can be extracted without too much difficulty, using the method we now describe.

Let

$$Q_j(x) = \sum_{u=0}^{n_j-1} b_{j,u} x^u. \tag{8.39}$$

Then

$$h_j\big(c_{j,t,l_j}\big) = Q_j\big(c_{j,t,l_j}\big) \tag{8.40}$$

We now find the c_{j,t,l_j} using the fact that they are the roots of the equation

$$\sum_{t=0}^{n_j-1} e_{j,t} x^t = 0. \tag{8.41}$$

The problem is, of course, that we do not *ab initio* know which particular root is equal to which particular coefficient c_{j,t,l_j}. To deal with this problem we choose a root at random, and label it $c'_{j,0,l_j}$. We then define c'_{j,t,l_j} recursively by

$$c'_{j,t+1,l_j} = Q_j\left(c'_{j,t,l_j}\right) \tag{8.42}$$

so that

$$c_{j,t,l_j} = c'_{j,t+r_j,l_j} \tag{8.43}$$

for all t, j and some unknown j-dependent constant r_j. We then extend the definition of $c'_{j,t,l}$ to arbitrary values of l by setting

$$c'_{j,t,l} = c_{j,t-r_j,l} \tag{8.44}$$

for all j, t, l. We then have

$$\begin{pmatrix} c'_{j,0,l} \\ \vdots \\ c'_{j,n_j-1,l} \end{pmatrix} = V'_j \begin{pmatrix} a_{j,0,l} \\ \vdots \\ a_{j,n_j-1,l} \end{pmatrix} \tag{8.45}$$

for all j, l, where

$$V'_j = \begin{pmatrix} 1 & c'_{j,0,l_j} & \dots & c'^{n_j-1}_{j,0,l_j} \\ \vdots & \vdots & & \vdots \\ 1 & c'_{j,n_j-1,l_j} & \dots & c'^{n_j-1}_{j,n_j-1,l_j} \end{pmatrix} \tag{8.46}$$

Equation (8.45) together with our knowledge of the c'_{j,t,l_j} and $a_{j,t,l}$ enables us to calculate $c'_{j,t,l}$ for all j, t, l

Now let $K'_{j,t}$ be the roots of the equation

$$\sum_{l=0}^{n/n_j} c'_{j,t,l} x^l = 0. \tag{8.47}$$

Then $K_{j,t} = K'_{j,t+r_j}$. In view of (8.37) this means that if we define $\mu'_{t_1,\dots,t_m}$ to be the unique member of the set

$$\bigcap_{j=1}^{m} K'_{j,t_j} \tag{8.48}$$

then $\mu_{t_1,\dots,t_m} = \mu'_{t_1+r_1,\dots,t_m+r_m}$ for all $t_1, \dots, t_m$.

Using the values of the $c'_{j,t,l}$, we can calculate the values of the quantities $\mu'_{t_1,\dots,t_m}$, which in turn fixes the quantities $\mu_{t_1,\dots,t_m}$ up to the unknown shifts $r_1, \dots, r_m$. It is convenient to re-phrase this slightly. Given an arbitrary element $\mathbf{p}$ of the $\mathcal{M}/\mathcal{S}$-orbit of $\mathbf{p}_1$, choose $t_1, \dots, t_m$ and $M \in \mathcal{M}$ such that $\mathbf{p} = L_1^{t_1} \dots L_m^{t_m} M \mathbf{p}_1$ and define

$$\mu'_{\mathbf{p}} = \mu'_{t_1,\dots,t_m}. \tag{8.49}$$

In view of (8.35) we then have

$$\mu_{\mathbf{p}} = \mu_{L_1^{t_1}\dots L_m^{t_m} M \mathbf{p}_1} = \mu_{L_1^{t_1}\dots L_m^{t_m} \mathbf{p}_1} = \mu_{t_1,\dots,t_m} = \mu'_{t_1+r_1,\dots,t_m+r_m} = \mu'_{L\mathbf{p}} \tag{8.50}$$

where

$$L = L^{r_1} \dots L^{r_m} \tag{8.51}$$

is an element of $\mathcal{M}/\mathcal{S}$, which we determine by trial-and-error.

There are two ways in which we can reduce the size of the search space. In the first place, if we only want *some* 1-SIC on the same $\mathrm{EC}(d)$ orbit as Π, not necessarily Π itself, we can use the fact that if $L'L^{-1} \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ then $\{\mu'_{L'\mathbf{p}}\}$ is a set of SIC overlaps if and only if $\{\mu'_{L\mathbf{p}}\}$ is. It is consequently only necessary to test one element from each coset $\mathcal{M}/\big(\mathcal{M} \cap \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})\big)$.

The search space can be further reduced using the following condition. Let $\mathcal{P}$ be the set $\{M\mathbf{p}_1 \colon M \in \mathcal{M}\}$, and define

$$B = \frac{1}{d} \sum_{\mathbf{p} \in \mathcal{P}} \mu_{\mathbf{p}} D_{\mathbf{p}} \tag{8.52}$$

The fact that $\mathcal{M}$ is maximal abelian means $-I \in \mathcal{M}$, which in turn implies B is Hermitian, and $\mathrm{Tr}(B(\Pi - B)) = 0$. Let $\lambda_{\max}$ be the largest eigenvalue of B. Then

$$\lambda_{\max} \geq \mathrm{Tr}(B\Pi) = \mathrm{Tr}(B^2) = \frac{|\mathcal{P}|}{d(d+1)} \tag{8.53}$$

where $|\mathcal{P}|$ is the cardinality of $\mathcal{P}$. We may therefore remove from consideration any set of candidate overlaps which do not satisfy this requirement.

8.6. **Convex optimization.** At this point, we have managed to construct an orbit of $\mathcal{M}$ acting on $\mathbf{p} \in (\mathbb{Z}/\bar{d}\mathbb{Z})^2$ and for which we know numerical approximations of the associated $\mu_{\mathbf{p}}$ up to a shift by the action of an unknown element $M \in \mathcal{M}$. In general, the group action of $\mathcal{M}$ will split the $\mathbf{p}$ into more than one orbit. In that case, the kth orbit can be learned in the above fashion. However, the unknown matrix shift will in general be different for each orbit, and must be guessed *simultaneously* across all orbits if one wishes to reconstruct all $d^2 - 1$ nontrivial values of $\mu_{\mathbf{p}}$. The total number of possibilities will in general grow exponentially in the number of orbits, which is an undesirably large search space. It might be that there are efficient ways to search this space, but we are not aware of any. We will instead describe an alternative method based on convex optimization that requires only knowing a single (correctly shifted) orbit of sufficient size.

Our idea is to use *low-rank matrix recovery*, which is a matrix analog of the better known method of compressive sensing. For simplicity, consider a square $d \times d$ matrix $X \in \mathcal{L}(\mathbb{C}^d)$. In the low-rank matrix recovery problem, one is given a collection of *measurements* $A_k \in \mathcal{L}(\mathbb{C}^d)$ and one learns the value of the *observations* b_k, which are linear functions $b_k = \mathrm{Tr}(A_k X)$ obtained by acting on an unknown matrix X. Written in a vector notation, we have $\mathbf{b} = \mathbf{A}(X)$ where the measurements are now a linear map $\mathbf{A} : \mathcal{L}(\mathbb{C}^d) \to \mathbb{C}^m$ and the observations are $\mathbf{b} \in \mathbb{C}^m$. One wishes to recover X from knowledge of measurements $\mathbf{A}$ and observations $\mathbf{b}$. If $m = d^2 = \mathrm{rank}(\mathbf{A})$, then the solution is trivially $X = \mathbf{A}^{-1}\mathbf{b}$.

Suppose that our measurements are expensive to implement, and we wish to recover X from $m \ll d^2$ observations, and hence $\mathrm{rank}(\mathbf{A}) \leq m$. In this case, it is clear that there is no unique solution since X and $X + Y$ are indistinguishable for nonzero Y in the null space of $\mathbf{A}$.

In many cases of interest, one has the additional knowledge that the unknown matrix X has rank $r \ll d$. One might hope that this fact would allow efficiently recovering X from far fewer measurements, despite the original problem being ill-posed. After all, information theoretically there are only $O(rd)$ parameters specifying X. This intuition turns out to be correct: it suffices to make $m = O\big(rd(\log d)^c\big)$ observations from a typical set of certain randomized measurements [51, 52], where c is an absolute constant. The algorithm which efficiently reconstructs X from only m observations is a convex relaxation of the naive algorithm that finds a minimal-rank matrix among

those consistent with the observations. The convex relaxation (which can be cast as a semidefinite program) returns the answer:

$$X^\star = \arg\min_Y \|Y\|_1 \text{ s.t. } \mathbf{A}(Y) = \mathbf{b}\,, \tag{8.54}$$

where $\|Y\|_1$ is the Schatten 1-norm, or the sum of the singular values of Y.

The final step in our necromancy procedure is now clear. Choose a specific large orbit $\mathcal{P}$ and reconstruct the $\mu_{\mathbf{p}}$ along that orbit, up to an unknown matrix $M \in \mathcal{M}$ using the methods above. In our examples, we have always chosen a maximal orbit, and in every case we've observed this orbit was unique and had a size many times larger than d. If our prior computations and conjectures are correct, then our unknown 1-SIC fiducial projector Π satisfies the following constraints

$$\mu_{M\mathbf{p}} = \mathrm{Tr}\big(D_{\mathbf{p}}^\dagger \Pi\big)\,,\ \mathbf{p} \in \mathcal{P}\,. \tag{8.55}$$

We also know that $\Pi = \Pi^\dagger$ and $\Pi \succeq 0$. Since Π is positive semidefinite, the Schatten 1-norm becomes simply the trace, so we do not enforce the constraint $\mathrm{Tr}(\Pi) = 1$ to avoid trivializing the objective function. We then output the matrix that minimizes $\mathrm{Tr}(\Pi)$ subject to the constraints (8.55) as well as the Hermitian and positive semidefinite constraints. If the result is not (numerically) a rank-1 matrix, we simply try another candidate matrix M and run the semidefinite program again. One can gain further confidence in a numerical solution by applying Newton's method, similar to section 8.3, to enhance the precision to any desired level.

The number of candidate solutions that must be checked is always at most the order of $\mathcal{M}$, which is at most polynomial in d. The semidefinite program also runs in polynomial time in d. Therefore, at least in this formal sense, this procedure is efficient with respect to the dimension.

Appendix A. Alternative fiducial data

In Definition 1.30 we defined the SF phase corresponding to the admissible tuple $t = (d, r, Q) \sim (K, j, m, Q)$ by

$$\phi_{\mathbf{p}}(t) = (-1)^{s_d(\mathbf{p})} e^{-\frac{\pi i}{12}\Psi(A_t)} \xi_d^{-\frac{f_{jm}}{f}Q(\mathbf{p})} \tag{A.1}$$

with

$$s_d(\mathbf{p}) = d + (1+d)(1+p_1)(1+p_2). \tag{A.2}$$

However, as we will see below, it would have been possible to have replaced $s_d(\mathbf{p})$ with the more general expression

$$s_d(\mathbf{w}, \mathbf{p}) = d + (1+d)(1+p_1)(1+p_2) + (1+d)\langle \mathbf{w}, \mathbf{p}\rangle \tag{A.3}$$

for arbitrary $\mathbf{w} \in \mathbb{Z}^2$. Similarly, in Definition 1.32 we defined the candidate normalized ghost overlaps corresponding to the admissible tuple $t = (d, r, Q) \sim (K, j, m, Q)$ by

$$\tilde{\nu}_{\mathbf{p}}(t) = \phi_{\mathbf{p}}(t) \mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho_{Q,+})\,. \tag{A.4}$$

However, as we will see below, it would have been possible to replace $\rho_{Q,+}$ with $\rho_{Q,-}$. The reason we did not make either of these choices in the main text is because they do not lead to new r-SICs, as we now show.

In this appendix we modify the notation used elsewhere in the paper, so as to include an explicit dependence on $\mathbf{w}$ and root $\rho_{Q,\pm}$. Let $s = (t, G, g)$ be a fiducial datum containing the admissible

tuple $t = (d, r, Q) \sim (K, j, m, Q)$, let f be the conductor of Q, let ρ be either of the two roots of Q, and let $\rho, \mathbf{w} \in \mathbb{Z}^2$. We define

$$\phi_{\mathbf{p}}(t, \mathbf{w}) = (-1)^{s_d(\mathbf{w},\mathbf{p})} e^{-\frac{\pi i}{12}\Psi(A_t)} \xi_d^{-\frac{f_{jm}}{f}Q(\mathbf{p})} \tag{A.5}$$

(A.6)

where $s_d(\mathbf{w}, \mathbf{p})$ is as given by (A.3),

$$\tilde{\nu}_{\mathbf{p}}(t, \mathbf{w}, \rho) = \phi_{\mathbf{p}}(t, \mathbf{w}) \mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho)\,, \tag{A.7}$$

$$\tilde{\Pi}_s(\mathbf{w}, \rho) = \frac{r}{d} I + \frac{1}{d\sqrt{d_j + 1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{G\mathbf{p}}(t, \mathbf{w}, \rho) D_{\mathbf{p}} \tag{A.8}$$

$$\Pi_s(\mathbf{w}, \rho) = g \left((\tilde{\Pi}_s(\mathbf{w}, \rho) \right). \tag{A.9}$$

The purpose of this appendix is to prove

Theorem A.1. *Assume Conjectures 1.35 and 1.51 are true. Let $s = (d, r, Q, G, g)$ be a fiducial datum, let ρ be either of the two roots of Q, and let $\mathbf{w}$ be any element of $\mathbb{Z}^2$. Then there exists a form Q' such that*

$$\Pi_s(\mathbf{w}, \rho) = \Pi_{s'}(\mathbf{0}, \rho_{Q',+}) \tag{A.10}$$

where $s' = (d, r, Q', G, g)$.

It follows from this result that there is no loss of generality if, as in the rest of the paper, we confine ourselves to the case $\mathbf{w} = \mathbf{0}$, $\rho = \rho_{Q,+}$.

In order to prove Theorem A.1 we need first to prove the following lemma.

Lemma A.2. *Assume Conjectures 1.35 and 1.51 are true. Let $s = (d, r, Q, G, g)$ be a fiducial datum, and let $\mathbf{w}, \mathbf{w}' \in \mathbb{Z}^2$. Then $s' = (d, r, -Q, G, g)$ is also a fiducial datum, and*

$$U_P \Pi_s(\mathbf{w}, \rho_{Q,\pm}) U_P^\dagger = \Pi_{s'}(\mathbf{w}, \rho_{-Q,\mp}) \tag{A.11}$$

$$U_{M_{G^{-1}\mathbf{w}'}} \Pi_s(\mathbf{w}, \rho_{Q,\pm}) U_{M_{G^{-1}\mathbf{w}'}}^\dagger = \Pi_s(\mathbf{w} + \mathbf{w}', \rho_{Q,\pm}) \tag{A.12}$$

where $M_{\mathbf{w}'} = \begin{pmatrix} 1 & w_1' d \\ w_2' d & 1 \end{pmatrix}$ and P is the parity matrix (see Definition 3.4).

Proof. Let $t = (d, r, Q)$, $t' = (d, r, -Q)$. Assuming Conjecture 1.35 is true, the fact that Q and $-Q$ have the same discriminant means $\mathcal{Z}_t = \mathcal{Z}_{t'}$ (see Definition 1.34). Also it follows from Conjecture 1.51 that $E_t = E_{t'}$. So G satisfies (1.51) for some $\lambda \in \mathcal{Z}_{t'}$ and $g \in \mathrm{Gal}(E_t/\mathbb{Q})$. It follows that s' is a fiducial datum.

It is easily seen that $A_{t'} = A_t^{-1}$ and $\rho_{-Q,\pm} = \rho_{Q,\mp}$. In view of Lemma 5.1 this means

$$\phi_{\mathbf{p}}(t', \mathbf{w}) = (-1)^{s_d(\mathbf{w},\mathbf{p})} e^{-\frac{\pi i}{12}\Psi(A_t^{-1})} \xi_d^{\frac{f_{jm}}{f}Q}(\mathbf{p}) = (\phi_{\mathbf{p}}(t, \mathbf{w}))^{-1}\,, \tag{A.13}$$

for all $\mathbf{p} \in \mathbb{Z}^2$, while it follows from Lemma 2.13 that

$$\mathfrak{w}_{A_{t'}}^{d^{-1}\mathbf{p}}(\rho_{-Q,\mp}) = \left(\mathfrak{w}_{A_t}^{d^{-1}\mathbf{p}}(\rho_{Q,\pm}) \right)^{-1} \tag{A.14}$$

for all $\mathbf{p} \in \mathbb{Z}^2$. Hence

$$\tilde{\nu}_{\mathbf{p}}(t', \mathbf{w}, \rho_{-Q,\mp}) = \phi_{\mathbf{p}}(t', \mathbf{w}) \mathfrak{w}_{A_{t'}}^{d^{-1}\mathbf{p}}(\rho_{-Q,\mp}) = (\tilde{\nu}_{\mathbf{p}}(t, \mathbf{w}, \rho_{Q,\pm}))^{-1}\,. \tag{A.15}$$

Taking account of Theorem 5.8 we deduce

$$\tilde{\nu}_{\mathbf{p}}(t', \mathbf{w}, \rho_{-Q,\mp}) = \tilde{\nu}_{-\mathbf{p}}(t, \mathbf{w}, \rho_{Q,\pm}) \tag{A.16}$$

for all $\mathbf{p} \in \mathbb{Z}^2$ such that $\mathbf{p} \notin d\mathbb{Z}^2$. Consequently

$$\begin{aligned}\tilde{\Pi}_{s'}(\mathbf{w}, \rho_{-Q,\mp}) &= \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{G\mathbf{p}}(t', \mathbf{w}, \rho_{-Q,\mp}) D_{\mathbf{p}} \\ &= \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{-G\mathbf{p}}(t, \mathbf{w}, \rho_{Q,\pm}) D_{\mathbf{p}} \\ &= U_P \tilde{\Pi}_s(\mathbf{w}, \rho_{Q,\pm}) U_P^{\dagger}. \end{aligned} \tag{A.17}$$

It follows from (3.17) that the matrix elements of U_P are all in $\mathbb{Z}$. So eqs. (A.17) and (A.9) imply

$$\Pi_{s'}(\mathbf{w}, \rho_{-Q,\mp}) = g\left(\tilde{\Pi}_{s'}(\mathbf{w}, \rho_{-Q,\mp})\right) = U_P \Pi_s(\mathbf{w}, \rho_{Q,\pm}) U_P^{\dagger}, \tag{A.18}$$

thereby proving (A.11). Turning to (A.12), observe that the statement is trivial if d is odd. Suppose, on the other hand, that d is even. Then it follows from Eq. (A.8) that

$$U_{M_{G^{-1}\mathbf{w}'}} \tilde{\Pi}_s(\mathbf{w}, \rho_{Q,\pm}) U^{\dagger}_{M_{G^{-1}\mathbf{w}'}} = \frac{r}{d} I + \frac{1}{d\sqrt{d_j+1}} \sum_{\mathbf{p} \notin d\mathbb{Z}^2} \tilde{\nu}_{GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p}}(t, \mathbf{w}, \rho_{Q,\pm}) D_{\mathbf{p}}. \tag{A.19}$$

Observe that $M^{-1}_{G^{-1}\mathbf{w}'} = M_{G^{-1}\mathbf{w}'}$ as an element of $\mathrm{SL}_2(\mathbb{Z}/2d\mathbb{Z})$. Since $M_{G^{-1}\mathbf{w}'} \equiv I \pmod 2$ it follows that

$$(-1)^{s_d(\mathbf{w}, GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p})} = (-1)^{s_d(\mathbf{w}, G\mathbf{p})}. \tag{A.20}$$

It follows from Corollary 5.4 that

$$\xi_d^{-\frac{f_{jm}}{f} Q\left(GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p}\right)} = \xi_d^{-a(GM_{G^{-1}\mathbf{w}'}\mathbf{p})_1^2 - b(GM_{G^{-1}\mathbf{w}'}\mathbf{p})_1 (GM_{G^{-1}\mathbf{w}'}\mathbf{p})_2 - c(GM_{G^{-1}\mathbf{w}'}\mathbf{p})_2^2} \tag{A.21}$$

where a, b, c are odd. Setting $G = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ we have

$$\xi_d^{-a(GM_{G^{-1}\mathbf{w}'}\mathbf{p})_1^2} = \xi_d^{-a\left((G\mathbf{p})_1 + d(\beta(G^{-1}\mathbf{w}')_2 p_1 + \alpha(G^{-1}\mathbf{w}')_1 p_2)\right)^2} = \xi_d^{-a(G\mathbf{p})_1^2}, \tag{A.22}$$

$$\xi_d^{-c(GM_{G^{-1}\mathbf{w}'}\mathbf{p})_2^2} = \xi_d^{-c\left((G\mathbf{p})_2 + d(\delta(G^{-1}\mathbf{w}')_2 p_1 + \gamma(G^{-1}\mathbf{w}')_1 p_2)\right)^2} = \xi_d^{-c(G\mathbf{p})_2^2}, \tag{A.23}$$

and

$$\begin{aligned} &\xi_d^{-b(GM_{G^{-1}\mathbf{w}'}\mathbf{p})_1 (GM_{G^{-1}\mathbf{w}'}\mathbf{p})_2} \\ &\quad = \xi_d^{-b\left((G\mathbf{p})_1 + d(\beta(G^{-1}\mathbf{w}')_2 p_1 + \alpha(G^{-1}\mathbf{w}')_1 p_2)\right)\left((G^{-1}\mathbf{p})_2 + d(\delta(G^{-1}\mathbf{w}')_2 p_1 + \gamma(G^{-1}\mathbf{w}')_1 p_2)\right)} \\ &\quad = (-1)^{(G\mathbf{p})_1(\delta(G^{-1}\mathbf{w}')_2 p_1 + \gamma(G^{-1}\mathbf{w}')_1 p_2) + (G\mathbf{p})_2(\beta(G^{-1}\mathbf{w}')_2 p_1 + \alpha(G^{-1}\mathbf{w}')_1 p_2)} \xi_d^{-b(G\mathbf{p})_1 (G\mathbf{p})_2} \\ &\quad = (-1)^{(\alpha p_1 + \beta p_2)(\delta(G^{-1}\mathbf{w}')_2 p_1 + \gamma(G^{-1}\mathbf{w}')_1 p_2) + (\gamma p_1 + \delta p_2)(\beta(G^{-1}\mathbf{w}')_2 p_1 + \alpha(G^{-1}\mathbf{w}')_1 p_2)} \xi_d^{-b(G\mathbf{p})_1 (G\mathbf{p})_2} \\ &\quad = (-1)^{(\alpha\delta + \beta\gamma)((G^{-1}\mathbf{w}')_2 p_1^2 + (G^{-1}\mathbf{w}')_1 p_2^2)} \xi_d^{-b(G\mathbf{p})_1 (G\mathbf{p})_2} \\ &\quad = (-1)^{\det(G)((G^{-1}\mathbf{w}')_2 p_1 + (G^{-1}\mathbf{w}')_1 p_2)} \xi_d^{-b(G\mathbf{p})_1 (G\mathbf{p})_2} \\ &\quad = (-1)^{\det(G)\langle G^{-1}\mathbf{w}', \mathbf{p}\rangle} \xi_d^{-b(G\mathbf{p})_1 (G\mathbf{p})_2} \\ &\quad = (-1)^{\langle \mathbf{w}', G\mathbf{p}\rangle} \xi_d^{-b(G\mathbf{p})_1 (G\mathbf{p})_2} \end{aligned} \tag{A.24}$$

Putting all this together we conclude

$$\xi_d^{-\frac{f_{jm}}{f}Q(GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p})} = (-1)^{\langle \mathbf{w}', G\mathbf{p}\rangle}\xi_d^{-\frac{f_{jm}}{f}Q(G\mathbf{p})}, \tag{A.25}$$

and, consequently,

$$\begin{aligned}
\phi_{GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p}}(t,\mathbf{w}) &= (-1)^{s_d\left(\mathbf{w},GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p}\right)}e^{-\frac{\pi i}{12}\Psi(A_t)}\xi_d^{-\frac{f_{jm}}{f}Q\left(GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p}\right)} \\
&= (-1)^{s_d(\mathbf{w},G\mathbf{p})+\langle \mathbf{w}', G\mathbf{p}\rangle}e^{-\frac{\pi i}{12}\Psi(A_t)}\xi_d^{-\frac{f_{jm}}{f}Q(G\mathbf{p})} \\
&= (-1)^{s_d(\mathbf{w}+\mathbf{w}',G\mathbf{p})}e^{-\frac{\pi i}{12}\Psi(A_t)}\xi_d^{-\frac{f_{jm}}{f}Q(G\mathbf{p})} \\
&= \phi_{G\mathbf{p}}(t,\mathbf{w}+\mathbf{w}').
\end{aligned} \tag{A.26}$$

The fact that $M^{-1}_{G^{-1}\mathbf{w}'} \equiv I \pmod d$ implies, in view of Lemma 2.14,

$$\mathfrak{w}_{A_t}^{d^{-1}GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p}}(\rho_{Q,\pm}) = \mathfrak{w}_{A_t}^{d^{-1}G\mathbf{p}}(\rho_{Q,\pm}) \tag{A.27}$$

for all $\mathbf{p} \not\equiv \mathbf{0} \pmod d$. Hence

$$\begin{aligned}
\tilde{\nu}_{GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p}}(t,\mathbf{w},\rho_{Q,\pm}) &= \phi_{GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p}}(t,\mathbf{w})\mathfrak{w}_{A_t}^{d^{-1}GM^{-1}_{G^{-1}\mathbf{w}'}\mathbf{p}}(\rho_{Q,\pm}) \\
&= \phi_{G\mathbf{p}}(t,\mathbf{w}+\mathbf{w}')\mathfrak{w}_{A_t}^{d^{-1}G\mathbf{p}}(\rho_{Q,\pm}) \\
&= \tilde{\nu}_{G\mathbf{p}}(t,\mathbf{w}+\mathbf{w}',\rho_{Q,\pm}).
\end{aligned} \tag{A.28}$$

Consequently

$$\begin{aligned}
U_{M_{G^{-1}\mathbf{w}'}}\tilde{\Pi}_s(\mathbf{w},\rho_{Q,\pm})U^\dagger_{M_{G^{-1}\mathbf{w}'}} &= \frac{r}{d}I + \frac{1}{d\sqrt{d_j+1}}\sum_{\mathbf{p}\notin d\mathbb{Z}^2}\tilde{\nu}_{G\mathbf{p}}(t,\mathbf{w}+\mathbf{w}',\rho_{Q,\pm})D_{\mathbf{p}} \\
&= \tilde{\Pi}_s(\mathbf{w}+\mathbf{w}',\rho_{Q,\pm}),
\end{aligned} \tag{A.29}$$

Write

$$G^{-1}\mathbf{w}' = \begin{pmatrix} l_1 \\ l_2 \end{pmatrix} \tag{A.30}$$

for $l_1, l_2 \in \mathbb{Z}/\bar{d}\mathbb{Z}$. It follows from Theorem 1 in ref. [4] that

$$U_{M_{G^{-1}\mathbf{w}'}} = e^{i\theta}X^{-\frac{dl_1}{2}}Z^{-\frac{dl_2}{2}} \tag{A.31}$$

for some $\theta \in \mathbb{R}$ such that $e^{i\theta} \in \mathbb{Q}(\xi_d)$ (see Definition 1.5 for X, Z). We have

$$X^{-\frac{dl_1}{2}}Z^{-\frac{dl_2}{2}} = \sum_{j=0}^{d}(-1)^{l_2 j}\left|j+\tfrac{l_1 d}{2}\right\rangle\left\langle j\right|. \tag{A.32}$$

So the matrix elements of $X^{-\frac{dl_1}{2}}Z^{-\frac{dl_2}{2}}$ are all in $\mathbb{Z}$. Hence

$$\begin{aligned}
\Pi_s(\mathbf{w}+\mathbf{w}',\rho_{Q,\pm}) &= g\left(\tilde{\Pi}_s(\mathbf{w}+\mathbf{w}',\rho_{Q,\pm})\right) \\
&= g\left(U_{M_{G^{-1}\mathbf{w}'}}\tilde{\Pi}_s(\mathbf{w},\rho_{Q,\pm})U^\dagger_{M_{G^{-1}\mathbf{w}'}}\right) \\
&= g\left(\left(X^{-\frac{dl_1}{2}}Z^{-\frac{dl_2}{2}}\right)\tilde{\Pi}_s(\mathbf{w},\rho_{Q,\pm})\left(X^{-\frac{dl_1}{2}}Z^{-\frac{dl_2}{2}}\right)^\dagger\right)
\end{aligned}$$

$$= \left(X^{-\frac{dl_1}{2}} Z^{-\frac{dl_2}{2}}\right) g \left(\tilde{\Pi}_s(\mathbf{w}, \rho_{Q,\pm})\right) \left(X^{-\frac{dl_1}{2}} Z^{-\frac{dl_2}{2}}\right)^\dagger$$
$$= U_{M_{G^{-1}}\mathbf{w}'} \Pi_s(\mathbf{w}, \rho_{Q,\pm}) U^\dagger_{M_{G^{-1}}\mathbf{w}'}. \tag{A.33}$$

□

We are now ready to prove the main result of this Appendix.

Proof of Theorem A.1. We first show that, given an arbitrary fiducial datum $s = (d, r, Q, G, g)$ there exists a datum $s' = (d, r, Q', G, g)$ such that

$$\Pi_s(\mathbf{0}, \rho_{Q,-}) = \Pi_{s'}(\mathbf{0}, \rho_{Q',+}). \tag{A.34}$$

Indeed, Lemma A.2 implies

$$\Pi_s(\mathbf{0}, \rho_{Q,-}) = U_P^\dagger \Pi_{s''}(\mathbf{0}, \rho_{-Q,+}) U_P \tag{A.35}$$

where s'' is the datum $(d, r, -Q, G, g)$. It then follows from Theorems 7.4 and 7.5 that there exists $R \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$U_P^\dagger \Pi_{s''}(\mathbf{0}, \rho_{-Q,+}) U_P = \Pi_{s''_R}(\mathbf{0}, \rho_{-Q_R,+}). \tag{A.36}$$

Equation (A.34) then follows by combining these statements and setting $Q' = -Q_R$, $s' = s''_R$.

Now consider the general case. Given an arbitrary datum $s = (d, r, Q, G, g)$, an arbitrary root $\rho_{Q,\pm}$, and arbitrary $\mathbf{w} \in \mathbb{Z}^2$, it follows from Lemma A.2 and the result just proved that

$$\begin{aligned} \Pi_s(\mathbf{w}, \rho_{Q,\pm}) &= U_{M_{G^{-1}}\mathbf{w}} \Pi_s(\mathbf{0}, \rho_{Q,\pm}) U^\dagger_{M_{G^{-1}}\mathbf{w}} \\ &= U_{M_{G^{-1}}\mathbf{w}} \Pi_{s''}(\mathbf{0}, \rho_{Q'',+}) U^\dagger_{M_{G^{-1}}\mathbf{w}} \end{aligned} \tag{A.37}$$

for some fiducial datum $s'' = (d, r, Q'', G, g)$. It then follows from Theorems 7.4 and 7.5 that there exists $R \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$U_{M_{G^{-1}}\mathbf{w}} \Pi_{s''}(\mathbf{0}, \rho_{Q'',+}) U^\dagger_{M_{G^{-1}}\mathbf{w}} = \Pi_{s''_R}(\mathbf{0}, \rho_{Q''_R,+}). \tag{A.38}$$

Setting $s' = s''_R$, $Q' = Q''_R$ the result follows. □

Appendix B. Canonical order 3 unitaries

The purpose of this Appendix is to prove Theorem 3.13, characterizing the conjugacy classes of the elements of $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ having trace equal to $d-1$. Our starting point is Lemma 9.2 in Bos and Waldron [19] which describes the conjugacy classes of the elements of $\mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})$ having trace equal to -1. We proceed in two steps:

(1) We first use Bos and Waldron's result to prove an analogous result for the elements of $\mathrm{ESL}_2(\mathbb{Z}/d\mathbb{Z})$ having trace equal to -1.
(2) We then use this to prove the result for the elements of $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ having trace equal to $d-1$.

Let F_z, F_a, F'_a be as specified in Definition 3.12, and let $\bar{F}_z$, $\bar{F}_a$, $\bar{F}'_a$ be their reductions modulo d. Thus

$$\bar{F}_z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad \bar{F}_a = \begin{pmatrix} 1 & 3 \\ \frac{d-3}{3} & -2 \end{pmatrix}, \qquad \bar{F}'_a = \begin{pmatrix} 1 & 3 \\ \frac{2d-3}{3} & -2 \end{pmatrix}. \tag{B.1}$$

We begin by stating the result of Bos and Waldron on which we rely. As in the rest of this paper we restrict ourselves to the case $d \geq 4$.

Lemma (Lemma 9.2 in Bos and Waldron [19])**.** *The set of matrices in* $\mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})$ *having trace equal to* -1 *consists of*

(1) The single conjugacy class $[\bar{F}_z]$ *if* $d \not\equiv 0 \pmod 3$,

(2) The two disjoint conjugacy classes $[\bar{F}_z]$, $[\bar{F}_z^{-1}]$ *if* $d \equiv 0 \pmod 9$,

(3) The three disjoint conjugacy classes $[\bar{F}_z]$, $[\bar{F}_z^{-1}]$, $[\bar{F}_a]$ *if* $d \equiv 3 \pmod 9$,

(4) The three disjoint conjugacy classes $[\bar{F}_z]$, $[\bar{F}_z^{-1}]$, $[\bar{F}'_a]$ *if* $d \equiv 6 \pmod 9$,

where the notation $[G]$ *means "conjugacy class of* G *considered as an element of* $\mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})$*".*

Remark. Note that Bos and Waldron state a more general version of the lemma applicable to all $d \geq 2$; in particular to $d = 3$ which requires special treatment.

The next result says that extending to $\mathrm{ESL}_2(\mathbb{Z}/d\mathbb{Z})$ reduces the number of conjugacy classes.

Lemma B.1. *The set of matrices in* $\mathrm{ESL}_2(\mathbb{Z}/d\mathbb{Z})$ *having determinant equal to* $+1$ *and trace equal to* -1 *consists of*

(1) The single conjugacy class $[\bar{F}_z]$ *if* $d \not\equiv 3, 6 \pmod 9$.

(2) The two disjoint conjugacy classes $[\bar{F}_z]$, $[\bar{F}_a]$ *if* $d \equiv 3 \pmod 9$,

(3) The two disjoint conjugacy classes $[\bar{F}_z]$, $[\bar{F}'_a]$ *if* $d \equiv 6 \pmod 9$,

where the notation $[G]$ *means "conjugacy class of* G *considered as an element of* $\mathrm{ESL}_2(\mathbb{Z}/d\mathbb{Z})$*".*

Proof. Let

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{B.2}$$

Then

$$M\bar{F}_z M^{-1} = \bar{F}_z^{-1}, \tag{B.3}$$

implying $[\bar{F}_z^{-1}] = [\bar{F}_z]$ for all d.

To see that $[\bar{F}_z]$ and $[\bar{F}_a]$ are disjoint when $d \equiv 3 \pmod 9$, assume on the contrary that

$$\bar{F}_z = G\bar{F}_a G^{-1} \tag{B.4}$$

for some $G \in \mathrm{ESL}_2(\mathbb{Z}/d\mathbb{Z})$. Since $\bar{F}_a \equiv I \pmod 3$, it would follow that $\bar{F}_z \equiv I \pmod 3$, which is a contradiction.

The fact that $[\bar{F}_z]$ and $[\bar{F}'_a]$ are disjoint when when $d \equiv 6 \pmod 9$ is proved similarly. □

We now use this to prove Theorem 3.13. If d is odd then $\bar{F}_z = F_z$, $\bar{F}_a = F_a$, $\bar{F}'_a = F'_a$, and the theorem is an immediate consequence of Lemma B.1.

Suppose, on the other hand, that d is even. Making the replacement $d \to 2d$ in Lemma B.1, and using the fact that $d \equiv 3 \pmod 9 \iff 2d \equiv 6 \pmod 9$ and $d \equiv 6 \pmod 9 \iff 2d \equiv 3 \pmod 9$, we find that the set of matrices in $\mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ having determinant equal to $+1$ and trace equal to -1 consists of:

(1) The single conjugacy class

$$\left[\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\right] \tag{B.5}$$

if $d \not\equiv 3, 6 \pmod 9$.

(2) The two disjoint conjugacy classes

$$\left[\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\right], \qquad \left[\begin{pmatrix} 1 & 3 \\ \frac{4d-3}{3} & -2 \end{pmatrix}\right] \tag{B.6}$$

if $d \equiv 3 \pmod 9$,

(3) The two disjoint conjugacy classes

$$\left[\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\right], \qquad \left[\begin{pmatrix} 1 & 3 \\ \frac{2d-3}{3} & -2 \end{pmatrix}\right] \tag{B.7}$$

if $d \equiv 6 \pmod 9$.

Now suppose that $F \in \mathrm{ESL}_2(\mathbb{Z}/\bar{d}\mathbb{Z})$ has determinant $+1$ and trace equal to $d-1$. Then $G = (d+1)F$ has trace equal to -1, so the result just proved implies that

$$F \in [(d+1)G] = \left[\begin{pmatrix} 0 & d-1 \\ d+1 & d-1 \end{pmatrix}\right] \tag{B.8}$$

if $d \not\equiv 3, 6 \pmod 9$,

$$F \in [(d+1)G] = \left[\begin{pmatrix} 0 & d-1 \\ d+1 & d-1 \end{pmatrix}\right] \quad \text{or} \quad \left[\begin{pmatrix} d+1 & d+3 \\ \frac{d-3}{3} & -2 \end{pmatrix}\right] \tag{B.9}$$

if $d \equiv 3 \pmod 9$, and

$$F \in [(d+1)G] = \left[\begin{pmatrix} 0 & d-1 \\ d+1 & d-1 \end{pmatrix}\right] \quad \text{or} \quad \left[\begin{pmatrix} d+1 & d+3 \\ \frac{5d-3}{3} & -2 \end{pmatrix}\right] \tag{B.10}$$

if $d \equiv 6 \pmod 9$. Using

$$\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix} \begin{pmatrix} d+1 & d+3 \\ \frac{d-3}{3} & -2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & d+3 \\ \frac{4d-3}{3} & d-2 \end{pmatrix} = F_a \tag{B.11}$$

$$\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix} \begin{pmatrix} d+1 & d+3 \\ \frac{5d-3}{3} & -2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & d+3 \\ \frac{2d-3}{3} & d-2 \end{pmatrix} = F'_a \tag{B.12}$$

we deduce

$$F \in [F_z] \qquad \text{if } d \not\equiv 3, 6 \pmod 9 \tag{B.13}$$

$$F \in [F_z] \text{ or } [F_a] \qquad \text{if } d \equiv 3 \pmod 9 \tag{B.14}$$

$$F \in [F_z] \text{ or } [F'_a] \qquad \text{if } d \equiv 6 \pmod 9 \tag{B.15}$$

The fact that $[F_z]$, $[F_a]$ are disjoint when $d \equiv 3 \pmod 9$ follows from the fact that $F_a = I \not\equiv F_z \pmod 3$. Similarly, if $d \equiv 6 \pmod 9$, then $F'_a = I \not\equiv F_z \pmod 3$, implying $[F_z]$, $[F'_a]$ are disjoint. Theorem 3.13 now follows.

APPENDIX C. HIRZEBRUCH–JUNG CONTINUED FRACTIONS

The purpose of this appendix is to show how continued fraction expansions can be used to choose a quadratic form which minimizes the length of the expansion on the right hand side of (8.1)

Expansions of the form

$$[k_1, k_2, k_3, k_4, \dots]_+ = k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 + \cfrac{1}{k_4 + \cdots}}} \tag{C.1}$$

are extremely well-known, and are described in considerable detail in standard texts such as [27,53]. Following Popescu-Pampu [83] we refer to them as *Euclidean (E-) continued fractions*. In this paper we need a different kind of expansion, which Popescu-Pampu refers to as a *Hirzebruch–Jung (HJ-) continued fraction*, of the form

$$[k_1, k_2, k_3, k_4, \dots]_- = k_1 - \cfrac{1}{k_2 - \cfrac{1}{k_3 - \cfrac{1}{k_4 - \cdots}}}. \tag{C.2}$$

In the literature [1,18,39,57–59,63,65,66,76,77,80,83,92] such fractions are also described as backwards, negative-regular, minus, reduced regular, and by-excess continued fractions. For the convenience of the reader in this appendix we collect their essential properties. Since we are only concerned with HJ-continued fractions in this paper, we will drop the subscript, and simply denote them $[k_1, k_2, k_3, k_4, \dots]$. We also review the related concept, of a *Hirzebruch–Jung (HJ-) reduced form*.

For all $x \in \mathbb{Q}$ (respectively $x \in \mathbb{R} \setminus \mathbb{Q}$) there exists a unique finite (respectively infinite) sequence of integers k_j such that $x = [k_1, k_2 \dots]$, $k_j \geq 2$ for all $j \geq 2$ and (in case the sequence is infinite) there is no integer m such that $k_j = 2$ for all $j \geq m$.

Define = $(k_1, k_2, \dots, k_n)$ recursively by

$$(k_1, k_2, \dots, k_n) = \begin{cases} k_1 & n = 1, \\ k_1 k_2 - 1 & n = 2, \\ (k_1, k_2, \dots, k_{n-1}) k_n - (k_1, k_2 \dots, k_{n-2}) & n > 2. \end{cases} \tag{C.3}$$

We refer to these quantities as HJ-convergents. They can be calculated using the following modified version of Euler's rule: first take the product of all n numbers $k_1, \dots, k_n$, then subtract all products obtained by omitting a pair of adjacent numbers, then add all products obtained by omitting two different pairs of adjacent numbers, and so on. In particular, they are symmetric under reversal:

$$(k_1, k_2, \dots, k_{n-1}, k_n) = (k_n, k_{n-1}, \dots, k_2, k_1). \tag{C.4}$$

One has

$$[k_1, k_2, \dots, k_n] = \begin{cases} (k_1) & n = 1, \\ \frac{(k_1, k_2, \dots, k_n)}{(k_2, \dots, k_n)} & n \geq 2, \end{cases} \tag{C.5}$$

for finite HJ-expansions,

$$[k_1, k_2, \dots, k_n, \dots] = \begin{cases} \frac{(k_1)[k_{n+1}, k_{n+2}, \dots] - 1}{[k_{n+1}, k_{n+2}, \dots]} & n = 1, \\ \frac{(k_1, k_2)[k_{n+1}, k_{n+2}, \dots] - (k_1)}{(k_2)[k_{n+1}, k_{n+2}, \dots] - 1} & n = 2, \\ \frac{(k_1, \dots, k_n)[k_{n+1}, k_{n+2}, \dots] - (k_1, \dots, k_{n-1})}{(k_2, \dots, k_n)[k_{n+1}, k_{n+2}, \dots] - (k_2, \dots, k_{n-1})} & n > 2, \end{cases} \tag{C.6}$$

for infinite HJ-expansions, and

$$T^{k_1}ST^{k_2}S\dots T^{k_n}S=\begin{cases}\begin{pmatrix}(k_1) & -1\\ 1 & 0\end{pmatrix} & n=1,\\ \begin{pmatrix}(k_1,k_2) & -(k_1)\\ (k_2) & -1\end{pmatrix} & n=2,\\ \begin{pmatrix}(k_1,\dots,k_n) & -(k_1,\dots,k_{n-1})\\ (k_2,\dots,k_n) & -(k_2,\dots,k_{n-1})\end{pmatrix} & n\geq 3.\end{cases}\tag{C.7}$$

In particular

$$T^{k_1}ST^{k_2}S\dots T^{k_n}S.([k_{n+1},k_{n+2},\dots])=[k_1,k_2,\dots,\dots]\tag{C.8}$$

for all n. This last relation is the reason HJ-continued fractions are relevant to this paper.

A continued fraction is said to be *periodic* if it is infinite and of the form

$$[l_1,l_2,\dots,l_m,\overline{k_1,k_2,\dots,k_n}]=[l_1,l_2,\dots,l_m,k_1,\dots,k_n,k_1,\dots,k_n,k_1,\dots,k_n,\dots]\tag{C.9}$$

It is said to be *purely periodic* if it is of the form $[\overline{k_1,\dots,k_n}]$. If $k_1,\dots,k_n$ doesn't break into two or more identical subsequences then we say that n is the *period* of $[\overline{k_1,\dots,k_n}]$.

The HJ-continued fraction expansion of a real number is periodic if and only if it is an irrational element of a real quadratic field. Let ρ be such a number. Then its HJ-continued fraction expansion is purely periodic if and only if $\rho>1>\rho'>0$, where ρ' is its Galois conjugate.

There is a close connection between purely periodic HJ-continued fractions and a class of quadratic forms which we now define. A form $Q=\langle a,b,c\rangle$ with discriminant $\Delta=b^2-4ac$ is reduced in the ordinary sense [20,21], or as we will say *Euclidean (E-) reduced*, if

$$0<\sqrt{\Delta}-b<2|a|<\sqrt{\Delta}+b.\tag{C.10}$$

Forms of this type have a connection with Euclidean continued fractions. Specifically, the number $\frac{b+\sqrt{\Delta}}{2|a|}$ has a purely periodic E-continued fraction expansion if and only if Q is E-reduced. Corresponding to this we say Q is *Hirzebruch–Jung (HJ-) reduced* if

$$0<-\sqrt{\Delta}-b<2|a|<\sqrt{\Delta}-b.\tag{C.11}$$

The number $\frac{-b+\sqrt{\Delta}}{2|a|}$ has a purely periodic HJ-continued fraction expansion if and only if Q is HJ-reduced.

Let $Q=\langle a,b,c\rangle$ and $J=\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$. Then $Q_J=\langle -a,b,-c\rangle$ (see section 1.3). It follows that Q_J is E-reduced (respectively HJ-reduced) if and only if Q is E-reduced (respectively HJ-reduced), in which case they define the same purely periodic E-continued (respectively HJ-continued) fraction. We may therefore, without loss of generality, confine ourselves to E-reduced (respectively HJ-reduced) forms $\langle a,b,c\rangle$ for which $a>0$. In the following this restriction will be assumed without comment. The map taking Q to $-\rho_{Q,-}$ (respectively $\rho_{Q,+}$) is then a bijective correspondence of the set of E-reduced (respectively HJ-reduced) forms onto the set of purely periodic E-continued (respectively HJ-continued) fractions.

There is a well-known algorithm [20,21] for calculating the complete set of E-reduced forms on a given $\mathrm{GL}_2(\mathbb{Z})$ orbit. We now show how this can be used to construct the complete set of HJ-reduced forms on the same orbit. Let W be the forms $\langle a,b,c\rangle$ on a $GL(2,\mathbb{Z})$ orbit for which $a>0$, and let

$$W_{\mathrm{E}}=\{Q\in W\colon \rho_{Q,-}<-1<0<\rho_{Q,+}<1\}\tag{C.12}$$

$$W_{\mathrm{HJ}} = \{Q \in W : 0 < \rho_{Q,-} < 1 < \rho_{Q,+}\} \tag{C.13}$$

(where $\rho_{Q,\pm}$ are given by (1.35)). Then W_{E} (respectively W_{HJ}) is precisely the set of E-reduced (respectively HJ-reduced) forms in W. Also define, for $n = 0, 1, \ldots$

$$W_{\mathrm{E}}^{(n)} = \{Q \in W : \rho_{Q,-} < -1 < 0 < \rho_{Q,+} < \frac{1}{n+1}\}, \tag{C.14}$$

$$W_{\mathrm{HJ}}^{(n)} = \{Q \in W : \frac{n}{n+1} < \rho_{Q,-} < \frac{n+1}{n+2} < 1 < \rho_{Q,+}\}. \tag{C.15}$$

Then

$$W_{\mathrm{E}} = W_{\mathrm{E}}^{(0)} \supseteq W_{\mathrm{E}}^{(1)} \supseteq \ldots, \qquad \bigcap_{n=0}^{\infty} W_{\mathrm{E}}^{(n)} = \emptyset. \tag{C.16}$$

$$W_{\mathrm{HJ}}^{(n)} \cap W_{\mathrm{HJ}}^{(n')} = \emptyset \quad \text{if } n \neq n', \qquad \bigcup_{n=0}^{\infty} W_{\mathrm{HJ}}^{(n)} = W_{\mathrm{HJ}} \tag{C.17}$$

Since W_{E} is finite, non-empty there must exist $n_0 \in \mathbb{N}$ such that $W_{\mathrm{E}}^{(n)} = \emptyset$ if and only if $n \geq n_0$. Let

$$L_n = \begin{pmatrix} n & -1 \\ n+1 & -1 \end{pmatrix}. \tag{C.18}$$

Then $x < -1$ if and only if $n/(n+1) < L_n x < (n+1)/(n+2)$, and $0 < x < 1/(n+1)$ if and only if $1 < L_n x$. In view of Lemma 4.51 this means the map $Q \to Q_{L_n^{-1}}$ is a bijection of $W_{\mathrm{E}}^{(n)}$ onto $W_{\mathrm{HJ}}^{(n)}$. It follows that the cardinality of W_{HJ} is at most n_0 times the cardinality of W_{E}. It also provides an algorithm for calculating the set W_{HJ}, given the set W_{E}.

Lemma C.1. *Suppose $k_j \geq 2$ for all j. Then*

$$(k_1, \ldots, k_n) > (k_1, \ldots, k_{n-1}) > \cdots > (k_1, k_2) > (k_1) > 1 \tag{C.19}$$

Proof. Straightforward consequence of the definition. □

Lemma C.2. *Suppose*

$$T^{k_1} S T^{k_2} S \ldots T^{k_n} S = L^m \tag{C.20}$$

for some sequence of integers $k_1, k_2, \ldots, k_n$ all greater than 1, and some positive integer m. Then $n = \ell m$ for some positive integer ℓ, $k_{j+\ell} = k_j$ for $j = 1, \ldots, n-\ell$, and

$$L = \begin{cases} T^{k_1} S \ldots T^{k_\ell} S & m \text{ is odd} \\ \pm T^{k_1} S \ldots T^{k_\ell} S & m \text{ is even} \end{cases}. \tag{C.21}$$

Proof. Let $\bar{T}$, $\bar{S}$ be the images of T, S under the canonical projection $h\colon\ \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$, and let $\bar{R} = \bar{T}\bar{S}$. Then (see for example ref. [2]) $\bar{S}$ is order 2, $\bar{R}$ is order 3 and every element of $\mathrm{PSL}_2(\mathbb{Z})$ is either the identity or else has a unique alternating expansion of the form $\bar{M}_1 \ldots \bar{M}_n$ where (1) each $\bar{M}_j$ is either $\bar{S}$ or $\bar{R}^k$ for $k = 1$ or 2 and (2) terms equal to $\bar{S}$ alternate with terms equal to a non-zero power of $\bar{R}$. Also define $\bar{S}_1 = \bar{S}$, $\bar{S}_2 = \bar{S}\bar{R}\bar{S}$, ... Now let $\bar{L} = h(L)$ and let $\bar{L} = \bar{M}_1 \ldots \bar{M}_q$ be its expansion in terms of alternating powers of $\bar{S}$ and $\bar{R}$. It follows from Eq. (C.20) that

$$\bar{L}^m = \bar{R}\bar{S}_{k_1 - 1}\bar{R}^2\bar{S}_{k_2 - 1}\bar{R}^2 \ldots \bar{R}^2\bar{S}_{k_n - 1}\bar{R}. \tag{C.22}$$

So $\bar{M}_1 = \bar{M}_q = \bar{R}$ and

$$L = \bar{R}\bar{S}_{\kappa_1 - 1}\bar{R}^2 \dots \bar{S}_{\kappa_\ell - 1}\bar{R} \tag{C.23}$$

for some sequence of integers $\kappa_1, \dots, \kappa_\ell$ all greater than one. Eq. (C.22) and the uniqueness of the alternating expansion then imply $n = m\ell$, $k_j = \kappa_j$ for $j = 1, \dots, \ell$, and $k_{j+\ell} = k_j$ for $j = 1, \dots, n - \ell$. Eq. (C.21) then follows. □

Theorem C.3. *Let $Q = \langle a, b, c\rangle$ be a form with $a > 0$, let f be its conductor, and let*

$$\rho_{Q,+} = [l_1, \dots, l_q, \overline{k_1, \dots, k_p}] \tag{C.24}$$

(where we set $q = 0$ if $\rho_{Q,+}$ has a purely periodic expansion equal to $[\overline{k_1, \dots, k_p}]$). Assume the sequences $l_1, \dots, l_q$ and $k_1, \dots, k_p$ are as short as possible (i.e. $k_1, \dots, k_p$ is not the conjunction of 2 or more identical subsequences, and $l_q \neq k_p$). Then

$$\chi_Q(\varepsilon_f) = (T^{l_1}S \dots T^{l_q}S)(T^{k_1}S \dots T^{k_p}S)(T^{l_1}S \dots T^{l_q}S)^{-1}. \tag{C.25}$$

Proof. Assume, to begin with, that $q = 0$ and $\rho_{Q,+} = [\overline{k_1, \dots, k_p}]$. Let

$$M = T^{k_1}S \dots T^{k_p}S. \tag{C.26}$$

Then it follows from Eq. (C.7) that

$$M\rho_{Q,+} = \rho_{Q,+}. \tag{C.27}$$

In view of Lemma 4.51 this means $M \in \mathcal{S}(Q)$. It then follows from Theorem 4.53 that

$$M = s_1\chi_Q(\varepsilon_f^{s_2\lambda}) = s_1\left(\frac{d_{\lambda j_{\min}(f)} - 1}{2}I + \frac{s_2 f_{\lambda j_{\min}(f)}}{f}SQ\right) \tag{C.28}$$

where λ is a positive integer, and s_1, s_2 are signs. Comparing this expression with Eq. (C.7) one sees

$$s_1(d_{\lambda j_{\min}(f)} - 1) = \operatorname{Tr}(M) = \begin{cases} (k_1) & p = 1 \\ (k_1, k_2) - 1 & p = 2 \\ (k_1, \dots, k_p) - (k_2, \dots, k_{p-1}) & p \geq 3 \end{cases} \tag{C.29}$$

$$\frac{s_1 s_2 f_{\lambda j_{\min}(f)}}{f} = M_{21} = \begin{cases} 1 & p = 1, \\ (k_2, \dots, k_p) & p \geq 2. \end{cases} \tag{C.30}$$

In view of Lemma C.1 this means $s_1 = s_2 = +1$. So $M = (\chi_Q(\varepsilon_f))^\lambda$. It then follows from Lemma C.2 and the assumption that the sequence $k_1, \dots, k_p$ is not the conjunction of 2 or more identical subsequences, that $\lambda = 1$ and $M = \chi_Q(\varepsilon_f)$.

Now suppose $q \geq 1$. Let

$$M = T^{k_1}S \dots T^{k_p}S, \tag{C.31}$$

$$N = T^{l_1}S \dots T^{l_q}S, \tag{C.32}$$

and let $Q' = \langle a', b', c'\rangle$ be the unique form such that $[\overline{k_1, \dots, k_p}] = \rho_{Q',+}$ and $a' > 0$. It follows from the result just proved that $M = \chi_{Q'}(\varepsilon_f)$, while it follows from Eq. (C.8) that

$$N\rho_{Q',+} = \rho_{Q,+}. \tag{C.33}$$

In view of Lemma 4.51 this means $Q = Q'_{N^{-1}}$. Hence

$$\chi_Q(\varepsilon_f) = \frac{d_{r_f} - 1}{2} I + \frac{f_{r_f}}{f} S(N^{-1})^{\mathrm{T}} Q' N^{-1} = NMN^{-1} \tag{C.34}$$

□

Theorem C.4. *Let* $L = \left(\begin{smallmatrix} \gamma_1 & \delta_1 \\ \gamma_2 & \delta_2 \end{smallmatrix}\right)$ *be any element of* $\mathrm{SL}_2(\mathbb{Z})$. *Then the following statements are equivalent:*

(1) $\gamma_2 > 0$.

(2) There exists an integer $n \geq 1$ *and sequence of integers* $r_1, r_2, \ldots, r_{n+1}$ *such that* $r_i \geq 2$ *unless* $i = 1$ *or* $n+1$, *and*

$$L = T^{r_1} S T^{r_2} S \ldots S T^{r_n} S T^{r_{n+1}}. \tag{C.35}$$

If these conditions are satisfied the integer n *and sequence* $r_1, \ldots, r_{n+1}$ *are unique.*

Continue to assume the conditions are satisfied. Define

$$L_i = \begin{pmatrix} \gamma_i & \delta_i \\ \gamma_{i+1} & \delta_{i+1} \end{pmatrix} = T^{r_i} S \ldots T^{r_{n+1}}. \tag{C.36}$$

Then

$$\gamma_2 > \gamma_3 > \cdots > \gamma_{n+1}, \tag{C.37}$$

$$\frac{\delta_2}{\gamma_2} < \frac{\delta_3}{\gamma_3} < \cdots < \frac{\delta_{n+1}}{\gamma_{n+1}}, \tag{C.38}$$

$$\mathcal{D}_L = \mathcal{D}_{L_1} \subset \mathcal{D}_{L_2} \subset \cdots \subset \mathcal{D}_{L_{n+1}} = \mathbb{C}. \tag{C.39}$$

Proof. Aside from uniqueness this is proved in ref. [70]. To prove uniqueness suppose

$$T^{r_1} S T^{r_2} S \ldots S T^{r_n} S T^{r_{n+1}} = T^{r'_1} S T^{r'_2} S \ldots S T^{r'_n} S T^{r'_{n'+1}}. \tag{C.40}$$

Assume to begin with that $r_i, r'_i \geq 2$ for all i, including $i = 1, n+1$. Let $h\colon\ \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$ and $\bar{S}$, $\bar{T}$, $\bar{R}$ and $\bar{S}_i$ be as in the proof of Lemma C.2. Then

$$\bar{R}\bar{S}_{r_1 - 1}\bar{R}^2 \ldots \bar{R}^2 \bar{S}_{r_{n+1}-1} \bar{R}\bar{S}_1 = \bar{R}\bar{S}_{r'_1 - 1}\bar{R}^2 \ldots \bar{R}^2 \bar{S}_{r'_{n'+1}-1} \bar{R}\bar{S}_1 \tag{C.41}$$

which, in view of the uniqueness of the alternating expansion [2], means $n = n'$ and $r_i = r'_i$ for all i. In the general case choose integers m, l such that $r_1 + m$, $r'_1 + m$, $r_{n+1} + l$, $r'_{n'+1} + l \geq 2$. Then multiplying both sides of Eq. (C.40) by T^m on the left and T^l on the right gives

$$T^{r_1+m} S T^{r_2} S \ldots S T^{r_n} S T^{r_{n+1}+l} = T^{r'_1+m} S T^{r'_2} S \ldots S T^{r'_n} S T^{r'_{n'+1}+l}. \tag{C.42}$$

Applying the result just proved, the claim follows. □

Definition C.5 (canonical expansion; length)**.** We refer to the expression on the right hand side of Eq. (C.35) as the canonical expansion of L, and to the integer n as its length.

Lemma C.6. *Let* $R = TS$. *Then*

$$T = -RS, \tag{C.43}$$

$$T^{-1} = -SR^2, \tag{C.44}$$

and, for every positive integer m,

$$ST^{-m}S = -(TST)^m \tag{C.45}$$

Proof. Straightforward consequences of the relations $R^3 = S^2 = -I$. □

Theorem C.7. *Let $\mathcal{F}$ be a $\mathrm{GL}_2(\mathbb{Z})$ orbit of forms, let $\mathcal{F}_+$ be the subset consisting of $\langle a, b, c\rangle \in \mathcal{F}$ for which $a > 0$, and let $\mathcal{F}_{\mathrm{HJ}}$ be the set of HJ-reduced forms in $\mathcal{F}_+$. Let $p_{\min}$ be the minimum value of the period p of $\rho_{Q,+} = [\overline{k_1, \ldots, k_p}]$ as Q ranges over the set $\mathcal{F}_{\mathrm{HJ}}$. Then for all $Q \in \mathcal{F}_+$, the length of $\chi_Q(\varepsilon_f)$ is greater than or equal to $p_{\min}$.*

Remark. For a given admissible tuple t we can use this result together with theorem 4.53 to find a matrix $M \in \mathrm{GL}_2(\mathbb{Z})$ for which L_{+,t_M} has minimum length.

Proof. Let $Q \in \mathcal{F}_+$ be arbitrary. The statement is immediate if Q is HJ-reduced, so assume not. Let $L = \chi_Q(v_f)$, and $\rho_{Q,+} = [l_1, \ldots, l_q, \overline{k_1, \ldots, k_p}]$ where the sequences $l_1, \ldots, l_q$ and $k_1, \ldots, k_p$ are chosen as short as possible. It follows from Theorem C.3 that

$$L = NMN^{-1} \tag{C.46}$$

where

$$N = T^{l_1} S \ldots T^{l_q} S \tag{C.47}$$

$$M = T^{k_1} S \ldots T^{k_p} S \tag{C.48}$$

and from Theorem C.4 that

$$L = T^{r_1} S \ldots T^{r_n} S T^{r_{n+1}} \tag{C.49}$$

where $r_i \geq 2$ for $1 < i \leq n$. We have

$$LN = NM, \tag{C.50}$$

$$LN = T^{r_1} S \ldots T^{r_n} S T^m S T^{l_2} S \ldots T^{l_q} S \tag{C.51}$$

where $m = r_{n+1} + l_1$, and

$$NM = T^{l_1} S \ldots T^{l_q} S T^{k_1} S \ldots T^{k_p} S \tag{C.52}$$

The expression on the right hand side of Eq. C.52 is the canonical expansion of NM with length equal to $\mathrm{length}(N) + \mathrm{length}(M)$. If $m \geq 2$ the expression on the right hand side of Eq. (C.51) is the canonical expansion of $LN = NM$ which, in view of Theorem C.4, means $\mathrm{length}(L) + \mathrm{length}(N) = \mathrm{length}(N) + \mathrm{length}(M)$ implying $\mathrm{length}(L) = \mathrm{length}(M) \geq p_{\min}$. Suppose $m < 2$. There are three cases to consider:

Case 1. $m = 1$. Then

$$LN = T^{r_1} S \ldots T^{r_n} S T S T^{l_2} S \ldots T^{l_q} S \tag{C.53}$$

Using Eq. (C.45) this becomes

$$LN = T^{r_1} S \ldots T^{r_n - 1} S T^{l_2 - 1} S \ldots T^{l_q} S \tag{C.54}$$

One goes on in this way, making repeated applications of Eq. (C.45), until one obtains an expansion in canonical form. Each application of Eq. (C.45) reduces the number of S operators, so the length of the expansion which results will be less than $l + r$. It follows that $\mathrm{length}(L) + \mathrm{length}(N) > \mathrm{length}(LN) = \mathrm{length}(NM) = \mathrm{length}(N) + \mathrm{length}(M)$, implying $\mathrm{length}(L) > \mathrm{length}(M) \geq p_{\min}$.

Case 2. $m = 0$. Then

$$LN = -T^{r_1} S \ldots T^{r_{n-1}} S T^{r_n + l_2} S T^{l_3} S \ldots T^{l_q} S. \tag{C.55}$$

Writing $LN = NM = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, Theorem C.4 applied to the expansion on the right hand side of (C.52) implies $\gamma > 0$, while the same theorem applied to the expansion on the right hand side of (C.55) implies $\gamma < 0$. It follows that this case is not possible.

Case 3. $m < 0$. It follows from Lemma C.6 that

$$LN = -T^{r_1} S \dots T^{r_n+1} S (T^2 S)^{|m|-1} T^{l_2+1} S \dots T^{l_q} S. \tag{C.56}$$

which is not possible for the same reason that case 2 is not possible. □

Appendix D. Shintani–Faddeev Jacobi cocycle

The definition of the SF Jacobi cocycle given in Definition 1.16 is a slightly modified version of the definition given in ref. [70]. The purpose of this Appendix is, firstly to explain that modification, secondly to explain how $\sigma_M(z,\tau)$ is defined when $\tau \notin \mathbb{H}$, and thirdly to prove the cocycle condition, Eq. (1.22).

Let $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. In ref. [70] the domain of $\sigma_M(z,\tau)$ is denoted $\mathbb{C} \times U_M$. If $\gamma \neq 0$, or if $\gamma = 0$ and $\delta > 0$ then $U_M = \mathcal{D}_M$. If, on the other hand, $\gamma = 0$ and $\delta < 0$ then $U_M = \mathbb{H}$ whereas $\mathcal{D}_M = \mathbb{C} \setminus \mathbb{R}$.

If $\tau \in \mathbb{H}$ then the value of $\sigma_M(z,\tau)$ is given by Eq. (1.21). There are two cases to consider. The first case is when either $\gamma \neq 0$, or $\gamma = 0, \delta > 0$, implying $\mathcal{D}_M$ has a non-empty intersection with $\mathbb{R}$. It is shown in ref. [70] that one can then meromorphically continue from $\mathbb{C} \times \mathbb{H}$ to the whole of $\mathbb{C} \times \mathcal{D}_M = \mathbb{C} \times U_M$. The second case is when $\gamma = 0, \delta < 0$, implying $\mathcal{D}_M \cap \mathbb{R} = \emptyset$, so that one cannot meromorphically continue. This is why in ref. [70] the domain is taken to be $\mathbb{C} \times \mathbb{H}$. However, there is a way round the problem. Observe that

$$\gamma = 0, \delta > 0 \qquad \Longleftrightarrow \qquad M = T^k, \qquad \text{for some } k \in \mathbb{Z}, \tag{D.1}$$

$$\gamma = 0, \delta < 0 \qquad \Longleftrightarrow \qquad M = -T^k, \qquad \text{for some } k \in \mathbb{Z}. \tag{D.2}$$

In the first case it follows from Eqs. (1.19) and (1.21) that if $\tau \in \mathbb{H}$ then

$$\sigma_{T^k}(z,\tau) = \frac{\varpi(z,\tau+k)}{\varpi(z,\tau)} = \frac{\varpi(z,\tau)}{\varpi(z,\tau)} = 1. \tag{D.3}$$

for all $k \in \mathbb{Z}$. Since $\mathcal{D}_{T^k} = \mathbb{C}$, we can use meromorphic continuation to extend this result to the whole of the complex plane:

Lemma D.1. *For any integer k,*

$$\sigma_{T^k}(z,\tau) = 1, \tag{D.4}$$

for all z, $\tau \in \mathbb{C}$.

Suppose, on the other hand, that $\gamma = 0, \delta < 0$. Then it follows from Eqs. (1.19) and (1.21) that if $\tau \in \mathbb{H}$,

$$\begin{aligned} \sigma_{-T^k}(z,\tau) &= \frac{\varpi(-z,\tau+k)}{\varpi(z,\tau)} \\ &= \frac{\varpi(-z,\tau)}{\varpi(z,\tau)} \\ &= \left(\frac{\varpi\left(z,-\frac{1}{\tau}\right)}{\varpi(z,\tau)}\right)\left(\frac{\varpi(-z,\tau)}{\varpi\left(\frac{z}{\tau},-\frac{1}{\tau}\right)}\right) \end{aligned}$$

$$= \sigma_S(z,\tau)\,\sigma_S\left(\frac{z}{\tau}, -\frac{1}{\tau}\right) \tag{D.5}$$

Since neither side of this equation is defined for $\tau \in \mathbb{R}$ we cannot meromorphically continue to the lower half-plane. However, since the right hand side is defined and meromorphic for $\tau \in -\mathbb{H}$, we can take the equation to be the definition of $\sigma_{-T^k}(z,\tau)$ for all $\tau \in \mathcal{D}_{-T^k} = \mathbb{C} \setminus \mathbb{R}$:

Definition D.2. For any integer k define

$$\sigma_{-T^k}(z,\tau) = \sigma_S(z,\tau)\,\sigma_S\left(\frac{z}{\tau}, -\frac{1}{\tau}\right) \tag{D.6}$$

for all $z \in \mathbb{C}$, $\tau \in \mathcal{D}_{-T^k}$.

Remark. Note that $\sigma_{-T^k}(z,\tau) = \sigma_{-I}(z,\tau)$, independent of k.

We now turn to the third task of this appendix, of showing that the SF Jacobi cocycle satisfies the cocycle condition

$$\sigma_{MM'}(z,\tau) = \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(z,\tau)\,. \tag{D.7}$$

for all values of τ in the set

$$\mathcal{D}_{M,M'} = \mathcal{D}_{MM'} \cap {M'}^{-1}\mathcal{D}_M \cap \mathcal{D}_{M'} \tag{D.8}$$

for which both sides of the equation are defined.

The fact that the condition is satisfied when $\tau \in \mathbb{H}$ is an immediate consequence of the definition. If $\mathcal{D}_{M,M'} \cap \mathbb{R}$ has non-empty interior then it follows from meromorphic continuation that the condition also holds in the lower half plane. However, this argument does not always work. Suppose, for instance

$$M = \begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix}, \qquad\qquad M' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{D.9}$$

Then one easily sees $\mathcal{D}_{M,M'} \cap \mathbb{R} = \emptyset$. We now show that, notwithstanding this difficulty, the relation does in fact hold for all $\tau \in \mathcal{D}_{M,M'}$. We begin with some preliminary results.

Lemma D.3.

$$\mathcal{D}_{M,M'} = \mathcal{D}_{MM'} \cap \mathcal{D}_{M'} = \mathcal{D}_{MM'} \cap (M')^{-1}\mathcal{D}_M = \mathcal{D}_{M'} \cap (M')^{-1}\mathcal{D}_M \tag{D.10}$$

Proof. Straightforward consequence of the definitions. □

Lemma D.4. *For all $z \in \mathbb{C}$, $\tau \in \mathcal{D}_{S^{-1}}$*

$$\sigma_{S^{-1}}(z,\tau) = \frac{1}{\sigma_S\left(-\frac{z}{\tau}, -\frac{1}{\tau}\right)}. \tag{D.11}$$

Proof. If $\tau \in \mathbb{H}$ then

$$\sigma_{S^{-1}}(z,\tau) = \frac{\varpi\left(-\frac{z}{\tau}, -\frac{1}{\tau}\right)}{\varpi(z,\tau)} = \frac{1}{\sigma_S\left(-\frac{z}{\tau}, -\frac{1}{\tau}\right)}. \tag{D.12}$$

We now meromorphically continue to all $\tau \in \mathcal{D}_{S^{-1}} = \{\tau \in \mathbb{C}\colon\ -\tau^{-1} \in \mathcal{D}_S\}$. □

Lemma D.5. *σ_S, $\sigma_{S^{-1}}$ satisfy the identities:*

$$\sigma_S\left(\frac{z}{\tau},\frac{1}{\tau}\right) = \sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right) e^{\frac{\pi i(\tau-1)z}{\tau}}\sigma_S(z,\tau) \qquad z\in\mathbb{C},\tau\in\mathcal{D}_S, \tag{D.13}$$

$$\sigma_{S^{-1}}\left(\frac{z}{\tau},-\frac{1}{\tau}\right) = \sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right) e^{\frac{\pi i(\tau-1)z}{\tau}}\sigma_{S^{-1}}(z,-\tau) \qquad z\in\mathbb{C},\tau\in\mathcal{D}_{S^{-1}} \tag{D.14}$$

$$\sigma_S(z,\tau)\,\sigma_S(-z,\tau) = -i\csc(\pi z)\sin\left(\frac{\pi z}{\tau}\right) e^{\frac{\pi i z^2}{\tau}} e^{\frac{\pi i}{6}\left(\tau+\frac{1}{\tau}\right)} \qquad z\in\mathbb{C},\tau\in\mathcal{D}_S \tag{D.15}$$

$$\sigma_{S^{-1}}(z,\tau)\,\sigma_{S^{-1}}(-z,\tau) = -i\csc(\pi z)\sin\left(\frac{\pi z}{\tau}\right) e^{\frac{\pi i z^2}{\tau}} e^{\frac{\pi i}{6}\left(\tau+\frac{1}{\tau}\right)} \qquad z\in\mathbb{C},\tau\in\mathcal{D}_{S^{-1}} \tag{D.16}$$

Proof. Using the identities [70]

$$\mathrm{Sin}_2(z+1,\tau) = \frac{\mathrm{Sin}_2(z,\tau)}{2\sin\left(\frac{\pi z}{\tau}\right)} \tag{D.17}$$

$$\mathrm{Sin}_2(z+\tau,\tau) = \frac{\mathrm{Sin}_2(z,\tau)}{2\sin\left(\pi z\right)} \tag{D.18}$$

$$\mathrm{Sin}_2\left(\frac{z}{\tau},\frac{1}{\tau}\right) = \mathrm{Sin}_2(z,\tau) \tag{D.19}$$

and the fact that $\tau\in\mathcal{D}_S \iff \tau^{-1}\in\mathcal{D}_S$ in Eq. (8.6) we find

$$\begin{aligned}
\sigma_S\left(\frac{z}{\tau},\frac{1}{\tau}\right) &= \frac{e^{\frac{\pi i\tau}{12}\left(\frac{6z^2}{\tau^2}+6\left(1-\frac{1}{\tau}\right)\frac{z}{\tau}+\frac{1}{\tau^2}-\frac{3}{\tau}+1\right)}}{\mathrm{Sin}_2\left(\frac{z}{\tau}+1,\frac{1}{\tau}\right)} \\
&= \frac{e^{\frac{\pi i}{12\tau}\left(6z^2-6(1-\tau)z+\tau^2-3\tau+1\right)}}{\mathrm{Sin}_2(z+\tau,\tau)} \\
&= \frac{2\sin(\pi z)e^{\frac{\pi i(\tau-1)z}{\tau}}e^{\frac{\pi i}{12\tau}\left(6z^2+6(1-\tau)z+\tau^2-3\tau+1\right)}}{\mathrm{Sin}_2(z,\tau)} \\
&= \sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right) e^{\frac{\pi i(\tau-1)z}{\tau}}\sigma_S(z,\tau)
\end{aligned} \tag{D.20}$$

for all $z\in\mathbb{C}$, $\tau\in\mathcal{D}_S$, which establishes Eq. (D.13).

To prove Eq. (D.14) observe it follows from Lemma D.4 and Eq. (D.13) that

$$\begin{aligned}
\sigma_{S^{-1}}\left(\frac{z}{\tau},-\frac{1}{\tau}\right) &= \frac{1}{\sigma_S(z,\tau)} \\
&= \frac{\sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right) e^{\frac{\pi i(\tau-1)z}{\tau}}}{\sigma_S\left(\frac{z}{\tau},\frac{1}{\tau}\right)} \\
&= \sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right) e^{\frac{\pi i(\tau-1)z}{\tau}}\sigma_{S^{-1}}(z,-\tau)\,.
\end{aligned} \tag{D.21}$$

for all $\tau\in\mathcal{D}_{S^{-1}}$.

To prove Eq. (D.15) observe that if $\mathrm{Re}(\tau)>0$ and $-\mathrm{Re}(\tau)<\mathrm{Re}(z)<1$ then we can use Eq. (8.7) to deduce

$$\begin{aligned}
&\mathrm{Sin}_2(-z+1,\tau)\,\mathrm{Sin}_2(z+\tau,\tau) \\
&\qquad = \exp\left(-\int_0^\infty\left(\frac{\sinh\left(\frac{\tau-1+2z}{2}\right)t}{2\sinh\left(\frac{t}{2}\right)\sinh\left(\frac{\tau t}{2}\right)}-\frac{\tau-1+2z}{\tau t}\right)\frac{dt}{t}\right)
\end{aligned}$$

$$\times \exp\left(-\int_0^\infty \left(\frac{\sinh\left(\frac{-\tau+1-2z}{2}\right)}{2\sinh\left(\frac{t}{2}\right)\sinh\left(\frac{\tau t}{2}\right)} - \frac{-\tau+1-2z}{\tau t}\right)\frac{dt}{t}\right)$$
$$= 1. \tag{D.22}$$

In view of Eqs. (D.17) and (D.18) this means

$$\begin{aligned}\operatorname{Sin}_2(-z+1,\tau)\operatorname{Sin}_2(z+1,\tau) &= \frac{\operatorname{Sin}_2(-z+1,\tau)\operatorname{Sin}_2(z,\tau)}{2\sin\left(\frac{\pi z}{\tau}\right)}\\ &= \frac{\sin(\pi z)\operatorname{Sin}_2(-z+1,\tau)\operatorname{Sin}_2(z+\tau,\tau)}{\sin\left(\frac{\pi z}{\tau}\right)}\\ &= \sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right).\end{aligned} \tag{D.23}$$

Using Eq. (8.6) we deduce

$$\begin{aligned}\sigma_S(z,\tau)\,\sigma_S(-z,\tau) &= \frac{e^{\frac{\pi i}{12\tau}\left(6z^2+6(1-\tau)z+\tau^2-3\tau+1\right)}e^{\frac{\pi i}{12\tau}\left(6z^2-6(1-\tau)z+\tau^2-3\tau+1\right)}}{\operatorname{Sin}_2(z+1,\tau)\operatorname{Sin}_2(-z+1,\tau)}\\ &= -i\csc(\pi z)\sin\left(\frac{\pi z}{\tau}\right)e^{\frac{\pi i z^2}{\tau}}e^{\frac{\pi i}{6}\left(\tau+\frac{1}{\tau}\right)}\end{aligned} \tag{D.24}$$

for all z,τ such that $\operatorname{Re}(\tau)>0$ and $-\operatorname{Re}(\tau)<\operatorname{Re}(z)<1$. We then use meromorphic continuation to deduce that the relation holds for all $z\in\mathbb{C}$, $\tau\in\mathcal{D}_S$.

Finally, to prove Eq. (D.16), use Lemma D.4 and Eq. (D.15) to deduce

$$\begin{aligned}\sigma_{S^{-1}}(z,\tau)\,\sigma_{S^{-1}}(-z,\tau) &= \frac{1}{\sigma_S\left(-\frac{z}{\tau},-\frac{1}{\tau}\right)\sigma_S\left(\frac{z}{\tau},-\frac{1}{\tau}\right)}\\ &= \frac{1}{-i\csc\left(\frac{\pi z}{\tau}\right)\sin\left(-\pi z\right)e^{-\frac{\pi i z^2}{\tau}}e^{-\frac{\pi i}{6}\left(\tau+\frac{1}{\tau}\right)}}\\ &= -i\csc(\pi z)\sin\left(\frac{\pi z}{\tau}\right)e^{\frac{\pi i z^2}{\tau}}e^{\frac{\pi i}{6}\left(\tau+\frac{1}{\tau}\right)}\end{aligned} \tag{D.25}$$

for all $z\in\mathbb{C}$, $\tau\in\mathcal{D}_{S^{-1}}$. □

Lemma D.6. *, σ_{-T^k} can be expressed in terms of σ_S, $\sigma_{S^{-1}}$ in the four equivalent ways:*

$$\sigma_{-T^k}(z,\tau) = \begin{cases}\sigma_S(z,\tau)\,\sigma_S\left(\frac{z}{\tau},-\frac{1}{\tau}\right)\\ \sigma_{S^{-1}}(z,\tau)\,\sigma_{S^{-1}}\left(-\frac{z}{\tau},-\frac{1}{\tau}\right)\\ -\sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right)e^{-\frac{\pi i(\tau+1)z}{\tau}}\sigma_S(z,\tau)\,\sigma_S(-z,-\tau)\\ \sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right)e^{-\frac{\pi i(\tau-1)z}{\tau}}\sigma_{S^{-1}}(z,\tau)\,\sigma_{S^{-1}}(-z,-\tau)\end{cases} \tag{D.26}$$

For all $z\in\mathbb{C}$, $\tau\in\mathcal{D}_{-T^k}$, $k\in\mathbb{Z}$.

Also

$$\sigma_{-T^k}(-z,-\tau) = -e^{-2\pi i z}\sigma_{-T^k}(z,\tau) \qquad k\in\mathbb{Z}, z\in\mathbb{C}, \tau\in\mathcal{D}_{-T^k}, \tag{D.27}$$

$$\sigma_{-T^k}(z,\tau+n) = \sigma_{-T^k}(z,\tau) \qquad k,n\in\mathbb{Z}, z\in\mathbb{C}, \tau\in\mathcal{D}_{-T^k}, \tag{D.28}$$

$$\sigma_{-T^k}(z,\tau)\,\sigma_{-T^k}(-z,\tau) = 1 \qquad k\in\mathbb{Z}, z\in\mathbb{C}, \tau\in\mathcal{D}_{-T^k}. \tag{D.29}$$

Proof. The first expression in Eq. (D.26) is that in Definition D.2. To prove the second use Lemma D.4 and Eq. (D.16) to deduce

$$\begin{aligned}\sigma_{-T^k}(z,\tau) &= \sigma_S(z,\tau)\,\sigma_S\left(\frac{z}{\tau},-\frac{1}{\tau}\right)\\ &= \frac{1}{\sigma_{S^{-1}}\left(\frac{z}{\tau},-\frac{1}{\tau}\right)\sigma_{S^{-1}}(-z,\tau)}\\ &= -\frac{\sigma_{S^{-1}}\left(-\frac{z}{\tau},-\frac{1}{\tau}\right)\sigma_{S^{-1}}(z,\tau)}{\csc\left(\frac{\pi z}{\tau}\right)\sin(-\pi z)e^{-\frac{\pi i z^2}{\tau}}e^{-\frac{\pi i}{6}\left(\tau+\frac{1}{\tau}\right)}\csc(\pi z)\sin\left(\frac{\pi z}{\tau}\right)e^{\frac{\pi i z^2}{\tau}}e^{\frac{\pi i}{6}\left(\tau+\frac{1}{\tau}\right)}}\\ &= \sigma_{S^{-1}}(z,\tau)\,\sigma_{S^{-1}}\left(-\frac{z}{\tau},-\frac{1}{\tau}\right)\end{aligned} \tag{D.30}$$

for all $z\in\mathbb{C}$, $\tau\in\mathcal{D}_{-T^k}$.

To prove the third expression in Eq. (D.26) use Eq. (D.13) to deduce

$$\begin{aligned}\sigma_{-T^k}(z,\tau) &= \sigma_S(z,\tau)\,\sigma_S\left(\frac{z}{\tau},-\frac{1}{\tau}\right)\\ &= \sigma_S(z,\tau)\left(\sin(-\pi z)\csc\left(\frac{\pi z}{\tau}\right)e^{-\frac{\pi(\tau+1)z}{\tau}}\sigma_S(-z,-\tau)\right)\\ &= -\sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right)e^{-\frac{\pi(\tau+1)z}{\tau}}\sigma_S(z,\tau)\,\sigma_S(-z,-\tau)\,.\end{aligned} \tag{D.31}$$

To prove the last expression in Eq. (D.26) use the second expression in Eq. (D.26) together with Eq. (D.14) to deduce

$$\begin{aligned}\sigma_{-T^k}(z,\tau) &= \sigma_{S^{-1}}(z,\tau)\,\sigma_{S^{-1}}\left(-\frac{z}{\tau},-\frac{1}{\tau}\right)\\ &= \sigma_{S^{-1}}(z,\tau)\left(\sin(-\pi z)\csc\left(-\frac{\pi z}{\tau}\right)e^{-\frac{\pi i(\tau-1)z}{\tau}}\sigma_{S^{-1}}(-z,-\tau)\right)\\ &= \sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right)e^{-\frac{\pi i(\tau-1)z}{\tau}}\sigma_{S^{-1}}(z,\tau)\,\sigma_{S^{-1}}(-z,-\tau)\,.\end{aligned} \tag{D.32}$$

To prove Eq. (D.27) use the third expression in Eq. (D.26) to deduce

$$\begin{aligned}\sigma_{-T^k}(-z,-\tau) &= -\sin(-\pi z)\csc\left(\frac{\pi z}{\tau}\right)e^{-\frac{\pi i(-\tau+1)z}{\tau}}\sigma_S(z,\tau)\,\sigma_S(-z,-\tau)\\ &= e^{2\pi i z}\sin(\pi z)\csc\left(\frac{\pi z}{\tau}\right)e^{-\frac{\pi i(\tau+1)z}{\tau}}\sigma_S(z,\tau)\,\sigma_S(-z,-\tau)\\ &= e^{2\pi i z}\sigma_S(z,\tau)\,\sigma_S(-z,-\tau)\,.\end{aligned} \tag{D.33}$$

To prove Eq. (D.28) observe that, if $\tau\in\mathbb{H}$, then it follows from Definitions 1.14 and 1.16 that

$$\sigma_{-T^k}(z,\tau+n) = \frac{\varpi(-z,\tau+n+k)}{\varpi(z,\tau+n)} = \frac{\varpi(-z,\tau+k)}{\varpi(z,\tau)} = \sigma_{-T^k}(z,\tau)\,. \tag{D.34}$$

If $\tau\in-\mathbb{H}$ it follows from this result together with Eq. (D.27) that

$$\sigma_{-T^k}(z,\tau+n) = -e^{2\pi i z}\sigma_{-T^k}(-z,-\tau-n) = -e^{2\pi i z}\sigma_{-T^k}(-z,-\tau) = \sigma_{-T^k}(z,\tau)\,. \tag{D.35}$$

Finally, to prove Eq. (D.29), use the third expression in Eq. (D.26) together with Eq. (D.15) to deduce

$$\sigma_{-T^k}(z,\tau)\,\sigma_{-T^k}(-z,\tau) = \sin^2(\pi z)\csc^2\left(\frac{\pi z}{\tau}\right)\sigma_S(z,\tau)\,\sigma_S(-z,\tau)\,\sigma_S(z,-\tau)\,\sigma_S(-z,-\tau)$$

$$= 1. \tag{D.36}$$

□

Theorem D.7. *Eq.* (D.7) *holds for all* $M, M' \in \mathrm{SL}_2(\mathbb{Z})$ *and all* $\tau \in \mathcal{D}_{M,M'}$,

Proof. Eq. (D.7) is an immediate consequence of the definitions if $\tau \in \mathbb{H}$. If $\mathcal{D}_{M,M'} \cap \mathbb{R}$ has non-empty interior we can use meromorphic continuation to deduce that it holds for all $\tau \in \mathcal{D}_{M,M'}$. It remains to prove the result for the cases when that is not the case. We group these as follows:

(1) All three of M, M', MM' are in $\langle -I, T\rangle$,
(2) Exactly one of M, M', MM' is in $\langle -I, T\rangle$,
(3) None of M, M', MM' are in $\langle -I, T\rangle$

(the fact that $\langle -I, T\rangle$ is a group means that if any two of M, M', MM' are in $\langle -I, T\rangle$, then so is the third).

Case 1. Referring to Lemma D.3 we see that if M, M' are both in $\langle T\rangle$ then $\mathcal{D}_{M,M'} = \mathbb{C}$ is connected. So the fact that $\mathcal{D}_{M,M'}$ is disconnected means one of the following must apply:

M	M'	$\mathcal{D}_{M,M'}$	$\sigma_{MM'}(z,\tau)$	$\sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\tau\right)\sigma_{M'}(z,\tau)$
T^k	$-T^{k'}$	$\mathbb{C}\setminus\mathbb{R}$	$\sigma_{-I}(z,\tau)$	$\sigma_{-I}(z,\tau)$
$-T^k$	$T^{k'}$	$\mathbb{C}\setminus\mathbb{R}$	$\sigma_{-I}(z,\tau)$	$\sigma_{-I}(z,\tau+k')$
$-T^k$	$-T^{k'}$	$\mathbb{C}\setminus\mathbb{R}$	1	$\sigma_{-I}(-z,\tau+k')\,\sigma_{-I}(z,\tau)$

where we use the fact that $\sigma_{T^k}(z,\tau) = 1$,$\sigma_{-T^k}(z,\tau) = \sigma_{-I}(z,\tau) = 1$ for all $k \in \mathbb{Z}$. The statement follows from this and Eqs. (D.28), (D.29).

Case 2. There are three possibilities to consider.

(a) $M \in \langle -I, T\rangle$, $M' = \left(\begin{smallmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{smallmatrix}\right)$ with $\gamma' \neq 0$. If $M \in \langle T\rangle$ then it follows from Lemma D.3 that $\mathcal{D}_{M,M'} \cap \mathbb{R} = \mathcal{D}_{M'} \cap {M'}^{-1}\mathbb{R}$ has non-empty interior. So $M = -T^k$ for some $k \in \mathbb{Z}$. Define

$$M'' = T^k M' = \begin{pmatrix}\alpha' + k\gamma' & \beta' + k\delta'\\ \gamma' & \delta'\end{pmatrix}, \tag{D.37}$$

and

$$I_+ = \left\{\tau \in \mathbb{R}\colon \tau > -\frac{\delta'}{\gamma'}\right\} \tag{D.38}$$

$$I_- = \left\{\tau \in \mathbb{R}\colon \tau < -\frac{\delta'}{\gamma'}\right\} \tag{D.39}$$

$$J_+ = \{\tau \in \mathbb{R}\colon (\alpha' + k\gamma')\tau + (\beta' + k\delta') > 0\} \tag{D.40}$$

$$J_- = \{\tau \in \mathbb{R}\colon (\alpha' + k\gamma')\tau + (\beta' + k\delta') < 0\}. \tag{D.41}$$

Suppose $\gamma' < 0$. Using Lemma D.3 we find

$$\mathcal{D}_{S,SM''} \cap \mathbb{R} = \mathcal{D}_{-M''} \cap \mathcal{D}_{SM''} \cap \mathbb{R} = I_+ \cap J_+, \tag{D.42}$$

$$\mathcal{D}_{S,M''} \cap \mathbb{R} = \mathcal{D}_{SM''} \cap \mathcal{D}_{M''} \cap \mathbb{R} = I_- \cap J_+. \tag{D.43}$$

Since $-\frac{\delta'}{\gamma'} \in J_+$ it follows that $\mathcal{D}_{S,SM''} \cap \mathbb{R}$ and $\mathcal{D}_{S,M''} \cap \mathbb{R}$ both have non-empty interiors. It is easily seen that $\mathcal{D}_{T^k,M'} \cap \mathbb{R}$ also has non-empty interior. So by three applications of the cocycle

condition, Eq. (D.7), together with Eqs. (2.44), (D.4), (D.26) and (D.28) we find

$$\begin{aligned}
\sigma_{MM'}(z,\tau) = \sigma_{-M''}(z,\tau) &= \sigma_S\left(\frac{z}{j_{SM''}(\tau)}, SM''\cdot\tau\right)\sigma_{SM''}(z,\tau)\\
&= \sigma_S\left(\frac{z}{j_S(M''\cdot\tau)j_{M''}(\tau)}, -\frac{1}{M''\cdot\tau}\right)\sigma_S\left(\frac{z}{J_{M''}(\tau)}, M''\cdot\tau\right)\sigma_{M''}(z,\tau)\\
&= \sigma_S\left(\frac{z}{(M''\cdot\tau)j_{M''}(\tau)}, -\frac{1}{M''\cdot\tau}\right)\sigma_S\left(\frac{z}{j_{M''}(\tau)}, M''\cdot\tau\right)\sigma_{M''}(z,\tau)\\
&= \sigma_{-T^k}\left(\frac{z}{j_{M''}(\tau)}, M''\cdot\tau\right)\sigma_{M''}(z,\tau)\\
&= \sigma_{-T^k}\left(\frac{z}{j_{T^kM'}(\tau)}, T^kM'\cdot\tau\right)\sigma_{T^kM'}(z,\tau)\\
&= \sigma_{-T^k}\left(\frac{z}{j_{T^k}(M'\cdot\tau)j_{M'}(\tau)}, M'\cdot\tau + k\right)\sigma_{T^k}\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(z,\tau)\\
&= \sigma_{-T^k}\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(\tau,z)\\
&= \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(\tau,z) \qquad \text{(D.44)}
\end{aligned}$$

for all $\tau \in \mathcal{D}_{M,M'}$.

Suppose, on the other hand, that $\gamma' > 0$. Using Lemma D.3 we find

$$\mathcal{D}_{S^{-1},S^{-1}M''} \cap \mathbb{R} = \mathcal{D}_{-M''} \cap \mathcal{D}_{S^{-1}M''} \cap \mathbb{R} = I_- \cap J_-, \qquad \text{(D.45)}$$

$$\mathcal{D}_{S^{-1},M''} \cap \mathbb{R} = \mathcal{D}_{S^{-1}M''} \cap \mathcal{D}_{M''} \cap \mathbb{R} = I_+ \cap J_-. \qquad \text{(D.46)}$$

Since $-\frac{\delta'}{\gamma'} \in J_-$ it follows that $\mathcal{D}_{S^{-1},S^{-1}M''} \cap \mathbb{R}$ and $\mathcal{D}_{S^{-1},M''} \cap \mathbb{R}$ both have non-empty interiors. So by an argument paralleling that leading to Eq. (D.44) but with S replaced with S^{-1} we again find

$$\sigma_{MM'}(z,\tau) = \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(\tau,z) \qquad \text{(D.47)}$$

for all $\tau \in \mathcal{D}_{M,M'}$.

(b) $M' \in \langle -I, T\rangle$, $M = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ with $\gamma \neq 0$. If $M' \in \langle T\rangle$ then it follows from Lemma D.3 that $\mathcal{D}_{M,M'} \cap \mathbb{R} = \mathcal{D}_{MM'} \cap \mathbb{R}$ has non-empty interior. So $M' = -T^k$ for some $k \in \mathbb{Z}$. Define

$$M'' = MT^k = \begin{pmatrix}\alpha & k\alpha+\beta\\ \gamma & k\gamma+\delta\end{pmatrix}, \qquad \text{(D.48)}$$

and

$$I_+ = \left\{\tau \in \mathbb{R}^\times : \tau > -\left(k + \frac{\delta}{\gamma}\right)\right\}, \qquad I_- = \left\{\tau \in \mathbb{R}^\times : \tau < -\left(k + \frac{\delta}{\gamma}\right)\right\}, \qquad \text{(D.49)}$$

$$J_+ = \left\{\tau \in \mathbb{R}^\times : \frac{1}{\tau} > k + \frac{\delta}{\gamma}\right\}, \qquad J_- = \left\{\tau \in \mathbb{R}^\times : \frac{1}{\tau} < k + \frac{\delta}{\gamma}\right\}, \qquad \text{(D.50)}$$

$$\mathbb{R}_+ = \{\tau \in \mathbb{R}^\times : \tau > 0\}, \qquad \mathbb{R}_- = \{\tau \in \mathbb{R}^\times : \tau < 0\}. \qquad \text{(D.51)}$$

Suppose $\gamma < 0$. Using Lemma D.3 we find

$$\mathcal{D}_{M''S,S} \cap \mathbb{R} = \mathcal{D}_{-M''} \cap \mathcal{D}_S \cap \mathbb{R} = I_+ \cap \mathbb{R}_+, \qquad \text{(D.52)}$$

$$\mathcal{D}_{M'',S} \cap \mathbb{R} = \mathcal{D}_{M''S} \cap \mathcal{D}_S \cap \mathbb{R} = J_+ \cap \mathbb{R}_+. \tag{D.53}$$

It follows that $\mathcal{D}_{M''S,S} \cap \mathbb{R}$ and $\mathcal{D}_{M'',S} \cap \mathbb{R}$ both have non-empty interiors. It is easily seen that $\mathcal{D}_{M,T^k} \cap \mathbb{R}$ also has non-empty interior. So by three applications of the cocycle condition, Eq. (D.7), together with Eqs. (D.4), and (D.26) we find

$$\begin{aligned}
\sigma_{MM'}(z,\tau) = \sigma_{-M''}(z,\tau) &= \sigma_{M''S}\left(\frac{z}{\tau}, -\frac{1}{\tau}\right)\sigma_S(z,\tau) \\
&= \sigma_{M''}(-z,\tau)\,\sigma_S\left(\frac{z}{\tau}, -\frac{1}{\tau}\right)\sigma_S(z,\tau) \\
&= \sigma_{MT^k}(-z,\tau)\,\sigma_{-T^k}(z,\tau) \\
&= \sigma_M(-z,\tau+k)\,\sigma_{T^k}(-z,\tau)\,\sigma_{-T^k}(z,\tau) \\
&= \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(z,\tau)\,.
\end{aligned} \tag{D.54}$$

for all $\tau \in \mathcal{D}_{M,M'}$.

Suppose, on the other hand, $\gamma > 0$. Using Lemma D.3 we find

$$\mathcal{D}_{M''S^{-1},S^{-1}} \cap \mathbb{R} = \mathcal{D}_{-M''} \cap \mathcal{D}_{S^{-1}} \cap \mathbb{R} = I_- \cap \mathbb{R}_-, \tag{D.55}$$

$$\mathcal{D}_{M'',S^{-1}} \cap \mathbb{R} = \mathcal{D}_{M''S^{-1}} \cap \mathcal{D}_{S^{-1}} \cap \mathbb{R} = J_- \cap \mathbb{R}_-. \tag{D.56}$$

It follows that $\mathcal{D}_{M''S^{-1},S^{-1}} \cap \mathbb{R}$ and $\mathcal{D}_{M'',S^{-1}} \cap \mathbb{R}$ both have non-empty interiors. So by an argument paralleling that leading to Eq. (D.54) but with S replaced with S^{-1} we again find

$$\sigma_{MM'}(z,\tau) = \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(\tau,z) \tag{D.57}$$

for all $\tau \in \mathcal{D}_{M,M'}$.

(c) $MM' \in \langle -I, T\rangle$. If $MM' \in \langle T\rangle$ then $\mathcal{D}_{M,M'} \cap \mathbb{R} = \mathcal{M}' \cap \mathbb{R}$ has non-empty interior, contrary to assumption. So $MM' = -T^k$ for some integer k. Observe that $\mathcal{D}_{M,-M'} \cap \mathbb{R} = \mathcal{D}_{-M'} \cap \mathbb{R}$ has non-empty interior. We can therefore apply the cocycle condition, Eq. (D.7), together with Eq. (D.4) to deduce

$$1 = \sigma_{-MM'}(-z,\tau) = \sigma_M\left(-\frac{z}{j_{-M'}(\tau)}, M'\cdot\tau\right)\sigma_{-M'}(-z,\tau)\,. \tag{D.58}$$

for all $z \in \mathbb{C}$, $\tau \in \mathcal{D}_{M,-M'}$. Notice that, although $\mathcal{D}_{M',-I} \cap \mathbb{R} = \emptyset$, it is shown in Case 2(b) above that we can still use the cocycle condition to deduce

$$\sigma_{-M'}(-z,\tau) = \sigma_{M'}(z,\tau)\,\sigma_{-I}(-z,\tau) \tag{D.59}$$

for all $z \in \mathbb{C}$, $\tau \in \mathbb{C} \setminus \mathbb{R}$. Substituting this result into Eq. (D.58) and multiplying both sides by $\sigma_{-I}(z,\tau)$ gives

$$\sigma_{-I}(z,\tau) = \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\tau\right)\sigma_{M'}(z,\tau)\,\sigma_{-I}(-z,\tau)\,\sigma_{-I}(z,\tau) \tag{D.60}$$

for all $z \in \mathbb{C}$, $\tau \in \mathbb{C} \setminus \mathbb{R}$. Using Eq. (D.29) this becomes

$$\sigma_{-I}(z,\tau) = \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(z,\tau) \tag{D.61}$$

for all $z \in \mathbb{C}$, $\tau \in \mathbb{C} \setminus \mathbb{R}$. Since $\sigma_{-I}(z,\tau) = \sigma_{-T^k}(z,\tau)$ this means

$$\sigma_{MM'}(z,\tau) = \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(z,\tau) \tag{D.62}$$

for all $z \in \mathbb{C}$, $\tau \in \mathcal{D}_{M,M'} = \mathbb{C}\setminus\mathbb{R}$.

Case 3. By assumption $\mathcal{D}_{M,M'} \cap \mathbb{R}$ has empty interior, and neither M' nor $MM' \in \langle -I, T\rangle$. So $M' = \left(\begin{smallmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{smallmatrix}\right)$, $MM' = \left(\begin{smallmatrix}\alpha'' & \beta''\\ \gamma'' & \delta''\end{smallmatrix}\right)$ with $\gamma', \gamma'' \neq 0$. It follows from Lemma D.3 that

$$\mathcal{D}_{M,M'} \cap \mathbb{R} = \mathcal{D}_{MM'} \cap \mathcal{D}_{M'} \cap \mathbb{R} = \begin{cases} \left\{\tau\in\mathbb{R}\colon \tau > -\frac{\delta'}{\gamma'}, \quad \tau > -\frac{\delta''}{\gamma''}\right\} & \text{if } \gamma', \gamma'' > 0,\\ \left\{\tau\in\mathbb{R}\colon \tau < -\frac{\delta'}{\gamma'}, \quad \tau < -\frac{\delta''}{\gamma''}\right\} & \text{if } \gamma', \gamma'' < 0,\end{cases} \tag{D.63}$$

which means that if γ', γ'' have the same sign then $\mathcal{D}_{M,M'} \cap \mathbb{R}$ has non-empty interior, contrary to assumption. So γ', γ'' must have opposite signs. By another application of Lemma D.3 we find

$$\mathcal{D}_{-M,M'} \cap \mathbb{R} = \mathcal{D}_{-MM'} \cap \mathcal{D}_{M'} \cap \mathbb{R} = \begin{cases} \left\{\tau\in\mathbb{R}\colon \tau > -\frac{\delta'}{\gamma'}, \quad \tau > -\frac{\delta''}{\gamma''}\right\} & \text{if } \gamma' > 0 > \gamma'',\\ \left\{\tau\in\mathbb{R}\colon \tau < -\frac{\delta'}{\gamma'}, \quad \tau < -\frac{\delta''}{\gamma''}\right\} & \text{if } \gamma' < 0 < \gamma'',\end{cases} \tag{D.64}$$

from which it follows that $\mathcal{D}_{-M,M'} \cap \mathbb{R}$ has non-empty interior. We may therefore apply the cocycle condition, Eq. (D.7), to get

$$\sigma_{-MM'}(z,\tau) = \sigma_{-M}\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{M'}(z,\tau)\,. \tag{D.65}$$

Although $\mathcal{D}_{-I,MM'} \cap \mathbb{R}$ and $\mathcal{D}_{-I,M} \cap \mathbb{R}$ are both empty, the result proved in Case 2(a) above means we can still use the cocycle condition, Eq. (D.7), to deduce

$$\sigma_{-MM'}(z,\tau) = \sigma_{-I}\left(\frac{z}{j_{MM'}(\tau)}, MM'\cdot\tau\right)\sigma_{MM'}(z,\tau) \tag{D.66}$$

and

$$\begin{aligned}\sigma_{-M}\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right) &= \sigma_{-I}\left(\frac{z}{j_M(M'\tau)j_{M'}(\tau)}, MM'\cdot\tau\right)\sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\tau\right)\\ &= \sigma_{-I}\left(\frac{z}{j_{MM'}(\tau)}, MM'\cdot\tau\right)\sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\tau\right)\end{aligned} \tag{D.67}$$

for all $z \in \mathbb{C}$, $\tau \in \mathbb{C}\setminus\mathbb{R}$. Substituting these expressions in Eq. (D.65) we find

$$\begin{aligned}\sigma_{-I}\left(\frac{z}{j_{MM'}(\tau)}, MM'\cdot\tau\right)\sigma_{MM'}(z,\tau) = \sigma_{-I}&\left(\frac{z}{j_{MM'}(\tau)}, MM'\cdot\tau\right)\\ &\times \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{MM'}(z,\tau)\end{aligned} \tag{D.68}$$

implying

$$\sigma_{MM'}(z,\tau) = \sigma_M\left(\frac{z}{j_{M'}(\tau)}, M'\cdot\tau\right)\sigma_{MM'}(z,\tau) \tag{D.69}$$

for all $z \in \mathbb{C}$, $\tau \in \mathcal{D}_{M,M'}$. □

APPENDIX E. REAL QUADRATIC FIELDS WITH AN ODD-TRACE UNIT

Theorem 1.52 splits the characterization of abelian extensions of real quadratic fields (conjecturally) generated by r-SICs into two cases, and it would be nice to know how often each case occurs. We give a partial result, showing that the trace of the fundamental unit is odd (the case when the full maximal abelian extension is conjecturally attained) a positive proportion of the time. Thus, for a positive proportion of real quadratic fields, r-SICs may be viewed as a geometric solution to Hilbert's twelfth problem (albeit a conjectural one, depending on the Stark–Tate Conjecture and the Twisted Convolution Conjecture).

If a quadratic field contains an odd trace unit, then elementary methods show that its discriminant must obey a congruence restriction modulo 8.

Lemma E.1. *If K is a real quadratic field containing a unit of odd trace, then* $\operatorname{disc} K \equiv 5 \pmod 8$.

Proof. Let $\Delta = \operatorname{disc} K$. If Δ is even, then $\mathcal{O}_K = \mathbb{Z} + \frac{\sqrt{\Delta}}{2}\mathbb{Z}$, so $\operatorname{Tr}(\alpha)$ is even for all $\alpha \in \mathcal{O}_K$. Thus, Δ must be odd; indeed, $\Delta \equiv 1 \pmod 4$ because Δ is a discriminant.

The ring of integers of K is therefore

$$\mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{\Delta}}{2}\mathbb{Z}. \tag{E.1}$$

The quotient ring $\mathcal{O}_K/2\mathcal{O}_K$ is represented by the congruence classes of $0, 1, \frac{-1+\sqrt{\Delta}}{2}$, and $\frac{1+\sqrt{\Delta}}{2}$. If ε is a unit of odd trace in $\mathcal{O}_K^\times$, then

$$\varepsilon \equiv \frac{\pm 1 + \sqrt{\Delta}}{2} \pmod{2\mathcal{O}_K}; \tag{E.2}$$

$$\varepsilon' \equiv \frac{\pm 1 - \sqrt{\Delta}}{2} \pmod{2\mathcal{O}_K}. \tag{E.3}$$

Thus, $\operatorname{Nm}(\varepsilon) = \varepsilon\varepsilon' \equiv -\frac{1-\Delta}{4} \pmod{2\mathcal{O}_K}$. If $\Delta \equiv 1 \pmod 8$, then it follows that $2 | \operatorname{Nm}(\varepsilon)$, which contradicts the fact that ε is a unit. Thus, $\Delta \equiv 5 \pmod 8$. □

Lemma E.2. *Let K be a real quadratic field such that* $\operatorname{disc} K \equiv 5 \pmod 8$. *Consider the following conditions:*

(1) There exists no cubic number field L such that $\operatorname{disc} L = \operatorname{disc} K$ *or* $\operatorname{disc} L = 4 \operatorname{disc} K$.
(2) The field K has a unit of odd trace.
(3) There exists no cubic number field L such that $\operatorname{disc} L = 4 \operatorname{disc} K$.

Then (1) implies (2), and (2) implies (3).

Proof. Consider the exact sequence of ray class groups

$$1 \to \frac{\mathcal{O}_K^\times}{\mathrm{U}_2(\mathcal{O}_K)} \xrightarrow{\iota} (\mathcal{O}_K/2\mathcal{O}_K)^\times \to \mathrm{Cl}_2(\mathcal{O}_K) \xrightarrow{\pi} \mathrm{Cl}(\mathcal{O}_K) \to 1. \tag{E.4}$$

This is the exact sequence given in [71, Thm. 5.4], specialized to the case when $\mathcal{O} = \mathcal{O}' = \mathfrak{m}' = \mathcal{O}_K$, $\mathfrak{m} = 2\mathcal{O}_K$, and $\Sigma = \Sigma' = \{\}$. The group $(\mathcal{O}_K/2\mathcal{O}_K)^\times \cong \mathbb{Z}/3\mathbb{Z}$ because $\operatorname{disc} K \equiv 5 \pmod 8$. The unit group $\mathcal{O}_K^\times$ has an element of odd trace if and only if the the map ι is an isomorphism, that is, if and only if the map π is an isomorphism. Setting $h_K = |\mathrm{Cl}(\mathcal{O}_K)|$, then exactly one of the following is true:

(A) $|\mathrm{Cl}_2(\mathcal{O}_K)| = h_K$, and K has a unit of odd trace; or
(B) $|\mathrm{Cl}_2(\mathcal{O}_K)| = 3h_K$, and K does not have a unit of odd trace.

Let ϕ be any nontrivial group homomorphism $\phi : \mathrm{Cl}_2(\mathcal{O}_K) \to \mathbb{Z}/3\mathbb{Z}$. By the existence theorem of class field theory and the Galois correspondence, there exists a cubic subextension M/K of the ray class field H_2/K corresponding to $\ker(\phi)$ under the Galois correspondence. The field M is sextic over $\mathbb{Q}$, with $\mathrm{Gal}(M/\mathbb{Q}) \cong S_3$. Pick a cubic subfield L of M; L is unique up to isomorphism. Using the conductor-discriminant formula, one can show that $\operatorname{disc} L = \operatorname{disc} K$ if ϕ factors through the map π, and $\operatorname{disc} L = 4 \operatorname{disc} K$ otherwise. Moreover, this correspondence defines bijections

$$\{\phi : \mathrm{Cl}(\mathcal{O}_K) \twoheadrightarrow \mathbb{Z}/3\mathbb{Z}\} \longleftrightarrow \{\text{cubic } L/\mathbb{Q} : \operatorname{disc}(L) = \operatorname{disc}(K)\}, \tag{E.5}$$

$$\{\phi : \mathrm{Cl}_2(\mathcal{O}_K) \twoheadrightarrow \mathbb{Z}/3\mathbb{Z}, \phi \neq \pi \circ \phi'\} \longleftrightarrow \{\text{cubic } L/\mathbb{Q} : \operatorname{disc}(L) = 4\operatorname{disc}(K)\}. \tag{E.6}$$

We now prove that (1) implies (2). Suppose that there is no cubic number field L with $\operatorname{disc} L = \operatorname{disc} K$ or $\operatorname{disc} L = 3 \operatorname{disc} K$. Thus, there is no nontrivial group homomorphism $\phi : \mathrm{Cl}_2(\mathcal{O}_K) \to \mathbb{Z}/3\mathbb{Z}$. Since $\mathrm{Cl}_2(\mathcal{O}_K)$ is abelian, this means that $3 \nmid |\mathrm{Cl}_2(\mathcal{O}_K)|$. It then follows that we are in case (A), and K has a unit of odd trace.

Finally, we prove that (2) implies (3). Suppose that K has a unit of odd trace, so we are in case (A): $|\mathrm{Cl}_2(\mathcal{O}_K)| = h_K$. Thus, every nontrivial group homomorphism $\phi : \mathrm{Cl}_2(\mathcal{O}_K) \to \mathbb{Z}/3\mathbb{Z}$ factors through $\mathrm{Cl}(\mathcal{O}_K)$. By (E.6), there is no cubic number field L with $\operatorname{disc}(L) = 4 \operatorname{disc}(K)$. □

In the authors' understanding, analytic number theory and arithmetic statistics have not yet produced techniques capable of finding the exact asymptotic density of the number of real quadratic fields with a unit of odd trace. However, techniques for counting quadratic and cubic fields may be used to give upper and lover bounds using Lemma E.1 and Lemma E.2. The following proof is based on ideas suggested by Frank Thorne [107] and Jiuya Wang [110].

Proof of Theorem 6.15. In the proof, we will use the notation $\Delta_K = \operatorname{disc} K$ for the field discriminant and

$$N_2(X; [\text{conditions}]) = \#\{K : [K : \mathbb{Q}] = 2, 0 < \Delta_K < X, \text{ [conditions]}\}, \tag{E.7}$$

$$N_3(X; [\text{conditions}]) = \#\{L : [L : \mathbb{Q}] = 3, 0 < \Delta_L < X, \text{ [conditions]}\} \tag{E.8}$$

for counts of quadratic and cubic fields of positive discriminant satisfying certain conditions. We write $N_2(X)$ and $N_3(X)$ if there are no conditions.

An integer $\Delta > 1$ is the discriminant of a quadratic field if and only if it satisfies the congruence conditions $\Delta \equiv 1, 5, 8, 9, 12, 13 \pmod{16}$ and $p^2 \nmid \Delta$ for all odd primes p. By the following standard sieve-theoretical calculation, taking $\mu(d)$ to be the Möbius function and taking r_d to be the smallest positive solution to $r_d \equiv n_0 \pmod{16}$ and $r_d \equiv 0 \pmod{d^2}$,

$$\{n \leq X : n \equiv n_0 \pmod{16}, p^2 \nmid n \text{ for } p \text{ odd}\} = \sum_{\substack{1 \leq d \leq X^{1/2} \\ 2 \nmid d}} \mu(d) \left\lfloor \frac{X - r_d}{16d^2} \right\rfloor \tag{E.9}$$

$$= \sum_{\substack{1 \leq d \leq X^{1/2} \\ 2 \nmid d}} \mu(d) \frac{X}{16d^2} + O(X^{1/2}) \tag{E.10}$$

$$= \left(\sum_{\substack{1 \leq d \\ 2 \nmid d}} \frac{\mu(d)}{16d^2} + O(X^{-1/2}) \right) X + O(X^{1/2}) \tag{E.11}$$

$$= \left(\frac{1}{16}\prod_{p\neq 2}\left(1-\frac{1}{p^2}\right)\right)X + O(X^{1/2}) \tag{E.12}$$

$$= \frac{1}{12\zeta(2)}X + O(X^{1/2}). \tag{E.13}$$

Thus, taking $n_0 \in \{1,5,8,9,12,13\}$ and $n_0 \in \{5,13\}$, respectively, we have

$$N_2(X) = \frac{1}{2\zeta(2)}X + O(X^{1/2}), \text{ and} \tag{E.14}$$

$$N_2(X;\Delta_K \equiv 5 \pmod 8) = \frac{1}{6\zeta(2)}X + O(X^{1/2}). \tag{E.15}$$

Thus, by using Lemma E.1 and dividing these two asymptotic equalities (E.15) and (E.14), we obtain the upper bound

$$\frac{N_2(X;2\nmid \mathrm{Tr}(\varepsilon_K))}{N_2(X)} \leq \frac{N_2(X;\Delta_K \equiv 5 \pmod 8)}{N_2(X)} = \frac{1}{3} + O(X^{-1/2}). \tag{E.16}$$

To obtain the lower bound, we appeal to the results of Taniguchi and Thorne [104] on counting cubic fields with local restrictions. If L is a cubic field, then $\mathcal{O}_L \otimes \mathbb{Z}_2$ a "maximal cubic ring over $\mathbb{Z}_2$," that is, a product of valuation rings of finite extensions of $\mathbb{Q}_2$ whose degrees sum to 3. There are exactly 10 maximal cubic rings over $\mathbb{Z}_2$, shown in the following table, which is based on the tables given in [104, p. 2487–2488] and on the database of Jones and Roberts [62]. In the table, ω is a root of $x^2+x+1=0$, and α is a root of $x^3-x-1=0$.

$\mathcal{O}_L \otimes \mathbb{Z}_2$	forced congruence conds.	density wt.
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\Delta_L \equiv 1 \pmod 8$	$1/6$
$\mathbb{Z}_2 \times \mathbb{Z}_2[\omega]$	$\Delta_L \equiv 5 \pmod 8$	$1/2$
$\mathbb{Z}_2[\alpha]$	$\Delta_L \equiv 1 \pmod 8$	$1/3$
$\mathbb{Z}_2[\sqrt[3]{2}]$	$\Delta_L \equiv 20 \pmod{32}$	$1/4$
$\mathbb{Z}_2 \times \mathbb{Z}_2[\sqrt{-1}]$	$\Delta_L \equiv 28 \pmod{32}$	$1/4$
$\mathbb{Z}_2 \times \mathbb{Z}_2[\sqrt{3}]$	$\Delta_L \equiv 12 \pmod{32}$	$1/4$
$\mathbb{Z}_2 \times \mathbb{Z}_2[\sqrt{2}]$	$\Delta_L \equiv 8 \pmod{64}$	$1/8$
$\mathbb{Z}_2 \times \mathbb{Z}_2[\sqrt{-2}]$	$\Delta_L \equiv 56 \pmod{64}$	$1/8$
$\mathbb{Z}_2 \times \mathbb{Z}_2[\sqrt{6}]$	$\Delta_L \equiv 24 \pmod{64}$	$1/8$
$\mathbb{Z}_2 \times \mathbb{Z}_2[\sqrt{-6}]$	$\Delta_L \equiv 40 \pmod{64}$	$1/8$

In particular, the congruence condition $\Delta_L \equiv 5 \pmod 8$ is equivalent to the local restriction $\mathcal{O}_L \otimes \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2[\omega]$, and the congruence condition $\Delta_L \equiv 20 \pmod{32}$ is equivalent to the local restriction $\mathcal{O}_L \otimes \mathbb{Z}_2 = \mathbb{Z}_2[\sqrt[3]{2}]$. The following asymptotics are thus special cases of [104, Thm. 1.3][10], with the secondary term absorbed into the error term:

$$N_3(X;\Delta_L \equiv 5 \pmod 8) = \frac{C^+(\mathcal{S}_{\mathbb{Z}_2\times\mathbb{Z}_2[\omega]})}{12\zeta(3)}X + O(X^{5/6}), \tag{E.17}$$

[10]Note that the more general result [104, Thm. 6.2] also allows one to impose additional congruence restrictions, but we don't need to do this.

$$N_3(X;\Delta_L \equiv 20 \pmod{32}) = \frac{C^+(\mathcal{S}_{\mathbb{Z}_2[\sqrt[3]{2}]})}{12\zeta(3)}X + O(X^{5/6}). \tag{E.18}$$

The constants $C^+(\mathcal{S}_{\mathbb{Z}_2\times\mathbb{Z}_2[\omega]})$ and $C^+(\mathcal{S}_{\mathbb{Z}_2[\sqrt[3]{2}]})$ are computed from the "density weights" in the table:

$$C^+(\mathcal{S}_{\mathbb{Z}_2\times\mathbb{Z}_2[\omega]}) = \frac{1/2}{1/6+1/2+1/3+1/4+1/4+1/4+1/8+1/8+1/8+1/8} = \frac{2}{9}, \tag{E.19}$$

$$C^+(\mathcal{S}_{\mathbb{Z}_2[\sqrt[3]{2}]}) = \frac{1/4}{1/6+1/2+1/3+1/4+1/4+1/4+1/8+1/8+1/8+1/8} = \frac{1}{9}. \tag{E.20}$$

However, these are not actually the asymptotics we want—we should also be removing non-fundamental discriminants by imposing the condition that $p^2 \nmid \Delta_L$ for odd primes p. The condition that $p^2 \nmid \Delta_L$ is equivalent to the condition that $\mathcal{O}_L \otimes \mathbb{Z}_p$ is not totally ramified at p; see [104, Sec. 6.1]. Let $C^+_{\mathrm{ntr}}(p)$ denote the local density of non-totally ramified $\mathcal{O}_L \otimes \mathbb{Z}_p$. The following asymptotic formulas are also special cases of [104, Thm. 1.3], treating Y as a constant.

$$N_3\left(X;\ \begin{array}{c}\Delta_L \equiv 5 \pmod 8,\\ p^2\nmid\Delta_L \text{ for odd } p \le Y\end{array}\right) = \frac{C^+(\mathcal{S}_{\mathbb{Z}_2\times\mathbb{Z}_2[\omega]})}{12\zeta(3)}\left(\prod_{\substack{p\le Y\\ 2\nmid p}} C^+_{\mathrm{ntr}}(p)\right)X + O_Y(X^{5/6}), \tag{E.21}$$

$$N_3\left(X;\ \begin{array}{c}\Delta_L \equiv 20 \pmod{32},\\ p^2\nmid\Delta_L \text{ for odd } p \le Y\end{array}\right) = \frac{C^+(\mathcal{S}_{\mathbb{Z}_2[\sqrt[3]{2}]})}{12\zeta(3)}\left(\prod_{\substack{p\le Y\\ 2\nmid p}} C^+_{\mathrm{ntr}}(p)\right)X + O_Y(X^{5/6}). \tag{E.22}$$

The $C^+_{\mathrm{ntr}}(p)$ are calculated using the table in [104, Sec. 6.2] to be

$$C^+_{\mathrm{ntr}}(p) = \frac{1/6+1/2+1/3+1/p}{1/6+1/2+1/3+1/p+1/p^2} = \frac{1+p^{-1}}{1+p^{-1}+p^{-2}} = \frac{(1-p^{-3})^{-1}}{(1-p^{-2})^{-1}}, \tag{E.23}$$

and hence

$$\prod_{\substack{p\le Y\\ 2\nmid p}} C^+_{\mathrm{ntr}}(p) = \frac{1-2^{-3}}{1-2^{-2}}\cdot\frac{\zeta(3)}{\zeta(2)} + O(Y^{-1}) = \frac{7\zeta(3)}{6\zeta(2)} + O(Y^{-1}). \tag{E.24}$$

Thus, we obtain the asymptotic formulas

$$N_3\left(X;\ \begin{array}{c}\Delta_L \equiv 5 \pmod 8,\\ p^2\nmid\Delta_L \text{ for odd } p \le Y\end{array}\right) = \frac{7}{162\zeta(2)}X + O(X/Y) + O_Y(X^{5/6}), \tag{E.25}$$

$$N_3\left(X;\ \begin{array}{c}\Delta_L \equiv 20 \pmod{32},\\ p^2\nmid\Delta_L \text{ for odd } p \le Y\end{array}\right) = \frac{7}{324\zeta(2)}X + O(X/Y) + O_Y(X^{5/6}). \tag{E.26}$$

By sending $Y \to \infty$ (sufficiently slowly compared to X), we have

$$N_3\left(X;\ \begin{array}{c}\Delta_L \equiv 5 \pmod 8,\\ \Delta_L \text{ fundamental}\end{array}\right) = \frac{7}{162\zeta(2)}X + o(X), \tag{E.27}$$

$$N_3\left(X;\ \begin{array}{c}\Delta_L \equiv 20 \pmod{32},\\ \Delta_L \text{ fundamental}\end{array}\right) = \frac{7}{324\zeta(2)}X + o(X). \tag{E.28}$$

By Lemma E.2 (specifically the fact that (1) implies (2)), we have the bound

$$N_2(X;2\mid \mathrm{Tr}(\varepsilon_K), \Delta_K \equiv 5 \pmod 8) \tag{E.29}$$

$$\leq N_3\left(X;\ \begin{matrix}\Delta_L \equiv 5 \pmod 8,\\ \Delta_L \text{ fundamental}\end{matrix}\right) + N_3\left(X;\ \begin{matrix}\Delta_L \equiv 20 \pmod{32},\\ \Delta_L \text{ fundamental}\end{matrix}\right) \tag{E.30}$$

$$= \frac{7}{162\zeta(2)}X + \frac{7}{324\zeta(2)}(4X) + o(X) \tag{E.31}$$

$$= \frac{7}{54\zeta(2)}X + o(X). \tag{E.32}$$

Thus, using Lemma E.1,

$$N_2(X; 2\nmid \mathrm{Tr}(\varepsilon_K)) = N_2(X, \Delta_K \equiv 5 \pmod 8) - N_2(X; 2 \mid \mathrm{Tr}(\varepsilon_K), \Delta_K \equiv 5 \pmod 8) \tag{E.33}$$

$$\geq \frac{1}{6\zeta(2)}X - \frac{7}{54\zeta(2)}X + o(X) \tag{E.34}$$

$$= \frac{1}{27\zeta(2)}X + o(X). \tag{E.35}$$

By dividing the asymptotic formulas (E.35) and (E.14), we obtain the lower bound

$$\frac{N_2(X; 2\nmid \mathrm{Tr}(\varepsilon_K))}{N_2(X)} \geq \frac{2}{27} + o(1). \tag{E.36}$$

Combining (E.16) and (E.36) completes the proof. □

The upper bound in Theorem 6.15 is fairly trivial, as it only uses the congruence restriction $\mathrm{disc}\, K \equiv 5 \pmod 8$; one might hope to get a better upper bound using the fact that "(2) implies (3)" from Lemma E.2, which we did not use at all! It is not clear how to so do at present, as we would need some additional result to tell us that the cubic fields with $\mathrm{disc}\, L \equiv 20 \pmod{32}$ hit enough *distinct* discriminants.

Numerical evidence suggests that the true asymptotic density of real quadratic fields with a unit of odd trace is about $2/9$ (or 22.2%), that is, about $2/3$ (or 66.7%) of the real quadratic fields with discriminant congruent to 5 modulo 8. According to a calculation performed in Mathematica, among real quadratic fundamental discriminants $\Delta = 8k - 3$ for integers $k \in [10^{10}, 10^{10} + 10^6]$, about 66.9% have a unit of odd trace. Calculations involving smaller discriminants suggest a positive bias in the count of such discriminants up to X that is going to zero slower than $X^{1-\delta}$ for any $\delta > 0$.

Finally, we give a brief comparison to the problem of solubility of the negative "Pell" equation. The existence of a unit of negative norm in the real quadratic field $\mathbb{Q}(\sqrt{D})$ is equivalent to the existence of an integer solution to the equation $x^2 - Dy^2 = -1$, whereas the existence of a unit of odd trace in the real quadratic field $\mathbb{Q}(\sqrt{D})$ with $D \equiv 1 \pmod 4$ is equivalent to the existence of an integer solution to the equation $x^2 + xy + \frac{1-D}{4}y^2 = 1$ with y odd. In the former case, however, the asymptotic density of such D is zero, and this leads to additional complications. Nonetheless, as in our problem, upper and lower bounds of the same order of magnitude can be given on the number of such D up to X; this was done by Fouvry and Klüners [41, Thm. 1]. The narrow class group of $\mathcal{O}_K$ plays a similar role in their work as does the ray class group modulo 2 in our Lemma E.2.

APPENDIX F. 1-SIC DATA TABLES

In this appendix, we collect tables containing the algebraic data canonically specifying ghost 1-SICs, and non-canonically specifying 1-SICs, in dimensions $d = 4$–100. This list is conjecturally complete for all Weyl–Heisenberg covariant 1-SICs; there is exactly one row corresponding to each predicted $\mathrm{EC}(d)$-orbit.

We have numerically computed an approximate ghost SIC using the Shintani–Faddeev modular cocycle and checked that the ghost overlaps satisfy

$$\left|\mathrm{Tr}(\tilde{\Pi}_{\mathbf{p}}\tilde{\Pi}_{\mathbf{0}}) - \frac{(1-\delta^d_{\mathbf{p},\mathbf{0}}) + \delta^d_{\mathbf{p},\mathbf{0}}(d+1)}{d+1}\right| < 10^{-66} \tag{F.1}$$

in all of the following cases:

(1) For the 251 rows corresponding to $d \leq 60$;
(2) For the 39 rows with $60 < d < 100$ where $Q = \langle 1, 1-d, 1\rangle$;
(3) For the 4 rows with $d = 100$.

For we have also used our necromancy procedure to numerically compute the set of associated 1-SICs. See section 8 for more details about our numerical calculations.

Each ghost fiducial is specified by an admissible tuple $t = (d, 1, Q)$ with dimension d and integer binary quadratic form Q. The relations between t and the remaining data in the table are as follows. First factorize $(d+1)(d-3) = f_d^2\Delta_0$ where Δ_0 is a fundamental discriminant. Then Q (conjecturally) yields a valid 1-SIC if $\mathrm{disc}(Q) = f^2\Delta_0$ where $f \mid f_d$. While d and Q determine all other data needed for constructing a ghost, the additional columns are included for convenience, since they contain additional algebraic data that may be "difficult" to compute, for example requiring integer factoring or finding a fundamental unit. The column Δ_0 contains the fundamental discriminant of Q and the column f the conductor of Q. The columns h and $\mathrm{Cl}(\mathcal{O}_f)$ contain the class number and class group respectively. The column $\mathrm{Gal}(E_s^{(1)}/H)$ is the Galois group of the candidate overlap field ramified at the first infinite place. (This is isomorphic to $\mathrm{Gal}(E_t^{(2)}/H)$, the Galois group of the candidate *ghost* overlap field ramified at the *second* infinite place.) The column L^n is of the form where L is the positive-trace generator of the stability group of Q with the same sign as Q, as defined in Definition 1.28, and $A = L^n$. The column 'a.u.' is marked 'Y' if there is an anti-unitary symmetry. Finally, $\ell(A)$ is the length of the word expansion of A using the Hirzebruch–Jung (negative regular) reduction into the standard (S and T) generators of $\mathrm{SL}_2(\mathbb{Z})$. This is one measure of the complexity of constructing the actual ghost fiducial vector for that input. The forms Q in this list were selected among class representatives to minimize this complexity, although this choice is not generally unique. In order to write down a ghost 1-SIC explicitly, one must also choose a twist G, which may canonically be taken to be the identity matrix $G = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$; the choice of twist does not affect the $\mathrm{EC}(d)$-orbit. The data in each row are sufficient to compute a ghost fiducial, but to fully specify a 1-SIC, one must additionally make an arbitrary, non-canonical choice of a sign-switching Galois automorphism g.

d	Δ_0	f	h	$\mathrm{Cl}(\mathcal{O}_f)$	$\mathrm{Gal}\big(E_s^{(1)}/H\big)$	Q	L^n	a.u.	ℓ
4	5	1	1	C_1	C_2^2	$\langle 1,-3,1\rangle$	$\left(\begin{smallmatrix}2&-1\\1&-1\end{smallmatrix}\right)^6$	Y	4
5	12	1	1	C_1	C_8	$\langle 1,-4,1\rangle$	$\left(\begin{smallmatrix}4&-1\\1&0\end{smallmatrix}\right)^3$		4
6	21	1	1	C_1	$C_2\times C_6$	$\langle 1,-5,1\rangle$	$\left(\begin{smallmatrix}5&-1\\1&0\end{smallmatrix}\right)^3$		4
7	8	1	1	C_1	C_6	$\langle 2,-4,1\rangle$	$\left(\begin{smallmatrix}3&-1\\2&-1\end{smallmatrix}\right)^6$	Y	7
		2	1	C_1	$C_2\times C_6$	$\langle 1,-6,1\rangle$	$\left(\begin{smallmatrix}6&-1\\1&0\end{smallmatrix}\right)^3$		4

8	5	1	1	C_1	$C_2 \times C_4$	$\langle 1, -3, 1\rangle$	$\left(\begin{smallmatrix} 2 & -1 \\ 1 & -1 \end{smallmatrix}\right)^{12}$	**Y**	7
		3	1	C_1	$C_2 \times C_4^2$	$\langle 1, -7, 1\rangle$	$\left(\begin{smallmatrix} 7 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
9	60	1	2	C_2	$C_3 \times C_6$	$\langle 1, -8, 1\rangle$	$\left(\begin{smallmatrix} 8 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
						$\langle 5, -10, 2\rangle$	$\left(\begin{smallmatrix} 9 & -2 \\ 5 & -1 \end{smallmatrix}\right)^{3}$		7
10	77	1	1	C_1	$C_2 \times C_{24}$	$\langle 1, -9, 1\rangle$	$\left(\begin{smallmatrix} 9 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
11	24	1	1	C_1	C_{40}	$\langle 3, -6, 1\rangle$	$\left(\begin{smallmatrix} 11 & -2 \\ 6 & -1 \end{smallmatrix}\right)^{3}$		7
		2	2	C_2	C_{40}	$\langle 1, -10, 1\rangle$	$\left(\begin{smallmatrix} 10 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
						$\langle 3, -12, 4\rangle$	$\left(\begin{smallmatrix} 11 & -4 \\ 3 & -1 \end{smallmatrix}\right)^{3}$		7
12	13	1	1	C_1	C_2^4	$\langle 3, -5, 1\rangle$	$\left(\begin{smallmatrix} 4 & -1 \\ 3 & -1 \end{smallmatrix}\right)^{6}$	**Y**	10
		3	1	C_1	$C_2^3 \times C_6$	$\langle 1, -11, 1\rangle$	$\left(\begin{smallmatrix} 11 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
13	140	1	2	C_2	$C_4 \times C_{12}$	$\langle 1, -12, 1\rangle$	$\left(\begin{smallmatrix} 12 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
						$\langle 7, -14, 2\rangle$	$\left(\begin{smallmatrix} 13 & -2 \\ 7 & -1 \end{smallmatrix}\right)^{3}$		7
14	165	1	2	C_2	$C_2 \times C_6^2$	$\langle 1, -13, 1\rangle$	$\left(\begin{smallmatrix} 13 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
						$\langle 5, -15, 3\rangle$	$\left(\begin{smallmatrix} 14 & -3 \\ 5 & -1 \end{smallmatrix}\right)^{3}$		7
15	12	1	1	C_1	C_{24}	$\langle 1, -4, 1\rangle$	$\left(\begin{smallmatrix} 4 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{6}$		7
		2	1	C_1	$C_2 \times C_{24}$	$\langle 4, -8, 1\rangle$	$\left(\begin{smallmatrix} 15 & -2 \\ 8 & -1 \end{smallmatrix}\right)^{3}$		7
		4	2	C_2	$C_2 \times C_{24}$	$\langle 1, -14, 1\rangle$	$\left(\begin{smallmatrix} 14 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
						$\langle 11, -18, 3\rangle$	$\left(\begin{smallmatrix} 16 & -3 \\ 11 & -2 \end{smallmatrix}\right)^{3}$		10
16	221	1	2	C_2	$C_2 \times C_8^2$	$\langle 1, -15, 1\rangle$	$\left(\begin{smallmatrix} 15 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
						$\langle 7, -19, 5\rangle$	$\left(\begin{smallmatrix} 17 & -5 \\ 7 & -2 \end{smallmatrix}\right)^{3}$		10
17	28	1	1	C_1	C_{96}	$\langle 2, -6, 1\rangle$	$\left(\begin{smallmatrix} 17 & -3 \\ 6 & -1 \end{smallmatrix}\right)^{3}$		7
		3	2	C_2	C_{96}	$\langle 1, -16, 1\rangle$	$\left(\begin{smallmatrix} 16 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
						$\langle 9, -18, 2\rangle$	$\left(\begin{smallmatrix} 17 & -2 \\ 9 & -1 \end{smallmatrix}\right)^{3}$		7
18	285	1	2	C_2	$C_3 \times C_6^2$	$\langle 1, -17, 1\rangle$	$\left(\begin{smallmatrix} 17 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{3}$		4
						$\langle 13, -21, 3\rangle$	$\left(\begin{smallmatrix} 19 & -3 \\ 13 & -2 \end{smallmatrix}\right)^{3}$		10
19	5	1	1	C_1	C_{18}	$\langle 1, -3, 1\rangle$	$\left(\begin{smallmatrix} 2 & -1 \\ 1 & -1 \end{smallmatrix}\right)^{18}$	**Y**	10
		2	1	C_1	$C_3 \times C_{18}$	$\langle 4, -6, 1\rangle$	$\left(\begin{smallmatrix} 5 & -1 \\ 4 & -1 \end{smallmatrix}\right)^{6}$	**Y**	13

		4	1	C_1	$C_6 \times C_{18}$	$\langle 5, -10, 1\rangle$	$\left(\begin{smallmatrix} 19 & -2 \\ 10 & -1 \end{smallmatrix}\right)^3$	7
		8	2	C_2	$C_6 \times C_{18}$	$\langle 1, -18, 1\rangle$	$\left(\begin{smallmatrix} 18 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 5, -20, 4\rangle$	$\left(\begin{smallmatrix} 19 & -4 \\ 5 & -1 \end{smallmatrix}\right)^3$	7
20	357	1	2	C_2	$C_2^3 \times C_{24}$	$\langle 1, -19, 1\rangle$	$\left(\begin{smallmatrix} 19 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 7, -21, 3\rangle$	$\left(\begin{smallmatrix} 20 & -3 \\ 7 & -1 \end{smallmatrix}\right)^3$	7
21	44	1	1	C_1	$C_2^2 \times C_{24}$	$\langle 5, -8, 1\rangle$	$\left(\begin{smallmatrix} 22 & -3 \\ 15 & -2 \end{smallmatrix}\right)^3$	10
		3	4	C_4	$C_2 \times C_6^2$	$\langle 1, -20, 1\rangle$	$\left(\begin{smallmatrix} 20 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 5, -24, 9\rangle$	$\left(\begin{smallmatrix} 22 & -9 \\ 5 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 11, -22, 2\rangle$	$\left(\begin{smallmatrix} 21 & -2 \\ 11 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 9, -24, 5\rangle$	$\left(\begin{smallmatrix} 22 & -5 \\ 9 & -2 \end{smallmatrix}\right)^3$	10
22	437	1	1	C_1	$C_2 \times C_{120}$	$\langle 1, -21, 1\rangle$	$\left(\begin{smallmatrix} 21 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
23	120	1	2	C_2	C_{176}	$\langle 6, -12, 1\rangle$	$\left(\begin{smallmatrix} 23 & -2 \\ 12 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 3, -12, 2\rangle$	$\left(\begin{smallmatrix} 23 & -4 \\ 6 & -1 \end{smallmatrix}\right)^3$	7
		2	4	C_2^2	C_{176}	$\langle 1, -22, 1\rangle$	$\left(\begin{smallmatrix} 22 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 19, -10, -5\rangle$	$\left(\begin{smallmatrix} 16 & 5 \\ 19 & 6 \end{smallmatrix}\right)^3$	13
						$\langle 8, -24, 3\rangle$	$\left(\begin{smallmatrix} 23 & -3 \\ 8 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 15, 0, -8\rangle$	$\left(\begin{smallmatrix} 11 & 8 \\ 15 & 11 \end{smallmatrix}\right)^3$	10
24	21	1	1	C_1	$C_2 \times C_4 \times C_{12}$	$\langle 1, -5, 1\rangle$	$\left(\begin{smallmatrix} 5 & -1 \\ 1 & 0 \end{smallmatrix}\right)^6$	7
		5	2	C_2	$C_2^2 \times C_4 \times C_{12}$	$\langle 1, -23, 1\rangle$	$\left(\begin{smallmatrix} 23 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 17, -27, 3\rangle$	$\left(\begin{smallmatrix} 25 & -3 \\ 17 & -2 \end{smallmatrix}\right)^3$	10
25	572	1	2	C_2	$C_5 \times C_{40}$	$\langle 1, -24, 1\rangle$	$\left(\begin{smallmatrix} 24 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 13, -26, 2\rangle$	$\left(\begin{smallmatrix} 25 & -2 \\ 13 & -1 \end{smallmatrix}\right)^3$	7
26	69	1	1	C_1	$C_2 \times C_{12}^2$	$\langle 3, -9, 1\rangle$	$\left(\begin{smallmatrix} 26 & -3 \\ 9 & -1 \end{smallmatrix}\right)^3$	7
		3	3	C_3	$C_2 \times C_{12}^2$	$\langle 1, -25, 1\rangle$	$\left(\begin{smallmatrix} 25 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 17, -3, -9\rangle$	$\left(\begin{smallmatrix} 14 & 9 \\ 17 & 11 \end{smallmatrix}\right)^3$	10
						$\langle 5, -29, 11\rangle$	$\left(\begin{smallmatrix} 27 & -11 \\ 5 & -2 \end{smallmatrix}\right)^3$	10
27	168	1	2	C_2	$C_9 \times C_{18}$	$\langle 7, -14, 1\rangle$	$\left(\begin{smallmatrix} 27 & -2 \\ 14 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 11, -16, 2\rangle$	$\left(\begin{smallmatrix} 29 & -4 \\ 22 & -3 \end{smallmatrix}\right)^3$	13

		2	4	C_2^2	$C_9 \times C_{18}$	$\langle 1, -26, 1\rangle$	$\left(\begin{smallmatrix} 26 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 7, 14, -17\rangle$	$\left(\begin{smallmatrix} 6 & 17 \\ 7 & 20 \end{smallmatrix}\right)^3$		7
						$\langle 19, -8, -8\rangle$	$\left(\begin{smallmatrix} 17 & 8 \\ 19 & 9 \end{smallmatrix}\right)^3$		10
						$\langle 11, -32, 8\rangle$	$\left(\begin{smallmatrix} 29 & -8 \\ 11 & -3 \end{smallmatrix}\right)^3$		10
28	29	1	1	C_1	$C_2^2 \times C_6^2$	$\langle 5, -7, 1\rangle$	$\left(\begin{smallmatrix} 6 & -1 \\ 5 & -1 \end{smallmatrix}\right)^6$	**Y**	16
		5	2	C_2	$C_2^3 \times C_6^2$	$\langle 1, -27, 1\rangle$	$\left(\begin{smallmatrix} 27 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 13, -33, 7\rangle$	$\left(\begin{smallmatrix} 30 & -7 \\ 13 & -3 \end{smallmatrix}\right)^3$		13
29	780	1	4	C_2^2	C_{280}	$\langle 1, -28, 1\rangle$	$\left(\begin{smallmatrix} 28 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 15, -30, 2\rangle$	$\left(\begin{smallmatrix} 29 & -2 \\ 15 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 10, -30, 3\rangle$	$\left(\begin{smallmatrix} 29 & -3 \\ 10 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 6, -30, 5\rangle$	$\left(\begin{smallmatrix} 29 & -5 \\ 6 & -1 \end{smallmatrix}\right)^3$		7
30	93	1	1	C_1	$C_2 \times C_6 \times C_{24}$	$\langle 7, -11, 1\rangle$	$\left(\begin{smallmatrix} 31 & -3 \\ 21 & -2 \end{smallmatrix}\right)^3$		10
		3	3	C_3	$C_2 \times C_6 \times C_{24}$	$\langle 1, -29, 1\rangle$	$\left(\begin{smallmatrix} 29 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 19, -1, -11\rangle$	$\left(\begin{smallmatrix} 15 & 11 \\ 19 & 14 \end{smallmatrix}\right)^3$		10
						$\langle 7, -33, 9\rangle$	$\left(\begin{smallmatrix} 31 & -9 \\ 7 & -2 \end{smallmatrix}\right)^3$		10
31	56	1	1	C_1	$C_{10} \times C_{30}$	$\langle 2, -8, 1\rangle$	$\left(\begin{smallmatrix} 31 & -4 \\ 8 & -1 \end{smallmatrix}\right)^3$		7
		2	2	C_2	$C_{10} \times C_{30}$	$\langle 8, -16, 1\rangle$	$\left(\begin{smallmatrix} 31 & -2 \\ 16 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 11, 2, -5\rangle$	$\left(\begin{smallmatrix} 13 & 10 \\ 22 & 17 \end{smallmatrix}\right)^3$		13
		4	4	C_4	$C_{10} \times C_{30}$	$\langle 1, -30, 1\rangle$	$\left(\begin{smallmatrix} 30 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 13, -34, 5\rangle$	$\left(\begin{smallmatrix} 32 & -5 \\ 13 & -2 \end{smallmatrix}\right)^3$		10
						$\langle 25, -36, 4\rangle$	$\left(\begin{smallmatrix} 33 & -4 \\ 25 & -3 \end{smallmatrix}\right)^3$		13
						$\langle 5, -34, 13\rangle$	$\left(\begin{smallmatrix} 32 & -13 \\ 5 & -2 \end{smallmatrix}\right)^3$		10
32	957	1	2	C_2	$C_2 \times C_{16}^2$	$\langle 1, -31, 1\rangle$	$\left(\begin{smallmatrix} 31 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 11, -33, 3\rangle$	$\left(\begin{smallmatrix} 32 & -3 \\ 11 & -1 \end{smallmatrix}\right)^3$		7
33	1020	1	4	C_2^2	$C_2 \times C_{120}$	$\langle 1, -32, 1\rangle$	$\left(\begin{smallmatrix} 32 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 17, -34, 2\rangle$	$\left(\begin{smallmatrix} 33 & -2 \\ 17 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 23, -36, 3\rangle$	$\left(\begin{smallmatrix} 34 & -3 \\ 23 & -2 \end{smallmatrix}\right)^3$		10
						$\langle 29, -40, 5\rangle$	$\left(\begin{smallmatrix} 36 & -5 \\ 29 & -4 \end{smallmatrix}\right)^3$		16
34	1085	1	2	C_2	$C_2 \times C_{288}$	$\langle 1, -33, 1\rangle$	$\left(\begin{smallmatrix} 33 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4

						$\langle 7,-35,5\rangle$	$\left(\begin{smallmatrix}34 & -5\\ 7 & -1\end{smallmatrix}\right)^3$		7
35	8	1	1	C_1	$C_6\times C_{12}$	$\langle 2,-4,1\rangle$	$\left(\begin{smallmatrix}3 & -1\\ 2 & -1\end{smallmatrix}\right)^{12}$	**Y**	13
		2	1	C_1	$C_2\times C_6\times C_{12}$	$\langle 1,-6,1\rangle$	$\left(\begin{smallmatrix}6 & -1\\ 1 & 0\end{smallmatrix}\right)^6$		7
		3	1	C_1	$C_2\times C_6\times C_{24}$	$\langle 7,-10,1\rangle$	$\left(\begin{smallmatrix}37 & -4\\ 28 & -3\end{smallmatrix}\right)^3$		13
		4	1	C_1	$C_2\times C_6\times C_{24}$	$\langle 4,-12,1\rangle$	$\left(\begin{smallmatrix}35 & -3\\ 12 & -1\end{smallmatrix}\right)^3$		7
		6	2	C_2	$C_2\times C_6\times C_{24}$	$\langle 9,-18,1\rangle$	$\left(\begin{smallmatrix}35 & -2\\ 18 & -1\end{smallmatrix}\right)^3$		7
						$\langle 4,-20,7\rangle$	$\left(\begin{smallmatrix}37 & -14\\ 8 & -3\end{smallmatrix}\right)^3$		10
		12	4	C_4	$C_2\times C_6\times C_{24}$	$\langle 1,-34,1\rangle$	$\left(\begin{smallmatrix}34 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 16,8,-17\rangle$	$\left(\begin{smallmatrix}13 & 17\\ 16 & 21\end{smallmatrix}\right)^3$		13
						$\langle 4,-36,9\rangle$	$\left(\begin{smallmatrix}35 & -9\\ 4 & -1\end{smallmatrix}\right)^3$		7
						$\langle 28,-12,-9\rangle$	$\left(\begin{smallmatrix}23 & 9\\ 28 & 11\end{smallmatrix}\right)^3$		13
36	1221	1	4	C_4	$C_2\times C_6^3$	$\langle 1,-35,1\rangle$	$\left(\begin{smallmatrix}35 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 15,-39,5\rangle$	$\left(\begin{smallmatrix}37 & -5\\ 15 & -2\end{smallmatrix}\right)^3$		10
						$\langle 25,-11,-11\rangle$	$\left(\begin{smallmatrix}23 & 11\\ 25 & 12\end{smallmatrix}\right)^3$		10
						$\langle 5,-39,15\rangle$	$\left(\begin{smallmatrix}37 & -15\\ 5 & -2\end{smallmatrix}\right)^3$		10
37	1292	1	4	C_4	$C_{12}\times C_{36}$	$\langle 1,-36,1\rangle$	$\left(\begin{smallmatrix}36 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 11,-40,7\rangle$	$\left(\begin{smallmatrix}38 & -7\\ 11 & -2\end{smallmatrix}\right)^3$		10
						$\langle 19,0,-17\rangle$	$\left(\begin{smallmatrix}18 & 17\\ 19 & 18\end{smallmatrix}\right)^3$		7
						$\langle 23,2,-14\rangle$	$\left(\begin{smallmatrix}17 & 14\\ 23 & 19\end{smallmatrix}\right)^3$		10
38	1365	1	4	C_2^2	$C_2\times C_{18}^2$	$\langle 1,-37,1\rangle$	$\left(\begin{smallmatrix}37 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 13,-39,3\rangle$	$\left(\begin{smallmatrix}38 & -3\\ 13 & -1\end{smallmatrix}\right)^3$		7
						$\langle 33,-45,5\rangle$	$\left(\begin{smallmatrix}41 & -5\\ 33 & -4\end{smallmatrix}\right)^3$		16
						$\langle 11,-43,11\rangle$	$\left(\begin{smallmatrix}40 & -11\\ 11 & -3\end{smallmatrix}\right)^3$		10
39	40	1	2	C_2	$C_2\times C_4\times C_{12}$	$\langle 6,-8,1\rangle$	$\left(\begin{smallmatrix}7 & -1\\ 6 & -1\end{smallmatrix}\right)^6$	**Y**	19
						$\langle 3,-8,2\rangle$	$\left(\begin{smallmatrix}7 & -2\\ 3 & -1\end{smallmatrix}\right)^6$	**Y**	13
		2	2	C_2	$C_2^2\times C_4\times C_{12}$	$\langle 9,-14,1\rangle$	$\left(\begin{smallmatrix}40 & -3\\ 27 & -2\end{smallmatrix}\right)^3$		10
						$\langle 3,-14,3\rangle$	$\left(\begin{smallmatrix}40 & -9\\ 9 & -2\end{smallmatrix}\right)^3$		10
		3	2	C_2	$C_2\times C_{12}^2$	$\langle 10,-20,1\rangle$	$\left(\begin{smallmatrix}39 & -2\\ 20 & -1\end{smallmatrix}\right)^3$		7
						$\langle 2,-20,5\rangle$	$\left(\begin{smallmatrix}39 & -10\\ 4 & -1\end{smallmatrix}\right)^3$		7

		6	4	C_2^2	$C_2 \times C_{12}^2$	$\langle 1, -38, 1\rangle$	$\left(\begin{smallmatrix} 38 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 31, -18, -9\rangle$	$\left(\begin{smallmatrix} 28 & 9 \\ 31 & 10 \end{smallmatrix}\right)^3$	13
						$\langle 8, -48, 27\rangle$	$\left(\begin{smallmatrix} 43 & -27 \\ 8 & -5 \end{smallmatrix}\right)^3$	13
						$\langle 8, 24, -27\rangle$	$\left(\begin{smallmatrix} 7 & 27 \\ 8 & 31 \end{smallmatrix}\right)^3$	7
40	1517	1	2	C_2	$C_2 \times C_4^2 \times C_{24}$	$\langle 1, -39, 1\rangle$	$\left(\begin{smallmatrix} 39 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 17, -49, 13\rangle$	$\left(\begin{smallmatrix} 44 & -13 \\ 17 & -5 \end{smallmatrix}\right)^3$	13
41	1596	1	8	$C_2 \times C_4$	C_{560}	$\langle 1, -40, 1\rangle$	$\left(\begin{smallmatrix} 40 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 5, -44, 17\rangle$	$\left(\begin{smallmatrix} 42 & -17 \\ 5 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 14, -42, 3\rangle$	$\left(\begin{smallmatrix} 41 & -3 \\ 14 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 17, -44, 5\rangle$	$\left(\begin{smallmatrix} 42 & -5 \\ 17 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 6, -42, 7\rangle$	$\left(\begin{smallmatrix} 41 & -7 \\ 6 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 34, -10, -11\rangle$	$\left(\begin{smallmatrix} 25 & 11 \\ 34 & 15 \end{smallmatrix}\right)^3$	13
						$\langle 21, 0, -19\rangle$	$\left(\begin{smallmatrix} 20 & 19 \\ 21 & 20 \end{smallmatrix}\right)^3$	7
						$\langle 13, -46, 10\rangle$	$\left(\begin{smallmatrix} 43 & -10 \\ 13 & -3 \end{smallmatrix}\right)^3$	13
42	1677	1	4	C_4	$C_2 \times C_6^3$	$\langle 1, -41, 1\rangle$	$\left(\begin{smallmatrix} 41 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 19, -47, 7\rangle$	$\left(\begin{smallmatrix} 44 & -7 \\ 19 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 29, -13, -13\rangle$	$\left(\begin{smallmatrix} 27 & 13 \\ 29 & 14 \end{smallmatrix}\right)^3$	10
						$\langle 7, -47, 19\rangle$	$\left(\begin{smallmatrix} 44 & -19 \\ 7 & -3 \end{smallmatrix}\right)^3$	13
43	440	1	2	C_2	$C_{14} \times C_{42}$	$\langle 11, -22, 1\rangle$	$\left(\begin{smallmatrix} 43 & -2 \\ 22 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 17, -24, 2\rangle$	$\left(\begin{smallmatrix} 45 & -4 \\ 34 & -3 \end{smallmatrix}\right)^3$	13
		2	4	C_2^2	$C_{14} \times C_{42}$	$\langle 1, -42, 1\rangle$	$\left(\begin{smallmatrix} 42 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 11, 22, -29\rangle$	$\left(\begin{smallmatrix} 10 & 29 \\ 11 & 32 \end{smallmatrix}\right)^3$	7
						$\langle 37, -24, -8\rangle$	$\left(\begin{smallmatrix} 33 & 8 \\ 37 & 9 \end{smallmatrix}\right)^3$	16
						$\langle 17, -48, 8\rangle$	$\left(\begin{smallmatrix} 45 & -8 \\ 17 & -3 \end{smallmatrix}\right)^3$	10
44	205	1	2	C_2	$C_2^3 \times C_{120}$	$\langle 5, -15, 1\rangle$	$\left(\begin{smallmatrix} 44 & -3 \\ 15 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 7, -17, 3\rangle$	$\left(\begin{smallmatrix} 47 & -9 \\ 21 & -4 \end{smallmatrix}\right)^3$	16
		3	4	C_4	$C_2^3 \times C_{120}$	$\langle 1, -43, 1\rangle$	$\left(\begin{smallmatrix} 43 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 7, -47, 13\rangle$	$\left(\begin{smallmatrix} 45 & -13 \\ 7 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 9, 27, -31\rangle$	$\left(\begin{smallmatrix} 8 & 31 \\ 9 & 35 \end{smallmatrix}\right)^3$	7

						$\langle 27,-3,-17\rangle$	$\left(\begin{smallmatrix}23 & 17\\ 27 & 20\end{smallmatrix}\right)^3$		10
45	1932	1	4	C_2^2	$C_3\times C_6\times C_{24}$	$\langle 1,-44,1\rangle$	$\left(\begin{smallmatrix}44 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 23,-46,2\rangle$	$\left(\begin{smallmatrix}45 & -2\\ 23 & -1\end{smallmatrix}\right)^3$		7
						$\langle 31,-48,3\rangle$	$\left(\begin{smallmatrix}46 & -3\\ 31 & -2\end{smallmatrix}\right)^3$		10
						$\langle 41,-54,6\rangle$	$\left(\begin{smallmatrix}49 & -6\\ 41 & -5\end{smallmatrix}\right)^3$		19
46	2021	1	3	C_3	$C_2\times C_{528}$	$\langle 1,-45,1\rangle$	$\left(\begin{smallmatrix}45 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 19,-49,5\rangle$	$\left(\begin{smallmatrix}47 & -5\\ 19 & -2\end{smallmatrix}\right)^3$		10
						$\langle 5,-49,19\rangle$	$\left(\begin{smallmatrix}47 & -19\\ 5 & -2\end{smallmatrix}\right)^3$		10
47	33	1	1	C_1	C_{736}	$\langle 4,-7,1\rangle$	$\left(\begin{smallmatrix}51 & -8\\ 32 & -5\end{smallmatrix}\right)^3$		13
		2	1	C_1	C_{736}	$\langle 3,-12,1\rangle$	$\left(\begin{smallmatrix}47 & -4\\ 12 & -1\end{smallmatrix}\right)^3$		7
		4	2	C_2	C_{736}	$\langle 12,-24,1\rangle$	$\left(\begin{smallmatrix}47 & -2\\ 24 & -1\end{smallmatrix}\right)^3$		7
						$\langle 4,16,-17\rangle$	$\left(\begin{smallmatrix}7 & 34\\ 8 & 39\end{smallmatrix}\right)^3$		7
		8	4	C_2^2	C_{736}	$\langle 1,-46,1\rangle$	$\left(\begin{smallmatrix}46 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 37,-22,-11\rangle$	$\left(\begin{smallmatrix}34 & 11\\ 37 & 12\end{smallmatrix}\right)^3$		13
						$\langle 3,-48,16\rangle$	$\left(\begin{smallmatrix}47 & -16\\ 3 & -1\end{smallmatrix}\right)^3$		7
						$\langle 31,2,-17\rangle$	$\left(\begin{smallmatrix}22 & 17\\ 31 & 24\end{smallmatrix}\right)^3$		13
48	5	1	1	C_1	$C_2\times C_8^2$	$\langle 1,-3,1\rangle$	$\left(\begin{smallmatrix}2 & -1\\ 1 & -1\end{smallmatrix}\right)^{24}$	**Y**	13
		3	1	C_1	$C_2\times C_8\times C_{24}$	$\langle 1,-7,1\rangle$	$\left(\begin{smallmatrix}7 & -1\\ 1 & 0\end{smallmatrix}\right)^6$		7
		7	1	C_1	$C_2\times C_8^2$	$\langle 11,-17,1\rangle$	$\left(\begin{smallmatrix}49 & -3\\ 33 & -2\end{smallmatrix}\right)^3$		10
		21	4	C_4	$C_2^2\times C_8\times C_{24}$	$\langle 1,-47,1\rangle$	$\left(\begin{smallmatrix}47 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 11,-51,9\rangle$	$\left(\begin{smallmatrix}49 & -9\\ 11 & -2\end{smallmatrix}\right)^3$		10
						$\langle 41,-55,5\rangle$	$\left(\begin{smallmatrix}51 & -5\\ 41 & -4\end{smallmatrix}\right)^3$		16
						$\langle 9,-51,11\rangle$	$\left(\begin{smallmatrix}49 & -11\\ 9 & -2\end{smallmatrix}\right)^3$		10
49	92	1	1	C_1	$C_{14}\times C_{42}$	$\langle 2,-10,1\rangle$	$\left(\begin{smallmatrix}49 & -5\\ 10 & -1\end{smallmatrix}\right)^3$		7
		5	6	C_6	$C_{14}\times C_{42}$	$\langle 1,-48,1\rangle$	$\left(\begin{smallmatrix}48 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 7,-54,22\rangle$	$\left(\begin{smallmatrix}51 & -22\\ 7 & -3\end{smallmatrix}\right)^3$		13
						$\langle 11,-54,14\rangle$	$\left(\begin{smallmatrix}51 & -14\\ 11 & -3\end{smallmatrix}\right)^3$		10
						$\langle 25,-50,2\rangle$	$\left(\begin{smallmatrix}49 & -2\\ 25 & -1\end{smallmatrix}\right)^3$		7
						$\langle 14,-54,11\rangle$	$\left(\begin{smallmatrix}51 & -11\\ 14 & -3\end{smallmatrix}\right)^3$		10

						$\langle 22,-54,7\rangle$	$\left(\begin{smallmatrix}51 & -7\\ 22 & -3\end{smallmatrix}\right)^3$		13
50	2397	1	2	C_2	$C_{10}\times C_{120}$	$\langle 1,-49,1\rangle$	$\left(\begin{smallmatrix}49 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 17,-51,3\rangle$	$\left(\begin{smallmatrix}50 & -3\\ 17 & -1\end{smallmatrix}\right)^3$		7
51	156	1	2	C_2	$C_2\times C_{288}$	$\langle 10,-14,1\rangle$	$\left(\begin{smallmatrix}53 & -4\\ 40 & -3\end{smallmatrix}\right)^3$		13
						$\langle 5,-14,2\rangle$	$\left(\begin{smallmatrix}53 & -8\\ 20 & -3\end{smallmatrix}\right)^3$		10
		2	4	C_4	$C_2\times C_{288}$	$\langle 13,-26,1\rangle$	$\left(\begin{smallmatrix}51 & -2\\ 26 & -1\end{smallmatrix}\right)^3$		7
						$\langle 5,-28,8\rangle$	$\left(\begin{smallmatrix}53 & -16\\ 10 & -3\end{smallmatrix}\right)^3$		13
						$\langle 23,-16,-4\rangle$	$\left(\begin{smallmatrix}41 & 8\\ 46 & 9\end{smallmatrix}\right)^3$		19
						$\langle 20,-8,-7\rangle$	$\left(\begin{smallmatrix}33 & 14\\ 40 & 17\end{smallmatrix}\right)^3$		13
		4	8	$C_2\times C_4$	$C_2\times C_{288}$	$\langle 1,-50,1\rangle$	$\left(\begin{smallmatrix}50 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 15,-54,7\rangle$	$\left(\begin{smallmatrix}52 & -7\\ 15 & -2\end{smallmatrix}\right)^3$		10
						$\langle 12,-60,23\rangle$	$\left(\begin{smallmatrix}55 & -23\\ 12 & -5\end{smallmatrix}\right)^3$		13
						$\langle 7,-54,15\rangle$	$\left(\begin{smallmatrix}52 & -15\\ 7 & -2\end{smallmatrix}\right)^3$		10
						$\langle 13,26,-35\rangle$	$\left(\begin{smallmatrix}12 & 35\\ 13 & 38\end{smallmatrix}\right)^3$		7
						$\langle 21,-54,5\rangle$	$\left(\begin{smallmatrix}52 & -5\\ 21 & -2\end{smallmatrix}\right)^3$		10
						$\langle 35,-16,-16\rangle$	$\left(\begin{smallmatrix}33 & 16\\ 35 & 17\end{smallmatrix}\right)^3$		10
						$\langle 5,-54,21\rangle$	$\left(\begin{smallmatrix}52 & -21\\ 5 & -2\end{smallmatrix}\right)^3$		10
52	53	1	1	C_1	$C_2^2\times C_{12}^2$	$\langle 7,-9,1\rangle$	$\left(\begin{smallmatrix}8 & -1\\ 7 & -1\end{smallmatrix}\right)^6$	**Y**	22
		7	3	C_3	$C_2^3\times C_{12}^2$	$\langle 1,-51,1\rangle$	$\left(\begin{smallmatrix}51 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 17,-59,13\rangle$	$\left(\begin{smallmatrix}55 & -13\\ 17 & -4\end{smallmatrix}\right)^3$		16
						$\langle 13,-59,17\rangle$	$\left(\begin{smallmatrix}55 & -17\\ 13 & -4\end{smallmatrix}\right)^3$		16
53	12	1	1	C_1	C_{312}	$\langle 1,-4,1\rangle$	$\left(\begin{smallmatrix}4 & -1\\ 1 & 0\end{smallmatrix}\right)^9$		10
		3	1	C_1	C_{936}	$\langle 9,-12,1\rangle$	$\left(\begin{smallmatrix}56 & -5\\ 45 & -4\end{smallmatrix}\right)^3$		16
		5	2	C_2	C_{936}	$\langle 6,-18,1\rangle$	$\left(\begin{smallmatrix}53 & -3\\ 18 & -1\end{smallmatrix}\right)^3$		7
						$\langle 3,-18,2\rangle$	$\left(\begin{smallmatrix}53 & -6\\ 9 & -1\end{smallmatrix}\right)^3$		7
		15	6	C_6	C_{936}	$\langle 1,-52,1\rangle$	$\left(\begin{smallmatrix}52 & -1\\ 1 & 0\end{smallmatrix}\right)^3$		4
						$\langle 22,-62,13\rangle$	$\left(\begin{smallmatrix}57 & -13\\ 22 & -5\end{smallmatrix}\right)^3$		13
						$\langle 9,-60,25\rangle$	$\left(\begin{smallmatrix}56 & -25\\ 9 & -4\end{smallmatrix}\right)^3$		16
						$\langle 27,-54,2\rangle$	$\left(\begin{smallmatrix}53 & -2\\ 27 & -1\end{smallmatrix}\right)^3$		7

						$\langle 25,-60,9\rangle$	$\left(\begin{smallmatrix}56 & -9\\ 25 & -4\end{smallmatrix}\right)^3$	16
						$\langle 13,-62,22\rangle$	$\left(\begin{smallmatrix}57 & -22\\ 13 & -5\end{smallmatrix}\right)^3$	13
54	2805	1	4	C_2^2	$C_3 \times C_{18}^2$	$\langle 1,-53,1\rangle$	$\left(\begin{smallmatrix}53 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 37,-57,3\rangle$	$\left(\begin{smallmatrix}55 & -3\\ 37 & -2\end{smallmatrix}\right)^3$	10
						$\langle 11,-55,5\rangle$	$\left(\begin{smallmatrix}54 & -5\\ 11 & -1\end{smallmatrix}\right)^3$	7
						$\langle 13,-59,13\rangle$	$\left(\begin{smallmatrix}56 & -13\\ 13 & -3\end{smallmatrix}\right)^3$	13
55	728	1	2	C_2	$C_8 \times C_{120}$	$\langle 14,-28,1\rangle$	$\left(\begin{smallmatrix}55 & -2\\ 28 & -1\end{smallmatrix}\right)^3$	7
						$\langle 7,-28,2\rangle$	$\left(\begin{smallmatrix}55 & -4\\ 14 & -1\end{smallmatrix}\right)^3$	7
		2	4	C_2^2	$C_8 \times C_{120}$	$\langle 1,-54,1\rangle$	$\left(\begin{smallmatrix}54 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 43,-26,-13\rangle$	$\left(\begin{smallmatrix}40 & 13\\ 43 & 14\end{smallmatrix}\right)^3$	13
						$\langle 8,-64,37\rangle$	$\left(\begin{smallmatrix}59 & -37\\ 8 & -5\end{smallmatrix}\right)^3$	13
						$\langle 8,-56,7\rangle$	$\left(\begin{smallmatrix}55 & -7\\ 8 & -1\end{smallmatrix}\right)^3$	7
56	3021	1	6	C_6	$C_2^3 \times C_{12}^2$	$\langle 1,-55,1\rangle$	$\left(\begin{smallmatrix}55 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 23,-59,5\rangle$	$\left(\begin{smallmatrix}57 & -5\\ 23 & -2\end{smallmatrix}\right)^3$	10
						$\langle 25,-61,7\rangle$	$\left(\begin{smallmatrix}58 & -7\\ 25 & -3\end{smallmatrix}\right)^3$	13
						$\langle 19,19,-35\rangle$	$\left(\begin{smallmatrix}18 & 35\\ 19 & 37\end{smallmatrix}\right)^3$	7
						$\langle 7,-61,25\rangle$	$\left(\begin{smallmatrix}58 & -25\\ 7 & -3\end{smallmatrix}\right)^3$	13
						$\langle 5,-59,23\rangle$	$\left(\begin{smallmatrix}57 & -23\\ 5 & -2\end{smallmatrix}\right)^3$	10
57	348	1	2	C_2	$C_6^2 \times C_{18}$	$\langle 13,-20,1\rangle$	$\left(\begin{smallmatrix}58 & -3\\ 39 & -2\end{smallmatrix}\right)^3$	10
						$\langle 17,-22,2\rangle$	$\left(\begin{smallmatrix}61 & -6\\ 51 & -5\end{smallmatrix}\right)^3$	19
		3	6	C_6	$C_2 \times C_{18}^2$	$\langle 1,-56,1\rangle$	$\left(\begin{smallmatrix}56 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 18,-66,17\rangle$	$\left(\begin{smallmatrix}61 & -17\\ 18 & -5\end{smallmatrix}\right)^3$	13
						$\langle 9,-60,13\rangle$	$\left(\begin{smallmatrix}58 & -13\\ 9 & -2\end{smallmatrix}\right)^3$	10
						$\langle 29,-58,2\rangle$	$\left(\begin{smallmatrix}57 & -2\\ 29 & -1\end{smallmatrix}\right)^3$	7
						$\langle 13,-60,9\rangle$	$\left(\begin{smallmatrix}58 & -9\\ 13 & -2\end{smallmatrix}\right)^3$	10
						$\langle 17,-66,18\rangle$	$\left(\begin{smallmatrix}61 & -18\\ 17 & -5\end{smallmatrix}\right)^3$	13
58	3245	1	4	C_4	$C_2 \times C_{840}$	$\langle 1,-57,1\rangle$	$\left(\begin{smallmatrix}57 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 7,-61,17\rangle$	$\left(\begin{smallmatrix}59 & -17\\ 7 & -2\end{smallmatrix}\right)^3$	10
						$\langle 49,-33,-11\rangle$	$\left(\begin{smallmatrix}45 & 11\\ 49 & 12\end{smallmatrix}\right)^3$	16

						$\langle 17,-61,7\rangle$	$\left(\begin{smallmatrix}59 & -7\\ 17 & -2\end{smallmatrix}\right)^3$	10
59	840	1	4	C_2^2	C_{1160}	$\langle 15,-30,1\rangle$	$\left(\begin{smallmatrix}59 & -2\\ 30 & -1\end{smallmatrix}\right)^3$	7
						$\langle 23,-32,2\rangle$	$\left(\begin{smallmatrix}61 & -4\\ 46 & -3\end{smallmatrix}\right)^3$	13
						$\langle 5,-30,3\rangle$	$\left(\begin{smallmatrix}59 & -6\\ 10 & -1\end{smallmatrix}\right)^3$	7
						$\langle 19,2,-11\rangle$	$\left(\begin{smallmatrix}27 & 22\\ 38 & 31\end{smallmatrix}\right)^3$	13
		2	8	C_2^3	C_{1160}	$\langle 1,-58,1\rangle$	$\left(\begin{smallmatrix}58 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 15,30,-41\rangle$	$\left(\begin{smallmatrix}14 & 41\\ 15 & 44\end{smallmatrix}\right)^3$	7
						$\langle 23,18,-33\rangle$	$\left(\begin{smallmatrix}20 & 33\\ 23 & 38\end{smallmatrix}\right)^3$	10
						$\langle 55,-70,7\rangle$	$\left(\begin{smallmatrix}64 & -7\\ 55 & -6\end{smallmatrix}\right)^3$	22
						$\langle 20,20,-37\rangle$	$\left(\begin{smallmatrix}19 & 37\\ 20 & 39\end{smallmatrix}\right)^3$	7
						$\langle 12,-60,5\rangle$	$\left(\begin{smallmatrix}59 & -5\\ 12 & -1\end{smallmatrix}\right)^3$	7
						$\langle 11,-62,11\rangle$	$\left(\begin{smallmatrix}60 & -11\\ 11 & -2\end{smallmatrix}\right)^3$	10
						$\langle 40,0,-21\rangle$	$\left(\begin{smallmatrix}29 & 21\\ 40 & 29\end{smallmatrix}\right)^3$	13
60	3477	1	4	C_4	$C_2^3\times C_6\times C_{24}$	$\langle 1,-59,1\rangle$	$\left(\begin{smallmatrix}59 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 17,-65,11\rangle$	$\left(\begin{smallmatrix}62 & -11\\ 17 & -3\end{smallmatrix}\right)^3$	10
						$\langle 41,-19,-19\rangle$	$\left(\begin{smallmatrix}39 & 19\\ 41 & 20\end{smallmatrix}\right)^3$	10
						$\langle 11,-65,17\rangle$	$\left(\begin{smallmatrix}62 & -17\\ 11 & -3\end{smallmatrix}\right)^3$	10
61	3596	1	6	C_6	$C_{20}\times C_{60}$	$\langle 1,-60,1\rangle$	$\left(\begin{smallmatrix}60 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 19,-66,10\rangle$	$\left(\begin{smallmatrix}63 & -10\\ 19 & -3\end{smallmatrix}\right)^3$	13
						$\langle 25,-64,5\rangle$	$\left(\begin{smallmatrix}62 & -5\\ 25 & -2\end{smallmatrix}\right)^3$	10
						$\langle 31,-62,2\rangle$	$\left(\begin{smallmatrix}61 & -2\\ 31 & -1\end{smallmatrix}\right)^3$	7
						$\langle 5,-64,25\rangle$	$\left(\begin{smallmatrix}62 & -25\\ 5 & -2\end{smallmatrix}\right)^3$	10
						$\langle 50,-14,-17\rangle$	$\left(\begin{smallmatrix}37 & 17\\ 50 & 23\end{smallmatrix}\right)^3$	13
62	413	1	1	C_1	$C_2\times C_{30}^2$	$\langle 7,-21,1\rangle$	$\left(\begin{smallmatrix}62 & -3\\ 21 & -1\end{smallmatrix}\right)^3$	7
		3	4	C_4	$C_2\times C_{30}^2$	$\langle 1,-61,1\rangle$	$\left(\begin{smallmatrix}61 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 9,51,-31\rangle$	$\left(\begin{smallmatrix}5 & 31\\ 9 & 56\end{smallmatrix}\right)^3$	16
						$\langle 7,-63,9\rangle$	$\left(\begin{smallmatrix}62 & -9\\ 7 & -1\end{smallmatrix}\right)^3$	7
						$\langle 29,11,-31\rangle$	$\left(\begin{smallmatrix}25 & 31\\ 29 & 36\end{smallmatrix}\right)^3$	16
63	60	1	2	C_2	$C_3^2\times C_6^2$	$\langle 1,-8,1\rangle$	$\left(\begin{smallmatrix}8 & -1\\ 1 & 0\end{smallmatrix}\right)^6$	7

						$\langle 5,-10,2\rangle$	$\left(\begin{smallmatrix}9&-2\\5&-1\end{smallmatrix}\right)^6$	13
		2	2	C_2	$C_3\times C_6^3$	$\langle 4,-16,1\rangle$	$\left(\begin{smallmatrix}63&-4\\16&-1\end{smallmatrix}\right)^3$	7
						$\langle 3,-18,7\rangle$	$\left(\begin{smallmatrix}67&-28\\12&-5\end{smallmatrix}\right)^3$	13
		4	4	C_2^2	$C_3\times C_6^3$	$\langle 16,-32,1\rangle$	$\left(\begin{smallmatrix}63&-2\\32&-1\end{smallmatrix}\right)^3$	7
						$\langle 28,-36,3\rangle$	$\left(\begin{smallmatrix}67&-6\\56&-5\end{smallmatrix}\right)^3$	19
						$\langle 21,6,-11\rangle$	$\left(\begin{smallmatrix}25&22\\42&37\end{smallmatrix}\right)^3$	13
						$\langle 12,12,-17\rangle$	$\left(\begin{smallmatrix}19&34\\24&43\end{smallmatrix}\right)^3$	10
		8	8	$C_2\times C_4$	$C_3\times C_6^3$	$\langle 1,-62,1\rangle$	$\left(\begin{smallmatrix}62&-1\\1&0\end{smallmatrix}\right)^3$	4
						$\langle 44,-76,11\rangle$	$\left(\begin{smallmatrix}69&-11\\44&-7\end{smallmatrix}\right)^3$	16
						$\langle 49,-30,-15\rangle$	$\left(\begin{smallmatrix}46&15\\49&16\end{smallmatrix}\right)^3$	13
						$\langle 11,-76,44\rangle$	$\left(\begin{smallmatrix}69&-44\\11&-7\end{smallmatrix}\right)^3$	16
						$\langle 43,-66,3\rangle$	$\left(\begin{smallmatrix}64&-3\\43&-2\end{smallmatrix}\right)^3$	10
						$\langle 28,12,-33\rangle$	$\left(\begin{smallmatrix}25&33\\28&37\end{smallmatrix}\right)^3$	13
						$\langle 53,-36,-12\rangle$	$\left(\begin{smallmatrix}49&12\\53&13\end{smallmatrix}\right)^3$	16
						$\langle 28,-68,7\rangle$	$\left(\begin{smallmatrix}65&-7\\28&-3\end{smallmatrix}\right)^3$	13
64	3965	1	4	C_2^2	$C_2\times C_{32}^2$	$\langle 1,-63,1\rangle$	$\left(\begin{smallmatrix}63&-1\\1&0\end{smallmatrix}\right)^3$	4
						$\langle 31,-73,11\rangle$	$\left(\begin{smallmatrix}68&-11\\31&-5\end{smallmatrix}\right)^3$	19
						$\langle 13,-65,5\rangle$	$\left(\begin{smallmatrix}64&-5\\13&-1\end{smallmatrix}\right)^3$	7
						$\langle 43,3,-23\rangle$	$\left(\begin{smallmatrix}30&23\\43&33\end{smallmatrix}\right)^3$	16
65	4092	1	8	$C_2\times C_4$	$C_4\times C_{12}\times C_{24}$	$\langle 1,-64,1\rangle$	$\left(\begin{smallmatrix}64&-1\\1&0\end{smallmatrix}\right)^3$	4
						$\langle 21,-72,13\rangle$	$\left(\begin{smallmatrix}68&-13\\21&-4\end{smallmatrix}\right)^3$	16
						$\langle 11,44,-49\rangle$	$\left(\begin{smallmatrix}10&49\\11&54\end{smallmatrix}\right)^3$	7
						$\langle 13,-72,21\rangle$	$\left(\begin{smallmatrix}68&-21\\13&-4\end{smallmatrix}\right)^3$	16
						$\langle 22,-66,3\rangle$	$\left(\begin{smallmatrix}65&-3\\22&-1\end{smallmatrix}\right)^3$	7
						$\langle 39,-6,-26\rangle$	$\left(\begin{smallmatrix}35&26\\39&29\end{smallmatrix}\right)^3$	10
						$\langle 33,0,-31\rangle$	$\left(\begin{smallmatrix}32&31\\33&32\end{smallmatrix}\right)^3$	7
						$\langle 7,-68,19\rangle$	$\left(\begin{smallmatrix}66&-19\\7&-2\end{smallmatrix}\right)^3$	10
66	469	1	3	C_3	$C_2^3\times C_{120}$	$\langle 15,-23,1\rangle$	$\left(\begin{smallmatrix}67&-3\\45&-2\end{smallmatrix}\right)^3$	10
						$\langle 3,-23,5\rangle$	$\left(\begin{smallmatrix}67&-15\\9&-2\end{smallmatrix}\right)^3$	10
						$\langle 5,-23,3\rangle$	$\left(\begin{smallmatrix}67&-9\\15&-2\end{smallmatrix}\right)^3$	10

		3	6	C_6	$C_2 \times C_6 \times C_{120}$	$\langle 1, -65, 1\rangle$	$\left(\begin{smallmatrix} 65 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 27, -75, 13\rangle$	$\left(\begin{smallmatrix} 70 & -13 \\ 27 & -5 \end{smallmatrix}\right)^3$		13
						$\langle 41, -11, -25\rangle$	$\left(\begin{smallmatrix} 38 & 25 \\ 41 & 27 \end{smallmatrix}\right)^3$		10
						$\langle 61, -77, 7\rangle$	$\left(\begin{smallmatrix} 71 & -7 \\ 61 & -6 \end{smallmatrix}\right)^3$		22
						$\langle 5, -69, 27\rangle$	$\left(\begin{smallmatrix} 67 & -27 \\ 5 & -2 \end{smallmatrix}\right)^3$		10
						$\langle 13, -75, 27\rangle$	$\left(\begin{smallmatrix} 70 & -27 \\ 13 & -5 \end{smallmatrix}\right)^3$		13
67	17	1	1	C_1	$C_{11} \times C_{66}$	$\langle 2, -5, 1\rangle$	$\left(\begin{smallmatrix} 9 & -2 \\ 4 & -1 \end{smallmatrix}\right)^6$	**Y**	16
		2	1	C_1	$C_{11} \times C_{66}$	$\langle 8, -10, 1\rangle$	$\left(\begin{smallmatrix} 9 & -1 \\ 8 & -1 \end{smallmatrix}\right)^6$	**Y**	25
		4	1	C_1	$C_{22} \times C_{66}$	$\langle 13, -18, 1\rangle$	$\left(\begin{smallmatrix} 69 & -4 \\ 52 & -3 \end{smallmatrix}\right)^3$		13
		8	2	C_2	$C_{22} \times C_{66}$	$\langle 17, -34, 1\rangle$	$\left(\begin{smallmatrix} 67 & -2 \\ 34 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 13, 10, -19\rangle$	$\left(\begin{smallmatrix} 23 & 38 \\ 26 & 43 \end{smallmatrix}\right)^3$		10
		16	4	C_4	$C_{22} \times C_{66}$	$\langle 1, -66, 1\rangle$	$\left(\begin{smallmatrix} 66 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 53, -18, -19\rangle$	$\left(\begin{smallmatrix} 42 & 19 \\ 53 & 24 \end{smallmatrix}\right)^3$		13
						$\langle 17, -68, 4\rangle$	$\left(\begin{smallmatrix} 67 & -4 \\ 17 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 52, -20, -19\rangle$	$\left(\begin{smallmatrix} 43 & 19 \\ 52 & 23 \end{smallmatrix}\right)^3$		13
68	4485	1	4	C_2^2	$C_2^3 \times C_{288}$	$\langle 1, -67, 1\rangle$	$\left(\begin{smallmatrix} 67 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 23, -69, 3\rangle$	$\left(\begin{smallmatrix} 68 & -3 \\ 23 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 57, -75, 5\rangle$	$\left(\begin{smallmatrix} 71 & -5 \\ 57 & -4 \end{smallmatrix}\right)^3$		16
						$\langle 15, -75, 19\rangle$	$\left(\begin{smallmatrix} 71 & -19 \\ 15 & -4 \end{smallmatrix}\right)^3$		10
69	4620	1	8	C_2^3	$C_2 \times C_{528}$	$\langle 1, -68, 1\rangle$	$\left(\begin{smallmatrix} 68 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 35, -70, 2\rangle$	$\left(\begin{smallmatrix} 69 & -2 \\ 35 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 47, -72, 3\rangle$	$\left(\begin{smallmatrix} 70 & -3 \\ 47 & -2 \end{smallmatrix}\right)^3$		10
						$\langle 61, -78, 6\rangle$	$\left(\begin{smallmatrix} 73 & -6 \\ 61 & -5 \end{smallmatrix}\right)^3$		19
						$\langle 14, -70, 5\rangle$	$\left(\begin{smallmatrix} 69 & -5 \\ 14 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 10, -70, 7\rangle$	$\left(\begin{smallmatrix} 69 & -7 \\ 10 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 17, -76, 17\rangle$	$\left(\begin{smallmatrix} 72 & -17 \\ 17 & -4 \end{smallmatrix}\right)^3$		16
						$\langle 21, -84, 29\rangle$	$\left(\begin{smallmatrix} 76 & -29 \\ 21 & -8 \end{smallmatrix}\right)^3$		13
70	4757	1	5	C_5	$C_2 \times C_6^2 \times C_{24}$	$\langle 1, -69, 1\rangle$	$\left(\begin{smallmatrix} 69 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 31, -75, 7\rangle$	$\left(\begin{smallmatrix} 72 & -7 \\ 31 & -3 \end{smallmatrix}\right)^3$		13

						$\langle 41,-1,-29\rangle$	$\left(\begin{smallmatrix}35 & 29\\ 41 & 34\end{smallmatrix}\right)^3$	10
						$\langle 11,-73,13\rangle$	$\left(\begin{smallmatrix}71 & -13\\ 11 & -2\end{smallmatrix}\right)^3$	10
						$\langle 31,13,-37\rangle$	$\left(\begin{smallmatrix}28 & 37\\ 31 & 41\end{smallmatrix}\right)^3$	13
71	136	1	2	C_2	C_{1680}	$\langle 2,-12,1\rangle$	$\left(\begin{smallmatrix}71 & -6\\ 12 & -1\end{smallmatrix}\right)^3$	7
						$\langle 5,-14,3\rangle$	$\left(\begin{smallmatrix}77 & -18\\ 30 & -7\end{smallmatrix}\right)^3$	16
		2	4	C_4	C_{1680}	$\langle 8,-24,1\rangle$	$\left(\begin{smallmatrix}71 & -3\\ 24 & -1\end{smallmatrix}\right)^3$	7
						$\langle 3,-26,11\rangle$	$\left(\begin{smallmatrix}74 & -33\\ 9 & -4\end{smallmatrix}\right)^3$	16
						$\langle 15,-28,4\rangle$	$\left(\begin{smallmatrix}77 & -12\\ 45 & -7\end{smallmatrix}\right)^3$	13
						$\langle 11,-26,3\rangle$	$\left(\begin{smallmatrix}74 & -9\\ 33 & -4\end{smallmatrix}\right)^3$	16
		3	4	C_4	C_{1680}	$\langle 18,-36,1\rangle$	$\left(\begin{smallmatrix}71 & -2\\ 36 & -1\end{smallmatrix}\right)^3$	7
						$\langle 11,-38,5\rangle$	$\left(\begin{smallmatrix}73 & -10\\ 22 & -3\end{smallmatrix}\right)^3$	13
						$\langle 2,-36,9\rangle$	$\left(\begin{smallmatrix}71 & -18\\ 4 & -1\end{smallmatrix}\right)^3$	7
						$\langle 5,-38,11\rangle$	$\left(\begin{smallmatrix}73 & -22\\ 10 & -3\end{smallmatrix}\right)^3$	13
		6	8	$C_2\times C_4$	C_{1680}	$\langle 1,-70,1\rangle$	$\left(\begin{smallmatrix}70 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 5,-74,29\rangle$	$\left(\begin{smallmatrix}72 & -29\\ 5 & -2\end{smallmatrix}\right)^3$	10
						$\langle 47,14,-25\rangle$	$\left(\begin{smallmatrix}28 & 25\\ 47 & 42\end{smallmatrix}\right)^3$	13
						$\langle 44,-12,-27\rangle$	$\left(\begin{smallmatrix}41 & 27\\ 44 & 29\end{smallmatrix}\right)^3$	10
						$\langle 55,-34,-17\rangle$	$\left(\begin{smallmatrix}52 & 17\\ 55 & 18\end{smallmatrix}\right)^3$	13
						$\langle 11,-76,20\rangle$	$\left(\begin{smallmatrix}73 & -20\\ 11 & -3\end{smallmatrix}\right)^3$	10
						$\langle 9,-72,8\rangle$	$\left(\begin{smallmatrix}71 & -8\\ 9 & -1\end{smallmatrix}\right)^3$	7
						$\langle 20,-76,11\rangle$	$\left(\begin{smallmatrix}73 & -11\\ 20 & -3\end{smallmatrix}\right)^3$	10
72	5037	1	4	C_4	$C_2\times C_6\times C_{12}^2$	$\langle 1,-71,1\rangle$	$\left(\begin{smallmatrix}71 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 21,-75,7\rangle$	$\left(\begin{smallmatrix}73 & -7\\ 21 & -2\end{smallmatrix}\right)^3$	10
						$\langle 49,-23,-23\rangle$	$\left(\begin{smallmatrix}47 & 23\\ 49 & 24\end{smallmatrix}\right)^3$	10
						$\langle 7,-75,21\rangle$	$\left(\begin{smallmatrix}73 & -21\\ 7 & -2\end{smallmatrix}\right)^3$	10
73	5180	1	4	C_2^2	$C_{24}\times C_{72}$	$\langle 1,-72,1\rangle$	$\left(\begin{smallmatrix}72 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 37,-74,2\rangle$	$\left(\begin{smallmatrix}73 & -2\\ 37 & -1\end{smallmatrix}\right)^3$	7
						$\langle 61,-80,5\rangle$	$\left(\begin{smallmatrix}76 & -5\\ 61 & -4\end{smallmatrix}\right)^3$	16
						$\langle 67,-84,7\rangle$	$\left(\begin{smallmatrix}78 & -7\\ 67 & -6\end{smallmatrix}\right)^3$	22

74	213	1	1	C_1	$C_2 \times C_{36}^2$	$\langle 3, -15, 1\rangle$	$\left(\begin{smallmatrix} 74 & -5 \\ 15 & -1 \end{smallmatrix}\right)^3$	7
		5	6	C_6	$C_2 \times C_{36}^2$	$\langle 1, -73, 1\rangle$	$\left(\begin{smallmatrix} 73 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 53, -5, -25\rangle$	$\left(\begin{smallmatrix} 39 & 25 \\ 53 & 34 \end{smallmatrix}\right)^3$	13
						$\langle 51, -87, 11\rangle$	$\left(\begin{smallmatrix} 80 & -11 \\ 51 & -7 \end{smallmatrix}\right)^3$	16
						$\langle 25, 25, -47\rangle$	$\left(\begin{smallmatrix} 24 & 47 \\ 25 & 49 \end{smallmatrix}\right)^3$	7
						$\langle 11, -87, 51\rangle$	$\left(\begin{smallmatrix} 80 & -51 \\ 11 & -7 \end{smallmatrix}\right)^3$	16
						$\langle 53, 5, -25\rangle$	$\left(\begin{smallmatrix} 34 & 25 \\ 53 & 39 \end{smallmatrix}\right)^3$	13
75	152	1	1	C_1	C_{40}^2	$\langle 11, -14, 1\rangle$	$\left(\begin{smallmatrix} 79 & -6 \\ 66 & -5 \end{smallmatrix}\right)^3$	19
		2	2	C_2	C_{40}^2	$\langle 17, -26, 1\rangle$	$\left(\begin{smallmatrix} 76 & -3 \\ 51 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 19, 0, -8\rangle$	$\left(\begin{smallmatrix} 37 & 24 \\ 57 & 37 \end{smallmatrix}\right)^3$	13
		3	4	C_4	$C_{10} \times C_{120}$	$\langle 19, -38, 1\rangle$	$\left(\begin{smallmatrix} 75 & -2 \\ 38 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 26, 4, -13\rangle$	$\left(\begin{smallmatrix} 33 & 26 \\ 52 & 41 \end{smallmatrix}\right)^3$	13
						$\langle 29, -40, 2\rangle$	$\left(\begin{smallmatrix} 77 & -4 \\ 58 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 26, -4, -13\rangle$	$\left(\begin{smallmatrix} 41 & 26 \\ 52 & 33 \end{smallmatrix}\right)^3$	13
		6	8	$C_2 \times C_4$	$C_{10} \times C_{120}$	$\langle 1, -74, 1\rangle$	$\left(\begin{smallmatrix} 74 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 44, -4, -31\rangle$	$\left(\begin{smallmatrix} 39 & 31 \\ 44 & 35 \end{smallmatrix}\right)^3$	10
						$\langle 71, -88, 8\rangle$	$\left(\begin{smallmatrix} 81 & -8 \\ 71 & -7 \end{smallmatrix}\right)^3$	25
						$\langle 44, 4, -31\rangle$	$\left(\begin{smallmatrix} 35 & 31 \\ 44 & 39 \end{smallmatrix}\right)^3$	10
						$\langle 19, 38, -53\rangle$	$\left(\begin{smallmatrix} 18 & 53 \\ 19 & 56 \end{smallmatrix}\right)^3$	7
						$\langle 11, 62, -37\rangle$	$\left(\begin{smallmatrix} 6 & 37 \\ 11 & 68 \end{smallmatrix}\right)^3$	19
						$\langle 29, 22, -43\rangle$	$\left(\begin{smallmatrix} 26 & 43 \\ 29 & 48 \end{smallmatrix}\right)^3$	10
						$\langle 11, -84, 36\rangle$	$\left(\begin{smallmatrix} 79 & -36 \\ 11 & -5 \end{smallmatrix}\right)^3$	19
76	5621	1	6	C_6	$C_2^3 \times C_{18}^2$	$\langle 1, -75, 1\rangle$	$\left(\begin{smallmatrix} 75 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 31, -79, 5\rangle$	$\left(\begin{smallmatrix} 77 & -5 \\ 31 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 23, -89, 25\rangle$	$\left(\begin{smallmatrix} 82 & -25 \\ 23 & -7 \end{smallmatrix}\right)^3$	16
						$\langle 11, 55, -59\rangle$	$\left(\begin{smallmatrix} 10 & 59 \\ 11 & 65 \end{smallmatrix}\right)^3$	7
						$\langle 61, 3, -23\rangle$	$\left(\begin{smallmatrix} 36 & 23 \\ 61 & 39 \end{smallmatrix}\right)^3$	16
						$\langle 5, -79, 31\rangle$	$\left(\begin{smallmatrix} 77 & -31 \\ 5 & -2 \end{smallmatrix}\right)^3$	10
77	5772	1	8	$C_2 \times C_4$	$C_2 \times C_6 \times C_{120}$	$\langle 1, -76, 1\rangle$	$\left(\begin{smallmatrix} 76 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 7, -82, 34\rangle$	$\left(\begin{smallmatrix} 79 & -34 \\ 7 & -3 \end{smallmatrix}\right)^3$	13

						$\langle 26,-78,3\rangle$	$\left(\begin{smallmatrix}77 & -3\\ 26 & -1\end{smallmatrix}\right)^3$	7
						$\langle 34,-82,7\rangle$	$\left(\begin{smallmatrix}79 & -7\\ 34 & -3\end{smallmatrix}\right)^3$	13
						$\langle 6,-78,13\rangle$	$\left(\begin{smallmatrix}77 & -13\\ 6 & -1\end{smallmatrix}\right)^3$	7
						$\langle 29,28,-43\rangle$	$\left(\begin{smallmatrix}24 & 43\\ 29 & 52\end{smallmatrix}\right)^3$	10
						$\langle 39,0,-37\rangle$	$\left(\begin{smallmatrix}38 & 37\\ 39 & 38\end{smallmatrix}\right)^3$	7
						$\langle 14,-82,17\rangle$	$\left(\begin{smallmatrix}79 & -17\\ 14 & -3\end{smallmatrix}\right)^3$	10
78	237	1	1	C_1	$C_2\times C_6\times C_{12}^2$	$\langle 13,-17,1\rangle$	$\left(\begin{smallmatrix}81 & -5\\ 65 & -4\end{smallmatrix}\right)^3$	16
		5	6	C_6	$C_2\times C_6\times C_{12}^2$	$\langle 1,-77,1\rangle$	$\left(\begin{smallmatrix}77 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 13,59,-47\rangle$	$\left(\begin{smallmatrix}9 & 47\\ 13 & 68\end{smallmatrix}\right)^3$	16
						$\langle 31,-91,19\rangle$	$\left(\begin{smallmatrix}84 & -19\\ 31 & -7\end{smallmatrix}\right)^3$	13
						$\langle 53,-25,-25\rangle$	$\left(\begin{smallmatrix}51 & 25\\ 53 & 26\end{smallmatrix}\right)^3$	10
						$\langle 19,-91,31\rangle$	$\left(\begin{smallmatrix}84 & -31\\ 19 & -7\end{smallmatrix}\right)^3$	13
						$\langle 25,35,-47\rangle$	$\left(\begin{smallmatrix}21 & 47\\ 25 & 56\end{smallmatrix}\right)^3$	16
79	380	1	2	C_2	$C_{26}\times C_{78}$	$\langle 5,-20,1\rangle$	$\left(\begin{smallmatrix}79 & -4\\ 20 & -1\end{smallmatrix}\right)^3$	7
						$\langle 13,-22,2\rangle$	$\left(\begin{smallmatrix}83 & -8\\ 52 & -5\end{smallmatrix}\right)^3$	13
		2	4	C_4	$C_{26}\times C_{78}$	$\langle 20,-40,1\rangle$	$\left(\begin{smallmatrix}79 & -2\\ 40 & -1\end{smallmatrix}\right)^3$	7
						$\langle 8,-44,13\rangle$	$\left(\begin{smallmatrix}83 & -26\\ 16 & -5\end{smallmatrix}\right)^3$	19
						$\langle 5,-40,4\rangle$	$\left(\begin{smallmatrix}79 & -8\\ 10 & -1\end{smallmatrix}\right)^3$	7
						$\langle 13,-44,8\rangle$	$\left(\begin{smallmatrix}83 & -16\\ 26 & -5\end{smallmatrix}\right)^3$	19
		4	8	$C_2\times C_4$	$C_{26}\times C_{78}$	$\langle 1,-78,1\rangle$	$\left(\begin{smallmatrix}78 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 13,-88,32\rangle$	$\left(\begin{smallmatrix}83 & -32\\ 13 & -5\end{smallmatrix}\right)^3$	13
						$\langle 16,-96,49\rangle$	$\left(\begin{smallmatrix}87 & -49\\ 16 & -9\end{smallmatrix}\right)^3$	13
						$\langle 32,-88,13\rangle$	$\left(\begin{smallmatrix}83 & -13\\ 32 & -5\end{smallmatrix}\right)^3$	13
						$\langle 61,-38,-19\rangle$	$\left(\begin{smallmatrix}58 & 19\\ 61 & 20\end{smallmatrix}\right)^3$	13
						$\langle 7,-82,23\rangle$	$\left(\begin{smallmatrix}80 & -23\\ 7 & -2\end{smallmatrix}\right)^3$	10
						$\langle 16,48,-59\rangle$	$\left(\begin{smallmatrix}15 & 59\\ 16 & 63\end{smallmatrix}\right)^3$	7
						$\langle 23,-82,7\rangle$	$\left(\begin{smallmatrix}80 & -7\\ 23 & -2\end{smallmatrix}\right)^3$	10
80	77	1	1	C_1	$C_8^2\times C_{24}$	$\langle 1,-9,1\rangle$	$\left(\begin{smallmatrix}9 & -1\\ 1 & 0\end{smallmatrix}\right)^6$	7
		3	2	C_2	$C_2\times C_8^2\times C_{24}$	$\langle 9,-27,1\rangle$	$\left(\begin{smallmatrix}80 & -3\\ 27 & -1\end{smallmatrix}\right)^3$	7
						$\langle 19,3,-9\rangle$	$\left(\begin{smallmatrix}35 & 27\\ 57 & 44\end{smallmatrix}\right)^3$	16

		9	6	C_6	$C_2 \times C_8^2 \times C_{24}$	$\langle 1, -79, 1\rangle$	$\left(\begin{smallmatrix} 79 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 19, -85, 13\rangle$	$\left(\begin{smallmatrix} 82 & -13 \\ 19 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 9, 69, -41\rangle$	$\left(\begin{smallmatrix} 5 & 41 \\ 9 & 74 \end{smallmatrix}\right)^3$	16
						$\langle 73, -55, -11\rangle$	$\left(\begin{smallmatrix} 67 & 11 \\ 73 & 12 \end{smallmatrix}\right)^3$	22
						$\langle 9, -87, 37\rangle$	$\left(\begin{smallmatrix} 83 & -37 \\ 9 & -4 \end{smallmatrix}\right)^3$	16
						$\langle 63, -21, -23\rangle$	$\left(\begin{smallmatrix} 50 & 23 \\ 63 & 29 \end{smallmatrix}\right)^3$	13
81	6396	1	12	$C_2 \times C_6$	$C_{27} \times C_{54}$	$\langle 1, -80, 1\rangle$	$\left(\begin{smallmatrix} 80 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 33, -84, 5\rangle$	$\left(\begin{smallmatrix} 82 & -5 \\ 33 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 25, -86, 10\rangle$	$\left(\begin{smallmatrix} 83 & -10 \\ 25 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 41, -82, 2\rangle$	$\left(\begin{smallmatrix} 81 & -2 \\ 41 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 66, -18, -23\rangle$	$\left(\begin{smallmatrix} 49 & 23 \\ 66 & 31 \end{smallmatrix}\right)^3$	13
						$\langle 5, -84, 33\rangle$	$\left(\begin{smallmatrix} 82 & -33 \\ 5 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 55, -84, 3\rangle$	$\left(\begin{smallmatrix} 82 & -3 \\ 55 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 11, -84, 15\rangle$	$\left(\begin{smallmatrix} 82 & -15 \\ 11 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 53, -6, -30\rangle$	$\left(\begin{smallmatrix} 43 & 30 \\ 53 & 37 \end{smallmatrix}\right)^3$	16
						$\langle 71, -90, 6\rangle$	$\left(\begin{smallmatrix} 85 & -6 \\ 71 & -5 \end{smallmatrix}\right)^3$	19
						$\langle 53, 6, -30\rangle$	$\left(\begin{smallmatrix} 37 & 30 \\ 53 & 43 \end{smallmatrix}\right)^3$	16
						$\langle 15, -84, 11\rangle$	$\left(\begin{smallmatrix} 82 & -11 \\ 15 & -2 \end{smallmatrix}\right)^3$	10
82	6557	1	3	C_3	$C_2 \times C_{1680}$	$\langle 1, -81, 1\rangle$	$\left(\begin{smallmatrix} 81 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 11, -87, 23\rangle$	$\left(\begin{smallmatrix} 84 & -23 \\ 11 & -3 \end{smallmatrix}\right)^3$	10
						$\langle 23, -87, 11\rangle$	$\left(\begin{smallmatrix} 84 & -11 \\ 23 & -3 \end{smallmatrix}\right)^3$	10
83	105	1	2	C_2	C_{2296}	$\langle 4, -11, 1\rangle$	$\left(\begin{smallmatrix} 85 & -8 \\ 32 & -3 \end{smallmatrix}\right)^3$	10
						$\langle 2, -11, 2\rangle$	$\left(\begin{smallmatrix} 85 & -16 \\ 16 & -3 \end{smallmatrix}\right)^3$	13
		2	2	C_2	C_{2296}	$\langle 16, -22, 1\rangle$	$\left(\begin{smallmatrix} 85 & -4 \\ 64 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 3, -24, 13\rangle$	$\left(\begin{smallmatrix} 89 & -52 \\ 12 & -7 \end{smallmatrix}\right)^3$	13
		4	4	C_2^2	C_{2296}	$\langle 21, -42, 1\rangle$	$\left(\begin{smallmatrix} 83 & -2 \\ 42 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 39, -30, -5\rangle$	$\left(\begin{smallmatrix} 71 & 10 \\ 78 & 11 \end{smallmatrix}\right)^3$	25
						$\langle 3, -42, 7\rangle$	$\left(\begin{smallmatrix} 83 & -14 \\ 6 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 28, 0, -15\rangle$	$\left(\begin{smallmatrix} 41 & 30 \\ 56 & 41 \end{smallmatrix}\right)^3$	13
		8	8	C_2^3	C_{2296}	$\langle 1, -82, 1\rangle$	$\left(\begin{smallmatrix} 82 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4

						$\langle 21, 42, -59\rangle$	$\left(\begin{smallmatrix} 20 & 59 \\ 21 & 62 \end{smallmatrix}\right)^3$		7
						$\langle 69, -48, -16\rangle$	$\left(\begin{smallmatrix} 65 & 16 \\ 69 & 17 \end{smallmatrix}\right)^3$		16
						$\langle 39, -96, 16\rangle$	$\left(\begin{smallmatrix} 89 & -16 \\ 39 & -7 \end{smallmatrix}\right)^3$		16
						$\langle 28, -84, 3\rangle$	$\left(\begin{smallmatrix} 83 & -3 \\ 28 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 12, -84, 7\rangle$	$\left(\begin{smallmatrix} 83 & -7 \\ 12 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 23, 48, -48\rangle$	$\left(\begin{smallmatrix} 17 & 48 \\ 23 & 65 \end{smallmatrix}\right)^3$		10
						$\langle 48, 0, -35\rangle$	$\left(\begin{smallmatrix} 41 & 35 \\ 48 & 41 \end{smallmatrix}\right)^3$		10
84	85	1	2	C_2	$C_2^4 \times C_6^2$	$\langle 9, -11, 1\rangle$	$\left(\begin{smallmatrix} 10 & -1 \\ 9 & -1 \end{smallmatrix}\right)^6$	**Y**	28
						$\langle 3, -11, 3\rangle$	$\left(\begin{smallmatrix} 10 & -3 \\ 3 & -1 \end{smallmatrix}\right)^6$	**Y**	16
		3	2	C_2	$C_2^3 \times C_6^3$	$\langle 19, -29, 1\rangle$	$\left(\begin{smallmatrix} 85 & -3 \\ 57 & -2 \end{smallmatrix}\right)^3$		10
						$\langle 27, -3, -7\rangle$	$\left(\begin{smallmatrix} 46 & 21 \\ 81 & 37 \end{smallmatrix}\right)^3$		19
		9	6	C_6	$C_2^3 \times C_6^3$	$\langle 1, -83, 1\rangle$	$\left(\begin{smallmatrix} 83 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 37, -89, 7\rangle$	$\left(\begin{smallmatrix} 86 & -7 \\ 37 & -3 \end{smallmatrix}\right)^3$		13
						$\langle 9, -87, 19\rangle$	$\left(\begin{smallmatrix} 85 & -19 \\ 9 & -2 \end{smallmatrix}\right)^3$		10
						$\langle 17, 51, -63\rangle$	$\left(\begin{smallmatrix} 16 & 63 \\ 17 & 67 \end{smallmatrix}\right)^3$		7
						$\langle 19, -87, 9\rangle$	$\left(\begin{smallmatrix} 85 & -9 \\ 19 & -2 \end{smallmatrix}\right)^3$		10
						$\langle 7, -89, 37\rangle$	$\left(\begin{smallmatrix} 86 & -37 \\ 7 & -3 \end{smallmatrix}\right)^3$		13
85	7052	1	4	C_4	$C_8 \times C_{288}$	$\langle 1, -84, 1\rangle$	$\left(\begin{smallmatrix} 84 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 58, -98, 11\rangle$	$\left(\begin{smallmatrix} 91 & -11 \\ 58 & -7 \end{smallmatrix}\right)^3$		16
						$\langle 43, 0, -41\rangle$	$\left(\begin{smallmatrix} 42 & 41 \\ 43 & 42 \end{smallmatrix}\right)^3$		7
						$\langle 11, -98, 58\rangle$	$\left(\begin{smallmatrix} 91 & -58 \\ 11 & -7 \end{smallmatrix}\right)^3$		16
86	7221	1	10	C_{10}	$C_2 \times C_{42}^2$	$\langle 1, -85, 1\rangle$	$\left(\begin{smallmatrix} 85 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$		4
						$\langle 21, 51, -55\rangle$	$\left(\begin{smallmatrix} 17 & 55 \\ 21 & 68 \end{smallmatrix}\right)^3$		16
						$\langle 53, 15, -33\rangle$	$\left(\begin{smallmatrix} 35 & 33 \\ 53 & 50 \end{smallmatrix}\right)^3$		10
						$\langle 41, 13, -43\rangle$	$\left(\begin{smallmatrix} 36 & 43 \\ 41 & 49 \end{smallmatrix}\right)^3$		19
						$\langle 25, -89, 7\rangle$	$\left(\begin{smallmatrix} 87 & -7 \\ 25 & -2 \end{smallmatrix}\right)^3$		10
						$\langle 29, -87, 3\rangle$	$\left(\begin{smallmatrix} 86 & -3 \\ 29 & -1 \end{smallmatrix}\right)^3$		7
						$\langle 7, -89, 25\rangle$	$\left(\begin{smallmatrix} 87 & -25 \\ 7 & -2 \end{smallmatrix}\right)^3$		10
						$\langle 41, -95, 11\rangle$	$\left(\begin{smallmatrix} 90 & -11 \\ 41 & -5 \end{smallmatrix}\right)^3$		19
						$\langle 35, -89, 5\rangle$	$\left(\begin{smallmatrix} 87 & -5 \\ 35 & -2 \end{smallmatrix}\right)^3$		10

						$\langle 17, 59, -55\rangle$	$\left(\begin{smallmatrix} 13 & 55 \\ 17 & 72 \end{smallmatrix}\right)^3$	16
87	1848	1	4	C_2^2	$C_2 \times C_{840}$	$\langle 22, -44, 1\rangle$	$\left(\begin{smallmatrix} 87 & -2 \\ 44 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 11, -44, 2\rangle$	$\left(\begin{smallmatrix} 87 & -4 \\ 22 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 38, -48, 3\rangle$	$\left(\begin{smallmatrix} 91 & -6 \\ 76 & -5 \end{smallmatrix}\right)^3$	19
						$\langle 19, -48, 6\rangle$	$\left(\begin{smallmatrix} 91 & -12 \\ 38 & -5 \end{smallmatrix}\right)^3$	13
		2	8	C_2^3	$C_2 \times C_{840}$	$\langle 1, -86, 1\rangle$	$\left(\begin{smallmatrix} 86 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 67, -42, -21\rangle$	$\left(\begin{smallmatrix} 64 & 21 \\ 67 & 22 \end{smallmatrix}\right)^3$	13
						$\langle 11, 66, -69\rangle$	$\left(\begin{smallmatrix} 10 & 69 \\ 11 & 76 \end{smallmatrix}\right)^3$	7
						$\langle 57, -96, 8\rangle$	$\left(\begin{smallmatrix} 91 & -8 \\ 57 & -5 \end{smallmatrix}\right)^3$	13
						$\langle 79, -60, -12\rangle$	$\left(\begin{smallmatrix} 73 & 12 \\ 79 & 13 \end{smallmatrix}\right)^3$	22
						$\langle 59, -90, 3\rangle$	$\left(\begin{smallmatrix} 88 & -3 \\ 59 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 19, -94, 19\rangle$	$\left(\begin{smallmatrix} 90 & -19 \\ 19 & -4 \end{smallmatrix}\right)^3$	10
						$\langle 56, 0, -33\rangle$	$\left(\begin{smallmatrix} 43 & 33 \\ 56 & 43 \end{smallmatrix}\right)^3$	16
88	7565	1	4	C_2^2	$C_2 \times C_4^2 \times C_{120}$	$\langle 1, -87, 1\rangle$	$\left(\begin{smallmatrix} 87 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 43, -99, 13\rangle$	$\left(\begin{smallmatrix} 93 & -13 \\ 43 & -6 \end{smallmatrix}\right)^3$	22
						$\langle 73, -95, 5\rangle$	$\left(\begin{smallmatrix} 91 & -5 \\ 73 & -4 \end{smallmatrix}\right)^3$	16
						$\langle 61, 1, -31\rangle$	$\left(\begin{smallmatrix} 43 & 31 \\ 61 & 44 \end{smallmatrix}\right)^3$	16
89	860	1	2	C_2	C_{2640}	$\langle 10, -30, 1\rangle$	$\left(\begin{smallmatrix} 89 & -3 \\ 30 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 5, -30, 2\rangle$	$\left(\begin{smallmatrix} 89 & -6 \\ 15 & -1 \end{smallmatrix}\right)^3$	7
		3	8	$C_2 \times C_4$	C_{2640}	$\langle 1, -88, 1\rangle$	$\left(\begin{smallmatrix} 88 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 9, 78, -46\rangle$	$\left(\begin{smallmatrix} 5 & 46 \\ 9 & 83 \end{smallmatrix}\right)^3$	16
						$\langle 10, -90, 9\rangle$	$\left(\begin{smallmatrix} 89 & -9 \\ 10 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 41, 14, -46\rangle$	$\left(\begin{smallmatrix} 37 & 46 \\ 41 & 51 \end{smallmatrix}\right)^3$	16
						$\langle 18, 54, -67\rangle$	$\left(\begin{smallmatrix} 17 & 67 \\ 18 & 71 \end{smallmatrix}\right)^3$	7
						$\langle 37, -102, 18\rangle$	$\left(\begin{smallmatrix} 95 & -18 \\ 37 & -7 \end{smallmatrix}\right)^3$	16
						$\langle 45, 0, -43\rangle$	$\left(\begin{smallmatrix} 44 & 43 \\ 45 & 44 \end{smallmatrix}\right)^3$	7
						$\langle 18, -102, 37\rangle$	$\left(\begin{smallmatrix} 95 & -37 \\ 18 & -7 \end{smallmatrix}\right)^3$	16
90	7917	1	4	C_2^2	$C_3 \times C_6^2 \times C_{24}$	$\langle 1, -89, 1\rangle$	$\left(\begin{smallmatrix} 89 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 61, -93, 3\rangle$	$\left(\begin{smallmatrix} 91 & -3 \\ 61 & -2 \end{smallmatrix}\right)^3$	10

						$\langle 13, -91, 7\rangle$	$\left(\begin{smallmatrix} 90 & -7 \\ 13 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 37, -105, 21\rangle$	$\left(\begin{smallmatrix} 97 & -21 \\ 37 & -8 \end{smallmatrix}\right)^3$	13
91	2024	1	6	C_6	$C_2 \times C_6 \times C_{12}^2$	$\langle 23, -46, 1\rangle$	$\left(\begin{smallmatrix} 91 & -2 \\ 46 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 5, -48, 14\rangle$	$\left(\begin{smallmatrix} 93 & -28 \\ 10 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 7, -48, 10\rangle$	$\left(\begin{smallmatrix} 93 & -20 \\ 14 & -3 \end{smallmatrix}\right)^3$	10
						$\langle 35, -48, 2\rangle$	$\left(\begin{smallmatrix} 93 & -4 \\ 70 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 10, -48, 7\rangle$	$\left(\begin{smallmatrix} 93 & -14 \\ 20 & -3 \end{smallmatrix}\right)^3$	10
						$\langle 14, -48, 5\rangle$	$\left(\begin{smallmatrix} 93 & -10 \\ 28 & -3 \end{smallmatrix}\right)^3$	13
		2	12	$C_2 \times C_6$	$C_2 \times C_6 \times C_{12}^2$	$\langle 1, -90, 1\rangle$	$\left(\begin{smallmatrix} 90 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 5, -94, 37\rangle$	$\left(\begin{smallmatrix} 92 & -37 \\ 5 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 40, -96, 7\rangle$	$\left(\begin{smallmatrix} 93 & -7 \\ 40 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 8, -96, 35\rangle$	$\left(\begin{smallmatrix} 93 & -35 \\ 8 & -3 \end{smallmatrix}\right)^3$	10
						$\langle 40, 16, -49\rangle$	$\left(\begin{smallmatrix} 37 & 49 \\ 40 & 53 \end{smallmatrix}\right)^3$	13
						$\langle 56, -16, -35\rangle$	$\left(\begin{smallmatrix} 53 & 35 \\ 56 & 37 \end{smallmatrix}\right)^3$	10
						$\langle 85, -104, 8\rangle$	$\left(\begin{smallmatrix} 97 & -8 \\ 85 & -7 \end{smallmatrix}\right)^3$	25
						$\langle 17, -100, 28\rangle$	$\left(\begin{smallmatrix} 95 & -28 \\ 17 & -5 \end{smallmatrix}\right)^3$	13
						$\langle 29, -98, 13\rangle$	$\left(\begin{smallmatrix} 94 & -13 \\ 29 & -4 \end{smallmatrix}\right)^3$	16
						$\langle 4, -92, 23\rangle$	$\left(\begin{smallmatrix} 91 & -23 \\ 4 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 29, 40, -56\rangle$	$\left(\begin{smallmatrix} 25 & 56 \\ 29 & 65 \end{smallmatrix}\right)^3$	16
						$\langle 28, -100, 17\rangle$	$\left(\begin{smallmatrix} 95 & -17 \\ 28 & -5 \end{smallmatrix}\right)^3$	13
92	8277	1	6	C_6	$C_2^3 \times C_{528}$	$\langle 1, -91, 1\rangle$	$\left(\begin{smallmatrix} 91 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 13, -101, 37\rangle$	$\left(\begin{smallmatrix} 96 & -37 \\ 13 & -5 \end{smallmatrix}\right)^3$	13
						$\langle 53, 3, -39\rangle$	$\left(\begin{smallmatrix} 44 & 39 \\ 53 & 47 \end{smallmatrix}\right)^3$	10
						$\langle 31, 31, -59\rangle$	$\left(\begin{smallmatrix} 30 & 59 \\ 31 & 61 \end{smallmatrix}\right)^3$	7
						$\langle 53, -3, -39\rangle$	$\left(\begin{smallmatrix} 47 & 39 \\ 53 & 44 \end{smallmatrix}\right)^3$	10
						$\langle 61, -15, -33\rangle$	$\left(\begin{smallmatrix} 53 & 33 \\ 61 & 38 \end{smallmatrix}\right)^3$	13
93	940	1	6	C_6	$C_2^2 \times C_{10} \times C_{30}$	$\langle 21, -32, 1\rangle$	$\left(\begin{smallmatrix} 94 & -3 \\ 63 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 7, -32, 3\rangle$	$\left(\begin{smallmatrix} 94 & -9 \\ 21 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 9, -34, 6\rangle$	$\left(\begin{smallmatrix} 97 & -18 \\ 27 & -5 \end{smallmatrix}\right)^3$	13
						$\langle 27, -20, -5\rangle$	$\left(\begin{smallmatrix} 76 & 15 \\ 81 & 16 \end{smallmatrix}\right)^3$	19

						$\langle 21, 4, -11\rangle$	$\left(\begin{smallmatrix} 40 & 33 \\ 63 & 52 \end{smallmatrix}\right)^3$	13
						$\langle 3, -32, 7\rangle$	$\left(\begin{smallmatrix} 94 & -21 \\ 9 & -2 \end{smallmatrix}\right)^3$	10
		3	12	$C_2 \times C_6$	$C_2 \times C_{30}^2$	$\langle 1, -92, 1\rangle$	$\left(\begin{smallmatrix} 92 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 55, -10, -38\rangle$	$\left(\begin{smallmatrix} 51 & 38 \\ 55 & 41 \end{smallmatrix}\right)^3$	10
						$\langle 26, -98, 11\rangle$	$\left(\begin{smallmatrix} 95 & -11 \\ 26 & -3 \end{smallmatrix}\right)^3$	10
						$\langle 77, -100, 5\rangle$	$\left(\begin{smallmatrix} 96 & -5 \\ 77 & -4 \end{smallmatrix}\right)^3$	16
						$\langle 11, -98, 26\rangle$	$\left(\begin{smallmatrix} 95 & -26 \\ 11 & -3 \end{smallmatrix}\right)^3$	10
						$\langle 55, 10, -38\rangle$	$\left(\begin{smallmatrix} 41 & 38 \\ 55 & 51 \end{smallmatrix}\right)^3$	10
						$\langle 47, -94, 2\rangle$	$\left(\begin{smallmatrix} 93 & -2 \\ 47 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 65, 20, -31\rangle$	$\left(\begin{smallmatrix} 36 & 31 \\ 65 & 56 \end{smallmatrix}\right)^3$	19
						$\langle 73, -24, -27\rangle$	$\left(\begin{smallmatrix} 58 & 27 \\ 73 & 34 \end{smallmatrix}\right)^3$	13
						$\langle 89, -108, 9\rangle$	$\left(\begin{smallmatrix} 100 & -9 \\ 89 & -8 \end{smallmatrix}\right)^3$	28
						$\langle 22, -98, 13\rangle$	$\left(\begin{smallmatrix} 95 & -13 \\ 22 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 14, -110, 65\rangle$	$\left(\begin{smallmatrix} 101 & -65 \\ 14 & -9 \end{smallmatrix}\right)^3$	19
94	8645	1	4	C_2^2	$C_2 \times C_{2208}$	$\langle 1, -93, 1\rangle$	$\left(\begin{smallmatrix} 93 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 85, -105, 7\rangle$	$\left(\begin{smallmatrix} 99 & -7 \\ 85 & -6 \end{smallmatrix}\right)^3$	22
						$\langle 19, -95, 5\rangle$	$\left(\begin{smallmatrix} 94 & -5 \\ 19 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 17, -99, 17\rangle$	$\left(\begin{smallmatrix} 96 & -17 \\ 17 & -3 \end{smallmatrix}\right)^3$	10
95	552	1	2	C_2	$C_2 \times C_{18} \times C_{72}$	$\langle 6, -24, 1\rangle$	$\left(\begin{smallmatrix} 95 & -4 \\ 24 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 3, -24, 2\rangle$	$\left(\begin{smallmatrix} 95 & -8 \\ 12 & -1 \end{smallmatrix}\right)^3$	7
		2	4	C_2^2	$C_2 \times C_{18} \times C_{72}$	$\langle 24, -48, 1\rangle$	$\left(\begin{smallmatrix} 95 & -2 \\ 48 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 31, 10, -17\rangle$	$\left(\begin{smallmatrix} 37 & 34 \\ 62 & 57 \end{smallmatrix}\right)^3$	13
						$\langle 29, 2, -19\rangle$	$\left(\begin{smallmatrix} 45 & 38 \\ 58 & 49 \end{smallmatrix}\right)^3$	13
						$\langle 3, -48, 8\rangle$	$\left(\begin{smallmatrix} 95 & -16 \\ 6 & -1 \end{smallmatrix}\right)^3$	7
		4	8	$C_2 \times C_4$	$C_2 \times C_{18} \times C_{72}$	$\langle 1, -94, 1\rangle$	$\left(\begin{smallmatrix} 94 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 16, 72, -57\rangle$	$\left(\begin{smallmatrix} 11 & 57 \\ 16 & 83 \end{smallmatrix}\right)^3$	19
						$\langle 73, -100, 4\rangle$	$\left(\begin{smallmatrix} 97 & -4 \\ 73 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 31, 42, -57\rangle$	$\left(\begin{smallmatrix} 26 & 57 \\ 31 & 68 \end{smallmatrix}\right)^3$	19
						$\langle 3, -96, 32\rangle$	$\left(\begin{smallmatrix} 95 & -32 \\ 3 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 76, -4, -29\rangle$	$\left(\begin{smallmatrix} 49 & 29 \\ 76 & 45 \end{smallmatrix}\right)^3$	16

						$\langle 12, -108, 59\rangle$	$\left(\begin{smallmatrix} 101 & -59 \\ 12 & -7 \end{smallmatrix}\right)^3$	13
						$\langle 76, 4, -29\rangle$	$\left(\begin{smallmatrix} 45 & 29 \\ 76 & 49 \end{smallmatrix}\right)^3$	16
96	9021	1	8	C_8	$C_2^2 \times C_{16} \times C_{48}$	$\langle 1, -95, 1\rangle$	$\left(\begin{smallmatrix} 95 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 39, -99, 5\rangle$	$\left(\begin{smallmatrix} 97 & -5 \\ 39 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 65, -109, 11\rangle$	$\left(\begin{smallmatrix} 102 & -11 \\ 65 & -7 \end{smallmatrix}\right)^3$	16
						$\langle 15, -99, 13\rangle$	$\left(\begin{smallmatrix} 97 & -13 \\ 15 & -2 \end{smallmatrix}\right)^3$	10
						$\langle 65, -31, -31\rangle$	$\left(\begin{smallmatrix} 63 & 31 \\ 65 & 32 \end{smallmatrix}\right)^3$	10
						$\langle 55, 1, -41\rangle$	$\left(\begin{smallmatrix} 47 & 41 \\ 55 & 48 \end{smallmatrix}\right)^3$	10
						$\langle 11, -109, 65\rangle$	$\left(\begin{smallmatrix} 102 & -65 \\ 11 & -7 \end{smallmatrix}\right)^3$	16
						$\langle 5, -99, 39\rangle$	$\left(\begin{smallmatrix} 97 & -39 \\ 5 & -2 \end{smallmatrix}\right)^3$	10
97	188	1	1	C_1	$C_{32} \times C_{96}$	$\langle 2, -14, 1\rangle$	$\left(\begin{smallmatrix} 97 & -7 \\ 14 & -1 \end{smallmatrix}\right)^3$	7
		7	8	C_8	$C_{32} \times C_{96}$	$\langle 1, -96, 1\rangle$	$\left(\begin{smallmatrix} 96 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 11, -106, 46\rangle$	$\left(\begin{smallmatrix} 101 & -46 \\ 11 & -5 \end{smallmatrix}\right)^3$	19
						$\langle 38, -110, 19\rangle$	$\left(\begin{smallmatrix} 103 & -19 \\ 38 & -7 \end{smallmatrix}\right)^3$	13
						$\langle 23, -106, 22\rangle$	$\left(\begin{smallmatrix} 101 & -22 \\ 23 & -5 \end{smallmatrix}\right)^3$	13
						$\langle 49, -98, 2\rangle$	$\left(\begin{smallmatrix} 97 & -2 \\ 49 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 22, -106, 23\rangle$	$\left(\begin{smallmatrix} 101 & -23 \\ 22 & -5 \end{smallmatrix}\right)^3$	13
						$\langle 62, 6, -37\rangle$	$\left(\begin{smallmatrix} 45 & 37 \\ 62 & 51 \end{smallmatrix}\right)^3$	13
						$\langle 11, 84, -49\rangle$	$\left(\begin{smallmatrix} 6 & 49 \\ 11 & 90 \end{smallmatrix}\right)^3$	19
98	1045	1	4	C_4	$C_2 \times C_{42}^2$	$\langle 11, -33, 1\rangle$	$\left(\begin{smallmatrix} 98 & -3 \\ 33 & -1 \end{smallmatrix}\right)^3$	7
						$\langle 3, -35, 15\rangle$	$\left(\begin{smallmatrix} 101 & -45 \\ 9 & -4 \end{smallmatrix}\right)^3$	16
						$\langle 5, -35, 9\rangle$	$\left(\begin{smallmatrix} 101 & -27 \\ 15 & -4 \end{smallmatrix}\right)^3$	10
						$\langle 3, 29, -17\rangle$	$\left(\begin{smallmatrix} 5 & 51 \\ 9 & 92 \end{smallmatrix}\right)^3$	16
		3	8	$C_2 \times C_4$	$C_2 \times C_{42}^2$	$\langle 1, -97, 1\rangle$	$\left(\begin{smallmatrix} 97 & -1 \\ 1 & 0 \end{smallmatrix}\right)^3$	4
						$\langle 43, -103, 7\rangle$	$\left(\begin{smallmatrix} 100 & -7 \\ 43 & -3 \end{smallmatrix}\right)^3$	13
						$\langle 29, -113, 29\rangle$	$\left(\begin{smallmatrix} 105 & -29 \\ 29 & -8 \end{smallmatrix}\right)^3$	13
						$\langle 43, 17, -53\rangle$	$\left(\begin{smallmatrix} 40 & 53 \\ 43 & 57 \end{smallmatrix}\right)^3$	13
						$\langle 81, -57, -19\rangle$	$\left(\begin{smallmatrix} 77 & 19 \\ 81 & 20 \end{smallmatrix}\right)^3$	16
						$\langle 63, 9, -37\rangle$	$\left(\begin{smallmatrix} 44 & 37 \\ 63 & 53 \end{smallmatrix}\right)^3$	16
						$\langle 11, 77, -79\rangle$	$\left(\begin{smallmatrix} 10 & 79 \\ 11 & 87 \end{smallmatrix}\right)^3$	7

						$\langle 63,-9,-37\rangle$	$\left(\begin{smallmatrix}53 & 37\\ 63 & 44\end{smallmatrix}\right)^3$	16
99	24	1	1	C_1	$C_3^2\times C_{120}$	$\langle 3,-6,1\rangle$	$\left(\begin{smallmatrix}11 & -2\\ 6 & -1\end{smallmatrix}\right)^6$	13
		2	2	C_2	$C_3^2\times C_{120}$	$\langle 1,-10,1\rangle$	$\left(\begin{smallmatrix}10 & -1\\ 1 & 0\end{smallmatrix}\right)^6$	7
						$\langle 3,-12,4\rangle$	$\left(\begin{smallmatrix}11 & -4\\ 3 & -1\end{smallmatrix}\right)^6$	13
		4	2	C_2	$C_3\times C_6\times C_{120}$	$\langle 4,-20,1\rangle$	$\left(\begin{smallmatrix}99 & -5\\ 20 & -1\end{smallmatrix}\right)^3$	7
						$\langle 3,-24,16\rangle$	$\left(\begin{smallmatrix}109 & -80\\ 15 & -11\end{smallmatrix}\right)^3$	19
		5	2	C_2	$C_3\times C_6\times C_{120}$	$\langle 19,-26,1\rangle$	$\left(\begin{smallmatrix}101 & -4\\ 76 & -3\end{smallmatrix}\right)^3$	13
						$\langle 23,-28,2\rangle$	$\left(\begin{smallmatrix}105 & -8\\ 92 & -7\end{smallmatrix}\right)^3$	25
		10	4	C_2^2	$C_3\times C_6\times C_{120}$	$\langle 25,-50,1\rangle$	$\left(\begin{smallmatrix}99 & -2\\ 50 & -1\end{smallmatrix}\right)^3$	7
						$\langle 8,-56,23\rangle$	$\left(\begin{smallmatrix}105 & -46\\ 16 & -7\end{smallmatrix}\right)^3$	16
						$\langle 19,14,-29\rangle$	$\left(\begin{smallmatrix}35 & 58\\ 38 & 63\end{smallmatrix}\right)^3$	10
						$\langle 43,-54,3\rangle$	$\left(\begin{smallmatrix}103 & -6\\ 86 & -5\end{smallmatrix}\right)^3$	19
		20	8	$C_2\times C_4$	$C_3\times C_6\times C_{120}$	$\langle 1,-98,1\rangle$	$\left(\begin{smallmatrix}98 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 47,24,-48\rangle$	$\left(\begin{smallmatrix}37 & 48\\ 47 & 61\end{smallmatrix}\right)^3$	16
						$\langle 4,-100,25\rangle$	$\left(\begin{smallmatrix}99 & -25\\ 4 & -1\end{smallmatrix}\right)^3$	7
						$\langle 32,48,-57\rangle$	$\left(\begin{smallmatrix}25 & 57\\ 32 & 73\end{smallmatrix}\right)^3$	16
						$\langle 67,-102,3\rangle$	$\left(\begin{smallmatrix}100 & -3\\ 67 & -2\end{smallmatrix}\right)^3$	10
						$\langle 19,-104,16\rangle$	$\left(\begin{smallmatrix}101 & -16\\ 19 & -3\end{smallmatrix}\right)^3$	13
						$\langle 75,0,-32\rangle$	$\left(\begin{smallmatrix}49 & 32\\ 75 & 49\end{smallmatrix}\right)^3$	13
						$\langle 16,-104,19\rangle$	$\left(\begin{smallmatrix}101 & -19\\ 16 & -3\end{smallmatrix}\right)^3$	13
100	9797	1	4	C_4	$C_2^2\times C_{10}\times C_{120}$	$\langle 1,-99,1\rangle$	$\left(\begin{smallmatrix}99 & -1\\ 1 & 0\end{smallmatrix}\right)^3$	4
						$\langle 29,-103,7\rangle$	$\left(\begin{smallmatrix}101 & -7\\ 29 & -2\end{smallmatrix}\right)^3$	10
						$\langle 43,-123,31\rangle$	$\left(\begin{smallmatrix}111 & -31\\ 43 & -12\end{smallmatrix}\right)^3$	16
						$\langle 7,-103,29\rangle$	$\left(\begin{smallmatrix}101 & -29\\ 7 & -2\end{smallmatrix}\right)^3$	10

REFERENCES

[1] R. L. Adler and L. Flatto. The backward continued fraction map and geodesic flow. *Ergodic Theory and Dynamical Systems*, 4:487–492, 1984.

[2] R. C. Alperin. $\mathrm{PSL}_2(\mathrm{Z}) = \mathrm{Z}_2 * \mathrm{Z}_3$. *The American Mathematical Monthly*, 100:385–386, 1993.

[3] O. Andersson and I. Dumitru. Aligned SICs and embedded tight frames in even dimensions. *Journal of Physics A: Mathematical and Theoretical*, 52:425302, 2019.

[4] D. M. Appleby. Symmetric informationally complete positive-operator valued measures and the extended Clifford group. *J. Math. Phys.*, 46:052107, 2005.

[5] D. M. Appleby. Symmetric informationally complete measurements of arbitrary rank. *Opt. Spect.*, 103:416–428, 2007.

[6] D. M. Appleby. Properties of the extended Clifford group with applications to SIC-POVMs and MUBs. 2009. Available at arXiv:0909.5233.

[7] D. M. Appleby, H. Yadsan-Appleby, and G. Zauner. Galois automorphisms of a symmetric measurement. *Quant. Inf. Comput.*, 13:672–720, 2013.

[8] M. Appleby, I. Bengtsson, I. Dumitru, and S. Flammia. Dimension towers of SICs. I. Aligned SICs and embedded tight frames. *J. Math. Phys.*, 58(11):112201, 2017.

[9] M. Appleby, I. Bengtsson, S. Flammia, and D. Goyeneche. Tight frames, Hadamard matrices, and Zauner's conjecture. *J. Phys. A*, 52:295301, 2019.

[10] M. Appleby, I. Bengtsson, M. Grassl, M. Harrison, and G. McConnell. SIC-POVMs from Stark units: Prime dimensions $n^2 + 3$. *J. Math. Phys.*, 63:112205, 2022.

[11] M. Appleby, T.-Y. Chien, S. T. Flammia, and S. Waldron. Constructing exact symmetric informationally complete measurements from numerical solutions. *J. Phys. A*, 51:165302, 2018.

[12] M. Appleby, S. Flammia, G. McConnell, and J. Yard. SICs and algebraic number theory. *Found. Phys.*, 47:1042–1059, 2017.

[13] M. Appleby, S. Flammia, G. McConnell, and J. Yard. Generating ray class fields of real quadratic fields via complex equiangular lines. *Acta Arithmetica*, 192(3):211–233, 2020.

[14] M. Appleby, S. T. Flammia, and G. S. Kopp. Representations of Galois groups of SICs, 2025. Forthcoming.

[15] I. Bengtsson, M. Grassl, and G. McConnell. SIC-POVMs from Stark units: Dimensions $n^2 + 3 = 4p$, p prime, 2024, 2403.02872.

[16] I. Bengtsson and B. Srivastava. Dimension towers of SICs: II. some constructions. *Journal of Physics A: Mathematical and Theoretical*, 55:215302, 2022.

[17] Å. Björck and V. Pereyra. Solution of Vandermonde systems of equations. *Mathematics of Computation*, 24(112):893, Oct. 1970.

[18] C. Bjorklund and M. Litman. Error approximation for backwards and simple continued fractions. *Research in Number Theory*, 10:1–26, 2024.

[19] L. Bos and S. Waldron. SICs and the elements of canonical order 3 in the Clifford group. *J. Phys. A*, 52:105301, 2019.

[20] J. Buchmann and U. Vollmer. *Binary Quadratic Forms: An Algorithmic Approach*. Algorithms and Computation in Mathematics, no. 20. Springer, 2007.

[21] D. A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. Springer-Verlag, 1989.

[22] P. G. Casazza, M. Fickus, D. G. Mixon, Y. Wang, and Z. Zhou. Constructing tight fusion frames. *Applied and Computational Harmonic Analysis*, 30:175–187, 2011.

[23] B. Chen, T. Li, and S.-M. Fei. General SIC measurement-based entanglement detection. *Quantum Information Processing*, 14:2281–2290, 2015.

[24] C. Closset and H. Kim. Three-dimensional $\mathcal{N} = 2$ supersymmetric gauge theories and partition functions on Seifert manifolds: A review. *Int. J. Mod. Phys. A*, 34:1930011, 2019.

[25] G. Cuffaro and C. A. Fuchs. Quantum states with maximal magic. 2024. Available at arXiv:2412.21083.

[26] H. Dai, S. Fu, and S. Luo. Detecting magic states via characteristic functions. *International Journal of Theoretical Physics*, 61:35, 2022.

[27] J. H. Davenport. *The Higher Arithmetic: An Introduction to the Theory of Numbers*. Cambridge University Press, eighth edition, 2008.

[28] J. B. DeBrota, C. A. Fuchs, and B. C. Stacey. Symmetric informationally complete measurements identify the essential difference between classical and quantum. *Phys. Rev. Res.*, 2, 2020.

[29] P. Delsarte, J. M. Goethals, and J. J. Seidel. Bounds for systems of lines, and Jacobi polynomials. *Philips Research Reports*, 30:91, 1975.
[30] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Springer, 2005.
[31] T. Dimofte. Complex Chern–Simons theory at level k via the 3d–3d correspondence. *Commun. Math. Phys.*, 339:619–662, 2015.
[32] T. D. Dimofte. *Refined BPS Invariants, Chern-Simons Theory, and the Quantum Dilogarithm*. PhD thesis, California Institute of Technology, 2010.
[33] L. D. Faddeev. Discrete Heisenberg-Weyl group and modular group. *Lett. Math. Phys.*, 34:249–254, 1995.
[34] L. D. Faddeev and R. M. Kashaev. Quantum dilogarithm. *Mod. Phys. Lett. A*, 9:427–434, 1994.
[35] L. D. Faddeev, R. M. Kashaev, and A. Y. Volkov. Strongly coupled quantum discrete Liouville theory. I: Algebraic approach and duality. *Commun. Math. Phys.*, 219:199–219, 2001.
[36] A. Fannjiang and T. Strohmer. The numerics of phase retrieval. *Acta Numerica*, 29:125–228, 2020.
[37] L. Feng and S. Luo. From stabilizer states to SIC-POVM fiducial states. *Theor. and Math. Phys.*, 213:1747–1761, 2022.
[38] M. Fickus, J. Jasper, D. G. Mixon, and C. E. Watson. A brief introduction to equi-chordal and equi-isoclinic tight fusion frames. In *Wavelets and Sparsity XVII*, volume 10394, pages 186–194. SPIE, 2017.
[39] Y. Y. Finkel'shtein. Klein polygons and reduced regular continued fractions. *Russ. Math. Surv.*, 48:198–200, 1993.
[40] S. T. Flammia. `Zauner.jl`. available at github.com/sflammia/Zauner.jl, 2024.
[41] E. Fouvry and J. Klüners. On the negative Pell equation. *Ann. Math.*, 172(3):2035–2104, 2010.
[42] C. A. Fuchs, M. C. Hoang, and B. C. Stacey. The SIC question: History and state of play. *Axioms*, 6:21, 2017.
[43] C. A. Fuchs and R. Schack. Quantum-Bayesian coherence. *Rev. Mod. Phys.*, 85:1693–1715, 2013.
[44] S. Garoufalidis and R. Kashaev. Resurgence of Faddeev's quantum dilogarithm. In A. Papadopoulos, editor, *Topology and Geometry*, pages 257–272. European Mathematical Society, 2021.
[45] S. Garoufalidis and R. Kashaev. Quantum dilogarithms over local fields and invariants of 3-manifolds. 2023. Available at arXiv:2306.01331.
[46] G. Gour and A. Kalev. Construction of all general symmetric informationally complete measurements. *J. Phys. A*, 47:335302, 2014.
[47] M. Grassl. Computing SIC-POVMs using permutation symmetries and Stark units, 26 October 2021. Available at codex seminar.
[48] M. Grassl. Computing numerical and exact SIC-POVMs, 29 March 2021. Available at Jagiellonian University seminar.
[49] M. A. Graydon and D. M. Appleby. Entanglement and designs. *J. Phys. A*, 49:33LT02, 2016.
[50] M. A. Graydon and D. M. Appleby. Quantum conical designs. *J. Phys. A*, 49:085301, 2016.
[51] D. Gross. Recovering low-rank matrices from few coefficients in any basis. *IEEE Trans. Inf. Theory*, 57(3):1548–1566, 2011.
[52] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.*, 105:150401, 2010.
[53] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, sixth edition, 2009. Revised by D. R. Heath-Brown and J. H. Silverman.
[54] M. A. Herman and T. Strohmer. High-resolution radar via compressed sensing. *Signal Processing, IEEE Transactions on*, 57:2275–2284, 2009.
[55] N. J. Higham. Error analysis of the Björck-Pereyra algorithms for solving Vandermonde systems. *Numer. Math.*, 50:613–632, 1987.
[56] D. Hilbert. Mathematische probleme. *Götttinger Nachrichten*, pages 253–297, 1900. Reprinted in *Archiv der Mathematik und Physik* **3**, 44–63; 213–237 (1901). English translation in *Bulletin of the American Mathematical Society* **8**, 437–479 (1902).
[57] F. Hirzebruch. Über vierdimensionale Riemannsche Flächen mehrdeutiger analytischer Funktionen von zwei komplexen Veränderlichen. *Math. Ann.*, 126:1–22, 1953.
[58] F. Hirzebruch. Hilbert modular surfaces. *Enseign. Math.*, 19:183–282, 1973.
[59] F. Hirzebruch, W. Neumann, and S. Koh. *Differentiable Manifolds and Quadratic Forms*. Marcel Dekker, Inc. New York, 1971.
[60] S. G. Hoggar. 64 lines from a quaternionic polytope. *Geom. Dedicata*, 69(3):287–289, 1998.

[61] P. Horodecki, Ł. Rudnicki, and K. Życzkowski. Five open problems in quantum information. *PRX Quantum*, page 010101, 2022.
[62] J. W. Jones and D. P. Roberts. A database of local fields. *J. Symbolic Comput.*, 41(1):80–97, 2006.
[63] H. W. E. Jung. Darstellung der Funktionen eines algebraischen Körpers zweier unabhängigen Veränderlichen x, y in der Umgebung einer Stelle $x = a$, $y = b$. *J. Reine Angew. Math.*, 1908:289–314, 1908.
[64] R. M. Kashaev. The hyperbolic volume of knots from the quantum dilogarithm. *Lett. Math. Phys.*, 39:269–275, 1997.
[65] S. Katok. Coding of closed geodesics after gauss and morse. *Geom. Dedicata*, 63:123–145, 1996.
[66] S. Katok. Continued fractions, hyperbolic geometry and quadratic forms. In S. Katok, A. Sossinsky, and S. Tabachnikov, editors, *MASS Selecta: Teaching and Learning Advanced Undergraduate Mathematics*, pages 121–160. American Mathematical Society, 2003.
[67] E. J. King. Constructing subspace packings from other packings. *Linear Algebra Appl.*, 625:68–80, 2021.
[68] H. Koch. *Number Theory. Algebraic Numbers and Functions*. Graduate Studies in Mathematics, vol. 24. American Mathematical Society, 2000.
[69] G. S. Kopp. SIC-POVMs and the Stark conjectures. *Int. Math. Res. Not. IMRN*, (18):13812–13838, 2021.
[70] G. S. Kopp. The Shintani–Faddeev modular cocycle: Stark units from q-Pochhammer ratios. 2024. Available at arXiv:2411.06763.
[71] G. S. Kopp and J. C. Lagarias. Ray class groups and ray class fields for orders of number fields. 2022. Available at arXiv:2212.09177.
[72] G. S. Kopp and J. C. Lagarias. SICs and orders of real quadratic fields. 2024. Available at arXiv:2407.08048.
[73] G. S. Kopp and J. C. Lagarias. Ray class monoids for orders of number fields. 2025. Forthcoming.
[74] D. S. Kubert and S. Lang. *Modular units*, volume 244 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, New York-Berlin, 1981.
[75] N. Kurokawa and S. Koyama. Multiple sine functions. *Forum Math.*, 15:839–876, 2003.
[76] F. I. B. López, V. N. Efremov, and A. M. H. Magdaleno. Algorithm for fast calculation of Hirzebruch-Jung continued fraction expansions to coding of graph manifolds. *Applied Mathematics*, 6:1676, 2015.
[77] L. Luzzi and S. Marmi. On the entropy of Japanese continued fractions. *Discrete and Continuous Dynamical Systems*, 20:673–711, 2007.
[78] D. A. Marcus. *Number fields*. Universitext. Springer-Verlag, New York-Heidelberg, 1977.
[79] H. Murakami and Y. Yokota. *Volume Conjecture for Knots*. Springer Briefs in Mathematical Physics Vol. 30. Springer, 2018.
[80] G. Myerson. On semi-regular finite continued fractions. *Arch. Math.*, 48:420–425, 1987.
[81] J. Neukirch. *Algebraic Number Theory*. Springer Berlin Heidelberg, 1999.
[82] B. Ponsot. Recent progress in Liouville field theory. *Int. J. Mod. Phys. A*, 19(supp02):311–335, 2004.
[83] P. Popescu-Pampu. The geometry of continued fractions and the topology of surface singularities. In J.-P. Brasselet and T. Suwa, editors, *Singularities in geometry and topology: : Proceedings of the third Franco-Japanese Symposium on Singularities, September 2004*, Advanced Studies in Pure Mathematics, Volume 46, pages 119–195. Mathematical Society of Japan, 2007. Available at arXiv:math/0506432.
[84] H. Rademacher. Zur Theorie der Dedekindschen Summen. *Math. Z.*, 63:445–463, 1955.
[85] H. Rademacher. *Topics in Analytical Number Theory*. Die Grundlehren der mathematischen Wissenschaften. Springer, 1973.
[86] H. Rademacher and E. Grosswald. *Dedekind sums*. The Carus Mathematical Monographs, No. 16. American Mathematical Society, 1972.
[87] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys.*, 45(6):2171–2180, June 2004.
[88] A. J. Scott. Tight informationally complete quantum measurements. *J. Phys. A*, 39:13507–13530, 2006.
[89] A. J. Scott. SICs: Extending the list of solutions. 2017, 1703.03993.
[90] A. J. Scott and M. Grassl. Symmetric informationally complete positive-operator-valued measures: A new computer study. *J. Math. Phys.*, 51(4):042203, 2010, 0910.5784.
[91] J. Shang, A. Asadian, H. Zhu, and O. Gühne. Enhanced entanglement criterion via symmetric informationally complete measurements. *Physical Review A*, 98:022309, 2018.
[92] T. Shintani. On evaluation of zeta functions of totally real algebraic number fields at non-positive integers. *J. Fac. Sci., Univ. Tokyo, Sect. IA*, 23:393–417, 1976.
[93] T. Shintani. On a Kronecker limit formula for real quadratic fields. *J. Fac. Sci. Univ. Tokyo*, 24:167–199, 1977.

[94] T. Shintani. On certain ray class invariants of real quadratic fields. *J. Math. Soc. Japan*, 30:139–167, 1977.
[95] T. Shintani. A proof of the classical kronecker limit formula. *Tokyo J. Math.*, 3:191–199, 1980.
[96] B. C. Stacey. *A First Course in the Sporadic SICs*. Springer Briefs in Mathematical Physics, Vol. 41. Springer, 2021.
[97] H. M. Stark. Values of L-functions at $s = 1$. I. L-functions for quadratic forms. *Adv. Math.*, 7(3):301–343, 1971.
[98] H. M. Stark. L-functions at $s = 1$. II. Artin L-functions with rational characters. *Adv. Math.*, 17(1):60–92, 1975.
[99] H. M. Stark. L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem. *Adv. Math.*, 22(1):64–84, 1976.
[100] H. M. Stark. Class fields for real quadratic fields and L-series at 1. In A. Fröhlich, editor, *Algebraic Number Fields (L-Functions and Galois Properties): Proceedings of a Symposium.*, pages 355–374. New York: Academic Press, 1977.
[101] H. M. Stark. L-functions at $s = 1$. IV. First derivatives at $s = 0$. *Adv. Math.*, 35(3):197–235, 1980.
[102] A. Szymusiak and W. Słomczyński. Informational power of the Hoggar SIC-POVM. *Phys. Rev. A*, 94:012122, 2016.
[103] B. A. Tangedal. Continued fractions, special values of the double sine function, and Stark units over real quadratic fields. *J. Number Theory*, 124(2):291–313, 2007.
[104] T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. *Duke Math. J.*, 162(13):2451–2508, 2013.
[105] J. Tate. On Stark's conjectures on the behavior of $L(s, \chi)$ at $s = 0$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):963–978, 1981.
[106] A. Tavakoli, I. Bengtsson, N. Gisin, and J. M. Renes. Compounds of symmetric informationally complete measurements and their application in quantum key distribution. *Phys. Rev. Res.*, 2:043122, 2020.
[107] F. Thorne, 2021. Personal correspondence.
[108] TOP500 Project. Online listing of the world's most powerful supercomputers, as ranked by the Linpack benchmark.
[109] S. F. D. Waldron. *An Introduction to Finite Tight Frames*. Birkhäuser, 2018.
[110] J. Wang, 2024. Personal correspondence.
[111] S. Woronowicz. Quantum exponential function. *Reviews in Mathematical Physics*, 12:873–920, 2000.
[112] H. Yokoi. On real quadratic fields containing units with norm -1. *Nagoya Math. J.*, 33:139–152, 1968.
[113] D. Zagier. The dilogarithm function. In P. Cartier, P. Moussa, B. Julia, and P. Vanhove, editors, *Les Houches School of Physics: Frontiers in Number Theory, Physics, and Geometry II: On Conformal Field Theories, Discrete Groups and Renormalization: Les Houches, France, March 9-21, 2003*, pages 3–65, 2007.
[114] G. Zauner. *Quantendesigns – Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Vienna, 1999. Available in English translation as: G. Zauner, Quantum Designs: Foundations of a Noncommutative Design Theory, *Int. J. Quant. Inf.*, 9(1):445–507, 2011.

SCHOOL OF PHYSICS, UNIVERSITY OF SYDNEY, SYDNEY AUSTRALIA
Email address: marcus.appleby@gmail.com

DEPARTMENT OF COMPUTER SCIENCE, VIRGINIA TECH, ALEXANDRIA, VA, USA &
PHASECRAFT INC., WASHINGTON DC, USA
Email address: stf@vt.edu

DEPARTMENT OF MATHEMATICS, LOUISIANA STATE UNIVERSITY, BATON ROUGE, LA, USA
Email address: kopp@math.lsu.edu