The Galois Group of a SIC

August 13, 2015
The talk will be in two parts.

- I will begin by explaining what SICs are, and how they are relevant to quantum mechanics.
- I will then go on to describe the Galois symmetries of a SIC

---

Let $\mathcal{H}$ be a $d$-dimensional complex inner product space. A SIC\(^2\) is a family of $d^2$ vectors $|\psi_1\rangle, \ldots, |\psi_{d^2}\rangle \in \mathcal{H}$ such that

$$|\langle \psi_j | \psi_k \rangle|^2 = \begin{cases} 1 & j = k \\ \frac{1}{d+1} & j \neq k \end{cases}$$

So a SIC defines a set of $d^2$ equiangular complex lines.

\(^2\)The reason for the name “SIC” will be explained below.
• SICs have been constructed numerically for all $d \leq 121$ (to 8000 digit precision), and for a handful of other dimensions up to $d = 323$.

• Exact examples have been published for $d = 2–17, 19, 24, 35, 48$. Further unpublished examples known for $d = 19, 21, 22, 31, 37, 43$. 52 unitarily and anti-unitarily inequivalent exact fiducials in total (not counting the infinite number for $d = 3$).

• This encourages the speculation that SICs exist for every finite dimension. But that is only a speculation.
SIC projectors

Instead of the vectors $|\psi_j\rangle$ I will usually work with the associated projection operators (in Dirac notation)

$$\Pi_j = |\psi_j\rangle\langle\psi_j|$$

In other words $\Pi_j$ is the matrix

$$\Pi_j = \begin{pmatrix} 
\psi_{j,1}\psi_{j,1}^* & \psi_{j,1}\psi_{j,2}^* & \cdots \\
\psi_{j,2}\psi_{j,1}^* & \psi_{j,2}\psi_{j,2}^* & \cdots \\
\vdots & \vdots & \ddots 
\end{pmatrix}$$

So

$$\text{Tr}(\Pi_j\Pi_k) = \begin{cases} 
1 & j = k \\
\frac{1}{d+1} & j \neq k 
\end{cases}$$
SICs were introduced into physics by Zauner \cite{3} and Renes et al \cite{4}. Their importance in physics stems chiefly from the fact that they describe a certain kind of measurement.

Although mathematicians had been interested in equiangular lines long before these papers, only a handful of examples of $d^2$ complex equiangular lines had been constructed. It was the work of Zauner and Renes et al which made it seem plausible, that these structures exist in every finite dimension.

\footnote{\textit{J. Math. Phys.}, 45, 2171 (2004)}
Quantum measurements

The state of a quantum system of dimension $d$ is described by a density matrix: i.e. a $d \times d$ matrix $\rho$ which

- is positive semi-definite.
- has trace $= 1$.

A measurement is described by a set of operators $E_1, \ldots, E_n$ which

- are positive semi-definite.
- are such that $\sum_j E_j = I$.

The probability of obtaining measurement outcome $j$ for state $\rho$ is $\text{Tr}(\rho E_j)$.

The $E_j$ are called a POVM (“positive operator valued measure”).
For many measurements—e.g. measurements of spin, or energy—there are infinitely many states giving rise to a given probability distribution.

However, there are some measurements for which the probability distribution fixes the state.

Such measurements are said to be informationally complete.

Important experimentally because they can be used to infer the state statistically (quantum tomography).

An informationally complete POVM must contain at least $d^2$ elements. If it contains exactly $d^2$ elements it is said to be minimal informationally complete.
Let $\Pi_1, \ldots, \Pi_{d^2}$ be a family of SIC projectors. Then the operators

$$E_j = \frac{1}{d} \Pi_j$$

are a minimal informationally complete POVM.

Symmetric in the sense that the overlaps $\text{Tr}(E_j E_k)$ take only two values, depending on whether $j = k$.

Hence the acronym:

**Symmetric Informationally Complete Positive Operator Valued Measure**

(phew)
Steve Flammia has said something about the immediate practical relevance of SICs to quantum information.

In addition to that there are (at least) 3 less immediate, but perhaps in the long run more important, ways in which SICs are interesting:

- QBism
- Geometry of quantum state space
- Number theory

Considerable overlap between items 1 and 2. I am separating them because I want to make the point that there are reasons for being interested in SICs which are independent of the QBist program.
Long after Newton worked out the principles of classical mechanics an alternative, very different formulation was devised by Hamilton. This formulation turned out to be very fruitful. One may wonder if something similar might be possible with quantum mechanics.

Quantum mechanics is a fundamentally probabilistic theory. However, it is not explicitly formulated that way. Perhaps it *should* be formulated that way, so that the fundamental objects in the theory were, not operators on a complex vector space (density matrices, POVMs, etc), but probability distributions.

This is the idea behind the QBist program of Fuchs and Schack\(^5\). SICs play a central role in that approach.

\(^5\textit{Rev. Mod. Phys., 85, 1693 (2013)}\)
Geometry of Quantum State Space (1)

Quantum state space is a convex body in a $d^2 - 1$ dimensional real Euclidean space. Best described using the parameterization

$$\rho = \frac{1}{d}(1 + B)$$

where $B$ is a trace 1 Hermitian matrix—the Bloch vector. State space can be identified with the set of all $B$ for which the corresponding $\rho$ is positive semi-definite.

Define the inner product

$$\langle B_1, B_2 \rangle = \frac{1}{d(d-1)} \text{Tr}(B_1 B_2)$$

Then boundary of state space lies between the in-sphere of radius $\frac{1}{d-1}$ and out-sphere of radius 1.
For \( d = 2 \) the in- and out-spheres coincide, and state space is simply a ball. For \( d > 2 \) the geometry is much more complicated.

- In a 2 dimensional section the set of pure states is discrete. But globally they are a continuous manifold.
- For \( d = 2 \) the in and out spheres coincide.
- For \( d > 2 \) the pure states are a proper sub-manifold of the out-sphere (real dimension \( 2d - 2 \) as opposed to \( d^2 - 2 \)).
A family of SIC projectors $\Pi_1, \ldots, \Pi_{d^2}$ describes a measurement. It is also a set of pure states.

Let $B_1, \ldots, B_{d^2}$ be the corresponding Bloch vectors. Then

$$\langle B_j, B_k \rangle = \begin{cases} 1 & j = k \\ -\frac{1}{d^2-1} & j \neq k \end{cases}$$

—a regular simplex with its vertices in the manifold of pure states.

The fact that SICs exist in as many dimensions as they do is therefore remarkable: for the out-sphere has real dimension $d^2 - 2$, but the manifold of pure states only has real dimension $2d - 2$.

So if SICs did exist in every finite dimension this would be telling us something interesting about the geometry of quantum state space.
Quantum state space is the central object in quantum mechanics: the basic structure about which all else revolves. It is therefore remarkable that for $d > 2$ its geometry is still very poorly understood.

If one wants to understand the geometry better the SIC problem is an obvious place to start.
SICs say something else that is geometrically interesting about quantum state space.

To understand this point we need to digress, and consider the group covariance properties of a SIC.
Group Covariance

All known SICs have a group covariance property.

The projectors are labelled by the elements of a finite group $\mathcal{G}$. For each group element $g$ there is a unitary $U_g$ such that

$$U_g \Pi_{g'} U_g^\dagger = \Pi_{gg'}$$

for all $g'$. If the action of the group is transitive we can construct the SIC by taking the single projector $\Pi_e$ (the fiducial projector) and acting on it with the unitaries $U_g$. 

The Galois Group of a SIC
With one exception every known SIC is covariant under a specific group: the discrete Weyl-Heisenberg group (the exception being a SIC in dimension 8 which is covariant with respect to the tensor product of 3 copies of this group).

Moreover, in prime dimensions it can be proved that Weyl-Heisenberg SICs are the only group covariant SICs (though it remains an open question whether non-group covariant SICs are possible).

Suggests that the Weyl-Heisenberg group is of special importance for this problem.
In infinite dimensions we have the position and momentum operators $\hat{x}$ and $\hat{p}$ satisfying the canonical commutation relation

$$[\hat{x}, \hat{p}] = i\hbar$$

Impossible to define such operators in the finite dimensional case because

$$\text{Tr}(\hat{x}\hat{p}) - \text{Tr}(\hat{p}\hat{x}) = 0 \neq \text{Tr}(i\hbar I)$$

Suppose, however, instead of considering $\hat{x}, \hat{p}$ we consider the displacement operators

$$e^{i(p\hat{x} - x\hat{p})}$$

These do have finite dimensional analogues.
Definition of the Discrete Weyl-Heisenberg Group (2)

Take an orthonormal basis $|0\rangle, \ldots |d - 1\rangle$ for $d$ dimensional Hilbert space. Regard the integer labels $0, 1, \ldots, d - 1$ as the points in a discrete configuration space.

Define operators $X$ and $Z$ by

$$X|x\rangle = |x \oplus 1\rangle$$

where $\oplus$ means addition mod $d$, and

$$Z|x\rangle = \omega^x|x\rangle$$

where $\omega = e^{\frac{2\pi i}{d}}$.

Finally, define discrete analogues of the infinite dimensional displacement operators by

$$D_u = \tau^{u_1 u_2} X^{u_1} Z^{u_2}$$

where $\tau = -e^{\frac{\pi i}{d}}$ and $u = (\frac{u_1}{u_2})$. 

The Galois Group of a SIC
In addition to the Weyl-Heisenberg group we also need to consider symplectic transformations.

In the infinite dimensional case symplectic unitaries transform the position and momentum operators according to

\[ U\hat{x}U^\dagger = \alpha \hat{x} + \beta \hat{p} \quad U\hat{p}U^\dagger = \gamma \hat{x} + \delta \hat{p} \]

\[ \alpha \delta - \beta \gamma = 1 \]

(the squeezing unitaries in quantum optics are of this type).

Symplectic unitaries act on the displacement operators \( D_u = e^{i(p\hat{x} - x\hat{p})} \) (where \( u = (x, p) \)) according to:

\[ UD_uU^\dagger = D_{Fu} \quad F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \]

The Galois Group of a SIC
In the discrete case one no longer has position and momentum operators. However, one still has the displacement operators, and one still has unitaries which transform them according to

\[ U_F D_u U_F^\dagger = D_{F_u} \]  \hspace{1cm} (1)

for suitable \( F \).

It is necessary, however, to make a distinction between the even and odd dimensional case. Define

\[ \bar{d} = \begin{cases} 
  d & \text{if } d \text{ is odd} \\
  2d & \text{if } d \text{ is even}
\end{cases} \]

—dimension doubling trick.

Then a \( U_F \) satisfying Eq. (1) exists if and only if \( F \in \text{SL}(2, \mathbb{Z}_{\bar{d}}) \).
The displacement operators and symplectic unitaries generate the Clifford group.

The Clifford group thus consists of all unitaries of the form

\[ e^{i\theta} U_F D_p \]
Symplectic unitaries are important for three reasons:

- They preserve SICness: if $\Pi_p$ is a Weyl-Heisenberg SIC, then $U_F^\dagger \Pi_p U_F$ is also a Weyl-Heisenberg SIC.
- It turns out that every known Weyl-Heisenberg SIC fiducial is an eigenvector of a certain special symplectic unitary (the Zauner matrix):

$$U_F \Pi_0 U_F^\dagger = \Pi_0 \quad \text{Tr}(F) = -1$$

(no one knows why).
- There is a fascinating interplay between the action of the symplectic unitaries and the Galois symmetries described below.

The Galois Group of a SIC
In an infinite dimensional system the position and momentum operators have an immediate physical significance. Consequently the infinite dimensional Weyl-Heisenberg and symplectic groups have an immediate physical significance.

But in finite dimensional systems these groups have no immediately obvious physical significance.

However, it is clear that SICs, when they exist, are saying something important about the geometry of quantum state space. Since the Weyl-Heisenberg and symplectic groups play a crucial role in the SIC problem it follows that they too describe an important, albeit non-obvious feature of quantum state space.

It would seem, therefore, that the groups have a hidden physical significance.
Historically connections between physics and number theory have been isolated gems: they exist, but they are thin on the ground.

SICs are fascinating because they promise to give us another such connection. It very much looks as though a fundamental geometrical feature of quantum state space is intimately connected to some deep results in algebraic number theory. Moreover, it may turn out that the influence goes both ways: that SICs will turn out to be important, not only to physics, but also to number theory.

The subject of the remainder of this talk.
Exact Weyl-Heisenberg SICs have been found (by Grassl and others) in dimensions 2–17 inclusive, and also 19, 24, 28, 35, 48.

Solutions are in general very complicated (often many pages of computer print out. However \((d = 3\) excepted) they have a certain striking property: namely, they are all expressible in terms of radicals (nested roots).
Galois showed that the solutions to a polynomial equation in one variable of degree $\geq 5$ are typically not expressible in terms of radicals.

A SIC fiducial projector $\Pi = |\psi\rangle\langle\psi|$ is a solution to the equations

$$|\langle\psi|D_p|\psi\rangle|^2 = \frac{d\delta_{p,0} + 1}{d + 1}$$

These are degree 4 polynomial equations in the components of $|\psi\rangle$. So the solution should be expressible in radicals?

—Not so: for they are equations in many variables.
Standard way to solve a system of equations like the one in the last slide is to construct a Gröbner basis. This reduces the problem to that of solving a series of polynomial equations each in a single variable. However the effect of the construction is usually to (greatly) increase the degree. As is the case here.

So one would not \textit{a priori} expect the solutions to be expressible in radicals.

Nevertheless in each of the 28 cases with $d \neq 3$ so far calculated they \textit{are} expressible in radicals.

—tells us that the Galois group is of a very special kind. Specifically: it is a solvable group.
Definition of a solvable group

A group $G$ is said to be solvable if there is a series of subgroups

$$\langle e \rangle = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{n-1} \triangleleft H_n = G$$

(where $e$ is the identity) such that the inclusions are all normal and the quotient groups

$$H_{j+1}/H_j$$

are Abelian for $j = 0, 1, \ldots, n - 1$.

—Generalization of the concept of an Abelian group

It turns out that for a SIC we can, in every known case, find such a series of length 3.

Could be said that for a SIC the Galois group is close to Abelian (if it was Abelian we could find a series of length 2).
Can we say more about the Galois structure? (beyond this basic fact, that the group is solvable).
The complex numbers
\[ \mathbb{C} = \mathbb{R}(i) \]

obtained by adding to the reals the single generator \( i \). Consists of all combinations of the form

\[ a + ib \]

with \( a, b \) real.

A galois conjugation is any map \( g : \mathbb{C} \to \mathbb{C} \) which

- Leaves \( \mathbb{R} \) fixed: \( g(x) = x \) for all \( x \in \mathbb{R} \).
- Preserves addition and multiplication:

\[ g(z + w) = g(z) + g(w) \quad g(zw) = g(z)g(w) \]

There are exactly two such maps: the identity map and ordinary complex conjugation

\[ g_c : a + ib \to a - ib \]
Another simple example

The number field

\[ F = \mathbb{Q}(\sqrt{2}) \]

by adding to the rationals the single generator \( \sqrt{2} \). Consists of all combinations of the form

\[ a + b\sqrt{2} \]

with \( a, b \) rational.

Galois group consists of the identity together with the map

\[ g : \sqrt{2} \rightarrow -\sqrt{2} \]
A slightly less trivial example

The number field

\[ F = \mathbb{Q}\left(i, \sqrt{\sqrt{2} + 1}\right) \]

consisting of all combinations of the form

\[(a_1 + ia_2) + (b_1 + ib_2)\sqrt{2} + (c_1 + ic_2)\sqrt{\sqrt{2} + 1} + (d_1 + id_2)\sqrt{\sqrt{2} - 1}\]

with \(a_1, \ldots, d_2\) rational. Galois group generated by

\[ g_c : i \to -i \quad \sqrt{\sqrt{2} + 1} \to \sqrt{\sqrt{2} + 1} \]

\[ g_1 : i \to -i \quad \sqrt{\sqrt{2} + 1} \to i\sqrt{\sqrt{2} - 1} \]

Non-Abelian (though still solvable): \( g_1g_c = g_cg_1^3 \).
Let $a$ be an algebraic number, and let $f(x)$ be the (unique) polynomial over the rationals of lowest degree for which $a$ is a root and the leading coefficient = 1. Then we can write

$$f(x) = (x - a_1) \ldots (x - a_n)$$

where $a_1 = a$. We say that $a_2, \ldots, a_n$ are the Galois conjugates of $a$.

So the Galois conjugate of a number is a generalization of its complex conjugate.

A number field $\mathbb{F}$ is said to be normal over the rationals if it contains all the Galois conjugates of $a$ whenever it contains $a$. 
Let $F$ be a normal extension of $Q$.

Let $G$ be the Galois group of $F$ over $Q$.

Then there is a bijection between subgroups and subfields, with inclusions reversed:

$$\begin{align*}
\{ e \} & \subseteq H \subseteq G \\
\uparrow & \uparrow \uparrow \\
F & \supseteq K_H \supseteq Q
\end{align*}$$

where $K_H$ consists of the elements of $F$ fixed by the elements of $H$. 
For the first 2 examples the Galois group was Abelian; for the last it was non-Abelian.

Kronecker’s question: can we fully characterize the fields having an Abelian Galois group? —The answer is yes.

**Kronecker-Weber theorem**: a field has Abelian Galois group over $\mathbb{Q}$ if and only if it is a subfield of

$$\mathbb{Q}(e^{\frac{2\pi i}{n}})$$

for some $n$ (a cyclotomic field).
Having got that far Kronecker then thought about generalizing the result.

Suppose we have a tower

\[ \mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L} \]

Let \( \mathcal{G}_K(\mathbb{L}) \) be the Galois group of \( \mathbb{L} \) over \( \mathbb{K} \) (i.e. the automorphisms of \( \mathbb{L} \) which fix the numbers in \( \mathbb{K} \)).

**Question:** for given \( \mathbb{K} \) can we fully characterize the set of fields \( \mathbb{L} \) for which \( \mathcal{G}_K(\mathbb{L}) \) is Abelian?
This question can be answered in the affirmative for imaginary quadratic fields: i.e. fields of the kind

\[ K = \mathbb{Q}(i\sqrt{n}) \]

with \( n \) a positive integer.

The proof uses Kronecker’s theory of complex multiplication (which, contrary to what the name might suggest, is emphatically not trivial).

Using this theory it can be shown that \( G_K(\mathbb{L}) \) is Abelian if and only if \( \mathbb{L} \) is a subfield of a field generated by the torsion points of a certain kind of elliptic curve.
Hilbert described the theory of complex multiplication as “not only the most beautiful part of mathematics but also of all science.”

Admittedly this is the recollection of one person, published 11 years after the event\(^6\). But there can be no doubt that it inspired Hilbert’s 12\(^{th}\) problem, which asks for the generalization of complex multiplication to other number fields.

This problem has been one of the main foci of algebraic number theory ever since, but in spite of an enormous amount of effort it remains open.

The obvious place to start is Abelian extensions of real quadratic fields. These are precisely the fields which feature in the SIC problem.

\(^6\)Taussky, *Nature*, **152**, 182 (1943)
Given a SIC fiducial projector $\Pi$ let

- $\mathbb{F}$ be the smallest normal extension of $\mathbb{Q}$ containing the standard basis components of $\Pi$ together with $e^{\frac{\pi i}{d}}$ (needed to for the Clifford unitaries).

- $\mathcal{G}$ be the Galois group of $\mathbb{F}$ over $\mathbb{Q}$.
If $\Pi$ is a fiducial projector then so is $\Pi^*$. Do we also get another fiducial if, instead of complex conjugation, we apply an arbitrary Galois conjugation?

In general, no. We need $g(\Pi)$ to be Hermitian. But if $g$ does not commute with complex conjugation it will typically happen that

$$(g(\Pi))^\dagger = (g(\Pi^T))^* \neq g(\Pi^\dagger) = g(\Pi)$$

Suppose, however, we define $G_c \subseteq G$ to be the subgroup consisting of all $g$ which commute with complex conjugation.

Then the elements of $G_c$ do preserve hermiticity and unitarity. They also take SICs to SICs.
The elements of $G_c$ map the Clifford group onto itself:

$g(D_u) = D_{H_g u}$

$g(U_F) = U_{H_g} F H_{g}^{-1}$

where

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

$k_g$ being the unique integer in the range $0 \leq k_g < \bar{d}$ such that $g(\tau) = \tau^{k_g}$. 

The Galois Group of a SIC
Let $\mathbb{F}_c$ be the subfield associated to $G_c$ under the Galois correspondence.

Then it turns out that in all 27 known exact cases with $d > 3$

$$\mathbb{F}_c = \mathbb{Q}(\sqrt{(d - 3)(d + 1)})$$

What happens when $d \leq 3$? If $d = 2$ then $\mathbb{F}_c = \mathbb{Q}$, while in dimension 3 the number field is typically transcendental.

The mathematical phenomenon responsible for driving SIC existence only sets in at $d = 4$. 

The Galois Group of a SIC
For all 27 known exact fiducials in dimension $d > 3$:

- The series $\langle e \rangle \triangleleft \mathcal{G}_c \triangleleft \mathcal{G}$ is normal.
- $\mathcal{G}_c$ is Abelian
- $\mathcal{G}/\mathcal{G}_c$ is Abelian of order 2

We knew already that $\mathcal{G}$ must be solvable. But it turns out (in the cases examined) to be a solvable group of a particularly simple kind. It could be said that $\mathcal{G}$ is as close to Abelian as it could get without actually being Abelian.
Orbit preserving automorphisms

Define

- $G_0 \subseteq G_c$ to consist of $g \in G_c$ which are $\text{EC}(d)$ orbit preserving.
- $F_0 \supseteq F_c$ to be the corresponding subfield.

The 27 known exact solutions for $d > 3$ fall into 2 classes: singlets ($\text{EC}(d)$ orbits closed under Galois conjugation) and doublets (pairs of $\text{EC}(d)$ orbits related by a Galois conjugation). We find

$$G_c/G_0 \cong \begin{cases} \mathbb{Z}_1 & \text{for a singlet} \\ \mathbb{Z}_2 & \text{for a doublet} \end{cases}$$

$$F_0 = \begin{cases} F_c & \text{for a singlet} \\ F_c(\sqrt{p}) & \text{for a doublet} \end{cases}$$

where $p$ is a prime divisor of $d(d - 3)(d + 1)$. 
g-Unitaries

Anti-unitary:

unitary + complex conjugation

g-unitary:

unitary + Galois conjugation

For each \( g \in \mathcal{G}_0 \) there exists a g-unitary \( V_g \) such that

\[
V_g \Pi V_g^\dagger = \Pi
\]

So \( \Pi \) is a joint eigenprojector of a family of g-unitaries.

g-unitaries are typically not diagonalizable so this is a strong constraint.
Define

\[ \chi_p = \text{Tr}(\Pi D_p^\dagger) \]

The overlaps \( \chi_p \) specify \( \Pi \):

\[ \Pi = \frac{1}{d} \sum_p \chi_p D_p \]
Let $S$ be the group consisting of all $F \in \text{ESL}(2, \mathbb{Z}_d)$ such that

$$\chi_{Fp} = \chi_p$$

Let $N$ be the normalizer of $S$ in $\text{GL}(2, \mathbb{Z}_d)$. Then for each $g \in G_0$ there is a unique coset $G_g S \in N/S$ such that

$$g(\chi_p) = \chi_{Gp}$$

for all $G \in G_g S$. 

The Galois Group of a SIC
Let $G_1$ be the kernel of the homomorphism

$$f : G_0 \to N/S$$

and let $F_1 \supseteq F_0$ be the corresponding subfield.

Then $G_0/G_1$ is isomorphic to a subgroup of $N/S$. 
For all 27 known exact fiducials with $d \geq 4$ a stronger statement holds:

$$\mathcal{G}_0/\mathcal{G}_1 \cong C/S$$

where $C$ is the centralizer of $S$ in $\text{GL}(2, \mathbb{Z}_d)$.

This structure is highly reminiscent of what happens in the theory of complex multiplication.
Putting it all together

For every published fiducial in dimension $\geq 4$ the Galois group has the normal series

$$\langle e \rangle \triangleleft G_0 \triangleleft G$$

where

$$G_0 \cong \mathbb{C}/S \oplus \mathbb{Z}_2$$

$$G/G_0 \cong \begin{cases} 
\mathbb{Z}_2 & \text{for a singlet} \\
\mathbb{Z}_2 \oplus \mathbb{Z}_2 & \text{for a doublet}
\end{cases}$$

These conjectures combined with the LLL algorithm allow one to lift numerical solutions to exact ones. For these new, so far unpublished exact SICs, one finds quartets of Galois conjugated orbits in dimensions 37 and 43. But $G/G_0$ still has a simple structure.
So far I have been describing the results in our 2012 paper. Since then we have made significant progress. In particular we now have conjectures (verified in 50 cases) which fully specify, not only the Galois group but the number field itself in an arbitrary dimension.

If these conjectures are correct SICs are number-theoretically universal in the sense that every Abelian extension of every real quadratic field is a subfield of a SIC field for some dimension $d$.

---

7 Appleby, Yadsan-Appleby, Zauner
8 Appleby, Flammia, Donnelly, McConnell, Coates, Yard, Waldron, Chien
Degree of the field

The Galois Group of a SIC
Degree of the field (log-log plot)
Supposing these conjectures could be proved it wouldn’t necessarily give us a solution to the $12^{th}$ problem for real quadratic fields.

What impressed Hilbert was the fact that important kinds of finite degree algebraic number fields can be generated, in a natural and beautiful way, by special values of analytic functions whose values are typically transcendental.

Is the same true of a SIC?
Perhaps.

The theory of complex multiplication for imaginary quadratic fields involves elliptic curves over $\mathbb{Q}$. Suppose one considered elliptic curves over some other number field. Might one get an Abelian extension of a real quadratic field?

In one case, yes. Specifically the SIC in dimension 5 is related to the torsion points of an elliptic curve. So far we have failed to find other examples. Possibly this is because there are no other examples. Or possibly it is because so far we haven’t guessed right (the search space is large).
Perhaps the SIC existence problem is a Hilbert problem in disguise.