Number-Theoretic Aspects of Maximal Sets of Complex Equiangular Lines

February 20, 2018

Joint work:

- Appleby, Yadsan-Appleby, Zauner, *Quantum. Inf. Comput.*, **13**, 672 (2013)
- Appleby, Flammia, McConnell, Yard, arXiv:1604.06098 (2016)
- Appleby, Flammia, McConnell, Yard, *Found. Phys.* **47**, 1042 (2017)
- Appleby, Chien, Flammia, Waldron, arXiv:1703.05891 (2017)

A piece of terminology

This talk is about maximal sets of complex equiangular lines. I am a physicist, so I am going to use the name usual in physics : SIC (short for Symmetric Iinformationally Complete Positive Operator Valued Measure), pronounced SEEK (as opposed to SICK).

A SIC is a geometrical structure.

However, quite unexpectedly, it turns out to have some remarkably rich and interesting number-theoretic properties, having connections with a major open problem in number theory (Hilbert's 12th problem). These are the subject of this talk.

Two-way connection: number theory may help us understand SICs better; SICs may help us understand number theory better.

Preliminaries (1)

A SIC is a set of d^2 equiangular lines in a d-dimensional complex vector space. It is therefore specified by a set d^2 normalized vectors $|\psi_1\rangle, \ldots, |\psi_{d^2}\rangle$ satisfying

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

Problem: the choice of the $|\psi_j\rangle$ is arbitrary, in that each can be a multiplied by an arbitrary phase factor $e^{i\theta_j}$. This non-uniqueness matters from a number-theoretical point of view. To get a unique, canonical object we therefore take the corresponding projectors $|\psi_j\rangle\langle\psi_j|$ to be the object of study.

So for our purposes a SIC is a set of d^2 rank-1 projectors $\Pi_1, \ldots \Pi_{d^2}$ on d-dimensional complex inner product space such that

$$\mathrm{Tr}(\Pi_j \Pi_k) = \begin{cases} 1 & j = k \\ \frac{1}{d+1} & j \neq k \end{cases}$$

Existence

- SICs have been calculated numerically[1] in dimensions 2–151 inclusive; also 168, 172, 195, 199, 228, 259, 323, 844.
- Exact SICs have been calculated[2] in dimensions 2–21 inclusive; also 24, 28, 30, 31, 35, 37, 39, 43, 48, 120, 323.
- This encourages the speculation that SICs exist for every finite dimension. But a proof is still lacking.

---

[1] Scott and Grassl, *J. Math. Phys*, **51** , 042203 (2010); Scott, arXiv:1703.03993; Fuchs, Hoang and Stacey, *Axioms*, **6**, 21 (2017); Grassl and Scott, *J. Math. Phys.* **58**, 122201 (2017)

[2] Scott and Grassl, *ibid*; Appleby, Chien, Flammia, Waldron, arXiv:1703.05891 (2017); Grassl and Scott, *ibid*; Grassl, to appear.

Group Covariance

A SIC is said to be group covariant if

- 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'.
- The group action is transitive.

This means that the SIC is fully specified by fixing a single projector (the fiducial projector).

Weyl-Heisenberg Group

With a single exception[3] every known SIC is covariant with respect to the Weyl-Heisenberg (or WH) group.

Moreover, in prime dimensions it can be proved that if a SIC has a group covariance at all, then it is necessarily covariant with respect to the Weyl-Heisenberg group[4] (though it remains an open question whether non-group covariant SICs are possible).

[3] The exception being a SIC in dimension 8 which is covariant with respect to the product of 3 copies of the group

[4] Zhu, *J. Phys. A*, **43**, 305305 (2010).

Definition of the WH group

- Fix an orthonormal basis $|0\rangle, \ldots |d-1\rangle$.
- Define operators X, Z by

$$X|r\rangle = |r \oplus 1\rangle \qquad\qquad Z|r\rangle = \omega^r |r\rangle$$

  where $r \oplus 1$ means addition *mod* d and $\omega = e^{2\pi i/d}$.
- Define WH displacement operators

$$D_{j,k} = X^j Z^k$$

- A WH SIC consists of the d^2 projectors

$$D_{j,k}^\dagger \Pi D_{j,k}$$

  where Π is the fiducial projector.

Extended Clifford Group

SICs are naturally classified using the extended Clifford group. This is the set of unitaries/anti-unitaries U which permute the WH displacement operators according to

$$UD_{\mathbf{p}}U^{\dagger} \doteq D_{F\mathbf{p}}$$

where $\doteq$ means "equal up to multiplication by a phase", and[5] F is a 2×2 matrix with entries in $\mathbb{Z}/d\mathbb{Z}$ such that $\det F = \pm 1 \mod d$. The set of all such 2×2 matrices will be denoted $\mathrm{ESL}(2, \mathbb{Z}/d\mathbb{Z})$.

[5] If d is even one needs to replace d with $2d$ in the rest of this paragraph. From now on I will ignore this complication.

Classification

The significance of the Clifford group is that if Π_j is a WH SIC and U is a Clifford unitary/anti-unitary then $U\Pi_j U^\dagger$ is another WH SIC. So the set of all WH SICs in a given dimension splits into orbits under the extended Clifford group.

With the exception of $d = 3$ there are only a finite number of orbits in every dimension studied so far. We follow the Scott-Grassl convention of labelling the orbits with a letter.

For example in dimension 4 there is a single extended Clifford group orbit $4a$, in dimension 7 there are two orbits $7a$, $7b$, in dimension 35 there are ten orbits $35a$–$35j$, and so on.

The numbers themselves

In this talk the emphasis will be on the numbers theoretic properties of the known SIC projectors.

Need to be a bit careful here: the matrix elements of a projector Π depend on the basis. In the following it will always be assumed that we are working in the *standard* basis: i.e. the basis in which the WH displacement operators act in the manner described earlier.

Also WH SICs in dimensions 2 and 3 have some special properties. In the following it will accordingly be assumed without comment that $d \geq 4$.

The observation which started all this

There are now 98 known examples of extended Clifford SIC orbits (exact solutions—many hundreds of numerical ones).

Solutions are in general very complicated (sometimes more than a 1000 pages of computer print out). However they all have a certain striking property: namely, they are all expressible in terms of radicals (nested roots).

Why is this surprising?

Galois showed that the solutions to a polynomial equation in one variable of degree ≥ 5 are typically not expressible in terms of radicals.

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

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

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.

Gröbner Bases

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 *a priori* expect the solutions to be expressible in radicals.

Nevertheless in each of the 98 cases calculated so far they are expressible in radicals.

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

The basic idea of Galois theory.

Simple example

There is one example which everyone knows: the complex numbers $\mathbb{C} = \mathbb{R}(i)$. Consists of all combinations of the form

$$a + ib \qquad\qquad a, b \in \mathbb{R}$$

A galois conjugation is any map $g : \mathbb{C} \to \mathbb{C}$ such that

$$g(x) = (x)$$
$$g(z + w) = g(z) + g(w)$$
$$g(zw) = g(z)g(w)$$

$\forall x \in \mathbb{R}$ and $z, w \in \mathbb{C}$. There are exactly two such maps: the identity map and complex conjugation.

So the Galois group is cyclic, order 2.

Generalization

Suppose we have a base field $\mathbb{B}$ and a generator $u \notin \mathbb{B}$. Then define $\mathbb{B}(a)$ to be the smallest field containing $\mathbb{B}$.

In the last example the base field was $\mathbb{R}$, the generator was i and the extension field was $\mathbb{C}$.

Assume that u is the root of a polynomial with coefficients in $\mathbb{B}$ (i.e. is algebraic over $\mathbb{B}$). Then $\mathbb{B}(u)$ consists of all combinations $c_0 + c_1 u + \ldots c_{n-1} u^{n-1}$ with $c_j \in \mathbb{B}$ for some integer n (the degree of the extension).

The Galois group consists of all bijections $g : \mathbb{B}(u) \to \mathbb{B}(u)$ which (a) fix the base field and (b) preserve addition and multiplication. It is a finite group of order $\leq n$. The extension is said to be normal if the order $= n$.

Fields over the rationals

In the SIC problem the base field is always $\mathbb{Q}$.

A very simple example of such an extension: $\mathbb{F} = \mathbb{Q}(\sqrt{2})$ consisting of all numbers of the form

$$a + b\sqrt{2} \qquad\qquad a, b \in \mathbb{Q}$$

Galois group consists of the identity together with the map

$$g : a + b\sqrt{2} \to a - b\sqrt{2}$$

(analogue of complex conjugation).

So as with $\mathbb{R}(i)$ the Galois group is cyclic, order 2.

Another example: Cyclotomic fields

Cyclotomic fields are fields generated by roots of unity over the rationals.

Let $\omega = e^{\frac{2\pi i}{p}}$ where p is a prime number and $\mathbb{F} = \mathbb{Q}(\omega)$. Then $\mathbb{F}$ consists of all combinations of the form

$$c_0 + c_1\omega + \cdots + c_{p-2}\omega^{p-2}$$

The Galois group consists of the $p-1$ automorphisms $g_k : \omega \to \omega^k$, $k = 1, \ldots, p-1$. It is therefore cyclic, order $p-1$.

In the case of an m^{th} root of unity for m not a prime number the group is still Abelian, but no longer cyclic.

Towers

We can extend the field repeatedly, to obtain a tower:

$$\mathbb{Q} \subset \mathbb{Q}(u_1) \subset \mathbb{Q}(u_1, u_2) \subset \cdots \subset \mathbb{Q}(u_1, \ldots, u_m)$$

Actually, it is always possible to replace the multiple generators $u_1, \ldots, u_m$ with a single generator v:

$$\mathbb{Q}(u_1, \ldots, u_m) = \mathbb{Q}(v)$$

However, one often gets more insight into the field by building it as a tower—as we will shortly see.

Example of a non-Abelian Galois group

Consider the tower

$$\mathbb{Q} \subset \mathbb{F} \subset \mathbb{E}$$

$$\mathbb{F} = \mathbb{Q}(i) \qquad \mathbb{E} = \mathbb{F}(\sqrt{\sqrt{2}+1})$$

The Galois group of $\mathbb{E}$ over $\mathbb{Q}$ is generated by

$$g_1 : i \to -i \qquad \sqrt{\sqrt{2}+1} \to \sqrt{\sqrt{2}+1}$$

$$g_2 : i \to -i \qquad \sqrt{\sqrt{2}+1} \to i\sqrt{\sqrt{2}-1}$$

It is non-Abelian, because $g_1 g_2 = g_2^3 g_1$.

Example of a non-Abelian Galois group (2)

In the tower

$$\mathbb{Q} \subset \mathbb{F} \subset \mathbb{E}$$

$$\mathbb{F} = \mathbb{Q}(i) \qquad\qquad \mathbb{E} = \mathbb{F}(\sqrt{\sqrt{2}+1})$$

we saw that the Galois group of $\mathbb{E}$ over $\mathbb{Q}$ is non-Abelian.

However, the Galois groups of the individual extensions—$\mathbb{F}$ over $\mathbb{Q}$ and $\mathbb{E}$ over $\mathbb{F}$—are Abelian.

This is connected with the fact that the field is generated by radicals (combinations of nested roots), and is a particular instance of a general phenomenon.

General theorem

A field $\mathbb{E}$ is generated by radicals if and only if it can be built as a tower

$$\mathbb{Q} \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_m \subset \mathbb{E}$$

such that

(a) Each successive extension is normal over the one before (degree of extension equals order of group).

(b) The Galois group of each field over the one before is Abelian.

It is possible to re-express this as a statement about the Galois group of $\mathbb{E}$ over $\mathbb{Q}$—which is how Galois proved his celebrated theorem, that polynomial equations of degree ≥ 5 cannot, in general, be solved in radicals.

Back to SICs

The exact expressions for SIC projectors are simply *horrible*—in some cases many pages of printout for a single matrix element. The fields they generate are huge—degree 10^4 or more.

However

In the 98 cases examined they are always expressible in radicals. Which tells us that the field they generate must be constructible as a tower with each successive extension Abelian over the one before.

Obvious question:

How tall is the tower?

Given the (seeming) horribleness of the numbers one might expect the tower to be horrible too. But in fact it isn't.

Structure of the SIC field

In every case examined the field has the structure

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{D}) \subset \mathbb{E}$$

where D is the square-free part of $(d-3)(d+1)$, and $\mathbb{E}$ is a normal Abelian extension of $\mathbb{Q}(\sqrt{D})$ (and, in fact, $\mathbb{Q}$).

This is striking because

(1) The tower is height 2—as short as it can be consistent with $\mathbb{E}$ not being Abelian over $\mathbb{Q}$.

(2) The intermediate field is degree 2—as low as it can be consistent with $\mathbb{E}$ not being Abelian over $\mathbb{Q}$.

(3) We have an ansatz for a generator of the intermediate field: namely the number $\sqrt{D}$.

However, it doesn't end there. $\mathbb{E}$ isn't just *any* Abelian extension of $\mathbb{Q}(\sqrt{D})$. It is a very remarkable one. To understand why we need to review some number theory.

Abelian extensions in general.

Abelian extensions have been the focus of an enormous amount of work over the last 150 years. Indeed, they are the subject of Hilbert's 12^{th} problem.

So a lot is known about them (though not as much as we would like—Hilbert's 12^{th} problem is still unsolved).

Kronecker-Weber theorem

Kronecker started this line of investigation back in the 19^{th} century, by asking what is the general form of an Abelian extension of the rationals. The answer is given by

> *Kronecker-Weber theorem: a finite degree field is Abelian over the rationals if and only if it is a subfield of a cyclotomic field (i.e. a subfield of $\mathbb{Q}(e^{\frac{2\pi i}{n}})$, for some n).*

Generalizing the Kronecker-Weber Theorem

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 $\mathcal{G}_{\mathbb{K}}(\mathbb{L})$ 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 $\mathcal{G}_{\mathbb{K}}(\mathbb{L})$ is Abelian?

Imaginary Quadratic Fields

This question can be answered in the affirmative for imaginary quadratic fields: i.e. fields of the kind

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

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 $\mathcal{G}_{\mathbb{K}}(\mathbb{L})$ 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's 12^{th} problem

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 (i.e. the type of field which features in the SIC problem).

[6] Taussky, *Nature*, **152**, 182 (1943)

Breaking the problem up

To solve Hilbert's 12^{th} problem for real quadratic fields you need to do two things:

(1) Identity the analogues of the fields $\mathbb{Q}(e^{\frac{2\pi i}{n}})$.

(2) Identify the analogue of the transcendental function e^x (supposing it exists).

It is (2) which remains open. (1) has been solved.

Ray class fields

The fields which play the role of $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ for Abelian extensions of an arbitrary field are called ray-class fields. The analogue of the integer n is called the conductor.

For a given real quadratic field and a given finite integer n there are actually four ray class fields. We are chiefly interested in the largest, which contains the other three, and is technically called the ray class field with ramification at both infinite places.

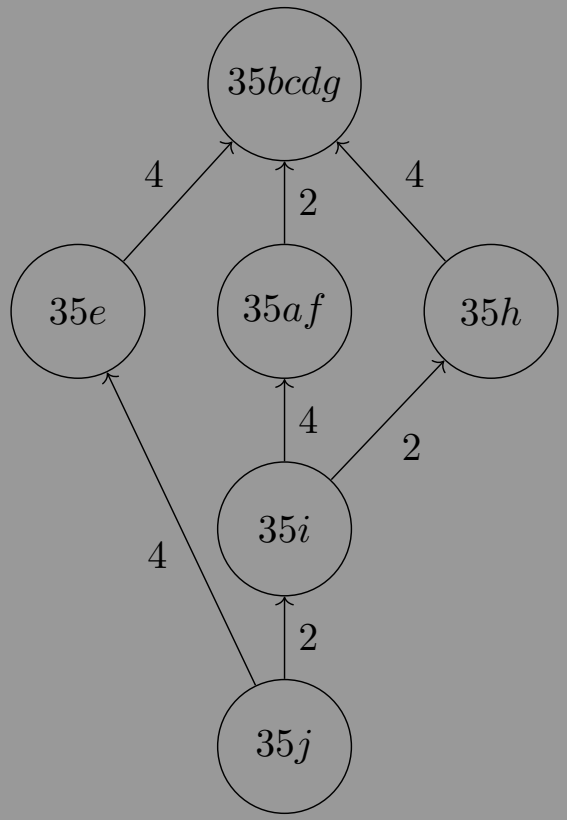
Although no one knows the analogue of the function e^x (or even whether it exists), there are algorithms for calculating ray class fields. Enter the appropriate commands into a program like *Magma* and it will give you a set of generators. Often (but not always) it will even do it fast: seconds or less.

Back to SICs: fields and multiplets

In a given dimension d there is typically more than one extended Clifford orbit of SICs. The orbits are grouped into multiplets: collections of orbits all corresponding to the same number field. It turns out that the fields associated to the different multiplets form a lattice under field inclusion. The lattice has unique minimal and maximal elements, with all other fields being intermediate between these two.

Field Lattice for Dimension 35

Labels $35j$, $35i$ etc are the corresponding extended Clifford orbits in Scott-Grassl notation. Numbers beside the arrows are extension degrees.



Remarkable fact

It turns out that each of the 24 minimal SIC fields which have been examined to date (for $d = 4$–21, 24, 28, 35, 48, 120, 323) is the ray class field over $\mathbb{Q}(\sqrt{D})$ with conductor d and ramification at both infinite places.

Two questions

This raises two natural questions:

(1) Supposing the phenomenon occurs in every dimension, just how many ray class fields are generated by SICs?

(2) The fact that a geometric structure generates a certain field does not usually tell one very much about the structure itself. For instance, the standard-basis components of a full set of Wootters-Fields MUBs generate a cyclotomic field. Knowing this is not, on its own, very much help if one wants to calculate the MUBs. Is the fact (if it is a fact) that SICs generate a ray class field similarly uninformative? Or can we work backwards, from the field to the geometry?

The construction I describe next gives some insight into both those questions.

Question 1

Suppose we are given an arbitrary square-free positive integer m and we want the set of conductors for which the ray class field over $\mathbb{Q}(\sqrt{m})$ is a minimal SIC field.

It turns out that the set is infinite for all m. Moreover, if we know the smallest conductor (dimension) d_1 then we can calculate all the others using the formula

$$d_n = 1 + 2T_n\left(\frac{d_1 - 1}{2}\right)$$

where T_n is a Chebyshev polynomial of the first kind. Calculating d_1 is less straightforward, but there is an algorithm for that also[7].

So the answer is: SICs generate a large class of ray class fields, but by no means all.

[7] Interestingly, there is a quantum algorithm giving an exponential speed-up.

Question 2

Let's look at the sequence of dimensions d corresponding to given D a little more closely. For $D = 5$ the sequence is

$$4,\ 8,\ 19,\ 48,\ 124,\ 323,\ 844,\ 2208,\ 5779,\ 15128, \ldots$$

Looking at this sequence we see that it contains subsequences in which each element is a multiple of the one before:

$$4,\ 8,\ 48,\ 2208,\ \ldots$$
$$19,\ 323,\ \ldots$$
$$4,\ 124,\ 15128,\ \ldots$$

One can show there are infinitely many such infinite subsequences. We call them dimension towers.

Question 2: Embeddings (1)

It is easily seen that if n_1 is a divisor of n_2 then $\mathbb{Q}(e^{\frac{2\pi i}{n_1}})$ is a subfield of $\mathbb{Q}(e^{\frac{2\pi i}{n_2}})$.

This is a general property of ray class fields. In particular, if $\mathbb{E}_1$, $\mathbb{E}_2$ are ray class fields over $\mathbb{Q}(\sqrt{D})$ with conductors d_1, d_2, and if d_1 is a divisor of d_2, then $\mathbb{E}_1$ is contained in $\mathbb{E}_2$.

Question 2: Embeddings (2)

As we go up a dimension tower the fields embed. So do the SICs themselves embed?

Amazingly, it turns out that they do, in a very intricate and surprising way which one would not have guessed. At least that is the case in the handful of cases we have been able to check.

This raises the prospect of an inductive proof: calculate a SIC for the bottom of the tower by brute force, and then lever one's way up.

It also gives a semi-positive answer to question 2. Knowing the field doesn't give you the geometry on a plate, just like that. But it seems to give you some useful clues.

Units (1)

Another important number-theoretic feature has to do with the unit group.

The rationals are the set of all quotients of pairs of ordinary integers n, m. It turns out that an analogous statement holds for an arbitrary algebraic number field: its elements are quotients of pairs of generalized, or algebraic integers.

Algebraic integers are the object of study in algebraic number theory. Just as ordinary number theory studies the divisibility properties of ordinary integers, so algebraic number theory studies the divisibility properties of algebraic integers. In particular, those properties are central to the theory of ray class fields.

Units (2)

However, going from ordinary to algebraic integers introduces a novelty. There are exactly two ordinary integers n with the property that n^{-1} is also an integer (namely ± 1). But in the case of the algebraic integers in an algebraic number field there are usually infinitely many. They form an Abelian group under multiplication, which is called the unit group.

For example, the unit group for $\mathbb{Q}(\sqrt{2})$ is the set of all numbers of the form

$$\pm(\sqrt{2}+1)^n$$

for n an arbitrary integer.

Units and SICs

Let $D_{j,k}$ be the Weyl-Heisenberg displacement operators and Π a SIC-fiducial. Then

$$\mathrm{Tr}(D_{j,k}\Pi) = \begin{cases} 1 & j = k = 0 \\ \frac{e^{i\theta_{j,k}}}{\sqrt{d+1}} & \text{otherwise} \end{cases}$$

where the $e^{i\theta_{j,k}}$ are phases. It turns out that they are units, in every case examined.

Units and SICs (2)

Let V be the group generated by the SIC phases, and let U be the set of *all* units which also happen to be phases. Then it turns out, in the 7 cases where we have been able to calculate the full unit group[8], that either

$$U = V,$$

or else

$$U = V \oplus V_c,$$

where V_c is another sub-group having the same rank.
There are indications that the same is true in the cases where we haven't been able to calculate the full unit group.

[8] Calculating the full unit group is impracticable once the degree gets at all large. Interestingly this is another case where there is a quantum algorithm giving an exponential speed-up.

Units and SICs (2)

We used the program *Magma* to calculate the unit group. *Magma* doesn't return an arbitrary set of generators, but a very special set which is LLL reduced.

It turns out (in the 7 cases examined) that the SIC phases have extremely simple expressions in terms of the set of generators *Magma* returns. Indeed, in some cases they are in the set.

This is one of several features suggesting that the SIC phases may be a very special set of numbers. Perhaps the numbers which play the same role for ray class fields over a real quadratic field that the numbers $e^{\frac{2\pi i}{n}}$ do for cyclotomic fields.

Hilbert again

It has occurred to many people that SIC existence might possibly boil down to a set of identities involving special functions[9]

These considerations give some added interest to that idea. If you could find such a set of identities you would not have solved a Hilbert problem (because minimal SICs don't generate the full set of ray class fields). But it would certainly make the algebraic number theorists prick up their ears.

[9] See, for instance, G. S. Kopp, "Indefinite Theta Functions and Zeta Functions," PhD thesis, University of Michigan (2017).