On the structure of SIC-POVMs

Jon Yard

Institute for Quantum Computing
Department of Combinatorics and Optimization
University of Waterloo
Perimeter Institute for Theoretical Physics
Waterloo, ON N2L 3G1, CANADA

July 7, 2023

Abstract

We consider the set of SIC-POVM fiducial projectors, by definition points in projective Hilbert space $\mathbb{CP}^{N-1}$ whose orbits under a finite Heisenberg group extension of $(\mathbb{Z}/N)^2$ span a maximal set of complex equiangular lines. We show that the set of complexified SIC-POVM fiducials is a closed subscheme of the scheme $\mathbb{P}_{\mathbb{Q}}^{N-1} \times_{\mathbb{Q}} \mathbb{P}_{\mathbb{Q}}^{N-1}$ of rank-1 $N \times N$ matrices and conjecture that the set of fiducials is a closed subscheme of $\mathbb{P}_K^{N-1}$ defined over $K = \mathbb{Q}(\sqrt{(N-3)(N+1)})$, which is real quadratic for $N \geq 4$. The closed points of these schemes are in 1-1 correspondence with Galois orbits of fiducials, and their $(\mathbb{Z}/N)^2$-orbifolds can be identified with sets of SIC-POVMs. We explore algebraic and geometric aspects of the defining equations as well as of the solutions, in terms of class fields of K.

1 Introduction

2 Polynomial functions on projective space

Let $\mathbb{Q}[z]$ be the graded $\mathbb{Q}$-algebra of polynomials in $z = (z_0, \ldots, z_{N-1})$ and let $\mathbb{P}_{\mathbb{Q}}^{N-1} = \mathrm{Proj}(\mathbb{Q}[z])$ be projective space defined over $\mathbb{Q}$. Then $\mathbb{Q}[z]_n = H^0(\mathbb{P}_{\mathbb{Q}}^{N-1}, \mathcal{O}(n))$, where $\mathcal{O}(n) = \mathcal{O}(1)^{\otimes n}$ and where $\mathcal{O}(1)$ is Serre's twisting sheaf, the canonical generator of $\mathrm{Pic}(\mathbb{P}_{\mathbb{Q}}^{N-1})$. The group $(\mathbb{Z}/N)^2$ acts on $\mathbb{P}_{\mathbb{Q}(\zeta_N)}^{N-1}$ by a finite Heisenberg group.

The Cartesian product

$$R = \mathbb{Q}[z] \times_{\mathbb{Q}} \mathbb{Q}[\bar{z}] = \mathbb{Q}[z, \bar{z}]_{\bullet,0,\bullet}$$

is the graded $\mathbb{Q}$-algebra with $R_n = \mathbb{Q}[z]_n \otimes_{\mathbb{Q}} \mathbb{Q}[\bar{z}]_n$. Then $\mathrm{Proj}(R) = \mathbb{P}_{\mathbb{Q}}^{N-1} \times_{\mathbb{Q}} \mathbb{P}_{\mathbb{Q}}^{N-1}$ is the product of projective spaces defined over $\mathbb{Q}$.

Let $\Delta = \sum_i \frac{d^2}{dz_i d\bar{z}_i} : R_n \to R_{n-1}$ be the Laplacian and let $H_n = \ker \Delta|_{R_n}$ be the subspace of harmonic polynomials. Then

$$R_n = H_n + \|z\|^2 H_{n-1} + \cdots + \mathbb{Q}\|z\|^{2n}$$

for all $n \geq 0$.

Acting by translation on the ring $R_{\mathbb{Q}(\zeta_N)}$, $(\mathbb{Z}/N)^2$ preserves the harmonic polynomials, hence the grading. Furthermore, the $(\mathbb{Z}/N)^2$-invariants are defined over $\mathbb{Q}$, so that

$$R_{\mathbb{Q}(\zeta_N)}^{(\mathbb{Z}/N)^2} = (R^{(\mathbb{Z}/N)^2})_{\mathbb{Q}(\zeta_N)}.$$

Because $H_1^{(\mathbb{Z}/N)^2} = 0$, the graded $\mathbb{Q}$-algebra $R^{(\mathbb{Z}/N)^2}$ of $(\mathbb{Z}/N)^2$-invariants therefore satisfies

$$R_n^{(\mathbb{Z}/N)^2} = H_n^{(\mathbb{Z}/N)^2} + \|z\|^2 H_{n-1}^{(\mathbb{Z}/N)^2} + \cdots + \|z\|^{2n-4} H_2^{(\mathbb{Z}/N)^2} + 0 + \mathbb{Q}\|z\|^{2n}.$$

Consider the projective scheme $\mathcal{F} = \operatorname{Proj}(R/RH_2^{(\mathbb{Z}/N)^2})$ and its quotient $\mathcal{F}/(\mathbb{Z}/N)^2 = \operatorname{Proj}(R^{(\mathbb{Z}/N)^2}/R^{(\mathbb{Z}/N)^2}H_2^{(\mathbb{Z}/N)^2})$. When $N \neq 3$, the closed points of

$$\mathcal{F}' = \operatorname{Spec}(R/(RH_2^{(\mathbb{Z}/N)^2} + R(\|z\|^2 - 1)) \simeq \operatorname{Spec}(R/RH_2^{(\mathbb{Z}/N)^2}) \setminus \{(0), (\|z\|^2)\}$$

are in bijection with $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of fiducials.

For each extension field $F/\mathbb{Q}$, the set $\mathbb{P}_{\mathbb{Q}}^{N-1}(F)$ of F-valued points $\operatorname{Spec}(F) \to \mathbb{P}_{\mathbb{Q}}^{N-1}$ is in bijection with the usual projective space $F\mathbb{P}^{N-1}$ of lines through the origin in F^N. The closed points are the maximal relevant homogeneous ideals; they are in bijection with the set $\mathbb{P}_{\mathbb{Q}}^{N-1}(\overline{\mathbb{Q}})/\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of Galois orbits and take the form

$$\mathbb{Q}[z] \cap \left(\sum_{\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} \mathfrak{m}_a^\sigma \right),$$

with $a \in \overline{\mathbb{Q}}^N$ and $\mathfrak{m}_a = (z_i a_j - z_j a_i : 0 \leq i < j < N)$. We identify the set $(\mathbb{P}_{\mathbb{Q}}^{N-1} \times_{\mathbb{Q}} \mathbb{P}_{\mathbb{Q}}^{N-1})(F)$ of F-valued points with the space of rank-1 matrices in $F^{N \times N}$.

The isomorphism theorem gives a bijection $I \mapsto I/R^G H_2^G$ from the set of intermediate ideals $R^G H_2^G \subset I \subset R^G$ to the set of ideals of $R^G/R^G H_2^G$. This bijection takes the irrelevant ideal R_+^G (for which $R^G = \mathbb{Q} + R_+^G$) to the ideal $R_+^G/R^G H^G = (R^G/R^G H^G)_+$ (for which $R^G/R^G H^G = \mathbb{Q} + (R^G/R^G H^G)_+$). We have

$$\operatorname{Proj}(R^G/R^G H_2^G) \simeq \{\text{homogeneous prime ideals } \mathfrak{p} \subset R^G, H_2^G \subset \mathfrak{p}, (R^G H_2^G)_+ \not\subset \mathfrak{p}\}$$

and there exists a SIC iff there exists a $\mathfrak{p} \in \operatorname{Proj}(R^G/R^G H_2^G)$ with $R^G/(R^G H_2^G + R^G(\|z\|_2^2 - 1))$.

If I is a homogeneous ideal of a graded ring S, we may define its **saturation**

$$I_{\text{sat}} = (I : S_+^\infty) = \bigcup_n (I : S_+^n) = \{f \in S : S_+^n f \subset I \text{ for some } n\}.$$

Then $Z(I_{\text{sat}})$ is the Zariski closure of $\overline{Z(I) \smallsetminus Z(S_+)}$. Then $R_+^G \notin (R^G H_2^G)_{\text{sat}}$ is a necessary condition for the existence of a Heisenberg-covariant SIC. We have $\dim(R) = \dim(R^G) = 2N$. In fact,

$$R^G = \bigoplus_{i=1}^{D/2} \eta_i \mathbb{Q}[z_i \bar{z}_j : 0 \leq j - i \leq 1].$$

If N is odd, then

$$\begin{aligned} \dim(R_2^G) &= \left(\frac{N+1}{2}\right)^2 \\ \dim(H_2^G) &= \dim(R_2^G) - 1 = \frac{(N+3)(N-1)}{4} = \frac{(N-3)(N+1)}{4} + N \end{aligned}$$

2.1 Closed points of schemes

If F/k is an extension of rings, the F-valued points of $\text{Proj}(R)$ can locally be described as homomorphisms $\phi : \mathcal{O}(U) \to F$ taking $f/g \in \mathcal{O}(U)$ (so f, g homogeneous of the same degree and g nowhere vanishing on U) to $\phi(f/g) = f(u,v)/g(u,v) \in F$, where $[u \otimes v] \in U$. If F has an involution extending that of k, the F-valued points of $(\mathbb{P}_k^{d-1})_{k'}$ correspond to the maps $\phi : \mathcal{O}(U) \to F$ that are equivariant with respect to the involutions, i.e. $\phi(\bar{f}/\bar{g}) = \overline{\phi(f/g)}$ for all $f/g \in \mathcal{O}(U)$.

The image of the embedding of $(\mathbb{P}_k^{d-1})_{k'}$ is contained in a specific affine patch of $\text{Proj}(R)$, constrasting the lack of an affine embedding of $\mathbb{P}_k^{d-1}$ over k. Let $\alpha_0 := \sum_a z_a \bar{z}_a \in R_1$ and note that it does not vanish on $(\mathbb{P}_k^{d-1})_{k'}$. Hence $(\mathbb{P}_k^{d-1})_{k'}$ is contained in the basic open set $D(\alpha_0) = \{[v \otimes w] : v \cdot w \neq 0\} \subset \text{Proj}(R)$, which we identify with the space of $k^\times$-orbits of all rank-1 matrices over k with nonvanishing trace. Furthermore, $D(\alpha_0)$ is in bijection with the closed subset $V(\alpha_0 - 1)$ of the affine cone $\text{Spec}(R)$ of $\text{Proj}(R)$, which we identify with the set of all rank-1 matrices over k with unit trace. Note that $R_+ \notin V(\alpha_0 - 1)$, so it is only inhomogeneity keeping it from being a subset of $\text{Proj}(R)$. Viewed as a subset of $V(\alpha_0 - 1)$, $(\mathbb{P}_k^{d-1})_{k'}$ is therefore identified with the set of rank-1 Hermitian projections. Taking $k/k' = \mathbb{C}/\mathbb{R}$ gives the usual setting, but the algebraic nature of the solutions requires this more general approach. Not sure if I'm saying this completely right (see Vakil 4.5.1, 8.2.12). There is a natural morphism $\text{Spec}(R) \smallsetminus V(R_+) \to \text{Proj}(R)$ corresponding to discarding the origin.

2.2 Schemes of finite type

A morphism $f : X \to Y$ of schemes is of **finite type at** $x \in X$ if there are open affine $x \ni U \subset X$ and $V \subset Y$ such that the corresponding ring homomorphism $f^\natural : \mathcal{O}_Y(V) \to \mathcal{O}_X(U)$ is of finite type, i.e. factors through the natural map $\mathcal{O}_Y(V) \to \mathcal{O}_Y(V)[t_1, \ldots, t_n]$ for some n. A morphism $f : X \to Y$ of schemes is **locally of finite type** if it is of finite type at each $x \in X$ and is **finite type** if it is locally of finite type and **quasicompact** (i.e. every open cover has a finite subcover - whereas **compact** means quasicompact and Hausdorff).

If X is locally of finite type over a field k (i.e. the structure morphism $X \to \operatorname{Spec}(k)$ is of finite type), then the closed points are in bijection with $X(\overline{k}) / \operatorname{Gal}(\overline{k}/k)$.

The closed sets in the Zariski topology are the affine subschemes. The components are clopen, and clopens are unions of components.

3 Polynomial functions on matrices

Let X be a $d \times d$ matrix of algebraically independent indeterminates and consider the polynomial ring $\mathbb{Q}[X]$ in the matrix entries. As a $\mathrm{GL}_N(\mathbb{Q}) \times \mathrm{GL}_N(\mathbb{Q})$-module, it decomposes as a direct sum

$$\mathbb{Q}[X] \simeq \bigoplus_{\lambda} M_\lambda$$

over all Young diagrams λ with at most N rows, where M_λ is the span, over all pairs s, t of semistandard tableaux of shape λ, of the products

$$m_{s,t} = \prod_{i=1}^{N} \det(X_{s_i t_i})$$

of the minors specified by the entries of the rows s_i, t_i. The ring $\mathbb{Q}[X]$ is $\mathbb{Z} \times \mathbb{Z}/N$-graded, with $\deg(X_{ab}) = (1, a-b)$. The natural map $\mathbb{Q}[X] \to R$ taking $f(X) \mapsto f(z, \bar{z}) := f(z\bar{z}^T)$ preserves the $\mathbb{Z} \times \mathbb{Z}/N$-grading, where $\deg(z_i) = (1, i)$ and $\deg(\bar{z}_i) = (1, -i)$.

The kernel of the natural map $\mathbb{Q}[X] \to R$ is the determinantal ideal $\mathcal{I}_2 \subset \mathbb{Q}[X]$ generated by the 2×2 minors

$$m_{j,\ell} = \det\begin{pmatrix} X_{j_1\ell_1} & X_{j_1\ell_2} \\ X_{j_2\ell_1} & X_{j_2\ell_2} \end{pmatrix} = X_{j_1\ell_1}X_{j_2\ell_2} - X_{j_1\ell_2}X_{j_2\ell_1}$$

of X for $j_1 < j_2$, $\ell_1 < \ell_2$, i.e. over pairs $\begin{array}{|c|}\hline j_1 \\ \hline j_2 \\ \hline \end{array}$ and $\begin{array}{|c|}\hline k_1 \\ \hline k_2 \\ \hline \end{array}$ of semistandard tableaux of shape $\begin{array}{|c|}\hline \\ \hline \\ \hline \end{array}$. The ideal $\mathcal{I}_2$ is prime and $\mathrm{GL}_N(\mathbb{Q}) \times \mathrm{GL}_N(\mathbb{Q})$-invariant, hence a module, known to decompose as

$$\mathcal{I}_2 = \bigoplus_{\lambda \supset \begin{array}{|c|}\hline \\ \hline \\ \hline \end{array}} M_\lambda$$

so that only single-row diagrams remain in the quotient

$$\mathbb{Q}[X]/I_2 \simeq \bigoplus_{n} M_{[n]} \simeq R.$$

Extending scalars to $\mathbb{Q}(\zeta_{2N})$, the ring $\mathbb{Q}[X]_{\mathbb{Q}(\zeta_{2N})}$ is generated by the linear forms

$$\alpha_j(X) = \langle \Delta_j, X \rangle = (-\zeta_{2N})^{j_1 j_2} \sum_a \zeta_d^{j_2 a} X_{a,a+j_1} \in \left(\mathbb{Q}[X]_{\mathbb{Q}(\zeta_{2N})}\right)_1,$$

for which

$$\alpha_j(X^\dagger) = \operatorname{Tr} \Delta_{-j} X^\dagger = \operatorname{Tr}(\Delta_j X)^\dagger = \overline{\operatorname{Tr} \Delta_j X} = \overline{\alpha_{-j}(X)}.$$

In particular, $\alpha_{-j}(X) = \overline{\alpha_j(X)}$ iff X is Hermitian.

The $\alpha_j(X)$ form a basis for $(\mathbb{Q}[X]_1)_{\mathbb{Q}(\zeta_{2N})}$ and generate $\mathbb{Q}[X]_{\mathbb{Q}(\zeta_{2N})}$ in degree 1, i.e.

$$\mathbb{Q}(\zeta_{2N})[X] = \mathbb{Q}(\zeta_{2N})[\alpha(X)].$$

The ring $\mathbb{Q}[X]_{\mathbb{Q}(\zeta_{2N})}$ is $\mathbb{Z} \times (\mathbb{Z}/N)^2$-graded with $\deg(\alpha_j(X)) = (1, j)$. When N is odd, $\mathbb{Q}[X]_{n,j}$ is spanned by the products $\alpha_J(X) = \alpha_{j_1}(X) \cdots \alpha_{j_n}(X)$ with $j_1 + \cdots + j_n = j$.

It is interesting to note that if we identify $(\mathbb{Z}/N)^2$ with the N-torsion $E[N]$ of a complex elliptic curve, then $\mathbb{Q}[X]_n^{(\mathbb{Z}/N)^2} = \mathbb{Q}[X]_{n,0}$ is spanned by α_J for positive degree-n divisors J on $E[N]$ in the kernel of the Abel-Jacobi map $\mathrm{Div}(E) \to E$.

The natural map $\mathbb{Q}[X]_{\mathbb{Q}(\zeta_{2N})} \to R_{\mathbb{Q}(\zeta_{2N})}$ takes $f(X)$ to $f(z,\bar{z}) = f(zz^\dagger)$. For instance, $\alpha_j(X)$ is mapped to

$$\alpha_j(z,\bar{z}) = (-\zeta_{2N})^{j_1 j_2} \sum_k \zeta_d^{j_2 k} z_k \bar{z}_{k+j_1},$$

providing a $\mathbb{Z} \times (\mathbb{Z}/N)^2$-graded with with $\deg(\alpha_j(z,\bar{z})) = (1,j)$. In particular, $R_{\mathbb{Q}(\zeta_{2N})} = \mathbb{Q}(\zeta_{2N})[\alpha(z,\bar{z})]$ is generated in degree 1.

The determinantal ideal remains prime after extending scalars to $\mathbb{Q}(\zeta_{2N})$ and can also be generated by the polynomials

$$\alpha_j(X)\alpha_k(X) - \frac{1}{d}\sum_\ell (-\zeta_{2N})^{[\ell,j-k]}\alpha_{j+\ell}(X)\alpha_{k-\ell}(X) \in \mathbb{Q}[X]_{2,j+k}$$

for $j,k \in (\mathbb{Z}/N)^2$.

Note that if f is a function on subsets of $\mathbb{CP}^{N-1}$ and S is a $(\mathbb{Z}/N)^2$-invariant subset, then $f(S) = f^{(\mathbb{Z}/N)^2}(S)$, where $f \mapsto f^{(\mathbb{Z}/N)^2}$ denotes the Reynolds operator = projection onto the subspace of $(\mathbb{Z}/N)^2$-invariant functions. The invariant subring $R^{(\mathbb{Z}/N)^2}$ can be interpreted as image of R under the Reynolds operator.

3.1 Quadratic invariants

Let

$$\beta_j(X) := \alpha_j(X)\alpha_{-j}(X) = \mathrm{Tr}(\Delta_j \otimes \Delta_{-j})(X \otimes X) = \sum_{ab} \zeta_N^{j_2(j_1+a-b)} X_{a,a+j_1} X_{b,b-j_2}.$$

The $\beta_j(X)$ are $(\mathbb{Z}/N)^2$-invariant, i.e $\beta_j(\Delta_k X \Delta_{-k}) = \beta_j(X)$. They also satisfy $\beta_j(X) = \beta_{-j}(X)$. They are otherwise distinct, labeled by the orbits of $(\mathbb{Z}/N)^2/\langle -I\rangle$. Via the Weil representation of $\mathrm{Aut}_0(\mathrm{Heis}((\mathbb{Z}/N)^2))$, the $\beta_j(X)$ carry a representation of $\mathrm{SL}_2(N)$ acting as $g \cdot \beta_j(X) = \beta g j(X)$ and factoring through $\mathrm{PSL}_2(N)$.

If N is odd, then $j = 0$ is the only fixed point of $-I$, so the number of orbits is equal to

$$1 + \frac{N^2-1}{2} = \frac{N^2+1}{2} = \dim \mathbb{Q}[X]_2^G = \dim \mathbb{Q}[X]_{\square\square}^G + \dim \mathbb{Q}[X]_{\substack{\square\\\square}}^{(\mathbb{Z}/N)^2} = \left(\frac{N+1}{2}\right)^2 + \left(\frac{N-1}{2}\right)^2.$$

If N is even, $-I$ has the 4 fixed points $j = 0, (0,N/2), (N/2,0), (N/2,N/2)$, so there are

$$4+\frac{N^2-4}{2} = \frac{N^2+4}{2} = \dim \mathbb{Q}[X]_2^{(\mathbb{Z}/N)^2} = \dim \mathbb{Q}[X]_{\square\square}^{(\mathbb{Z}/N)^2} + \dim \mathbb{Q}[X]_{\substack{\square\\\square}}^{(\mathbb{Z}/N)^2} = \left(\frac{N+2}{2}\right)^2 + \left(\frac{N-2}{2}\right)^2$$

orbits. In each case, the $\beta_j(X)$ span $\mathbb{Q}[X]_2^{(\mathbb{Z}/N)^2}$.

Let $'$ be the map on $\mathbb{Q}[X]_2$ acting as the identity on $\mathbb{Q}[X]_{\square\square}^G$ and minus the identity on on $\mathbb{Q}[X]_{\substack{\square\\\square}}^{(\mathbb{Z}/N)^2}$. It commutes with the action of $(\mathbb{Z}/N)^2$ and acts on monomials as $(X_{ab}X_{cd})' = X_{ad}X_{bc}$. In particular,

$$\beta_0(X) = \mathrm{Tr}(X)^2 \text{ and } \beta_0'(X) = \mathrm{Tr}(X^2).$$

Extend the Laplacian Δ to $\mathbb{Q}[X]$ via

$$\Delta = \sum_a \frac{d}{dX_{aa}}.$$

If $f_M(X) = \operatorname{Tr} X^{\otimes n} M \in \mathbb{Q}[X]_n$ for $M \in \operatorname{Sym}^n\big(\mathbb{Q}^{N\times N}\big)$, then $\Delta f_M(X) = f_{\operatorname{Tr}_1 M}(X) \in \mathbb{Q}[X]_{n-1}$. Then $\mathcal{H}_2^{\pm} = \ker \Delta|_{\mathbb{Q}[X]_2^{\pm}}$, whereas there is only a proper inclusion $\mathcal{H}_2 \subset \ker \Delta|_{\mathbb{Q}[X]_2}$ because $\Delta(\mathbb{Q}[X]_2) = \mathbb{Q}[X]_1$.

Define

$$\begin{aligned} \beta_j^{\pm}(X) &:= \frac{\beta_j(X) \pm \beta_j'(X)}{2} \\ &= \langle P_{\pm}(\Delta_j \otimes \Delta_{-j})P_{\pm}, X \otimes X\rangle \\ &= \frac{\operatorname{Tr}(\Delta_j \otimes \Delta_{-j})(X \otimes X) \pm \operatorname{Tr}(\Delta_j \otimes \Delta_{-j})S(X \otimes X)}{2}, \end{aligned}$$

noting that

$$\beta_j(X) = \beta_j^+(X) + \beta_j^-(X) \text{ and } \beta_j'(X) = \beta_j^+(X) - \beta_j^-(X).$$

Then the $\beta_j^+(X)$ span $\mathbb{Q}[X]_{2,0}^+$ and the $\beta_j^-(X)$ span $\mathbb{Q}[X]_{2,0}^-$ because $\widetilde{\beta}_{aa}^-(X) = 0$ for all a (prove it). Furthermore,

$$\Delta\beta_j(X) = \delta_j 2d\alpha_0(X) \text{ and } \Delta\beta_j'(X) = 2\alpha_0(X), \text{ so } \Delta\beta_j^{\pm}(X) = (d\delta_j \pm 1)\alpha_0(X).$$

Bases for $\mathcal{H}_{2,0}^{\pm}$, can be obtained from the $\beta_j^{\pm}(X)$ by projecting out the non-harmonic parts. giving

$$\widetilde{\beta}_j^{\pm}(X) = \beta_j^{\pm}(X) - \frac{d\delta_j \pm 1}{d \pm 1}\beta_0^{\pm}(X).$$

The projections $\widetilde{\beta}_j(X)$ of the $\beta_j(X)$ onto $\mathcal{H}_{2,0}$ are therefore

$$\widetilde{\beta}_j(X) \quad = \quad \beta_j(X) - \frac{d\delta_j + 1}{d+1}\beta_0^+(X) - \frac{d\delta_j - 1}{d-1}\beta_0^-(X) = (1-\delta_j)\left(\beta_j(X) + \frac{\beta_0(X) - d\beta_0'(X)}{d^2-1}\right).$$

A Fourier transform in j_2 gives new coordinates

$$f_j(X) = \frac{1}{N}\sum_b \zeta_d^{j_2 b}\beta_{j_1 b}(X) = \sum_a X_{a,a+j_1}X_{a+j_1+j_2,a+j_2}$$

satisfying

$$f_j'(X) \quad = \quad \sum_a X_{a,a+j_2}X_{a+j_1+j_2,a+j_1} = f_{wj},$$

where $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Let $f_j^{\pm}(X) = \frac{f_j(X) \pm f_w j(X)}{2}$. Then

$$f_{-j}(X) = f_j(X), \;\; \Delta f_j = 2\delta_{j_1}\alpha_0(X), \;\; \Delta f_j'(X) = 2\delta_{j_2}\alpha_0(X) \text{ and } \Delta f_j^{\pm}(X) = (\pm\delta_{j_1} + \delta_{j_2})\alpha_0(X).$$

Therefore,

$$\widetilde{f}_j^{\pm}(X) = f_j^{\pm}(X) + \frac{\pm\delta_{j_1} - \delta_{j_2}}{d \pm 1}\beta_0^{\pm}(X).$$

When N is odd, a complete set of representatives for the $f_j^+(X)$ is given by the "forward lightcone"

$$\left\{ j : 0 \leq j_1 \leq \frac{N-1}{2}, |j_2| \leq j_1 \right\}$$

and a complete set for the $f_j^-(X)$ is given by the "spacelike" interior

$$\left\{ j : 0 \leq j_1 \leq \frac{N-1}{2}, |j_2| < j_1 \right\}$$

(a picture will do it justice). The projections onto $\mathcal{H}_{2,0}$ are given by

$$\widetilde{f}_j^\pm(X) = f_j^\pm(X) - \frac{\delta_{j_1} \pm \delta_{j_2}}{N \pm 1} \beta_0^\pm(X), \;\; \widetilde{f}_j(X) = f_j(X) - \frac{N\delta_{j_1} - \delta_{j_2}}{N^2 - 1} \beta_0(X) - \frac{-\delta_{j_1} + N\delta_{j_2}}{N^2 - 1} \beta_0'(X).$$

The $f_j^+(X)$, for j in the forward lightcone, are a basis for $\mathbb{Q}[X]_{2,0}^+$, while the $f_j^-(X)$, for j in the interior, are a basis for the $\mathbb{Q}[X]_{2,0}^-$. The "light-like" j, with $j_1 + j_2 = 0$ or $j_1 - j_2 = 0$, satisfy $f_j(X) = f_j^+(X)$, and therefore $f_j^-(X) = 0$. I would like to believe that they form a basis for $\mathcal{P}_0$ but I'm not so sure after the Fourier transform. More likely that the $\beta_{aa}^+(X)$ span $\mathcal{P}_0$, with $\widetilde{\mathcal{P}}_0$ spanned by the ones with $a \neq 0$ and $\beta_0^+(X)$ transforming trivially.

Then

$$\mathbb{Q}[X]_{2,0} = k\beta_0^+(X) + \mathcal{H}_{2,0}^+ + k\beta_0^-(X) + \mathcal{H}_{2,0}^-,$$

where $\mathcal{H}_{2,0}^\pm$ is the span of the $\widetilde{\beta}_j^\pm(X)$ or $\widetilde{f}_j^\pm(X)$.

Then $\mathcal{H}_{2,0} := \mathcal{H}_{2,0}^+ + \mathcal{H}_{2,0}^-$ are equations for the $(\mathbb{Z}/N)^2$-orbit of X to be a 2-design. Furthermore, I conjecture that the equation $\beta_0^-(X) = 0$ is all that is needed to get SICs. As this could generate a non-saturated ideal, we need to consider its saturation. This could easily be checked: Let $J = \mathbb{Q}[X]\mathcal{H}_{2,0} + \mathbb{Q}[X]B_0^-$. Is $I \subset J$? Do we have $I^p \subset J$ for sufficiently large $p > 1$, and if so, how large?. The primary decompositions of the ideals I^p of higher-order vanishing are known [**DEP80**].

Suppose k is a number field. Then we expect that $RH_{2,0}$ is a 0-dimensional ideal carrying a $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$-action. Furthermore, $R/RH_{2,0}$ is a k-algebra of degree $2N^2s$, where s is the number of SICs. When k contains the ring-ray class field $F = K^{d\mathcal{O}_D\infty}$, then $R/RH_{2,0} \simeq F^{2N^2s}$. On the other hand, $R^{(\mathbb{Z}/N)^2}/R^{(\mathbb{Z}/N)^2}H_{2,0}$ will be a k-algebra of degree $2N$. If k is contained in F, the components of $\mathrm{Proj}(R/RH_{2,0})$ are $\mathrm{Gal}(F/k)$-orbits of fiducials, and those of $\mathrm{Proj}(R^{(\mathbb{Z}/N)^2}/R^{(\mathbb{Z}/N)^2}H_{2,0})$ are $\mathrm{Gal}(F/k)$-orbits of SICs. In particular, the hermitian solutions decompose into $\mathrm{Gal}(F/K)$-orbits. It is this fact we would most like to explain, as it may provide the key to solving everything.

In degree-2, the determinantal ideal is $I_2 = M_{[1,1]}$. It is generated by the minors $M_{j,k}$, which are homogeneous of degree $(2, j+k)$.

Note that the dimension of $\mathbb{Q}[X]$ is d^2 and the dimension of R is $2N - 1$, so the dimension of I is $N^2 - 2N + 1 = (N-1)^2$. If N is odd, then

$$\dim \mathcal{H}_{2,0}^\pm = \left(\frac{N \pm 1}{2}\right)^2 - 1 = \frac{N^2 \pm 2N - 3}{4} = \frac{(N \pm 3)(N \mp 1)}{4}.$$

These sum to $(N^2-3)/2$.

Also note that $B_0^- = -B_0^+$ on the subspace of traceless matrices, where $B_0 = 0$.

Magma computes the dimension of the set of $(\mathbb{Z}/N)^2$-SICs (not necessarily of rank 1), for $N = 2, 3, 4, 5, 6, \ldots$ is $0, 4, 6, 12, 16, \ldots$. So far could check that $N = 3$ has 8 4-dimensional components, $d = 4$ has 12 6-dimensional components.

The real ones have dimension $0, 2, 3, 6, 7$. For $N = 7$, the real ones have dimension 12, the T_3-invariant ones have dimension 8, and the real T_3-invariant ones have dimension 4. Note that the real ones have dimension half the complex ones, except in $N = 6$. Could it always be half for prime powers? Actually still not sure if I am getting the general matrix polynomials right. Double check above formulas for the harmonic parts of the f_j.

3.2 Quadratic forms on endomorphisms

Assume N is odd. Let

$$U|i\rangle|j\rangle = \left|\frac{i+j}{2}\right\rangle\left|\frac{i-j}{2}\right\rangle, \quad U^\dagger|i\rangle|j\rangle = |i+j\rangle|i-j\rangle.$$

Then

$$\begin{aligned} U(X_d \otimes X_N)U^\dagger &= X_N \otimes I_V \\ U(Z_d \otimes Z_N)U^\dagger &= Z_N^2 \otimes I_V \\ U^\dagger(X_N \otimes X_N)U &= X_N^2 \otimes I_V \\ U^\dagger(Z_N \otimes Z_N)U &= Z_N \otimes I_V. \end{aligned}$$

Therefore,

$$\begin{aligned} U(\Delta_j \otimes \Delta_j)U^{-1} &= \Delta_{j_1,2j_2} \otimes I_V, \\ U\,\mathrm{Sym}^2(\Delta_j)U^\dagger &= \Delta_{j_1,2j_2} \otimes P_{V_+}, \\ U\Lambda^2(\Delta_j)U^\dagger &= \Delta_{j_1,2j_2} \otimes P_{V_-}. \end{aligned}$$

Note that $\zeta_N I$ acts as $\zeta_N^2 I$ (i.e. the central character is different).

Let $C = \left(\frac{-1}{d}\right)U_{-I} = (-1)^{\frac{d-1}{2}}U_{-I}$ be the unitary from the Weil representation, which acts as $C|i\rangle \mapsto |-i\rangle$, and write $C = P_{V_+} - P_{V_-}$. Let $S = P_{\mathrm{Sym}^2(V)} - P_{\Lambda^2(V)}$ be the swap, which satisfies $S|i\rangle|j\rangle = |j\rangle|i\rangle$. Then

$$\begin{aligned} USU^{-1} &= I_V \otimes C, \\ UP_{\mathrm{Sym}^2(V)}U^{-1} &= I_V \otimes P_{V_+}, \\ UP_{\mathrm{Sym}^2(V)}U^{-1} &= I_V \otimes P_{V_-}. \end{aligned}$$

Therefore,

$$\begin{aligned} \mathrm{Sym}^2(\mathrm{End}(V))^{(\mathbb{Z}/N)^2} &= U(I_V \otimes \mathrm{End}(V))U^{-1}, \\ \mathrm{End}(\mathrm{Sym}^2(V))^{(\mathbb{Z}/N)^2} &= U(I_V \otimes \mathrm{End}(V_+))U^{-1}, \\ \mathrm{End}(\Lambda^2(V))^{(\mathbb{Z}/N)^2} &= U(I_V \otimes \mathrm{End}(V_-))U^{-1}. \end{aligned}$$

In other words, an operator $B \in \mathrm{Sym}^2(\mathrm{End}(V))$ is $(\mathbb{Z}/N)^2$-invariant iff $B = U(I_V \otimes A)U^{-1}$ for some $A \in \mathrm{End}(V)$, with $B \in \mathrm{End}(\mathrm{Sym}^2(V))^{(\mathbb{Z}/N)^2}$ iff $A \in \mathrm{End}(V_+)$, and $B \in \mathrm{End}(\Lambda^2(V))^{(\mathbb{Z}/N)^2}$ iff $A \in \mathrm{End}(V_-)$.

On the other hand,

$$(U(X \otimes X)U^{-1})_{ij,k\ell} = \frac{X_{i+j,k+\ell}X_{i-j,k-\ell} + X_{i+j,k-\ell}X_{i-j,k+\ell}}{2} = z_{i+j}z_{i-j}\bar{z}_{k+\ell}\bar{z}_{k-\ell},$$

with the latter holding for rank-1 $X = zz^\dagger$. The corresponding polynomials

$$f_{U(I\otimes A)U^{-1}}(z, \bar{z}) = \sum_{i,j,\ell} A_{j,\ell} z_{i+j}z_{i-j}\bar{z}_{i+\ell}\bar{z}_{i-\ell}$$

are also $(\mathbb{Z}/N)^2$-invariant. Under the Weil representation, $\left(\begin{pmatrix} a & \\ & a^{-1}\end{pmatrix} \cdot A\right)_{j,\ell} = A_{aj,a\ell}$ (or a^{-1}?). So it turns out

$$f_{U(I\otimes|j_1\rangle\langle j_2|)U^{-1}}(z, \bar{z}) = f_j(z, \bar{z})???$$

Under the action $g \cdot A = (g \otimes g)A(g^\dagger \otimes g^\dagger)$, we have the decomposition into irreducible representations of $\mathrm{GL}(V)$:

$$\begin{aligned}
\mathrm{Sym}^2(\mathrm{End}(V)) &\simeq_{\mathrm{GL}(V)} \mathrm{End}(\mathrm{Sym}^2(V)) \oplus \mathrm{End}(\Lambda^2(V)) \\
W\,\mathrm{Sym}^2(\mathrm{End}(V))W^\dagger &\simeq_{\mathrm{GL}(V)} (\mathrm{End}(V) \otimes \mathrm{End}(V_+)) \oplus (\mathrm{End}(V) \otimes \mathrm{End}(V_-))
\end{aligned}$$

Under $\mathrm{U}(V)$, these decompose further into irreducible representations

$$\begin{aligned}
\mathrm{End}(\mathrm{Sym}^2(V)) &\simeq_{U(V)} \mathbb{C}P_+ + \mathrm{Ad}_+(V) + \mathrm{Sym}^{2,2}(V) \\
\mathrm{End}(\Lambda^2(V)) &\simeq_{U(V)} \mathbb{C}P_- + \mathrm{Ad}_-(V) + \Lambda^{2,2}(V),
\end{aligned}$$

where

$$\begin{aligned}
\mathrm{Ad}_+(V) &= \mathfrak{sl}(V) \otimes P_{V_+} \\
\mathrm{Ad}_-(V) &= \mathfrak{sl}(V) \otimes P_{V_-} \\
\mathrm{Sym}^{2,2}(V) &= \mathfrak{gl}(V) \otimes \mathfrak{sl}(V_+) \\
\Lambda^{2,2}(V) &= \mathfrak{gl}(V) \otimes \mathfrak{sl}(V_-).
\end{aligned}$$

Question: Is $\mathrm{Tr}_{V_+\oplus V_-} WAW^\dagger = \mathrm{Tr}_1 A = \mathrm{Tr}_2 A$ for all $A \in \mathrm{Sym}^2(\mathrm{End}(V))$? Also, a general degree-2 polynomial function on $\mathbb{P}^{d-1}(\mathbb{C})$ has the form

$$f_A(z, \bar{z}) = \sum_{ijkl} \bar{z}_i\bar{z}_j A_{ij,kl} z_k z_l = \langle z|\langle z|A|z\rangle|z\rangle,$$

where $A_{ij,kl}$ is symmetric under the interchanges $i \leftrightarrow j$, $k \leftrightarrow l$, i.e. $A \in \mathrm{End}(\mathrm{Sym}^2 V)$. In terms of $P = |z\rangle\langle z|$,

$$f_A(P) = \mathrm{Tr}\, A(P \otimes P) = \langle A, P \otimes P\rangle.$$

The harmonic functions in $\mathrm{End}(\mathrm{Sym}^2(V))$ are the kernel of the Laplacian

$$\frac{d^2}{dzd\bar{z}} = \sum_i \frac{d^2}{dz_i d\bar{z}_i}.$$

Show that $\frac{d^2}{dzd\bar{z}} f_A(z) = f_{\mathrm{Tr}_1 A}(z)$, where for $B \in \mathrm{End}(V)$, $f_B(z) = \sum_{ij} \bar{z}_i B_{ij} z_j = \langle z|B|z\rangle$.

3.3 Decoupling?

Recall the super old idea of finding a $|\psi\rangle^V$ such that $W|\psi\rangle^V|\psi\rangle^V = |\Phi\rangle^{VV_+}$, with Φ^{V_+} maximally mixed. So fiducials are somehow equivalent to isometric encodings $U : V_+ \hookrightarrow V$ under which W^{-1} completely disentangle the maximally entangled state $|\Phi\rangle^{V_+V_+}$, in the sense that $W^{-1}(U \otimes I_{V_+})|\Phi\rangle^{V_+V_+}$ is a product.

Can I somehow introduce a third system and instead try to show that V_+ is decoupled from that system? Maybe embed $\mathrm{Sym}^2(V)$ into $V \otimes V_+ \otimes \mathbb{C}^2$ by identifying V_- with a subspace of V_+, i.e. $V_+ \simeq V_+ \otimes |0\rangle$ and $V_- \hookrightarrow V_+ \otimes |1\rangle$.

3.4 $(\mathbb{Z}/N)^2$-invariant polynomial functions

The $(\mathbb{Z}/N)^2$-invariant subrings $\mathbb{Q}[X]^{(\mathbb{Z}/N)^2} = \mathbb{Q}[X]_{\cdot,0}$ and $R^{(\mathbb{Z}/N)^2} = R_{\cdot,0}$ are defined over $\mathbb{Q}$. We have

$$R_n^{(\mathbb{Z}/N)^2} = k\alpha_0^n + 0 + \alpha_0^{n-2}H_2^{(\mathbb{Z}/N)^2} + \alpha_0^3 H_3^{(\mathbb{Z}/N)^2} + \cdots + \alpha_0 H_{n-1}^{(\mathbb{Z}/N)^2} + H_{n,0}$$

as $H_1^{(\mathbb{Z}/N)^2} = 0$. The polynomials from the introduction span the space $H := H_2^G$ of degree-$(2,2)$ harmonic $(\mathbb{Z}/N)^2$-invariant polynomials. In particular, H is defined over $\mathbb{Q}$.

Is this is a good place for extensive discussion about for the two dual problems these solve (equiangular lines and 2-designs)? Show how the equations for matrices differ by the swap, etc.

Better to first define the $\beta_j = \alpha_j\alpha_{-j}$. Equivalence follows from the following theorem:

Theorem 3.1. *The defining equations* $(N+1)\beta_j(z,\bar{z}) - \delta_{j_1+j_2}\beta_0(z,\bar{z})$ *for fiducials span* H.

If X is rank-1, the overlaps

$$\operatorname{Tr}\Delta_j X \Delta_{-j} X = \alpha_j(X)\alpha_{-j}(X) = \beta_j(X)$$

need to equal $\operatorname{Tr}(X)^2/(N+1)$.

Then $\mathbb{Q}[X]_2 \simeq R_2 + \mathcal{I}_2$, as $\mathcal{I}_2 \simeq M_{[1,1]}$, while $R_{2,0} \simeq k\alpha_0^2 + H_{2,0}$, we have something slightly different for $\mathbb{Q}[X]_{2,0}$.

A conjecture with a chance of holding for odd prime N: $R^{(\mathbb{Z}/N)^2}$ and $\mathbb{Q}[X]^{(\mathbb{Z}/N)^2}$ are generated by the monomials $\alpha_J := \prod_{j\in J}\alpha_j$, $A_J := \prod_{j\in J} A_j$, where $J \in G/T$ for some torus $T \subset \mathrm{SL}_2(N)$. General results from invariant theory show that these rings are finitely generated and Cohen-Macaulay (or does that imply the first?). Check notebook for specific calculations.

One more thing: The Abel-Jacobi map gives a nice way to organize the monomials for $R_{n,0}$ invariants using degree-n divisors on $E[N]$ in the kernel of the Abel-Jacobi map. Can I somehow state it as a theorem? What curve E???

It also turns out that $R^{(\mathbb{Z}/N)^2}$ and $\mathbb{Q}[X]^G$ are stable under the the $\mathrm{SL}_2(N)$-action, which factors through $\mathrm{PSL}_2(N)$.

Okay, note this. When $u_+ = u_f^2$, we have $\sqrt{N+1} = u_f^{3r} + u_f^{-3r}$.

3.5 $\mathbb{Q}[X]^{(\mathbb{Z}/N)^2}$

Let $F = \mathbb{Q}(\zeta_N)$ and let $\mathbb{Q}[X] = F[\alpha]$. For each $m \in \mathbb{N}^{N\times N}$, define the monomial

$$\alpha^m := \prod_{j\in(\mathbb{Z}/N)^2} \alpha_j^{m_j}.$$

Then $\mathbb{Q}[X]_{n,k}$ is spanned by monomials α^m with

$$\sum_{j\in(\mathbb{Z}/N)^2} m_j = n, \quad \sum_{j\in(\mathbb{Z}/N)^2} m_j \cdot j \equiv k \bmod N.$$

In particular, the invariant subring $\mathbb{Q}[X]^{(\mathbb{Z}/N)^2} = \mathbb{Q}[X]_{\bullet,0}$ is spanned by monomials α^m with m in the monoid

$$\mathcal{M} = \left\{ m \in \mathbb{N}^{N\times N} : \operatorname{Tr} m \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ N-1 & \cdots & N-1 \end{pmatrix}, \operatorname{Tr} m \begin{pmatrix} 0 & \cdots & N-1 \\ \vdots & & \vdots \\ 0 & \cdots & N-1 \end{pmatrix} \in N\mathbb{N} \right\}.$$

Let $\mathcal{H}$ be a Hilbert basis (generating set) for $\mathcal{M}$, so that $\mathbb{N}\mathcal{H} = \mathcal{M}$. Then the invariant subring $\mathbb{Q}[X]^{(\mathbb{Z}/N)^2}$ is generated by the α^m for $m \in \mathcal{H}$.

Suppose that N is an odd prime. Then $Q = \{\alpha_0\} \cup \{\alpha_j^N : j \neq 0\}$ is a set of quasigenerators of $\mathcal{M}$ with associated descent set $D(\mathcal{M}) = \{m \in \mathcal{F} : m_j < N \text{ for all } j\}$, so that $\mathcal{M} = \mathbb{N}Q + D(\mathcal{M})$. Then we have

$$\mathbb{Q}[X]^{(\mathbb{Z}/N)^2} = F[\alpha^{\mathcal{M}}] = F[\alpha^{\mathcal{H}}] = \bigoplus_{\mu\in D(\mathcal{F})} F[\alpha^Q]\alpha^\mu.$$

Actually this will work for all odd N. For even N it would work on $\left(\mathbb{Q}[X]^{(\mathbb{Z}/N)^2}\right)^{(2)}$ (keeping only even degrees), which for technical reasons could be better to work with in certain situations.

Given a torus $T \subset \mathrm{SL}_2(N)$ (N odd say), $\alpha^{Tj} = \prod_{t\in T\alpha_{tj}}$. I think that if $|T| = 3$ then $\alpha^{Tj} \in \mathbb{Q}[X]_3^{(\mathbb{Z}/N)^2}$ for all j but this should be checked. On the other hand, for $T = \langle t\rangle$ of order m, α^{Tj} has degree $j + tj + \cdots t^{m-1}j = (I + t + \cdots + t^{m-1})j = 0 \bmod N$ and is automatically $(\mathbb{Z}/N)^2$ invariant.

3.6 The ring generated by the overlaps

Our key tool will be to describe $\mathbb{Q}[\alpha]$ as a quotient of a polynomial ring. The idea is that if the α are coordinates in matrices, then no quotient is needed (as it is already a polynomial ring). It will be a quotient by a *determinantal ideal.* There is good discussion about these in Eisenbud (p. 106–108).

Here is the main idea for how to give explicit generators for the determinantal ideal. Let ρ be a $d \times d$ matrix of indeterminates. First note that

$$\alpha_j(\rho)\alpha_k(\rho) = \operatorname{Tr}\rho^{\otimes 2}\big(\Delta_{-j} \otimes \Delta_{-k}\big) = \frac{1}{2}\operatorname{Tr}\rho^{\otimes 2}\big(\Delta_{-j} \otimes \Delta_{-k} + \Delta_{-k} \otimes \Delta_{-j}\big).$$

Define

$$\gamma_{jk}(\rho) = \operatorname{Tr}\rho^{\otimes 2}\mathrm{SWAP}\Delta_{jk} = \operatorname{Tr}\rho\Delta_{-j}\rho\Delta_{-k},$$

as well as $\beta^{\pm}_{jk}(\rho) = \frac{1}{2}(\beta_{jk}(\rho) \pm \gamma_{jk}(\rho))$. The $\beta^{-}_{jk}(\rho)$ are linear combinations of 2×2 minors. Rewriting the γ_{jk} in terms of the $\alpha_j\alpha_k$ will give formulae for the β^{-}_{jk} in terms of the α_j. For this, we expand $\rho = \frac{1}{d}\sum_j \alpha_j(\rho)\Delta_j$ to give

$$\begin{aligned}
\gamma_{jk}(\rho) &= \frac{1}{d^2}\sum_{\ell}\alpha_{\ell}\alpha_{j+k-\ell}\operatorname{Tr}\Delta_{\ell}\Delta_{-j}\Delta_{k+j-\ell}\Delta_{-k} \\
&= \frac{1}{N}\sum_{\ell}(-\zeta_{2d})^{\ell_1 j_2 - \ell_2 j_1 + k_1(\ell_2 - j_2) - k_2(\ell_1 - j_1)}\alpha_{\ell}\alpha_{j+k-\ell} \\
&= \frac{1}{N}\sum_{\ell}(-\zeta_{2d})^{\ell_1(j_2 - k_2) - \ell_2(j_1 - k_1) + j_1 k_2 - j_2 k_1}\alpha_{\ell}\alpha_{j+k-\ell} \\
&= \frac{1}{N}\sum_{\ell}(-\zeta_{2d})^{\ell_1(j_2 - k_2) - \ell_2(j_1 - k_1)}\alpha_{j+\ell}\alpha_{k-\ell}.
\end{aligned}$$

In particular, the $\alpha_j\alpha_{-j}$ are fixed by the symplectic Fourier transform:

$$\alpha_j\alpha_{-j} = \frac{1}{N}\sum_{\ell}\zeta_d^{\ell_1 j_2 - \ell_2 j_1}\alpha_{\ell}\alpha_{-\ell}.$$

Note that this implies that

$$\alpha_0^2 = \frac{1}{N}\sum_{\ell}\alpha_{\ell}\alpha_{-\ell}$$

3.7 Equations from equiangularity

For $j \in (\mathbb{Z}/N)^2$, let

$$\alpha_j(X) := \langle \Delta_j, X \rangle = (-\zeta_{2N})^{j_1 j_2} \sum_k \zeta_d^{j_2 k} X_{k,k+j_1}.$$

Then each $X \in \mathrm{End}(V)$ has an expansion

$$X = \frac{1}{N} \sum_j \alpha_j(X) \Delta_j.$$

There is an action on the coordinates via $k\alpha_j(X) = \alpha_j(\Delta_k X \Delta_{-k}) = c_{k,j}\alpha_j(X)$. They satisfy $\alpha_j(\Delta_k X \Delta_{-k}) = c_{k,j}\alpha_j$. If X is Hermitian and rank 1, it is fiducial iff $|\alpha_j(X)|^2 = \frac{d\delta_j+1}{N+1}$ for all j. This gives a set of real algebraic equations in matrices. Note that a $(\mathbb{Z}/N)^2$-orbit $|v_j\rangle\langle v_j| = \Delta_j |v_0\rangle\langle v_0| \Delta_{-j}$ satisfies $\alpha_j(|v_0\rangle\langle v_0|) = \langle v_j, v_0 \rangle$.

For each j, consider the quadratic form on $\mathrm{End}(V)$:

$$\beta_j(X) = \alpha_j(X)\alpha_{-j}(X) = \langle \Delta_j \otimes \Delta_{-j}, X \otimes X \rangle = \sum_{a,b} \zeta_d^{j_2(a-b)} X_{a,a+j_1} X_{b+j_1,b}.$$

The phases can be eliminated by a Fourier transform in the second coordinate

$$\hat{\beta}_j(X) := \frac{1}{N} \sum_k \zeta_d^{kj_2} \beta_{j_1,k}(X) = \sum_{ab} \frac{1}{N} \sum_k \zeta_d^{k(j_2+a-b)} X_{a,a+j_1} X_{b+j_1,b} = \sum_a X_{a,a+j_1} X_{a+j_1+j_2,a+j_2}.$$

If X is Hermitian, then $\beta_j(X) = |\alpha_j(X)|^2$, so a Hermitian rank-1 $X \in \mathrm{End}(V)$ is fiducial iff $\beta_j(X) = \frac{N\delta_j+1}{N+1}$.

3.8 Invariant harmonics

The B_j are $(\mathbb{Z}/N)^2$-invariant, i.e $B_j(\Delta_k X \Delta_{-k}) = B_j(X)$ and satisfy $B_{-j}(X) = B_j(X)$.

Define

$$B_j^{\pm}(X) := \langle P_{\pm}(\Delta_j \otimes \Delta_{-j}) P_{\pm}, X \otimes X \rangle$$

and note that $B_j(X) = B_j^+(X) + B_j^-(X)$. Furthermore, we have

$$\begin{aligned} \hat{B}_j^+(X) - \hat{B}_j^-(X) &= \langle \Delta_j \otimes \Delta_{-j}, (X \otimes X) S \rangle \\ &= \sum_a X_{a,a+j_2} X_{a+j_1+j_2,a+j_1} = \hat{B}_{wj}, \end{aligned}$$

where $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Therefore, $\hat{B}_j^{\pm} = \frac{\hat{B}_j \pm \hat{B}_{wj}}{2}$.

There should be $\frac{(N+3)(N-1)}{4} = \left(\frac{N+1}{2}\right)^2 - 1$ of the B_j^+s if N is odd and $\frac{N(N+2)}{4} = \frac{(N+3)(N-1)+3}{4}$ if N is even.

Let $c = \lfloor\frac{N-1}{2}\rfloor$ and set

$$A = \{j : 1 \le j_1, j_2 \le c, B = \{j : 1 \le j_1 \le c, d - c \le j_2 \le N - 1\}$$

and note that $A \cup B \cup -A \cup -B$ consists of all points not fixed by $-I$. Furthermore, $w(A) = A$ while $w(B) = -B$. A splits into c w-invariant points and $\frac{c^2-c}{2}$ orbits of size 2. Therefore there are

The matrix w fixes the d points $j = (0,0), (1,1), \dots, (N-1, N-1)$, giving $N + \frac{N^2-N}{2} = \frac{N^2+N}{2}$ orbits of $\langle w\rangle$.

If N is odd, then $-I$ only fixes $(0,0)$, giving $1 + \frac{N^2-1}{2} = \frac{N^2+1}{2}$ orbits of $\langle -I\rangle$. Therefore $\langle w, -I\rangle$ fixes $(0,0)$, has size-2 orbits $\{(0,a),(a,0)\}, \{(a,-a),(-a,a)\}, 1 \le a \le \frac{N-1}{2}$ and size-4 orbits.

If $N = 2c$ is even, $-I$ fixes 4 points: $j = (0,0),(0,N/2),(N/2,0),(N/2,N/2)$, giving $4 + \frac{N^2-4}{2} = \frac{N^2+4}{2}$ orbits of $-I$. The combined group $\langle w, -I\rangle$ therefore fixes $(0,0)$ and $(N/2,N/2)$. The size-2 orbits are remaining size-2 and 4 orbits are given by all $1 \le a, b \le \frac{N-2}{2}, \epsilon = 0$: $\{(0,N/2),(N/2,0)\}, \{(a,a),(-a,-a)\}, \{(a,\epsilon N/2),(\epsilon N/2,a)\}, \{(a,b),(b,a),(-a,-b),(-b,a)\}$. Therefore there are $2 + \frac{N-2}{2} + 2(N2) + \left(\frac{N-2}{2}\right)^2$.

Let $\mathcal{S}(A) = \frac{1}{2}(A + SAS) = \frac{1}{2}(P_+AP_+ + P_-AP_-)$.

$$\mathcal{S}((\Delta_j \otimes \Delta_{-j})S) \;=\; \frac{1}{2}P_+(\Delta_j \otimes \Delta_{-j})P_+ - \frac{1}{2}P_-(\Delta_j \otimes \Delta_{-j})P_-$$

can I make it equal $\mathcal{S}(\Delta_{wj} \otimes \Delta_{-wj})$?

Note that $\beta_0^\pm(X) = \frac{\mathrm{Tr}(X)^2 - \mathrm{Tr}(X^2)}{2}$ span $\mathrm{Sym}^{0,0}V$ and $\Lambda^{0,0}(V)$, respectively.

I believe the β_j^+ with $j \ne 0$ span $\mathrm{Sym}^{2,2}(V)^{(\mathbb{Z}/d)^2}$ and the β_j^- $\Lambda^{2,2}(V)^{(\mathbb{Z}/d)^2}$. Let $\beta_j^\pm = \frac{1}{2}(\beta_j \pm \beta_{xj}))$ spanning each subspace separately. Therefore $\beta_j(X) = 0$ for all $j \ne 0$ iff

$$\frac{1}{d^2}\sum_j (\Delta_j X \Delta_{-j})^{\otimes 2} = \frac{2\beta_0^+(X)}{d^2+d}P_+ + \frac{2\beta_0^-(X)}{d^2-d}P_-.$$

So the last condition we need is that $\mathrm{Tr}(X^2) = \mathrm{Tr}(X)^2$ ($\beta^-(X) = 0$).

$\beta_{j_2 j_1}(X) = \overline{\beta_j(X)}$.

in which case $\beta_{j_2 j_1}(X) = \beta_j$. On the other hand, we can write

Furthermore, note that

$$\beta_{j_2 j_1}(X) = \mathrm{Tr}\, X\Delta_j X\Delta_- j = \mathrm{Tr}((\Delta_j \otimes \Delta_- j)(X \otimes X)S).$$

The phases can be eliminated by a Fourier transform in the second coordinate

$$\hat{\beta}_j(X) := \frac{1}{N}\sum_k \zeta_d^{kj_2}\beta_{j_1,k}(X) = \sum_{ab}\frac{1}{d}\sum_k \zeta_N^{k(j_2+a-b)} X_{a,a+j_1} X_{a+j_1+j_2,a+j_2},$$

after which

$$\hat{\beta}_j(zz^\dagger) = \sum_a z_a \bar{z}_{a+j_1} z_{a+j_1+j_2} \bar{z}_{a+j_2}.$$

Define $f_j(X) = (d+1)\hat{\beta}_j(X) - (\delta_{j_1} + \delta_{j_2})(\operatorname{Tr} X^2)$. Then a rank-1 Hermitian X is a fiducial iff $f_j(X) = 0$ for all j.

On the other hand, we may generalize the squared overlaps $\operatorname{Tr} P_j P_0$ to

$$\gamma_j(X) \coloneqq \operatorname{Tr} X\Delta_j X \Delta_{-j} = \operatorname{Tr}(\Delta_j \otimes \Delta_{-j})(X \otimes X)(P_+ - P_-) = \beta_j^+(X) - \beta_j^-(X).$$

If X has rank 1, then $\beta_j^-(X) = 0$ for all j, in which case $\beta_j = \beta_j^+ = \gamma_j$. If X is Hermitian, on the other hand, then $|\alpha_j|^2 = \beta_j$. Hence, rank-1 Hermitian matrices satisfy $|\alpha_j|^2 = \beta_j = \mu_j = \gamma_j^+$. The coordinates β_j, γ_j^+ and μ_j give three natural generalizations to all matrices, depending on whether or not we add or subtract γ_j^- from the γ_j^+.

On the other hand, the 2-design condition is global. For rank-1 X with $\operatorname{Tr} X = 1$,

$$\frac{1}{d^2} \sum_j (\Delta_j \otimes \Delta_j)(X \otimes X)(\Delta_{-j} \otimes \Delta_{-j}) - \frac{2}{d^2 + d} P_+ = 0$$

iff X is fiducial.

Actually, the $(\operatorname{Tr} X^2)$ might be subtle (see earlier attempts). Point is that

$$q_\pm(X) \coloneqq \operatorname{Tr} P_\pm(X \otimes X) = \frac{I_{d^2} \pm S}{2}(X \otimes X) = \frac{\operatorname{Tr}(X)^2 \pm \operatorname{Tr}(X^2)}{2}.$$

Rank-1 X will satisfy $q_-(X) = 0$ since if $X = vw^\dagger$, then

$$X^2 = vw^\dagger vw^\dagger = \langle w, v\rangle vw^\dagger = \operatorname{Tr}(X)X,$$

so that $\operatorname{Tr}(X^2) = \operatorname{Tr}(X)^2$. Note that if $X = zz^\dagger$, then $\operatorname{Tr}(X^2) = \operatorname{Tr}(X)^2 = \|z\|^4$.

Note that

$$\begin{aligned} |\alpha_j(X)|^2 &= \left| \sum_k \zeta_d^{j_2 k} X_{k,k+j_1} \right|^2 = \sum_{k,r} \zeta_d^{j_2(k-\ell)} X_{k,k+j_1} \bar{X}_{\ell,\ell+j_1} \\ &= \operatorname{Tr} X\Delta_j \overline{\operatorname{Tr} X\Delta_j} = \operatorname{Tr} X\Delta_j \operatorname{Tr} \Delta_j^\dagger X^\dagger \\ &= \operatorname{Tr} X\Delta_j \operatorname{Tr} X^\dagger \Delta_j^\dagger = \operatorname{Tr}(X \otimes X^\dagger)(\Delta_j \otimes \Delta_{-j}). \end{aligned}$$

A Fourier transform in the second coordinate gives

$$\begin{aligned} \alpha_j^\vee(X) &\coloneqq \frac{1}{d} \sum_r \zeta_d^{r j_2} |\alpha_{j_1,r}(X)|^2 = \sum_{k,\ell} \left(\frac{1}{d} \sum_r \zeta_d^{r(k+j_2-\ell)} \right) X_{k,k+j_1} \bar{X}_{\ell,\ell+j_1} \\ &= \sum_k X_{k,k+j_1} \bar{X}_{k+j_2,k+j_1+j_2}. \end{aligned}$$

Restricting to $\mathbb{CP}^{d-1}$ amounts to replacing X with $zz^\dagger$, i.e. $X_{k\ell}$ with $z_k \bar{z}_\ell$, giving

$$\beta_j^\vee(zz^\dagger) = \sum_k z_k \bar{z}_{k+j_1} \bar{z}_{k+j_2} z_{k+j_1+j_2}.$$

We then obtain homogeneous degree-$(2,2)$ equations

$$f_j(z,\bar{z}) = (d+1)\beta_j^\vee(z,\bar{z}) = (\delta_{j_1} + \delta_{j_2})\|z\|^4$$

such that $[v]$ is fiducial iff $f_j(v,\bar{v}) = 0$ for all j.

We have that $d^{2,2} := \dim \operatorname{End}(\operatorname{Sym}^{2,2} V)^{(\mathbb{Z}/d)^2}$ is equal to $\frac{(d+3)(d-1)}{4} = \left(\frac{d+1}{2}\right)^2 - 1$ if d is odd and $\frac{(d+3)(d-1)+3}{4} = \frac{d(d+2)}{4}$ if d is even. Apparently the f_j are harmonic, $(\mathbb{Z}/d)^2$-invariant and generate a rank-$d^{2,2}$ $\mathbb{Z}$-module. Hence, they span $\operatorname{Sym}^{2,2}(V)$. They cut out a projective subscheme of $\mathbb{P}(V \oplus \bar{V}$ of dimension $d-1$. On the other hand, $|\{f_j\}| = |\{f'_j\}| = \dim \operatorname{Harm}_{2,2}(\mathbb{C})^{(\mathbb{Z}/d)^2} + 1$ (show this). Note that $\tilde{f}_j$ is not harmonic if $j_1 = 0$ or $j_2 = 0$. They satisfy $f_j = f_{-j} = f_{j_2,j_1} = f_{-j_2,-j_1}$, so as a function on $(\mathbb{Z}/d)^2$, f_j is contant on orbits of $\langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$. We also have $|z|^4 = f_{0,0} + \cdots + f_{d-1,0}$, which explains why there is one extra equation. So the f'_j simply span the space of H-invariant polynomials and the f_j are the projections onto their harmonic parts.

If X is Hermitian, then

$$|\alpha_j|^2 \quad = \quad \operatorname{Tr}(X \otimes X)(\Delta_j \otimes \Delta_{-j}) = \sum_{k,r} \zeta_d^{j_2(k-\ell)} X_{k,k+j_1} X_{\ell+j_1,\ell}.$$

The corresponding Fourier transform is the same (or am I missing something here):

$$\tilde{f}_{ij} = \sum_k X_{k,k+j_1} X_{k+j_1+j_2,k+j_2} = \sum_k z_k \bar{z}_{k+j_1} z_{k+j_1+j_2} \bar{z}_{k+j_2}.$$

This should be compared with

$$\operatorname{Tr} X\Delta_j X\Delta_{-j} = \operatorname{Tr}(X \otimes X)(\Delta_j \otimes \Delta_{-j})(P_+ - P_-),$$

which for pure $X = |\psi\rangle\langle\psi|$ also gives

$$\operatorname{Tr}|\psi\rangle\langle\psi|\Delta_j|\psi\rangle\langle\psi|\Delta_{-j} = \langle\psi, \Delta_j\psi\rangle\langle\psi, \Delta_j^\dagger\psi\rangle = |\langle\psi, \Delta_j\psi\rangle|^2.$$

However, whenever $X \otimes X$ is supported on $\bigwedge^2 V$ (i.e. whenever $\operatorname{rank}(X) > 1$), these quantities will differ. How about for $X = P - \frac{1}{d}I$? Then we have

$$X \otimes X = P \otimes P + \frac{1}{d} P \otimes I_d + \frac{1}{d} I_d \otimes P + \frac{1}{d^2} I_d \otimes I_d.$$

Work out how this changes the antisymmetric parts. Note that the minors $\det_{ab,cd}(X) = X_{ac}X_{bd} - X_{ad}X_{bc}$ with $\{a,b\} \cap \{c,d\} = \varnothing$ are unaffected. The minors $\det_{ab,cb}$ and $\det_{ab,ab}(X)$ do change however, although they are no longer homogeneous. What are the dimensions of these spaces of minors? Not going to look into it now since I'd rather keep things projective if possible - though this might be a mistake since the affine aspects may be important.

Also note that these two functions are just the traces of $X \otimes X$ against the operators

$$\Pi_+(\Delta_j \otimes \Delta_{-j})\Pi_+ \pm \Pi_-(\Delta_j \otimes \Delta_{-j})\Pi_-.$$

Should be $\simeq I \otimes C_\pm \Delta_{j,2j} C_\pm$, where $C = C_+ - C_-$ is the charge conjugation operator $C|i\rangle = |-i\rangle$. What is $\operatorname{Tr} C_\pm \Delta_j$?

Let $\operatorname{Harm}_j^H \subset \operatorname{Harm}_j$ be the subspace of functions that are invariant under this action of M. As observed by Sobolev [1] for designs on the 2-sphere, we have the following theorem:

Theorem 3.2. *Let $N \geq 2$. The orbit $H \cdot P$ of a point $P \in \mathbb{P}^{N-1}(\mathbb{C})$ is a 2-design if and only if $f(P) = 0$ for every $f \in \mathrm{Harm}_{2,2}^{H}$.*

Let $\Psi \equiv \Psi(\mathbb{C}) \subset \mathbb{P}^{N-1}(\mathbb{C})$ be the set of **fiducial points** $\psi \in \mathbb{P}^{N-1}(\mathbb{C})$, i.e. those such that $M\psi$ is a 2-design. According to this theorem, Ψ is is a real projective algebraic set. Specifically, it is the intersection of complex projective algebraic set consisting of simultaneous zeros of degree-4 homogeneous polynomials in independent variables $z_1, \ldots, z_N, w_1, \ldots, w_N$ with the real hypersurface $\{w_i = \bar{z}_i\}$. This raises further questions: Is Ψ irreducible, and thus a projective variety? If not, are the orbits of M in Ψ irreducible?

If z is normalized, then $\psi = [v]$ is fiducial iff it saturates the $k = 2$ **Welch bound**:

$$\frac{1}{N} \sum_j |\tilde{f}_j(v, \bar{v})|^2 \geq \frac{2}{N+1}.$$

Then z is fiducial iff

$$f_{00} = \frac{2}{N+1}, \; f_{i0} = f_{0j} = \frac{1}{N+1}, \; f_{ij} = 0, \quad \text{where } 1 \leq i, j \leq N-1.$$

This shows that fiducials are defined over $\mathbb{Q}$. I claim that the non-projective part can be removed by restricting to harmonics of type $(2,2)$.

3.9 Quadratic forms on operators

Let $V = \mathbb{C}^d$. For each $k \in \mathbb{N}$, the Hermitian form $\langle A, B\rangle = \operatorname{Tr} A^\dagger B$ induces an antilinear isomorphism $\mathrm{End}(V^{\otimes k}) \to \mathrm{End}(V^{\otimes k})^*$ via $A \mapsto \langle A, \cdot\rangle$. Under this isomorphism, each $A \in \mathrm{Sym}^n(V)$ is identified with a degree-n homogeneous polynomial $f_A\langle A, X^{\otimes n}\rangle$ on $\mathrm{End}(V)$. In particular, each $A \in \mathrm{Sym}^2(\mathrm{End}(V))$ is identified with a quadratic form $f_A(X) = \langle A, X \otimes X\rangle$ on $\mathrm{End}(V)$. This space of quadratic forms further decomposes as

$$\mathrm{Sym}^2(\mathrm{End}(V)) = \mathrm{End}(\mathrm{Sym}^2(V)) + \mathrm{End}(\Lambda^2(V))$$

as irreducible $\mathrm{GL}(V)$-modules with respect to the action $X \mapsto gXg^\dagger$. Then

$$\begin{aligned}(gf_A)(X) &= \langle A, (g\otimes g)X(g\otimes g)^\dagger\rangle = \operatorname{Tr} A^\dagger(g\otimes g)X(g\otimes g)^\dagger = \operatorname{Tr}(g\otimes g)^\dagger A^\dagger (g\otimes g)X \\ &= \langle (g\otimes g)A(g\otimes g)^\dagger, X\otimes X\rangle = f_{(g\otimes g)A(g\otimes g)^\dagger}(X).\end{aligned}$$

These further decompose into irreducible $\mathrm{U}(V)$-modules as

$$\begin{aligned}\mathrm{End}(\mathrm{Sym}^2(V)) &= \mathrm{Sym}^{0,0}(V) + \mathrm{Sym}^{1,1}(V) + \mathrm{Sym}^{2,2}(V) \\ \mathrm{End}(\Lambda^2(V)) &= \Lambda^{0,0}(V) + \Lambda^{1,1}(V) + \Lambda^{2,2}(V),\end{aligned}$$

where $\mathrm{Sym}^{0,0}(V) = \mathbb{C}P_+$, $\Lambda^{1,1}(V) = \mathbb{C}P_-$, etc..

We may identify each $A \in \mathrm{End}(\mathrm{Sym}^n(V))$ with degree-n polynomial functions on $\mathbb{P}(V)$, which are represented by degree-(n,n) homogeneous $f_A(z,\bar z) = \langle A, (zz^\dagger)^{\otimes n}\rangle = z^{\dagger^{\otimes n}} A z^{\otimes n}$. The Laplacian $\nabla = \sum \frac{d}{dz_i d\bar z_i}$ acts on such polynomials as $f_A \mapsto f_{\operatorname{Tr}_1 A}$, mapping $\mathrm{End}(\mathrm{Sym}^n(V)) \to \mathrm{End}(\mathrm{Sym}^{n-1}(V))$ with kernel $\mathrm{Sym}^{n,n}(V)$. As subspaces of $\mathrm{End}(\mathrm{Sym}^2(V))$, $\mathrm{Sym}^{1,1}(V) + \mathrm{Sym}^{2,2}(V)$ consists of the traceless matrices and $\mathrm{Sym}^{2,2}$ the partial-traceless matrices.

I believe $\Lambda^{2,2}(V)$ consists of the $A \in \mathrm{End}(\Lambda^2(V))$ with $\operatorname{Tr}_1 A = 0$, so there might be a sense in which we can call these harmonic as well (check Ikeda and T..). Do they correspond to degree-0 harmonic $(2,2)$-forms on $\mathbb{P}(V)$? Are they called primitive forms? Sort this out.

Let $T \subset V$ be a $(d-1)$-dimensional subspace, viewed as the tangent space to a point. If $\omega \in \Lambda^{1,1}(T)$ is the Kahler form, Ikeda and T give a similar decomposition to the case for harmonic functions:

$$\mathrm{End}(\Lambda^2(T)) \simeq \Lambda^2(T)\otimes\Lambda^2\bar{T} \simeq \omega^n + \omega^{n-1}\wedge\Lambda_0^{1,1}(T) + \omega^{n-2}\wedge\Lambda_0^{2,2}(T) + \cdots + \Lambda_0^{n,n}(T).$$

3.10 Seeking $\sqrt{D}$

Why is every fiducial in dimension d defined over $\mathbb{Q}(\sqrt{D})$ for $D = (d-3)(d+1)$? Must have to do with the fact that $\dim\Lambda^{2,2}(V) = \frac{d^2 D}{4}$.

$$\begin{aligned}Q_0(x) &= 1 \\ Q_1(x) &= (d+1)(dx-1) \\ Q_2(x) &= \frac{d(d+3)}{4}((d+1)(d+2)x^2 - 4(d+1)x + 2).\end{aligned}$$

$$Q_1(x)^2 = \frac{4d(d+1)}{(d+2)(d+3)} Q_2(x) + 2\frac{(d-2)(d+1)}{d+2} Q_1(x) + (d^2-1)Q_0(x).$$

What does this have to do with the decomposition

$$\operatorname{Sym}^2 V_{\square,\square} = V_{[2],[2]} + V_{[1],[1]} + V_0 + V_{[1,1],[1,1]}?$$

Probably nothing! $Q_1(\langle P, P_0\rangle) = d(d+1)\operatorname{Tr} P_0\big(P - \frac{1}{d}I\big)$, so $\operatorname{Tr} PP_0 = \frac{1}{d(d+1)} Q_1(\langle P, P_0\rangle) + 1$. Therefore But then $Q_1(\langle P, P_0\rangle)Q_1(\langle P, P_1\rangle)$ might have another interesting decomposition, especially when $\operatorname{Tr} P_0 P_1 = \frac{1}{d+1}$.

Let $P_i = |\psi_i\rangle\langle\psi_i|$ satisfy $\operatorname{Tr} P_0 P_1 = |\langle\psi_0, \psi_1\rangle|^2 = \beta$. The symmetrized tensor product satisfies

$$\frac{1}{2}(P_0 \otimes P_1 + P_1 \otimes P_0) = \beta|\psi_+\rangle\langle\psi_+| + (1-\beta)|\psi_-\rangle\langle\psi_-|,$$

where

$$|\psi_\pm\rangle = \frac{P_\pm|\psi_0\rangle|\psi_1\rangle}{\beta_\pm} = \frac{|\psi_0\rangle|\psi_1\rangle \pm |\psi_1\rangle|\psi_0\rangle}{2\beta_\pm}$$

and $\alpha_+ = \sqrt{\beta}$ and $\alpha_- = \sqrt{1-\beta}$. In particular,

$$|\psi_0\rangle|\psi_1\rangle = \alpha_+|\psi_+\rangle + \alpha_-|\psi_-\rangle \text{ and } |\psi_1\rangle|\psi_0\rangle = \alpha_+|\psi_+\rangle - \alpha_-|\psi_-\rangle.$$

BIG QUESTION:

Is $V_{[1,1],[1,1]}$ the kernel of a space of polynomial functions on hermitian matrices?

4 Triple products

If P_j is a SIC, let $T_{ijk} = \operatorname{Tr} P_i P_j P_k$. Order-2 permutations of the indices of T_{ijk} act by complex conjugation. The imaginary part $J_{ijk} = \frac{d+1}{d}(T_{ijk} - T^*_{ijk})$ gives structure constants for $\mathfrak{gl}_N$ in the basis P_j, i.e. $[P_i, P_j] = \sum_k J_{ijk} P_k$. The real part $R_{ijk} = \frac{d+1}{d}(T_{ijk} - T^*_{ijk})$ appears in the anticommutator (see Appleby, Flammia & Fuchs) $\{P_i, P_j\} = \sum_k R_{ijk} P_k - \frac{d\delta_{ij}+1}{N+1} I$.

4.1 Triple products

Suppose P_i are N^2 Hermitian projections on $\mathbb{C}^N$ satisfying

$$\operatorname{Tr} P_i P_j = \begin{cases} 1 & i = j \\ \frac{1}{N+1} & i \neq j \end{cases}$$

for all i, j. Then they form a basis for the space of operators and we can write any A as

$$A = \sum_j a_j P_j, \text{ with } \operatorname{Tr} A P_k = \frac{N a_k + \operatorname{Tr} A}{N+1}, \ a_k = \frac{(N+1) \operatorname{Tr} A P_k - \operatorname{Tr} A}{N}.$$

Let $\alpha_{ijk} = \operatorname{Tr} P_i P_j P_k$. Then

$$P_i P_j = \sum_k \left(\frac{N+1}{N} \alpha_{ijk} - \frac{1}{N^2 + N} \right) P_k := \sum_k c_{ijk} P_k,$$

and the triple products are related to the structure constants via

$$\alpha_{ijk} = \frac{N}{N+1} c_{ijk} + \frac{1}{(N+1)^2}.$$

Given two rank-1 Hermitian projections P, Q, the corresponding geodesic distance in $\mathbb{CP}^{N-1}$ according to the Fubini-Study metric is

$$\theta = 2 \arccos\left(\sqrt{\langle P, Q \rangle} \right) = \arccos(2\langle P, Q \rangle - 1) \in [0, \pi]$$

and is equal to the angle on the Bloch sphere for $\mathbb{CP}^{d-1}$. It satisfies

$$\langle P, Q \rangle = \frac{1 + \cos\theta}{2} = \cos^2(\theta/2),$$

$$\sin(\theta/2) = \sqrt{1 - \langle P, Q \rangle} = \frac{1}{2} \| P - Q \|_1 = \frac{1}{\sqrt{2}} \| P - Q \|_2 = \| P - Q \|_\infty.$$

Orthogonal projections have distance π.

Hangan and Masala (or Blaschke, or Brehm?) showed that any three such projections P, Q, R satisfy

$$\operatorname{Tr} PQR = \sqrt{\operatorname{Tr} PQ \cdot \operatorname{Tr} QR \cdot \operatorname{Tr} RP} e^{i\phi}.$$

Let I be the integral of the Kahler form $\omega_P(v,w) = \mathrm{Re}\langle v, iw\rangle = -\mathrm{Im}\langle v,w\rangle$ on $\mathbb{CP}^{N-1}$ over the geodesic triangle with vertices P, Q, R. Then $\cos(2I) = \cos(\phi)$. A complete set of invariants for 3 points under $\mathrm{PU}(d)$ is given by the mutual inner products and I.

This means that the triple products satisfy $\alpha_{ijk} = \frac{e^{i\phi_{ijk}}}{(d+1)^3}$. Rescaling to $\tilde{P}_j = (d+1)P_j$, the corresponding triple products are then just phases $\tilde{\alpha}_{ijk} = e^{i\phi_{ijk}}$.

Proposition 4.1. *Suppose that* $|\alpha_{ijk}| = \alpha^3$ *for all* $\{i,j,k\}$*. Then* $\alpha_{ij} = \alpha$ *for all* $\{i,j\}$*.*

Proof. Let i,j,k,ℓ be distinct. Then $\alpha_{ij}\alpha_{jk}\alpha_{ki} = \alpha^3 = \alpha_{i\ell}\alpha_{\ell k}\alpha_{ki}$ implies $\alpha_{ij}\alpha_{jk} = \alpha_{i\ell}\alpha_{\ell k}$. Similarly, $\alpha_{\ell i}\alpha_{ij} = \alpha_{ellk}\alpha_{kj}$, from which

$$\alpha_{ij}^2 = \alpha_{jk}^2 = \alpha_{k\ell}^2 = \alpha_{\ell i}^2$$

follows. The same holds if we swap $j \leftrightarrow k$ or $k \leftrightarrow \ell$, further giving equality with α_{ik}^2 and $\alpha_{j\ell}^2$. Since the overlaps are positive, they must all be equal and the result follows. □

This gives an equivalent characterization of a SIC-POVM: $|\alpha_{ijk}| = \frac{1}{(N+1)^3}$ for distinct triples. Can I prove anything about the triple phases?

The imaginary part $J_{ijk} = \frac{N+1}{N}(\alpha_{ijk} - \alpha_{ijk}^*)$ gives structure constants for $\mathfrak{gl}_N$ in the basis P_j, i.e. $[P_i, P_j] = \sum_k J_{ijk}P_k$. The real part $R_{ijk} = \frac{N1}{N}(\alpha_{ijk} - \alpha_{ijk}^*)$ appears in the anticommutator (see Appleby, Flammia & Fuchs) $\{P_i, P_j\} = \sum_k R_{ijk}P_k - \frac{N\delta_{ij}+1}{N+1}I$. The real part $\mathrm{Re}\,\alpha_{ijk}$ is symmetric under index permutations and the imaginary parts $\mathrm{Im}\,\alpha_{ijk}$ are antisymmetric.

4.2 Triple products for $N = 2$ and $N = 3$

5 Examples

5.1 Notation

Let $V = \mathbb{C}^d$ and let $H = \mathrm{Sym}^{2,2}(V)^{(\mathbb{Z}/d)^2}$ be the space of harmonic invariant degree-$(2,2)$ polynomials on $V \oplus \bar{V}$. Let $\mathcal{F}_{\mathbb{C}} \subset \mathbb{P}(V) \times_{\mathbb{C}} \mathbb{P}(\bar{V})$ be the zero set of H and let $\mathcal{F}$ (the set of fiducials) be the solutions (v, w) with $w = \bar{v}$. Apparently, these are 0-dimensional varieties.

We may also consider subvarieties of $\mathbb{P}(\mathrm{End}(V))$ or $\mathbb{P}(\mathrm{Herm}(V))$ respectively containing $\mathcal{F}_{\mathbb{C}}$ and $\mathcal{F}$, by imposing some of the polynomials in $\Lambda^2(\mathrm{End}(V))$. One idea is to impose the harmonic ones in $\Lambda^{2,2}(V)$. Might there be any relevance to the $(\mathbb{Z}/d)^2$-symmetric polynomials? Would be worth checking to see if they define the same scheme in the lower dimensions. Also may be beneficial to affinize my scheme code.

The group $\mathrm{Aut}_{\mathbb{C}}(H_d)$ of automorphisms of the Heisenberg group fixing the center has a unitary projective representation on $\mathrm{End}(V)$ (and hence on $\mathrm{Herm}(V)$ and $\mathbb{P}(V)$) and is a group extension

$$0 \to (\mathbb{Z}/d)^2 \to \mathrm{Aut}_{\mathbb{C}}(H_d) \to \mathrm{SL}_2(d) \to 1.$$

If $4 \mid d$, this extension does not split – the cocycle of any lift of $\mathrm{SL}_2(d)$ will represent the nontrivial class in $H^2(\mathrm{SL}_2(d), (\mathbb{Z}/d)^2)$. This means that $\mathrm{SL}_2(d)$ has a well-defined action on SICs but on fiducials, it is only defined up to a $(\mathbb{Z}/d)^2$-valued 2-cocycle on $\mathrm{SL}_2(d)$ (probably even $\frac{d}{2}\mathbb{Z}/d\mathbb{Z}$-valued). Note that the kernel of the natural homomorphism $\mathrm{SL}_2(2d) \to \mathrm{SL}_2(d)$ is $\left\{\left(\begin{smallmatrix} ad & bd \\ cd & ad \end{smallmatrix}\right) : a, b, c = 0, 1\right\}$.

Below, we take $I = RH_2^G + R(\alpha_0 - 1)$.

5.2 $d = 2$

Here $K = \mathbb{Q}(\sqrt{-3})$, $D = -3$, $F = K^{(4)} = \mathbb{Q}(\zeta_{12})$. $\mathbb{Z}[\zeta_3]/2\mathbb{Z}[\zeta_3] \simeq \mathbb{F}_4$. There is no fundamental unit but note that $-\zeta_3 - \zeta_3^{-1} + 1 = 2$.

$\dim R_2 = 8$, $\dim H = 2$.

Here there are two degree-4 components, each with residue field $\mathbb{Q}(\zeta_{12})$, so all points are Hermitian. We have $\dim(H) = 2$, with basis

$$\begin{aligned} f_0 &= f_{00} = f_{10} = -f_{01} \\ &= 3(z_0^2\bar{z}_0^2 + z_1^2\bar{z}_1^2) - 2(z_0\bar{z}_0 + z_1\bar{z}_1)^2 = z_0^2\bar{z}_0^2 + z_1^2\bar{z}_1^2 - 4z_0\bar{z}_0z_1\bar{z}_1 \\ f_1 &= f_{11}/3 = z_0^2\bar{z}_1^2 + z_1^2\bar{z}_0^2. \end{aligned}$$

In terms of the α_j, the equations are $(d+1)\alpha_j\alpha_{-j} - \alpha_0^2$.

The elimination ideals $\mathbb{Q}[Y_{ij}] \cap (RH + R(\alpha_0^2 - 6))$ are generated by...

Note we really do need f_0 unlike in the odd dimensions.

5.3 $d = 3$

Here $K = \mathbb{Q}$, $D = 0$, $F = K^{(3)\infty} = \mathbb{Q}(\zeta_3)$ for the SIC with stabilizer $\mathrm{SL}_2(3)$ and maybe also the one with Borel stabilizer.

$$\begin{aligned} f_{00} &= 4(z_0^2\bar{z}_0^2 + z_1^2\bar{z}_1^2 + z_2^2\bar{z}_2^2) - 2(z_0\bar{z}_0 + z_1\bar{z}_1 + z_2\bar{z}_2)^2 = z_0^2\bar{z}_0^2 + z_1^2\bar{z}_1^2 - 4z_0\bar{z}_0z_1\bar{z}_1 \\ f_{01} = f_{10} &= 4(z_0^2\bar{z}_0^2 + z_1^2\bar{z}_1^2 + z_2^2\bar{z}_2^2) - 2(z_0\bar{z}_0 + z_1\bar{z}_1 + z_2\bar{z}_2)^2 = z_0^2\bar{z}_0^2 + z_1^2\bar{z}_1^2 - 4z_0\bar{z}_0z_1\bar{z}_1 \\ f_{11} &= 3(z_0^2\bar{z}_1^2 + z_1^2\bar{z}_0^2), \end{aligned}$$

There are 3 kinds of SICs: The maximally symmetric one $(\mathbb{Z}/3)^2 \cdot (0:1:-1)$ has stabilizer $\mathrm{SL}_2(3)$ of order 24. There are four intermediate SICs: each has an order-6 stabilizer given by one of the four Borel subgroups conjugate to $\langle \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & \\ & -1 \end{smallmatrix}\right) \rangle$ (corresponding to the SIC $(\mathbb{Z}/3)^2 \cdot (0:1:1)$. The remaining generic SICs $(\mathbb{Z}/3)^2 \cdot (0:1:\alpha)$ with $|\alpha| = 1$ and $\alpha^6 \neq 1$ form a continuous family, each of whose stabilizers are the order-3 subgroups of Borels, i.e. the conjugates of $\langle \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right) \rangle$.

The moduli space of SICs is a bouquet of four circles glued at a common point corresponding to the maximally symmetric SIC, with an intermediate SIC on the opposite side of each circle. The $\mathrm{SL}_2(3)$-orbits of SICs make up a single circle, with the $\mathrm{GL}_2(3)$-orbits forming a closed interval.

This describes the structure of $\mathcal{F}$. I do not know how it relates to $\mathcal{F}_{\mathbb{C}}$ but might conjecture they coincide. Magma confirms that $\mathcal{F}_{\mathbb{C}}$ has 8 components of dimension 1.

Since $\mathrm{Proj}(R/RH^{(\mathbb{Z}/3)^2})$ and $\mathrm{Proj}(R^{(\mathbb{Z}/3)^2}/RH^{(\mathbb{Z}/3)^2})$ are curves, it is natural to ask for their genus, singular points, etc.

5.4 $d = 4$

Here $D = D_0 = 5$, $h_5 = 1$, $h_5^+ = 2$, so there is a single Clifford orbit of 256 fiducials, partitioned into $|\mathrm{SL}_2(4)|/3 = 48/3 = 16$ SICs. Furthermore, $[R/I : \mathbb{Q}] = 512$.

There is not a real fiducial, but the extended symmetry group lifts to

$$\left\langle \left(\begin{smallmatrix} 0 & 3 \\ 5 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 6 & 5 \end{smallmatrix}\right) \right\rangle \subset \mathrm{ESL}_2(8).$$

Earlier attempts to use Magma to define a non-reduced 0-dimensional scheme of degree 1024, with 4 degree-64 components, 8 degree-32 components, and 32 components of degree 16. Somehow I lost my scheme5.m and can't reproduce it. Instead I'm always getting the reduced subscheme. Maybe there had been a bug and it's always reduced. Older code gave degree 1280 (scheme2.m).

The reduced subscheme has degree 512 and consists of 32 degree-16 components. So we got rid of the other components. Since it is defined over $\mathbb{Q}$, $\mathcal{F}_{\mathbb{C}}$ carries a $\mathrm{Gal}(F/\mathbb{Q})$ action and decomposes into two orbits $\mathcal{F}_{\mathbb{C}} = \mathcal{F} \cup \mathcal{F}^\tau$ of the centralizer $\mathrm{Gal}(F/K)$ of both complex conjugations. Each component contains a $\mathrm{Gal}(F/K)$-orbit of 8 fiducials, together with their 8 τ-conjugates. Each of the 16 SICs seems to intersect 8 components, with P_i and P_j in the same component iff $j = i + (2,2)$.

There are 64 components over $K = \mathbb{Q}(\sqrt{5})$. Magma indicates that each $\mathbb{Q}$-component $\mathcal{C}$ splits into two K-components, $\mathcal{C} \cap \mathcal{F}$ and $\mathcal{C} \cap \mathcal{F}^\tau$.

Hilbert series of harmonic ideal:

$$1 + 8s + 36s^2 + 120s^3 + 324s^4 + 744s^5 + 1500s^6 + 2712s^7 + \cdots$$

Markus Grassl finds 56 irreducible components in Magma with $\|z\| = 0$ on 24 of them, leaving 32 the

5.5 $d = 5$

There are 80 SICs and thus 2000 fiducials. They make up two Clifford orbits, each of which has $|\mathrm{SL}_2(3)|/3 = 120/3 = 40$ SICs, so $|\mathcal{F}| = 40 \cdot 5^2 = 1000$. Using an affine embedding into operators, Magma confirms that $|\mathcal{F}_{\mathbb{C}}| = 2000$. This is actually surprising as I would expect this to be 4000.

The Cartan tori in $\mathrm{GL}_2(d)$ consist of 10 nonsplit tori $T_{\mathrm{GL}} \subset \mathrm{GL}_2(d)$ and 15 split tori T'_{GL}. The normalizers $N_{\mathrm{GL}}(T)$ of the $\mathrm{GL}_2(d)$-Cartan tori are all distinct, and any two $\mathrm{GL}_2(d)$-Cartan tori generate $\mathrm{GL}_2(d)$. The Cartan tori of $\mathrm{SL}_2(d)$ are in 1-1 correspondence with those of $\mathrm{GL}_2(d)$ via $T_{\mathrm{SL}} = T_{\mathrm{GL}} \cap \mathrm{SL}_2(d)$ and $T'_{\mathrm{SL}} = T'_{\mathrm{GL}} \cap \mathrm{SL}_2(d)$. The normalizers in $\mathrm{GL}_2(d)$ of the $\mathrm{SL}_2(d)$-Cartan tori equal the corresponding normalizers of the $\mathrm{GL}_2(d)$-tori are distinct, as are the $N_{\mathrm{SL}}(T_{\mathrm{SL}})$, but there are only 5 $N_{\mathrm{SL}}(T'_{\mathrm{SL}})$. In other words, there are triples of T'_{SL} that are not distinguished by their $\mathrm{SL}_2(d)$-normalizers, but are distinguished by their $\mathrm{GL}_2(d)$-normalizers. Each T_{SL} is normalized by two T'_{SL} and each T'_{SL} normalizes three T_{SL}, so the Cartan tori form a $(2,3)$-regular bipartite graph. Furthermore, T'_{SL} normalizes T_{SL} iff it normalizes T_{GL} iff $\langle T_{\mathrm{SL}}, T'_{\mathrm{SL}}\rangle = N_{\mathrm{SL}}(T_{\mathrm{SL}})$ iff $\langle T_{\mathrm{GL}}, T'_{\mathrm{SL}}\rangle = N_{\mathrm{GL}}(T_{\mathrm{GL}})$. Otherwise, $\langle T_{\mathrm{GL}}, T'_{\mathrm{SL}}\rangle = \mathrm{GL}_2(d)$ (though $\langle T_{\mathrm{SL}}, T'_{\mathrm{SL}}\rangle$) varies).

We have $SH_{2,0} = \cap_N I_N$, $N \subset \mathrm{SL}_2(d)$ ranging over normalizers of split tori with each $V(I_N)$ containing a $\mathrm{Gal}(F/\mathbb{Q})$-orbit of 32 points. Over $K = \mathbb{Q}(\sqrt{3})$ we expect to have $S_K I_T = I_T^+ \cap I_T^-$. Each $V(I_T^+)$ contains a $\mathrm{Gal}(F/K)$-orbit of 16 fiducials. Over $K^\infty = \mathbb{Q}(\zeta_{12})$, we expect that $S_{K^\infty} I_T^+ = J_T J'_T$ (how are they related?). Each $V(J_T)$ consists of a $\mathrm{Gal}(F/K^\infty)$-orbit of 8 fiducials. If $F' = \mathbb{Q}(\zeta_{60})$ is the max CM subfield, these factor as $S_{F'} J_T = J''_T J'''_T$, etc.

Let $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$. The class number is 1 and the narrow class number is 2, with narrow class field $K^\infty = K(\sqrt{-1}) = \mathbb{Q}(\zeta_{12})$. As the fundamental unit $u_+ = 2 + \sqrt{3}$ is totally positive, u_+ has order 3 and $\mathcal{O}^\times = \langle u_+, -1\rangle$ has order 6 mod $(5)\mathfrak{m}_\infty$, for every $\mathfrak{m}_\infty \in \{\infty_1, \infty_2\}$. The $24/6 = 4$ Hecke characters mod (5) are characters of $\mathrm{Gal}(K^{(5)}/K)$: one is trivial and three are primitive. The $48/6 = 8$ Hecke characters mod $(5)\infty_{1/2}$ are characters of $\mathrm{Gal}(K^{(5)\infty_{1/2}}/K)$ and include four primitive characters together with the three of conductor (5) and the trivial character. The $96/6 = 16$ Hecke characters mod $(5)\infty$ are characters of the full Galois group $\mathrm{Gal}(K^{(5)\infty}/K)$. These include the trivial character, the three of conductor (5), 4 of conductor $(5)\infty_1$, 4 of conductor $(5)\infty_2$, 1 of conductor ∞ and 3 of conductor $(5)\infty$.

The class fields and some of their subfields are related as follows, with each line representing a quadratic extension:

$$\begin{tikzcd}
& K^{(5)\infty} & \\
K^{(5)\infty_1} \arrow[ur] & K^{(5)\infty_2} \arrow[u] & K^{\infty}(\zeta_5) \arrow[ul] \\
& K^{(5)} \arrow[ul] \arrow[u] \arrow[ur] & \\
& K(\sqrt{5}) \arrow[u] & K^{\infty} \arrow[uu] \\
& K. \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Note that $K^{\infty}(\zeta_5) = \mathbb{Q}(\zeta_{60})$ is the max CM field and $K^{(5)} = \mathbb{Q}(\zeta_{60} + \zeta_{60}^{-1})$ the totally real subfield. The discriminants of the class fields are $\mathrm{disc}(K^{(5)\infty}/K) = (5)^{14}$, $\mathrm{disc}(K^{(5)\infty_{1/2}}) = (5)^7$ and $\mathrm{disc}(K^{(5)}) = (5)^3$. For $E = K^{(5)}, K^{(5)\infty_i}, K^{(5)\infty}$, the prime factorization of $d\mathcal{O}_E$ is $\mathfrak{p}^4$, $\mathfrak{q}_i^8$ and $\mathfrak{r}_1^8\mathfrak{r}_2^8$, with $\mathfrak{p}\mathcal{O}_{K^{(5)\infty_i}} = \mathfrak{q}_i^2$ and $\mathfrak{q}_i\mathcal{O}_{K^{(5)\infty}} = \mathfrak{r}_i^2$. In particular, (5) is totally nonsplit in each $K^{(5)\infty_i}$ and its subfields.

5.6 $d = 6$

Here there are two Clifford orbits, each containing $|\mathrm{SL}_2(6)|/3 = 48$ SICs, so $|\mathcal{F}| = 2{\cdot}48{\cdot}6^2 = 3456$ fiducials.

5.7 $d = 7$

Here there are two discriminants, $D_0 = 8$ and $D = 56$, giving rise to two EC orbits. These are partitioned into three Clifford orbits, each containing $|\mathrm{SL}_2(7)|/3 = 112$ SICs, and therefore $|\mathcal{F}| = 3 \cdot 112 \cdot 7^2 = 16464$ fiducials in total.

There are 28 order-3 subgroups of $\mathrm{SL}_2(7)$, each stabilizing $112/28 = 4$ fiducials on each Clifford orbit. The $7b$ orbit is defined over the ray class field $F = \mathbb{Q}\Big(\sqrt{2\sqrt{2} - 1}, \zeta_7\Big)$. The other two are defined over $F(i)$ and are related by complex conjugation, constituting the single EC orbit $7a$. Note that $[F : K] = [F(i) : K(i)] = 12$.

We can view R as an $\mathcal{O}_K$-module via the Weil representation, under which the action of the diagonal subgroup $T_cT_6 \subset \mathrm{ESL}_2(d)$ is defined over $\mathbb{Q}$, with $\left(\begin{smallmatrix} a & \\ & a^{-1} \end{smallmatrix}\right) f(z, \bar{z}) = f(\phi(a)z, \phi(a)\bar{z})$, where $\phi(a)z_b = z_{ab}$, $\phi(a)\bar{z}_b = \bar{z}_{ab}$

Let I_3 be the ideal generated by I and the polynomials $z_{2a}\bar{z}_{2b} - z_a\bar{z}_b$, amounting to imposing symmetry by the order-3 subgroup generated by $\left(\begin{smallmatrix} 2 & \\ & 4 \end{smallmatrix}\right)$ under the Weil representation. Let I_c be the ideal generated by I and the polynomials $z_a\bar{z}_b - z_b\bar{z}_a$, which cuts out the points whose residue field has a real embedding. Let $I_{c'}$ be the ideal generated by I and the polynomials $z_a\bar{z}_b - z_{-b}\bar{z}_{-a}$. Then $[R/I_c : \mathbb{Q}] = 28$, so there are 14 real fiducials. Furthermore, $[R/I_3 : \mathbb{Q}] = 24$ and $[R/(I_3 + I_c) : \mathbb{Q}] = 4$ verify that 12 fiducials have the order-3 symmetry, 2 of which are real.

Magma computations are consistent with the assertion that $R/I_3 \simeq L \times L \times L(i) \times L(i)$. In particular, the degrees of the irreducible components are $4, 4, 8, 8$. The first two components account for the 4 stabilized fiducials on the first Clifford orbit. The Hermitian points of the second two components make up the the points of the second and third Clifford orbits.

Note that only $1 + 48/3 = 17$ variables are needed for I_3, and $1 + 48/6 = 9$ for $I_3 + I_c$

5.8 Comments

So far what we've seen is consistent with the conjecture that when $d \geq 4$, we have $|\mathcal{F}_{\mathbb{C}}| = 2|\mathcal{F}|$. Note that $\mathrm{Gal}(F/\mathbb{Q})$ should act on the F-points. So far, a check in $d = 4$ seems to say that $|\mathcal{F}_{\mathbb{C}}(F)| = 2|\mathcal{F}|$, which would be consistent with an action by $\tau \in \mathrm{Gal}(F/\mathbb{Q}) \setminus \mathrm{Gal}(F/K)$ on $\mathcal{F}_{\mathbb{C}}$.

Here is some more insight: If indeed there is an underlying torus, it really should involve the overlaps $\alpha_j(P_0)$, as they satify the reciprocity law. Is there a similar law for the other fiducials?

Must decide whether the degree is artificially bigger. Magma says that for reduced schemes, the degree equals the number of points over an algebric closure. Could this scheme be non-reduced with all the points doubled?

It will be interesting to understand why the first schemes I constructed in Magma were not reduced. Must need more equations. Should view it this way: The coordinate ring for $\mathbb{P}(V) \times_{\mathbb{C}} \mathbb{P}(\bar{V})$ decomposes under $\mathrm{U}(V)$ as $R = \bigoplus_n R_n$, with $R_n \simeq \mathrm{Sym}^{n,n}(V)$. Furthermore, it should also be $(\mathbb{Z}/d)^2$-graded. So really we "just" need to understand the ideal $I = R_{2,0}R$

and how it decomposes into primes. Note that $R_{2,0}R_n \subset R_{n+2}$. So it would seem that we need to understand the images maps

$$\mathrm{Sym}^{2,2}(V)^{(\mathbb{Z}/d)^2} \times \mathrm{Sym}^{n,n}(V) \to \mathrm{Sym}^{n+2,n+2}(V).$$

6 Special dimensions

Let $d \geq 4$ and set $D = (d-3)(d+1) = f^2 D_0$. Let $K = \mathbb{Q}(\sqrt{(d-3)(d+1)}$ and let F/K be the ray class field modulo $d'\infty$ where ∞ is the product of both real places of K.

6.1 Primes $d \geq 5$

Let $d \geq 5$ be prime, so that $D = (d-3)(d+1) = f^2 D_0 > 0$ and $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D_0})$ is real quadratic. Let $\mathcal{O}_K = \mathcal{O}_{D_0} := \mathbb{Z}\left[\frac{D_0+\sqrt{D_0}}{2}\right]$ be the maximal order, let u_f be the fundamental unit, for which $\mathcal{O}_K^\times = \langle -1, u_f \rangle$, and let u_+ generate the totally positive units $\mathcal{O}_K^+ = \langle u_+ \rangle$. By FLMY, $u_+^r + u_+^{-r} = d-1$, where $3r$ is the order of the image of u_+ in $(\mathcal{O}_K/d)^\times$.

The fiducials live in subspaces of dimension $\lceil \frac{d}{3} \rceil$. For $d \equiv 1 \bmod 3$, this is the $+1$ eigenspace of an order-3 Clifford unitary, of dimension $\frac{d+2}{3}$. For $d \equiv 2 \bmod 3$, fiducials live in the $\zeta_3^{\pm 1}$-eigenspaces, each of dimension $\frac{d+1}{3}$.

Periodicity of the Legendre symbol and quadratic reciprocity give

$$\left(\frac{D_0}{d}\right) = \left(\frac{D}{d}\right) = \left(\frac{-3}{d}\right) = \left(\frac{d}{3}\right).$$

So, the character of the solution for prime dimensions depends on the dimension mod 3: If $d \equiv 1 \bmod 3$, then $(d) = \mathfrak{p}_1\mathfrak{p}_2$ splits and $\mathcal{O}_K/d \simeq \mathbb{F}_d \times \mathbb{F}_d$. If $d \equiv 2 \bmod 3$, then (d) is prime so that $\mathcal{O}_K/d \simeq \mathbb{F}_{d^2}$.

6.2 Prime $d \equiv 1 \bmod 3$

Let $d \equiv 1 \bmod 3$ be prime. Then (d) splits in $\mathcal{O}_K$ as $\mathfrak{p}_1\mathfrak{p}_2 = (d)$, where u_+ has order $3r$ in $\mathcal{O}_K/\mathfrak{p}_2$ and order $3r\frac{2h}{h_+}$ in $\mathcal{O}_K/\mathfrak{p}_1$. As verified by Magma,

$$[K^{\mathfrak{p}_2} : K] = h\frac{d-1}{6r},\ [K^{\mathfrak{p}_2\infty_1} : K] = h_+\frac{d-1}{6r},\ [K^{\mathfrak{p}_2\infty_2} : K] = h\frac{d-1}{3r},\ [K^{\mathfrak{p}_2\infty} : K] = h_+\frac{d-1}{3r}.$$

Furthermore,

$$[K^{(d)\infty} : K] = h_+\frac{(d-1)^2}{3r}$$

implies that $[K^{(d)\infty} : K^{\mathfrak{p}_2\infty}] = d-1$. In fact, $K^{(d)\infty} = K^{\mathfrak{p}_2\infty}(\zeta_d)$.

A Hecke character χ mod $\mathfrak{f}\infty$ has conductor $\mathfrak{f}(\chi) = \mathfrak{f}_0(\chi)\mathfrak{f}_\infty(\chi)$, with infinite part $\mathfrak{f}_\infty(\chi) = \infty_1^{\varepsilon_1(\chi)}\infty_2^{\varepsilon_2(\chi)}$, where $\chi(c_i) = (-1)^{\varepsilon_i(\chi)}$ and with finite part $\mathfrak{f}_0(\chi) \mid \mathfrak{f}$.

Let $m = \frac{d-1}{6r}$. There are in general h primitive characters mod (1) and $h(m-1)$ primitive characters mod $\mathfrak{p}_2$, giving hm characters mod $\mathfrak{p}_2$. There are also hm primitive characters mod $\mathfrak{p}_2\infty_2$, accounting for all the $2hm$ Hecke characters mod $\mathfrak{p}_2\infty_2$. Therefore, $[K^{\mathfrak{p}_2\infty_2} : K^{(1)}] = 2m$.

If $h_+ = 2h$, there are in addition h primitive characters mod ∞, $h(m-1)$ primitive characters mod $\mathfrak{p}_2\infty_1$, as well as hm primitive characters mod $\mathfrak{p}_2\infty$, giving a total of $4hm$ characters mod $\mathfrak{p}_2\infty$. In this case, $[K^{\mathfrak{p}_2\infty} : K^{(1)}] = 4m$ and $[K^{\mathfrak{p}_2\infty} : K^{\infty}] = 2m$.

Shintani: Assume that $\mathrm{Gal}(K^{\mathfrak{f}\infty}/K^{\mathfrak{f}}) = \langle c_1, c_2\rangle$ has order 4 (i.e. that c_1 and c_2 are distinct and nontrivial). Let $G = \mathrm{Gal}(K^{\mathfrak{f}\infty}/K^{(1)})$ and suppose $H \subset G$ is a subgroup containing c_1 but not c (equivalently, not c_2). Then $(K^{\mathfrak{f}\infty})^H = (K^{\mathfrak{f}\infty_2})^H$ is the compositum of cyclic subextensions $K^\chi = (K^{\mathfrak{f}\infty})^{\ker(\chi)} \simeq K^{\mathfrak{f}(\chi)}$ for primitive $\chi \mid \mathfrak{f}\infty_2$. He conjectured that $K^{\mathfrak{f}\infty_2}$ is generated by some power of the ray class invariants

$$X_{\mathfrak{f}}(\mathfrak{C}) = e^{\zeta'(0,\mathfrak{C})-\zeta'(0,c\mathfrak{C})} = e^{\zeta'(0,\mathfrak{C})-\zeta'(0,c_2\mathfrak{C})}$$

for $\mathfrak{C} \in G/H \simeq \mathrm{Gal}((K^{\mathfrak{f}\infty})^H/K^{(1)})$, some power of which generate $(K^{\mathfrak{f}\infty})^H$. Taking $\mathfrak{f} = \mathfrak{p}_2$ and $H = \langle c_2\rangle$ realizes $K^{\mathfrak{p}_2\infty_2}$ inside $K^{\mathfrak{p}_2\infty}$. However, taking $\mathfrak{f} = (d)$ and $H = \mathrm{Gal}(K^{(d)\infty}/K^{\mathfrak{p}_2\infty_2}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$(!!!???) realizes the same field inside the full ray class field $K^{(d)\infty}$ in a way that matches the conjecture exactly, i.e. with c_1 and c_2 nontrivial. And yet my conjecture may relate the coordinates to the overlaps in a precise way, by relating stark units for $K^{\mathfrak{p}_2\infty_2}$ to Stark units for $K^{(d)\infty_1}$.

We can avoid thinking about the class group for the primes

$$d = \mathbf{7}, \mathbf{19}, 31, \mathbf{67}, 97, 127, \mathbf{199}, 337, \ldots,$$

with $h = 1$. Boldfaced dimensions have $h_+ = 1$ while the rest have $h_+ = 2$. We can expect similarity between the ring class fiducials in $d = 7$ and the ray class ones in the latter class, with $d = 31$ being the simplest of the prime dimensions. The only dimensions with $m = 1$ appear to be $d = 7$ and $d = 19$, leading to particularly simple formulas in those cases.

I am still a bit confused regarding factors of 2 but dimension $d = 31$ may clear that up: There we have $K = K^{(1)} = \mathbb{Q}(\sqrt{14})$, $K^\infty = \mathbb{Q}(\sqrt{-2}, \sqrt{-7})$, $r = 1$ and $m = 5$. The relevant fields satisfy $[K^{\mathfrak{p}_2\infty} : K] = 20$ and $[K^{(31)\infty} : K] = 600 = 20 \cdot 30$. Magma does verify that the cyclotomic polynomial $\Phi_{31}(x)$ does not split in $\mathcal{O}_{K^{\mathfrak{p}_2\infty}}[x]$, validating my conjecture. But the Stark units are going to be fixed by c_1, but these are not: I also have $\sqrt{-2}$ and/or $\sqrt{-7}$ to play with. Recall van der Geer talked about the genus characters...

ALSO: Even though a fiducial is not fixed by c_1, we can still note that it still gives another fiducial – the complex conjugate. We can either lump that into the extended Clifford group, or treat it as a different Clifford orbit.

Is there a simple guess? Maybe it is indeed better to look at the other $d = 7$ orbit. Everything goes through replacing $\mathcal{O}_K$ with $\mathcal{O} := \mathcal{O}_{32}$, only now $K^{\mathcal{O}} = K = \mathbb{Q}(\sqrt{2})$ with $K^{\mathcal{O}\infty} = K(i) = \mathbb{Q}(\zeta_8)$. Interesting, don't think I'd realized that.

The idea is to use $\mathfrak{p}_{1/2} = (1 \pm 2\sqrt{2})$ and the choice doesn't matter this time as $u_+ = 3 + 2\sqrt{2}$ has order 3 mod each of them.

Maybe it is cleaner to work inside $\mathcal{O}_D = \mathbb{Z}[b]$ throughout.

Class field theory gives

$$[K^{(d)\infty} : K^{\infty}] = \frac{(d-1)^2}{3r}, \quad [K^{\mathfrak{p}_i\infty} : K^{\infty}] = \frac{2hm}{h_+},$$

which implies that $[K^{(d)\infty} : K^{\mathfrak{p}_i\infty}] = d-1$. Can also show that $K^{\infty}(\zeta_d) = (K^{(d)\infty})^{\mathrm{Gal}(K^{(d)\infty}/K^{\mathfrak{p}_2\infty})}$. Therefore $K^{\mathfrak{p}_i\infty} \cap K^{\infty}(\zeta_d) = K^{\infty}$, implying that the Galois group splits as a direct product

$$\mathrm{Gal}(K^{(d)\infty}/K^{\infty}) = \mathrm{Gal}(K^{(\infty}/K^{\mathfrak{p}_i\infty})\,\mathrm{Gal}(K^{(d)\infty}/K^{\infty}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \times \mathrm{Gal}(K^{\mathfrak{p}_i\infty}/K^{\infty}).$$

Similarly, the extension

$$1 \to T_{\mathrm{SL}} \to T_{\mathrm{GL}} \to \mathbb{F}_d^{\times} \to 1$$

splits as $T_{\mathrm{GL}} = T_{\mathrm{SL}}\{\begin{pmatrix} 1 & \\ & k \end{pmatrix}\}$. For each $t \in T_{\mathrm{GL}}$, a fiducial should satisfy $U_{s_t}|\psi\rangle^{\sigma_t} = |\psi\rangle$, where $s \mapsto U_s$ is the Weil representation of $\mathrm{SL}_2(d)$ (which one?) and $s_t = \begin{pmatrix} t_1 & \\ & t_1^{-1} \end{pmatrix} = t\begin{pmatrix} 1 & \\ & t_1 t_2 \end{pmatrix}^{-1} \in T_{\mathrm{SL}}$. A general ansatz is expected to be

$$|\psi\rangle = |0\rangle + \sum_{\chi \in \widehat{\mathrm{CL}}_{\mathfrak{p}_2\infty}} w_\chi |\chi\rangle = |0\rangle + \sum_{a=1}^{d-1} w^{\sigma_{(a)}} |a\rangle,$$

where $(a) \mapsto \sigma_{(a)} \in \mathrm{Gal}(K^{\mathfrak{p}_2\infty}/K^{\infty})$ is the Artin map.

6.2.1 Example: $d = 7$, $d = 19$

In $d = 7$ we have $K = K^\infty = \mathbb{Q}(\sqrt{2})$, so the fundamental unit $u_f = 1 + \sqrt{2}$ is not totally positive, with $N(u_f) = -1$. Then $(7) = \mathfrak{p}_1\mathfrak{p}_2$ for prime ideals $\mathfrak{p}_1 = (3 - \sqrt{2})$ and $\mathfrak{p}_2 = (3 + \sqrt{2})$. There are two fiducials defined over $K^{\mathfrak{p}_2\infty_2} = \mathbb{Q}(\sqrt{2\sqrt{2} - 1})$, with order-3 unitary symmetry group $S = \left\langle \begin{pmatrix} 2 & \\ & 4 \end{pmatrix} \right\rangle \subset T_{\mathrm{SL}}$. Their symmetry under c_1 is reflected by $\begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$, but recall that $\langle -I \rangle$ is also not relevant for the invariants. Here $K^{\mathfrak{p}_2\infty} = \mathbb{Q}(\sqrt{2\sqrt{2} - 1})$. $u = -\frac{1+\sqrt{2}+\sqrt{2\sqrt{2}-1}}{2}$

$$|\psi_+\rangle \quad = \quad |0\rangle - \frac{1 + \sqrt{2}}{2}|\chi_1\rangle \mp \frac{\sqrt{2\sqrt{2} - 1}}{2}|\chi_{-1}\rangle = \sum_{j=0}^{d-1} u^{\pm\left(\frac{j}{7}\right)}|j\rangle,$$

is a linear combination of characters in $\ker \widehat{T}_{d-1} \to \widehat{T}_3$. These are in bijection with characters of $(\mathcal{O}_K/\mathfrak{p}_2)^\times$ of $\mathbb{F}_d^\times$ that are trivial on the image of the totally positive units, which is identified with the stabilizer subgroup. Equivalently, they are characters of $\mathrm{Gal}(K^{\mathfrak{p}_2\infty}/K^\infty)$, so Hecke characters mod $\mathfrak{p}_2\infty$. Here

$$\mathrm{Gal}(K^{\mathfrak{p}_2\infty}/K^\infty) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2\sqrt{2} - 1})/\mathbb{Q}(\sqrt{2})) = \langle c_2 \rangle,$$

where $u^{c_2} = u^{-1}$, adding to the miracle of the formula.

A further miracle is that
$$e^{2\zeta'(0,\sigma_\pm)} = e^{\pm L'(0,\chi)} = u^\pm,$$

where $\sigma_+ = 1$ and $\sigma_- = c_2$ and where χ is the nontrivial character mod $(3 + \sqrt{2})\infty_2$. Note that

$$\zeta'(0, \sigma_\pm) = \frac{1}{2}L'(0, 1) + \frac{1}{2}\chi(\sigma_\pm)L'(0, \chi) = \pm\frac{1}{2}L'(0, \chi).$$

So the coordinates are *precisely* Stark units. It absolutely has to generalize.

Here's how.

For a simpler example, let $K = \mathbb{Q}(\sqrt{2})$ and consider the characters mod $(7)\infty$. Factoring $(7) = (3+\sqrt{2})(3-\sqrt{2})$. There is one character with trivial conductor, one with conductor $(3+\sqrt{2})\infty_2$, one with conductor $(3-\sqrt{2})\infty_1$, two with conductor (7), two with conductor $(7)\infty_1$, two with conductor $(7)\infty_2$ and three with conductor $(7)\infty$.

Let $L = K^{(3+\sqrt{2})\infty_-} = \mathbb{Q}\left(\sqrt{2\sqrt{2}-1}\right)$ and $L' = K^{(3-\sqrt{2})\infty_+} = \mathbb{Q}\left(\sqrt{-2\sqrt{2}-1}\right)$ and note that the Galois closure of either is $LL' = L \otimes_K L' = L(\sqrt{-7})$. Furthermore, these fields are linearly disjoint from $\mathbb{Q}(\zeta_7)$, so that $F = L(\zeta_7) = L'(\zeta_7) = LL'(\zeta_7 + \zeta_7^{-1})$. The discriminant of the quadratic extension L/K is $(3+\sqrt{2})$ and the discriminant of F/K is $(7)^{10}$.

By quadratic reciprocity, the two examples above generalize to all odd primes, depending on whether $d \equiv 1$ or 2 mod3.

6.2.2 Organize it

Do I need these extensions?

$$1 \to \mathrm{Gal}(K^{(d)\infty}/K^{\mathfrak{p}_i\infty}) \to \mathrm{Gal}(K^{(d)\infty}/K^{\infty}) \to \mathrm{Gal}(K^{\mathfrak{p}_i\infty}/K^{\infty}) \to 1.$$

splits via $\mathrm{Gal}(K^{(d)\infty}/K^{\infty}) \to \mathrm{Gal}(K^{(d)\infty}/K^{\infty}(\zeta_d))$, so that $K^{(d)\infty} = K^{\mathfrak{p}_i\infty}(\zeta_d)$, with Galois group

When $[K^{\infty} : K^{(1)}] = 2$ and $\nu \subset \{\infty_1, \infty_2\}$ is a real modulus, we have

$$[K^{(d)\nu} : K^{(1)}] = 2^{|\nu|}\frac{(d-1)^2}{6r}, \quad [K^{\mathfrak{p}_i\nu} : K^{(1)}] = 2^{|\nu|}\frac{d-1}{6r},$$

where $|\nu|$ is the number of places in the real modulus ν. Furthermore,

for $\mathfrak{a} = \mathfrak{p}_1, \mathfrak{p}_2$ or (d) and any real modulus the fundamental unit $u_f = u_+$ has order $3r$ mod $\mathfrak{a}\nu$. Therefore,

$$[K^{\mathfrak{p}_i\nu} : K^{(1)}] = 2^{|\nu|}\frac{d-1}{3r} \text{ and } [K^{(d)\nu} : K^{(1)}] = 2^{|\nu|}\frac{d-1}{3r}.$$

The possible conductors of Hecke characters modulo $(d)\infty$ are in 1-1 correspondence with the ray class fields contained in $K^{(d)\infty}$.

There are two possibilities:

- $d-3$ is a square, in which case $K^{\infty} = K^{(1)}$, $N(u_f) = -1$ and $u_+ = u_f^2$. Furthermore, $K^{\mathfrak{p}_1\infty} = K^{\mathfrak{p}\infty_1}$ and $K^{\mathfrak{p}_2\infty} = K^{\mathfrak{p}_2\infty_2}$.

- $d-3$ nonsquare. The generic case (where $K^{\infty} \neq K^{(1)}$) is going to have

$$K^{\mathfrak{p}} \neq K^{\mathfrak{p}_1\infty_1} \simeq K^{\mathfrak{p}_1\infty_2} \neq K^{\mathfrak{p}_1\infty},$$

  but when $K^{\infty} = K^{(1)}$, the above diagram should work after removing K^{∞}.

The corresponding ray class fields obey the following inclusions:

$$\begin{tikzcd}
 & K^{(d)\infty} & \\
K^{(d)\infty_1} \arrow[ur] & & K^{(d)\infty_2} \arrow[ul] \\
K^{\mathfrak{p}_1\infty_1} \arrow[u] & K^{(d)} \arrow[ul] \arrow[ur] & K^{\mathfrak{p}_2\infty_2} \arrow[u] \\
K^{\mathfrak{p}_1} \arrow[u] \arrow[ur] & & K^{\mathfrak{p}_2} \arrow[u] \arrow[ul] \\
 & K^{(1)} \arrow[ul] \arrow[ur] & \\
 & K \arrow[u] & \\
 & \mathbb{Q} \arrow[u] &
\end{tikzcd}$$

$$\begin{tikzcd}
 & & & (d)\infty & & & \\
 & (d)\infty_1 \arrow[urr] & & & & (d)\infty_2 \arrow[ull] & \\
 & & \mathfrak{p}_1\infty \arrow[ur] & & \mathfrak{p}_2\infty \arrow[ul] & & \\
\mathfrak{p}_1\infty_1 \arrow[uur] \arrow[urr] & & \mathfrak{p}_2\infty_1 \arrow[uul] \arrow[urr] & & \mathfrak{p}_1\infty_2 \arrow[uur] \arrow[ull] & & \mathfrak{p}_2\infty_2 \arrow[uul] \arrow[ull] \\
 & & \mathfrak{p}_1 \arrow[ull] \arrow[urr] & & \mathfrak{p}_2 \arrow[ull] \arrow[urr] & & \\
 & & & \infty \arrow[uuul] \arrow[uuur] & & & \\
 & & & (1) \arrow[u] \arrow[uul] \arrow[uur] & & &
\end{tikzcd}$$

Note that restricting to $(d)\infty_i$ gives a simpler diagram.

A subextension F/K of an abelian extension F/K gives an extension of Galois groups

$$1 \to \mathrm{Gal}(F/L) \to \mathrm{Gal}(F/K) \to \mathrm{Gal}(L/K) \to 1$$

that splits iff there is a subfield

6.3 Odd prime $d \equiv 2 \bmod 3$

This case was investigated by Kopp

6.4 The splitting of algebras

A central simple algebra A/K is split iff A_{K_v} is split for every v. If L/K is an extension, then $A_L := A \otimes_K L$ is split iff $m_v \mid [L_w : K_v]$ for all $w|v$, where the local index m_v is the degree of the division algebra D/K_v Brauer-equivalent to $A_v = A \otimes_K K_v$ and where $[F_w : K_v] = e_{w|v} f_{w|v}$.

If A/K is a quaternion algebra, then a quadratic F/K splits A iff there is an embedding $F \hookrightarrow A$ iff every ramified v of A/K extends uniquely to F (i.e. $F_v := F \otimes_K K_v$ is a field) iff there are embeddings $F_v \hookrightarrow A_v$ for all v. There are three possibilities for (e_v, f_v, g_v) in a quadratic field: ramified $(2,1,1)$, inert $(1,2,1)$ or totally split $(1,1,2)$. Since $m_v = 2$ at every ramified prime, A_F is split iff $f_v = 2$ at every ramified prime. Okay, so why isn't the condition $m_v \mid e_v f_v$? I would think that if $\mathfrak{p}\mathcal{O}_F = \mathfrak{q}^2$ (so $\mathfrak{p} \mid \mathrm{disc}(F/K)$), this would also count as a uniquely extended valuation.

The discriminant of a maximal $\mathcal{O}_K$-order $\mathcal{O}_A \subset A$ is $\mathrm{disc}(A/K) = \prod_v \mathfrak{p}_v^{m_v - 1}$.

Really? Its discriminant has the explicit form where Roquette (5.1) says that A_K is split iff A_{K_v} is split for all v iff $m_v \mid f_v$ for all v (the conditions holding automatically for unramfied v. For a quaternion algebra this means f_v must be even at every ramified v.

6.5 The negative Pell equation

To simplify some aspects of the relevant number theory, is helpful to assume that $h^+ = h$.

Let D_0 be a fundamental discriminant, let m be the squarefree part of D_0 and let $K = \mathbb{Q}(\sqrt{D_0}) = \mathbb{Q}(\sqrt{m})$. Then $x^2 - my^2 = -1$ has an integral solution iff $h_+ = h$ iff $N(u_f) = -1$, because $[\mathcal{O}_K : \mathbb{Z}[\sqrt{m}]] \in \{1, 2\}$ and $[\mathcal{O}_K^\times : \mathbb{Z}[\sqrt{m}]^\times] \in \{1, 3\}$. A necessary condition for $h_+ = h$ is that D_0 be a special discriminant, i.e. not divisible by any $p \equiv 3 \bmod 4$. A discriminant D_0 is non-special iff $\mathrm{CL}_+(K) = \mathbb{Z}/2 \times \mathrm{CL}(K)$, so there are two possibilities for a special discriminant: either $\mathrm{CL}_+ = \mathrm{CL}$, or $\mathcal{L}_+$ is a nontrivial non-split extension of $\mathcal{L}$.

It is a theorem that $h = h_+$ iff D_0 is a special discriminant and $\mathrm{rank}_{2^k}(\mathrm{CL}_+(K)) = \mathrm{rank}_{2^k}(\mathrm{CL}(K))$ for all $k \geq 2$, where

$$\mathrm{rank}_{2^k}(C) = \mathrm{rank}_2(C^{2^k - 1}) = \dim_{\mathbb{F}_2}(C^{2^{k-1}}/C^{2^k})$$

is the 2^k-rank (Fouvry & Kluners). I think this is the same as saying their 2-primary parts are equal.

6.6 Dimensions of the form $d = 4k^2 + 3$

It is also helpful to assume that d is an odd prime, in which case arithmetic in K and the representation theory of $\mathrm{SL}_d(d)$ are simpler than in the general case.

Lemma 6.1. *Let $d = 4k^2 + 3$ for $k \geq 1$. Then $h^+ = h$.*

Proof. Then $D = 16k^2(k^2 + 1)$. If k is even, then $k^2 + 1 \equiv 1 \bmod 4$ and so $D_2 = 1$. If k is odd, then $k^2 + 1 \equiv 2 \bmod 4$ and therefore $D_2 = 8$.

Magma and Sage confirm this. Can't be terribly hard. Maybe my proof that $d \equiv 3 \bmod 4$ is necessary for this generalizes. Scott conjectures this is where the real fiducials live. I conjecture that $h^+ = h$ implies antiunitary stabilizer, though not by complex conjugation in general.

Actually even this might be tricky though at least I know that $h = O(d)$.

□

Lemma 6.2. *Let $d \geq 5$ be prime with $h^+ = h$. Then $d = 4k^2 + 3$.*

Proof. TBP - I proved it has to be $7 \bmod 12$, so $1 \bmod 3$ and $3 \bmod 4$. This means $k^2 \equiv 1 \bmod 3$, so 3 can't divide k. Also note that d is even when k is odd and vice-versa, so we need $k \equiv 1 \bmod 2$ (why did I write that?).

□

The Bunyakovky conjecture implies the following conjecture:

Conjecture 6.3. *There are infinitely many primes of the form $d = 4k^2 + 3$.*

Proof. The polynomial $4k^2 + 3$ is irreducible over $\mathbb{Z}$ and satisfies $\gcd(\{4k^2 + 3 : k \geq 1\}) = 1$, since it represents at least two primes. So the Bunyakovsky conjecture implies the lemma. □

There are 108 primes less than a million of the form $4k^2 + 3$, making up nearly 22% of all such numbers. The primes less than 10000 of this form are

$$7, 19, 67, 103, 199, 487, 787, 1447, 2503, 2707, 3847, 4099, 4903, 5479, 5779, 8467, 8839,$$

corresponding to

$$k = 1, 2, 4, 5, 7, 11, 14, 19, 25, 26, 31, 32, 35, 37, 38, 46, 47.$$

Let $d = 4k^2{+}3$ be prime. Then $D = (d{-}3)(d{+}1) = 16k^2(k^2{+}1) = (4k)^2 D'$, with $D' = k^2{+}1 = \frac{d+1}{4}$. Let $\mathfrak{p}\mathfrak{p}' = d\mathcal{O}_K$.

Among the 108 such primes less than a million, there are ten for which K has trivial class group: $d = 7, 19, 67, 199, 787, 2707, 4099, 5779, 19603, 132499$. Among these, $d = 19, 199, 19603, 132499$ have $r = 3$, $d = 5779$ has $r = 9$ and the remaining 103 primes have $r = 1$. The 3-parts of $d - 1$ for the 10 d with $h = 1$ are $3, 9, 3, 9, 3, 3, 3, 27, 81, 9$, which are divisible by $3r$ but not equal to the last two. I don't yet know how to predict r but we should note that $d = 1 + u_+^r + u_+^{-r}$ implies that $4k^2 = u_+^r + u_+^{-r} - 2 = (u_f^r - u_f^{-r})^2$, so $k = \frac{u_f^r + u_f^{-1}}{2}$ (nice!). Then H decomposes under the action of $\mathrm{SL}_2(d)$ into a direct sum of $1 + k^2 = 1 + \frac{d-3}{4}$ principal series representations

$$H = \bigoplus_{\chi \in \Lambda} \widetilde{\mathcal{P}}_\chi,$$

where Λ is a complete set of representatives for the orbits of $\chi \mapsto \chi^{-1}$ in $\ker(\widehat{T}_{d-1} \to \widehat{T}_2)$.

For $3r \mid m \mid d-1$, let $t_m = \left(\begin{smallmatrix} a_m & \\ & a_{-m} \end{smallmatrix}\right)$ generate T_m, and let $T'_m = \langle T_m, \left(\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right)\rangle$, where $t_m z_i = z_{a_m i}, t_m \bar{z}_i = \bar{z}_{a_m i}$, and $\left(\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right) z_i = \bar{z}_i$.

Conjecture 6.4. *Let*

$$J_m = R[\{z_i \bar{z}_j - z_i^t \bar{z}_j^t : t \in T'_m\}] = I(\mathrm{Proj}(R)^{T'_m})$$

be the ideal of the T'_m-fixed points in $\mathrm{Proj}(R)$. *Then there exists a polynomial $f(x) \in \mathbb{Q}[x]$ such that $\mathbb{Q}[z_1] \cap (RH + J + R(z_0 - 1)) = (f(z_1))$ and $\mathbb{Q}[x]/(f(x)) \simeq K^{\mathfrak{p}\infty_-}$, where $d\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$.*

Actually, this conjecture needs to be souped up a bit. Handle loss of $\bar{z}$s better.

6.7 $d = 4k^2 + 3$

Let $d = 4m + 3$. Then $D = 16(m^2 + m)$. If $d = 4k^2 + 3$, then $D = 16k^2(k^2 + 1)$ and we have observed that $N(u_f) = -1$. We have seen that if $N(u_f) = -1$, then we must have $d \equiv 0, 3 \bmod 4$. So for odd d, it is necessary to have $d = 4m + 3$ to have $N(u_f) = -1$ – most such d are such that m is a square, but there are plenty of exceptions such as

$$m = 8, 80, 288, 360, 1088, 2600, 5328, 9800, 16640, 25920, 26568, 40400, 59048, 83520, \ldots,$$

i.e.

$$d = 35, 323, 1155, 1443, 4355, 10403, 21315, 39203, 66563, 103683, 106275, 161603, 236195, 334083 \ldots,$$

up to $m \le 100000$, i.e. $d \le 400000$.

The fundamental discriminant factors as $D_0 = D_2 D'$, with $D_2 \in \{1, -4, -8, 8\}$ and D' odd. If k is even, then $k^2 + 1 \equiv 1 \bmod 4$, so $D_2 = 1$ and $D_0 = D' = (k^2 + 1)/f^2$ for some odd f. If k is odd, then $D_2 = 8$ and $D' = (k^2 + 1)/(2f)^2$ for some odd f. Since squares of odd numbers are $\equiv 1 \bmod 4$, this implies that $D' \equiv 1 \bmod 4$ for all k. Therefore, $D_p \mid D'$ implies that $p \equiv 1 \bmod 4$, so D is only divisible by positive prime discriminants, hence every quadratic subfield of the genus field is real. Why does this imply the existence of a negative norm unit? Does the nonexistence imply that the genus field is complex???

Let n be squarefree. Then $n \not\equiv 0 \bmod 4$. If $n \equiv 1 \bmod 4$, then it is a quadratic discriminant and $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$. Otherwise, $4n$ is a quadratic discriminant and $\mathcal{O}_K = \mathbb{Z}[\sqrt{n}]$. So when k is odd, we need to show there is a negative norm unit $a + b\sqrt{n}$ (with $n = 2D'$) i.e. with $a^2 - 2D'b^2 = -1$. When k is even, we need a unit $a + b\frac{1+\sqrt{n}}{2}$ (with $n = D'$) with $a^2 - \frac{D'-1}{4}b^2 = -1$.

7 Existence

7.1 Conjectural structure of complexified fiducials.

Here we further refine the conjecture of [**Kop18**, 2, 3]: For each $d \geq 2$, $\mathrm{Proj}(R/RH_2)$ is non-empty and consists only of Hermitian points. If $d = 3$, $\mathrm{Proj}(R/RH_2)$ consists of 8 one-dimensional components.

Let $d \geq 4$ and let $D = (d-3)(d+1) = f^2 D_0$ with D_0 a fundamental discriminant. Let $b = \frac{d-1-\sqrt{D}}{2}$ and note that $\mathcal{O}_D = \mathbb{Z}[b]$ is the order of discriminant D. Let $K = \mathbb{Q}(\sqrt{D})$ be the quadratic field with maximal order $\mathcal{O}_K = \mathcal{O}_{D_0}$. Then $\mathrm{Proj}(R/RH_2)$ is 0-dimensional, with residue fields embedding into the ring-ray class field $K^{d'\mathcal{O}_D\infty}$ of the quadratic order $\mathcal{O}_D$ of conductor $d'\mathcal{O}_D\infty$, where d' is d for odd d and $2d$ for even d. Furthermore, there is a 1-1 correspondence between the closed points of $\mathrm{Proj}(R/RH_2)$ and pairs $(\mathcal{O}, \phi)$, with $\mathcal{O}$ an order containing b and $\phi : \mathcal{O} \to (\mathbb{Z}/d')^{2\times 2}$ a homomorphism taking units to $\mathrm{ESL}_2(d')$ giving a reciprocity law for the relevant class fields via the Weil representation.

In particular, $\phi(\mathcal{O}^\times)$ contains an order-3 torus.

Because

$$b^3 = 1 - d\left(\frac{d^2-3d}{2} - \left(\frac{d-1}{2}\right)\sqrt{D}\right),$$

we see that $b^3 \equiv 1 \bmod d\mathbb{Z}[b]$.

7.2 Towards an existence proof.

Here we aim to prove that $\mathrm{Proj}(R/RH)$ contains at least one Hermitian point in infinitely many dimensions through the following steps:

1. Prove that $\mathfrak{p} \supset RH$ for some $\mathfrak{p} \in \mathrm{Proj}(R)$ with $\mathfrak{p} = \overline{\mathfrak{p}}$.

2. Prove that $\kappa(\mathfrak{p})$ has a complex embedding with $\bar{\cdot}$ acting as complex conjugation.

For 1., I can produce a prime ideal by adding generators for the ideal of fixed points of group of transformations, producing an ideal $I = RH + I' = \mathfrak{p} + J$, where $\mathfrak{p}$ is prime and $\sqrt{J} = R_+$ (at least in dimension 7, though it seems to generalize). For 2., it may be necessary to prove that the residue fields are abelian extensions of K, then to verify that $\bar{\cdot}$ agrees with the Artin map σ^+_{-1}.

Note the points $\mathfrak{p}$ fixed by $\bar{\cdot}$ are precisely those in the image of the embedding $\phi : \mathrm{Proj}(S) \to \mathrm{Proj}(R)$ given by $\mathfrak{q} \mapsto \bigoplus \mathfrak{q}_n \otimes \overline{\mathfrak{q}}_n$. To be a closed embedding, would need that for every affine open $\mathrm{Spec}(B) \subset \mathrm{Proj}(R)$ with $\pi^{-1}(\mathrm{Spec}(B)) \simeq \mathrm{Spec}(A)$, the corresponding map $B \to A$ is surjective. For instance, if $\mathrm{Spec}(B) = D(\alpha)$, then what is $\mathrm{Spec}(A) \subset \mathrm{Proj}(S)$? In this case $B = R[\alpha^{-1}]_0$, wh

If $F/\mathbb{Q}$ is an extension field, an F-valued point $\mathrm{Spec}(F) \to \mathrm{Proj}(R)$ determines a closed point $\mathfrak{p}$ together with compatible algebra homomorphisms $\mathcal{O}_{\mathrm{Proj}(R)}(U) \to F$ on the affine opens $U \subset \mathrm{Proj}(R)$ not containing $\mathfrak{p}$. Given $\alpha \in R_1$, the basic open $D(\alpha) = \{\mathfrak{p} \in \mathrm{Proj}(R) : \alpha \notin \mathfrak{p}\}$ satisfies $D(\alpha) \simeq \mathrm{Spec}(R[\alpha^{-1}]_0)$, with $\mathfrak{p}$ corresponding to the prime ideal

$$(R[\alpha^{-1}]\mathfrak{p}_0) = R[\alpha^{-1}](\mathfrak{p}_0 + \mathfrak{p}_1/\alpha_0 + \mathfrak{p}_2/\alpha_0^2 + \cdots)$$

of $R[\alpha^{-1}]_0$.

If the corresponding closed point $\mathfrak{p} \in \mathrm{Proj}(R)$ is Hermitian and the pullback $\phi : R[\alpha^{-1}]_0 \to F$ to any affine $\mathrm{Spec}(R[\alpha^{-1}]_0) \simeq D(\alpha_0) \subset \mathrm{Proj}(R)$ satisfies $\phi^*(\overline{f}/\overline{g}) = \overline{\phi^*(f/g)}$ for all f, g, homogeneous of the same degree with $g \notin \mathfrak{p}$. In particular, the Hermitian points are contained in the distinguished open $D(\alpha_0) \subset \mathrm{Proj}(R)$, where $\alpha_0 = \|z\|_2^2 = \sum z_i \bar{z}_i$.

7.3 Real points

Let $R = \mathbb{Q}[z] \times_{\mathbb{Q}} \mathbb{Q}[\bar{z}]$ and equip it with the involution $\bar{\cdot}$. If M is an R-module, a **Hermitian form** is a function $h : M \times M \to R$ such that $h(ra, b) = \bar{r}h(a, b)$ and $h(a, rb) = rh(a, b)$. This is a very general definition that might make sense for more basic rings with involution (such as complex number fields) but it may be useful in this context, as it is over $\mathbb{Q}$ yet remembers enough structure for base changes. The relevant R-modules for me are the points of $\mathrm{Proj}(R)$, and more specifically, of $\mathrm{Proj}(R/RH)$ or even of $\mathrm{Proj}(R/(RH + R[R_1^{T_3}])$, etc.

$\mathbb{P}^{d-1}_{\mathbb{R}} = \mathrm{Proj}(\mathbb{R}[z])$ are the homogeneous ideals of $\mathbb{R}[z]$ not containing (z). The set of $\mathbb{C}$-valued points $\mathbb{P}_{\mathbb{R}}(\mathbb{C})$ consists of morphisms $\mathrm{Spec}(\mathbb{C}) \to \mathbb{P}_{\mathbb{R}}$ determining a closed point $\mathfrak{p} \in \mathbb{P}_{\mathbb{R}}$ and an embedding $k_{\mathfrak{p}} \hookrightarrow \mathbb{C}$ of the residue field.

The closed points are those points of dimension 0 and are in 1-1 correspondence with the $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-orbits of $\mathbb{C}$-valued points.

The $\mathbb{R}$-valued points $\operatorname{Spec}(\mathbb{R}) \to \mathbb{P}_{\mathbb{R}}$ are in 1-1 correspondence with the closed points the form $\mathfrak{p} = (z_i a_j - z_j a_i : 0 \le i, j < d)$ for some $a \in \mathbb{R}^d \smallsetminus 0$. These are the points with residue field $\mathbb{R}$. The closed points are in 1-1 correspondence with the $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-orbits in $\mathbb{P}^{d-1}(\mathbb{C})$. So how does $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ act on points $\operatorname{Spec}(\mathbb{C}) \to \mathbb{P}^{d-1}_{\mathbb{R}}$?

The closed points $\mathfrak{p}$ with residue field $\mathbb{C}$ satisfy $\mathbb{C}[z]\mathfrak{p} = \mathfrak{q}\bar{\mathfrak{q}}$, where $\mathfrak{q} = (z_i a_j - z_j a_i : 0 \le i, j < d)$ for some $a \in \mathbb{C}^d \smallsetminus \mathbb{R}^d$. In particular, $\mathfrak{p} = \mathfrak{q}\bar{\mathfrak{q}} \cap \mathbb{R}[z]$.

The closed points are in 1-1 correspondence with the space $\mathbb{P}^{d-1}(\mathbb{C})/\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ of orbits of $\mathbb{C}$-valued points under complex conjugation. The orbits of size 1 are in 1-1 correspondence with the $\mathbb{R}$-valued points $\mathbb{P}^{d-1}_{\mathbb{R}}(\mathbb{R})$, as well as with the closed points with residue field $\mathbb{R}$, which are generated by linear forms and have the form

The orbits of size 2 are in 1-1 correspondence with the closed points $\mathfrak{p}$ with residue field $\mathbb{C}$. In $\mathbb{C}[z]$, these split into a product of ideals generated by linear forms

$$\mathfrak{p}\mathbb{C}[z] = ((z_i a_j - z_j a_i)(z_k \bar{a}_\ell - z_\ell \bar{a}_k)) : 0 \le i, j, k, \ell < d)$$

or rather,

$$\mathfrak{p}\mathbb{C}[z] = ((z_i z_k a_j \bar{a}_\ell - z_i z_\ell a_j \bar{a}_k - z_j z_k a_i \bar{a}_\ell + a_i z_\ell a_j \bar{a}_k)) : 0 \le i, j, k, \ell < d).$$

Is this ideal invariant under complex conjugation? Get $\mathfrak{p}$ by intersecting with $\mathbb{R}[z]$, leaving

The cartesian product satisfies $R = \mathbb{R}[z] \times_{\mathbb{R}} \mathbb{R}[\bar{z}] = \mathbb{R}[z, \bar{z}]_0$ for the grading with $\deg(z_i) = -\deg(z_i) = 1$. Each pair of points $\mathfrak{p} \in \operatorname{Proj}(\mathbb{R}[z])$ and $\mathfrak{q} \in \operatorname{Proj}(\mathbb{R}[\bar{z}])$determines a point

$$\mathfrak{p}_0\mathfrak{q}_0 + \mathfrak{p}_1\mathfrak{q}_1 + \cdots \in \operatorname{Proj}(R)$$

and every point of $\operatorname{Proj}(R)$ has such a form.

8 Polynomial functions on projective space

Let k be a commutative ring and consider the graded k-algebra

$$R = k[z] \times_k k[\bar{z}] = \bigoplus_{n \geq 0} R_n,$$

where $R_n = k[z]_n \otimes_k k[\bar{z}]_n = k[z, \bar{z}]_{n,n}$ is the space of homogeneous degree-(n,n) polynomials. We may identify $\operatorname{Proj}(R) \simeq \mathbb{P}_k^{d-1} \times_k \mathbb{P}_k^{d-1}$ with with the space of $k^\times$-orbits of rank-1 matrices in $k^{d \times d}$.

Let $a \mapsto \bar{a}$ be an involution on k (possibly trivial) with fixed subring k'. Extend the involution to R so that it swaps z_i and $\bar{z}_i$ as the notation suggests. We may embed $\mathbb{P}_k^{d-1} \hookrightarrow \operatorname{Proj}(R)$ over k' via $[v] \mapsto [v \otimes \bar{v}]$, where the involution acts coordinatewise on $v \in k^d \smallsetminus 0$. This identifies the Weil restriction $(\mathbb{P}_k^{d-1})_{k'}$ with the Hermitian fixed points under the "conjugate transpose" involution $[v \otimes w]^\dagger = [\bar{w} \otimes \bar{v}]$. If $k \subset \mathbb{C}$ and the involution is complex conjugation, this identifies $\mathbb{P}_k^{d-1}$ with the rank-1 Hermitian matrices in $k^{d \times d}$.

In what follows, choices for the base ring k may include $\mathbb{Z}, \mathbb{Q}, \mathbb{Q}(\zeta_d)$ as well as $K = \mathbb{Q}(\sqrt{D})$ and $\mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$ for quadratic discriminants $D > 0$.

Make sure this is all properly set up so that, e.g. it still works when the involution is trivial on k such as for $\mathbb{Q}$. What role does $\operatorname{Gal}(K/\mathbb{Q})$ play? If F/K is an abelian extension with complex conjugation $c \in \operatorname{Gal}(F/K)$, then $U_d(F, c)^\tau = \mathrm{U}_d(F, c')$, where $c' = \tau c \tau \in \operatorname{Gal}(F/K)$ is not complex conjugation in the chosen embedding, but is for half the embeddings. If F_{CM} is the max CM subfield, then $\mathrm{U}_d(F, c) \cap \mathrm{U}_d(F, c') = \mathrm{U}_d(F_{\mathrm{CM}})$.

If F/k is an extension of rings, the F-valued points of $\operatorname{Proj}(R)$ can locally be described as homomorphisms $\phi : \mathcal{O}(U) \to F$ taking $f/g \in \mathcal{O}(U)$ (so f, g homogeneous of the same degree and g nowhere vanishing on U) to $\phi(f/g) = f(u,v)/g(u,v) \in F$, where $[u \otimes v] \in U$. If F has an involution extending that of k, the F-valued points of $(\mathbb{P}_k^{d-1})_{k'}$ correspond to the maps $\phi : \mathcal{O}(U) \to F$ that are equivariant with respect to the involutions, i.e. $\phi(\bar{f}/\bar{g}) = \overline{\phi(f/g)}$ for all $f/g \in \mathcal{O}(U)$.

The image of the embedding of $(\mathbb{P}_k^{d-1})_{k'}$ is contained in a specific affine patch of $\operatorname{Proj}(R)$, constrasting the lack of an affine embedding of $\mathbb{P}_k^{d-1}$ over k. Let $\alpha_0 \coloneqq \sum_a z_a \bar{z}_a \in R_1$ and note that it does not vanish on $(\mathbb{P}_k^{d-1})_{k'}$. Hence $(\mathbb{P}_k^{d-1})_{k'}$ is contained in the basic open set $D(\alpha_0) = \{[v \otimes w] : v \cdot w \neq 0\} \subset \operatorname{Proj}(R)$, which we identify with the space of $k^\times$-orbits of all rank-1 matrices over k with nonvanishing trace. Furthermore, $D(\alpha_0)$ is in bijection with the closed subset $V(\alpha_0 - 1)$ of the affine cone $\operatorname{Spec}(R)$ of $\operatorname{Proj}(R)$, which we identify with the set of all rank-1 matrices over k with unit trace. Note that $R_+ \notin V(\alpha_0 - 1)$, so it is only inhomogeneity keeping it from being a subset of $\operatorname{Proj}(R)$. Viewed as a subset of $V(\alpha_0 - 1)$, $(\mathbb{P}_k^{d-1})_{k'}$ is therefore identified with the set of rank-1 Hermitian projections. Taking $k/k' = \mathbb{C}/\mathbb{R}$ gives the usual setting, but the algebraic nature of the solutions requires this more general approach. Not sure if I'm saying this completely right (see Vakil 4.5.1, 8.2.12). Note that there is a natural morphism $\operatorname{Spec}(R) \smallsetminus V(R_+) \to \operatorname{Proj}(R)$, corresponding to discarding the origin.

8.1 Solving the equations

Let

$$R = \mathbb{Q}[z] \times_{\mathbb{Q}} \mathbb{Q}[\bar{z}] = \bigoplus_n \mathbb{Q}[z]_n \otimes_{\mathbb{Q}} \mathbb{Q}[\bar{z}]_n = \bigoplus_n \mathbb{Q}[z, \bar{z}]_{n,n} \simeq \bigoplus_n \mathrm{End}(\mathrm{Sym}^n(V))$$

so that $\mathrm{Proj}(R) \simeq \mathbb{P}^{d-1} \times \mathbb{P}^{d-1}$. Points of $\mathrm{Proj}(R)$ are homogeneous prime ideals $\mathfrak{p} \not\supset R_+$. F-rational points of $\mathrm{Proj}(R)$ are morphisms $\mathrm{Spec}(F) \to \mathrm{Proj}(R)$, i.e. of locally ringed spaces. They correspond to homogeneous maximal ideals $\mathfrak{p} \in \mathrm{Proj}(R)$ equipped with an embedding of the residue field $R_{(\mathfrak{p})}/\mathfrak{m}_{\mathfrak{p}}$ into F, where $\mathfrak{m}_{\mathfrak{p}}$ is the unique maximal ideal of $R_{(\mathfrak{p})}$.

Let $\alpha_0 = \bar{z}^T z$ and consider the closed subscheme $V(\alpha_0 - 1) \subset \mathrm{Proj}(R)$. Elements of R restrict to functions on $V(\alpha_0 - 1)$. More specifically, its coordinate ring is $R/(\alpha_0 - 1)$. The open projective subscheme $D(\alpha_0)$ on which α_0 does not vanish is the cone over $V(z^\dagger z - 1)$. Elements $f \in R_n$ determine functions f/α_0^n

Equivalently, they should be (certain) algebra homomorphisms $\phi : R \to F$.

If $F \subset \mathbb{C}$, F-rational points satisfying $\phi(\bar{f}) = \phi(f)^c$ can be identified with points of $F\mathbb{P}^{d-1}$ as follows.

For $j \in (\mathbb{Z}/d)^2$, define

$$\alpha_j := \bar{z}^T \Delta_j z = (-\zeta_{2d})^{j_1 j_2} \sum_k \zeta_d^{j_2 k} z_k \bar{z}_{k+j_1}.$$

I claim the α_j span $R_1 \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d)$, while $R \simeq_{\mathbb{Q}(\zeta_d)} \mathbb{Q}[\alpha]$ is generated by its degree-1 elements. The corresponding cyclotomic coordinate ring $R_{\mathbb{Q}(\zeta_d)} = R \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d)$ is multigraded

$$R_{\mathbb{Q}(\zeta_d)} = \bigoplus_{n \geq 0, j \in (\mathbb{Z}/d)^2} R_{n,j}$$

with $\deg(\alpha_j) = (1, j)$. Then $R_{0,0} = \mathbb{Q}(\zeta_d)$, $R_{0,j} = 0$ and $R_{1,j} = \mathbb{Q}(\zeta_d)\alpha_j$.

The space $R_{2,0}$ of quadratic invariants is spanned by the polynomials

$$\beta_j = \alpha_j \alpha_{-j} = \sum_{a,b} \zeta_d^{j_2(a-b)} z_a \bar{z}_{a+j_1} z_{b+j_1} \bar{z}_b.$$

which are in 1-1 correspondence with the set of orbits $(\mathbb{Z}/d)^2/\langle -I, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$. Fiducials are the solutions to the equations $\tilde{\beta}_j = (d+1)\beta_j - \beta_0$ for $j \neq 0$. These equations are harmonic, as $\nabla \beta_0 = 2(d+1)\alpha_0$ and $\nabla \beta_j = 2\alpha_0$ for $j \neq 0$ (CHECK THAT!!!). Furthermore, $R_{2,0}$ is rational, as can be seen by computing the j_2-Fourier transform of the β_j

$$\gamma_j = \frac{1}{d} \sum_k \zeta_d^{-kj_2} \beta_j = \sum_a z_a \bar{z}_{a+j_1} \bar{z}_{a+j_2} z_{a+j_1+j_2},$$

which span the same space but have rational coefficients. On the other hand, we may also write $\tilde{\beta}_j = (d+1)\beta_j - (d\delta_j + 1)\beta_0$ (which implies that $\tilde{\beta}_0 = 0$). Then the identity

$$\frac{1}{d} \sum_k \zeta_d^{-kj_2} (d\delta_j + 1) = \delta_{j_1} + \delta_{j_2}$$

implies that the transformed $\tilde{\beta}_j$ are $\tilde{\gamma}_j = (d+1)\hat{\beta}_j - (\delta_{j_1} + \delta_{j_2})\beta_0$. Hence the fiducials are defined over $\mathbb{Q}$. The $\tilde{\gamma}_j$ are also harmonic but I don't have a good argument yet.

Projectively, the coordinate α_0 can be anything nonzero and I get a function on the open set $\{\alpha_0 \neq 0\}$ by taking β_j/α_0^2. *This* is the way to view this.

In all the above, I think the $\tilde{\gamma}_j$ and $\tilde{\beta}_j$ are just restricting things to the harmonic subspace.

More things: The degree shift $R(-2,0)$ is generated in degree $(2,0)$. Is this literally the module $R_{2,0}R$?

One thing hard about multigrading by torsion is that the associated primes of graded modules may not be graded. This is apparently handled by lifting to modules graded by an infinitely generated torsion-free group. However, there is still Proposition 8.18 in Miller-Sturmfels: Every finitely generated multigraded R-module has a finite multigraded free resolution by modules of the form $R(-b_1) \oplus \cdots \oplus R(-b_r)$, even if multigraded by torsion.

The multigraded ideal $R_{2,0}R$ generated by all degree-2 invariants should be the degree shift $R(-2,0)$, for which $R(-2,0)_{n,j} = R_{n-2,j}$. However, this ideal is too large and we really want the ideal generated by the harmonic subspace $H_{2,0} \subset R_{2,0}$.

First note that $\nabla z_a \bar{z}_b z_c \bar{z}_d$ vanishes if $\{a,c\} \cap \{b,d\} = \varnothing$. If the intersection is $\{a\}$ (say $a = b$ but $b \neq d$), it is $z_c \bar{z}_d$ and if $a = b \neq c = d$, it gives We compute

$$\nabla z_a \bar{z}_b z_c \bar{z}_d = \delta_{ab} z_c \bar{z}_d + \delta_{ad} z_c \bar{z}_b + \delta_{bc} z_a \bar{z}_d,$$

which gives

$$\nabla \beta_j =$$

but note this vanishes for $j = 0$ since we made it projective. Therefore all we need to have is $\beta_j - \frac{1}{d+1}\beta_0 = 0$. Are those the harmonic parts? I thought the β_j were harmonic to start with, since their operators are traceless. Ahah, but maybe restricting to $P_\pm$ just means what I was calling $\beta_j^\pm$ would just have opposite traces...

Note that $\nabla \beta_0 = 2(d+1)\alpha_0$. So I would think that to be harmonic, we would need $\nabla \beta_j = 2\alpha_0$ for all j.

The subspace $R_{2,0}$ decomposes as $\mathbb{Q}(\zeta_d)\|z\|_2^2 + \mathrm{Sym}^{2,2}(V)_0$; the second term is the harmonic ones and the subscript means homogeneous for the $(\mathbb{Z}/d)^2$-grading. Projecting on to the harmonic subspace gives $\gamma_j = (d+1)\beta_j - d\delta_j - 1$ and

$$\hat{\gamma}_j = (d+1)\beta_j - (\delta_{j_1} + \delta_{j_2})\|z\|_2^2.$$

Since they are defined over $\mathbb{Q}$, ($\mathbb{Z}$ in fact), let $\mathfrak{a} = R_{2,0}R$ be the ideal they generate. I want to show that $\mathfrak{a}$ is 0-dimensional, reduced and that

$$\mathfrak{a} = \prod_{D_0|D'|D} \mathfrak{a}_{D'} = \bigcap_{D_0|D'|D} \mathfrak{a}_{D'},$$

where $V(\mathfrak{a})$ is a Clifford orbit of fiducials (and their τ-conjugates). Furthermore, each $\mathfrak{a}_{D'}$ should factor into a product $\mathfrak{a}_{D'} = \mathfrak{b}_1 \cdots \mathfrak{b}_{m_{D'}}$ of prime ideals, where $m_{D'} = \ldots$ The Clifford gropu acts on each set of $\mathfrak{b}_i$ transitively. Finally, I want to show that over $R_{\mathcal{O}_{D'}}$, each of these ideals factors further into a $\mathrm{Gal}(K/\mathbb{Q})$-orbit of primes as $\mathfrak{b}_i R_{\mathcal{O}_{D'}} = \mathfrak{c}_i \mathfrak{c}_i'$.

8.2 Where we are

Let $R = \mathbb{Q}[z] \times_{\mathbb{Q}} \mathbb{Q}[\bar{z}]$ and let $X = \operatorname{Proj} R = \{\text{homogeneous prime } \mathfrak{p} \subset R : R_+ \not\subset \mathfrak{p}\}$. If $k \subset \overline{\mathbb{Q}}$, then the k-rational points $X(k)$ are morphisms $\operatorname{Spec}(k) \to X$. To do: unpack this definition to see if it gives $X(\mathbb{R}) \simeq \mathbb{CP}^{d-1}$ or even $X(K^{(d)\infty_-}) \simeq K^{(d)\infty}\mathbb{P}^{d-1}$. Note that k-rational points of $\operatorname{Spec}(R)$ are just algebra homomorphisms $R \to k$. Another idea is to work with $\operatorname{Spec}(R/(\alpha_0 - 1))$.

$\mathbb{Q}$-algebra homomorphisms $R \to k$. TO DO: Define properly so that

Let $S = R^{(\mathbb{Z}/N)^2}$ be the graded algebra of invariants and note that $\operatorname{Proj} R_{\cdot,0} \simeq X//(\mathbb{Z}/d)^2$ (GIT quotient). We are interested in the ideals $RH_{2,0}$ and $SH_{2,0}$ generated by the harmonic invariants in degree 2.

In $d = 2$, RH_{20} factors into two prime ideals, whereas $SH_{2,0}$ factors into two *maximal* ideals, one for each SIC.

In $d = 3$ may require more work to do properly.

In $d = 4$, there is a single Clifford orbit, containing $|\mathrm{SL}_2(4)|/3 = 16$ SICs. Each fiducial corresponds to two solutions over $\mathbb{C}$ but only one over the real subfield $\mathbb{R}$. The ideal $RH_{2,0}$ factors into 32 primary ideals of R, whereas $SH_{2,0}$ factors into only 2 primary ideals of S. Each associated prime factors into a $\mathrm{Gal}(K/\mathbb{Q})$ orbit of 2 prime ideals over K. I think one splits over F_+ and the other over F_-, in each case into a $\mathrm{Gal}(F/K)$-orbit of 8 fiducials/SICs. In other words, there are two prime ideals of S_K, teach of whose zero set contains 8 of the 16 SICs.

The thing to note is that the $(\mathbb{Z}/d)^2$-grading is gone if we focus on the ring S of invariants. However, there is at this point a $\mathrm{GL}_2(d)$-action on the β (or maybe $\mathrm{SL}_2(d)$ or $\mathrm{SL}_2(2d)$).

Now, the β are defined over $\mathbb{Q}(\zeta_d)$, but the $\hat{\beta}_j = \frac{1}{d}\sum_a \zeta^{-kj_2}\beta_{j_1 k}$ are defined over $\mathbb{Z}$. Note that $\nabla\beta_j = 2(d\delta_j + 1)\alpha_0$, so $(d+1)\beta_j - \beta_0$ is harmonic for $j \neq 0$. Also must be the case that $\nabla\hat{\beta}_j = \ldots$

9 Algebraic properties of fiducials

Assume for now that d is odd. Let $D = (d-3)(d+1) = f^2 D_0$, with D_0 a fundamental discriminant and let $K = \mathbb{Q}(\sqrt{D})$. The set of fiducials is actually contained in $F\mathbb{P}^{d-1}$, where F is the ring-ray class field $K^{d\mathcal{O}_D\infty}$ associated to the quadratic order $\mathcal{O}_D = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right] = \mathbb{Z} + f\mathcal{O}_K$. The centralizer of complex conjugation is $\mathrm{Gal}(F/K)$, which acts on fiducials since it commutes through the hermitian inner product. Does $\mathrm{Gal}(F/\mathbb{Q})$ act on the set of not-necessarily-Hermitian fiducials in $\mathbb{CP}^{d-1} \times_{\mathbb{C}} \overline{\mathbb{CP}}^{d-1}$?

The projective generalized Clifford group

$$0 \to (\mathbb{Z}/d)^2 \to \mathrm{Aut}_{\mathbb{C}}(H) \to \mathrm{SL}_2(d) \to 1$$

acts on the set of fiducials, decomposing them into finitely many orbits, each an $\mathrm{SL}_2(d)$-orbit of $(\mathbb{Z}/d)^2$-orbits, or SIC-POVMs.

We can also look at $\mathrm{Aut}_{\mathbb{R}}(H)$, which includes complex conjugation, but I'm not sure whether that is a good idea. On the other hand, if we choose the Δ_j so that $H = \langle\{\Delta_j\}\rangle \subset \mathrm{U}_d(F)$, we could define $\mathrm{Aut}_L(H)$ for various subfields $L \subset F$. Here is a plausible way that the fields of definition could be organized:

- $[v_0]$ defined over F (or an index-2 subfield if $K^\infty = K^{(1)}$)
- $(\mathbb{Z}/d)^2 \cdot [v_0]$ defined over K^∞
- $\mathrm{Aut}_{\mathbb{C}}(H) \cdot [v_0]$ defined over K
- Set of all fiducials defined over $\mathbb{Q}$

The multiplets of SIC-POVMs in dimension d are in 1-1 correspondence with quadratic orders $\mathcal{O}_D \subset \mathcal{O} \subset \mathcal{O}_{D_0} = \mathcal{O}_K$, where $D = (d-3)(d+1)$. The field of definition is the ring-ray class field $K^{d'\mathcal{O}\infty} = K^{\mathcal{O}} K^{(d')\infty}$ (sure that's the right definition?). We mainly focus on the minimal multiplets, which are defined over the ray class field $K^{(d')\infty}$.

We have

$$\begin{aligned}
P_0^{\sigma_a} &= \frac{1}{d}\sum_j \alpha_j^{\sigma_a} \Delta_{-j}^{\sigma} = \frac{1}{d}\sum_j \alpha_{g_a j} \Delta_{-h_a j} \\
&= \frac{1}{d}\sum_j \alpha_{f_a j} \Delta_{-j} \frac{1}{d}\sum_j \alpha_j \Delta_{-f_a^{-1} j} \\
&= U_{f_a^{-1}} P_0 U_{f_a},
\end{aligned}$$

where $g_a = f_a h_a$, with $h_a = \left(\begin{smallmatrix} 1 & 0 \\ 0 & k_a \end{smallmatrix}\right)$ such that $\zeta_d^{\sigma_a} = \zeta_d^{k_a}$. Therefore, $f_a P_0^{\sigma_a} f_a^{=1} = P_0$. Therefore, if $\sigma \mapsto f_\sigma = f_{\sigma_a}$ for some a with $\sigma_a = \sigma$, then P_0 is a fixed point for the f-twisted "action" $\sigma \cdot_f P_0 = P_0$. If we can choose the f_σ to be a 1-cocycle ($f_{\sigma\tau} = f_\sigma f_\tau^\sigma$), this does give a group action and the fixed points in some interesting algebra? One thing: I think the algebra has to be split to contain any rank-1 element, so any twisting that fixes P_0 would need to be by a cohomologically trivial 1-cocycle.

We always have extensions

$$\begin{tikzcd}
1 \arrow[r] & T_{\mathrm{SL}} \arrow[r] \arrow[d] & T_{\mathrm{GL}} \arrow[r] \arrow[d] & (\mathbb{Z}/d)^\times \arrow[r] & 1 \\
1 \arrow[r] & \mathrm{SL}_2(d) \arrow[r] & \mathrm{GL}_2(d) \arrow[r] & (\mathbb{Z}/d)^\times \arrow[r] & 1
\end{tikzcd}$$

Choose a section $\phi : (\mathbb{Z}/d)^\times \to T_{\mathrm{GL}}$ and let $s_{\alpha_1,\alpha_2} \in T_{\mathrm{SL}}$ be the corresponding 2-cocycle, for which $s_1\phi(\alpha_1)s_2\phi(\alpha_2) = s_{\alpha_1,\alpha_2}s_1s_2\phi(\alpha_1\alpha_2)$. For prime $d \equiv 1 \bmod 3$, we can choose $\phi(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$ and the cocycle is trivial, but for prime $d \equiv 2 \bmod 3$, this is not possible as T_{GL} is not split.

Assume $P_0 = v_0v_0^\dagger$ be a strongly centered fiducial and let $v_j = \Delta_j v_0$ and $P_j = v_jv_j^\dagger$. The overlaps for P_0 satisfy

$$\alpha_j = \operatorname{Tr} P_0\Delta_j = \langle v_0, \Delta_j v_0\rangle = \langle v_0, v_j\rangle,$$

while those for P_k satisfy

$$\operatorname{Tr} P_k\Delta_j = \zeta_d^{j_1k_2-j_2k_1}\alpha_j$$

(or something like that ±).

Let $K_d^\times = \{a \in K^\times : ((a),(d)) = 1\}$ (a localization of $\mathcal{O}_K$?). There is apparently a homomorphism $K^\times(d) \to T_{\mathrm{GL}}$, $a \mapsto g_a$, with image a maximal torus, such that $\alpha_j^{\sigma_a} = \alpha_{g_aj}$, where $\sigma_a = \mathrm{Art}((a)) \in \mathrm{Gal}(K^{(d)\infty_+}/K^{(1)})$. Maybe better to phrase in terms of the ideal group $(K^\times(d)) \subset P$, or just $(\mathcal{O}_K/d)^\times$.

The numbers $(d+1)\alpha_j^2$ are Galois conjugates of Stark units $e^{Z'_\sigma(0)}$ for $\sigma \in \mathrm{Gal}(K^{(d)\infty_-})$. What does the Weil representation have to do with this?

10 Algebraic formulation

Let $S = \mathbb{Q}[z]$ and let $R = S \times_{\mathbb{Q}} \bar{S}$. If $F/\mathbb{Q}$ is an extension field, the set $\mathrm{Proj}(R)(F)$ of F-points is in bijection with the set of embeddings $\kappa(\mathfrak{p}) \hookrightarrow F$ of the residue fields $\kappa(\mathfrak{p}) = \mathcal{O}(\mathfrak{p})/\mathfrak{m}(\mathfrak{p})$ of closed points $\mathfrak{p}$ of $\mathrm{Proj}(R)$ into F. If F is complex, call an F-point over the closed point $\mathfrak{p} \in \mathrm{Proj}(R)$ **Hermitian** if $\bar{\mathfrak{p}} = \mathfrak{p}$ and if $\bar{\cdot}$ maps to complex conjugation in F. More generally, we call a closed point $\mathfrak{p}$ **Hermitian** if it has a Hermitian point, i.e. if $\mathfrak{p} = \overline{\mathfrak{p}}$ and if the residue field $\kappa(\mathfrak{p})$ has a complex embedding taking $\bar{\cdot}$ to complex conjugation.

In particular, the associated closed point of a Hermitian F-point is Hermitian. The Hermitian F-points are therefore in 1-1 correspondence with the embeddings $\kappa(\mathfrak{p}) \hookrightarrow F$ of Hermitian $\mathfrak{p}$ that preserve complex conjugation. If $F/\mathbb{Q}$ is Galois, then each closed point $\mathfrak{p}$ for which $\kappa(\mathfrak{p})$ embeds into F corresponds to a $\mathrm{Gal}(F/\mathbb{Q})$-orbit of F-points. If $\mathfrak{p}$ is Hermitian, the Hermitian F-points form a $\mathrm{Gal}(F/F^C)$-orbit, where C is the centralizer of complex conjugation in $\mathrm{Gal}(F/\mathbb{Q})$.

Let $G = (\mathbb{Z}/d)^2$ and let

$$1 \to \mathrm{U}(1) \to \widetilde{G} \to G \to 0$$

be a Heisenberg group, by definition inducing a skew-multiplicative pairing $G \times G \to \langle \zeta_d \rangle$. The Heisenberg group $\widetilde{G}$ determines a projective unitary representation $G \to \mathrm{PU}_d(\mathbb{Q}(\zeta_d))$ inducing an action on $R_{\mathbb{Q}(\zeta_d)}$. The G-invariant subring R^G is defined over $\mathbb{Q}$ because $(R_{\mathbb{Q}(\zeta_d)})^G_n = R^G_n \otimes \mathbb{Q}(\zeta_d)$ for each n.

Let $H \subset R^G_2$ be the subspace of harmonic invariants in degree 2, i.e. $H = \{f \in R^G_2 : \Delta f = 0\}$. Then $R^G_2 = \mathbb{Q}\alpha_0(z,\bar{z})^2 + H$, where $\alpha_0(z,\bar{z}) = \sum_i z_i \bar{z}_i$. We conjecture that $\mathrm{Proj}(R/RH)$ contains Hermitian points for every $d \geq 2$. Points have been computed for a growing – but still finite – list of dimensions d, and all of them are Hermitian. The known solutions are highly structured, with residue fields being explicit class fields of real quadratic fields for all $d \geq 4$. We summarize these conjectural number theoretic aspects in the next section.

The group $\mathrm{Aut}_0(\widetilde{G})$ of automorphisms of $\widetilde{G}$ acting trivially on the center lies in an extension

$$0 \to G \to \mathrm{Aut}_0(\widetilde{G}) \to \mathrm{SL}_2(d) \to 1$$

that splits iff $4 \nmid d$. The Weil representation $\mathrm{Aut}_0(\widetilde{G}) \to \mathrm{PU}_d(\mathbb{Q}(\zeta_{2d}))$ determines an action on each $(R_n)_{\mathbb{Q}(\zeta_{2d})}$, in particular stabilizing $H_{\mathbb{Q}(\zeta_{2d})}$. Therefore it acts on $\mathrm{Proj}(R/RH)(\mathbb{C})$, taking Hermitian $\mathbb{C}$-points to Hermitian $\mathbb{C}$-points. Moreover, since H is G-invariant, this gives a representation of $\mathrm{SL}_2(d)$ (even if d is even) on $H_{\mathbb{Q}(\zeta_d)}$. Below, we explicitly decompose this representation for prime d into a direct sum of principal series representations.

10.1 Relating formalisms

For $G = \mathrm{GL}_d(\mathbb{C})$, $U = \mathrm{U}_d(\mathbb{C})$ and $H = \mathrm{Herm}_d(\mathbb{C})$, Madonald defines $\mathbb{C}[G]$ by restricting $\mathbb{C}[X, \bar{X}]$. He uses the G-action $gf(x) = f(xg)$ on $\mathbb{C}[G]$, which amounts to the action $gf(X, \bar{X}) = g(Xg, \bar{X}\bar{g})$ on $\mathbb{C}[X, \bar{X}]$. The action on $\mathbb{C}[H]$ is then $gf(h) = f(g^\dagger hg)$. He proves there are isomorphisms

$$\mathbb{C}[G]^U_{2m} = \mathbb{C}[G/U]_{2m} \simeq \mathbb{C}[H]_m \simeq \mathrm{Sym}^m(\mathrm{End}(\mathbb{C}^d)).$$

Furthermore,

$$\mathbb{C}[U\backslash G/U] \simeq \bigoplus_\lambda \mathbb{C}\Omega_\lambda$$

is commutative with zonal spherical functions $\Omega_\lambda(g) = \frac{s_\lambda(g^\dagger g)}{s_\lambda(1)}$, where s_λ is the Schur function associated to λ.

Eisenbud-DeConcini-Procesi use the action of $G = \mathrm{GL}_n \times \mathrm{GL}_m$ on $k[X]$ given by $(g_1, g_2)f(X) = f(g_1^{-1}Xg_2)$. The diagonal subgroup $\{(g^{-\dagger}, g) : g \in \mathrm{GL}_d\}$ reproduces the above action on Hermitian matrices.

The “complexifications” of $\mathrm{U}_d(F, c)$ and $\mathrm{U}_d(F, c')$ should both equal $\mathrm{GL}_d(F)$, as e.g. $\mathrm{U}_d(F, c) = \{g \in \mathrm{GL}_d(F) : g^c = g^{-T}\}$.

10.2 2-design condition

Let

$$T_2(X) := \frac{d+1}{2d}\sum_j (\Delta_j X \Delta_{-j})^{\otimes 2}.$$

Then the $(\mathbb{Z}/d)^2$-orbit of a rank-1 Hermitian projection X is a 2-design iff $T_2(X) = P_+$. Since $T_2 : \mathrm{End}(V) \to \mathrm{Sym}^2(\mathrm{End}(V))^{(\mathbb{Z}/d)^2}$, each $A \in \mathrm{Sym}^2(\mathrm{End}(V))^{(\mathbb{Z}/d)^2}$ gives a quadratic form $\langle A, T_2(X)\rangle$ on $\mathrm{End}(V)$. Furthermore, since $\beta(X)$ is $(\mathbb{Z}/d)^2$-invariant, we have $\beta(X) = \langle \Delta_j \otimes \Delta_{-j}, T_2(X)\rangle$. So indeed it *is* sufficient to only require vanishing of the quadratic forms for $\mathrm{Sym}^{2,2}(V)$, $\Lambda^{2,2}(V)$ and P_-.

Let

$$S = \sum_{ij} |j,i\rangle\langle i,j| = \sum_{ij} |j\rangle\langle i| \otimes |i\rangle\langle j|$$

be the swap operator and note that

$$\mathrm{Tr}_1(X \otimes I)S = \sum_{ij} \langle i|X|j\rangle |i\rangle\langle j| = X \text{ and } \mathrm{Tr}_1(X \otimes I) = (\mathrm{Tr}\, X)I.$$

Therefore, $\mathrm{Tr}_1(X \otimes I)P_\pm = \frac{1}{2}(X \pm \mathrm{Tr}\, X)$. Now suppose P_j form a 2-design. Then

$$\frac{d^2+d}{n}\sum_j \langle P_j, X\rangle P_j = 2\,\mathrm{Tr}_1(X \otimes I)P_+ = X + \mathrm{Tr}\, X$$

is an invertible linear map $\mathrm{End}(V) \to \mathrm{End}(V)$ (with inverse $X \mapsto X - \frac{1}{d+1}\mathrm{Tr}\, X$). Since the number of P_j cannot be less than the rank of this linear map, we must have $n \geq d^2$. More generally, $X \mapsto aX + b\,\mathrm{Tr}\, X$ has inverse $X \mapsto \frac{1}{a}X - \frac{b}{a(d+b)}\mathrm{Tr}\, X$ for every a, b with $a \neq 0$. The 50%-depolarizing channel is $X \mapsto \frac{1}{2}(X + \mathrm{Tr}\, X)$.

A more natural relaxation might be

$$\frac{1}{n}\sum_j (\Delta_j X \Delta_{-j})^{\otimes 2} = \frac{2q_+(X)}{d^2+d}P_+ + \frac{2q_-(X)}{d^2-d}P_-,$$

as the Haar integral over $\mathrm{PU}(d)$ would give. A general X will also have terms in $\mathrm{Sym}^{2,2}(V)^{(\mathbb{Z}/d)^2}$ and $\Lambda^{2,2}(V)^{(\mathbb{Z}/d)^2}$.

Another realization: imposing the β_j and γ_j conditions together is the same as imposing the β^+ and β^- conditions.

11 Some geometric aspects

11.1 Equations and eigenforms

First some generalities on compact 2-point homogeneous spaces G/H. This means that G/H is a Gelfand pair. The algebra of polynomial functions on G/H decomposes into irreducible representations of G:

$$\mathbb{C}[G/H] = \bigoplus_{t \geq 0} V_t.$$

Then $V_t^H \simeq \mathbb{C}$ for each t, spanned by a zonal spherical function f_t, unique up to scaling and often chosen such that $f_t(1) = \dim V_t$.

Let $V = (\mathbb{R}^d)^* = \mathbb{R}x_1 + \cdots + \mathbb{R}x_d$, where x_i is the coordinate function $x_i(v) = v_i$. Let $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$. Then the symmetric algebra $\mathrm{Sym}(V_{\mathbb{C}})$ is naturally isomorphic to $\mathbb{C}[x]$. The symmetric algebra is graded by degree $\mathrm{Sym}(V_{\mathbb{C}}) = \bigoplus_{t \geq 0} \mathrm{Sym}^t(V)$, and we identify $\mathrm{Sym}^t(V_{\mathbb{C}})$ with the degree-t homogeneous polynomials $\mathbb{C}[x]$. The right action of $\mathrm{GL}_d(\mathbb{R})$ on $\mathbb{R}^d$ induces a left action, via translation, on polynomials, via $f^g(x) = f(gx)$.

Let $G = \mathrm{O}_B(V)$ be the isometry group of the standard bilinear form on V. The Laplacian $\Delta = \sum_i \frac{d^2}{dx_i^2}$ is G-invariant and maps each $\mathrm{Sym}^t(V)$ onto $\mathrm{Sym}^{t-2}(V)$ ($\mathrm{Sym}^t = 0$ for $t < 0$). The kernel $\mathrm{Harm}_t(V) = \ker(\Delta) \cap \mathrm{Sym}^t(V)$ of the laplacian is the subspace of harmonic degree-t polynomials. For each t, there is a decomposition

$$\mathrm{Sym}^t(V) = \bigoplus_{k=0}^{\lfloor \frac{t}{2} \rfloor} |x|^{2k} \mathrm{Harm}_{t-2k}(V).$$

Restricting from $\mathbb{R}^d$ to the sphere $S^{d-1} = \{v \in \mathbb{R}^d : |v|^2 = 1\}$ gives the ring of polynomial functions $\mathbb{C}[S^{d-1}] = \bigoplus_{t \geq 0} \mathrm{Harm}_t(V)$. Isn't this just $\mathbb{C}[x]/(|x|^2 - 1)$??? This realizes the $S^{d-1} \subset \mathbb{R}^d$ as an affine variety, so that would seem to be the affine coordinate ring. Let $v_0 \in S^{d-1}$ be arbitrary. Then $S^{d-1} \simeq H \backslash G$, where $G = \mathrm{O}_B(V)$ and H is the stabilizer of v_0 in G. For each degree t, there is a unique H-invariant harmonic polynomial $f_t(x)$ such that $f_t^h = f_t$ for all $h \in H$, and $f_t(t) = \dim \mathrm{Harm}_t$.

There is something else here I'm not understanding. Apparently if $f \in \mathrm{Harm}_t(S^{d-1})$, then $\Delta_{S^{d-1}} f = -t(t+d-2)f$, where $\Delta_{S^{d-1}}$ is the spherical Laplacian (i.e. the associated Laplace-Beltrami operator).

A polynomial f satisfies $f(-x) = f(x)$ iff it is a a sum of even-degree homogeneous polynomials. Therefore, the ring of polynomial functions on real projective space decomposes as

$$\mathbb{C}[\mathbb{P}^{d-1}(\mathbb{R})] = \bigoplus_{t \geq 0} \mathrm{Harm}_{2t}(V).$$

Let $V \simeq \mathbb{C}^d$ and let $J \in \mathrm{End}_{\mathbb{R}}(V)$ be the corresponding complex structure. Let $V_{\mathbb{C}} := V_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}$ and extend J to $V_{\mathbb{C}}$ by linearity. Then $V_{\mathbb{C}} \simeq V^+ \oplus V^-$, where $V^{\pm}$ are the $\pm i$-eigenspaces of J. As complex vector spaces, they are isomorphic to V via $\phi^{\pm}(v) = \left(\begin{smallmatrix} v \\ \pm iv \end{smallmatrix}\right)$, but as J acts on $V^{\pm}$ as multiplication by $\pm i$, we may identify $V = (V^+, J)$ and $\bar{V} = (V^-, J)$.

A choice of Hermitian inner product $\langle \cdot, \cdot \rangle$ on V determines a bilinear symmetric form $B(v,w) = \mathrm{Re}\langle v, w \rangle$ and a symplectic form $E(v,w) = \mathrm{Im}\langle v, w \rangle$ that are compatible with J. In the standard basis, these are represented by block matrices with respect to the decompositition $V_{\mathbb{C}} = V^+ \oplus V^-$:

$$B = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}, \quad E = \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

I think.

In general, for a given J, a choice of B satisfying $B(Jv,w) = -B(v,Jw)$ determines $E(v,w) = B(Jv,w)$, and thus $\langle\cdot,\cdot\rangle = B+iE$. Furthermore, a choice of E satisfying $E(Jv,Jw) = E(v,w)$ determines $B(v,w) = E(v,Jw)$, and thus $\langle\cdot,\cdot\rangle = B+iE$. This is essentially because $\mathrm{U}_d(\mathbb{C})$ is equal to the intersection of any two of the three subgroups of $\mathrm{GL}_{2d}(\mathbb{R})$ in the triple intersection $\mathrm{U}_d(\mathbb{C}) = \mathrm{GL}_d(\mathbb{C}) \cap \mathrm{O}_{2d}(\mathbb{R}) \cap \mathrm{Sp}_{2d}(\mathbb{R})$.

Because $V^{\pm}$ are isotropic for B, there are isomorphisms $V^{\pm} \to (V^{\mp})^*$ given by $\bar{v} \mapsto B(\bar{v},\cdot)$. The subgroup of $\mathrm{O}(B)$ preserving the decomposition $V^+ \oplus V^-$ is isomorphic to $\mathrm{GL}(V)$ via $g \mapsto \left(\begin{smallmatrix} g^T & 0 \\ 0 & g^{-1} \end{smallmatrix}\right)$. The complex structure J exchanges V and $\bar{W}$, and its centralizer in $\mathrm{GL}(W)$ is isomorphic to the unitary group $\mathrm{U}(V)$ via $u \mapsto \left(\begin{smallmatrix} \bar{u} & 0 \\ 0 & u^{\dagger} \end{smallmatrix}\right)$. (Is there a nicer way to work this action?). So we could also (and would usually) work with the unitary group in this context, thought we might as well work with $\mathrm{GL}(V)$ (as BC once suggested).

Then the ring of polynomials $\mathbb{C}[z,\bar{z}] := \mathbb{C}[z_1,\dots,z_d,\bar{z}_1,\dots,z_d]$ is isomorphic to the symmetric algebra

$$\mathrm{Sym}(V_{\mathbb{C}}^*) \simeq \mathrm{Sym}(V_+) \otimes \mathrm{Sym}(V_-) = \bigoplus_{p,q=0}^{\infty} \mathrm{Sym}^{p,q}(V_{\mathbb{C}}^*),$$

where $\mathrm{Sym}^{p,q}(W_{\mathbb{C}}) = \mathrm{Sym}^p(W) \otimes \mathrm{Sym}^q(\bar{W})$. The Laplacian $\Delta = \sum_j \frac{d^2}{dz_j d\bar{z}_j}$ maps $\mathrm{Sym}^{p,q}(W_{\mathbb{C}})$ onto $\mathrm{Sym}^{p-1,q-1}(W_{\mathbb{C}})$; its kernel is the subspace $\mathrm{Harm}^{p,q}(W_{\mathbb{C}}) = \ker(\Delta) \cap \mathrm{Sym}^{p,q}(W_{\mathbb{C}})$ of harmonic degree-(p,q) polynomials. Then

$$\mathrm{Sym}^{p,q}(W_{\mathbb{C}}) = \bigoplus_{t=0}^{\min(p,q)} |z|^{2t} \mathrm{Harm}_{p-t,q-t}(W_{\mathbb{C}}).$$

Each polynomial in $\mathbb{C}[z,\bar{z}]$ determines a function on the unit sphere $S^{2d-1} \subset V$ by restriction. $\mathrm{GL}(W)$ acts on $\mathbb{C}[z,\bar{z}]$ from the right by translation: $f^g(z,\bar{z}) = f(gz,\bar{g}\bar{z})$. The polynomials of weight 0 with respect to the $\mathrm{U}(1)$ subgroup of $\mathrm{GL}(W)$ determine functions on $\mathbb{P}(V)$, as if $|w|^2 = 1$, then $f([w]) := f(w,\bar{w})$ only depends on $[w] \in \mathbb{P}(V)$. Still trying to find the right language to describe the coordinate ring. There is a notion of a "ring of polynomial functions on $\mathbb{P}(V)$" of the form

$$\bigoplus_{t\geq 0} \mathrm{Harm}^{t,t}(W_{\mathbb{C}})$$

but not even this appears to be a graded ring, i.e. $f \in \mathrm{Harm}^{t,t}$ and $g \in \mathrm{Harm}^{k,k}$ doesn't necessarily mean that $fg \in \mathrm{Harm} t+k, t+k$. Figure out the right way to say this with Proj.

The exterior algebra on $W_{\mathbb{C}}$ has a similar decomposition:

$$\Lambda(V_{\mathbb{C}}^*) \simeq \Lambda(V) \otimes \Lambda(\bar{V}) = \bigoplus_{t=0}^{\infty} \bigoplus_{k=0}^{t} \Lambda^{t-k}(V) \otimes \Lambda^k(\bar{V})$$

. As V and $\bar{V}$ are also isotropic for E, it also induces a pairing $\bar{v} \mapsto E(\bar{v},\cdot) \in V^*$

We observe that D is the dimension of the space of harmonic $(2,2)$-forms on $\mathbb{C}^d$. Note that the space of p-forms on $\mathbb{P}^{d-1}(\mathbb{C})$ is 1-dimensional if p is even and is 0 if p is odd. I might imagine it is concentrated in degrees (p,p). The Kahler form e.g. is a $(1,1)$-form on projective space is $\omega = \frac{i}{2}\sum_{i,j} \omega_{ij} dz_i \wedge d\bar{z}_j = 4i\partial\bar{\partial}\log|z|^2$. It has a compatible Riemannian metric $g = g_{ij} dz_i \otimes d\bar{z}_j$ such that $h = g + i\omega$ is a Hermitian metric.

We integrate it along geodesics to measure distance. Therefore we expect there to exist a distinguished $(2,2)$-form that we can integrate over geodesic triangles. It will be fruitful to relate the "symplectic area" coming up in the triple products to these integrals. as well as to the distance sphere in $\mathbb{C}^d$ is, to compare against the triangles. What do the triple products have to do with curvature?

For a Kahler manifold, $g_{ij}(z,\bar{z}) = \frac{d^2K(z,\bar{z})}{dz_i d\bar{z}_j}$ and the curvature tensor has signature $(2,2)$. Note that if $K(z,\bar{z})$ is harmonic then the metric is traceless and therefore cannot be positive. So it must have non-harmonic parts.

Ikeda & Taniguchi [4] define a certain harmonic subspace $H^{pq}_{k\ell}$ of the space of polynomial (p,q)-forms $\alpha \in \Lambda^{p,q}(\mathbb{C}^d)$ of the form

$$\alpha = \sum \alpha_{i,j}(z,\bar{z}) dz_{i_1} \wedge \cdots \wedge dz_{i_{d-1}} \wedge d\bar{z}_1 \wedge \cdots \wedge d\bar{z}_{d-1},$$

where $i,j \in \{1,\dots,d\}$ have size $|i| = p$ and $|j| = q$ and $\alpha_{i,j}(z,\bar{z})$ is a homogeneous polynomial of degree-(k,ℓ). Each cohomology class has a unique harmonic representative. So the dimension of the space of harmonic forms equals the Betti number.

Let $\varepsilon_1,\dots,\varepsilon_d$ be fundamental weights for GL_d, satisfying $\varepsilon_i(x_1,\dots,x_d) = x_i$ for each i. The fundamental weights for SL_d are $\omega_i = \varepsilon_1 + \cdots + \varepsilon_i - \frac{i}{d}(\varepsilon_1 + \cdots + \varepsilon_d)$, where $1 \le i \le d-1$. Set $\omega_0 = \omega_d = 0$. The relevant representation exists when $dgeq4$ and has highest weight $\varepsilon_1 + \varepsilon_2 - \varepsilon_{d-1} - \varepsilon_d$. In terms of SL_d, it is $\omega_2 + \omega_{d-1}$. Note that the highest root is

$$\theta = \alpha_1 + \cdots + \alpha_{d-1} = \varepsilon_1 - \varepsilon_d = \omega_1 + \omega_{d-1},$$

where $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$, $1 \le i \le d-1$, are the simple roots of SL_d. Also note that $\mathrm{Harm}^{t,t}(\mathbb{C}^d)$ is a $\mathrm{U}(d)$ irrep with highest weight $t\theta$.

Perhaps one should seek harmonic maps from complex tori, such as a 2-dimensional abelian variety with real multiplication by $K = \mathbb{Q}(\sqrt{D})$, to products of projective space, such that the real subtorus maps to projective space. See e.g. Birkenhake and Lange in Section 9.2 of the big book for how to construct them.

11.2 The entire idea

The entire idea is to inscribe a regular simplex into the convex set

$$\Omega = \{\rho \in \mathrm{Herm}_d(\mathbb{C}) : \rho \geq 0 \text{ and } \operatorname{Tr}\rho = 1\}$$

of quantum states. The extremal points of Ω are rank-1 projections and correspond to points of $\mathbb{P}^{d-1}(\mathbb{C})$ via $vv^\dagger \mapsto [v]$. The boundary of Ω consists of the ρ with $\det(\rho) = 0$ and contains the extremal points as a proper subset when $d > 2$. When $d = 2$, Ω is topologically a ball in $\mathbb{R}^3$ with boundary $\mathbb{P}^1(\mathbb{C}) \simeq S^2$. Given a state $\rho = \frac{1}{d}I + \widetilde{\rho} \in \Omega$ the matrix $\frac{1}{d}I - \widetilde{\rho}$ will not generally be contained in Ω when $d > 2$, although its trace will remain equal to 1.

The set Ω is a homogeneous space for $\mathrm{PU}(d)$. The orbits are distinguished by the spectrum of any ρ on the orbit. The extremal points sit on a unique orbit, characterized by the distance to $\frac{1}{d}I$ from any point ρ on the orbit, as measured by any unitarily invariant matrix norm such as the trace norm $\|\cdot\|_1$, the Euclidean norm $\|\cdot\|_2$, the Schatten norms $\|\cdot\|_p$ and the operator norm $\|\cdot\|_\infty$.

Is Ω a proper subset of the unit ball for all of these norms?

I think the upshot of this problem is to understand the relationship between the projection Ω_0 of Ω onto the set of traceless matrices and the A_r lattice with $r = d^2 - 1$. Note that A_r has $r^2 + r = d^4 - d^2$ roots, which seems to be a very convenient number. In particular, I should be able to identify the dual problem using the geometry of the Voronoi cell and the fundamental simplex. How are these related to the embedded simplex? Why should it be the simplex of maximal volume? Also note I had the idea that $\frac{1}{4}(d-3)(d+1)$ is the dimension of an orthogonal Lie algebra, acting transitively on a space of invariant harmonic tensors. It also makes sense that I could possibly verify the rank-1 condition by showing that $\rho \otimes \rho$ is $\mathbb{Z}/d$-invariant while $\rho \wedge \rho = 0$.

11.3 Equations

First note that for any Hermitian X,

$$\int_{\mathrm{PU}(d)} (UXU^{-1})^{\otimes 2} dU = \frac{2Q_+(X)}{d^2+d} P_+ + \frac{2Q_-(X)}{d^2-d} P_-,$$

where $Q_\pm(X) = \frac{(\operatorname{Tr} X)^2 - \operatorname{Tr}(X^2)}{2}$. If we replace $\mathrm{PU}(d)$ with the image of the Heisenberg group, then

$$\frac{1}{d}\sum_j (\Delta_j X \Delta_j^{-1})^{\otimes 2} = \frac{2Q_+(X)}{d^2+d} P_+ + \frac{2Q_-(X)}{d^2-d} P_- + X_+ + X_-,$$

where $X_+ \in (\mathrm{Sym}^{2,2} V)^H$ and $X_- \in (\Lambda^{2,2} V)^H$. Note that $X_- = 0$ if $\operatorname{rank}(X) = 1$. However, we would seem to need $\mathrm{Ad}_+(X) = 0$ as well for the converse, and this space does not contain any H-invariant functions. But maybe it follows somehow just as it does for the harmonic functions. And yet, I think it may be more complicated as we also need $\mathrm{Ad}_-(X) = 0$, where

Note here that

For odd d, this gives $\frac{(d+3)(d-1)}{4} + d$ equations in $2d$ variables if we restrict to X of rank 1. Otherwise, we get $1 + \frac{(d+3)(d-1)}{4} + 1 + \frac{(d-3)(d+1)}{4} = \frac{d^2+1}{2} < d^2$ equations in d^2 complex variables. I think that working with traceless matrices can give $\frac{d^2-1}{2}$ (maybe $\frac{d^2-3}{2}$) equations in d^2-1 complex variables. So there are certainly solutions in $\mathrm{End}(V)$! The “only” thing to do is to show that there are Hermitian solutions. Why did I ignore this before??? So it seems that I can prove (nonconstructively) the existence of v, w such that $\sum_j (\Delta_j v w^\dagger \Delta_j^\dagger)^{\otimes 2} \propto P_+$, i.e. a non-Hermitian SIC-POVM. Hmm... seems like these are the sorts of things that Vern is looking at.

Hermiticity involves $\frac{d(d+1)}{2}$ equations: $z_{ii} = \bar{z}_{ii}$ $z_{ij} = \bar{z}_{ji}$ for $i < j$ but we also need to double the number of variables to $2d^2$. What is happening with $\operatorname{Tr} A(Z \otimes Z)$? Or do we want to use $\operatorname{Tr} A(Z \otimes Z^\dagger)$?

Suppose $s \in \mathrm{SL}_2(d)$ has order $d+1$ (i.e. it generates a nonsplit torus). I once proved (under what conditions on d?) that U_s has d eigenvectors v_j over $\mathbb{Q}(\zeta_{p(p+1)})$ with distinct eigenvalues $\zeta_{d+1}^j, j = \frac{d-1}{2}, \frac{d-3}{2}, \ldots, -\frac{d-1}{2}$. When $d \equiv 2 \bmod 3$, then $s^{\frac{d+1}{3}}$ has order 3, with eigenvalues $(\zeta_{d+1}^j)^{\frac{d+1}{3}} = \zeta_3^j$. When $d \equiv 1 \bmod 4$ (i.e. $d \equiv 5 \bmod 12$), then the order-3 unitary has eigenvalue $+1$ with multiplicity $\frac{d-2}{3}$ and $\zeta_3^{\pm 1}$ each with multiplicity $\frac{d+1}{3}$.

12 Symmetric spaces

Let M be a Riemannian manifold. The Laplace de Rham operator $\Delta = d^* d$ on $\mathbb{C}(M)$ is a self-adjoint compact unbounded operator, defined on the dense filtered algebra

$$\mathbb{C}[M] = \bigcup_{j=0}^{\infty} \mathbb{C}(M)_j$$

of polynomial functions, where $\mathbb{C}[M]_j$ is the sum of the lowest $j+1$ eigenspaces of Δ. A finite subset $\mathcal{D} \subset M$ is a **t-design** if

$$\frac{1}{|\mathcal{D}|}\sum_{p\in M} f(p) = 0 \text{ for all } f \in \mathbb{C}[M]_t = \mathrm{Harm}_1(M) \oplus \cdots \oplus \mathrm{Harm}_t(M),$$

where $H_t(M) \subset \mathbb{C}(M)$ is the tth eigenspace of the Laplacian Δ operator, ordered by eigenvalue.

Suppose a compact Lie group G acts transitively by isometries on M. Each basepoint $p \in M$ determines an isomorphism $M \simeq G/H$, where $H \subset G$ is the stabilizer of p in G, taking $gp \in M$ to $gG_p \in G/H$. There is furthermore an involution $\tau \in \mathrm{Aut}(G)$ with $(G^\tau)_0 \subset H \subset G^\tau$ whose induced action on M reverses geodesics through p.

Under the $G \times G$ action

$$(g_1, g_2)f(X) = f(g_1 X \tau(g_2^{-1})),$$

the ring $\mathbb{C}[G]$ of polynomial functions decomposes as a direct sum

$$\mathbb{C}[G] = \bigoplus_\lambda \mathbb{C}[G]_\lambda$$

over positive integral weights λ, with $\mathbb{C}[G]_\lambda \simeq \mathrm{End}(V_\lambda)$ for an irreducible representation V_λ with highest weight λ. The ring of polynomial functions on M is the H-invariant subring

$$\mathbb{C}[M] = \mathbb{C}[G]^H \simeq \bigoplus_\lambda V_\lambda^* \otimes V_\lambda^H.$$

The ring

$$\mathbb{C}[M]^H = \mathbb{C}[G]^{H\times H} = \bigoplus_\lambda \mathrm{End}(V_\lambda^H).$$

of H-invariant polynomial functions is identified with the Hecke algebra of bi-H-invariant polynomial functions on G.

Suppose that τ is an order-two automorphism of G satisfying $(G^\tau)_0 \subset H \subset G^\tau$. Then M is a symmetric space with geodesic-reversing isometry $\tau(gp_0) = \tau(g)p_0$. Because M is a symmetric space, then D is the Levi-Civita connection (Burstall p. 10), equal to the orthogonal projection of d onto $[\mathfrak{h}]$. The derivative of τ (also written τ) acts on $\mathfrak{g}$ with $+1$ eigenspace $\mathfrak{h}$ and -1-eigenspace $\mathfrak{m}$. Furthermore, if $p = gp_0$, then $\tau_p := g\tau g^{-1}$ reverses geodesics through p, splitting $\mathfrak{g}$ as $[\mathfrak{h}]_p + [\mathfrak{m}]_p$.

A symmetric space can admit various invariant metrics. Those that are 2-point homogeneous admit a unique G-invariant metric that is unique up to rescaling. We may study codes in such spaces for the corresponding geodesic distance, a naturally associated metric on M.

13 Heisenberg group and Weil representation

Let p be an odd prime and let $\psi : \mathbb{F}_p \to \langle \zeta_p \rangle$ be a primitive character of the additive group of $\mathbb{F}_p$. The quadratic gauss sum of ψ, with respect to the quadratic character $\left(\frac{\cdot}{p}\right)$ of the multiplicative group $\mathbb{F}_p^\times$, is

$$\tau_\psi = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right)\psi(x) = 0 + \sum_{x \in (\mathbb{F}_p^\times)^2} \psi(x) - \sum_{x \in \mathbb{F}_p^\times \smallsetminus (\mathbb{F}_p^\times)^2} \psi(x) = \sum_{x \in \mathbb{F}_p} \psi(x^2).$$

The following is a lift of the Weil representation of $\mathrm{SL}_2(p)$ to $\mathrm{SU}_2(\zeta_p)$ (is it really SU_2?) (see e.g. [5]):

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} |j\rangle = \left(\frac{a}{p}\right) |a^{-1} j\rangle, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} |j\rangle = \psi\big(j^2/2\big)|j\rangle, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} |j\rangle = \frac{\tau_\psi}{p} \sum_k \psi(jk)|k\rangle.$$

For the character $\psi_a(x) = e^{2\pi i a x/p}$, the Gauss sum explicitly evaluates to

$$\tau_a := \tau_{\psi_a} = \sum_x e^{2\pi i a x^2/p} = \left(\frac{a}{p}\right)\sqrt{p^*},$$

where $p^* = (-1)^{\frac{p-1}{2}} p$ satisfies $\sqrt{p^*} = \varepsilon_p \sqrt{p}$ for

$$\varepsilon_p = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ i & \text{if } p \equiv 3 \pmod 4). \end{cases}$$

The operators $\Delta_j = \psi(j_1 j_2/2) X^{j_1} Z^{j_2}$ satisfy

$$\Delta_j^\dagger = \Delta_{-j}, \quad \Delta_k \Delta_j = \psi([j,k]/2)\Delta_{j+k}, \quad \Delta_k \Delta_j \Delta_{-k} = \psi([j,k])\Delta_j.$$

The skew-multiplicative pairing $\psi([j,k])$ identifies $\mathbb{F}_p^2$ with its dual $(\mathbb{F}_p^2)^*$

The group $\mathrm{SL}_2(p)$ preserves $\psi([j,k])$ and satisfies $g\Delta_j g^{-1} = \Delta_{gj}$ for all g and j.

13.1 Explicit section of Heisenberg group

Each section $j \mapsto \Delta_j$ of the Heisenberg group determines a unitary lifting of the projective representation $j \mapsto [\Delta_j] \in \mathrm{PU}_d(\mathbb{Q}(\zeta_d))$ of G with $\mathrm{U}(1)$-valued 2-cocycle $c_{j,k}$ on G satisfying $\Delta_j \Delta_k = c_{j,k} \Delta_{j+k}$. The 2-cocycle determines a skew-multiplicative pairing $e_{j,k} = c_{j,k}/c_{k,j} = \zeta_d^{[k,j]}$, where $[j,k] = j_1 k_2 - j_2 k_1$ is the symplectic inner product. It satisfies $\Delta_j \Delta_k \Delta_{-j} = e_{j,k} \Delta_k$, showing that the Δ_j diagonalize the G-action on $\mathbb{Q}(\zeta_d)^{d \times d}$. In particular, $\Delta_j \Delta_{-j} = c_{j,-j} I = c_{-j,j} I$ so that $\Delta_j^\dagger = c_{j,-j} \Delta_{-j}$.

Let $X_d, Z_d \in \mathrm{U}_d(\mathbb{Q}(\zeta_d))$ be the matrices $X_d|a\rangle = |a+1\rangle$ and $Z_d|a\rangle = \zeta_d^a$. For $j \in G' := (\mathbb{Z}/d')^2$, let $\Delta_j = (-\zeta_{2d})^{j_1 j_2} X_d^{j_1} Z_d^{j_2}$. Then $\Delta_j^\dagger = \Delta_{-j}$ for every $j \in G'$ and

$$\Delta_j \Delta_k = (-\zeta_{2d})^{-[j,k]} \Delta_{j+k}$$

for every $j, k \in G'$. When d is odd, then 2 is invertible mod d, so that $-\zeta_{2d} = \zeta_d^{2^{-1} \bmod d}$, giving the explicit cocycle $c_{j,k} = \zeta_d^{-[j,k]/2}$ on $G = G'$. When d is even, then $\Delta_{j+d(a,b)} = (-1)^{a+b}\Delta_j$. Choosing a section over G via the same formula, we find that for $j, k \in G$,

$$\Delta_j \Delta_k = (-\zeta_{2d})^{-[j,k]} \Delta_{j+k} = \zeta_d^{j_1+k_1+j_2+k_2} (-\zeta_{2d})^{-[j,k]} \Delta_{j+k \bmod d},$$

giving the explicit cocycle $c_{j,k} = \zeta_d^{j_1+k_1+j_2+k_2} (-\zeta_{2d})^{-[j,k]}$ on G.

13.2 Irreducible representations of $\mathrm{SL}_2(p)$

Let $G = \mathrm{SL}_2(p)$. When $p = 2$, then $G \simeq S_3$ has three irreps: the trivial character, the alternating character and the two-dimensional irrep.

When p is odd, G has two kinds of maximal tori: split T_{p-1} and non-split T_{p+1}. For each character $\chi \in \widehat{T}_{p-1}$ of a split torus, a **principal series** representation $\mathcal{P}_\chi$ of $\mathrm{SL}_2(p)$ is induced from the 1-dimensional representation $\chi\left(\left(\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix}\right)\right) = \chi(a)$ of B. Explicitly,

$$\begin{aligned} \mathcal{P}_\chi &= \chi \uparrow_B^{\mathrm{SL}_2} \\ &= \{f : \mathrm{SL}_2 \to \mathbb{C} | f(bg) = \chi(b) f(g)\} \\ &\simeq \mathbb{C}(\mathrm{SL}_2/B) \\ &\simeq \bigoplus_{i \in \mathbb{P}^1(\mathbb{F}_p)} s_i \mathbb{C}, \end{aligned}$$

where $s_0, s_1, \ldots, s_{d-1}, s_\infty$ is a complete set of representatives for the cosets $B \backslash G$, which may be taken to be $s_x = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -x \end{smallmatrix}\right)$, $s_\infty = I$. Better way to write this with tensor products rather than use explicit matrices???

The principal series representations satisfy $\mathcal{P}_\chi \simeq \mathcal{P}_{\chi'}$ iff $\chi' = \chi^{-1}$, giving $\frac{d+1}{2}$ distinct representations of dimension $d+1$. The representation $\mathcal{P}_\chi$ is irreducble unless $\mathrm{ord}(\chi)|2$, i.e. unless χ is the trivial χ_1 or quadratic $\chi_2 := \left(\frac{\cdot}{d}\right)$ character. For a fixed generator $\widehat{T}_{d-1} = \langle \chi_{d-1} \rangle$, we may write $\mathcal{P}_j = \mathcal{P}_{\chi_{d-1}^j}$, giving inequivalent representations $\mathcal{P}_0, \mathcal{P}_1 \ldots \mathcal{P}_{\frac{d-1}{2}}$. We can further decompose $\mathcal{P}_0 = 1 + \widetilde{\mathcal{P}}_0$ (as $s_0 + s_\infty$ transforms trivially) and $\mathcal{P}_{\frac{d-1}{2}} \simeq \mathcal{P}_\tau + \mathcal{P}_{-\tau}$, where in the latter case these are distinguished by their character values $\frac{\pm\tau+1}{2}$ on $t = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

The representation matrices are monomial in the s_x basis:

$$\begin{aligned} \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) s_x &= s_{bx}, \\ \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right) s_x &= \begin{cases} \chi(a^{-1}) s_{a^2 x} & x \neq \infty \\ \chi(a) s_\infty & x = \infty, \end{cases} \\ \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) s_x &= \begin{cases} s_\infty & x = 0 \\ \chi(x) s_{-x^{-1}} & x \neq 0, \infty \\ \chi(-1) s_0 & x = \infty. \end{cases} \end{aligned}$$

If $\langle a_0 \rangle = \mathbb{F}_d^\times$, we can order the basis as $s_{a_0^2}, s_{a_0^4}, \ldots, s_{a_0^{d-3}}, s_{a_0}, s_{a_0^3}, \ldots, s_{a_0^{d-2}}, s_0, s_\infty$, in which case $\begin{pmatrix} a_0^j & \\ & a_0^{-j} \end{pmatrix}$ acts as

$$\begin{pmatrix} \zeta^{-1} X_{\frac{p-1}{2}}^j & & & \\ & \zeta^{-1} X_{\frac{p-1}{2}}^j & & \\ & & \zeta^{-1} & \\ & & & \zeta \end{pmatrix},$$

where $\zeta = \chi(a_0^j)$.

The **discrete series** consists of $(d-1)$-dimensional representations $\mathcal{D}_\nu$ associated to the nontrivial characters $\nu \in \widehat{T}_{p+1}$ of a non-split torus $T_{d+1} \simeq \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times \simeq \{x \in \mathbb{F}_{p^2} : x\overline{x} = 1\}$. These satisfy $\mathcal{D}_\nu \simeq \mathcal{D}_{\nu^{-1}}$ and are irreducible unless ν is the quadratic character of T_{p+1}. Similarly choosing a generator ν_0 for the character group gives a list of inequivalent representations $\mathcal{D}_1, \ldots, \mathcal{D}_{\frac{p+1}{2}}$, with all but the last irreducible, as $\mathcal{D}_{\frac{p+1}{2}} = \mathcal{D}_\tau + \mathcal{D}_{-\tau}$ according to the character value of t being $\frac{\pm\tau-1}{2}$.

Given a primitive character $\chi \in \widetilde{\mathbb{F}}_p^\times$, the Weil representation W associated to the quadratic form $\psi(x^2/2)$ is isomorphic to $\mathcal{P}_{\tau_\psi} + \mathcal{D}_{\tau_\psi}$.

In general we have $W_\tau^* \simeq W_{\overline{\tau}}$. When $p \equiv 1 \bmod 4$, $\tau_2 = \left(\frac{2}{p}\right)\sqrt{p}$ is real which gives $W_{\tau_2}^* \simeq W_{\tau_2}$. For $d \equiv 3 \bmod 4$, we have $\tau_2 = i\left(\frac{2}{p}\right)\sqrt{p}$ so that $W_{\tau_2}^* \simeq W_{-\tau_2}$. This should all be expanded and double checked, as I think I changed my convention from the first code I wrote 10 years ago.

Theorem 13.1. *H is stable under the action of* $\mathrm{SL}_2(p)$*, under which it decomposes as*

$$H \simeq \mathrm{End}_0(\mathcal{P}_\tau) \simeq \widetilde{\mathcal{P}}_0 + \mathrm{End}_0(\mathcal{D}_\tau).$$

If $p \equiv 1$ mod 4, then $\mathrm{End}_0(\mathcal{D}_\tau) \simeq \mathcal{P}_2 + \mathcal{P}_4 + \cdots \mathcal{P}_{\frac{p-5}{2}} + \mathcal{P}_\tau$.

If $p \equiv 3$ mod 4, then $\mathrm{End}_0(\mathcal{D}_\tau) \simeq \mathcal{P}_2 + \mathcal{P}_4 + \cdots \mathcal{P}_{\frac{p-3}{2}}$.

In particular,

$$\dim \mathrm{End}_0(\mathcal{D}_\tau) = \left(\frac{p-1}{2}\right)^2 - 1 = \left(\frac{p-1}{2} + 1\right)\left(\frac{d-1}{2} - 1\right) = \frac{(p-3)(p+1)}{4}.$$

Note that the subset of $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{\frac{p-3}{2}}$ contained in $\mathrm{End}_0(\mathcal{D}_\tau)$ consists of real representations (with Frobenius-Schur indicator equal to 1), so they are $\mathbb{C}$-linearly self-dual. These are all the nontrivial principal series irreps on which $\left(\begin{smallmatrix} -1 & \\ & -1 \end{smallmatrix}\right)$ acts trivially. Therefore H is a representation of $\mathrm{PSL}_2(p)$. This makes sense because $-I$ acts as ±1 on $\mathcal{D}_\tau$ and $\mathcal{P}_\tau$, so it has no effect on endomorphisms.

We will also find that $\mathcal{H}^- \simeq \mathrm{End}(\mathcal{D}_\tau)$ as well. Now I wonder if this should be put in the next chapter, starting with an expansion on the representations of $\mathrm{SL}_2(p)$, especially the Weil representation.

*

14 Old Heisenberg and Weil

Let ζ be a primitive pth root of unity and let $\psi(a) = \zeta^a$ be the corresponding nontrivial additive character of $\mathbb{F}_p$. The Weil representation can be considered to be the projective unitary representation defined on the following generators of $\mathrm{SL}_2(p)$ for $a \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p^\times$ (see e.g. [5]):

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} |j\rangle = \left(\frac{a}{p}\right) |a^{-1} j\rangle, \quad \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} |j\rangle = \psi\left(\tfrac{1}{2} b j^2\right) |j\rangle, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} |j\rangle = \frac{G_2(\psi)}{p} \sum_k \psi(jk) |k\rangle.$$

Here, $\left(\frac{\cdot}{p}\right)$ is the quadratic character of the multiplicative group $\mathbb{F}_p^\times$ and

$$G_a(\psi) = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \psi(ax) = \sum_{x \in \mathbb{F}_p} \psi(ax^2)$$

is a Gauss sum.

14.1 Gauss sums

When $\zeta = e^{2\pi i/p}$ so that the character has the form $\psi(x) = e^{2\pi i x/p}$ the Gauss sum can be explicitly evaluated as

$$G_a = \sum_x e^{2\pi i a x^2/p} = \left(\frac{a}{p}\right) \varepsilon_p \sqrt{p}$$

where

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{otherwise} \end{cases}$$

is the **Legendre symbol**, or quadratic character of $\mathbb{F}_p^\times$, and

$$\varepsilon_p = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ i & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

So the **Weyl element** $w \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ acts as $\left(\frac{2}{p}\right)\varepsilon_p$ times the usual discrete Fourier transform.

14.2 Quadratic and bilinear forms on $\mathbb{Z}/d$

The general case reduces to prime powers $d = p^n$. For odd p, there are precisely two quadratic forms, each of level p^n, and two corresponding bilinear forms. On $\mathbb{Z}/2$, there are two level-4 quadratic forms $q_2^\pm$ and one bilinear form b_2. There are 2 bilinear forms $b_4^\pm$ on $\mathbb{Z}/4$ and 4 bilinear forms $b_{2^n}^{1,3,5,7}$ on $\mathbb{Z}/2^n$ for $n \geq 3$. There are 4 level-8 quadratic forms $q_{2^n}^{1,3,5,7}$ on $\mathbb{Z}/2^n$ for $n \geq 2$. The mapping $q \mapsto b(x,y) = q(x+y) - q(x) - q(y)$ is 1-1 for $n \geq 3$ and is 2-1 for $d = 2, 4$. What does this say about the Heisenberg group and Weil representation?

Note that when $\mathcal{O}/d \simeq \mathcal{O}/\mathfrak{p} \times \mathcal{O}/\mathfrak{p}' \simeq \mathbb{Z}/d \times \mathbb{Z}/d$, we can use a quadratic form on $\mathcal{O}$ with kernel $\mathfrak{p}$

14.3 Bruhat decomposition for SL_2 and GL_2

When $c \neq 0$, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a/c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & e/c \end{pmatrix}$$

where $e = ad - bc$. The last matrix decomposes further as

$$\begin{pmatrix} c & d \\ 0 & e/c \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} 1 & d/ce \\ 0 & 1 \end{pmatrix}\begin{pmatrix} e^{-1} & 0 \\ 0 & e \end{pmatrix}\begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix}.$$

14.4 Weil representation from lattices

There is a general way of describing the Weil representation using lattices, following Borcherds. This formalism naturally leads to a description of the double cover, and perhaps makes a more fundamental connection with the number theory. I am hopeful that I can characterize the eigenvectors of non-split tori in this setting.

Some definitions: a **lattice** L is a finitely-generated free $\mathbb{Z}$-module equipped with a integer-valued symmetric bilinear form $(x, y) \mapsto x \cdot y$. The lattice is **even** if $x^2 = x \cdot x$ is even for every $x \in L$. Otherwise, it is **odd**, with the even vectors forming an index-two sublattice. The term "lattice" is also used to refer to the group without the bilinear form, so maybe a better terminology is to say that a lattice is integral, even or odd, with the understanding that this is with respect to some underlying bilinear form.

The **dual** of an integral lattice is

$$L' = \{y \in L \otimes \mathbb{R} : x \cdot y \in \mathbb{Z} \text{ for every } x \in L\}.$$

It is the dual of L as a $\mathbb{Z}$-module, i.e. every $\mathbb{Z}$-linear map $L \to \mathbb{Z}$ can be written uniquely as $\lambda \mapsto \lambda' \cdot \lambda$ with $\lambda' \in L'$. The **discriminant group** of L is the abelian group L'/L of order $|\det G|$, where $G_{ij} = e_i \cdot e_j$ is the Gram matrix of L and the e_i form an integral basis for L, i.e. $L = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r$. The mod-1 reduction of the bilinear form gives rise to a $\mathbb{Q}/\mathbb{Z}$-valued bilinear form on L'/L. If L is nondegenerate and even, then the mod 1 reduction of the quadratic form $x^2/2$ is trivial on L and gives a $\mathbb{Q}/\mathbb{Z}$-valued quadratic form on L'/L; together they are called a **discriminant form**. In fact, any finite abelian group A equipped with a $\mathbb{Q}/\mathbb{Z}$-valued quadratic form is called a discriminant form, since they all arise in this way from even nondegenerate lattices.

Milgram's formula relates the quadratic form on L'/L to the **signature** $\mathrm{sig}(L) = b_+ - b_-$ of the lattice L by

$$\sum_{\lambda \in L'/L} e^{2\pi i \lambda^2/2} = \sqrt{|L'/L|} e^{2\pi i \mathrm{sig}(L)/8}.$$

The signature $\mathrm{sig}(A) \in \mathbb{Z}/8$ of a discriminant form A is the mod 8 reduction of the signature of any even lattice L with the same discriminant form.

The double cover $\widetilde{\mathrm{GL}}_2^+(\mathbb{Z})$ of $\mathrm{GL}_2^+(\mathbb{R})$ consists of pairs (g, ϕ) with $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ and $\phi : \mathfrak{H} \to \mathbb{C}$ a holomorphic function such that $\phi(\tau)^2 = c\tau + d$ (there are two such choices of holomorphic square roots for each g), with multiplication

$$(g_1, \phi_1)(g_2, \phi_2) = (g_1 g_2, \phi), \;\; \phi(\tau) = \phi(g_2\tau)\phi_2(\tau)).$$

Example. $\mathbb{Z}^2$ is an odd lattice with respect to the usual form $n \cdot m = n_1 m_1 + n_2 m_2$.

Example. $\mathbb{Z}^2$ is an even lattice with respect to the form $n \cdot m = n_1 m_2 + n_2 m_1$. It is *not* a lattice with respect to $n \cdot m = \frac{1}{2}(n_1 m_2 + n_2 m_1)$ because $(1, 0) \cdot (0, 1) = 1/2$, even though each $n^2 \in \mathbb{Z}$.

Example. Let K be a number field and let e_i be any integral basis for its ring of integers $\mathcal{O}_K$. Recall that the **discriminant** of K is the determinant of the matrix $\mathrm{Tr}\, e_i e_j$ for the

trace form. Let $K = \mathbb{Q}(\sqrt{d})$ be the quadratic field with discriminant $d \equiv 1 \bmod 4$. Then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ is the unique quadratic order of discriminant d, and the trace form is given by the matrix

$$\begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix}$$

relative to the basis $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$. Note that $\mathcal{O}_K$ is an odd lattice with respect to the trace form because $d + 1 \equiv 2 \bmod 4$. Similarly, for the order $\mathcal{O}_D = \mathbb{Z} + \frac{D+\sqrt{D}}{2}\mathbb{Z}$ of discriminant D, the trace form is given by the matrix

$$\begin{pmatrix} 2 & D \\ D & \frac{D^2+D}{2} \end{pmatrix},$$

and this also doesn't make $\mathcal{O}_D$ into an even lattice because $D(D+1)$...

Suppose further that $|d| = p$ is prime Let p be prime and let $d = p$ if $p \equiv 1 \bmod 4$ and $d = -p$ if $p \equiv 3 \bmod 4$. Then $d \equiv 1 \bmod 4$ and $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_p)$ is the quadratic field of discriminant d. Relative to the basis $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ for $\mathcal{O}_K$, the norm on K gives the following quadratic form (the **norm form**) on K

$$Q(x) = N\left(x_1 + x_2\frac{1+\sqrt{d}}{2}\right) = x\overline{x} = \frac{1}{2}\operatorname{Tr} x\overline{x} = x_1^2 + x_1x_2 + \left(\frac{1-d}{4}\right)x_2^2 = \frac{1}{2}x^T\begin{pmatrix} 2 & 1 \\ 1 & \frac{1-d}{2} \end{pmatrix}x.$$

This makes $\mathcal{O}_K$ into an even lattice (since $\frac{1-d}{2}$ is even) with respect to the symmetric bilinear form

$$x \cdot y = \operatorname{Tr} x\overline{y} = Q(x+y) - Q(x) - Q(y) = x^T\begin{pmatrix} 2 & 1 \\ 1 & \frac{1-d}{2} \end{pmatrix}y.$$

Indeed, recall that the discriminant of K is defined to be the discriminant of its maximal order, which turns out to equal minus the determinant (the famous b^2-4ac from the quadratic formula) of the matrix of the bilinear form associated to any integral basis of $\mathcal{O}_K$.

For $p = 3, 5, 7, 11, 13$, these forms have the matrices $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 1 \\ 1 & -2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 6 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 1 \\ 1 & -6 \end{smallmatrix}\right)$. Note that $\mathcal{O}_K$ has indefinite signature $(1,1)$ when $p \equiv 1 \bmod 4$ and positive definite signature $(2,0)$ when $p \equiv 3 \bmod 4$. Also note that the discriminant of K is equal to the determinant (without a minus) of the matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{smallmatrix}\right)$ corresponding to the form $\operatorname{Tr} xy$. Is there an obvious reason for this coming from linear algebra (i.e. involving a matrix of determinant -1)? Note that $\mathcal{O}_K$ is not an even lattice for the trace form because $1 + d \equiv 2 \bmod 4$.

These are the *only* quadratic orders with discriminant groups of odd prime order. But why use quadratic orders? Can I find sublattices of $\mathbb{Q}(\zeta_3)$ that are dual to $\mathbb{Z}[\zeta_3]$ with respect to some bilinear form?

Because it is the only prime dividing the discriminant, the only rational prime that ramifies in K is p. It factors as $p\mathcal{O}_K = \mathfrak{p}^2$, where $\mathfrak{p} = \sqrt{p}\mathcal{O}_K$, and $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$. The ideal $\mathfrak{p}$ is called the **different** ideal of $\mathcal{O}_K$, and in general, its norm equals the absolute value of the discriminant. The dual lattice with respect to the trace form $\operatorname{Tr} xy$ can be expressed as a fractional ideal using the different: $\mathcal{O}_K' = \mathfrak{p}^{-1}$. How can I get it for the norm form?? We therefore have

$$\mathcal{O}_K'/\mathcal{O}_K = \mathfrak{p}^{-1}/\mathcal{O}_K \simeq \mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p.$$

How can I get a basis for the dual lattice $\mathfrak{p}^{-1}$? Well, I think we have $\mathfrak{p}^{-1} = \frac{1}{\sqrt{d}}\mathcal{O}_K$. I think the quotient, which is what I really want, is $\mathcal{O}'_K/\mathcal{O}_K = \left\{\frac{j}{\sqrt{d}} + \mathcal{O}_K : j = 0, \ldots, d-1\right\}$.

Given the basis $e_1 = 1$, $e_2 = \frac{1}{2}(\sqrt{p} + 1)$,

Example. Let n be a non-square integer. The quadratic ring $\mathbb{Z}[\sqrt{n}]$ has norm form $N(x_1 + x_2\sqrt{n}) = x_1^2 - nx_2^2$, and so $x \cdot y = 2x_1y_1 - 2nx_2y_2$. This case is boring because the matrix $\left(\begin{smallmatrix}2 & \\ & -2n\end{smallmatrix}\right)$ is diagonal and thus reduces to tensor products of Weil representations corresponding to 1-dimensional lattices.

Let n be squarefree. If $n \equiv 2$ or $3 \bmod 4$, then $\mathbb{Z}[\sqrt{n}]$ is the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{n})$ of discriminant $d = 4n$. If $n \equiv 1 \bmod 4$, then $\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$ is the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{n})$ of discriminant $d = n$, while $\mathbb{Z}[\sqrt{n}]$ is the order of conductor 2 and discriminant $4n = 4d$.

The order of conductor f in the quadratic field $\mathbb{Q}(\sqrt{d})$ of discriminant d is the unique quadratic order of discriminant $D = f^2d$, satisfying

$$\mathcal{O}_D = \mathbb{Z}\left[\frac{D + \sqrt{D}}{2}\right] = \mathbb{Z}\left[f\frac{d + \sqrt{d}}{2}\right] = \mathbb{Z} + f\mathcal{O}_d.$$

When d is a fundamental discriminant satisfying $d \equiv 1 \bmod 4$, we can express the bilinear form in the basis $\left\{1, \frac{d+\sqrt{d}}{2}\right\}$ for the maximal order $\mathcal{O}_d \subset \mathbb{Q}(\sqrt{d})$ as

$$\begin{pmatrix}2 & d \\ d & \frac{d^2-d}{2}\end{pmatrix} = \begin{pmatrix}1 & 0 \\ \frac{d-1}{2} & 1\end{pmatrix}\begin{pmatrix}2 & 1 \\ 1 & \frac{1-d}{2}\end{pmatrix}\begin{pmatrix}1 & \frac{d-1}{2} \\ 0 & 1\end{pmatrix}.$$

Actually I think if u_3 is the Zauner unit then $\mathcal{O}_D = \mathbb{Z}[u_3]$ and the corresponding quadratic form really is $\begin{pmatrix}2 & d-1 \\ d-1 & 2\end{pmatrix}$.

14.5 Weil representation from Bump

Let E be a semisimple commutative algebra over $\mathbb{F}_p$ of dimension 2. If $x \mapsto \overline{x}$ is the unique order-two involution on E, then the trace and norm homomorphisms $\mathrm{tr}, \mathrm{N} \colon E \to F$ are defined as $\mathrm{tr}(x) = x + \overline{x}$ and $\mathrm{N}(x) = x\overline{x}$. There are two possibilities: the **split** case

$$E = \mathbb{F}_p^2,\ \ \overline{(x_1, x_2)} = (x_2, x_1),\ \ \mathrm{tr}((x_1, x_2)) = x_1 + x_2,\ \ \mathrm{N}((x_1, x_2)) = x_1 x_2$$

and the **anisotropic**, or **non-split** case

$$E = \mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{\nu}),\ \ \overline{x_1 + \sqrt{\nu} x_2} = x_1 - \sqrt{\nu} x_2,\ \ \mathrm{tr}(x_1 + \sqrt{\nu} x_2) = 2x_1,\ \ \mathrm{N}(x_1 + \sqrt{\nu} x_2) = x_1^2 - \nu x_2^2.$$

Bump defines the **Weil representation** of $\mathrm{SL}_2(\mathbb{F}_p)$ on the complex-valued functions $\mathbb{C}(E)$ on E as

$$\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \Phi(v) = \Phi(av),\ \ \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \Phi(v) = \zeta_p^{bN(v)} \Phi(v),\ \ \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \Phi(v) = \frac{\epsilon}{p} \sum_{w \in E} \zeta_p^{\mathrm{tr}(v\overline{w})} \Phi(w),$$

where $\epsilon = 1$ or -1 according to whether E is split or non-split. I believe this representation is also defined over the $\mathbb{Q}(\zeta_p)$-valued functions as well. $\mathbb{C}(E)$ contains all the principal series representations when E is split, and all the discrete-series representations when E is non-split.

Let V be a vector space over $\mathbb{F}_p$ and let $B \colon V \times V \to \mathbb{F}_p$ be a nondegenerate, symmetric bilinear form. This defines a Heisenberg group $H = V \times V \times \mathbb{F}_p$ with product

$$(x, y, z) \cdot (x', y', z') = (x + x', y + y', z + z' + B(x, y') - B(x', y))$$

Up to isomorphism, there is a unique irreducible representation of H acting on the center as $(0, 0, z) \mapsto \zeta_p^z$; it is given on $\mathbb{C}(V)$ (actually, on $\mathbb{Q}(\zeta_p)(V)$) as

$$(x, 0, 0)\phi(v) = \zeta_p^{-2B(v,x)} \phi(v),\ \ (0, y, 0)\phi(v) = \phi(v + y).$$

The $\mathrm{SL}_2(\mathbb{F}_p)$ action $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(x, y, z) = (ax + by, cx + dy, z)$ on H by automorphisms fixing the center defines, in the usual way, a projective representation of $\mathrm{SL}_2(\mathbb{F}_p)$. It lifts to a linear representation – the Weil representation – on $\mathbb{C}(V)$ as

$$\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \phi(v) = \left(\frac{a}{p}\right)^{|V|} \phi(av),\ \ \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \phi(v) = \zeta_p^{bB(v,v)} \phi(v),\ \ \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \phi(v) = \varepsilon p^{-\frac{|V|}{2}} \sum_{w \in V} \zeta_p^{2B(w,v)} \phi(w),$$

where ε is a certain 4th root of unity coming from a Gauss sum (work it out). Note that the Gauss sum of the quadratic character $\chi \in \widehat{\mathbb{F}_p^\times}$ evaluates to

$$G(\chi) = \sum_{y \in \mathbb{F}_p^\times} \chi(y) \zeta_p^y = \sum_{\substack{\text{squares} \\ y \in \mathbb{F}_p^\times}} \zeta_p^y - \sum_{\substack{\text{non-squares} \\ y \in \mathbb{F}_p^\times}} \zeta_p^y = 1 + 2 \sum_{\substack{\text{squares} \\ y \in \mathbb{F}_p^\times}} \zeta_p^y = \zeta_p^0 + \sum_{x \in \mathbb{F}_p^\times} \zeta_p^{x^2} = \sum_{x \in \mathbb{F}_p} \zeta_p^{x^2}.$$

For the embedding $\zeta_p \mapsto e^{2\pi i a/p}$, it is known that $G(\chi) = \chi(a)\sqrt{\chi(-1)p}$ with $\sqrt{-1} = i$.

The two representations from the exercises coincide with the one in the text by taking V as the underlying vector space of E and setting $B(x, y) = \frac{1}{2}\,\mathrm{tr}(x\overline{y})$.

14.6 Metaplectic Weil representation

The Weil representation can be viewed as a representation of the preimage $\widetilde{\mathrm{SL}_2(\mathbb{Z})}$ of $\mathrm{SL}_2(\mathbb{Z})$ under the double cover
$$1 \to \pm 1 \to \widetilde{\mathrm{SL}_2(\mathbb{R})} \to \mathrm{SL}_2(\mathbb{R}) \to 1,$$
where
$$\widetilde{\mathrm{SL}_2(\mathbb{R})} = \left\{ \left(\phi, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) : \phi : \mathfrak{H} \to \mathbb{C} \text{ holomorphic s.t. } \phi(\tau)^2 = c\tau + d \right\}.$$

It is known that $\widetilde{\mathrm{SL}_2(\mathbb{Z})}$ is generated by $t = \left(1, \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\right)$ and $\tilde{s} = \left(\sqrt{\tau}, \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\right)$ satisfying $\tilde{s}^2 = (\tilde{s}t)^3 = (i, -I)$. Let L be an even lattice with level N and let $Q(v) = \frac{v\dot{v}}{2}$ Then $e^{2\pi i Q(L)} = \langle \zeta_N \rangle$ and there is an explicit realization of this Weil representation on $\mathbb{Q}(\zeta_N)[L^\vee/L]$ given by
$$t[v] = e^{2\pi i Q(v)}[v], \quad \tilde{s}[v] = \frac{1}{\mathfrak{g}_L} \sum_{[w] \in L^\vee/L} e^{-2\pi i v\cdot w}[w],$$
where
$$\mathfrak{g}_L = \sqrt{|L^\vee/L|}\zeta_8^{\sigma_L}$$
is the quadratic Gauss sum (more on this... relation to $\mathrm{Tr}\, T$?). Then $C[v] = i^{-\sigma_L}[-v]$.

Now I basically worked out that when d is prime, we should normalize by $\frac{1}{\sqrt{d^*}}$, where $d^* = (-1)^{\frac{d-1}{4}} d$, since $\sqrt{d^*} \in \mathbb{Z}[\zeta_d]$. Therefore I expect a lattice with even signature when $d \equiv 1 \bmod 4$ and one with odd signature when $d \equiv 3 \bmod 4$. The lattice $(\mathbb{Z}, \frac{xy}{d})$ should work in the $d \equiv 3 \bmod 4$ cases, but what about the $d \equiv 1 \bmod 4$ cases?

When d is odd, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D_0}}{2}\right]$. There is a homomorphism $\mathcal{O}_K \mapsto \mathbb{Z}^{2\times 2}$ such that $\sqrt{D_0} \mapsto \begin{pmatrix} 1 & \frac{D_0-1}{4} \\ 0 & 1 \end{pmatrix}$ or something like that (check notes).

15 Lattices

15.1 Strongly perfect complex lattices

A lattice is **perfect** if the projections vv^T onto the minimal vectors v span the space of symmetric matrices. Korkine and Zolotarev (see e.g. Nebe) showed that a lattice is perfect iff it is proportional to an integral lattice. A lattice is **eutactic** if I is in the relative interior of the cone generated by the rank-1 matrices vv^T determined by the minimal vectors v, and is **strongly eutactic** if the minimal vectors are a tight frame. Voronoi proved that a lattice in $\mathbb{R}^d$ is extreme iff it is perfect and eutactic. Venkov further defined a lattice to be **strongly perfect** if its minimal vectors form a spherical 4-design, and **dual strongly perfect** if both it and its dual are strongly perfect.

Strongly perfect lattices are strongly eutactic and perfect, implying that they are extreme. In the Euclidean case, the theta function is

$$\theta(\tau) = \sum_{x \in L} q^{Q(x)} = \sum_{n \geq 0} a_n q^n.$$

In the general case L can have infinitely many vectors of a given length, as well as vectors of negative length. We may hope that there is a rank-$2d$ $\mathbb{Z}$-lattice $L \subset F^d$. If it is a complex lattice, complex conjugation should be an automorphism.

If it is also a rank-d $\mathcal{O}$-lattice for a quadratic order $\mathcal{O}_D \subset \mathcal{O} \subset \mathcal{O}_K$, we expect the $\mathcal{O}$-action to induce an action of $K_d^\times$ on L^*/L. It would have to work like this: Let I be the group of fractional ideals prime to (d) and let P be its subgroup of principal ideals. More generally, for a modulus $\mathfrak{m}$ in K, let $P_\mathfrak{m}$ be the principal ideals with an $\mathfrak{m}$-positive generator, i.e. of the form (a) with $a \equiv 1 \bmod \mathfrak{m}$. Then

$$P_{d\infty} \subset P_{d\infty_\pm} \subset P_d \subset P_1 = P_{\infty_\pm} = P \subset I,$$

with $P_{d\infty_+}$ and $P_{d\infty_-}$ Galois conjugates of one another.

The Artin map $\sigma : I \to \mathrm{Gal}(K^{(d)\infty}/K)$ has kernel $P_{d\infty}$, giving isomorphisms

$$\mathrm{Gal}(K^{(d)\infty}/K) \simeq I/P_{d\infty},\ \mathrm{Gal}(K^{(d)\infty}/K^{(1)}) \simeq P/P_{d\infty},\ \mathrm{Gal}(K^{(d)\infty}/K^{\infty}) \simeq P_\infty/P_{d\infty}.$$

Restricting to the subfields $K^{(d)\infty_\pm}$ gives isomorphisms

$$\mathrm{Gal}(K^{(d)\infty_\pm}/K) \simeq I/P_{d\infty_\pm},\ \mathrm{Gal}(K^{(d)\infty_\pm}/K^{(1)}) \simeq P/P_{d\infty_\pm}.$$

Let $u_0 \in \mathcal{O}^\times$ be the fundamental unit and let u_+ generate the totally positive units. Then $u_+ = u_0^2$ iff $N(u_0) = -1$ iff $P_\infty = P$ iff $K^\infty = K^{(1)}$. Otherwise, $u_+ = u_-$, etc. We showed that $d = u_+^r + u_+^{-r} + 1$ for some r, and that $\mathrm{ord}(u_+ \bmod d) = 3r$. Let h be the class number of $\mathcal{O}$ and h_+ the narrow class number. Then the order of u_0 is $3rh_+/h$. There are h_+ Clifford orbits of fiducials in the corresponding multiplet, and h extended Clifford ones. Surprisingly, this exact statement seems to hold for all d, not just d even.

Furthermore, the mod-$d\infty$ reduction map $\phi : K^\times(d) \to (\mathcal{O}/d)^\times \times \langle -1 \rangle^2$ seems to be surjective, which I think follows from strong approximation. Under multiplication, the unit group $\mathcal{O}^\times$ acts transitively on the generators of each principal ideal.

For prime $d \equiv 2 \bmod 3$, we always have $u_0 = u_+$, and so $K^\infty \neq K^{(1)}$. If $T_{\mathrm{GL}} = \langle t \rangle$, then $u_0 \equiv (t^{(d^2-1)/3r}, 1, 1) \bmod d\infty$.

For prime $d \equiv 1 \bmod 3$, then $T_{\mathrm{GL}} \simeq (\mathbb{Z}/d)^2 \times (\mathbb{Z}/d)^2$ is split and $u_0 \equiv (\alpha^{(d-1)/6r}, \alpha^{-1(d-1)/6r}, 1, -1)$ and $u_+ \equiv (\alpha^{(d-1)/3r}, \alpha^{-1(d-1)/3r}, 1, 1)$. Actually that's a guess that is probably not true - do it more carefully.

If K is imaginary quadratic, the rank-2 $\mathbb{Z}$-lattices $L \subset K$ is an $\mathcal{O}$-lattice and $\mathfrak{a}$ is prime to (what?), then $j(L)^{\mathfrak{a}} = j(L\mathfrak{a})$

There is a generalization of the notion of perfection described e.g. in Martinet, accompanied by a suitable generalization (and strengthening of Voronoi's theorem). What is the correct notion for complex lattices? I expect that a perfect complex lattice is extreme iff its minimal vectors determine an IC-POVM.

15.2 Lattices in K and Boylan's Weil representation

The quadratic field $K = \mathbb{Q}(\sqrt{D})$ is a quadratic space with respect to the trace bilinear form $b(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$. Each fractional ideal $\mathfrak{a}$ of K is a rank-2 $\mathbb{Z}$-lattice (as well as a rank-1 $\mathcal{O}_K$-lattice). The ring of integers $\mathcal{O}_K$ are an even $\mathbb{Z}$-lattice for b Let $\mathfrak{D} \subset \mathcal{O}_K$ (be the **different**, by definition the largest ideal on which b is integral. For our quadratic field, it is given by $\mathfrak{D} = \sqrt{D_0}\mathcal{O}_K$. The dual lattice $\mathcal{O}_K^\vee$ to $\mathcal{O}_K$ with respect to b is then equal to the fractional ideal $\mathfrak{D}^{-1}$.

Let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal. Then $\mathfrak{a}$ is a sublattice of $\mathcal{O}_K$, hence an even lattice. The dual lattice to $\mathfrak{a}$ for the trace form is the fractional ideal

$$\mathfrak{a}^\vee = \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(x\mathfrak{a}) \subset \mathbb{Z}\} = \mathfrak{a}\mathfrak{D}^{-1},$$

The inverse different $\mathcal{O}_K^\vee = \mathfrak{D}^{-1}$ is the largest fractional ideal on which $\mathrm{Tr}_{K/\mathbb{Q}}$ is integral. However, each integral ideal $\mathfrak{a} \subset \mathcal{O}_K$ has the same discriminant with respect to the trace norm:

$$|\mathfrak{a}^\vee/\mathfrak{a}| = |\mathfrak{a}\mathfrak{D}^{-1}/\mathfrak{a}| = |\mathfrak{D}^{-1}/\mathcal{O}_K| = |\mathcal{O}_K/\mathfrak{D}| = \mathrm{N}(\mathfrak{D}) = D_0.$$

This could probably be repeated for quadratic orders $\mathcal{O}_D$ of not-necessarily-fundamental discriminant D, replacing D_0 with D throughout.

Suppose we use $b_\alpha(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{xy}{\alpha}\right)$ for the inner product. Then the dual lattice to a fractional ideal $\mathfrak{a}$ is

$$\{x \in K : b_\alpha(x, \mathfrak{a}) \subset \mathbb{Z}\} = (\mathfrak{a}/\alpha)^\vee = \mathfrak{a}(\alpha\mathfrak{D})^{-1} = \alpha^{-1}\mathfrak{a}^\vee.$$

Then $[\mathfrak{a}(\alpha\mathfrak{D})^{-1} : \mathfrak{a}] = \mathrm{N}(\alpha\mathfrak{D}) = \mathrm{N}(\alpha)D_0$ So we need $\mathrm{N}(\alpha) = \alpha\alpha' = d/D_0$, which for the $d = 7$ example is $7/8$. Indeed, $\alpha = \frac{1}{4}(4 - \sqrt{2})$ has $\mathrm{N}(\alpha) = 7/8$. While it is tempting to conjecture that $\mathbb{Q}(\sqrt{D_0})$ always contains a solution to the norm equation $\mathrm{N}(\alpha) = d/D_0$., it seems to hold often but not always. Any pattern? What about the class number? Could it have to do with whether or not $\sqrt{d} \in \mathcal{O}_K$?

Boylan gives a theory of Weil representations associated to finite quadratic over number fields. A **finite quadratic $\mathcal{O}$-module** (M, q) consists of a finite $\mathcal{O}$-module M and a **finite quadratic form** $q : M \to K/\mathfrak{D}^{-1}$, meaning that $q(ax) = a^2 q(x)$ for all $a \in \mathcal{O}$ and that $b(x,y) = q(x+y) - q(x) - q(y)$ is a nondegenerate ($b(x, M) = 0$ iff $x = 0$) bilinear symmetric form.

Let (L, B) be an **even $\mathcal{O}$-lattice**, i.e. an $\mathcal{O}$-lattice L and a symmetric nondegenerate $\mathcal{O}$-bilinear form $B : L \times L \to \mathfrak{D}^{-1}$ with $B(x,x) \in 2\mathfrak{D}^{-1}$ for all $x \in L$. Let $L^\vee = \{x \in K \otimes_{\mathcal{O}} L : B(x, L) \subset \mathfrak{D}^{-1}\}$. Then $(L^\vee/L, q)$ is a finite quadratic $\mathcal{O}$-module where $q([x]) = [B(x,x)/2]$ (i.e. $q(x+L) = \frac{1}{2}B(x,x) + \mathfrak{D}^{-1}$). Furthermore, $(L^\vee/L, \mathrm{Tr}_{K/\mathbb{Q}}\, q)$ is a finite quadratic $\mathbb{Z}$-module. The **level** of a finite quadratic module (M, q) is $\mathfrak{n} = \{a \in \mathcal{O} : aq(M) = 0\}$ and the **annihilator** is $\mathfrak{a} := \{a \in \mathcal{O} : aM = 0\}$. These are integral ideals satisfying $\mathfrak{n} \subset \mathfrak{a} \subset \mathfrak{n}/2$. If $a \nmid \mathfrak{n}$, then we can **twist** by a: $(M, q)^a = (M, aq)$.

Boylan defines a Weil representation on $\mathbb{C}[M]$ via the matrices

$$T_b = \sum_{[x]\in M} e^{2\pi i\, \mathrm{Tr}_{K/\mathbb{Q}}\, bq(x)} |[x]\rangle\langle[x]|, \quad S = \frac{\mathfrak{g}_M}{\sqrt{|M|}} \sum_{[x],[y]\in M} e^{-2\pi i\, \mathrm{Tr}_{K/\mathbb{Q}}\, B(y,x)} |[y]\rangle\langle[x]|,$$

where

$$\mathfrak{g}_M = \sum_{[x]\in M} e^{-2\pi i q([x])} = \sum_{[x]\in M} e^{-\pi i N_{K/\mathbb{Q}}(x)}.$$

Then $\langle S, T_b : b \in \mathcal{O}\rangle = \tilde{\Gamma} \to \Gamma_{\mathcal{O}} = \mathrm{SL}_2(\mathcal{O})$ is a (finite?) cover of the Hilbert modular group $\mathrm{SL}_2(\mathcal{O})$. This seems to factor through the associated finite quadratic $\mathbb{Z}$-module. Is there a natural way to get the relevant maximal tori using the T_b and S?

If M is cyclic (i.e. a principal fractional $\mathcal{O}$-ideal) of level $\mathfrak{n}$, then the annihilator satisfies $\mathfrak{a} = \mathfrak{n}(2, \mathfrak{n})^{-1}$ and we have $M \simeq \mathcal{O}/\mathfrak{a}$. Let $\mathfrak{m} = \mathfrak{n}(2,\mathfrak{n})^{-1} \subset \mathcal{O}$ denote the **modified level**. Boylan shows that each isotropic submodule has the form $U = \mathfrak{a}\mathfrak{b}^{-1}M$ for some $\mathfrak{b} \subset \mathcal{O}$ with $\mathfrak{b}^2 \mid \mathfrak{m}$. The **quotient** of M/U by such a submodule is (defined as?) $U^\vee/U$. Note that it is well-defined by restriction since $Q(U) = 0$.

Note that in generalizing from $\mathbb{Q}$ to K, we replace $\mathbb{Q}/\mathbb{Z}$ with $K/\mathfrak{D}^{-1}$, and the discriminant group then gets an action by $\mathcal{O}$.

Here is a conjecture: For each SIC, there exists a 2-dimensional abelian variety/scheme A with real multiplication by $\mathcal{O}$ and defined over the real ring class field $K^{\mathcal{O}}$, as well as an embedding $A \hookrightarrow \mathrm{Proj}(R_{K^{\mathcal{O}}})$ taking the d^2 real d-torsion points in $A[d]$ to a SIC.

For each fractional ideal $\mathfrak{a} \in I(K)$, there should be a fiducial $P_{\mathfrak{a}}$, such that for every fractional ideal $\mathfrak{b} \in I_{(d)}(K)$, we have $P_{\mathfrak{a}}^{\left(\frac{F}{\mathfrak{b}}\right)} = P_{\mathfrak{a}\mathfrak{b}}$, where $\mathfrak{b} \mapsto \left(\frac{F}{\mathfrak{b}}\right) \in \mathrm{Gal}(F/K)$ is the Artin map from class field theory. If $\mathfrak{b} \in P_{(d)}(K)$, then $\mathfrak{a}$ and $\mathfrak{a}\mathfrak{b}$ are in the same ideal class, and if $\mathfrak{b}$ also has a totally positive generator, then $\mathfrak{a}$ and $\mathfrak{a}\mathfrak{b}$ are in the same strict ideal class.

More generally, for each $\mathcal{O}$-lattice in K, where $\mathcal{O}_D \subset \mathcal{O} \subset \mathcal{O}_{D_0} = \mathcal{O}_K$, there should be a similar story... Work it out. Recall that if $L \subset K$ is a rank-2 $\mathbb{Z}$-lattice, then $\mathcal{O}_L := \{x \in K : xL \subset \mathcal{O}_K\}$ is an order. What is the relationship between its conductor f_L (here $\mathcal{O}_L = \mathcal{O}_{f_L^2 D_0}$ and the lattice? Is it that the lattice is no longer primitive, being a module over a Noetherian domain that is not integrally closed and is therefore not a Dedekind domain? Given a $\mathbb{Z}$-basis, is it the case that f divides the coefficients of the corresponding quadratic form $ax^2 + bx + c$?

15.3 Abelian varieties with real multiplication

Let K be a totally real number field of degree e. For each $m \in \mathbb{N}$, there are complex abelian varieties of dimension $g = me$ with real multiplication by K. Tensoring with $\mathbb{R}$ gives an isomorphism $K^{2m} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{2g}$ via

$$v \mapsto \nu(v) := v \otimes 1 = \begin{pmatrix} \nu_1(v) \\ \vdots \\ \nu_e(v) \end{pmatrix} \in \mathbb{R}^{2g},$$

where $\nu_i : K \hookrightarrow \mathbb{R}$ are the e real embeddings of K. Let $\tau = (\tau_1, \ldots, \tau_e)$, where each τ_i is in the Siegel upper-half space $\mathfrak{H}_m$, and let

$$h_\tau(\psi, \phi) = \psi^\dagger \begin{pmatrix} (\operatorname{Im}\tau_1)^{-1} & & \\ & \ddots & \\ & & (\operatorname{Im}\tau_e)^{-1} \end{pmatrix} \phi$$

be the associated positive-definite Hermitian form on $\mathbb{C}^{2g}$. For $v = \left(\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right) \in K^{2m}$, let

$$v_\tau = \begin{pmatrix} \tau_1\nu_1(v_1) + \nu_1(v_2) \\ \vdots \\ \tau_e\nu_e(v_1) + \nu_e(v_2) \end{pmatrix} \in \mathbb{C}^g.$$

Then

$$\operatorname{Im} h_\tau(v_\tau, w_\tau) = \operatorname{Tr}_{K/\mathbb{Q}}\left(v^T \begin{pmatrix} & I_m \\ -I_m & \end{pmatrix} w \right) = v_{\mathbb{R}}^T \begin{pmatrix} & I_m & & & & & \\ -I_m & & & & & & \\ & & & I_m & & & \\ & & -I_m & & & & \\ & & & & \ddots & & \\ & & & & & & I_m \\ & & & & & -I_m & \end{pmatrix} w_{\mathbb{R}}.$$

Let L be a free rank-$2g$ $\mathbb{Z}$-submodule of K^{2m} on which the above symplectic form is integral (e.g. $L = \mathcal{O}_K^m$). Then $\mathbb{C}^g/L$ is an abelian variety with real multiplication by K, where $a \in K$ acts on $\mathbb{C}^g$ as

$$\rho(a) = \begin{pmatrix} \nu_1(a)I_m & & \\ & \ddots & \\ & & \nu_e(a)I_m \end{pmatrix},$$

so that $\rho(a)v_\tau = (av)_\tau$.

15.4 Real quadratic multiplication

Now suppose that K is real quadratic ($e = 2$) so that $g = 2m$.

Then for $a \in K$ and $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in K^{2m}$, we have

$$\rho(a) = \begin{pmatrix} aI_m & \\ & a'I_m \end{pmatrix}, \quad \nu(v) = v \otimes 1_{\mathbb{R}} = \begin{pmatrix} v \\ v' \end{pmatrix} \in \mathbb{R}^{4m},$$

where we identify K with its image under the real embedding in which $\sqrt{D} > 0$. For $\tau = (\tau_1, \tau_2) \in \mathfrak{H}_m \times \mathfrak{H}_m$, we have

$$v_\tau = \begin{pmatrix} \tau_1 & 1 & & \\ & & \tau_2 & 1 \end{pmatrix} \nu(v) = \begin{pmatrix} \tau_1 v_1 + v_2 \\ \tau_2 v_1' + v_2' \end{pmatrix} \in \mathbb{C}^{2m}.$$

The corresponding Hermitian form

$$h_\tau(\psi, \phi) = \psi^\dagger \begin{pmatrix} (\operatorname{Im}\tau_1)^{-1} & \\ & (\operatorname{Im}\tau_2)^{-1} \end{pmatrix} \phi$$

satisfies

$$\begin{aligned} \operatorname{Im} h_\tau(v_\tau, w_\tau) &= \begin{pmatrix} v_1 \\ v_2 \\ v_1' \\ v_2' \end{pmatrix}^T \begin{pmatrix} & I_m & & \\ -I_m & & & \\ & & & I_m \\ & & -I_m & \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_1' \\ v_2' \end{pmatrix} \\ &= \operatorname{Tr}_{K/\mathbb{Q}} \left(v^T \begin{pmatrix} & I_m \\ -I_m & \end{pmatrix} w \right) \\ &= \operatorname{Tr}_{K/\mathbb{Q}}(v_1 \cdot w_2 - v_2 \cdot w_1). \end{aligned}$$

Let $L \subset K^m$ be a rank-$2m$ $\mathbb{Z}$-lattice with

$$\operatorname{Tr}_{K/\mathbb{Q}}(v_1 \cdot w_2 - v_2 \cdot w_1) \in \mathbb{Z}$$

for all $v, w \in L$. Then $A = \mathbb{C}^{2m}/L_\tau$ is an abelian variety with real multiplication. The Hermitian form $h_\tau(\phi, \psi) = \phi^\dagger \begin{pmatrix} \operatorname{Im}\tau_1 & \\ & \operatorname{Im}\tau_2 \end{pmatrix}^{-1} \psi$ on $\mathbb{C}^{2m}$ determines a polarization in the form of an isogeny $A \to \hat{A} = \operatorname{Pic}_0(A)$ to the dual abelian variety. Because A is polarized, $\operatorname{End}(A)$ is finite. The polarization also determines a Rosatti involution on $\operatorname{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}$

For example, $L = \mathcal{O}_K^2$ works, in which case we probably get Hilbert modular forms for $\operatorname{SL}_2(\mathcal{O}_K)$. More generally, probably consider ideals of the form $\mathfrak{a} \oplus \mathcal{O}_K$ or mabe with intermediate quadratic orders $\mathcal{O}$. Note that $\mathbb{P}^1(\mathcal{O}_K) \simeq \operatorname{CL}(\mathcal{O}_K)$. Each rank-2 $\mathcal{O}_K$-lattice in K^2 should be $\operatorname{SL}_2(\mathcal{O}_K)$-equivalent to one of the form $\mathfrak{a} \oplus \mathcal{O}$, where $\mathfrak{a}$ is an ideal of a quadratic order $\mathcal{O} \subset \mathcal{O}_K$. Is there a form of stable equivalence here?

There is a bijection between the cusps $\operatorname{PSL}_2(\mathcal{O}_K)\backslash\mathbb{P}^1(K)$ and the class group $\operatorname{CL}(\mathcal{O}_K)$ taking $(x : y) \in \mathbb{P}^1(K)$, for $x, y \in \mathcal{O}_K$, to the class of the fractional ideal $x\mathcal{O}_K + y\mathcal{O}_K$.

Here is what van der Geer has to say: If $A = V/L$ is an abelian variety with $\dim_{\mathbb{C}} V = g$, then there is an ample line bundle whose first Chern class in $H^2(A,\mathbb{Z}) = \Lambda^2 L^*$ gives an alternating blinear form $\omega : L \times L \to \mathbb{Z}$. The $\mathbb{R}$-linear extension of ω represents the image of $H^2(A,\mathbb{Z})$ in

$$H^2(A,\mathbb{C}) \simeq \Lambda^2 \operatorname{Hom}_{\mathbb{R}}(V,\mathbb{C}) = \Lambda^2(W \oplus \bar{W}), \;\; W = \operatorname{Hom}_{\mathbb{C}}(V,\mathbb{C}).$$

Natural choices for m are $1, d-1 = Q$ and d, so $g = 2, 2Q$ or $2d$. $m = d$, so $g = 2d$. There are lots of good reasons to expect a Lorenzian torus, all stemming from the fact that $K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{1,1}$ for the norm form. Over $\mathbb{C}$ this should not matter although I may end up needing an indefinite polarization.

15.5 SICs as branched covers?

We might consider taking a hint from $N = 2$ and considering the possibility that SIC-POVMs could "be" branched covers of $\mathbb{P}^{N-1}$. Let $v_z = \frac{1}{\sqrt{1+|z|^2}}\begin{pmatrix}1 & z\end{pmatrix}$. Is there a complex lattice $L \subset \mathbb{C}^{N-1}$ such that $[v_L]$ is a SIC-POVM? In particular, v_0 should be a fiducial, so we need $\frac{1}{N+1} = |\langle v_0, v_z\rangle|^2 = \frac{1}{1+|z|^2}$, i.e. every other v_z in the SIC must satisfy $|z|^2 = N$. Furthermore if v_w and v_z are two other vectors on the SIC, they must satisfy $\frac{1}{N+1}|\langle v_w, v_z\rangle|^2 = \frac{|1+w^\dagger z|^2}{N+1}$, i.e. $|1 + w^\dagger z|^2 = 1$.

16 Appendix on class field theory

16.1 Valuations

A **valuation** v on a field K is a map restricting to a homomorphism from $K^\times$ to a totally ordered abelian group $v(K^\times)$ (the **value group**) such that $v(xy) = v(x) + v(y)$ and $v(x + y) \geq \min\{v(x), v(y)\}$ with equality if $v(x) \neq v(y)$. Furthermore one sets $v(0) = \infty$, where $\infty > v(K^\times)$ and $\infty + v(K^\times) = \infty$. A field equipped with a valuation is called a **valued field**.

A **valuation ring** is a Dedekind domain R equal to $\{x \in \operatorname{Frac}(R) : v(x) \geq 0\}$ for some valuation v on its field $\operatorname{Frac}(R)$ of fractions. Equivalently it is a Dedekind domain R such that for every $x \in \operatorname{Frac}(R)$, either $x \in R$ or $x^{-1} \in R$. Every valuation ring is a local ring with maximal ideal $\mathfrak{m} = \{x \in R : v(x) > 0\}$.

An **absolute value** on K satisfies $|xy| = |x| \cdot |y|$ and $|x + y| \leq \max\{|x|, |y|\}$ with equality if $|x| = |y|$. Each valuation gives an absolute value $|x|_v = \exp(-v(x))$. A **place** is an equivalence class of valuations/absolute values under scaling by $\mathbb{R}_+$. There are two kinds of places:

- A place is **infinite** if the value group is isomorphic to $\mathbb{R}$. Then the residue field is infinite and the absolute value is **Archimedean** ($|x + y|_v \leq |x|_v + |y|_v$). Infinite places are also called Archimedean.
- A place is **finite** if the value group is isomorphic to the integers $\mathbb{Z}$. Then R is a **discrete valuation ring** (**DVR**), the residue field $R/\mathfrak{m}$ is finite and the absolute value $|x|_v$ is non-Archimedean. Finite places are also called non-Archimedean.

The completions of number fields at Archimedean places are $\mathbb{R}$ and $\mathbb{C}$. The completions of $\mathbb{Q}$ at finite places are the p-adics $\mathbb{Q}_p$.

16.2 Galois theory

Let F/K be a normal extension of number fields and let v be a place of K. The Galois group $G = \mathrm{Gal}(F/K)$ acts transitively on the places w of F above v. For each place w above v, the pointwise stabilizer

$$G_w = \{\sigma \in G : \sigma(w) = w\}$$

depends only on v and is called **decomposition group** G_v. Therefore G_v acts on each completion F_w. The common pointwise stabilizer is the **inertia subgroup**

$$I_v = \sigma \in G_v : a^\sigma = a \text{ for all } a \in F_w.$$

The decomposition group is therefore an extension

$$1 \to I_v \to G_v \to \mathrm{Gal}(F_w/K_v) \to 1.$$

At finite places we have

$$\mathrm{Gal}(F_w/K_v) \simeq \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v) \simeq \mathrm{Gal}(\mathbb{F}_{N(\mathfrak{q}_w)}/\mathbb{F}_{N(\mathfrak{p}_v)}) \simeq \mathbb{Z}/f_v.$$

At infinite places v, I_v is trivial and v is **ramified** if $F_w/K_v = \mathbb{C}/\mathbb{R}$ with G_v generated by complex conjugation, or is otherwise **unramified** if $F_w/K_v = \mathbb{R}/\mathbb{R}$ or $\mathbb{C}/\mathbb{C}$ with G_v trivial. In particular, among the infinite places, only the real places can ramify.

Let $n = |G| = [F : K]$, let $e_v = |I_v|$ be the ramification degree and $f_v = |G_v|/e_v$ the inertial degree. There are $g_v = n/e_v f_v$ places w of F above v. Then v is unramified iff I_v is trivial ($e = 1$) and is completely split iff G_v is trivial ($ef = 1$). We have $[F_w : K_v] = e_v f_v$. If v is infinite, then $f_v = 1$ and if $w|v = \mathfrak{q}|\mathfrak{p}$, then $f_\mathfrak{p} = [\mathcal{O}_F/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$.

The decomposition group $G_v \subset \mathrm{Gal}(F/K)$ is the pointwise stabilizer of the places w above v and the inertia group I_v pointwise stabilizes each F_w. There an exact sequence

$$1 \to I_v \to G_v \to \mathrm{Gal}(F^{I_v}/F^{G_v}) \to 1$$

of abelian groups. For $\mathfrak{q} \mid \mathfrak{p}$, we have

$$\mathrm{Gal}(F^{I_\mathfrak{p}}/F^{G_\mathfrak{p}}) \simeq \mathrm{Gal}((\mathcal{O}_F/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p})) \simeq \mathrm{Gal}(\mathbb{F}_{N(\mathfrak{p})^f}/\mathbb{F}_{N(\mathfrak{p})}).$$

Their fixed fields form a chain of subextensions

$$\begin{tikzcd}
F \\
F^{I_v} \arrow[u, "e"'] \\
F^{G_v} \arrow[u, "f"'] \\
K. \arrow[u, "g"']
\end{tikzcd}$$

The decomposition field F^{G_v} is the largest subextension in which v splits completely, as well as the smallest subextension such that the places $v'|v$ divide w. The inertia field F^{I_v} is the largest subextension in which v is unramified, as well as the smallest subextension such w is totally ramified over the $v'|v$.

For infinite v, the decomposition field F^{G_v} is the real subfield in any embedding extending v. This gives two possibilities:

- v complex: $(e_v, f_v, g_v) = (2, 1, n/2)$ (v ramified), in which case v is real and w complex. Furthermore, $I_v = G_v = \langle c_v \rangle$, where c_v is complex conjugation in the places over v.
- v real: $(e_v, f_v, g_v) = (1, 1, n)$ (v completely split), in which case v and w are either both real or both complex. The decomposition group is trivial.

For finite $v = \mathfrak{p}$ and $w = \mathfrak{q}$, the groups I_v and G_v are repectively the pointwise and setwise stabilizers of $\mathfrak{q}$. If $q = N\mathfrak{p}$, then

$$G_v/I_v \simeq \mathrm{Gal}(F_w/K_v) \simeq \mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q) \simeq \mathbb{Z}/f.$$

When v is unramified, the Frobenius automorphism $x \mapsto x^q$ of the residue extension $\mathbb{F}_{q^f}/\mathbb{F}_q$ lifts to a canonical generator Frob_v of G_v, defining the Artin map on unramified prime ideals. However, there is no Frobenius element if v is ramified.

The local Artin symbol $(\alpha, F/K)_v$ is nevertheless defined at all places v and for all $\alpha \in K^\times$. If v is real and ramified, then $(\alpha, F/K)_v$ is trivial or c_v according to whether $v(\alpha) > 0$ or $v(\alpha) < 0$. To define the symbol for finite $v = \mathfrak{p}$, assume first that $\mathrm{Gal}(F/K) = \langle \sigma \rangle \simeq \mathbb{Z}/n$. The cyclic algebra

$$A = (F/K, \sigma, \alpha) := K[x : x^n = \alpha, x\beta x^{-1} = \beta^\sigma]$$

is a central simple K-algebra that is split by F, i.e. $A \otimes_K F \simeq F^{n\times n}$. The local Artin symbol is then $(\alpha, F/K)_v = \sigma^{a_v}$, where a_v is the mod-n invariant of the localized cyclic algebra $A \otimes_K K_v \simeq (K_v^{(n)}/K_v, \mathrm{Frob}, \pi^{a_v})$, where $K_v^{(n)}$ is the degree-n unramified extension of K_v, $\langle \mathrm{Frob} \rangle = \mathrm{Gal}(K_v^{(n)}/K_v)$ and $\pi \in K_v$ is a uniformizer (i.e. $\mathrm{ord}_{v'}(\pi) = 1$ if $v' = v$ and 0 otherwise). The algebra A is a $\mathrm{Gal}(F/K)$-twisted form of $F^{n\times n}$, twisted by the 1-cocycle $\mathrm{Gal}(F/K) \to \mathrm{PGL}_n(K)$ taking σ to conjugation by the matrix

$$\begin{pmatrix} & & & \alpha \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}.$$

Ramification "fractionalizes" the valuations above v in the sense that $\mathfrak{q}^e$ divides $\mathfrak{p}$. Extending the Artin map to ramified primes I think gives $G_v = \langle \sigma_\mathfrak{p} \rangle$ and $I_v = \langle \sigma_\mathfrak{p}^e \rangle$. For example, we have $|x|_v = |v(x)|$ for real v, whereas for complex v, we have $|x|_v = |v(x)|^2 = v(x)\overline{v(x)}$. For finite $v = \mathfrak{p}$ we have $|x|_\mathfrak{p} = q^{-\mathrm{ord}_\mathfrak{p}(x)}$.

16.3 L-functions

Let F/K be an abelian extension of a real quadratic field K with Galois group $G = \mathrm{Gal}(F/K)$. The Dedekind zeta function decomposes into a sum over ideal classes

$$\zeta_K(s) = \sum_{\mathfrak{C}} \zeta(s, \mathfrak{C})$$

of partial zeta functions $\zeta(s, \mathfrak{C})$. Including the gamma factors

$$\Lambda(s, \mathfrak{C}) = \pi^{-s}\Gamma(s/2)^2\zeta(s, \mathfrak{C})$$

gives a functional equation

$$\Lambda(s, \mathfrak{C}) = |D_F|^{1/2-s}\Lambda(1-s, (\mathfrak{c}\mathfrak{d}_K)^{-1}),$$

where $\mathfrak{d}_K$ is the ideal class of the different of K.

Note this example ([**BKS+03**] Ch. 2) is nice and elementary but unfortunately Stark needs ray class groups. Is there a similar formula? Is it in Roblot?

Each finite-dimensional complex Galois representation $\rho : G \to \mathrm{End}(V)$ has an associated Artin L-function

$$L(s, \rho) = \prod_{\mathfrak{p}} \det\big(1 - \rho(\mathfrak{p})|_{V^{I_\mathfrak{p}}} N(\mathfrak{p})^{-s}\big),$$

where the Euler product, converges for all $s > 1$. If $\rho = \chi$ is a 1-dimensional, then $V^{I_\mathfrak{p}}$ is trivial for ramified $\mathfrak{p}$, so this reduces to the Hecke L-function

$$L(s, \chi) = \prod_{\mathfrak{p}} \det(1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s}) = \sum_{\mathfrak{a}} \chi(\mathfrak{a})N(\mathfrak{a})^{-s}.$$

We have

$$\zeta_F(s) = \prod_{\chi \in \hat{G}} L(\chi, s)$$

16.4 Class field theory

Let K be a number field and let $\mathcal{O} \subset \mathcal{O}_K$ be an order of conductor $\mathfrak{f} := \{a \in \mathcal{O} : a\mathcal{O} \subset \mathcal{O}_K\}$. An ideal of $\mathcal{O}$ is also an ideal of $\mathcal{O}_K$ iff it is contained in $\mathfrak{f}$. By an $\mathcal{O}$-ideal, we mean an invertible fractional ideal of $\mathcal{O}$, i.e. a rank-$[K : \mathbb{Q}]$ $\mathbb{Z}$-submodule $\mathfrak{a} \subset K$ satisfying the following equivalent conditions:

- The order $\mathcal{O}(\mathfrak{a}) := \{a \in K : a\mathfrak{a} \subset \mathfrak{a}\}$ of $\mathfrak{a}$ is $\mathcal{O}$.
- $D_\mathfrak{a} = D_\mathcal{O}$.
- $\mathfrak{a}$ is a projective $\mathcal{O}$-module.
- There exists a rank-$[K : \mathbb{Q}]$ $\mathbb{Z}$-submodule $\mathfrak{b} \subset K$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$.

Let $I(\mathcal{O})$ denote the group of $\mathcal{O}$-ideals and let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be an $\mathcal{O}$-modulus, where $\mathfrak{m}_0 \subset \mathcal{O}$ is an ideal and $\mathfrak{m}_\infty$ is a formal product of real places of K. Let $I_\mathfrak{m}(\mathcal{O}) \subset I(\mathcal{O})$ be the the subgroup of $\mathcal{O}$-ideals prime to $\mathfrak{m}_0$. If F/K is an abelian extension ramified only at places dividing $\mathfrak{m}$, the Artin map $I_\mathfrak{m}(\mathcal{O}) \to \mathrm{Gal}(F/K)$, $\mathfrak{a} \mapsto \sigma_\mathfrak{a}$ is surjective by the Strong Approximation Theorem.

An integral ideal $\mathfrak{a} \subset \mathcal{O}$ is a $\mathcal{O}$-ideal iff $N(\mathfrak{a}) := |\mathcal{O}/\mathfrak{a}|$ is prime to $f_\mathcal{O}$. There is a 1-1 correspondence between invertible ideals $\mathfrak{a} \subset \mathcal{O}$ and ideals $\mathfrak{b} \subset \mathcal{O}_K$ prime to $f_\mathcal{O}$, given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$, $\mathfrak{b} \mapsto \mathfrak{b} \cap \mathcal{O}$. This correspondence induces an isomorphism $I_\mathfrak{m}(\mathcal{O}) \simeq I_{\mathfrak{m}f_\mathcal{O}}(K)$. The unit groups $\mathcal{O}^\times_{(\mathfrak{m}_0)}$ and $(\mathcal{O}_K)^\times_{(f\mathfrak{m}_0)}$ of the localizations away from primes dividing $f\mathfrak{m}_0$ both coincide with the S-units

$$\mathcal{O}^\times_{(f\mathfrak{m}_0)} = (\mathcal{O}_K)^\times_{(f\mathfrak{m}_0)} = \{\alpha \in K^\times : (\alpha, \mathfrak{m}_0 f) = 1\},$$

which generate the subgroups of principal ideals in $I_\mathfrak{m}(\mathcal{O})$ and $I_{f\mathfrak{m}}(K)$.

Let $P_\mathfrak{m}(\mathcal{O}) \subset (\mathcal{O}^\times_{(f\mathfrak{m}_0)})$ be the subgroup of principal ideals generated by (a) with $a \equiv^\times 1 \bmod \mathfrak{m}$ (i.e. for which a maps to the identity element of the group $(\mathcal{O}/\mathfrak{m})^\times \simeq (\mathcal{O}/\mathfrak{m}_0)^\times \times \langle -1\rangle^{|\mathfrak{m}_\infty|}$).

Let $H_\mathfrak{m}(F/K) = N_{F/K}(I_\mathfrak{m}(K))P_\mathfrak{m}(K)$. One main inequality of class field theory is the following:

Proposition 16.1. *Let F/K be Galois. Then $[I_\mathfrak{m}(F) : H_\mathfrak{m}(F/K)] \leq [F : K]$ for every $\mathfrak{m}$.*

If this inequality is saturated for some modulus $\mathfrak{m}$, then F/K is called a **class field** and the modulus $\mathfrak{m}$ is called **admissible** for F/K. Each class field has a least admissible modulus, the **conductor**, which divides each admissible modulus. For a proof see [**Jan96**] IV 5.6.

A set $S \subset \mathrm{Spec}(\mathcal{O}_K)$ of primes has **density** $\delta(S)$ if

$$\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s} = \delta \log \frac{1}{s-1} + O(1).$$

The partial zeta function is then

$$\zeta(s, S) = \prod_{\mathfrak{p} \in S} (1 - N(\mathfrak{p})^{-s})^{-1}.$$

The other main inequality of class field theory concerns abelian extensions:

Proposition 16.2. *Let F/K be abelian. Then $[I_{\mathfrak{m}}(K) : H_{\mathfrak{m}}(F/K)] \geq [F : K]$ for some $\mathfrak{m}$.*

Because abelian representations are Galois, The Artin map therefore sits in an exact sequence

$$1 \to H_{\mathfrak{m}}(F/K) \to I_{\mathfrak{m}}(F) \to \mathrm{Gal}(F/K) \to 1,$$

giving a 1-1 correspondence between generalized ideal groups $P_{\mathfrak{m}}(K) \subset H_{\mathfrak{m}} \subset I_{\mathfrak{m}}(K)$ and abelian extensions F/K with $\mathrm{Gal}(F/K) \simeq I_{\mathfrak{m}}(K)/P_{\mathfrak{m}}(K)$.

The $\mathfrak{m}$-ring class field $K^{\mathfrak{m}}$ associated to an $\mathcal{O}$-modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, is the class field associated to the ideal group

$$H = \{(\alpha) \in P_{f\mathfrak{m}\mathcal{O}_K}(K) : \alpha \equiv a \bmod {}^{\times}\mathfrak{m}\mathcal{O}_K \text{ for some } a \in \mathbb{Z} \text{ with } a \equiv 1 \bmod f\mathbb{Z}\}.$$

is the maximum abelian extension $K^{\mathfrak{m}}/K$ ramified only at primes dividing $\mathfrak{m}$, such that the kernel of the Artin map contains (in fact, equals) $P_{\mathfrak{m}}(\mathcal{O})$. The Galois group of the $\mathfrak{m}$-ring class field therefore sits in the exact sequence

$$1 \to P_{\mathfrak{m}}(\mathcal{O}) \to I_{\mathfrak{m}}(\mathcal{O}) \to \mathrm{Gal}(K^{\mathfrak{m}}/K) \to 1$$

determined by the Artin map. For the trivial modulus $\mathfrak{m} = \mathcal{O}$, one obtains the ring class field $K^{\mathcal{O}}$ and $\mathrm{Gal}(K^{\mathcal{O}}/K)$ is isomorphic to the ring class group $I(\mathcal{O})/P(\mathcal{O})$, or equivalently, the Picard group $\mathrm{Pic}(\mathcal{O})$ of projective $\mathcal{O}$-modules modulo free $\mathcal{O}$-modules. When $\mathcal{O}$ is the maximal order $\mathcal{O}_K$, the $\mathfrak{m}$-ring class field is known as the $\mathfrak{m}$-ray class field.

Restricting the Artin map to principal ideals fixes the ring class field, so the above sequence restricts to

$$1 \to P_{\mathfrak{m}}(\mathcal{O}) \to (\mathcal{O}^{\times}_{(\mathfrak{m}_0)}) \to \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}}) \to 1.$$

The homomorphism $\mathcal{O}^{\times}_{(\mathfrak{m}_0)} \to \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}})$ given by the Artin map via $x \mapsto \sigma_{(x)}$ is known to factor through $(\mathcal{O}/\mathfrak{m})^{\times}$, and the map $\mathcal{O}^{\times}_{(\mathfrak{m}_0)} \to (\mathcal{O}/\mathfrak{m})^{\times}$ is known to be surjective, so the diagram

$$\begin{tikzcd}
\mathcal{O}^{\times}_{(\mathfrak{m}_0)} \arrow[r] \arrow[dr] & (\mathcal{O}/\mathfrak{m})^{\times} \arrow[r] & \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}}) \\
& (\mathcal{O}^{\times}_{(\mathfrak{m}_0)}) \arrow[ur] &
\end{tikzcd}$$

commutes. Therefore

$$\sigma_x = \sigma_{x+\mathfrak{m}_0} \prod_{v|\mathfrak{m}_0} \sigma_x^v,$$

where if $v(x) < 0$, then σ_x^v is complex conjugation in every embedding of $K^{\mathfrak{m}}$ extending v, otherwise σ_x^v is trivial. The kernel of the map $(\mathcal{O}/\mathfrak{m})^{\times} \to \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}})$ is $\mathcal{O}^{\times} + \mathfrak{m}$, giving the isomorphism

$$(\mathcal{O}/\mathfrak{m})^{\times}/(\mathcal{O}^{\times} + \mathfrak{m}) \simeq \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}}).$$

Let $\mathcal{O}^{\times,\mathfrak{m}_\infty}_{(\mathfrak{m}_0)} \subset \mathcal{O}^{\times}_{(\mathfrak{m}_0)}$ be the subgroup that is positive at every place dividing $\mathfrak{m}_\infty$. Then

$$1 \to P_{\mathfrak{m}}(\mathcal{O}) \to (\mathcal{O}^{\times,\mathfrak{m}_\infty}_{(\mathfrak{m}_0)}) \to \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}\infty}) \to 1$$

is exact. Since $\mathcal{O}^{\times,\mathfrak{m}_\infty}_{(\mathfrak{m}_0)}$ is the kernel of reduction mod $\mathfrak{m}_\infty$, we obtain an isomorphism $(\mathcal{O}/\mathfrak{m}_0)^{\times} \simeq \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}\mathfrak{m}_\infty})$.

16.5 Class fields of real quadratic fields

Let K be a real quadratic field. For a rank-2 $\mathbb{Z}$-sublattice $L \subset K$, let D_L be its discriminant. Each quadratic order $\mathcal{O}$ is uniquly determined by its discriminant $D_{\mathcal{O}} = f_{\mathcal{O}}^2 D_0$, where $f_{\mathcal{O}}$ is the conductor of $\mathcal{O}$ and the corresponding fundamental discriminant $D_0 = D_{\mathcal{O}_K}$ is the discriminant of the maximal order $\mathcal{O}_K \subset K = \mathbb{Q}(\sqrt{D_{\mathcal{O}}}) = \mathbb{Q}(\sqrt{D_0})$, in which case

$$\mathcal{O} = \mathbb{Z}\left[\frac{D_{\mathcal{O}} + \sqrt{D_{\mathcal{O}}}}{2}\right] = \mathbb{Z} + f_{\mathcal{O}}\mathcal{O}_K.$$

Let $\varepsilon^{\pm}$ be the real embeddings of K, under which $\varepsilon^{\pm}(\sqrt{D_0}) = \pm\sqrt{D_0}$. For each $a \in K^{\times}$, let $\sigma_a^{\pm}$ be complex conjugation in the embeddings of $K^{\mathfrak{m}}$ extending $\varepsilon^{\pm}$ with $\varepsilon^{\pm}(a) < 0$, and let it be trivial otherwise. The homomorphism $a \mapsto \sigma_{(a)}$ from $\mathcal{O}^{\times}_{(f\mathfrak{m}_0)}$ to $\mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}})$ factors through $(\mathcal{O}/\mathfrak{m})^{\times}$, hence $\sigma_{(a)} = \sigma_{a+\mathfrak{m}_0}\sigma_a^{+}\sigma_a^{-}$. This gives another exact sequence

$$\mathcal{O}^{\times} \to (\mathcal{O}/\mathfrak{m})^{\times} \to \mathrm{Gal}(K^{\mathfrak{m}}/K) \to \mathrm{Gal}(K^{\mathcal{O}}/K) \to 1.$$

Furthermore, we may define the following homomorphism $\mathcal{O}^{\times}_{(\mathfrak{m}_0 f)} \to \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}\infty})$, which factors through $(\mathcal{O}/\mathfrak{m}_0)^{\times}$:

$$a \mapsto \sigma_a := \sigma_{a+\mathfrak{m}_0} = \sigma_{(a)}\sigma_a^{+}\sigma_a^{-}.$$

where $a + \mathfrak{m} \in (\mathcal{O}/\mathfrak{m})^{\times}$ maps to Therefore, there are isomorphisms

$$(\mathcal{O}^{\times}_{(f\mathfrak{m}_0)})/P_{\mathfrak{m}}(\mathcal{O}) \simeq (\mathcal{O}/\mathfrak{m})^{\times}/(\mathcal{O}^{\times} + \mathfrak{m}) \simeq \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}}).$$

In particular, if a is totally positive, then $\sigma_{\pm a} = \sigma_{a\mathcal{O}} \in \mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathcal{O}\infty})$.

and $P_{\mathfrak{m}}(\mathcal{O}) \simeq P_{\mathfrak{m}f_{\mathcal{O}}}(K)$. In particular, $K^{\mathfrak{m}}$ is a subfield of the $\mathfrak{m}f_{\mathcal{O}}\mathcal{O}_K$-ray class field.

When $f_{\mathcal{O}}$ is prime to $\mathfrak{m}$, the $\mathfrak{m}$-ring class field $K^{\mathfrak{m}}$ is the compositum $K^{\mathcal{O}}K^{\mathfrak{m}\cap\mathcal{O}_K}$ of the ring class field $K^{\mathcal{O}}$ with the ray class field $K^{\mathfrak{m}\cap\mathcal{O}_K}$. Otherwise, this will not be the case, the first examples being $d = 12, 21$ and 30, where $D = 3^2 D_0$ and thus the ring class field $K^{\mathcal{O}}$ is contained in the ray class field, but $[K^{\mathcal{O}d'\infty} : K^{\mathcal{O}_K d'\infty}] = 3$ [AYZ, ACFW]. Computations suggest that $\gcd(f, d')$ is always either 1 or 3, so probably the compositum works in those other cases. Maybe work it out for $d = 21$ since at least that's odd? Anyway, this is better suited for the next section where we take $D_{\max} = (d-3)(d+1)$. Plus, I think I proved something along these lines while showing that the extensions always split.

The class number $h_{\mathcal{O}} = |\mathrm{Pic}(\mathcal{O})|$ is (known/conjectured?) to satisfy $h_{\mathcal{O}} = O(\sqrt{D}) = O(d)$ (the conjectured bound is $(e^{2\gamma} + o(1))\sqrt{D}\frac{\log\log D}{\log D}$); can it fit into C in the largest cases?

The Galois group $\mathrm{Gal}(K^{\mathfrak{m}}/K)$ of the class field $K^{\mathfrak{m}}$ sits in several exact sequences:

Let $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}}$ denotes the Artin map $I_d(\mathcal{O}) \to \mathrm{Gal}(F_{\mathcal{O}}/K^{\mathcal{O}})$. Then the homomorphism

$$a \mapsto \sigma_a := \sigma_{(a)}\sigma_a^{+}\sigma_a^{-} \in \mathrm{Gal}(F_{\mathcal{O}}/K^{\mathcal{O}\infty}),$$

factors through $(\mathcal{O}/\mathfrak{m})^{\times}$.

For each G-orbit in that Clifford orbit, there is a homomorphism $\mathcal{O}^{\times}_{(d)} \to \mathrm{Aut}_{\mathbb{C}}(\widetilde{G})$ taking $a \mapsto [U_a]$ such that $[U_a v] = [v^{\sigma_a}]$.

In particular, $\mathbb{Q}(\zeta_{d'})$ is the ray class field $\mathbb{Q}^{(d')\infty}$ of $\mathbb{Q}$ with conductor $(d')\infty$.

The coordinates of these points apparently generate the relevant class fields and appear to give instances of Stark's conjectural units, placing the analytic approach to Hilbert's 12th problem for real quadratics under new light.

16.6 Quadratic fields

Let $D > 0$ be a squarefree integer and let

$$D_f = \begin{cases} D & \text{if } D \equiv 1 \bmod 4 \\ 4D & \text{if } D \equiv 2,3 \bmod 4. \end{cases}$$

Then $D_f \equiv 0, 1 \bmod 4$ is a fundamental discriminant, equal to the discriminant of K (= the signed discriminant of the maximal order $\mathfrak{o}$ of the real quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Let h be the class number of K and let h^+ be the narrow class number. Let u_f be the fundamental unit of $\mathfrak{o}$ and let u_D generate the totally positive units. Then $\mathfrak{o}^+ = U_{\infty_+}(K) = \langle u_f \rangle$ is the positive units and $\mathfrak{o}^{++} = U_\infty(K) = \langle u_D \rangle$ the totally positive units. Let $\iota\colon \mathfrak{o} \to \mathfrak{o}/d'$ be the map $\iota(a) = a + (d') = a \bmod (d')$.

For a subset $R \subset K$, let $U_\mathfrak{m}(R) = \{x \in R^\times : x \equiv 1 \bmod \mathfrak{m}\}$. Then $P^1_\mathfrak{m}(K) = U_\mathfrak{m}(K)/U_\mathfrak{m}(\mathfrak{o})$. When D is the squarefree part of $(d-3)(d+1)$, AFMY showed that $d = 1 + u_D^r + u_D^{-r}$ for some integer $r \geq 1$ and $\operatorname{ord}(\iota(u_D)) = 3rd'/d$, while $U_{d'\infty_+}(\mathfrak{o}) = U_{d'\infty}(\mathfrak{o})$, so that

$$P^1_{d'\infty}(K) = U_{d'}(K)/U_{d'\infty}(\mathfrak{o}) = U_{d'}(K)/U_{d'\infty_+}(\mathfrak{o}) = P^1_{d'\infty_+}(K)$$

This was used to guarantee that the fields $K^{(d')\infty}$, $K^{(d')\infty_+}$, $K^{(d')\infty_-}$ and $K^{(d')}$ are all distinct, with maximal CM subfield $K^{(d')\infty_+} \cap K^{(d')\infty_-}$.

Given ideals $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{(\mathfrak{a})_\mathfrak{p}}$, $\mathfrak{b} = \prod_\mathfrak{p} \mathfrak{p}^{(\mathfrak{b})_\mathfrak{p}} \subset \mathfrak{o}$, recall that

$$\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{b}) = \prod_\mathfrak{p} \mathfrak{p}^{\min((\mathfrak{a})_\mathfrak{p}, (\mathfrak{b})_\mathfrak{p})},$$

$$\mathfrak{a} \cap \mathfrak{b} = \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod_\mathfrak{p} \mathfrak{p}^{\max((\mathfrak{a})_\mathfrak{p}, (\mathfrak{b})_\mathfrak{p})}$$

Then

$$\mathfrak{a}\mathfrak{b} = \prod_\mathfrak{p} \mathfrak{p}^{(\mathfrak{a})_\mathfrak{p} + (\mathfrak{b})_\mathfrak{p}} = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b})$$

and in particular, $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ iff $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime (i.e. $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$). For a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ in K, the ideal groups

$$\begin{aligned} P_\mathfrak{m}(K) &= \{(a) := a\mathfrak{o} : ((a), \mathfrak{m}_0) = (1)\} \\ P^+_\mathfrak{m}(K) &= \{(a) \in P_\mathfrak{m}(K) : v(a) > 0 \text{ for every } v \mid \mathfrak{m}_\infty\} \\ P^1_\mathfrak{m}(K) &= \{(a) \in P_\mathfrak{m}(K) : a \equiv 1 \bmod^\times \mathfrak{m}\} \end{aligned}$$

satisfy

$$P^1_\mathfrak{m} \subset P^+_\mathfrak{m} \subset P_\mathfrak{m} = P_{\mathfrak{m}_0}$$

There is an exact sequence

$$1 \to P^1_{d'\infty} \to P_{d'} \to \mathrm{Gal}(K^{(d')\infty}/K) \to \mathrm{Gal}(K^{(1)}/K) \to 1$$

and the image of the Artin map (the middle map) is

$$\begin{aligned}\mathrm{Gal}(K^{(d')\infty}/K^{(1)}) &\simeq P_{d'}(K)/P^1_{d'\infty}(K)\\ &\simeq (\mathcal{O}_K/(d')\infty)^\times/\,\mathrm{im}(\mathcal{O}_K^\times)\\ &\simeq ((\mathcal{O}_K/d')^\times \times \langle -1\rangle^2)/\langle(\iota(-1),-1,-1),(\iota(u_f),1,\mathrm{N}(u_f))\rangle\end{aligned}$$

We distinguish the cases $\mathrm{N}(u_f) = \pm 1$. In the first case, we have

$$\mathrm{N}(u_f) = 1, u_D = u_f, h^+ = 2h, K^\infty \neq K^{\infty_+} = K^{(1)}, \mathcal{O}_K^\times = \langle -1, u_D\rangle,$$

which gives

$$\mathrm{Gal}(K^{(d')\infty}/K^{(1)}) \simeq ((\mathcal{O}_K/d')^\times \times \langle -1\rangle^2)/\langle(\iota(-1),-1,-1),(\iota(u_f),1,1)\rangle$$

while in the second case, we have

$$\mathrm{N}(u_f) = -1, u_D = u_f^2, h^+ = h, K^\infty = K^{\infty_+} = K^{(1)}, \mathcal{O}_K^\times = \langle -1, u_f\rangle$$

which gives

$$\mathrm{Gal}(K^{(d')\infty}/K^{(1)}) \simeq ((\mathcal{O}_K/d')^\times \times \langle -1\rangle^2)/\langle(\iota(-1),-1,-1),(\iota(u_D),1,-1)\rangle.$$

And yet in both cases, the Artin map gives a surjection $P^+_{d'\infty}(K) \to \mathrm{Gal}(K^{(d')\infty}/K^\infty)$.

If $a \in \mathcal{O}_K$ with $((a),(d')) = 1$, let $\sigma_{|a|} := \left(\frac{K^{(d')\infty}/K}{(a)}\right) \in \mathrm{Gal}(K^{(d')\infty}/K^{(1)})$ be the image of (a) under the Artin map on the associated principal ideal and let σ_{-1} be complex conjugation. By multiplicativity, this defines σ_a for all $a \in K^\times$ with $((a),(d')) = 1$. Then $\mathrm{Gal}(K^{(d')\infty}/K^\infty)$ is generated by the σ_a such that $a \gg 0$. Or should σ_{-1} be both complex conjugations since it changes the sign under both embeddings?

$$\begin{aligned}\mathrm{Gal}(K^{(d')\infty}/K^\infty) &\simeq P_{(d')\infty}(K)/P_{1,(d')\infty}(K)\\ &\simeq (\mathcal{O}_K/(d')\infty)/\,\mathrm{im}(\mathcal{O}_K^{++})\\ &\simeq ((\mathcal{O}_K/d')^\times \times \langle -1\rangle^2)/\langle(\iota(-1),-1,1),(\iota(u_D),1,1)\rangle\end{aligned}$$

$$\begin{aligned}\mathrm{Gal}(K^{(d')\infty_1}/K^{(1)}) &\simeq (\mathcal{O}_K/(d')\infty_1)/\,\mathrm{im}(\mathcal{O}_K^\times)\\ &\simeq ((\mathcal{O}_K/d')^\times \times \langle -1\rangle)/\langle(\iota(-1),-1),(\iota(u_f),1)\rangle\end{aligned}$$

16.7 Ray classes

Let $\mathfrak{m}$ be an ideal. Let $I_{\mathfrak{m}}$ be the fractional invertible ideals prime to $\mathfrak{m}$ and let $P_{\mathfrak{m}\infty,1} \subset I_{\mathfrak{m}}$ be the subgroup of principal fractional ideals (α) generated by totally positive $\alpha \in \mathcal{O}_K$ with $\alpha \equiv 1 \bmod \mathfrak{m}$. Each Hecke character χ mod $\mathfrak{m}$ determines a character on the group $G = I_{\mathfrak{m}}/P_{\mathfrak{m}\infty,1}$ of narrow ray classes modulo $\mathfrak{m}$, and vice-versa. A Dirichlet character mod $\mathfrak{m}$, on the other hand, is a multiplicative character on $\mathcal{O}_K$ factoring through $\mathcal{O}_K/\mathfrak{m}$. When the narrow class group is trivial, then it seems these Hecke characters are Dirichlet characters, but otherwise it seems that because principal ideals map into the ideal group $P_{\mathfrak{m}} \to I_{\mathfrak{m}}$, the the group of Hecke characters should be an extension of the group of Dirichlet characters by the narrow Hilbert characters

$$1 \to \widehat{\mathrm{CL}_{\mathfrak{m}}} \to \widehat{I_{\mathfrak{m}}/P_{\mathfrak{m},1}} \to \widehat{P_{\mathfrak{m}}/P_{\mathfrak{m},1}} \to 1.$$

Let $\mathfrak{f}_\chi$ be the conductor of χ and $\mathfrak{f}_{\chi,0}$ its finite part. The ray class field $F = K^{\mathfrak{m}\infty}$ is a compositum over $\chi \in \hat{G}$ of cyclic extensions $F^{\ker(\chi)} \simeq K^{\mathfrak{f}_\chi}$, for which $\mathrm{Gal}(K^{\mathfrak{f}_\chi}/K) \simeq \chi(G)$, the discriminant is the product of the $\mathfrak{f}_{\chi,0}$ and the conductor $\mathfrak{f}$ is the least common multiple of the $\mathfrak{f}$. The Artin map provides an isomorphism $G \to \mathrm{Gal}(F/K)$ and defines the Artin symbol $\left(\frac{F/K}{\mathfrak{a}}\right)_{\mathfrak{p}}$ at finite primes $\mathfrak{p}$. The Artin symbol is defined at ramified places v, and thus on the idele group, by invariants of cyclic central simple algebras over the localizations K_v.

For example, there are four Dirichlet characters mod $(5) = 5\mathbb{Z}$, generated by $\chi_0(n) = 0, 1, i, -i, -1$ (for e.g. $n = 0, \ldots, 4$). There are eight characters mod $(5)\infty$, consisting of χ_0^i and $\chi_0^i \operatorname{sgn}$ for $i = 0, \ldots, 3$. The Hecke characters mod $(5)\infty$ are the even Dirichlet characters $(\chi_0 \operatorname{sgn})^i$, $i = 0, \ldots, 3$, which are trivial on the units ± 1. The corresponding conductors are $\mathcal{O}_K$, $(5)\infty$, (5) and $(5)\infty$. So the discriminant of $\mathbb{Q}(\zeta_5)$ is (5^3), and the global conductor $(5)\infty$ is the GCD of the conductors of the characters as expected. The real subfield similarly has discriminant and conductor (5). For general p, the Hecke characters mod (p) consist of the trivial one (trivial conductor), along with

I suppose we expect that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has discriminant (p^{p-2}) (since there are $p-1$ characters with conductor divisible by p) and $\mathbb{Q}(\zeta_p + \zeta_p^{-1})/\mathbb{Q}$ has discriminant $(p^{\frac{p-3}{2}})$ (since there are $\frac{p-3}{2}$ even characters with conductor p).

Let $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$. The class number is 1 and the narrow class number is 2, with narrow class field $K^\infty = K(\sqrt{-1}) = \mathbb{Q}(\zeta_{12})$. As the fundamental unit $u_+ = 2 + \sqrt{3}$ is totally positive, u_+ has order 3 and $\mathcal{O}^\times = \langle u_+, -1 \rangle$ has order 6 mod $(5)\mathfrak{m}_\infty$, for every $\mathfrak{m}_\infty \in \{\infty_1, \infty_2\}$. The $24/6 = 4$ Hecke characters mod (5) are characters of $\mathrm{Gal}(K^{(5)}/K)$: one is trivial and three are primitive. The $48/6 = 8$ Hecke characters mod $(5)\infty_{1/2}$ are characters of $\mathrm{Gal}(K^{(5)\infty_{1/2}}/K)$ and include four primitive characters together with the three of conductor (5) and the trivial character. The $96/6 = 16$ Hecke characters mod $(5)\infty$ are characters of the full Galois group $\mathrm{Gal}(K^{(5)\infty}/K)$. These include the trivial character, the three of conductor (5), 4 of conductor $(5)\infty_1$, 4 of conductor $(5)\infty_2$, 1 of conductor ∞ and 3 of conductor $(5)\infty$.

The class fields and some of their subfields are related as follows, with each line representing a quadratic extension:

$$\begin{tikzcd}
 & K^{(5)\infty} & \\
K^{(5)\infty_1} \arrow[ur] & K^{(5)\infty_2} \arrow[u] & K^{\infty}(\zeta_5) \arrow[ul] \\
 & K^{(5)} \arrow[ul] \arrow[u] \arrow[ur] & \\
 & K(\sqrt{5}) \arrow[u] & K^{\infty} \arrow[uu] \\
 & K. \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Note that $K^{\infty}(\zeta_5) = \mathbb{Q}(\zeta_{60})$ is the max CM field and $K^{(5)} = \mathbb{Q}(\zeta_{60} + \zeta_{60}^{-1})$ the totally real subfield. The discriminants of the class fields are $\mathrm{disc}(K^{(5)\infty}/K) = (5)^{14}$, $\mathrm{disc}(K^{(5)\infty_{1/2}}) = (5)^7$ and $\mathrm{disc}(K^{(5)}) = (5)^3$. For $E = K^{(5)}, K^{(5)\infty_i}, K^{(5)\infty}$, the prime factorization of $d\mathcal{O}_E$ is $\mathfrak{p}^4$, $\mathfrak{q}_i^8$ and $\mathfrak{r}_1^8\mathfrak{r}_2^8$, with $\mathfrak{p}\mathcal{O}_{K^{(5)\infty_i}} = \mathfrak{q}_i^2$ and $\mathfrak{q}_i\mathcal{O}_{K^{(5)\infty}} = \mathfrak{r}_i^2$. In particular, (5) is totally nonsplit in each $K^{(5)\infty_i}$ and its subfields.

17 References

[1] S. L. Sobolev. “Cubature formulas on the sphere invariant under finite groups of rotations”. In: *Doklady Akademii Nauk SSSR* (1962).

[2] Gerhard Zauner. “Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie”. PhD thesis. Universität Wien, 1999.

[3] Marcus Appleby et al. “Generating ray class fields of real quadratic fields via complex equiangular lines”. In: *Acta Arithmetica* 192 (2020), pp. 211–233.

[4] Akira Ikeda and Yoshiharu Taniguchi. “Spectra and eigenforms of the Laplacian on S^n and $\mathbb{P}^n(\mathbb{C})$”. In: *Osaka Journal of Mathematics* (1978).

[5] Daniel Bump. *Automorphic Forms and Representations*. Cambridge Studies in Advanced Mathematics. Cambridge: Cambridge University Press, 1997.