Title: Explicit class field theory from quantum measurements

Date: Oct 16, 2017 02:00 PM

URL: http://pirsa.org/17100080

Abstract: <p>It is easy to prove that d-dimensional complex Hilbert space can contain at most d^2 equiangular lines. But despite considerable evidence and effort, sets of this size have only been proved to exist for finitely many d. Such sets are relevant in quantum information theory, where they define optimal quantum measurements known as SIC-POVMs (Symmetric Informationally Complete Positive Operator-Valued Measures). They also correspond to complex projective 2-designs of the minimum possible cardinality.   Numerical evidence points to their existence for all d as orbits of finite Heisenberg groups, the current record being d=844 [Scott-Grassl '17]. However, to date, they are only proven to exist for finitely many d (the current record being d=323 [SG17]) via computer-assisted calculations in number fields of degree increasing with d. In this talk, I will discuss the structure of these number fields, which turn out to be specific abelian extensions of specific real quadratic number fields [Appleby, Flammia, McConnell, Y. 1604.06098]. Such fields are known to exist by general theorems of class field theory, but until now, had never been found 'explicitly' in Nature. This contrasts the classical situation for abelian extensions of CM fields, which are generated by the torsion points of abelian varieties with complex multiplication.   All known Heisenberg-covariant SIC-POVMs have unitary symmetries under the associated Weil representation that are intimately related to the structure of the underlying number fields. A proper understanding of this relationship may ultimately lead to a general proof of their existence in all dimensions, rather than the finite number of examples currently proved to exist. </p>

$v_1, v_2, \dots, v_n \in \mathbb{C}^d$ or $\mathbb{R}^d$

$$|\langle v_i, v_j\rangle|^2 = \begin{cases} 1 & i=j \\ \alpha & i\neq j \end{cases}$$

n?

$\mathbb{R}$, $n \le \frac{d^2+d}{2}$

$\mathbb{C}$ $n \le d^2$

$P_i = v_i v_i^\dagger$

$\det(\mathrm{Tr}\, P_i P_j) =$

$\mathbb{R}^d$

$P_i = v_i v_i^\dagger \in \mathrm{Herm}_d$

$\in \mathrm{Sym}_d$ for $\mathbb{R}$

$0 \leq \alpha \leq 1$

$\det(\mathrm{Tr}\, P_i P_j) = (1-\alpha)^{n-1}(1+(n-1)\alpha) \geq 0$

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

$\Longrightarrow n \leq \dim_{\mathbb{R}}(\mathrm{Herm}_d \text{ or } \mathrm{Sym}_d)$

for $\mathbb{R}$, $n = \frac{d^2+d}{2}$ only possible when

$d = 3$ or $m^2 - 2$

$d = 2$

$0 \le \alpha < 1$

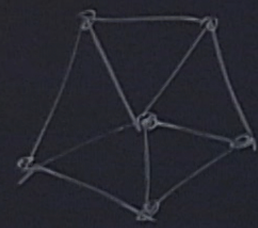
...or $\mathbb{R}$

$(\ldots)^{n-1}\,(1+(n-1)\alpha) \geq 0$

$n \le \dim_{\mathbb{R}}(\mathrm{Herm}_d \text{ or } \mathrm{Sym}_d)$

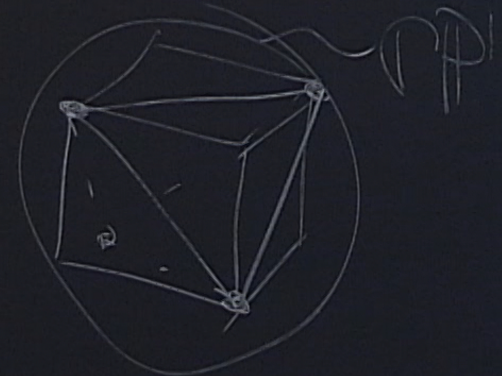
...possible when

$d=3$



For $\mathbb{C}$, $n=d^2$ is "always" achievable $\Rightarrow \left(\alpha = \frac{1}{d+1}\right)$

e.g. $d=2$



$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$= \frac{1}{d+1})$$

$$P_0 = \frac{1}{2}\left(I + \frac{1}{\sqrt{3}}(X+Y+Z)\right)$$

$$P_1 = X P_0 X,$$

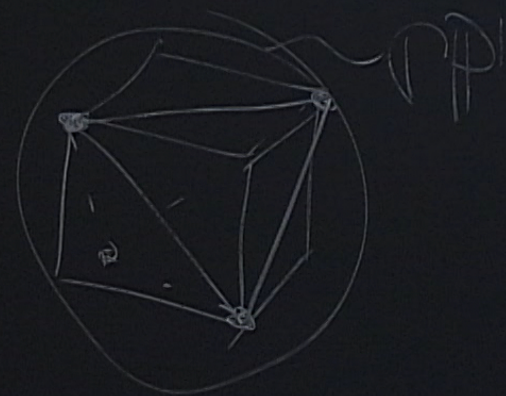
$$P_2 = Y P_0 Y$$

$$P_3 = Z P_0 Z$$

rm_d or Sym_d)

For $\mathbb{C}$, $n = d^2$ is "always" achievable $\Rightarrow$ $\left(\alpha = \frac{1}{d+1}\right)$

e.g. $d = 2$



$(\mathbb{Z}/2)^2 \rtimes SL_2(2)$

$P_1 = X P_0$

$P_2 = Y P_0$

$P_3 = Z P_0 Z$

$\mathbb{Z}/2 \times \mathbb{Z}/2$

$X_d \begin{pmatrix} & 1 \\ 1 & 0 \end{pmatrix}, \quad Z_d \begin{pmatrix} 1 & & \\ & e^{\frac{2\pi i}{d}} & \\ & & \ddots \\ & & & \zeta_d^{d-1} \end{pmatrix}$

$+ \frac{1}{\sqrt{3}}(X+Y+Z))$

$X,$

Y

$$V_0, \rightsquigarrow X_d^{j_1} Z_d^{j_2} v_0 = v_j$$

$$1 \to U(1) \to \langle U(1), X_d, Z_d \rangle \to (\mathbb{Z}/d)^2 \to 0$$

explicit $d = 2-16, 19, 24, 35, 48$ (SG '09)
over number fields
in Magma

$V_0, \rightsquigarrow X_d^{j_1} Z_d^{j_2} V_0 = V_j$

$$1 \to U(1) \to \langle U(1), X_d, Z_d \rangle \to (\mathbb{Z}/d)^2 \to 0$$

explicit $d = 2-16, 19, 24, 35, 48$ (SG '09)
over number fields
in Magma

numerical up to 67, $\xrightarrow{\text{all}}$ 121 (GS '17) 844

explicit for $d = \underline{4, 8, 19, 48}, 121, 323$;

$$\sum_k z_k \bar{z}_{k+i} \bar{z}_{k+j} z_{k+i+j} - \frac{\delta_i + \delta_j}{d+1} \|z\|_2^4, \quad d^2 \text{ eqns } i,j=0,\dots,d-1$$

$$\bar{z}_k = z_k^*$$

$$\Delta_j = \zeta_{2d}^{-j_1 j_2} X_d^{j_1} Z_d^{j_2}$$

$$\frac{1}{d^2}\sum_{j\in(\mathbb{Z}/d)^2} \left(\Delta_j P \Delta_j^\dagger\right)^{\otimes 2} = \frac{2}{d^2+d} P_{sym}$$

$\{P_1, \dots, P_n\}$ s.t. $\frac{1}{n}\sum P_i \otimes P_i =$

is a $\mathbb{CP}$ 2-design

$(X+Y+Z))$

$e^{\frac{2\pi i}{d}}$

$$V_0, \rightsquigarrow X_d^{j_1} Z_d^{j_2} V_0 = V_j$$

$$H_d = U(d)$$

$$1 \to U(1) \to \langle U(1), X_d, Z_d \rangle \to (\mathbb{Z}/d)^2 \to 0$$

explicit $d = 2-16, 19, 24, 35, 48$ (SG '09)
over number fields
in Magma

numerical up to 67, $\xrightarrow{\text{all}}$ 121 (GS '17) 844

explicit for $d = \underline{4, 8, 19, 48}, 121, 323,$

ζ_d^{d-1}

$e^{\frac{2\pi i}{d}}$

$\{$automorphisms fixing center$\}$

$\rightarrow$ P_0, rep. of $SL_2(d)$

"Weil representation"

"generalized Clifford group"

$Sp_2(\mathbb{F}_2^n)$

$V_0 = V_j$

$H_d = U(d)$

$\cup$

$\langle U(1), X_d, Z_d \rangle \to (\mathbb{Z}/d)^2 \to 0$

, 24, 35, 48 (SG '09)

up to 67, $\xrightarrow{911}$ 121 (GS '17) 844

$\{P_1, \ldots, P_n\}$

is a $\mathbb{CP}$ 2-de

d^2 eqns $i, j = 0, \ldots, d-1$

$$\|A\|_2^2 = \mathrm{Tr}(A^2)$$

Assume d odd.

Then $g \in SL_2(d)$ acts via

$$g \circ \Delta_j = \Delta_{gj} = U_g \Delta_j U_g^\dagger$$

$$(S\,T)^2$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$1 \to \Gamma(d) \to SL_2(\mathbb{Z}) \to SL_2(d) \to 1$$

number a is algebraic if

$$f(a)=0, \text{ for } f \in \mathbb{Q}[x].$$

number field F is generated by some roots of an irreducible polynomial

$$F = \mathbb{Q}(\sqrt{m})/\mathbb{Q} \hookrightarrow \mathbb{C}/\mathbb{R}$$

$\mathbb{Q}(\sqrt{d})$

F/K, gen by roots of $f \in K[x]$

$$P_i = V_i V_i^{+}$$

$$\det(\mathrm{Tr}\, P_i P_j) =$$

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

for $\mathbb{R}$, $n = d^2$

$d = 3$ or

$\mathbb{Q}(\sqrt{m})/\mathbb{Q} \hookrightarrow \mathbb{C}/\mathbb{R}$

$\to \mathbb{Q}(\zeta_d)$

F/K, gen by roots of $f \in K[x]$

Galois (or normal) if gen. by <u>all</u> the roots of f

if

$\mathbb{Q}[x]$.

by some

nomial

$\mathbb{C}/\mathbb{R}$

$\in K[x]$

$$\longrightarrow \mathrm{Gal}(F/\mathbb{Q}) \simeq A \rtimes \mathbb{Z}/2.$$

$$\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \simeq (\mathbb{Z}/d)^\times$$

$$\underset{(\mathbb{Z}/d)^\times}{\overset{}{a}} \mapsto (\zeta_d \mapsto \zeta_d^a)$$

$$a \mapsto (\zeta_d \mapsto \zeta_d^a)$$

$a \in (\mathbb{Z}/d)^\times$

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

$K = \mathbb{Q}(\sqrt{m}) \subset F$.

algebraic <u>integer</u> root of monic poly. $f \in \mathbb{Z}[x]$

$$x^n + a_{n-1}x^{n-1} + \dots + a_0$$

$(\mathbb{Z}/2)^2$

$\mathbb{R}^2$

$a \mapsto (\zeta_d \mapsto \zeta_d^a)$

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

omial

$\mathbb{C}/\mathbb{R}$

$K[x]$

all the roots on

$$1 \to Gal(F/K) \to Gal(F/\mathbb{Q}) \to Gal(K/\mathbb{Q}) \to 1$$

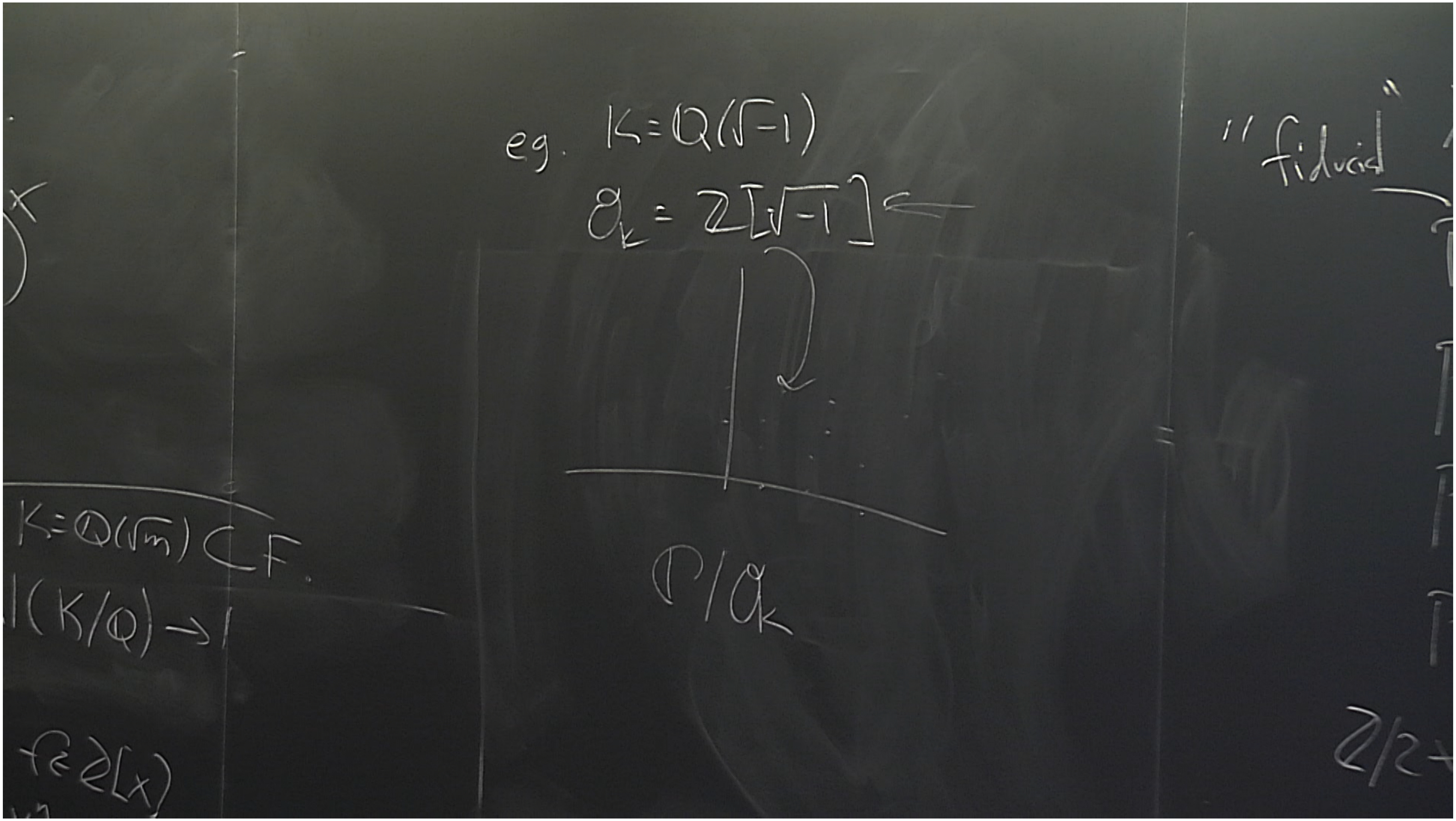
$K = \mathbb{Q}(\sqrt{m}) \subset F.$

algebraic integer root of monic poly. $f \in \mathbb{Z}[x]$

$x^n + a_{n-1}x^{n-1} + \dots + a_0$

$\mathcal{O}_K \subset K$

$\mathbb{Z}_K$



e.g. $K=\mathbb{Q}(\sqrt{-1})$
$\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$
$\mathbb{C}/\mathcal{O}_K$
$K=\mathbb{Q}(\sqrt{m}) \subset F.$
$(K/\mathbb{Q}) \to 1$
$f \in \mathbb{Z}[x]$
"fiducial"
$\mathbb{Z}/2$

$\mathbb{Q}[x]$.

ed by some

polynomial

$\mathbb{C}/\mathbb{R}$

$f \in K[x]$

$\longrightarrow \mathrm{Gal}(F/\mathbb{Q}) \simeq A \times \mathbb{Z}/2$.

$\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \simeq (\mathbb{Z}/d)^\times$

$a \mapsto (\zeta_d \mapsto \zeta_d^a)$

$a \in (\mathbb{Z}/d)^\times$

abelian $\Rightarrow$ ab. ext

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

$K = \mathbb{Q}(\sqrt{m}) \subset F$.

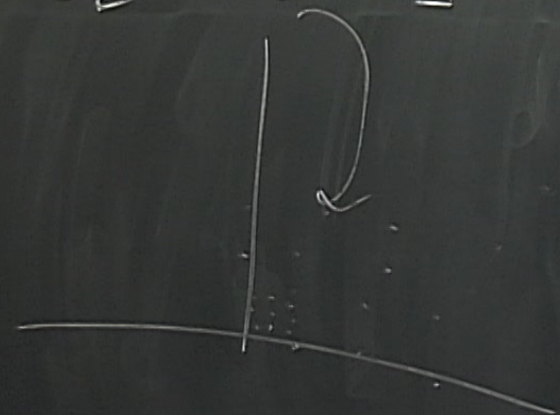
algebraic <u>integer</u> root of monic poly $f \in \mathbb{Z}[x]$

$\mathcal{O}_K \subset K$

$x^n + a\, x^{n-1}$

e.g. $K = \mathbb{Q}(\sqrt{-1})$

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$



$\mathbb{C}/\mathcal{O}_K$

$\Lambda / \frac{1}{4}\Lambda \cong (\mathbb{Z}/4)^n$

$) \subset F.$

"fiducial" $X = (\dots$

$P_0 = \frac{1}{2} \dots$

$P_1 = X$

$P_2 = Y$

$P_3 = Z \dots$

$\mathbb{Z}/2 \times \mathbb{Z}/2$

AAZ: Conj: $K = \mathbb{Q}(\sqrt{(d-3)(d+1)})$

F/K

$\uparrow$

ray class field over K with conductor

$(d')\infty$, $d' = \begin{cases} d & d \text{ odd} \\ 2d & d \text{ even} \end{cases}$

$X_d = \begin{pmatrix} 0 & & 1 \\ 1 & \ddots & \\ & 1 & 0 \end{pmatrix}$, Z

$e^{\frac{2\pi i}{d}}$

$V_0, \rightsquigarrow X_d^{j_1} Z_d^{j_2} V_0 =$

$H_d = U$

$1 \to U(1) \to \langle U(1),$

explicit $d = 2-16, 19, 24,$

over number fields

in Magma

numerical up to 67

explicit for $d = 4$

$\sqrt{(d-3)(d+1)}\Big)$

$\mathcal{O}_K \subset K$,

$I \subset \mathcal{O}_K$, factors uniquely in prime ideals

$I = \mathfrak{p}_1 \mathfrak{p}_2 \ \mathfrak{p}_m$

prime ideals

$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

h conductor

odd

even

morphisms fix

P_{0}, ... of

"Weil rep

$\to 0$ "gener

$0\,9)$

844

ctor

$I \subset \mathcal{O}_K$, factors uniquely in prime ideals

$$I = \mathfrak{p}_1 \mathfrak{p}_2 \; \mathfrak{p}_m$$

prime ideals

$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

$\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_q$, F/K, Galois

$\mathcal{O}_F \mathfrak{p} = (\mathfrak{q}_1 \cdots \mathfrak{q}_n)^{e}$ — ramific index

...morphisms fixing center

P_0, aut. of $SL_2(d)$

"Weil representation"

"generalized Clifford group"

$Sp_{2n}(\mathbb{F}_2^n)$

$\rightarrow 0$

844

3,

prime ideals

$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

$\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_q$, F/K Galois

$\mathcal{O}_F \mathfrak{p} = (\mathfrak{q}_1 \cdots \mathfrak{q}_g)^e$ — ramific index

$[F:K] = n = efg$.

$(\mathcal{O}_F/\mathfrak{q}_i \simeq \mathbb{F}_{q^f})/\mathbb{F}_q$

$\to \mathcal{O}$

"generalized Clifford group"

$Sp_{2}(\mathbb{F}_2^n)$

$\mathcal{O}\,q)$

844

3,

me ideals

Modulus in K:

$$\left(\prod \text{ideal of } K\right) \times \{\text{embeddings } K \hookrightarrow \mathbb{R}\}$$

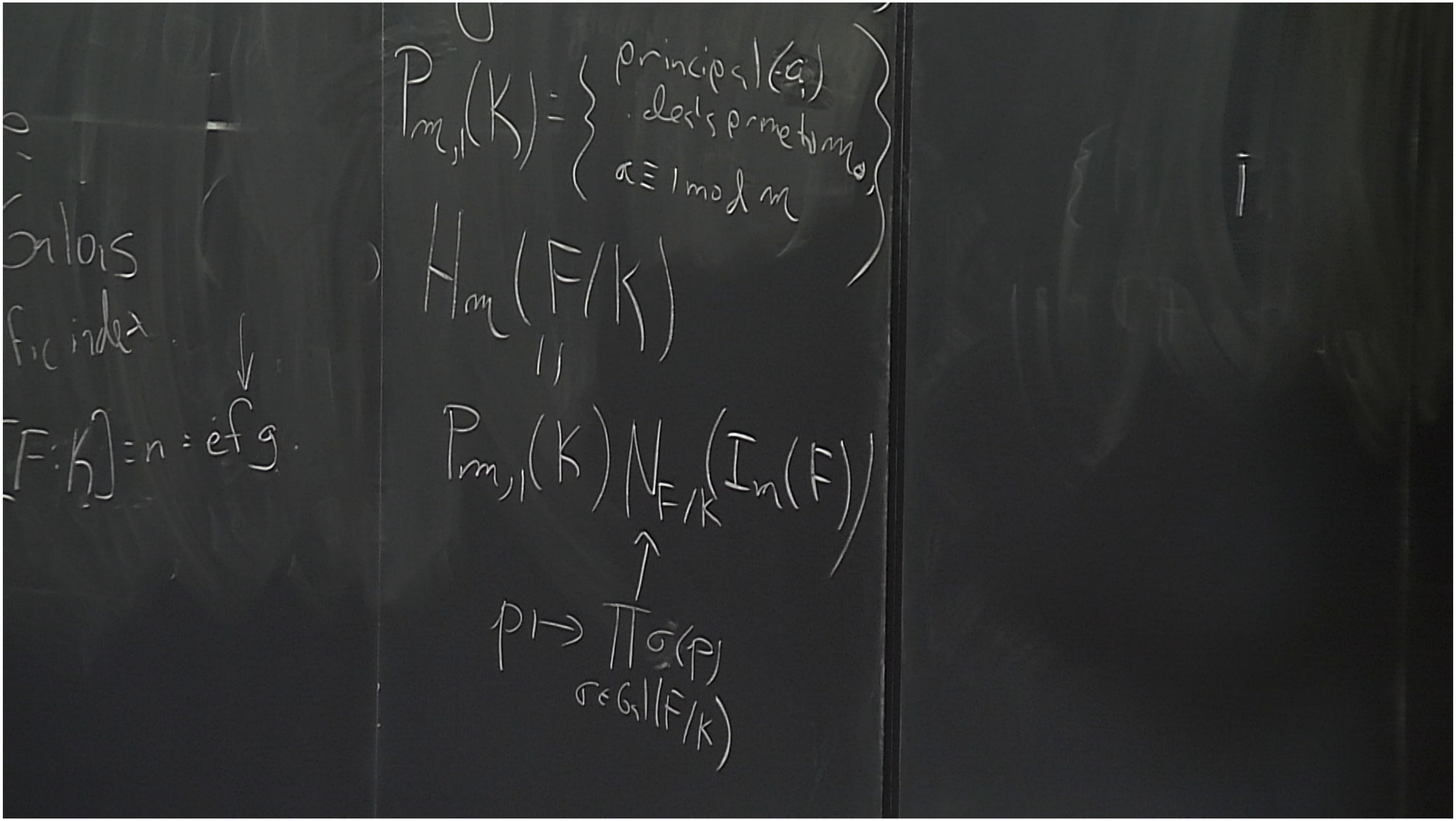
$$\mathfrak{m} = \mathfrak{m}_0 \, \mathfrak{m}_\infty$$

$$I_{\mathfrak{m}}(K) = \left\{ \begin{array}{l} \text{fractional ideals} \\ \text{prime to } \mathfrak{m}_0 \end{array} \right\}$$

$$\cup$$

$$P_{\mathfrak{m},1}(K) = \left\{ \begin{array}{l} \text{principal } (a) \\ \text{ideals prime to } \mathfrak{m}_0 \\ a \equiv 1 \bmod \mathfrak{m} \ldots \end{array} \right.$$

$\{P \ldots P\}$ st


Galois
f, e index
$[F:K] = n = efg$
$P_{m,1}(K) = \{$ principal (a) ideals prime to m, $a \equiv 1 \bmod m \}$
$H_m(F/K)$
$P_{m,1}(K) N_{F/K}(I_m(F))$
$p \mapsto \prod_{\sigma \in Gal(F/K)} \sigma(p)$

Weber: if $\mathfrak{m}$ is a modulus in K,

and F/K is Galois,

then $[I_{\mathfrak{m}}(K) : H_{\mathfrak{m}}(F/K)] \le [F:K]$

Defn: F/K is a <u>class field</u> if

$\exists\, \mathfrak{m}$ in K s.t. is equality.

Such an $\mathfrak{m}$ is called <u>admissible</u> for F/K,

Minimal $\mathfrak{m}$ called <u>conductor</u> of F/K

Otoh, if F/K abelian, then $\ge$.

...n K,

$\ldots] \leq [F : K]$

... field if

...s equality.

...missible for F/K,

...onductor of

...then $\geq$

Ray class field K^{m}

is a maximal class field

with modulus m.

Assume d odd.

Then $g \in SL_2(d)$ acts via

$$g \circ \Delta_j = \Delta_{gj} = u_g \Delta_j$$

$$(ST)^2$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\to SL_2(\mathbb{Z}) \to SL_2(d) \to 1$$

...class field K^m

...s a maximal class field with modulus m.

$v_1, \dots, v_{d^2}$

$P_i = v_i v_i^\dagger$

$$\sum_i \frac{1}{d} P_i = I$$

$$\mathrm{Tr}\, P_i P_j = \frac{1}{d+1}$$

SIC-POVM

$$\sum_i A_i = I, \quad A_i \geq 0$$

$S \subset \{1, \dots, d^2\}$, $A_S = \sum_{i \in S} A_i$, $\Pr\{i \in S\} = \mathrm{Tr}\, \rho A_S$

$\rho^\dagger = \rho$, $\rho \geq 0$, $\mathrm{Tr}\, \rho = 1$

$\mathcal{O}_K \subset K$, $K = \mathbb{Q}(\sqrt{m})$

$\mathcal{O}_K = \mathbb{Z}[\sqrt{m}], \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$

$\mathcal{O}_K^\times = \langle -1, u_f \rangle$ $u_f^r + u_f^{-r} + 1 = d$

$I \subset \mathcal{O}_K$, factors uniquely in prime ideals

$I = P_1 P_2 \cdots P_m$

prime ideals

$xy \in P \Rightarrow x \in P$ or $y \in P$.

Modul

(Π ide

$m =$

$I_m(K) =$

$\cup$

$P_{m,1}(K) = \{$

$K = \mathbb{Q}(\sqrt{m})$

$\mathcal{O}_K \subset K,\quad \mathcal{O}_K = \mathbb{Z}[\sqrt{m}],\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$

$\mathcal{O}_K^\times = \langle -1, u_f \rangle \quad u_f^r + u_f^{-r} + 1 = d$

$I \subset \mathcal{O}_K$, factors uniquely in prime ideals

$u_f = \frac{1+\sqrt{5}}{2}$

$I = \mathfrak{p}_1 \mathfrak{p}_2 \ \mathfrak{p}_m$

prime ideals

$u_f^2 = u_f \pm \frac{3+\sqrt{5}}{2}$

$d = 4, 8, 19, 48, 124, 323, 844, \ldots$

$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

$\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_q$, $\quad F/K$ Galois

$\mathcal{O}_F \mathfrak{p} = (\mathfrak{P} \ldots)^{e}$ ramific index

Modulus in K:

$\left(\prod \text{ideal of } K\right) \times$ {embedd}

$\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$

$I_{\mathfrak{m}}(K) = \left\{ \begin{array}{l} \text{fractional ideals} \\ \text{prime to } \mathfrak{m}_0 \end{array} \right\}$

$\cup$

$P_{\mathfrak{m},1}(K) = \left\{ \begin{array}{l} \text{principal } (\alpha) \\ \text{ideals prime to } \mathfrak{m}_0 \\ \alpha \equiv 1 \bmod \mathfrak{m} \end{array} \right\}$

$H_{\mathfrak{m}}(F/K) \ldots$