Galois fields in quantum mechanics

A. Vourdas
University of Bradford

Phase space methods:
position and momentum in the ring $\mathcal{Z}(d)$ and the field $GF(p^\ell)$

- Finite quantum systems (eg spin)
  phase space: toroidal lattice $\mathcal{Z}(d) \times \mathcal{Z}(d)$
  displacements

- Symplectic transf: isotropy of phase space
  $\mathcal{Z}(p) \equiv GF(p)$(field)
  phase space: finite geometry

- Galois field $GF(p^\ell)$

- quantum systems in $GF(p^\ell)$
  quantum engineering : ℓ spins with
  $j = (p-1)/2$ **coupled in a particular way**

- Frobenius transformations and Galois group:
  algebraic concepts in harmonic analysis
  implications for physics

Motivation:
symplectic transf in discrete systems
mutually unbiased bases
classical/quantum information processing
field extension in quantum mechanics and harmonic analysis

Finite quantum systems

- d-dimensional Hilbert space $\mathcal{H}$
  e.g., spin $j = (d-1)/2$
  position states $|\mathcal{X}; m\rangle$
  $m \in \mathcal{Z}(d)$ ring (field when $d = p^\ell$).

- Fourier transform:

$$\mathcal{F} \;=\; d^{-1/2} \sum_{m,n} \omega(mn) |\mathcal{X}; m\rangle\langle\mathcal{X}; n|$$

$$\omega(\alpha) \;=\; \exp\left[i\frac{2\pi\alpha}{d}\right]; \qquad \mathcal{F}^4 = \mathbf{1}$$

- momentum states $|\mathcal{P}; m\rangle$:

$$|\mathcal{P}; m\rangle = \mathcal{F}|\mathcal{X}; m\rangle = d^{-1/2} \sum_n \omega(mn) |\mathcal{X}; n\rangle$$

- arbitrary state

$$|f\rangle = \sum f_m |\mathcal{X}; m\rangle = \sum \tilde{f}_m |\mathcal{P}; m\rangle$$

  entropic uncertainty relations

- position and momentum operators

$$\widehat{x} = \sum_m m |\mathcal{X}; m\rangle\langle\mathcal{X}; m|; \qquad \widehat{p} = \sum_m m |\mathcal{P}; m\rangle\langle\mathcal{P}; m|$$

- in harmonic oscillator: phase space $R \times R$
  displacements: $\exp(i\alpha\hat{x})$, $\exp(i\beta\hat{p})$
  where $\alpha, \beta \in R$

$$\begin{aligned} \exp(-i\beta\hat{p})|x\rangle &= |x+\beta\rangle \\ \exp(-i\beta\hat{p})|p\rangle &= \exp(-i\beta p)|p\rangle \\ \exp(i\alpha\hat{x})|x\rangle &= \exp(i\alpha x)|x\rangle \\ \exp(i\alpha\hat{x})|p\rangle &= |p+\alpha\rangle \end{aligned}$$

- position-momentum phase space:
  $\mathcal{Z}(d) \times \mathcal{Z}(d)$(toroidal lattice)
  Displacement operators:

$$\mathcal{X} = \exp\left[-i\frac{2\pi}{d}\hat{p}\right] \quad ; \qquad \mathcal{Z} = \exp\left[i\frac{2\pi}{d}\hat{x}\right]$$

$$\begin{aligned} \mathcal{X}^\beta|\mathcal{X};m\rangle &= |\mathcal{X};m+\beta\rangle \\ \mathcal{X}^\beta|\mathcal{P};m\rangle &= \omega(-m\beta)|\mathcal{P};m\rangle \\ \mathcal{Z}^\alpha|\mathcal{X};m\rangle &= \omega(m\alpha)|\mathcal{X};m\rangle \\ \mathcal{Z}^\alpha|\mathcal{P};m\rangle &= |\mathcal{P};m+\alpha\rangle \end{aligned}$$

  here $\alpha, \beta \in \mathcal{Z}(d)$

- general displacements

  $\mathcal{D}(\alpha,\beta) = \mathcal{Z}^\alpha\mathcal{X}^\beta\omega(-2^{-1}\alpha\beta); \quad [\mathcal{D}(\alpha,\beta)]^\dagger = \mathcal{D}(-\alpha,-\beta)$

- Heisenberg-Weyl group

$$\begin{aligned} &\mathcal{X}^d = \mathcal{Z}^d = \mathbf{1} \text{ toroidal} \\ &\mathcal{X}^\beta\mathcal{Z}^\alpha = \mathcal{Z}^\alpha\mathcal{X}^\beta\omega(-\alpha\beta) \end{aligned}$$

- marginal properties (d odd)

$$\frac{1}{d}\sum_{\alpha}\mathcal{D}(\alpha,\beta)=|X;2^{-1}\beta\rangle\langle X;-2^{-1}\beta|$$

$$\frac{1}{d}\sum_{\beta}\mathcal{D}(\alpha,\beta)=|P;2^{-1}\alpha\rangle\langle X;-2^{-1}\alpha|$$

- arbitrary operator Θ

$$\Theta=\frac{1}{d}\sum_{\alpha,\beta}\mathcal{D}(\alpha,\beta)\;\mathcal{W}(-\alpha,-\beta)$$

$$\mathcal{W}(\alpha,\beta)=\mathrm{tr}[\Theta\mathcal{D}(\alpha,\beta)]$$

$\mathcal{W}(\alpha,\beta)$: Weyl function

- arbitrary operator Θ

$$\frac{1}{d}\sum_{\alpha,\beta}\mathcal{D}(\alpha,\beta)\;\frac{\Theta}{\mathrm{tr}\Theta}[\mathcal{D}(\alpha,\beta)]^{\dagger}=\mathbf{1}$$

In the special case $\Theta=|s\rangle\langle s|$

$$\frac{1}{d}\sum_{\alpha,\beta}|\alpha,\beta;s\rangle\langle\alpha,\beta;s|=\mathbf{1}$$

$$|\alpha,\beta;s\rangle\equiv\mathcal{D}(\alpha,\beta)|s\rangle$$

resolution of the identity

- Wigner and Weyl functions, etc

Symplectic transformations in Galois quantum systems

- Transformations:

  $$\mathcal{X}' = S\mathcal{X}S^\dagger = \mathcal{X}^\kappa \mathcal{Z}^\lambda; \qquad \mathcal{Z}' = S\mathcal{Z}S^\dagger = \mathcal{X}^\mu \mathcal{Z}^\nu$$
  $$\kappa\nu - \lambda\mu = 1 \ (mod\ d)$$

  preserve the

  $$\mathcal{X}'^d = \mathcal{Z}'^d = \mathbf{1}; \qquad \mathcal{X}'^\beta \mathcal{Z}'^\alpha = \mathcal{Z}'^\alpha \mathcal{X}'^\beta \omega^{-\alpha\beta}$$

  3 independent integer parameters.

- For a given triplet (κ,λ,μ) can we find integer ν such that $\nu = \kappa^{-1}(\lambda\mu + 1)$ (mod d)?
  Yes, if parameters in $\mathcal{Z}(p) \equiv GF(p)$ or $GF(p^\ell)$

- 'Galois quantum systems': position and momentum in $GF(p^\ell)$
  Phase space $GF(p^\ell) \times GF(p^\ell)$ **finite geometry**.
  symplectic trs: $Sp(2, GF(p^\ell))$ group

- now $\mathcal{Z}(p) \equiv GF(p)$(later $GF(p^\ell)$)
  construct explicitly symplectic operator S

$$\begin{aligned} S(\kappa,\lambda,\mu) &= S(1,0,\xi_1)S(1,\xi_2,0)S(\xi_3,0,0) \\ \xi_1 &= \mu\kappa(1+\lambda\mu)^{-1} \\ \xi_2 &= \lambda\kappa^{-1}(1+\lambda\mu) \\ \xi_3 &= \kappa(1+\lambda\mu)^{-1} \end{aligned}$$

  where

$$\begin{aligned} S(\xi_3,0,0) &= \sum_m |X;\xi_3 m\rangle\langle X;m| \\ S(1,\xi_2,0) &= \sum_m \omega(2^{-1}\xi_2 m^2)|X;m\rangle\langle X;m| \\ S(1,0,\xi_1) &= \sum_m \omega(-2^{-1}\xi_1 m^2)|P;m\rangle\langle P;m| \end{aligned}$$

- $S(\xi_3,0,0)$ dilation/contraction (squeezing) transformations

$$\begin{aligned} S(\xi_3,0,0)|\mathcal{X};m\rangle &= |\mathcal{X};\xi_3 m\rangle \\ S(\xi_3,0,0)|\mathcal{P};m\rangle &= |\mathcal{P};\xi_3^{-1} m\rangle \end{aligned}$$

  example:$p=3$, $\xi_3=2$, $\xi_3^{-1}=2$:

$$\begin{aligned} S|\mathcal{X};0\rangle &= |\mathcal{X};0\rangle; \quad S|\mathcal{X};1\rangle = |\mathcal{X};2\rangle; \quad S|\mathcal{X};2\rangle = |\mathcal{X};1\rangle \\ S|\mathcal{P};0\rangle &= |\mathcal{P};0\rangle; \quad S|\mathcal{P};1\rangle = |\mathcal{P};2\rangle; \quad S|\mathcal{P};2\rangle = |\mathcal{P};1\rangle \end{aligned}$$

  reordering of the points

Galois fields

- $\mathcal{Z}(p)$: field
  Field extension: elements of $GF(p^\ell)$

  $$\alpha = \alpha_0 + \alpha_1\epsilon + ... + \alpha_{\ell-1}\epsilon^{\ell-1}; \quad \alpha_i \in \mathcal{Z}(p)$$

  defined modulo **irreducible** polynomial of degree ℓ:

  $$P(\epsilon) = c_0 + c_1\epsilon + ... + c_{\ell-1}\epsilon^{\ell-1} + \epsilon^\ell; \quad c_i \in \mathcal{Z}(p)$$

  different $P(\epsilon)$, isomorphic results
  addition, multiplication

- Frobenius automorphism:

  $$\sigma : \alpha \rightarrow \alpha^p; \qquad \sigma^\ell = \mathbf{1}$$
  $$\alpha \rightarrow \alpha^p \rightarrow \alpha^{p^2} \rightarrow ... \rightarrow \alpha^{p^{\ell-1}} \rightarrow \alpha^{p^\ell} = \alpha$$

  Galois conjugates: α, α^p,...$\alpha^{p^{\ell-1}}$
  Galois group:$\{\mathbf{1}, \sigma, ..., \sigma^{\ell-1}\} \cong \mathcal{Z}(\ell)$

- Trace: sum of all conjugates

  $$\mathrm{Tr}\alpha = \alpha + \alpha^p + ... + \alpha^{p^{\ell-1}}; \quad \mathrm{Tr}\alpha \in \mathcal{Z}(p)$$

  trace of $\alpha\beta$ can be written as

  $$\mathrm{Tr}(\alpha\beta) = \sum g_{ij}\alpha_i\beta_j; \quad g_{ij} = \mathrm{Tr}[\epsilon^{i+j}]$$

  g_{ij}: depends on irreducible polynomial
  matrix g has inverse

- $(1, \epsilon, ..., \epsilon^{\ell-1}) \to (E_0, E_1, ..., E_{\ell-1})$
  dual basis E_i such that $\mathrm{Tr}(\epsilon^\kappa E_\lambda) = \delta_{\kappa\lambda}$.

$$\begin{aligned} \alpha &= \sum_{\lambda=0}^{\ell-1} \alpha_\lambda \epsilon^\lambda = \sum_{\lambda=0}^{\ell-1} \bar{\alpha}_\lambda E_\lambda \\ \alpha_\lambda &= \mathrm{Tr}[\alpha E_\lambda]; \quad \bar{\alpha}_\lambda = \mathrm{Tr}[\alpha \epsilon^\lambda] = \sum_\kappa g_{\lambda\kappa} \alpha_\kappa \end{aligned}$$

  trace of $\alpha\beta$ can be written as

$$\mathrm{Tr}(\alpha\beta) = \sum g_{ij}\alpha_i\beta_j = \sum \bar{\alpha}_i\beta_i = \sum \alpha_i\bar{\beta}_i$$

- exponential of α (complex valued function):

$$\chi(\alpha) = \omega(\mathrm{Tr}\alpha); \quad \omega = \exp(i2\pi/p)$$

  additive characters: $\chi(\alpha)\chi(\beta) = \chi(\alpha + \beta)$
  later in Fourier transforms:

$$\chi(\alpha\beta) = \omega\left(\sum g_{ij}\alpha_i\beta_j\right) = \omega\left(\sum \bar{\alpha}_i\beta_i\right) = \omega\left(\sum \alpha_i\bar{\beta}_i\right)$$

  where

$$\sum_\alpha \chi(\alpha\beta) = \delta(\beta, 0)$$

- example: $GF(9)$(where $p = 3$, $\ell = 2$)
  choose $P(\epsilon) = \epsilon^2 + \epsilon + 2$

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

  off-diagonal elements: coupling between subsystems later

Ring $[\mathcal{Z}(p)]^\ell$ versus Galois field $GF(p^\ell)$

- **ring** $[\mathcal{Z}(p)]^\ell \equiv \mathcal{Z}(p) \times ... \times \mathcal{Z}(p)$
  Addition and multiplication:

  $(\alpha_\lambda) + (\beta_\lambda) = (\alpha_\lambda + \beta_\lambda); \qquad (\alpha_\lambda)(\beta_\lambda) = (\alpha_\lambda \beta_\lambda)$

  $(0, ..., 0)$ zero; and $(1, ..., 1)$ unity

- additive characters

$$\psi[(\alpha_\lambda)] = \omega\left(\sum_\lambda \alpha_\lambda\right)$$

  and

$$\frac{1}{p^\ell}\sum_{(\alpha_\lambda)} \psi[(\alpha_\lambda)(\beta_\lambda)] = \delta[(\beta_\lambda), (0)]$$

- **compare** harmonic analysis on $GF(p^\ell)$ with harmonic analysis on $[\mathcal{Z}(p)]^\ell$
  at this stage compare

$$\psi[(\alpha_\lambda \beta_\lambda)] = \omega\left(\sum_\lambda \alpha_\lambda \beta_\lambda\right)$$

  with the

$$\chi(\alpha\beta) = \omega\left(\sum_{\lambda,\mu} g_{\lambda\mu}\alpha_\lambda\beta_\mu\right) = \omega\left(\sum_\lambda \overline{\alpha}_\lambda \beta_\lambda\right) = \omega\left(\sum_\lambda \alpha_\lambda \overline{\beta}_\lambda\right)$$

  g_{ij} related to Galois multiplication rule

Galois quantum systems

- tensor product of ℓ spaces:
  $H = \mathcal{H} \otimes ... \otimes \mathcal{H}$
  $\mathcal{H}$ is p-dimensional
  H is p^ℓ-dimensional
  e.g., ℓ **coupled** spins $j = (p-1)/2$

  in this space:

  - Galois systems with position/momentum in $GF(p^\ell)$
    position states in H

    $$|X; m\rangle \equiv |\mathcal{X}; m_0\rangle \otimes ... \otimes |\mathcal{X}; m_{\ell-1}\rangle$$
    $$m = \sum_i m_i \epsilon^i \ \in GF(p^\ell); \qquad m_i \in \mathcal{Z}(p)$$

  - 'R-systems' with position/momentum in the ring $\mathcal{Z}(p) \times ... \times \mathcal{Z}(p)$.
    Position states

    $$|X; (m_\lambda)\rangle \equiv |\mathcal{X}; m_0\rangle \otimes ... \otimes |\mathcal{X}; m_{\ell-1}\rangle$$

- Fourier transform in Galois systems:

$$\begin{aligned} F &= (p^\ell)^{-1/2} \sum_{m,n} \chi(mn) |X; m\rangle\langle X; n| \\ &= (p^\ell)^{-1/2} \sum_{m_i, n_j} \omega \left[\sum_{i,j} g_{ij} m_i n_j \right] \\ &\times \quad |\mathcal{X}; m_0\rangle\langle \mathcal{X}; n_0| \otimes ... \otimes |\mathcal{X}; m_{\ell-1}\rangle\langle \mathcal{X}; n_{\ell-1}| \end{aligned}$$

  g_{ij} related to Galois theory

- Fourier transform in R-systems:

$$\begin{aligned} \mathcal{F} \otimes ... \otimes \mathcal{F} &= (p^\ell)^{-1/2} \sum_{m_i, n_i} \omega \left[\sum_{i,j} m_i n_i \right] \\ &\times \quad |\mathcal{X}; m_0\rangle\langle \mathcal{X}; n_0| \otimes ... \otimes |\mathcal{X}; m_{\ell-1}\rangle\langle \mathcal{X}; n_{\ell-1}| \end{aligned}$$

  different from F

- Hamiltonian for Galois systems:

$$h = h(\hat{Q}, \hat{P}) = h(\hat{Q}, F\hat{Q}F^{\dagger})$$

special coupling between component systems related to off-diagonal g_{ij} which embodies Galois theory
in contrast:
Hamiltonian for 'R-systems':

$$h' = h'(\hat{\mathcal{Q}}_0, \hat{\mathcal{P}}_0; ...; \hat{\mathcal{Q}}_{\ell-1}, \hat{\mathcal{P}}_{\ell-1})$$

arbitrary coupling between component systems h **special case of** h'

- quantum engineering of a Galois system:
ℓ spins with $j = (p-1)/2$ described with the Hamiltonian h.

- momentum states:

$$|P; m\rangle = F|X; m\rangle = |\mathcal{P}; \bar{m}_0\rangle \otimes ... \otimes |\mathcal{P}; \bar{m}_{\ell-1}\rangle$$
$$m = \sum_i m_i \epsilon^i = \sum_i \bar{m}_i E_i$$

- displacement operators: as before **with trace**

$$Z^{\alpha} \equiv \sum_n \chi(\alpha n)|X; n\rangle\langle X; n|$$

- $GF(p^\ell) \times GF(p^\ell)$ phase space:
  general displacements

  $$D(\alpha, \beta) = Z^\alpha X^\beta \chi(-2^{-1}\alpha\beta)$$

  relationship between displacement operator and displacement operators in component systems

  $$D(\alpha, \beta) = \mathcal{D}(\bar{\alpha}_0, \beta_0) \otimes ... \otimes \mathcal{D}(\bar{\alpha}_{\ell-1}, \beta_{\ell-1})$$

- symplectic transformations $Sp(2, GF(p^\ell))$:
  previous formulas **with trace**
  uses Galois multiplication

- marginal properties of Wigner and Weyl functions with respect to (X, P) axes, also valid with respect to other axes
  discrete isotropy of phase space

Frobenius transformations

- positions have the Frobenius property

  $$\alpha \rightarrow \alpha^{p} \rightarrow \alpha^{p^2} \rightarrow ... \rightarrow \alpha^{p^{\ell-1}} \rightarrow \alpha^{p^{\ell}} = \alpha$$

  implications for physics

- Frobenius transformations:

  $$\mathcal{G} \equiv \sum_{m} |X; m^{p}\rangle\langle X; m| = \sum_{m} |P; m^{p}\rangle\langle P; m|$$

  $$\mathcal{G}\mathcal{G}^{\dagger} = \mathbf{1}; \quad \mathcal{G}^{\ell} = \mathbf{1}; \quad [\mathcal{G}, F] = 0$$

  $\{\mathbf{1}, \mathcal{G}, ..., \mathcal{G}^{\ell-1}\} \cong \mathcal{Z}(\ell)$
  Galois group (algebraic concept) in harmonic analysis

-

$$\begin{aligned} \mathcal{G}^{\lambda}|X; m\rangle &= |X; m^{p^{\lambda}}\rangle \\ \mathcal{G}^{\lambda}|P; m\rangle &= |P; m^{p^{\lambda}}\rangle \\ \mathcal{G}^{\lambda} D(\alpha, \beta)(\mathcal{G}^{\dagger})^{\lambda} &= D\left(\alpha^{p^{\lambda}}, \beta^{p^{\lambda}}\right) \end{aligned}$$

for $\alpha, \beta \in \mathcal{Z}_p$ the $\mathcal{G}$ commutes with $D(\alpha, \beta)$.

- **if $\mathcal{G}$ commutes with the Hamiltonian h:** density submatrices ($p^\ell \times p^\ell$ matrices)

$$\rho_{\lambda\mu}(t) = \varpi(\lambda)\rho(t)\varpi(\mu)$$

  each submatrix evolves independently:

$$\rho_{\lambda\mu}(t) = \exp(iht)\rho_{\lambda\mu}(0)\exp(-iht)$$

- eigenvalues of $\rho_{\lambda\lambda}(t)$ constant in time

- $\rho_{\lambda\mu}(t)$ with $\lambda \neq \mu$ in general not normal
  singular values of $\rho_{\lambda\mu}(t)$ constant in time

- $\ell - 1$ constants of motion

$$\mathrm{tr}[\rho(t)\varpi(\lambda)] = \mathrm{tr}[\rho(0)\varpi(\lambda)]$$

- example: $GF(9)$(where $p = 3$, $\ell = 2$)
  choose $P(\epsilon) = \epsilon^2 + \epsilon + 2$

$$\mathcal{G} = \varpi(0) - \varpi(1)$$

If hamiltonian commutes with $\mathcal{G}$

$$\begin{aligned}
\text{tr}[\rho\varpi(1)] &= \frac{1}{2}[\rho_X(\epsilon,\epsilon) + \rho_X(1+\epsilon,1+\epsilon) \\
&+ \rho_X(2+\epsilon,2+\epsilon) + \rho_X(1+2\epsilon,1+2\epsilon) \\
&+ \rho_X(2\epsilon,2\epsilon) + \rho_X(2+2\epsilon,2+2\epsilon) \\
&- \rho_X(2+2\epsilon,\epsilon) - \rho_X(\epsilon,2+2\epsilon) \\
&- \rho_X(2\epsilon,1+\epsilon) - \rho_X(1+\epsilon,2\epsilon) \\
&- \rho_X(1+2\epsilon,2+\epsilon) - \rho_X(2+\epsilon,1+2\epsilon)]
\end{aligned}$$

constant in time
Notation:

$$\rho_X(m,n) = \langle X; m|\rho|X; n\rangle$$

tr$[\rho\varpi(0)]$ also constant in time (not independent)

Discussion

- d-dimensinal Hilbert space
  Phase space $\mathcal{Z}(d) \times \mathcal{Z}(d)$
  Displacements, displaced parity operators

- $\mathcal{Z}(p) \equiv GF(p)$
  Phase space: finite geometry
  symplectic transformations well defined

- $GF(p^\ell)$
  $H = \mathcal{H} \otimes ... \otimes \mathcal{H}$
  Fourier transform, displacements, etc
  similar expressions as before **with Galois trace**

- quantum engineering of such system:
  ℓ spins with $j = (p-1)/2$ described with the Hamiltonian h (special coupling)

- Frobenius transformations and Galois group:
  algebraic concepts in harmonic analysis
  physically: constants of motion

- J. Phys. A38, 8453 (2005)
  J. Math. Phys. 47, 092104 (2006)
  Acta Appl. Math.93, 197 (2006)
  J. Fourier Anal. Appl. 14, 102 (2008)
  reviews:
  Rep. Prog. Phys. 67 (2004) 267
  JPA 40, R285 (2007)