Quantum systems with finite Hilbert space: Galois fields in quantum mechanics

J. Phys. A: Math. Theor. **40** (2007) R285–R331 doi:10.1088/1751-8113/40/33/R01

TOPICAL REVIEW

Quantum systems with finite Hilbert space: Galois fields in quantum mechanics

A Vourdas

Department of Computing, University of Bradford, Bradford BD7 1DP, UK

Received 11 May 2007
Published 1 August 2007
Online at stacks.iop.org/JPhysA/40/R285

Abstract
A 'Galois quantum system' in which the position and momentum take values in the Galois field $\mathrm{GF}(p^\ell)$ is considered. It is comprised of ℓ-component systems which are coupled in a particular way and is described by a certain class of Hamiltonians. Displacements in the $\mathrm{GF}(p^\ell) \times \mathrm{GF}(p^\ell)$ phase space and the corresponding Heisenberg–Weyl group are studied. Symplectic transformations are shown to form the $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$ group. Wigner and Weyl functions are defined and their properties are studied. Frobenius symmetries, which are based on Frobenius automorphisms in the theory of Galois fields, are a unique feature of these systems (for $\ell \geqslant 2$). If they commute with the Hamiltonian, there are constants of motion which are discussed. An analytic representation in the ℓ-sheeted complex plane provides an elegant formalism that embodies the properties of Frobenius transformations. The difference between a Galois quantum system and other finite quantum systems where the position and momentum take values in the ring $[\mathbb{Z}_p]^\ell$ is discussed.

PACS numbers: 03.65.Ca, 02.10.De

Contents

1751-8113/07/330285+47$30.00

1. Introduction

Quantum mechanics is usually studied in the context of the harmonic oscillator where position and momentum take values in $\mathbb{R}$ (real numbers). In this case the position–momentum phase space is $\mathbb{R} \times \mathbb{R}$. Various functions in phase space (e.g., Wigner and Weyl functions) have been shown to provide a deep description of the system. There is an important class of transforms in this phase space which includes Fourier transforms, displacements and symplectic $\mathrm{Sp}(2, \mathbb{R})$ transforms. Their properties are intimately related to the powerful properties of the Wigner and Weyl functions. In particular, symplectic transformations play an important role in areas like quantum tomography, Bogoliubov transformations and their applications to superfluidity and superconductivity, etc.

Quantum mechanics on a circle $\mathbb{S}$ is also an important area, which has applications in Aharonov–Bohm phenomena, mesoscopic rings, etc. In this case the momentum takes values in $\mathbb{Z}$ (the integers), and the phase space is $\mathbb{S} \times \mathbb{Z}$.

In both the above cases the Hilbert space of the system is infinite dimensional. We now consider systems where the position and momentum take values in $\mathbb{Z}_q$ (the integers modulo q). In this case the Hilbert space is q dimensional, and the phase space is the toroidal lattice $\mathbb{Z}_q \times \mathbb{Z}_q$. When we develop a phase-space formalism for this system, which is analogous to the harmonic oscillator, we encounter difficulties. We easily define Fourier transform and displacements in $\mathbb{Z}_q \times \mathbb{Z}_q$. The difficulties appear in symplectic transformations (and related concepts like quantum tomography). The root of these difficulties is that $\mathbb{Z}_q$ is, in general, a ring. Consequently, the $\mathbb{Z}_q \times \mathbb{Z}_q$ is a set of points with no geometrical structure. Therefore the phase-space formalism in these systems is less powerful than in a harmonic oscillator.

All these difficulties disappear, when q is equal to a prime number p. In this case, $\mathbb{Z}_p$ is a field, inverses exist (i.e., division is well defined) and the $\mathbb{Z}_p \times \mathbb{Z}_p$ is a finite geometry [1]. We can define symplectic transformations and show that they form the $\mathrm{Sp}(2, \mathbb{Z}_p)$ group. Their physical significance lies in the fact that the $\mathbb{Z}_p \times \mathbb{Z}_p$ phase space has a (discrete) isotropy, and all results that are valid with respect to a pair of directions are also valid with respect to other pairs of directions. One consequence of this is that we can define tomographic techniques based on Radon transformations, which are analogous to similar techniques in $\mathbb{R} \times \mathbb{R}$ for the harmonic oscillator. Therefore, the phase-space formalism in these systems is equally powerful to the harmonic oscillator formalism.

Even more interesting is the case where q is equal to a power of a prime number ($q = p^\ell$). In this case the position and momentum take values in the Galois field $\mathrm{GF}(p^\ell)$ [2], and for this reason we call them Galois quantum systems (or G-systems). Here symplectic transformations are also well defined and form the $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$ group. In addition to that we have an extra symmetry, which is absent in the harmonic oscillator case and it is trivial in the finite case with $q = p$. It is based on Frobenius automorphisms in Galois fields, and we call them Frobenius symmetries. Due to this extra symmetry, the phase-space formalism in Galois systems is more powerful than in a harmonic oscillator. This is due to the fact that although in general, lattices have less symmetry than the continuum; when they are based on Galois fields they are a geometry with more symmetry than the continuum.

There are various other problems which lead to Galois quantum systems. One is the problem of mutually unbiased bases, which has applications to quantum information processing [3–14]. The number of such bases in a q-dimensional Hilbert space cannot exceed $q+1$; and when q is the power of a prime, the number of such bases is equal to $q+1$. Related is the 'mean king's problem' which has been studied in [15–18]. Applications of these ideas to positive operator valued measures have been discussed in [19, 20]. Applications to quantum coding have been discussed in [21, 22].

General finite quantum systems have been studied originally by Weyl [23] and Schwinger [24], and later by many authors [25–39]. Related is also the mathematical work of [40]. We have reviewed this work in [41]. We have explained there the importance of Galois quantum systems and we have discussed simple examples where the dimension is a prime number p. The purpose of the present review is to complement [41] with a discussion of systems with dimension p^{ℓ}, where $\ell \geqslant 2$. The work applies algebraic concepts from field extension and Galois theory to quantum mechanics. Special emphasis is given to Frobenius transformations and the Galois group, which are based on related concepts in the subject of field extension, in algebra. Physically, they are discrete symmetries, and for Hamiltonians which commute with them, we get constants of motion. These symmetries are a unique feature of p^{ℓ}-dimensional systems with $\ell \geqslant 2$.

Phase space methods in quantum mechanics are related to time-frequency methods in signal processing which have been studied originally by Gabor [42]and by Ville [43] and later by many authors [44]. These are also related to the general area of applied harmonic analysis. Therefore the ideas of the present paper can be used in these contexts also. We note here that early work about wavelets on Galois fields has been presented in [45].

In section 2 we present concepts from Galois theory in an applied form suitable for our context. For example, we present labelling methods of the irreducible polynomials, for later use. We also give the trace of the product of two elements of a Galois field, in terms of their components. In section 3 we present very briefly the theory of finite quantum systems. This has been reviewed in [41], and here we only present some basic concepts and explain the notation.

In section 4 we introduce Galois quantum systems and explain the concept of Frobenius subspaces. In section 5 we introduce Fourier transforms for Galois quantum systems and explain their physical meaning. In section 6 we explain how a Galois quantum system with position and momentum in $\mathrm{GF}(p^{\ell})$ can be viewed as a system comprised of ℓ-component systems which are p dimensional and which are coupled in a particular way. Only a special class of Hamiltonians, which describe this particular coupling, can give the system Galois structure.

In section 7 we discuss the Heisenberg–Weyl group of displacements in Galois systems. In section 8 we discuss symplectic $\mathrm{Sp}(2, \mathrm{GF}(p^{\ell}))$ transformations, Radon transforms and quantum tomography [46–48]. In section 9 we study the semidirect product of the Heisenberg–Weyl group of displacements by the group of symplectic transformations. This larger group which we call $\mathfrak{T}[\mathrm{GF}(p^{\ell})]$ contains both displacements and symplectic transformations. Wigner and Weyl functions, their properties and the related problem of quantum tomography are studied in section 10.

It is very important to compare and contrast a Galois quantum system with position and momentum in $\mathrm{GF}(p^{\ell})$ with a p^{ℓ}-dimensional system where the position and momentum take values in the ring $[\mathbb{Z}_p]^{\ell}$. We call the latter R-system and discuss it in section 11. Different multiplication rules in $\mathrm{GF}(p^{\ell})$ and $[\mathbb{Z}_p]^{\ell}$ lead to different quantum systems. A clear understanding of the difference between the two is essential for this work.

Frobenius transformations and the Galois group [49], which as we explained earlier are unique symmetries in Galois systems with dimension p^{ℓ} with $\ell \geqslant 2$, and are presented in section 12. Constants of motion, in systems with Hamiltonians that commute with the

Frobenius transformations, are discussed in section 13. In section 14 we consider the semidirect product of the $\mathfrak{T}[\mathrm{GF}(p^\ell)]$ by the Galois group of Frobenius transformations and get a larger group which contains Frobenius, displacements and symplectic transformations.

In the theory of Galois fields in algebra, the Galois group of Frobenius automorphisms contains *all* automorphisms of $\mathrm{GF}(p^\ell)$ which map the conjugates to each other. In our context the Galois group of Frobenius transformations leave invariant the Frobenius subspaces. But there are much more general transformations that leave invariant the Frobenius subspaces, which we discuss in section 15.

In section 16 we present an analytic representation of Galois systems in the ℓ-sheeted complex plane. To each irreducible polynomial of order d, correspond d Galois conjugates and this can be viewed as a kind of multivaluedness. This multivaluedness can be connected to multivaluedness in Riemann surfaces. Work in this direction in a very different context has been presented in [50] and here we show this explicitly in our context [49]. The Frobenius transformations and their properties are expressed in an elegant way in the language of analytic functions, on Riemann surfaces.

In section 17 we discuss a physical implementation of Galois systems with spins. We conclude in section 18 with a discussion of our results.

2. Galois fields

Let $\mathbb{Z}_q$ be the ring of integers modulo q. In the special case that q is a prime number p the $\mathbb{Z}_p$ is a field. Field extensions lead to larger fields and below we use the Galois field $\mathrm{GF}(p^\ell)$. Some theorems in Galois theory are valid only for $p \neq 2$ and this is the case considered here. Quantum systems corresponding to the $p = 2$ case have been discussed in [6, 9].

An important aspect of Galois theory is the relation of a field with its subfields. If d is a divisor of ℓ (which we denote as $d|\ell$) the $\mathrm{GF}(p^d)$ is a subfield of $\mathrm{GF}(p^\ell)$. In this case $\mathbb{Z}_p$ is a subfield of $\mathrm{GF}(p^d)$; and $\mathrm{GF}(p^d)$ is a subfield of $\mathrm{GF}(p^\ell)$.

We denote as $\mathbb{Z}_p[\epsilon]$ the ring of polynomials with coefficients in $\mathbb{Z}_p$. Let $P(\epsilon)$ be an irreducible polynomial of degree ℓ:

$$P(\epsilon) \equiv c_0 + c_1\epsilon + \cdots + c_{\ell-1}\epsilon^{\ell-1} + \epsilon^\ell; \qquad c_\lambda \in \mathbb{Z}_p. \tag{1}$$

The quotient $\mathbb{Z}_p[\epsilon]/(P(\epsilon))$ provides a representation of the field $\mathrm{GF}(p^\ell)$. Its elements can be written as polynomials

$$\alpha = \alpha_0 + \alpha_1\epsilon + \cdots + \alpha_{\ell-1}\epsilon^{\ell-1}; \qquad \alpha_\lambda \in \mathbb{Z}_p, \tag{2}$$

which are defined modulo the irreducible polynomial $P(\epsilon)$. We refer to α_λ as components of α with respect to the $\{1, \epsilon, \ldots, \epsilon^{\ell-1}\}$ basis. Below we will introduce other bases also. We note that different irreducible polynomials $P(\epsilon)$ of the same degree ℓ, lead to isomorphic finite fields.

2.1. Frobenius automorphism and Galois groups

The Frobenius map

$$\sigma(\alpha) = \alpha^p; \qquad \sigma^\ell = \mathbf{1} \tag{3}$$

defines an automorphism in $\mathrm{GF}(p^\ell)$. The $\alpha, \alpha^p, \ldots, \alpha^{p^{\ell-1}}$ are Galois conjugates and

$$\alpha^{p^\ell} = \alpha. \tag{4}$$

Elements in the subfield $\mathbb{Z}_p$ of $\mathrm{GF}(p^\ell)$ are self-conjugates:

$$\alpha \in \mathbb{Z}_p \rightarrow \alpha^p = \alpha. \tag{5}$$

Therefore the Frobenius automorphism maps the Galois conjugates to each other and leaves all elements of $\mathbb{Z}_p$ fixed. The

$$\mathrm{Gal}[\mathrm{GF}(p^\ell)/\mathbb{Z}_p] = \{\mathbf{1}, \sigma, \ldots, \sigma^{\ell-1}\} \tag{6}$$

form the Galois group which is a cyclic group of order ℓ. It comprises all automorphisms of $\mathrm{GF}(p^\ell)$ which leave the elements of the subfield $\mathbb{Z}_p$ fixed.

More generally, we consider a subfield $\mathrm{GF}(p^d)$ of $\mathrm{GF}(p^\ell)$ (where $d|\ell$). Elements of $\mathrm{GF}(p^d)$ satisfy the relation

$$\alpha \in \mathrm{GF}(p^d) \rightarrow \alpha^{p^d} = \alpha. \tag{7}$$

In this case

$$\mathrm{Gal}[\mathrm{GF}(p^\ell)/\mathrm{GF}(p^d)] = \{\mathbf{1}, \sigma^d, \ldots, \sigma^{\ell-d}\} \tag{8}$$

is a cyclic group of order ℓ/d and is a subgroup of $\mathrm{Gal}[\mathrm{GF}(p^\ell)/\mathbb{Z}_p]$. It comprises all automorphisms of $\mathrm{GF}(p^\ell)$ which leave the elements of the subfield $\mathrm{GF}(p^d)$ fixed.

The product

$$f(y) \equiv (y-\alpha)(y-\alpha^p)\cdots\left(y-\alpha^{p^{d-1}}\right) \tag{9}$$

involves all Galois conjugates and is an irreducible polynomial of degree d in $\mathbb{Z}_p[y]$. Such a polynomial labels a set of d Galois numbers which are all conjugate to each other.

The number of irreducible polynomials of degree d in $\mathbb{Z}_p[y]$ is

$$n(d, p) = \frac{1}{d}\sum_{e|d} \mu(e) p^{d/e}, \tag{10}$$

where μ is the Möbius μ-function and the summation is over all e which are divisors of d (starting with $e = 1$ and finishing with $e = d$). In the special case $d = 1$ we get:

$$n(1, p) = p. \tag{11}$$

For later use we introduce below two labelling methods of the irreducible polynomials.

2.2. First labelling method of the irreducible polynomials

We label the irreducible polynomials in $\mathbb{Z}_p[y]$ with two indices. The first index d is the degree of the polynomial. The second index κ labels all irreducible polynomials of degree d in $\mathbb{Z}_p[y]$ and takes values from 1 to $n(d, p)$. In this labelling method the irreducible polynomials will be denoted as $f_{d\kappa}(y)$.

The product of all distinct irreducible polynomials in $\mathbb{Z}_p[y]$ of degree d, where d is a divisor of ℓ, is

$$\prod_{d|\ell}\prod_{\kappa=1}^{n(d,p)} f_{d\kappa}(y) = y^{p^\ell} - y. \tag{12}$$

The total number of irreducible polynomials entering in this relation is

$$\sum_{d|\ell} n(d, p) \equiv \mathfrak{M}(\ell, p). \tag{13}$$

Counting the degrees of these polynomials we show that

$$\sum_{d|\ell} d n(d, p) = p^\ell. \tag{14}$$

We next consider a subfield $\mathrm{GF}(p^d)$ of $\mathrm{GF}(p^\ell)$ (where $d|\ell$). The analogue of equation (12) is in this case

$$\prod_{e|d} \prod_{\kappa=1}^{n(e,p)} f_{e\kappa}(y) = y^{p^d} - y. \tag{15}$$

The $y^{p^d} - y$ is a divisor of $y^{p^\ell} - y$.

2.3. Second labelling method of the irreducible polynomials

Here we introduce a one-to-one map between the pair of indices (d, κ) and a single index $\mathfrak{N}$. This provides another labelling method of the irreducible polynomials as

$$f_{\mathfrak{N}}(y) \equiv f_{d\kappa}(y); \qquad \mathfrak{N} = 1, \ldots, \mathfrak{M}(\ell, p). \tag{16}$$

We first write all divisors of ℓ in ascending order as

$$d_1 = 1 < d_2 < \cdots < d_{\mathfrak{q}_{\ell-1}} < d_{\mathfrak{q}_\ell} = \ell, \tag{17}$$

where $\mathfrak{q}_\ell$ denotes the number of divisors of ℓ. We then define the $w(\ell, d, p)$ as

$$w(\ell, d, p) = \sum_{d_i<d} n(d_i, p); \qquad w(\ell, 1, p) = 0. \tag{18}$$

The summation is over all divisors d_i of ℓ which are smaller than d. We now define the index $\mathfrak{N}$ as

$$\mathfrak{N} = w(\ell, d, p) + \kappa. \tag{19}$$

When $\mathfrak{N}$ is given, we can calculate the corresponding (d, κ) by finding the largest d_i among the divisors of ℓ, such that the $w(\ell, d_i, p)$ is smaller than $\mathfrak{N}$ and then

$$d = d_{i+1}; \qquad \kappa = \mathfrak{N} - w(\ell, d_i, p). \tag{20}$$

2.4. Labelling of the elements of $GF(p^\ell)$

We label all elements in $\mathrm{GF}(p^\ell)$ in a way that indicates the corresponding irreducible polynomial $f_{d\kappa}(y)$. We take any of the d Galois conjugates corresponding to $f_{d\kappa}(y)$, and denote it as $m(d, \kappa, 1)$. We then denote the rest of them as

$$m(d, \kappa, \nu) = [m(d, \kappa, 1)]^{p^{\nu-1}}; \qquad \kappa = 1, \ldots, n(d, p); \qquad \nu \in \mathbb{Z}_d. \tag{21}$$

The index ν is cyclic and therefore starting from a different conjugate will simply label the same elements as $m(d, \kappa, \nu + \nu_0)$, where ν_0 is a constant.

We have seen in equations (19) and (20) that there is one-to-one map between the pair of indices (d, κ) and the index $\mathfrak{N}$. Therefore an alternative labelling scheme of the elements of $\mathrm{GF}(p^\ell)$ is

$$m(d, \kappa, \nu) = m(\mathfrak{N}, \nu). \tag{22}$$

2.5. *Trace*

The trace of an element depends on the field extension that we consider. We use the notation Tr for the trace in the extension from $\mathbb{Z}_p$ to $\mathrm{GF}(p^\ell)$; the notation Tr_d for the trace in the extension from $\mathbb{Z}_p$ to $\mathrm{GF}(p^d)$; and the notation $\mathrm{Tr}_{\ell/d}$ for the trace in the extension from $\mathrm{GF}(p^d)$ to $\mathrm{GF}(p^\ell)$ (where $d|\ell$).

The trace of α in $\mathrm{GF}(p^\ell)$ is defined as the sum of all its conjugates:

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{\ell-1}}; \qquad \mathrm{Tr}(\alpha) \in \mathbb{Z}_p; \qquad \alpha \in \mathrm{GF}(p^\ell). \tag{23}$$

All conjugates have the same trace. The fact that $\mathrm{Tr}(\alpha)$ belongs to $\mathbb{Z}_p$ shows that $[\mathrm{Tr}(\alpha)]^p = \mathrm{Tr}(\alpha)$.

The Tr_d of α in $\mathrm{GF}(p^d)$ is defined as

$$\mathrm{Tr}_d(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{d-1}}; \qquad \mathrm{Tr}_d(\alpha) \in \mathbb{Z}_p; \qquad \alpha \in \mathrm{GF}(p^d). \tag{24}$$

The $\mathrm{Tr}_{\ell/d}$ of α in $\mathrm{GF}(p^\ell)$ is defined as

$$\mathrm{Tr}_{\ell/d}(\alpha) = \alpha + \alpha^{p^d} + \alpha^{p^{2d}} + \cdots + \alpha^{p^{\ell-d}}; \qquad \mathrm{Tr}_{\ell/d}(\alpha) \in \mathrm{GF}(p^d); \qquad \alpha \in \mathrm{GF}(p^\ell). \tag{25}$$

It can be shown that

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}_d[\mathrm{Tr}_{\ell/d}(\alpha)]; \qquad \alpha \in \mathrm{GF}(p^\ell). \tag{26}$$

In the special case that α belongs to $\mathrm{GF}(p^d)$ equation (26) reduces to

$$\mathrm{Tr}(\alpha) = \frac{\ell}{d}\mathrm{Tr}_d(\alpha); \qquad \alpha \in \mathrm{GF}(p^d). \tag{27}$$

2.6. *Trace and conjugates of Galois numbers in terms of their components*

We introduce the following symmetric $\ell \times \ell$ matrices g with elements in $\mathbb{Z}_p$ [47]:

$$g_{\lambda\kappa} \equiv \mathrm{Tr}(\epsilon^{\lambda+\kappa}); \qquad G \equiv g^{-1}; \qquad \kappa, \lambda = 0, \ldots, \ell - 1. \tag{28}$$

The elements of these matrices do depend on the choice of the irreducible polynomial $P(\epsilon)$ in equation (1); but different choices lead to isomorphic results. We explain below that the inverse of the matrix $(g_{\lambda\kappa})$ does exist.

We used earlier the basis $\{1, \epsilon, \ldots, \epsilon^{\ell-1}\}$ for the elements of $\mathrm{GF}(p^\ell)$. We now introduce the dual basis $\{E_\kappa\}$, as follows:

$$E_\kappa = \sum_\lambda G_{\kappa\lambda}\epsilon^\lambda; \qquad \mathrm{Tr}(\epsilon^\kappa E_\lambda) = \delta_{\kappa\lambda}. \tag{29}$$

Any $\alpha \in \mathrm{GF}(p^\ell)$ can be expressed in the two bases as

$$\alpha = \sum_{\lambda=0}^{\ell-1} \alpha_\lambda \epsilon^\lambda = \sum_{\lambda=0}^{\ell-1} \overline{\alpha}_\lambda E_\lambda, \tag{30}$$

where

$$\alpha_\lambda = \mathrm{Tr}[\alpha E_\lambda]; \qquad \overline{\alpha}_\lambda = \mathrm{Tr}[\alpha\epsilon^\lambda], \tag{31}$$

where $\overline{\alpha}_\lambda$ are the dual components of α related to the α_λ as

$$\alpha_\lambda = \sum_\kappa G_{\lambda\kappa}\overline{\alpha}_\kappa; \qquad \overline{\alpha}_\lambda = \sum_\kappa g_{\lambda\kappa}\alpha_\kappa. \tag{32}$$

We express the trace of any product $\alpha\beta$ in terms of their components:

$$\begin{aligned}\mathrm{Tr}(\alpha\beta) &= \sum_{\lambda,\kappa} g_{\lambda\kappa}\alpha_\lambda\beta_\kappa = \sum_{\lambda,\kappa} G_{\lambda\kappa}\overline{\alpha}_\lambda\overline{\beta}_\kappa \\ &= \sum_\lambda \alpha_\lambda\overline{\beta}_\lambda = \sum_\lambda \overline{\alpha}_\lambda\beta_\lambda. \end{aligned} \tag{33}$$

It is seen that the trace of $\alpha\beta$ involves the components of α and the dual components of β; or vice versa.

We can now show that the determinant of g is non-zero and therefore the g^{-1} exists. If the determinant of g is zero, then there exist non-zero β such that $\mathrm{Tr}(\alpha\beta) = 0$ for all α. But then for an arbitrary $\gamma \in \mathrm{GF}(p^\ell)$, we can choose $\alpha = \gamma\beta^{-1}$ and prove that $\mathrm{Tr}(\gamma) = 0$. This contradicts a theorem which states that at least one element in a Galois field has non-zero trace. Therefore the determinant of g is non-zero and the g^{-1} exists.

For the calculation of conjugates we introduce the $\ell \times \ell$ matrix $\mathcal{C}$ with elements in $\mathbb{Z}_p$ as

$$\epsilon^{\mu p} = \sum_{\kappa=0}^{\ell-1} \epsilon^\kappa \mathcal{C}_{\kappa\mu}; \qquad \kappa, \mu = 0, \ldots, \ell - 1. \tag{34}$$

Its elements do depend on the choice of the irreducible polynomial $P(\epsilon)$ in equation (1); but different choices lead to isomorphic results. The conjugates of an arbitrary number α are given by

$$\alpha^{p^\lambda} = \sum_{\kappa,\mu} \epsilon^\kappa (\mathcal{C}^\lambda)_{\kappa\mu}\alpha_\mu. \tag{35}$$

It is easily seen that

$$\mathcal{C}^\ell = \mathbf{1}; \qquad \mathcal{C}_{\kappa 0} = \delta(\kappa, 0), \tag{36}$$

where δ is the Kronecker delta.

2.7. Example

We consider the Galois field GF(9) and choose the irreducible polynomial $P(\epsilon) = \epsilon^2 + \epsilon + 2$. In this case the irreducible polynomials are

$$\begin{aligned} &f_{11}(y) = y; && f_{12}(y) = y - 1; && f_{13}(y) = y - 2 \\ &f_{21}(y) = y^2 + 1; && f_{22}(y) = y^2 + y + 2; && f_{23}(y) = y^2 + 2y + 2. \end{aligned} \tag{37}$$

The elements of GF(9) can be labelled using the first labelling method as follows:

$$\begin{aligned} &m(1,1,1) = 0; && m(1,2,1) = 1; && m(1,3,1) = 2 \\ &m(2,1,1) = 1 + 2\epsilon; && m(2,1,2) = 2 + \epsilon \\ &m(2,2,1) = \epsilon; && m(2,2,2) = 2 + 2\epsilon \\ &m(2,3,1) = 1 + \epsilon; && m(2,3,2) = 2\epsilon. \end{aligned} \tag{38}$$

These can also be labelled using the second labelling method as follows:

$$\begin{aligned} &m(1,1) = 0; && m(2,1) = 1; && m(3,1) = 2 \\ &m(4,1) = 1 + 2\epsilon; && m(4,2) = 2 + \epsilon \\ &m(5,1) = \epsilon; && m(5,2) = 2 + 2\epsilon \\ &m(6,1) = 1 + \epsilon; && m(6,2) = 2\epsilon. \end{aligned} \tag{39}$$

The matrices g, G and $\mathcal{C}$ defined in equations (28) and (34) are in this case

$$g = \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}; \qquad G = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}; \qquad \mathcal{C} = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}. \tag{40}$$

2.8. Additive characters

We use the general notation

$$\Omega_q(\alpha) \equiv \Omega_q^\alpha = \exp\left[\mathrm{i}\frac{2\pi\alpha}{q}\right]; \qquad \alpha \in \mathbb{Z}_q. \tag{41}$$

In the special case $q = p$, we use the more special notation

$$\omega(m) \equiv \omega^m = \exp\left(\mathrm{i}\frac{2\pi m}{p}\right); \qquad m \in \mathbb{Z}_p. \tag{42}$$

We consider the following complex-valued function:

$$\chi(\alpha) = \omega[\mathrm{Tr}(\alpha)]; \qquad \chi(\alpha)\chi(\beta) = \chi(\alpha+\beta); \qquad \alpha, \beta \in \mathrm{GF}(p^\ell), \tag{43}$$

where $\chi(\alpha)$ is an additive character in $\mathrm{GF}(p^\ell)$. Taking into account equation (33) we show that

$$\chi(\alpha\beta) = \omega[\mathrm{Tr}(\alpha\beta)] = \omega\left[\sum_{\lambda,\kappa} g_{\lambda\kappa}\alpha_\lambda\beta_\kappa\right] = \omega\left[\sum_\lambda \overline{\alpha}_\lambda\beta_\lambda\right] = \omega\left[\sum_\lambda \alpha_\lambda\overline{\beta}_\lambda\right]. \tag{44}$$

We also show that

$$\frac{1}{p^\ell}\sum_{\alpha\in\mathrm{GF}(p^\ell)} \chi(\alpha\beta) = \delta(\beta, 0); \qquad \beta \in \mathrm{GF}(p^\ell). \tag{45}$$

This relation plays a very important role in Fourier transforms below. A more general relation is

$$\frac{1}{p^\ell}\sum_{\alpha\in\mathrm{GF}(p^\ell)} \chi\big(\alpha\beta - \alpha^{p^\lambda}\gamma\big) = \delta\big(\beta, \gamma^{p^{\ell-\lambda}}\big) = \delta\big(\beta^{p^\lambda}, \gamma\big). \tag{46}$$

Above we have defined characters in $\mathrm{GF}(p^\ell)$. In a similar way we can define characters in the subfield $\mathrm{GF}(p^d)$ (where $d|\ell$). We consider the complex-valued function:

$$\chi_d(\alpha) = \omega[\mathrm{Tr}_d(\alpha)]; \qquad \alpha \in \mathrm{GF}(p^d), \tag{47}$$

where $\chi_d(\alpha)$ is an additive character in $\mathrm{GF}(p^d)$. Taking into account equation (26) we show that for $\alpha \in \mathrm{GF}(p^\ell)$

$$\chi(\alpha) = \chi_d[\mathrm{Tr}_{\ell/d}(\alpha)]; \qquad \alpha \in \mathrm{GF}(p^\ell). \tag{48}$$

When $\alpha \in \mathrm{GF}(p^d)$ this relation becomes

$$\chi(\alpha) = [\chi_d(\alpha)]^{\ell/d}; \qquad \alpha \in \mathrm{GF}(p^d). \tag{49}$$

We can easily extend these ideas to *diagonal* matrices with elements in $\mathrm{GF}(p^\ell)$. We consider the $N \times N$ matrix

$$\Theta_{ij} = \Theta_i\delta(i, j); \qquad \Theta_i \in \mathrm{GF}(p^\ell). \tag{50}$$

It is easily seen that

$$\Theta^{p^\ell} = \Theta. \tag{51}$$

The matrix Θ can be written as

$$\Theta = \Theta_0 + \Theta_1\epsilon + \cdots + \Theta_{\ell-1}\epsilon^{\ell-1}, \tag{52}$$

where Θ_λ are $N \times N$ diagonal matrices with elements in $\mathbb{Z}_p$. We define the Galois trace of Θ as

$$\mathrm{Tr}_\mathrm{G}\Theta = \Theta + \Theta^p + \cdots + \Theta^{p^{\ell-1}}; \qquad [\mathrm{Tr}_\mathrm{G}\Theta]^p = \mathrm{Tr}_\mathrm{G}\Theta. \tag{53}$$

The Galois trace is another $N \times N$ diagonal matrix with elements in $\mathbb{Z}_p$; and it is a different concept from the ordinary trace of a matrix, which is a number. Taking into account equation (33) we easily show that if Θ and Φ are two diagonal matrices with elements in $\mathrm{GF}(p^\ell)$ then

$$\mathrm{Tr}_{\mathrm{G}}(\Theta\Phi) = \sum_{\lambda,\mu} g_{\lambda\mu}\Theta_\lambda\Phi_\mu. \tag{54}$$

We can define the character of Θ which is another diagonal matrix with elements which are complex numbers:

$$\chi(\Theta) = \exp\left(\frac{\mathrm{i}2\pi}{p}\mathrm{Tr}_{\mathrm{G}}\Theta\right). \tag{55}$$

3. Finite quantum systems

We consider a quantum system where position and momentum take values in $\mathbb{Z}_q$. An orthonormal basis in this system consists of the position states $|\mathcal{X}; m\rangle$, where $m \in \mathbb{Z}_q$. Here $\mathcal{X}$ is not a variable, it simply indicates position states. The Hilbert space $\mathcal{H}$ of this system is q dimensional. The theory of these systems has been reviewed in [41]. Here we introduce very briefly some basic concepts which are needed later and define the notation.

3.1. Fourier transform

The Fourier operator is a unitary operator defined as

$$\mathcal{F} = q^{-1/2} \sum_{m,n\in\mathbb{Z}_q} \Omega_q(mn)|\mathcal{X}; m\rangle\langle\mathcal{X}; n|; \qquad \mathcal{F}^4 = \mathbf{1}. \tag{56}$$

Acting with the Fourier operator on the position states we get momentum states which form another orthonormal basis

$$|\mathcal{P}; m\rangle = \mathcal{F}|\mathcal{X}; m\rangle = q^{-1/2} \sum_{n\in\mathbb{Z}_q} \Omega_q(mn)|\mathcal{X}; n\rangle. \tag{57}$$

Here $\mathcal{P}$ is not a variable; it simply indicates momentum states.

Position and momentum operators $\hat{\mathcal{Q}}$ and $\hat{\mathcal{P}}$ are defined as

$$\hat{\mathcal{Q}} = \sum_{n\in\mathbb{Z}_q} n|\mathcal{X}; n\rangle\langle\mathcal{X}; n|; \qquad \hat{\mathcal{P}} = \sum_{n\in\mathbb{Z}_q} n|\mathcal{P}; n\rangle\langle\mathcal{P}; n|; \qquad \hat{\mathcal{P}} = \mathcal{F}\hat{\mathcal{Q}}\mathcal{F}^\dagger. \tag{58}$$

Since n are integers modulo q, the $\hat{\mathcal{Q}}$ and $\hat{\mathcal{P}}$ are defined modulo $q\mathbf{1}$. However, below we will use exponentials of these operators and they are single-valued.

3.2. Displacements in the $\mathbb{Z}_q \times \mathbb{Z}_q$ phase space

The position-momentum phase space of this system is the toroidal lattice $\mathbb{Z}_q \times \mathbb{Z}_q$. In this phase space, we define the displacement operators

$$\begin{aligned} \mathcal{Z}(\alpha) &= \Omega_q(\alpha\hat{\mathcal{Q}}) = \sum_{n\in\mathbb{Z}_q} \Omega_q(n\alpha)|\mathcal{X}; n\rangle\langle\mathcal{X}; n| \\ \mathcal{X}(\beta) &= \Omega_q(-\beta\hat{\mathcal{P}}) = \sum_{n\in\mathbb{Z}_q} \Omega_q(-n\beta)|\mathcal{P}; n\rangle\langle\mathcal{P}; n|; \qquad \alpha, \beta \in \mathbb{Z}_q. \end{aligned} \tag{59}$$

Acting with these operators on position and momentum states we get

$$\begin{aligned}&\mathcal{Z}(\alpha)|\mathcal{P};m\rangle = |\mathcal{P};m+\alpha\rangle; \qquad &&\mathcal{Z}(\alpha)|\mathcal{X};m\rangle = \Omega_q(\alpha m)|\mathcal{X};m\rangle\\ &\mathcal{X}(\beta)|\mathcal{P};m\rangle = \Omega_q(-m\beta)|\mathcal{P};m\rangle; \qquad &&\mathcal{X}(\beta)|\mathcal{X};m\rangle = |\mathcal{X};m+\beta\rangle.\end{aligned} \tag{60}$$

The displacement operators obey the relations

$$\mathcal{X}(\beta)\mathcal{Z}(\alpha) = \mathcal{Z}(\alpha)\mathcal{X}(\beta)\Omega_q(-\alpha\beta); \qquad \alpha,\beta\in\mathbb{Z}_q. \tag{61}$$

General displacement operators are given by

$$\mathcal{D}(\alpha,\beta) = \mathcal{Z}(\alpha)\mathcal{X}(\beta)\Omega_q(-2^{-1}\alpha\beta). \tag{62}$$

Multiplication of two such operators is given by

$$\mathcal{D}(\alpha_1,\beta_1)\mathcal{D}(\alpha_2,\beta_2) = \mathcal{D}(\alpha_1+\alpha_2,\beta_1+\beta_2)\Omega_q[2^{-1}(\alpha_1\beta_2-\alpha_2\beta_1)]. \tag{63}$$

The operators $\mathcal{D}(\alpha,\beta)$ form the Heisenberg–Weyl group.

4. Galois quantum systems

A Galois quantum system consists of ℓ-component systems with p-dimensional Hilbert space $\mathcal{H}$. Its Hilbert space H is the tensor product

$$H = \mathcal{H}\otimes\cdots\otimes\mathcal{H}. \tag{64}$$

We use calligraphic letters for operators and states on the various p-dimensional Hilbert spaces $\mathcal{H}$, and ordinary letters for operators and states on the p^ℓ-dimensional Hilbert space H. We stress from the outset that only special couplings between the component systems can give the system 'Galois structure'. This is explained later when we discuss Fourier transform and the Hamiltonians of these systems.

The position states $|X;m\rangle$ in H, are by definition

$$|X;m\rangle \equiv |\mathcal{X};m_0\rangle\otimes\cdots\otimes|\mathcal{X};m_{\ell-1}\rangle; \qquad m = m_0+m_1\epsilon+\cdots+m_{\ell-1}\epsilon^{\ell-1}, \tag{65}$$

where $m\in\mathrm{GF}(p^\ell)$ and $m_0,\ldots,m_{\ell-1}\in\mathbb{Z}_p$.

4.1. Frobenius subspaces

We consider the following d-dimensional subspace of H:

$$\mathfrak{H}_{d\kappa} = \mathrm{span}\{|X;m(d,\kappa,1)\rangle, |X;m(d,\kappa,2)\rangle,\ldots,|X;m(d,\kappa,d)\rangle\}. \tag{66}$$

This space is spanned by all position states labelled with Galois conjugate numbers. There is one-to-one map between the 'Frobenius subspaces' $\mathfrak{H}_{d\kappa}$ and the irreducible polynomials $f_{d\kappa}(y)$ corresponding to these conjugates. The indices of $\mathfrak{H}_{d\kappa}$ indicate the corresponding irreducible polynomial. There are $\mathfrak{M}(\ell,p)$ Frobenius subspaces (see equation (13)) and their direct sum is the space H.

We have introduced earlier a second method of labelling irreducible polynomials where the indices (d,κ) are replaced with the index $\mathfrak{N}$. The one-to-one map between the two has been given in equations (19) and (20). With this notation equation (66) can be rewritten as

$$\mathfrak{H}_{\mathfrak{N}} = \mathrm{span}\{|X;m(\mathfrak{N},1)\rangle, |X;m(\mathfrak{N},2)\rangle,\ldots,|X;m(\mathfrak{N},d)\rangle\}. \tag{67}$$

We call $\pi_{d\kappa}$ (or $\pi_{\mathfrak{N}}$) the projection operators to the spaces $\mathfrak{H}_{d\kappa}$.

$$\pi_{d\kappa}\pi_{d'\kappa'} = \delta(d,d')\delta(\kappa,\kappa'); \qquad \sum_{d,\kappa}\pi_{d\kappa} = \mathbf{1}. \tag{68}$$

As an example, we consider a Galois quantum system where position and momentum take values in GF(9). For calculations we choose the irreducible polynomial $P(\epsilon) = \epsilon^2 + \epsilon + 2$. Taking into account equations (38) and (39) we see that the Frobenius subspaces are

$$\begin{aligned} \mathfrak{H}_{11} &= \mathfrak{H}_1 = \{|X; 0\rangle\} \\ \mathfrak{H}_{12} &= \mathfrak{H}_2 = \{|X; 1\rangle\} \\ \mathfrak{H}_{13} &= \mathfrak{H}_3 = \{|X; 2\rangle\} \\ \mathfrak{H}_{21} &= \mathfrak{H}_4 = \text{span}\{|X; 1 + 2\epsilon\rangle, |X; 2 + \epsilon\rangle\} \\ \mathfrak{H}_{22} &= \mathfrak{H}_5 = \text{span}\{|X; \epsilon\rangle, |X; 2 + 2\epsilon\rangle\} \\ \mathfrak{H}_{23} &= \mathfrak{H}_6 = \text{span}\{|X; 1 + \epsilon\rangle, |X; 2\epsilon\rangle\}. \end{aligned} \tag{69}$$

We have used here both labelling methods.

4.2. G_d-subsystems

We consider a Galois subsystem where the position and momentum take values in the subfield GF(p^d), where $d|\ell$. Its Hilbert space is a p^d-dimensional subspace of H which we denote as H_d. We call it G_d-subsystem. An example is the G_1-subsystem where the position and momentum take values in the subfield $\mathbb{Z}_p$.

We call Π_d the projection operator to the subspace H_d. An important aspect of Galois theory is the relationship of a field with its subfields, and in the present context we discuss throughout the paper the relationship between the formalism in the G-system and the corresponding formalism in the G_d-subsystem.

It is easily seen that

$$H_d = \bigoplus_{e|d} \bigoplus_{\kappa=1}^{n(e,p)} \mathfrak{H}_{d\kappa} = \bigoplus_{e|d} \bigoplus_{\mathfrak{N}} \mathfrak{H}_{\mathfrak{N}}; \qquad \mathfrak{N} = w(\ell, e, p) + 1, \ldots, w(\ell, e, p) + n(e, p). \tag{70}$$

In the special case $d = 1$ the space H_1 is p dimensional and is spanned by position states labelled with integers in $\mathbb{Z}_p$. In the other extreme special case $d = \ell$ it is clear that $H_\ell = H$.

A direct consequence of equation (70) is that

$$\Pi_d = \sum_{e|d} \sum_{\kappa=1}^{n(e,p)} \pi_{e\kappa} = \sum_{e|d} \sum_{\mathfrak{N}=w(\ell,e,p)+1}^{w(\ell,e,p)+n(e,p)} \pi_{\mathfrak{N}}. \tag{71}$$

Also if e is a divisor of d then

$$e|d \rightarrow \Pi_e \Pi_d = \Pi_e. \tag{72}$$

5. Fourier transform

The Fourier transform in a Galois quantum system is given in terms of the additive characters of equation (43) as

$$\begin{aligned} F &= (p^\ell)^{-1/2} \sum_{m,n \in \text{GF}(p^\ell)} \chi(mn) |X; m\rangle\langle X; n| \\ &= (p^\ell)^{-1/2} \sum_{m_\lambda, n_\kappa} \omega\left(\sum g_{\lambda\kappa} m_\lambda n_\kappa\right) |\mathcal{X}; m_0\rangle\langle\mathcal{X}; n_0| \otimes \cdots \otimes |\mathcal{X}; m_0\rangle\langle\mathcal{X}; n_0|. \end{aligned} \tag{73}$$

The non-diagonal terms of g_{ij} describe the coupling between the (i, j) components. This is also seen later in the Hamiltonian of the system which is a function of the position and momentum operators, or equivalently of the position and Fourier operators.

There is some analogy between this system and a system of ℓ coupled harmonic oscillators, but there are two important differences. The first is that here we cannot diagonalize the matrix g (because it has elements in $\mathbb{Z}_p$). The second is that here the matrix g is *not* arbitrary, it is intimately related to Galois theory through equation (28). Only a very specific coupling between the components of the system, described by the matrix g of equation (28), gives it the Galois structure.

If we consider an arbitrary matrix g (with elements in $\mathbb{Z}_p$) we will get a coupled finite quantum system which is *not* a Galois quantum system. Its position and momentum take values in the ring $[\mathbb{Z}_p]^\ell \equiv \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ and we call it the R-system. This system does not have the extra properties that distinguish a Galois quantum system from other finite quantum systems (finite geometry as phase space, symplectic transformations, quantum tomography, Frobenius transformations, etc). Later, we consider an R-system with Fourier transform given by equation (73) with $g = \mathbf{1}$. We compare and contrast the properties of R-systems with those of G-systems.

Acting with F on position states we get momentum states in G-systems:

$$\begin{aligned}|P; m\rangle = F|X; m\rangle &= F[|\mathcal{X}; m_0\rangle \otimes \cdots \otimes |\mathcal{X}; m_{\ell-1}\rangle] \\ &= |\mathcal{P}; \overline{m}_0\rangle \otimes \cdots \otimes |\mathcal{P}; \overline{m}_{\ell-1}\rangle.\end{aligned} \tag{74}$$

The dual components $\overline{m}_\lambda$ of m enter in the component momentum states, while the components m_λ enter in the component position states of equation (65).

We can show that

$$F^4 = \mathbf{1}. \tag{75}$$

This implies that the eigenvalues of F are $1, i, -1, -i$. We call η_r the orthogonal projectors to the eigenspaces corresponding to the various eigenvalues of F. Then

$$\begin{aligned}&F = \eta_0 + \mathrm{i}\eta_1 - \eta_2 - i\eta_3 \\ &\eta_r\eta_s = \eta_r\delta(r, s); \qquad \eta_0 + \eta_1 + \eta_2 + \eta_3 = \mathbf{1}; \qquad r, s = 0, 1, 2, 3.\end{aligned} \tag{76}$$

The projectors η_r can be expressed in terms of the Fourier operator as

$$\eta_r = \tfrac{1}{4}[\mathbf{1} + (\mathrm{i}^{-r}F) + (\mathrm{i}^{-r}F)^2 + (\mathrm{i}^{-r}F)^3]; \qquad r = 0, 1, 2, 3. \tag{77}$$

5.1. Position and momentum operators

The position operator is

$$\hat{Q} = \sum_m m|X; m\rangle\langle X; m| = \sum_\lambda \epsilon^\lambda[\mathbf{1} \otimes \cdots \otimes \hat{\mathcal{Q}}_\lambda \otimes \cdots \otimes \mathbf{1}]. \tag{78}$$

The momentum operator is given by

$$\begin{aligned}\hat{P} = F\hat{Q}F^\dagger &= \sum_m m|P; m\rangle\langle P; m| = \sum_\lambda E_\lambda[\mathbf{1} \otimes \cdots \otimes \hat{\mathcal{P}}_\lambda \otimes \cdots \otimes \mathbf{1}] \\ &= \sum_{\lambda,\mu} G_{\lambda\mu}\epsilon^\mu[\mathbf{1} \otimes \cdots \otimes \hat{\mathcal{P}}_\mu \otimes \cdots \otimes \mathbf{1}].\end{aligned} \tag{79}$$

It involves the Fourier transform of equation (73) and the special coupling associated with the off-diagonal elements of the matrix g, which we discussed earlier. Consequently, functions of the position and momentum operators $\hat{Q}$ and $\hat{P}$:

$$\varphi = \varphi(\hat{Q}, \hat{P}) = \varphi(\hat{Q}, F\hat{Q}F^\dagger) \tag{80}$$

embody this particular coupling and can be used in the description of Galois systems. More general functions of the ℓ positions $\hat{\mathcal{Q}}_\lambda$ and the ℓ momenta $\hat{\mathcal{P}}_\lambda$

$$\varphi' = \varphi'(\hat{\mathcal{Q}}_0, \hat{\mathcal{P}}_0; \ldots; \hat{\mathcal{Q}}_{\ell-1}, \hat{\mathcal{P}}_{\ell-1}) \tag{81}$$

describe general coupling between the component systems, and are suitable for R-systems. We discuss this point further below, in connection with the Hamiltonians.

The eigenvalues of $\hat{Q}$ and $\hat{P}$ are elements of GF(p^ℓ) and their characteristic equation is

$$\hat{Q}^{p^\ell} = \hat{Q}; \qquad \hat{P}^{p^\ell} = \hat{P}. \tag{82}$$

We note that there are difficulties in practical calculations that involve the matrices $\hat{Q}$ and $\hat{P}$. For example, if we want to change basis, we need to define multiplication of elements of GF(p^ℓ) with complex numbers.

The Galois traces of these operators are defined as (see equation (53)):

$$\begin{aligned} &\mathrm{Tr_G}\,\hat{Q} = \hat{Q} + \hat{Q}^p + \cdots + \hat{Q}^{p^{\ell-1}} = \sum_m (\mathrm{Tr}\,m)|X; m\rangle\langle X; m| \\ &[\mathrm{Tr_G}\,\hat{Q}]^p = \mathrm{Tr_G}\,\hat{Q} \end{aligned} \tag{83}$$

and similarly for $\mathrm{Tr_G}\,\hat{P}$. In practical calculations, they also have similar problems. For example, if we want to change basis, we need to multiply integers defined modulo p, with complex numbers. This leads to multivaluedness and it needs to be handled very carefully. All these difficulties disappear if we work with characters of these matrices which are matrices of complex numbers. We explain this below in examples that involve the $\hat{Q}^2$ and $\hat{P}^2$ which will be used later in Hamiltonians for these systems.

We consider the matrix $\hat{Q}^2$ which in the basis of position states is a $p^\ell \times p^\ell$ diagonal matrix with elements in GF(p^ℓ). The Galois trace of $\hat{Q}^2$ is a diagonal $p^\ell \times p^\ell$ matrix with elements in $\mathbb{Z}_p$, and using equation (54) we show that

$$\begin{aligned} \mathrm{Tr_G}\,\hat{Q}^2 &= \sum_m (\mathrm{Tr}\,m^2)|X; m\rangle\langle X; m| \\ &= \sum_{\lambda,\mu\in\mathbb{Z}_\ell} g_{\lambda\mu} \mathbf{1}\otimes\cdots\otimes\hat{\mathcal{Q}}_\lambda\otimes\cdots\otimes\hat{\mathcal{Q}}_\mu\otimes\cdots\otimes\mathbf{1}. \end{aligned} \tag{84}$$

The diagonal $g_{\lambda\lambda}$ are related to terms of the type $\mathbf{1}\otimes\cdots\otimes\hat{\mathcal{Q}}^2_{(\lambda)}\otimes\cdots\otimes\mathbf{1}$. The non-diagonal $g_{\lambda\mu}$ are related to the coupling between the components in these systems. We stress again that g is not an arbitrary matrix, it is intimately related to Galois theory through equation (28). The character of $\hat{Q}^2$ is given by

$$\chi(\hat{Q}^2) = \exp\left(\frac{\mathrm{i}2\pi}{p}\mathrm{Tr_G}\,\hat{Q}^2\right) = \sum_m \chi(m^2)|X; m\rangle\langle X; m|. \tag{85}$$

It is a diagonal $p^\ell \times p^\ell$ matrix with complex elements and it is free of the problems that we mentioned above. We can now change basis if we wish, without any difficulty. For example, we can go to the basis of momentum states with the Fourier transform:

$$\begin{aligned} &\chi(\hat{Q}^2) = \sum_{k,n} \gamma_{kn}|P; k\rangle\langle P; n| \\ &\gamma_{kn} = \sum_{m\in\mathrm{GF}(p^\ell)} \chi(m^2)\chi[m(n-k)] = \chi[2^{-2}(n-k)^2]G(1), \end{aligned} \tag{86}$$

where

$$G(A) = \sum_{r\in\mathrm{GF}(p^\ell)} \chi(Ar^2) \tag{87}$$

is the Gauss sum related to GF(p^ℓ) [51].

In a similar way we can define in the basis of momentum states the Galois trace of $\hat{P}^2$

$$\begin{aligned}\mathrm{Tr}_{\mathrm{G}}\hat{P}^2 &= \sum_m (\mathrm{Tr}\, m^2)|P; m\rangle\langle P; m| \\ &= \sum_{\lambda,\mu\in\mathbb{Z}_\ell} G_{\lambda\mu}\mathbf{1}\otimes\cdots\otimes\hat{\mathcal{P}}_\lambda\otimes\cdots\otimes\hat{\mathcal{P}}_\mu\otimes\cdots\otimes\mathbf{1}\end{aligned} \tag{88}$$

and the character

$$\chi(\hat{P}^2) = F\chi(\hat{Q}^2)F^\dagger = \exp\left(\frac{\mathrm{i}2\pi}{p}\mathrm{Tr}_{\mathrm{G}}\hat{P}^2\right) = \sum_m \chi(m^2)|P; m\rangle\langle P; m|. \tag{89}$$

For later use we consider the

$$\begin{aligned}\chi(\hat{Q}^2)\chi(\hat{P}^2) &= G(1)\sum_{k,n}\chi[2^{-2}(n-k)^2+n^2]|P; k\rangle\langle P; n| \\ \chi(\hat{P}^2)\chi(\hat{Q}^2) &= G(1)\sum_{k,n}\chi[2^{-2}(n-k)^2+k^2]|P; k\rangle\langle P; n|.\end{aligned} \tag{90}$$

Their analogues in the harmonic oscillator context are $\exp(\mathrm{i}\alpha x^2)\exp(\mathrm{i}\beta p^2)$ and $\exp(\mathrm{i}\alpha x^2)\exp(\mathrm{i}\beta p^2)$ (where x and p are here harmonic oscillator position and momentum operators, correspondingly). We can find relations between them using the harmonic oscillator commutation relation $[x, p] = \mathrm{i}\mathbf{1}$. As we explain below, in the present context the Heisenberg–Weyl group is discrete, there is no Lie algebra and the commutator $[Q, P]$ plays no important role. Consequently, there is no simple relation between $\chi(\hat{Q}^2)\chi(\hat{P}^2)$ and $\chi(\hat{P}^2)\chi(\hat{Q}^2)$.

5.2. *Fourier transform in G_d-subsystems*

The Hilbert space H_d is spanned by the position states $|X; m\rangle$, where $m \in \mathrm{GF}(p^d)$. We also use the notation $|X_d; m\rangle$ for them:

$$|X_d; m\rangle = |X; m\rangle; \qquad m \in \mathrm{GF}(p^d). \tag{91}$$

The Fourier transform F_d in H_d is defined in terms of the additive characters of equation (47) as

$$F_d = (p^d)^{-1/2}\sum_{m,n\in\mathrm{GF}(p^d)}\chi_d(mn)|X; m\rangle\langle X; n|; \qquad F_d^4 = \Pi_d, \tag{92}$$

where Π_d is the projection operator to the subspace H_d. The momentum states $|P_d; m\rangle$ are given by

$$|P_d; m\rangle = F_d|X_d; m\rangle = (p^d)^{-1/2}\sum_{n\in\mathrm{GF}(p^d)}\chi_d(mn)|X; n\rangle; \qquad m \in \mathrm{GF}(p^d) \tag{93}$$

and they are different from the corresponding momentum states $|P; m\rangle$. Indeed the state $|P_d; m\rangle$ belongs entirely in the space H_d, while a part of the state $|P; m\rangle$ is outside H_d:

$$(\mathbf{1}-\Pi_d)|P; m\rangle = p^{-\ell/2}\sum_n \chi(mn)|X; n\rangle; \qquad n \in \mathrm{GF}(p^\ell) - \mathrm{GF}(p^d); \qquad m \in \mathrm{GF}(p^d). \tag{94}$$

The matrix $\Pi_d F \Pi_d$ is different from the matrix F_d. We calculate the matrix elements of these two matrices and using equation (49) we find that for $m, n \in \mathrm{GF}(p^d)$:

$$\langle X; m|\Pi_d F\Pi_d|X; n\rangle = [\langle X; m|F_d|X; n\rangle]^{\ell/d}; \qquad m, n \in \mathrm{GF}(p^d). \tag{95}$$

5.3. Fourier transform in the Frobenius subspaces

For later use we introduce a Fourier transform within the d-dimensional Frobenius subspace $\mathfrak{H}_{d\kappa}$ as

$$\mathfrak{F}_{d\kappa} = d^{-1/2} \sum_{\nu,\mu\in\mathbb{Z}_d} \Omega_d(\nu\mu)|X; m(d,\kappa,\nu)\rangle\langle X; m(d,\kappa,\mu)|; \qquad \mathfrak{F}_{d\kappa}^4 = \pi_{d\kappa}. \tag{96}$$

Acting with it on the states $|X; m(d,\kappa,\nu)\rangle$ we get the states

$$|\mathfrak{P}; m(d,\kappa,\mu)\rangle\rangle = \mathfrak{F}_{d\kappa}|X; m(d,\kappa,\mu)\rangle = d^{-1/2} \sum_{\nu\in\mathbb{Z}_d} \Omega_d(\nu\mu)|X; m(d,\kappa,\nu)\rangle. \tag{97}$$

We might call them 'momentum states with respect to the $\mathfrak{F}_{d\kappa}$ Fourier transform'. We stress that the $|\mathfrak{P}; m(d,\kappa,\mu)\rangle\rangle$ are different from the states $|P; m\rangle$. In the special case $d = 1$, we get

$$\mathfrak{F}_{1\kappa} = \pi_{1\kappa}; \qquad |\mathfrak{P}; m(1,\kappa,1)\rangle\rangle = |X; m(1,\kappa,1)\rangle\rangle. \tag{98}$$

In the example related to GF(9) considered in equations (38) and (69) we get:

$$\begin{aligned}
&|\mathfrak{P}; m(1,1,1)\rangle\rangle = |X; 0\rangle\\
&|\mathfrak{P}; m(1,2,1)\rangle\rangle = |X; 1\rangle\\
&|\mathfrak{P}; m(1,3,1)\rangle\rangle = |X; 2\rangle\\
&|\mathfrak{P}; m(2,1,1)\rangle\rangle = 2^{-1/2}\,[-|X; 1+2\epsilon\rangle + |X; 2+\epsilon\rangle]\\
&|\mathfrak{P}; m(2,1,2)\rangle\rangle = 2^{-1/2}\,[|X; 1+2\epsilon\rangle + |X; 2+\epsilon\rangle]\\
&|\mathfrak{P}; m(2,2,1)\rangle\rangle = 2^{-1/2}\,[-|X; \epsilon\rangle + |X; 2+\epsilon\rangle]\\
&|\mathfrak{P}; m(2,2,2)\rangle\rangle = 2^{-1/2}\,[|X; \epsilon\rangle + |X; 2+\epsilon\rangle]\\
&|\mathfrak{P}; m(2,3,1)\rangle\rangle = 2^{-1/2}\,[-|X; 1+\epsilon\rangle + |X; 2\epsilon\rangle]\\
&|\mathfrak{P}; m(2,3,2)\rangle\rangle = 2^{-1/2}\,[|X; 1+\epsilon\rangle + |X; 2\epsilon\rangle]\,.
\end{aligned} \tag{99}$$

6. Hamiltonians of Galois quantum systems

The Hamiltonian of a Galois quantum system is

$$h = h(\hat{Q}, \hat{P}) = h(\hat{Q}, F\hat{Q}F^{\dagger}). \tag{100}$$

It is a function of $\hat{Q}$ and $\hat{P}$ which embody Galois theory as we explained earlier. In other words, h is a function of $\hat{Q}$ and F and it involves the special coupling associated with the Fourier transform of equation (73), which we discussed earlier. The Hamiltonian h is a very special case of the more general Hamiltonian

$$h' = h'(\hat{\mathcal{Q}}_0, \hat{\mathcal{P}}_0; \ldots; \hat{\mathcal{Q}}_{\ell-1}, \hat{\mathcal{P}}_{\ell-1}), \tag{101}$$

which involves the arbitrary coupling between the ℓ components of the system. This system is *not* a Galois system, it is an R-system (discussed briefly later). Only the specialized class of Hamiltonians of equation (100), which involves the Fourier transform of equation (73), can give the system Galois structure.

As examples we consider the $\chi(\hat{Q}^2)\chi(\hat{P}^2)$ and the $\chi(\hat{P}^2)\chi(\hat{Q}^2)$ of equation (90). These are complex matrices and their logarithms can be used as Hamiltonians of the system

$$h_A = \ln[\chi(\hat{Q}^2)\chi(\hat{P}^2)]; \qquad h_B = \ln[\chi(\hat{P}^2)\chi(\hat{Q}^2)]. \tag{102}$$

Table 1. The evolution operator $[\mathfrak{U}_A(1)]_P(m,n)$ of equation (106) in the basis of momentum states for a Galois quantum system which has position and momentum in GF(9). In the calculations we choose the irreducible polynomial $P(\epsilon)=\epsilon^2+\epsilon+2$. In the table $r=1/3$ and $w=\exp(\mathrm{i}2\pi/3)/3$.

	0	ϵ	2ϵ	1	$1+\epsilon$	$1+2\epsilon$	2	$2+\epsilon$	$2+2\epsilon$
0	r	r	r	r	r	r	r	r	r
ϵ	r	r	r	w	w	w	w^*	w^*	w^*
2ϵ	r	r	r	w^*	w^*	w^*	w	w	w
1	w	w^*	r	w^*	r	w	r	w	w^*
$1+\epsilon$	r	w	w^*	w^*	r	w	w	w^*	r
$1+2\epsilon$	w^*	r	w	w^*	r	w	w^*	r	w
2	w	r	w^*	r	w^*	w	w^*	w	r
$2+\epsilon$	w^*	w	r	w^*	w	r	w^*	w	r
$2+2\epsilon$	r	w^*	w	w	r	w^*	w^*	w	r

The logarithm of a matrix is of course multivalued, and a choice has to be made which of these describes the system (e.g., the principal matrix logarithm).

The evolution operator for the system is then

$$\mathfrak{U}_A(t)=\exp(\mathrm{i}th_A)=[\chi(\hat{Q}^2)\chi(\hat{P}^2)]^t;\qquad \mathfrak{U}_B(t)=\exp(\mathrm{i}th_B)=[\chi(\hat{P}^2)\chi(\hat{Q}^2)]^t. \tag{103}$$

A more general Hamiltonian is

$$h_C=\ln\{[\chi(\hat{Q}^2)]^\sigma\chi(\hat{P}^2)[\chi(\hat{Q}^2)]^{1-\sigma}\};\qquad 0\leqslant\sigma\leqslant 1. \tag{104}$$

All these Hamiltonians are analogues of the $h=(x^2+p^2)/2$ of the harmonic oscillator. Below (in equation (151)) we will act with displacement and symplectic transformations on these Hamiltonians to get the analogue of the squeezed and displaced harmonic oscillator $h=\alpha_1x^2+\alpha_2p^2+\alpha_3xp+\alpha_4x+\alpha_5p$.

6.1. Example

As a numerical example, we consider a Galois quantum system which has position and momentum in GF(9). We choose the irreducible polynomial $P(\epsilon)=\epsilon^2+\epsilon+2$. Equations (40), (84) and (88) show that in this case

$$\mathrm{Tr_G}\,\hat{Q}^2=-\hat{\mathcal{Q}}^2\otimes\mathbf{1}-2\hat{\mathcal{Q}}\otimes\hat{\mathcal{Q}}\qquad \mathrm{Tr_G}\,\hat{P}^2=-2\hat{\mathcal{P}}\otimes\hat{\mathcal{P}}+\mathbf{1}\otimes\hat{\mathcal{P}}^2. \tag{105}$$

We have calculated numerically the operators $\chi(\hat{Q}^2)$ and $\chi(\hat{P}^2)$ in the basis of momentum states. For the Hamiltonian h_A of equation (102), we present in table 1 the evolution operator at $t=1$:

$$[\mathfrak{U}_A(1)]_P(m,n)=\langle P;m|\mathfrak{U}_A(1)|P;n\rangle=\langle P;m|\exp(\mathrm{i}h_A)|P;n\rangle. \tag{106}$$

7. Displacements and the HW[GF(p^ℓ)] Heisenberg–Weyl group

Displacement operators in Galois systems are similar to those in equation (59) but they involve the additive characters of equation (43):

$$\begin{aligned}Z(\alpha)&=\omega[\mathrm{Tr_G}(\alpha\hat{Q})]=\sum_{n\in\mathrm{GF}(p^\ell)}\chi(\alpha n)|X;n\rangle\langle X;n|\\ X(\beta)&=\omega[-\mathrm{Tr_G}(\beta\hat{P})]=\sum_{n\in\mathrm{GF}(p^\ell)}\chi(-\beta n)|P;n\rangle\langle P;n|;\qquad \alpha,\beta\in\mathrm{GF}(p^\ell).\end{aligned} \tag{107}$$

The $Z(\alpha)$ and $X(\beta)$ are $p^\ell \times p^\ell$ matrices with eigenvalues which are powers of ω. Therefore they have at most p distinct eigenvalues (there is a large degeneracy). It is easily seen that

$$Z(\alpha_1)Z(\alpha_2) = Z(\alpha_1 + \alpha_2); \qquad X(\beta_1)X(\beta_2) = X(\beta_1 + \beta_2). \tag{108}$$

These operators act on position and momentum states as follows:

$$Z(\alpha)|P;m\rangle = |P;m+\alpha\rangle; \qquad Z(\alpha)|X;m\rangle = \chi(\alpha m)]|X;m\rangle \tag{109}$$

$$X(\beta)|P;m\rangle = \chi(-m\beta)]|P;m\rangle; \qquad X(\beta)|X;m\rangle = |X;m+\beta\rangle. \tag{110}$$

Using them we show that

$$X(\beta)Z(\alpha) = Z(\alpha)X(\beta)\chi(-\alpha\beta). \tag{111}$$

General displacement in the GF(p^ℓ) × GF(p^ℓ) phase space is defined as

$$D(\alpha,\beta) = Z(\alpha)X(\beta)\chi(-2^{-1}\alpha\beta); \qquad [D(\alpha,\beta)]^\dagger = D(-\alpha,-\beta). \tag{112}$$

We note that $2^{-1}\alpha\beta$ is an element of GF(p^ℓ). We easily show that

$$D(\alpha,\beta)D(\gamma,\delta) = \chi[2^{-1}(\alpha\delta - \beta\gamma)]D(\alpha+\gamma,\beta+\delta). \tag{113}$$

The displacement operators $D(\alpha,\beta)\chi(\gamma)$ form the Heisenberg–Weyl group HW[GF(p^ℓ)], which has $p^{3\ell}$ elements. We note that in finite quantum systems there are no infinitesimal displacements; the Heisenberg–Weyl group is finite; there is no Lie algebra; the role of the position and momentum operators Q, P is limited, and the commutator $[Q,P]$ plays no important role.

We can easily show that

$$FD(\alpha,\beta)F^\dagger = D(\beta,-\alpha). \tag{114}$$

The matrix elements of the displacements operators are given by

$$\begin{aligned}\langle X;n|D(\alpha,\beta)|X;m\rangle &= \chi(2^{-1}\alpha\beta + \alpha m)\delta(n,m+\beta)\\ \langle P;n|D(\alpha,\beta)|P;m\rangle &= \chi(-2^{-1}\alpha\beta - \beta m)\delta(n,m+\alpha).\end{aligned} \tag{115}$$

The displacement operators acting on H are expressed in terms of the displacement operators $\mathcal{D}$ acting on the various components of the system as

$$D(\alpha,\beta) = \mathcal{D}(\overline{\alpha}_0,\beta_0)\otimes\cdots\otimes\mathcal{D}(\overline{\alpha}_{\ell-1},\beta_{\ell-1}). \tag{116}$$

It is seen that the various subsystems are displaced by the corresponding dual components of α and by the components of β. This is a consequence of the coupling between the components in G-systems. Equation (116) should be compared and contrasted with the analogous for R-systems given later (in equation (189)). Special cases of equation (116) are

$$\begin{aligned}X(\epsilon^i) &= \mathbf{1}\otimes\cdots\otimes\mathbf{1}\otimes\mathcal{X}(1)\otimes\mathbf{1}\otimes\cdots\otimes\mathbf{1}\\ Z(E_i) &= \mathbf{1}\otimes\cdots\otimes\mathbf{1}\otimes\mathcal{Z}(1)\otimes\mathbf{1}\otimes\cdots\otimes\mathbf{1}.\end{aligned} \tag{117}$$

The trace of $D(\alpha,\beta)$ is given by

$$\frac{1}{p^\ell}\mathrm{tr}[D(\alpha,\beta)] = \delta(\alpha,0)\delta(\beta,0), \tag{118}$$

where 'tr' denotes the usual trace of an operator.

An important property of the displacement operators is the 'generalized resolution of the identity'. For an arbitrary operator Θ we can show that

$$\frac{1}{p^\ell}\sum_{\alpha,\beta\in\mathrm{GF}(p^\ell)} D(\alpha,\beta)\frac{\Theta}{\mathrm{tr}\Theta}[D(\alpha,\beta)]^\dagger = \mathbf{1}. \tag{119}$$

This is easily proved by calculating the matrix elements of both sides using equation (115). In the special case that $\Theta = |s\rangle\langle s|$, where $|s\rangle$ is any state in H, it reduces to the resolution of the identity

$$\frac{1}{p^{\ell}} \sum_{\alpha,\beta\in \mathrm{GF}(p^{\ell})} |\alpha, \beta; s\rangle\langle \alpha, \beta; s| = \mathbf{1}; \qquad |\alpha, \beta; s\rangle \equiv D(\alpha, \beta)|s\rangle. \tag{120}$$

The $p^{2\ell}$ states $|\alpha, \beta; s\rangle$ form an overcomplete set of states in H, analogous to coherent states in the harmonic oscillator context.

We next consider the displacement operators $D(\alpha, \beta)\chi(\gamma)$, where α, β, γ are in the subfield $\mathrm{GF}(p^d)$ (where $d|\ell$). It is easily seen that they form a subgroup of $\mathrm{HW}[\mathrm{GF}(p^{\ell})]$ which has p^{3d} elements and which we denote as $\mathrm{HW}[\mathrm{GF}(p^d)]$. We note that in this representation of $\mathrm{HW}[\mathrm{GF}(p^d)]$ the displacement operators act on H and use the characters $\chi(\alpha)$ of equation (43).

We can have another representation of $\mathrm{HW}[\mathrm{GF}(p^d)]$, where the displacement operators act only on the subspace H_d using the characters $\chi_d(\alpha)$ of equation (47). We explain this briefly, considering a G_d-subsystem described by the Hilbert space H_d. We define displacement operators $D_d(\alpha, \beta)$ (where $\alpha, \beta \in \mathrm{GF}(p^d)$) acting on H_d using the additive characters $\chi_d(\alpha)$ of equation (47). We do not present explicit formulas for $D_d(\alpha, \beta)$ because they are analogous to those above. We only mention a relation between the elements of the matrices $D_d(\alpha, \beta)$ and the elements of the corresponding matrices $\Pi_d D(\alpha, \beta)\Pi_d$. Using equation (49) we show that for $m, n, \alpha, \beta \in \mathrm{GF}(p^d)$

$$\langle X; m|\Pi_d D(\alpha, \beta)\Pi_d|X; n\rangle = [\langle X; m|D_d(\alpha, \beta)|X; n\rangle]^{\ell/d}; \qquad m, n, \alpha, \beta \in \mathrm{GF}(p^d). \tag{121}$$

7.1. Displaced parity operators

The parity operator $P(0, 0)$ around the origin is defined as

$$\begin{aligned} &P(0, 0) = F^2; \qquad [P(0, 0)]^2 = \mathbf{1} \\ &P(0, 0)|X; m\rangle = |X; -m\rangle; \qquad P(0, 0)|P; m\rangle = |P; -m\rangle. \end{aligned} \tag{122}$$

Using equation (76) we express $P(0, 0)$ in terms of the projection operators $\mathcal{A}_0$ and $\mathcal{A}_1$ as

$$\begin{aligned} &P(0, 0) = \mathcal{A}_0 - \mathcal{A}_1; \qquad \mathcal{A}_0 = \eta_0 + \eta_2; \qquad \mathcal{A}_1 = \eta_1 + \eta_3 \\ &\mathcal{A}_r\mathcal{A}_s = \delta(r, s)\vartheta_r; \qquad \mathcal{A}_0 + \mathcal{A}_1 = \mathbf{1}; \qquad r, s = 0, 1. \end{aligned} \tag{123}$$

The displaced parity operators are defined as

$$\begin{aligned} &P(\alpha, \beta) = D(\alpha, \beta)P(0, 0)[D(\alpha, \beta)]^{\dagger} = D(2\alpha, 2\beta)P(0, 0) = P(0, 0)[D(2\alpha, 2\beta)]^{\dagger} \\ &[P(\alpha, \beta)]^2 = \mathbf{1}. \end{aligned} \tag{124}$$

These are related to the displacement operators through a two-dimensional Fourier transform

$$P(\alpha, \beta) = \sum_{\gamma,\delta} D(\gamma, \delta)\chi(\alpha\delta - \beta\gamma). \tag{125}$$

We introduce the displaced projection operators $\mathcal{A}_0(\alpha, \beta)$ and $\mathcal{A}_1(\alpha, \beta)$ and express $P(\alpha, \beta)$ in terms of them as

$$P(\alpha, \beta) = \mathcal{A}_0(\alpha, \beta) - \mathcal{A}_1(\alpha, \beta); \qquad \mathcal{A}_r(\alpha, \beta) = D(\alpha, \beta)\mathcal{A}_r[D(\alpha, \beta)]^{\dagger}; \qquad r = 0, 1. \tag{126}$$

We also combine equation (125) with equation (116) and express the displaced parity operator $P(\alpha, \beta)$ in terms of displaced parity operators acting on the component systems:

$$P(\alpha, \beta) = \mathcal{P}(\overline{\alpha}_0, \beta_0) \otimes \cdots \otimes \mathcal{P}(\overline{\alpha}_{\ell-1}, \beta_{\ell-1}). \tag{127}$$

8. $\mathrm{Sp}(2,\mathrm{GF}(p^\ell))$ symplectic transformations and isotropy of the $\mathrm{GF}(p^\ell) \times \mathrm{GF}(p^\ell)$ phase space

The $\mathrm{GF}(p^\ell) \times \mathrm{GF}(p^\ell)$ phase space of Galois quantum systems is a finite geometry and the symplectic transformations $S(q,r,s)$ perform 'discrete rotations' in it. Acting on the operators Z and X which perform displacements along the momentum and position axes correspondingly, they give new operators which perform displacements along new axes:

$$\begin{aligned}
&Z_{(q,r,s)}(\alpha) = S(q,r,s)Z(\alpha)S^\dagger(q,r,s) = D(t\alpha, s\alpha)\\
&X_{(q,r,s)}(\beta) = S(q,r,s)X(\beta)S^\dagger(q,r,s) = D(r\beta, q\beta); \qquad q,r,s,t \in \mathrm{GF}(p^\ell).
\end{aligned} \tag{128}$$

We require that these transformations are unitary and preserve equation (111), i.e., that

$$X_{(q,r,s)}(\beta)Z_{(q,r,s)}(\alpha) = Z_{(q,r,s)}(\alpha)X_{(q,r,s)}(\beta)\chi(-\alpha\beta). \tag{129}$$

This leads to the constraint

$$qt - rs = 1. \tag{130}$$

Therefore there are three independent variables q,r,s in these transformations and $t = q^{-1}(rs+1)$. For this reason we have omitted t in the notation. It is crucial here that the variables belong to a field and therefore q^{-1} exists (for $q \neq 0$).

In the case of general finite systems the variables belong to a ring and in general we cannot solve the constraint of equation (130). Consequently, we cannot define symplectic transformations which form a group in these systems. Intuitively, this is easily understood because symplectic transformations are intimately connected to a (discrete) isotropy of the phase space. In the general case, the phase space is a toroidal lattice with X and P as 'important directions', and with no geometrical structure. We can define displacements in it, but not symplectic transformations. In Galois quantum systems the phase space is a finite geometry, there is a finite number of 'straight lines' (finite sets of points) which are all equally important, and we can define both displacements and symplectic transformations.

Symplectic transformations form a group, which we call $\mathrm{Sp}(2,\mathrm{GF}(p^\ell))$. We first show that the product of two such transformations is a transformation of the same type:

$$\begin{aligned}
&S(q_2,r_2,s_2)S(q_1,r_1,s_1) = S(\epsilon,\zeta,\eta)\\
&\epsilon = q_1q_2 + r_1s_2\\
&\zeta = q_1r_2 + r_1q_2^{-1}(1+r_2s_2)\\
&\eta = q_2s_1 + s_2q_1^{-1}(1+r_1s_1).
\end{aligned} \tag{131}$$

We can also show that associativity holds; that identity element exists; and that inverses exist.

Below we give several formulas for the generic case that $qt = 1 + rs \neq 0$. The cases were $qt = 1 + rs = 0$ can easily be considered separately. For example, for $q = t = 0$ and $r = -s = 1$ it is easily seen that

$$S(0,1,-1) = F. \tag{132}$$

Symplectic transformations act on general displacement operators as follows:

$$S(q,r,s)D(\alpha,\beta)[S(q,r,s)]^\dagger = D(t\alpha + r\beta, s\alpha + q\beta); \qquad t = q^{-1}(1+rs). \tag{133}$$

This is a generalization of equation (128).

Following [41], we give an analytic expression for the symplectic operators $S(q,r,s)$. Before we discuss the general case, we first study three special cases of operators which form three important subgroups of $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$. The first one is the operators

$$\begin{aligned} &S(\xi, 0, 0) = \sum_{m\in \mathrm{GF}(p^\ell)} |X; \xi m\rangle\langle X; m| = \sum_{m\in \mathrm{GF}(p^\ell)} |P; \xi^{-1} m\rangle\langle P; m| \\ &S(\xi_1, 0, 0)S(\xi_2, 0, 0) = S(\xi_1\xi_2, 0, 0); \qquad [S(\xi, 0, 0)]^{p^\ell} = S(\xi, 0, 0). \end{aligned} \tag{134}$$

It is easily seen that they form a subgroup of $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$. The fact that ξ belongs to a field is crucial for the proof that these operators are unitary. We note that the relation $[S(\xi, 0, 0)]^{p^\ell} = S(\xi, 0, 0)$ is true for all ξ in the field $\mathrm{GF}(p^\ell)$. If however ξ belongs to a subfield $\mathrm{GF}(p^d)$ of $\mathrm{GF}(p^\ell)$ (where $d|\ell$) then we can prove the stronger relation

$$\xi \in \mathrm{GF}(p^d) \rightarrow [S(\xi, 0, 0)]^{p^d} = S(\xi, 0, 0). \tag{135}$$

The second special case is the operators

$$\begin{aligned} &S(1, \xi, 0) = \sum_{m\in \mathrm{GF}(p^\ell)} \chi(2^{-1}\xi m^2)|X; m\rangle\langle X; m| \\ &S(1, \xi_1, 0)S(1, \xi_2, 0) = S(1, \xi_1 + \xi_2, 0); \qquad [S(1, \xi, 0)]^p = \mathbf{1}. \end{aligned} \tag{136}$$

These also form a subgroup of $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$. The third special case is the operators

$$\begin{aligned} &S(1, 0, \xi) = \sum_{m\in \mathrm{GF}(p^\ell)} \chi(-2^{-1}\xi m^2)|P; m\rangle\langle P; m| \\ &S(1, 0, \xi_1)S(1, 0, \xi_2) = S(1, 0, \xi_1 + \xi_2); \qquad [S(1, 0, \xi)]^p = \mathbf{1} \\ &S(1, 0, \xi) = FS(1, \xi, 0)F^\dagger. \end{aligned} \tag{137}$$

These also form a subgroup of $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$. The general symplectic operator $S(\kappa, \lambda, \mu)$ can be written in terms of them as

$$\begin{aligned} &S(q, r, s) = S(1, 0, \xi_1)S(1, \xi_2, 0)S(\xi_3, 0, 0) \\ &\xi_1 = qs(1 + rs)^{-1} \\ &\xi_2 = rq^{-1}(1 + rs) \\ &\xi_3 = q(1 + rs)^{-1}. \end{aligned} \tag{138}$$

Combining equations (135), (136), (137) and (138) we get

$$\begin{aligned} &S(q, r, s) = p^{-\ell}G(A) \sum_{n,m\in \mathrm{GF}(p^\ell)} \chi[(2q)^{-1}(s^{-1} + r)n^2 - s^{-1}nm + (2s)^{-1}qm^2]|X; n\rangle\langle X; m| \\ &A = -2^{-1}(1 + rs)^{-1}qs, \end{aligned} \tag{139}$$

where $G(A)$ is the Gauss sum related to $\mathrm{GF}(p^\ell)$ defined in equation (87).

We next consider the operators $S(q, r, s)$, where q, r, s are in the subfield $\mathrm{GF}(p^d)$ (where $d|\ell$). These form a subgroup of $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$ which we denote as $\mathrm{Sp}(2, \mathrm{GF}(p^d))$. We note that in this representation of $\mathrm{Sp}(2, \mathrm{GF}(p^d))$ the symplectic operators act on H and use the characters $\chi(\alpha)$ of equation (43). We can have another representation of $\mathrm{Sp}(2, \mathrm{GF}(p^d))$ with the operators $S(q, r, s)$ acting on the subspace H_d using the characters $\chi_d(\alpha)$ of equation (47). We made a similar comment earlier for the Heisenberg–Weyl group.

Symplectic transformations on finite fields from an abstract pure mathematics point of view have been studied in [52–54].

8.1. Radon transforms

An important property of the displacement operators is the 'marginal relations'

$$\begin{aligned}
\frac{1}{p^\ell}\sum_{\alpha\in \mathrm{GF}(p^\ell)} D(\alpha,\beta) &= |X;2^{-1}\beta\rangle\langle X;-2^{-1}\beta| \\
\frac{1}{p^\ell}\sum_{\beta\in \mathrm{GF}(p^\ell)} D(\alpha,\beta) &= |P;2^{-1}\alpha\rangle\langle P;-2^{-1}\alpha| \qquad (140)\\
\frac{1}{p^\ell}\sum_{\alpha,\beta\in \mathrm{GF}(p^\ell)} D(\alpha,\beta) &= P(0,0).
\end{aligned}$$

These are proved by calculating the matrix elements of both sides using equation (115). These are expressed here with respect to the *X*–*P* axes. Acting with the symplectic operator $S(q,r,s)$ on both sides of equation (140) we get analogous relations with respect to different axes in the $\mathrm{GF}(p^\ell)\times\mathrm{GF}(p^\ell)$ phase space determined by the parameters (q,r,s):

$$\begin{aligned}
\frac{1}{p^\ell}\sum_{\epsilon,\zeta} D(\epsilon,\zeta)\delta(-s\epsilon+t\zeta,\beta) &= |X(q,r,s);2^{-1}\beta\rangle\langle X(q,r,s);-2^{-1}\beta| \\
\frac{1}{p^\ell}\sum_{\epsilon,\zeta} D(\epsilon,\zeta)\delta(q\epsilon-r\zeta,\alpha) &= |P(q,r,s);2^{-1}\alpha\rangle\langle P(q,r,s);-2^{-1}\alpha|.
\end{aligned} \qquad (141)$$

Here we sum over all points on the lines $-s\epsilon+t\zeta=\beta$ and $q\epsilon-r\zeta=\alpha$. The left-hand sides of these relations are Radon transforms in a finite geometry (the integration along a line in the continuum, becomes here a summation). The '(q,r,s)-states' are related to the original ones through the symplectic transform

$$|X(q,r,s);\gamma\rangle = S(q,r,s)|X;\gamma\rangle; \qquad |P(q,r,s);\gamma\rangle = S(q,r,s)|P;\gamma\rangle. \qquad (142)$$

In the special case that $q=t=1$ and $r=s=0$ equation (141) reduce to equation (140). It is seen that the phase space is isotropic in the sense that equation (141) are valid not only for the *X*–*P* axes, but for any axes.

In a similar way we can show the following relations for the displaced parity operator:

$$\begin{aligned}
\frac{1}{p^\ell}\sum_{\alpha\in \mathrm{GF}(p^\ell)} P(\alpha,\beta) &= |X;\beta\rangle\langle X;\beta| \\
\frac{1}{p^\ell}\sum_{\beta\in \mathrm{GF}(p^\ell)} P(\alpha,\beta) &= |P;\alpha\rangle\langle P;\alpha| \qquad (143)\\
\frac{1}{p^\ell}\sum_{\alpha,\beta\in \mathrm{GF}(p^\ell)} P(\alpha,\beta) &= \mathbf{1}.
\end{aligned}$$

The right-hand sides of these equations are projection operators. Acting with the symplectic operator $S(q,r,s)$ on both sides of equation (143) we get analogous relations with respect to different axes:

$$\begin{aligned}
\frac{1}{p^\ell}\sum_{\epsilon,\zeta} P(\epsilon,\zeta)\delta(-s\epsilon+t\zeta,\beta) &= |X(q,r,s);\beta\rangle\langle X(q,r,s);\beta| \\
\frac{1}{p^\ell}\sum_{\epsilon,\zeta} P(\epsilon,\zeta)\delta(q\epsilon-r\zeta,\alpha) &= |P(q,r,s);\alpha\rangle\langle P(q,r,s);\alpha|.
\end{aligned} \qquad (144)$$

The left-hand sides of these relations are Radon transforms (studied in a general context in [55]).

The inverse Radon transform expresses the displacement operators (or the displaced parity operators) in terms of the projection operators which appear on the right-hand side of equation (144). We Fourier transform equation (144) and express the displacement operators in terms of these projection operators as

$$\begin{aligned}D(r\beta, q\beta) &= \sum_{\alpha\in\mathrm{GF}(p^\ell)} |P(q,r,s);\alpha\rangle\langle P(q,r,s);\alpha|\chi(-\alpha\beta)\\ D(t\alpha, s\alpha) &= \sum_{\beta\in\mathrm{GF}(p^\ell)} |X(q,r,s);\beta\rangle\langle X(q,r,s);\beta|\chi(\alpha\beta).\end{aligned} \tag{145}$$

If we need the displaced parity operators, we perform the two-dimensional Fourier transform of equation (125). These relations will be used below for quantum tomography in Galois quantum systems.

9. The $\mathfrak{T}[\mathrm{GF}(p^\ell)]$ group of displacements and symplectic transformations

The unitary operators

$$\begin{aligned}&T(q,r,s;\alpha,\beta,\gamma) \equiv S(q,r,s)D(\alpha,\beta)\chi(\gamma) = D(t\alpha + r\beta, s\alpha + q\beta)S(q,r,s)\chi(\gamma)\\ &t = q^{-1}(1+rs)\end{aligned} \tag{146}$$

perform both displacements and symplectic transformations. It is easily seen that

$$T(q_1,r_1,s_1;\alpha_1,\beta_1,\gamma_1)T(q_2,r_2,s_2;\alpha_2,\beta_2,\gamma_2) = T(q,r,s;\alpha,\beta,\gamma), \tag{147}$$

where

$$\begin{aligned}q &= q_1q_2 + r_2s_1\\ r &= q_2r_1 + r_2q_1^{-1}(1+r_1s_1)\\ s &= q_1s_2 + s_1q_2^{-1}(1+r_2s_2)\\ \alpha &= \alpha_1q_2 + \alpha_2 - \beta_1r_2\\ \beta &= -\alpha_1s_2 + \beta_2 + \beta_1(1+r_2s_2)q_2^{-1}\\ \gamma &= \gamma_1 + \gamma_2 + 2^{-1}\left[\alpha_1\alpha_2s_2 + \alpha_1\beta_2q_2 - \beta_1\beta_2r_2 - \beta_1\alpha_2(1+r_2s_2)q_2^{-1}\right].\end{aligned} \tag{148}$$

The operators $T(q,r,s;\alpha,\beta,\gamma)$ form a group which we denote as $\mathfrak{T}[\mathrm{GF}(p^\ell)]$ and which is sometimes called the Clifford group. The Heisenberg–Weyl group is a normal subgroup of $\mathfrak{T}[\mathrm{GF}(p^\ell)]$. Indeed, using equation (133) we show that

$$\begin{aligned}&T(q,r,s;\alpha,\beta,\gamma)D(\kappa,\lambda)[T(q,r,s;\alpha,\beta,\gamma)]^\dagger = D(t\kappa + r\lambda, s\kappa + q\lambda)\chi(\alpha\lambda - \beta\kappa)\\ &t = q^{-1}(1+rs).\end{aligned} \tag{149}$$

The $\mathrm{Sp}(2,\mathrm{GF}(p^\ell))$ is also a subgroup of $\mathfrak{T}[\mathrm{GF}(p^\ell)]$ and

$$\mathrm{Sp}(2,\mathrm{GF}(p^\ell)) \bigcap \mathrm{HW}[\mathrm{GF}(p^\ell)] = \{\mathbf{1}\}. \tag{150}$$

Therefore, $\mathfrak{T}[\mathrm{GF}(p^\ell)]$ is the semidirect product of the $\mathrm{HW}[\mathrm{GF}(p^\ell)]$ group of displacements by the $\mathrm{Sp}(2,\mathrm{GF}(p^\ell))$ group of symplectic transformations. Consequently, the quotient group $\mathfrak{T}[\mathrm{GF}(p^\ell)]/\mathrm{HW}[\mathrm{GF}(p^\ell)]$ is isomorphic to the $\mathrm{Sp}(2,\mathrm{GF}(p^\ell))$ group.

Acting with the operators $T(q,r,s;\alpha,\beta,\gamma)$ on the Hamiltonians of equation (102) we get more general ones:

$$\begin{aligned}h'_A &= T(q,r,s;\alpha,\beta,\gamma)h_A[T(q,r,s;\alpha,\beta,\gamma)]^\dagger\\ h'_B &= T(q,r,s;\alpha,\beta,\gamma)h_B[T(q,r,s;\alpha,\beta,\gamma)]^\dagger.\end{aligned} \tag{151}$$

These are analogues of the squeezed and displaced harmonic oscillator described by the Hamiltonian $h = \alpha_1x^2 + \alpha_2p^2 + \alpha_3xp + \alpha_4x + \alpha_5p$.

10. Wigner and Weyl functions

10.1. Wigner functions

We consider an operator Θ and its matrix elements

$$\Theta_X(m,n) \equiv \langle X; m|\Theta|X; n\rangle; \qquad \Theta_P(m,n) \equiv \langle P; m|\Theta|P; n\rangle. \tag{152}$$

The Wigner function of the operator Θ is defined as

$$\begin{aligned} W(\Theta; \alpha, \beta) = \mathrm{tr}[\Theta P(\alpha, \beta)] &= \chi(2\alpha\beta) \sum_{\gamma} \chi(-2\alpha\gamma)\Theta_X(\gamma, 2\beta - \gamma) \\ &= \chi(-2\alpha\beta) \sum_{\gamma} \chi(2\beta\gamma)\Theta_P(\gamma, 2\alpha - \gamma). \end{aligned} \tag{153}$$

If Θ is a Hermitian operator then the Wigner function is real; but for non-Hermitian operators it is complex.

The Wigner function of a density matrix ρ is real, and it can be interpreted as a pseudoprobability distribution of the particle in the position–momentum phase space. It is pseudoprobability distribution because it can take negative values. Using Eq(126) we can express the Wigner function of a density matrix ρ as the difference of two probabilities $\sigma_i(\rho; \alpha, \beta)$:

$$\begin{aligned} &W(\rho; \alpha, \beta) = \sigma_0(\rho; \alpha, \beta) - \sigma_1(\rho; \alpha, \beta) \\ &\sigma_i(\rho; \alpha, \beta) \equiv \mathrm{tr}[\rho \mathcal{A}_i(\alpha, \beta)]; \qquad \sigma_0(\rho; \alpha, \beta) + \sigma_1(\rho; \alpha, \beta) = 1. \end{aligned} \tag{154}$$

This shows that $-1 \leqslant W(\rho; \alpha, \beta) \leqslant 1$.

As an example, we consider the Fourier and displacement operators and we find

$$\begin{aligned} &W(F; \alpha, \beta) = p^{-\ell/2} \chi(\alpha^2 + \beta^2 + 4\alpha\beta) G(-1) \\ &W(D(\kappa, \lambda); \alpha, \beta) = \chi(\beta\kappa - \alpha\lambda), \end{aligned} \tag{155}$$

where $G(-1)$ is a Gauss sum for $\mathrm{GF}(p^\ell)$, defined in equation (87). We also consider the symplectic operators and using equation (139) we find

$$\begin{aligned} &W(S(q, r, s); \alpha, \beta) = p^{-\ell} G(A) G(B) \chi(\Gamma) \\ &A = -2^{-1}(1 + rs)^{-1} qs; \qquad B = (2qs)^{-1} + (2q)^{-1} r + s^{-1} + (2s)^{-1} q \\ &\Gamma = s^{-1} 2q\beta^2 + 2\alpha\beta - (4B)^{-1}[s^{-1} 2\beta(q + 1) + 2\alpha]^2. \end{aligned} \tag{156}$$

We next consider the special case of operators Θ which can be written as a product

$$\Theta = \Theta_0 \times \cdots \times \Theta_{\ell-1} \tag{157}$$

of operators acting on the ℓ components of the system. Taking into account equation (127) we see that the corresponding Wigner function factorizes as

$$W(\Theta; \alpha, \beta) = \mathcal{W}(\Theta_0; \overline{\alpha}_0, \beta_0) \cdots \mathcal{W}(\Theta_{\ell-1}; \overline{\alpha}_{\ell-1}, \beta_{\ell-1}). \tag{158}$$

The Wigner function of the sum of two operators is simply the sum of the Wigner functions of the two operators. The Wigner function of the product of two operators is given by the Moyal star product, which in the present context is

$$\begin{aligned} W(\Theta_1) \star W(\Theta_2) \equiv W(\Theta_1\Theta_2; \alpha, \beta) = p^{-2\ell} &\sum_{\alpha_1, \beta_1, \alpha_2, \beta_2} \chi(2\alpha_2\beta_1 - 2\alpha_1\beta_2) \\ &\times W(\Theta_1; \alpha + \alpha_1, \beta + \beta_1) W(\Theta_2; \alpha + \alpha_2, \beta + \beta_2). \end{aligned} \tag{159}$$

The Moyal star product has similar properties to the product of operators. For example, the Moyal star product of two operators is (in general) non-commutative, and the Moyal star product of three operators is associative.

An arbitrary operator Θ can be expanded in terms of the displaced parity operators with the Wigner functions as coefficients

$$\Theta = \frac{1}{p^\ell} \sum_{\alpha,\beta} W(\Theta; \alpha, \beta) P(\alpha, \beta). \tag{160}$$

This is proved by taking the matrix elements of both sides.

10.2. Radon transforms of Wigner functions

The properties of the Wigner function are intimately related to the properties of the displaced parity operators. Indeed equation (143) lead to the following marginal properties of the Wigner function with respect to the $X - P$ axes:

$$\begin{aligned} \frac{1}{p^\ell} \sum_{\alpha} W(\Theta; \alpha, \beta) &= \Theta_X(\beta, \beta) \\ \frac{1}{p^\ell} \sum_{\beta} W(\Theta; \alpha, \beta) &= \Theta_P(\alpha, \alpha) \\ \frac{1}{p^\ell} \sum_{\alpha,\beta} W(\Theta; \alpha, \beta) &= \mathrm{tr}\Theta. \end{aligned} \tag{161}$$

We note that if Θ is a density matrix then the $\Theta_X(\beta, \beta)$ and $\Theta_P(\alpha, \alpha)$ are probabilities.

Similar properties can be proved with respect to different axes using equation (144):

$$\begin{aligned} \frac{1}{p^\ell} \sum_{\epsilon,\zeta} W(\Theta; \epsilon, \zeta) \delta(-s\epsilon + t\zeta, \beta) &= \Theta_{X(q,r,s)}(\beta, \beta) \\ \frac{1}{p^\ell} \sum_{\epsilon,\zeta} W(\Theta; \epsilon, \zeta) \delta(q\epsilon - r\zeta, \alpha) &= \Theta_{P(q,r,s)}(\alpha, \alpha), \end{aligned} \tag{162}$$

where $\Theta_{P(q,r,s)}(\alpha, \alpha)$ and $\Theta_{X(q,r,s)}(\beta, \beta)$ are the matrix elements of Θ with respect to the (q, r, s)-states of equation (142):

$$\begin{aligned} \Theta_{X(q,r,s)}(m, n) &\equiv \langle X(q, r, s); m|\Theta|X(q, r, s); n\rangle = \langle X; m|[S(q, r, s)]^\dagger \Theta S(q, r, s)|X; n\rangle \\ \Theta_{P(q,r,s)}(m, n) &\equiv \langle P(q, r, s); m|\Theta|P(q, r, s); n\rangle = \langle P; m|[S(q, r, s)]^\dagger \Theta S(q, r, s)|P; n\rangle. \end{aligned} \tag{163}$$

The left-hand side of equation (162) are the Radon transform of the Wigner function.

The Wigner function is the Fourier transform of the matrix elements $\Theta_X(\gamma, 2\beta - \gamma)$ and $\Theta_P(\gamma, 2\alpha - \gamma)$ in equation (153). Using Parceval's theorem we get another set of marginal properties that involves the absolute value of the Wigner function squared:

$$\begin{aligned} \frac{1}{p^\ell} \sum_{\alpha} |W(\Theta; \alpha, \beta)|^2 &= \sum_{\gamma} |\Theta_X(\gamma, 2\beta - \gamma)|^2 \\ \frac{1}{p^\ell} \sum_{\beta} |W(\Theta; \alpha, \beta)|^2 &= \sum_{\gamma} |\Theta_P(\gamma, 2\alpha - \gamma)|^2 \\ \frac{1}{p^\ell} \sum_{\alpha,\beta} |W(\Theta; \alpha, \beta)|^2 &= \mathrm{tr}[\Theta\Theta^\dagger]. \end{aligned} \tag{164}$$

10.3. Weyl functions

The Weyl function of the operator Θ is defined as

$$\begin{aligned}\tilde{W}(\Theta;\alpha,\beta) &= \mathrm{tr}[\Theta D(\alpha,\beta)] = \chi(2^{-1}\alpha\beta)\sum_{\gamma}\chi(\alpha\gamma)\Theta_X(\gamma,\beta+\gamma)\\ &= \chi(-2^{-1}\alpha\beta)\sum_{\gamma}\chi(-\beta\gamma)\Theta_P(\gamma,\alpha+\gamma).\end{aligned}\tag{165}$$

The Weyl function is related to the Wigner function through a two-dimensional Fourier transform (indicated with the tilde in the notation):

$$\tilde{W}(\Theta;\alpha,\beta) = \frac{1}{p^{\ell}}\sum_{\gamma,\delta}W(\Theta;\gamma,\delta)\chi(\alpha\delta-\beta\gamma).\tag{166}$$

This is a direct consequence of the two-dimensional Fourier transform between the displacement operators and the displaced parity operators in equation (125).

As an example, we consider the Fourier and displacement operators and we find

$$\begin{aligned}&\tilde{W}(F;\alpha,\beta) = p^{-\ell/2}\chi(-\alpha^2-\beta^2-2^{-1}3\alpha\beta)G(1)\\ &\tilde{W}(D(\kappa,\lambda);\alpha,\beta) = p^{\ell}\delta(\kappa,-\alpha)\delta(\lambda,-\beta).\end{aligned}\tag{167}$$

We also consider the symplectic operators and using equation (139) we find

$$\begin{aligned}&\tilde{W}(S(q,r,s);\alpha,\beta) = p^{-\ell}G(A)G(B)\chi(\Gamma)\\ &A = -2^{-1}(1+rs)^{-1}qs; \qquad B = (2qs)^{-1}+(2q)^{-1}r-s^{-1}+(2s)^{-1}q\\ &\Gamma = (2s)^{-1}q\beta^2+2^{-1}\alpha\beta-(4B)^{-1}[s^{-1}\beta(q-1)+\alpha]^2,\end{aligned}\tag{168}$$

where $G(A)$, $G(B)$ are Gauss sums for $\mathrm{GF}(p^{\ell})$, defined in equation (87).

We next consider the special case of operators Θ which are factorized as in equation (157). Taking into account equation (116) we see that the corresponding Weyl function factorizes as

$$\tilde{W}(\Theta;\alpha,\beta) = \tilde{\mathcal{W}}(\Theta_0;\overline{\alpha}_0,\beta_0)\cdots\tilde{\mathcal{W}}(\Theta_{\ell-1};\overline{\alpha}_{\ell-1},\beta_{\ell-1}).\tag{169}$$

10.4. Expansion of an arbitrary operator in terms of displacement operators

An arbitrary operator Θ can be expanded in terms of the displacement operators with the Weyl functions as coefficients:

$$\Theta = \frac{1}{p^{\ell}}\sum_{\alpha,\beta}\tilde{W}(\Theta;-\alpha,-\beta)D(\alpha,\beta); \qquad \alpha,\beta\in\mathrm{GF}(p^{\ell}).\tag{170}$$

This is proved by taking the matrix elements of both sides. An important special case of such operators is the unitary $U(p^{\ell})$ transformations. In this case the displacement operators $D(\alpha,\beta)$ can be viewed as the $p^{2\ell}$ generators of the $U(p^{\ell})$ group [56].

We next consider the special case of operators Θ which are product as in equation (157). Taking into account equation (169) we see that in this case equation (170) becomes

$$\begin{aligned}\Theta_0\times\cdots\times\Theta_{\ell-1} = &\left[\frac{1}{p}\sum\tilde{\mathcal{W}}(\Theta_0;-\overline{\alpha}_0,-\beta_0)\mathcal{D}(\overline{\alpha}_0,\beta_0)\right]\\ &\times\cdots\left[\frac{1}{p}\sum\tilde{\mathcal{W}}(\Theta_{\ell-1};-\overline{\alpha}_{\ell-1},-\beta_{\ell-1})\mathcal{D}(\overline{\alpha}_{\ell-1},\beta_{\ell-1})\right].\end{aligned}\tag{171}$$

10.5. Radon transforms of Weyl functions

The properties of the Weyl functions are intimately related to the properties of the displacement operators. For example equation (140) lead to the following marginal properties of the Weyl functions with respect to the $X - P$ axes:

$$\begin{aligned}
&\frac{1}{p^\ell}\sum_\alpha \tilde{W}(\Theta;\alpha,\beta) = \Theta_X(-2^{-1}\beta, 2^{-1}\beta)\\
&\frac{1}{p^\ell}\sum_\beta \tilde{W}(\Theta;\alpha,\beta) = \Theta_P(-2^{-1}\alpha, 2^{-1}\alpha)\\
&\frac{1}{p^\ell}\sum_{\alpha,\beta} \tilde{W}(\Theta;\alpha,\beta) = W(\Theta;0,0).
\end{aligned} \tag{172}$$

Similar properties can be proved with respect to different axes using equation (141):

$$\begin{aligned}
&\frac{1}{p^\ell}\sum_{\epsilon,\zeta} \tilde{W}(\Theta;\epsilon,\zeta)\delta(-s\epsilon+t\zeta,\beta) = \Theta_{X(q,r,s)}(-2^{-1}\beta, 2^{-1}\beta)\\
&\frac{1}{p^\ell}\sum_{\epsilon,\zeta} \tilde{W}(\Theta;\epsilon,\zeta)\delta(q\epsilon-r\zeta,\alpha) = \Theta_{P(q,r,s)}(-2^{-1}\alpha, 2^{-1}\alpha),
\end{aligned} \tag{173}$$

where the '(q,r,s) matrix elements' of Θ have been defined in equation (163). The left-hand side of these relations are the Radon transform of the Weyl function.

The Weyl function is the Fourier transform of the matrix elements $\Theta_X(\gamma,\beta+\gamma)$ and $\Theta_P(\gamma,\alpha+\gamma)$ in equation (165). Using Parceval's theorem we get another set of marginal properties that involves the absolute value of the Weyl function squared:

$$\begin{aligned}
&\frac{1}{p^\ell}\sum_\alpha |\tilde{W}(\Theta;\alpha,\beta)|^2 = \sum_\gamma |\Theta_X(\gamma,\beta+\gamma)|^2\\
&\frac{1}{p^\ell}\sum_\beta |\tilde{W}(\Theta;\alpha,\beta)|^2 = \sum_\gamma |\Theta_P(\gamma,\alpha+\gamma)|^2\\
&\frac{1}{p^\ell}\sum_{\alpha,\beta} |\tilde{W}(\Theta;\alpha,\beta)|^2 = \mathrm{tr}[\Theta\Theta^\dagger].
\end{aligned} \tag{174}$$

10.6. Quantum tomography

Using the inverse Radon transform of equation (145) we can show that

$$\begin{aligned}
&\tilde{W}(\Theta;t\alpha,s\alpha) = \sum_{\beta\in\mathrm{GF}(p^\ell)} \Theta_{X(q,r,s)}(\beta,\beta)\chi(\alpha\beta)\\
&\tilde{W}(\Theta;r\beta,q\beta) = \sum_{\alpha\in\mathrm{GF}(p^\ell)} \Theta_{P(q,r,s)}(\alpha,\alpha)\chi(-\alpha\beta).
\end{aligned} \tag{175}$$

If Θ is a density matrix then the $\Theta_{X(q,r,s)}(\beta,\beta)$ and $\Theta_{P(q,r,s)}(\alpha,\alpha)$ are probabilities. Measurement of these probabilities along all lines of the finite geometry phase space, and use of these relations will give the Weyl function. Equation (166) can then be used to calculate the corresponding Wigner function; and equation (170) to calculate the density matrix.

It is seen that in Galois quantum systems we can use tomography techniques similar to the ones used in the harmonic oscillator context. This is an example of the fact that phase-space methods in Galois quantum systems are as powerful as in harmonic oscillators.

11. *R*-systems with position and momentum in the ring $[\mathbb{Z}_p]^\ell$

In this section we consider a system comprised of ℓ-component systems, each of which is described by a p-dimensional Hilbert space $\mathcal{H}$. The position and momentum take values in the ring $[\mathbb{Z}_p]^\ell \equiv \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, and for this reason, we refer to it as an R-system. The Hilbert space of the system is the tensor product of equation (64), as in Galois systems. But its Hamiltonian is the *generic* Hamiltonian of equation (101), in contrast to Galois systems which are described by the specialized Hamiltonian of equation (100).

The field GF(p^ℓ) and the ring $[\mathbb{Z}_p]^\ell$ are very similar with respect to addition; but they are very different when we consider multiplication. A consequence of this is that a G-system is very different from an R-system. We study displacements and symplectic transformations in R-systems so that the reader can compare and contrast them with their counterparts in Galois quantum systems.

11.1. Additive characters in the ring $[\mathbb{Z}_p]^\ell$

We consider the ring $[\mathbb{Z}_p]^\ell$ and denote its elements as

$$(\alpha_\lambda) \equiv (\alpha_0, \ldots, \alpha_{\ell-1}). \tag{176}$$

Let $(0, \ldots, 0)$ be its zero element and $(1, \ldots, 1)$ its unity. Addition and multiplication are defined componentwise as

$$\begin{aligned} &(\alpha_\lambda) + (\beta_\lambda) = (\alpha_\lambda + \beta_\lambda); \qquad (\alpha_\lambda)(\beta_\lambda) = (\alpha_\lambda\beta_\lambda);\\ &\alpha_\lambda, \beta_\lambda \in \mathbb{Z}_p; \qquad \lambda = 0, \ldots, \ell - 1. \end{aligned} \tag{177}$$

We note that elements like $(0, 1, 0, \ldots, 0)$ have no inverse.

We define the additive characters

$$\psi[(\alpha_\lambda)] = \omega\left(\sum_\lambda \alpha_\lambda\right); \qquad \psi[(\alpha_\lambda)]\psi[(\beta_\lambda)] = \psi[(\alpha_\lambda) + (\beta_\lambda)]. \tag{178}$$

The $[\mathbb{Z}_p]^\ell$ can be viewed as an ℓ-dimensional vector space over the field $\mathbb{Z}_p$. The scalar product of two vectors (α_λ) and (β_λ) is an integer in $\mathbb{Z}_p$ and we denote it as $(\alpha_\lambda, \beta_\lambda)$. Then:

$$\psi[(\alpha_\lambda)(\beta_\lambda)] = \omega[(\alpha_\lambda, \beta_\lambda)]. \tag{179}$$

It is easily seen that

$$\frac{1}{p^\ell}\sum_{(\alpha_\lambda)} \psi[(\alpha_\lambda)(\beta_\lambda)] = \delta[(\beta_\lambda), (0)]. \tag{180}$$

11.2. Fourier transform in *R*-systems

Position states in R-systems are defined in analogous way to equation (65) as

$$|\mathbb{X}; (m_\lambda)\rangle \equiv |\mathcal{X}; m_0\rangle \otimes \cdots \otimes |\mathcal{X}; m_{\ell-1}\rangle. \tag{181}$$

The Fourier transform is given in terms of the characters of equation (178) as

$$\mathbb{F} = \mathcal{F} \otimes \cdots \otimes \mathcal{F} = (p^\ell)^{-1/2} \sum_{(m_\lambda),(n_\lambda)} \psi[(m_\lambda)(n_\lambda)]|\mathbb{X}; (m_\lambda)\rangle\langle\mathbb{X}; (n_\lambda)|. \tag{182}$$

This operator performs independent Fourier transforms in the component systems. It is similar to the Fourier transform of equation (73) for G-systems, but here $g = \mathbf{1}$.

In order to quantify the difference between $\mathbb{F}$ and the Fourier transform F in G-systems, we define the unitary operator

$$\begin{aligned} U &= \sum |\mathcal{X}; \overline{m}_0\rangle\langle\mathcal{X}; m_0| \otimes \cdots \otimes |\mathcal{X}; \overline{m}_{\ell-1}\rangle\langle\mathcal{X}; m_{\ell-1}| \\ &= \sum |\mathcal{P}; \overline{m}_0\rangle\langle\mathcal{P}; m_0| \otimes \cdots \otimes |\mathcal{P}; \overline{m}_{\ell-1}\rangle\langle\mathcal{P}; m_{\ell-1}|, \end{aligned} \tag{183}$$

where the summation is over all $(m_0, \ldots, m_{\ell-1})$. $\overline{m}_\lambda$ have been given in terms of $\{m_\lambda\}$ in equation (32). The equality in the two expressions in equation (183) is proved using equation (33). It is then easily seen that

$$F = U\mathbb{F}; \qquad [U, F] = [U, \mathbb{F}] = [F, \mathbb{F}] = 0. \tag{184}$$

Acting with $\mathbb{F}$ on the position states $|\mathbb{X}; m\rangle$ we get momentum states in R-systems

$$|\mathbb{P}; (m_\lambda)\rangle = \mathbb{F}|\mathbb{X}; (m_\lambda)\rangle = |\mathcal{P}; m_0\rangle \otimes \cdots \otimes |\mathcal{P}; m_{\ell-1}\rangle = U^\dagger|P; m\rangle. \tag{185}$$

It is seen that the momentum states $|\mathbb{P}; m\rangle$ in R-systems are different from the corresponding momentum states $|P; m\rangle$ in G-systems.

11.3. Displacements in R-systems

Displacements in R-systems are defined in a similar way to displacements in G-systems but the formulas involve now the characters of equation (178):

$$\begin{aligned} \mathbb{Z}[(\alpha_\lambda)] &= \sum_{(n_\lambda)} \psi[(\alpha_\lambda)(n_\lambda)]|\mathbb{X}; (n_\lambda)\rangle\langle\mathbb{X}; (n_\lambda)| = \mathcal{Z}(\alpha_0) \otimes \cdots \otimes \mathcal{Z}(\alpha_{\ell-1}) \\ \mathbb{X}[(\beta_\lambda)] &= \sum_{(n_\lambda)} \psi[-(\beta_\lambda)(n_\lambda)]|\mathbb{P}; (n_\lambda)\rangle\langle\mathbb{P}; (n_\lambda)| = \mathcal{X}(\beta_0) \otimes \cdots \otimes \mathcal{X}(\beta_{\ell-1}). \end{aligned} \tag{186}$$

These obey the relation

$$\mathbb{X}[(\beta_\lambda)]\mathbb{Z}[(\alpha_\lambda)] = \mathbb{Z}[(\alpha_\lambda)]\mathbb{X}[(\beta_\lambda)]\psi[-(\alpha_\lambda)(\beta_\lambda)]. \tag{187}$$

General displacement in these systems is defined as

$$\mathbb{D}[(\alpha_\lambda), (\beta_\lambda)] = \mathbb{Z}[(\alpha_\lambda)]\mathbb{X}[(\beta_\lambda)]\psi[-2^{-1}(\alpha_\lambda)(\beta_\lambda)]; \qquad \{\mathbb{D}[(\alpha_\lambda), (\beta_\lambda)]\}^\dagger = \mathbb{D}[(-\alpha_\lambda), (-\beta_\lambda)]. \tag{188}$$

These can be expressed in terms of the displacement operators $\mathcal{D}$ acting on the various components of the system as

$$\mathbb{D}[(\alpha_\lambda), (\beta_\lambda)] = \mathcal{D}(\alpha_0, \beta_0) \otimes \cdots \otimes \mathcal{D}(\alpha_{\ell-1}, \beta_{\ell-1}). \tag{189}$$

Using equation (116) we prove the following relationship between displacements in G-systems and the corresponding displacements in R-systems:

$$X(\beta) = \mathbb{X}[(\beta_\lambda)]; \qquad Z(\alpha) = \mathbb{Z}[(\overline{\alpha}_\lambda)] = U\mathbb{Z}[(\alpha_\lambda)]U^\dagger. \tag{190}$$

As we explained earlier if α is an element of a Galois field, α_λ are its components in the $1, \epsilon, \ldots, \epsilon^{\ell-1}$ basis and $\overline{\alpha}_\lambda$ its components in the dual basis $\{E_i\}$.

11.4. Symplectic Sp$(2\ell, \mathbb{Z}_p)$ *transformations in R-systems*

We consider an R-system and study briefly Sp$(2\ell, \mathbb{Z}_p)$ symplectic transformations in its $[\mathbb{Z}_p]^{2\ell}$ phase space. These are as

$$\begin{aligned} \mathbb{Z}'[(\alpha_\lambda)] &= \mathbb{S}\mathbb{Z}[(\alpha_\lambda)]\mathbb{S}^\dagger = \mathbb{D}\left[\left(\sum t_{\lambda\kappa}\alpha_\kappa\right), \left(\sum s_{\lambda\kappa}\alpha_\kappa\right)\right] \\ \mathbb{X}'[(\beta_\lambda)] &= \mathbb{S}\mathbb{X}[(\beta_\lambda)]\mathbb{S}^\dagger = \mathbb{D}\left[\left(\sum r_{\lambda\kappa}\beta_\kappa\right), \left(\sum q_{\lambda\kappa}\beta_\kappa\right)\right]. \end{aligned} \tag{191}$$

Here q, r, s, t are $\ell \times \ell$ matrices with elements in $\mathbb{Z}_p$.

We require that the transformations (191) preserve equation (187); that all $\mathbb{Z}'[(\alpha_\lambda)]$ commute with each other; and that all $\mathbb{X}'[(\beta_\lambda)]$ commute with each other. This leads to the constraints:

$$q^T r - r^T q = 0; \qquad s^T t - t^T s = 0; \qquad q^T t - r^T s = \mathbf{1}. \tag{192}$$

These transformations contain $4\ell^2$ parameters in $\mathbb{Z}_p$. Equation (192) impose $2\ell^2 - \ell$ constraints among them. Therefore the symplectic transformations $\mathbb{S}$ are functions of $2\ell^2 + \ell$ independent parameters in $\mathbb{Z}_p$. These transformations form the symplectic $\mathrm{Sp}(2\ell, \mathbb{Z}_p)$ group. Numerical evaluation of the symplectic operator $\mathbb{S}$ has been discussed in [41] for the simple case $\ell = 2$.

Symplectic transformations act on general displacement operators as follows:

$$\mathbb{S}\mathbb{D}[(\alpha_\lambda), (\beta_\lambda)]\mathbb{S}^\dagger = \mathbb{D}\left[\left(\sum t_{\lambda\kappa}\alpha_\kappa + \sum r_{\lambda\kappa}\beta_\kappa\right), \left(\sum s_{\lambda\kappa}\alpha_\kappa + \sum q_{\lambda\kappa}\beta_\kappa\right)\right]. \tag{193}$$

An important subgroup of $\mathrm{Sp}(2\ell, \mathbb{Z}_p)$ is the $\mathrm{Sp}(2, \mathbb{Z}_p) \times \cdots \times \mathrm{Sp}(2, \mathbb{Z}_p)$ which corresponds to the special case that the matrices q, r, s, t are diagonal.

$$\begin{aligned} &q_{\lambda\kappa} = Q_\lambda \delta_{\lambda\kappa}; \qquad r_{\lambda\kappa} = R_\lambda \delta_{\lambda\kappa}; \qquad s_{\lambda\kappa} = S_\lambda \delta_{\lambda\kappa}; \qquad t_{\lambda\kappa} = T_\lambda \delta_{\lambda\kappa} \\ &Q_\lambda T_\lambda - R_\lambda S_\lambda = 1; \qquad Q_\lambda, R_\lambda, S_\lambda, T_\lambda \in \mathbb{Z}_p. \end{aligned} \tag{194}$$

Equations (128) and (191) look similar to each other but they use a very different multiplication. In equation (128) we have Galois multiplication and in equation (191) matrix multiplication. Consequently, it is difficult to find a simple relationship between symplectic $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$ transformations in G-systems and symplectic $\mathrm{Sp}(2\ell, \mathbb{Z}_p)$ transformations in R-systems. For Fourier transforms and displacements we gave such relations in equations (184) and (190).

12. Frobenius symmetry in Galois systems

An important aspect of Galois theory is the Frobenius transformations of equation (3) and the Galois groups of equations (6) and (8). In this section we extend these ideas in our context [49].

We define the Frobenius transformations in the Frobenius subspace $\mathfrak{H}_{d\kappa}$ as

$$\mathcal{G}_{d\kappa} = \sum_{\nu \in \mathbb{Z}_d} |X; m(d, \kappa, \nu + 1)\rangle\langle X; m(d, \kappa, \nu)|; \qquad \mathcal{G}_{d\kappa}^d = \pi_{d\kappa}. \tag{195}$$

Using the states of equation (97) we can express $\mathcal{G}_{d\kappa}$ in a diagonal form as

$$\mathcal{G}_{d\kappa} = \sum_{\nu \in \mathbb{Z}_d} \Omega_d(-\nu)|\mathfrak{P}; m(d, \kappa, \nu)\rangle\langle \mathfrak{P}; m(d, \kappa, \nu)|. \tag{196}$$

In the special case $d = 1$ we get $\mathcal{G}_{1\kappa} = \pi_{1\kappa}$.

General Frobenius transformations in H are defined as

$$\mathcal{G} = \sum_{d|\ell} \sum_{\kappa=1}^{n(d,p)} \mathcal{G}_{d\kappa}. \tag{197}$$

These transformations are intimately related to Galois theory. There is no analogue of these transformations in general finite quantum systems or in the harmonic oscillator.

It is easily seen that

$$\begin{aligned} &\mathcal{G}\mathcal{G}^\dagger = \mathbf{1}; \qquad \mathcal{G}^\ell = \mathbf{1} \\ &\mathcal{G}\pi_{d\kappa} = \pi_{d\kappa}\mathcal{G} = \mathcal{G}_{d\kappa}; \qquad \mathcal{G}^d \pi_{d\kappa} = \pi_{d\kappa} \\ &[\mathcal{G}, \Pi_d] = 0. \end{aligned} \tag{198}$$

From these it follows that

$$\Pi_1 \mathcal{G} = \Pi_1. \tag{199}$$

Therefore the

$$\mathrm{Gal}[H/H_1] = \{\mathbf{1}, \mathcal{G}, \mathcal{G}^2, \ldots, \mathcal{G}^{\ell-1}\}. \tag{200}$$

form a cyclic group of order ℓ whose elements leave fixed all states in H_1 (i.e., all states which are superpositions of $|X; m\rangle$ with $m \in \mathbb{Z}_p$). This is the analogue of the Galois group of equation (6) in the present context.

More generally, for $d|\ell$

$$\Pi_d \mathcal{G}^d = \Pi_d. \tag{201}$$

Therefore the

$$\mathrm{Gal}[H/H_d] = \{\mathbf{1}, \mathcal{G}^d, \mathcal{G}^{2d}, \ldots, \mathcal{G}^{\ell-d}\}. \tag{202}$$

form a cyclic group of order ℓ/d whose elements leave fixed all the states in H_d (i.e., all states which are superpositions of $|X; m\rangle$ with $m \in \mathrm{GF}(p^d)$). This is a subgroup of $\mathrm{Gal}[H/H_1]$, and it is the analogue of the Galois group of equation (8) in the present context.

The Frobenius transformations commute with the Fourier operator:

$$[\mathcal{G}, F] = 0. \tag{203}$$

Acting with $\mathcal{G}^\lambda$ on position and momentum states we get

$$\mathcal{G}^\lambda|X; m\rangle = |X; m^{p^\lambda}\rangle; \qquad \mathcal{G}^\lambda|P; m\rangle = |P; m^{p^\lambda}\rangle. \tag{204}$$

Acting with $\mathcal{G}^\lambda$ on both sides of displacement and symplectic operators we get

$$\begin{aligned}
&\mathcal{G}^\lambda D(\alpha, \beta)(\mathcal{G}^\dagger)^\lambda = D\big(\alpha^{p^\lambda}, \beta^{p^\lambda}\big)\\
&\mathcal{G}^\lambda S(q, r, s)(\mathcal{G}^\dagger)^\lambda = S\big(q^{p^\lambda}, r^{p^\lambda}, s^{p^\lambda}\big)\\
&\mathcal{G}^\lambda T(q, r, s; \alpha, \beta, \gamma)(\mathcal{G}^\dagger)^\lambda = T\big(q^{p^\lambda}, r^{p^\lambda}, s^{p^\lambda}; \alpha^{p^\lambda}, \beta^{p^\lambda}, \gamma\big).
\end{aligned} \tag{205}$$

In the special case that $\alpha, \beta, q, r, s \in \mathrm{GF}(p^d)$ we get

$$\begin{aligned}
&\alpha, \beta \in \mathrm{GF}(p^d) \rightarrow [\mathcal{G}^d, D(\alpha, \beta)] = 0\\
&q, r, s \in \mathrm{GF}(p^d) \rightarrow [\mathcal{G}^d, S(q, r, s)] = 0\\
&q, r, s, \alpha, \beta \in \mathrm{GF}(p^d) \rightarrow [\mathcal{G}^d, T(q, r, s; \alpha, \beta, \gamma)] = 0.
\end{aligned} \tag{206}$$

We next calculate the Wigner and Weyl functions of $\mathcal{G}$:

$$\begin{aligned}
W(\mathcal{G}; \alpha, \beta) &= \sum_m \chi(2\alpha\beta - 2\alpha m^p)\delta(2\beta, m + m^p)\\
\tilde{W}(\mathcal{G}; \alpha, \beta) &= \sum_m \chi(2^{-1}\alpha\beta + \alpha m^p)\delta(\beta, m - m^p).
\end{aligned} \tag{207}$$

Using equation (170) we expand $\mathcal{G}$ in terms of displacement operators:

$$\mathcal{G} = \frac{1}{p^\ell} \sum_{\alpha,\beta} \chi[-2^{-1}\alpha(\beta^p + \beta)]D(\alpha, \beta^p - \beta). \tag{208}$$

12.1. Spectrum of Frobenius transformations

The fact that $\mathcal{G}^{\ell} = \mathbf{1}$ implies that its eigenvalues are powers of Ω_{ℓ}:

$$\begin{gathered}\mathcal{G} = \varpi(0) + \Omega_{\ell}(1)\varpi(1) + \cdots + \Omega_{\ell}(\ell-1)\varpi(\ell-1)\\ \varpi(\lambda)\varpi(\mu) = \varpi(\lambda)\delta(\lambda,\mu); \qquad \sum_{\lambda}\varpi(\lambda) = \mathbf{1}; \qquad \lambda,\mu\in\mathbb{Z}_{\ell}.\end{gathered} \tag{209}$$

Here $\varpi(\lambda)$ are orthogonal projectors to the eigenspaces corresponding to the various eigenvalues of $\mathcal{G}$. These can be expressed in terms of powers of $\mathcal{G}$ as

$$\varpi(\lambda) = \frac{1}{\ell}\{\mathbf{1} + \mathcal{G}\Omega_{\ell}(-\lambda) + [\mathcal{G}\Omega_{\ell}(-\lambda)]^2 + \cdots + [\mathcal{G}\Omega_{\ell}(-\lambda)]^{\ell-1}\}. \tag{210}$$

Using the diagonal form of $\mathcal{G}$ given in equation (196) we find that

$$\varpi(0) = \sum_{d|\ell}\sum_{\kappa=1}^{n(d,p)}|\mathfrak{P}; m(d,\kappa,d)\rangle\langle\mathfrak{P}; m(d,\kappa,d)|, \tag{211}$$

where $\varpi(0)$ is a projector into a space spanned by one vector from each Frobenius subspace and whose dimension is $\mathfrak{M}(\ell,p)$ (see equation (13)). More generally, taking into account that $\Omega_d(-\nu) = \Omega_{\ell}(-\nu\ell/d)$ we find that

$$\varpi(\lambda) = \sum_{d|\ell}\sum_{\kappa=1}^{n(d,p)}|\mathfrak{P}; m(d,\kappa,\nu)\rangle\langle\mathfrak{P}; m(d,\kappa,\nu)|; \qquad -\nu\ell/d = \lambda(\mathrm{mod}\ \ell). \tag{212}$$

The summation here involves only those divisors d of ℓ for which there exists some ν so that $-\nu\ell/d = \lambda(\mathrm{mod}\,\ell)$.

Using equation (209) we show that $\mathcal{G}^d$ (where $d|\ell$) can be written as

$$\begin{gathered}\mathcal{G}^d = \varpi_d(0) + \Omega_{\ell/d}(1)\varpi_d(1) + \cdots + \Omega_{\ell/d}\left(\frac{\ell}{d}-1\right)\varpi_d\left(\frac{\ell}{d}-1\right)\\ \varpi_d(m) = \varpi(m) + \varpi\left(m+\frac{\ell}{d}\right) + \cdots + \varpi\left(m+\frac{(d-1)\ell}{d}\right); \qquad m\in\mathbb{Z}_{\ell/d}\end{gathered} \tag{213}$$

and we can then prove that

$$\Pi_d\varpi_d(m) = \delta(m,0)\Pi_d. \tag{214}$$

This shows that the space H_d is a subspace of the combined eigenspace of $\mathcal{G}$ corresponding to the eigenvalues $1, \Omega_{\ell}(d), \ldots, \Omega_{\ell}(\ell-d)$. A special case of equation (214) is that

$$\Pi_1\varpi(m) = \delta(m,0)\Pi_1. \tag{215}$$

13. Constants of motion in Galois systems with Frobenius symmetry

We say that a Galois quantum system has a Frobenius symmetry, when its Hamiltonian h commutes with $\mathcal{G}$ (and therefore with all $\varpi(\lambda)$):

$$[\mathcal{G}, h] = [\varpi(\lambda), h] = 0. \tag{216}$$

Examples are systems with the Hamiltonians h_A and h_B of equation (102).

We assume that at the time $t = 0$, a system with Frobenius symmetry is described by the density matrix $\rho(0)$ (which is a $p^{\ell}\times p^{\ell}$ matrix). Then at time t, its density matrix is

$$\rho(t) = \exp(\mathrm{i}th)\rho(0)\exp(-\mathrm{i}th). \tag{217}$$

We consider the following ℓ^2 'submatrices' (which are also $p^\ell \times p^\ell$ matrices):

$$\begin{aligned}&\rho_{\lambda\mu}(t) \equiv \varpi(\lambda)\rho(t)\varpi(\mu); \qquad \sum_{\lambda,\mu}\rho_{\lambda\mu}(t) = \rho(t);\\ &[\rho_{\lambda\mu}(t)]^\dagger = \rho_{\mu\lambda}(t); \qquad \lambda, \mu \in \mathbb{Z}_\ell.\end{aligned} \tag{218}$$

It is easily seen that in the special case that ρ commutes with $\mathcal{G}$ (and therefore with all $\varpi(\lambda)$), the off-diagonal submatrices are equal to 0. But in general, they are not zero.

A consequence of the fact that the evolution operator $\exp(\mathrm{i}th)$ commutes with $\varpi(\lambda)$ is that each submatrix evolves independently of the other submatrices, as

$$\rho_{\lambda\mu}(t) = \exp(\mathrm{i}th)\rho_{\lambda\mu}(0)\exp(-\mathrm{i}th). \tag{219}$$

13.1. Time evolution of the submatrices

We first consider the diagonal submatrices $\rho_{\lambda\lambda}(t)$, which are Hermitian matrices. Their eigenvalues are constant in time, because time evolution is a unitary transformation. These can be written in a diagonal form as

$$\begin{aligned}&\rho_{\lambda\lambda}(t) = \mathcal{U}_\lambda(t)K_\lambda[\mathcal{U}_\lambda(t)]^\dagger\\ &\mathcal{U}_\lambda(t) = \exp(\mathrm{i}th)\mathcal{U}_\lambda(0); \qquad \mathcal{U}_\lambda(t)[\mathcal{U}_\lambda(t)]^\dagger = \mathbf{1}.\end{aligned} \tag{220}$$

Here $\mathcal{U}_\lambda(t)$ is unitary operator. K_λ is a diagonal matrix with non-negative diagonal elements, which contains the eigenvalues of $\rho_{\lambda\lambda}(t)$, and does not depend on time. It is easily seen that

$$\mathrm{tr}K_\lambda = \mathrm{tr}[\rho(t)\varpi(\lambda)]; \qquad \sum_\lambda \mathrm{tr}K_\lambda = 1. \tag{221}$$

Physically, the eigenvalues of $\rho_{\lambda\lambda}(t)$ divided by $\mathrm{tr}\rho_{\lambda\lambda}(t) = \mathrm{tr}[\rho(t)\varpi(\lambda)]$ are probabilities.

We next consider the off-diagonal submatrices $\rho_{\lambda\mu}(t)$ with $\lambda \neq \mu$. All their eigenvalues are zero and in an appropriate basis, they are strictly triangular matrices, i.e., all elements $\rho_{\lambda\mu}(i, j)$ with indices $i \geqslant j$ (or $i \leqslant j$) are zero. We work in an arbitrary basis and define the

$$\begin{aligned}&R_{\lambda\mu}(t) = \rho_{\lambda\mu}(t)[\rho_{\lambda\mu}(t)]^\dagger = \varpi(\lambda)\rho(t)\varpi(\mu)\rho(t)\varpi(\lambda)\\ &S_{\lambda\mu}(t) = [\rho_{\lambda\mu}(t)]^\dagger\rho_{\lambda\mu}(t) = \varpi(\mu)\rho(t)\varpi(\lambda)\rho(t)\varpi(\mu).\end{aligned} \tag{222}$$

In general, $R_{\lambda\mu}(t)$ is not equal to $S_{\lambda\mu}(t)$, i.e., the matrices $\rho_{\lambda\mu}(t)$ are not normal. We consider the singular values of $\rho_{\lambda\mu}(t)$, i.e., the eigenvalues of $[R_{\lambda\mu}(t)]^{1/2}$, which are also the eigenvalues of $[S_{\lambda\mu}(t)]^{1/2}$ and are non-negative numbers. Under unitary time evolution, the singular values are constant in time. We write $R_{\lambda\mu}(t)$ as

$$\begin{aligned}&R_{\lambda\mu}(t) = \mathcal{V}_{\lambda\mu}(t)\mathcal{K}_{\lambda\mu}[\mathcal{V}_{\lambda\mu}(t)]^\dagger\\ &\mathcal{V}_{\lambda\mu}(t) = \exp(\mathrm{i}th)\mathcal{V}_{\lambda\mu}(0); \qquad \mathcal{V}_{\lambda\mu}(t)[\mathcal{V}_{\lambda\mu}(t)]^\dagger = \mathbf{1},\end{aligned} \tag{223}$$

where $\mathcal{K}_{\lambda\mu}$ is a diagonal matrix with non-negative diagonal elements, which contains the eigenvalues of $R_{\lambda\mu}(t)$ (which are the squares of the singular values of $\rho_{\lambda\mu}(t)$), and does not depend on time. $\mathcal{V}_{\lambda\mu}(t)$ is a unitary matrix.

A polar decomposition of the matrix $\rho_{\lambda\mu}(t)$ gives

$$\begin{aligned}&\rho_{\lambda\mu}(t) = [R_{\lambda\mu}(t)]^{1/2}\Phi_{\lambda\mu}(t); \qquad \Phi_{\lambda\mu}(t)[\Phi_{\lambda\mu}(t)]^\dagger = \mathbf{1}\\ &\rho_{\mu\lambda}(t) = [\rho_{\lambda\mu}(t)]^\dagger = [\Phi_{\lambda\mu}(t)]^\dagger[R_{\lambda\mu}(t)]^{1/2},\end{aligned} \tag{224}$$

where $\Phi_{\lambda\mu}(t)$ are unitary matrices representing the 'exponential of the phase'. Equation (223) shows that

$$[R_{\lambda\mu}(t)]^{1/2} = \mathcal{V}_{\lambda\mu}(t)\mathcal{K}_{\lambda\mu}^{1/2}[\mathcal{V}_{\lambda\mu}(t)]^\dagger, \tag{225}$$

and we can write $\rho_{\lambda\mu}(t)$ as

$$\rho_{\lambda\mu}(t) = \mathcal{V}_{\lambda\mu}(t)\mathcal{K}_{\lambda\mu}^{1/2}\mathcal{T}_{\lambda\mu}(t); \qquad \mathcal{T}_{\lambda\mu}(t) = [\mathcal{V}_{\lambda\mu}(t)]^{\dagger}\Phi(t). \tag{226}$$

This is the singular value decomposition of $\rho_{\lambda\mu}(t)$.

It is easily seen that

$$\sum_{\lambda,\mu} \mathrm{tr}\big(\mathcal{K}_{\lambda\mu}^2\big) = \mathrm{tr}[\rho^2(t)], \tag{227}$$

where the summation includes both diagonal and off-diagonal terms. For the diagonal terms the $\mathcal{K}_{\lambda\lambda}$ is the same as the K_λ in equation (220).

13.2. Constants of motion

We study in more detail the diagonal submatrices $\rho_{\lambda\lambda}(t)$. Their characteristic polynomials are

$$\det[y\mathbf{1} - \rho_{\lambda\lambda}(t)] = y^{p^\ell} + a_{\lambda\lambda}(p^\ell - 1)y^{p^\ell - 1} + \cdots + a_{\lambda\lambda}(0), \tag{228}$$

where $a_{\lambda\lambda}(\mu)$ denotes the coefficient of p^μ. The eigenvalues of $\rho_{\lambda\lambda}(t)$ are constant in time, and therefore their characteristic polynomials are constant in time:

$$\det[y\mathbf{1} - \rho_{\lambda\lambda}(t)] = \det[y\mathbf{1} - \rho_{\lambda\lambda}(0)]. \tag{229}$$

In other words the coefficients $a_{\lambda\lambda}(\mu)$ do not depend on time.

The $-a_{\lambda\lambda}(p^\ell - 1)$ is equal to the trace of $\rho_{\lambda\lambda}(t)$ and is a probability. These probabilities are constant in time:

$$\mathrm{tr}[\rho(t)\varpi(\lambda)] = \mathrm{tr}[\rho(0)\varpi(\lambda)]. \tag{230}$$

The probabilities $\mathrm{tr}[\rho(t)\varpi(\lambda)]$ are ℓ constants of motion in systems with Frobenius symmetries. Their sum is equal to 1 and therefore $\ell - 1$ of them are independent.

13.3. Example with GF(9)

As an example, we consider a Galois quantum system where position and momentum take values in GF(9). For calculations we choose the irreducible polynomial $P(\epsilon) = \epsilon^2 + \epsilon + 2$. Taking into account equation (69), we see that

$$\begin{aligned}\mathcal{G} = |X;0\rangle\langle X;0| + |X;1\rangle\langle X;1| + |X;2\rangle\langle X;2| + |X;1+2\epsilon\rangle\langle X;2+\epsilon| \\ + |X;2+\epsilon\rangle\langle X;1+2\epsilon| + |X;\epsilon\rangle\langle X;2+2\epsilon| + |X;2+2\epsilon\rangle\langle X;\epsilon| \\ + |X;1+\epsilon\rangle\langle X;2\epsilon| + |X;2\epsilon\rangle\langle X;1+\epsilon|.\end{aligned} \tag{231}$$

In this case

$$\mathcal{G}^2 = \mathbf{1}; \qquad \mathcal{G} = \varpi(0) - \varpi(1). \tag{232}$$

We assume that the Hamiltonian of this system is h_A of equation (102), which commutes with $\mathcal{G}$. If ρ is the density matrix of the system we use the notation

$$\rho_X(m,n) = \langle X;m|\rho|X;n\rangle. \tag{233}$$

Using the fact that $\varpi(1) = (\mathbf{1} - \mathcal{G})/2$ we find

$$\begin{aligned}\mathrm{tr}[\rho\varpi(1)] = \tfrac{1}{2}[\rho_X(\epsilon,\epsilon) + \rho_X(1+\epsilon,1+\epsilon) + \rho_X(2+\epsilon,2+\epsilon) + \rho_X(1+2\epsilon,1+2\epsilon) \\ + \rho_X(2\epsilon,2\epsilon) + \rho_X(2+2\epsilon,2+2\epsilon) - \rho_X(2+2\epsilon,\epsilon) - \rho_X(\epsilon,2+2\epsilon) \\ - \rho_X(2\epsilon,1+\epsilon) - \rho_X(1+\epsilon,2\epsilon) - \rho_X(1+2\epsilon,2+\epsilon) - \rho_X(2+\epsilon,1+2\epsilon)].\end{aligned} \tag{234}$$

This probability is constant in time and it is a constant of motion in this example. The $\mathrm{tr}[\rho\varpi(0)]$ is also constant, but it is not independent:

$$\mathrm{tr}[\rho\varpi(0)] = 1 - \mathrm{tr}[\rho\varpi(1)]. \tag{235}$$

13.4. Example with GF(81)

As a second example, we consider a Galois quantum system where position and momentum take values in GF(81). In this case in addition to the irreducible polynomials of equation (37), we have 18 more irreducible polynomials of order 4. The Frobenius transformation $\mathcal{G}$ obeys the relations

$$\mathcal{G}^4 = \mathbf{1}; \qquad \mathcal{G} = \varpi(0) + \mathrm{i}\varpi(1) - \varpi(2) - \mathrm{i}\varpi(3). \tag{236}$$

Following our general notation, we call Π_1 the projector to the three-dimensional Hilbert space H_1 which is spanned by the position states $|X; m\rangle$, where m belongs to the subfield $\mathbb{Z}_3$, and Π_2 the projector to the nine-dimensional Hilbert space H_2 which is spanned by the position states $|X; m\rangle$, where m belongs to the subfield GF(9). Then

$$\begin{aligned}
&\mathcal{G}\Pi_1 = \Pi_1; \qquad \mathcal{G}^2\Pi_2 = \Pi_2; \qquad \mathcal{G}^2 = [\varpi(0) + \varpi(2)] - [\varpi(1) + \varpi(3)]\\
&\varpi(0)\Pi_1 = \Pi_1; \qquad \varpi(1)\Pi_1 = \varpi(2)\Pi_1 = \varpi(3)\Pi_1 = 0\\
&[\varpi(0) + \varpi(2)]\Pi_2 = \Pi_2; \qquad [\varpi(1) + \varpi(3)]\Pi_2 = 0.
\end{aligned} \tag{237}$$

In this example, the $\mathrm{tr}[\rho\varpi(0)]$, $\mathrm{tr}[\rho\varpi(1)]$ and $\mathrm{tr}[\rho\varpi(2)]$ are three independent constants of motion. The

$$\mathrm{tr}[\rho\varpi(3)] = 1 - \mathrm{tr}[\rho\varpi(0)] - \mathrm{tr}[\rho\varpi(1)] - \mathrm{tr}[\rho\varpi(2)] \tag{238}$$

is also a constant of motion, but it is not independent.

14. The group $\mathfrak{R}[\mathrm{GF}(p^\ell)]$ of Frobenius, displacement and symplectic transformations

The unitary operators

$$R(\lambda; q, r, s; \alpha, \beta, \gamma) \equiv \mathcal{G}^\lambda T(q, r, s; \alpha, \beta, \gamma) = T\big(q^{p^\lambda}, r^{p^\lambda}, s^{p^\lambda}; \alpha^{p^\lambda}, \beta^{p^\lambda}, \gamma\big)\mathcal{G}^\lambda \tag{239}$$

perform Frobenius, displacement and symplectic transformations. It is easily seen that

$$R(\lambda_1; q_1, r_1, s_1; \alpha_1, \beta_1, \gamma_1)R(\lambda_2; q_2, r_2, s_2; \alpha_2, \beta_2, \gamma_2) = R(\lambda; q, r, s; \alpha, \beta, \gamma), \tag{240}$$

where

$$\begin{aligned}
\lambda &= \lambda_1 + \lambda_2\\
q &= q_1^n q_2 + r_2 s_1^n; \qquad n = p^{\ell - \lambda_2}\\
r &= q_2 r_1^n + r_2 q_1^{-n}\big(1 + r_1^n s_1^n\big)\\
s &= q_1^n s_2 + s_1^n q_2^{-1}(1 + r_2 s_2)\\
\alpha &= \alpha_1^n q_2 + \alpha_2 - \beta_1^n r_2\\
\beta &= -\alpha_1^n s_2 + \beta_2 + \beta_1^n (1 + r_2 s_2) q_2^{-1}\\
\gamma &= \gamma_1 + \gamma_2 + 2^{-1}\big[\alpha_1^n \alpha_2 s_2 + \alpha_1^n \beta_2 q_2 - \beta_1^n \beta_2 r_2 - \beta_1^n \alpha_2 (1 + r_2 s_2) q_2^{-1}\big].
\end{aligned} \tag{241}$$

The operators $R(\lambda; q, r, s; \alpha, \beta, \gamma)$ form a group which we denote as $\mathfrak{R}[\mathrm{GF}(p^\ell)]$. Using equation (205), we easily show that the $\mathfrak{T}[\mathrm{GF}(p^\ell)]$ group of displacement and symplectic transformations is a normal subgroup of $\mathfrak{R}[\mathrm{GF}(p^\ell)]$. The $\mathrm{Gal}[H/H_1]$ is also a subgroup of $\mathfrak{R}[\mathrm{GF}(p^\ell)]$ and

$$\mathfrak{T}[\mathrm{GF}(p^\ell)] \bigcap \mathrm{Gal}[H/H_1] = \{\mathbf{1}\}. \tag{242}$$

Therefore, the group $\mathfrak{R}[\mathrm{GF}(p^\ell)]$ is the semidirect product of the $\mathfrak{T}[\mathrm{GF}(p^\ell)]$ by the $\mathrm{Gal}[H/H_1]$ group of equation (200). Consequently, the quotient group $\mathfrak{R}[\mathrm{GF}(p^\ell)]/\mathfrak{T}[\mathrm{GF}(p^\ell)]$ is isomorphic to the $\mathrm{Gal}[H/H_1]$ group.

15. General transformations that leave invariant the Frobenius subspaces

In Galois fields, the Galois group of equation (6) consists of *all* automorphisms of $\mathrm{GF}(p^\ell)$ which map the conjugates to each other. In this section we study the corresponding problem in our context, which is to find *all* transformations that leave invariant the Frobenius subspaces. The Galois group of equation (200) is only a very small subgroup, of the group of these transformations.

15.1. Dual Frobenius transformations

We act with the Fourier transform of equation (96) on both sides of $\mathcal{G}_{d\kappa}$ and get the dual Frobenius transforms

$$\begin{aligned}\mathcal{L}_{d\kappa} &= \mathfrak{F}_{d\kappa}\mathcal{G}_{d\kappa}\mathfrak{F}_{d\kappa}^\dagger = \sum_{\nu\in\mathbb{Z}_d}\Omega_d(\nu)|X;m(d,\kappa,\nu)\rangle\langle X;m(d,\kappa,\nu)| \\ &= \sum_{\nu\in\mathbb{Z}_d}|\mathfrak{P};m(d,\kappa,\nu+1)\rangle\langle\mathfrak{P};m(d,\kappa,\nu)|. \end{aligned} \tag{243}$$

General dual Frobenius transformations in H are defined as

$$\mathcal{L} = \sum_{d|\ell}\sum_{\kappa=1}^{n(d,p)}\mathcal{L}_{d\kappa}. \tag{244}$$

It has properties similar to those of $\mathcal{G}$. For example,

$$\mathcal{L}\Pi_1 = \Pi_1\mathcal{L} = \Pi_1 \tag{245}$$

and the

$$\mathrm{Gal}[H/H_1] = \{\mathbf{1},\mathcal{L},\mathcal{L}^2,\ldots,\mathcal{L}^{\ell-1}\} \tag{246}$$

form a cyclic group of order ℓ whose elements leave fixed all states in H_1. More generally, for $d|\ell$,

$$\mathcal{L}^d\Pi_d = \Pi_d\mathcal{L}^d = \Pi_d \tag{247}$$

and the

$$\mathrm{Gal}[H/H_d] = \{\mathbf{1},\mathcal{L}^d,\mathcal{L}^{2d},\ldots,\mathcal{L}^{\ell-d}\} \tag{248}$$

form a cyclic group of order ℓ/d whose elements leave fixed all the states in H_d.

15.2. General transformations in $\mathfrak{H}_{d\kappa}$

The operators $\mathcal{G}_{d\kappa}$ and $\mathcal{L}_{d\kappa}$ form a Heisenberg–Weyl group in the Frobenius subspace $\mathfrak{H}_{d\kappa}$:

$$\mathcal{G}_{d\kappa}^\beta\mathcal{L}_{d\kappa}^\alpha = \mathcal{L}_{d\kappa}^\alpha\mathcal{G}_{d\kappa}^\beta\Omega_d(-\alpha\beta); \qquad \mathcal{G}_{d\kappa}^d = \mathcal{L}_{d\kappa}^d = \pi_{d\kappa}; \qquad \alpha,\beta\in\mathbb{Z}_d. \tag{249}$$

An arbitrary operator $\Theta_{d\kappa}$ acting on the Frobenius subspace $\mathfrak{H}_{d\kappa}$ can be written as

$$\Theta_{d\kappa} = \sum_{\alpha,\beta}\tau_{d\kappa}(\alpha,\beta)\mathcal{L}_{d\kappa}^\alpha\mathcal{G}_{d\kappa}^\beta; \qquad \tau_{d\kappa}(\alpha,\beta) = \frac{1}{d}\mathrm{tr}\big[\Theta_{\mathrm{d}\kappa}\mathcal{L}_{\mathrm{d}\kappa}^{-\alpha}\mathcal{G}_{\mathrm{d}\kappa}^{-\beta}\big]\Omega_{\mathrm{d}}(-\alpha\beta); \qquad \alpha,\beta\in\mathbb{Z}_{\mathrm{d}} \tag{250}$$

This is analogous to equation (170).

15.3. Unitary transformations that leave invariant the Frobenius subspaces

We consider the following direct product of groups:

$$g = \prod_{d|\ell} \prod_{\kappa=1}^{n(d,p)} U(d)_{d\kappa}. \tag{251}$$

Here we use the notation $U(d)_{d\kappa}$ for the group of $U(d)$ transformations acting on the Frobenius subspace $\mathfrak{H}_{d\kappa}$. These are the most general unitary transformations which leave all the $\mathfrak{H}_{d\kappa}$ invariant in the sense that when they act on a state that belongs in $\mathfrak{H}_{d\kappa}$ they produce another state that belongs entirely in $\mathfrak{H}_{d\kappa}$. Operators $\mathcal{U}$ in g obey the relations:

$$[\mathcal{U}, \pi_{d\kappa}] = 0. \tag{252}$$

The transformations $\mathcal{U}$ can be written in terms of the operators of equation (250) as

$$\mathcal{U} = \sum_{d|\ell} \sum_{\kappa=1}^{n(d,p)} \left[\sum_{\alpha,\beta} \tau_{d\kappa}(\alpha_{d\kappa}, \beta_{d\kappa}) \mathcal{L}_{d\kappa}^{\alpha_{d\kappa}} \mathcal{G}_{d\kappa}^{\beta_{d\kappa}} \right]; \qquad \alpha_{d\kappa}, \beta_{d\kappa} \in \mathbb{Z}_d, \tag{253}$$

where the requirement of unitary $\mathcal{U}$ imposes constraints on the coefficients $\tau_{d\kappa}(\alpha_{d\kappa}, \beta_{d\kappa})$.

16. Discrete symmetries and analytic representations in Riemann surfaces

A discrete symmetry, like the Frobenius symmetry in Galois quantum systems, introduces a 'multivaluedness'. Quantum states related to each other through this symmetry, behave in the same way with regard to certain properties. In this section we use analytic representations to show a conceptual link between this kind of multivaluedness and the multivaluedness in coverings of Riemann surfaces.

A general review on analytic representations in quantum mechanics has been given in [57]. Analytic representations in Riemann surfaces for general systems with discrete symmetries have been discussed in [58]. These are briefly summarized in the subsection below and then applied in the context of Galois quantum systems with Frobenius symmetries.

16.1. Analytic representation of general systems with discrete symmetries in the d-sheeted complex plane

We consider a harmonic oscillator described by the infinite-dimensional Hilbert space H. Let $a^\dagger, a$ be the creation and annihilation operators and $|M\rangle_n$ the number eigenstates:

$$|M\rangle_n = \frac{(a^\dagger)^M}{(M!)^{1/2}} |0\rangle_n, \tag{254}$$

where the subscript n indicates the number states. We split the Hilbert space H of the system as

$$\begin{aligned} \mathsf{H} &= \bigoplus_{m=0}^{d-1} \mathbb{H}_m = \bigoplus_{N=0}^{\infty} \mathsf{H}_N \\ \mathbb{H}_m &= \mathrm{span}\{|m\rangle_n, |d+m\rangle_n, |2d+m\rangle_n, \ldots\} \\ \mathsf{H}_N &= \mathrm{span}\{|dN\rangle_n, |dN+1\rangle_n, \ldots, |dN+d-1\rangle_n\}. \end{aligned} \tag{255}$$

The spaces $\mathbb{H}_m$ are infinite dimensional and the spaces H_N are d dimensional. We call $\mathbb{P}(m)$ the projectors to the spaces $\mathbb{H}_m$. Within the spaces H_N we perform Fourier transforms with the operator

$$\mathsf{F} = d^{-1/2} \sum_{N=0}^{\infty} \left[\sum_{m,k \in \mathbb{Z}_d} \Omega_d(-mk) |m + dN\rangle_{n\,n}\langle k + dN| \right]; \qquad \mathsf{F}^4 = \mathbf{1}. \tag{256}$$

Acting with it on the number states we get the 'dual number states'

$$|M\rangle_d = \mathsf{F}|M\rangle_n. \tag{257}$$

Here the subscript d indicates dual number states. We call $\wp(m)$ the projectors:

$$\wp(m) = \mathsf{F}\mathbb{P}(m)\mathsf{F}^\dagger = \sum_{N=0}^{\infty} |m + dN\rangle_{d\,d}\langle m + dN|. \tag{258}$$

We consider the unitary operator

$$\begin{aligned} \mathsf{G} &= \sum_{N=0}^{\infty} \left[\sum_{m \in \mathbb{Z}_d} |dN + m + 1\rangle_{n\,n}\langle dN + m| \right] \\ &= \wp(0) + \Omega_d(1)\wp(1) + \cdots + \Omega_d(d-1)\wp(d-1). \end{aligned} \tag{259}$$

It is easily seen that

$$\mathsf{G}^d = \mathsf{G}\mathsf{G}^\dagger = \mathbf{1}. \tag{260}$$

The projectors $\wp(m)$ can be written in terms of G as

$$\wp(m) = \frac{1}{d}\{\mathbf{1} + \Omega_d(-m)\mathsf{G} + \Omega_d(-2m)\mathsf{G}^2 + \cdots + \Omega_d[-m(d-1)]\mathsf{G}^{d-1}\}. \tag{261}$$

We assume that the Hamiltonian h of the system commutes with G:

$$[\mathsf{G}, \mathsf{h}] = 0. \tag{262}$$

Then the system has a discrete symmetry and there is a multivaluedness associated with it. For example, if $|s\rangle$ is an eigenstate of h (or any other operator which commutes with G), then all states $\mathsf{G}^m|s\rangle$ are also eigenstates with the same eigenvalue.

We assume that at the time $t = 0$, the system is described by the density matrix $\rho(0)$. Since the Hamiltonian h commutes with G, it also commutes with all the $\wp(m)$. Therefore the probabilities $\mathrm{tr}[\rho(t)\wp(m)]$ are constant in time:

$$\mathrm{tr}[\rho(t)\wp(m)] = \mathrm{tr}[\rho(0)\wp(m)]; \qquad \rho(t) = \exp(\mathrm{i}t\mathsf{h})\rho(0)\exp(-\mathrm{i}t\mathsf{h}). \tag{263}$$

The sum of these probabilities is equal to 1, and therefore there are $d-1$ independent conserved quantities.

Let $C^* = C - \{0\}$ be the punctured complex plane. We consider the Riemann surface $C^*/\mathbb{Z}_d$ associated with the map $z^{1/d}$. The covering surface of this Riemann surface is the d-sheeted complex plane with the cuts T_m

$$T_m = \{z = r\Omega_d(m); r \geqslant 0\}; \qquad m = 0, \ldots, d-1 \tag{264}$$

and the sheets

$$\Xi_m = \left\{ z = r\exp(\mathrm{i}\phi); r \geqslant 0; \ \frac{2\pi m}{d} < \phi < \frac{2\pi(m+1)}{d} \right\}. \tag{265}$$

The sheet number of a complex number z is defined as

$$\tau(z; d) = \mathrm{IP}\left(\frac{d\arg(z)}{2\pi}\right); \qquad \tau(z; d) \in \mathbb{Z}_d, \tag{266}$$

where IP stands for the integer part of the number.

Let

$$|s\rangle = \sum_{M=0}^{\infty} s(M)|M\rangle_n; \qquad \sum_{M=0}^{\infty} |s(M)|^2 = 1 \tag{267}$$

be an arbitrary state in H. To each M corresponds a pair (m, N) such that:

$$\begin{aligned} m &= M(\text{mod } d); \qquad && m \in \mathbb{Z}_d \\ N &= \frac{M-m}{d}; && N \in \mathbb{Z}. \end{aligned} \tag{268}$$

We represent the $s(M)|M\rangle_n$ part of the state $|s\rangle$ with a function which is non-zero only in the m-sheet and it is $s(M)z^{Nd}(N!)^{-1/2}$. Therefore the full state $|s\rangle$ is represented with the following function in the d-sheeted complex plane:

$$S_1(z) = \sum_{N=0}^{\infty} s[\tau(z; d) + Nd]z^{Nd}(N!)^{-1/2}. \tag{269}$$

In the sheet Ξ_m, this function represents only the projection $\mathbb{P}_m|s\rangle$ of the state $|s\rangle$ in the subspace $\mathbb{H}_m$. But when we consider the function $S_1(z)$ in all the d sheets we get all the projections $\mathbb{P}_m|s\rangle$ and therefore the full state $|s\rangle$.

The function $S_1(z)$ is analytic in the interior of all sheets Ξ_m and has discontinuities across the cuts T_m given by

$$\Delta_1(z; m) = \sum_{N=0}^{\infty}[s(m + Nd) - s(m + Nd - 1)]z^{dN}(N!)^{-1/2}. \tag{270}$$

In this representation the transformations G are implemented as

$$\mathsf{G}^m|s\rangle \to S_1[\Omega_d(-m)z]. \tag{271}$$

This is easily seen from the fact that

$$\tau[\Omega_d(-m)z; d] = \tau(z; d) - m. \tag{272}$$

The fact that $\Omega_d(d) = 1$ expresses the relation $\mathsf{G}^d = \mathbf{1}$ in this formalism.

The scalar product of two states $|s\rangle$ and $|r\rangle$ is given by

$$\begin{aligned} \langle s|r\rangle &= \int_C \mathrm{d}\mu_d(z) \exp(-|z|^{2d})[S_1(z)]^* R_1(z) = \sum_{M=0}^{\infty}[s(M)]^* r(M) \\ \mathrm{d}\mu_d(z) &= \mathrm{d}^2|z|^{2(d-1)}\frac{\mathrm{d}z_R\, \mathrm{d}z_I}{\pi}, \end{aligned} \tag{273}$$

where z_R, z_I are the real and imaginary parts of z, correspondingly.

We next introduce another analytic representation for the same system, in the ℓ-sheeted complex plane where ℓ is an integer multiple of d. In the present context this is a more complicated representation, without any physical motivation behind it. However, in the following subsection this representation will be very important, and the physical motivation for it will become clear.

In the ℓ-sheeted complex plane the sheet number $\tau(z; \ell)$ of a complex number z, takes values in $\mathbb{Z}_\ell$. We define the sheet number modulo d (where $d|\ell$) of a complex number z in the ℓ-sheeted complex plane as

$$\tau(z; \ell; \text{mod } d) = \tau(z; \ell)(\text{mod } d); \qquad \tau(z; \ell; \text{mod } d) \in \mathbb{Z}_d. \tag{274}$$

In this way the first d sheets are numbered from 0 to $d - 1$; and then the next d sheets from 0 to $d - 1$; until the last sheet which is numbered with $d - 1$. It is clear that we have ℓ/d sheets with the same number $\tau(z; \ell; \text{mod } d)$.

We now represent the state of equation (271) with the following function in the ℓ-sheeted complex plane:

$$S_2(z) = \frac{d}{\ell} \sum_{N=0}^{\infty} s[\tau(z;\ell;\operatorname{mod} d) + Nd] z^{N\ell} (N!)^{-1/2}. \tag{275}$$

In the first d sheets we have d functions which represent the $\mathbb{P}_m|s\rangle$ components of the state $|s\rangle$. The fact that $\tau_d(z;\ell;\operatorname{mod} d)$ is defined modulo d, implies that there is periodicity in the next d sheets, which continues up to the last d sheets (the d is a divisor of ℓ). In other words, $S_2(z)$ is the same in all ℓ/d sheets with the same $\tau(z;\ell;\operatorname{mod} d)$:

$$S_2[z\Omega_\ell(d)] = S_2(z). \tag{276}$$

In this representation the transformations G are implemented as

$$\mathsf{G}^m|s\rangle \to S_2[z\Omega_\ell(-m)] \tag{277}$$

and equation (276) expresses the relation $\mathsf{G}^d = \mathbf{1}$ in this formalism.

In this representation the scalar product of two states $|s\rangle$ and $|r\rangle$ is given by

$$\begin{aligned}\langle s|r\rangle &= \int_C \mathrm{d}\mu_\ell(z)\exp(-|z|^{2\ell})[S_1(z)]^* R_1(z) = \sum_{M=0}^{\infty}[s(M)]^* r(M)\\ \mathrm{d}\mu_\ell(z) &= \ell^2|z|^{2(\ell-1)}\frac{\mathrm{d}z_R\,\mathrm{d}z_I}{\pi},\end{aligned} \tag{278}$$

which is the same as equation (273) with d replaced by ℓ. The factor d/ℓ in equation (275) compensates for the periodicity, so that the scalar product is the same.

16.2. Analytic representation of Galois quantum systems with Frobenius symmetries in the ℓ-sheeted complex plane

We now apply the formalism of the previous subsection to Galois quantum systems [49]. We will see that here there is a lot of extra structure related to the fact that the Frobenius symmetry obeys not only the relation $\mathcal{G}^\ell = \mathbf{1}$ but also the relations $\mathcal{G}^d \pi_{d\kappa} = \pi_{d\kappa}$ for all divisors d of ℓ. This needs to be embodied in the analytic representation.

We consider a Galois quantum system described by the Hilbert space H. Using the orthonormal basis $|X; m(\mathfrak{N},\nu)\rangle$, we express the general state of this system as

$$|s\rangle = \sum_{\mathfrak{N}=1}^{\mathfrak{M}(\ell,p)} \sum_{\nu=1}^{d} s(\mathfrak{N},\nu)|X; m(\mathfrak{N},\nu)\rangle. \tag{279}$$

We first consider the projection of this state to the d-dimensional space $\mathfrak{H}_{\mathfrak{N}}$

$$\pi_{\mathfrak{N}}|s\rangle = \sum_{\nu=1}^{d} s(\mathfrak{N},\nu)|X; m(\mathfrak{N},\nu)\rangle. \tag{280}$$

Using equation (275), we represent it in the ℓ-sheeted complex plane (where $d|\ell$) with the function

$$\mathfrak{S}_{\mathfrak{N}}(z) = \frac{d}{\ell} s\,[\mathfrak{N}, \nu = \tau(z;\ell;\operatorname{mod} d)]\, z^{\ell\mathfrak{N}} (\mathfrak{N}!)^{-1/2}. \tag{281}$$

As we explained in equation (276), in this representation there is a periodicity

$$\mathfrak{S}_{\mathfrak{N}}[z\Omega_\ell(d)] = \mathfrak{S}_{\mathfrak{N}}(z). \tag{282}$$

The Frobenius transformations $\mathcal{G}$ are implemented as

$$\mathcal{G}^m \pi_{\mathfrak{N}}|s\rangle \to \mathfrak{S}_{\mathfrak{N}}[z\Omega_\ell(-m)] \tag{283}$$

and equation (282) expresses the relation $\mathcal{G}^d\pi_{\mathfrak{N}} = \pi_{\mathfrak{N}}$ (or $\mathcal{G}^d\pi_{d\kappa} = \pi_{d\kappa}$) in this formalism. We see here the motivation for introducing the representation of equation (275).

We now consider the full state $|s\rangle$ and represent it with the function

$$\mathfrak{S}(z) = \sum_{\mathfrak{N}=1}^{\mathfrak{M}(\ell,p)} \frac{d}{\ell} s\,[\mathfrak{N}, \nu = \tau(z; \ell; \bmod d)]\, z^{\ell\mathfrak{N}}(\mathfrak{N}!)^{-1/2}. \tag{284}$$

We recall that when $\mathfrak{N}$ is given, the corresponding (d, κ) are calculated using equation (20). In this representation, the Frobenius transformations $\mathcal{G}$ are implemented as

$$\mathcal{G}^m|s\rangle \to \mathfrak{S}[z\Omega_\ell(-m)]. \tag{285}$$

We have seen that the relations $\mathcal{G}^d\pi_{d\kappa} = \pi_{d\kappa}$ are embodied in the periodic structure of this formalism. Consequently, the relations $\mathcal{G}^d\Pi_d = \Pi_d$ are also embodied in the formalism (see equation (71)). The scalar product of two states is given by equation (278).

The function $\mathfrak{S}(z)$ is analytic in the interior of all sheets Ξ_m and has discontinuities across the cuts T_m given by

$$\Delta_m(z) = \sum_{\mathfrak{N}=1}^{\mathfrak{M}(\ell,p)} \frac{d}{\ell}\{s[\mathfrak{N}, \nu = m(\bmod d)] - s[\mathfrak{N}, \nu = m - 1(\bmod d)]\}z^{\ell\mathfrak{N}}(\mathfrak{N}!)^{-1/2}. \tag{286}$$

16.3. Example

We consider a Galois quantum system where the position and momentum take values in GF(9). For calculations we choose the irreducible polynomial $P(\epsilon) = \epsilon^2 + \epsilon + 2$. Taking into account equation (39) we write an arbitrary state in the nine-dimensional Hilbert space H as

$$\begin{aligned}|s\rangle = {} & s(1,1)|X;0\rangle + s(2,1)|X;1\rangle + s(3,1)|X;2\rangle + s(4,1)|X;1+2\epsilon\rangle + s(4,2)|X;2+\epsilon\rangle \\ & + s(5,1)|X;\epsilon\rangle + s(5,2)|X;2+2\epsilon\rangle + s(6,1)|X;1+\epsilon\rangle + s(6,2)|X;2\epsilon\rangle.\end{aligned} \tag{287}$$

The second labelling method has been used here.

We next consider the complex plane with a cut along the real axes. The sheet Ξ_1 consists of the complex numbers with $z_I > 0$; and the sheet Ξ_2 consists of the complex numbers with $z_I < 0$ The state $|s\rangle$ is represented with the functions $\mathfrak{S}(z)$ which in the sheet Ξ_1 is given by

$$\begin{aligned}\mathfrak{S}(z) = \frac{1}{2}\Bigg[& s(1,1)z^2 + s(2,1)\frac{z^4}{(2!)^{1/2}} + s(3,1)\frac{z^6}{(3!)^{1/2}} \\ & + s(4,1)\frac{z^8}{(4!)^{1/2}} + s(5,1)\frac{z^{10}}{(5!)^{1/2}} + s(6,1)\frac{z^{12}}{(6!)^{1/2}}\Bigg]\end{aligned} \tag{288}$$

and in the sheet Ξ_2 is given by

$$\begin{aligned}\mathfrak{S}(z) = \frac{1}{2}\Bigg[& s(1,1)z^2 + s(2,1)\frac{z^4}{(2!)^{1/2}} + s(3,1)\frac{z^6}{(3!)^{1/2}} \\ & + s(4,2)\frac{z^8}{(4!)^{1/2}} + s(5,2)\frac{z^{10}}{(5!)^{1/2}} + s(6,2)\frac{z^{12}}{(6!)^{1/2}}\Bigg].\end{aligned} \tag{289}$$

There is a discontinuity along the real axis given by

$$\Delta(z) = [s(4,1) - s(4,2)]\frac{z^8}{(4!)^{1/2}} + [s(5,1) - s(5,2)]\frac{z^{10}}{(5!)^{1/2}} + [s(6,1) - s(6,2)]\frac{z^{12}}{(6!)^{1/2}}. \tag{290}$$

If we perform the Frobenius transform of equation (231) on the state $|s\rangle$ we get the state $\mathcal{G}|s\rangle$ which is represented with the function $\mathfrak{S}(-z)$. This is given by equation (289) in the sheet Ξ_1 and by equation (288) in the sheet Ξ_2.

The scalar product of two states $|s\rangle$ and $|r\rangle$ represented with the functions $\mathfrak{S}(z)$ and $\mathfrak{R}(z)$ is given by

$$\langle s|r\rangle = \int_C \mathrm{d}\mu(z)\exp(-|z|^4)[\mathfrak{S}(z)]^*\mathfrak{R}(z); \qquad \mathrm{d}\mu_2(z) = 4|z|^2\frac{\mathrm{d}z_R\mathrm{d}z_I}{\pi}. \tag{291}$$

17. Physical implementation of a Galois system with spins

17.1. Angle states and operators in a spin $j = (p-1)/2$

An obvious physical system described by the p-dimensional Hilbert space $\mathcal{H}$ is a spin $j = (p-1)/2$. In this section we explain the correspondence between the various quantities introduced earlier and the usual quantities within the spin formalism.

We use the notation $|\mathcal{J}; jm\rangle$ for the angular momentum states. The extra $\mathcal{J}$ to the usual notation is not a variable, but it simply indicates angular momentum states. The correspondence with the states introduced earlier is given by

$$|\mathcal{X}; m\rangle; \leftrightarrow |\mathcal{J}; jm\rangle; \qquad j = \frac{p-1}{2}. \tag{292}$$

Here p is an odd prime and therefore j is an integer.

The Fourier operator of equation (56) is in this case

$$\mathcal{F} = (2j+1)^{-1/2}\sum_{m,n\in\mathbb{Z}_p}\omega(mn)|\mathcal{J}; jm\rangle\langle\mathcal{J}; jn|. \tag{293}$$

Acting with it on the angular momentum states we get the dual states which we call ‘angle states’ [33]:

$$|\vartheta; jm\rangle = F|\mathcal{J}; jm\rangle = (2j+1)^{-1/2}\sum_{n\in\mathbb{Z}_p}\omega(mn)|\mathcal{J}; jn\rangle. \tag{294}$$

These correspond to the states $|\mathcal{P}; m\rangle$ introduced earlier:

$$|\mathcal{P}; m\rangle; \leftrightarrow |\vartheta; jm\rangle. \tag{295}$$

Let $\mathcal{J}_z$, $\mathcal{J}_+$, $\mathcal{J}_-$ be the angular momentum operators which obey the commutation relations of the $SU(2)$ algebra:

$$[\mathcal{J}_z, \mathcal{J}_+] = \mathcal{J}_+; \qquad [\mathcal{J}_z, \mathcal{J}_-] = -\mathcal{J}_-; \qquad [\mathcal{J}_+, \mathcal{J}_-] = 2\mathcal{J}_z. \tag{296}$$

The Casimir operator is given by

$$\mathcal{J}^2 = \mathcal{J}_z^2 + \tfrac{1}{2}(\mathcal{J}_+\mathcal{J}_- + \mathcal{J}_-\mathcal{J}_+) = j(j+1)\mathbf{1}. \tag{297}$$

Acting with the Fourier operator on both sides of the angular momentum operators we get the angle operators

$$\mathcal{F}\mathcal{J}_z\mathcal{F}^\dagger = \vartheta_z; \qquad \mathcal{F}\mathcal{J}_+\mathcal{F}^\dagger = \vartheta_+; \qquad \mathcal{F}\mathcal{J}_-\mathcal{F}^\dagger = \vartheta_-. \tag{298}$$

These obey the $SU(2)$ algebra

$$[\vartheta_z, \vartheta_+] = \vartheta_+; \qquad [\vartheta_z, \vartheta_-] = -\vartheta_-; \qquad [\vartheta_+, \vartheta_-] = 2\vartheta_z \tag{299}$$

and their Casimir operator is

$$\vartheta^2 = \vartheta_z^2 + \tfrac{1}{2}(\vartheta_+\vartheta_- + \vartheta_-\vartheta_+) = j(j+1)\mathbf{1}. \tag{300}$$

The angular momentum operators act on the angular momentum states as follows:

$$\begin{aligned}
&\mathcal{J}_+|\mathcal{J}; jm\rangle = [j(j+1) - m(m+1)]^{1/2}|\mathcal{J}; jm+1\rangle \\
&\mathcal{J}_-|\mathcal{J}; jm\rangle = [j(j+1) - m(m-1)]^{1/2}|\mathcal{J}; jm-1\rangle \\
&\mathcal{J}_z|\mathcal{J}; jm\rangle = m|\mathcal{J}; jm\rangle \\
&\mathcal{J}^2|\mathcal{J}; jm\rangle = j(j+1)|\mathcal{J}; jm\rangle.
\end{aligned} \tag{301}$$

The angle operators act on the angle states in a similar way:

$$\begin{aligned}
&\vartheta_+|\vartheta; jm\rangle = [j(j+1) - m(m+1)]^{1/2}|\vartheta; jm+1\rangle \\
&\vartheta_-|\vartheta; jm\rangle = [j(j+1) - m(m-1)]^{1/2}|\vartheta; jm-1\rangle \\
&\vartheta_z|\vartheta; jm\rangle = m|\vartheta; jm\rangle \\
&\vartheta^2|\vartheta; jm\rangle = j(j+1)|\vartheta; jm\rangle.
\end{aligned} \tag{302}$$

The 'angular momentum-angle' phase space is $\mathbb{Z}_p \times \mathbb{Z}_p$ and as in equations (59) and (60) we introduce the displacement operators $\mathcal{Z}(\alpha)$ and $\mathcal{X}(\beta)$ which act on the angle and angular momentum states as follows:

$$\begin{aligned}
&\mathcal{Z}(\alpha)|\vartheta; jm\rangle = |\vartheta; jm+\alpha\rangle; &\qquad &\mathcal{Z}(\alpha)|\mathcal{J}; jm\rangle = \omega(\alpha m)|\mathcal{J}; jm\rangle \\
&\mathcal{X}(\beta)|\vartheta; jm\rangle = \omega(-m\beta)|\vartheta; jm\rangle; &\qquad &\mathcal{X}(\beta)|\mathcal{J}; jm\rangle = |\mathcal{J}; jm+\beta\rangle.
\end{aligned} \tag{303}$$

We can show that they are exponentials of $\mathcal{J}_z$ and ϑ_z

$$\mathcal{Z}(\alpha) = \omega(\alpha\mathcal{J}_z); \qquad \mathcal{X}(\beta) = \omega(-\beta\vartheta_z). \tag{304}$$

A polar decomposition of the operators $(\mathcal{J}_+, \mathcal{J}_-)$ can be given in terms of a radial operator $\mathcal{J}_r$ and the displacement operator $\mathcal{X}(1)$ (which is the exponential of ϑ_z):

$$\begin{aligned}
&\mathcal{J}_+ = \mathcal{J}_r\mathcal{X}(1); \qquad \mathcal{J}_- = [\mathcal{X}(1)]^\dagger\mathcal{J}_r \\
&\mathcal{J}_r = (\mathcal{J}_+\mathcal{J}_-)^{1/2} = \left[j(j+1)\mathbf{1} - \mathcal{J}_z^2 + \mathcal{J}_z\right]^{1/2} \\
&[\mathcal{J}_r, \mathcal{J}_z] = 0.
\end{aligned} \tag{305}$$

A similar decomposition can be given for the operators $(\vartheta_+, \vartheta_-)$ in terms of a radial operator ϑ_r and the displacement operator $\mathcal{Z}(1)$ (which is the exponential of $\mathcal{J}_z$):

$$\begin{aligned}
&\vartheta_+ = \vartheta_r\mathcal{Z}(1); \qquad \vartheta_- = [\mathcal{Z}(1)]^\dagger\vartheta_r \\
&\vartheta_r = (\vartheta_+\vartheta_-)^{1/2} = \mathcal{F}J_r\mathcal{F}^\dagger = \left[j(j+1)\mathbf{1} - \vartheta_z^2 + \vartheta_z\right]^{1/2} \\
&[\vartheta_r, \vartheta_z] = 0.
\end{aligned} \tag{306}$$

17.2. ℓ coupled spins as a Galois system

We consider ℓ spins with $j = (p-1)/2$. This system is described by the p^ℓ-dimensional Hilbert space $H = \mathcal{H} \otimes \cdots \otimes \mathcal{H}$. In analogy with equation (65) we introduce the angular momentum states

$$|J; jm\rangle \equiv |\mathcal{J}; jm_0\rangle \otimes \cdots \otimes |\mathcal{J}; jm_{\ell-1}\rangle; \qquad m = m_0 + m_1\epsilon + \cdots + m_{\ell-1}\epsilon^{\ell-1} \tag{307}$$

and through the Fourier transform of equation (73) (expressed in the present context), the angle states

$$|\theta; jm\rangle \equiv |\vartheta; j\overline{m}_0\rangle \otimes \cdots \otimes |\vartheta; j\overline{m}_{\ell-1}\rangle. \tag{308}$$

We also introduce the operators (equations (78) and (79)):

$$\begin{aligned}
&J_z = \sum_\lambda \epsilon^\lambda\,[\mathbf{1} \otimes \cdots \otimes \mathcal{J}_\lambda \otimes \cdots \otimes \mathbf{1}] \\
&\theta_z = FJ_zF^\dagger = \sum_{\lambda,\mu} G_{\lambda\mu}\epsilon^\mu[\mathbf{1} \otimes \cdots \otimes \vartheta_\mu \otimes \cdots \otimes \mathbf{1}].
\end{aligned} \tag{309}$$

We can then define the $\chi\left(J_z^2\right)$, $\chi\left(\theta_z^2\right)$ and Hamiltonians analogous to equations (102) and (104). For the Hamiltonian

$$h_A = \ln\left[\chi\left(J_z^2\right)\chi\left(\theta_z^2\right)\right], \tag{310}$$

we gave the corresponding evolution operator at $t = 1$, in table 1. Similar calculations can be performed for other Hamiltonians.

We stress again that only spins which are coupled in the special way discussed earlier, form Galois systems which have many symmetries and strong properties. General couplings give R-systems with weaker properties.

18. Discussion

Finite quantum systems where the position and momentum take values in the ring $\mathbb{Z}_q$ are of great interest in physics. The phase space of these systems is the toroidal lattice $\mathbb{Z}_q \times \mathbb{Z}_q$ and has (in general) a fewer symmetries than the $\mathbb{R} \times \mathbb{R}$ phase space of the harmonic oscillator. In particular, we highlight the lack of isotropy. Consequently, phase-space methods in finite systems are less powerful than in the harmonic oscillator.

In this review, we have discussed a special case of finite systems, the Galois quantum systems, where the position and momentum take values in $\mathrm{GF}(p^\ell)$. In this case the phase space is a finite geometry and has isotropy and Frobenius symmetries. The link between the axioms and properties of finite geometry and the displacements, symplectic transformations and Frobenius transformations studied here, requires further study.

Galois quantum systems are comprised of ℓ-component systems, coupled in a special way which is described by the Hamiltonian of equation (100). We have discussed displacements and symplectic transformations in these systems. The displacements form the Heisenberg–Weyl group and the symplectic transformations the $\mathrm{Sp}(2, \mathrm{GF}(p^\ell))$ group. Using them we have shown that the Wigner and Weyl functions have powerful properties and they can be used for quantum tomography. These are techniques analogous to those in a harmonic oscillator.

The Frobenius symmetry in Galois quantum systems has no analogue in the harmonic oscillator. Systems with Hamiltonians which commute with the Frobenius symmetry have the constants of motion given in equations (229) and (230).

To each irreducible polynomial of order d, correspond d Galois conjugates. This can be viewed as a multivaluedness in Galois theory which can be connected to multivaluedness in Riemann surfaces. We have introduced an analytic representation in the ℓ-sheeted complex plane which shows explicitly this connection. In this language Frobenius transformations are elegantly performed with equation (285) and their cyclic property is embodied in the periodic structure of the formalism.

As a concluding remark we highlight several points where Galois theory enters into the quantum mechanical formalism. It is the Fourier transform of equation (73), the position and momentum of equations (78) and (79) which enter in the Hamiltonian of equation (100), the symplectic transformation of equation (128) which involves products of Galois numbers, the Frobenius transformations, etc.

A different but related area which is not reviewed here is the use of p-adic fields in quantum mechanics [59] and condensed matter [60]. Other works that involves Galois fields in a quantum context are [61, 62]

References

[1] Hirschfeld J W P 1979 *Projective Geometries Over Finite Fields* (Oxford: Oxford University Press)
Batten L M 1997 *Combinatorics of Finite Geometries* (Cambridge: Cambridge University Press)

[2] Lidl R and Niederreiter H 1997 *Finite Fields* (Cambridge: Cambridge University Press)

[3] Wootters W 1987 *Ann. Phys., NY* **176** 1
Wootters W and Fields B D 1989 *Ann. Phys., NY* **191** 363
Gibbons K, Hoffman M J and Wootters W 2004 *Phys. Rev.* A **70** 062101

[4] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512

[5] Chaturvedi S 2002 *Phys. Rev.* A **65** 044301

[6] Klimov A, Sanchez-Soto L and de Guise H 2005 *J. Phys. A: Math. Gen.* **38** 2747
Klimov A, Sanchez-Soto L and de Guise H 2005 *J. Opt. B: Quantum Semiclass. Opt.* **7** 283
Romero J L, Bjork G, Klimov A B and Sanchez-Soto L L 2005 *Phys. Rev.* A **72** 062310
Klimov A B, Munoz C and Romero J L 2006 *J. Phys. A: Math. Gen.* **39** 14471
Bjork G, Romero J L, Klimov A B and Sanchez-Soto L L 2007 *J. Opt. Soc. Am.* B **24** 371
Klimov A B, Romero J L, Bjork G and Sanchez-Soto L L 2007 *J. Phys. A: Math. Gen.* **40** 3987

[7] Kibler M R and Planat M 2006 *Int. J. Mod. Phys.* B **20** 1802
Kibler M R 2006 *Int. J. Mod. Phys.* B **20** 1792

[8] Saniga M, Planat M and Rosu H 2004 *J. Opt. B: Quantum Semiclass. Opt.* **6** L19
Planat M and Rosu H 2005 *Eur. Phys. J.* D **36** 133
Saniga M and Planat M 2006 *J. Phys. A: Math. Gen.* **39** 435
Saniga M and Planat M 2007 *Adv. Studies Theor. Phys.* **1** 1
Planat M and Saniga M 2007 *Preprint* quant-ph/0703154

[9] Durt T 2006 *Int. J. Laser Phys.* **16** 1557
Durt T 2005 *J. Phys. A: Math. Gen.* **38** 5267
Colin S, Corbett J, Durt T and Gross D 2005 *J. Opt. B: Quantum Semiclass. Opt.* **7** S778
Durt T 2006 *Open Syst. Inf. Dyn.* **13** 403

[10] Pittenger A O and Rubin M H 2004 *Linear Algebr. Appl.* **390** 255
Pittenger A O and Rubin M H 2005 *J. Phys. A: Math. Gen.* **38** 6005

[11] Klappenecker A and Rotteler M 2004 *Lect. Notes Comput. Sci.* **2948** 137

[12] Wocjan P and Beth T 2005 *Quantum Inf. Comput.* **5** 181

[13] Calvao E F 2005 *Phys. Rev.* A **71** 042302

[14] Bengtsson I and Ericsson A 2005 *Open Syst. Inf. Dyn.* **12** 107

[15] Englert B G and Aharonov Y 2001 *Phys. Lett.* A **284** 1

[16] Hayashi A, Horibe M and Hashimoto T 2005 *Phys. Rev.* A **71** 052331

[17] Durt T 2006 *Int. J. Mod. Phys.* B **20** 1742

[18] Paz J P, Roncaglia A J and Saraceno M 2005 *Phys. Rev.* A **72** 012309

[19] Appleby D M 2005 *J. Math. Phys.* **46** 052107

[20] Flammia S T 2006 *J. Phys. A: Math. Gen.* **39** 13483

[21] Asikhmin A and Knill E 2001 *IEEE Trans. Inf. Theory* **47** 3065

[22] Vourdas A 2002 *Phys. Rev.* A **65** 042321
Vourdas A 2004 *J. Phys. A: Math. Gen.* **37** 3305

[23] Weyl H 1950 *Theory of Groups and Quantum Mechanics* (New York: Dover)

[24] Schwinger J 1960 *Proc. Natl Acad. Sci. USA* **46** 570
Schwinger J 1970 *Quantum Kinematics and Dynamics* (New York: Benjamin)

[25] Ramakrishnan A, Chandrasekaran P S, Ranganathan N R, Santhanam T S and Vasudevan R 1969 *J. Math. Anal. Appl.* **27** 164
Santhanam T S and Tekumalla A R 1976 *Found. Phys.* **6** 583

[26] Auslander L and Tolimieri R 1979 *Bull. Am. Math. Soc.* **1** 847

[27] Hannay J and Berry M V 1980 *Physica* D **1** 267

[28] Balian R and Itzykson C 1986 *C. R. Acad. Sci.* **303** 773

[29] Mehta M L 1987 *J. Math. Phys.* **28** 781

[30] Galetti D and de Toledo-Piza A F R 1988 *Physica* **149A** 267

[31] Varilly J C and Gracia-Bondia J M 1989 *Ann. Phys., NY* **190** 107
Figueroa H, Gracia-Bondia J M and Varilly J C 1990 *J. Math. Phys.* **31** 2664

[32] Cohendet O, Combe P, Sirugue M and Sirugue-Collin M 1988 *J. Phys. A: Math. Gen.* **21** 2875
Cohendet O, Combe P and Sirugue-Collin M 1990 *J. Phys. A: Math. Gen.* **23** 2001

[33] Vourdas A 1990 *Phys. Rev.* A **41** 1653
Vourdas A 1991 *Phys. Rev.* A **43** 1564
Vourdas A and Bendjaballah C 1993 *Phys. Rev.* A **47** 3523

[34] Lulek T 1992 *Acta Phys. Polon.* A **82** 377
Lulek T 1994 *Rep. Math. Phys.* **34** 71

[35] Hadzitaskos G and Tolar J 1993 *Int. J. Theor. Phys.* **32** 517
Tolar J and Hadzitaskos G 1997 *J. Phys. A: Math. Gen.* **30** 2509

[36] Leonhardt U 1995 *Phys. Rev. Lett.* **74** 4101
Leonhardt U 1996 *Phys. Rev.* A **53** 2998

[37] Digernes T, Varadarajan V S and Varadhan S R S 1994 *Rev. Math. Phys.* **6** 621
Varadarajan V S 1995 *Lett. Math. Phys.* **34** 319

[38] Hakioglu T 1998 *J. Phys. A: Math. Gen.* **31** 6975

[39] Gross D 2006 *J. Math. Phys.* **47** 122107

[40] Weil A 1964 *Acta Math.* **111** 143
Weil A 1965 *Acta Math.* **113** 1

[41] Vourdas A 2004 *Rep. Prog. Phys.* **67** 267

[42] Gabor D 1946 *J. Inst. Electr. Eng.* **93** 429

[43] Ville J 1948 *Cables Transm.* **1** 61

[44] Grochenig K 2001 *Foundations of Time-frequency Analysis* (Boston: Birkhauser)

[45] Flornes K, Grossmann A, Holschneider M and Torresani B 1994 *Appl. Comput. Harmon. Anal.* **1** 137–46

[46] Vourdas A 1996 *J. Phys. A: Math. Gen.* **29** 4275
Vourdas A 1997 *Rep. Math. Phys.* **40** 367
Vourdas A 2003 *J. Opt. B: Quantum Semiclass. Opt.* **5** S581

[47] Vourdas A 2005 *J. Phys. A: Math. Gen.* **38** 8453

[48] Neuhauser M 2002 *J. Lie Theory* **12** 15
Feichtinger H G, Hazewinkel M, Kaiblinger N, Matusiak E and Neuhauser M *Q. J. Math.* to appear

[49] Vourdas A 2006 *Acta Appl. Math.* **93** 197
Vourdas A 2006 *J. Math. Phys.* **47** 092104

[50] Reyssat E 1992 *From Number Theory to Physics* ed M Waldschmidt, P Moussa, J M Louck and C Itzykson (Berlin: Springer)

[51] Berndt B C, Evans R J and Williams K S 1998 *Gauss and Jacobi Sums* (New York: Wiley)
Konyagin S V and Shparlinski I E 1999 *Character Sums with Exponential Functions and Their Applications* (Cambridge: Cambridge University Press)

[52] Gel'fand I M, Graev M I and Piatetskii-Shapiro I I 1990 *Representation Theory and Automorphic Functions* (London: Academic)
Gel'fand I M and Graev M I 1962 *Dokl. Akad. Nauk. SSSR* **147** 529
Piatetskii-Shapiro I I 1983 *Complex Representations of $GL(2, K)$ for Finite Fields K* (Providence, RI: American Mathematical Society)

[53] Tanaka S 1966 *Osaka J. Math.* **3** 229
Tanaka S 1967 *Osaka J. Math.* **4** 65

[54] Terras A 1999 *Fourier Analysis on Finite Groups and Applications* (Cambridge: Cambridge University Press)

[55] Gel'fand I M, Graev M I and Vilenkin N Ya 1966 *Generalized Functions* vol 5 (London: Academic)
Ludwig D 1966 *Commun. Pure Appl. Math.* **19** 49

[56] Fairlie D B, Fletcher P and Zachos C K 1990 *J. Math. Phys.* **31** 1088

[57] Vourdas A 2006 *J. Phys. A: Math. Gen.* **39** R65

[58] Vourdas A 1994 *J. Math. Phys.* **35** 2687

[59] Vladimirov V S and Volovich I V 1989 *Commun. Math. Phys.* **123** 659
Ruelle Ph, Thiran E, Verstegen D and Weyers J 1989 *J. Math. Phys.* **30** 2854
Zelonov E I 1991 *Theor. Math. Phys.* **86** 143

[60] Rammal R, Toulouse G and Virasoro M A 1986 *Rev. Mod. Phys.* **58** 765

[61] Vivaldi F 1992 *Nonlinearity* **5** 133

[62] Lev F 2006 *Finite Fields Appl.* **12** 336