Hamiltonians of quantum systems with positions and momenta in $GF(p^\ell)$

A. Vourdas
Department of Computing,
University of Bradford,
Bradford BD7 1DP, United Kingdom

A quantum system with positions and momenta in $GF(p^\ell)$ is considered. Such a system can be constructed from ℓ smaller systems, in which the positions and momenta take values in $\mathbb{Z}_p$, if the Hamiltonian of this ℓ-partite system is compatible with $GF(p^\ell)$. The concept of compatibility of a Hamiltonian with $GF(p^\ell)$, allows the quantum formalism in the ℓ-partite system to be expressed in terms of Galois arithmetic. Transformations of the basis in $GF(p^\ell)$, produce unitary transformations of the quantum states, which form a representation of $GL(\ell, \mathbb{Z}_p)$. They are used to define which subset of the general set of Hamiltonians in the ℓ-partite system, is compatible with $GF(p^\ell)$.

I. INTRODUCTION

There has been a lot of work on quantum systems with positions and momenta in the ring $\mathbb{Z}_d$ (the integers modulo d). Reviews with many references have been presented in [1, 2]. The mathematical work in [3–5] is also relevant. The phase space of these systems is the toroidal lattice $\mathbb{Z}_d \times \mathbb{Z}_d$ and various phase space methods (displacements and the Heisenberg-Weyl group, symplectic transformations, Wigner functions, quantum tomography, etc) have been studied in this context.

When d is a prime number, $\mathbb{Z}_d$ is a field and the system has stronger properties. For example, the number of mutually unbiased bases [6–13] which is known to be less or equal to $d+1$, becomes in the case of prime number d, equal to $d+1$. Another result [14] is that the order of the symplectic group $Sp(2, \mathbb{Z}_d)$ is in general $dJ_2(d)$, where $J_2(d)$ is the Jordan totient function. It can be shown that $dJ_2(d) \leq d^3 - d$ with the equality occuring when d is a prime number.

The next step is to consider a quantum system with positions and momenta in a Galois field $GF(p^\ell)$ [15, 16]. Such a systems will not be found in nature, but it could be engineered from ℓ subsystems, each of which has positions and momenta in $\mathbb{Z}_p$. Position states and momentum states in this ℓ-partite system, are labelled with elements in $GF(p^\ell)$, and the whole formalism is expressed in terms of 'Galois arithmetic'. This can be done if and only if the Hamiltonian of the ℓ-partite system, belongs to a particular subset of the set of all Hamiltonians of these systems. We say that these Hamiltonians are compatible with $GF(p^\ell)$, and we discuss this concept in detail. Several mathematical aspects of these quantum systems have been studied in [15, 16]. Related is also the area of harmonic analysis on a Galois field [17].

In this paper we study how a change in the basis in $GF(p^\ell)$, produces unitary transformations of the quantum states (and operators) which form a representation of the group $GL(\ell, \mathbb{Z}_p)$. These transformations are used to

define which subset of the general set of Hamiltonians in the ℓ-partite system, is compatible with $GF(p^\ell)$. Also, from a theoretical point of view it is desirable to know how the the various quantum mechanical quantities are transformed, as the basis in $GF(p^\ell)$ changes. Furthermore, from a practical point of view, the Hamiltonians are much simpler in some bases (e.g., diagonal and self-dual bases), and this is important for the quantum engineering of these systems.

In section II we discuss various aspects of Galois fields, with emphasis on transformations of the basis in $GF(p^\ell)$. We also introduce the concept of compatibility of a multilinear form in $[\mathbb{Z}_p]^\ell$, with $GF(p^\ell)$. This is the first step towards developing later the compatibility of Hamiltonians with $GF(p^\ell)$.

In section III, we discuss very briefly quantum systems with positions and momenta in $\mathbb{Z}_p$. In section IV, we consider ℓ such systems, which form a general ℓ-partite system with positions and momenta in $[\mathbb{Z}_p]^\ell$ (mainly in order to define the notation).

In section V we discuss quantum systems with positions and momenta in $GF(p^\ell)$. In particular we show how a change in the basis in $GF(p^\ell)$, produces unitary transformations of the quantum states, which form a representation of $GL(\ell, \mathbb{Z}_p)$. In section VI we develop the concept of Hamiltonians which are compatible with $GF(p^\ell)$, and show that they belong to a subset of the general set of Hamiltonians in the ℓ-partite system. We conclude in section VII with a discussion of our results.

II. GALOIS FIELDS

$GF(p^\ell)$ is a finite Galois extension of the field $\mathbb{Z}_p = GF(p)$. In Galois theory, some of the theorems are valid for odd prime numbers only. Also in finite quantum systems, some of the phase space methods are different in systems with dimension which is an odd number, from those in systems with dimension which is an even number. For these reasons we take p to be an odd prime number.

The $\ell \times \ell$ invertible matrices with elements in $\mathbb{Z}_p$ form the $GL(\ell, \mathbb{Z}_p)$ group. A basis $\{\mathcal{E}_\lambda\}$ in $GF(p^\ell)$ is related to another basis $\{\mathcal{E}'_\lambda\}$ through the transformation $\mathcal{E}_\lambda = \sum \mathcal{V}_{\lambda\mu}\mathcal{E}_\mu$ where $\mathcal{V} \in GL(\ell, \mathbb{Z}_p)$. We call $\mathfrak{B}[GF(p^\ell)]$ the set of all bases in $GF(p^\ell)$, where different ordering of a basis is regarded as a different basis. It is known (e.g.[19]) that

$$|\mathfrak{B}[GF(p^\ell)]| = |GL(\ell, \mathbb{Z}_p)| = p^{\ell(\ell-1)/2} \prod_{n=1}^{\ell} (p^n - 1). \tag{1}$$

A. The Frobenius map and the Galois group

The Frobenius map

$$\sigma(\alpha) = \alpha^p; \qquad \sigma^\ell = \mathbf{1}; \qquad \alpha \in GF(p^\ell), \tag{2}$$

defines an automorphism in $GF(p^\ell)$ and leaves all elements of $\mathbb{Z}_p$ fixed. The α, α^p,...,$\alpha^{p^{\ell-1}}$ are Galois conjugates. The

$$\mathrm{Gal}[GF(p^\ell)/\mathbb{Z}_p] = \{\mathbf{1}, \sigma, ..., \sigma^{\ell-1}\}, \tag{3}$$

form the Galois group which is isomorphic to $\mathbb{Z}_\ell$.

The trace of α is defined as:

$$\mathrm{Tr}(\alpha) = \alpha + \sigma(\alpha) + ... + \sigma^{\ell-1}(\alpha); \qquad \mathrm{Tr}(\alpha) \in \mathbb{Z}_p. \tag{4}$$

B. Polynomial bases and their dual bases

Let $\mathbb{Z}_p[\epsilon]$ be the ring of polynomials with coefficients in $\mathbb{Z}_p$, and $P(\epsilon)$ an irreducible polynomial of degree ℓ. The quotient $\mathbb{Z}_p[\epsilon]/P(\epsilon)$ provides a representation of the field $GF(p^\ell)$. A commonly used basis is the polynomial basis $\{1, \epsilon, ..., \epsilon^{\ell-1}\}$. In this basis the elements of the Galois field $GF(p^\ell)$ can be written as polynomials

$$\alpha = \alpha_0 + \alpha_1\epsilon + ... + \alpha_{\ell-1}\epsilon^{\ell-1}; \qquad \alpha_0, \alpha_1, ..., \alpha_{\ell-1} \in \mathbb{Z}_p, \tag{5}$$

which are defined modulo

$$P(\epsilon) \equiv c_0 + c_1\epsilon + ... + c_{\ell-1}\epsilon^{\ell-1} + \epsilon^\ell; \qquad c_0, c_1, ..., c_{\ell-1} \in \mathbb{Z}_p. \tag{6}$$

Let g, G be the following symmetric matrices in $GL(\ell, \mathbb{Z}_p)$:

$$g_{\lambda\kappa} \equiv \mathrm{Tr}\left(\epsilon^{\lambda+\kappa}\right); \qquad G \equiv g^{-1}; \qquad \kappa, \lambda = 0, ..., \ell-1. \tag{7}$$

The dual basis to $\{1, \epsilon, ..., \epsilon^{\ell-1}\}$ is a set $\{E_0, E_1, ..., E_{\ell-1}\}$ of elements in $GF(p^\ell)$, such that:

$$E_\kappa = \sum_\lambda G_{\kappa\lambda}\epsilon^\lambda; \qquad \mathrm{Tr}(\epsilon^\kappa E_\lambda) = \delta_{\kappa\lambda}. \tag{8}$$

The matrix G can now be expressed as

$$G_{\lambda\kappa} = \mathrm{Tr}\left(E_\lambda E_\kappa\right). \tag{9}$$

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

$$\alpha = \sum_{\lambda=0}^{\ell-1} \alpha_\lambda \epsilon^\lambda = \sum_{\lambda=0}^{\ell-1} \overline{\alpha}_\lambda E_\lambda. \tag{10}$$

$\alpha_\lambda \in \mathbb{Z}_p$ and $\overline{\alpha}_\lambda \in \mathbb{Z}_p$ are the components and dual components of α, in these two bases:

$$\begin{aligned} \alpha_\lambda &= \mathrm{Tr}[\alpha E_\lambda]; \qquad \overline{\alpha}_\lambda = \mathrm{Tr}[\alpha\epsilon^\lambda] \\ \alpha_\lambda &= \sum_\kappa G_{\lambda\kappa}\overline{\alpha}_\kappa; \qquad \overline{\alpha}_\lambda = \sum_\kappa g_{\lambda\kappa}\alpha_\kappa. \end{aligned} \tag{11}$$

The trace of any product $\alpha\beta$ can be written as:

$$\mathrm{Tr}(\alpha\beta) = \sum_{\lambda,\kappa} g_{\lambda\kappa}\alpha_\lambda\beta_\kappa = \sum_{\lambda,\kappa} G_{\lambda\kappa}\overline{\alpha}_\lambda\overline{\beta}_\kappa = \sum_\lambda \alpha_\lambda\overline{\beta}_\lambda = \sum_\lambda \overline{\alpha}_\lambda\beta_\lambda. \tag{12}$$

A generalization of the g, G matrices are the symmetric tensors

$$\begin{aligned} g^{(N)}_{\lambda_1...\lambda_N} &\equiv \mathrm{Tr}\left[\epsilon^{\lambda_1+...+\lambda_N}\right]; \qquad \lambda_i = 0, ..., \ell-1 \\ G^{(N)}_{\lambda_1...\lambda_N} &\equiv \mathrm{Tr}\left[E_{\lambda_1}...E_{\lambda_N}\right] = \sum G_{\lambda_1\mu_1}...G_{\lambda_N\mu_N} g^{(N)}_{\mu_1...\mu_N}, \end{aligned} \tag{13}$$

which take values in $\mathbb{Z}_p$. For simplicity, we ommit the superfix in the notation, when $N = 2$. The transformations of these tensors, as the basis in $GF(p^\ell)$ changes, are dicsussed later.

The trace of a product of N elements of $GF(p^\ell)$ can be written as

$$\mathrm{Tr}\left[\alpha^{(1)}...\alpha^{(N)}\right] = \sum g^{(N)}_{\lambda_1...\lambda_N}\alpha^{(1)}_{\lambda_1}...\alpha^{(N)}_{\lambda_N} = \sum G^{(N)}_{\lambda_1...\lambda_N}\overline{\alpha}^{(1)}_{\lambda_1}...\overline{\alpha}^{(N)}_{\lambda_N}. \tag{14}$$

Clearly, we have relations like $g_{\kappa\lambda} = g_{\kappa+\lambda,0}$ if $\kappa + \lambda \leq \ell - 1$, or $g^{(3)}_{\lambda_1\lambda_2\lambda_3} = g_{\lambda_1+\lambda_2,\lambda_3}$ if $\lambda_1 + \lambda_2 \leq \ell - 1$, or $g^{(3)}_{\lambda_1\lambda_2\lambda_3} = g_{\lambda_1,\lambda_2+\lambda_3}$ if $\lambda_2 + \lambda_3 \leq \ell - 1$, etc. In these relations, it is important to remember that the indices of the tensors take values from 0 to $\ell - 1$. It is an interesting open problem whether we can find general relations that express high order tensors $g^{(N)}$ in terms of lower order tensors $g^{(K)}$ (with $K < N$).

We call $\mathfrak{G}(\mathbf{1})$ and $\overline{\mathfrak{G}}(\mathbf{1})$ the following sets of tensors

$$\mathfrak{G}(\mathbf{1}) = \{g, g^{(3)}, g^{(4)}, ...\}; \qquad \overline{\mathfrak{G}}(\mathbf{1}) = \{G, G^{(3)}, G^{(4)}, ...\}. \tag{15}$$

C. General bases

Here we construct explicitly all bases in $GF(p^\ell)$. Let V be a matrix in $GL(\ell, \mathbb{Z}_p)$. We consider the following elements of $GF(p^\ell)$:

$$\mathcal{E}_\kappa = \sum_\lambda \epsilon^\lambda (V^{-1})_{\lambda\kappa}. \tag{16}$$

The $\{\mathcal{E}_0, \mathcal{E}_1, ..., \mathcal{E}_{\ell-1}\}$ can be used as a basis. For simplicity, we do not indicate explicitly in the notation that $\mathcal{E}_\kappa$ depend on V, but later it is important to remember that this is the case. An arbitrary element α of Eq.(10) can be written as

$$\alpha = \sum_{\lambda=0}^{\ell-1} A_\lambda \mathcal{E}_\lambda; \qquad A_\lambda = \sum_{\kappa=0}^{\ell-1} V_{\lambda\kappa}\alpha_\kappa. \tag{17}$$

In this basis we introduce the symmetric matrices g_V and G_V:

$$g_V = (V^{-1})^T g V^{-1}; \qquad G_V = g_V^{-1} = V G V^T; \qquad (g_V)_{\kappa\lambda} = \mathrm{Tr}(\mathcal{E}_k\mathcal{E}_\lambda). \tag{18}$$

Here V^T is the transpose matrix of V. Then the dual basis is defined as

$$\overline{\mathcal{E}}_\kappa = \sum_\lambda (G_V)_{\kappa\lambda}\mathcal{E}_\lambda; \qquad \mathrm{Tr}(\overline{\mathcal{E}}_\kappa\mathcal{E}_\lambda) = \delta_{\kappa\lambda}, \tag{19}$$

and

$$(G_V)_{\kappa\lambda} = \mathrm{Tr}(\overline{\mathcal{E}}_\kappa \overline{\mathcal{E}}_\lambda). \tag{20}$$

The relationship between the dual bases $\{\overline{\mathcal{E}}_\lambda\}$ and $\{E_\lambda\}$, is given by

$$\overline{\mathcal{E}}_\kappa = \sum_\lambda V_{\kappa\lambda} E_\lambda. \tag{21}$$

A number $\alpha \in GF(p^\ell)$ can be expressed in the two bases as:

$$\begin{aligned} \alpha &= \sum_{\lambda=0}^{\ell-1} A_\lambda \mathcal{E}_\lambda = \sum_{\lambda=0}^{\ell-1} \overline{A}_\lambda \overline{\mathcal{E}}_\lambda; \qquad A_\lambda, \overline{A}_\lambda \in \mathbb{Z}_p \\ A_\lambda &= \mathrm{Tr}[\alpha \overline{\mathcal{E}}_\lambda]; \qquad \overline{A}_\lambda = \mathrm{Tr}[\alpha \mathcal{E}_\lambda] \\ A_\lambda &= \sum (G_V)_{\lambda\kappa} \overline{A}_\kappa; \qquad \overline{A}_\lambda = \sum (g_V)_{\lambda\kappa} A_\kappa. \end{aligned} \tag{22}$$

The relationship between $\overline{A}_\lambda$ and $\overline{a}_\lambda$ (the components of α in the dual bases $\{\overline{\mathcal{E}}_\lambda\}$ and $\{E_\lambda\}$) is given by

$$\overline{A}_\lambda = \sum_{\kappa=0}^{\ell-1} \overline{\alpha}_\kappa (V^{-1})_{\kappa\lambda}. \tag{23}$$

Eqs.(17),(23) show that (a_λ) is a contravariant vector (i.e., it transforms with the matrix V) and $(\overline{a}_\lambda)$ is a covariant vector (i.e., it transforms with the matrix V^{-1}).

The trace of a product $\alpha\beta$ is given in terms of the components of these numbers as

$$\mathrm{Tr}(\alpha\beta) = \sum_{\lambda,\kappa} (g_V)_{\lambda\kappa} A_\lambda B_\kappa = \sum_{\lambda,\kappa} (G_V)_{\lambda\kappa} \overline{A}_\lambda \overline{B}_\kappa = \sum_\lambda A_\lambda \overline{B}_\lambda = \sum_\lambda \overline{A}_\lambda B_\lambda. \tag{24}$$

This can also be rewritten as

$$\mathrm{Tr}(\alpha\beta) = \sum_\lambda \mathrm{Tr}(\alpha \mathcal{E}_\lambda) \mathrm{Tr}(\beta \overline{\mathcal{E}}_\lambda). \tag{25}$$

More generally we introduce the symmetric tensors

$$\left(g_V^{(N)}\right)_{\lambda_1 ... \lambda_N} \equiv \mathrm{Tr}\left[\mathcal{E}_{\lambda_1} ... \mathcal{E}_{\lambda_N}\right] = \sum g^{(N)}_{\mu_1 ... \mu_N} (V^{-1})_{\mu_1\lambda_1} ... (V^{-1})_{\mu_N\lambda_N}, \tag{26}$$

and

$$\begin{aligned} \left(G_V^{(N)}\right)_{\lambda_1 ... \lambda_N} &\equiv \mathrm{Tr}\left[\overline{\mathcal{E}}_{\lambda_1} ... \overline{\mathcal{E}}_{\lambda_N}\right] = \sum V_{\lambda_1\mu_1} ... V_{\lambda_N\mu_N} G^{(N)}_{\mu_1 ... \mu_N} \\ &= \sum (G_V)\lambda_1\mu_1 ... (G_V)_{\lambda_N\mu_N} \left(g_V^{(N)}\right)_{\mu_1 ... \mu_N}, \end{aligned} \tag{27}$$

which take values in $\mathbb{Z}_p$. $g^{(N)}$ and $G^{(N)}$ are covariant and contravariant tensors correspondingly. The trace of a product of ℓ elements of $GF(p^\ell)$ is given in terms of their components in this basis, as

$$\mathrm{Tr}\left[\alpha^{(1)} ... \alpha^{(N)}\right] = \sum \left(g_V^{(N)}\right)_{\lambda_1 ... \lambda_N} A^{(1)}_{\lambda_1} ... A^{(N)}_{\lambda_N} = \sum \left(G_V^{(N)}\right)_{\lambda_1 ... \lambda_N} \overline{A}^{(1)}_{\lambda_1} .... \overline{A}^{(N)}_{\lambda_N} \tag{28}$$

The trace of a product of elements of a Galois field does not depend on the basis.

We call $\mathfrak{G}(V)$ and $\overline{\mathfrak{G}}(V)$ the following sets of tensors

$$\mathfrak{G}(V) = \{g_V, g_V^{(3)}, g_V^{(4)}, ...\}; \qquad \overline{\mathfrak{G}}(V) = \{G_V, G_V^{(3)}, G_V^{(4)}, ...\}. \tag{29}$$

D. The sets $\mathfrak{G}_N$ and $\mathfrak{R}_N$

Let $\mathcal{S}_2$ be the set of symmetric matrices which are elements of $GL(\ell,\mathbb{Z}_p)$. If $\tau\in\mathcal{S}_2$ then $\mathcal{V}^T\tau\mathcal{V}\in\mathcal{S}_2$ for all $\mathcal{V}\in GL(\ell,\mathbb{Z}_p)$. In $\mathcal{S}_2$ we introduce the 'congruence equivalence relation' $\sim$, where $\sigma\sim\tau$ if σ is congruent to τ, i.e., if there exists a matrix $\mathcal{V}\in GL(\ell,\mathbb{Z}_p)$ so that $\sigma=\mathcal{V}^T\tau\mathcal{V}$. It is easy to prove that this is indeed an equivalence relation. Congruent symmetric matrices represent the same symmetric bilinear form (with respect to different bases).

We call $\mathfrak{G}_2$ the equivalence class of the matrix g in Eq.(7) and $\mathfrak{R}_2$ the subset which contains the rest of the matrices in $\mathcal{S}_2$:

$$\mathfrak{G}_2=\{\sigma\in\mathcal{S}_2|\ \sigma\sim g\};\quad \mathfrak{R}_2=\{\sigma\in\mathcal{S}_2|\ \sigma\notin\mathfrak{G}_2\};\quad \mathfrak{G}_2\bigcup\mathfrak{R}_2=\mathcal{S}_2;\quad \mathfrak{G}_2\bigcap\mathfrak{R}_2=\emptyset. \tag{30}$$

If $\sigma\in\mathfrak{G}_2$, then $\sigma^{-1}\in\mathfrak{G}_2$ (it is related to the dual basis). We prove this using the fact that if $\sigma=V^TgV$ then $\sigma^{-1}=W^TgW$ with $W=g^{-1}(V^{-1})^T$. We note that the map from $\mathfrak{B}[GF(p^\ell)]$ (or $GL(\ell,\mathbb{Z}_p)$) to $\mathfrak{G}_2$, which maps the basis defined by V into $g_V=V^TgV$, is surjective (but it is not injective). There are several matrices V which give the same g_V.

More generally let $\mathcal{S}_N$ be the set of symmetric tensors $\sigma^{(N)}_{\lambda_1...\lambda_N}$ ($\lambda_i=0,...,\ell-1$) which take values in $\mathbb{Z}_p$. In it we introduce the equivalence relation $\sim$, with $\sigma^{(N)}\sim\tau^{(N)}$ (where $\sigma^{(N)},\tau^{(N)}\in\mathcal{S}_N$) if there exists a matrix $\mathcal{V}\in GL(\ell,\mathbb{Z}_p)$ so that

$$\sigma^{(N)}_{\lambda_1...\lambda_N}=\sum\tau^{(N)}_{\mu_1...\mu_N}(\mathcal{V}^{-1})_{\mu_1\lambda_1}...(\mathcal{V}^{-1})_{\mu_N\lambda_N}. \tag{31}$$

We call $\mathfrak{G}_N$ the equivalence class of the tensor $g^{(N)}$ in Eq.(13) and $\mathfrak{R}_N$ the subset which contains the rest of the elements in $\mathcal{S}_N$:

$$\mathfrak{G}_N=\{\sigma^{(N)}\in\mathcal{S}_N|\ \sigma^{(N)}\sim g^{(N)}\};\qquad \mathfrak{R}_N=\{\sigma^{(N)}\in\mathcal{S}_N|\ \sigma^{(N)}\notin\mathfrak{G}_N\}. \tag{32}$$

If $\tau^{(N)}\in\mathfrak{G}_N$ then there exists a matrix $V\in GL(\ell,\mathbb{Z}_p)$ so that

$$\tau^{(N)}_{\lambda_1...\lambda_N}=\sum g^{(N)}_{\mu_1...\mu_N}(V^{-1})_{\mu_1\lambda_1}...(V^{-1})_{\mu_N\lambda_N}. \tag{33}$$

Then the

$$T^{(N)}_{\lambda_1...\lambda_N}=\sum g^{(N)}_{\mu_1...\mu_N}(W^{-1})_{\mu_1\lambda_1}...(W^{-1})_{\mu_N\lambda_N};\qquad W=(V^{-1})^Tg, \tag{34}$$

also belongs in $\mathfrak{G}_N$, and Eq.(27) shows that it is related to the dual basis.

Below we use the notation

$$\mathcal{S}=\bigcup_{N=2}^{\infty}\mathcal{S}_N;\qquad \mathfrak{G}=\bigcup_{V\in GL(\ell,\mathbb{Z}_p)}\mathfrak{G}(V)=\bigcup_{N=2}^{\infty}\mathfrak{G}_N. \tag{35}$$

Clearly $\mathfrak{G}\subset\mathcal{S}$.

E. Symmetric multilinear forms on $[\mathbb{Z}_p]^\ell$ compatible with $GF(p^\ell)$

Later we have symmetric multilinear forms and it is important to know whether we can regard them as trace of a product of elements in $GF(p^\ell)$.

Definition II.1. Let $(\alpha_0^{(i)},...,\alpha_{\ell-1}^{(i)})$ be N vectors in $[\mathbb{Z}_p]^\ell$ (with $i=1,...,N$) and $\sigma^{(N)}\in\mathcal{S}_N$. The symmetric multilinear form

$$\mathcal{L}_N(\sigma^{(N)})=\sum\sigma^{(N)}_{\mu_1...\mu_N}\alpha^{(1)}_{\mu_1}...\alpha^{(N)}_{\mu_N},, \tag{36}$$

is compatible with $GF(p^\ell)$ if there exist a basis $\{\mathcal{E}_\lambda\}$ in $GF(p^\ell)$ such that

$$\mathcal{L}_N(\sigma^{(N)})=\mathrm{Tr}\left(\alpha^{(1)}...\alpha^{(N)}\right);\qquad \alpha^{(i)}=\sum\alpha^{(i)}_\lambda\mathcal{E}_\lambda\in GF(p^\ell). \tag{37}$$

Proposition II.2. *The symmetric multilinear form $\mathcal{L}_N(\sigma^{(N)})$ of Eq.(36) is compatible with $GF(p^\ell)$, if and only if $\sigma^{(N)}\in\mathfrak{G}_N$.*

Proof. If $\sigma^{(N)}\in\mathfrak{G}_N$, there exist matrix V which relates $\sigma^{(N)}$ and $g^{(N)}$ as in Eq.(33). Then we define the basis $\{\mathcal{E}_\kappa\}$ using Eq.(16), and show that

$$\sum_{\mu_1,...,\mu_N}\sigma^{(N)}_{\mu_1...\mu_N}\alpha^{(1)}_{\mu_1}...\alpha^{(N)}_{\mu_N}=\mathrm{Tr}(\alpha^{(1)}...\alpha^{(N)});\qquad \alpha^{(i)}=\sum_\mu\alpha^{(i)}_\mu\mathcal{E}_\mu;\qquad \alpha^{(i)}\in GF(p^\ell). \tag{38}$$

Therefore $\mathcal{L}_N(\sigma^{(N)})$ is compatible with $GF(p^\ell)$.

Conversely, we show that if Eq.(38) is valid, then $\sigma^{(N)}_{\mu_1...\mu_N}=\mathrm{Tr}(\mathcal{E}_{\mu_1}...\mathcal{E}_{\mu_N})$. Therefore according to Eq.(26), $\sigma^{(N)}\in\mathfrak{G}_N$. □

F. Diagonal and self-dual bases

The general theory of symmetric bilinear forms on a field (e.g., p.385 in [18]) proves that there exist matrices in $\mathfrak{G}_2$ which are diagonal:

$$g_{\mathrm{diag}}=\mathrm{diag}(\mathfrak{g}_0,...,\mathfrak{g}_{\ell-1});\qquad G_{\mathrm{diag}}=\mathrm{diag}(\mathfrak{g}_0^{-1},...,\mathfrak{g}_{\ell-1}^{-1});\qquad \mathfrak{g}_i\neq 0. \tag{39}$$

We refer to the corresponding bases as diagonal. Let $\mathfrak{E}_\kappa$ be such a basis and $\overline{\mathfrak{E}}_\kappa$ its dual basis. Then

$$\mathrm{Tr}(\mathfrak{E}_\kappa\mathfrak{E}_\lambda)=\delta_{\kappa\lambda}\mathfrak{g}_\lambda;\qquad \overline{\mathfrak{E}}_\kappa=\mathfrak{g}_\kappa^{-1}\mathfrak{E}_\kappa. \tag{40}$$

If $\alpha=\sum\alpha_\kappa\mathfrak{E}_\kappa$ and $\beta=\sum\beta_\kappa\mathfrak{E}_\kappa$, the trace of the product $\alpha\beta$ is given by

$$\mathrm{Tr}(\alpha\beta)=\sum_\kappa\mathfrak{g}_\kappa\alpha_\kappa\beta_\kappa. \tag{41}$$

It has only diagonal terms, but we note that the trace of the product of three or more Galois numbers does have off-diagonal terms (the higher order $g^{(n)}$-matrices do have non-diagonal elements).

An important special case of diagonal bases are the self dual bases where $g_{\rm SD} = G_{\rm SD} = \mathbf{1}$ (the index 'SD' indicates self-dual). In the case of odd prime number p considered here, it is known [19–21] that $GF(p^\ell)$ has self-dual bases if and only if ℓ is an odd integer. Therefore, $\mathbf{1} \in \mathfrak{G}_2$ when ℓ is an odd number, and $\mathbf{1} \in \mathfrak{R}_2$ when ℓ is an even number. We use the notation $\widetilde{E}_\kappa$ for self-dual bases. They obey the relation

$$\mathrm{Tr}(\widetilde{E}_\kappa \widetilde{E}_\lambda) = \delta_{\kappa\lambda}. \tag{42}$$

If $\alpha = \sum \widetilde{\alpha}_\kappa \widetilde{E}_\kappa$ and $\beta = \sum \widetilde{\beta}_\kappa \widetilde{E}_\kappa$, the trace of the product $\alpha\beta$ is given by the simple relation

$$\mathrm{Tr}(\alpha\beta) = \sum_\kappa \widetilde{\alpha}_\kappa \widetilde{\beta}_\kappa. \tag{43}$$

However, the higher order $g_{\rm SD}^{(n)}$-matrices do have non-diagonal elements.

The number N of self-dual bases is [19]

$$N = \frac{2p^{\lambda^2}}{\ell!} \prod_{i=1}^{\lambda} (p^{2i} - 1); \qquad \ell = 2\lambda + 1. \tag{44}$$

In practice, it is not always easy to find a self-dual basis. Following [21], we give a self-dual basis for the special case of the Galois field $GF(p^p)$.

Proposition II.3. *The Artin-Schreier irreducible polynomial $P(\epsilon) = \epsilon^p - \epsilon - 1$ is chosen and $GF(p^p)$ is represented with the quotient $\mathbb{Z}_p[\epsilon]/P(\epsilon)$. Then the*

$$\widetilde{E}_0 = \epsilon^{p-1} - 1; \qquad \widetilde{E}_\kappa = \widetilde{E}_0^{p^\kappa} = (\epsilon + \kappa)^{p-1} - 1 = \frac{\epsilon^p - \epsilon}{\epsilon + \kappa}, \tag{45}$$

is a self-dual basis in $GF(p^p)$.

Proof. All elements are defined modulo $P(\epsilon) = \epsilon^p - \epsilon - 1$ and therefore

$$\epsilon^{p^\kappa} = \epsilon + \kappa. \tag{46}$$

Using this we prove that $\widetilde{E}_0^{p^\kappa} = (\epsilon + \kappa)^{p-1} - 1 = \frac{\epsilon^p - \epsilon}{\epsilon + \kappa}$.

We next show that $\mathrm{Tr}(\widetilde{E}_\kappa \widetilde{E}_\lambda) = \delta_{\kappa\lambda}$. We will use the following relation (e.g., p.90 in [22]):

$$\begin{aligned} p - 1 \mid \nu \quad &\rightarrow \quad S_\nu(p) \equiv \sum_{n=0}^{p-1} n^\nu = -1 \\ p - 1 \nmid \nu \quad &\rightarrow \quad S_\nu(p) \equiv \sum_{n=0}^{p-1} n^\nu = 0 \end{aligned} \tag{47}$$

where $a \mid b$ (and $a \nmid b$) denotes that a is (is not) a divisor of b.

Since $\widetilde{E}_\kappa = \widetilde{E}_0^{p^\kappa}$ it is sufficient to show that $\mathrm{Tr}(\widetilde{E}_0^2) = 1$ and $\mathrm{Tr}(\widetilde{E}_0 \widetilde{E}_\kappa) = 0$ for $\kappa \neq 0$. We first prove that $\mathrm{Tr}(\widetilde{E}_0^2) = 1$:

$$\mathrm{Tr}(\widetilde{E}_0^2) = \mathrm{Tr}(\epsilon^{2p-2}) - 2\mathrm{Tr}(\epsilon^{p-1}) + \mathrm{Tr}(1) \tag{48}$$

But

$$\mathrm{Tr}(\epsilon^{p-1}) = \sum_{\kappa}(\epsilon+\kappa)^{p-1} = \sum_{\kappa,\nu}\begin{pmatrix} p-1 \\ \nu \end{pmatrix}\kappa^{\nu}\epsilon^{p-1-\nu} = \sum_{\nu}\begin{pmatrix} p-1 \\ \nu \end{pmatrix}S_{\nu}(p)\epsilon^{p-1-\nu} = -1 \tag{49}$$

In the last sum all $S_\nu(p)$ apart from $S_{p-1}(p)$ are zero, and the result is -1.

In addition to that

$$\mathrm{Tr}(\epsilon^{2p-2}) = \sum_{\kappa}(\epsilon+\kappa)^{2p-2} = \sum_{\kappa,\nu}\begin{pmatrix} 2p-2 \\ \nu \end{pmatrix}\kappa^{\nu}\epsilon^{2p-2-\nu} = \sum_{\nu}\begin{pmatrix} 2p-2 \\ \nu \end{pmatrix}S_{\nu}(p)\epsilon^{2p-2-\nu} = -1 \tag{50}$$

In the last sum all $S_\nu(p)$ apart from $S_{p-1}(p)$ and $S_{2p-2}(p)$ are zero. The result is -1 because the contribution of the term which contains $S_{p-1}(p)$ is zero due to the fact that in $\mathbb{Z}_p$

$$\begin{pmatrix} 2p-2 \\ p-1 \end{pmatrix} = \frac{p...(2p-2)}{1...(p-1)} = p(p-1)^{-1} = 0. \tag{51}$$

Eqs.(49),(50) and the fact that $\mathrm{Tr}(1) = 0$ prove that $\mathrm{Tr}(\widetilde{E}_0^2) = 1$.

In order to show that for $\kappa \neq 0$ we get $\mathrm{Tr}(\widetilde{E}_0\widetilde{E}_\kappa) = 0$, we use the formula

$$(\widetilde{E}_0\widetilde{E}_\kappa)^{p^\nu} = \widetilde{E}_\nu\widetilde{E}_{\kappa+\nu} = \frac{\epsilon^p-\epsilon}{\epsilon+\nu}\frac{\epsilon^p-\epsilon}{\epsilon+\kappa+\nu} = \frac{(\epsilon^p-\epsilon)^2}{\kappa}\left[\frac{1}{\epsilon+\nu} - \frac{1}{\epsilon+\kappa+\nu}\right]. \tag{52}$$

Therefore

$$\mathrm{Tr}(\widetilde{E}_0\widetilde{E}_\kappa) = \sum_{\nu}\widetilde{E}_\nu\widetilde{E}_{\kappa+\nu} = \frac{(\epsilon^p-\epsilon)^2}{\kappa}\left[\sum_{\nu}\frac{1}{\epsilon+\nu} - \sum_{\nu}\frac{1}{\epsilon+\kappa+\nu}\right] = 0. \tag{53}$$

This completes the proof.

□

G. Example

As an example we consider the $GF(27)$ and we choose the irreducible polynomial $P(\epsilon) = \epsilon^3 - \epsilon - 1$. In the polynomial basis $\{1, \epsilon, \epsilon^2\}$ we find:

$$g = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix}; \quad G = \begin{pmatrix} 1 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \tag{54}$$

Therefore the dual basis is $E_0 = 1-\epsilon^2$, $E_1 = -\epsilon$ and $E_2 = -1$. The higher order symmetric tensor $g^{(n)}$ has 3^n elements and as an example we give

$$g^{(4)}_{0112} = \mathrm{Tr}(\epsilon^4) = -1; \qquad g^{(4)}_{0012} = \mathrm{Tr}(\epsilon^3) = 0; \qquad g^{(4)}_{1112} = \mathrm{Tr}(\epsilon^5) = 1 \tag{55}$$

We next choose the matrix

$$V = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix}, \tag{56}$$

and transform the polynomial basis $\{1, \epsilon, \epsilon^2\}$ to the basis

$$\mathcal{E}_0 = -1 - \epsilon^2; \qquad \mathcal{E}_1 = 1 + \epsilon + \epsilon^2; \qquad \mathcal{E}_2 = -\epsilon^2. \tag{57}$$

The general element $\alpha_0 + \alpha_1\epsilon + \alpha_2\epsilon^2$ is written in the new basis as $A_0\mathcal{E}_0 + A_1\mathcal{E}_1 + A_2\mathcal{E}_2$ where

$$A_0 = -\alpha_0 + \alpha_1; \qquad A_1 = \alpha_1; \qquad A_2 = \alpha_0 - \alpha_2. \tag{58}$$

We calculate the products $\mathcal{E}_i\mathcal{E}_j$ and express the results in terms of $\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2$:

$$\begin{gathered} \mathcal{E}_0^2 = \mathcal{E}_1 + \mathcal{E}_2; \qquad \mathcal{E}_1^2 = -\mathcal{E}_0 - \mathcal{E}_1 - \mathcal{E}_2; \qquad \mathcal{E}_2^2 = \mathcal{E}_0 + \mathcal{E}_1 - \mathcal{E}_2 \\ \mathcal{E}_0\mathcal{E}_1 = -\mathcal{E}_0 + \mathcal{E}_2; \qquad \mathcal{E}_0\mathcal{E}_2 = \mathcal{E}_0 + \mathcal{E}_1 + \mathcal{E}_2; \qquad \mathcal{E}_1\mathcal{E}_2 = -\mathcal{E}_0 + \mathcal{E}_1 + \mathcal{E}_2. \end{gathered} \tag{59}$$

This can be useful in multiplication calculations in this basis. The 'g-matrices' for this basis are:

$$g_V = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & -1 \\ 1 & -1 & -1 \end{pmatrix}; \qquad G_V = \begin{pmatrix} 0 & -1 & 1 \\ -1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}. \tag{60}$$

Therefore the dual basis is

$$\overline{\mathcal{E}}_0 = -\mathcal{E}_1 + \mathcal{E}_2; \qquad \overline{\mathcal{E}}_1 = -\mathcal{E}_0 - \mathcal{E}_1; \qquad \overline{\mathcal{E}}_2 = \mathcal{E}_0. \tag{61}$$

We next use Eq.(45) and get the self-dual basis

$$\widetilde{E}_0 = -1 + \epsilon^2; \qquad \widetilde{E}_1 = -\epsilon + \epsilon^2; \qquad \widetilde{E}_2 = \epsilon + \epsilon^2 \tag{62}$$

The corresponding 'V-matrix' is in this case

$$V_{\mathrm{SD}} = \begin{pmatrix} -1 & 0 & 0 \\ -1 & 1 & -1 \\ -1 & -1 & -1 \end{pmatrix} \tag{63}$$

The general element $\alpha_0 + \alpha_1\epsilon + \alpha_2\epsilon^2$ is written in this self-dual basis as $\widetilde{\alpha}_0\widetilde{E}_0 + \widetilde{\alpha}_1\widetilde{E}_1 + \widetilde{\alpha}_2\widetilde{E}_2$ where

$$\widetilde{\alpha}_0 = -\alpha_0.; \qquad \widetilde{\alpha}_1 = -\alpha_0 + \alpha_1 - \alpha_2; \qquad \widetilde{\alpha}_2 = -\alpha_0 - \alpha_1 - \alpha_2 \tag{64}$$

The following relations are useful in multiplication calculations:

$$\begin{gathered} (\widetilde{E}_0)^2 = -\widetilde{E}_0 + \widetilde{E}_1 - \widetilde{E}_2; \qquad (\widetilde{E}_1)^2 = -\widetilde{E}_0 - \widetilde{E}_1 + \widetilde{E}_2; \qquad (\widetilde{E}_2)^2 = \widetilde{E}_0 - \widetilde{E}_1 - \widetilde{E}_2 \\ \widetilde{E}_0\widetilde{E}_1 = \widetilde{E}_0 - \widetilde{E}_1; \qquad \widetilde{E}_0\widetilde{E}_2 = -\widetilde{E}_0 + \widetilde{E}_2; \qquad \widetilde{E}_1\widetilde{E}_2 = \widetilde{E}_1 - \widetilde{E}_2. \end{gathered} \tag{65}$$

We have already explained that in the self-dual basis $g_{\rm SD} = G_{\rm SD} = \mathbf{1}$, but the higher order symmetric $g^{(n)}_{\rm SD}$ tensors do have non-diagonal elements. An example of this is

$$\left[g^{(4)}_{\rm SD}\right]_{0112} = {\rm Tr}\left[\widetilde{E}_0(\widetilde{E}_1)^2\widetilde{E}_2\right] = -1; \quad \left[g^{(4)}_{\rm SD}\right]_{0012} = \left[(\widetilde{E}_0)^2\widetilde{E}_1\widetilde{E}_2\right] = -1; \quad \left[g^{(4)}_{\rm SD}\right]_{1112} = {\rm Tr}\left[(\widetilde{E}_1)^3\widetilde{E}_2\right] = 1. \tag{66}$$

H. Additive characters

We use the notation

$$\omega(m) = \exp\left(i\frac{2\pi m}{p}\right); \qquad m \in \mathbb{Z}_p. \tag{67}$$

The complex-valued function

$$\chi(\alpha) = \omega[{\rm Tr}(\alpha)]; \qquad \alpha \in GF(p^\ell), \tag{68}$$

is an additive character in $GF(p^\ell)$. We can show that

$$\frac{1}{p^\ell}\sum_\gamma \chi(\alpha\gamma - \beta\gamma) = \delta(\alpha,\beta). \tag{69}$$

The character of a product of two elements in $GF(p^\ell)$ can be written in terms of their components, as

$$\chi(\alpha\beta) = \omega\left[\sum_{\lambda,\kappa}\sigma_{\lambda\kappa}\alpha_\lambda\beta_\kappa\right] = \omega\left[\sum_\lambda \alpha_\lambda\overline{\beta}_\lambda\right] = \omega\left[\sum_\lambda \overline{\alpha}_\lambda\beta_\lambda\right]; \qquad \sigma \in \mathfrak{G}_2. \tag{70}$$

Here $\alpha_\lambda, \overline{\alpha}_\lambda$ are the components and dual components of α in the basis corresponding to σ (i.e., in the basis defined by the matrix V corresponding to σ). The character does not depend on the basis.

More generally Eq.(14) gives

$$\chi\left[\alpha^{(1)}...\alpha^{(N)}\right] = \omega\left[\sum \sigma^{(N)}_{\lambda_1...\lambda_N}\alpha^{(1)}_{\lambda_1}...\alpha^{(N)}_{\lambda_N}\right]; \qquad \sigma^{(N)} \in \mathfrak{G}_N. \tag{71}$$

Here also we can use any $\sigma^{(N)} \in \mathfrak{G}_N(\ell,\mathbb{Z}_p)$ together with the components of $\alpha^{(i)}$ in the corresponding basis, and get the same character.

In a diagonal basis the character of the product of two Galois numbers, contains only diagonal terms

$$\chi(\alpha\beta) = \omega\left[\sum_\kappa \mathfrak{g}_\kappa\alpha_\kappa\beta_\kappa\right]. \tag{72}$$

When ℓ is an odd number, there exist self-dual bases. In these bases

$$\chi(\alpha\beta) = \omega\left[\sum_\kappa \widetilde{\alpha}_\kappa\widetilde{\beta}_\kappa\right]. \tag{73}$$

However the character of the product of three (or more) Galois numbers, does have off-diagonal terms, in diagonal bases and also in self-dual bases.

I. Galois trace and characters of diagonal matrices with elements in $GF(p^\ell)$

For later use we extend the concepts of Galois trace and character, to diagonal matrices with elements in $GF(p^\ell)$ [16]. $\mathfrak{D}_N[GF(p^\ell)]$ and $\mathfrak{D}_N(\mathbb{Z}_p)$ are the vector spaces of diagonal $N \times N$ matrices with elements in $GF(p^\ell)$ and $\mathbb{Z}_p$, correspondingly.

Let $\Theta \in \mathfrak{D}_N[GF(p^\ell)]$. We can express Θ as

$$\Theta = \sum_i \theta_{ii}\Pi_i; \qquad \theta_{ii} \in GF(p^\ell); \qquad \Theta^{p^\ell} = \Theta, \tag{74}$$

where Π_i is such that $(\Pi_i)_{\kappa\lambda} = 1$ if $\kappa = \lambda = i$ and $(\Pi_i)_{\kappa\lambda} = 0$ otherwise. The Π_i are orthogonal projectors (i.e., $\Pi_i\Pi_j = \delta_{ij}\Pi_i$). It is easily seen that $\Theta^{p^\ell} = \Theta$.

The character of Θ is defined to be the $N \times N$ diagonal matrix

$$\chi(\Theta) = \sum_i \chi(\theta_{ii})\Pi_i. \tag{75}$$

Its elements are complex numbers.

The matrix Θ can also be written as

$$\Theta = \Theta_0\mathcal{E}_0 + ... + \Theta_{\ell-1}\mathcal{E}_{\ell-1}; \qquad \Theta_\lambda \in \mathfrak{D}_N(\mathbb{Z}_p), \tag{76}$$

where Θ_λ are 'component matrices'. We can also define the dual component matrices $\overline{\Theta}_\lambda$ through Eqs.(22).

The Galois trace of Θ is defined by:

$$\mathrm{Tr_G}\Theta = \Theta + \Theta^p + ... + \Theta^{p^{\ell-1}}; \qquad [\mathrm{Tr_G}\Theta]^p = \mathrm{Tr_G}\Theta; \qquad \mathrm{Tr_G}\Theta \in \mathfrak{D}_N(\mathbb{Z}_p). \tag{77}$$

$\mathrm{Tr_G}\Theta$ does not depend on the basis $\{\mathcal{E}_\lambda\}$ used for the Galois field. The character of Θ defined earlier, is also given by

$$\chi(\Theta) = \omega\left(\mathrm{Tr_G}\Theta\right). \tag{78}$$

If Θ and Φ are two matrices in $\mathfrak{D}_N[GF(p^\ell)]$, then

$$\mathrm{Tr_G}(\Theta\Phi) = \sum_{\lambda,\mu}(g_V)_{\lambda\mu}\Theta_\lambda\Phi_\mu = \sum_\mu \overline{\Theta}_\mu\Phi_\mu = \sum_\mu \Theta_\mu\overline{\Phi}_\mu; \qquad g_V \in \mathfrak{G}_2. \tag{79}$$

The elements of the matrix $\mathrm{Tr_G}(\Theta\Phi)$ are symmetric bilinear forms. More generally the elements of the trace of the product of many matrices in $\mathfrak{D}_N[GF(p^\ell)]$ are symmetric multilinear forms. Definition II.1 and proposition II.2 can be generalized in the present context, and for clarity we give them explicitly below:

Definition II.4. Let $\{\Theta_0^{(i)}, ..., \Theta_{\ell-1}^{(i)}\}$ be matrices in $\mathfrak{D}_N(\mathbb{Z}_p)$ (with $i = 1, ..., N$) and $\sigma^{(N)} \in \mathcal{S}_N$. The symmetric multilinear form

$$\mathfrak{L}_N(\sigma^{(N)}) = \sum \sigma^{(N)}_{\mu_1...\mu_N}\Theta^{(1)}_{\mu_1}...\Theta^{(N)}_{\mu_N}, \tag{80}$$

is compatible with $GF(p^\ell)$ if there exist a basis $\{\mathcal{E}_\lambda\}$ in $GF(p^\ell)$ such that

$$\mathfrak{L}_N(\sigma^{(N)}) = \mathrm{Tr}_G\left(\Theta^{(1)}...\Theta^{(N)}\right); \qquad \Theta^{(i)} = \sum \Theta^{(i)}_\lambda\mathcal{E}_\lambda \in \mathfrak{D}_N[GF(p^\ell)]. \tag{81}$$

Proposition II.5. *The symmetric multilinear form $\mathfrak{L}_N(\sigma^{(N)})$ of Eq.(80) is compatible with $GF(p^\ell)$, if and only if $\sigma^{(N)} \in \mathfrak{G}_N$.*

Proof. The proof is analogous to the proof of proposition II.2. □

III. QUANTUM SYSTEMS WITH POSITIONS AND MOMENTA IN $\mathbb{Z}_p$

We consider a quantum system where the position and momentum take values in $\mathbb{Z}_p$. The corresponding Hilbert space $\mathcal{H}$ is p-dimensional. Let $|\mathcal{X}; m\rangle$ be an orthonormal basis which we call position states. Here $\mathcal{X}$ is not a variable but a symbol which indicates 'position states', and m takes values in $\mathbb{Z}_p$. The Fourier transform is given by:

$$\mathcal{F} = p^{-1/2} \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \omega(mn) |\mathcal{X}; m\rangle\langle\mathcal{X}; n|; \qquad \mathcal{F}^4 = \mathbf{1}. \tag{82}$$

The orthonormal basis of momentum states is

$$|\mathcal{P}; m\rangle = \mathcal{F}|\mathcal{X}; m\rangle = p^{-1/2} \sum_n \omega(mn) |\mathcal{X}; n\rangle. \tag{83}$$

Here $\mathcal{P}$ is not a variable but a symbol which indicates 'momentum states'.

Position and momentum operators are defined as

$$\begin{aligned} \mathcal{Q} &= \sum_m m |\mathcal{X}; m\rangle\langle\mathcal{X}; m|; \qquad \mathcal{Q}^p = \mathcal{Q} \\ \mathcal{P} &= \sum_m m |\mathcal{P}; m\rangle\langle\mathcal{P}; m|; \qquad \mathcal{P}^p = \mathcal{P}. \end{aligned} \tag{84}$$

They are $p \times p$ matrices with elements in $\mathbb{Z}_p$. We note that there are difficulties, if we act directly with these matrices, on wavefunctions which are complex p-dimensional vectors (this will require multiplication of complex numbers with numbers in $\mathbb{Z}_p$). $\mathcal{Q}$, $\mathcal{P}$ are used through characters $\omega(\alpha\mathcal{Q}^n)$, $\omega(\beta\mathcal{P}^n)$ (where $\alpha, \beta \in \mathbb{Z}_p$), which are $p \times p$ complex matrices.

The position-momentum phase space is the toroidal lattice $\mathbb{Z}_p \times \mathbb{Z}_p$. Displacement operators are defined as

$$\begin{aligned} \mathcal{Z} &= \omega(\mathcal{Q}) = \sum_{n=0}^{p-1} \omega(n) |\mathcal{X}; n\rangle\langle\mathcal{X}; n| \\ \mathcal{X} &= \omega(-\mathcal{P}) = \sum_{n=0}^{p-1} \omega(-n) |\mathcal{P}; n\rangle\langle\mathcal{P}; n| \\ \mathcal{X}^p &= \mathcal{Z}^p = \mathbf{1}; \qquad \mathcal{X}^\beta \mathcal{Z}^\alpha = \mathcal{Z}^\alpha \mathcal{X}^\beta \omega(-\alpha\beta); \qquad \alpha, \beta \in \mathbb{Z}_p. \end{aligned} \tag{85}$$

General displacement operators are defined as

$$\mathcal{D}(\alpha, \beta) = \mathcal{Z}^\alpha \mathcal{X}^\beta \omega(-2^{-1}\alpha\beta). \tag{86}$$

The $\mathcal{D}(\alpha, \beta)\omega(\gamma)$ form a representation of the Heiseberg-Weyl group.

For later use we also introduce the 'rescaled Fourier transform'

$$\mathcal{F}_\eta = p^{-1/2} \sum_{m=0}^{p-1} \sum_{n=0}^{d-1} \omega(\eta m n) |\mathcal{X}; m\rangle\langle\mathcal{X}; n|; \qquad \mathcal{F}_\eta^4 = \mathbf{1}. \tag{87}$$

$\eta \in \mathbb{Z}_p$ is a constant which could be called 'inverse Planck constant'. Then

$$\mathcal{F}_\eta |\mathcal{X}; m\rangle = |\mathcal{P}; \eta m\rangle. \tag{88}$$

The Hamiltonian is a complex $p \times p$ Hermitian matrix which is a function of $\mathcal{Q}$ and $\mathcal{P}$. Taking into account our comment earlier that the matrices $\mathcal{Q}$, $\mathcal{P}$ are used through characters, we write it as function of $\omega(\alpha_1 \mathcal{Q})$, $\omega(\beta_1 \mathcal{P})$, $\omega(\alpha_2 \mathcal{Q}^2)$, $\omega(\beta_2 \mathcal{P}^2)$, etc.

$$h = h[\omega(\alpha_n \mathcal{Q}^n), \omega(\beta_n \mathcal{P}^n)]; \qquad \alpha_n, \beta_n \in \mathbb{Z}_p. \tag{89}$$

An example of such a Hamiltonian is

$$ih = \ln U; \qquad U = \omega(\beta_2 \mathcal{P}^2)\omega(\alpha_2 \mathcal{Q}^2)\omega(\alpha_4 \mathcal{Q}^4); \qquad \alpha_2, \alpha_4, \beta_4 \in \mathbb{Z}_p. \tag{90}$$

The logarithm is a multivalued function and we take the principal logarithm. In this case the evolution operator is $\exp(ith) = U^t$.

IV. ℓ-PARTITE SYSTEMS WITH POSITIONS AND MOMENTA IN $[\mathbb{Z}_p]^\ell$

We consider an ℓ-partite system where each component system is of the type described in the previous section III. Its Hilbert space is

$$H = \mathcal{H} \otimes ... \otimes \mathcal{H}. \tag{91}$$

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.

Position states are labelled with vectors $(m_\ell) \in [\mathbb{Z}_p]^\ell$

$$|X; (m_\ell)\rangle \;\equiv\; |\mathcal{X}; m_0\rangle \otimes ... \otimes |\mathcal{X}; m_{\ell-1}\rangle, \tag{92}$$

and similarly the momentum states. The Fourier transform is $\mathcal{F} \otimes ... \otimes \mathcal{F}$.

We use the notation

$$\mathfrak{Q}_\lambda = \mathbf{1} \otimes ... \otimes \mathbf{1} \otimes \mathcal{Q}^{(\lambda)} \otimes \mathbf{1} \otimes ... \otimes \mathbf{1}; \qquad \mathfrak{P}_\lambda = \mathbf{1} \otimes ... \otimes \mathbf{1} \otimes \mathcal{P}^{(\lambda)} \otimes \mathbf{1} \otimes ... \otimes \mathbf{1}, \tag{93}$$

where $\mathcal{Q}^{(\lambda)}$ indicates that the operator Q acts on the λ-subsystem (where $\lambda = 0, ..., \ell - 1$), and similarly for $\mathcal{P}^{(\lambda)}$. We note the relations

$$\begin{aligned} \mathfrak{Q}_\lambda \mathfrak{Q}_\mu &= \mathbf{1} \otimes ... \otimes \mathcal{Q}^{(\lambda)} \otimes ... \otimes \mathcal{Q}^{(\mu)} \otimes ... \otimes \mathbf{1}, \\ \mathfrak{Q}_\lambda \mathfrak{Q}_\mu \mathfrak{Q}_\nu &= \mathbf{1} \otimes ... \otimes \mathcal{Q}^{(\lambda)} \otimes ... \otimes \mathcal{Q}^{(\mu)} \otimes ... \otimes \mathcal{Q}^{(\nu)} \otimes ... \otimes \mathbf{1}, \end{aligned} \tag{94}$$

etc.

The Hamiltonian of such system is a generalization of Eq.(89). We first introduce the following diagonal matrices with elements which are multilinear forms

$$\begin{aligned}
\mathfrak{L}_1(\sigma) &= \sum \sigma_\lambda \mathfrak{Q}_\lambda; \qquad \mathfrak{K}_1(\tau) = \sum \tau_\lambda \mathfrak{P}_\lambda; \qquad \sigma, \tau \in [\mathbb{Z}_p]^\ell, \\
\mathfrak{L}_n(\sigma^{(n)}) &= \sum \sigma^{(n)}_{\lambda_1 \ldots \lambda_n} \mathfrak{Q}_{\lambda_1} \ldots \mathfrak{Q}_{\lambda_n}; \qquad \sigma^{(n)} \in \mathcal{S}_n \\
\mathfrak{K}_n(\tau^{(n)}) &= \sum \tau^{(n)}_{\lambda_1 \ldots \lambda_n} \mathfrak{P}_{\lambda_1} \ldots \mathfrak{P}_{\lambda_n}; \qquad \tau^{(n)} \in \mathcal{S}_n.
\end{aligned} \tag{95}$$

The Hamiltonian is a function of $\omega(\alpha_1 \mathfrak{L}_1)$, $\omega(\beta_1 \mathfrak{K}_1)$, $\omega(\alpha_2 \mathfrak{L}_2)$, $\omega(\beta_2 \mathfrak{K}_2)$, etc.

$$h = h\left[\omega[\alpha_n \mathfrak{L}_n(\sigma^{(n)})], \omega[\beta_n \mathfrak{K}_n(\tau^{(n)})]\right]; \qquad \alpha_n, \beta_n \in \mathbb{Z}_p. \tag{96}$$

We use the notation $\mathbf{h}(\mathcal{S})$ for the set of these Hamiltonians, where the $\mathcal{S}$ in the notation indicates the fact that $\sigma^{(n)}, \tau^{(n)} \in \mathcal{S}$.

We note that terms like $\ln \omega[\mathfrak{L}_1(\sigma)] \ln \omega[\mathfrak{K}_1(\tau)]$ involve products of both positions and momenta (i.e., $\mathbf{1} \otimes \ldots \otimes \mathcal{Q}^{(\lambda)} \otimes \ldots \otimes \mathcal{P}^{(\mu)} \otimes \ldots \otimes \mathbf{1}$). More generally terms like $\ln \omega[\alpha_n \mathfrak{L}_n(\sigma^{(n)})] \ln \omega[\beta_n \mathfrak{K}_n(\tau^{(n)})]$ involve products of powers of positions and powers of momenta.

V. QUANTUM SYSTEMS WITH POSITIONS AND MOMENTA IN $GF(p^\ell)$

We consider an ℓ-partite system similar to the one described in the previous section IV. Its Hilbert space has been given in Eq.(91). Here we will label the position and momentum states with elements in $GF(p^\ell)$ and we will express the whole quantum mechanical formalism in terms of Galois arithmetic. This cannot be done for a general ℓ-partite system. This is because $GF(p^\ell)$ is an ℓ-dimensional vector space over $\mathbb{Z}_p$, but in addition to that it has a lot of extra structure (related to the multiplication rule, the trace, etc). Therefore we start with a system similar to that in section IV, and we will show that in order to give it Galois structure, its Hamiltonian should belong to a subset of the set of Hamiltonians $\mathbf{h}(\mathcal{S})$.

A. Position bases

Using the polynomial basis in $GF(p^\ell)$, we label the position state $|\mathcal{X}; m_0\rangle \otimes \ldots \otimes |\mathcal{X}; m_{\ell-1}\rangle$ in H (where $m_\kappa \in \mathbb{Z}_p$) with elements in $GF(p^\ell)$ as follows:

$$|X; m\rangle \equiv |\mathcal{X}; m_0\rangle \otimes \ldots \otimes |\mathcal{X}; m_{\ell-1}\rangle; \qquad m = \sum_{\kappa=0}^{\ell-1} m_\kappa \epsilon^\kappa; \qquad m_\kappa = \mathrm{Tr}(m E_\kappa). \tag{97}$$

It is clear that a basis in $GF(p^\ell)$ is required for this labelling method. If we use the basis of Eq.(16), we get a different labelling of the position state $|\mathcal{X}; m_0\rangle \otimes \ldots \otimes |\mathcal{X}; m_{\ell-1}\rangle$ as follows:

$$|X; V; n\rangle = |\mathcal{X}; m_0\rangle \otimes \ldots \otimes |\mathcal{X}; m_{\ell-1}\rangle; \qquad n = \sum m_\kappa \mathcal{E}_\kappa = \sum \epsilon^\lambda (V^{-1})_{\lambda\kappa} m_\kappa; \qquad m_\kappa = \mathrm{Tr}(n \overline{\mathcal{E}}_\kappa). \tag{98}$$

The matrix V in the notation, specifies the basis in $GF(p^\ell)$ (if there is no V in the notation, it means that we use the polynomial basis of Eq.(5)). We can show that

$$|X;V;n\rangle = |X;m\rangle \qquad n = \sum \mathcal{E}_\kappa \mathrm{Tr}(mE_\kappa); \qquad m = \sum \epsilon^\kappa \mathrm{Tr}(n\overline{\mathcal{E}}_\kappa). \tag{99}$$

There is a bijection between $\mathfrak{B}[GF(p^\ell)]$ and the set of labelling methods. Below we introduce transformations from one labelling method to another.

B. A representation of the $GL(\ell,\mathbb{Z}_p)$ group: B_V transformations

Let B_V be the following unitary transformation in the Hilbert space H:

$$\begin{aligned} B_V &= \sum_{n\in GF(p^\ell)} |X;m\rangle\langle X;n| = \sum_{n_0,\ldots,n_{\ell-1}} |\mathcal{X};m_0\rangle\langle\mathcal{X};n_0|\otimes\ldots\otimes|\mathcal{X};m_{\ell-1}\rangle\langle\mathcal{X};n_{\ell-1}| \\ m &= \sum \epsilon^\kappa \mathrm{Tr}(n\overline{\mathcal{E}}_\kappa) \qquad m_\lambda = \sum_{\kappa=0}^{\ell-1} V_{\lambda\kappa} n_\kappa. \end{aligned} \tag{100}$$

With these transformations we can change the $GF(p^\ell)$ basis used in the labelling method:

$$B_V|X;n\rangle = |X;V;n\rangle = |X;m\rangle \qquad m = \sum \epsilon^\kappa \mathrm{Tr}(n\overline{\mathcal{E}}_\kappa). \tag{101}$$

We can easily show that

$$B_{V_1} B_{V_2} = B_{V_1 V_2}; \qquad B_{\mathbf{1}} = \mathbf{1}. \tag{102}$$

Therefore the B_V transformations form a unitary representation of the $GL(\ell,\mathbb{Z}_p)$ group. Below we have states $|s\rangle$ and operators Θ which are calculated using the polynomial basis in $GF(p^\ell)$ and we go to their counterparts $|s;V\rangle$ and Θ_V which correspond to another basis in $GF(p^\ell)$, as follows

$$|s;V\rangle \equiv B_V|s\rangle; \qquad \Theta_V = B_V\,\Theta\,B_V^\dagger. \tag{103}$$

C. Fourier transform and momentum bases

We use the polynomial basis of Eq.(5) and define the Fourier operator, as

$$\begin{aligned} F &= p^{-\ell/2} \sum_{m,n\in GF(p^\ell)} \chi(mn)|X;m\rangle\langle X;n| \\ &= p^{-\ell/2} \sum \omega\left[\sum g_{\kappa\lambda} m_\kappa n_\lambda\right] |\mathcal{X};m_0\rangle\langle\mathcal{X};n_0|\otimes\ldots\otimes|\mathcal{X};m_{\ell-1}\rangle\langle\mathcal{X};n_{\ell-1}| \\ F^4 &= \mathbf{1}, \end{aligned} \tag{104}$$

where $m = \sum m_\kappa \epsilon^\kappa$ and $n = \sum n_\kappa \epsilon^\kappa$.

Acting with the Fourier operator on position states we get the momentum states:

$$\begin{aligned} |P;m\rangle &= F|X;m\rangle = p^{-\ell/2}\sum_n \chi(mn)|X;n\rangle \\ &= |\mathcal{P};\overline{m}_0\rangle\otimes ...\otimes|\mathcal{P};\overline{m}_{\ell-1}\rangle. \end{aligned} \tag{105}$$

The dual components $\overline{m}_i$ of m appear in the momentum states.

We can go to the general basis of Eq.(16), with the B_V transformations::

$$\begin{aligned} F_V &\equiv B_V F B_V^\dagger = p^{-\ell/2}\sum_{m,n\in GF(p^\ell)}\chi(mn)|X;V;m\rangle\langle X;V;n| \\ &= p^{-\ell/2}\sum\omega\left[\sum(g_V)_{\kappa\lambda}m_\kappa n_\lambda\right]|\mathcal{X};m_0\rangle\langle\mathcal{X};n_0|\otimes ...\otimes|\mathcal{X};m_{\ell-1}\rangle\langle\mathcal{X};n_{\ell-1}|. \end{aligned} \tag{106}$$

Here $m=\sum m_\kappa\mathcal{E}_\kappa$ and $n=\sum n_\kappa\mathcal{E}_\kappa$.

The momentum states with respect to this basis in $GF(p^\ell)$, are:

$$|P;V;n\rangle = F_V|X;V;n\rangle = |\mathcal{P};\overline{n}_0\rangle\otimes ...\otimes|\mathcal{P};\overline{n}_{\ell-1}\rangle;\qquad n=\sum\overline{n}_\kappa\overline{\mathcal{E}}_\kappa. \tag{107}$$

We can show that

$$|P;V;n\rangle = |P;m\rangle;\qquad n=\sum\overline{\mathcal{E}}_\kappa\mathrm{Tr}(m\epsilon^\kappa);\qquad m=\sum E_\kappa\mathrm{Tr}(n\mathcal{E}_\kappa). \tag{108}$$

Eqs.(99),(108) show that if $|X;V;n\rangle=|X;m\rangle$ and $|P;V;n'\rangle=|P;m'\rangle$ then $\mathrm{Tr}(nn')=\mathrm{Tr}(mm')$.

In a diagonal basis Eq.(72) shows that

$$F_{\mathrm{diag}} = \mathcal{F}_{\mathfrak{g}_0}\otimes ...\otimes\mathcal{F}_{\mathfrak{g}_{\ell-1}}. \tag{109}$$

In this case Eq.(107) reduces to

$$|P;V_{\mathrm{diag}};m\rangle = |\mathcal{P};\mathfrak{g}_0 m_0\rangle\otimes ...\otimes|\mathcal{P};\mathfrak{g}_{\ell-1}m_{\ell-1}\rangle;\qquad m=\sum m_\kappa\mathfrak{E}_\kappa=\sum\mathfrak{g}_\kappa m_\kappa\overline{\mathfrak{E}}_\kappa. \tag{110}$$

In the case of odd ℓ, there exist self-dual bases. In this case Eq.(73) shows that

$$F_{\mathrm{SD}} = \mathcal{F}\otimes ...\otimes\mathcal{F}, \tag{111}$$

and Eq.(107) reduces to

$$|P;V_{\mathrm{SD}};m\rangle = |\mathcal{P};\widetilde{m}_0\rangle\otimes ...\otimes|\mathcal{P};\widetilde{m}_{\ell-1}\rangle;\qquad m=\sum\widetilde{m}_\kappa\widetilde{E}_\kappa. \tag{112}$$

D. Position and momentum operators

The position operator is a $p^\ell\times p^\ell$ diagonal matrix with elements in $GF(p^\ell)$:

$$Q = \sum_m m|X;m\rangle\langle X;m| = \sum_\lambda\mathfrak{Q}_\lambda\epsilon^\lambda;\qquad Q^{p^\ell}=Q. \tag{113}$$

The product αQ where $\alpha \in GF(p^\ell)$, is also defined and it is a $p^\ell \times p^\ell$ diagonal matrix with elements in $GF(p^\ell)$.

Characters of powers of Q, are $p^\ell \times p^\ell$ complex matrices given by

$$\chi(\alpha Q^r) = \sum_{m \in GF(p^\ell)} \chi(\alpha m^r)|X;m\rangle\langle X;m|; \qquad \alpha \in GF(p^\ell). \tag{114}$$

We note that Q is a matrix with elements in $GF(p^\ell)$ and cannot act on wavefunctions which are vectors with p^ℓ components which are complex numbers. The Q is used through the characters of Eq.(114), which are complex matrices. In fact we can introduce directly the complex matrices of Eq.(114), without introducing Q. The only reason for introducing Q is in order to interpret physically the complex matrices of Eq.(114) as exponentials of powers of the position operator, and use them in Hamiltonians below which are analogous to harmonic oscillator Hamiltonians.

The discussion above can be extended to the momentum operator, which is given by

$$P = \sum_m m|P;m\rangle\langle P;m| = \sum_\lambda E_\lambda \mathfrak{P}_\lambda; \qquad P^{p^\ell} = P. \tag{115}$$

In this case

$$\chi(\beta P^r) = \sum_{m \in GF(p^\ell)} \chi(\beta m^r)|P;m\rangle\langle P;m| = F\chi(\beta Q^r)F^\dagger; \qquad \beta \in GF(p^\ell). \tag{116}$$

Clearly

$$[\chi(\alpha Q^r)]^p = [\chi(\beta P^r)]^p = \mathbf{1}. \tag{117}$$

Characters with $r = 1$ are used below in displacements.

Above we used the polynomial basis in $GF(p^\ell)$. We can go to an arbitrary basis with the operators B_V. For example,

$$\begin{aligned} Q_V &= B_V Q B_V^\dagger = \sum_m m|X;V;m\rangle\langle X;V;m| = \sum_\lambda \mathfrak{Q}_\lambda \mathcal{E}_\lambda \\ P_V &= B_V P B_V^\dagger = \sum_m m|P;V;m\rangle\langle P;V;m| = \sum_\lambda \mathfrak{P}_\lambda \overline{\mathcal{E}}_\lambda. \end{aligned} \tag{118}$$

E. Displacements and the Heisenberg-Weyl group

Displacement operators in the $GF(p^\ell) \times GF(p^\ell)$ phase space are given by:

$$\begin{aligned} Z^\alpha &= \chi(\alpha Q) = \sum_n \chi(\alpha n)|X;n\rangle\langle X;n| \\ X^\beta &= \chi(-\beta P) = \sum_n \chi(-\beta n)|P;n\rangle\langle P;n|, \end{aligned} \tag{119}$$

where $\alpha, \beta \in GF(p^\ell)$. They displace the position and momentum states as follows:

$$Z^\alpha|P;m\rangle = |P;m+\alpha\rangle; \qquad Z^\alpha|X;m\rangle = \chi(\alpha m)|X;m\rangle \tag{120}$$

$$X^\beta|P;m\rangle = \chi(-m\beta)]|P;m\rangle; \qquad X^\beta|X;m\rangle = |X;m+\beta\rangle. \tag{121}$$

We can show that

$$X^\beta Z^\alpha = Z^\alpha X^\beta \chi(-\alpha\beta). \tag{122}$$

General displacement operators are given by:

$$D(\alpha,\beta) = Z^\alpha X^\beta \chi(-2^{-1}\alpha\beta). \tag{123}$$

The $D(\alpha,\beta)\chi(\gamma)$ form a representation of the Heisenberg-Weyl group, which we denote as $HW[GF(p^\ell)]$.

Proposition V.1. *The displacement operators transform under the B_V transformations as follows:*

$$D_V(\alpha,\beta) \equiv B_V D(\alpha,\beta) B_V^\dagger = D(\alpha',\beta'); \qquad \alpha' = \sum E_\kappa \mathrm{Tr}(\alpha\mathcal{E}_\kappa); \qquad \beta' = \sum \epsilon^\kappa \mathrm{Tr}(\beta\overline{\mathcal{E}}_\kappa). \tag{124}$$

The trace of $\alpha\beta$ is preserved, i.e., $\mathrm{Tr}(\alpha\beta) = \mathrm{Tr}(\alpha'\beta')$.

Proof. Using Eq.(99) we prove that

$$\begin{aligned} B_V Z^\alpha B_V^\dagger &= \sum_{n\in GF(p^\ell)} \chi(\alpha n)|X;V;n\rangle\langle X;V;n| = \sum_{n\in GF(p^\ell)} \chi(\alpha n)|X;m\rangle\langle X;m| \\ m &= \sum \epsilon^\kappa \mathrm{Tr}(n\overline{\mathcal{E}}_\kappa). \end{aligned} \tag{125}$$

But

$$\chi(\alpha n) = \chi(\alpha' m); \qquad m = \sum \epsilon^\kappa \mathrm{Tr}(n\overline{\mathcal{E}}_\kappa); \qquad \alpha' = \sum E_\kappa \mathrm{Tr}(\alpha\mathcal{E}_\kappa). \tag{126}$$

Combining Eqs (125),(126) we prove that $Z_V^\alpha = Z^{\alpha'}$.

In a similar way using Eq.(108) we get

$$\begin{aligned} B_V X^\beta B_V^\dagger &= \sum_{n\in GF(p^\ell)} \chi(\beta n)|P;V;n\rangle\langle P;V;n| = \sum_{n\in GF(p^\ell)} \chi(\beta n)|P;m\rangle\langle P;m| \\ m &= \sum E_\kappa \mathrm{Tr}(n\mathcal{E}_\kappa). \end{aligned} \tag{127}$$

But

$$\chi(\beta n) = \chi(\beta' m); \qquad m = \sum E_\kappa \mathrm{Tr}(n\mathcal{E}_\kappa); \qquad \beta' = \sum \epsilon^\kappa \mathrm{Tr}(\beta\overline{\mathcal{E}}_\kappa). \tag{128}$$

Combining Eqs (127),(128) we prove that $X_V^\beta = X^{\beta'}$. Finally we prove that $\chi(-2^{-1}\alpha\beta) = \chi(-2^{-1}\alpha'\beta')$. This shows that $D_V(\alpha,\beta) = D(\alpha',\beta')$.

We next use Eq.(25) to prove

$$\mathrm{Tr}(\alpha\beta) = \mathrm{Tr}(\alpha\mathcal{E}_\kappa)\mathrm{Tr}(\beta\overline{\mathcal{E}}_\kappa) = \mathrm{Tr}(\alpha'\beta'). \tag{129}$$

□

In an arbitrary basis of $GF(p^\ell)$, we use Eq.(70) to show that the displacement operators acting on H can be expressed in terms of the displacement operators $\mathcal{D}$ acting on the various subsystems as follows:

$$D_V(\alpha,\beta)=\mathcal{D}(\overline{\alpha}_0,\beta_0)\otimes ...\otimes\mathcal{D}(\overline{\alpha}_{\ell-1},\beta_{\ell-1});\qquad \alpha=\sum_\lambda \overline{\alpha}_\lambda\overline{\mathcal{E}}_\lambda;\qquad \beta=\sum_\lambda\beta_\lambda\mathcal{E}_\lambda, \tag{130}$$

where $\overline{\alpha}_\lambda$ are the dual components of α, and β_λ the components of β, in the basis $\{\mathcal{E}_\lambda\}$.

In a diagonal basis Eq.(130) becomes

$$D_{\rm diag}(\alpha,\beta)=\mathcal{D}(\mathfrak{g}_0\alpha_0,\beta_0)\otimes ...\otimes\mathcal{D}(\mathfrak{g}_{\ell-1}\alpha_{\ell-1},\beta_{\ell-1});\qquad \alpha=\sum_\lambda \alpha_\lambda\mathfrak{E}_\lambda=\sum_\lambda\mathfrak{g}_\lambda\alpha_\lambda\overline{\mathfrak{E}}_\lambda;\qquad \beta=\sum_\lambda\beta_\lambda\mathfrak{E}_\lambda. \tag{131}$$

For odd ℓ, there exist self-dual bases. In this case

$$D_{\rm SD}(\alpha,\beta)=\mathcal{D}(\widetilde{\alpha}_0,\widetilde{\beta}_0)\otimes ...\otimes\mathcal{D}(\widetilde{\alpha}_{\ell-1},\widetilde{\beta}_{\ell-1});\qquad \alpha=\sum\widetilde{\alpha}_\lambda\widetilde{E}_\lambda;\qquad \beta=\sum\widetilde{\beta}_\lambda\widetilde{E}_\lambda. \tag{132}$$

VI. COMPATIBILITY OF HAMILTONIANS IN $\mathbf{h}(\mathcal{S})$ WITH $GF(p^\ell)$

The Hamiltonian of a system with positions and momenta in $GF(p^\ell)$ is a function of Q and P. As we explained earlier, Q and P are used through characters $\chi(\alpha_N Q^N)$, $\chi(\beta_N P^N)$ which are complex matrices. Therefore we write the Hamiltonian as a function of $\chi(\alpha_1 Q)$, $\chi(\beta_1 P)$, $\chi(\alpha_2 Q^2)$, $\chi(\beta_2 P^2)$, etc.

$$h=h\left[\chi(\alpha_N Q^N),\chi(\beta_N P^N)\right] \tag{133}$$

We consider the class of Hamiltonians in Eq.(133), and for simplicity, we take the coefficients α_N,β_N to be in $\mathbb{Z}_p$ when $N\geq 2$ (so that $\mathrm{Tr}_G(\alpha_N Q^N)=\alpha_N\mathrm{Tr}_G(Q^N)$ and $\mathrm{Tr}_G(\beta_N P^N)=\beta_N\mathrm{Tr}_G(P^N)$). We denote as $\mathbf{h}_{\rm Gal}$ the set of these Hamiltonians.

We note that it might be that there are other complex functions of Q and P which can be used as Hamiltonians. For example, the norm of an element of a Galois field is an element of $\mathbb{Z}_p$ and it can be used in characters. These characters are multiplicative and they are not suitable for Fourier transforms (which are a basic part of our formalism). Nevertheless, they might lead to a wider class of Hamiltonians.

Below we introduce the concept of a Hamiltonian in $\mathbf{h}(\mathcal{S})$ which is compatible with $GF(p^\ell)$ (generalizing definition II.4 and proposition II.5).

Definition VI.1. A Hamiltonian $h\left[\omega[\alpha_N\mathfrak{L}_N(\sigma^{(N)})],\omega[\beta_N\mathfrak{K}_N(\tau^{(N)})]\right]$ in $\mathbf{h}(\mathcal{S})$ (i.e., of the type given in Eq.(96)) is compatible with $GF(p^\ell)$ if there exists a basis $\{\mathcal{E}_\lambda\}$ in $GF(p^\ell)$, such that the $Q_V=\sum\mathfrak{Q}_\lambda\mathcal{E}_\lambda$ and $P_V=\sum\mathfrak{P}_\lambda\overline{\mathcal{E}}_\lambda$ satisfy the relations

$$\mathfrak{L}_N(\sigma^{(N)})=\mathrm{Tr}_G(Q_V^N);\qquad \mathfrak{K}_N(\tau^{(N)})=\mathrm{Tr}_G(P_V^n), \tag{134}$$

for all $N\geq 2$. In this case there exists a Hamiltonian $h\left[\{\chi(\alpha_N Q_V^N),\chi(\beta_N P_V^N)\}\right]$ in $\mathbf{h}_{\rm Gal}$ such that

$$h\left[\omega[\alpha_N\mathfrak{L}_N(\sigma^{(N)})],\omega[\beta_N\mathfrak{K}_N(\tau^{(N)})]\right]=h\left[\{\chi(\alpha_N Q_V^N),\chi(\beta_N P_V^N)\}\right], \tag{135}$$

where $\alpha_N,\beta_N\in\mathbb{Z}_p$.

Remark VI.2. The above definition refers to $N \geq 2$. The case $N = 1$ corresponds to terms like $\omega(\sum \sigma_\lambda \mathfrak{Q}_\lambda)$ and $\omega(-\sum \tau_\lambda \mathfrak{P}_\lambda)$ and they are always compatible with $GF(p^\ell)$, in the sense that they can be writen as displacement operators with parameters in $GF(p^\ell)$ (Eq.(130)):

$$\omega\left(\sum \sigma_\lambda \mathfrak{Q}_\lambda\right)\omega\left(-\sum \tau_\lambda \mathfrak{P}_\lambda\right) = \mathcal{Z}^{\sigma_0}\mathcal{X}^{\tau_0} \otimes ... \otimes \mathcal{Z}^{\sigma_{\ell-1}}\mathcal{X}^{\tau_{\ell-1}} = \chi(\sigma Q)\chi(-\tau P) = D(\sigma,\tau)\chi(2^{-1}\sigma\tau)$$
$$\sigma = \sum \sigma_\lambda \overline{\mathcal{E}}_\lambda; \quad \tau = \sum \tau_\lambda \mathcal{E}_\lambda. \tag{136}$$

Here $\mathcal{E}_\lambda$ can be any basis in $GF(p^\ell)$ because proposition V.1 shows that a change in the basis simply gives a displacement operator with different parameters.

Theorem VI.3. *Let $h\left[\omega[\alpha_N \mathfrak{L}_N(\sigma^{(N)})],\, \omega[\beta_N \mathfrak{K}_N(\tau^{(N)})]\right]$ be a Hamiltonian in $\mathbf{h}(\mathcal{S})$. This Hamiltonian is compatible with $GF(p^\ell)$ if and only if there exists $V \in GL(\ell, \mathbb{Z}_p)$ (which does not depend on N) such that $\sigma^{(N)} \in \mathfrak{G}(V)$ and $\tau^{(N)} \in \overline{\mathfrak{G}}(V)$, for all $N \geq 2$*

Proof. If there exists $V \in GL(\ell, \mathbb{Z}_p)$ such that $\sigma^{(N)} \in \mathfrak{G}(V)$ and $\tau^{(N)} \in \overline{\mathfrak{G}}(V)$, we define the basis $\{\mathcal{E}_\kappa\}$ using Eq.(16), and show that

$$\sum_{\mu_1,...,\mu_N} \sigma^{(N)}_{\mu_1...\mu_N} \mathfrak{Q}_{\mu_1}...\mathfrak{Q}_{\mu_N} = \mathrm{Tr}_G(Q^N); \quad Q = \sum_\mu \mathfrak{Q}_\mu \mathcal{E}_\mu$$
$$\sum_{\mu_1,...,\mu_N} \tau^{(N)}_{\mu_1...\mu_N} \mathfrak{P}_{\mu_1}...\mathfrak{P}_{\mu_N} = \mathrm{Tr}_G(P^N); \quad P = \sum_\mu \mathfrak{P}_\mu \overline{\mathcal{E}}_\mu. \tag{137}$$

Therefore Eqs(134),(135) are valid and the Hamiltonian is compatible with $GF(p^\ell)$.

Conversely, if Eqs.(137) are valid (for all N), then

$$\sigma^{(N)}_{\mu_1...\mu_N} = \mathrm{Tr}(\mathcal{E}_{\mu_1}...\mathcal{E}_{\mu_N}); \quad \tau^{(N)}_{\mu_1...\mu_N} = \mathrm{Tr}(\overline{\mathcal{E}}_{\mu_1}...\overline{\mathcal{E}}_{\mu_N}) \tag{138}$$

Eq.(26) shows that $\sigma^{(N)} \in \mathfrak{G}_N$ and Eq.(27) shows that $\tau^{(N)} \in \overline{\mathfrak{G}}_N$. □

In view of this theorem we denote the set of Hamiltonians in $\mathbf{h}(\mathcal{S})$ which are compatible with $GF(p^\ell)$, as $\mathbf{h}(\mathfrak{G})$. Clearly $\mathbf{h}(\mathfrak{G})$ is a proper subset of $\mathbf{h}(\mathcal{S})$. Also $\mathbf{h}(\mathfrak{G})$ is isomorphic to $\mathbf{h}_{\mathrm{Gal}}$. The quantum formalism in an ℓ-partite system with Hamiltonian in $\mathbf{h}(\mathfrak{G})$ can be expressed in terms of Galois arithmetic.

A. Coupling between the subsystems by the $g^{(N)}$-tensors

The Hamiltonian $h\left[\{\chi(\alpha_N Q_V^N), \chi(\beta_N P_V^N)\}\right]$ contains terms $\mathrm{Tr}_G(Q_V^N)$, $\mathrm{Tr}_G(P_V^N)$ (for $\alpha_N, \beta_N \in \mathbb{Z}_p$). These terms describe coupling of N subsystems (some of which can be the same subsystem) related to the off-diagonal elements of the tensor $g_V^{(N)}$. For example,

$$\mathrm{Tr_G} {Q_V}^2 = \sum_{\lambda,\mu} (g_V)_{\lambda\mu} \mathbf{1} \otimes ... \otimes \mathcal{Q}^{(\lambda)} \otimes ... \otimes \mathcal{Q}^{(\mu)} \otimes ... \otimes \mathbf{1},$$
$$\mathrm{Tr_G} {P_V}^2 = \sum_{\lambda,\mu} (G_V)_{\lambda\mu} \mathbf{1} \otimes ... \otimes \mathcal{P}^{(\lambda)} \otimes ... \otimes \mathcal{P}^{(\mu)} \otimes ... \otimes \mathbf{1}. \tag{139}$$

In these equations we have a particular bi-partite coupling, created by the off-diagonal elements $(g_V)_{\lambda\mu}$, $(G_V)_{\lambda\mu}$. The strength of this coupling is not arbitrary but it is intimately related to Galois arithmetic in the sense that $g_V, G_V \in \mathfrak{G}_2$. If we use matrices in $\mathfrak{R}_2$ we get an ℓ-partite quantum system with positions and momenta in $[\mathbb{Z}_p]^\ell$, and with Hamiltonian which is incompatible with $GF(p^\ell)$. In this case we cannot express the quantum formalism in terms of Galois arithmetic.

The coupling depends on the basis. Mathematically all bases lead to isomorphic results, but practically the Hamiltonians are much simpler in diagonal (and self-dual) bases. Bipartite coupling (related to g_V) is eliminated in a diagonal basis:

$$\mathrm{Tr_G} {Q_V}^2 = \sum_\lambda \mathfrak{g}_\lambda \mathbf{1} \otimes ... \otimes [\mathcal{Q}^2]^{(\lambda)} \otimes ... \otimes \mathbf{1}. \tag{140}$$

Higher order coupling (related to $g_V^{(N)}$ with $N \geq 3$) cannot be eliminated. As an example we consider the $GF(27)$ and get

$$\mathrm{Tr_G} Q^4 = g^{(4)}_{0112} \mathcal{Q} \otimes \mathcal{Q}^2 \otimes \mathcal{Q} + g^{(4)}_{0012} \mathcal{Q}^2 \otimes \mathcal{Q} \otimes \mathcal{Q} + g^{(4)}_{1112} \mathbf{1} \otimes \mathcal{Q}^3 \otimes \mathcal{Q} + ... \tag{141}$$

In a polynomial basis, the $g^{(4)}_{0112}$, $g^{(4)}_{0012}$, $g^{(4)}_{1112}$ have been given in Eq.(55), and in a self-dual basis in Eq.(66).

VII. DISCUSSION

$GF(p^\ell)$ is an ℓ-dimensional vector space over $\mathbb{Z}_p$, but it has a lot of extra structure. We have introduced the concept of symmetric multilinear forms in $[\mathbb{Z}_p]^\ell$ which are compatible with $GF(p^\ell)$ (definition II.1 and proposition II.2).

We have then considered a quantum system with positions and momenta in $GF(p^\ell)$. This is an ℓ-partite system with the Hilbert space given in Eq.(91), and with a Hamiltonian compatible with $GF(p^\ell)$. A change in the basis in $GF(p^\ell)$, produces the unitary transformations B_V studied in section V B. Using these transformations, and our results on symmetric multilinear forms which are compatible with $GF(p^\ell)$, we have proved theorem VI.3 for the Hamiltonians which are compatible with $GF(p^\ell)$. We have explained that these Hamiltonians impose a particular coupling between the ℓ subsystems, described with the $g^{(N)}$-tensors. This is the first step towards quantum engineering of such systems. The second step (which we have not studied here) is to engineer systems with the required Hamiltonians, using ℓ spins with $2j+1 = p$. The desired coupling, might be achieved using quantum control techniques (e.g., by interacting the system with lasers which are switched on and off at appropriate times).

Quantum systems with positions and momenta in $GF(p^\ell)$, might be useful in the general area of information processing, especially in subareas which use Galois fields.

---

[1] A. Vourdas, Rep. Prog. Phys. 67, 267 (2004)

[2] M. Kibler, J. Phys. A42, 353001 (2009)

[3] A. Weil Acta Math. 111, 143 (1964)

[4] A. Terras, 'Fourier analysis on finite groups and applications' (London Math. Soc. London, 1999)

[5] B.C. Berndt, R.J. Evans, K.S. Williams, 'Gauss and Jacobi sums' (Wiley, NY, 1998)

[6] W. Wootters, B.D. Fields, Ann. Phys. (NY), 191, 363 (1989)
K. Gibbons, M.J. Hoffman, W. Wootters, Phys. Rev. A70, 062101 (2004)

[7] S. Chaturvedi, Phys. Rev. A65, 044301 (2002)

[8] S. Bandyopadhyay, P.O. Boykin, V.Roychowdhury, F. Vatan, Algorithmica 34, 512 (2002)

[9] A.O. Pittenger, M.H. Rubin, Linear Algebra Appl. 390, 255 (2004)

[10] A. Klimov, L. Sanchez-Soto, H. de Guise, J. Phys. A38, 2747 (2005)
J.L. Romero, G. Bjork, A.B. Klimov, L.L. Sanchez-Soto, Phys. Rev. A72, 062310 (2005)
G. Bjork, A.B. Klimov, L.L. Sanchez-Soto, Prog. Optics 51, 469 (2008)

[11] M. Saniga, M. Planat, H. Rosu, J. Opt. B-Quantum Semiclass. Optics 6, L19 (2004)
M. Saniga, M. Planat, J. Phys. A39, 435 (2006)

[12] M. Kibler, Int. J. Mod. Phys. 20, 1792 (2006)
M. Kibler, Int. J. Mod. Phys. 20, 1802 (2006)

[13] J. Tolar, G. Hadzitaskos, J. Phys. A42, 245306 (2009)

[14] A. Vourdas, C. Banderier, J. Phys. A43, 042001 (2010)

[15] A. Vourdas, J. Phys.A38, 8453 (2005)
A. Vourdas, Acta Appl. Math. 93, 197 (2006)
A. Vourdas, J. Math. Phys. 47, 092104 (2006)

[16] A. Vourdas, J. Phys. A40, R285 (2007)

[17] A. Vourdas, J. Fourier Anal. Appl. 14, 102 (2008)

[18] S. MacLane, G. Birkhoff, 'Algebra' (MacMillan, New York, 1967)

[19] Z.X. Wan, 'Lectures on finite fields and Galois rings' (World Scintific, Singapore, 2003)

[20] G. Seroussi, A. Lempel, SIAM J. Comput. 9, 758 (1980)
A. Lempel, M. Weinberger, SIAM J. Discrete Math. 1, 193 (1988)

[21] A. Lempel, G. Seroussi, IEEE Trans. Info. The. 37, 1220 (1991)

[22] H.E. Rose, 'A course in number theory' (Oxford U. P., Oxford, 1988)