Harmonic analysis on a Galois field and its subfields

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

Complex functions $\chi(m)$ where m belongs to a Galois field $GF(p^\ell)$, are considered. Fourier transforms, displacements in the $GF(p^\ell) \times GF(p^\ell)$ phase space and symplectic transforms of these functions are studied. It is shown that the formalism inherits many features from the theory of Galois fields. For example, Frobenius transformations and Galois groups are introduced in the present context. The relationship between harmonic analysis on $GF(p^\ell)$ and harmonic analysis on its subfields, is studied.

key words: phase space methods, Heisenberg-Weyl group, Galois fields
MSC: 81S30, 42C30,13B05, 12F10

I. INTRODUCTION

Harmonic analysis of complex functions $\chi(m)$ where m belongs to the ring $\mathbb{Z}_d$ (the integers modulo d) has been studied in a quantum mechanical context, by Weyl [39] and Schwinger [25, 26]. Later many authors continued this line of research (a review with the relevant literature has been presented in [30, 31]). Fourier transforms and displacements in the 'position-momentum' (or 'time-frequency') phase space which in this case is the toroidal lattice $\mathbb{Z}_d \times \mathbb{Z}_d$, have been studied extensively.

When d is equal to a prime number p, we get stronger results. This is due to the fact that the $\mathbb{Z}_p$ is a field and the corresponding phase space $\mathbb{Z}_p \times \mathbb{Z}_p$ is a finite geometry [10, 17, 29]. In this case there is nothing special about the 'position-momentum' (or 'time-frequency') directions in phase space; all results can be proved with respect to other directions in the finite geometry (isotropy of phase space). Symplectic transformations are well defined and form the $Sp(2, \mathbb{Z}_p)$ group.

In [32–34] we have studied in a quantum mechanical context, how we can go from $\mathbb{Z}_p$ to a bigger Galois field $GF(p^\ell)$. This work uses concepts from harmonic analysis of complex functions $\chi(m)$ where m belongs in $GF(p^\ell)$. Related work has also been reported in [7, 8, 19, 35].

With a very different motivation there has been a lot of related work in the context of mutually unbiased bases in quantum systems with d-dimensional Hilbert space. They are bases $\{v_i\}, \{u_i\}$ such that the scalar product $|(v_i, u_j)|^2 = d^{-1}$. It is known that the number of such bases is less or equal to $d + 1$; and that when d is the power of a prime, it is equal to $d + 1$. This problem has recently been studied extensively in the quantum mechanical literature [2, 4, 5, 9, 11, 12, 14, 15, 20–24, 40, 41].

In this paper we continue the work of [32–34] with emphasis on the mathematical aspects. We use ideas from field extension to go from harmonic analysis on $\mathbb{Z}_p$, to harmonic analysis on $GF(p^\ell)$. This mathematical structure inherits many features from the theory of field extension. For example, Frobenius transformations and Galois groups in the context of finite fields, have counterparts in the present context. Also, displacements and symplectic transformations, involve in our context Galois multiplication. We compare and contrast these transformations and other aspects of harmonic analysis on $GF(p^\ell)$, with harmonic analysis on the ring $[\mathbb{Z}_p]^\ell \equiv \mathbb{Z}_p \times ... \times \mathbb{Z}_p$. Different multiplication rules in the two cases, lead to different mathematical structures.

Another aspect of Galois theory which has implications in the present context, is the relationship

between a Galois field with its subfields. We discuss the relationship between harmonic analysis on $GF(p^\ell)$ and harmonic analysis on a subfield $GF(p^d)$ of $GF(p^\ell)$.

In section II we consider complex functions on a Galois field and we discuss the basic formalism. In section III we present Fourier transforms. In section IV, we present theorem IV.3 on Frobenius transforms and the corresponding Galois groups, in the present context. In section V we define displacements and show in lemma V.4 that they form a representation of the Heisenberg-Weyl group. Proposition V.5 presents various properties of the displacement operators. In section VI we consider symplectic transformations and in theorem VI.10 we show that they form a representation of the $Sp(2, GF(p^\ell))$ group [1, 13, 18, 27, 28, 37, 38, 42]. We conclude in section VII with a discussion of our results.

A. Additive characters in Galois fields

In this subsection we explain our notation in relation to Galois fields. We also introduce additive characters which are used later in Fourier transforms.

Notation I.1 (Galois fields)**.** *The elements of the Galois field $GF(p^\ell)$ can be written as polynomials in terms of an 'indeterminate' ϵ as*

$$m = m_0 + m_1\epsilon + ... + m_{\ell-1}\epsilon^{\ell-1}; \qquad m_0, m_1, ..., m_{\ell-1} \in \mathbb{Z}_p \tag{1}$$

They are defined modulo an irreducible polynomial of degree ℓ:

$$P(\epsilon) \equiv c_0 + c_1\epsilon + ... + c_{\ell-1}\epsilon^{\ell-1} + \epsilon^\ell; \qquad c_0, c_1, ..., c_{\ell-1} \in \mathbb{Z}_p \tag{2}$$

Different irreducible polynomials of the same degree ℓ lead to isomorphic finite fields. The $m_0, m_1, ..., m_{\ell-1}$ are the Galois components of m in the basis $1, \epsilon, ..., \epsilon^{\ell-1}$.

Notation I.2 (Frobenius map and Galois group)**.** *The Frobenius map is*

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

The m, m^p,...,$m^{p^{\ell-1}}$ are Galois conjugates. The Galois group is

$$\mathrm{Gal}[GF(p^\ell)/\mathbb{Z}_p] = \{\mathbf{1}, \sigma, ..., \sigma^{\ell-1}\} \tag{4}$$

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

Notation I.3 (Subfields)**.** *If d is a divisor of ℓ (which we denote as $d|\ell$) the $GF(p^d)$ is a subfield of $GF(p^\ell)$. The Galois group for the extension from $GF(p^d)$ to $GF(p^\ell)$ is*

$$\mathrm{Gal}[GF(p^\ell)/GF(p^d)] = \{\mathbf{1}, \sigma^d, ..., \sigma^{\ell-d}\}. \tag{5}$$

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

Notation I.4 (Trace)**.** *The trace of $m \in GF(p^\ell)$ is defined as:*

$$\mathrm{Tr}(m) = m + m^p + ... + m^{p^{\ell-1}}; \qquad \mathrm{Tr}(m) \in \mathbb{Z}_p; \qquad m \in GF(p^\ell) \tag{6}$$

When m belongs to the subfield $GF(p^d)$ we make the distinction between the trace with regard to the extension from $\mathbb{Z}_p$ to $GF(p^\ell)$ given in Eq.(6) and the trace with regard to the extension from $\mathbb{Z}_p$ to $GF(p^d)$ given by

$$\mathrm{Tr}_d(m) = m + m^p + ... + m^{p^{d-1}}; \qquad \mathrm{Tr}_d(m) \in \mathbb{Z}_p; \qquad m \in GF(p^d) \tag{7}$$

It is easily seen that

$$\mathrm{Tr}(m) = \frac{\ell}{d}\,\mathrm{Tr}_d(m); \qquad m \in GF(p^d) \tag{8}$$

In the special case that ℓ/d is a multiple of the prime p, all m in $GF(p^d)$ have $\mathrm{Tr}(m) = 0$. We note that this does not contradict a theorem which states that in every finite field there exists at least one element with non-zero trace. According to this theorem it is impossible to have $\mathrm{Tr}_d(m) = 0$ for all m in $GF(p^d)$. But it is possible to have $\mathrm{Tr}(m) = 0$ for all m in $GF(p^d)$ because this is a different trace.

The results in the following three lemmas have been proved in [32] and will not be proved here:

Lemma I.5. *Let g be the $\ell \times \ell$ matrix*

$$g_{\lambda\kappa} \equiv \mathrm{Tr}\left(\epsilon^{\lambda+\kappa}\right); \qquad g_{\lambda\kappa} \in \mathbb{Z}_p; \qquad \lambda, \kappa = 0, ..., \ell - 1 \tag{9}$$

Its inverse matrix

$$G \equiv g^{-1}; \qquad G_{\lambda\kappa} \in \mathbb{Z}_p \tag{10}$$

exists

Lemma I.6. *Let $E_0, E_1, ..., E_{\ell-1}$ be the dual basis to the $1, \epsilon, ..., \epsilon^{\ell-1}$ basis, defined as*

$$E_\kappa = \sum_\lambda G_{\kappa\lambda}\epsilon^\lambda; \qquad \mathrm{Tr}(\epsilon^\kappa E_\lambda) = \delta_{\kappa\lambda} \tag{11}$$

Then

(1) a number $m \in GF(p^\ell)$ can be expressed in the two bases as:

$$\begin{aligned} m &= \sum_{\lambda=0}^{\ell-1} m_\lambda \epsilon^\lambda = \sum_{\lambda=0}^{\ell-1} \overline{m}_\lambda E_\lambda \\ m_\lambda &= \mathrm{Tr}[mE_\lambda]; \qquad \overline{m}_\lambda = \mathrm{Tr}[m\epsilon^\lambda] \\ m_\lambda &= \sum_\kappa G_{\lambda\kappa}\overline{m}_\kappa; \qquad \overline{m}_\lambda = \sum_\kappa g_{\lambda\kappa} m_\kappa \end{aligned} \tag{12}$$

where $\bar{m}_\lambda$ are the dual Galois components of m.

(2) The trace of a product mn is given in terms of the components of m, n as

$$\begin{aligned} \mathrm{Tr}(mn) &= \sum_{\lambda,\kappa} g_{\lambda\kappa} m_\lambda n_\kappa = \sum_{\lambda,\kappa} G_{\lambda\kappa}\overline{m}_\lambda \overline{n}_\kappa \\ &= \sum_\lambda m_\lambda \overline{n}_\lambda = \sum_\lambda \overline{m}_\lambda n_\lambda \end{aligned} \tag{13}$$

Lemma I.7. *Let*

$$\omega(m) \equiv \omega^m = \exp\left(i\frac{2\pi m}{p}\right); \qquad m \in \mathbb{Z}_p \tag{14}$$

Then the

$$\chi(\alpha) = \omega[\mathrm{Tr}(\alpha)]; \qquad \alpha \in GF(p^\ell) \tag{15}$$

are additive characters in $GF(p^\ell)$

$$\chi(\alpha)\chi(\beta) = \chi(\alpha+\beta) \tag{16}$$

and obey the relation

$$\frac{1}{p^\ell}\sum_{\alpha\in GF(p^\ell)} \chi(\alpha\beta) = \delta(\beta,0); \qquad \beta \in GF(p^\ell) \tag{17}$$

where δ *is the Kronecker delta.*

Remark I.8. Eq.(17) can be written in a more general form as

$$\frac{1}{p^\ell}\sum_{\alpha\in GF(p^\ell)} \chi\left(\alpha\beta - \alpha^{p^\lambda}\gamma\right) = \delta\left(\beta, \gamma^{p^{\ell-\lambda}}\right) = \delta\left(\beta^{p^\lambda}, \gamma\right) \tag{18}$$

Remark I.9. Additive characters in a subfield $GF(p^d)$ of $GF(p^\ell)$ are given in terms of the trace of Eq.(7) (with regard to the extension from $\mathbb{Z}_p$ to $GF(p^d)$) as

$$\chi_d(\alpha) = \omega[\mathrm{Tr}_d(\alpha)]; \qquad \alpha \in GF(p^d) \tag{19}$$

Using Eq.(8) we show that

$$\chi_d(\alpha) = [\chi(\alpha)]^{d/\ell}; \qquad \alpha \in GF(p^d) \tag{20}$$

Remark I.10. We consider the ring $[\mathbb{Z}_p]^\ell \equiv \mathbb{Z}_p \times ... \times \mathbb{Z}_p$ with elements

$$(\alpha_\lambda) \equiv (\alpha_0, ..., \alpha_{\ell-1}) \tag{21}$$

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

$$(\alpha_\lambda) + (\beta_\lambda) = (\alpha_\lambda + \beta_\lambda); \qquad (\alpha_\lambda)(\beta_\lambda) = (\alpha_\lambda\beta_\lambda); \qquad \alpha_\lambda, \beta_\lambda \in \mathbb{Z}_p; \qquad \lambda = 0, ..., \ell-1 \tag{22}$$

It is easily seen that the

$$\psi[(\alpha_\lambda)] = \omega\left(\sum_\lambda \alpha_\lambda\right) \tag{23}$$

are additive characters and that

$$\frac{1}{p^\ell}\sum_{(\alpha_\lambda)}\psi[(\alpha_\lambda)(\beta_\lambda)]=\delta[(\beta_\lambda),(0)] \tag{24}$$

It is important to clarify the distinction between harmonic analysis on the field $GF(p^\ell)$ and harmonic analysis on the ring $[\mathbb{Z}_p]^\ell$ and at this stage we compare and contrast the

$$\psi[(\alpha_\lambda\beta_\lambda)]=\omega\left(\sum_\lambda\alpha_\lambda\beta_\lambda\right) \tag{25}$$

with the

$$\chi(\alpha\beta)=\omega\left(\sum_\lambda\overline{\alpha}_\lambda\beta_\lambda\right)=\omega\left(\sum_\lambda\alpha_\lambda\overline{\beta}_\lambda\right) \tag{26}$$

II. COMPLEX FUNCTIONS ON A GALOIS FIELD AND ITS SUBFIELDS

Definition II.1. Let H_ℓ be the p^ℓ-dimensional Hilbert space of complex vectors $\xi(m)$ where $m\in GF(p^\ell)$. The scalar product (ξ,h) is defined as

$$(\xi,h)=\sum_{m\in GF(p^\ell)}[\xi(m)]^*h(m) \tag{27}$$

We consider a subfield $GF(p^d)$ of $GF(p^\ell)$ (d is a divisor of ℓ). The vectors $\xi(m)$ where $m\in GF(p^d)$, span a p^d-dimensional Hilbert space H_d which is a subspace of H_ℓ. We say that H_ℓ is an extension of H_d (a term taken from field extension in algebra).

Example II.2. *H_ℓ is an extension of H_1 which is spanned by complex vectors $\xi(m)$ where $m\in\mathbb{Z}_p$.*

Remark II.3. The subspaces H_d depend on the basis that we choose. With a unitary transformation U we can go to a different basis and then we get different subspaces which we denote as UH_d.

Lemma II.4. *An orthonormal basis in the Hilbert space H_ℓ is the functions*

$$\phi_n(m)=(p^\ell)^{-1/2}\chi(nm) \tag{28}$$

Proof. Using Eqs(16),(17) we show that for $k,n,m,r\in GF(p^\ell)$:

$$\begin{aligned}(\phi_n,\phi_r)&=\delta(n,r)\\ \sum_n[\phi_n(m)]^*\phi_n(k)&=\delta(m,k)\end{aligned} \tag{29}$$

□

Remark II.5. The properties of the trace lead to the relation

$$\phi_n(m)=\phi_{n^p}(m^p)=...=\phi_{n^{p^{\ell-1}}}(m^{p^{\ell-1}}) \tag{30}$$

Lemma II.6. *The Hilbert space H_ℓ is isomorphic to the tensor product $H_1^\ell \equiv H_1 \otimes ... \otimes H_1$ of ℓ H_1 'component Hilbert spaces'. More generally, the Hilbert space H_ℓ is isomorphic to the tensor product $H_d^{\ell/d}$.*

Proof. Using Eq.(13) we show that

$$\begin{aligned} \phi_n(m) &= \varphi_{n_0}(\overline{m}_0)...\varphi_{n_{\ell-1}}(\overline{m}_{\ell-1}) \\ &= \varphi_{\overline{n}_0}(m_0)...\varphi_{\overline{n}_{\ell-1}}(m_{\ell-1}) \end{aligned} \tag{31}$$

where

$$\varphi_\alpha(\beta) = p^{-1/2}\omega(-\alpha\beta); \qquad \alpha, \beta \in \mathbb{Z}_p \tag{32}$$

is a basis in H_1. This shows that H_ℓ can be written as the tensor product $H_1 \otimes ... \otimes H_1$. In a similar way we show that H_ℓ can be viewed as the tensor product of ℓ/d H_d spaces. □

Remark II.7. At this stage we see that when H_ℓ is an extension of H_d, the H_ℓ is isomorphic to the tensor product of ℓ/d spaces H_d. We stress that the extension from H_d to H_ℓ is not 'just' a tensor product; there is a lot of extra structure in it which we explain throughout the paper.

This is analogous to the fact that numbers in $GF(p^\ell)$ can be viewed as ℓ-dimensional vectors of integers in $\mathbb{Z}_p$, but there is a lot of extra structure in them.

Definition II.8. The projection operators $\mathcal{Q}_k$ are defined as

$$\begin{aligned} &\mathcal{Q}_k(n,m) = 1; \quad \text{if } \ n = m = k \\ &\mathcal{Q}_k(n,m) = 0; \quad \text{otherwise} \end{aligned} \tag{33}$$

and obey the relations

$$\mathcal{Q}_k\mathcal{Q}_m = \delta(k,m)\mathcal{Q}_k; \qquad \sum_{k \in GF(p^\ell)} \mathcal{Q}_k = \mathbf{1} \tag{34}$$

Lemma II.9. *The projection operator $\Pi_d(n,m)$ from H_ℓ to H_d is*

$$\Pi_d = \sum_{k \in GF(p^d)} \mathcal{Q}_k \tag{35}$$

If c is a divisor of d then

$$c|d \ \rightarrow \ \Pi_c\Pi_d = \Pi_c \tag{36}$$

The projection of the vector $\xi(n)$ in H_ℓ to the subspace H_d is $\sum_m \Pi_d(n,m)\xi(m)$.

Proof. The proof is straightforward □

III. FOURIER TRANSFORM

Definition III.1. The Fourier transform of a vector $\xi(m)$ in H_ℓ, is given by

$$\tilde{\xi}(n) = (\phi_n, \xi) = \sum_m F(n,m)\xi(m); \qquad m, n \in GF(p^\ell) \tag{37}$$

where F is the $p^\ell \times p^\ell$ Fourier matrix:

$$F(n,m) = (p^\ell)^{-1/2}\chi(nm) \tag{38}$$

Remark III.2. The variable m which we might call 'position' (in quantum mechanical applications) or 'time' (in signal analysis applications) takes values in $GF(p^\ell)$. The variable n which we might call 'momentum' or 'frequency' also takes values in $GF(p^\ell)$. The 'phase-space' of position-momenta (or time-frequency) is $GF(p^\ell) \times GF(p^\ell)$.

Lemma III.3.

(1)

$$F^4 = \mathbf{1}; \qquad FF^\dagger = \mathbf{1} \tag{39}$$

(2) the Fourier transform can be written as a tensor product of Fourier transforms acting on the component Hilbert spaces H_1, as

$$\begin{aligned} F(n,m) &= \mathcal{F}(\overline{n}_0, m_0)...\mathcal{F}(\overline{n}_{\ell-1}, m_{\ell-1}) \\ &= \mathcal{F}(n_0, \overline{m}_0)...\mathcal{F}(n_{\ell-1}, \overline{m}_{\ell-1}) \end{aligned} \tag{40}$$

where

$$\mathcal{F}(\alpha,\beta) = p^{-1/2}\omega(\alpha\beta); \qquad \alpha, \beta \in \mathbb{Z}_p \tag{41}$$

are Fourier transforms in H_1.

(3)

$$F(n,m) = F(n^p, m^p) = ... = F(n^{p^{\ell-1}}, m^{p^{\ell-1}}) \tag{42}$$

(4) F can be written in terms of its eigenvalues as:

$$\begin{aligned} &F = \pi_0 + i\pi_1 - \pi_2 - i\pi_3 \\ &\pi_r\pi_s = \pi_r\delta(r,s); \qquad \pi_0 + \pi_1 + \pi_2 + \pi_3 = \mathbf{1}; \qquad r, s = 0, 1, 2, 3 \end{aligned} \tag{43}$$

where π_λ are orthogonal projectors to its eigenspaces. They can be expressed in terms of F as:

$$\pi_r = \frac{1}{4}\left[\mathbf{1} + (i^{-r}F) + (i^{-r}F)^2 + (i^{-r}F)^3\right]; \qquad r = 0, 1, 2, 3 \tag{44}$$

Proof. Eq.(39) is proved using Eq.(17). Eq.(40) is proved using Eq.(13). The proof of Eq.(42) is based on the fact that conjugates have the same trace.

The fact that $F^4 = \mathbf{1}$ shows that the eigenvalues of F are $1, i, -1, -i$ and this leads to Eq.(43). The proof of Eq.(44) is then straightforward. □

Remark III.4. Harmonic analysis on the ring $[\mathbb{Z}_p]^\ell$ will use the Fourier transform

$$f[(n_\lambda),(m_\lambda)] = \mathcal{F}(n_0, m_0)...\mathcal{F}(n_{\ell-1}, m_{\ell-1}) \tag{45}$$

which is different from the Fourier transform $F(n, m)$ of Eq.(40). The former is based on the characters of Eq.(25), while the latter is based on the characters of Eq.(26).

Above we have considered the $p^\ell \times p^\ell$ Fourier matrix F in the Hilbert space H_ℓ which is based on the characters of Eq.(15) related to the field extension from $\mathbb{Z}_p$ to $GF(p^\ell)$. In analogy with this we now introduce the $p^d \times p^d$ Fourier matrix $\mathfrak{F}$ in the Hilbert space H_d which is based on the trace $\chi_d(\alpha)$ of Eq.(19) related to the field extension from $\mathbb{Z}_p$ to $GF(p^d)$. In the following lemma we compare the matrix $\mathfrak{F}$ with the matrix $\Pi_d F \Pi_d$. We note that the $\Pi_d F \Pi_d$ is a $p^\ell \times p^\ell$ matrix but only $p^d \times p^d$ of its elements are non-zero.

Lemma III.5. *Let $\mathfrak{F}$ be the $p^d \times p^d$ Fourier matrix in H_d:*

$$\mathfrak{F}(n, m) = (p^d)^{-1/2}\chi_d(nm); \qquad n, m \in GF(p^d) \tag{46}$$

For $n, m \in GF(p^d)$ we show that

$$(\Pi_d F \Pi_d)(n, m) = [\mathfrak{F}(n, m)]^{\ell/d} \tag{47}$$

Proof. The proof is based on Eq.(20). □

Remark III.6. This lemma shows that the elements of F with indices in $GF(p^d)$ are powers of the corresponding elements of $\mathfrak{F}$. Of course, the matrix F has other elements also, with indices in the set $GF(p^\ell) - GF(p^d)$. In the special case that ℓ/d is a multiple of the prime p, Eq.(47) shows that the $p^d \times p^d$ submatrix of $F(n, m)$ with indices in $GF(p^d)$, has all its elements equal to $p^{-\ell/2}$.

IV. FROBENIUS TRANSFORM

The Frobenius map of Eq.(3) leads in the present context to the Frobenius transform.

Definition IV.1. The Frobenius transform of a function $\xi(n)$ in H_ℓ is given by

$$(\mathcal{G}\xi)(n) = \sum_m \mathcal{G}(n, m)\xi(m) = \xi(n^{p^{\ell-1}}). \tag{48}$$

where $\mathcal{G}$ is the $p^\ell \times p^\ell$ Frobenius matrix

$$\mathcal{G}(n, m) = \delta(n, m^p) \tag{49}$$

Remark IV.2. $\mathcal{G}$ depends on the basis that we choose. With a unitary transformation U we can go to a different basis and then the Frobenius transform becomes $U\mathcal{G}U^\dagger$.

Theorem IV.3.

(1) The Frobenius transformation leaves all the vectors in H_1 fixed:

$$\mathcal{G}\Pi_1 = \Pi_1 \tag{50}$$

(2) The Frobenius transform commutes with the projection operators Π_d (where d is a divisor of ℓ):

$$[\mathcal{G}, \Pi_d] = 0 \tag{51}$$

(3)

$$\mathcal{G}^\ell = \mathbf{1}; \qquad \mathcal{G}\mathcal{G}^\dagger = \mathbf{1} \tag{52}$$

and the

$$\mathrm{Gal}(H_\ell/H_1) = \{\mathbf{1}, \mathcal{G}, ..., \mathcal{G}^{\ell-1}\} \tag{53}$$

form a cyclic group of order ℓ which we call Galois group.

(4) $\mathcal{G}$ can be written in terms of its eigenvalues as:

$$\begin{aligned} &\mathcal{G} = \varpi_0 + \Omega\varpi_1 + ... + \Omega^{\ell-1}\varpi_{\ell-1}; \qquad \Omega = \exp\left(i\frac{2\pi}{\ell}\right) \\ &\varpi_\lambda\varpi_\mu = \varpi_\lambda\delta(\lambda,\mu); \qquad \sum_\lambda \varpi_\lambda = \mathbf{1}; \qquad \lambda,\mu \in \mathbb{Z}_\ell \end{aligned} \tag{54}$$

where ϖ_λ are orthogonal projectors to its eigenspaces. They can be expressed in terms of $\mathcal{G}$ as

$$\varpi_\lambda = \frac{1}{\ell}\left[\mathbf{1} + (\Omega^{-\lambda}\mathcal{G}) + (\Omega^{-\lambda}\mathcal{G})^2 + ... + (\Omega^{-\lambda}\mathcal{G})^{\ell-1}\right] \tag{55}$$

(5) The Frobenius transform commutes with the Fourier transform and also with the projection operators π_r:

$$[F, \mathcal{G}] = [\pi_r, \mathcal{G}] = 0; \qquad r = 0, 1, 2, 3 \tag{56}$$

Proof. Eq.(50) is proved using Eq.(48) and the fact that $n^p = n$ for all $n \in \mathbb{Z}_p$.

Eq.(51) is proved using the fact that $GF(p^n)$ is a subfield. Therefore for any $n \in GF(p^d)$ the $n^{p^{\ell-1}}$ is also an element of $GF(p^d)$. Consequently, the Frobenius transformation maps states in H_d to other states which are also in H_d.

Eq.(52) is proved using the fact that $m^{p^\ell} = m$ for all $m \in GF(p^\ell)$. The powers of $\mathcal{G}$ form a group and the fact that $\mathcal{G}^\ell = \mathbf{1}$ proves that this is a cyclic group of order ℓ.

Eq.(54) is a direct consequence of the $\mathcal{G}^\ell = \mathbf{1}$. Using Eq.(54) and the relation

$$\frac{1}{\ell}\sum_\lambda \Omega^{\lambda\mu} = \delta(\mu, 0); \qquad \lambda,\mu \in \mathbb{Z}_\ell \tag{57}$$

we prove Eq.(55).

Eq.(56) is proved using Eq.(18). □

Remark IV.4. Using Eqs. (50),(55) we prove that

$$\Pi_1 \varpi_0 = \varpi_0 \Pi_1 = \Pi_1 \tag{58}$$

Therefore the space H_1 is a subspace of the eigenspace of $\mathcal{G}$ corresponding to the eigenvalue 1.

Remark IV.5. Using Eq.(56) we show that

$$(\mathcal{G}\tilde{\xi})(n) = \tilde{\xi}(n^{p^{\ell-1}}). \tag{59}$$

This together with Eq.(48) show that $\mathcal{G}$ can be interpreted as magnification of the phase space, where the 'coordinates' are replaced by their powers. We stress however that we are in a finite field, magnification is simply reordering and $\mathcal{G}^\ell = \mathbf{1}$. There is no analogue of the Frobenius transformation in harmonic analysis on the field of real numbers or on $\mathbb{Z}_p$. This is a unique feature of harmonic analysis on $GF(p^\ell)$ with $\ell \geq 2$.

Example IV.6. *We consider the field $GF(9)$ ($p = 3$ and $\ell = 2$). The elements of this field are $m_0 + m_1\epsilon$ where $m_0, m_1 \in \mathbb{Z}_3$. They are defined modulo an irreducible polynomial which we choose to be $\epsilon^2 + \epsilon + 2$. Below we present matrices using the following order for their indices which are elements of $GF(9)$:*

$$\{0, 1, 2, \epsilon, 1+\epsilon, 2+\epsilon, 2\epsilon, 1+2\epsilon, 2+2\epsilon\} \tag{60}$$

We calculate the matrix $\mathcal{G}(n, m)$ and its eigenvalues and eigenvectors. There are six eigenvectors corresponding to the eigenvalue 1 and we call ϖ_0 the corresponding projection operator. There are three eigenvectors corresponding to the eigenvalue -1 and we call ϖ_1 the corresponding projection operator. They are:

$$\varpi_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0.5 \\ 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0.5 \end{pmatrix}; \quad \varpi_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0 & -0.5 \\ 0 & 0 & 0 & 0 & 0.5 & 0 & -0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & -0.5 & 0 \\ 0 & 0 & 0 & 0 & -0.5 & 0 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -0.5 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & -0.5 & 0 & 0 & 0 & 0 & 0.5 \end{pmatrix} \tag{61}$$

According to Eq(54)

$$\mathcal{G} = \varpi_0 - \varpi_1; \qquad \varpi_0 + \varpi_1 = \mathbf{1}; \qquad \varpi_0 \varpi_1 = 0 \tag{62}$$

A. Frobenius transform for the extension from H_d to H_ℓ

The Galois group of Eq.(5) consists of automorphisms in $GF(p^\ell)$ which leave all the elements of the subfield $GF(p^d)$ fixed. Motivated from this we consider the powers of $\mathcal{G}^d$ and show that they play the role of Frobenius transformations for the extension from H_d to H_ℓ.

Corollary IV.7.

(1) The Frobenius transformation $\mathcal{G}^d$ leaves all the vectors in H_d fixed:

$$\mathcal{G}^d \Pi_d = \Pi_d. \tag{63}$$

The Galois group

$$\mathrm{Gal}(H_\ell/H_d) = \{\mathbf{1}, \mathcal{G}^d, ..., \mathcal{G}^{\ell-d}\} \tag{64}$$

is a cyclic group of order ℓ/d and is a subgroup of $\mathrm{Gal}(H_\ell/H_1)$.

(2) $\mathcal{G}^d$ can be written in terms of its eigenvalues as:

$$\mathcal{G}^d \;=\; \mathfrak{P}_0 + \Omega^d \mathfrak{P}_1 + ... + \Omega^{\ell-d}\mathfrak{P}_{\ell/d} \tag{65}$$

where $\mathfrak{P}_\lambda$ are orthogonal projectors to its eigenspaces. They are given by:

$$\begin{aligned} \mathfrak{P}_\lambda \;&=\; \frac{1}{d}\left[\mathbf{1} + (\Omega^{-d\lambda}\mathcal{G}^d) + (\Omega^{-d\lambda}\mathcal{G}^d)^2 + ... + (\Omega^{-d\lambda}\mathcal{G}^d)^{\ell-1}\right] \\ &=\; \varpi_\lambda + \varpi_{\lambda+\ell/d} + ... + \varpi_{\lambda+(d-1)\ell/d}; \qquad \lambda = 0, 1, ..., \frac{\ell}{d} - 1 \end{aligned} \tag{66}$$

Proof. We first show that

$$(\mathcal{G}^d \xi)(n) = \xi(n^{p^{d(\ell-1)}}). \tag{67}$$

and then use the fact that $n^{p^d} = n$ for all $n \in GF(p^d)$, to prove Eq.(63).

Eq.(52) can be used to prove that the group of Eq.(64) is cyclic of order ℓ/d.

The proof of Eq.(66) is based on Eq.(54). □

Remark IV.8. Using Eqs. (63),(66) we prove that

$$\Pi_d \mathfrak{P}_0 = \mathfrak{P}_0 \Pi_d = \Pi_d \tag{68}$$

It is seen that the space H_d is a subspace of the combined eigenspace of $\mathcal{G}$ corresponding to the eigenvalues $1, \Omega^{\ell/d}, ..., \Omega^{(d-1)\ell/d}$.

V. DISPLACEMENTS IN THE $GF(p^\ell) \times GF(p^\ell)$ PHASE SPACE AND THE HEISENBERG-WEYL GROUP

Definition V.1. The Heisenberg-Weyl group has elements $g(\alpha, \beta, \gamma)$ that depend on three numbers α, β, γ (which in our case are elements of a Galois field) and the multiplication rule:

$$g(\alpha_1, \beta_1, \gamma_1) g(\alpha_2, \beta_2, \gamma_2) = g(\alpha_1 + \alpha_2, \beta_1 + \beta_2, \gamma); \qquad \gamma = \gamma_1 + \gamma_2 + 2^{-1}(\alpha_1\beta_2 - \alpha_2\beta_1) \tag{69}$$

Definition V.2. The displacement operators $Z(\alpha)$ and $X(\beta)$ are $p^\ell \times p^\ell$ unitary matrices with elements

$$\begin{aligned} &[Z(\alpha)](n, m) = \chi(\alpha m)\, \delta(n, m) \\ &[X(\beta)](n, m) = [F^\dagger Z(\beta) F](n, m) = \delta(n, m + \beta); \qquad \alpha, \beta, m, n \in GF(p^\ell) \end{aligned} \tag{70}$$

More general displacement operators are the unitary matrices:

$$D(\alpha, \beta) = Z(\alpha) X(\beta) \chi(-2^{-1}\alpha\beta) \tag{71}$$

Remark V.3. The term displacement operators is justified from the following relations:

$$[Z(\alpha)\ \xi](n) = \chi(\alpha n)\ \xi(n); \qquad [X(\beta)\ \xi](n) = \xi(n-\beta) \tag{72}$$

where $\xi(m)$ is any vector in H_ℓ.

Lemma V.4. *The $D(\alpha,\beta)\chi(\gamma)$ form a representation of the Heisenberg-Weyl group.*

Proof. We first prove that

$$Z(\alpha)X(\beta) = X(\beta)Z(\alpha)\chi(\alpha\beta); \qquad \alpha,\beta \in GF(p^\ell) \tag{73}$$

and then use this to show that

$$D(\alpha,\beta)D(\gamma,\delta) = D(\alpha+\gamma,\beta+\delta)\ \chi\left[2^{-1}(\alpha\delta-\beta\gamma)\right] \tag{74}$$

This proves that the $D(\alpha,\beta)\chi(\gamma)$ form a representation of the Heisenberg-Weyl group. □

The following proposition summarizes the main properties of the displacement operators:

Proposition V.5.

(1) The $D(\alpha,\beta)$ obey the relation

$$[D(\alpha,\beta)]^p = \mathbf{1} \tag{75}$$

Their eigenvalues are powers of ω and they can be written as

$$\begin{aligned} &D(\alpha,\beta) = q_0 + \omega(1)\ q_1 + ... + \omega(p-1)\ q_{p-1} \\ &q_\lambda q_\mu = \delta(\lambda,\mu)q_\lambda; \qquad \sum_\lambda q_\lambda = \mathbf{1}; \qquad \lambda,\mu \in \mathbb{Z}_p \end{aligned} \tag{76}$$

where q_λ are projection operators to the various eigenspaces.

(2) The Frobenius transform acts on the displacement operators as follows:

$$\mathcal{G}^\lambda D(\alpha,\beta)(\mathcal{G}^\dagger)^\lambda = D(\alpha^{p^\lambda},\beta^{p^\lambda}); \qquad \lambda = 0,...,\ell-1 \tag{77}$$

(3) Let $\mathcal{D}(m,n)$ where $m,n \in \mathbb{Z}_p$ be the displacement operators acting on the various component spaces H_1. Then:

$$D(\alpha,\beta)\ =\ \mathcal{D}(\overline{\alpha}_0,\beta_0) \otimes ... \otimes \mathcal{D}(\overline{\alpha}_{\ell-1},\beta_{\ell-1}) \tag{78}$$

The dual components of α and the components of β, enter in this relation.

(4) An arbitrary operator Θ acting on H_ℓ can be expanded in terms of the displacement operators as

$$\Theta = \frac{1}{p^\ell}\sum_{\alpha,\beta} D(\alpha,\beta)\mathcal{W}(-\alpha,-\beta); \qquad \mathcal{W}(\alpha,\beta) = \mathrm{tr}[\Theta D(\alpha,\beta)] \tag{79}$$

where tr denotes the usual trace of a matrix. $\mathcal{W}(\alpha,\beta)$ is called the Weyl (or ambiguity) function.

(5) For an arbitrary operator Θ

$$\frac{1}{p^\ell}\sum_{\alpha,\beta} D(\alpha,\beta)\,\frac{\Theta}{\mathrm{tr}\Theta}\,[D(\alpha,\beta)]^\dagger = \mathbf{1} \tag{80}$$

This is a 'generalized resolution of the identity'.

Proof. Using Eq.(74) we show that

$$[D(\alpha,\beta)]^p = D(p\alpha,p\beta) = D(0,0) = \mathbf{1} \tag{81}$$

A direct consequence of this is that $D(\alpha,\beta)$ can be expressed as in Eq.(76).

Eqs(77),(78),(79) have been proved in [32].

In order to prove Eq.(80) we first combine Eqs(70) to show that the elements of the matrix $D(\alpha,\beta)$ are

$$[D(\alpha,\beta)](n,m) = \chi(2^{-1}\alpha\beta+\alpha m)\delta(n,m+\beta) \tag{82}$$

We then use this in the left hand side of Eq.(80) and perform the summations taking into account Eq.(17). □

Remark V.6. Eq.(78) shows another difference between harmonic analysis on $GF(p^\ell)$ and harmonic analysis on the ring $\mathbb{Z}_p^\ell$. Displacements in the latter will be

$$d[(\alpha_\lambda),(\beta_\lambda)] = \mathcal{D}(\alpha_0,\beta_0)\otimes ...\otimes \mathcal{D}(\alpha_{\ell-1},\beta_{\ell-1}). \tag{83}$$

Remark V.7. We consider Eq.(79) in the case where Θ is an infinitesimal $SU(p^\ell)$ transformation. Then

$$\Theta = \mathbf{1} + \sum_{\alpha,\beta} D(\alpha,\beta)\mathfrak{e}(\alpha,\beta) \tag{84}$$

where $\mathfrak{e}(\alpha,\beta)$ are infinitesimal coefficients. This shows that the $D(\alpha,\beta)$ (with $(\alpha,\beta)\neq(0,0)$) are generators of an irreducible representation of $SU(p^\ell)$[6].

Remark V.8. As special case of Eq.(80) we use

$$\Theta(m,n) = \psi(m)[\psi(n)]^*; \qquad \mathrm{tr}\Theta = 1 \tag{85}$$

where $\psi(m)$ is an arbitrary normalized vector in H_ℓ. In this case we show that the $p^{2\ell}$ vectors $D(\alpha,\beta)\psi$ (for all $\alpha,\beta\in GF(p^\ell)$) form an 'overcomplete basis' of vectors in the p^ℓ dimensional space H. Indeed Eq.(80) shows that we can expand an arbitrary vector $\xi(m)$ in terms of them, as:

$$\xi(m) = \frac{1}{p^\ell}\sum_{\alpha,\beta} u(\alpha,\beta)[D(\alpha,\beta)\psi](m); \qquad u(\alpha,\beta) = (D(\alpha,\beta)\psi,\xi) \tag{86}$$

A. Displacements and the Heisenberg-Weyl group in H_d

In analogy with Eq.(70) introduce the displacement matrices in the space H_d.

Definition V.9. The displacement matrices in H_d are defined as

$$\begin{aligned}&[\mathfrak{Z}(\alpha)](n,m) = \chi_d(\alpha m)\ \delta(n,m)\\ &[\mathfrak{X}(\beta)](n,m) = [\mathfrak{F}^\dagger\mathfrak{Z}(\beta)\mathfrak{F}](n,m) = \delta(n,m+\beta); \qquad \alpha,\beta,n,m \in GF(p^d)\end{aligned} \tag{87}$$

More general displacement matrices are defined as

$$\mathfrak{D}(\alpha,\beta) = \mathfrak{Z}(\alpha)\mathfrak{X}(\beta)\chi_d(-2^{-1}\alpha\beta) \tag{88}$$

The $\mathfrak{D}(\alpha,\beta)$ are $p^d \times p^d$ matrices. We compare the matrices $\mathfrak{D}(\alpha,\beta)$ with their counterparts $\Pi_d D(\alpha,\beta)\Pi_d$. We note that the $\Pi_d D(\alpha,\beta)\Pi_d$ are $p^\ell \times p^\ell$ matrices but only $p^d \times p^d$ of their elements are non-zero.

Proposition V.10.

$$[\Pi_d D(\alpha,\beta)\Pi_d](n,m) = \{[\mathfrak{D}(\alpha,\beta)](n,m)\}^{\ell/d}; \qquad \alpha,\beta,n,m \in GF(p^d) \tag{89}$$

Proof. The proof is based on Eq.(20). □

Remark V.11. This shows that the elements of $D(\alpha,\beta)$ (with $\alpha,\beta \in GF(p^d)$) which have indices (n,m) in $GF(p^d)$ are powers of the corresponding elements of $\mathfrak{D}(\alpha,\beta)$. Of course, the matrices $D(\alpha,\beta)$ (with $\alpha,\beta \in GF(p^d)$) have other elements also, with indices (n,m) in the set $GF(p^\ell) - GF(p^d)$. Furthermore, there are more matrices $D(\alpha,\beta)$ with α,β in the set $GF(p^\ell) - GF(p^d)$, which do not enter in Eq.(89).

VI. SYMPLECTIC TRANSFORMATIONS AND THE $Sp(2, GF(p^\ell))$ GROUP

Definition VI.1. The symplectic group $Sp(2, GF(p^\ell))$ consists of the 2×2 matrices

$$g(q,r,s) = \begin{pmatrix} q & s \\ r & t \end{pmatrix}; \qquad qt - rs = 1; \qquad q,r,s,t \in GF(p^\ell) \tag{90}$$

The group operation is the matrix multiplication:

$$\begin{aligned}&g(q_2,r_2,s_2)g(q_1,r_1,s_1) = g(q,r,s)\\ &q = q_1q_2 + r_1s_2\\ &r = q_1r_2 + r_1q_2^{-1}(1 + r_2s_2)\\ &s = q_2s_1 + s_2q_1^{-1}(1 + r_1s_1)\end{aligned} \tag{91}$$

Remark VI.2. We ommit in the notation the fourth parameter $t = q^{-1}(1 + rs)$. However, in the case that $q = 0$, we need to indicate the value of t and we will use the notation $g(0,r,-r^{-1}|t)$. We will also use the notation

$$g_F = g(0,1,-1|0) \tag{92}$$

Definition VI.3. The Gauss sum related to $GF(p^\ell)$[3, 16] is

$$G(A) = \sum_{k \in GF(p^\ell)} \chi(Ak^2) \tag{93}$$

Lemma VI.4.

(1) The 2×2 matrices $g(1,0,\xi)$ where $\xi \in GF(p^\ell)$ form a subgroup $\mathfrak{G}_1$ of $Sp(2, GF(p^\ell))$ and

$$[g(1,0,\xi)]^p = \mathbf{1} \tag{94}$$

(2) The $p^\ell \times p^\ell$ unitary matrices $S(1,0,\xi)$ with elements

$$\begin{aligned} [S(1,0,\xi)](n,m) &= p^{-\ell}\chi\left[(2\xi)^{-1}(n-m)^2\right] G(-2^{-1}\xi); \qquad \xi \neq 0 \\ S(1,0,0) &= \mathbf{1} \end{aligned} \tag{95}$$

where $n, m \in GF(p^\ell)$, form a representation of $\mathfrak{G}_1$. Furthermore

$$[S(1,0,\xi)]^p = \mathbf{1} \tag{96}$$

Proof. We first prove that

$$g(1,0,\xi_1)\, g(1,0,\xi_2) \;=\; g(1,0,\xi_1+\xi_2) \tag{97}$$

and then we easily prove that the matrices $g(1,0,\xi)$ form a group. The proof of Eqs(94) is based on the properties of the Galois elements.

Straightforward matrix multiplication shows that

$$S(1,0,\xi_1)\, S(1,0,\xi_2) \;=\; S(1,0,\xi_1+\xi_2) \tag{98}$$

and therefore the $S(1,0,\xi_1)$ form a representation of $\mathfrak{G}_1$. Eq.(96) is then a consequence of Eq.(94). □

Lemma VI.5.

(1) The 2×2 matrices $g(1,\xi,0)$ where $\xi \in GF(p^\ell)$ form a subgroup $\mathfrak{G}_2$ of $Sp(2, GF(p^\ell))$ and

$$[g(1,\xi,0)]^p = \mathbf{1} \tag{99}$$

(2) The $p^\ell \times p^\ell$ unitary matrices $S(1,\xi,0)$ with elements

$$[S(1,\xi,0)](n,m) = \chi(2^{-1}\xi m^2)\delta(n,m) \tag{100}$$

where $n, m \in GF(p^\ell)$, form a representation of $\mathfrak{G}_2$. Furthermore

$$[S(1,\xi,0)]^p = \mathbf{1} \tag{101}$$

Proof. The proof is analogous to the proof of lemma VI.4 □

Lemma VI.6.

(1) The 2×2 matrices $g(\xi, 0, 0)$ where $\xi \in GF(p^\ell) - \{0\}$ form a subgroup $\mathfrak{G}_3$ of $Sp(2, GF(p^\ell))$ and

$$[g(\xi, 0, 0)]^{p^\ell} = g(\xi, 0, 0) \tag{102}$$

(2) The $p^\ell \times p^\ell$ unitary matrices $S(\xi, 0, 0)$ with elements

$$[S(\xi, 0, 0)](n, m) = \delta(\xi^{-1} n, m) \tag{103}$$

where $n, m \in GF(p^\ell)$, form a representation of $\mathfrak{G}_3$. Furthermore

$$[S(\xi, 0, 0)]^{p^\ell} = S(\xi, 0, 0) \tag{104}$$

Proof. We first prove that

$$g(\xi_1, 0, 0)\ g(\xi_2, 0, 0) \ = \ g(\xi_1 \xi_2, 0, 0) \tag{105}$$

and then we easily prove that the matrices $g(\xi, 0, 0)$ form a group. The proof of Eqs(102) is based on the properties of the Galois elements.

Straightforward matrix multiplication shows that

$$S(\xi_1, 0, 0)\ S(\xi_2, 0, 0) \ = \ S(\xi_1 \xi_2, 0, 0) \tag{106}$$

and therefore the $S(\xi_1, 0, 0)$ form a representation of $\mathfrak{G}_3$. Eq.(104) is then a consequence of Eq.(102). □

Lemma VI.7.

(1) The powers of the 2×2 matrix g_F form a subgroup $\mathfrak{G}_F$ of $Sp(2, GF(p^\ell))$ which is a cyclic group of order 4.

(2) The Fourier operator F of Eq.(38) and its powers, form a representation of $\mathfrak{G}_F$.

Proof. We easily show that $g_F^4 = \mathbf{1}$ and therefore the $\{\mathbf{1}, g_F, g_F^2, g_F^3\}$ form a cyclic group of order 4. We have seen in Eq.(39) that $F^4 = \mathbf{1}$ and therefore the $\{\mathbf{1}, F, F^2, F^3\}$ form a a representation of $\mathfrak{G}_F$. □

Proposition VI.8.

(1) If $1 + rs \neq 0$ and $q \neq 0$ we can decompose the matrix $g(q, r, s)$ as

$$g(q, r, s) = g(1, 0, \xi_1) g(1, \xi_2, 0) g(\xi_3, 0, 0) \tag{107}$$

where

$$\xi_1 = qs(1 + rs)^{-1}; \qquad \xi_2 = rq^{-1}(1 + rs); \qquad \xi_3 = q(1 + rs)^{-1} \tag{108}$$

(2) If $1 + rs = 0$ and $q \neq 0$ we can decompose the matrix $g(q, r, -r^{-1})$ as

$$g(q, r, -r^{-1}) = g_F\ g(1, -qr^{-1}, 0)\ g(r, 0, 0) \tag{109}$$

(3) If $q = 0$ (and therefore $1 + rs = 0$) we can decompose the matrix $g(0, r, -r^{-1}|t)$ as

$$g(0, r, -r^{-1}|t) = g_F\ g(1, 0, rt)\ g(r, 0, 0) \tag{110}$$

Proof. The proof is based on straightforward multiplication of 2×2 matrices. □

Proposition VI.9.

(1) If $1 + rs \neq 0$ and $q \neq 0$, we define the $p^\ell \times p^\ell$ unitary matrix $S(q, r, s)$ as:

$$S(q, r, s) = S(1, 0, \xi_1)S(1, \xi_2, 0)S(\xi_3, 0, 0) \tag{111}$$

Then its elements are given by:

$$\begin{aligned} [S(q, r, s)]\ (n, m) &= p^{-\ell}\ G(A)\ \chi\left[(2qs)^{-1}(n^2 + srn^2 - 2qnm + q^2m^2)\right] \\ A &= -2^{-1}(1 + rs)^{-1}qs \end{aligned} \tag{112}$$

when $s \neq 0$; and by

$$[S(q, r, 0)]\ (n, m) = \chi\left[2^{-1}rqm^2\right]\ \delta(n, qm) \tag{113}$$

when $s = 0$.

(2) If $1 + rs = 0$ and $q \neq 0$, we define the $p^\ell \times p^\ell$ unitary matrix $S(q, r, -r^{-1})$ as:

$$S(q, r, -r^{-1}) = F\ S(1, -qr^{-1}, 0)\ S(r, 0, 0) \tag{114}$$

where F is the Fourier matrix. Then its elements are given by:

$$[S(q, r, s)]\ (n, m) = p^{-\ell/2}\ \chi(rnm - 2^{-1}qrm^2) \tag{115}$$

(3) When $q = 0$ (and therefore $1 + rs = 0$) we define the $p^\ell \times p^\ell$ unitary matrix $S(0, r, -r^{-1}|t)$ as:

$$S(0, r, -r^{-1}|t) = F\ S(1, 0, rt)\ S(r, 0, 0) \tag{116}$$

Then its elements are given by:

$$[S(0, r, -r^{-1}|t)]\ (n, m) = p^{-3\ell/2}\ \chi[-(2t)^{-1}r(tn - m)^2]\ G(-2^{-1}rt)\ G[(2rt)^{-1}] \tag{117}$$

when $t \neq 0$. When $t = 0$, then $S(0, r, -r^{-1}|0) = F$.

Proof. the proof is based on straightforward multiplication of $p^\ell \times p^\ell$ matrices. □

Theorem VI.10. *The $S(q, r, s)$ form a representation of the $Sp(2, GF(p^\ell))$ group.*

Proof. We need to prove that as in Eq.(91)

$$S(q_2, r_2, s_2)\ S(q_1, r_1, s_1) = S(q, r, s) \tag{118}$$

where q, r, s are given in Eq.(91).

We first show how each of the operators $S(1, 0, \xi)$, $S(1, \xi, 0)$, $S(\xi, 0, 0)$, F acts on the displacement operators:

$$\begin{aligned} S(1, 0, \xi)\ D(\alpha, \beta)\ [S(1, 0, \xi)]^\dagger &= D(\alpha, \xi\alpha + \beta) \\ S(1, \xi, 0)\ D(\alpha, \beta)\ [S(1, \xi, 0)]^\dagger &= D(\alpha + \xi\beta, \beta) \\ S(\xi, 0, 0)\ D(\alpha, \beta)\ [S(\xi, 0, 0)]^\dagger &= D(\xi^{-1}\alpha, \xi\beta) \\ F\ D(\alpha, \beta)\ F^\dagger &= D(\beta, -\alpha) \end{aligned} \tag{119}$$

We then combine these results to show that the general $S(q,r,s)$ act on the displacement operators as follows:

$$S(q,r,s)\ D(\alpha,\beta)\ [S(q,r,s)]^\dagger = D(t\alpha + r\beta, s\alpha + q\beta) \tag{120}$$

where $t = q^{-1}(1+rs)$ (the case $q=0$ needs to be considered separately).

Using this relation we show that

$$V\ D(\alpha,\beta)\ V^\dagger = S(q,r,s)\ D(\alpha,\beta)\ [S(q,r,s)]^\dagger; \qquad V = S(q_2,r_2,s_2)\ S(q_1,r_1,s_1) \tag{121}$$

where q,r,s are given in Eq.(91). This proves that the operator $U = V[S(q,r,s)]^\dagger$ commutes with all $D(\alpha,\beta)$. We have explained earlier that $D(\alpha,\beta)$ are generators of an **irreducible** representation of the $SU(p^\ell)$. The fact that U commutes with all of them shows that $U = \lambda\mathbf{1}$ where λ is a constant. In fact λ is a phase factor, because U is a unitary matrix. If we consider some special cases in both sides of Eq.(118) we can show that $\lambda = 1$. This proves Eq.(118).

An alternative proof of Eq.(118), can be based on matrix multiplication using Eq.(112) (the special cases of Eqs.(113), (115), (117) need also to be considered). But this is clearly more lengthy than the one presented here.

□

We have seen in Eq.(40) that there is a simple relation between Fourier transforms in H_ℓ and Fourier transforms in the component spaces H_1. The same is true about displacements in Eq.(78). The example below shows that there is **no** simple relation between symplectic transforms in H_ℓ and symplectic transforms in the component spaces H_1.

Example VI.11. *We consider the $GF(9)$ and choose the irreducible polynomial $\epsilon^2+\epsilon+2$ (this is the same as in example IV.6). In this case we show that*

$$S(1,1+\epsilon,\epsilon)X^\epsilon[S(1,1+\epsilon,\epsilon)]^\dagger = D(2\epsilon,1+2\epsilon) \tag{122}$$

We can show that $X^\epsilon = \mathbf{1}\otimes\mathcal{X}$ and also that

$$D(2\epsilon,1+2\epsilon) = \mathcal{D}(1,1)\otimes\mathcal{D}(0,2) \tag{123}$$

Therefore we can rewrite Eq.(124) as

$$S(1,1+\epsilon,\epsilon)\ (\mathbf{1}\otimes\mathcal{X})\ [S(1,1+\epsilon,\epsilon)]^\dagger = \mathcal{D}(1,1)\otimes\mathcal{D}(0,2) \tag{124}$$

It is seen that the $S(1,1+\epsilon,\epsilon)$ can not be the tensor product of two symplectic transformations $\mathcal{S}_1\otimes\mathcal{S}_2$ acting on $H_1\otimes H_1$ (the $\mathcal{S}_1\mathbf{1}\mathcal{S}_1^\dagger$ cannot give the $\mathcal{D}(1,1)$).

Proposition VI.12. *The Frobenius transformations act on the symplectic transformations as follows:*

$$\mathcal{G}^\lambda S(r,s,t)(\mathcal{G}^\dagger)^\lambda = S(r^{p^\lambda}, s^{p^\lambda}, t^{p^\lambda}); \qquad \lambda = 0,...,\ell-1 \tag{125}$$

If α,β belong to the subfield $GF(p^d)$ then

$$\alpha,\beta\in GF(p^d)\ \rightarrow\ \mathcal{G}^d S(r,s,t)(\mathcal{G}^\dagger)^d = S(r,s,t) \tag{126}$$

Proof. The proof is based on multiplication of the matrices given in Eqs(49),(112) (the special cases of Eqs.(113), (115), (117) need also to be considered). □

VII. DISCUSSION

Harmonic analysis on $GF(p^\ell)$ inherits various features from field extension. The Hilbert space H_ℓ is isomorphic to the tensor product H_1^ℓ but it also has a lot of extra structure which is intimately related to Galois theory. Both, the Fourier transform of Eq.(40) and the displacements of Eq.(78), involve (in the dual components) the matrix g of Eq.(9). In contrast, harmonic analysis on $\mathbb{Z}_p^\ell$ uses the same Hilbert space but the Fourier transform of Eq.(45) and the displacements of Eq.(83).

An important aspect of the theory of Galois fields is the relationship of the 'large' field with its subfields. In the present context, we have studied the relationship between harmonic analysis on $GF(p^\ell)$ and harmonic analysis on the subfield $GF(p^d)$. The relationship between Fourier transforms in H_ℓ and Fourier transforms in H_d is presented in lemma III.5. The relationship between displacements in H_ℓ and displacements in H_d is discussed in proposition V.10.

The Frobenius map plays a central role in Galois theory and in the present context it leads to the Frobenius transformations of Eqs. (49) and to the Galois groups of Eqs. (53), (64).

Symplectic transformations are related to the isotropy of the $GF(p^\ell) \times GF(p^\ell)$ phase space and they have been discussed in section VI. It has been shown that the matrices of Eqs(112), (113), (115), (117), form a representation of the $Sp(2, GF(p^\ell))$ group.

The work uses algebraic concepts from field extension in the context of harmonic analysis.

---

[1] A. Barut, R. Raczka, 'Theory of group representations and applications' (Polish Scintific Publishers, Warsaw, 1977)

[2] S. Bandyopadhyay, P.O. Boykin, V.Roychowdhury, F. Vatan, 'A new proof of the existence of mutually unbiased bases', Algorithmica 34, 512-528 (2002)

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

[4] S. Colin, J. Corbett, T. Durt, D. Gross, 'About SICPOVMs and discrete Wigner distributions', J. Opt. B-Quantum Semiclass. Optics 7, S778-S785 (2005)

[5] T. Durt, 'About mutually unbiased bases in even and odd prime power dimensions', J. Phys. A38, 5267-5283 (2005)

[6] D.B. Fairlie, P. Fletcher, C.K. Zachos, 'Infinite-dimensional algebrasand a trigonometric basis for the classical Lie-algebras', J. Math. Phys. 31, 1088-1094 (1990)

[7] H.G. Feichtinger, M. Hazewinkel, N. Kaiblinger, E. Matusiak, M. Neuhauser, 'Metaplectic operators on C^n, preprint

[8] K. Flornes, A. Grossmann, M. Holschneider, B. Torresani, ' Wavelets on discrete fields', Appl. Comput. Harmon. Anal., 1, 137-146 (1994)

[9] K. Gibbons, M.J. Hoffman, W. Wootters, 'Discrete phase space based on finite fields', Phys. Rev. A70, 062101, 1-23(2004)

[10] J.W.P. Hirschfeld, 'Projective geometries over finite fields' (Oxford University Press, Oxford, 1979)

[11] M.R. Kibler, 'A $SU(2)$ recipe for mutually unbiased bases', Intern. J. Mod. Phys. B20, 1802-1807 (2006)

[12] M.R. Kibler, 'Angular momentum and mutually unbiased bases', Intern. J. Mod. Phys. B20, 1792-1801 (2006)

[13] A.A. Kirillov, 'Elements of the theory of representations' (Springer, Berlin, 1976)

[14] A. Klimov, L. Sanchez-Soto, H. de Guise, 'Multicomplementary operators via finite Fourier transform', J. Phys. A38, 2747-2760 (2005)

[15] A. Klimov, L. Sanchez-Soto, H. de Guise, 'A complementarity based approach to phase in finite dimensional quantum systems', J. Opt. B:Quantum Semiclass. Opt. 7, 283-287 (2005)

[16] S.V. Konyagin, I.E. Shparlinski, 'Character sums with exponential functions and their applications' (Cambridge Univ. Press, Cambridge, 1999)

[17] R. Lidl, H. Niederreiter, 'Finite fileds' (Cambridge Univ. Press Cambridge, 1997)
[18] G.W. Mackey, 'Induced representations of groups and quantum mechanics' (Benjamin, New York, 1968)
[19] M. Neuhauser, 'An explicit construction of the metaplectic representation over a finite field', J. Lie Theory 12, 15-30 (2002)
[20] A.O. Pittenger, M.H. Rubin, 'Mutually unbiased bases, generalized spin matrices and separability', Linear Algebra Appl. 390, 255-278 (2004)
[21] A.O. Pittenger, M.H. Rubin, 'Wigner functions and separability for finite systems', J. Phys. A38, 6005-6036 (2005)
[22] J.L. Romero, G. Bjork, A.B. Klimov, L.L. Sanchez-Soto, 'Structure of sets of mutually unbiased bases for N qubits', Phys. Rev. A72, 062310, 1-8 (2005)
[23] M. Saniga, M. Planat, H. Rosu, 'Mutually unbiased bases and finite projective planes', J. Opt. B-Quantum Semiclass. Optics 6, L19-L20 (2004)
[24] M. Saniga, M. Planat, 'Hjelmslev geometry of mutually unbiased bases', J. Phys. A39, 435-440 (2006)
[25] J. Schwinger, 'Unitary operator bases', Proc. Nat. Acad. Sci. U.S.A. 46, 570-579 (1960);
[26] J. Schwinger, Quantum Kinematics and Dynamics (Benjamin, New York, 1970).
[27] S. Tanaka 'On irreducible unitary representations of some special linear groups of the second order: I' Osaka J. Math. 3, 217-227 (1966)
[28] S. Tanaka 'On irreducible unitary representations of some special linear groups of the second order: II' Osaka J. Math. 3, 229-242 (1966)
[29] A. Terras, 'Fourier analysis on finite groups and applications' (Cambridge Univ. Press, Cambridge, 1997)
[30] A. Vourdas, 'Quantum systems with finite Hilbert space', Rep. Prog. Phys. 67, 267-320 (2004)
[31] A. Vourdas, 'Quantum systems with finite Hilbert space: Galois fields in quantum mechanics' J. Phys A40, R285-R331 (2007)
[32] A. Vourdas, 'Galois quantum systems', J.Phys.A38, 8453-8471 (2005)
[33] A. Vourdas, 'The Frobenius formalism in Galois quantum systems', Acta Applicandae Mathematicae, 93, 197-214 (2006)
[34] A. Vourdas, 'Galois quantum systems irreducible polynomials and Riemann surfaces', J. Math. Phys. 47, 092104, 1-15 (2006)
[35] A. Vourdas, 'The angle-angular momentum quantum phase space', J.Phys.A29, 4275-4288 (1996)
[36] A. Vourdas, 'Analytic representations in quantum mechanics', J. Phys. A39, R65-R141 (2006)
[37] N.J. Vilenkin, 'Special functions and the theory of group representations' (Amer. Math. Soc., Rhode Island, 1968)
[38] A. Weil, 'Sur certains groupes d'operateurs unitaires' Acta Math. 111, 143-211 (1964)
[39] H. Weyl, Theory of Groups and Quantum Mechanics (Dover, New York, 1950)
[40] W. Wootters,'A Wigner function formulation of finite state quantum mechanics', Ann. Phys. (NY), 176, 1-21 (1987)
[41] W. Wootters, B.D. Fields, 'Optimal state determination by mutually unbiased measurements', Ann. Phys. (NY), 191, 363-381 (1989)
[42] D.P. Zelobenko, 'Compact lie groups and their representations' (Amer. Math. Soc., Rhode Island, 1973)