Abstract. Quantum mechanics in Hilbert spaces of finite dimension \( N \) is reviewed from the number theoretic point of view. For composite numbers \( N \) possible quantum kinematics are classified on the basis of Mackey’s Imprimitivity Theorem for finite Abelian groups. This yields also a classification of finite Weyl-Heisenberg groups and the corresponding finite quantum systems. Simple number theory gets involved through the fundamental theorem describing all finite discrete Abelian groups of order \( N \) as direct products of cyclic groups, whose orders are powers of not necessarily distinct primes contained in the prime decomposition of \( N \). The corresponding symmetries - normalizers of Weyl-Heisenberg groups in unitary groups (in quantum information conventionally called Clifford groups) - are fully described.

Contents

1. Introduction 2
2. Simple quantum kinematics on cyclic groups 5
3. A classification of finite quantum systems 10
4. Quantum degrees of freedom taken seriously 11
5. Fine gradings of \( C^* \)-algebras 13
6. Complementarity in \( C^{n*} \)-algebras 16
7. Symmetries of simple quantum kinematics 18
8. Symmetries of composite systems 19
9. Examples and open problems 22
10. Conclusions 23
Acknowledgements 24
References 25
1. Introduction

Non-relativistic quantum mechanics of particle systems can be divided into quantum kinematics and quantum dynamics. First the Hilbert space and the non-commuting operators of complementary observables, position and momentum, are constructed. This kinematical structure then remains the same for all possible quantum dynamics which are determined by the respective system Hamiltonians.

For systems with configuration space $\mathbb{R}^n$ one can define quantum kinematics according to H. Weyl [4] in terms of the Weyl system — a projective unitary representation of the Abelian group of translations of the corresponding classical phase space $\mathbb{R}^n \times \mathbb{R}^n$. Using Weyl's system of unitary operators, J. von Neumann was then able to prove the uniqueness theorem stating that there is, up to unitary equivalence, unique irreducible quantum kinematics, commonly taken in the form of the Schrödinger representation. In the most general form the uniqueness theorem was proved on the basis of G.W. Mackey’s Imprimitivity Theorem. In this mathematical generalization the configuration space $\mathbb{R}^n$ was replaced by an arbitrary locally compact second countable Abelian group $G$ [5]. The direct product of $G$ and its Pontryagin dual then plays the role of the phase space.

Quantum mechanics in finite-dimensional Hilbert spaces originally seemed to be only a nice and simple exercise in linear algebra. During the last quarter century it unexpectedly became the mathematical framework for the study and introduction of methods of quantum information processing with numerous applications in quantum cryptography, teleportation and quantum computing. For instance, the mathematical notion of complementary bases lies at the heart of quantum cryptography.

Historically, H. Weyl — not successful with the proof of the uniqueness theorem — wanted to present a simple example in $\mathbb{C}^n$ analogous to one-dimensional quantum particle and at the same time exhibiting the uniqueness feature. This example was further developed by J. Schwinger [6] from the point of view of quantum mechanics. The complementary nature of position and momentum observables is here built
in the finite Weyl-Heisenberg group generated by the generalized Pauli matrices. The elements of this group provide a useful set of quantum observables of finite quantum systems.

The special role of the finite Weyl-Heisenberg group has been recognized also in a mathematically completely different domain — the classification of fine gradings of classical Lie algebras [11, 12]. For classical Lie algebras of the type $\text{sl}(n, \mathbb{C})$, $n = 2, 3, \ldots$, this classification contains — among others — the Pauli grading based on generalized Pauli matrices [13, 3]. The finite group generated by them has been called the Pauli group — a notion identical with the Weyl-Heisenberg group.

In our paper [22] we succeeded to prove the uniqueness of finite quantum kinematics using a simple version of Mackey’s Imprimitivity Theorem. In this way also a geometric view finite quantum kinematics was obtained as quantum mechanics where a cyclic group serves as the configuration space. For composite dimensions $n$ we applied the fundamental theorem on finitely generated Abelian groups with the surprising result — the classification of all finite quantum kinematics. This classification was also independently noted in 1995 by V.S. Varadarajan [14].

Here we propose to use general formulation of quantum mechanics in terms of $C^*$-algebras [15]. For finite quantum systems, they are the associative complex matrix algebras $M_n(\mathbb{C})$. The involution is the Hermitian conjugation and for the operator norm the usual supremum norm is taken. Inspired by the Pauli gradings of $\text{sl}(n, \mathbb{C})$, we shall introduce complementarity structures on $M_n(\mathbb{C})$ defined by fine gradings of $M_n(\mathbb{C})$ satisfying the property of quasi-orthogonality [35].

It is a remarkable fact that in spite of the boom of quantum information science the community of quantum information and communication has not used this general classification up to now. One just perceives only the visible aspect and works out examples using standard operator systems constructed from generalized Pauli matrices in an ad hoc manner. However, the underlying structure remains hidden. In our approach we explicitly exhibit the elementary quantum degrees
of freedom, since their relevance has not been emphasized in most of the literature on finite quantum systems.

It is clear that automorphisms or symmetries of the finite Heisenberg group play very important role in the investigation of Lie algebras on the one hand [3, 7, 8] and of quantum mechanics in finite dimensions on the other [9, 10]. These symmetries find proper expression in the notion of the quotient group of certain normalizer [11]. The groups of symmetries given by inner automorphisms were described in [3] as isomorphic to $\text{SL}(2, \mathbb{Z}_n)$ for arbitrary $n \in \mathbb{N}$ and as $\text{Sp}(4, \mathbb{Z}_p)$ for $n = p^2$, $p$ prime in [8].

Note that such symmetry groups are finite-dimensional analogues of the group $\text{Sp}(2N, \mathbb{R})$ of linear canonical transformations of the continuous phase space $\mathbb{R}^{2N}$. Their matrix forms then correspond to the metaplectic representation of $\text{Sp}(2N, \mathbb{R})$ in the infinite-dimensional Hilbert space $L^2(\mathbb{R}^N)$ in which the Heisenberg Lie algebra is represented [16].

Our results [1, 2] concern symmetries of the finite Heisenberg group for systems composed of two subsystems (qudits) of arbitrary dimensions $n, m$, and also of an arbitrary finite number of subsystems of arbitrary dimensions. Such composite systems have been studied over finite fields, e.g. for both $n = m$ prime [8] as well as for arbitrary number of equal dimensions [23]. There exist numerous studies of various aspects of the finite Heisenberg group over finite fields in connection with finite-dimensional quantum mechanics in Hilbert spaces of prime or prime power dimensions (see e.g. [18, 19, 20, 10, 21]).

Our main motivation to study symmetries of the finite Heisenberg group not in prime or prime power dimensions but for arbitrary dimensions stems from our previous research where we obtained results valid for arbitrary dimensions [3, 22, 24]. Recent paper [25] belongs to this direction, too, by dealing with quantum tomography over modular rings. Also papers [26, 27] support our motivation, since they show that finite-dimensional quantum mechanics over growing arbitrary dimensions yields surprisingly good approximations of ordinary quantum mechanics on the real line.

This investigation can also be viewed as an indirect contribution to the study of the up to now unsolved problem — the existence or
non-existence of the maximal set of $N + 1$ mutually unbiased bases in Hilbert spaces of arbitrary dimensions $N$. Let us point out that a constructive existence proof for $N$ prime presented in [10] was based on consistent use of the symmetry group $\text{SL}(2, \mathbb{Z}_N)$. It is well known that such maximal sets exist in all prime and prime power dimensions [28] but the maximal number of mutually unbiased bases for composite dimensions is unknown as yet. If known, it would provide a very important contribution to quantum communication science, where mutually unbiased bases serve as basic ingredient of secure protocols in quantum cryptography [29, 30]. Perhaps this paper may help to unveil the structure of the maximal set of mutually unbiased bases.

In section 2 we reproduce the group theoretical approach based on representation theory of Abelian groups which directly leads to complementarity of the basic operators. Sections 3 and 4 are devoted to the classification of finite quantum kinematics and some historical remarks. In sections 5 and 6 fine gradings in matrix $C^*$-algebras are studied in connection with complementarity of $*$-subalgebras. After these generalities the symmetry groups of finite quantum systems are studied in sections 7 and 8. There the suitable normalizer is completely described and it is shown that the symmetry group is the quotient group of the normalizer. In section 9 the theory is illustrated by some examples and unsolved problems are pointed out.

2. Simple quantum kinematics on cyclic groups

Ordinary quantum mechanics prescribes that the mathematical quantities representing the position and momentum should be self-adjoint operators on the Hilbert space of the system. Their algebraic properties constitute quantum kinematics, while quantum dynamics of the system is given by the unitary group generated by the Hamiltonian which is expressed as a function of the position and momentum operators.

According to Mackey, quantum kinematics of a system localized on a homogeneous space $M = G/H$ is determined by an irreducible transitive system of imprimitivity $(\mathcal{U}, \mathcal{E})$ for $G$ based on $M$ in a Hilbert space $\mathcal{H}$. Here $\mathcal{U} = \{U(g)|g \in G\}$ is a unitary representation of $G$ in $\mathcal{H}$ and $\mathcal{E} = \{E(S)|S \text{ Borel subset of } M\}$ is a projection–valued measure in
satisfying the covariance condition
\[ U(g)E(S)U(g)^{-1} = E(g^{-1}.S). \]

Given a positive integer \( N \geq 2 \), we assume that the configuration space \( M \) is the finite set
\[ M = Z_N = \{ \rho | \rho = 0, 1, \ldots, N - 1 \} \]
with additive group law modulo \( N \). Since there is a natural transitive action of \( Z_N \) on itself, we may consider \( M \) as a homogeneous space of
\[ G = Z_N = \{ j | j = 0, 1, \ldots, N - 1 \}, \]
realized as an additive group modulo \( N \) with the action
\[ G \times M \to M : (j, \rho) \mapsto \rho + j \text{(mod } N) \]
and the isotropy subgroup \( H = \{ 0 \} \). For the finite set \( M = Z_N \) the covariance condition simplifies to
\[ U(j)E(\rho)U(j)^{-1} = E(\rho - j), \]
where \( \rho \in M, j \in G, E(\rho) = E(\{ \rho \}) \) and \( E(S) = \sum_{\rho \in S} E(\rho). \)

Complete classification of transitive systems of imprimitivity up to simultaneous unitary equivalence of both \( U \) and \( E \) is obtained from Mackey’s Imprimitivity Theorem. Its application to our system yields

**Theorem 2.1.** If \( (U, E) \) acts irreducibly in \( \mathcal{H} \), then there is, up to unitary equivalence, only one system of imprimitivity, where:

1. \( \mathcal{H} \) is a Hilbert space \( \mathbb{C}^N \) with the inner product
   \[ (\varphi, \psi) = \sum_{\rho=0}^{N-1} \overline{\varphi_\rho}\psi_\rho, \]
   where \( \varphi_\rho, \psi_\rho, \rho = 0, 1, \ldots, N - 1 \), denote the components of \( \varphi, \psi \) in the standard basis.
2. \( U \) is the induced representation \( U = \text{Ind}_{H}^{G} I \) called the (right) regular representation
   \[ [U(j)\psi]_\rho = \psi_{\rho+j} \quad (j \in G). \]
   Its matrix form in the standard basis is
   \[ (U(j))_{\rho\sigma} = \delta_{\rho+j,\sigma}. \]
(3) $E$ is given by
\[ [E(\rho)\psi]_\sigma = \delta_{\rho\sigma} \psi_\sigma. \]

This unique system of imprimitivity has a simple physical meaning. The localization operators $E(\rho)$ are projectors on the eigenvectors $e^{(\rho)} \in \mathcal{H}$ corresponding to the positions $\rho = 0, 1, \ldots, N - 1$. Since the set $\{e^{(\rho)}\}$ forms the standard basis of $\mathcal{H}$ in the above matrix realization, this realization may be called position representation. Then in a normalized state $\psi = (\psi_0, \ldots, \psi_{N-1})$ the probability to measure the position $\rho$ is equal to
\[ (\psi, E(\rho)\psi) = |\psi_\rho|^2. \]

Unitary operators $U(j)$ act as displacement operators
\[ U(j)e^{(\rho)} = e^{(\rho-j)}. \]

In the position representation they are given by unitary matrices equal to the powers $U(j) = A^j$ of the one-step cyclic matrix
\[
A \equiv U(1) = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & & & \ddots & \\
0 & 0 & 0 & \cdots & 0 \\
1 & 0 & 0 & \cdots & 0
\end{pmatrix}.
\]

Finite-dimensional quantum mechanics has been developed as quantum mechanics on configuration spaces given by finite sets equipped with the structure of a finite Abelian group [22]. In the first step we consider a single cyclic group $\mathbb{Z}_n$ for given $n \in \mathbb{N}$ as the underlying configuration space.

**Definition 2.2.** For a given $n \in \mathbb{N}$ set
\[ \omega_n := e^{2\pi i/n} \in \mathbb{C}. \]
Denote $Q_n$ and $P_n$ the *generalized Pauli matrices* of order $n$,
\[ Q_n := \text{diag}(1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}) \in \text{GL}(n, \mathbb{C}) \]
and
\[ P_n \in \text{GL}(n, \mathbb{C}), \text{ where } (P_n)_{i,j} := \delta_{i,j-1}, \quad i, j \in \mathbb{Z}_n. \]
The $n \times n$ unit matrix will be denoted as $I_n$. The subgroup of unitary matrices in $\text{GL}(n, \mathbb{C})$ generated by $Q_n$ and $P_n$,

$$\Pi_n := \{ \omega_n^j Q_n^k P_n^l | j, k, l \in \{0, 1, \ldots, n - 1\} \}$$

is called the \textit{finite Heisenberg group}.

The special role of the generalized Pauli matrices has been confirmed in physical literature as the cornerstone of FDQM, since their integral powers have physical interpretation of exponentiated position and momentum operators in position representation [6]. As quantum mechanical operators, $Q_n$ and $P_n$ act in the $n$-dimensional Hilbert space $\mathcal{H}_n = \ell^2(\mathbb{Z}_n)$. Further properties of $\Pi_n$ are contained in the following obvious lemma.

\textbf{Lemma 2.3.} \hspace{1em} (1) The order of $\Pi_n$ is $n^3$.

(2) The center of $\Pi_n$ is $\{ \omega_n^j I_n | j \in \{0, 1, \ldots, n - 1\} \}$.

(3) $P_n Q_n = \omega_n Q_n P_n$.

In order to describe this quantum kinematics in terms of the equivalent \textit{discrete Weyl system} we need the dual system of unitary operators $\mathcal{V} = \{ V(\rho) | \rho \in M \}$ acting via displacements on the dual basis of momentum states $f^{(j)}$ — eigenvectors of the commuting set $\{ U(k) = A^k \}$, $A f^{(j)} = \lambda_j f^{(j)}$. Eigenvalues $\lambda_j$ and eigenvectors $f^{(j)}$ are easily found using the discrete Fourier transform $F : \psi \mapsto \tilde{\psi}$, where

$$\tilde{\psi}_j = \frac{1}{\sqrt{N}} \sum_{\rho=0}^{N-1} \omega^{-j \rho} \psi_\rho, \quad \text{i.e.} \quad F_{j\rho} = \frac{1}{\sqrt{N}} \omega^{-j \rho},$$

and $\omega = \exp \left(\frac{2\pi i}{N}\right)$ is the primitive $N$-th root of unity. Then it can be verified that $A$ and all its integer powers are simultaneously diagonalized by $F$ with the result

$$FAF^{-1} = B = \text{diag}(1, \omega, \ldots, \omega^{N-1}) = \sum_{\rho=0}^{N-1} \omega^\rho E(\rho).$$

The eigenvectors $f^{(j)}$ of $A$ belonging to eigenvalues $\omega^j$ are

$$f^{(j)} = \sum_{\rho=0}^{N-1} (F^{-1})_{j\rho} e(\rho) = \frac{1}{\sqrt{N}} \sum_{\rho=0}^{N-1} \omega^{j \rho} e(\rho) = \frac{1}{\sqrt{N}} (1, \omega^j, \ldots, \omega^{j(N-1)})$$
and the operators
\[ V(\rho) \equiv B^\rho = \sum_{\sigma=0}^{N-1} \omega^{\rho\sigma} E(\sigma) \]
act on \( f^{(j)} \) via displacements
\[ V(\rho)f^{(j)} = B^\rho f^{(j)} = f^{(j+\rho)}. \]

Hence the quantum kinematics \((\mathcal{U}, \mathcal{E})\) can be equivalently replaced by the discrete Weyl system \((\mathcal{U}, \mathcal{V})\) satisfying
\[ U(j)V(\rho) = \omega^{j\rho} V(\rho) U(j) \]
or
\[ A^j B^\rho = \omega^{j\rho} B^\rho A^j. \]
The discrete Weyl displacement operators are defined by unitary operators\(^1\)
\[ W(\rho, j) = \omega^{j\rho/2} V(\rho) U(j) = \omega^{-j\rho/2} U(j) V(\rho). \]
They satisfy the composition law for a ray representation of \(\mathbb{Z}_N \times \mathbb{Z}_N\)
\[ W(\rho, j)W(\rho', j') = \omega^{(\rho'j'-\rho j)/2} W(\rho + \rho, j + j'). \]

According to Schwinger, the discrete Weyl system \(\mathcal{W}\) consisting of \(N^2\) operators \(W(\rho, j)\) provides an orthogonal operator basis in the space of all linear operators in \(\mathbb{C}^N\). The operators \(W(\rho, j)/\sqrt{N}\) are orthogonal with respect to the inner product
\[ \text{Tr}(W(\rho, j)W(\rho', j')^*) = N\delta_{\rho\rho'}\delta_{jj'} \]
and satisfy the completeness relation
\[ \sum_{\rho, j} W(\rho, j)W(\rho', j')^* = N^2 1. \]

This important result can be summarized as follows:

**Theorem 2.4.** The set of \(N^2\) matrices \(S(\rho, j) = B^\rho A^j/\sqrt{N}, \ j, \rho = 0, 1, \ldots, N-1,\) constitutes a complete and orthonormal basis for \(N \times N\) complex matrices. Any \(N \times N\) complex matrix can thus be uniquely expanded in this basis. If \(N\) is odd, then the operator basis can be taken in the form \(\omega^{j\rho/2} S(\rho, j) = W(\rho, j)/\sqrt{N}.\)

\(^1\)If \(N\) is odd, the factors \(\omega^{j\rho/2}_N\) are well-defined on \(\mathbb{Z}_N \times \mathbb{Z}_N.\)
3. A classification of finite quantum systems

The cyclic group $\mathbb{Z}_N = \{0, 1, \ldots, N - 1\}$ was a configuration space for $N$-dimensional quantum kinematics of a single $N$-level system. However, the reasoning on the basis of the Imprimitivity Theorem allows direct extension to any finite Abelian group as configuration space because of a fundamental theorem for finite Abelian groups [17].

**Theorem 3.1.** Let $G$ be a finite Abelian group. Then $G$ is isomorphic with the direct product $\mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_f}$ of a finite number of cyclic groups for integers $N_1, \ldots, N_f$ greater than 1, each of which is a power of a prime, i.e. $N_k = p_k^{r_k}$, where the primes $p_k$ need not be mutually different.

The integers $N_k = p_k^{r_k}$ are called the *elementary divisors* of $G$. Two finite Abelian groups are isomorphic if and only if they have the same elementary divisor decomposition. In the special case of $G = \mathbb{Z}_N$ with composite $N = p_1^{r_1} \ldots p_f^{r_f}$ and distinct primes $p_k > 1$, the unique decomposition

$$\mathbb{Z}_N = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_f}, \quad N_k = p_k^{r_k}$$

is obtained by the Chinese Remainder Theorem.

Returning to a general finite Abelian group as configuration space, a transitive system of imprimitivity for $G = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_f}$ based on $M = \mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_f}$ is equivalent to the tensor product

$$\mathcal{U} = \mathcal{U}_1 \otimes \cdots \otimes \mathcal{U}_f, \quad \mathcal{E} = \mathcal{E}_1 \otimes \cdots \otimes \mathcal{E}_f$$

and acts in the Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_f$, where the dimensions are $\dim \mathcal{H}_k = N_k$, $\dim \mathcal{H} = N_1 \ldots N_f$. Each such system of imprimitivity $(\mathcal{U}, \mathcal{E})$ is irreducible, if and only if each $(\mathcal{U}_k, \mathcal{E}_k)$ is irreducible, hence if irreducible, it is unique up to unitary equivalence by the Imprimitivity Theorem.

Given a composite dimension $N$, then according to the Fundamental Theorem it is sufficient to take all inequivalent choices of elementary divisors $N_k = p_k^{r_k}$ with not necessarily distinct primes $p_k > 1$ to obtain all irreducible quantum kinematics in the Hilbert space of given finite dimension $N$. One can give physical interpretation to these tensor
products in the sense that the factors describe the elementary building blocks forming the finite quantum system.

Our results are summarized in

**Theorem 3.2.** For a given finite Abelian group $G$ there is a unique class of unitarily equivalent, irreducible imprimitivity systems $(U, E)$ in a finite-dimensional Hilbert space $\mathcal{H}$. In the special case $G = \mathbb{Z}_N$ the irreducible imprimitivity system is unitarily equivalent to the tensor product with $N_k = p_k^r_k$ and distinct primes $p_1, \ldots, p_f > 1$.

**Corollary 3.3.** For a given finite Abelian group $G$ there is a unique class of unitarily equivalent discrete Weyl systems $\mathcal{W}$ in a finite-dimensional Hilbert space $\mathcal{H}$,

$$\mathcal{W} = \mathcal{W}_1 \otimes \cdots \otimes \mathcal{W}_f.$$  

The above classification conclusively shows that finite quantum systems are mathematically composed from elementary constituents which are of standard types associated with finite Abelian groups $G = \mathbb{Z}_p, \mathbb{Z}_{p^2}, \ldots, \mathbb{Z}_{p^r}, \ldots$, where $p$ runs through the set of prime numbers $> 1$. We shall return to these standard types in connection with our study of symmetries.

4. Quantum degrees of freedom taken seriously

A historical remark is in order: the structure of the finite-dimensional Weyl operators was thoroughly investigated by J. Schwinger. He noted in particular that, if the dimension $N$ is a composite number which can be decomposed as a product $N = N_1 N_2$, where the positive integers $N_1, N_2 > 1$ are relatively prime, then all the Weyl operators in dimension $N$ can be simultaneously factorized in tensor products of the Weyl operators in the dimensions $N_1$ and $N_2$. J. Schwinger then states ([6], pp. 578–579): “The continuation of the factorization terminates in

$$N = \prod_{k=1}^{f} \nu_k,$$

where $f$ is the total number of prime factors in $N$, including repetitions. We call this characteristic property of $N$ the number of degrees of freedom for a system possessing $N$ states.” And further, “each degree of freedom is classified by the value of the prime integer $\nu = 2, 3, 5, \ldots \infty$.”
However, our application of the Fundamental Theorem for finite Abelian groups leads to the building blocks $\mathbb{Z}_{p^r}$ with $r \geq 1$ as constituent configuration spaces. This fact was independently noted by V.S. Varadarajan in his paper [14] devoted to the memory of J. Schwinger: “Curiously, Schwinger missed the systems associated to the indecomposable groups $\mathbb{Z}_N$ where $N$ is a prime power $p^r$, $r \geq 2$ being an integer.” And in another paper: “In this way he arrived at the principle that the Weyl systems associated to $\mathbb{Z}_p$ where $p$ runs over all the primes are the building blocks. Curiously this enumeration is incomplete and one has to include the cases with $\mathbb{Z}_{p^r}$ where $p$ is as before a prime but $r$ is any integer $\geq 1.”

It has to be pointed out that among possible factorizations into constituent subsystems special role is played by the factorization associated with the “best” prime decomposition of the dimension $N = p_1^{r_1} \cdots p_f^{r_f}$ with mutually distinct primes $p_1, \ldots, p_f$. By the Chinese Remainder Theorem the discrete Weyl system of composite dimension $N$ is equivalent to a composite system where the constituent Weyl subsystems act in the Hilbert spaces of relatively prime dimensions $p_1^{r_1}, \ldots, p_f^{r_f}$.

In physics, the dimensions of constituent Hilbert spaces are fixed by the numbers of the corresponding levels of physical subsystems. It follows that $G$ is isomorphic to a direct product of cyclic groups of the respective orders. Whenever this is the case, in order to be able to work with the elementary building blocks of the composite system, we should find the elementary divisors. For example, if $G = \mathbb{Z}_6 \times \mathbb{Z}_{15}$, we factor $6 = 2.3$ and $15 = 3.5$. Then the elementary divisor decomposition of $G$ is $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

Besides the elementary divisor decomposition, in mathematics exists another, so called invariant factor decomposition [17]. In this approach a finite Abelian group $G$ is uniquely determined by an ordered finite list of integers $n_1 \geq n_2 \geq \cdots \geq n_s$ greater than 1 determining the invariant factors $\mathbb{Z}_{n_i}$ of $G$ such that $n_{i+1}$ divides $n_i$ and $N = n_1 n_2 \ldots n_s$. For instance, if $N = 180$, the full list of non-isomorphic Abelian groups of order 180 consists of $\mathbb{Z}_{180}$, $\mathbb{Z}_{90} \times \mathbb{Z}_2$, $\mathbb{Z}_{60} \times \mathbb{Z}_3$, $\mathbb{Z}_{30} \times \mathbb{Z}_6$. However, for exhibiting the elementary building blocks of the corresponding composite system, the elementary divisor decomposition is indispensable. In the
above example all inequivalent choices of elementary divisors $N_k = p_k^{r_k}$ with not necessarily distinct primes $p_k > 1$ are $2^2.3^2.5, 2.2.3^2.5, 2^2.3.3.5, 2.2.3.3.5$.

The task of enumerating all finite quantum systems in dimension $N$ amounts to the determination of all finite Abelian groups of the order $N$. It starts with the factorization of $N = p_1^{r_1} \ldots p_f^{r_f}$ with mutually distinct primes $p_1, \ldots, p_f$. First one finds all permissible lists for groups of orders $p_i^{r_i}$ for each $i$. For a prime power $p_i^{r_i}$ the problem of determining all permissible lists is equivalent to finding all partitions of the exponent $r_i$ and does not depend on $p_i$. Recall that the number of partitions of a natural number $r$ is called Bell’s number $B(r)$. Then the total number of groups of order $N$ is equal to the product of Bell’s numbers $B(r_1)B(r_2) \ldots B(r_f)$.

5. Fine gradings of $C^*$-algebras

From the $C^*$-algebraic point of view, finite quantum systems in quantum information theory are given by full matrix algebras $M_n(\mathbb{C})$. We are going to equip $M_n(\mathbb{C})$ with additional structures — the inner product defined by the standard trace (defining also the Hilbert-Schmidt norm) and fine gradings defined by commuting inner automorphisms.

First, a grading of an associative algebra $A$ is a direct sum decomposition of $A$ as a vector space

$$ (1) \quad \Gamma : \quad A = \bigoplus_{\alpha} A_{\alpha} $$

satisfying the property

$$ x \in A_{\alpha}, \quad y \in A_{\beta} \quad \Rightarrow \quad xy \in A_{\gamma}. $$

Note that if $\Gamma$ is a grading of the matrix algebra $M_n(\mathbb{C})$, then $\Gamma$ is also a grading of the matrix Lie algebra $\text{gl}(n, \mathbb{C})$. Similarly, as is well known for Lie algebras, linear subspaces $A_{\alpha}$ can be defined as eigen-spaces of automorphisms of $A$. For an automorphism $g$ of $A$, $g(xy) = g(x)g(y)$ holds for all $x,y \in A$. Now if $g(x) = \lambda_{\alpha}x$ defines the subspace $A_{\alpha}$ and $g(y) = \lambda_{\beta}y$ defines the subspace $A_{\beta}$, then

$$ g(xy) = g(x)g(y) = \lambda_{\alpha}\lambda_{\beta}xy $$
defines the subspace $A_\gamma$ with $\lambda_\gamma = \lambda_\alpha \lambda_\beta$. In this way $g$ defines the grading decomposition $A = \bigoplus_\alpha \text{Ker}(g - \lambda_\alpha)$. Further commuting automorphisms may refine the grading. If $gh = hg$, we have

$$g(h(x)) = h(g(x)) = h(\lambda_\alpha x) = \lambda_\alpha h(x)$$

implying that the grading decomposition using both $g$ and $h$ may lead to a refinement. By extending the set of commuting automorphisms we are going to arrive at so called fine gradings where the grading subspaces have the lowest possible dimension.

For the associative algebra $M_n(\mathbb{C})$ of all matrices $n \times n$ over $\mathbb{C}$, we shall consider the inner automorphisms:

**Definition 5.1.** For $M \in \text{GL}(n, \mathbb{C})$ let $\text{Ad}_M \in \text{Int}(M_n(\mathbb{C}))$ be the inner automorphism of $M_n(\mathbb{C})$ induced by operator $M \in \text{GL}(n, \mathbb{C})$, i.e.

$$\text{Ad}_M(X) = MXM^{-1} \text{ for } X \in M_n(\mathbb{C}).$$

The following lemma summarizes relevant properties of $\text{Ad}_M$.

**Lemma 5.2.** Let $M, N \in \text{GL}(n, \mathbb{C})$. Then:

(i) $\text{Ad}_M \text{Ad}_N = \text{Ad}_{MN}$.
(ii) $(\text{Ad}_M)^{-1} = \text{Ad}_{M^{-1}}$.
(iii) $\text{Ad}_M = \text{Ad}_N$ if and only if there is a constant $0 \neq \alpha \in \mathbb{C}$ such that $M = \alpha N$.

Since the commuting inner automorphisms form an Abelian subgroup of $\text{Int}(M_n(\mathbb{C}))$, fine gradings of $M_n(\mathbb{C})$ can be found using the maximal Abelian groups of diagonalizable automorphisms – as subgroups of $\text{Int}(M_n(\mathbb{C}))$ – to be shortly called the MAD-groups. Thus we are going to obtain fine gradings via diagonalizable elements of finitely generated Abelian subgroups of $\text{Int}(M_n(\mathbb{C}))$.

We remind our earlier notation

$$B = Q_N = \text{diag} \left( 1, \omega_N, \omega_N^2, \cdots, \omega_N^{N-1} \right)$$
and

\[
A = P_N = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & \cdots & 0 & 1 \\
1 & 0 & 0 & \cdots & 0 & 0
\end{pmatrix}.
\]

Note that the finite Heisenberg group \( \Pi_n \) was introduced as a subgroup of \( \text{GL}(n, \mathbb{C}) \).

**Definition 5.3.** We define \( \mathcal{P}_n \) as the group

\[\mathcal{P}_n = \{ \text{Ad}_{Q_i P_j} \mid (i, j) \in \mathbb{Z}_n \times \mathbb{Z}_n \} \].

It is an Abelian subgroup of \( \text{Int}(M_n(\mathbb{C})) \) and is generated by two commuting automorphisms \( \text{Ad}_{Q_n}, \text{Ad}_{P_n} \), each of order \( n \),

\[\mathcal{P}_n = \langle \text{Ad}_{Q_n}, \text{Ad}_{P_n} \rangle \).

A geometric view is sometimes useful that \( \mathcal{P}_n \) is isomorphic to the quantum phase space identified with the Abelian group \( \mathbb{Z}_n \times \mathbb{Z}_n \).

The MAD-groups of inner automorphisms of \( M_n(\mathbb{C}) \) were already completely determined in a study of the MAD-groups for \( \text{sl}(n, \mathbb{C}) \) [12]:

**Theorem 5.4.** Any MAD-group contained in \( \text{Int}(M_n(\mathbb{C})) \) is conjugated to one and only one of the groups of the form

\[(2) \quad \mathcal{P}_{n_1} \otimes \mathcal{P}_{n_2} \otimes \ldots \otimes \mathcal{P}_{n_s} \otimes D(m),\]

where \( n_i = p_i^{r_i} \) are powers of primes, \( n = mn_1n_2\ldots n_s \) and \( D(m) \) is the image in \( \text{Int}(M_n(\mathbb{C})) \) of the group of \( m \times m \) complex diagonal matrices under the adjoint action.

If \( m = 1 \), the corresponding fine grading is the Pauli grading and it decomposes in \( M_n(\mathbb{C}) \) into \( n^2 \) one-dimensional subspaces.

According to [12], Corollary 3.3, the number of elements of the set consisting of \( D(n) \) and the MAD-groups (2) for given \( n \) can be computed using Bell’s numbers \( B(r_i) \) as the product \( \tilde{B}(r_1)\tilde{B}(r_2)\ldots\tilde{B}(r_s) \), where \( \tilde{B}(r) = \sum_{r' \leq r} B(r') \) and \( B(0) = 0 \).

For future reference, we give the list of MAD-groups in low dimensions:
\* \* \*  

- \( n = 2 \): \( \mathcal{P}_2 \otimes D(1), D(2) \)
- \( n = 3 \): \( \mathcal{P}_3 \otimes D(1), D(3) \)
- \( n = 4 \): \( \mathcal{P}_4 \otimes D(1), \mathcal{P}_2 \otimes D(1), \mathcal{P}_2 \otimes D(2), D(4) \)
- \( n = 5 \): \( \mathcal{P}_5 \otimes D(1), D(5) \)
- \( n = 6 \): \( \mathcal{P}_3 \otimes \mathcal{P}_2 \otimes D(1), \mathcal{P}_3 \otimes D(2), \mathcal{P}_2 \otimes D(3), D(6) \)
- \( n = 7 \): \( \mathcal{P}_7 \otimes D(1), D(7) \)
- \( n = 8 \): \( \mathcal{P}_8 \otimes D(1), \mathcal{P}_4 \otimes \mathcal{P}_2 \otimes D(1), \mathcal{P}_2 \otimes \mathcal{P}_2 \otimes D(1), \mathcal{P}_4 \otimes D(2), \mathcal{P}_2 \otimes \mathcal{P}_2 \otimes D(2), \mathcal{P}_2 \otimes D(4), D(4) \)

A nonstandard way to describe some gradings is by using elements of finite order. V. Kac gave a beautiful classification of all such gradings on semi-simple Lie algebras [33]. In our case, for a positive integer \( M \) such grading is a decomposition (1) where \( \alpha \in \mathbb{Z}_M \). Let \( \omega \) be a primitive \( M \)-th root of unity and \( \text{Ad}_{X^\alpha} \) an inner automorphism of \( A \) of order \( M \) induced by an element of finite order in the compact subgroup \( \text{SU}(n) \) of \( \text{GL}(n, \mathbb{C}) \). Then the eigen-subspaces of \( \text{Ad}_{X^\alpha} \) in \( A \)

\[
\text{Ad}_{X^\alpha} x = X^\alpha x(X^\alpha)^{-1} = \omega^\alpha x
\]

define the (not necessarily fine) grading (1). In the case of the Pauli grading the corresponding inner automorphisms of finite order are generated by \( \text{Ad}_{Q_n} \) and \( \text{Ad}_{P_n} \) and induce the group \( \mathbb{Z}_n \times \mathbb{Z}_n \).

6. Complementarity in \( C^* \)-algebras

The quantal notion of complementarity concerns a specific relation among quantum observables. Let us start with two almost identical definitions.

**Definition 6.1.** [?]. Two observables \( A \) and \( B \) of a quantum system with Hilbert space of finite dimension \( N \) are called complementary, if their eigenvalues are non-degenerate and any two normalized eigenvectors \( |u_i\rangle \) of \( A \) and \( |v_j\rangle \) of \( B \) satisfy

\[
|\langle u_i | v_j \rangle| = \frac{1}{\sqrt{N}}.
\]

Then in an eigenstate \( |u_i\rangle \) of \( A \) all eigenvalues \( b_1, \ldots, b_N \) of \( B \) are measured with equal probabilities, and vice versa. This means that exact knowledge of the measured value of \( A \) implies maximal uncertainty to
any measured value of $B$. For the next definition note that the (non-degenerate) eigenvalues $a_i$ of $A$ and $b_j$ of $B$ are in fact irrelevant, since only the corresponding orthonormal bases $|u_i\rangle$ and $|v_j\rangle$ are involved.

**Definition 6.2.** [28]. Two orthonormal bases in an $N$-dimensional complex Hilbert space

$$\{ |u_i\rangle | i = 1, 2, \ldots, N \} \quad \text{and} \quad \{ |v_j\rangle | j = 1, 2, \ldots, N \}$$

are called mutually unbiased if inner products between all possible pairs of vectors taken from distinct bases have the same magnitude $1/\sqrt{N}$,

$$|\langle u_i | v_j \rangle| = \frac{1}{\sqrt{N}} \quad \text{for all} \quad i, j \in \{1, 2, \ldots, N\}. \quad (4)$$

In the sense of these definitions one may call two measurements to be mutually unbiased, if the bases composed of the eigenstates of their observables (with non-degenerate spectra) are mutually unbiased. If the system is prepared in any eigenstate of $A$, then the transition probabilities to all eigenstates of the complementary observable $B$ are the same (equal to $1/N$).

Further, a set of bases is called mutually unbiased if every two different bases from the set are mutually unbiased. An important fact was proved in [28] that the upper limit to the maximal possible number of bases that can form a set of mutually unbiased bases in an $N$-dimensional Hilbert space is $N + 1$ and that this maximal number is attained for $N$ prime or a power of a prime. For composite numbers $N$ the maximal number of mutually unbiased bases is unknown. Our studies may also shed light on this long-standing unsolved problem related to complementary observables in finite-dimensional quantum mechanics.

In the first part of the paper we started from finite Abelian groups and arrived, via representation theory expressed by Mackey’s systems of imprimitivity, at the system of $N^2$ unitary operators forming complete orthonormal basis of $M_N(\mathbb{C})$ with respect to the Hilbert-Schmidt inner product. The basic unitary operators $Q_N$ and $P_N$ exactly satisfy the above criterion of complementarity. Thus the notion of complementarity of observables with non-degenerate eigenvalues is equivalently
reformulated in terms of their eigenvectors forming mutually unbiased bases. The needed bases can be constructed as common eigenvectors of subsets formed by commuting operators $Q^a_N P^b_N$ and the decomposition of the set of all operators $Q^a_N P^b_N$ into subsets of commuting operators may be reflected in the corresponding finite geometry [32].

In this section we would like to pass the opposite journey, starting from the full matrix algebras $M_n(\mathbb{C})$ representing operator algebras of finite quantum systems and to introduce complementarity structures via fine gradings satisfying suitable conditions. Complementarity of observables was generalized to complementarity of subalgebras of $M_n(\mathbb{C})$ in the papers [34, 37, 35] based on earlier work by S. Popa [36]. Two subalgebras are complementary if their traceless parts are orthogonal with respect to the Hilbert-Schmidt inner product. This criterion applied to the one-dimensional grading subspaces induced by the MAD-groups containing $D(1)$ is clearly satisfied. These Pauli gradings deserve to be called complementarity structures in $M_n(\mathbb{C})$.

7. Symmetries of simple quantum kinematics

Consider those inner automorphisms acting on elements of $\Pi_N$ which induce permutations of cosets in $\Pi_N/Z(\Pi_N)$:

$$\text{Ad}_X(\omega^j_N Q^i_N P^j_N) = X\omega^j_N Q^i_N P^j_N X^{-1},$$

where $X$ are unitary matrices from $GL(N, \mathbb{C})$.

These inner automorphisms are equivalent if they define the same transformation of cosets in $\Pi_N/Z(\Pi_N)$:

$$\text{Ad}_Y \sim \text{Ad}_X \iff YQ^i P^j Y^{-1} = XQ^i P^j X^{-1}$$

for all $(i, j) \in \mathbb{Z}_N \times \mathbb{Z}_N$.

The group $\mathcal{P}_N = \Pi_N/Z(\Pi_N)$ has two generators, the cosets $Q$ and $P$ (or $\text{Ad}_Q$ and $\text{Ad}_P$, respectively). Hence if $\text{Ad}_Y$ induces a permutation of cosets in $\Pi_N/Z(\Pi_N)$, then there must exist elements $a, b, c, d \in \mathbb{Z}_N$ such that

$$YQY^{-1} = Q^a P^b \quad \text{and} \quad YPY^{-1} = Q^c P^d.$$ 

It follows that to each equivalence class of inner automorphisms $\text{Ad}_Y$ a quadruple $(a, b, c, d)$ of elements in $\mathbb{Z}_N$ is assigned.
Theorem 7.1. [3, 19] For integer $N \geq 2$ there is an isomorphism $\Phi$ between the set of equivalence classes of inner automorphisms $\text{Ad}_Y$ which induce permutations of cosets and the group $\text{SL}(2,\mathbb{Z}_N)$ of $2 \times 2$ matrices with determinant equal to $1 \pmod{N}$,

$$\Phi(\text{Ad}_Y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{Z}_N;$$

the action of these automorphisms on $\Pi_N/\mathbb{Z}(\Pi_N)$ is given by the right action of $\text{SL}(2,\mathbb{Z}_N)$ on elements $(i, j)$ of the phase space $\mathcal{P}_N = \mathbb{Z}_N \times \mathbb{Z}_N$,

$$(i', j') = (i, j) \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$ 

8. Symmetries of composite systems

According to the well-known rules of quantum mechanics, finite-dimensional quantum mechanics on $\mathbb{Z}_n$ can be extended in a straightforward way to arbitrary finite direct products

$$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

as configuration spaces. The cyclic groups involved describe independent constituent quantum systems. The Hilbert space of such a composite system is constructed as the tensor product

$$\mathcal{H}_{n_1} \otimes \cdots \otimes \mathcal{H}_{n_k}$$

of dimension $N = n_1 \ldots n_k$, where $n_1, \ldots, n_k \in \mathbb{N}$.

We recall the usual properties of the matrix tensor product $\otimes$. Let $A, A' \in \text{GL}(n, \mathbb{C}), B, B' \in \text{GL}(m, \mathbb{C})$ and $\alpha \in \mathbb{C}$. Then:

(i) $(A \otimes B)(A' \otimes B') = AA' \otimes BB'$.
(ii) $\alpha(A \otimes B) = (\alpha A) \otimes B = A \otimes (\alpha B)$.
(iii) $A \otimes B = I_{nm}$ if and only if there is $0 \neq \alpha \in \mathbb{C}$ such that $A = \alpha I_n$ and $B = \alpha^{-1} I_m$.

For the multipartite system, quantum phase space is an Abelian subgroup of $\text{Int}(\text{GL}(N, \mathbb{C}))$ defined by

$$\mathcal{P}_{(n_1, \ldots, n_k)} = \{ \text{Ad}_{M_1 \otimes \cdots \otimes M_k} | M_i \in \Pi_{n_i} \}.$$
Its generating elements are the inner automorphisms 
\[ e_j := \text{Ad}_{A_j} \quad \text{for} \quad j = 1, \ldots, 2k, \]
where (for \( i = 1, \ldots, k \))
\[ A_{2i-1} := I_{n_1 \cdots n_{i-1}} \otimes P_{n_i} \otimes I_{n_{i+1} \cdots n_k}, \quad A_{2i} := I_{n_1 \cdots n_{i-1}} \otimes Q_{n_i} \otimes I_{n_{i+1} \cdots n_k}. \]

The normalizer of \( \mathcal{P}_{(n_1, \ldots, n_k)} \) in \( \text{Int}(\text{GL}(n_1 \cdot \cdots \cdot n_k; \mathbb{C})) \) will be denoted
\[ \mathcal{N}(\mathcal{P}_{(n_1, \ldots, n_k)}) := N_{\text{Int}(\text{GL}(n_1 \cdot \cdots \cdot n_k; \mathbb{C}))}(\mathcal{P}_{(n_1, \ldots, n_k)}). \]

We need also the normalizer of \( \mathcal{P}_n \) in \( \text{Int}(\text{GL}(n; \mathbb{C})) \),
\[ \mathcal{N}(\mathcal{P}_n) := N_{\text{Int}(\text{GL}(n; \mathbb{C}))}(\mathcal{P}_n), \]
and
\[ \mathcal{N}(\mathcal{P}_{n_1}) \times \cdots \times \mathcal{N}(\mathcal{P}_{n_k}) := \{ \text{Ad}_{M_1 \otimes \cdots \otimes M_k} | M_i \in \mathcal{N}(\mathcal{P}_{n_i}) \} \subseteq \text{Int}(\text{GL}(N; \mathbb{C})). \]

Further,
\[ \mathcal{N}(\mathcal{P}_{n_1}) \times \cdots \times \mathcal{N}(\mathcal{P}_{n_k}) \subseteq \mathcal{N}(\mathcal{P}_{(n_1, \ldots, n_k)}). \]

Now the symmetry group \( \mathcal{H}_{[n_1, \ldots, n_k]} \) is defined in several steps. We note that in the community of quantum information this group is called the Clifford group [38].

First let \( \mathcal{S}_{[n_1, \ldots, n_k]} \) be a set consisting of \( k \times k \) matrices \( H \) of \( 2 \times 2 \) blocks
\[ H_{ij} = \frac{n_i}{\gcd(n_i, n_j)} A_{ij}, \]
where \( A_{ij} \in M_2(\mathbb{Z}_{n_i}) \) for \( i, j = 1, \ldots, k \). Then \( \mathcal{S}_{[n_1, \ldots, n_k]} \) is (with the usual matrix multiplication) a monoid.

Next, for a matrix \( H \in \mathcal{S}_{[n_1, \ldots, n_k]} \), we define its adjoint \( H^* \in \mathcal{S}_{[n_1, \ldots, n_k]} \) by
\[ (H^*)_{ij} = \frac{n_i}{\gcd(n_i, n_j)} A_{ji}^T. \]

Further, we need a skew-symmetric matrix
\[ J = \text{diag}(J_2, \ldots, J_2) \in \mathcal{S}_{[n_1, \ldots, n_k]} \]
where
\[ J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \]
Then the symmetry group is defined as
\[
\mathcal{H}_{[n_1,\ldots,n_k]} := \{ H \in S_{[n_1,\ldots,n_k]} | \ H^* J H = J \}
\]
and is a finite subgroup of the monoid \( S_{[n_1,\ldots,n_k]} \).

Our first theorem states the group isomorphism:

**Theorem 8.1.** \( \mathcal{N}(\mathcal{P}_{(n_1,\ldots,n_k)}) / \mathcal{P}_{(n_1,\ldots,n_k)} \cong \text{Sp}_{[n_1,\ldots,n_k]} \).

Our second theorem describes the generating elements of the normalizer:

**Theorem 8.2.** The normalizer \( \mathcal{N}(\mathcal{P}_{(n_1,\ldots,n_k)}) \) is generated by
\[
\mathcal{N}(\mathcal{P}_{n_1}) \times \cdots \times \mathcal{N}(\mathcal{P}_{n_k}) \quad \text{and} \quad \{ \text{Ad}_{R_{ij}} \},
\]
where (for \( 1 \leq i < j \leq k \))
\[
R_{ij} = I_{n_1\cdots n_{i-1}} \otimes \text{diag}(I_{n_{i+1}\cdots n_j}, T_{ij}, \ldots, T_{ij}^{n_{i-1}}) \otimes I_{n_{i+1}\cdots n_k}
\]
and
\[
T_{ij} = I_{n_{i+1}\cdots n_{j-1}} \otimes Q_{n_j}^{\gcd(n_i,n_j)}.
\]

**Corollary 8.3.** If \( n_1 = \cdots = n_k = n \), i.e. \( N = n^k \), the symmetry group is \( \text{Sp}_{[n,\ldots,n]} \cong \text{Sp}_{2k}(\mathbb{Z}_n) \).

These cases are of particular interest, since they uncover symplectic symmetry of \( k \)-partite systems composed of subsystems with the same dimensions. This state of affairs was found, to our knowledge, first by [8] for \( k = 2 \) under additional assumption that \( n = p \) is prime, leading to \( \text{Sp}(4, \mathbb{F}_p) \) over the field \( \mathbb{F}_p \). We have generalized this result to bipartite systems with arbitrary \( n \) (non-prime) leading to \( \text{Sp}(4, \mathbb{Z}_n) \) over the modular ring, and also to multipartite systems. The corresponding result has independently been obtained [?] who studied symmetry group of the tensored Pauli grading of \( \text{sl}(n^k, \mathbb{C}) \), which he called the Weyl group of the Pauli grading in analogy with the Weyl groups of the root systems of semi-simple Lie algebras.
9. Examples and open problems

In our paper [1] we presented detailed description of the symmetry group of the finite Heisenberg group in the case of a bipartite quantum system consisting of two subsystems with arbitrary dimensions $n$, $m$. The corresponding finite Heisenberg group is embedded in $GL(N, \mathbb{C})$, $N = nm$. Via inner automorphisms it induces an Abelian subgroup in $\text{Int}(GL(N, \mathbb{C}))$. The normalizer of this Abelian subgroup in the group of inner automorphisms of $GL(N, \mathbb{C})$ contains all inner automorphisms transforming the phase space $\mathcal{P}_N$ onto itself, hence necessarily contains $\mathcal{P}_N$ as an Abelian semidirect factor. The true symmetry group is then given by the quotient group of the normalizer with respect to this Abelian subgroup. Restricting our study to configuration spaces involving just two factors $\mathbb{Z}_n \times \mathbb{Z}_m$ with arbitrary $n, m \in \mathbb{N}$, the corresponding Hilbert space of finite-dimensional quantum mechanics is $\mathcal{H} = \mathcal{H}_n \otimes \mathcal{H}_m$ of dimension $N = nm$.

The special case of $n = m = p$, $p$ prime, $N = p^2$, is simply observed to correspond to the symmetry group

$$\text{Sp}_{[p,p]} \cong \text{Sp}(4, \mathbb{Z}_p),$$

fully described in [8]. We have generalized their result to $n = m$ arbitrary (non-prime), leading to the symmetry group

$$\text{Sp}_{[n,n]} \cong \text{Sp}(4, \mathbb{Z}_n).$$

If $N = nm$, $n, m$ coprime, the symmetry group is, according to [1, 3]

$$\text{Sp}_{[n,m]} \cong \text{SL}(2, \mathbb{Z}_n) \times \text{SL}(2, \mathbb{Z}_m) \cong \text{SL}(2, \mathbb{Z}_{nm}).$$

These simple standard types do not exhaust possible groups for arbitrary numbers $n$, $m$. In general, if $d = \gcd(n, m)$, $n = ad$, $m = bd$, the finite configuration space can be further decomposed under the condition that $a, b$ are both coprime to $d$,

$$\mathbb{Z}_n \times \mathbb{Z}_m = \mathbb{Z}_{ad} \times \mathbb{Z}_{bd} \cong \mathbb{Z}_a \times \mathbb{Z}_d \times (Z_b \times Z_d) = \mathbb{Z}_a \times \mathbb{Z}_b \times Z_d \times Z_d.$$

Thus the symmetry group is reduced to the direct product

$$\text{Sp}_{[n,m]} \cong \text{Sp}_{[a,b]} \times \text{Sp}(4, \mathbb{Z}_d)$$
In the case when $n = 15$, $m = 12$ and $d = 3$ is coprime to both $a = 5$ and $b = 4$, and also $a$ and $b$ are coprime, then the symmetry group is reduced to the standard types SL and Sp,

$$\text{Sp}_{[n,m]} \cong \text{SL}(2, \mathbb{Z}_a) \times \text{SL}(2, \mathbb{Z}_b) \times \text{Sp}(4, \mathbb{Z}_d).$$

However, the general situation is more complicated and requires different treatment. For instance, let $n = 180$ and $m = 150$. Then $d = 30$, $a = 180/30 = 6$ and $b = 150/30 = 5$, hence $a|d$ and $b|d$ and simple reduction to standard groups is not possible. One has to break down the composite system consisting of two single systems into its *elementary constituents*. Thus decompose each of the finite configuration spaces

$$\mathbb{Z}_{180} \times \mathbb{Z}_{150} = (\mathbb{Z}_2^2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5^2) \times (\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5^2),$$

and take notice of coprime factors $2^2$, $3^2$ and $5^2$ leading to the factorization in agreement with elementary divisors decomposition

$$\text{Sp}_{[180,150]} \cong \text{Sp}_{[2^2,2^2]} \times \text{Sp}_{[3^2,3^2]} \times \text{Sp}_{[5^2,5^2]}.$$ 

We have thus arrived at an *open problem* to properly characterize the symmetry groups of the form $\text{Sp}_{[p^k,p^{k'}]}$ as constituting the building blocks of the symmetry groups in the general case. Therefore these groups and more general ones with finite numbers of indices given by powers of a given prime $p$, deserve to be attached to the standard types given above.

10. Conclusions

The structures of finite-dimensional quantum mechanics go back to H. Weyl and J. Schwinger [4, 6]. The basic operators in dimension $N$ are unitary operators ($N \times N$ matrices) $Q_N$ and $P_N$ and all their powers and products. The eigenvalues of $Q_N^a P_N^b$ are integer powers of the primitive $N$-th root of unity $\omega_N = \exp 2\pi i/N$. From their mathematical structure the finite phase space emerges: pairs $(a, b) \in \mathbb{Z}_N \times \mathbb{Z}_N$.

In our study unexpectedly rich structures are obtained from number-theoretic properties connected with prime decompositions of numbers $N$. Our studies may also shed light on a long-standing unsolved problem related to complementary observables in finite-dimensional quantum mechanics. There the notion of complementarity of observables
$A, B$ with non-degenerate eigenvalues is equivalently reformulated in terms of their eigenvectors forming mutually unbiased bases: if the system is prepared in any eigenstate of $A$, then the transition probabilities to all eigenstates of the complementary observable $B$ are the same (equal to $1/N$). It is known that the maximal set of mutually unbiased bases contains at most $N + 1$ bases and that this maximal number is attained for $N$ prime or a power of a prime. For composite numbers $N$ the maximal number of mutually unbiased bases is unknown. The needed bases can be constructed as common eigenvectors of subsets formed by commuting operators $Q_N^a P_N^b$. In this way the decomposition of the set of all operators $Q_N^a P_N^b$ into subsets of commuting operators is faithfully reflected in the corresponding finite geometry [32]. The study of mutually unbiased bases may have implications for quantum information and communication science, since mutually unbiased bases are indispensable ingredients of quantum key distribution protocols.

Finite quantum systems are basic constituents of quantum information processing. Except single 2- and $d$-level quantum systems — qubits and qudits — many authors pay their attention to finitely composed systems, where the basic operators are formed by tensor products. Multiple qubits with Hilbert spaces $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \mathbb{C}^2$ are routinely employed in quantum algorithms, while multiple qudits with Hilbert spaces $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \ldots \mathbb{C}^d$ may be interesting for quantum error-correction codes and for multipartite communication (as on hypothetical quantum internet). What about most general systems? Authors call them sometimes mixtures of multiple qudits. We have shown the general classification of finite quantum systems: for given dimension there exists a broad variety of finitely composed distinct quantum systems given by explicit tensorial factorizations into elementary constituents.

**Acknowledgements**

The author is grateful to M. Havlíček and P. Novotný for fruitful discussions on the subject of the paper. Support by the Ministry of Education of Czech Republic from the research plan RVO:68407700 is acknowledged.
References


[23] Han G 2010 The symmetries of the fine gradings of $\text{sl}(n^k, \mathbb{C})$ associated with direct product of Pauli groups *J. Math. Phys.* 51 092104


DEPARTMENT OF PHYSICS, FACULTY OF NUCLEAR SCIENCES AND PHYSICAL ENGINEERING, CZECH TECHNICAL UNIVERSITY IN PRAGUE, BŘEHOVÁ 7, 115 19 PRAGUE 1, CZECH REPUBLIC
E-mail address: jiri.tolar@fjfi.cvut.cz