ARITHMETIC METHODS
IN MATHEMATICAL PHYSICS AND BIOLOGY
BANACH CENTER PUBLICATIONS, VOLUME 109
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2016

BETHE ANSATZ, GALOIS SYMMETRIES, AND FINITE QUANTUM SYSTEMS

TADEUSZ LULEK

Faculty of Physics, Adam Mickiewicz University
Umultowska 85, 61-614 Poznań, Poland
E-mail: tadlulek@amu.edu.pl

Abstract. We demonstrate some applications of arithmetic structures in Bethe Ansatz — the famous substitution which yields an exact solution of a quantum N-body problem for the linear magnetic ring of N spins 1/2 within the XXX model. We point out the purely arithmetic form of the eigenproblem of the associated Heisenberg Hamiltonian in the initial (calculational) basis of all magnetic configurations, together with the resulting solution, expressed in terms of a *finite* extension of the prime field of rationals. The Galois group of this extension acquires the natural physical interpretation in terms of admissible permutations of rigged string configurations. The cyclotomic number field proves to be an important subfield of this extension, responsible for the translational symmetry of the magnetic ring, reflected in quasimomenta of a finite Brillouin zone. We also point out the role of the cyclotomic fields in determination of all mutually unbiased bases for a Hilbert space with the dimension N being a power of a prime.

1. Introduction. Motivated by the title of the Conference, I am going to point out in this article a partial answer to the question, *how arithmetic enters mathematical physics*. Clearly, the question encompasses a huge area, and I would like to constrain on quantum mechanics of finite systems [6], [21], [23], [24]. A quantum system is determined by its Hilbert space $\mathcal{H}$, whose elements $|\psi\rangle \in \mathcal{H}$ yield pure states, and Hermitian operators $\rho \in \operatorname{End}\mathcal{H}$ with the trace 1 constitute the set of all quantum states of the system. In particular, operators of the form $\rho = |\psi\rangle\langle\psi|$, $|\psi\rangle \in \mathcal{H}$, $\langle\psi|\psi\rangle = 1$, represent pure states. A quantum system is called finite when $\dim\mathcal{H} = N$ is an integer, and thus a Troian horse for arithmetic in quantum mechanics.

A pivotal example of a quantum finite system is the magnetic ring, consisting of N nodes, each with spin 1/2, with the isotropic exchange interaction between nearest neighbours in the ring, known also as the XXX solvable model [2]. It provides unique quantum

2010 *Mathematics Subject Classification*: 82B23, 82D80, 11T71, 81V65.
Key words and phrases: Heisenberg magnet, Bethe Ansatz, Galois group, arithmetic qubits.
The paper is in final form and no version of it will be published elsewhere.

DOI: 10.4064/bc109-0-7

counterpart of the N-body problem which claims to have an exact solution, both for an arbitrary finite N and for the thermodynamic limit $N \to \infty$, has been given by Bethe [3] in 1931, and is commonly known as Bethe Ansatz. Mathematically, the problem consists in determination of all eigenvalues and eigenvectors of the Heisenberg Hamiltonian for the magnetic ring. Here, we expose the role of finite extensions of the prime field $\mathbb{Q}$ of rationals, and the physical meaning of the associated Galois symmetries of number field extensions arising in the process of diagonalization, and appropriate comparisons with Bethe Ansatz [1], [16], [17], [18]. In particular, cyclotomic fields $\mathbb{Q}(\omega)$, $\omega = \exp(2\pi i/N)$, are associated with the translational symmetry of the magnetic ring. For $N > 5$, exact diagonalization of the Heisenberg Hamiltonian requires further extensions of the cyclotomic field $\mathbb{Q}(\omega)$, resulting in the so called Heisenberg number field — the minimal field of characteristic zero which is sufficient to express all related eigenvalues and eigenvectors. Still, this field is insufficient to present these solutions in the form of the so called rigged string configurations, provided by Bethe Ansatz. The last requirement is realized by a further extension, referred to as the Bethe field. Associated Galois groups of field extensions provide a considerable unification of rigged string configurations since they allow to generate a variety of such eigenstates from a single one by simple arithmetic substitutions of appropriate radicals imposed by the corresponding Galois symmetries.

In this way, Galois automorphisms of finite extensions of number fields of characteristic zero acquire a physical meaning within the midst of integrable systems.

Another example is the qunit, the model finite quantum system, represented by the Hilbert space $h = \mathbb{C}^N$, well known in quantum information processing [6], [19]. In a particular case of $N = 2$, it is the qubit, or "quantum bit", the elementary memory unit of a hypothetical quantum computer.

An important problem in quantum information processing, usually referred to as the state tomography, consist in reproducing an arbitrary quantum state $\rho \in \operatorname{End} h$ of the qunit h along a definite protocol of measurement. It requires an infinite series of measurements in the so called mutually unbiased bases [6], [20], [25], [26], [27], that is, physical devices for measurements with respect to such reference frames in the qunit h which guarantee maximal mutual independence of outcomes. For example, the case of a qubit ($N = 2$) requires $N + 1 = 3$ mutually unbiased polarizers, which can be associated with the three mutually perpendicular axes x, y, z for the spin $1/2$. We explain this notion in detail in Section 3, mentioning here only the fact that description of such quantum measurements involves number fields of finite characteristic.

2. Bethe Ansatz and number fields of characteristic zero

2.1. The eigenproblem of the Heisenberg Hamiltonian. Let $h = \mathbb{C}^2$ be a qubit, and $\mathcal{H} = h^{\otimes N}$ — the space of all quantum states for the system of N qubits arranged into a ring, and referred to as the magnetic ring. The tetraiad $(\sigma^x, \sigma^y, \sigma^z, I_2)$, with σ^α, $\alpha \in \{x, y, z\}$, being the standard Pauli matrices,

$$\sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

and I_2 — the unit 2×2 matrix, is a basis in $\operatorname{End} h$.

Then

$$\mathbf{s} = \frac{1}{2}(\sigma^x, \sigma^y, \sigma^z) \tag{2}$$

is the vector operator for the spin 1/2, and

$$s_j^\alpha = I_2 \otimes I_2 \otimes \ldots \otimes \sigma^\alpha \otimes \ldots \otimes I_2, \quad \alpha \in \{x, y, z\},\ j \in \tilde{N}, \tag{3}$$

is the α-th component of the spin 1/2, localized at the node $j \in \tilde{N}$, where

$$\tilde{N} = \{j = 1, 2, \ldots, N\} \tag{4}$$

is the set of nodes of the magnetic ring. Within this notation, the Heisenberg Hamiltonian for the magnetic ring reads

$$\hat{H} = J \sum_{j \in \tilde{N}} \Big(\mathbf{s}_j \cdot \hat{\mathbf{s}}_{(j+1) \bmod N} - \frac{1}{4}\, I_2^{\otimes N} \Big) \tag{5}$$

with

$$\hat{\mathbf{s}}_1 \cdot \hat{\mathbf{s}}_2 = \hat{s}_1^x \otimes \hat{s}_2^x + \hat{s}_1^y \otimes \hat{s}_2^y + \hat{s}_1^z \otimes \hat{s}_2^z, \tag{6}$$

and J being the coupling parameter. We put in the following $J = 1$. It is a Hermitian operator in the Hilbert space $\mathcal{H}$, and we write its eigenproblem as

$$\hat{H}\,|\psi\rangle = E\,|\psi\rangle\,. \tag{7}$$

Each eigenvalue $E \in \operatorname{spec} \hat{H}$ is an admissible energy of the magnetic ring, and all linearly independent eigenstates $|\psi\rangle \in \mathcal{H}$ form an orthogonal basis in $\mathcal{H}$.

The key observation from the arithmetic point of view is that the eigenproblem (7), formulated in the initial basis of magnetic configurations of the space $\mathcal{H}$, involves only integers. We specify this observation in some more detail.

Let $f : \tilde{N} \to \tilde{2} \equiv \{+, -\}$ be a magnetic configuration, which can be also written as $f = (f_1, \ldots, f_N)$ such that $f(j)$ is the spin projection ($+1/2$ or $-1/2$) at the node $j \in \tilde{N}$. Let $f_0 \equiv (+, \ldots, +)$ be the magnetic configuration with all spins $+1/2$, referred to as the ferromagnetic saturation, or the *vacuum configuration*, and let

$$|\mathbf{j}\rangle = |j_1, j_2, \ldots, j_r\rangle\,, \quad 1 \le j_1 < j_2 < \ldots < j_r \le N \tag{8}$$

be a quantum pure state of the magnetic ring, corresponding to r reversed spins, localized at the nodes $j_1, \ldots, j_r$, and ordered according to the *Yang–Baxter inequality* in (8). Clearly, the set

$$Q^{(r)} = \big\{\mathbf{j} : 1 \le j_1 < j_2 < \ldots < j_r \le N\big\}, \quad |Q^{(r)}| = \binom{N}{r}, \tag{9}$$

is a subset of the set $\tilde{2}^{\tilde{N}}$ consisting of all magnetic configurations with r reversed spins, and

$$\tilde{2}^{\tilde{N}} = \bigcup_{r=0}^{N} Q^{(r)} \tag{10}$$

defines a decomposition of $\mathcal{H}$ into direct sum

$$\mathcal{H} = \bigoplus_{r=0}^{N} \mathcal{H}^r \tag{11}$$

of mutually orthogonal subspaces

$$\mathcal{H}^r = \ell c_{\mathbb{C}} Q^{(r)}, \tag{12}$$

where $\ell c_{\mathbb{C}}$ denotes the linear closure (of the set $Q^{(r)}$) over $\mathbb{C}$. Each space $\mathcal{H}^r$ "below equator", that is for $0 \leq r \leq N/2$, will be referred to as the space of all quantum states of the system

$$\tilde{r} = \{\alpha = 1, 2, \ldots, r\} \tag{13}$$

of r *Bethe pseudoparticles*, represented by reversed spins, which move on the magnetic ring $\tilde{N}$. Within such a definition, Eq. (12) is readily recognized as the Schrödinger picture of quantization, and thus the set $Q^{(r)}$ acquires the meaning of the *classical configuration space* for the system $\tilde{r}$ of Bethe pseudoparticles on the ring $\tilde{N}$.

It is easy to show that each space $\mathcal{H}^r$ is invariant under the action of the Heisenberg Hamiltonian $\hat{H}$, namely

$$\hat{H}\,|\mathbf{j}\rangle = \sum_{\mathbf{j}' \in Q^{(r)}_{\mathbf{j}}} \big(|\mathbf{j}'\rangle - |\mathbf{j}\rangle\big) \tag{14}$$

where $Q^{(r)}_{\mathbf{j}} \subset Q^{(r)}$ is the set of all nearest neighbours of $\mathbf{j}$ in $Q^{(r)}$. More specifically, for each $\mathbf{j}' \in Q^{(r)}_{\mathbf{j}}$ there exists such $\alpha_0 \in \tilde{r}$ that

$$j'_\alpha = \begin{cases} j_\alpha & \text{for } \alpha \neq \alpha_0, \\ (j_{\alpha_0 \pm 1}) \bmod N & \text{for } \alpha = \alpha_0. \end{cases} \tag{15}$$

Geometrically, the classical configuration space $Q^{(r)}$ for the system of r Bethe pseudoparticles can be seen as a hypercubic lattice, generically in r dimensions, with some F-dimensional boundaries, $1 \leq F \leq r-1$, resulting from the "hard core" condition: two Bethe pseudoparticles cannot occupy the same node [12], [13], [14], [15]. Globally, $Q^{(r)}$ has a homotopy implied by the periodicity of the magnetic ring $\tilde{N}$ [10].

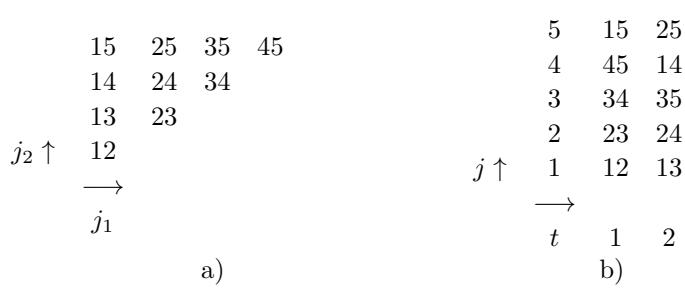

Fig. 1. The classical configuration space $Q^{(2)}$ for two Bethe pseudoparticles ($r = 2$) in a pentagonal magnetic ring ($N = 5$).
a) The Yang–Baxter map, (j_1, j_2), $1 \leq j_1 < j_2 \leq 5$.
b) The map of C_5-orbits, (t, j), $t = 1, 2$, $j \in \tilde{5}$. The orbit $t = 2$ constitutes the generic case $r = 2$, and $t = 1$ is the boundary ($F = 1$).

The Yang–Baxter structure of the classical configuration space $Q^{(2)}$ for two Bethe pseudoparticles is illustrated in Figs. 1 and 2 for a simple, but representative case $N = 5$. The map in Fig. 1a forms an isosceles right-angled triangle whose hypotenuse $(12, 23, 34, 45)$, taken together with apex (15), form the C_5-orbit of the nearest neighbours, whereas the rest is another C_5-orbit $(13, 24, 35, 14, 25)$ of the next nearest neighbours (cf. Fig. 1b). Fig. 2 demonstrates that the local dimension (the half of the number of nearest neighbours) in the first and second C_5-orbit is one and two, respectively. It

means that the orbit of nearest neighbours forms the one-dimensional boundary ($F = 1$) of $Q^{(2)}$ whereas the second is its interior, with the generic dimension $r = 2$. A proper gluing of the vertical and horizontal edge of the Yang–Baxter map of Fig. 1a along the pattern of Fig. 2b yields the global structure of $Q^{(2)}$ as a locally square lattice on a Möbius strip, with the orbit of nearest neighbours as its boundary. Somehow more involved, but essentially similar considerations apply for higher N and r.

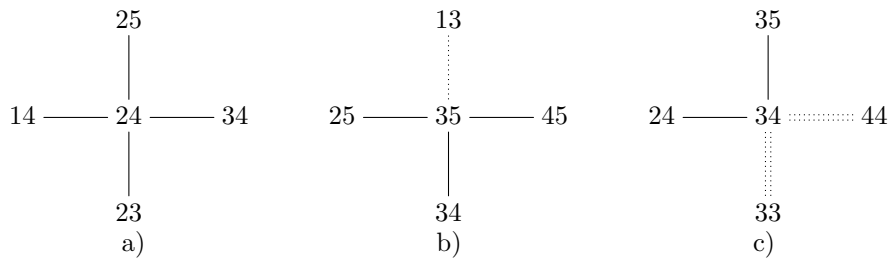

Fig. 2. Examples of neighbourhood $Q^{(2)}$ of a magnetic configuration for $N = 5$, $r = 2$.
a) $\mathbf{j} = (24)$ is placed *inside* the Yang–Baxter map of Fig. 1a,
and thus the set $Q^{(2)}_{24}$ of nearest neighbours of (24) just surrounds it,
b) $\mathbf{j} = (35)$ is placed at the horizontal edge of the Yang–Baxter map, and thus
three neighbours $(25, 34, 45)$ are nearby in the map Fig. 1a, whereas the fourth, $\mathbf{j}' = (13)$,
connected with (35) by a dotted line, is apparently remote in this map. This fact points out
that the horizontal edge of the map in Fig. 1a, $\mathbf{j} = (j5)$, $j = 1, 2, 3, 4$, is just an edge of the
map, and not that of $Q^{(2)}$. The same remark applies to the vertical edge, $\mathbf{j} = (1j)$, $j = 2, 3, 4, 5$.
c) $\mathbf{j} = (34)$ is placed on the diagonal edge, $\mathbf{j} = (j(j+1) \bmod 5)$, and thus has only
two neighbours, $\mathbf{j}' = (24)$ or (35). The remaining edges, (33) and (44), do not belong to $Q^{(2)}$
on the basis of "hard core" condition for Bethe pseudoparticles.

Eq. (14) determines the form of the secular matrix of the Heisenberg Hamiltonian $\hat{H}$ for each space $\mathcal{H}^r$, in the basis given by the corresponding classical configuration space $Q^{(r)}$, ordered along the map of C_N-orbits. For example, the case $N = 5$ yields

$$\hat{H} = \begin{array}{c|ccccc|ccccc} & & & & & & j_1' & & & & \\ & & & & & & j_2' & & & & \\ & 1 & 2 & 3 & 4 & 1 & 1 & 2 & 3 & 1 & 2 \\ j_1 j_2 & 2 & 3 & 4 & 5 & 5 & 3 & 4 & 5 & 4 & 5 \\ \hline 12 & -2 & & & & & 1 & & & & 1 \\ 23 & & -2 & & & & 1 & 1 & & & \\ 34 & & & -2 & & & & 1 & 1 & & \\ 34 & & & & -2 & & & & 1 & 1 & \\ 15 & & & & & -2 & & & & 1 & 1 \\ \hline 13 & 1 & 1 & & & & -4 & & 1 & 1 & \\ 24 & & 1 & 1 & & & & -4 & & 1 & 1 \\ 35 & & & 1 & 1 & & 1 & & -4 & & 1 \\ 14 & & & & 1 & 1 & 1 & 1 & & -4 & \\ 25 & 1 & & & & 1 & & 1 & 1 & & -4 \end{array} \tag{16}$$

for $r = 2$ and

			j'		
j	1	2	3	4	5
1	-2	1			1
2	1	-2	1		
3		1	-2	1	
4			1	-2	1
5	1			1	-2

(17)

for $r = 1$, with zeros omitted. Clearly, such matrices precisely reflect the Yang–Baxter and C_N-orbit structures of the corresponding classical configuration spaces. The most essential point which we wish to stress now is the fact that all entries of these secular matrices are *integers*. Thus, the roots E of the characteristic polynomial

$$w^{\hat{H}}(x) = \det\bigl(\hat{H} - xI_{\mathcal{H}^r}\bigr) \equiv \prod_{E\in\operatorname{spec} H} (x - E)^{m(E)}, \tag{18}$$

where $I_{\mathcal{H}^r}$ is the identity in $\mathcal{H}^r$, and $m(E)$ — the multiplicity of the root $E \in \operatorname{spec} H$ (in $\mathcal{H}^r$), define a finite extension $\mathbb{Q}(\operatorname{spec}\hat{H})$ of the prime field $\mathbb{Q}$ of rationals within the quantum space $\mathcal{H}^r$.

The extension $\mathbb{Q}(\operatorname{spec}\hat{H})$ is usually referred to as the *real Heisenberg field* [17], since it suffices to express all eigenvalues of $\hat{H}$ (for given N, r). One also considers a larger extension, $\mathbb{Q}(\{\psi\})$, by all corresponding eigenfunctions $|\psi\rangle$ (more exactly, all expansion coefficients in the basis of magnetic configurations), referred to as the *complex Heisenberg field* [17].

The eigenproblems (16) and (17) for the pentagon ($N = 5$) yield [16]

$$\operatorname{spec}\hat{H} = \begin{cases} 0, (-5-\sqrt{5})/2, -5+\sqrt{5})/2, -4-\sqrt{5}, -4+\sqrt{5} & \text{for Eq. (16)},\\ 0, (-5-\sqrt{5})/2, -5+\sqrt{5})/2, & \text{for Eq. (17)}, \end{cases} \tag{19}$$

and thus the real Heisenberg field is

$$\mathbb{H}_{\text{real}} = \mathbb{Q}(\sqrt{5}), \tag{20}$$

whereas the complex case gives

$$\mathbb{H}_{\text{complex}} = \mathbb{Q}(e^{2\pi i/5}), \tag{21}$$

that is, the cyclotomic field for $N = 5$. Clearly, the corresponding extensions for larger values of N are more elaborate, with orders dependent on the number of C_N-orbits in the classical configuration space $Q^{(r)}$ of interest.

2.2. Translational symmetry, Brillouin zone, and cyclotomic fields. Magnetic ring $\tilde{N}$ exhibits the translational symmetry, given by the cyclic group C_N. Clearly, the space $\mathcal{H}^1$ of all states with a single Bethe pseudoparticle is invariant under C_N. One defines the Weyl–Schwinger shift operator [8], [21] $\hat{U} \in \operatorname{End}\mathcal{H}^1$ by putting

$$\hat{U}\,|j\rangle = |(j+1) \bmod N\rangle\,, \tag{22}$$

which realizes the elementary translation on the ring $\tilde{N}$. The characteristic polynomial of the shift operator $\tilde{U}$ in the space $\mathcal{H}^1$,

$$w^{\hat{U}}(x) = x^N - 1 = \prod_{k\in B}(x - \omega^k), \quad \omega = e^{2\pi i/N}, \tag{23}$$

defines, by means of its roots ω^k, the *Brillouin zone* of the ring $\tilde{N}$, as

$$B = \left\{k = 0, \pm 1, \pm 2, \ldots, \begin{cases} \pm(N/2-1), N/2 & \text{for } N \text{ even} \\ \pm(N-1)/2 & \text{for } N \text{ odd} \end{cases}\right\}. \tag{24}$$

In this way, the Brillouin zone consists of all admissible (quantized) quasimomenta k on $\tilde{N}$, and can also be seen as the Pontryagin dual of the cyclic group C_N, generated by the Weyl–Schwinger shift operator $\hat{U}$.

The spectrum of the Weyl–Schwinger operator

$$\operatorname{spec}\hat{U} = \{\omega^k : k \in B\} \cong B, \tag{25}$$

consisting of all integer powers of the N-th primitive root ω of unity, yields construction of the *Fourier operator* $\hat{F} \in \operatorname{End}\mathcal{H}^1$ in terms of matrix elements of the basis of positions in $\mathcal{H}^1$, denoted here by $\left|\tilde{N}j\right\rangle \equiv |j\rangle$, as

$$\left\langle \tilde{N}j_1 \,|\, \hat{F} \,|\, \tilde{N}j_2 \right\rangle = \frac{1}{\sqrt{N}}\,\omega^{-j_1 j_2}, \quad j_1, j_2 \in \tilde{N}. \tag{26}$$

The Fourier operator $\hat{F}$ defines another basis in the space $\mathcal{H}^1$, denoted by $|B,k\rangle$, $k \in B$, and referred to as *the basis of quasimomentum*, by the formula

$$\hat{F}\left|\tilde{N}j\right\rangle = |B, \beta(j)\rangle\,, \quad j \in \tilde{N}, \tag{27}$$

where $\beta : \tilde{N} \to B$ is a bijection between the set $\tilde{N}$ of positions and B of quasimomenta, given by

$$\beta(j) = j \bmod B, \quad j \in \tilde{N}, \tag{28}$$

that is,

$$\beta(j) = \begin{cases} j & \text{for } 1 \le j \le N/2, \\ -(N-j) & \text{otherwise.} \end{cases} \tag{29}$$

One thus has

$$|B,k\rangle = \frac{1}{\sqrt{N}} \sum_{j\in\tilde{N}} \omega^{-kj}\left|\tilde{N}, j\right\rangle, \quad k \in B, \tag{30}$$

with the inverse transformation

$$\left|\tilde{N}, j\right\rangle = \frac{1}{\sqrt{N}} \sum_{k\in B} \omega^{kj}\,|B,k\rangle\,, \quad j \in \tilde{N}. \tag{31}$$

In quantum informatics, the space $\mathcal{H}^1$ is a realization of a qunit ($\dim\mathcal{H}^1 = N$), and these two bases, that $\left|\tilde{N}, j\right\rangle$ of positions and $|B,k\rangle$ of quasimomenta, have the property

$$\left|\langle \tilde{N}, j \,|\, B,k\rangle\right|^2 = \frac{1}{N}\,, \quad j \in \tilde{N}, \quad k \in B. \tag{32}$$

It means that for any state $\left|\tilde{N}, j\right\rangle$ (or $|B,k\rangle$) with given position $j \in \tilde{N}$ (quasimomentum $k \in B$), probability of any quasimomentum $k \in B$ (position $j \in \tilde{N}$) is equally distributed.

For this reason, these two bases are referred to as *mutually unbiased* [2], [20], [25], [26], [27]. We have thus demonstrated that each qunit disposes at least two mutually unbiased bases. In the next section we return to this subject in a more detail.

Clearly, both the Weyl–Schwinger shift operator $\hat{U}$ and the corresponding Fourier operator $\hat{F}$ can be defined in each space $\mathcal{H}^r$. We omit here a detail discussion associated with divisors of N and corresponding rarefied C_N-orbits, but only state that the formula

$$\hat{F}\,|rtj\rangle = |rtk\rangle\,, \quad k = \beta(j), \tag{33}$$

where $|rtj\rangle$ is a magnetic configuration in $\mathcal{H}^r$ related to C_N-orbit t, defines *the basis of wavelets* [12] in $\mathcal{H}^r$. We point out two facts, related to the basis of wavelets. Firstly, the original eigenproblem of the Heisenberg Hamiltonian $\hat{H}$ decomposes in this basis into diagonal subeigenproblems, along with

$$\mathcal{H}^r = \bigoplus_{k\in B} \mathcal{H}^{rk}. \tag{34}$$

Secondly, each subeigenproblem, reduced to the subspace $\mathcal{H}^{rk}$ with a definite quasimomentum $k \in B$, is no longer expressible in terms of integers, and the necessary number field is extended to $\mathbb{Q}(\omega)$, that is, to the cyclotomic field, just due to the Fourier transform.

2.3. Rigged string configurations and the Bethe number field. We proceed to formulate explicitly the celebrated Bethe Ansatz form of an eigenstate of the Heisenberg Hamiltonian $\hat{H}$ in the space $\mathcal{H}^r$. It is given, along with the Schrödinger quantization picture, as a complex-valued function $\psi : Q^{(r)} \to \mathbb{C}$ on the classical configuration space $Q^{(r)}$ of the system of r Bethe pseudoparticles on the magnetic ring $\tilde{N}$. This function reads

$$\psi(j_1, \ldots, j_r) = \sum_{\pi\in\Sigma_r} A_\pi \exp\bigl(i(p_1 j_{\pi(1)} + \ldots + p_r j_{\pi(r)})\bigr), \tag{35}$$

where

$$\pi = \begin{pmatrix} 1 & \ldots & r \\ \pi(1) & \ldots & \pi(r) \end{pmatrix} \tag{36}$$

is a permutation on the set $\tilde{r}$ of Bethe pseudoparticles, referred to as a *scattering channel*, Σ_r is the symmetric group on $\tilde{r}$, $p_\alpha \in \mathbb{C}$, $\alpha \in \tilde{r}$, are parameters referred to as *pseudomomenta*,

$$A_\pi = A \exp\left(\frac{i}{2} \sum_{\substack{\alpha<\beta \\ \pi(\alpha)>\pi(\beta)}} \phi_{\pi(\alpha),\pi(\beta)}\right) \tag{37}$$

is the scattering amplitude for the channel π, the summation in Eq. (37) is over all descents in the permutation $\pi \in \Sigma_r$, and $\phi_{\alpha\beta}$ is the phase of solitonic scattering of pseudoparticle α on β, determined by the so called *reflection condition*

$$2\operatorname{ctg}\frac{\phi}{2} = \operatorname{ctg}\frac{p_\alpha}{2} - \operatorname{ctg}\frac{p_\beta}{2}\,, \quad \alpha \in \tilde{r},\ \beta \in \tilde{r},\ \alpha \neq \beta. \tag{38}$$

Each term in the right hand side of Eq. (35) corresponds to composition of a free motion of r Bethe pseudoparticles, such that the pseudoparticle $\alpha \in \tilde{r}$ has pseudomomentum $p_{\pi^{-1}(\alpha)}$, and the whole BA solution is a superposition of all possible scattering channels $\pi \in \Sigma_r$.

This is the form of BA eigenstates in our notation. Each BA solution is thus determined by the set of r pseudomomenta p_α, $\alpha \in \tilde{r}$, together with the set of $\binom{N}{2}$ phases $\phi_{\alpha\beta}$, $1 \le \alpha < \beta \le r$ (observe that $\phi_{\alpha\beta} = -\phi_{\beta\alpha}$), that is $r(r+1)/2$ parameters which should obey $r(r-1)/2$ reflection conditions (38), together with r periodicity conditions

$$Np_\alpha - \sum_{\beta \neq \alpha} \phi_{\alpha\beta} = 2\pi n_\alpha, \quad \alpha \in \tilde{r}, \tag{39}$$

where $n_\alpha \in \mathbb{Z}$ are quantum numbers which specify the eigenstate. The following change of variables

$$\lambda_\alpha = \frac{1}{2} \operatorname{ctg} \frac{p_\alpha}{2}, \quad \text{with the inverse} \quad e^{ip_\alpha} = \frac{\lambda_\alpha + i/2}{\lambda_\alpha - i/2}, \tag{40}$$

yields the system of r equations

$$\Big(\frac{\lambda_\alpha + i/2}{\lambda_\alpha - i/2}\Big)^N = \prod_{\beta \in \tilde{r} \setminus \{\alpha\}} \frac{\lambda_\alpha - \lambda_\beta + i}{\lambda_\alpha - \lambda_\beta - i}, \quad \alpha \in \tilde{r}. \tag{41}$$

These equations are not transcendental but only polynomial with respect to *spectral parameters* λ_α, known as the *Bethe Ansatz equations*. Each regular solution $(\lambda_1, \dots, \lambda_r)$ of (41) determines an exact eigenstate of the Heisenberg Hamiltonian in the space $\mathcal{H}^r$.

It is natural to ask whether the BA eigenstates of the form (35) span the whole space $\mathcal{H}^r$ or not. The answer is negative: they span at most the subspace $\mathcal{H}^{rr}$ of the so called *highest weight states* in $\mathcal{H}^r$, of dimension

$$\dim \mathcal{H}^{rr} = \binom{N}{r} - \binom{N}{r-1} = \dim \Delta^{\{N-r,r\}}, \tag{42}$$

where $\Delta^{\{N-r,r\}}$ is the irreducible representation of the symmetric group Σ_N, labelled by the *shape* $\{N-r, r\}$. Physically, $\mathcal{H}^r$ is the space of all states of the magnetic ring with the magnetization

$$M = \frac{N}{2} - r, \tag{43}$$

i.e. with the z-projection M of a total spin S of the magnet, the latter being written in a form

$$S = \frac{N}{2} - r'. \tag{44}$$

Clearly, the XXX model exhibits the spherical symmetry, and thus both M and S are exact quantum numbers. Within the space $\mathcal{H}^r$, the defining space for BA, M and r are fixed, but r' varies in the range $0 \le r' \le r$, and correspondingly

$$\mathcal{H}^r = \bigoplus_{r'=0}^{r} \mathcal{H}^{rr'}. \tag{45}$$

BA yields only the highest weight states $S = M$, or, equivalently, $r' = r$, which belong to the subspace $\mathcal{H}^{rr}$.

Now, the question above can be refined as follows: is the number of BA solutions sufficient to span the whole space $\mathcal{H}^{rr}$? Or, more concisely, is BA complete? This question has no rigorous answer, but an affirmative conjecture is given by the famous *Bethe hypothesis of strings* [7], [22], [24], [28]. This conjecture has no proof, but is commonly believed to

hold, despite of known counterexamples. It claims that the BA states, parametrized by the sequence $(\lambda_1, \ldots, \lambda_r)$ of spectral parameters, have in the thermodynamic limit

$$N \to \infty, \quad r \text{ fixed}, \tag{46}$$

the following property: spectral parameters gather into strings, in the form

$$\lambda_\alpha \longmapsto \lambda^{lv} + im, \tag{47}$$

where

1. $\lambda^{lv} \in \mathbb{R}$ is a real number, referred to as *the centre* of the string (lv).
2. l is an integer, $1 \leq l \leq r$, referred to as *the length* of the string (lv); it is the number of those spectral parameters which enter the string. Sometimes, one considers the associated quantity
$$s = \frac{l-1}{2}, \quad \text{or} \quad l = 2s+1, \tag{48}$$
with integer or half-integer s referred to as the *spin* of the (lv)-string.
3. The imaginary part m of the spectral parameter $\lambda_\alpha \equiv \lambda_m^{lv}$ ranges within
$$-s \leq m \leq s, \tag{49}$$
resembling thus the "z-projection" of the spin s.

Bethe hypothesis of strings admits a classification of exact BA eigenstates in terms of a class of combinatorial objects, called rigged string configurations, introduced by Kerov, Kirillov and Reshetikhin [9] in 1986. This classification scheme can be summarized as follows.

1. A string configuration is a partition $\nu \vdash r'$.
2. Each box of the Young diagram of ν represents a spectral parameter λ_m^{lv}.
3. Each row (lv) of ν forms an l-string. Strings of the same length l are labelled by $v = 1, 2, \ldots, m_l$, such that
$$\sum_l l m_l = r'. \tag{50}$$
4. Each l-string of a given string configuration ν is equipped (originally "rigged", a term coming from sail navigation) with a quasimomentum, within the range provided by "admissible Brillouin zone" [11]
$$B_a(\nu, l) = B \setminus B_f(\nu, l), \tag{51}$$
with
$$B_f(\nu, l) = \{k \in B : |k| \leq Q_l^{-1}\}, \tag{52}$$
where Q_l is the total number of boxes within first l columns of the Young diagram of the partition ν (cf. Fig. 3).

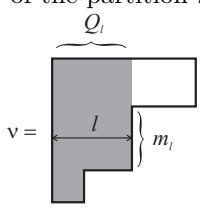

Fig. 3. A string configuration is a partition $\nu \vdash r'$, whose rows represent strings, and boxes — spectral parameters. The integer m_l is the number of rows of the length l, and Q_l denotes the number of boxes in the first l columns of the Young diagram ν (the shaded area).

Such a decomposition of the Brillouin zone B into forbidden part $B_f(\nu, l)$ and admissible $B_a(\nu, l)$ is the result of kinematical restrictions for the motion of strings, imposed by the "hard core" of Bethe pseudoparticles: an l-string should move with the quasimomentum not smaller than the combinatoric quantity Q_l, which thus plays the role somehow similar to Fermi momentum for electrons in solids.

Eventually, the exact BA eigenstate $(\lambda_1, \ldots, \lambda_r)$ is labelled by a rigged string configuration as

$$|\nu\mathcal{L}\rangle\,, \tag{53}$$

where $\nu \vdash r'$ is the configuration of strings, and $\mathcal{L}$ — the corresponding collection of riggings.

The quantity

$$P_l = N - 2Q_l \tag{54}$$

plays the role of the size of "sea of holes" for l-strings within a given string configuration ν, that is, the number of available steps in the reciprocal space. It implies that the number of riggings of a string configuration ν is

$$|z(\nu)| = \prod_l \binom{P_l + m_l}{m_l}, \tag{55}$$

and

$$\sum_{\nu \vdash r'} |z(\nu)| = \dim \Delta^{\{N-r', r'\}}, \tag{56}$$

which demonstrates that Bethe hypothesis of strings assures the completeness of BA eigenstates.

Let us consider the case $N = 5$, $r = 2$ [17]. The Hamiltonian in the basis of C_5-orbits is given by Eq. (16), and the Fourier transform to the basis of wavelets yields a quasidiagonal form, with the k-blocks given by

$$H_k = \begin{pmatrix} -2 & 1 + \omega^k \\ 1 + \omega^{-k} & -4 + \omega^{2k} + \omega^{-2k} \end{pmatrix}, \quad k \in B. \tag{57}$$

Thus the one-magnon spectrum reads

$$E_{1k} = -2 + \omega^k + \omega^{-k} = (-5 - (-1)^k\sqrt{5})/2, \tag{58}$$

and for two-magnon states

$$E_{2k} = -4 + (\omega^{2k} + \omega^{-2k}) - (\omega^k + \omega^{-k}) = -4 + (-1)^k\sqrt{5}. \tag{59}$$

Rigged string configurations $\nu\mathcal{L}$ for two-magnon states ($r = r' = 2$), together with their eigenstates $|\nu\mathcal{L}\rangle$ presented as the corresponding density matrices

$$\rho_{\nu\mathcal{L}} = |\nu\mathcal{L}\rangle\,\langle\nu\mathcal{L}| \tag{60}$$

(to avoid arbitrary norms), are collected in Table 1. One observes that the centre $k = 0$ and its vicinity $k = \pm 1$ of the Brillouin zone of pentagon corresponds to two 1-strings, that is to *scattered* states of two magnons, whereas $k = \pm 2$ yields a single 2-string, i.e. the *bound* state.

k	$\nu\mathcal{L}$	$E_{\nu\mathcal{L}}$	$\rho_{\nu\mathcal{L}}$
0	$\begin{array}{\|c\|}\hline 2 \\ \hline -2 \\ \hline \end{array}$	-4	$\frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$
± 1	$\begin{array}{\|c\|}\hline \mp 2 \\ \hline \mp 2 \\ \hline \end{array}$	$-4-\sqrt{5}$	$\frac{1}{3}\begin{pmatrix} 2+\omega^2+\omega^3 & \omega^{\mp 2} \\ \omega^{\pm 2} & 2+\omega+\omega^4 \end{pmatrix}$
± 2	$\begin{array}{\|c\|c\|}\hline \pm 2 & \\ \hline \end{array}$	$-4+\sqrt{5}$	$\frac{1}{3}\begin{pmatrix} 2+\omega+\omega^4 & \omega^{\mp 4} \\ \omega^{\pm 4} & 2+\omega^2+\omega^3 \end{pmatrix}$

Table 1. Rigged string configurations for two-magnon states in pentagonal magnetic ring. The first column gives the quasimomentum k, the second provides the Young diagram $\nu \vdash 2$, with each row being a string, and the leftmost box of each string gives its rigging, as a quasimomentum. The third and fourth column give the eigenvalue E_{2k} and the density matrix $\rho_{\nu\mathcal{L}}$ of the eigenstate, respectively.

Table 1 implies that the solution of the eigenproblem of the Heisenberg Hamiltonian is expressible in the cyclotomic field $\mathbb{Q}(e^{2\pi i/5})$, referred to as the complex Heisenberg field for the pentagon, whereas the spectrum $\operatorname{spec}\hat{H}$ needs the field

$$\mathbb{Q}(\omega+\omega^{-1}) \equiv \mathbb{Q}(\sqrt{5}), \tag{61}$$

the real Heisenberg field. The Galois group

$$G\big(\mathbb{Q}(e^{2\pi i/5})/\mathbb{Q}\big) \cong C_4 \equiv \{\tau_1,\tau_2,\tau_3,\tau_4\}, \tag{62}$$

where τ_l sends $e^{2\pi i/5}$ to $e^{2\pi l i/5}$, $l \in \{\pm 1, \pm 2\}$, permutes eigenvalues and eigenstates of Table 1 in such a way that the interior $\{k = \pm 1, \pm 2\}$ of the Brillouin zone becomes a regular orbit of this group. In other words, the Galois group (62) permutes the eigenstates within the interior of the Brillouin zone, in particular it exchanges bound and scattered eigenstates. In this way, one reaches a unification of BA eigenstates: it is sufficient to know only a representative of each orbit of the Galois group; all other members of this orbit are easily generated just by number-theoretic substitution of appropriate radicals, dictated by an element of the Galois group (in our example, $\tau_l : \omega \longmapsto \omega^l$, $\omega = e^{2\pi i/5}$).

Table 1 demonstrates the exact solution of the eigenproblem of the Heisenberg Hamiltonian, but this solution is not yet given in a form provided by Bethe Ansatz. In particular, it might be not too clear why columns 3 and 4 of this table imply the rigged string configurations of column 2. It is an example of a more general problem. Suppose that one disposes the exact solution of the eigenproblem; how to resolve the corresponding structure of a rigged string configuration? The answer is given by solving the so called inverse Bethe Ansatz [1], [16], [18]. In our case, let

$$a = e^{ip_1}, \quad b = e^{ip_2} \tag{63}$$

be the portions of phase which determine the Bethe Ansatz form (35). Clearly they should satisfy conservation of quasimomentum

$$p_1 + p_2 = \frac{2\pi k}{5} \bmod 2\pi, \tag{64}$$

which yields

$$ab = \omega^{-k}, \tag{65}$$

and conservation of energy

$$a + a^{-1} + b + b^{-1} - 4 = E_k. \tag{66}$$

Eqs. (65) and (66) constitute, for given quasimomentum $k \in B$ and energy E_k (known by the assumption), the system of two equations for unknown a, b. It results in a single quadratic equation, whose roots (a_k, b_k) determine BA eigenstate for each k and E. The discriminant for this equation, namely

$$\Delta_k = \begin{cases} -16 < 0 & \text{for } k = 0 \\ -1 - 2\sqrt{5} < 0 & \text{for } k = \pm 1 \\ -1 + 2\sqrt{5} > 0 & \text{for } k = \pm 2 \end{cases} \tag{67}$$

is not a square in the number field of its coefficients ($\mathbb{Q}$ and $\mathbb{Q}(\omega)$ for the centre $k = 0$, and the interior $k \neq 0$ of the Brillouin zone, respectively), and thus defines new quadratic extensions, $\mathbb{Q}(i)$, $\mathbb{Q}(\omega, \sqrt{\Delta_1})$, and $\mathbb{Q}(\omega, \sqrt{\Delta_2})$, respectively. The number field $B_0' = \mathbb{Q}(\omega, \sqrt{\Delta_1}, \sqrt{\Delta_2})$ is thus responsible for the whole interior of the Brillouin zone. The corresponding Galois group $G(B_0'/\mathbb{Q})$ is an extension of the passive group

$$G(B_0'/\mathbb{Q}(\omega)) \cong C_2 \times C_2 \tag{68}$$

by the active group

$$G(\mathbb{Q}(\omega)/\mathbb{Q}) \cong C_4, \tag{69}$$

in accordance with the short exact sequence [1]

$$1 \to C_2 \times C_2 \to G(B_0'/\mathbb{Q}) \to C_4 \to 1, \tag{70}$$

and can be identified as the $\langle 4, 4 \,|\, 2, 2 \rangle$ group in the Coxeter [5] notation. Within this approach, natural generators a, b, c of $G(B_0'/\mathbb{Q})$ are defined in Table 2 by means of permutations of radicals ω, $\sqrt{\Delta_1}$, $\sqrt{\Delta_2}$ which generate the number field B_0'. The defining relations for the group $G(B_0'/\mathbb{Q})$ are

$$a^4 = b^2 = c^2 = e, \quad bc = cb, \quad ba = ca, \quad ac = ba, \tag{71}$$

and a translation to Coxeter generators R, S is

$$a = R, \quad b = SR^{-1}, \quad c = R^{-1}S. \tag{72}$$

	ω	$\sqrt{\Delta_1}$	$\sqrt{\Delta_2}$
a	ω^2	$\sqrt{\Delta_1}$	$\sqrt{\Delta_2}$
b	ω	$-\sqrt{\Delta_1}$	$\sqrt{\Delta_2}$
c	ω^2	$\sqrt{\Delta_1}$	$-\sqrt{\Delta_2}$

Table 2. Generators of the Galois group $G(B_0'/\mathbb{Q})$, defined by action on radicals ω, $\sqrt{\Delta_1}$, $\sqrt{\Delta_2}$ ($B_0' = \mathbb{Q}(\omega, \sqrt{\Delta_1}, \sqrt{\Delta_2})$).

The number field

$$B = B_0'(i) = \mathbb{Q}(\omega, \sqrt{\Delta_1}, \sqrt{\Delta_2}, i) \tag{73}$$

is the minimal field to express all Bethe parameters, involved in exact solutions for pentagon. It is referred to as *the Bethe number field*. The corresponding Galois group $G(B/\mathbb{Q}) \cong G(B_0'/\mathbb{Q}) \times C_2$ permutes not only the eigenstates and eigenvalues of Table 1 within the whole interior of the Brillouin zone, but also boxes of Young diagrams of the corresponding rigged string configurations, when interpreted as portions of phase, i.e. (a_k, b_k). Remarkably, they interchange bound states $\{2\}$ with the scattered ones $\{1^2\}$, despite evident differences in their physical behaviour. One concludes that Galois symmetries provide a unification of BA solutions.

3. Mutually unbiased bases and number fields of characteristic p

3.1. Complementarity and Weyl–Schwinger shift operators. Let now $h = \mathbb{C}^N \equiv \ell c_{\mathbb{C}}\tilde{N}$ be a qunit, which defines a finite quantum system. In particular, it can be implemented as the subspace $\mathcal{H}^1$ of the space $\mathcal{H}$ of all quantum states of the magnetic ring $\tilde{N}$ (cf. Eq. (11)). We recall that an arbitrary state of such a system is represented by a Hermitian operator $\hat{\rho} \in \operatorname{End} h$ with the trace 1, i.e.

$$\hat{\rho} = \hat{\rho}^\dagger, \quad \operatorname{Trace} \rho = 1. \tag{74}$$

Each operator $\hat{\rho}$ with these properties is referred to as a *density matrix*. In particular, if

$$\hat{\rho}^2 = \hat{\rho}, \tag{75}$$

i.e. ρ is projection operator onto a unit vector $|\psi\rangle \in h$ ($\langle\psi\,|\,\psi\rangle = 1$), that is

$$\rho = |\psi\rangle\,\langle\psi|\,, \tag{76}$$

then $\hat{\rho}$ represents a *pure state*; otherwise $\hat{\rho}$ corresponds to a *mixed state*. An important question of quantum informatics is how to (i) measure, (ii) reconstruct, (iii) perform a tomography, for a quantum state $\hat{\rho}$.

Clearly, an arbitrary operator in $\operatorname{End} h$ is determined by its (complex in general) matrix elements, i.e. $2N^2$ real parameters. Hermicity of $\hat{\rho}$ admits N real diagonal and $N(N-1)$ complex off-diagonal parameters, i.e. N^2 real parameters altogether. The condition for trace yields that an arbitrary state ρ is determined by

$$N^2 - 1 = (N+1)(N-1) \tag{77}$$

independent parameters. They should be measured within a quantum protocol, able to reproduce the state $\hat{\rho}$.

We briefly recall from quantum mechanics (see, e.g. [19]), that a measurement consists there in adjusting a measuring device to an orthonormal basis $|Aa\rangle \in h$, with $a \in \tilde{N}$ and A specifying the adjustment, such that repetition of measurements on an ensemble of qunits in the same state $\hat{\rho}$ yields eventually the outcome of probabilities,

$$(p_1, \ldots, p_r), \quad \sum_{a \in N} p_a = 1, \tag{78}$$

with $p_a \in \mathbb{R}$ being the probability of finding a qunit in the state $|Aa\rangle$. Such a single orthogonal measurement yields thus $N-1$ real parameters. It follows from Eq. (77) that a full reconstruction of the state $\hat{\rho}$ requires $N+1$ independent orthogonal measurements, that is, $N+1$ mutually unbiased bases A (cf. Eq. (32)).

Formally, the states $\left|\tilde{N}, j\right\rangle$, i.e. for $A = \tilde{N}$, have definite positions, whereas $|B, k\rangle$, i.e. for $A = B$, have definite quasimomenta. These two quantities, positions and quasimomenta, are examples of *complementary* variables, which are, according to the concise phrase of Bohr ([4], cf. also [6]), "equally real but mutually exclusive". A formal definition of complementarity stems essentially from Eq. (32) which defines mutually unbiased bases, each basis intimately associated with the corresponding variable. Eq. (32) states, along probabilistic interpretation of quantum mechanics, that, say, if the system is in a state $\hat{\rho} = \left|\tilde{N}, j\right\rangle \left\langle \tilde{N}, j\right|$ with definite position $j \in \tilde{N}$ then the probability of a quasimomentum $k \in B$ in this state, given by $\left|\langle \tilde{N}, j \,|\, B, k\rangle\right|^2$, is equal to $1/N$, for each $k \in B$. In other words, this probability is equally distributed over the Brillouin zone B. The same statement works for appropriate interchange of quasimomenta and positions.

Schwinger [21] introduced another shift operator, $V \in \operatorname{End} h$, corresponding to the basis of quasimomentum, by putting

$$\hat{V}\,|B, k\rangle = |B, (k+1) \bmod B\rangle\,, \quad k \in B, \tag{79}$$

where $(k+1) \bmod B$ is determined by identifying the Brillouin zone B with the Pontryagin dual C_N^* of the cyclic group C_N, generated by the shift operator U. Clearly,

$$\hat{U}\,|B, k\rangle = \omega^k\,|B, k\rangle\,, \quad \hat{V}\left|\tilde{N}, j\right\rangle = \omega^{-j}\left|\tilde{N}, j\right\rangle, \quad \omega = \exp(2\pi i/N), \tag{80}$$

that is, each basis, positional and momentum, is an eigenbasis of the dual Schwinger shift operator, $\hat{V}$ and $\hat{U}$, respectively. Moreover, one has

$$\hat{U}^j \hat{V}^k = \hat{V}^k \hat{U}^j \omega^{-jk}, \quad j \in \tilde{N}, \quad k \in B, \tag{81}$$

which is the version of the Heisenberg uncertainty principle, applied to a qunit as a finite quantum system. Along the Heisenberg picture of quantization, the algebra

$$\operatorname{End} h = \ell c_{\mathbb{C}}\{U^j V^k : j \in \tilde{N}, k \in B\} \cong \ell c_{\mathbb{C}}(\tilde{N} \times B) \tag{82}$$

of all observables of the qunit is spanned — by means of appropriate powers of shift operators U and V — on the classical phase space $\tilde{N} \times B$ of this qunit. This algebra is non-commutative (cf. Eq. (81)), which means that the position j and quasimomentum k of the qunit cannot be measured simultaneously.

Clearly, eigenbases $\left|\tilde{N}, j\right\rangle$ and $|B, k\rangle$ of Schwinger shift operators V and U, respectively, are mutually unbiased. It proves that an arbitrary qunit $h = \mathbb{C}^N$ disposes at least two mutually unbiased bases. But for a full reconstruction of an arbitrary state ρ of such a qunit, one requires $N + 1$ such bases. The question arises whether or not such mutually unbiased bases exist for an arbitrary N. The positive answer is known for the case $N = p^M$, with a prime p. For other integers N, divisible by two or more primes, e.g. 6, 10, 12, 14, 15,..., there is no formal proof, but a strong evidence towards the negative answer.

3.2. Construction of mutually unbiased bases. The construction is easy for a prime N, say $N = p$. Then the eigenbases of the following $p + 1$ operators

$$U, UV, UV^2, \ldots, UV^{p-1}, V, \tag{83}$$

are mutually unbiased.

For $N = p^M$, the qunit $\mathbb{C}^N$ is interpreted as a composite system, along the decomposition

$$\mathbb{C}^N = \mathbb{C}^p \times \mathbb{C}^p \times \ldots \times \mathbb{C}^p, \tag{84}$$

i.e. it is presented as composed of M elementary qupits. In more detail, each element $j \in \tilde{N}$ of the positional basis of the qunit is written in a form

$$j \equiv (j_0, j_1, \ldots, j_{M-1}) \quad \text{iff} \quad j = \sum_{l=0}^{M-1} j_l p^l. \tag{85}$$

Now, instead of ordinary Fourier transform, based on the N-th root of unity, $\omega = \exp(2\pi i/N)$, one uses the Galois–Fourier transform to define the basis

$$|G, k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \gamma^{\ominus k \odot j} \left|\tilde{N}, j\right\rangle, \tag{86}$$

where

$$\gamma = e^{2\pi i/p} \tag{87}$$

is the primitive p-th root of unity, and the symbols $\ominus$, $\oplus$ and $\odot$ denote, respectively, subtraction, addition, and multiplication in the Galois field $GF(p^M)$. In more detail, these operations read

$$a \oplus b = (a_0 + b_0, a_1 + b_1, \ldots, a_{M+1} + b_{M+1}) \tag{88}$$

and

$$a \odot b = a\mathcal{M}_0 b^T, a\mathcal{M}_1 b^T, \ldots, a\mathcal{M}_{M-1} b^T, \tag{89}$$

where $\oplus$ and $+$ denote addition in $GF(p^M)$ and $GF(p) \equiv \mathbb{Z}_p$, respectively, and $\mathcal{M}_m$, $m = 0, 1, \ldots, M-1$ are $M \times M$ matrices with entries in $GF(p)$, which accomplish multiplication $\odot$ in $GF(p^M)$; these matrices depend upon the indecomposable polynomial

$$w(x) = x^M - \sum_{i=0}^{M-1} \mu_i x^i, \tag{90}$$

in $GF(p^M)$, with coefficients $\mu_i \in GF(p)$, which rule the multiplication $\odot$. Here, a and b are row matrices of the form (85), and b^T is the transpose of b. We do not quote the form of matrices $\mathcal{M}_m$ — it is given, e.g., in [6]. In this way, the qunit $\mathbb{C}^N$ is presented as a *composite system*, with M constituents being *qupits* $\mathbb{C}^p$. In particular, both positional basis $\left|\tilde{N}, j\right\rangle$, $j \in \tilde{N}$, and quasimomentum $|G, k\rangle$, $k \in B$, are expressed entirely as M-component vectors with entries in the prime field $GF(p) = \mathbb{Z}_p$.

Now, the shift operators U^l and V^l, defined by

$$\hat{U}^l \left|\tilde{N}, j\right\rangle = \left|\tilde{N}, j \oplus l\right\rangle \tag{91}$$

and

$$\hat{V}^l |G, k\rangle = |G, k \ominus l\rangle, \tag{92}$$

form a basis of a non-commutative algebra over the phase space of the qunit $\mathbb{C}^N$, i.e.

$$\operatorname{End} \mathbb{C}^N = \ell c_{\mathbb{C}}\left\{\hat{U}^j \hat{V}^k : j, k = 0, 1, \ldots, N-1\right\} \cong \ell c_{\mathbb{C}}(\tilde{N} \times B). \tag{93}$$

Moreover, among the set of all $\hat{U}^j \hat{V}^k$ there exists $N+1$ independent subsets

$$U^i = \left\{u_l^i : l = 0, 1, \ldots, N-1\right\}, \quad i = 0, 1, \ldots, N, \tag{94}$$

each of which forms a cyclic group of order N, composed of unitary operators, with the only common unit element $u_0^0 = \mathrm{id}_h$, $h = \mathbb{C}^N$. The corresponding eigenkets

$$\left|e_i^l\right\rangle, \quad i = 0, 1, 2, \ldots, N, \quad l = 0, 1, 2, \ldots, N-1, \tag{95}$$

constitute, for each fixed index i, an orthonormal basis in the qunit $\mathbb{C}^N$, and all these $N+1$ bases are mutually unbiased, that is

$$\left|\langle e_l^i \,|\, e_{l'}^{i'}\rangle\right|^2 = \delta_{ii'}\delta_{ll'} + (1-\delta_{ii'})/N = \begin{cases} \delta_{ll'} & \text{for } i = i' \text{ (orthonormality)}, \\ \frac{1}{N} & \text{otherwise (mutual unbiasedness)}. \end{cases} \tag{96}$$

The construction presented above cannot be extended to N divisible by several primes, since the only existing finite fields have p^M elements.

4. Final remarks and conclusions. We have presented some applications of arithmetic notions in mathematical physics, related to finite quantum systems. We pointed out that eigenproblems of operators with integer matrix entries in the initial (computational) basis yield finite extensions of the prime field $\mathbb{Q}$ of rationals. The associated Galois groups of these extensions acquire a natural dynamical interpretation. A pivotal example is provided by Bethe Ansatz.

Cyclotomic fields of arithmetic are naturally associated with the Fourier transformation from initial basis of positions to that of quasimomenta for finite quantum systems. Further extensions of cyclotomic fields to those generated by the spectrum of arithmetic operators admit a unification of a remarkable amount of exact BA eigenstates: those belonging to an orbit of the corresponding Galois group can be reproduced from a single one by a simple replacement of radicals.

Finite quantum systems of dimension $N = p^M$ dispose a full amount of $N+1$ mutually unbiased bases, necessary for state reconstruction in quantum information processing. The key ingredient is provided by number fields of characteristic p.

References

[1] G. Banaszak, B. Lulek, T. Lulek, J. Milewski, B. Szydło, *Galois symmetries of Bethe parameters for the Heisenberg pentagon*, Rep. Math. Phys. 71 (2013), 205–215.

[2] R. J. Baxter, *Exactly Solved Models in Statistical Physics*, Academic Press, New York 1982.

[3] H. Bethe, *Zur Theorie der Metalle I. Eigenwerte und Eigenfunktionen der linearen Atomkette*, Z. Physik 71 (1931), 205–226 (German); English translation in: *The Many-Body Problem*, D. C. Mattis (ed.), World Sci., Singapore 1993, 689–716.

[4] N. Bohr, *The quantum postulate and the recent development of atomic theory*, Nature 121 (1928), 580–590.

[5] H. M. S. Coxeter, W. O. J. Moser, *Generators and Relations for Discrete Groups*, Springer, Berlin 1957.

[6] T. Durt, B. G. Englert, I. Bengtsson, K. Życzkowski, *On mutually unbiased bases*, Int. J. Quantum Inform. 8 (2010), 535–640.

[7] M. Gaudin, *Le fonction d'onde de Bethe*, Massons, Paris 1983 (French); English transl.: *The Bethe Wavefunction*, Cambridge Univ. Press, Cambridge 2014.

[8] P. Jakubczyk, S. Topolewicz, A. Wal, T. Lulek, *Schwinger geometry, Bethe Ansatz, and a magnonic qudit*, Open Syst. Inf. Dyn. 16 (2009), 221–233.

[9] S. V. Kerov, A. N. Kirillov, N. Yu. Reshetikhin, *Combinatorics, the Bethe Ansatz and representations of the symmetric group* (Russian), Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) 155 (1986), Differentsialnaya Geom., Gruppy Li i Mekh. VIII, 50–64; English transl.: J. Soviet Math. 41 (1988), 916–924.

[10] B. Lulek, D. Jakubczyk, *Homotopy of the classical configuration space for the two-magnon sector of a magnetic Heisenberg ring*, Cent. Eur. J. Phys. 1 (2003), 132–144.

[11] B. Lulek, T. Lulek, M. Łabuz, R. Stagraczyński, *Rigged strings and quasimomenta in Bethe Ansatz*, Physica B 405 (2010), 2654–2658.

[12] B. Lulek, T. Lulek, A. Wal, P. Jakubczyk, *The basis of wavelets for a finite Heisenberg magnet*, Physica B 337 (2003), 375–387.

[13] T. Lulek, *Bethe Ansatz and the geography of rigged strings*, in: Noncommutative Harmonic Analysis with Applications to Probability, Banach Center Publ. 78, Polish Acad. Sci. Inst. Math., Warsaw 2007, 231–247.

[14] T. Lulek, B. Lulek, D. Jakubczyk, P. Jakubczyk, *Rigged strings, Bethe Ansatz, and the geometry of the classical configuration space of the Heisenberg magnetic ring*, Physica B 382 (2006), 162–180.

[15] J. Milewski, G. Banaszak, T. Lulek, *Arithmetic of partial fibres in relative position space of Bethe-Ansatz*, Open Syst. Inf. Dyn. 17 (2010), 89–106.

[16] J. Milewski, G. Banaszak, T. Lulek, M. Łabuz, *Algebraic and geometric properties of Bethe Ansatz eigenfunctions on a pentagonal magnetic ring*, Physica B 406 (2011), 520–526.

[17] J. Milewski, G. Banaszak, T. Lulek, M. Łabuz, R. Stagraczyński, *Galois actions on the eigenproblem of the Heisenberg heptagon*, Open Syst. Inf. Dyn. 19 (2012), no. 2, 1250012.

[18] J. Milewski, B. Lulek, T. Lulek, M. Łabuz, R. Stagraczyński, *Internal parity symmetry and degeneracy of Bethe Ansatz strings in the isotropic heptagonal magnetic ring*, Physica B 434 (2014), 14–20.

[19] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge, 2000.

[20] M. Planat, H. Rosu, *Mutually unbiased phase states, phase uncertainties, and Gauss sums*, Europ. Phys. J. D 36 (2005), 133–139.

[21] J. Schwinger, *Quantum Kinematics and Dynamics*, Benjamin, New York 1970.

[22] M. Takahashi, *One-dimensional Heisenberg model at finite temperature*, Progr. Theor. Phys. 46 (1971), 401–415.

[23] A. Vourdas, *Quantum systems with finite Hilbert space: Galois fields in quantum mechanics*, J. Phys. A 40 (2007), R285–R331.

[24] H. Weyl, *Gruppentheorie und Quantenmechanik*, Hirzel, Leipzig 1928 (in German); English transl.: Dover, New York 1932.

[25] W. K. Wootters, *A Wigner-function formulation of finite-state quantum mechanics*, Ann. Phys. 176 (1987), 1–21.

[26] W. K. Wootters, *Quantum measurements and finite geometry*, Found. Phys. 36 (2006), 112–126.

[27] W. K. Wootters, B. K. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. Phys. 191 (1989), 363–381.

[28] C. N. Yang, C. P. Yang, *Ground-state energy of a Heisenberg–Ising lattice*, Phys. Rev. 147 (1966), 303–306.