Quantum Science and Technology

Apostolos Vourdas

Finite and Profinite Quantum Systems

Springer

Quantum Science and Technology

Aims and Scope

The book series Quantum Science and Technology is dedicated to one of today's most active and rapidly expanding fields of research and development. In particular, the series will be a showcase for the growing number of experimental implementations and practical applications of quantum systems. These will include, but are not restricted to: quantum information processing, quantum computing, and quantum simulation; quantum communication and quantum cryptography; entanglement and other quantum resources; quantum interfaces and hybrid quantum systems; quantum memories and quantum repeaters; measurement-based quantum control and quantum feedback; quantum nanomechanics, quantum optomechanics and quantum transducers; quantum sensing and quantum metrology; as well as quantum effects in biology. Last but not least, the series will include books on the theoretical and mathematical questions relevant to designing and understanding these systems and devices, as well as foundational issues concerning the quantum phenomena themselves. Written and edited by leading experts, the treatments will be designed for graduate students and other researchers already working in, or intending to enter the field of quantum science and technology.

More information about this series at http://www.springer.com/series/10039

Apostolos Vourdas

Finite and Profinite Quantum Systems

Springer

Apostolos Vourdas
Department of Computer Science
University of Bradford
Bradford
UK

ISSN 2364-9054 ISSN 2364-9062 (electronic)
Quantum Science and Technology
ISBN 978-3-319-59494-1 ISBN 978-3-319-59495-8 (eBook)
DOI 10.1007/978-3-319-59495-8

Library of Congress Control Number: 2017944304

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Quantum mechanics is usually studied for systems where the position and momentum take all real values. Weyl and later Schwinger studied quantum systems where the position and momentum take a finite number of values. The emergence of the subject of quantum information created a lot of interest in such systems, which became known as qudits. This research is interdisciplinary and combines ideas from mathematics, physics, computer science, chemistry, and materials science. Within this general area, the so-called problem of mutually unbiased bases led to the study of quantum systems with variables in Galois fields. The monograph discusses various aspects of these 'finite quantum systems.'

It also considers rigorously the limit where the dimension of the system becomes very large using ideas from the timely area of profinite groups. These 'profinite quantum systems' have links to a different area of research, known as p-adic physics. The latter studies quantum systems with variables which are p-adic numbers and combines algebraic number theory with quantum physics. It has applications in condensed matter, particle physics, string theory, etc. The monograph approaches this area from a different angle, using inverse and direct limits and profinite groups.

I have a strong interest in all these areas, and I have written three review articles on finite quantum systems (in 2004), on systems with variables in Galois fields (in 2007), and on systems with variables which are p-adic numbers (in 2013). They are the background for this monograph, but the material is completely rewritten, some gaps have been filled, and other topics such as finite geometries, mutually unbiased bases, weak mutually unbiased bases, and quantum logic have been added.

Overall, the aim of this monograph is to present the material by adding a novel flavor to it (as discussed in section 1.4 below). The presentation is concise but informative, and the general theory is complemented with examples. The level of rigor is appropriate for a mathematical physics monograph. The proofs describe the important steps, so that the reader can easily fill the gaps.

The monograph is suitable for Ph.D. students and other researchers in quantum physics, quantum optics, quantum information, p-adic physics, mathematical

physics, applied mathematics, and computer science. The reader is expected to have some knowledge of certain mathematical areas, as follows:

- In Chap. 5, about finite geometries.
- In Chap. 6, about lattice theory.
- In Chaps. 8 and 9 about Galois theory.
- In Chaps. 10, 11, and 12 about p-adic numbers, profinite groups, and inverse and direct limits.

There is a brief introduction to these concepts in the monograph (with references to the literature), but the aim is to establish the notation and explain how to do practical calculations. So some prior knowledge of these topics will be helpful.

I would like to thank some of my ex-Ph.D. students Dr. C. Lei, Dr. S. Zhang, Dr. L. Wang, Dr. H. Al Hadhrami, Dr. M. Shalaby, Dr. S. Oladejo, Dr. P. Evangelides, and Dr. T. Olupitan, who worked with me on related problems. I would also like to thank Tom Spicer and Cindy Zitter from Springer, and the referee, for their encouragement and support.

Bradford, UK Apostolos Vourdas
April 2017

Contents

1 Introduction 1
1.1 Finite Quantum Systems 1
1.2 Profinite Quantum Systems 2
1.3 Brief Overview. 2
1.4 Aim of the Monograph 4
References 5

2 Partial Orders and Pontryagin Duality 7
2.1 Partial Orders 7
2.2 The Directed-Complete Partial Order of Supernatural (Steinitz) Numbers 8
2.3 Pontryagin Duality 9
References 10

3 The Ring $\mathbb{Z}(\boldsymbol{d})$ 11
3.1 The Ring $\mathbb{Z}(d)$ and its Characters 11
3.1.1 Quadratic Gauss Sums 12
3.1.2 Totient Functions and the Dedekind psi Function 12
3.1.3 Invertible and Non-invertible Elements in $\mathbb{Z}(d)$ 13
3.2 Factorization of the Ring $\mathbb{Z}(d)$ Based on the Chinese Remainder Theorem 14
3.3 The Symplectic Group $Sp[2, \mathbb{Z}(d)]$ 16
3.4 Factorization of the Symplectic Group $Sp[2, \mathbb{Z}(d)]$ Based on the Chinese Remainder Theorem 17
References 21

4 Quantum Systems with Variables in $\mathbb{Z}(\boldsymbol{d})$ 23
4.1 Fourier Transforms in $\Sigma[\mathbb{Z}(d)]$ 23
4.2 Time Evolution 25
4.3 The Heisenberg-Weyl Group $HW[\mathbb{Z}(d)]$ 26

4.4 Coherence in Finite Quantum Systems 29
4.4.1 Coherent States 29
4.4.2 Coherent Density Matrices 30
4.4.3 Coherent Projectors of Rank n 31
4.5 Symplectic Transformations and the $Sp[2, \mathbb{Z}(d)]$ Group 33
4.6 The $HWSp[\mathbb{Z}(d)]$ Group of Displacements and Symplectic Transformations 36
4.7 Parity Operators 37
4.8 Wigner and Weyl Functions 41
4.9 Factorization of $\Sigma[\mathbb{Z}(d)]$ Based on the Chinese Remainder Theorem 46
4.10 Analytic Representation of Finite Quantum Systems 49
References 53

5 Finite Geometries and Mutually Unbiased Bases 57
5.1 The $\mathbb{Z}(d) \times \mathbb{Z}(d)$ as a Non-near-linear Finite Geometry 58
5.1.1 Symplectic Transformations in the Finite Geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$ 59
5.1.2 Factorization of the Finite Geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$ Based on the Chinese Remainder Theorem 61
5.2 Mutually Unbiased Bases 64
5.2.1 Mutually Unbiased Bases in $H[\mathbb{Z}(p)]$ 65
5.3 Weak Mutually Unbiased Bases and Duality with Finite Geometries 68
5.4 Other Topics 74
References 75

6 Quantum Logic of Finite Quantum Systems 77
6.1 Classical Logic: Boolean Algebras 78
6.1.1 Boolean Rings 80
6.1.2 Classical Gates 81
6.2 The Modular Orthocomplemented Lattice $\mathfrak{L}(d)$ 83
6.2.1 Quantum Versus Classical Disjunction 83
6.2.2 Projectors to the Subspaces 84
6.2.3 The Modularity Property of $\mathfrak{L}(d)$ 85
6.2.4 Non-distributivity of the Lattice $\mathfrak{L}(d)$ 86
6.2.5 Transpose Intervals in the Lattice $\mathfrak{L}(d)$ 87
References 91

7 Applications 93
7.1 Angle States and Angular Momentum States 93
7.1.1 The Schwinger Representation 95
7.1.2 Angle States and Angular Momentum States in $\mathscr{H}_B$ 96
7.1.3 Area Preserving Diffeomorphisms on a Sphere 97

7.2 Interferometry in Multimode Systems . . . 100
7.2.1 Fourier Interferometry and Applications to Metrology . . . 101
7.2.2 Other Types of Interferometry . . . 102
7.3 Orbital Angular Momentum States . . . 103
7.4 Other Applications . . . 104
References . . . 104

8 Galois Fields . . . 107
8.1 The Galois Field $GF(p^e)$ . . . 107
8.2 Subfields of $GF(p^e)$ and Galois Groups . . . 108
8.3 Trace and Characters . . . 111
8.4 General Bases in $GF(p^e)$ . . . 116
References . . . 117

9 Quantum Systems with Variables in $GF(p^e)$ . . . 119
9.1 Fourier Transforms in $\Sigma[GF(p^e)]$ . . . 120
9.1.1 Change of the Basis in $GF(p^e)$ . . . 122
9.1.2 Comparison of the System $\Sigma[GF(p^e)]$ with the System $\Sigma\{[\mathbb{Z}(p)]^e\}$ . . . 122
9.2 Frobenius Transformations . . . 123
9.3 The Heisenberg-Weyl Group $HW[GF(p^e)]$ . . . 127
9.4 Symplectic Transformations and the $Sp[2, GF(p^e)]$ Group . . . 131
9.5 Parity Operators and Wigner and Weyl Functions . . . 136
9.6 Hamiltonians of Galois Quantum Systems and Time Evolution . . . 137
9.6.1 Example . . . 138
9.6.2 Galois Systems with Frobenius Symmetry . . . 139
9.7 Mutually Unbiased Bases in $H[GF(p^e)]$ and Duality to $GF(p^e) \times GF(p^e)$ . . . 140
9.7.1 The Finite Geometry $GF(p^e) \times GF(p^e)$ . . . 141
References . . . 142

10 *p*-adic Numbers and Profinite Groups . . . 145
10.1 The Field $\mathbb{Q}_p$ and the Ring $\mathbb{Z}_p$ . . . 145
10.1.1 Absolute Values of p-adic Numbers . . . 146
10.1.2 Additive Characters . . . 147
10.2 $\mathbb{Q}_p/\mathbb{Z}_p$ as the Pontryagin Dual Group of $\mathbb{Z}_p$ . . . 147
10.3 The Group $\widehat{\mathbb{Z}}$ . . . 148
10.4 $\mathbb{Q}/\mathbb{Z}$ as the Pontryagin Dual Group of $\widehat{\mathbb{Z}}$ . . . 149
10.4.1 Additive Characters . . . 150
10.4.2 The Directed-Complete Partial Order of Subgroups of $\mathbb{Q}/\mathbb{Z}$ . . . 151
10.5 Inverse and Direct Limits . . . 152

10.6 The Profinite Group $\mathbb{Z}_p$ as Inverse Limit . . . 153
10.6.1 $\mathbb{Z}_p$ as a Compact and Totally Disconnected Topological Group . . . 154
10.7 $\mathbb{Q}_p/\mathbb{Z}_p$ as Direct Limit . . . 155
10.8 A Complete Chain of Pontryagin Dual Pairs of Groups . . . 156
10.9 The Profinite Group $\widehat{\mathbb{Z}}_p$ as Inverse Limit . . . 157
10.9.1 $\widehat{\mathbb{Z}}_p$ as a Compact and Totally Disconnected Topological Group . . . 158
10.10 $\mathbb{Q}/\mathbb{Z}$ as Direct Limit . . . 159
10.11 A Directed-Complete Partial Order of Pontryagin Dual Pairs of Groups . . . 160
References . . . 160

11 A Quantum System with Positions in the Profinite Group $\mathbb{Z}_p$ . . . 161
11.1 Locally Constant Functions with Compact Support . . . 161
11.2 Integrals of Complex Functions on $\mathbb{Q}_p$ . . . 162
11.3 Integrals of Complex Functions on $\mathbb{Q}_p/\mathbb{Z}_p$ and Weil Transforms . . . 164
11.3.1 Weil Transforms . . . 166
11.3.2 Delta Functions . . . 167
11.4 The Quantum System $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ . . . 168
11.5 The Heisenberg-Weyl Group $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ . . . 170
11.5.1 $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ as a Locally Compact and Totally Disconnected Topological Group . . . 170
11.6 Wigner and Weyl Functions . . . 173
11.7 The Complete Chain of Subsystems of $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ . . . 178
References . . . 179

12 A Quantum System with Positions in the Profinite Group $\widehat{\mathbb{Z}}$ . . . 181
12.1 The System $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ . . . 181
12.2 Fourier Transforms . . . 183
12.2.1 Change of Variables . . . 184
12.3 The Heisenberg-Weyl Group $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ . . . 185
12.3.1 $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ as a Locally Compact and Totally Disconnected Topological Group . . . 186
12.4 Wigner and Weyl Functions . . . 188
12.5 The Directed-Complete Partial Order of Subsystems of $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ . . . 192
12.6 Other Topics . . . 192
References . . . 192

Index . . . 195

Mathematical Symbols

$\mathbb{R}$	Real numbers
$\mathbb{Q}$	Rational numbers
$\mathbb{Z}$	Integers
$\mathbb{Z}^+$ or $\mathbb{N}$	Natural numbers
$\mathbb{Z}_0^+$	Positive integers and zero
$\mathbb{R}/\mathbb{Z}$	Real numbers on a circle
$\mathbb{Z}(d)$	Integers modulo d
$[\mathbb{Z}(d)]^*$	Group of reduced residue classes modulo d (invertible elements of $\mathbb{Z}(d)$)
$\varphi(d)$	Euler's totient function
$J_k(d)$	Jordan totient function
$\psi(d)$	Dedekind psi function
Π	Set of prime numbers
$\prec$	Partial order (the same symbol is used for different partial orders, e.g., divisor, subset, subgroup, and subsystem.)
$k\|n$ or $k \prec n$	k is a divisor of n (the partial order is divisibility)
$\triangleleft$	Normal subgroup
$\Pi(\lambda)$	Set of prime numbers which are divisors of λ
$\mathrm{GCD}(\rho, \sigma)$	Greatest common divisor
$\mathbb{N}_S$	The directed complete partial order of supernatural (Steinitz) numbers
$\mathbb{N}_S(p)$	The complete chain $\{p, p^2, \ldots, p^\infty\}$
Υ	$\prod_{p\in\Pi} p^\infty$ (the supremum element of $\mathbb{N}_S$)
$\mathscr{E}$	$\prod_{p\in\Pi} p$ (element of $\mathbb{N}_S$)
$\widetilde{G}$	Pontryagin dual group to G
$C(d) \cong \mathbb{Z}(d)$	Pontryagin dual group to $\mathbb{Z}(d)$
$GF(p^e)$	Galois field
$\Sigma[\mathbb{Z}(d)]$	Quantum system with positions and momenta in $\mathbb{Z}(d)$

$\omega_d(\alpha) = \omega(\alpha)$	$\exp\left(i\frac{2\pi\alpha}{d}\right); \quad \alpha \in \mathbb{Z}(d)$
$H[\mathbb{Z}(d)]$	d-dimensional Hilbert space of the system $\Sigma[\mathbb{Z}(d)]$
$\lvert X; m\rangle; \quad m \in \mathbb{Z}(d)$	Position states in $H[\mathbb{Z}(d)]$
$\lvert P; m\rangle; \quad m \in \mathbb{Z}(d)$	Momentum states in $H[\mathbb{Z}(d)]$
$D(\alpha, \beta); \quad \alpha, \beta \in \mathbb{Z}(d)$	Displacement operators for $\Sigma[\mathbb{Z}(d)]$
$P(\alpha, \beta); \quad \alpha, \beta \in \mathbb{Z}(d)$	Parity operators for $\Sigma[\mathbb{Z}(d)]$
$HW[\mathbb{Z}(d)]$	Heisenberg–Weyl group for the system $\Sigma[\mathbb{Z}(d)]$
$\lvert C; \alpha, \beta\rangle; \quad \alpha, \beta \in \mathbb{Z}(d)$	Coherent states in $H[\mathbb{Z}(d)]$ (C indicates coherent states)
$S(\kappa, \lambda \lvert \mu, \nu)\ \kappa, \lambda, \mu, \nu \in \mathbb{Z}(d)$	Symplectic transformations for the system $\Sigma[\mathbb{Z}(d)]$ $\kappa\nu - \lambda\mu = 1$
$Sp[2, \mathbb{Z}(d)]$	Symplectic group for the system $\Sigma[\mathbb{Z}(d)]$
$\lvert X(\mu, \nu); m\rangle$	$\lvert X(\mu, \nu); m\rangle = S(\kappa, \lambda \lvert \mu, \nu) \lvert X; m\rangle$ in $H[\mathbb{Z}(d)]$
$\lvert P(\kappa, \lambda); m\rangle$	$\lvert P(\kappa, \lambda); m\rangle = S(\kappa, \lambda \lvert \mu, \nu) \lvert P; m\rangle$ in $H[\mathbb{Z}(d)]$
$HWSp[\mathbb{Z}(d)]$	The group $HW[\mathbb{Z}(d)] \rtimes Sp[2, \mathbb{Z}(d)]$ of displacements and symplectic transformations for the system $\Sigma[\mathbb{Z}(d)]$
$W(\alpha, \beta; \theta); \quad \alpha, \beta \in \mathbb{Z}(d)$	Wigner function of the operator θ, for $\Sigma[\mathbb{Z}(d)]$
$\widetilde{W}(\alpha, \beta; \theta); \quad \alpha, \beta \in \mathbb{Z}(d)$	Weyl function of the operator θ, for $\Sigma[\mathbb{Z}(d)]$
$L(\rho, \sigma)\ \rho, \sigma \in \mathbb{Z}(d)$	Line through the origin in the $\mathbb{Z}(d) \times \mathbb{Z}(d)$ finite geometry (unfactorized notation)
$\mathscr{L}(v_1, v_2)$	Line through the origin in the $\mathbb{Z}(p_1 p_2) \times \mathbb{Z}(p_1 p_2)$
$v_i = -1, \ldots p_i - 1$	finite geometry (factorized notation)
$\lvert \mathscr{X}(v_1, v_2); \overline{m}_1, \overline{m}_2\rangle$	Weak mutually unbiased bases in $H[\mathbb{Z}(p_1 p_2)]$
$v_i = -1, \ldots p_i - 1$	(factorized notation)
$\wedge$	Conjunction (logical AND)
$\vee$	Disjunction (logical OR)
$\neg$	Negation (logical NOT)
$\uparrow$	Logical NAND
$\downarrow$	Logical NOR
$\Sigma[GF(p^e)]$	Quantum system with positions and momenta in $GF(p^e)$
$\Omega(s)$	$\exp\left(i\frac{2\pi s}{e}\right); \quad s \in \mathbb{Z}(e)$
$H[GF(p^e)]$	p^e-dimensional Hilbert space of the $\Sigma[GF(p^e)]$
$\lvert X; m\rangle; \quad m \in GF(p^e)$	Position states in $H[GF(p^e)]$
$\lvert P; m\rangle; \quad m \in GF(p^e)$	Momentum states in $H[GF(p^e)]$
$D(\alpha, \beta) \alpha, \beta \in GF(p^e)$	Displacement operators for $\Sigma[GF(p^e)]$
$HW[GF(p^e)]$	Heisenberg–Weyl group for $\Sigma[GF(p^e)]$
$P(\alpha, \beta) \alpha, \beta \in GF(p^e)$	Parity operators for $\Sigma[GF(p^e)]$
$S(\kappa, \lambda \lvert \mu, \nu)$	Symplectic transformations for $\Sigma[GF(p^e)]$
$\kappa, \lambda, \mu, \nu \in GF(p^e)$	$\kappa\nu - \lambda\mu = 1$
$Sp[2, GF(p^e)]$	Symplectic group for the system $\Sigma[GF(p^e)]$
$HWSp[GF(p^e)]$	The group $HW[GF(p^e)] \rtimes Sp[2, GF(p^e)]$ of displacements and symplectic transformations for $\Sigma[GF(p^e)]$

$\mathscr{G}$	Frobenius transformations for $\Sigma[GF(p^e)]$
$\mathrm{Gal}(e\|1)$	Galois group of Frobenius transformations for $\Sigma[GF(p^e)]$
$HWGal[GF(p^e)]$	The group $HW[GF(p^e)] \rtimes Gal[GF(p^e)]$ of displacements and Frobenius transformations for $\Sigma[GF(p^e)]$
$SpGal[GF(p^e)]$	The group $Sp[2, GF(p^e)] \rtimes Gal[GF(p^e)]$ of symplectic and Frobenius transformations for $\Sigma[GF(p^e)]$
$HWSpGal[GF(p^e)]$	The group $HWSp[GF(p^e)] \rtimes Gal[GF(p^e)]$ of displacements and symplectic and Frobenius transformations for $\Sigma[GF(p^e)]$
$\mathbb{Q}_p$	p-adic numbers
$\mathbb{Z}_p$	p-adic integers
$\mathbb{Q}_p/\mathbb{Z}_p$	Fractional p-adic numbers
$C(p^\infty) \cong \mathbb{Q}_p/\mathbb{Z}_p$	Prüfer group
$\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$	Quantum system with positions in $\mathbb{Z}_p$ and momenta in $\widetilde{\mathbb{Z}_p} \cong \mathbb{Q}_p/\mathbb{Z}_p$
$\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$	The Schwartz–Bruhat space for $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$
$\mathbf{LC}[f_p(a_p)]$	Degree of local constancy of a complex function $f_p(a_p)$ with $a_p \in \mathbb{Q}_p$
$\mathbf{CS}[f_p(a_p)]$	Degree of compact support of a complex function $f_p(a_p)$ with $a_p \in \mathbb{Q}_p$
$\mathscr{A}_p(k, n)$	Set of functions on $\mathbb{Q}_p$ with $\mathbf{CS}[f_p(a_p)] = k$ and $\mathbf{LC}[f_p(a_p)] = n$
$\mathscr{A}_p(k, *)$	$\bigcup_n \mathscr{A}_p(k, n)$
$\mathscr{A}_p(*, n)$	$\bigcup_k \mathscr{A}_p(k, n)$
$\mathscr{A}_p$	$\bigcup_{k,n} \mathscr{A}_p(k, n)$
$D_p(\mathfrak{a}_p, b_p)$ $\mathfrak{a}_p \in \mathbb{Q}_p/\mathbb{Z}_p; \quad b_p \in \mathbb{Z}_p$	Displacement operators for $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$
$HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$	Heisenberg–Weyl group for the system $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$
$\mathbb{Q}/\mathbb{Z} \cong \sum_{p \in \Pi} \mathbb{Q}_p/\mathbb{Z}_p$	Rational numbers on a circle
$\widehat{\mathbb{Z}}$	$\prod_{p \in \Pi} \mathbb{Z}_p$
$\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$	System with positions in $\widehat{\mathbb{Z}}$ and momenta in $\widetilde{\widehat{\mathbb{Z}}} \cong \mathbb{Q}/\mathbb{Z}$
$\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$	The Schwartz–Bruhat space for $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$
$D(\mathfrak{a}, b)$ $\mathfrak{a} \in \mathbb{Q}/\mathbb{Z}; \quad b \in \widehat{\mathbb{Z}}$	Displacement operators for $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$
$HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$	Heisenberg–Weyl group of displacements for $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$

Chapter 1
Introduction

Abstract This chapter presents the contents of this monograph, and highlights its novel flavour.

Quantum mechanics is usually studied for systems where both position and momentum take values in $\mathbb{R}$. However more generally, the position can take values in an Abelian locally compact group G, and the momentum in its Pontryagin dual group $\widetilde{G}$ [1–3]. Pontryagin duality between two groups which are used for positions and momenta, is the fundamental starting point for quantum mechanics (and harmonic analysis). In this monograph G is one of the finite or profinite groups discussed below.

1.1 Finite Quantum Systems

We study quantum mechanics on the following finite groups:

- $G \cong \widetilde{G} = \mathbb{Z}(d)$: We study a quantum system with variables in the ring $\mathbb{Z}(d)$, and denote it as $\Sigma[\mathbb{Z}(d)]$ [4–7]. In quantum information this system is called qudit. Genuine examples of such systems are spins. Other examples are infinite-dimensional systems, which due to low energy operate in the lowest d states. In this case the infinite-dimensional system is approximated with a finite-dimensional quantum system. Superconducting qubits are examples of this.
  In the case that $d = p$ (where p is a prime number), $\mathbb{Z}(p)$ is a field and has stronger properties than a ring. Consequently the corresponding systems $\Sigma[\mathbb{Z}(p)]$ have stronger properties (e.g., in relation to mutually unbiased bases) which are discussed in this monograph.
- $G \cong \widetilde{G} = GF(p^e)$: Apart from $\mathbb{Z}(p)$, the Galois fields $GF(p^e)$ are also finite fields. Quantum systems with variables in $GF(p^e)$, are denoted as $\Sigma[GF(p^e)]$

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_1

and are called Galois quantum systems [8]. They inherit Galois structure (e.g., Frobenius transformations and the Galois group), and have other desirable properties (e.g., in relation to mutually unbiased bases).

We call the systems $\Sigma[\mathbb{Z}(d)]$ and $\Sigma[GF(p^e)]$, finite quantum systems.

1.2 Profinite Quantum Systems

Profinite groups are groups at the edge of very large finite groups. The concept of inverse limit defines this in a rigorous manner. Topologically, they are totally disconnected (an intermediate concept between discrete and continuous). We consider the following profinite groups:

- $G = \mathbb{Z}_p$ and $\widetilde{G} = \mathbb{Q}_p/\mathbb{Z}_p$: The profinite group $\mathbb{Z}_p$ of p-adic integers, can be viewed as the group $\mathbb{Z}(p^e)$, with very large e. Its Pontryagin dual group is the group of fractional p-adic numbers $\mathbb{Q}_p/\mathbb{Z}_p$. We study a quantum system with positions in $\mathbb{Z}_p$ and momenta in $\mathbb{Q}_p/\mathbb{Z}_p$, and denote it $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ [9–11]. It can be viewed as a quantum system $\Sigma[\mathbb{Z}(p^e)]$ with very large e, in the following sense. The set of systems $\Sigma[\mathbb{Z}(p^e)]$ with the order 'subsystem', is a chain. This chain is not complete, but it becomes complete if we add the $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ to it.
- $G = \widehat{\mathbb{Z}}$ and $\widetilde{G} = \mathbb{Q}/\mathbb{Z}$: The profinite group $\widehat{\mathbb{Z}}$, can be viewed as the group $\mathbb{Z}(d)$, with very large d. Its Pontryagin dual group is the group $\mathbb{Q}/\mathbb{Z}$ of rational numbers on a circle. We study a quantum system with positions in $\widehat{\mathbb{Z}}$ and momenta in $\mathbb{Q}/\mathbb{Z}$, and denote it $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ [9–11]. It can be viewed as a quantum system with variables in $\Sigma[\mathbb{Z}(d)]$ with very large d, in the following sense. The set of the systems $\Sigma[\mathbb{Z}(d)]$ with the order 'subsystem', is a directed partial order. It becomes a directed-complete partial order, if we add the $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ (and also some other systems as discussed later) to it.

We call the $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ and $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, profinite quantum systems.

1.3 Brief Overview

We describe briefly the content of each chapter.

In Chap. 2, we present some background material on partial orders. In particular we consider the set $\mathbb{N}$ of natural numbers, which with the order divisibility, is a directed partial order. We add 'top elements' to it, and extend it into the set of supernatural (Steinitz) numbers, which is a directed-complete partial order. We also present briefly some aspects of Pontryagin duality.

In Chap. 3, we discuss the ring $\mathbb{Z}(d)$ and its factorization in terms of smaller rings, which is based on the Chinese remainder theorem. We also discuss the symplectic group $Sp[2, \mathbb{Z}(d)]$ and its factorization in terms of smaller symplectic groups based on the Chinese remainder theorem.

In Chap. 4, we study quantum systems $\Sigma[\mathbb{Z}(d)]$, with variables in $\mathbb{Z}(d)$. There are technical differences in the two cases that d is odd or even integer. In this monograph we consider the case that d is an odd integer. We discuss various phase space methods in this context. The phase space is the toroidal lattice $\mathbb{Z}(d) \times \mathbb{Z}(d)$, and in it we study displacements and the Heisenberg-Weyl group $HW[\mathbb{Z}(d)]$, and symplectic transformations and the $Sp[2, \mathbb{Z}(d)]$ group. We also study coherent states, Wigner functions, and Weyl functions, in this context. Using the factorization of the ring $\mathbb{Z}(d)$ in terms of smaller rings, the system $\Sigma[\mathbb{Z}(d)]$ is factorized in terms of smaller systems. An analytic representation of the quantum states, that uses Theta functions, is also discussed.

In Chap. 5, we discuss the phase space $\mathbb{Z}(d) \times \mathbb{Z}(d)$ as a finite geometry [12–14]. We also discuss mutually unbiased bases [15–17]. They have important applications in quantum communications and quantum cryptography, and their study involves deep problems in discrete mathematics. We consider the following cases:

- For $d = p$ (where p is a prime number), $\mathbb{Z}(p) \times \mathbb{Z}(p)$ is a near-linear finite geometry (two lines have at most one point in common). In this case, the number of mutually unbiased bases is $p + 1$, and there is a duality between them and the $p + 1$ lines through the origin in $\mathbb{Z}(p) \times \mathbb{Z}(p)$.
- For $d = p^e$ (a power of prime number), the discussion on mutually unbiased bases involves the Galois field $GF(p^e)$, and is presented later in Chap. 9.
- For d which is not a prime number or a power of prime number, it is difficult to find the maximum number of mutually unbiased bases. In this case the $\mathbb{Z}(d) \times \mathbb{Z}(d)$ is a non-near-linear finite geometry (two lines have many points in common). Motivated by a desire to have a duality between bases and lines, we discuss a weaker concept which we call weak mutually unbiased bases [18–20].

Overall, Chap. 5 discusses mutually unbiased bases and their generalizations, and their duality to lines in the finite geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$.

In Chap. 6, we discuss the quantum logic of finite quantum systems. The discussion starts with Boolean algebras and Boolean rings describing classical logic, and classical computation. We then discuss the Birkhoff-von Neumann lattice [21–25], which describes the quantum logic, and which for systems with finite-dimensional Hilbert space, is a modular orthocomplemented lattice.

In Chap. 7, we discuss applications of the formalism of finite quantum systems. They include angle and angular momentum states, interferometry of multimode systems, orbital angular momentum states, etc. Each of these topics is a subject in its own right, and the intention is to define the basic quantities and provide a guide to the literature.

In Chap. 8, we present background material from Galois theory, which is needed later. The emphasis is on how to do practical calculations with Galois numbers.

In Chap. 9, we discuss the Galois quantum systems $\Sigma[GF(p^e)]$. Many of the properties of these systems are similar to those of the finite quantum systems $\Sigma[\mathbb{Z}(d)]$. The emphasis in our presentation is on extra 'Galois properties' that they have, like the Frobenius transformations and the Galois group. We also discuss mutually unbiased bases in these systems.

In Chap. 10, we present background material from p-adic numbers and profinite groups, which is needed later. We explain that the Pontryagin dual group to $\mathbb{Z}_p$ is the $\mathbb{Q}_p/\mathbb{Z}_p$, and the Pontryagin dual group to $\widehat{\mathbb{Z}}$ is $\mathbb{Q}/\mathbb{Z}$. The inverse and direct limits are central concepts, for these discussions. The emphasis is on how to do practical calculations with p-adic numbers.

In Chap. 11, we discuss the quantum system $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. Using the theory of profinite groups and inverse and direct limits, we show rigorously that the $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ can be viewed as the system $\Sigma[\mathbb{Z}(p^e)]$ in the limit of large e. We discuss the concepts of locally constant functions, and functions with constant support, which are designed to make integrals to converge. We also define the Schwartz-Bruhat space $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ of wavefunctions, and then Fourier transforms, the Heisenberg-Weyl group $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, and Wigner and Weyl functions. It is shown that the $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ is a totally disconnected and locally compact topological group.

In Chap. 12, we discuss the quantum system $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$. Using the theory of profinite groups and inverse and direct limits, we show that the $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ can be viewed as the system $\Sigma[\mathbb{Z}(d)]$ in the limit of large d. We show that the Schwartz-Bruhat space $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ of wavefunctions is the restricted tensor product of all the Schwartz-Bruhat spaces $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ with all prime p (this is the tensor product with an extra restriction). We also discuss Fourier transforms, the Heisenberg-Weyl group $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, and Wigner and Weyl functions. It is shown that the $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ is the restricted direct product of the Heisenberg-Weyl groups $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ with all prime p (this is the direct product with an extra restriction). The $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ is a totally disconnected and locally compact topological group.

1.4 Aim of the Monograph

The aim of the monograph, is to present the above described material, by adding a novel flavor to it. In addition to the standard material, we emphasize some topics which either have not been discussed extensively in the literature, or they have been discussed from a different angle to the one presented here. The choice of such topics is of course subjective, and we briefly highlight them below, firstly in the context of Quantum Mechanics and Quantum Information [26–28] and secondly in the context of p-adic Physics [10, 11, 29–31].

1. **Quantum Mechanics and Quantum Information**:
   - Within the formalism of qudits, we highlight the following:
     - The study of coherent states in finite quantum systems, and generalizations like coherent density matrices, and coherent projectors of rank n.
     - The factorization of the quantum system $\Sigma[\mathbb{Z}(d)]$ in terms of smaller quantum systems. This is based on the Chinese remainder theorem.

  - The study of the $\mathbb{Z}(d) \times \mathbb{Z}(d)$ phase space, as a finite geometry. It is a near-linear finite geometry when d is a prime number, and a non-near-linear finite geometry when d is not a prime number.
  - Within the formalism of mutually unbiased bases, which has been studied extensively in the literature, we also discuss a weaker concept called weak mutually unbiased bases, and emphasize their duality to the finite geometry of the phase space.
- Finite quantum systems with variables in Galois fields, have been used in mutually unbiased bases for systems with power of prime dimension. Here we study them as a subject in its own right, with emphasis on Frobenius transformations and the Galois group, which are the pillars of the Galois structure. Groups that combine Frobenius transformations with displacements and symplectic transformations, are also discussed.
- We discuss quantum logic for finite quantum systems, and compare and contrast it with classical logic. Logic is the heart of (classical and quantum) computer science, and it provides a language for the algebraic description of circuits with classical and quantum gates.

2. **p-adic Physics**: p-adic numbers have been used in various branches of Physics: string theory, condensed matter, etc. In Chaps. 10, 11 and 12 we present a rigorous approach to the study of finite quantum systems, as the dimension goes to infinity. This part of the monograph belongs to the subject of 'p-adic Physics', but we approach this area from a different angle, using the theory of profinite groups and inverse and direct limits. The concept 'profinite' is extended from groups to quantum systems. We show that:

   - The set of all $\Sigma[\mathbb{Z}(p^e)]$ with $e \in \mathbb{N}$, is a chain which is not complete. It becomes complete if we add to it, the $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. All the systems $\Sigma[\mathbb{Z}(p^e)]$ with $e \in \mathbb{N}$, are subsystems of $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. In this sense, $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ can be viewed as the $\Sigma[\mathbb{Z}(p^e)]$ in the limit of large e.
   - The set of all $\Sigma[\mathbb{Z}(d)]$ with $d \in \mathbb{N}$ is a directed partially ordered set, which is not complete. It becomes complete if we add to it the $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ (and also some other systems). All systems $\Sigma[\mathbb{Z}(d)]$ are subsystems of the $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$. In this sense, $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ can be viewed as the $\Sigma[\mathbb{Z}(d)]$ in the limit of large d.

References

1. Pontryagin, L. S. (1966). *Topological groups*. New York: Gordon and Breach.
2. Ribes, L., & Zalesskii, P. (2000). *Profinite groups*. Berlin: Springer.
3. Wilson, J. (1998). *Profinite groups*. Oxford: Clarendon.
4. Weyl, H. (1950). *Theory of groups and quantum mechanics*. New York: Dover.
5. Schwinger, J. (1960). *Proceedings of the National Academy of Science of the United States of America*, *46*, 570.
6. Schwinger, J. (1970). *Quantum kinematics and dynamics*. New York: Benjamin.

7. Vourdas, A. (2004). *Reports on Progress in Physics*, *67*, 267.
8. Vourdas, A. (2007). *Journal of Physics A*, *40*, R285.
9. Gel'fand, I. M., Graev, M. I., & Piatetskii-Shapiro, I. I. (1990). *Representation theory and automorphic functions*. London: Academic.
10. Vladimirov, V. S., Volovich, I. V., & Zelonov, E. I. (1994). *p-adic analysis and mathematical physics*. Singapore: World Scientific.
11. Vourdas, A. (2013). *Journal of Physics A*, *46*, 043001.
12. Batten, L. M. (1997). *Combinatorics of finite geometries*. Cambridge: Cambridge University Press.
13. Hirchfeld, J. W. P. (1979). *Projective geometries over finite fields*. Oxford: Oxford University Press.
14. Hirchfeld, J. W. P., & Thas, J. A. (1991). *General Galois geometries*. Oxford: Oxford University Press.
15. Wootters, W., & Fields, B. D. (1989). *Annals of Physics (NY)*, *191*, 363.
16. Kibler, M. (2009). *Journal of Physics A*, *42*, 353001.
17. Durt, T., Englert, B. G., Bengtsson, I., & Zyczkowski, K. (2010). *International Journal of Quantum Computation*, *8*, 535.
18. Shalaby, M., & Vourdas, A. (2012). *Journal of Physics A*, *45*(052001), 1–15.
19. Shalaby, M., & Vourdas, A. (2013). Mutually unbiased projectors and duality between lines and bases in finite quantum systems. *Annals of Physics*, *337*, 208.
20. Olupitan, T., Lei, C., & Vourdas, A. (2016). An analytic function approach to weak mutually unbiased bases. *Annals of Physics*, *371*, 1.
21. Birkhoff, G., & von Neumann, J. (1936). *Annals of Mathematics*, *37*, 823.
22. Mackey, G. W. (1963). *Mathematical foundations of quantum mechanics*. New York: Benjamin.
23. Piron, C. (1976). *Foundations of quantum physics*. New York: Benjamin.
24. Jauch, J. (1968). *Foundations of quantum mechanics*. Reading: Addison-Wesley
25. Beltrametti, E., Cassinelli, G. (1981). *The logic of quantum mechanics*. Reading: Addison-Wesley
26. Nielsen, M., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge: Cambridge University Press.
27. Kitaev, A Yu., Shen, A. H., & Vyalyi, M. N. (2002). *Classical and quantum computation*. Province: American Mathematical Society.
28. Kaye, P., Laflamme, R., & Moscha, M. (2006). *Introduction to quantum computing*. Oxford: Oxford University Press.
29. Rammal, R., Toulouse, G., & Virasoro, M. A. (1986). *Reviews of Modern Physics*, *58*, 765.
30. Brekke, L., & Freund, P. (1993). *Physics Reports*, *233*, 1.
31. Albeverio, S., Khrennikov, A., & Shelkovich, V. M. (2010). *Theory of p-adic distributions*. Cambridge U. P: Cambridge.

Chapter 2
Partial Orders and Pontryagin Duality

Abstract Partial orders, supernatural numbers, and Pontryagin duality, are discussed.

2.1 Partial Orders

Definition 2.1 (i) A partially ordered set is a set S with a relation $\prec$, and the properties:

(1) (reflexivity) $a \prec a$, for all $a \in S$;
(2) (antisymmetry) if $a \prec b$ and $b \prec a$, then $a = b$;
(3) (transitivity) if $a \prec b$ and $b \prec c$, then $a \prec c$.

(ii) A directed partially ordered set S, is a partially ordered set with the additional property that for $a, b \in S$, there exists $c \in S$ such that $a \prec c$ and $b \prec c$.

a, b are comparable if $a \prec b$ or $b \prec a$. A partially ordered set where any pair of elements is comparable, is a chain (total order).

Definition 2.2 Two partially ordered sets $(S, \prec)$ and $(S', \prec')$ are order isomorphic, if there is a bijective map f from S to S', and $f(a_1) \prec' f(a_2)$, if and only if $a_1 \prec a_2$.

Example 2.1

- the partial order 'subgroup' in a set of groups
- the partial order 'less or equal' in the set of natural numbers $\mathbb{N}$ (i.e., $a \prec b$ if $a \leq b$)
- the partial order 'divisibility' in the set of natural numbers $\mathbb{N}$ (i.e., $a \prec b$ if $a|b$)

For simplicity we use the same symbol $\prec$ for different partial orders, and its precise meaning is clear from the context.

Definition 2.3 An upper bound of a subset T of the partially ordered set S, is an element $a \in S$ such that $b \prec a$ for all $b \in T$. If the set of all upper bounds of T has a smallest element, it is called the supremum of T.

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_2

An element $m \in S$ is called maximal, if there is no element $k \in S$ such that $m \prec k$. A partially ordered set might have many maximal elements, or it might have no maximal element.

Definition 2.4 A partially ordered set S, is called directed-complete partial order (dcpo) if one of the following two statements, which can be proved to be equivalent to each other [1–3], holds:

(1) Every directed subset of S has a supremum.
(2) Every chain in S has a supremum.

A chain which has a supremum, is called a complete chain.

Directed partially ordered sets which are not complete, can sometimes be enlarged into directed-complete partial orders, by adding extra elements.

Example 2.2 The set $\mathbb{N}$ of natural numbers, with divisibility as an order is a directed partially ordered set, but it is not a directed-complete partial order. For example the chain $p, p^2, p^3, ...$ where $p \in \Pi$, has no supremum. $\mathbb{N}$ has no maximal elements. Below we enlarge this set into the supernatural (Steinitz) numbers, which is a directed-complete partial order.

2.2 The Directed-Complete Partial Order of Supernatural (Steinitz) Numbers

The set $\mathbb{N}_S$ of supernatural (Steinitz) numbers [4, 5] is:

$$\mathbb{N}_S = \left\{ n = \prod p^{e_p} \mid p \in \Pi; \quad e_p \in \mathbb{Z}_0^+ \cup \{\infty\} \right\} \tag{2.1}$$

The index S indicates supernatural or Steinitz. Here:

- The exponents can take the value ∞.
- The product might contain an infinite number of prime numbers.

In this set only multiplication is well defined, and by definition

$$p^\infty p^e = p^\infty; \quad e \in \mathbb{Z}_0^+ \cup \{\infty\}. \tag{2.2}$$

$\mathbb{N}$ is a subset of $\mathbb{N}_S$. Indeed, if all $e_p \neq \infty$ and only a finite number of them are different from zero, the $\prod p^{e_p} \in \mathbb{N}$.

Definition 2.5

- Let (e_p) (where $p \in \Pi$ and $e_p \in \mathbb{Z}_0^+ \cup \{\infty\}$) be an infinite sequence of exponents. The $(e_p) \prec (e'_p)$ indicates that $e_p \leq e'_p$ for all p. By definition all numbers in $\mathbb{Z}_0^+$ are smaller than ∞.
- $n = \prod p^{e_p}$ is a divisor of $n' = \prod p^{e'_p}$, if $(e_p) \prec (e'_p)$. We denote this as $n|n'$ or as $n \prec n'$.

- $\mathscr{E}$ is the element of $\mathbb{N}_S$, corresponding to the sequence where all $e_p = 1$:

$$\mathscr{E} = \prod_{p \in \Pi} p \tag{2.3}$$

- Υ is the element of $\mathbb{N}_S$, corresponding to the sequence where all $e_p = \infty$:

$$\Upsilon = \prod_{p \in \Pi} p^{\infty} \tag{2.4}$$

Every element of $\mathbb{N}_S$ is a divisor of Υ.

The set $\mathbb{N}_S$ ordered by divisibility (as defined above) is a directed-complete partial order, with Υ as supremum. Examples of complete chains in $\mathbb{N}_S$, are

$$\begin{aligned}
&p, p^2, ..., p^{\infty}; \quad p \in \Pi \\
&p_1 \prec p_1^2 \prec ... \prec p_1^{\infty} \prec p_1^{\infty} p_2 \prec p_1^{\infty} p_2^2 \prec ... \prec p_1^{\infty} p_2^{\infty} \\
&2 \prec 2 \cdot 3 \prec 2 \cdot 3 \cdot 5 \prec ... \prec \mathscr{E} \\
&2^{\infty} \prec 2^{\infty} 3^{\infty} \prec 2^{\infty} 3^{\infty} 5^{\infty} \prec ... \prec \Upsilon
\end{aligned} \tag{2.5}$$

The suprema in these chains are p^{∞}, $p_1^{\infty} p_2^{\infty}$, $\mathscr{E}$ and Υ, correspondingly. They are examples of the elements that have been added into $\mathbb{N}$, in order to make it the directed-complete partial order $\mathbb{N}_S$.

We use the notation $\mathbb{N}_S(p)$ for the complete chain

$$\mathbb{N}_S(p) = \{p, p^2, ..., p^{\infty}\}. \tag{2.6}$$

2.3 Pontryagin Duality

Let G be an Abelian group and $\widetilde{G}$ its Pontryagin dual group, i.e. the group of its characters (we use the notation χ for characters). For locally compact Abelian groups, the Pontryagin duality theorem states that

$$\widetilde{\widetilde{G}} \cong G. \tag{2.7}$$

Let $\mathfrak{G}$ be a set of groups, and $\widetilde{\mathfrak{G}}$ the set of their Pontryagin dual groups. The partial order subgroup in $\mathfrak{G}$, endows a partial order in $\widetilde{\mathfrak{G}}$, where $\widetilde{A} \prec \widetilde{G}$ if $A \prec G$.

Definition 2.6 Let A be a subgroup of G (we denote this as $A \prec G$). The annihilator $\mathrm{Ann}_{\widetilde{G}}(A)$ of A, is the subgroup of $\widetilde{G}$:

$$\mathrm{Ann}_{\widetilde{G}}(A) = \{b \in \widetilde{G} \mid \chi_b(a) = 1, \forall a \in A\} \tag{2.8}$$

Table 2.1 The groups G relevant to this monograph, together with their Pontryagin dual groups $\widetilde{G}$, and the corresponding quantum system

G	$\widetilde{G}$	$\Sigma(G, \widetilde{G})$
$\mathbb{Z}(d)$	$\mathbb{Z}(d)$	$\Sigma[\mathbb{Z}(d)]$
$GF(p^e)$	$GF(p^e)$	$\Sigma[GF(p^e)]$
$\mathbb{Z}_p$	$\mathbb{Q}_p/\mathbb{Z}_p$	$\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$
$\widehat{\mathbb{Z}}$	$\mathbb{Q}/\mathbb{Z}$	$\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$

The following proposition gives the Pontryagin dual group $\widetilde{A}$ of a subgroup A of a group G, and we present it without proof (e.g., [6]).

Proposition 2.1 *If $A \prec G$, then the Pontryagin dual group of A is isomorphic to $\widetilde{G}/\mathrm{Ann}_{\widetilde{G}}(A)$:*

$$\widetilde{A} \cong \widetilde{G}/\mathrm{Ann}_{\widetilde{G}}(A). \tag{2.9}$$

In quantum mechanics G can be used as the group of 'positions', and its Pontryagin dual $\widetilde{G}$ as the group of 'momenta'. We denote such a quantum system as $\Sigma(G, \widetilde{G})$. For some groups $G \cong \widetilde{G}$, and then we use the simpler notation $\Sigma(G)$ for the corresponding quantum system.

Definition 2.7 $\Sigma(A, \widetilde{A})$ is a subsystem of $\Sigma(G, \widetilde{G})$ if $A \prec G$ (in which case the $\widetilde{A}$ is related to $\widetilde{G}$ as in Eq. (2.9)). We denote this as $\Sigma(A, \widetilde{A}) \prec \Sigma(G, \widetilde{G})$.

The groups G relevant to this monograph, together with their Pontryagin dual groups $\widetilde{G}$, and the corresponding quantum system, are shown in Table 2.1.

References

1. Birkhoff, G. (1995). *Lattice theory*. Rhode Island: American Mathematical Society
2. Szasz, G. (1963). *Introduction to lattice theory*. London: Academic.
3. Gratzer, G. A. (2003). *General lattice theory*. Berlin: Springer.
4. Ribes, L., & Zalesskii, P. (2000). *Profinite groups*. Berlin: Springer.
5. Wilson, J. (1998). *Profinite groups*. Oxford: Clarendon.
6. Pontryagin, L. S. (1966). *Topological groups*. New York: Gordon and Breach.

Chapter 3
The Ring $\mathbb{Z}(d)$

Abstract The ring $\mathbb{Z}(d)$ of integers modulo d, and its properties are discussed. The material of this chapter is prerequisite for the study of finite quantum systems, in chapter 4.

3.1 The Ring $\mathbb{Z}(d)$ and its Characters

Additive characters in the ring $\mathbb{Z}(d)$ are given by

$$\omega_d(\alpha) = \omega(\alpha) = \exp\left(i\frac{2\pi\alpha}{d}\right); \quad [\omega(\alpha)]^d = 1; \quad \alpha \in \mathbb{Z}(d) \tag{3.1}$$

If d is clear from the context, we omit the index d in the notation. The group $C(d)$ of characters of $\mathbb{Z}(d)$, i.e., the Pontryagin dual group to $\mathbb{Z}(d)$, is isomorphic to $\mathbb{Z}(d)$:

$$C(d) = \{\omega(\alpha) \mid \alpha \in \mathbb{Z}(d)\} \cong \mathbb{Z}(d). \tag{3.2}$$

The following relation holds:

$$\frac{1}{d}\sum_{\alpha=0}^{d-1} \omega[\alpha(\beta-\gamma)] = \delta(\beta,\gamma). \tag{3.3}$$

$\delta(\beta,\gamma)$ is the Kronecker delta which is equal to 1 when $\beta = \gamma \,(\mathrm{mod}\ \ d)$.

If d is a prime number p, then $\mathbb{Z}(p)$ is a field. Elements in the field $\mathbb{Z}(p)$ obey the relation

$$\alpha^p = \alpha; \quad \alpha \in \mathbb{Z}(p). \tag{3.4}$$

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_3

When d is a power of a prime number p^e, the $\mathbb{Z}(p^e)$ is a ring. However there exists a Galois field $GF(p^e)$ with p^e elements, which differs from the ring $\mathbb{Z}(p^e)$ in the multiplication rule, and which is discussed later.

3.1.1 Quadratic Gauss Sums

The quadratic Gauss sum is defined as [1, 2]

$$G[\alpha; \mathbb{Z}(d)] = \sum_{\beta=0}^{d-1} \omega(\alpha\beta^2). \tag{3.5}$$

If d is an odd integer, then

$$|G[1; \mathbb{Z}(d)]| = \sqrt{d}. \tag{3.6}$$

If $d = d_1 d_2$ where d_1, d_2 are coprime, then

$$G[\alpha; \mathbb{Z}(d_1 d_2)] = G[d_1\alpha; \mathbb{Z}(d_2)]G[d_2\alpha; \mathbb{Z}(d_1)]. \tag{3.7}$$

This reduces the study of Gauss sums to the special cases of $G[\alpha; \mathbb{Z}(p^e)]$ where p is a prime number.

If $d = p$ is an odd prime number and $\alpha \neq 0$, then

$$G[\alpha; \mathbb{Z}(p)] = (\alpha|p)G[1; \mathbb{Z}(p)]. \tag{3.8}$$

where $(\alpha|p)$ is the Legendre symbol. But $|(\alpha|p)| = 1$ for $\alpha \neq 0$. Therefore for an odd prime p:

$$\begin{aligned} |G[\alpha; \mathbb{Z}(p)]| &= \sqrt{p} \ \text{ if } \ \alpha \neq 0 \\ |G[0; \mathbb{Z}(p)]| &= p. \end{aligned} \tag{3.9}$$

3.1.2 Totient Functions and the Dedekind psi Function

Let d be an integer, which is factorized in terms of N prime numbers p_i as

$$d = \prod_{i=1}^{N} p_i^{e_i}. \tag{3.10}$$

The Jordan totient function is given by [1]

$$J_k(d) = d^k \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^k}\right). \tag{3.11}$$

For $k = 1$ the Jordan totient function reduces to the Euler totient function $\varphi(d)$, given by

$$\varphi(d) = J_1(d) = d \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right). \tag{3.12}$$

For $k = 2$,

$$J_2(d) = d^2 \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^2}\right) = \varphi(d)\psi(d), \tag{3.13}$$

where

$$\psi(d) = d \prod_{i=1}^{N} \left(1 + \frac{1}{p_i}\right) \tag{3.14}$$

is the Dedekind ψ-function. For prime numbers p_1, p_2

$$\psi(p_1) = p_1 + 1; \quad \psi(p_1 p_2) = (p_1 + 1)(p_2 + 1). \tag{3.15}$$

All $\varphi(d)$, $J_k(d)$, $\psi(d)$ are multiplicative functions (i.e., $f(d_1 d_2) = f(d_1) f(d_2)$ for coprime d_1, d_2).

3.1.3 Invertible and Non-invertible Elements in $\mathbb{Z}(d)$

A non-zero element $m \in \mathbb{Z}(d)$ is invertible if $\mathrm{GCD}(m, d) = 1$ (where GCD indicates the greatest common divisor). The number of invertible elements in $\mathbb{Z}(d)$ is given by the Euler totient function $\varphi(d)$.

The invertible elements in $\mathbb{Z}(d)$, form a group with respect to multiplication, which is called the group of reduced residue classes modulo d, and which is usually denoted as $[\mathbb{Z}(d)]^*$. The cardinality of this group is $|[\mathbb{Z}(d)]^*| = \varphi(d)$.

A non-zero element $n \in \mathbb{Z}(d)$ is non-inverible if $\mathrm{GCD}(n, d) > 1$. There are $d - \varphi(d)$ non-invertible elements in $\mathbb{Z}(d)$.

Example 3.1 For $\mathbb{Z}(15)$ we get $\varphi(15) = 8$ and

$$[\mathbb{Z}(15)]^* = \{1, 2, 4, 7, 8, 11, 13, 14\}. \tag{3.16}$$

3.2 Factorization of the Ring $\mathbb{Z}(d)$ Based on the Chinese Remainder Theorem

We factorize d as $d = d_1 \times ... \times d_N$ where the factors d_1,…,d_n are coprime with respect to each other. Using the Chinese remainder theorem, we introduce two bijective maps between $\mathbb{Z}(d)$ and $\mathbb{Z}(d_1) \times ... \times \mathbb{Z}(d_N)$. They have been used by Good in the context of fast Fourier transforms [3–5]. We will use them later, to factorize a quantum system with variables in $\mathbb{Z}(d)$, in terms of N smaller subsystems with variables in $\mathbb{Z}(d_1)$,…,$\mathbb{Z}(d_N)$. One of these maps will be used with positions and the other with momenta, and this will ensure that that the Fourier transform in $\mathbb{Z}(d)$, is factorized in terms of Fourier transforms in $\mathbb{Z}(d_1)$,…,$\mathbb{Z}(d_N)$.

We first introduce the integers r_i and t_i:

$$r_i = \frac{d}{d_i}; \quad t_i r_i = 1 \ (mod\ d_i). \tag{3.17}$$

Here t_i is the 'inverse' of r_i within $\mathbb{Z}(d_i)$. It exists because r_i and d_i are coprime. We also introduce the

$$s_i = t_i r_i \in \mathbb{Z}(d). \tag{3.18}$$

Since t_i is the inverse of r_i in $\mathbb{Z}(d_i)$, the $s_i = t_i r_i$ defined in $\mathbb{Z}(d)$ is an integer multiple of d_i plus 1. Consequently

$$s_i r_i = r_i (\text{mod } d). \tag{3.19}$$

Also since d_i, d_j are coprime

$$i \neq j \ \rightarrow \ s_i r_j = 0 (\text{mod } d). \tag{3.20}$$

The first map between $\mathbb{Z}(d)$ and $\mathbb{Z}(d_1) \times ... \times \mathbb{Z}(d_N)$, is

$$\begin{aligned} &m \leftrightarrow (m_1, \ldots, m_N); \quad m_i = m (\text{mod } d_i); \quad m = \sum_i m_i s_i \\ &m \in \mathbb{Z}(d); \quad m_i \in \mathbb{Z}(d_i) \end{aligned} \tag{3.21}$$

The second map (which we call dual) is

$$\begin{aligned} &m \leftrightarrow (\overline{m}_1, \ldots, \overline{m}_N); \quad \overline{m}_i = m_i t_i = m t_i (\text{mod } d_i); \quad m = \sum_i \overline{m}_i r_i (\text{mod } d) \\ &m \in \mathbb{Z}(d); \quad \overline{m}_i \in \mathbb{Z}(d_i) \end{aligned} \tag{3.22}$$

The proof that these maps are bijective, is based on the Chinese remainder theorem [1]. The sum and product of two numbers in $\mathbb{Z}(d)$ is factorized as follows, according

to the map in Eq. (3.21):

$$\begin{aligned} m+\ell &\leftrightarrow (m_1+\ell_1,\ldots,m_N+\ell_N) \\ m\ell &\leftrightarrow (m_1\ell_1,\ldots,m_N\ell_N) \end{aligned} \tag{3.23}$$

It is also factorized as follows, according to the map in Eq. (3.22):

$$\begin{aligned} m+\ell &\leftrightarrow (\overline{m}_1+\overline{\ell}_1,\ldots,\overline{m}_N+\overline{\ell}_N) \\ m\ell &\leftrightarrow (\overline{m_1\ell_1},\ldots\overline{m_n\ell_N}) = (m_1\overline{\ell}_1,\ldots m_N\overline{\ell}_N) \end{aligned} \tag{3.24}$$

In the second of these equations we use the components of m according to the map in Eq. (3.21) and the components of ℓ according to the map of Eq. (3.22).

We use the notation

$$\omega_i(\alpha_i) = \exp\left[i\frac{2\pi\alpha_i}{d_i}\right]; \quad \alpha_i \in \mathbb{Z}(d_i). \tag{3.25}$$

for additive characters in $\mathbb{Z}(d_i)$, and the notation in Eq. (3.1) for additive characters in $\mathbb{Z}(d)$. Using Eqs. (3.19), (3.20), we show that

$$mn = \sum_i r_i m_i \overline{n}_i; \quad \omega(mn) = \prod_{i=1}^{N} \omega_i(m_i\overline{n}_i) \tag{3.26}$$

This is an important relation, which will be used later to factorize Fourier transforms. It is seen that both maps of Eqs. (3.21), (3.22) are needed here, and this is precisely the reason for introducing them.

Later we will consider the case with $d = p_1p_2$ where p_1, p_2 are prime numbers different from each other. In this case the constants entering in the factorization of $\mathbb{Z}(p_1p_2)$ as $\mathbb{Z}(p_1) \times \mathbb{Z}(p_2)$, are:

$$\begin{aligned} &r_1 = p_2; \quad r_2 = p_1; \quad t_1 = p_2^{-1} \in \mathbb{Z}(p_1); \quad t_2 = p_1^{-1} \in \mathbb{Z}(p_2) \\ &s_1 = t_1r_1; \quad s_2 = r_2t_2. \end{aligned} \tag{3.27}$$

They obey the following relations, modulo p_1p_2:

$$\begin{aligned} &s_1s_2 = 0; \quad s_1+s_2 = 1; \quad s_1^2 = s_1; \quad s_2^2 = s_2 \\ &p_1s_1 = p_2s_2 = 0; \quad p_2s_1 = p_2; \quad p_1s_2 = p_1. \end{aligned} \tag{3.28}$$

Then

$$\begin{aligned} &m \leftrightarrow (m_1,m_2) \leftrightarrow (\overline{m}_1,\overline{m}_2) \\ &m_i = m(\text{mod } p_i); \quad \overline{m}_i = m_it_i = mt_i(\text{mod } p_i) \\ &m = m_1s_1+m_2s_2 = \overline{m}_1r_1+\overline{m}_2r_2 \end{aligned} \tag{3.29}$$

Example 3.2 We consider the case $d = 15$, and then $d_1 = 3$ and $d_2 = 5$. In this case

$$r_1 = 5; \quad t_1 = 2; \quad s_1 = 10; \quad r_2 = 3; \quad t_2 = 2; \quad s_2 = 6. \tag{3.30}$$

Therefore

$$m = 10m_1 + 6m_2 = 5\overline{m}_1 + 3\overline{m}_2. \tag{3.31}$$

For example, $m = 8$ and $n = 11$ are mapped with these two maps into

$$\begin{aligned} 8 &\leftrightarrow (2, 3) \leftrightarrow (1, 1) \\ 11 &\leftrightarrow (2, 1) \leftrightarrow (1, 2) \end{aligned} \tag{3.32}$$

In this case Eq. (3.26) becomes

$$\begin{aligned} &8 \times 11 = (5 \times 2 \times 1) + (3 \times 3 \times 2) \text{ (mod 15)} \\ &\omega(8 \times 11) = \omega_1(2 \times 1)\omega_2(3 \times 2). \end{aligned} \tag{3.33}$$

3.3 The Symplectic Group $Sp[2, \mathbb{Z}(d)]$

We consider the 2×2 matrices

$$g(\kappa, \lambda|\mu, \nu) \equiv \begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix}; \quad \det(g) = \kappa\nu - \lambda\mu = 1 \text{ (mod } d), \tag{3.34}$$

where $\kappa, \lambda, \mu, \nu \in \mathbb{Z}(d)$. The product of two such matrices is a matrix of the same type. The inverse matrix exists and it is the $g(\nu, -\lambda| - \mu, \kappa)$. Therefore these matrices form a group which is the $Sp[2, \mathbb{Z}(d)]$ group (general references for groups in physics are [6–11]).

It will be convenient later (see Eq. 4.57) to define the multiplication as 'right multiplication', i.e., as the product of the second matrix times the first matrix:

$$\begin{aligned} &g(\kappa_1, \lambda_1|\mu_1, \nu_1) \circ g(\kappa_2, \lambda_2|\mu_2, \nu_2) = \begin{pmatrix} \kappa_2 & \lambda_2 \\ \mu_2 & \nu_2 \end{pmatrix} \begin{pmatrix} \kappa_1 & \lambda_1 \\ \mu_1 & \nu_1 \end{pmatrix} \\ &= \begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix} = g(\kappa, \lambda|\mu, \nu) \\ &\kappa = \kappa_2\kappa_1 + \lambda_2\mu_1, ; \quad \lambda = \kappa_2\lambda_1 + \lambda_2\nu_1 \\ &\mu = \mu_2\kappa_1 + \nu_2\mu_1; \quad \nu = \mu_2\lambda_1 + \nu_2\nu_1. \end{aligned} \tag{3.35}$$

The inverse of $g(\kappa, \lambda|\mu, \nu)$ is

$$[g(\kappa, \lambda|\mu, \nu)]^{-1} = g(\nu, -\lambda| - \mu, \kappa) \tag{3.36}$$

The following are three subgroups of $Sp[2, \mathbb{Z}(d)]$:

$$\begin{aligned} G_A &= \{g(\kappa, 0|0, \kappa^{-1}) | \kappa \in [\mathbb{Z}(d)]^*\} \cong [\mathbb{Z}(d)]^* \\ G_B &= \{g(1, \lambda|0, 1) | \lambda \in \mathbb{Z}(d)\} \cong \mathbb{Z}(d) \\ G_C &= \{g(1, 0|\mu, 1) | \mu \in \mathbb{Z}(d)\} \cong \mathbb{Z}(d). \end{aligned} \tag{3.37}$$

The subgroups G_B and G_C are isomorphic to the additive group $\mathbb{Z}(d)$. The G_A is isomorphic to the multiplicative group $[\mathbb{Z}(d)]^*$.

Proposition 3.1 *For $\nu \in [\mathbb{Z}(d)]^*$, the general matrix $g(\kappa, \lambda|\mu, \nu)$ can be written as*

$$g(\kappa, \lambda|\mu, \nu) = g(1, 0|\xi_1, 1) \circ g(1, \xi_2|0, 1) \circ g(\xi_3, 0|0, \xi_3^{-1}), \tag{3.38}$$

where

$$\kappa = \xi_3(1 + \xi_1\xi_2); \quad \lambda = \xi_2\xi_3; \quad \mu = \xi_1\xi_3^{-1}; \quad \nu = \xi_3^{-1}. \tag{3.39}$$

This is the Iwasawa decomposition. Inverting these equations, we get

$$\xi_1 = \mu\nu^{-1}; \quad \xi_2 = \lambda\nu; \quad \xi_3 = \nu^{-1}. \tag{3.40}$$

Proof The proof is straightforward, using the multiplication rule in Eq. (3.35).

A special case of the matrices $g(\kappa, \lambda|\mu, \nu)$ with $\nu \notin [\mathbb{Z}(d)]^*$, is the matrices $g(\kappa, -\mu^{-1}|\mu, 0)$. A special case of these matrices is the Fourier matrix

$$\mathscr{F} = g(0, 1| - 1, 0); \quad \mathscr{F}^4 = \mathbf{1}. \tag{3.41}$$

Example 3.3 We consider the matrix $g(3, 4|2, 8)$ (with elements in $\mathbb{Z}(15)$), which is an element of $Sp[2, \mathbb{Z}(15)]$. In this case

$$\begin{aligned} \kappa = 3; \quad \lambda = 4; \quad \mu = 2; \quad \nu = 8 \\ \xi_1 = 4; \quad \xi_2 = 2; \quad \xi_3 = 2. \end{aligned} \tag{3.42}$$

The Iwasawa decomposition in this case is

$$g(3, 4|2, 8) = g(1, 0|4, 1) \circ g(1, 2|0, 1) \circ g(2, 0|0, 8). \tag{3.43}$$

3.4 Factorization of the Symplectic Group $Sp[2, \mathbb{Z}(d)]$ Based on the Chinese Remainder Theorem

The following proposition shows that the symplectic group $Sp[2, \mathbb{Z}(d)]$ can be factorized in terms of smaller symplectic groups $Sp[2, \mathbb{Z}(e_i)]$, where $e_i|d$. In order to avoid a complex notation, and without loss of generality, we consider the case $d = p_1 p_2$ where p_1, p_2 are of two prime numbers.

Proposition 3.2 *Let $d = p_1 p_2$ where the p_1, p_2 are different prime numbers. The $Sp[2, \mathbb{Z}(p_1 p_2)]$ is isomorphic to $Sp[2, \mathbb{Z}(p_1)] \times Sp[2, \mathbb{Z}(p_2)]$, where:*

$$g(\kappa, \lambda|\mu, \nu) \leftrightarrow (g_1(\kappa_1, \lambda_1 r_1|\overline{\mu}_1, \nu_1), g_2(\kappa_2, \lambda_2 r_2|\overline{\mu}_2, \nu_2)) \tag{3.44}$$

The $\kappa_i, \lambda_i, \nu_i, \overline{\mu}_i$ are related to $\kappa, \lambda, \nu, \mu$ as in Eq. (3.29).

Proof Given the $\kappa, \lambda, \mu, \nu$ we can calculate the $\kappa_i, \lambda_i, \overline{\mu}_i, \nu_i$, and vice-versa. Also since $\kappa\nu - \lambda\mu = 1(\text{mod}(d))$ we easily prove that $\kappa_i \nu_i - \lambda_i r_i \overline{\mu}_i = 1(\text{mod}(d_i))$. This establishes a bijective map between $Sp[2, \mathbb{Z}(p_1 p_2)]$ and $Sp[2, \mathbb{Z}(p_1)] \times Sp[2, \mathbb{Z}(p_2)]$.

We then prove for the product:

$$\begin{aligned} &g(\kappa, \lambda|\mu, \nu) \circ g(\kappa', \lambda'|\mu', \nu') \leftrightarrow \\ &(g_1(\kappa_1, \lambda_1 r_1|\overline{\mu}_1, \nu_1) \circ g_1(\kappa'_1, \lambda'_1 r_1|\overline{\mu}'_1, \nu'_1), \\ &g_2(\kappa_2, \lambda_2 r_2|\overline{\mu}_2, \nu_2) \circ g_2(\kappa'_2, \lambda'_2 r_2|\overline{\mu}'_2, \nu'_2)) \end{aligned} \tag{3.45}$$

Also the $\mathbf{1}$, corresponds to $(\mathbf{1}, \mathbf{1})$. This proves the isomorphism between the groups.

Example 3.4 We consider the matrix $g(3, 4|2, 8) \in Sp[2, \mathbb{Z}(15)]$, and factorize $\mathbb{Z}(15)$ as $\mathbb{Z}(3) \times \mathbb{Z}(5)$. Then

$$g(3, 4|2, 8) \leftrightarrow (g_1(0, 2|1, 2), g_2(3, 2|4, 3)) \tag{3.46}$$

Remark 3.1 Another bijective map between the isomorphic groups $Sp[2, \mathbb{Z}(p_1 p_2)]$ and $Sp[2, \mathbb{Z}(p_1)] \times Sp[2, \mathbb{Z}(p_2)]$, is

$$g(\kappa, \lambda|\mu, \nu) \leftrightarrow (g_1(\kappa_1, \lambda_1|\mu_1, \nu_1), g_2(\kappa_2, \lambda_2|\mu_2, \nu_2)) \tag{3.47}$$

But it is the map of Eq. (3.44) that is needed later, and in particular the special cases in the following corollary.

Corollary 3.1 *The following are special cases of the bijective map in Eq. (3.44):*

(1) If $\nu_1 \in \mathbb{Z}(p_1)$ and $\nu_2 \in \mathbb{Z}(p_2)$

$$\begin{aligned} &(g_1(0, -1|1, \nu_1), g_2(0, -1|1, \nu_2)) \leftrightarrow \\ &g(0, -s_1 t_1 - s_2 t_2|p_1 + p_2, \nu_1 s_1 + \nu_2 s_2) \end{aligned} \tag{3.48}$$

(2) If $\nu_2 \in \mathbb{Z}(p_2)$

$$(\mathbf{1}, g_2(0, -1|1, \nu_2)) \leftrightarrow g(s_1, -s_2 t_2|p_1, s_1 + \nu_2 s_2) \tag{3.49}$$

(3) If $\nu_1 \in \mathbb{Z}(p_1)$

$$(g_1(0, -1|1, \nu_1), \mathbf{1}) \leftrightarrow g(s_2, -s_1 t_1|p_2, \nu_1 s_1 + s_2) \tag{3.50}$$

(4)

$$(\mathbf{1}, \mathbf{1}) \leftrightarrow \mathbf{1}. \tag{3.51}$$

(5)

$$(g_1(0, r_1| - t_1, 0), g_2(0, r_2| - t_2, 0)) \leftrightarrow g(0, 1| - 1, 0) = \mathscr{F}. \tag{3.52}$$

Proof (1) We will start with the parameters in the right hand side in Eq. (3.48)

$$\kappa = 0; \quad \lambda = -s_1 t_1 - s_2 t_2; \quad \mu = p_1 + p_2; \quad \nu = \nu_1 s_1 + \nu_2 s_2 \tag{3.53}$$

and show that they lead to

$$\begin{aligned} &\kappa_1 = 0; \quad \lambda_1 r_1 = -1; \quad \overline{\mu}_1 = 1; \quad \nu_1 \\ &\kappa_2 = 0; \quad \lambda_2 r_2 = -1; \quad \overline{\mu}_2 = 1; \quad \nu_2. \end{aligned} \tag{3.54}$$

Since $s_1 = t_1 r_1$ and $t_1 r_1 = 1 \pmod{p_1}$, it follows that $s_1 = 1 + N p_1$. Therefore

$$\lambda_1 = -s_1 t_1 - s_2 t_2 = -t_1 - s_2 t_2 \pmod{p_1}. \tag{3.55}$$

We multiply this with r_1 and use the fact that $r_1 = p_2$ and $s_2 p_2 = 0 \pmod{p_1 p_2}$. We get

$$\lambda_1 r_1 = -t_1 r_1 = -1 \pmod{p_1}. \tag{3.56}$$

Also

$$\overline{\mu}_1 = (p_1 + p_2) t_1 = p_2 t_1 = r_1 t_1 = 1 \pmod{p_1}. \tag{3.57}$$

In analogous way we prove that the other parameters on the left hand side have the values given in Eq. (3.54).

(2) We will start with the parameters in the right hand side in Eq. (3.49)

$$\kappa = s_1; \quad \lambda = -s_2 t_2; \quad \mu = p_1; \quad \nu = s_1 + \nu_2 s_2 \tag{3.58}$$

and show that they lead to

$$\begin{aligned} &\kappa_1 = 1; \quad \lambda_1 r_1 = 0; \quad \overline{\mu}_1 = 0; \quad \nu_1 = 1 \\ &\kappa_2 = 0; \quad \lambda_2 r_2 = -1; \quad \overline{\mu}_2 = 1; \quad \nu_2. \end{aligned} \tag{3.59}$$

The technical details to prove this, are analogous to those in the first part.

(3) We will start with the parameters in the right hand side in Eq. (3.50)

$$\kappa = s_2; \quad \lambda = -s_1 t_1; \quad \mu = p_2; \quad \nu = \nu_1 s_1 + s_2 \tag{3.60}$$

and show that they lead to

$$\begin{aligned} &\kappa_1 = 1; \quad \lambda_1 r_1 = 0; \quad \overline{\mu}_1 = 0; \quad \nu_1 = 1 \\ &\kappa_2 = 0; \quad \lambda_2 r_2 = -1; \quad \overline{\mu}_2 = 1; \quad \nu_2. \end{aligned} \tag{3.61}$$

The proof is analogous to the one in the first part.

(4) The proof of this case is straightforward.

(5) The proof follows immediately from the general Eq. (3.44).

Proposition 3.3 *The cardinality of the symplectic group* $Sp[2, \mathbb{Z}(d)]$ *is [12]*

$$|Sp[2, \mathbb{Z}(d)]| = dJ_2(d), \tag{3.62}$$

where $J_2(d)$ *is the Jordan totient function (Eq. 3.13).*

Proof We first assume that $d = p^e$ and prove that

$$|Sp[2, \mathbb{Z}(d)]| = d^2\varphi(d)\left(1 + \frac{1}{p}\right). \tag{3.63}$$

In order to prove this, we partition the set of all elements of $Sp[2, \mathbb{Z}(p^e)]$ into two subsets, as follows. There are two possibilities for the element κ in the matrix $g(\kappa, \lambda|\mu, \nu)$. Either $\text{GCD}(\kappa, p) = 1$ and κ is one of the $\varphi(d)$ invertible elements of $\mathbb{Z}(d)$, or $\kappa = Np$ and κ is a non-invertible element of $\mathbb{Z}(d)$. In the former case the set of matrices is

$$S_1 = \left\{g(\kappa, \lambda|\mu, \kappa^{-1}(1 + \lambda\mu))|\kappa \in [\mathbb{Z}(d)]^*; \quad \lambda, \mu \in \mathbb{Z}(d)\right\} \tag{3.64}$$

and therefore its cardinality is $|S_1| = d^2\varphi(d)$. In the latter case the set of the matrices is

$$S_2 = \left\{g(Np, \lambda|\mu, \nu)|N = 0, 1, \ldots, p^{e-1} - 1; \lambda, \mu \in [\mathbb{Z}(d)]^*; \ \nu \in \mathbb{Z}(d)\right\}. \tag{3.65}$$

Here the $\lambda\mu = Np\nu - 1$ and therefore λ, μ are invertible elements. Consequently the cardinality of S_2 is $d^2\varphi(d)\frac{1}{p}$. We add these two cardinalities, and we prove Eq. (3.63).

We next use the bijective map in Eq. (3.47), to show that $|Sp[2, \mathbb{Z}(d)]|$ is a multiplicative function, i.e., to show that for coprime d_1 and d_2

$$|Sp[2, \mathbb{Z}(d_1 d_2)]| = |Sp[2, \mathbb{Z}(d_1)]| \times |Sp[2, \mathbb{Z}(d_2)]|. \tag{3.66}$$

This together with Eq. (3.63) proves the proposition (because the Jordan totient function is multiplicative).

References

1. Apostol, T. (1976). *Introduction to analytic number theory*. New York: Springer.
2. Berndt, B. C., Evans, R. J., & Williams, K. S. (1998). *Gauss and Jacobi sums*. New York: Wiley.
3. Good, I. J., I. E. E. E. Transcations (1971). *Computers*, *C20*, 310.
4. McClellan, J. H., & Rader, C. M. (1979). *Number theory in digital signal processing*. London: Prentice Hall.
5. Elliott, D. F., & Rao, K. R. (1982). *Fast transforms*. London: Academic.
6. Biedenharn, L. C., & Van Dam, H. (Eds.). (1965). *Quantum theory of angular momentum*. New York: Academic.
7. Biedenharn, L. C., & Louck, J. C. (1981). *Encyclopedia of mathematics and its applications* (Vols. 8, 9). Reading Mass: Addison wesley.
8. Vilenkin, N. J. (1968). *Special functions and the theory of group representations*. Providence, RI: American Mathematical Society.
9. Vilenkin, N. J., & Klimyk, A. V. (1991). *Representations of lie groups and special functions*. Dordrecht: Kluwer.
10. Gelfand, I. M., Minlos, R. A., & Shapiro, Z. Y. (1963). *Representations of the rotation and lorentz groups and their applications*. London: Pergamon.
11. Zelobenko, P. (1973). *Compact Lie groups and their representations*. Providence, RI: American Mathematical Society.
12. Vourdas, A., & Banderier, C. (2010). *Journal of Physics A*, *43*, 042001.

Chapter 4
Quantum Systems with Variables in $\mathbb{Z}(d)$

Abstract The formalism of finite quantum systems with variables in $\mathbb{Z}(d)$, is presented. Displacement operators and the Heisenberg-Weyl group, the Symplectic group, Wigner and Weyl functions, etc, are discussed.

After the original work by Weyl [1] and Schwinger [2, 3], there has been a lot of work on various aspects of quantum systems with finite Hilbert space (e.g., [4–28]). The uncertainty relations in this context have been studied in [29–32]. Related is also work on finite oscillators and relevant special functions and polynomials [33–40]. Mathematical work on finite Fourier transforms, is presented in [41–43].

There are technical differences in the two cases that the dimension of the Hilbert space is an odd or even integer (e.g. [44, 45]). In this monograph we discuss the case where the dimension is an odd integer.

4.1 Fourier Transforms in $\Sigma[\mathbb{Z}(d)]$

We consider a quantum system $\Sigma[\mathbb{Z}(d)]$ with variables in $\mathbb{Z}(d)$. It is described with a d-dimensional Hilbert space $H[\mathbb{Z}(d)]$, that contains complex functions $f(m)$ where $m \in \mathbb{Z}(d)$.

In the space $H[\mathbb{Z}(d)]$ we consider an orthonormal basis of 'position states', which we denote as $|X; m\rangle$ where $m \in \mathbb{Z}(d)$. X is not a variable, but it simply indicates position states.

Definition 4.1 The Fourier transform, is given by

$$F = \frac{1}{\sqrt{d}} \sum_{m,n} \omega(mn) |X; m\rangle\langle X; n|; \quad \omega(\alpha) = \exp\left(i \frac{2\pi\alpha}{d}\right). \tag{4.1}$$

In the position basis, F is the $d \times d$ matrix:

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_4

$$F = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 & 1 & \cdot & 1 \\ 1 & \omega(1) & \cdots & \omega(d-1) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega(d-1) & \cdots & \omega(1) \end{pmatrix} \tag{4.2}$$

Using the Fourier transform we define the basis of 'momentum states', as:

$$|P; m\rangle = F|X; m\rangle = \frac{1}{\sqrt{d}} \sum_n \omega(mn)|X; n\rangle \tag{4.3}$$

The P in the notation is not a variable, it simply indicates momentum states. The position and momentum states can be represented with the vectors

$$|X; n\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}; \quad |P; n\rangle = \begin{pmatrix} 1 \\ \omega(n) \\ \vdots \\ \omega[n(d-1)] \end{pmatrix} \tag{4.4}$$

Proposition 4.1 *(1) Acting successively with the Fourier operator on position states we get*

$$|X; m\rangle \xrightarrow{F} |P; m\rangle \xrightarrow{F} |X; -m\rangle \xrightarrow{F} |P; -m\rangle \xrightarrow{F} |X; m\rangle. \tag{4.5}$$

(2)

$$F^4 = \mathbf{1}. \tag{4.6}$$

Proof (1) The $F|X; m\rangle = |P; m\rangle$ by definition. Acting with F on $|P; m\rangle$ and using Eq. (3.3), we get $|X; -m\rangle$. Then by definition $F|X; -m\rangle = |P; -m\rangle$. And finally, we just proved that $F|P; m\rangle = |X; -m\rangle$ and therefore $F|P; -m\rangle = |X; m\rangle$.

(2) From the first part of the proposition, follows immediately that $F^4 = \mathbf{1}$.

The fact that $F^4 = \mathbf{1}$, implies that the Fourier operator has four eigenvalues $1, -1, i, -i$. The multiplicity of these eigenvalues, and the $\mathrm{Tr}F$, are given in Table 4.1 [41].

Table 4.1 The multiplicity of the eigenvalues $1, -1, i, -i$ and the trace of the Fourier operator in a d-dimensional Hilbert space

	1	-1	i	$-i$	$\mathrm{Tr}F$
$d = 4m$	$m+1$	m	m	$m-1$	$1+i$
$d = 4m+1$	$m+1$	m	m	m	1
$d = 4m+2$	$m+1$	$m+1$	m	m	0
$d = 4m+3$	$m+1$	$m+1$	$m+1$	m	i

Position and momentum operators x and p, are given by

$$x = \sum_{n=0}^{d-1} n|X;n\rangle\langle X;n|; \quad p = \sum_{n=0}^{d-1} n|P;n\rangle\langle P;n|. \tag{4.7}$$

The x and p are defined modulo $d\mathbf{1}$, because n are integers modulo d. However, exponentials of these operators are single-valued. It is easily seen that

$$p = FxF^\dagger; \quad FxF^\dagger = p; \quad FpF^\dagger = -x. \tag{4.8}$$

For practical calculations, it is convenient to define the functions

$$\Delta_0(x) = \frac{1}{d}\sum_{n=0}^{d-1} \omega(nx) \tag{4.9}$$

and more generally

$$\Delta_m(x) = \partial_x^m \Delta_0(x) = \frac{1}{d}\sum_{n=0}^{d-1} \left(i\frac{2\pi n}{d}\right)^m \omega(nx); \quad \Delta_m(x+d) = \Delta_m(x). \tag{4.10}$$

For example, the matrix elements of the operators p^k are:

$$\langle X,n|p^k|X,m\rangle = \frac{1}{d}\sum_{\ell} \ell^k \omega[\ell(n-m)] = \left(\frac{d}{2\pi i}\right)^k \Delta_k(n-m). \tag{4.11}$$

Extra care is needed in numerical calculations, due to the circular nature of the variables.

Remark 4.1 We can calculate the commutator

$$[x,\,p] = \frac{d}{2\pi i}\sum_{m,n}(m-n)\Delta_1(m-n)|X;m\rangle\langle X;n| \tag{4.12}$$

This is an important quantity in the case of continuous Heisenberg-Weyl groups, related to infinitesimal displacements in phase space. In our case the Heisenberg-Weyl group (discussed below) is discrete, and this quantity is of less importance.

4.2 Time Evolution

Let $\mathfrak{H}$ be the Hamiltonian describing the system, which we express in terms of its eigenvalues h_i and eigenprojectors π_i as

$$\mathfrak{H} = \sum h_i \pi_i; \quad \sum \pi_i = \mathbf{1}; \quad \pi_i \pi_j = \pi_i \delta(i, j). \tag{4.13}$$

The time evolution operator of this system is

$$\exp(it\mathfrak{H}) = \sum_{i=0}^{d-1} \exp(ih_i t)\pi_i. \tag{4.14}$$

If $\rho(t)$ is the $d \times d$ density matrix of the system at time t, then

$$\rho(t) = \exp(it\mathfrak{H})\rho(0)\exp(-it\mathfrak{H}) = \sum_{i,j} \exp[it(h_i - h_j)]\sigma_{ij}$$
$$\sigma_{ij} = \pi_i \rho(0) \pi_j. \tag{4.15}$$

If all the ratios $(h_i - h_0)/(h_1 - h_0)$ are rational numbers the system is periodic.

We next consider the d probabilities $\mathrm{Tr}[\rho(t)\pi_i]$, and show that they are constants of motion:

$$\mathrm{Tr}[\rho(t)\pi_i] = \mathrm{Tr}[\rho(0)\pi_i]. \tag{4.16}$$

The proof is based on the fact that the $\exp(it\mathfrak{H})$ commute with the π_i.

4.3 The Heisenberg-Weyl Group $HW[\mathbb{Z}(d)]$

Definition 4.2 The Heisenberg-Weyl group has elements $g(\alpha, \beta, \gamma)$, where α, β, γ are elements of some ring, and the multiplication rule:

$$g(\alpha_1, \beta_1, \gamma_1)g(\alpha_2, \beta_2, \gamma_2) = g(\alpha_1 + \alpha_2, \beta_1 + \beta_2, \gamma)$$
$$\gamma = \gamma_1 + \gamma_2 + 2^{-1}(\alpha_1\beta_2 - \alpha_2\beta_1) \tag{4.17}$$

In our case, the ring is $\mathbb{Z}(d)$ with odd d, and the 2^{-1} exists (if $d = 2j + 1$ then $2^{-1} = j + 1$).

Definition 4.3 The displacement operators X, Z are the unitary operators

$$X = \exp\left[-i\frac{2\pi}{d}p\right]; \quad Z = \exp\left[i\frac{2\pi}{d}x\right]. \tag{4.18}$$

In the position basis X, Z are the $d \times d$ matrices

$$X = \begin{pmatrix} 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}; \quad Z = \begin{pmatrix} 1 & 0 & 0 & \cdot & 0 \\ 0 & \omega(1) & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega(d-1) \end{pmatrix}. \tag{4.19}$$

Various properties of the displacement operators X, Z, are given below.

Proposition 4.2 *(1) The X, Z act on position and momentum states as follows:*

$$\begin{aligned} Z^\alpha |P; m\rangle &= |P; m+\alpha\rangle; \quad Z^\alpha |X; m\rangle = \omega(\alpha m)|X; m\rangle \\ X^\beta |P; m\rangle &= \omega(-m\beta)|P; m\rangle; \quad X^\beta |X; m\rangle = |X; m+\beta\rangle \end{aligned} \tag{4.20}$$

where $\alpha, \beta \in \mathbb{Z}(d)$.

(2) The X, Z obey the relations

$$X^d = Z^d = \mathbf{1}; \qquad X^\beta Z^\alpha = Z^\alpha X^\beta \omega(-\alpha\beta); \quad \mathrm{Tr}(X) = \mathrm{Tr}(Z) = 0. \tag{4.21}$$

(3)

$$F X F^\dagger = Z; \qquad F Z F^\dagger = X^\dagger \tag{4.22}$$

Proof (1) In order to prove Eq. (4.20), we act with the matrices in Eq. (4.19) on the vectors in Eq. (4.4).

(2) In order to prove Eq. (4.21), we calculate the matrix elements of both sides in the position basis, taking into account Eq. (4.20).

(3) We act with F and $F^\dagger$ on the left and right hand side of Eq. (4.18), and using Eq. (4.8), we prove Eq. (4.22).

The position-momentum phase space is the toroidal lattice $\mathbb{Z}(d) \times \mathbb{Z}(d)$, and the relations $X^d = Z^d = \mathbf{1}$ indicate the toroidal nature of the phase space. As an example, Fig. 4.1 shows the $\mathbb{Z}(15) \times \mathbb{Z}(15)$ phase space.

Definition 4.4 General displacement operators are the unitary operators

$$D(\alpha, \beta) = Z^\alpha X^\beta \omega(-2^{-1}\alpha\beta); \quad \alpha, \beta \in \mathbb{Z}(d), \tag{4.23}$$

The following proposition generalizes Proposition 4.2, for general displacement operators.

Proposition 4.3 *(1)*

$$D(\alpha_1, \beta_1) D(\alpha_2, \beta_2) = D(\alpha_1 + \alpha_2, \beta_1 + \beta_2) \omega[2^{-1}(\alpha_1\beta_2 - \alpha_2\beta_1)] \tag{4.24}$$

The operators $D(\alpha, \beta)\omega(\gamma)$ form a representation of the $HW[\mathbb{Z}(d)]$ Heisenberg-Weyl group.

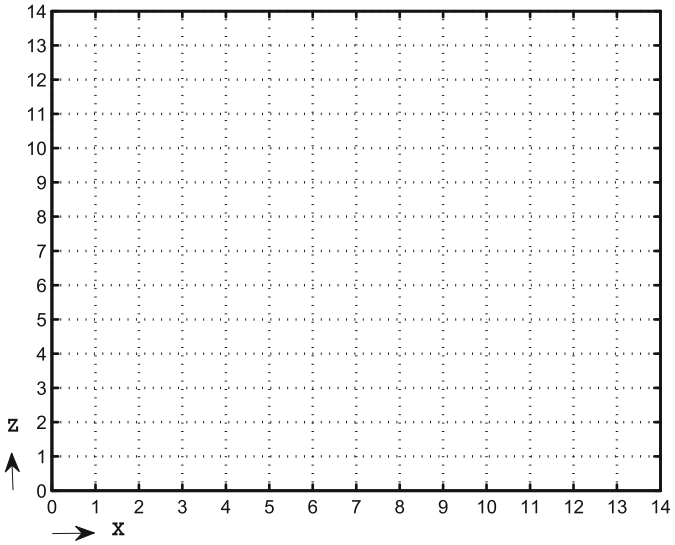

Fig. 4.1 The $\mathbb{Z}(15) \times \mathbb{Z}(15)$ phase space. There is periodicity in both directions, i.e., the phase space is a toroidal lattice. The operator X shifts the position states in the *horizontal direction*, and gives a phase to the momentum states (see Eq. 4.20). The operator Z shifts the momentum state in the *vertical direction*, and gives a phase to the position states

(2) The displacement operators act on the position and momentum states as follows:

$$\begin{aligned} D(\alpha,\beta)|X;m\rangle &= \omega(2^{-1}\alpha\beta+\alpha m)|X;m+\beta\rangle; \\ D(\alpha,\beta)|P;m\rangle &= \omega(-2^{-1}\alpha\beta-\beta m)|P;m+\alpha\rangle \end{aligned} \tag{4.25}$$

(3) The displacement operators act on the position and momentum operators as follows:

$$D(\alpha,\beta)x[D(\alpha,\beta)]^\dagger = x-\beta\mathbf{1}; \qquad D(\alpha,\beta)p[D(\alpha,\beta)]^\dagger = p-\alpha\mathbf{1} \tag{4.26}$$

(4)

$$FD(\alpha,\beta)F^\dagger = D(\beta,-\alpha). \tag{4.27}$$

Proof (1) The proof of Eq. (4.24), is based on Eq. (4.21). Therefore under multiplication the $D(\alpha,\beta)\omega(\gamma)$ have a closure property. It is also easily seen that the unity exists ($D(0,0)\omega(0)=\mathbf{1}$), that the inverse of $D(\alpha,\beta)\omega(\gamma)$ exists (it is $D(-\alpha,-\beta)\omega(-\gamma)$), and that associativity holds. Therefore the $D(\alpha,\beta)\omega(\gamma)$ form a group, which is the Heisenberg-Weyl group (see the Definition 4.2).
(2) The proof of Eq. (4.25), is based on Eq. (4.20).
(3) The proof of Eq. (4.26), is based on Eqs. (4.25), (4.7).
(4) The proof of Eq. (4.27), is based on Eq. (4.22).

The following proposition is a generalized resolution of the identity, that involves displacement operators. It will be used to prove several resolutions of the identity that involve coherent states, later.

Proposition 4.4 *Let θ be an arbitrary operator (acting on $H[\mathbb{Z}(d)]$). Then*

$$\frac{1}{d}\sum_{\alpha,\beta} D(\alpha,\beta)\frac{\theta}{\mathrm{Tr}(\theta)}[D(\alpha,\beta)]^{\dagger} = \mathbf{1}; \quad \mathrm{Tr}(\theta) \neq 0. \tag{4.28}$$

Proof We express θ as

$$\theta = \sum_{m,n} \theta_{mn}|X;m\rangle\langle X;n|. \tag{4.29}$$

Then using Eq. (4.25), we get

$$D(\alpha,\beta)\theta[D(\alpha,\beta)]^{\dagger} = \sum_{m,n} \omega[\alpha(m-n)]\theta_{mn}|X;m+\beta\rangle\langle X;n+\beta|. \tag{4.30}$$

Therefore

$$\begin{aligned}
&\frac{1}{d}\sum_{\alpha,\beta} D(\alpha,\beta)\theta[D(\alpha,\beta)]^{\dagger} = \frac{1}{d}\sum_{\alpha,\beta,m,n} \omega[\alpha(m-n)]\theta_{mn}|X;m+\beta\rangle\langle X;n+\beta| \\
&= \sum_{\beta,m,n} \delta(m,n)\theta_{mn}|X;m+\beta\rangle\langle X;n+\beta| = \sum_{\beta,n} \theta_{nn}|X;n+\beta\rangle\langle X;n+\beta| \\
&= \sum_{n} \theta_{nn}\mathbf{1} = \mathbf{1}\mathrm{Tr}(\theta).
\end{aligned} \tag{4.31}$$

4.4 Coherence in Finite Quantum Systems

4.4.1 Coherent States

We define coherent states in the context of finite quantum systems [46–50]:

Definition 4.5 The d^2 states given by

$$\begin{aligned}
&|C;\alpha,\beta\rangle = D(\alpha,\beta)|\eta\rangle; \quad \alpha,\beta \in \mathbb{Z}(d) \\
&|\eta\rangle = \sum_{m} \eta_m|X;m\rangle; \quad \sum_{m}|\eta_m|^2 = 1.
\end{aligned} \tag{4.32}$$

are coherent states. $|\eta\rangle$ is a 'generic' vector, called fiducial vector. The C in the notation indicates coherent states.

The fiducial vector is generic, if any subset of d coherent states, from the full set of d^2 coherent states, are linearly independent. Position and momentum states, are examples of non-generic fiducial vectors.

The use of the term 'coherent' for these states, is justified by the following properties:

Proposition 4.5 *(1) The coherent states resolve the identity, as follows:*

$$\frac{1}{d}\sum_{\alpha,\beta}|C;\alpha,\beta\rangle\langle C;\alpha,\beta| = \mathbf{1} \tag{4.33}$$

(2) Closure property: under displacements, coherent states are transformed into other coherent states.

$$D(\gamma,\delta)|C;\alpha,\beta\rangle = \omega[2^{-1}(\gamma\beta-\alpha\delta)]|C;\alpha+\gamma,\beta+\delta\rangle \tag{4.34}$$

Proof (1) Equation (4.33) is a special case of Eq. (4.28) with $\theta = |\eta\rangle\langle\eta|$.
(2) Equation (4.34) is proved using Eq. (4.24).

Using the resolution of the identity, we expand an arbitrary state $|s\rangle$ in terms of coherent states as

$$|s\rangle = \sum_{\alpha,\beta} s(\alpha,\beta)|C;\alpha,\beta\rangle; \qquad s(\alpha,\beta) = \frac{1}{d}\langle C;\alpha,\beta|s\rangle. \tag{4.35}$$

4.4.2 Coherent Density Matrices

We can define coherent density matrices (coherent mixed states), if we use a mixed state as fiducial vector:

Definition 4.6 Let σ_0 be a generic density matrix, which we call fiducial density matrix. The d^2 density matrices

$$\sigma(\alpha,\beta) = D(\alpha,\beta)\sigma_0 D^\dagger(\alpha,\beta), \tag{4.36}$$

are coherent density matrices.

The use of the term 'coherent' for these mixed states, is justified by the following properties [51]:

Proposition 4.6 *(1) The coherent density matrices resolve the identity, as follows:*

$$\frac{1}{d}\sum_{\alpha,\beta}\sigma(\alpha,\beta) = \mathbf{1} \tag{4.37}$$

(2) Closure property: under displacements, coherent density matrices are transformed into other coherent density matrices.

$$D(\gamma,\delta)\sigma(\alpha,\beta)D^{\dagger}(\gamma,\delta)=\sigma(\alpha+\gamma,\beta+\delta) \tag{4.38}$$

Proof (1) Equation (4.37) is a special case of Eq. (4.28) with $\theta=\sigma_0$.
(2) Equation (4.38) is proved using Eq. (4.24).

An arbitrary state can be expanded as

$$|s\rangle=\frac{1}{d}\sum_{\alpha,\beta}\sigma(\alpha,\beta)|s\rangle. \tag{4.39}$$

4.4.3 Coherent Projectors of Rank n

We consider the n-dimensional subspace of $H[\mathbb{Z}(d)]$ (where $n<d$) that contains all superpositions $\kappa_1|C;\alpha_1,\beta_1\rangle+...+\kappa_n|C;\alpha_n,\beta_n\rangle$. We call it coherent subspace and denote it as $H_C(\alpha_1,\beta_1;...;\alpha_n,\beta_n)$ or simply as $H_C(1,...,n)$ or as $H_C(A)$ where

$$A=\{(\alpha_1,\beta_1);...;(\alpha_n,\beta_n)\}\subset\mathbb{Z}(d)\times\mathbb{Z}(d);\quad |A|=n<d. \tag{4.40}$$

We call $\Pi_C(\alpha_1,\beta_1;...;\alpha_n,\beta_n)$ or simply $\Pi_C(1,...,n)$ or $\Pi_C(A)$, the projector to this subspace. The index C in the notation indicates 'coherent'. The subspace $H_C(A)$ is n-dimensional because we consider generic fiducial vectors, and consequently the rank of the projector $\Pi_C(A)$ is n.

We use the notation $\Pi_C^{\perp}(1,...,n)=\mathbf{1}-\Pi_C(1,...,n)$. The projector $\Pi_C(1,...,n)$ can be calculated inductively, using the Gram-Schmidt method, as follows:

$$\Pi_C(1,...,n)=\Pi_C(1,...,n-1)+\frac{\Pi_C^{\perp}(1,...,n-1)\Pi_C(n)\Pi_C^{\perp}(1,...,n-1)}{\mathrm{Tr}[\Pi_C^{\perp}(1,...,n-1)\Pi_C(n)]}. \tag{4.41}$$

We use the shorthand notation

$$A+(\gamma,\delta)=\{(\alpha_1+\gamma,\beta_1+\delta);...;(\alpha_n+\gamma,\beta_n+\delta)\}. \tag{4.42}$$

The $H_C(A)$ are coherent subspaces, and the $\Pi_C(A)$ are coherent projectors in the sense of the following properties [52, 53]:

Proposition 4.7 *(1) The coherent projectors $\Pi_C(A)$ resolve the identity as follows:*

$$\frac{1}{d|A|}\sum_{\gamma,\delta}\Pi_C[A+(\gamma,\delta)]=\mathbf{1} \tag{4.43}$$

(2) *Closure property: under displacements, the coherent projectors are transformed into other coherent projectors.*

$$D(\gamma,\delta)\Pi_C(A)D^\dagger(\gamma,\delta)=\Pi_C[A+(\gamma,\delta)]. \tag{4.44}$$

Proof (1) We use Eq. (4.28) with $\theta=\Pi_C(A)$ and we prove Eq. (4.43).
(2) We act on the left and right hand side of Eq. (4.41), with the $D(\gamma,\delta)$ and $D^\dagger(\gamma,\delta)$ correspondingly, and we prove Eq. (4.44).

Using the resolution of the identity in Eq. (4.43), we can express an arbitrary state $|s\rangle$ as

$$|s\rangle=\frac{1}{d|A|}\sum_{\gamma,\delta}\Pi_C[A+(\gamma,\delta)]|s\rangle. \tag{4.45}$$

Proposition 4.8 *The coherent projector $\Pi_C(A)$ can be expressed in terms of coherent states, as follows:*

$$\Pi_C(A)=\sum_{i,j}G_{ij}(A)|C;i\rangle\langle C;j|;\quad i,j\in A;\quad |A|<d \tag{4.46}$$

For simplicity we use here a single index, for a pair of indices. The $G_{ij}(A)$ is the inverse of the $|A|\times|A|$ Hermitian positive definite matrix

$$g_{ij}(A)=\langle C;i|C;j\rangle;\quad G=g^{-1};\quad i,j\in A. \tag{4.47}$$

Proof Acting with the $\Pi_C(A)$ given in Eq. (4.46), on a coherent state $|C;k\rangle$ with $k\in A$, we get

$$\Pi_C(A)|C;k\rangle=\sum_{i,j}G_{ij}(A)|C;i\rangle g_{jk}=\sum_i\delta_{ik}|C;i\rangle=|C;k\rangle. \tag{4.48}$$

Also if $|u\rangle$ is a state orthogonal to all $|C;k\rangle$ with $k\in A$ then $\Pi_C(A)|u\rangle=0$. Therefore the $\Pi_C(A)$ in Eq. (4.46), is a projector to the subspace $H_C(A)$.

Since $|A|\le d$, an arbitrary (normalized) state $|s\rangle$ in the $|A|$-dimensional space $H_C(A)$, can be written as

$$|s\rangle=\sum_i s_i|C;i\rangle;\quad i\in A \tag{4.49}$$

The coherent states $|C;i\rangle$ with $i\in A$, are linearly independent because we use a generic fiducial vector. Then

$$\langle s|s\rangle=\sum_{i,j}s_i^*s_jg_{ij}(A)=1. \tag{4.50}$$

This shows that the $|A| \times |A|$ Hermitian matrix $g_{ij}(A)$, is positive definite. Therefore it is invertible, and its inverse $G_{ij}(A)$ is also a Hermitian positive definite matrix.

4.5 Symplectic Transformations and the $Sp[2, \mathbb{Z}(d)]$ Group

In this section we study symplectic transformations in the context of finite quantum systems [54–56].

Definition 4.7 $S(\kappa, \lambda|\mu, \nu)$ are $d \times d$ unitary matrices which perform the following transformations on the operators X, Z:

$$\begin{aligned} &X(\kappa, \lambda) = S(\kappa, \lambda|\mu, \nu)X[S(\kappa, \lambda|\mu, \nu)]^\dagger = X^\kappa Z^\lambda \omega(2^{-1}\kappa\lambda) = D(\lambda, \kappa) \\ &Z(\mu, \nu) = S(\kappa, \lambda|\mu, \nu)Z[S(\kappa, \lambda|\mu, \nu)]^\dagger = X^\mu Z^\nu \omega(2^{-1}\mu\nu) = D(\nu, \mu) \\ &\kappa\nu - \lambda\mu = 1 \ (\mathrm{mod}(d)); \quad \kappa, \lambda, \mu, \nu \in \mathbb{Z}(d). \end{aligned} \tag{4.51}$$

These matrices are constructed explicitly below (and this proves their existence). We note the special cases

$$S(1, 0|0, 1) = \mathbf{1}; \quad S(0, 1| - 1, 0) = F, \tag{4.52}$$

where F is the Fourier matrix in Eq. (4.2).

Remark 4.2 We see in Eq. (4.51) that the $Z(\mu, \nu)$ does not depend on κ, λ. Consequently their eigenstates

$$|X(\mu, \nu); m\rangle = S(\kappa, \lambda|\mu, \nu)|X; m\rangle, \tag{4.53}$$

do not depend on κ, λ, and this is reflected in the notation. Similarly the $X(\kappa, \lambda)$ and their eigenstates

$$|P(\kappa, \lambda); m\rangle = S(\kappa, \lambda|\mu, \nu)|P; m\rangle, \tag{4.54}$$

do not depend on μ, ν. Special cases are:

$$\begin{aligned} &|X(0, 1); m\rangle = |X; m\rangle; \quad |X(-1, 0); m\rangle = |P; m\rangle \\ &|P(0, 1); m\rangle = |P; m\rangle; \quad |P(0, 1); m\rangle = |X; -m\rangle \end{aligned} \tag{4.55}$$

Proposition 4.9 *(1) The $d \times d$ matrices $S(\kappa, \lambda|\mu, \nu)$ form a unitary representation of the $Sp[2, \mathbb{Z}(d)]$ group.*

(2) The symplectic group $Sp[2, \mathbb{Z}(d)]$ is a group of outer automorphisms of the Heisenberg-Weyl group $HW[\mathbb{Z}(d)]$:

$$S(\kappa,\lambda|\mu,\nu)D(\alpha,\beta)[S(\kappa,\lambda|\mu,\nu)]^{\dagger} = D(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa)$$
$$\kappa,\lambda,\mu,\nu,\alpha,\beta \in \mathbb{Z}(d) \tag{4.56}$$

Proof (1) We use Eq. (4.51), first with the $S(\kappa_2,\lambda_2|\mu_2,\nu_2)$ and after that with the $S(\kappa_1,\lambda_1|\mu_1,\nu_1)$. We prove that there is a closure property for their product, analogous to Eq. (3.35), with the $S(\kappa,\lambda|\mu,\nu)$ corresponding to $g(\kappa,\lambda|\mu,\nu)$. In particular, we note that

$$g(\kappa_1,\lambda_1|\mu_1,\nu_1)\circ g(\kappa_2,\lambda_2|\mu_2,\nu_2) \;\rightarrow\; S(\kappa_1,\lambda_1|\mu_1,\nu_1)S(\kappa_2,\lambda_2|\mu_2,\nu_2). \tag{4.57}$$

The reason for introducing the right multiplication rule in Eq. (3.35), is because we wanted to have this correspondence. Therefore the $S(\kappa,\lambda|\mu,\nu)$ form a representation of the $Sp[2,\mathbb{Z}(d)]$ group with the multiplication rule

$$S(\kappa_1,\lambda_1|\mu_1,\nu_1)S(\kappa_2,\lambda_2|\mu_2,\nu_2) = S(\kappa,\lambda|\mu,\nu), \tag{4.58}$$

where the κ,λ,μ,ν have been given in Eq. (3.35).

(2) Eq. (4.56) is proved using Eq. (4.51).

The inverse of $S(\kappa,\lambda|\mu,\nu)$ (in analogy to Eq. (3.36)), is

$$[S(\kappa,\lambda|\mu,\nu)]^{-1} = S(\nu,-\lambda|-\mu,\kappa). \tag{4.59}$$

The following proposition constructs explicitly the analogues of the matrices $g(1,0|\xi_1,1)$, $g(1,\xi_2|0,1)$, $g(\xi_3,0|0,\xi_3^{-1})$ in Eq. (3.38):

Proposition 4.10 *The $S(1,0|\xi_1,1)$, $S(1,\xi_2|0,1)$, $S(\xi_3,0|0,\xi_3^{-1})$ (defined in general in Eq. 4.51) are given by:*

$$S(1,0|\xi_1,1) = \sum_m \omega(-2^{-1}\xi_1 m^2)|P;m\rangle\langle P;m|$$
$$S(1,\xi_2|0,1) = \sum_m \omega(2^{-1}\xi_2 m^2)|X;m\rangle\langle X;m|$$
$$S(\xi_3,0|0,\xi_3^{-1}) = \sum_n |X;\xi_3 n\rangle\langle X;n| = \sum_n |P;\xi_3^{-1}n\rangle\langle P;n| \tag{4.60}$$

For $\nu \in [\mathbb{Z}(d)]^*$,

$$S(\kappa,\lambda|\mu,\nu) = S(1,0|\xi_1,1)S(1,\xi_2|0,1)S(\xi_3,0|0,\xi_3^{-1}), \tag{4.61}$$

where the relationship between κ,λ,μ,ν and ξ_1,ξ_2,ξ_3 is given in Eqs. (3.39), (3.40). This is the Iwasawa decomposition.

Proof Acting with $S(1,0|\xi_1,1)$, $S(1,\xi_2|0,1)$, $S(\xi_3,0|0,\xi_3^{-1})$ in the form given in Eq. (4.60), on both sides of X, Z, we get

$$S(1,0|\xi_1,1)X[S(1,0|\xi_1,1)]^\dagger = D(0,1)$$
$$S(1,0|\xi_1,1)Z[S(1,0|\xi_1,1)]^\dagger = D(1,\xi_1) \tag{4.62}$$

and

$$S(1,\xi_2|0,1)X[S(1,\xi_2|0,1)]^\dagger = D(\xi_2,1)$$
$$S(1,\xi_2|0,1)Z[S(1,\xi_2|0,1)]^\dagger = D(1,0) \tag{4.63}$$

and

$$S(\xi_3,0|0,\xi_3^{-1})XS(\xi_3,0|0,\xi_3^{-1})^\dagger = D(0,\xi_3)$$
$$S(\xi_3,0|0,\xi_3^{-1})ZS(\xi_3,0|0,\xi_3^{-1})^\dagger = D(\xi_3^{-1},0) \tag{4.64}$$

They confirm the definition in Eq. (4.51), for these values of the parameters. Therefore the expressions for $S(1,0|\xi_1,1)$, $S(1,\xi_2|0,1)$, $S(\xi_3,0|0,\xi_3^{-1})$ in Eq. (4.60), are the correct ones.

We have shown earlier, that the $S(\kappa,\lambda|\mu,\nu)$ form a representation of $Sp[2,\mathbb{Z}(d)]$, with the $S(\kappa,\lambda|\mu,\nu)$ corresponding to $g(\kappa,\lambda|\mu,\nu)$. Eq. (4.61) is analogous to Eq. (3.38) (for $\nu \in [\mathbb{Z}(d)]^*$).

Lemma 4.1 *For* $\mu, \nu \in [\mathbb{Z}(d)]^*$

$$\langle X;r|S(\kappa,\lambda|\mu,\nu)|X;n\rangle = \frac{1}{d}G[-2^{-1}\mu\nu^{-1};\mathbb{Z}(d)] \times \omega\left[2^{-1}\lambda\nu^{-1}n^2 + 2^{-1}\mu^{-1}\nu^{-1}(r\nu-n)^2\right], \tag{4.65}$$

where $G[s;\mathbb{Z}(d)]$ *is the Gauss sum in Eq. (3.5).*

Proof From Eqs. (4.60), (4.61) we get

$$S(\kappa,\lambda|\mu,\nu) = \frac{1}{d}\sum_{m,n,r}\omega(A)|X;r\rangle\langle X;n|$$
$$A = -2^{-1}\mu\nu^{-1}m^2 + 2^{-1}\lambda\nu^{-1}n^2 - \nu^{-1}mn + mr. \tag{4.66}$$

Then we change the variable m into $M = m - \mu^{-1}(r\nu - n)$, and we prove the lemma.

Example 4.1 In $\mathbb{Z}(3)$, we used Eq. (4.65) to calculate $S(2,0|2,2)$ in the position basis:

$$S(2,0|2,2) = \frac{1}{3}[1+2\omega(1)]\begin{pmatrix} 1 & \omega(-1) & \omega(-1) \\ \omega(-1) & \omega(-1) & 1 \\ \omega(-1) & 1 & \omega(-1) \end{pmatrix}$$
$$\omega(1) = \exp\left(\frac{2\pi i}{3}\right); \quad G[1;\mathbb{Z}(3)] = 1 + 2\omega(1) \tag{4.67}$$

We give the Iwasawa decomposition, for this example. For $\kappa = \mu = \nu = 2$ and $\lambda = 0$, we get $\xi_1 = 1$, $\xi_2 = 0$ and $\xi_3 = 2$. Therefore

$$\begin{aligned} S(1,0|\xi_1,1) &= F^\dagger \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega(1) & 0 \\ 0 & 0 & \omega(1) \end{pmatrix} F \\ S(1,\xi_2|0,1) &= \mathbf{1} \\ S(\xi_3,0|0,\xi_3^{-1}) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{aligned} \tag{4.68}$$

Here F is the Fourier matrix given (for the general case) in Eq. (4.2). The Iwasawa product in Eq. (4.61) with these matrices, gives the matrix $S(2,0|2,2)$.

Remark 4.3 The metaplectic group covers the symplectic group twice, and it has been studied in [54, 55].

4.6 The $HWSp[\mathbb{Z}(d)]$ Group of Displacements and Symplectic Transformations

In this section we study a group that combines both displacements and symplectic transformations. We use the self-explanatory notation $HWSp[\mathbb{Z}(d)]$ for this group.

Proposition 4.11 *The unitary operators*

$$T(\kappa,\lambda|\mu,\nu|\alpha,\beta,\gamma) = S(\kappa,\lambda|\mu,\nu)D(\alpha,\beta)\omega(\gamma) \tag{4.69}$$

where $\kappa, \lambda, \mu, \nu, \alpha, \beta, \gamma \in \mathbb{Z}(d)$, form a group which we denote as $HWSp[\mathbb{Z}(d)]$, and which is the semidirect product of the $HW[\mathbb{Z}(d)]$ by the $Sp[2,\mathbb{Z}(d)]$:

$$HWSp[\mathbb{Z}(d)] = HW[\mathbb{Z}(d)] \rtimes Sp[2,\mathbb{Z}(d)]. \tag{4.70}$$

Proof We first give the closure property under multiplication:

$$\begin{aligned} &T(\kappa_1,\lambda_1|\mu_1,\nu_1|\alpha_1,\beta_1,\gamma_1)T(\kappa_2,\lambda_2|\mu_2,\nu_2|\alpha_2,\beta_2,\gamma_2) \\ &= T(\kappa,\lambda|\mu,\nu|\alpha,\beta,\gamma) \end{aligned} \tag{4.71}$$

where the $\kappa, \lambda, \mu, \nu$ are given in Eq. (3.35), and

$$\begin{aligned} \alpha &= \alpha_1\kappa_2 - \beta_1\lambda_2 + \alpha_2 \\ \beta &= \beta_1\nu_2 - \alpha_1\mu_2 + \beta_2 \\ \gamma &= \gamma_1 + \gamma_2 + 2^{-1}\left[(\alpha_1\kappa_2 - \beta_1\lambda_2)\beta_2 - (\beta_1\nu_2 - \alpha_1\mu_2)\alpha_2\right] \end{aligned} \tag{4.72}$$

The inverse of $T(\kappa, \lambda|\mu, \nu|\alpha, \beta, \gamma)$ is

$$[T(\kappa, \lambda|\mu, \nu|\alpha, \beta, \gamma)]^{-1} = T(\nu, -\lambda|-\mu, \kappa|A, B, -\gamma)$$
$$A = -\alpha\nu - \beta\lambda; \quad B = -\alpha\mu - \beta\kappa \tag{4.73}$$

The Heisenberg-Weyl group is a normal subgroup of $HWSp[\mathbb{Z}(d)]$. Indeed, we show that:

$$T(\kappa, \lambda|\mu, \nu|\alpha, \beta, \gamma)\ D(A, B)\ [T(\kappa, \lambda|\mu, \nu|\alpha, \beta, \gamma)]^{\dagger}$$
$$= D(A\nu + B\lambda, A\mu + B\kappa)\ \omega(B\alpha - A\beta) \tag{4.74}$$

The $Sp[2, \mathbb{Z}(d)]$ is also a subgroup of $HWSp[\mathbb{Z}(d)]$ and

$$Sp[2, \mathbb{Z}(d)] \bigcap HW[\mathbb{Z}(d)] = \{\mathbf{1}\}. \tag{4.75}$$

Therefore $HWSp[\mathbb{Z}(d)]$ is the semidirect product of the $HW[\mathbb{Z}(d)]$ by the $Sp[2, \mathbb{Z}(d)]$.

4.7 Parity Operators

Parity operators have been studied extensively in the context of the harmonic oscillator (e.g., [57–61]). In the present context they are defined as follows.

Definition 4.8 (1) The parity operator around the origin in phase space, is given by

$$P(0, 0) = F^2; \quad [P(0, 0)]^2 = \mathbf{1}; \quad [P(0, 0)]^{\dagger} = P(0, 0). \tag{4.76}$$

(2) The parity operator around the point (α, β) in phase space (displaced parity operator), is given by:

$$P(\alpha, \beta) = D(\alpha, \beta)P(0, 0)[D(\alpha, \beta)]^{\dagger}; \quad [P(\alpha, \beta)]^2 = \mathbf{1} \tag{4.77}$$

Some properties of the parity operator, are given below:

Proposition 4.12 *(1)*

$$P(\alpha, \beta)|X; m\rangle = \omega(2\alpha\beta - 2\alpha m)|X; 2\beta - m\rangle$$
$$P(\alpha, \beta)|P; m\rangle = \omega(-2\alpha\beta - 2\beta m)|P; 2\alpha - m\rangle \tag{4.78}$$

(2)

$$P(0, 0)D(\alpha, \beta)P(0, 0) = D(-\alpha, -\beta) \tag{4.79}$$

(3)

$$[P(0,0), S(\kappa,\lambda|\mu,\nu)] = 0. \tag{4.80}$$

(4)

$$P(\alpha,\beta) = D(2\alpha,2\beta)P(0,0) = P(0,0)[D(2\alpha,2\beta)]^{\dagger} \tag{4.81}$$

(5) The product of two displaced parity operators is a displacement operator:

$$P(\alpha,\beta)P(\gamma,\delta) = D(2\alpha-2\gamma,2\beta-2\delta)\omega(2\beta\gamma-2\alpha\delta) \tag{4.82}$$

(6)

$$S(\kappa,\lambda|\mu,\nu)P(\alpha,\beta)[S(\kappa,\lambda|\mu,\nu)]^{\dagger} = P(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa) \tag{4.83}$$

Proof (1) From Eq. (4.5) it follows that $P(0,0)|X;m\rangle = |X;-m\rangle$ and $P(0,0)$ $|P;m\rangle = |P;-m\rangle$. We then use Eq. (4.24) and we prove Eq. (4.78).

(2) From Eq. (4.25) it follows that

$$D(\alpha,\beta) = \sum_m \omega(2^{-1}\alpha\beta+\alpha m)|X;m+\beta\rangle\langle X;m| \tag{4.84}$$

Therefore

$$\begin{aligned} P(0,0)D(\alpha,\beta)P(0,0) &= \sum_m \omega(2^{-1}\alpha\beta+\alpha m)|X;-m-\beta\rangle\langle X;-m| \\ &= D(-\alpha,-\beta) \end{aligned} \tag{4.85}$$

(3) We first prove that the $P(0,0)$ commutes with the $S(1,0|\xi_1,1)$.

$$P(0,0)S(1,0|\xi_1,1) = \sum_m \omega(-2^{-1}\xi_1 m^2)|P;-m\rangle\langle P;m| \tag{4.86}$$

Also

$$\begin{aligned} S(1,0|\xi_1,1)P(0,0) &= \sum_m \omega(-2^{-1}\xi_1 m^2)|P;m\rangle\langle P;-m| \\ &= \sum_n \omega(-2^{-1}\xi_1 n^2)|P;-n\rangle\langle P;n| = P(0,0)S(1,0|\xi_1,1). \end{aligned} \tag{4.87}$$

In a similar way we prove that $P(0,0)$ commutes with the $S(1,\xi_2|0,1)$ and $S(\xi_3,0|0,\xi_3^{-1})$. From Eq. (4.61), follows that the $P(0,0)$ commutes with the $S(\kappa,\lambda|\mu,\nu)$.

(4) We prove this using the definition in Eqs. (4.77) and (4.85).
(5) This follows from the definition in Eqs. (4.77) and (4.24).
(6) This follows from Eq. (4.56), taking into account that the $P(0,0)$ and $S(\kappa,\lambda|\mu,\nu)$ commute.

An important set of properties of both the displacement operators and the parity operators, are the marginal properties. They will be used later to prove marginal properties for the Weyl and Wigner functions.

Proposition 4.13 *Let $\Pi_X(\alpha)$, $\Pi_P(\alpha)$, be projectors to position and momentum states:*

$$\Pi_X(\alpha) = |X;\alpha\rangle\langle X;\alpha|; \quad \Pi_P(\alpha) = |P;\alpha\rangle\langle P;\alpha|. \tag{4.88}$$

The indices X, P in the notation indicate 'position' and 'momentum'.

(1) The displacement operators obey the following 'marginal relations' along the 'horizontal' and 'vertical' lines in the phase space $\mathbb{Z}(d)\times\mathbb{Z}(d)$:

$$\begin{aligned}
\frac{1}{d}\sum_{\beta=0}^{d-1} D(\alpha,\beta) &= \Pi_P(2^{-1}\alpha)P(0,0)\\
\frac{1}{d}\sum_{\alpha=0}^{d-1} D(\alpha,\beta) &= \Pi_X(2^{-1}\beta)P(0,0)\\
\frac{1}{d}\sum_{\alpha,\beta} D(\alpha,\beta) &= P(0,0)
\end{aligned} \tag{4.89}$$

(2) The parity operators obey the the following 'marginal relations' along the 'horizontal' and 'vertical' lines in the phase space $\mathbb{Z}(d)\times\mathbb{Z}(d)$:

$$\begin{aligned}
\frac{1}{d}\sum_{\beta=0}^{d-1} P(\alpha,\beta) &= \Pi_P(\alpha)\\
\frac{1}{d}\sum_{\alpha=0}^{d-1} P(\alpha,\beta) &= \Pi_X(\beta)\\
\frac{1}{d}\sum_{\alpha,\beta} P(\alpha,\beta) &= \mathbf{1}
\end{aligned} \tag{4.90}$$

Proof (1) In order to prove the first two relations, we take the matrix elements of both sides with $\langle X;m|$ and $|X;n\rangle$, and we use Eq. (4.25). For the third relation, we take the summation over α of both sides of the first relation (or the summation over β of both sides of the second relation).

(2) In order to prove these three relations, we multiply by $P(0,0)$ the three relations in the first part of this proposition.

Proposition 4.14 *The displacement operators are related to parity operators through Fourier transforms:*

$$\frac{1}{d}\sum_{\alpha,\beta} D(\alpha,\beta)\omega(\beta\gamma-\alpha\delta) = P(\gamma,\delta) \tag{4.91}$$

In this sense the parameters α, β in the displacement operators $D(\alpha,\beta)$, are dual to the parameters γ,δ in the parity operators $P(\gamma,\delta)$. The inverse Fourier transform gives

$$\frac{1}{d}\sum_{\gamma,\delta} P(\gamma,\delta)\omega(-\beta\gamma+\alpha\delta) = D(\alpha,\beta) \tag{4.92}$$

Proof We multiply the third relation in Eq. (4.89) by $D(\gamma,\delta)$ on the left, and by $[D(\gamma,\delta)]^\dagger$ on the right. We then use the multiplication rule of Eq. (4.24), to prove Eq. (4.91). Inverting the Fourier transform, we then prove Eq. (4.92).

Equations (4.89), (4.90) are marginal properties along the 'horizontal or position' axis, and 'vertical or momentum ' axis, in the $\mathbb{Z}(d)\times\mathbb{Z}(d)$ phase space (finite geometry). Performing symplectic transformations on them, we get marginal properties along other axes, which are the Radon transform. We also give the inverse Radon transform, which is used later with Wigner and Weyl functions, for quantum tomography.

We use the notation

$$\begin{aligned}\Pi_X^{(\mu,\nu)}(\alpha) &= S(\kappa,\lambda|\mu,\nu)\Pi_X(\alpha)[S(\kappa,\lambda|\mu,\nu)]^\dagger\\ &= |X(\mu,\nu);\alpha\rangle\langle X(\mu,\nu);\alpha|\end{aligned} \tag{4.93}$$

and

$$\begin{aligned}\Pi_P^{(\kappa,\lambda)}(\alpha) &= S(\kappa,\lambda|\mu,\nu)\Pi_P(\alpha)[S(\kappa,\lambda|\mu,\nu)]^\dagger\\ &= |P(\kappa.\lambda);\alpha\rangle\langle P(\kappa.\lambda);\alpha|\end{aligned} \tag{4.94}$$

They are projectors associated with symplectically transformed position and momentum states. We note that

$$\Pi_X^{(0,1)}(\alpha) = \Pi_X(\alpha);\quad \Pi_X^{(-1,0)}(\alpha) = \Pi_P(\alpha). \tag{4.95}$$

Proposition 4.15 *(1) The Radon transform is given by:*

$$\frac{1}{d}\sum_{\beta} P(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa) = \Pi_P^{(\kappa,\lambda)}(\alpha)$$
$$\frac{1}{d}\sum_{\alpha} P(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa) = \Pi_X^{(\mu,\nu)}(\beta) \tag{4.96}$$

(2) The inverse Radon transform is given by:

$$D(\lambda\beta,\kappa\beta) = \sum_{\alpha} \Pi_P^{(\kappa,\lambda)}(\alpha)\omega(-\alpha\beta)$$
$$D(\nu\alpha,\mu\alpha) = \sum_{\beta} \Pi_X^{(\mu,\nu)}(\beta)\omega(\alpha\beta) \tag{4.97}$$

Proof (1) We perform symplectic transformations on both sides of Eq. (4.90), and using Eq. (4.83), we get Eq. (4.96).
(2) We perform a two-dimensional Fourier transform on Eq. (4.96), and using Eq. (4.92), we get Eq. (4.97).

4.8 Wigner and Weyl Functions

The Wigner and Weyl functions play a central role in phase space methods in Quantum mechanics (e.g., [62–68]). In particular the subject of tomography constructs the Wigner function, from its Radon transforms which can be measured experimentally (e.g., [69–71]). The Wigner and Weyl functions also play an important role in Signal Processing (e.g., [72, 73]) where the Weyl function is known as ambiguity function. Wigner functions in the context of finite quantum systems have been discussed in [74–80].

Definition 4.9 Let θ be an arbitrary operator. The corresponding Wigner function $W(\alpha,\beta;\theta)$ and Weyl function $\widetilde{W}(\alpha,\beta;\theta)$, are defined as:

$$W(\alpha,\beta;\theta) = \mathrm{Tr}[\theta P(\alpha,\beta)]; \quad \widetilde{W}(\alpha,\beta;\theta) \equiv \mathrm{Tr}[\theta D(\alpha,\beta)]. \tag{4.98}$$

The Wigner function is intimately related to the displaced parity operators, and the Weyl function to the displacement operators. If θ is a density matrix, the Wigner function can be interpreted as a pseudo-probability distribution of the particle in the position-momentum phase space (which might take negative values). The marginal properties in Eq. (4.106) below, support this interpretation.

The Weyl function is a generalized correlation function. For $\theta = |s\rangle\langle s|$, the Weyl function is the overlap of $|s\rangle$ with the displaced state $D(\alpha,\beta)|s\rangle$. In this sense the

parameters α, β entering in the Weyl function are position and momentum increments.

Proposition 4.16 *For an arbitrary operator θ, let*

$$\theta_X(m,n) \equiv \langle X; m|\theta|X; n\rangle; \quad \theta_P(m,n) \equiv \langle P; m|\theta|P; n\rangle \tag{4.99}$$

(1) The Wigner function is the Fourier transform of $\theta_X(m,n)$ and $\theta_P(m,n)$:

$$\begin{aligned} W(\alpha,\beta;\theta) &= \sum_n \omega(2\alpha n)\theta_X(\beta-n,\beta+n) \\ &= \sum_n \omega(2\beta n)\theta_P(\alpha+n,\alpha-n) \end{aligned} \tag{4.100}$$

(2) The Weyl function is also the Fourier transform of $\theta_X(m,n)$ and $\theta_P(m,n)$:

$$\begin{aligned} \widetilde{W}(\alpha,\beta;\theta) &= \sum_n \omega(\alpha n)\theta_X(n-2^{-1}\beta,n+2^{-1}\beta) \\ &= \sum_n \omega(-\beta n)\theta_P(n-2^{-1}\alpha,n+2^{-1}\alpha) \end{aligned} \tag{4.101}$$

(3) The Weyl function is related to the Wigner function through the Fourier transform:

$$\widetilde{W}(\alpha,\beta;\theta) = \frac{1}{d}\sum_{\gamma,\delta} W(\theta;\gamma,\delta)\omega(\alpha\delta-\beta\gamma) \tag{4.102}$$

In this sense the parameters α, β in the Weyl function $\widetilde{W}(\alpha,\beta;\theta)$ are dual to the parameters γ, δ in the Wigner function $W(\gamma,\delta;\theta)$.

Proof (1) We express the definition of the Wigner function in Eq. (4.98), as

$$W(\alpha,\beta;\theta) = \sum_n \langle X; n|\theta\, P(\alpha,\beta)]|X; n\rangle. \tag{4.103}$$

We then use Eq. (4.78), to prove the first relation in Eq. (4.100). In a similar way we prove the second relation.

(2) We express the definition of the Weyl function in Eq. (4.98), as

$$\widetilde{W}(\alpha,\beta;\theta) = \sum_n \langle X; n|\theta\, D(\alpha,\beta)]|X; n\rangle. \tag{4.104}$$

We then use Eq. (4.25), to prove the first relation in Eq. (4.101). In a similar way we prove the second relation.

(3) We multiply both sides of Eq. (4.91) by θ, and then we take the trace.

Proposition 4.17 *An operator θ can be expanded in terms of the displacement operators with the Weyl functions as coefficients, and in terms of the displaced parity operators with the Wigner functions as coefficients:*

$$\theta = \frac{1}{d}\sum_{\alpha,\beta} \widetilde{W}(-\alpha,-\beta;\theta)D(\alpha,\beta) = \frac{1}{d}\sum_{\alpha,\beta} W(\alpha,\beta;\theta)P(\alpha,\beta) \tag{4.105}$$

Proof We take the matrix elements of both sides with $\langle X;m|$ and $|X;n\rangle$, and then use Eqs. (4.100), (4.101).

The following proposition is based on proposition 4.13, and it gives marginal properties of the Wigner and Weyl functions, along the horizontal and vertical axes, in the $\mathbb{Z}(d)\times\mathbb{Z}(d)$ phase space.

Proposition 4.18 *(1) The Wigner function obeys the following 'marginal properties':*

$$\begin{aligned}
\frac{1}{d}\sum_{\beta=0}^{d-1} W(\alpha,\beta;\theta) &= \theta_P(\alpha,\alpha)\\
\frac{1}{d}\sum_{\alpha=0}^{d-1} W(\alpha,\beta;\theta) &= \theta_X(\beta,\beta)\\
\frac{1}{d}\sum_{\alpha,\beta} W(\alpha,\beta;\theta) &= \mathrm{Tr}\theta
\end{aligned} \tag{4.106}$$

(2) The Weyl function obeys the following 'marginal properties':

$$\begin{aligned}
\frac{1}{d}\sum_{\beta=0}^{d-1} \widetilde{W}(\alpha,\beta;\theta) &= \theta_P(-2^{-1}\alpha, 2^{-1}\alpha)\\
\frac{1}{d}\sum_{\alpha=0}^{d-1} \widetilde{W}(\alpha,\beta;\theta) &= \theta_X(-2^{-1}\beta, 2^{-1}\beta)\\
\frac{1}{d}\sum_{\alpha,\beta} \widetilde{W}(\alpha,\beta;\theta) &= W(0,0;\theta)
\end{aligned} \tag{4.107}$$

Proof (1) We multiply both sides of Eq. (4.90) by θ, and take the trace.
(2) We multiply both sides of Eq. (4.89) by θ, and take the trace.

The Wigner and Weyl functions are related to the matrix elements of the operator θ, through the Fourier transforms in Eqs. (4.100), (4.101). Parseval's theorem in this context, leads to the following marginal properties of the Wigner and Weyl functions, that involve the square of their absolute values [23]

Proposition 4.19 *(1)*

$$\begin{aligned}
\frac{1}{d}\sum_{\beta=0}^{d-1}|W(\alpha,\beta;\theta)|^2 &= \sum_{k=0}^{d-1}|\theta_P(k,2\alpha-k)|^2\\
\frac{1}{d}\sum_{\alpha=0}^{d-1}|W(\alpha,\beta;\theta)|^2 &= \sum_{k=0}^{d-1}|\theta_X(k,2\beta-k)|^2\\
\frac{1}{d}\sum_{\alpha,\beta}|W(\alpha,\beta;\theta)|^2 &= \mathrm{Tr}[\theta\theta^\dagger]
\end{aligned} \tag{4.108}$$

(2)

$$\begin{aligned}
\frac{1}{d}\sum_{\beta=0}^{d-1}|\widetilde{W}(\alpha,\beta;\theta)|^2 &= \sum_{\ell=0}^{d-1}|\theta_P(\ell,\alpha+\ell)|^2\\
\frac{1}{d}\sum_{\alpha=0}^{d-1}|\widetilde{W}(\alpha,\beta;\theta)|^2 &= \sum_{\ell=0}^{d-1}|\theta_X(\ell,\beta+\ell)|^2\\
\frac{1}{d}\sum_{\alpha,\beta}|\widetilde{W}(\alpha,\beta;\theta)|^2 &= \mathrm{Tr}[\theta\theta^\dagger]
\end{aligned} \tag{4.109}$$

Proof (1) The first two relations in Eq. (4.108), are Parseval's relations for the Fourier transforms that involve the Wigner function in Eq. (4.100). The last relation follows easily from the first two.

(2) The first two relations in Eq. (4.109), are Parseval's relations for the Fourier transforms that involve the Weyl function in Eq. (4.101). The last relation follows easily from the first two.

The following proposition gives the Radon transform, and is used in quantum tomography. The first part generalizes Proposition 4.18, and gives the marginal properties of the Wigner function, along arbitrary axes in the $\mathbb{Z}(d)\times\mathbb{Z}(d)$ phase space. The second part gives the inverse Radon transform.

Proposition 4.20 *(1) The Radon transform is given by:*

$$\begin{aligned}
\frac{1}{d}\sum_{\beta} W(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa;\theta) &= \mathrm{Tr}[\theta\Pi_P^{(\kappa,\lambda)}(\alpha)]\\
\frac{1}{d}\sum_{\alpha} W(\alpha\nu+\beta\lambda,\alpha\mu+\beta\kappa;\theta) &= \mathrm{Tr}[\theta\Pi_X^{(\mu,\nu)}(\beta)]
\end{aligned} \tag{4.110}$$

(2) The inverse Radon transform is given by:

$$\widetilde{W}(\lambda\beta, \kappa\beta; \theta) = \sum_{\alpha} \mathrm{Tr}[\theta \Pi_P^{(\kappa,\lambda)}(\alpha)]\omega(-\alpha\beta)$$
$$\widetilde{W}(\nu\alpha, \mu\alpha; \theta) = \sum_{\beta} \mathrm{Tr}[\theta \Pi_X^{(\mu,\nu)}(\beta)]\omega(\alpha\beta) \tag{4.111}$$

Proof (1) We multiply both sides of Eq. (4.96) by θ, and take the trace.
(2) We multiply both sides of Eq. (4.97) by θ, and take the trace.

If θ is a density matrix, the $\mathrm{Tr}[\theta \Pi_P^{(\kappa,\lambda)}(\alpha)]$ are probabilities which can be measured experimentally. Using the inverse Radon transform, we can calculate the Weyl function, and then from Eq. (4.105) the density matrix θ.

Example 4.2 In $H[\mathbb{Z}(3)]$ we consider the state

$$|s\rangle = \frac{1}{\sqrt{6}}[|X;0\rangle + i|X;1\rangle + 2|X;2\rangle] \tag{4.112}$$

Using Eq. (4.100), we calculated the Wigner function, which we present here as 3×3 matrix:

$$W = \begin{pmatrix} 0.166 & 0.833 & 0.666 \\ -0.410 & -0.166 & 0.955 \\ 0.744 & -0.166 & 0.378 \end{pmatrix} \tag{4.113}$$

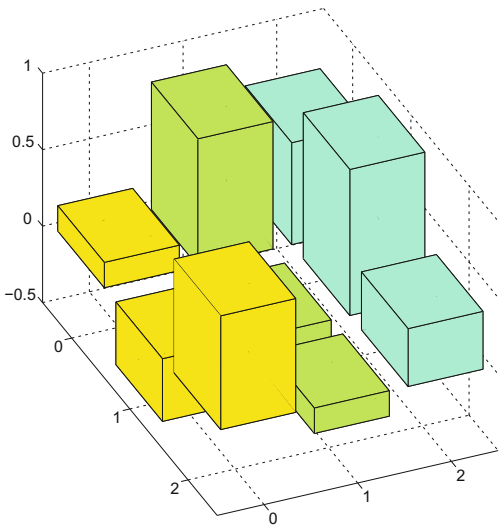

Fig. 4.2 The Wigner function in Eq. (4.113), for the state in Eq. (4.112)

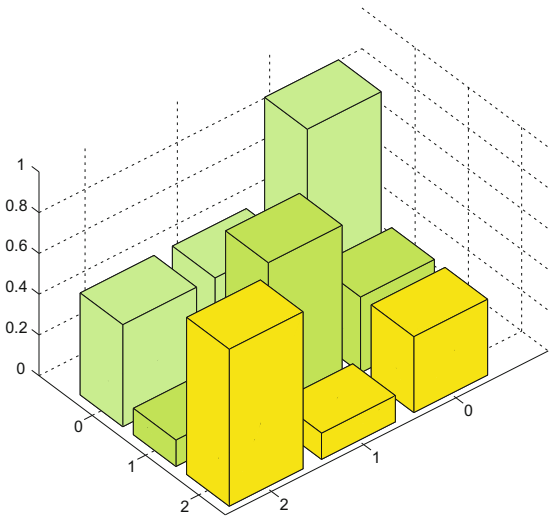

Fig. 4.3 The absolute value of the Weyl function in Eq. (4.114), for the state in Eq. (4.112)

A plot of this Wigner function is shown in Fig. 4.2. We also used Eq. (4.101), and calculated the Weyl function:

$$\widetilde{W} = \begin{pmatrix} 1 & 0.333 + 0.166i & 0.333 - 0.166i \\ -0.250 - 0.433i & -0.311 + 0.705i & -0.022 - 0.128i \\ -0.250 + 0.433i & -0.022 + 0.128i & -0.311 - 0.705i \end{pmatrix}. \quad (4.114)$$

A plot of the absolute value of this Weyl function is shown in Fig. 4.3.

4.9 Factorization of $\Sigma[\mathbb{Z}(d)]$ Based on the Chinese Remainder Theorem

In Sect. 3.2, we have considered the ring $\mathbb{Z}(d)$, and factorized d as $d = d_1 \times ... \times d_N$ where any pair of the factors $d_1, ..., d_N$ are coprime. We then introduced two bijective maps between $\mathbb{Z}(d)$ and $\mathbb{Z}(d_1) \times ... \times \mathbb{Z}(d_N)$ given in Eqs. (3.21), (3.22). Based on these maps we will now factorize the 'whole quantum formalism' of the system $\Sigma[\mathbb{Z}(d)]$, in terms of quantum formalisms of the systems $\Sigma[\mathbb{Z}(d_i)]$, where $i = 1, ..., N$ [14, 81–83]. We denote this as

$$\Sigma[\mathbb{Z}(d)] = \Sigma[\mathbb{Z}(d_1)] \otimes \Sigma[\mathbb{Z}(d_2)] \otimes ... \otimes \Sigma[\mathbb{Z}(d_n)]. \quad (4.115)$$

Proposition 4.21 *We map the position basis $|X; m\rangle$ in the Hilbert space $H[\mathbb{Z}(d)]$, in the following product of position bases in $H[\mathbb{Z}(d_1)] \otimes ... \otimes H[\mathbb{Z}(d_N)]$:*

$$|X; m\rangle \leftrightarrow |X_1; \overline{m}_1\rangle \otimes ... \otimes |X_N; \overline{m}_N\rangle. \tag{4.116}$$

The map of Eq. (3.22) is used here. Then

(1) The basis of momentum states in $H[\mathbb{Z}(d)]$, is mapped into a product of momentum bases in $H[\mathbb{Z}(d_1)] \otimes ... \otimes H[\mathbb{Z}(d_N)]$:

$$|P; m\rangle \leftrightarrow |P_1; m_1\rangle \otimes ... \otimes |P_N; m_N\rangle \tag{4.117}$$

The dual map of Eq. (3.21) is used here.

(2) The Fourier transform F in $H[\mathbb{Z}(d)]$, is factorized in terms of Fourier transforms F_1, ..., F_N in $H[\mathbb{Z}(d_1)]$, ..., $H[\mathbb{Z}(d_N)]$, as

$$\begin{aligned} F &= F_1 \otimes ... \otimes F_N \\ F_i &= \sum_{m_i} |P_i; m_i\rangle\langle X_i; \overline{m}_i| = \sum_{m_i} |P_i; m_i\rangle\langle X_i; m_i t_i| \end{aligned} \tag{4.118}$$

(3) The displacement operators in $H[\mathbb{Z}(d)]$, are factorized in terms of displacement operators in $H[\mathbb{Z}(d_1)]$, ..., $H[\mathbb{Z}(d_N)]$, as

$$D(\alpha, \beta) = D_1(\alpha_1, \overline{\beta}_1) \otimes ... \otimes D_N(\alpha_N, \overline{\beta}_N). \tag{4.119}$$

Also the parity operators in $H(d)$, are factorized in terms of parity operators in $H(d_1)$, ..., $H(d_N)$, as

$$P(\alpha, \beta) = P_1(\alpha_1, \overline{\beta}_1) \otimes ... \otimes P_N(\alpha_N, \overline{\beta}_N). \tag{4.120}$$

Proof (1) We use Eqs. (3.26), (4.116) to express the momentum states as

$$\begin{aligned} |P; m\rangle &= d^{-1/2} \sum \omega(mn)|X; n\rangle \\ &= (d_1...d_N)^{-1/2} \sum \omega_1(m_1\overline{n}_1)...\omega_N(m_N\overline{n}_N)|X_1; \overline{n}_1\rangle \otimes ... \otimes |X_N; \overline{n}_N\rangle \\ &= |P_1; m_1\rangle \otimes ... \otimes |P_N; m_N\rangle \end{aligned} \tag{4.121}$$

(2) The Fourier transform can be written as

$$F = \sum_m |P; m\rangle\langle X; m| = \sum \bigotimes_{i=1}^{N} |P_i; m_i\rangle\langle X_i; \overline{m}_i| = \bigotimes_{i=1}^{N} F_i \tag{4.122}$$

where F_i is given in Eq. (4.118).

(3) We first prove that:

$$Z = \sum_m |P;\ m+1\rangle\langle P;\ m| = \sum_m \bigotimes_{i=1}^{N} |P_i; m_i+1\rangle\langle P_i; m_i| = \bigotimes_{i=1}^{N} Z_i$$
$$X = \sum_m |X; m+1\rangle\langle X; m| = \sum_m \bigotimes_{i=1}^{N} |X_i; \overline{m}_i + t_i\rangle\langle X_i; \overline{m}_i| = \bigotimes_{i=1}^{N} X_i^{t_i} \quad (4.123)$$

Therefore

$$\left(\bigotimes_{i=1}^{N} Z_i\right)^{\alpha} \left(\bigotimes_{i=1}^{N} X_i^{t_i}\right)^{\beta} = \bigotimes_{i=1}^{N} \left(Z_i^{\alpha_i} X_i^{\bar{\beta}_i}\right) \quad (4.124)$$

Here we used the fact that

$$Z_i^{\alpha} = Z_i^{\alpha_i}; \quad \left(X_i^{t_i}\right)^{\beta} = X_i^{\bar{\beta}_i} \quad (4.125)$$

We then prove Eq. (4.120).

From the above it is clear that the phase space $\mathbb{Z}(d) \times \mathbb{Z}(d)$ is factorized in terms of the phase spaces $\mathbb{Z}(d_i) \times \mathbb{Z}(d_i)$, where $i = 1, ..., N$, as

$$(m, n) \ \leftrightarrow\ [(\overline{m}_1, n_1), ..., (\overline{m}_N, n_N)]. \quad (4.126)$$

Example 4.3 We consider the quantum system $\Sigma[\mathbb{Z}(15)]$ and we factorize it in terms of the systems $\Sigma_1[\mathbb{Z}(3)]$ and $\Sigma_2[\mathbb{Z}(5)]$. The general maps in Eqs. (4.116), (4.117), become

$$|X; m\rangle \leftrightarrow |X_1; \overline{m}_1\rangle |X_2; \overline{m}_2\rangle; \quad |P; m\rangle \leftrightarrow |P_1; m_1\rangle \otimes |P_2; m_2\rangle. \quad (4.127)$$

The relationship between m and m_1, m_2 and also $\overline{m}_1, \overline{m}_2$ is given in Example 3.2, in Eq. (3.31). The Fourier transform in the large system, is

$$|P; m\rangle = \frac{1}{\sqrt{15}} \sum_n \omega_{15}(mn) |X; n\rangle \quad (4.128)$$

and in the two smaller systems is

$$|P_1; m_1\rangle = \frac{1}{\sqrt{3}} \sum_{\overline{n}_1} \omega_3(m_1 \overline{n}_1) |X; \overline{n}_1\rangle$$
$$|P_2; m_2\rangle = \frac{1}{\sqrt{5}} \sum_{\overline{n}_2} \omega_5(m_2 \overline{n}_2) |X; \overline{n}_2\rangle \quad (4.129)$$

Equation (3.26) gives for the present example

$$\omega_{15}(mn) = \omega_3(m_1\overline{n}_1)\omega_5(m_2\overline{n}_2). \tag{4.130}$$

It is easy to check the consistency of Eqs. (4.127), (4.128), (4.129), (4.130).

Remark 4.4 The factorization of the Fourier transform in Eq. (4.118) has been used by Good [84] in the context of Fast Fourier transforms. Here we have factorized the whole quantum formalism in $\Sigma[\mathbb{Z}(d)]$ in terms of quantum formalisms in the factor systems $\Sigma[\mathbb{Z}(d_i)]$.

4.10 Analytic Representation of Finite Quantum Systems

Analytic representations play an important role in quantum mechanics. After the original work by Bargmann [85, 86], various analytic representations have been studied extensively in the literature (e.g., [87]). In this section we discuss analytic representation of finite quantum systems, based on Theta Functions [49, 50, 88].

We first define the Θ_3 function [89–91] as:

$$\Theta_3(u,\tau) = \sum_{n=-\infty}^{\infty} \exp(i\pi\tau n^2 + i2nu). \tag{4.131}$$

This is a Weil transform [92], which in this case maps a Gaussian function on $\mathbb{R}$, into a function on $\mathbb{R}/\mathbb{Z}$. In this sense, the Theta function is a Gaussian function wrapped on a circle.

The zeros of $\Theta_3(u,\tau)$ are at

$$u = (2M-1)\frac{\pi}{2} + (2N-1)\frac{\tau\pi}{2}. \tag{4.132}$$

The Jacobi triple product identity, factorizes the Theta function, as:

$$\Theta_3(u,\tau) = \prod_{m=1}^{\infty}\left[1 - e^{2i\pi\tau m^2}\right]\left[1 + e^{i\pi\tau(2m-1)+i2u}\right]\left[1 + e^{i\pi\tau(2m-1)-i2u}\right]. \tag{4.133}$$

Definition 4.10 Let $|g\rangle$ be an arbitrary ket state in $H[\mathbb{Z}(d)]$, and $\langle g|$ the corresponding bra state:

$$|g\rangle = \sum_m g_m|X;m\rangle; \quad \langle g| = \sum_m g_m^*\langle X;m|; \quad \sum_m |g_m|^2 = 1. \tag{4.134}$$

Their analytic representations, are the analytic functions

$$\begin{aligned} |g\rangle &\rightarrow G(z) = \sum_{m=0}^{d-1} g_m \, \Theta_3 \left[\frac{\pi(m-z)}{d}; \frac{i}{d} \right] \\ \langle g| &\rightarrow [G(z)]^* = \sum_{m=0}^{d-1} g_m^* \, \Theta_3 \left[\frac{\pi(m-z^*)}{d}; \frac{i}{d} \right] \end{aligned} \tag{4.135}$$

Below z_R and z_I are the real and imaginary parts of z.

Lemma 4.2

$$\begin{aligned} &\frac{\sqrt{2}}{d^{5/2}} \int_{\mathbf{S}} dz_R dz_I \exp\left(\frac{-2\pi}{d} z_I^2 \right) \Theta_3 \left[\frac{\pi(m-z)}{d}; \frac{i}{d} \right] \Theta_3 \left[\frac{\pi(n-z^*)}{d}; \frac{i}{d} \right] \\ &= \delta(m,n). \end{aligned} \tag{4.136}$$

where $\mathbf{S}$ *is the square cell*

$$\mathbf{S} = [0,d] \times [0,d], \tag{4.137}$$

in the complex plane.

Proof Using the definition of Theta functions in Eq. (4.131), we rewrite the left hand side of Eq. (4.136) as

$$\begin{aligned} &\frac{\sqrt{2}}{d^{5/2}} \sum_{k,k'} \exp\left(-\frac{\pi(k^2+k'^2) - i2\pi(mk+nk')}{d} \right) \\ &\times \int dz_I \exp\left(\frac{-2\pi z_I^2 + 2\pi(k-k')z_I}{d} \right) \int dz_R \exp\left(-\frac{i2\pi(k+k')z_R}{d} \right) \end{aligned} \tag{4.138}$$

The last integral is $d\delta(k+k',0)$ and we get

$$\begin{aligned} &\frac{\sqrt{2}}{d^{3/2}} \sum_{k=-\infty}^{\infty} \exp\left(-\frac{2\pi k^2 + i2\pi k(n-m)}{d} \right) \int_0^d dz_I \exp\left(\frac{-2\pi z_I^2 + 4\pi k z_I}{d} \right) \\ &= \frac{\sqrt{2}}{d^{3/2}} \sum_{k=-\infty}^{\infty} \exp\left(-\frac{i2\pi k(n-m)}{d} \right) \int_0^d dz_I \exp\left(\frac{-2\pi(z_I-k)^2}{d} \right) \end{aligned} \tag{4.139}$$

We substitute $k = k_1 d + k_2$ where $k_2 = 0, ..., d-1$, and we get

$$\frac{\sqrt{2}}{d^{3/2}}\sum_{k_2=0}^{d-1}\exp\left(-\frac{i2\pi k_2(n-m)}{d}\right)\sum_{k_1=-\infty}^{\infty}\int_0^d dz_I\exp\left(\frac{-2\pi(z_I-k_1d-k_2)^2}{d}\right)$$
$$=\frac{\sqrt{2\pi}}{d^{3/2}}\sum_{k_2=0}^{d-1}\exp\left(-\frac{i2\pi k_2(n-m)}{d}\right)\int_{-\infty}^{\infty}dz_I\exp\left(\frac{-2\pi(z_I-k_2)^2}{d}\right)$$
$$=\frac{1}{d}\sum_{k_2=0}^{d-1}\exp\left(-\frac{i2\pi k_2(n-m)}{d}\right)=\delta(m,n). \tag{4.140}$$

Proposition 4.22 *(1) $G(z)$ is an analytic function and obeys the quasi-periodicity relations*

$$G(z+d)=G(z)$$
$$G(z+id)=G(z)\exp(\pi d-2i\pi z). \tag{4.141}$$

Consequently, it is sufficient to define the function in the cell **S** *in Eq. (4.137), which is a torus with periodicity in the real axis, and quasi-periodicity in the imaginary axis.*

(2) The scalar product is given by the integral

$$\langle g_1|g_2\rangle=\frac{\sqrt{2}}{d^{5/2}}\int_{\mathbf{S}}dz_Rdz_I\exp\left(\frac{-2\pi}{d}z_I^2\right)[G_1(z)]^*G_2(z) \tag{4.142}$$

over the cell **S**.

(3) The analytic function $G(z)$ has exactly d zeros ζ_n within the cell **S** *(i.e., $G(\zeta_n)=0$), and the sum of these zeros is [49, 50, 88]*

$$\sum_{n=1}^{d}\zeta_n=\frac{d^2}{2}(1+i)+d(M+iN). \tag{4.143}$$

Here M, N are integers, related to the toroidal nature of the cell **S**.

(4) Given d zeros ζ_n which satisfy the constraint of Eq. (4.143), the corresponding quantum state is represented by the analytic function

$$G(z)=A\exp\left(\frac{i2\pi z}{d}\right)\prod_{n=1}^{d}\Theta_3[u_n(z);i]$$
$$u_n(z)=\frac{\pi}{d}(z-\zeta_n)+\frac{\pi}{2}(1+i) \tag{4.144}$$

A is a constant determined by the normalization condition.

Proof (1) This is proved using the periodicity properties of Theta functions.

(2) This is proved using Lemma 4.2.
(3) It is known that the number $\mathscr{N}$ of zeros of an analytic function $G(z)$ within a contour C, and also the sum of these zeros, are given by the contour integrals

$$\oint_C \frac{dz}{2\pi i}\frac{\partial_z G(z)}{G(z)} = \mathscr{N}; \quad \oint_C \frac{dz}{2\pi i}\frac{\partial_z G(z)}{G(z)} = \sum_n \zeta_n. \tag{4.145}$$

Taking as a contour the perimeter of the cell **S**, and using the quasi-periodicity conditions in Eq. (4.141), we find that the number of zeros is d and that the sum of zeros is given by Eq. (4.143).
(4) The Theta functions on the right hand side have $\tau = i$ and therefore their zeros are at

$$u = (2M-1)\frac{\pi}{2} + (2N-1)\frac{i\pi}{2}. \tag{4.146}$$

Within a given cell, the M, N have fixed integer values. The various values of M, N, simply shift the zeros to different cells. It is easily seen that the $u_n(\zeta_n)$ are indeed zeros of the $G(z)$ in Eq. (4.144). Also change of ζ_n into $\zeta_n + d$ or $\zeta_n + id$ (i.e., going to an adjacent cell), corresponds to change of M into $M-1$ or change of N into $N-1$ in Eq. (4.146), as it should be.
The prefactor is determined by the fact that the $G(z)/\prod_n \Theta_3[u_n(z); i]$ is an entire function with no zeros, and as such it is an exponential of an entire function. The growth of $G(z)$ is of order $\rho = 2$ (for convergence), and this together with the quasiperiodicity condition of Eq. (4.141), lead to the prefactor given in Eq. (4.144).

Using the Jacobi triple product identity in Eq. (4.133), we can factorize the product in Eq. (4.144) even further, as

$$G(z) = A\exp\left(\frac{i2\pi z}{d}\right)\prod_{n=1}^{d}\prod_{m=1}^{\infty}\left[1-e^{-2\pi m^2}\right]\left[1+e^{-\pi(2m-1)+i2u_n(z)}\right] \times\left[1+e^{-\pi(2m-1)-i2u_n(z)}\right]. \tag{4.147}$$

where the $u_n(z)$ are given in Eq. (4.144).

Example 4.4 The momentum state $|P; k\rangle$ is represented with the function

$$\begin{aligned} G(z;k) &= \frac{1}{\sqrt{d}}\sum_m \omega(km)\Theta_3\left[\frac{\pi(m-z)}{d}; \frac{i}{d}\right] \\ &= \sqrt{d}\exp\left(-\frac{\pi k^2}{d} + i2kz\frac{\pi}{d}\right)\Theta_3\left(-i\pi k - z\pi; id\right). \end{aligned} \tag{4.148}$$

We prove this as follows:

$$\begin{aligned}
&\frac{1}{\sqrt{d}}\sum_m \omega(km)\Theta_3\left[\frac{\pi m}{d} - z\frac{\pi}{d}; \frac{i}{d}\right] \\
&= \frac{1}{\sqrt{d}}\sum_{n=-\infty}^{\infty} \exp\left(-\frac{\pi n^2}{d} - i2zn\frac{\pi}{d}\right)\sum_{m=0}^{d-1}\omega[m(n+k)] \\
&= \sqrt{d}\sum_{n=-k+dN} \exp\left(-\frac{\pi n^2}{d} - i2zn\frac{\pi}{d}\right) \\
&= \sqrt{d}\exp\left(-\frac{\pi k^2}{d} + i2kz\frac{\pi}{d}\right)\Theta_3\left(-i\pi k - z\pi; id\right). \qquad (4.149)
\end{aligned}$$

Using Eq. (4.132), we find that the zeros of the analytic representation of the position state $|X; m\rangle$ are:

$$\zeta = m - \left(M - \frac{1}{2}\right)d - i\left(N - \frac{1}{2}\right). \qquad (4.150)$$

Within a given cell M is fixed, and $N = 0, ..., d-1$.

In a similar way, we find that the zeros of the analytic representation of the momentum state $|P; m\rangle$ are:

$$\zeta = -im - \left(M - \frac{1}{2}\right) - i\left(N - \frac{1}{2}\right)d. \qquad (4.151)$$

Within a given cell N is fixed, and $M = 0, ..., d-1$.

References

1. Weyl, H. (1950). *Theory of groups and quantum mechanics*. New York: Dover.
2. Schwinger, J. (1960). *Proceedings of the National Academy of Science of the United States of America*, *46*, 570.
3. Schwinger, J. (1970). *Quantum Kinematics and Dynamics*. New York: Benjamin.
4. Ramakrishnan, A., Chandrasekaran, P. S., Ranganathan, N. R., Santhanam, T. S., & Vasudevan, T. (1969). *Journal of Mathematical Analysis and Applications*, *27*, 164.
5. Santhanam, T. S., & Tekumalla, A. R. (1976). *Foundations of Physics*, *6*, 583.
6. Hannay, J., & Berry, M. V. (1980). *Physica D*, *1*, 267.
7. Stovicek, P., & Tolar, J. (1984). *Reports on Mathematical Physics*, *20*, 157.
8. Balian, R., Itzykson, C., & Acad, C. R. (1986). *Science*, *303*, 773.
9. Mehta, M. L. (1987). *Journal of Mathematical Physics*, *28*, 781.
10. Galetti, D., & de Toledo-Piza, A. F. R. (1988). *Physica*, *149A*, 267.
11. Vourdas, A. (1990). *Physical Review A*, *41*, 1653.
12. Vourdas, A. (1991). *Physical Review A*, *43*, 1564.
13. Lulek, T. (1992). *Acta Physica Polonica A*, *82*, 377.
14. Vourdas, A., & Bendjaballah, C. (1993). *Physical Review A*, *47*, 3523.

15. Hadzitaskos, G., & Tolar, J. (1993). *International Journal of Theoretical Physics*, *32*, 517.
16. Varadarajan, V. S. (1995). *Letters in Mathematical Physics*, *34*, 319.
17. Leonhardt, U. (1995). *Physical Review Letters*, *74*, 4101.
18. Leonhardt, U. (1996). *Physics Review A*, *53*, 2998.
19. Vourdas, A. (1996). *Journal of Physics A*, *29*, 4275.
20. Vourdas, A. (1997). *Reports on Mathematical Physics*, *40*, 367.
21. Hakioglu, T. (1998). *Journal of Physics A*, *31*, 6975.
22. Digernes, T., Husstad, E., & Varadarajan, V. S. (1999). *Mathematica Scandinavica*, *84*, 261.
23. Vourdas, A. (2004). *Reports on Progress in Physics*, *67*, 267.
24. Gross, D. (2006). *Journal of Mathematical Physics*, *47*, 122107.
25. Kibler, M. (2008). *Journal of Physics A*, *41*, 375302.
26. Cotfas, N., & Gazeau, J. P. (2010). *Journal of Physics A*, *43*, 193001.
27. Cotfas, N., Gazeau, J.-P., & Vourdas, A. (2011). *Journal of Physics A*, *44*, 175303.
28. Korbelar, M., & Tolar, J. (2012). *Journal of Physics A*, *45*, 285305.
29. Deutsch, D. (1983). *Physical Review Letter*, *50*, 631.
30. Partovi, M. H. (1983). *Physical Review Letter*, *50*, 1883.
31. Marchiolli, M., & Ruzzi, M. (2012). *Annals of Physics*, *327*, 1538.
32. Marchiolli, M., & Ruzzi, M. (2013). *Annals of Physics*, *336*, 76.
33. Atakishiyev, N. M., Chumakov, S. M., & Wolf, K. B. (1998). *Journal of Mathematical Physics*, *39*, 6247.
34. Atakishiyev, N. M., Vincent, L. E., & Wolf, K. B. (1999). *Journal of Computational and Applied Mathematics and Physics*, *107*, 73.
35. Hakioglu, T., & Wolf, K. B. (2000). *Journal of Physics A*, *33*, 3313.
36. Atakishiyev, N. M., Pogosyan, G., Vincent, L. E., & Wolf, K. B. (2001). *Journal of Physics A*, *34*, 9381.
37. Atakishiyev, N. M., Pogosyan, G., Vincent, L. E., & Wolf, K. B. (2001). *Journal of Physics A*, *34*, 9399.
38. Atakishiyev, N. M., Klimyk, A. V., & Wolf, K. B. (2008). *Journal of Physics A*, *41*, 085201.
39. Jafarov, E. I., Stoilova, N. I., & Van der Jeugt, J. (2011). *Journal of Physics A*, *44*, 265203.
40. Van der Jeugt, J. (2013). *Journal of Physics A*, *46*, 475302.
41. Auslander, L., & Tolimieri, R. (1979). *Bulletin of the American Mathematical Society*, *1*, 847.
42. Terras, A. (1999). *Fourier Analysis on Finite Groups and Applications*. Cambridge: Cambridge Univ. Press.
43. Gurevich, S., & Hadani, R. (2009). *Applied and Computational Harmonic Analysis*, *27*, 87.
44. Durt, T. (2005). *Journal of Physics A*, *38*, 5267.
45. Zak, J. (2011). *Journal of Physics A*, *44*, 345303.
46. Athanasiu, G., & Floratos, E. (1994). *Nuclear Physics B*, *245*, 343.
47. Galleti, D., & Marchiolli, M. A. (1996). *Annals of Physics*, *249*, 454.
48. Tolar, J., & Hadzitaskos, G. (1997). *Journal of Physics A*, *30*, 2509.
49. Zhang, S., & Vourdas, A. (2004). *Journal of Physics A*, *37*, 8349–8363.
50. Evangelides, P., Lei, C., & Vourdas, A. (2015). *Journal of Mathematical Physics*, *56*, 072108.
51. Vourdas, A. (2017). *Annals of Physics*, *376*, 153.
52. Vourdas, A. (2016). *Journal of Geometry and Physics*, *101*, 38.
53. Vourdas, A. (2016). *Annals of Physics*, *373*, 557.
54. Neuhauser, M. (2002). *Journal of Lie Theory*, *12*, 15.
55. Feichtinger, H., Hazewinkel, M., Kaiblinger, N., Matusiak, E., & Neuhauser, M. (2008). *The Quarterly Journal of Mathematics*, *59*, 15.
56. Wang, L., Al Hadhrami, H., & Vourdas, A. (2008). *The European Physical Journal D*, *49*, 265.
57. Grossmann, A. (1976). *Communications in Mathematical Physics*, *48*, 191.
58. Daubechies, I., & Grossmann, A. (1980). *Journal of Mathematical Physics*, *21*, 2080.
59. Royer, A. (1977). *Physical Review A*, *15*, 449.
60. Royer, A. (1992). *Physical Review A*, *45*, 793.
61. Bishop, R. F., & Vourdas, A. (1994). *Physical Review A*, *50*, 4488.
62. Moyal, J. E. (1949). *Proceedings of the Cambridge Philosophical Society*, *45*, 99.

63. Bartlett, M. S., & Moyal, J. E. (1949). *Proceedings of the Cambridge Philosophical Society*, *45*, 545.
64. Baker, G. A. (1958). *Physical Review*, *109*, 2198.
65. Berezin, F. A. (1974). *Mathematics of the USSR-Izvestiya*, *8*, 1109.
66. Berezin, F. A. (1975). *Mathematics of the USSR-Izvestiya*, *9*, 341.
67. Berezin, F. A. (1975). *Communications in Mathematical Physics*, *40*, 153.
68. Zachos, C., Fairlie, D., & Curtright, T. (2005). *Quantum mechanics in phase space*. Singapore: World Scientific.
69. Mancini, S., Man'ko, V. I., & Tombesi, P. (1996). *Physical Review A*, *213*, 1.
70. Man'ko, O., & Man'ko, V. I. (1999). *Journal of Russian Laser Research*, *20*, 67.
71. Man'ko, M. (2001). *Journal of Russian Laser Research*, *22*, 505.
72. Grochenig, K. (2001). *Foundations of time-frequency analysis*. Boston: Birkhauser.
73. Cohen, L. (1995). *Time-frequency Analysis*. New Jersey: Prentice-Hall.
74. Wootters, W. K. (1987). *Annals of Physics*, 176, 1. (N.Y).
75. Miquel, C., Paz, J. P., & Saraceno, M. (2002). *Physical Review A*, *65*, 062309.
76. Paz, J. P. (2002). *Physical Review A*, *65*, 062311.
77. Klimov, A. B., & Munoz, C. (2005). *Journal of Optics B: Quantum and Semiclassical Optics*, *7*, S588.
78. Cormick, C., Galvao, E., Gottesman, D., Paz, J. P., & Pittenger, A. O. (2006). *Physical Review A*, *73*, 012301.
79. Bjork, G., Klimov, A. B., & Sanchez-Soto, L. L. (2008). *Progress in Optics*, *51*, 469.
80. Chaturvedi, S., Mukunda, N., & Simon, R. (2010). *Journal of Physics A*, *43*, 075302.
81. Vourdas, A. (2003). *Journal of Physics A*, *36*, 5645.
82. Revzen, M., Khanna, F. C., Mann, A., & Zak, J. (2006). *Journal of Physics A*, *39*, 5151.
83. Simkhovich, B., Mann, A., & Zak, J. (2010). *Journal of Physics A*, *43*, 045301.
84. Good, I. J., & Trans, I. E. E. E. (1971). *Computers*, *C20*, 310.
85. Bargmann, V. (1961). *Communications on Pure and Applied Mathematics*, *14*, 187.
86. Bargmann, V. (1967). *Communications on Pure and Applied Mathematics*, *20*, 1.
87. Vourdas, A. (2006). *Journal of Physics A*, *39*, R65.
88. Leboeuf, P., & Voros, A. (1990). *Journal of Physics A*, *23*, 1765.
89. Mumford, D. (1983). *Tata lectures on Theta* (Vols. 1, 2, 3) Boston: Birkhauser.
90. Igusa, J. (1972). *Theta functions*. Berlin: Springer.
91. Fay, J. (1973). *Theta functions on Riemann surfaces*. Berlin: Springer.
92. Weil, A. (1964). *Acta Mathematica*, *111*, 143.

Chapter 5
Finite Geometries and Mutually Unbiased Bases

Abstract Finite geometries, mutually unbiased bases, and weak mutually unbiased bases, are discussed.

In this section we first discuss the $\mathbb{Z}(d) \times \mathbb{Z}(d)$ as a finite geometry [1–3], and its link to the subject of mutually unbiased bases [4–22]. There are deep mathematical problems related to these bases, and they also have important applications in quantum communications and quantum cryptography. For these reasons, they have been studied extensively in the literature.

We make the distinction between two cases:

- $d = p$, where p is a prime number. In this case, $\mathbb{Z}(p)$ is a field. $\mathbb{Z}(p) \times \mathbb{Z}(p)$ is a near-linear finite geometry, based on the axiom that two lines have at most one point in common. The number of mutually unbiased bases is $p + 1$ and there is a duality between the finite geometry and the mutually unbiased bases. These results can be extended to the case that $d = p^e$, using the Galois field $GF(p^e)$, as discussed later in Sect. 9.7.
- d is not a prime number. In this case, $\mathbb{Z}(d)$ is a ring. $\mathbb{Z}(d) \times \mathbb{Z}(d)$ is a non-near-linear finite geometry, and two lines might have more than one point in common (the axiom that two lines have at most one point in common does not hold). The number of mutually unbiased bases is not known, but it is probably smaller than $d+1$ (although there is no rigorous proof of this). Here there is no duality between the finite geometry and the mutually unbiased bases. Motivated by this, Refs. [23–26] have introduced weak mutually unbiased bases, which are dual to lines in the finite geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$. In order to avoid a complex notation, and without loss of generality, we discuss the case with $d = p_1 p_2$, where p_1, p_2 are odd prime numbers, different from each other.

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_5

5.1 The $\mathbb{Z}(d) \times \mathbb{Z}(d)$ as a Non-near-linear Finite Geometry

A finite geometry [1–3] is a finite set P of points, and a set L of some subsets of P which are called lines. In our context, $P = \mathbb{Z}(d) \times \mathbb{Z}(d)$. The geometry (P, L) satisfies certain axioms. A special class of finite geometries are the near-linear geometries, with the axiom that two lines have at most one point in common. We will see below, that this axiom is valid when d is a prime number (in which case $\mathbb{Z}(d)$ is a field), but it is not valid when d is not a prime number (in which case $\mathbb{Z}(d)$ is a ring). Therefore our geometry is a non-near-linear geometry, in the case of non-prime d.

A line through the point (α, β) is the set of points

$$L(\rho, \sigma|\alpha, \beta) = \{(\tau\rho + \alpha, \tau\sigma + \beta)|\tau \in \mathbb{Z}(d)\}; \quad \rho, \sigma, \alpha, \beta \in \mathbb{Z}(d) \tag{5.1}$$

Below we only consider lines through the origin (0, 0), which we denote as $L(\rho, \sigma)$:

$$L(\rho, \sigma) = \{(\tau\rho, \tau\sigma)|\tau \in \mathbb{Z}(d)\}. \tag{5.2}$$

Mathematically this is a cyclic module generated by (ρ, σ), but in a physical context we will use the intuitive term line. In this section we present three propositions which describe $\mathbb{Z}(d) \times \mathbb{Z}(d)$ as a finite geometry [23–26].

Proposition 5.1 *(1) The number of points in $L(\rho, \sigma)$ is $d/\mathrm{GCD}(\rho, \sigma, d)$. We call maximal lines the ones with d points (i.e., the lines with $\mathrm{GCD}(\rho, \sigma, d) = 1$).*

(2) If λ is an invertible element in $\mathbb{Z}(d)$ ($\lambda \in [\mathbb{Z}(d)]^*$), then $L(\rho\lambda, \sigma\lambda) = L(\rho, \sigma)$. If λ is a non-invertible element, then $L(\rho\lambda, \sigma\lambda) \subset L(\rho, \sigma)$.

(3) The intersection of two lines $L(\rho_1, \sigma_1)$ and $L(\rho_2, \sigma_2)$ is a line, which we call subline. The number of common points between these two lines, is a divisor of d.

Proof (1) For a given ρ, as τ takes all values in $\mathbb{Z}(d)$, the $\rho\tau$ takes $d/\mathrm{GCD}(\rho, d)$ different values, because there are $\delta = \mathrm{GCD}(\rho, d)$ different values of τ which give the same $\rho\tau$. We next need to find how many different values of $\tau\sigma$, correspond to these δ values of τ (which give the same $\rho\tau$).

The δ values of τ, lead to δ values of $\sigma\tau$, but using the same argument we find that only $\delta/\mathrm{GCD}(\sigma, \delta)$, are different from each other. Therefore the total number of pairs $(\rho\tau, \sigma\tau)$ is

$$\frac{d}{\mathrm{GCD}(\rho, d)} \frac{\delta}{\mathrm{GCD}(\sigma, \delta)} = \frac{d}{\mathrm{GCD}(d, \rho, \sigma)}. \tag{5.3}$$

(2) For any $\lambda \in \mathbb{Z}(d)$, if $(\rho\lambda\tau, \sigma\lambda\tau)$ is a point in $L(\rho\lambda, \sigma\lambda)$ then this point can also be written as $(\rho\tau', \sigma\tau')$ with $\tau' = \lambda\tau$ and therefore it belongs to the line $L(\rho, \sigma)$. This proves that $L(\rho\lambda, \sigma\lambda) \subseteq L(\rho, \sigma)$.

For $\lambda \in [\mathbb{Z}(d)]^*$, if $(\rho\tau, \sigma\tau)$ is a point in $L(\rho, \sigma)$ and then this point can also be written as $(\rho\lambda\tau', \sigma\lambda\tau')$ with $\tau' = \lambda^{-1}\tau$, and therefore it belongs to the line $L(\rho\lambda, \sigma\lambda)$. This proves that for an invertible element λ, $L(\rho\lambda, \sigma\lambda) = L(\rho, \sigma)$.

(3) If $(\rho, \sigma) \in L(\rho_1, \sigma_1)$ and also $(\rho, \sigma) \in L(\rho_2, \sigma_2)$ then clearly for any $\tau \in \mathbb{Z}(d)$, we have $(\rho\tau, \sigma\tau) \in L(\rho_1, \sigma_1)$ and also $(\rho\tau, \sigma\tau) \in L(\rho_2, \sigma_2)$. Therefore the common points of two lines, form a line (which we call subline, and which according to the first part of the proposition, has a divisor of d as number of points).

In the case $d = p$ where p is a prime number, the $\mathbb{Z}(p)$ is a field. In this case the only divisor of p is 1, and two lines through the origin have one point in common. Consequently the geometry $\mathbb{Z}(p) \times \mathbb{Z}(p)$ is a near-linear geometry. In the case of non-prime d, the $\mathbb{Z}(d)$ is a ring (which is not a field). In this case the geometry is a non-near-linear geometry, and has both maximal lines and sublines.

Example 5.1 Examples of maximal lines in $\mathbb{Z}(15) \times \mathbb{Z}(15)$ are

$$\begin{aligned} L(1,2) = \{&(0,0), (1,2), (2,4), (3,6), (4,8), (5,10), (6,12), (7,14), \\ &(8,1), (9,3), (10,5), (11,7), (12,9), (13,11), (14,13)\}, \end{aligned} \tag{5.4}$$

and

$$\begin{aligned} L(1,7) = \{&(0,0), (1,7), (2,14), (3,6), (4,13), (5,5), (6,12), (7,4), \\ &(8,11), (9,3), (10,10), (11,2), (12,9), (13,1), (14,8)\}. \end{aligned} \tag{5.5}$$

The $L(3, 6)$ is an example of a line through the origin which is not maximal line (it has 5 points):

$$L(3,6) = \{(0,0), (3,6), (6,12), (9,3), (12,9)\}. \tag{5.6}$$

The intersection of the maximal lines $L(1, 2)$ and $L(1, 7)$, is $L(3, 6)$:

$$L(1,2) \cap L(1,7) = L(3,6). \tag{5.7}$$

This is shown in Fig. 5.1.

5.1.1 Symplectic Transformations in the Finite Geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$

In order to perform symplectic transformations on a point $(\rho, \sigma) \in \mathbb{Z}(d) \times \mathbb{Z}(d)$, we multiply the row (ρ, σ) times the matrix $g(\kappa, \lambda|\mu, \nu) \in Sp[2, \mathbb{Z}(d)]$:

$$g(\kappa, \lambda|\mu, \nu) \circ (\rho, \sigma) = (\rho, \sigma) g(\kappa, \lambda|\mu, \nu) = (\kappa\rho + \mu\sigma, \lambda\rho + \nu\sigma) \tag{5.8}$$

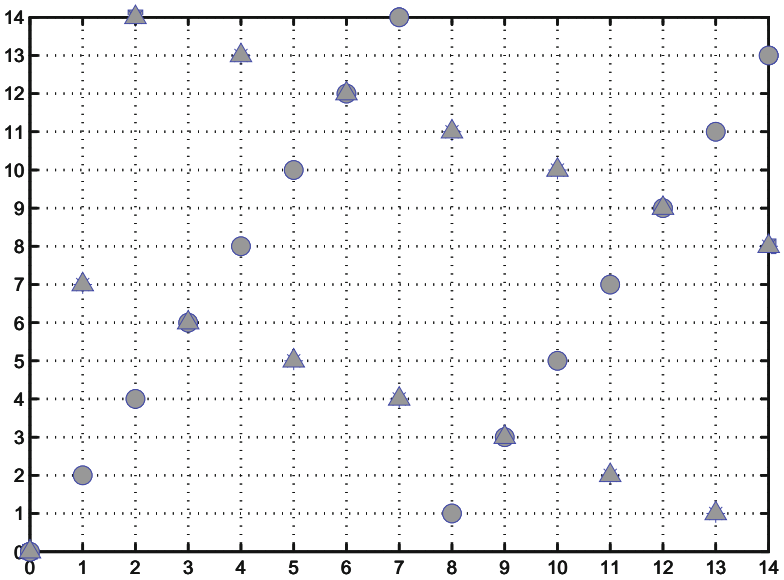

Fig. 5.1 The *maximal lines* $L(1,2)$ (*circles*), and $L(1,7)$ (*triangles*) in the $\mathbb{Z}(15) \times \mathbb{Z}(15)$ finite geometry

This is consistent with the 'right multiplication rule' in Eq. (3.35). In particular we note that the Fourier matrix $\mathscr{F}$ of Eq. (3.41) maps the points $(\alpha, 0)$ on the 'horizontal axis', to the points $(0, \alpha)$ on the 'vertical axis':

$$\mathscr{F} \circ (\alpha, 0) = (\alpha, 0) g(0, 1| - 1, 0) = (0, \alpha) \tag{5.9}$$

Symplectic transformations on points lead to symplectic transformations on lines:

$$g(\kappa, \lambda | \mu, \nu) \circ L(\rho, \sigma) = L(\kappa\rho + \mu\sigma, \lambda\rho + \nu\sigma). \tag{5.10}$$

In particular, with the Fourier matrix we get:

$$\mathscr{F} \circ L(\rho, \sigma) = L(-\sigma, \rho). \tag{5.11}$$

Example 5.2 In $\mathbb{Z}(15)$ we act with the matrix $g(3, 4|2, 8) \in Sp[2, \mathbb{Z}(15)]$ on the line $L(1, 2)$ and we get:

$$g(3, 4|2, 8) \circ L(1, 2) = L(7, 5). \tag{5.12}$$

This is shown in Fig. 5.2.

Proposition 5.2 *For prime p, the geometry* $\mathbb{Z}(p) \times \mathbb{Z}(p)$ *is a near-linear geometry, which has only maximal lines with p points, given in terms of symplectic transfor-*

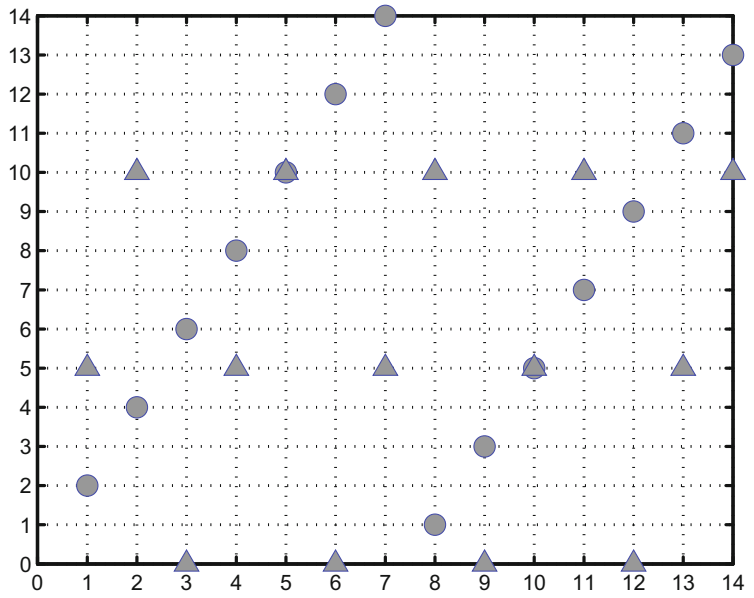

Fig. 5.2 The *maximal lines* $L(1,2)$ (*circles*), and $L(7,5) = g(3,4|2,8) \circ L(1,2)$ (*triangles*) in the $\mathbb{Z}(15) \times \mathbb{Z}(15)$ finite geometry

mations as

$$g(0,-1|1,\nu) \circ L(0,1) = L(1,\nu). \tag{5.13}$$

The $L(0,1)$ *together with the* $L(1,\nu)$ *with* $\nu = 0, ..., p-1$, *form the set of all* $\psi(p) = p+1$ *lines through the origin, in this geometry (*ψ *is the Dedekind psi).*

Proof For the proof we use symplectic transformations in conjunction with Proposition 5.1.

Notation 5.1 *For a prime* p, *we introduce the notation*

$$\mathscr{L}(\nu) = L(1,\nu); \quad \mathscr{L}(-1) = L(0,1). \tag{5.14}$$

In $\mathscr{L}(\nu)$, *the* ν *takes the* $\psi(p) = p+1$ *values* $-1, ..., p-1$.

5.1.2 *Factorization of the Finite Geometry* $\mathbb{Z}(d) \times \mathbb{Z}(d)$ *Based on the Chinese Remainder Theorem*

As we mentioned earlier, for simplicity and without loss of generality, we consider the case where $d = p_1 p_2$ where p_1, p_2 are odd prime numbers. The following

proposition describes the maximal lines through the origin in $\mathbb{Z}(p_1 p_2) \times \mathbb{Z}(p_1 p_2)$, as products of lines in $\mathbb{Z}(p_1) \times \mathbb{Z}(p_1)$ and $\mathbb{Z}(p_2) \times \mathbb{Z}(p_2)$.

There is an analogy between the factorization of the finite geometry, and the factorization of position and momentum states in Sect. 4.9, with the points $(\alpha, 0)$ in the 'horizontal axis' corresponding to position states, and the points $(0, \beta)$ in the 'vertical axis' corresponding to momenta. Motivated by this we factorize the points (α, β) using the dual map in Eq. (3.22) for α, and the map of Eq. (3.21) for β:

$$(\alpha, \beta) \;\leftrightarrow\; ((\overline{\alpha}_1, \beta_1), (\overline{\alpha}_2, \beta_2)); \quad \overline{\alpha}_i, \beta_i \in \mathbb{Z}(p_i). \tag{5.15}$$

This is consistent with the relation of Eq. (3.52) that factorized the Fourier matrix. Indeed

$$\mathscr{F} \circ (\alpha, \beta) = (-\beta, \alpha) \;\leftrightarrow\; ((\overline{\beta}_1, \alpha_1), (\overline{\beta}_2, \alpha_2)) \tag{5.16}$$

Also

$$\mathscr{F} \circ (\alpha, \beta) \leftrightarrow (g_1(0, r_1| - t_1, 0) \circ (\overline{\alpha}_1, \beta_1), g_2(0, r_2| - t_2, 0) \circ (\overline{\alpha}_2, \beta_2)) \tag{5.17}$$

with

$$\begin{aligned} g_1(0, r_1| - t_1, 0) \circ (\overline{\alpha}_1, \beta_1) &= (\overline{\beta}_1, \alpha_1) \\ g_2(0, r_2| - t_2, 0) \circ (\overline{\alpha}_2, \beta_2) &= (\overline{\beta}_2, \alpha_2). \end{aligned} \tag{5.18}$$

Proposition 5.3 *There are $\psi(p_1 p_2)$ maximal lines through the origin in $\mathbb{Z}(p_1 p_2) \times \mathbb{Z}(p_1 p_2)$, which belong to one of the following four categories:*

(1) If $\nu_1 \in \mathbb{Z}(p_1)$ and $\nu_2 \in \mathbb{Z}(p_2)$

$$\mathscr{L}(\nu_1, \nu_2) \equiv L_1(1, \nu_1) \times L_2(1, \nu_2) = L(p_1 + p_2, \nu_1 s_1 + \nu_2 s_2) \tag{5.19}$$

There are $p_1 p_2$ lines in this category, with $\nu_1 = 0, ..., p_1 - 1$, and $\nu_2 = 0, ..., p_2 - 1$. The $\mathscr{L}(\nu_1, \nu_2)$ is another notation for these lines, which we call 'factorized notation'. We call the $L(p_1 + p2, \nu_1 s_1 + \nu_2 s_2)$, unfactorized notation.

(2) If $\nu_2 \in \mathbb{Z}(p_2)$

$$\mathscr{L}(-1, \nu_2) \equiv L(0, 1) \times L(1, \nu_2) = L(p_1, s_1 + \nu_2 s_2) \tag{5.20}$$

There are p_2 lines in this category, with $\nu_2 = 0, ..., p_2 - 1$. $\mathscr{L}(-1, \nu_2)$ is the factorized notation for these lines.

(3) If $\nu_1 \in \mathbb{Z}(p_1)$

$$\mathscr{L}(\nu_1, -1) \equiv L(1, \nu_1) \times L(0, 1) = L(p_2, \nu_1 s_1 + s_2) \tag{5.21}$$

There are p_1 lines in this category, with $\nu_1 = 0, ..., p_1 - 1$. $\mathscr{L}(\nu_1, -1)$ is the factorized notation for these lines.

(4)

$$\mathscr{L}(-1, -1) \equiv L(0, 1) \times L(0, 1) = L(0, 1). \tag{5.22}$$

$\mathscr{L}(-1, -1)$ is the factorized notation for this line.

Proof From Eq. (5.10) follows that

$$g(\kappa, \lambda|\mu, \nu) \circ L(0, 1) = L(\mu, \nu). \tag{5.23}$$

We note here that the $L(\mu, \nu)$ does not depend on κ, λ, and this should be compared and contrasted with Eq. (4.53). The proof then follows immediately from Corollary 3.1.

Example 5.3 In $\mathbb{Z}(15) \times \mathbb{Z}(15)$ there are $\psi(15) = 24$ maximal lines through the origin. As an example we consider the following line

$$\mathscr{L}(2, 1) = L_1(1, 2) \times L_2(1, 1) \tag{5.24}$$

$L_1(1, 2)$ is a line in $\mathbb{Z}(3) \times \mathbb{Z}(3)$, and $L_2(1, 1)$ is a line in $\mathbb{Z}(5) \times \mathbb{Z}(5)$. In the unfactorized notation the $\mathscr{L}(2, 1)$ is $L(8, 2s_1 + s_2)$. We have seen in Eq. (3.30) that

Table 5.1 The points in the line $L(1, 7) = \mathscr{L}(2, 1)$ (in the unfactorized and factorized notations). The corresponding points in the first factor line $L_1(1, 2)$ (in $\mathbb{Z}(3) \times \mathbb{Z}(3)$), and in the second factor line $L_2(1, 1)$ (in $\mathbb{Z}(5) \times \mathbb{Z}(5)$) are also shown

$L(1, 7)$		$L_1(1, 2)$		$L_2(1, 1)$	
0	0	0	0	0	0
1	7	2	1	2	2
2	14	1	2	4	4
3	6	0	0	1	1
4	13	2	1	3	3
5	5	1	2	0	0
6	12	0	0	2	2
7	4	2	1	4	4
8	11	1	2	1	1
9	3	0	0	3	3
10	10	2	1	0	0
11	2	1	2	2	2
12	9	0	0	4	4
13	1	2	1	1	1
14	8	1	2	3	3

$s_1 = 10$ and $s_2 = 6$, and therefore $2s_1 + s_2 = 26 = 11 \pmod{15}$. Therefore in the unfactorized notation the $\mathscr{L}(2, 1)$ is $L(8, 11) = L(1, 8^{-1} \times 11) = L(1, 7)$. The points in this line, and also in its factor lines $L_1(1, 2)$ and $L_2(1, 1)$ are shown in Table 5.1.

5.2 Mutually Unbiased Bases

There is a lot of work on various aspects of mutually unbiased bases [4–22]. Their study incorporates many areas of discrete Mathematics. Below we summarize the main points. Mutually unbiased bases in systems with variables in Galois fields, are discussed later in Sect. 9.7.

Definition 5.1 A set of orthonormal bases in $H[\mathbb{Z}(d)]$ are called mutually unbiased, if the vectors in any two of these bases obey the relation

$$|\langle X; m|Y; n\rangle|^2 = \frac{1}{d}; \quad m, n \in \mathbb{Z}(d). \tag{5.25}$$

for all m, n.

Proposition 5.4 *The number of mutually unbiased bases in* $H[\mathbb{Z}(d)]$*, is*

$$\mathscr{M}(d) \leq d + 1. \tag{5.26}$$

Proof A measurement with the projectors $|X; m\rangle\langle X; m|$ gives d probabilities, $d - 1$ of which are independent. A density matrix has $d^2 - 1$ degrees of freedom, and therefore we need at least $d + 1$ measurements in order to get all the information in it. If the information that we get from each measurement is totally independent from the information that we get from the other measurements, then the total number of measurements needed is exactly $d + 1$. This is the case with the mutually unbiased bases. Indeed

$$\langle X; m|\rho|X; m\rangle = \frac{1}{d} + \sum_{n_1 \neq n_2} \langle X; m|Y; n_1\rangle\langle Y; n_1|\rho|Y; n_2\rangle\langle Y; n_2|X; m\rangle. \tag{5.27}$$

This shows that the information obtained from the measurement with the projectors $|X; m\rangle\langle X; m|$, is contained entirely in the off-diagonal terms $\langle Y; n_1|\rho|Y; n_2\rangle$ with $n_1 \neq n_2$. The measurement with the projectors $|X; m\rangle\langle X; m|$ gives totally independent information from the measurement with the projectors $|Y; m\rangle\langle Y; m|$. Consequently, the maximum number of mutually unbiased bases is $d + 1$. We note that the argument does not guarantee the existence of $d + 1$ mutually unbiased bases.

In systems with prime, or power of prime dimension, the inequality in Eq. (5.26) becomes equality. In the following proposition we consider a system with prime

dimension p, and construct a set of $\mathscr{M}(p) = p + 1$ mutually unbiased bases. The construction is based on symplectic transformations. This result is generalized to systems with power of prime dimension p^e, and variables in the Galois fields $GF(p^e)$, later in Sect. 9.7.

5.2.1 Mutually Unbiased Bases in $H[\mathbb{Z}(p)]$

Notation 5.2 *In $H[\mathbb{Z}(p)]$ where p is an odd prime, we consider the p orthonormal bases*

$$|\mathscr{X}(\nu); m\rangle = S(0, -1|1, \nu)|X; m\rangle; \quad \nu, m \in \mathbb{Z}(p) \tag{5.28}$$

where $S(0, -1|1, \nu)$ are symplectic matrices (discussed in Sect. 4.5). In the case $\nu = 0$, this is the basis of momentum states:

$$|\mathscr{X}(0); m\rangle = S(0, -1|1, 0)|X; m\rangle = F^{\dagger}|X; m\rangle = |P; -m\rangle. \tag{5.29}$$

In addition to them, we also consider the orthonormal basis of position states, and we use the convention

$$|\mathscr{X}(-1); m\rangle = |X; m\rangle. \tag{5.30}$$

So we have $p + 1$ orthonormal bases

$$|\mathscr{X}(\nu); m\rangle; \quad \nu \in \{-1\} \cup \mathbb{Z}(p). \tag{5.31}$$

There should be no confusion between the $\nu = -1$ which is used as an extra element that indicates position states, and the $p - 1 = -1 \pmod p$ which is an element of $\mathbb{Z}(p)$.

Proposition 5.5 *For $\nu \neq \nu'$,*

$$|\langle \mathscr{X}(\nu'); n|\mathscr{X}(\nu); m\rangle|^2 = \frac{1}{p}; \quad \nu, \nu' \in \{-1\} \cup \mathbb{Z}(p). \tag{5.32}$$

Therefore they are a set of $p + 1$ mutually unbiased bases.

Proof We consider the following four cases.

(1) In the first case $\nu, \nu' = 1, ..., p - 1$. We use Eq. (4.65) with $d = p$, $\kappa = 0$, $\lambda = -1$, $\mu = 1$, and we get

$$|\mathscr{X}(\nu); m\rangle = \frac{1}{p} G[-2^{-1}\nu^{-1}; \mathbb{Z}(p)] \sum_r \omega(2^{-1}r^2\nu - rm)|X; r\rangle. \tag{5.33}$$

Here G is the Gauss sum. Therefore

$$\langle \mathscr{X}(\nu'); n|\mathscr{X}(\nu); m\rangle = \frac{1}{p^2} G[-2^{-1}(\nu')^{-1}; \mathbb{Z}(p)]G[-2^{-1}\nu^{-1}; \mathbb{Z}(p)] \times \sum_r \omega(-2^{-1}r^2\nu' + rn + 2^{-1}r^2\nu - rm). \quad (5.34)$$

We replace the variable r with $R = r + (\nu - \nu')^{-1}(n - m)$ and we show that

$$\langle \mathscr{X}(\nu'); n|\mathscr{X}(\nu); m\rangle = \frac{1}{p^2} G[-2^{-1}(\nu')^{-1}; \mathbb{Z}(p)]G[-2^{-1}\nu^{-1}; \mathbb{Z}(p)] \times G[2^{-1}(\nu - \nu'); \mathbb{Z}(p)] \times \omega(-2^{-1}(\nu - \nu')^{-1}(n - m)^2]. \quad (5.35)$$

This result is actually true for any odd dimension. We now use the fact that for prime p and $\alpha \neq 0$, we get $|G[\alpha; \mathbb{Z}(p)]| = \sqrt{p}$ (see Eq. (3.9)). Therefore

$$\langle \mathscr{X}(\nu'); n|\mathscr{X}(\nu); m\rangle = \frac{1}{\sqrt{p}}. \quad (5.36)$$

(2) In the second case $\nu = 1, ..., p - 1$ and $\nu' = -1$, and we prove that

$$|\langle X; n|\mathscr{X}(\nu); m\rangle| = \frac{1}{\sqrt{p}}. \quad (5.37)$$

Eq. (5.38) gives

$$\langle X; n|\mathscr{X}(\nu); m\rangle = \frac{1}{p} G[-2^{-1}\nu^{-1}; \mathbb{Z}(p)]\omega(2^{-1}n^2\nu - nm). \quad (5.38)$$

Taking into account Eq. (3.9), we prove Eq. (5.37).

(3) In the third case $\nu = 1, ..., p - 1$ and $\nu' = 0$, and we prove that

$$|\langle P; n|\mathscr{X}(\nu); m\rangle| = \frac{1}{\sqrt{p}}. \quad (5.39)$$

The proof here is very similar to the previous cases.

(4) In the fourth case $\nu = -1$ and $\nu' = 0$ and we see immediately that

$$|\langle P; n|X; m\rangle| = \frac{1}{\sqrt{p}}. \quad (5.40)$$

This completes the proof.

Table 5.2 The six lines through the origin in the finite geometry $\mathbb{Z}(5) \times \mathbb{Z}(5)$, and the corresponding mutually unbiased bases in $H[\mathbb{Z}(5)]$

Lines in $\mathbb{Z}(5) \times \mathbb{Z}(5)$	Bases in $H[\mathbb{Z}(5)]$
$\mathscr{L}(-1) = L(0, 1)$	$\|\mathscr{X}(-1); m\rangle = \|X; m\rangle$
$\mathscr{L}(0) = L(1, 0) = \mathscr{F}^{\dagger} \circ L(0, 1)$	$\|\mathscr{X}(-0); m\rangle = F^{\dagger}\|X; m\rangle = \|P; -m\rangle$
$\mathscr{L}(1) = L(1, 1) = g(0, -1\|1, 1) \circ L(0, 1)$	$\|\mathscr{X}(1); m\rangle = S(0, -1\|1, 1)\|X; m\rangle$
$\mathscr{L}(2) = L(1, 2) = g(0, -1\|1, 2) \circ L(0, 1)$	$\|\mathscr{X}(2); m\rangle = S(0, -1\|1, 2)\|X; m\rangle$
$\mathscr{L}(3) = L(1, 3) = g(0, -1\|1, 3) \circ L(0, 1)$	$\|\mathscr{X}(3); m\rangle = S(0, -1\|1, 3)\|X; m\rangle$
$\mathscr{L}(4) = L(1, 4) = g(0, -1\|1, 4) \circ L(0, 1)$	$\|\mathscr{X}(4); m\rangle = S(0, -1\|1, 4)\|X; m\rangle$

Proposition 5.6 *There is a duality between the $\psi(p) = p + 1$ lines through the origin in the near-linear finite geometry $\mathbb{Z}(p) \times \mathbb{Z}(p)$, and the $\psi(p) = p + 1$ mutually unbiased bases in the Hilbert space $H[\mathbb{Z}(p)]$, where*

$$\mathscr{L}(\nu) \quad \leftrightarrow \quad \{|\mathscr{X}(\nu); m\rangle\}; \quad \nu = -1, ..., p - 1. \tag{5.41}$$

The p points in the line $\mathscr{L}(\nu)$ correspond to the p vectors in the basis $\{|\mathscr{X}(\nu); m\rangle\}$.

Proof We compare and contrast Eqs. (5.13), (5.14) with Eqs. (5.28), (5.29), (5.30). We get

$$\mathscr{L}(-1) = L(0, 1) \quad \leftrightarrow \quad |\mathscr{X}(-1); m\rangle = |X; m\rangle \tag{5.42}$$

for $\nu = -1$, and

$$\mathscr{L}(\nu) = g(0, -1|1, \nu) \circ L(0, 1) \quad \leftrightarrow \quad |\mathscr{X}(\nu); m\rangle = S(0, -1|1, \nu)|X; m\rangle \tag{5.43}$$

for $\nu = 0, ..., p - 1$. This proves the proposition.

Example 5.4 In the finite geometry $\mathbb{Z}(5) \times \mathbb{Z}(5)$ there are six lines through the origin, shown in Table 5.2. The corresponding mutually unbiased bases in $H[\mathbb{Z}(5)]$ are also shown.

We note that the above duality between mutually unbiased bases and finite geometries, does not hold for non-prime dimensions. This motivates the revision of the concept of mutually unbiased bases into another concept (which we call weak mutually unbiased bases), so that this duality is preserved. This is studied in the section below.

5.3 Weak Mutually Unbiased Bases and Duality with Finite Geometries

In systems where the variables take values in a field ($\mathbb{Z}(p)$ or $GF(p^e)$ with prime p) the number of mutually unbiased bases is equal to the maximum possible value $d+1$ (where d is the dimension of the system). In systems where the variables take values in a ring ($\mathbb{Z}(d)$ with non-prime d), it seems that the maximum number of mutually unbiased bases is smaller than $d+1$ (but there is no rigorous proof of this). The existence of non-invertible elements (apart from zero) in rings, seems to be linked to the fact that the number of mutually unbiased bases is smaller than $d+1$.

In this section we discuss the concept of weak mutually unbiased bases [23–26] which is tailored for rings, in the sense that there is a duality (correspondence) between the finite geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$ (discussed in Sect. 5.1) and weak mutually unbiased bases in $H[\mathbb{Z}(d)]$. This is a strong motivation for their study.

As the name indicates, the weak mutually unbiased bases are weaker structures than mutually unbiased bases, and this is related to the fact that rings are weaker structures than fields. Roughly speaking, we replace the requirement $|\langle X;m|Y;n\rangle|^2 = \frac{1}{d}$ in Eq. (5.25), with the requirement that $|\langle X;m|Y;n\rangle|^2$ is $\frac{1}{e_i}$ where e_i is a divisor of the dimension d. In the case of prime dimension there are no non-trivial divisors, and the weak mutually unbiased bases are mutually unbiased bases.

The number of weak mutually unbiased bases is shown to be $\psi(d)$ (the Dedekind psi function). For non-prime d we have $\psi(d) > d+1$, and measurements with the weak mutually unbiased bases provide $(d-1)\psi(d)$ probabilities, which is greater than the d^2-1 degrees of freedom in a density matrix. Therefore weak mutually unbiased bases do not provide independent information, and Eq. (5.27) does not hold.

As above, we consider the case where the dimension d is the product of two odd prime numbers $d = p_1 p_2$, which are different from each other.

Definition 5.2 A set of orthonormal bases in $H[\mathbb{Z}(p_1 p_2)]$ is weakly mutually unbiased, if the vectors in any two of these bases $|X;m\rangle$ and $|Y;n\rangle$, obey the relations in one of the following three categories:

(1)

$$\begin{aligned} |\langle X;m|Y;n\rangle|^2 &= \frac{1}{p_1}; \quad \text{if } \; n = m \pmod{p_2} \\ |\langle X;m|Y;n\rangle|^2 &= 0; \quad \text{otherwise} \end{aligned} \tag{5.44}$$

(2)

$$\begin{aligned} |\langle X;m|Y;n\rangle|^2 &= \frac{1}{p_2}; \quad \text{if } \; n = m \pmod{p_1} \\ |\langle X;m|Y;n\rangle|^2 &= 0; \quad \text{otherwise} \end{aligned} \tag{5.45}$$

(3)

$$|\langle X; m|Y; n\rangle|^2 = \frac{1}{p_1 p_2}. \tag{5.46}$$

Apart from the third option which is the standard definition of mutually unbiased bases, we have here two more options. Therefore any set of mutually unbiased bases in $H[\mathbb{Z}(p_1 p_2)]$, can be regarded as a subset of a bigger set of weak mutually unbiased bases.

Proposition 5.7 *We factorize the system $\Sigma[\mathbb{Z}(p_1 p_2)]$ as $\Sigma[\mathbb{Z}(p_1)] \otimes \Sigma[\mathbb{Z}(p_2)]$, as discussed in Sect. 4.9. For any set S_{WMUB} of weak mutually unbiased bases in $H[\mathbb{Z}(p_1 p_2)]$, there exists a set $|\mathscr{X}_1(\nu_1); \overline{m}_1\rangle$ of mutually unbiased bases in $H[\mathbb{Z}(p_1)]$, and a set $|\mathscr{X}_2(\nu_2); \overline{m}_2\rangle$, of mutually unbiased bases in $H[\mathbb{Z}(p_2)]$, such that the*

$$\begin{aligned} &S^{\max}_{\text{WMUB}} = \{|\mathscr{X}_1(\nu_1); \overline{m}_1\rangle \otimes |\mathscr{X}_2(\nu_2); \overline{m}_2\rangle\} \\ &\nu_1 = -1, ..., p_1 - 1; \quad \nu_2 = -1, ..., p_2 - 1 \end{aligned} \tag{5.47}$$

is a set of weak mutually unbiased bases, and $S_{\text{WMUB}} \subseteq S^{\max}_{\text{WMUB}}$. The cardinality of $S^{\max}_{\text{WMUB}}$ is $\psi(p_1 p_2)$.

Proof Let $|X; m\rangle$ and $|Y; n\rangle$ be two bases in $H[\mathbb{Z}(p_1 p_2)]$, which are factorized as

$$\begin{aligned} &|X; m\rangle = |X_1; \overline{m}_1\rangle \otimes |X_2; \overline{m}_2\rangle; \quad |Y; n\rangle = |X_1; \overline{n}_1\rangle \otimes |X_2; \overline{n}_2\rangle \\ &\overline{m}_1, \overline{n}_1 \in \mathbb{Z}(p_1); \quad \overline{m}_2, \overline{n}_2 \in \mathbb{Z}(p_2). \end{aligned} \tag{5.48}$$

We assume that the relations in the Definition 5.2 hold, and we will construct the corresponding set $S^{\max}_{\text{WMUB}}$ of weak mutually unbiased bases. We consider the following three cases:

(1) In the case that Eq. (5.44) holds, we get

$$|\langle X_1; \overline{m}_1|Y_1; \overline{n}_1\rangle||\langle X_2; \overline{m}_2|Y_2; \overline{n}_2\rangle|^2 = \frac{1}{p_1}. \tag{5.49}$$

The condition $n = m \pmod{p_2}$ gives $\overline{n}_2 = \overline{m}_2$. As (n, m) take all values in $\mathbb{Z}(p_1 p_2) \times \mathbb{Z}(p_1 p_2)$ such that $n = m \pmod{p_2}$, the $(\overline{n}_1, \overline{m}_1)$ take all values in $\mathbb{Z}(p_1) \times \mathbb{Z}(p_1)$. From Eq. (5.49), it follows that

$$|\langle X_1; \overline{m}_1|Y_1; \overline{n}_1\rangle|^2 \geq \frac{1}{p_1}; \quad \sum_{\overline{m}_1} |\langle X_1; \overline{m}_1|Y_1; \overline{n}_1\rangle|^2 = 1 \tag{5.50}$$

The first of these relations follows from Eq. (5.49). From this we conclude that

$$|\langle X_1; \overline{m}_1|Y_1; \overline{n}_1\rangle|^2 = \frac{1}{p_1}; \quad |\langle X_2; \overline{m}_2|Y_2; \overline{m}_2\rangle| = 1. \tag{5.51}$$

Therefore the $|X_1; \overline{m}_1\rangle$, $|Y_1; \overline{n}_1\rangle$, ..., are mutually unbiased bases in $H[\mathbb{Z}(p_1)]$. In this case the $|X_2; \overline{m}_2\rangle$ is the same basis as $|Y_2; \overline{n}_2\rangle$, so we have the tensor product of mutually unbiased bases in $H[\mathbb{Z}(p_1)]$, with one basis in $H[\mathbb{Z}(p_2)]$.

(2) The case where Eq. (5.45) holds, is similar to the above case.

(3) In the case that Eq. (5.46) holds, we get

$$|\langle X_1; \overline{m}_1|Y_1; \overline{n}_1\rangle|^2 |\langle X_2; \overline{m}_2|Y_2; \overline{n}_2\rangle|^2 = \frac{1}{p_1 p_2} \tag{5.52}$$

We also consider the overlap of $|X; m\rangle$ with another vector $|Y; n'\rangle$ in the second basis, such that $n = n' \pmod{p_1}$. Then $\overline{n}_1 = \overline{n}'_1$ and as n' takes all values in $\mathbb{Z}(p_1 p_2)$ subject to the constraint $n = n' \pmod{p_1}$, the $\overline{n}'_2$ takes all values in $\mathbb{Z}(p_2)$. We get

$$|\langle X_1; \overline{m}_1|Y_1; \overline{n}_1\rangle|^2 |\langle X_2; \overline{m}_2|Y_2; \overline{n}'_2\rangle|^2 = \frac{1}{p_1 p_2} \tag{5.53}$$

From Eqs. (5.52), (5.53) we see that $|\langle X_2; \overline{m}_2|Y_2; \overline{n}_2\rangle|$ is constant for all $\overline{n}_2 \in \mathbb{Z}(p_2)$. This and the relation

$$\sum_{\overline{n}_2 \in \mathbb{Z}(p_2)} |\langle X_2; \overline{m}_2|Y_2; \overline{n}_2\rangle|^2 = 1 \tag{5.54}$$

prove that $|\langle X_2; \overline{m}_2|Y_2; \overline{n}_2\rangle|^2 = \frac{1}{p_2}$. Therefore the $|X_2; \overline{m}_2\rangle$, $|Y_2; \overline{n}_2\rangle$ are mutually unbiased bases in $H[\mathbb{Z}(p_2)]$.
In a 'dual' way we prove that $|\langle X_1; \overline{m}_1|Y_1; \overline{n}_1\rangle|^2 = \frac{1}{p_1}$, and therefore the $|X_1; \overline{n}_1\rangle$, $|Y_1; \overline{m}_1\rangle$ are mutually unbiased bases in $H[\mathbb{Z}(p_1)]$.

The number of mutually unbiased bases in $H[\mathbb{Z}(p_1)]$ is $p_1 + 1$, and in $H[\mathbb{Z}(p_2)]$ is $p_2 + 1$. Therefore the maximum number of weak mutually unbiased bases in $H[\mathbb{Z}(p_1 p_2)]$ is $\psi(p_1 p_2) = (p_1 + 1)(p_2 + 1)$.

Notation 5.3 *We use an alternative 'factorized notation' for the states in Eq. (5.47), which is analogous to the 'factorized notation' for lines*

$$\begin{aligned}
|\mathscr{X}(\nu_1, \nu_2); \overline{m}_1, \overline{m}_2\rangle &= |\mathscr{X}_1(\nu_1); \overline{m}_1\rangle \otimes |\mathscr{X}_2(\nu_2); \overline{m}_2\rangle \\
|\mathscr{X}(-1, \nu_2); \overline{m}_1, \overline{m}_2\rangle &= |X_1; \overline{m}_1\rangle \otimes |\mathscr{X}_2(\nu_2); \overline{m}_2\rangle \\
|\mathscr{X}(\nu_1, -1); \overline{m}_1, \overline{m}_2\rangle &= |\mathscr{X}_1(\nu_1); \overline{m}_1\rangle \otimes |X_2; \overline{m}_2\rangle \\
|\mathscr{X}(-1, -1); \overline{m}_1, \overline{m}_2\rangle &= |X_1; \overline{m}_1\rangle \otimes |X_2; \overline{m}_2\rangle.
\end{aligned} \tag{5.55}$$

In order to establish a correspondence between the factorized and unfactorized notations for the weak mutually unbiased bases, we need the following corollary, which is analogous to Corollary 3.1.

Corollary 5.1 *Let S_1, S_2, S be symplectic transformations in $H[\mathbb{Z}(p_1)]$, $H[\mathbb{Z}(p_2)]$ and $H[\mathbb{Z}(p_1 p_2)]$, correspondingly. Then*

(1) If $\nu_1 \in \mathbb{Z}(p_1)$ and $\nu_2 \in \mathbb{Z}(p_2)$

$$\begin{aligned} &S_1(0,-1|1,\nu_1) \otimes S_2(0,-1|1,\nu_2) \\ &= S(0,-s_1t_1 - s_2t_2|p_1+p_2, \nu_1 s_1 + \nu_2 s_2) \end{aligned} \tag{5.56}$$

(2) If $\nu_2 \in \mathbb{Z}(p_2)$

$$\mathbf{1} \otimes S_2(0,-1|1,\nu_2) = S(s_1, -s_2t_2|p_1, s_1 + \nu_2 s_2) \tag{5.57}$$

(3) If $\nu_1 \in \mathbb{Z}(p_1)$

$$S_1(0,-1|1,\nu_1) \otimes \mathbf{1} = S(s_2, -s_1t_1|p_2, \nu_1 s_1 + s_2) \tag{5.58}$$

(4)

$$\mathbf{1} \otimes \mathbf{1} = \mathbf{1}. \tag{5.59}$$

Proof The proof is analogous to the one in Corollary 3.1, because the matrices g and S are different representations of the same group (the symplectic group).

The following proposition gives the relation between the factorized and unfactorized notation, for the weak mutually unbiased bases in $H[\mathbb{Z}(p_1 p_2)]$.

Proposition 5.8 *The correspondence between the factorized notation for weak mutually unbiased bases, and the unfactorized one (for which the notation in Eq. (4.53) is used), is as follows.*

(1) If $\nu_1 \in \mathbb{Z}(p_1)$ and $\nu_2 \in \mathbb{Z}(p_2)$, then

$$\begin{aligned} &|\mathscr{X}(\nu_1,\nu_2);\overline{m}_1,\overline{m}_2\rangle = |X(\alpha,\beta);m\rangle \\ &\alpha = p_1 + p_2; \quad \beta = \nu_1 s_1 + \nu_2 s_2; \quad m = \overline{m}_1 p_2 + \overline{m}_2 p_1. \end{aligned} \tag{5.60}$$

(2) If $\nu_2 \in \mathbb{Z}(p_2)$, then

$$\begin{aligned} &|\mathscr{X}(-1,\nu_2);\overline{m}_1,\overline{m}_2\rangle = |X(\alpha,\beta);m\rangle \\ &\alpha = p_1; \quad \beta = s_1 + \nu_2 s_2; \quad m = \overline{m}_1 p_2 + \overline{m}_2 p_1 \end{aligned} \tag{5.61}$$

(3) If $\nu_1 \in \mathbb{Z}(p_1)$, then

$$\begin{aligned} &|\mathscr{X}(\nu_1,-1);\overline{m}_1,\overline{m}_2\rangle = |X(\alpha,\beta);m\rangle \\ &\alpha = p_2; \quad \beta = \nu_1 s_1 + s_2; \quad m = \overline{m}_1 p_2 + \overline{m}_2 p_1 \end{aligned} \tag{5.62}$$

(4)

$$|\mathscr{X}(-1,-1);\overline{m}_1,\overline{m}_2\rangle = |X;m\rangle$$
$$m = \overline{m}_1 p_2 + \overline{m}_2 p_1 \tag{5.63}$$

Proof The proof follows immediately from Corollary 5.1.

Our notation and terminology so far, aimed to show the existence of duality between maximal lines in $\mathbb{Z}(p_1p_2)\times\mathbb{Z}(p_1p_2)$ and weak mutually unbiased bases in the Hilbert space $H[\mathbb{Z}(p_1p_2)]$. This is formalized in the proposition below.

Proposition 5.9 *There is a duality between the $\psi(p_1p_2)$ maximal lines through the origin in the non-near-linear finite geometry $\mathbb{Z}(p_1p_2)\times\mathbb{Z}(p_1p_2)$ and the $\psi(p_1p_2)$ weak mutually unbiased bases in the Hilbert space $H[\mathbb{Z}(p_1p_2)]$, where*

$$\mathscr{L}(\nu_1,\nu_2) \quad\leftrightarrow\quad \{|\mathscr{X}(\nu_1,\nu_2);\overline{m}_1,\overline{m}_2\rangle\}$$
$$\nu_1 = -1,...,p_1-1; \quad \nu_2 = -1,...,p_2-1. \tag{5.64}$$

The $d = p_1p_2$ points in the maximal line $\mathscr{L}(\nu_1,\nu_2)$ correspond to the $d = p_1p_2$ vectors in the basis $\{|\mathscr{X}(\nu_1,\nu_2);\overline{m}_1,\overline{m}_2\rangle\}$.

Proof For the proof we compare and contrast Propositions 5.3, 5.8, using the correspondence

$$L(0,1) \quad\leftrightarrow\quad |X;m\rangle$$
$$g(\kappa,\lambda|\mu,\nu) \quad\leftrightarrow\quad S(\kappa,\lambda|\mu,\nu). \tag{5.65}$$

For $\nu_1 = -1$ and $\nu_2 = -1$, we get

$$\mathscr{L}(-1,-1) = L_1(0,1)\times L_2(0,1) \quad\leftrightarrow$$
$$|\mathscr{X}(-1,-1);\overline{m}_1,\overline{m}_2\rangle = |X_1;\overline{m}_1\rangle\otimes|X_2;\overline{m}_2\rangle. \tag{5.66}$$

For $\nu_1 = 0,...,p_1-1$ and $\nu_2 = -1$, we get

$$\mathscr{L}(\nu_1,-1) = [g_1(0,-1|1,\nu_1)\circ L_1(0,1)]\times L_2(0,1) \quad\leftrightarrow$$
$$|\mathscr{X}(\nu_1,-1);\overline{m}_1,\overline{m}_2\rangle = [S_1(0,-1|1,\nu_1)|X_1;\overline{m}_1\rangle]\otimes|X_2;\overline{m}_2\rangle. \tag{5.67}$$

For $\nu_1 = -1$ and $\nu_2 = 0,...,p_2-1$, we get

$$\mathscr{L}(-1,\nu_2) = L_1(0,1)\times[g_2(0,-1|1,\nu_2)\circ L_2(0,1)] \quad\leftrightarrow$$
$$|\mathscr{X}(-1,\nu_2);\overline{m}_1,\overline{m}_2\rangle = |X_1;\overline{m}_1\rangle\otimes[S_2(0,-1|1,\nu_2)|X_2;\overline{m}_2\rangle]. \tag{5.68}$$

For $\nu_1 = 0,...,p_1-1$ and $\nu_2 = 0,...,p_2-1$, we get

$$\mathscr{L}(\nu_1, \nu_2) = [g_1(0, -1|1, \nu_1) \circ L_1(0, 1)] \times [g_2(0, -1|1, \nu_2) \circ L_2(0, 1)] \quad \leftrightarrow$$
$$|\mathscr{X}(\nu_1, \nu_2); \overline{m}_1, \overline{m}_2\rangle = [S_1(0, -1|1, \nu_1)|X_1; \overline{m}_1\rangle] \otimes [S_2(0, -1|1, \nu_2)|X_2; \overline{m}_2\rangle]. \tag{5.69}$$

These equations show the exact analogy between maximal lines through the origin in the finite geometry and weak mutuall unbiased bases, and prove the proposition.

Example 5.5 In $\mathbb{Z}(15) \times \mathbb{Z}(15)$ there are $\psi(15) = 24$ maximal lines through the origin. The dual statement is that in $H[\mathbb{Z}(15)]$ there are $\psi(15) = 24$ weak mutually unbiased bases. In the factorized notation for both lines and bases, the duality between them is

$$\mathscr{L}(\nu_1, \nu_2) \quad \leftrightarrow \quad \{|\mathscr{X}(\nu_1, \nu_2); \overline{m}_1, \overline{m}_2\rangle \mid \overline{m}_1 \in \mathbb{Z}(3); \quad \overline{m}_2 \in \mathbb{Z}(5)\}$$
$$\nu_1 = -1, ..., 2; \quad \nu_2 = -1, ..., 4. \tag{5.70}$$

This is shown in Table 5.3. Both the factorized and unfactorized notations are used (the correspondence is given in Proposition 5.3 for the lines, and in Proposition 5.8 for the bases).

We conclude this section with a brief summary on weak mutually unbiased bases and their duality to the finite geometries. In the case of prime dimension $d = p$, the weak mutually unbiased bases, are the same as mutually unbiased bases (prime numbers have only trivial divisors). In this case:

- Measurements with the $\psi(p) = p + 1$ mutually unbiased bases in $H[\mathbb{Z}(p)]$ provide independent information. Each basis is associated with $p - 1$ independent probabilities. The total number of independent probabilities is $(p - 1)\psi(p) = p^2 - 1$, and is equal to the number of degrees of freedom in a density matrix.
- The $\psi(p) = p + 1$ lines through the origin in the finite geometry $\mathbb{Z}(p) \times \mathbb{Z}(p)$, have no points in common, apart from the origin. Each line consists of $p - 1$ points, in addition to the origin. The total number of points is $(p - 1)\psi(p) = p^2 - 1$, plus the origin.

In the case of non-prime dimension d, the weak mutually unbiased bases, are different from mutually unbiased bases (non-prime numbers have non-trivial divisors). In this case:

- Measurements with the $\psi(d)$ weak mutually unbiased bases in $H[\mathbb{Z}(d)]$, provide $\psi(d)(d - 1)$ probabilities. Since $\psi(d)(d - 1)$ is greater than $d^2 - 1$ (which is the number of degrees of freedom in a density matrix), these probabilities are not independent.
- The $\psi(d)$ maximal lines through the origin in the finite geometry $\mathbb{Z}(d) \times \mathbb{Z}(d)$, have a total of $\psi(d)(d - 1)$ points, apart from the origin. Since $\psi(d)(d - 1)$ is greater than $d^2 - 1$ (which is the number of points in $\mathbb{Z}(d) \times \mathbb{Z}(d)$ apart from the origin), two lines might have more points in common apart from the origin.

Table 5.3 The 24 maximal lines through the origin in the finite geometry $\mathbb{Z}(15) \times \mathbb{Z}(15)$ and the corresponding weak mutually unbiased bases in $H[\mathbb{Z}(15)]$. Both the factorized and unfactorized notation, are used

Lines in $\mathbb{Z}(15) \times \mathbb{Z}(15)$	Bases in $H[\mathbb{Z}(15)]$
$\mathscr{L}(-1,-1) = L(0,1)$	$\lvert\mathscr{X}(-1,-1);\overline{m}_1,\overline{m}_2\rangle = \lvert X(0,1);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,0) = L(3,10)$	$\lvert\mathscr{X}(-1,0);\overline{m}_1,\overline{m}_2\rangle = \lvert X(3,10);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,1) = L(3,1)$	$\lvert\mathscr{X}(-1,1);\overline{m}_1,\overline{m}_2\rangle = \lvert X(3,1);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,2) = L(3,7)$	$\lvert\mathscr{X}(-1,2);\overline{m}_1,\overline{m}_2\rangle = \lvert X(3,7);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,3) = L(3,13)$	$\lvert\mathscr{X}(-1,3);\overline{m}_1,\overline{m}_2\rangle = \lvert X(3,13);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(-1,4) = L(3,4)$	$\lvert\mathscr{X}(-1,4);\overline{m}_1,\overline{m}_2\rangle = \lvert X(3,4);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,-1) = L(5,6)$	$\lvert\mathscr{X}(0,-1);\overline{m}_1,\overline{m}_2\rangle = \lvert X(5,6);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,0) = L(8,0)$	$\lvert\mathscr{X}(0,0);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,0);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,1) = L(8,6)$	$\lvert\mathscr{X}(0,1);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,6);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,2) = L(8,12)$	$\lvert\mathscr{X}(0,2);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,12);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,3) = L(8,3)$	$\lvert\mathscr{X}(0,3);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,3);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(0,4) = L(8,9)$	$\lvert\mathscr{X}(0,4);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,9);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,-1) = L(5,1)$	$\lvert\mathscr{X}(1,-1);\overline{m}_1,\overline{m}_2\rangle = \lvert X(5,1);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,0) = L(8,10)$	$\lvert\mathscr{X}(1,0);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,10);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,1) = L(8,1)$	$\lvert\mathscr{X}(1,1);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,1);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,2) = L(8,7)$	$\lvert\mathscr{X}(1,2);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,7);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,3) = L(8,13)$	$\lvert\mathscr{X}(1,3);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,13);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(1,4) = L(8,4)$	$\lvert\mathscr{X}(1,4);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,4);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,-1) = L(5,11)$	$\lvert\mathscr{X}(2,-1);\overline{m}_1,\overline{m}_2\rangle = \lvert X(5,11);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,0) = L(8,5)$	$\lvert\mathscr{X}(2,0);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,5);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,1) = L(8,11)$	$\lvert\mathscr{X}(2,1);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,11);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,2) = L(8,2)$	$\lvert\mathscr{X}(2,2);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,2);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,3) = L(8,8)$	$\lvert\mathscr{X}(2,3);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,8);5\overline{m}_1+3\overline{m}_2\rangle$
$\mathscr{L}(2,4) = L(8,14)$	$\lvert\mathscr{X}(2,4);\overline{m}_1,\overline{m}_2\rangle = \lvert X(8,14);5\overline{m}_1+3\overline{m}_2\rangle$

5.4 Other Topics

There has been an enormous amount of work on various aspects of mutually unbiased bases. We summarize some problems, which are not discussed here:

(1) The problem of finding the maximum number of mutually unbiased bases, in a system with dimension which is not a power of a prime number. This is a difficult problem even in the simple case of dimension $d = 6$ [27–31].
(2) The study of various finite geometries, related to finite quantum systems [32–38].
(3) Related to mutually unbiased bases is the so-called 'King's problem' [39–41].
(4) Acting with a unitary transformation on a set of mutually unbiased bases, we get another set of mutually unbiased bases. But there are unitarily inequivalent mutually unbiased bases which have been discussed in [42].

(5) There are links between mutually unbiased bases and latin squares [43] which have been studied in [44–47].
(6) There are links between mutually unbiased bases and designs [48] which have been studied in [49, 50].
(7) We can approach mutually unbiased bases, and also weak mutually unbiased bases, using the formalism of analytic representations discussed in Sect. 4.10. In particular it is interesting to study the zeros of the analytic functions that represent the vectors in mutually unbiased bases, and also in weak mutually unbiased bases. It has been shown in [26], that the duality discussed above is extended to a triality, that involves

- the maximal lines in the finite geometry
- the weak mutually unbiased bases
- the zeros of the analytic functions that represent the vectors in weak mutually unbiased bases.

(8) There is a partial order in the set of all finite geometries $\mathbb{Z}(d) \times \mathbb{Z}(d)$, where $\mathbb{Z}(e) \times \mathbb{Z}(e)$ is a subgeometry of $\mathbb{Z}(d) \times \mathbb{Z}(d)$, when e is a divisor of d. Through duality, there is also a partial order in the set of all weak mutually unbiased bases [51].
(9) Mutually unbiased bases in systems with dimension $d = 2^N$ have been studied in [52, 53].
(10) Deep links between mutually unbiased bases and path integrals, have been studied in [54].
(11) Symmetric informationally complete positive operator valued measures, have been studied in [55–58].

References

1. Batten, L. M. (1997). *Combinatorics of finite geometries*. Cambridge: Cambridge University Press.
2. Hirchfeld, J. W. P. (1979). *Projective geometries over finite fields*. Oxford: Oxford University Press.
3. Hirchfeld, J. W. P., & Thas, J. A. (1991). *General Galois geometries*. Oxford: Oxford University Press.
4. Ivanovic, I. D. (1981). *Journal of Physics A*, *14*, 3241.
5. Wootters, W. K., & Fields, B. D. (1989). *Annals of Physics (N.Y)*, *191*, 363.
6. Bandyopadhyay, S., Boykin, P. O., Roychowdhury, V., & Vatan, F. (2002). *Algorithmica*, *34*, 512.
7. Kibler, M. (2006). *International Journal of Modern Physics B*, *20*, 1792.
8. Kibler, M., & Planat, M. (2006). *International Journal of Modern Physics B*, *20*, 1802.
9. Sulc, P., & Tolar, J. (2007). *Journal of Physics A*, *40*, 15099.
10. Aschbachev, M., Childs, A. M., & Wocjan, P. (2007). *Journal of Algebraic Combinatorics*, *25*, 111.
11. Klimov, A., Romero, J. L., Bjork, G., & Sanchez-Soto, L. L. (2007). *Journal of Physics A*, *40*, 9177.
12. Albouy, O. (2009). *Journal of Physics A*, *42*, 072001.

13. Kibler, M. (2009). *Journal of Physics A*, *42*, 353001.
14. Godsil, C., & Roy, A. (2009). *European Journal of Combinatorics*, *30*, 246.
15. Klimov, A., Romero, J. L., Bjork, G., & Sanchez-Soto, L. L. (2009). *Annals of Physics*, *324*, 53.
16. Durt, T., Englert, B. G., Bengtsson, I., & Zyczkowski, K. (2010). *International Journal of Quantum Computation*, *8*, 535.
17. Daoud, M., & Kibler, M. (2010). *Journal of Physics A*, *43*, 115303.
18. Mandayam, P., Bandyopadhyay, S., Grassl, M., & Wootters, W. K. (2014). *Quantum Information and Computation*, *14*, 823.
19. Seyfarth, U., Sanchez-Soto, L. L., & Leuchs, G. (2014). *Journal of Physics A*, *47*, 455303.
20. Blanchfield, K. (2014). *Journal of Physics A*, *47*, 135303.
21. Kalev, A., & Gour, G. (2014). *New Journal of Physics*, *16*, 053038.
22. Fillipov, S. N., & Man'ko, V. I. (2011). *Physica Scripta*, *2011*, 014010.
23. Shalaby, M., & Vourdas, A. (2011). *Journal of Physics A*, *44*, 345303.
24. Shalaby, M., & Vourdas, A. (2012). *Journal of Physics A*, *45*, 052001.
25. Shalaby, M., & Vourdas, A. (2013). *Annals of Physics*, *337*, 208.
26. Olupitan, T., Lei, C., & Vourdas, A. (2016). *Annals of Physics*, *371*, 1.
27. M. Grassl, arXiv, quant-phys/0406175
28. Brierley, S., & Weigert, S. (2008). *Physical Review A*, *78*, 042312.
29. Brierley, S., & Weigert, S. (2009). *Physical Review A*, *79*, 052316.
30. Jaming, P., Matolcsi, M., Mora, P., Szollosi, F., & Weiner, M. (2009). *Journal of Physics A*, *42*, 245305.
31. Goyeneche, D. (2013). *Journal of Physics A*, *46*, 105301.
32. Calderbank, A. R., Cameron, P. J., Kantor, W. M., & Seidel, J. J. (1997). *Proceedings of the London Mathematical Society*, *75*, 436.
33. Planat, M., Saniga, M., & Kibler, M. (2006). *SIGMA*, *2*, 066.
34. Saniga, M., & Planat, M. (2006). *Journal of Physics A*, *39*, 435.
35. Saniga, M., Planat, M., Kibler, M., & Pracna, P. (2007). *Chaos, Solitons, Fractals*, *33*, 1095.
36. Planat, M., & Baboin, A. C. (2007). *Journal of Physics A*, *40*, F1005.
37. Havlicek, H., & Saniga, M. (2008). *Journal of Physics A*, *41*, 015302.
38. Saniga, M., Levay, P., & Pracna, P. (2012). *Journal of Physics A*, *45*, 295304.
39. Englert, B. G., & Aharanov, Y. (2001). *Physics Letter A*, *284*, 1.
40. Vaidman, L., Aharanov, Y., & Albert, D. Z. (1987). *Physical Review Letters*, *58*, 1385.
41. Kalev, A., Mann, A., & Revzen, M. (2013). *Europhysics Letters*, *104*, 50008.
42. Kantor, W. (2012). *Journal of Mathematical Physics*, *53*, 032204.
43. Denes, J., & Keedwell, A. D. (1974). *Latin squares and their applications*. New York: Academic.
44. Patarek, T., Dikic, B., & Brukner, C. (2009). *Physical Review A*, *79*, 01209.
45. Patarek, T., Pawlowski, M., Grassl, M., & Brukner, C. (2009). *Physical Review A*, *79*, 01209.
46. Hall, J. L., & Rao, A. (2010). *Journal of Physics A*, *43*, 135302.
47. Gaeta, M., di Mateo, O., Klimov, A. B., & de Guise, H. (2014). *Journal of Physics A*, *47*, 435303.
48. Beth, T., Jungnickel, D., & Lenz, H. (1993). *Design theory*. Cambridge: Cambridge University Press.
49. Zauner, G. (2011). *International Journal of Quantum Information*, *1*, 445.
50. Graydon, M., & Appleby, D. M. (2016). *Journal of Physics A*, *49*, 085301.
51. Oladejo, S., Lei, C., & Vourdas, A. (2014). *Journal of Physics A*, *47*, 485204.
52. Durt, T. (2005). *Journal of Physics A*, *38*, 5267.
53. Kern, O., Ranade, K. S., & Seyfarth, U. (2010). *Journal of Physics A*, *43*, 275305.
54. Tolar, J., & Hadzitaskos, G. (2009). *Journal of Physics A*, *42*, 245306.
55. Renes, J. M., Blume-Kohut, R., Scott, A. J., & Caves, C. M. (2004). *Journal of Mathematical Physics*, *45*, 2171.
56. Scott, A. J., & Grassl, M. (2010). *Journal of Mathematical Physics*, *51*, 042203.
57. Appleby, D. M. (2005). *Journal of Mathematical Physics*, *46*, 052107.
58. Appleby, D. M., Flammia, S. T., & Fuchs, C. A. (2011). *Journal of Mathematical Physics*, *52*, 022202.

Chapter 6
Quantum Logic of Finite Quantum Systems

Abstract The modular orthocomplemented lattice that describes the quantum logic of finite quantum systems, is discussed. The formalism provides the theoretical computer science foundation for the study of quantum gates.

After the fundamental work of Birkhoff and von Neumann [1], quantum logic has been studied extensively in the literature [2–10]. In the case of an infinite-dimensional Hilbert space $\mathscr{H}$, it is based on the Birkhoff-von Neumann orthomodular lattice $\mathscr{L}(\mathscr{H})$, which consists of the closed subspaces in $\mathscr{H}$, with the operations of conjunction, disjunction and complementation. In our case of a finite-dimensional Hilbert space $H[\mathbb{Z}(d)]$, all subspaces are closed and the lattice of subspaces $\mathfrak{L}(d)$ is a modular orthocomplemented lattice [11–15].

Both of these lattices violate distributivity. The modular orthocomplemented lattice $\mathfrak{L}(d)$ obeys modularity (which is a weak version of distributivity), but the orthomodular lattice $\mathscr{L}(\mathscr{H})$ violates modularity. Orthomodularity is a weaker concept than orthocomplemented modularity.

Below we present the basic properties of the modular orthocomplemented lattice $\mathfrak{L}(d)$, of subspaces of $H[\mathbb{Z}(d)]$. They describe the quantum logic of finite quantum systems, and provide the theoretical foundations for quantum computation. For comparison we first discuss briefly the classical logic, described with Boolean algebras [16, 17] and Boolean rings [18–20], which are the theoretical foundations for classical computation.

An important difference between classical computation and quantum computation (with finite Hilbert spaces), is that the disjunction is different, and also that the property of distributivity in the former, is replaced with the weaker property of modularity in the latter.

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_6

Table 6.1 The $A \vee B$, $A \wedge B = A \cdot B$, $A \uparrow B$, $A \downarrow B$, and $A + B$ for all subsets of $S = \{1, 2\}$, in the simplifying notation of Eq. (6.11)

A	B	$A \vee B$	$A \wedge B = A \cdot B$	$A \uparrow B$	$A \downarrow B$	$A + B$
0	0	0	0	3	3	0
1	0	1	0	3	2	1
2	0	2	0	3	1	2
3	0	3	0	3	0	3
0	1	1	0	3	2	1
1	1	1	1	2	2	0
2	1	3	0	3	0	3
3	1	3	1	2	0	2
0	2	2	0	3	1	2
1	2	3	0	3	0	3
2	2	2	2	1	1	0
3	2	3	2	1	0	1
0	3	3	0	3	0	3
1	3	3	1	2	0	2
2	3	3	2	1	0	1
3	3	3	3	0	0	0

6.1 Classical Logic: Boolean Algebras

Classical Boolean logic is defined on the powerset 2^S of a finite set S (i.e., on the set of the subsets of S). The disjunction (logical OR), conjunction (logical AND) and complementation (logical NOT) operations are the union, intersection and complement of set theory, correspondingly:

$$A \vee B = A \cup B; \quad A \wedge B = A \cap B; \quad \neg A = S \setminus A; \quad A, B \subseteq S. \tag{6.1}$$

The powerset 2^S with these operations is a Boolean algebra (complemented distributive lattice). The least element is the empty set $0 = \emptyset$, and the greatest element is $I = S$. The partial order $\prec$ in this lattice is the subset $\subseteq$. For every element A

$$0 \prec A \prec I. \tag{6.2}$$

The following proposition summarizes the important properties of Boolean algebras, and is given without proof [16, 17]

Proposition 6.1 *The following properties hold in Boolean algebras:*

(1) Commutativity and associativity for both disjunction and conjunction.
(1) The distributivity property:

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C). \tag{6.3}$$

(2) The 'law of the excluded middle', which states that a statement is either true or not true (there is no third option). It is expressed with the first of the following relations, which are equivalent to each other:

$$A \vee (\neg A) = I; \quad \neg(\neg A) = A. \tag{6.4}$$

(3) The De Morgan relations:

$$\neg(A \wedge B) = (\neg A) \vee (\neg B)$$
$$\neg(A \vee B) = (\neg A) \wedge (\neg B). \tag{6.5}$$

(4)

$$\neg I = 0; \quad \neg 0 = I; \quad A \vee A = A; \quad A \wedge A = A; \quad A \wedge (\neg A) = 0$$
$$A \vee I = I; \quad A \vee 0 = A; \quad A \wedge I = A; \quad A \wedge 0 = 0. \tag{6.6}$$

(5) If $A_1 \prec B_1$ and $A_2 \prec B_2$ then

$$A_1 \vee A_2 \prec B_1 \vee B_2; \quad A_1 \wedge A_2 \prec B_1 \wedge B_2. \tag{6.7}$$

(6) If $A_1 \prec B_1$ then $\neg A_1 \succ \neg B_1$.
(7) If $A_1 \prec B_1$ then $A_1 \setminus B_1 = 0$.

Other logical operations are the NAND and NOR operations.

Definition 6.1 The NAND operation denoted with $\uparrow$, and the NOR operation denoted with $\downarrow$, are given by:

$$A \uparrow B = \neg(A \wedge B); \quad A \downarrow B = \neg(A \vee B) \tag{6.8}$$

Their importance lies in the following result.

Proposition 6.2 *The conjuction, disjunction and negation can be expressed in terms of only the NAND operation, or only the NOR operation, as:*

$$A \vee B = (A \uparrow A) \uparrow (B \uparrow B); \quad A \wedge B = (A \uparrow B) \uparrow (A \uparrow B); \quad \neg A = A \uparrow A, \tag{6.9}$$

and

$$A \wedge B = (A \downarrow A) \downarrow (B \downarrow B); \quad A \vee B = (A \downarrow B) \downarrow (A \downarrow B); \quad \neg A = A \downarrow A. \tag{6.10}$$

Proof The proof is straightforward.

Example 6.1 We consider the four subsets of the set $S = \{1, 2\}$. In Table 6.1, we give the results for $A \vee B$, $A \wedge B$, $A \uparrow B$, $A \downarrow B$, using the simplifying notation

$$\emptyset \rightarrow 0; \quad \{1\} \rightarrow 1; \quad \{2\} \rightarrow 2; \quad \{1, 2\} \rightarrow 3. \tag{6.11}$$

They are the OR, AND, NAND, NOR gates with inputs and outputs that take $2^{|S|}$ values, where in this example $|S| = 2$.

6.1.1 Boolean Rings

There are deep connections between set theory and Boolean algebras, with Boolean rings. The Stone formalism [18–20], reveals the existence of links between these two apparently different areas. It also links these areas with topology, but this is not discussed here.

Definition 6.2 A Boolean ring, is a ring with idempotent multiplication (i.e. $A \cdot A = A$).

It can be proved that a ring with idempotent multiplication is commutative.

The Stone formalism replaces the disjunction (logical OR) in Boolean algebra, with the addition (logical XOR) in Boolean rings, which is defined as the symmetric difference of sets:

$$A + B = (A \setminus B) \cup (B \setminus A) \tag{6.12}$$

The multiplication in Boolean rings, is the same as the conjunction (logical AND) in Boolean algebra:

$$A \cdot B = A \wedge B. \tag{6.13}$$

Lemma 6.1 *(1) The $A \vee B$ can be expressed in terms of addition and multiplication, as*

$$A \vee B = A + B + (A \cdot B). \tag{6.14}$$

(2) Both addition and multiplication are commutative and associative.
(3) Distributivity holds:

$$A \cdot (B + C) = (A \cdot B) + (A \cdot C) \tag{6.15}$$

(4) The $0 = \emptyset$ plays the role of additive zero.

$$A + 0 = A \tag{6.16}$$

(5) The additive inverse of a set is the set itself:

$$-A = A; \quad A + A = 0. \tag{6.17}$$

(6) The $I = S$ plays the role of unity (multiplicative zero).

$$A \cdot I = A \tag{6.18}$$

(7) The complementation $\neg A$ (logical NOT) of Boolean algebra, corresponds to I+A=I-A in Boolean rings:

$$\neg A = I + A = I - A. \tag{6.19}$$

(8) The multiplication is idempotent:

$$A \cdot A = A. \tag{6.20}$$

(9) The NAND, NOR operations, can be written as:

$$A \uparrow B = I + A \cdot B; \quad A \downarrow B = I + A + B + A \cdot B. \tag{6.21}$$

Proof All these properties involve operations with sets and can be seen using Venn diagrams.

Proposition 6.3 *The powerset 2^S with the addition and multiplication in Eqs. (6.12) and (6.13) is a Boolean ring.*

Proof The above lemma shows that the powerset 2^S with the addition and multiplication in Eqs. (6.12) and (6.13) is a ring, and that the multiplication is idempotent (Eq. (6.20)). Therefore it is Boolean ring.

6.1.2 Classical Gates

Let S be a finite set. A classical gate with n inputs and m outputs is a function

$$\mathscr{G} : \left(2^S\right)^n \rightarrow \left(2^S\right)^m, \tag{6.22}$$

that maps an input $(A_1, ..., A_n)$ to an output $(B_1, ..., B_m)$:

$$\mathscr{G}(A_1, ..., A_n) = (B_1, ..., B_m); \quad A_i, B_j \subseteq S. \tag{6.23}$$

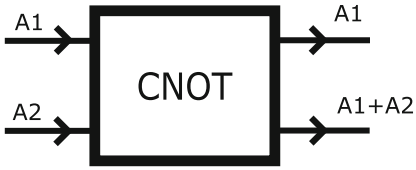

Fig. 6.1 The CNOT gate

In most of the literature $S = \{1\}$, i.e., the input and output variables are binary ($\emptyset$ or $\{1\}$). The case where they take d values has also been studied, but to a lesser extent (e.g., [21] in a classical context, and [22, 23] in a quantum context).

Examples of gates are:

$$\begin{aligned}
&\mathscr{G}_{\mathrm{OR}}(A_1, A_2) = A_1 + A_2 + A_1 \cdot A_2 = A_1 \vee A_2 \\
&\mathscr{G}_{\mathrm{AND}}(A_1, A_2) = A_1 \cdot A_2 = A_1 \wedge A_2 \\
&\mathscr{G}_{\mathrm{XOR}}(A_1, A_2) = A_1 + A_2 \\
&\mathscr{G}_{\mathrm{NAND}}(A_1, A_2) = I + A_1 \cdot A_2 \\
&\mathscr{G}_{\mathrm{NOR}}(A_1, A_2) = I + A_1 + A_2 + A_1 \cdot A_2 \\
&\mathscr{G}_{\mathrm{NOT}}(A) = \neg A = I + A.
\end{aligned} \tag{6.24}$$

In a reversible classical gate, there is a bijective map between the set of all inputs and the set of all outputs. In other words, to every output corresponds exactly one input. The OR, AND, XOR, are not reversible gates, but the NOT is a reversible gate. We are interested in reversible classical gates, because they can be linked to quantum gates (unitary quantum transformations are reversible).

An example of reversible gate is the CNOT gate (Fig. 6.1), which is the following bijective map from $\left(2^S\right)^2$ to $\left(2^S\right)^2$:

$$\mathscr{G}_{\mathrm{CNOT}}(A_1, A_2) = (A_1, A_1 + A_2). \tag{6.25}$$

Using the properties of Boolean rings , we easily show that:

$$\begin{aligned}
&\mathscr{G}_{\mathrm{CNOT}}(A, A) = (A, 0) \\
&\mathscr{G}_{\mathrm{CNOT}}(A, 0) = (A, A) \\
&\mathscr{G}_{\mathrm{CNOT}}(A, I) = (A, \neg A) \\
&\mathscr{G}_{\mathrm{CNOT}} \circ \mathscr{G}_{\mathrm{CNOT}} = \mathbf{1}.
\end{aligned} \tag{6.26}$$

$\mathscr{G}_{\mathrm{CNOT}} \circ \mathscr{G}_{\mathrm{CNOT}}$ is the composition of two of these functions, and describes two of these gates in a series.

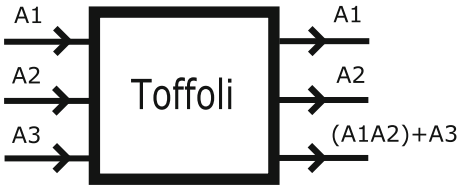

Fig. 6.2 The Toffoli gate

Another example of reversible gate is the Toffoli gate (Fig. 6.2), which is the following bijective map from $\left(2^S\right)^3$ to $\left(2^S\right)^3$:

$$\begin{aligned} &\mathscr{G}_{\text{Toffoli}}(A_1, A_2, A_3) = (A_1, A_2, (A_1 \cdot A_2) + A_3) \\ &\mathscr{G}_{\text{Toffoli}} \circ \mathscr{G}_{\text{Toffoli}} = \mathbf{1}. \end{aligned} \tag{6.27}$$

6.2 The Modular Orthocomplemented Lattice $\mathfrak{L}(d)$

6.2.1 Quantum Versus Classical Disjunction

Let $\mathfrak{L}(d)$ be the set of subspaces of $H[\mathbb{Z}(d)]$. $\mathscr{O}$ is the zero-dimensional subspace which contains only the zero vector, and belongs to $\mathfrak{L}(d)$. Let H_1, H_2 be elements of $\mathfrak{L}(d)$. The conjunction operation (logical 'AND') and disjunction operation (logical 'OR'), are defined as

$$H_1 \wedge H_2 = H_1 \cap H_2; \qquad H_1 \vee H_2 = \text{span}(H_1 \cup H_2) \tag{6.28}$$

The disjunction contains all superpositions in the two subspaces. $\mathfrak{L}(d)$ with these operations is a lattice. The corresponding partial order $\prec$ is 'subspace'. The least element is $\mathscr{O}$, and the greatest element is $I = H[\mathbb{Z}(d)]$. The logical NOT operation is defined in the next section.

The classical OR is very different from the quantum OR operation. The classical OR operation is defined on Boolean algebras and is the union of two subsets. The quantum OR operation is defined on the lattice $\mathfrak{L}(d)$, and it is much more than the union of two subspaces, because it contains all superpositions of vectors in the two subspaces. The discussion in the literature on Schrodinger cats, elucidates the difference between classical and quantum OR.

From the logic point of view, the difference between classical and quantum OR, is central for the fact that classical computation is different from quantum computation.

Remark 6.1 In an infinite-dimensional Hilbert space $\mathscr{H}$, the disjunction is defined as

$$H_1 \vee H_2 = \overline{\text{span}}(H_1 \cup H_2) \tag{6.29}$$

where the overline indicates closure. This is not needed in the case of finite-dimensional Hilbert spaces, considered here.

6.2.2 Projectors to the Subspaces

Let $\Pi(H_1)$ be the projector to a subspace H_1 of $H[\mathbb{Z}(d)]$. Projectors to the subspaces are related to measurements, and the following lemma gives some relations which can be useful in practical calculations.

Lemma 6.2 *(1)*

$$\begin{aligned}&\Pi(H_1 \wedge H_2)\Pi(H_1) = \Pi(H_1)\Pi(H_1 \wedge H_2) = \Pi(H_1 \wedge H_2)\\ &\Pi(H_1 \vee H_2)\Pi(H_1) = \Pi(H_1)\Pi(H_1 \vee H_2) = \Pi(H_1).\end{aligned} \tag{6.30}$$

(2) If $\Pi(H_1)\Pi(H_2) = 0$ *then*

$$\begin{aligned}&H_1 \wedge H_2 = \mathscr{O}; \quad \Pi(H_1) + \Pi(H_2) = \Pi(H_1 \vee H_2)\\ &\Pi(H_2)\Pi(H_1) = 0.\end{aligned} \tag{6.31}$$

But the $H_1 \wedge H_2 = \mathscr{O}$ *does not necessarily imply that* $\Pi(H_1)\Pi(H_2) = 0$.

(3) $\Pi(H_1 \wedge H_2) = \Pi(H_1)\Pi(H_2)$ *if and only if* $[\Pi(H_1), \Pi(H_2)] = 0$.

Proof The proof of the first two parts is straightforward. For the third part, we note that if $[\Pi(H_1), \Pi(H_2)] = 0$ then

$$[\Pi(H_1)\Pi(H_2)]^2 = \Pi(H_1)\Pi(H_2). \tag{6.32}$$

Therefore the $\Pi(H_1)\Pi(H_2)$ is a projector into a space with vectors which belong to both spaces H_1, H_2, i.e., to $H_1 \wedge H_2$. This proves that $\Pi(H_1 \wedge H_2) = \Pi(H_1)\Pi(H_2)$. The proof of the converse is straightforward.

$H^\perp$ denotes the orthocomplement of H (the logical 'NOT'), and it is a subspace of $H[\mathbb{Z}(d)]$, orthogonal to H, which obeys the properties

$$\begin{aligned}&H \wedge H^\perp = \mathscr{O}; \quad H \vee H^\perp = I; \quad (H^\perp)^\perp = H\\ &(H_1 \wedge H_2)^\perp = H_1^\perp \vee H_2^\perp; \quad (H_1 \vee H_2)^\perp = H_1^\perp \wedge H_2^\perp.\end{aligned} \tag{6.33}$$

The corresponding projectors obey the properties:

$$\begin{aligned}&\Pi(H)\Pi(H^\perp) = 0; \quad \Pi(H) + \Pi(H^\perp) = \mathbf{1}\\ &\Pi(H_1 \wedge H_2)\Pi(H_1^\perp \wedge H_3) = 0.\end{aligned} \tag{6.34}$$

We will use the notation

$$\Pi^{\perp}(H) = \mathbf{1} - \Pi(H) = \Pi(H^{\perp}). \tag{6.35}$$

6.2.3 The Modularity Property of $\mathfrak{L}(d)$

The lattice $\mathfrak{L}(d)$ is a modular orthocomplemented lattice. The modularity property is that if $H_1 \prec H_3$ then

$$H_1 \vee (H_2 \wedge H_3) = (H_1 \vee H_2) \wedge H_3. \tag{6.36}$$

Modularity is a weak version of distributivity.

Example 6.2 In $H[\mathbb{Z}(3)]$ we consider the spaces H_1, H_2, H_3, that contain the vectors

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}; \; v_2 = \begin{pmatrix} a_2 \\ a_2' \\ 0 \end{pmatrix}; \; v_3 = \begin{pmatrix} a_3 \\ 0 \\ a_3' \end{pmatrix}, \tag{6.37}$$

correspondingly, where a_i, a_i' take all complex values. The space H_1 is one-dimensional and the spaces H_2, H_3 are two-dimensional. H_1 is a subspace of H_3, and we will confirm that the modularity relation holds.

The space $H_2 \wedge H_3$ contains the vector

$$v_{2\wedge 3} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}. \tag{6.38}$$

We use a self-explanatory notation for the indices of the vectors. Therefore the space $H_1 \vee (H_2 \wedge H_3)$ contains vectors of the form

$$v_{1\vee(2\wedge 3)} = \begin{pmatrix} a+b \\ 0 \\ a \end{pmatrix}. \tag{6.39}$$

Also the space $H_1 \vee H_2$ contains the vectors

$$v_{1\vee 2} = \begin{pmatrix} a_1 + a_2 \\ a_2' \\ a_1' \end{pmatrix} \tag{6.40}$$

and therefore the space $(H_1 \vee H_2) \wedge H_3$ contains vectors of the form

$$v_{(1\vee 2)\wedge 3} = \begin{pmatrix} a_3 \\ 0 \\ a_3' \end{pmatrix}. \tag{6.41}$$

It is therefore clear that the modularity relation $H_1 \vee (H_2 \wedge H_3) = (H_1 \vee H_2) \wedge H_3$ holds.

6.2.4 Non-distributivity of the Lattice $\mathfrak{L}(d)$

The lattice $\mathfrak{L}(d)$ is not distributive. We introduce projectors, which can be used in measurements that demonstrate the non-distributive nature of the lattice $\mathfrak{L}(d)$.

In any lattice the following distributivity inequalities hold:

$$\begin{aligned} (H_1 \wedge H_2) \vee H_0 &\prec (H_1 \vee H_0) \wedge (H_2 \vee H_0) \\ (H_1 \vee H_2) \wedge H_0 &\succ (H_1 \wedge H_0) \vee (H_2 \wedge H_0) \end{aligned} \tag{6.42}$$

They become equalities in distributive lattices. The following projectors can detect deviations from distributivity [24]:

$$\begin{aligned} \mathscr{P}_1 &= \Pi[(H_1 \vee H_0) \wedge (H_2 \vee H_0)] - \Pi[(H_1 \wedge H_2) \vee H_0] \\ \mathscr{P}_2 &= \Pi[(H_1 \vee H_2) \wedge H_0] - \Pi[(H_1 \wedge H_0) \vee (H_2 \wedge H_0)] \end{aligned} \tag{6.43}$$

Measurements with these projectors which give a non-zero result, prove the non-distributive nature of the lattice $\mathfrak{L}(d)$.

Example 6.3 In $H[\mathbb{Z}(3)]$ we consider the one dimensional spaces H_0, H_1, H_2, defined by the vectors

$$v_0 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}; \quad v_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}; \quad v_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \tag{6.44}$$

correspondingly. In this case

$$H_0 \wedge H_1 = H_0 \wedge H_2 = H_1 \wedge H_2 = \mathscr{O}. \tag{6.45}$$

The spaces $H_0 \vee H_1$, $H_0 \vee H_2$, $H_1 \vee H_2$ contain vectors of the form

$$v_{0\vee 1} = \begin{pmatrix} a_0 + a_1 \\ 2a_1 \\ a_0 + a_1 \end{pmatrix}; \; v_{0\vee 2} = \begin{pmatrix} a_0' + a_2 \\ a_2 \\ a_0' + a_2 \end{pmatrix}; \; v_{1\vee 2} = \begin{pmatrix} a_1' + a_2' \\ 2a_1' + a_2' \\ a_1' + a_2' \end{pmatrix}, \tag{6.46}$$

correspondingly, where a_i, a_i' take all values in $\mathbb{C}$. We can show that $H_0 \vee H_1 = H_0 \vee H_2$, by inserting $a_2 = 2a_1$ and $a_0' = a_0 - a_1$ in the vector $v_{0\vee 2}$, and then comparing it with $v_{0\vee 1}$. We then find that

$$\begin{aligned}&(H_1 \vee H_0) \wedge (H_2 \vee H_0) = H_0 \vee H_1; \quad (H_1 \wedge H_2) \vee H_0 = H_0\\ &(H_1 \vee H_2) \wedge H_0 = H_0; \quad (H_1 \wedge H_0) \vee (H_2 \wedge H_0) = \mathscr{O}.\end{aligned} \tag{6.47}$$

The relation $(H_1 \vee H_2) \wedge H_0 = H_0$ is shown by considering the relation $v_{1\vee 2} = \lambda v_0$. Therefore

$$\mathscr{P}_1 = \Pi(H_1 \vee H_0) - \Pi(H_0); \quad \mathscr{P}_2 = \Pi(H_0) \tag{6.48}$$

H_1 is one-dimensional space, and we can calculate the $\Pi(H_1 \vee H_0) - \Pi(H_0)$ using the Gram-Schmidt orthogonalization method, which we express in our notation as

$$\Pi(H_1 \vee H_0) - \Pi(H_0) = \frac{\Pi^{\perp}(H_0)\Pi(H_1)\Pi^{\perp}(H_0)}{\mathrm{Tr}[\Pi^{\perp}(H_0)\Pi(H_1)]}. \tag{6.49}$$

We get

$$\mathscr{P}_1 = \begin{pmatrix}0&0&0\\0&1&0\\0&0&0\end{pmatrix}; \quad \mathscr{P}_2 = \frac{1}{2}\begin{pmatrix}1&0&1\\0&0&0\\1&0&1\end{pmatrix}. \tag{6.50}$$

6.2.5 *Transpose Intervals in the Lattice $\mathfrak{L}(d)$*

If $H_1 \prec H_2$, we use the notation $[H_1, H_2]$, for the set that contains all the spaces H_0 such that $H_1 \prec H_0 \prec H_2$. It can be shown that $[H_1, H_2]$ is a sublattice of $\mathfrak{L}(d)$, and it is called interval sublattice. If $H_0 \in [H_1, H_2]$, then

$$[\Pi(H_0), \Pi(H_1)] = [\Pi(H_0), \Pi(H_2)] = 0. \tag{6.51}$$

An important concept in modular lattices, is the transpose intervals [11–15], presented in our context below [24].

Definition 6.3 Let $[H_1, H_2]$ and $[H_3, H_4]$ be interval sublattices of $\mathfrak{L}(d)$, such that

$$H_4 = H_2 \vee H_3; \quad H_1 = H_2 \wedge H_3. \tag{6.52}$$

We say that $[H_3, H_4]$ is upper transpose of $[H_1, H_2]$ or that $[H_1, H_2]$ is lower transpose of $[H_3, H_4]$ and denote this as

$$[H_1, H_2] \sqsubset [H_3, H_4]. \tag{6.53}$$

Proposition 6.4 $\sqsubset$ *is a partial order in the set of all interval sublattices.*

Proof We prove the following three properties, which show that $\sqsubset$ is a partial order.

(1)

$$[H_1, H_2] \sqsubset [H_1, H_2]. \tag{6.54}$$

Indeed $H_1 \prec H_2$ and therefore $H_1 = H_1 \wedge H_2$ and $H_2 = H_1 \vee H_2$.

(2) If

$$[H_1, H_2] \sqsubset [H_3, H_4] \text{ and } [H_3, H_4] \sqsubset [H_1, H_2], \tag{6.55}$$

then $H_1 = H_3$ and $H_2 = H_4$. In order to prove this, we note that from Eq. (6.55) we get the relations

$$\begin{aligned} H_1 &= H_2 \wedge H_3; \quad H_4 = H_2 \vee H_3 \\ H_3 &= H_1 \wedge H_4; \quad H_2 = H_1 \vee H_4. \end{aligned} \tag{6.56}$$

But the $H_1 = H_2 \wedge H_3$ implies that $H_1 \prec H_3$, and the $H_3 = H_1 \wedge H_4$ implies that $H_3 \prec H_1$. Therefore $H_1 = H_3$. In a similar way we prove that $H_2 = H_4$.

(3) If

$$[H_1, H_2] \sqsubset [H_3, H_4] \text{ and } [H_3, H_4] \sqsubset [H_5, H_6], \tag{6.57}$$

then $[H_1, H_2] \sqsubset [H_5, H_6]$. In order to prove this, we note that from Eq. (6.57) we get the relations

$$\begin{aligned} H_1 &= H_2 \wedge H_3; \quad H_4 = H_2 \vee H_3 \\ H_3 &= H_4 \wedge H_5; \quad H_6 = H_4 \vee H_5, \end{aligned} \tag{6.58}$$

and we need to prove that

$$H_1 = H_2 \wedge H_5; \quad H_6 = H_2 \vee H_5. \tag{6.59}$$

Combining the $H_1 = H_2 \wedge H_3$ with the $H_3 = H_4 \wedge H_5$ we get $H_1 = H_2 \wedge H_4 \wedge H_5$. But the $H_4 = H_2 \vee H_3$ shows that $H_4 \succ H_2$ and therefore

$$H_1 = H_2 \wedge H_4 \wedge H_5 = H_2 \wedge H_5. \tag{6.60}$$

In a similar way we prove that $H_6 = H_2 \vee H_5$.

The following proposition is well known for modular lattices [11–13], and we give it in the context of the lattice $\mathfrak{L}(d)$, without proof. Sometimes it is called 'parallelogram law' because it involves the subspaces in the parallelogram $(H_1 \wedge H_2, H_1, H_1 \vee H_2, H_2)$:

Proposition 6.5 *There is a bijective map between the interval sublattices* $[H_1 \wedge H_2, H_1]$ *and* $[H_2, H_1 \vee H_2]$*, which maps* $H_A \in [H_1 \wedge H_2, H_1]$ *into* $H_B \in [H_2, H_1 \vee H_2]$*, where*

$$H_B = H_A \vee H_2; \qquad H_A = H_B \wedge H_1. \tag{6.61}$$

There is also a bijective map between the interval sublattices $[H_1 \wedge H_2, H_2]$ *and* $[H_1, H_1 \vee H_2]$*, which maps* $H_C \in [H_1 \wedge H_2, H_2]$ *into* $H_D \in [H_1, H_1 \vee H_2]$*, where*

$$H_D = H_C \vee H_1; \quad H_C = H_D \wedge H_2. \tag{6.62}$$

A quantity that characterizes the parallelogram $(H_1 \wedge H_2, H_1, H_1 \vee H_2, H_2)$, is

$$\mathfrak{D}(H_1, H_2) = \Pi(H_1 \vee H_2) - \Pi(H_1) - \Pi(H_2) + \Pi(H_1 \wedge H_2). \tag{6.63}$$

The proposition below discusses some of its properties.

Proposition 6.6 *(1)* $\mathfrak{D}(H_1, H_2)$ *is related to the commutator* $[\Pi(H_1), \Pi(H_2)]$*, as follows:*

$$[\Pi(H_1), \Pi(H_2)] = \mathfrak{D}(H_1, H_2)[\Pi(H_1) - \Pi(H_2)]. \tag{6.64}$$

Therefore $\mathfrak{D}(H_1, H_2) = 0$ *if and only if the* $\Pi(H_1), \Pi(H_2)$ *commute.*

(2) $\mathrm{Tr}[\mathfrak{D}(H_1, H_2)] = 0$.

(3) The $\mathfrak{D}(H_1, H_2)$ *has d real eigenvalues, and at least* $d - \dim(H_1 \vee H_2)$ *of them, are equal to zero.*

(4) In transpose intervals, the $\mathfrak{D}(H_1, H_2)$ *has the following additivity property. If* $[H_1, H_2] \sqsubset [H_3, H_4] \sqsubset [H_5, H_6]$ *then*

$$\mathfrak{D}(H_2, H_3) + \mathfrak{D}(H_4, H_5) = \mathfrak{D}(H_2, H_5). \tag{6.65}$$

Proof (1) We multiply both sides of Eq. (6.63) by $\Pi(H_1)$ on the left, and we get

$$\mathfrak{D}(H_1, H_2)\Pi(H_1) = \Pi(H_1 \wedge H_2) - \Pi(H_2)\Pi(H_1). \tag{6.66}$$

We also multiply both sides of Eq. (6.63) by $\Pi(H_2)$ on the left, and we get

$$\mathfrak{D}(H_1, H_2)\Pi(H_2) = \Pi(H_1 \wedge H_2) - \Pi(H_1)\Pi(H_2). \tag{6.67}$$

Subtracting these two equations we prove Eq. (6.64).

(2) $\mathrm{Tr}[\Pi(H_1)]$ is equal to the dimension of H_1, which we denote as $\dim(H_1)$. In modular lattices (e.g., [11], p.41)

$$\dim(H_1 \vee H_2) + \dim(H_1 \wedge H_2) - \dim(H_1) - \dim(H_2) = 0. \tag{6.68}$$

and this proves that $\mathrm{Tr}[\mathfrak{D}(H_1, H_2)] = 0$.

(3) $\mathfrak{D}(H_1, H_2)$ is a $d \times d$ Hermitian matrix, and therefore it has d real eigenvalues. The $(H_1 \vee H_2)^{\perp}$ is a space orthogonal to $H_1 \vee H_2$, with dimension $d - \dim(H_1 \vee H_2)$. Every vector v in $(H_1 \vee H_2)^{\perp}$, gives

$$\Pi(H_1)v = \Pi(H_2)v = \Pi(H_1 \vee H_2)v = \Pi(H_1 \wedge H_2)v = 0, \tag{6.69}$$

and therefore $\mathfrak{D}(H_1, H_2)v = 0$. This shows that v is an eigenvector of $\mathfrak{D}(H_1, H_2)$ with eigenvalue 0. The fact that the dimension of $(H_1 \vee H_2)^{\perp}$ is $d - \dim(H_1 \vee H_2)$, shows that at least $d - \dim(H_1 \vee H_2)$ of the eigenvalues of $\mathfrak{D}(H_1, H_2)$ are equal to 0.

(4) Since $[H_1, H_2] \sqsubset [H_3, H_4] \sqsubset [H_5, H_6]$, it follows that

$$\begin{aligned} H_1 &= H_2 \wedge H_3; \quad H_4 = H_2 \vee H_3 \\ H_3 &= H_4 \wedge H_5; \quad H_6 = H_4 \vee H_5 \\ H_1 &= H_2 \wedge H_5; \quad H_6 = H_2 \vee H_5 \end{aligned} \tag{6.70}$$

Using them we can prove that

$$\begin{aligned} &\Pi(H_2 \vee H_3) - \Pi(H_2) - \Pi(H_3) + \Pi(H_2 \wedge H_3) + \\ &\Pi(H_4 \vee H_5) - \Pi(H_4) - \Pi(H_5) + \Pi(H_4 \wedge H_5) = \\ &\Pi(H_2 \vee H_5) - \Pi(H_2) - \Pi(H_5) + \Pi(H_2 \wedge H_5) \end{aligned} \tag{6.71}$$

which proves Eq. (6.65).

Remark 6.2 If ρ is a density matrix, the

$$p(H_1|\rho) = \mathrm{Tr}[\Pi(H_1)\rho] \tag{6.72}$$

is a probability. The trace of the product of a density matrix ρ with $\mathfrak{D}(H_1, H_2)$, gives

$$\mathrm{Tr}[\rho\mathfrak{D}(H_1, H_2)] = p(H_1 \vee H_2|\rho) + p(H_1 \wedge H_2|\rho) - p(H_1|\rho) - p(H_2|\rho). \tag{6.73}$$

This quantity is zero when the $\Pi(H_1)$, $\Pi(H_2)$ commute, but in general it is different from zero. This should be compared and contrasted to the fact that at a classical level, Kolmogorov probabilities always obey the relation

$$p(A \vee B) + p(A \wedge B) - p(A) - p(B) = 0. \tag{6.74}$$

Here A, B are sets and $A \vee B$, $A \wedge B$ are their union and intersection. This point is discussed further in [25].

References

1. Birkhoff, G., & von Neumann, J. (1936). *Annals of Mathematics*, *37*, 823.
2. Mackey, G. W. (1963). *Mathematical foundations of quantum mechanics*. New York: Benjamin.
3. Jauch, J. (1968). *Foundations of quantum mechanics*. Reading: Addison-Wesley.
4. Varadarajan, V. S. (1968). *Geometry of quantum theory*. Heidelberg: Springer.
5. Foulis, D. J., & Randall, C. H. (1972). *Journal of Mathematical Physics*, *13*, 1667.
6. Randall, C. H., & Foulis, D. J. (1973). *Journal of Mathematical Physics*, *14*, 1472.
7. Piron, C. (1976). *Foundations of quantum physics*. New York: Benjamin.
8. Beltrametti, E., Cassinelli, G. (1981). *The logic of quantum mechanics*. Reading: Addison-Wesley.
9. Abramsky, S., Coecke, B. (2004). In *Proceedings of 19th Annual IEEE Symposium on Logic in Computer Science*, (p. 415)
10. Engesser, K., Gabbay, D. M., & Lehmann, D. (2009). *Handbook of quantum logic and quantum structures*. Amsterdam: Elsevier.
11. Birkhoff, G. (1995). Lattice theory. *American Mathematical Society*, Rhode Island.
12. Szasz, G. (1963). *Introduction to lattice theory*. London: Academic.
13. Gratzer, G. A. (2003). *General lattice theory*. Heidelberg: Springer.
14. Kalmbach, G. (1983). *Orthomodular lattices*. London: Academic.
15. Ptak, P., & Pulmannova, S. (1991). *Orthomodular lattices as quantum logics*. Dordrecht: Kluwer.
16. Halmos, P. R. (1963). *Lectures on boolean algebras*. New York: Springer.
17. Sikorski, R. (1969). *Boolean algebras*. New York: Springer.
18. Stone, M. (1936). *Transactions of the American Mathematical Society*, *40*, 37.
19. Stone, M. (1937). *Transactions of the American Mathematical Society*, *41*, 375.
20. Johnstone, M. (1982). *Stone spaces*. Cambridge: Cambridge University Press.
21. Su, S. Y. H., Sarris, A. A. (1970). *IEEE Transactions on Computers*, *C-21*, 479.
22. Muthukrishman, A., & Stroud, C. R. (2000). *Physical Review A*, *62*, 052309.
23. Lanyon, B. P., et al. (2009). *Nature Physics*, *5*, 134.
24. Vourdas, A. (2016). *Journal of Geometry and Physics*, *101*, 38.
25. Vourdas, A. (2014). *Journal of Mathematical Physics*, *55*, 082107.

Chapter 7
Applications

Abstract Applications of the formalism of finite quantum systems, to angle and angular momentum operators, interferometry, orbital angular momentum states, etc, are briefly discussed.

In this chapter we discuss applications of the formalism into the area of Quantum Optics and Quantum Information, and also into other areas. Each of these applications is a subject in its own right, and here we briefly define the basic quantities and guide the reader through the literature.

7.1 Angle States and Angular Momentum States

In this section we apply the general formalism of finite quantum systems, to a system with angular momentum j. In this case $d = 2j + 1$ where j is an integer ('Bose case'), and the variables take values in $\mathbb{Z}(2j + 1)$. The relevant Hilbert space is $H[\mathbb{Z}(2j + 1)]$, which in this chapter we denote for simplicity $H(2j + 1)$.

The analogue of the momentum states are here the usual angular momentum states, which we denote as $|J;\ j\ m\rangle$. The extra J to the usual notation is not a variable, but it simply indicates angular momentum states. The analogue of position states are the angle states [1], which we denote as $|\theta;\ j\ m\rangle$, and which are defined through Fourier transform below.

The angular momentum operators J_z, J_+, J_-, form the $SU(2)$ algebra

$$[J_z, J_+] = J_+; \qquad [J_z, J_-] = -J_-; \qquad [J_+, J_-] = 2J_z. \tag{7.1}$$

The Casimir operator is

$$J^2 = J_z^2 + \frac{1}{2}(J_+J_- + J_-J_+) = j(j + 1)\mathbf{1}. \tag{7.2}$$

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_7

Then

$$\begin{aligned} J_+|J;\, j\; m\rangle &= [j(j+1) - m(m+1)]^{1/2}|J;\, j\; m+1\rangle \\ J_-|J;\, j\; m\rangle &= [j(j+1) - m(m-1)]^{1/2}|J;\, j\; m-1\rangle \\ J_z|J;\, j\; m\rangle &= m|J;\, j\; m\rangle \\ J^2|J;\, j\; m\rangle &= j(j+1)|J;\, j\; m\rangle. \end{aligned} \tag{7.3}$$

The Fourier transform in the present context is

$$F = \frac{1}{\sqrt{2j+1}} \sum_{m,n} \omega(mn)|J;\, j\; m\rangle\langle J;\, j\; n|; \quad F^4 = \mathbf{1}. \tag{7.4}$$

Acting with it on the angular momentum states, we get angle states:

$$|\theta;\, j\; m\rangle = F^\dagger|J;\, j\; m\rangle = \frac{1}{\sqrt{2j+1}} \sum_n \omega(-mn)|J;\, j\; n\rangle \tag{7.5}$$

Also acting with it on the angular momentum operators we get the angle operators

$$F^\dagger J_z F = \theta_z; \quad F^\dagger J_+ F = \theta_+; \quad F^\dagger J_- F = \theta_- \tag{7.6}$$

which form the $SU(2)$ algebra

$$[\theta_z, \theta_+] = \theta_+; \quad [\theta_z, \theta_-] = -\theta_-; \quad [\theta_+, \theta_-] = 2\theta_z \tag{7.7}$$

The corresponding Casimir operator is

$$\theta^2 = \theta_z^2 + \frac{1}{2}(\theta_+\theta_- + \theta_-\theta_+) = j(j+1)\mathbf{1}. \tag{7.8}$$

Relations analogous to Eqs. (7.3), also hold for angle operators and angle states (because we have performed a Fourier transform, which is a unitary transform):

$$\begin{aligned} \theta_+|\theta;\, j\; m\rangle &= [j(j+1) - m(m+1)]^{1/2}|\theta;\, j\; m+1\rangle \\ \theta_-|\theta;\, j\; m\rangle &= [j(j+1) - m(m-1)]^{1/2}|\theta;\, j\; m-1\rangle \\ \theta_z|\theta;\, j\; m\rangle &= m|\theta;\, j\; m\rangle \\ \theta^2|\theta;\, j\; m\rangle &= j(j+1)|\theta;\, j\; m\rangle \end{aligned} \tag{7.9}$$

We next introduce a polar decomposition of the 'Cartesian operators' J_+ and J_- in terms of the 'radial operator' J_r and the 'exponential of the phase operator' Z:

$$
\begin{aligned}
&J_+ = J_r Z; \qquad J_- = Z^\dagger J_r \\
&J_r = (J_+ J_-)^{1/2} = [j(j+1)\mathbf{1} - J_z^2 + J_z]^{1/2}; \quad [J_r, J_z] = 0 \\
&Z = \sum_m |J;\, j\ m+1\rangle\langle J;\, j\ m| \qquad (7.10)
\end{aligned}
$$

The dual relations to them are

$$
\begin{aligned}
&\theta_+ = \theta_r X; \qquad \theta_- = X^\dagger \theta_r \\
&\theta_r = (\theta_+ \theta_-)^{1/2} = [j(j+1)\mathbf{1} - \theta_z^2 + \theta_z]^{1/2}; \quad [\theta_r, \theta_z] = 0 \\
&X = \sum_m |\theta;\, j\ m+1\rangle\langle\theta;\, j\ m|. \qquad (7.11)
\end{aligned}
$$

We can show that the X, Z obey Proposition 4.2, with the following correspondence:

$$
|X; m\rangle \ \rightarrow\ |\theta;\, j\ m\rangle; \quad |P; m\rangle \ \rightarrow\ |J;\, j\ m\rangle. \qquad (7.12)
$$

Also the analogue of Eq. (4.18), is here

$$
X = \exp\left[-i\frac{2\pi}{d}J_z\right]; \quad Z = \exp\left[i\frac{2\pi}{d}\theta_z\right]. \qquad (7.13)
$$

Therefore all the formalism in Chap. 4, can be used here also.

7.1.1 The Schwinger Representation

We consider a two-mode harmonic oscillator with Hilbert space $\mathscr{H}_1 \times \mathscr{H}_2$. Let $a_1^\dagger$, a_1 and $a_2^\dagger$, a_2 be the creation and annihilation operators for the two modes, and $|N_1, N_2\rangle$ the number eigenstates:

$$
a_1^\dagger a_1 |N_1, N_2\rangle = N_1 |N_1, N_2\rangle; \quad a_2^\dagger a_2 |N_1, N_2\rangle = N_2 |N_1, N_2\rangle. \qquad (7.14)
$$

In the Schwinger representation of $SU(2)$ [2], the angular momentum operators are expressed as

$$
J_+ = a_1^\dagger a_2; \qquad J_- = a_1 a_2^\dagger; \qquad J_z = \frac{1}{2}\left(a_1^\dagger a_1 - a_2^\dagger a_2\right). \qquad (7.15)
$$

The Casimir operator is

$$
\begin{aligned}
&J^2 = n_s\,(n_s+1)\,; \quad n_s = \frac{1}{2}(a_1^\dagger a_1 + a_2^\dagger a_2) \\
&[n_s, J_+] = [n_s, J_-] = [n_s, J_z] = 0. \qquad (7.16)
\end{aligned}
$$

The number eigenstates play the role of the angular momentum states, as follows:

$$|N_1, N_2\rangle \;\leftrightarrow\; |J; j\ m\rangle; \quad j = \frac{1}{2}(N_1 + N_2); \quad m = \frac{1}{2}(N_1 - N_2) \tag{7.17}$$

With this correspondence, we can easily show that the standard angular momentum relations in Eq. (7.3) hold. Here the $(2j+1)$-dimensional Hilbert space $H(2j+1)$, contains superpositions of the states

$$H(2j+1) = \{|N, 2j+1-N\rangle \mid N = 0, ..., 2j+1\} \tag{7.18}$$

Then the Hilbert space $\mathscr{H}_1 \times \mathscr{H}_2$ can be written as the direct sum:

$$\begin{aligned} &\mathscr{H}_1 \times \mathscr{H}_2 = \mathscr{H}_B \oplus \mathscr{H}_F \\ &\mathscr{H}_B = \bigoplus_j H(2j+1); \quad j = 0, 1, 2, ... \\ &\mathscr{H}_F = \bigoplus_j H(2j+1); \quad j = \frac{1}{2}, \frac{3}{2}, ... \end{aligned} \tag{7.19}$$

$\mathscr{H}_B$ is the Bose Hilbert space (the direct sum of spaces with integer j), and $\mathscr{H}_F$ is the Fermi Hilbert space (the direct sum of spaces with half-integer j). $\mathscr{H}_B$ is spanned by number eigenstates with an odd total number of photons in the two modes. $\mathscr{H}_F$ is spanned by number eigenstates with an even total number of photons in the two modes.

As an application of this we consider a two-mode system described by the following Hamiltonian, which is used for the description of frequency converters in Quantum Optics:

$$\begin{aligned} \mathfrak{H} &= E_1 a_1^\dagger a_1 + E_2 a_2^\dagger a_2 + \lambda a_1^\dagger a_2 + \lambda^* a_1 a_2^\dagger \\ &= (E_1 + E_2) n_s + (E_1 - E_2) J_z + \lambda J_+ + \lambda^* J_- \end{aligned} \tag{7.20}$$

Systems with this Hamiltonian can be studied with the above formalism.

7.1.2 Angle States and Angular Momentum States in $\mathscr{H}_B$

Let α, β be spherical coordinates describing the points on a two-dimensional sphere S_2, with radius one. We define the following angular momentum states in $\mathscr{H}_B$:

$$|J; \alpha, \beta\rangle = \sum_{j,m} Y^*_{jm}(\alpha, \beta) |J; j\ m\rangle; \quad 0 \le \alpha \le \pi; \quad 0 \le \beta < 2\pi \tag{7.21}$$

$Y_{jm}(\alpha, \beta)$ are the usual spherical harmonics. We also introduce the 'dual spherical harmonics' [3] which are related to the usual spherical harmonics through a finite Fourier transform:

$$X_{jn}(\alpha, \beta) = \frac{1}{\sqrt{2j+1}} \sum_m Y_{jm}(\alpha, \beta)\omega(nm) \tag{7.22}$$

We define angle states in $\mathscr{H}_B$, as:

$$|\theta; \alpha, \beta\rangle = \sum_{j,m} Y^*_{jm}(\alpha, \beta)|\theta; j\ m\rangle = \sum_{j,m} X^*_{jm}(\alpha, \beta)|J; j\ m\rangle. \tag{7.23}$$

The states $|\theta; \alpha, \beta\rangle$ and also the states $|J; \alpha, \beta\rangle$ form orthonormal bases in $\mathscr{H}_B$.

$$\int |\theta; \alpha, \beta\rangle\langle\theta; \alpha, \beta| d\cos\alpha d\beta = \int |J; \alpha, \beta\rangle\langle J; \alpha, \beta| d\cos\alpha d\beta = \mathbf{1}. \tag{7.24}$$

An arbitrary state $|f\rangle$ in $\mathscr{H}_B$, can be represented with the functions

$$f_J(\alpha, \beta) = \langle J; \alpha, \beta|f\rangle; \quad f_\theta(\alpha, \beta) = \langle\theta; \alpha, \beta|f\rangle. \tag{7.25}$$

7.1.3 Area Preserving Diffeomorphisms on a Sphere

Above we discussed angle and angular momentum operators based on the $SU(2)$ group. The $SU(2)$ is locally isomorphic to $SO(3)$ which describes rotations of a solid sphere.

A more general group is the $SDiff(S_2)$ of area preserving diffeomorphisms on a sphere S_2. They describe general transformations of a perfect liquid on a sphere. Since rotations of a solid sphere are a very special case of these transformations, we expect that this more general formalism will lead to the standard angular momentum operators plus many other operators. Such groups for a sphere and also other surfaces, have been studied in the context of string theory [4–10].

We consider the following transformations from $(\cos\alpha, \beta)$ to

$$\begin{aligned} &\cos\gamma = \mathscr{A}(\cos\alpha, \beta); \quad \delta = \mathscr{B}(\cos\alpha, \beta) \\ &\frac{\partial(\cos\gamma, \delta)}{\partial(\cos\alpha, \beta)} = \frac{\partial\cos\gamma}{\partial\cos\alpha}\frac{\partial\delta}{\partial\beta} - \frac{\partial\delta}{\partial\cos\alpha}\frac{\partial\cos\gamma}{\partial\beta} = 1. \end{aligned} \tag{7.26}$$

Since the Jacobian is equal to one, the area is preserved under these transformations.

An infinitesimal version of these transformations is

$$\cos\gamma = \cos\alpha + A(\cos\alpha, \beta)\varepsilon; \quad \delta = \beta + B(\cos\alpha, \beta)\varepsilon$$
$$\frac{\partial A}{\partial \cos\alpha} + \frac{\partial B}{\partial \beta} = 0. \tag{7.27}$$

ε is an infinitesimal parameter. The last equation comes from the fact that the Jacobian is equal to one, and for topologically trivial manifolds like a sphere, implies the existence of a function $g(\alpha, \beta)$ such that

$$A = -\frac{\partial g}{\partial \beta}; \quad B = \frac{\partial g}{\partial \cos\alpha}. \tag{7.28}$$

We consider two bases $|J; \alpha, \beta\rangle$ and $|J; \gamma, \delta\rangle$, where γ, δ are related to α, β through the infinitesimal transformations in Eq. (7.27). We represent an arbitrary state $|f\rangle$ in $\mathscr{H}_B$, with the functions

$$f(\alpha, \beta) = \langle J; \alpha, \beta | f\rangle; \quad f(\gamma, \delta) = \langle J; \gamma, \delta | f\rangle. \tag{7.29}$$

Then

$$\frac{f(\gamma, \delta) - f(\alpha, \beta)}{\varepsilon} \approx \frac{\partial(g(\alpha, \beta), f(\alpha, \beta))}{\partial(\cos\alpha, \beta)}. \tag{7.30}$$

This leads to the following definition.

Definition 7.1 The operator J_g acts on $f_J(\alpha, \beta)$, as follows:

$$J_g f(\alpha, \beta) = \langle J; \alpha, \beta | J_g | f\rangle = \frac{\partial(g(\alpha, \beta), f(\alpha, \beta))}{\partial(\cos\alpha, \beta)}. \tag{7.31}$$

In analogous way we define the operators θ_g. The following proposition describes some properties of J_g.

Proposition 7.1 *(1) The commutator of J_g and J_h, is given in terms of the Poisson bracket of g, h (with respect to $\cos\alpha, \beta$), by*

$$[J_g, J_h] = J_{\{g,h\}}; \quad \{g, h\} = \frac{\partial g}{\partial \cos\alpha}\frac{\partial h}{\partial \beta} - \frac{\partial h}{\partial \beta}\frac{\partial g}{\partial \cos\alpha}. \tag{7.32}$$

(2) J_g acts on the sum of two functions as follows:

$$J_g[\mu_1 f_1(\alpha, \beta) + \mu_2 f_2(\alpha, \beta)] = \mu_1 J_g f_1(\alpha, \beta) + \mu_2 J_g f_2(\alpha, \beta). \tag{7.33}$$

(3) J_g acts on the product of two functions as follows:

$$J_g[f_1(\alpha, \beta) f_2(\alpha, \beta)] = f_1(\alpha, \beta) J_g f_2(\alpha, \beta) + f_2(\alpha, \beta) J_g f_1(\alpha, \beta). \tag{7.34}$$

(4) The exponential of J_g acts on the sum of two functions as follows:

$$\exp(\lambda J_g)[\mu_1 f_1(\alpha,\beta)+\mu_2 f_2(\alpha,\beta)] = \mu_1 \exp(\lambda J_g) f_1(\alpha,\beta) + \mu_2 \exp(\lambda J_g) f_2(\alpha,\beta). \quad (7.35)$$

(5) The exponential of J_g acts on the product of two functions as follows:

$$\exp(\lambda J_g)[f_1(\alpha,\beta) f_2(\alpha,\beta)] = [\exp(\lambda J_g) f_1(\alpha,\beta)][\exp(\lambda J_g) f_2(\alpha,\beta)]. \quad (7.36)$$

Proof For the proof we refer to Ref. [11].

We expand the function $g(\alpha,\beta)$ in terms of spherical harmonics, as

$$g(\alpha,\beta) = \sum_{j,m} g_{jm} Y_{jm}(\alpha,\beta). \quad (7.37)$$

Then

$$J_g = \sum_{j,m} g_{jm} J_{jm}; \quad J_{jm} f(\alpha,\beta) = \frac{\partial(Y_{jm}(\alpha,\beta),\, f(\alpha,\beta))}{\partial(\cos\alpha,\beta)}. \quad (7.38)$$

In particular

$$J_{jm} Y_{\ell n}(\alpha,\beta) = \langle J;\alpha,\beta|J_{jm}|J;\ell\ n\rangle = \frac{\partial(Y_{jm}(\alpha,\beta), Y_{\ell n}(\alpha,\beta))}{\partial(\cos\alpha,\beta)}. \quad (7.39)$$

The Poisson bracket of $Y_{j_1 m_1}(\alpha,\beta)$ and $Y_{j_2 m_2}(\alpha,\beta)$, is given by

$$\{Y_{j_1 m_1}, Y_{j_2 m_2}\} = \sum_{\ell,n} \tau(j_1,m_1;\, j_2,m_2|\ell,n) Y_{\ell n}. \quad (7.40)$$

The structure constants $\tau(j_1,m_1;\, j_2,m_2|\ell,n)$ are given in [5]. Consequently

$$[J_{j_1 m_1}, J_{j_2 m_2}] = \sum_{\ell,n} \tau(j_1,m_1;\, j_2,m_2|\ell,n) J_{\ell n}. \quad (7.41)$$

The J_{jm} are generalizations of the angular momentum operators. The J_{1m} are simply the standard angular momentum operators J_+, J_z, J_- (with a different normalization).

This formalism has been used in string theory, but it might also be useful in the general area of quantum optics and quantum information, because it generalizes the angular momentum formalism.

7.2 Interferometry in Multimode Systems

In this section we use the formalism of finite quantum systems, in the context of interferometry that involves d harmonic oscillators. The overall Hilbert space in this problem is $H_{\text{osc}} \otimes ... \otimes H_{\text{osc}}$, where H_{osc} is the infinite-dimensional Hilbert space of the harmonic oscillator. The mode index is the 'position' in this problem, and it takes values in $\mathbb{Z}(d)$. Through a finite Fourier transform of the d modes, we get a dual mode index which plays the role of 'momentum', and which also takes values in $\mathbb{Z}(d)$. So in this context, the $\mathbb{Z}(d) \times \mathbb{Z}(d)$ is a 'mode phase space'.

The formalism has important applications in metrology, because it leads to resolutions below the standard quantum limit [12]. It has been studied extensively both with photons and also with Bose-Einstein condensates. Here we present briefly the link between this area, and the formalism of finite quantum systems studied in Chap. 4. We refer to the literature for more details, and for practical applications of these devices [13–23].

We consider a system comprised of d harmonic oscillators. The creation and annihilation operators corresponding to the m-th mode, are:

$$\begin{aligned} &a_m^\dagger = \mathbf{1} \otimes ... \otimes a^\dagger \otimes ... \otimes \mathbf{1}; \quad a_m = \mathbf{1} \otimes ... \otimes a \otimes ... \otimes \mathbf{1} \\ &[a_m, a_n^\dagger] = \delta(m,n); \quad m,n \in \mathbb{Z}(d). \end{aligned} \tag{7.42}$$

Let Λ be a $d \times d$ Hermitian matrix, and U the unitary operator

$$U = \exp\left[i \sum_{m,n} a_m^\dagger \Lambda_{mn} a_n \right]. \tag{7.43}$$

It is known (e.g. [24]) that

$$\begin{aligned} &b_m = U a_m U^\dagger = \sum_n V_{mn} a_n; \quad b_m^\dagger = U a_m^\dagger U^\dagger = \sum_n V_{mn}^* a_n^\dagger \\ &V = \exp(-i\Lambda); \qquad V V^\dagger = \mathbf{1}. \end{aligned} \tag{7.44}$$

The vacuum state remains invariant under these transformations. Also the total average number of photons in a state remains invariant under the U transformations:

$$U|0, ..., 0\rangle = |0, ..., 0\rangle; \quad \sum_m b_m^\dagger b_m = \sum_m a_m^\dagger a_m. \tag{7.45}$$

7.2.1 Fourier Interferometry and Applications to Metrology

A special case of the formalism above, is the Fourier transform of the modes:

$$U_F = \exp\left[i \sum_{m,n} a_m^\dagger \Lambda_{mn} a_n \right]; \quad \Lambda = i \ln F; \quad ; \quad (U_F)^4 = \mathbf{1}, \tag{7.46}$$

where F is the $d \times d$ Fourier matrix, in Eq. (4.2). Then

$$\begin{aligned} b_m &= U_F a_m U_F^\dagger = \frac{1}{\sqrt{d}} \sum_n \omega(mn) a_n \\ b_m^\dagger &= U_F a_m^\dagger U_F^\dagger = \frac{1}{\sqrt{d}} \sum_n \omega(-mn) a_n^\dagger \end{aligned} \tag{7.47}$$

The dual mode index related to b_m, $b_m^\dagger$ plays the role of momentum. So in the present context position and momentum is the mode index related to the a_m, $a_m^\dagger$ and b_m, $b_m^\dagger$, correspondingly. Experiments that use beam splitters to implement these transforms have been discussed in [14]. The use of the factorization in Sect. 4.9 reduces the number of beam splitters, as discussed in [23].

There are various applications of these devices. As an example, we consider the case where the input is a number state with N photons in the m-th mode, and vacuum in the other modes:

$$|s\rangle = |0, ..., 0, N, 0, ...0\rangle \tag{7.48}$$

Then in the large d limit, the phase uncertainty in the m-th output is [20]

$$\Delta\theta_m \sim \frac{\sqrt{d}}{N}. \tag{7.49}$$

This is below the standard quantum limit and can have applications in metrology.

It is seen that the formalism of finite quantum systems presented in this monograph, can also be used for the study of interferometry in multimode systems (with a finite number of modes).

7.2.2 Other Types of Interferometry

Here we consider other special cases of the general operators U in Eq. (7.43). The first one, is:

$$U_X = \exp\left[i \sum_{m,n} a_m^\dagger \Lambda_{mn} a_n \right]; \quad \Lambda = i \ln X; \quad (U_X)^d = \mathbf{1}. \tag{7.50}$$

where X is the $d \times d$ matrix, in Eq. (4.19). Then

$$\begin{aligned} b_m &= U_X a_m U_X^\dagger = a_{m+1} \\ b_m^\dagger &= U_X a_m^\dagger U_X^\dagger = a_{m+1}^\dagger \end{aligned} \tag{7.51}$$

This shifts the modes by one place (and the last mode becomes first). In other words, it shifts the modes in the 'mode-position' direction, in the $\mathbb{Z}(d) \times \mathbb{Z}(d)$ mode phase space.

Another special case is

$$U_Z = \exp\left[i \sum_{m,n} a_m^\dagger \Lambda_{mn} a_n \right]; \quad \Lambda = i \ln Z; \quad (U_Z)^d = \mathbf{1}. \tag{7.52}$$

where Z is the $d \times d$ matrix, in Eq. (4.19). Then

$$\begin{aligned} b_m &= U_Z a_m U_Z^\dagger = a_m \omega(m) \\ b_m^\dagger &= U_Z a_m^\dagger U_Z^\dagger = a_m \omega(-m). \end{aligned} \tag{7.53}$$

This multiplies each mode a_m by $\omega(m)$, i.e., it shifts the modes in the 'mode-momentum' direction, in the $\mathbb{Z}(d) \times \mathbb{Z}(d)$ mode phase space.

We next divide the Hilbert space $H_{\text{osc}} \otimes ... \otimes H_{\text{osc}}$, into d 'sectors':

$$\begin{aligned} H_{\text{osc}} \otimes ... \otimes H_{\text{osc}} &= \bigoplus_{n=0}^{d-1} \mathscr{H}_n \\ \mathscr{H}_n &= \text{span}\{|N_0, ..., N_{d-1}\rangle \mid N_0 + ... + N_{d-1} = n (\text{mod } d)\}; \quad n \in \mathbb{Z}(d). \end{aligned} \tag{7.54}$$

The sector $\mathscr{H}_n$ is spanned by number eigenstates, with a total number of photons equal to $n (\text{mod } d)$. We call π_n the projector to $\mathscr{H}_n$. It can be shown that π_n commutes with both U_X, U_Z, and we define the:

$$U_{Xn} = U_X \pi_n; \quad U_X = \sum_{n=0}^{d-1} U_{Xn}; \quad [U_X, \pi_n] = 0$$
$$U_{Zn} = U_Z \pi_n; \quad U_Z = \sum_{n=0}^{d-1} U_{Zn}; \quad [U_Z, \pi_n] = 0. \tag{7.55}$$

Then the U_{Xn}, U_{Zn} form a Heisenberg-Weyl group within $\mathscr{H}_n$, which has been studied in [21]:

$$U_{Xn}^{\alpha} U_{Zn}^{\beta} = U_{Zn}^{\beta} U_{Xn}^{\alpha} \omega(-n\alpha\beta); \quad \alpha, \beta \in \mathbb{Z}(d). \tag{7.56}$$

So apart from the Fourier interferometry devices, there are many other devices which can have various applications in Quantum Optics and Quantum Information.

7.3 Orbital Angular Momentum States

The paraxial wave equation in cylindrical coordinates, leads to the Laguerre-Gauss modes

$$u_{nm}(r, \phi) \sim r^{|m|} L_n^{|m|} \left(\frac{2r^2}{w^2} \right) \exp\left(-\frac{r^2}{w^2} \right) \exp(-im\phi) \tag{7.57}$$

Here $L_n^{|m|}$ are Laguerre polynomials, and n, m are the radial quantum number, and the orbital angular momentum quantum number, correspondingly. The physical meaning of the radial quantum number n is discussed in [25]. w describes the width of the beam. Photons in these beams have angular momentum m.

These solutions describe the orbital angular momentum states or twisted light [26–29], and they are an important tool in modern quantum optical technologies. They are created experimentally by imposing $\exp(im\phi)$ phase structure on a laser beam. There is currently much work on the generation of orbital angular momentum states and their applications (e.g., [30–34]). They are robust in noisy environments (e.g., [35]), and therefore important for quantum communications.

In our context, they are important because they provide an experimental implementation of a quantum system with a finite dimensional Hilbert space. The whole formalism of this monograph can be used in the context of orbital angular momentum states. Mutually unbiased bases with orbital angular momentum states have been studied in [36, 37], and entanglement in [38]. Applications to quantum cryptography have been discussed in [39].

7.4 Other Applications

We discussed above applications in the area of quantum optics and quantum information. Applications in other areas include quantum maps [40–45], two-dimensional electron system in a uniform magnetic field and the magnetic translation group [46–50], and the quantum Hall effect [51, 52].

All these ideas are also used in the context of Signal Processing, where the dual variables position and momentum become time and frequency [54, 55]. For example, the factorization discussed in Sect. 4.9, is inspired by Ref. [56] on fast Fourier transforms, in the context of Signal Processing.

Work related to the formalism of finite quantum systems, in the context of Applied Mathematics is summarized in [57].

References

1. Vourdas, A. (1990). *Physical Review A*, *41*, 1653.
2. Schwinger, J. (1965). In L.C. Biedenharn, H. van Dam (Eds.) *Quantum Theory of Angular Momentum*. New York: Academic.
3. Vourdas, A. (1991). *Physical Review A*, *43*, 1564.
4. Arnold, V. I. (1966). *Annales- Institut Fourier*, *16*, 319.
5. Arakelyan, T., & Savvidy, G. K. (1988). *Physics Letters B*, *214*, 350.
6. Floratos, E., & Iliopoulos, J. (1988). *Physics Letters B*, *201*, 237.
7. Pope, C. N., & Stelle, K. (1989). *Physics Letters B*, *226*, 257.
8. de Witt, B., Hoppe, J., Nicolai, H. (1988). *Nuclear Physics*, B305 [FS23], 545 (1988)
9. Marquard, V., & Nicolai, H. (1990). *Communications in Mathematical Physics*, *128*, 39.
10. Dowker, J. S. (1990). *Classical and Quantum Gravity*, *7*, 1241.
11. Deprit, A. (1969). *Cel Mech*, *1*, 12.
12. Holland, M. J., & Burnett, K. (1993). *Physical Review Letters*, *71*, 1355.
13. Lane, A. S., Braunstein, S., & Caves, C. M. (1993). *Physical Review*, *47*, 1667.
14. Reck, M., Zeillinger, A., Bernstein, H. J., & Bertani, P. (1994). *Physical Review Letters*, *73*, 58.
15. Jex, I., Stenholm, S., & Zeillinger, A. (1995). *Optics Communication*, *117*, 95.
16. Torma, P., Stenholm, S., & Jex, I. (1995). *Physical Review A*, *52*, 4853.
17. Dunningham, J., & Burnett, K. (2000). *Physical Review*, *61*, 065601.
18. Dunningham, J., Burnett, K., & Burnett, S. M. (2002). *Physical Review Letters*, *89*, 150401.
19. Campos, R. A., Gerry, C., & Benmoussa, A. (2003). *Physical Review A*, *68*, 023810.
20. Vourdas, A., & Dunningham, J. (2005). *Physical Review A*, *71*, 013809.
21. Vourdas, A. (2005). *Physical Review A*, *71*, 043821.
22. Dunnigham, J., & Vourdas, A. (2006). *Journal of Physics B: Atomic, Molecular and Optical Physics*, *39*, 1579.
23. Zhang, S., Lei, C., Vourdas, A., & Dunnigham, J. (2006). *Journal of Physics B: Atomic, Molecular and Optical Physics*, *39*, 1625.
24. Ma, X., & Rhodes, W. (1990). *Physical Review A*, *41*, 4625.
25. Plick, W. N., & Krenn, M. (2015). *Physical Review A*, *92*, 063841.
26. Allen, L., Beijersbergen, M., Spreeuw, R., & Woerdman, J. (1992). *Physical Review A*, *45*, 8185.
27. Allen, L., Barnett, S. M., & Padgett, M. J. (Eds.). (2003). *Optical Angular Momentum*. Bristol: Institute of Physics.

28. Torres, J. P., & Torner, L. (Eds.). (2011). *Twisted photons: applications of light with orbital angular momentum*. Bristol: Wiley.
29. Andrews, D. L., & Babiker, M. (Eds.). (2012). *The angular momentum of light*. Cambridge: Cambridge University Press.
30. Mair, A., Vaziri, A., Weihs, G., & Zeillinger, A. (2001). *Nature*, *412*, 313.
31. Gibson, G., et al. (2004). *Optics Express*, *12*, 5448.
32. Marrucci, L., Manzo, C., & Paparo, D. (2006). *Physical Review Letters*, *96*, 163905.
33. Wang, J., et al. (2012). *Nature Photonics*, *6*, 488.
34. Bozinovic, N., et al. (2013). *Science*, *340*, 1545.
35. Krenn, M., et al. (2014). *New Journal of Physics*, *16*, 113028.
36. Giovannini, D., et al. (2013). *Physical Review Letters*, *110*, 143601.
37. D'Ambrosio, V., et al. (2013). *Science Reports*, *3*, 2726.
38. Jack, B., et al. (2010). *Physical Review A*, *81*, 043844.
39. Mirhosseini, M., et al. (2015). *New Journal of Physics*, *17*, 033033.
40. Berry, M. V. (1987). *Proceedings of the Royal Society*, *A473*, 183.
41. Balazs, N. L., & Voros, A. (1986). *Physics Reports*, *C143*, 109.
42. Leboeuf, P., & Voros, A. (1990). *Journal of Physics A*, *23*, 1765.
43. Leboeuf, P., Kurchan, J., Feingold, M., & Arovas, D. P. (1992). *Chaos*, *2*, 125.
44. Vivaldi, F. (1994). *Nonlinearity 5*, 133 (1992); Keating, J.P. *Journal of Physics*, *A27*, 6605.
45. Athanasiu, G. G., Floratos, E., & Nicolis, S. (1996). *Journal of Physics A*, *29*, 6737.
46. Brown, E. (1964). *Physical Review A*, *133*, 1038.
47. Zak, J. (1964). *Physical Review A*, *134*, 1602.
48. Zak, J. (1989). *Physical Review B*, *39*, 694.
49. Dubrovin, B. A., & Novikov, S. P. (1980). *Soviet Mathematics Doklady*, *22*, 240.
50. Novikov, S. P. (1980). *Soviet Mathematics Doklady*, *23*, 298.
51. Wen, X. G., & Niu, Q. (1990). *Physical Review B*, *41*, 9377.
52. Martinez, J., & Stone, M. (1993). *International Journal of Modern Physics B*, *7*, 4389.
53. Abarbanel, H., & Rouhi, A. (1994). *Physical Review E*, *48*, 3643.
54. Grochenig, K. (2001). *Foundations of time-frequency analysis*. Boston: Birkhauser.
55. Cohen, L. (1995). *Time-frequency analysis*. New Jersey: Prentice-Hall.
56. Good, I. J., & Trans, I. E. E. E. (1971). *Computers*, *C20*, 310.
57. Terras, A. (1999). *Fourier analysis on finite groups and applications*. Cambridge: Cambridge University Press.

Chapter 8
Galois Fields

Abstract Basic concepts from Galois theory, are presented. The material in this chapter is needed, for the study of finite quantum systems with variables in Galois fields, in Chap. 9.

In this chapter we review briefly some aspects of Galois theory which are needed later for the study of quantum systems with variables in Galois fields. The emphasis is on how to do practical calculations with Galois numbers. General references on Galois fields are [1–8].

8.1 The Galois Field $GF(p^e)$

The concept of field extension, enlarges $\mathbb{Z}(p)$ into the Galois field $GF(p^e)$, which is a field with characteristic the prime number p, and degree the integer e. In this section we state briefly some known results about Galois theory, and give some propositions which are useful in practical calculations. Some theorems in Galois theory are valid only for a prime $p \neq 2$, and this is the case considered here.

We consider the ring of polynomials $[\mathbb{Z}(p)](\varepsilon)$ with coefficients in the field $\mathbb{Z}(p)$. Let $\mathfrak{P}(\varepsilon)$ be an irreducible polynomial of degree e:

$$\mathfrak{P}(\varepsilon) \equiv c_0 + c_1\varepsilon + \cdots + c_{e-1}\varepsilon^{e-1} + \varepsilon^e; \qquad c_n \in \mathbb{Z}(p) \tag{8.1}$$

The $[\mathbb{Z}(p)](\varepsilon)/\mathfrak{P}(\varepsilon)$ has as elements polynomials in $[\mathbb{Z}(p)](\varepsilon)$ which are defined modulo $\mathfrak{P}(\varepsilon)$:

$$\alpha = \alpha_0 + \alpha_1\varepsilon + \cdots + \alpha_{e-1}\varepsilon^{e-1}; \qquad \alpha_n \in \mathbb{Z}(p) \tag{8.2}$$

The $[\mathbb{Z}(p)](\varepsilon)/\mathfrak{P}(\varepsilon)$ is a representation of the Galois field $GF(p^e)$. **Different irreducible polynomials $\mathfrak{P}(\varepsilon)$ of the same degree e, lead to isomorphic finite fields.**

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_8

Addition and multiplication of two Galois numbers is the standard addition and multiplication of polynomials, and the result is defined modulo the polynomial $\mathfrak{P}(\varepsilon)$. The Galois number α can be viewed as a vector $(\alpha_0, \alpha_1, ..., \alpha_{e-1})$ in $[\mathbb{Z}(p)]^e$, in the basis $\{1, \varepsilon, ..., \varepsilon^{e-1}\}$. Then addition of two Galois numbers is the standard addition of vectors in $[\mathbb{Z}(p)]^e$.

Lemma 8.1

$$(\alpha + \beta)^p = \alpha^p + \beta^p. \tag{8.3}$$

Proof Other terms in the expansion, like $p\alpha^{p-1}\beta$ are zero, in the modulo p arithmetic.

Example 8.1 In $GF(9)$ we consider the irreducible polynomial $\mathfrak{P}_1(\varepsilon) = \varepsilon^2 + \varepsilon + 2$. Let

$$\alpha = 1 + \varepsilon; \quad \beta = 2 + \varepsilon \tag{8.4}$$

Then

$$\begin{aligned} &\alpha + \beta = 2\varepsilon \\ &\alpha\beta = 2 + 3\varepsilon + \varepsilon^2 = -\varepsilon \end{aligned} \tag{8.5}$$

If instead of $\mathfrak{P}_1(\varepsilon)$ we consider the irreducible polynomial $\mathfrak{P}_2(\varepsilon) = \varepsilon^2 + 1$, then

$$\begin{aligned} &\alpha + \beta = 2\varepsilon \\ &\alpha\beta = 1 + 3\varepsilon + \varepsilon^2 = 0. \end{aligned} \tag{8.6}$$

It is seen that using different irreducible polynomials, leads to different results in specific calculations, but the overall results are isomorphic.

8.2 Subfields of $GF(p^e)$ and Galois Groups

The following proposition summarizes known results on subfields of $GF(p^e)$ and Galois groups.

Proposition 8.1 *(1) The elements of $GF(p^e)$ obey the relation*

$$\alpha^{p^e} = \alpha. \tag{8.7}$$

(2) The Frobenius transformation

$$\sigma(\alpha) = \alpha^p; \qquad \sigma^e = \mathbf{1} \tag{8.8}$$

defines an automorphism in $GF(p^e)$, and it leads to the Galois conjugates

$$\alpha \overset{\sigma}{\rightarrow} \alpha^p \overset{\sigma}{\rightarrow} \ldots \overset{\sigma}{\rightarrow} \alpha^{p^{e-1}} \overset{\sigma}{\rightarrow} \alpha. \tag{8.9}$$

Elements in the subfield $\mathbb{Z}(p)$ of $GF(p^e)$ are self-conjugates, because for $\alpha \in \mathbb{Z}(p)$ we get $\alpha^p = \alpha$ (Eq. (3.4)).

(3) The

$$\mathrm{Gal}(e|1) = \{\mathbf{1}, \sigma, ..., \sigma^{e-1}\} \cong \mathbb{Z}(e), \tag{8.10}$$

form a cyclic group of order e, which is called Galois group. It consists of the automorphisms of $GF(p^e)$ which leave the elements of the subfield $\mathbb{Z}(p)$ fixed.

(4) If $d|e$ the $GF(p^d)$ is a subfield of $GF(p^e)$ (we denote this as $GF(p^d) \prec GF(p^e)$). Elements of $GF(p^d)$ satisfy the relation

$$\alpha^{p^d} = \alpha; \quad \alpha \in GF(p^d). \tag{8.11}$$

The

$$\mathrm{Gal}(e|d) = \{\mathbf{1}, \sigma^d, ..., \sigma^{e-d}\} \cong \mathbb{Z}(e/d), \tag{8.12}$$

consists of the automorphisms of $GF(p^e)$ that leave the elements of the subfield $GF(p^d)$ fixed, and it is a cyclic group of order e/d. $\mathrm{Gal}(e|e) = \{1\}$. The $\mathrm{Gal}(e|d)$ is a subgroup of $\mathrm{Gal}(e|1)$ (and we denote this as $\mathrm{Gal}(e|d) \prec \mathrm{Gal}(e|1)$).

Proof For the proof we refer to the general literature on Galois fields.

We use the notation $\mathfrak{d}(e)$ for the set of all divisors of e.

Proposition 8.2 *(1) $GF(p^e)$ can be partitioned into 'Frobenius sets' $S_{d\kappa}$, each of which has elements that are Galois conjugates to each other. The cardinalities of these sets are divisors of e. To each of these sets corresponds an irreducible polynomial of degree $d|e$*

$$\begin{aligned} \mathfrak{P}_{d\kappa}(y) &= [y - \alpha_{d\kappa}(1)][y - \alpha_{d\kappa}(2)]...[y - \alpha_{d\kappa}(d)] \\ \alpha_{d\kappa}(\nu) &= [\alpha_{d\kappa}(1)]^{p^{\nu-1}}; \quad \nu = 1, ..., d \end{aligned} \tag{8.13}$$

that involves all Galois conjugates in the set. The index d indicates the degree of the polynomial. The index κ labels the various irreducible polynomials of the same degree d, and it takes the values $1, ..., n(d)$. The $n(d)$ is given by

$$n(d) = \frac{1}{d} \sum_{r \in \mathfrak{d}(d)} \mu(r) p^{d/r} \tag{8.14}$$

where $\mu(r)$ is the Möbius μ-function.

In the special case $d = 1$ the $\mathfrak{P}_{1\kappa}(y) = y - \kappa$, where $\kappa \in \mathbb{Z}(p)$.

(2) *The product of all distinct irreducible polynomials in $[\mathbb{Z}(p)](y)$ of degree d, for all $d|e$, is:*

$$\prod_{d\in\mathfrak{d}(e)}\left[\prod_{\kappa=1}^{n(d)}\mathfrak{P}_{d\kappa}(y)\right] = y^{p^e} - y \tag{8.15}$$

Proof For the proof we refer to the general literature on Galois fields.

Based on the above proposition, we partition $GF(p^e)$ as:

$$GF(p^e) = \bigcup_{d\in\mathfrak{d}(e)}\left[\bigcup_{\kappa=1}^{n(d)} S_{d\kappa}\right]; \quad S_{d\kappa} = \{\alpha_{d\kappa}(\nu)|\nu \in \mathbb{Z}(d)\}$$
$$\alpha_{d\kappa}(\nu) = [\alpha_{d\kappa}(1)]^{p^{\nu-1}} \tag{8.16}$$

The index ν labels the various Galois conjugates in the set. In the special case $d = 1$, $S_{1\kappa} = \{\kappa \in \mathbb{Z}(p)\}$.

The sets $S_{d\kappa}$ are invariant under Frobenius transformations. The partition depends on the choice of the irreducible polynomial $\mathfrak{P}(\varepsilon)$. There is a bijective map between the irreducible polynomials $\mathfrak{P}_{d\kappa}$ and the Frobenius sets $S_{d\kappa}$:

$$\mathfrak{P}_{d\kappa} \;\leftrightarrow\; S_{d\kappa}. \tag{8.17}$$

If $d|e$ then $\mathfrak{d}(d) \subseteq \mathfrak{d}(e)$ and

$$GF(p^d) = \bigcup_{g\in\mathfrak{d}(d)}\left[\bigcup_{\kappa=1}^{n(g)} S_{g\kappa}\right] \subseteq \bigcup_{g\in\mathfrak{d}(e)}\left[\bigcup_{\kappa=1}^{n(g)} S_{g\kappa}\right] = GF(p^e). \tag{8.18}$$

The following theorem is the fundamental theorem of Galois theory.

Theorem 8.1 *There is a bijective map between the fields $\mathbb{Z}(p) \prec GF(p^d) \prec GF(p^e)$ (where $d|e$), and the Galois groups* $\mathrm{Gal}(e|1) \succ \mathrm{Gal}(e|d) \succ \{1\}$*, with the Galois field $GF(p^d)$ corresponding to the Galois group* $\mathrm{Gal}(e|d)$*:*

$$\mathbb{Z}(p) \prec GF(p^d) \prec GF(p^e) \;\leftrightarrow\; \mathrm{Gal}(e|1) \succ \mathrm{Gal}(e|d) \succ \{1\}. \tag{8.19}$$

This map is inclusion reversing.

Proof The proof is given in the general literature on Galois fields.

Proposition 8.3 *The set $\mathscr{G}(p) = \{\mathbb{Z}(p), GF(p^2), GF(p^3), ...,\}$ with the subfield relation $\prec$, is a directed partially ordered set, isomorphic to the set of natural numbers $\mathbb{N} = \{1, 2, 3, ...\}$ with the partial order divisibility.*

Proof The following properties hold:

- $GF(p^e) \prec GF(p^e)$, for all e;
- if $GF(p^d) \prec GF(p^e)$ and $GF(p^e) \prec GF(p^d)$, then $GF(p^e) = GF(p^d)$;
- if $GF(p^{e_1}) \prec GF(p^{e_2})$ and $GF(p^{e_2}) \prec GF(p^{e_3})$, then $GF(p^{e_1}) \prec GF(p^{e_3})$;
- for any pair $GF(p^{e_1}), GF(p^{e_2})$ there exists e (e.g., the least common multiplier of e_1, e_2), such that $GF(p^{e_1}) \prec GF(p^e)$ and $GF(p^{e_2}) \prec GF(p^e)$.

Therefore $\mathscr{G}(p)$ is directed partially ordered set, and it is easily seen that it is isomorphic to the set of natural numbers $\mathbb{N}$, with the partial order divisibility.

Example 8.2 For $GF(9)$ the irreducible polynomials are

$$\begin{aligned} &\mathfrak{P}_{11}(y) = y; \quad \mathfrak{P}_{12}(y) = y - 1; \quad \mathfrak{P}_{13}(y) = y - 2 \\ &\mathfrak{P}_{21}(y) = y^2 + 1; \quad \mathfrak{P}_{22}(y) = y^2 + y + 2; \quad \mathfrak{P}_{23}(y) = y^2 + 2y + 2 \end{aligned} \tag{8.20}$$

We choose the irreducible polynomial $P(\varepsilon) = \varepsilon^2 + \varepsilon + 2$, and partition $GF(9)$ into the Frobenius sets:

$$\begin{aligned} &S_{11} = \{0\}; \quad S_{12} = \{1\}; \quad S_{13} = \{2\} \\ &S_{21} = \{1 + 2\varepsilon, 2 + \varepsilon\}; \quad S_{22} = \{\varepsilon, 2 + 2\varepsilon\}; \quad S_{23} = \{1 + \varepsilon, 2\varepsilon\}. \end{aligned} \tag{8.21}$$

If we choose the irreducible polynomial $P(\varepsilon) = \varepsilon^2 + 1$, then the partition of $GF(9)$ into Frobenius sets is:

$$\begin{aligned} &S_{11} = \{0\}; \quad S_{12} = \{1\}; \quad S_{13} = \{2\} \\ &S_{21} = \{\varepsilon, 2\varepsilon\}; \quad S_{22} = \{1 + \varepsilon, 1 + 2\varepsilon\}; \quad S_{23} = \{2 + \varepsilon, 2 + 2\varepsilon\}. \end{aligned} \tag{8.22}$$

8.3 Trace and Characters

The trace of $\alpha \in GF(p^e)$ is the sum of all its conjugates, and it is an element of $\mathbb{Z}(p)$:

$$\begin{aligned} &\mathrm{Tr}(\alpha) = \mathrm{Tr}_{e/1}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{e-1}} \\ &\mathrm{Tr}(\alpha) \in \mathbb{Z}(p); \quad \alpha \in GF(p^e) \end{aligned} \tag{8.23}$$

This is the trace with respect to the extension from $\mathbb{Z}(p)$ to $GF(p^e)$ and depending on the context we might use the notation $\mathrm{Tr}_{e/1}$ which shows this explicitly, or we might use the simpler notation Tr. All conjugates have the same trace.

The trace with respect to the extension from $GF(p^d)$ to $GF(p^e)$ (where $d|e$) is defined as:

$$\begin{aligned} &\mathrm{Tr}_{e/d}(\alpha) = \alpha + \alpha^{p^d} + \alpha^{p^{2d}} + ... + \alpha^{p^{e-d}} \\ &\mathrm{Tr}_{e/d}(\alpha) \in GF(p^d); \quad \alpha \in GF(p^e) \end{aligned} \tag{8.24}$$

For $d = 1$, this reduces to the trace in Eq. (8.23).

It can be shown that

$$\mathrm{Tr}_{e/1}(\alpha) = \mathrm{Tr}_{d/1}[\mathrm{Tr}_{e/d}(\alpha)]; \quad \alpha \in GF(p^e) \tag{8.25}$$

In the special case that α belongs to the subfield $GF(p^d)$ of $GF(p^e)$ (where $d|e$) Eq. (8.25) gives

$$\mathrm{Tr}(\alpha) = \frac{e}{d}\mathrm{Tr}_d(\alpha); \quad \alpha \in GF(p^d). \tag{8.26}$$

Lemma 8.2

(1)

$$\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta) \tag{8.27}$$

(2) If $\alpha \in \mathbb{Z}(p)$ and $\beta \in GF(p^e)$ then

$$\mathrm{Tr}(\alpha\beta) = \alpha\mathrm{Tr}(\beta). \tag{8.28}$$

(3)

$$\mathrm{Tr}(1) = e \ (\mathrm{mod}\ p) \tag{8.29}$$

Proof

(1) The proof of this is based on Eq. (8.3).
(2) This is proved using the fact that for $\alpha \in \mathbb{Z}(p)$, we get $\alpha^p = \alpha$ (Eq. (3.4)).
(3) Inserting $\alpha = 1$ into the definition of trace in Eq. (8.23), we find that $\mathrm{Tr}(1) = e$.

The following proposition provides a practical tool for the calculation of traces of Galois numbers, in terms of their components.

Proposition 8.4 *Let g, G be the following symmetric and invertible $e \times e$ matrices with elements in $\mathbb{Z}(p)$:*

$$g_{ij} \equiv \mathrm{Tr}\left(\varepsilon^{i+j}\right); \quad G = g^{-1}; \quad i, j = 0, ..., e-1. \tag{8.30}$$

Their elements depend on the choice of the irreducible polynomial $\mathfrak{P}(\varepsilon)$. *Also let* $\{E_0, E_1, ..., E_{e-1}\}$ *be a dual basis to* $\{1, \varepsilon, \varepsilon^2, ..., \varepsilon^{e-1}\}$, *defined as*

$$E_i = \sum_j G_{ij}\varepsilon^j \tag{8.31}$$

Then

(1)

$$\mathrm{Tr}(\varepsilon^i E_j) = \delta(i, j) \tag{8.32}$$

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

$$\alpha = \sum_{i=0}^{e-1} \alpha_i \varepsilon^i = \sum_{i=0}^{e-1} \overline{\alpha}_i E_i \tag{8.33}$$

where

$$\alpha_i = \mathrm{Tr}[\alpha E_i]; \qquad \overline{\alpha}_i = \mathrm{Tr}[\alpha \varepsilon^i] \tag{8.34}$$

and

$$\alpha_i = \sum_j G_{ij}\overline{\alpha}_j; \qquad \overline{\alpha}_i = \sum_j g_{ij}\alpha_j \tag{8.35}$$

We refer to α_i *and* $\overline{\alpha}_i$ *as components and dual components of* α, *correspondingly.*

(3) The trace of $\alpha\beta$ *is given by:*

$$\mathrm{Tr}(\alpha\beta) = \sum_{i,j} g_{ij}\alpha_i\beta_j = \sum_{i,j} G_{ij}\overline{\alpha}_i\overline{\beta}_j = \sum_i \alpha_i\overline{\beta}_i = \sum_i \overline{\alpha}_i\beta_i \tag{8.36}$$

Proof

(1) This is proved using the fact that $Gg = \mathbf{1}$
(2) Here we express a vector in two bases which are dual to each other in the sense that they obey Eq. (8.32). The relations in Eqs. (8.33),(8.34),(8.35), are standard for such expansions.
(3) Using Eq. (8.28), we prove that

$$\mathrm{Tr}(E_i E_j) = G_{ij}. \tag{8.37}$$

Using these two relations, we easily prove Eq. (8.36).

The following proposition provides a practical tool for the calculation of conjugates of Galois numbers, in terms of their components.

Proposition 8.5 *Let $\mathscr{C}$ be the $e \times e$ matrix with elements in $\mathbb{Z}(p)$, defined through the relations:*

$$\varepsilon^{kp} = \sum_{j=0}^{e-1} \varepsilon^j \mathscr{C}_{jk}; \quad j,k = 0,...,e-1. \tag{8.38}$$

Its elements depend on the choice of the irreducible polynomial $\mathfrak{P}(\varepsilon)$. Then

(1)

$$\mathscr{C}^e = \mathbf{1}; \qquad \mathscr{C}_{i0} = \delta(i,0) \tag{8.39}$$

(2) If $\alpha = \sum \alpha_k \varepsilon^k$, its conjugates are given by

$$\alpha^{p^i} = \sum_{j,k} \varepsilon^j (\mathscr{C}^i)_{jk} \alpha_k \tag{8.40}$$

Proof (1) We first point out that

$$\varepsilon^{kp^2} = \left(\sum_j \varepsilon^j \mathscr{C}_{jk} \right)^p = \sum_j \varepsilon^{jp} \mathscr{C}_{jk} = \sum_{j,\ell} \varepsilon^\ell \mathscr{C}_{\ell j} \mathscr{C}_{jk} = \sum_\ell \varepsilon^\ell (\mathscr{C}^2)_{\ell k}. \tag{8.41}$$

Inductively, we then prove that

$$\varepsilon^{kp^i} = \sum_\ell \varepsilon^\ell (\mathscr{C}^i)_{\ell k}. \tag{8.42}$$

For $i = e$, we have $\varepsilon^{kp^e} = \varepsilon^k$, and this shows that $\mathscr{C}^e = \mathbf{1}$. We note that this is basically the result $\sigma^e = \mathbf{1}$, written in the language of matrices.
If we put $k = 0$ into Eq. (8.38), we find that $\mathscr{C}_{j0} = \delta(j,0)$.

(2) Using Eq. (8.42), we get

$$\alpha^{p^i} = \left(\sum_k \alpha_k \varepsilon^k \right)^{p^i} = \sum_k (\alpha_k \varepsilon^k)^{p^i} = \sum_k \alpha_k \varepsilon^{kp^i} = \sum_{j,k} \varepsilon^j (\mathscr{C}^i)_{jk} \alpha_k \tag{8.43}$$

The matrices g, G can be generalized into the following symmetric tensors

$$\begin{aligned} g^{(N)}_{i_1 \ldots i_N} &\equiv \mathrm{Tr}\left[\varepsilon^{i_1 + \ldots + i_N}\right]; \quad i_k = 0,...,e-1 \\ G^{(N)}_{i_1 \ldots i_N} &\equiv \mathrm{Tr}\left[E_{i_1} \ldots E_{i_N}\right] = \sum G_{i_1 j_1} \ldots G_{i_N j_N} g^{(N)}_{i_1 \ldots j_N}, \end{aligned} \tag{8.44}$$

which take values in $\mathbb{Z}(p)$. For simplicity, we omit the superfix in the notation, when $N = 2$. Then the trace of a product of N elements of $GF(p^e)$ can be written as

$$\mathrm{Tr}\left[\alpha^{(1)}...\alpha^{(N)}\right] = \sum g^{(N)}_{i_1...i_N}\alpha^{(1)}_{i_1}...\alpha^{(N)}_{i_N} = \sum G^{(N)}_{i_1...i_N}\overline{\alpha}^{(1)}_{i_1}...\overline{\alpha}^{(N)}_{i_N}. \tag{8.45}$$

We note relations like $g^{(3)}_{ijk} = g_{i,j+k} = g_{i+j+k,0}$, etc.

Example 8.3 We consider the Galois field $GF(9)$ and choose the irreducible polynomial $\mathfrak{P}_1(\varepsilon) = \varepsilon^2 + \varepsilon + 2$. The matrices g, G and $\mathscr{C}$ are in this case

$$g = \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}; \quad G = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}; \quad \mathscr{C} = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \tag{8.46}$$

For $\alpha = 1 + \varepsilon$ and $\beta = 2 + \varepsilon$ we get $\mathrm{Tr}(\alpha\beta) = -2$.

We also choose the irreducible polynomial $\mathfrak{P}_2(\varepsilon) = \varepsilon^2 + 1$. In this case

$$g = G = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \quad \mathscr{C} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{8.47}$$

For $\alpha = 1 + \varepsilon$ and $\beta = 2 + \varepsilon$ we get $\mathrm{Tr}(\alpha\beta) = 0$.

Additive characters in $GF(p^e)$ are defined as

$$\begin{aligned} &\chi(\alpha) = \omega[\mathrm{Tr}(\alpha)]; \quad \alpha \in GF(p^e) \\ &\omega(r) = \exp\left(i\frac{2\pi r}{p}\right); \quad [\chi(\alpha)]^p = 1; \quad r \in \mathbb{Z}(p). \end{aligned} \tag{8.48}$$

All conjugates have the same character. From Eq. (8.36), it is seen that

$$\begin{aligned} \chi(\alpha\beta) = \omega[\mathrm{Tr}(\alpha\beta)] &= \omega\left[\sum_{i,j} g_{ij}\alpha_i\beta_j\right] = \omega\left[\sum_{i,j} G_{ij}\overline{\alpha}_i\overline{\beta}_j\right] \\ &= \omega\left[\sum_i \overline{\alpha}_i\beta_i\right] = \omega\left[\sum_i \alpha_i\overline{\beta}_i\right] \end{aligned} \tag{8.49}$$

The following relation is a generalization of Eq. (3.3):

$$\frac{1}{p^e}\sum_{\alpha\in GF(p^e)} \chi(\alpha\beta) = \delta(\beta, 0) \tag{8.50}$$

The quadratic Gauss sum (given in Eq. (3.5)), is in the present context:

$$G[s; GF(p^e)] = \sum_{k\in GF(p^e)} \chi(sk^2). \tag{8.51}$$

The Pontryagin dual group to $GF(p^e)$, i.e., the group of its characters, is isomorphic to $GF(p^e)$:

$$\widetilde{GF(p^e)} \cong GF(p^e). \tag{8.52}$$

Remark 8.1 The $Sp[2, GF(p^e)]$ group is very similar to the $Sp[2, \mathbb{Z}(p)]$ group. It consists of 2×2 matrices as in Eq. (3.34), with elements in $GF(p^e)$. We note that in the present case:

- The cardinality of the $Sp[2, GF(p^e)]$ is

$$|Sp[2, GF(p^e)]| = p^e \left(p^{2e} - 1\right). \tag{8.53}$$

- The finite geometry $GF(p^e) \times GF(p^e)$ is near-linear (i.e., two lines have at most one point in common).

8.4 General Bases in $GF(p^e)$

Let $\mathscr{U}$ be an invertible $e \times e$ matrix, with elements in $\mathbb{Z}(p)$. Such matrices form the $GL[e, \mathbb{Z}(p)]$ group. We consider the following transformations of the basis $\{\varepsilon^i\}$ and its dual basis $\{E_i\}$, in $GF(p^e)$ [7]:

$$\mathscr{E}_j = \sum_i \varepsilon^i (\mathscr{U}^{-1})_{ij}; \quad \overline{\mathscr{E}}_j = \sum_i \mathscr{U}_{ji} E_i; \quad \mathrm{Tr}(\overline{\mathscr{E}}_j \mathscr{E}_i) = \delta(j, i). \tag{8.54}$$

The arbitrary element $\alpha \in GF(p^e)$ in Eq. (8.33), can be written in the new basis, as

$$\alpha = \sum_i A_i \mathscr{E}_i = \sum_i \overline{A}_i \overline{\mathscr{E}}_i; \quad A_i = \sum_j \mathscr{U}_{ij} \alpha_j; \quad \overline{A}_i = \sum_j \overline{\alpha}_j (\mathscr{U}^{-1})_{ji} \tag{8.55}$$

With respect to the transformed bases, we introduce the symmetric $e \times e$ matrices $g_{\mathscr{U}}$ and $G_{\mathscr{U}}$, with elements in $\mathbb{Z}(p)$:

$$\begin{aligned} (g_{\mathscr{U}})_{ij} &= \mathrm{Tr}(\mathscr{E}_i \mathscr{E}_j) = (\mathscr{U}^{-1})^T g \mathscr{U}^{-1} \\ (G_{\mathscr{U}})_{ij} &= \mathrm{Tr}(\overline{\mathscr{E}}_i \overline{\mathscr{E}}_j) = \mathscr{U} G \mathscr{U}^T. \end{aligned} \tag{8.56}$$

Here $\mathscr{U}^T$ is the transpose matrix of $\mathscr{U}$.

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

$$\mathrm{Tr}(\alpha\beta) = \sum_{i,j} (g_{\mathscr{U}})_{ij} A_i B_j = \sum_{i,j} (G_{\mathscr{U}})_{ij} \overline{A}_i \overline{B}_j = \sum_i A_i \overline{B}_i = \sum_i \overline{A}_i B_i. \tag{8.57}$$

It is known (p.385 in Ref. [9]) that in fields with characteristic $p \neq 2$ (which is the case considered here), every symmetric matrix is congruent to a diagonal matrix. Therefore with appropriate $\mathscr{U}$, the g can be transformed to a diagonal matrix (which is not unique):

$$\mathfrak{g} = \mathrm{diag}(\mathfrak{g}_0, ..., \mathfrak{g}_{e-1}); \quad \mathfrak{G} = \mathrm{diag}(\mathfrak{g}_0^{-1}, ..., \mathfrak{g}_{e-1}^{-1}); \quad \mathfrak{g}_i \neq 0. \tag{8.58}$$

In this basis $\mathrm{Tr}(\alpha\beta) = \sum \mathfrak{g}_i \alpha_i \beta_i$.

It is also known [10–12] that g can be transformed into $\mathbf{1}$ if and only if e is an odd integer. In this case the basis is self-dual and $\mathrm{Tr}(\alpha\beta) = \sum \alpha_i \beta_i$.

References

1. Liddl, R., & Niederreiter, H. (1986). *Introduction to finite fields and their applications*. Cambridge: Cambridge University Press.
2. Artin, E. (1998). *Galois theory* Dover, New York.
3. Edwards, H.M. (1997). *Galois theory* New York: Springer.
4. Postnikov, M. M. (2004). *Foundations of Galois theory*. New York: Dover.
5. Howie, J. M. (2010). *Fields and Galois theory*. New York: Springer.
6. Weintraub, S. H. (2016). *Galois theory*. New York: Springer.
7. Wan, Z. X. (2003). *Lectures on finite fields and Galois rings*. Singapore: World Scientific.
8. Piatetski-Shapiro, I. (1983). *Complex representations of GL(2, K) for finite fields K*. Rhode Island: American Mathematical Society.
9. MacLane, S., & Birkhoff, G. (1967). *Algebra*. New York: MacMillan.
10. Seroussi, G., & Lempel, A. (1980). *SIAM Journal on Computing*, *9*, 758.
11. Lempel, A., & Weinberger, M. (1988). *SIAM Journal on Discrete Mathematics*, *1*, 193.
12. Lempel, A., & Seroussi, G., (1991). *I.E.E.E. Transactions on Information Theory*, *37*, 1220.

Chapter 9
Quantum Systems with Variables in $GF(p^e)$

Abstract Finite quantum systems with variables in Galois fields, are discussed. The emphasis is on 'Galois properties', which are not present in general finite quantum systems.

Quantum systems with variables in the Galois field $GF(p^e)$, have been studied both as a subject in its own right [1–6], and also in connection with mutually unbiased bases [7–21]. Related is also work on finite Fourier transforms over Galois fields in the context of Signal Processing and classical coding [22–27].

We consider a quantum system with variables in $GF(p^e)$, where p is a prime number ($p \neq 2$). We call it Galois quantum system, and denote it as $\Sigma[GF(p^e)]$. For comparison, we also consider an e-partite system where each component is a quantum system with variables in $\mathbb{Z}(p)$. In this system the variables take values in $\mathbb{Z}(p) \times \cdots \times \mathbb{Z}(p) = [\mathbb{Z}(p)]^e$, and we denote it as $\Sigma\{[\mathbb{Z}(p)]^e\}$.

The elements of $GF(p^e)$ are vectors in $[\mathbb{Z}(p)]^e$ with regard to addition, but they also have the 'Galois structure' related to multiplication, which includes Galois conjugates and trace, Frobenius transformations, etc. Consequently, the $\Sigma[GF(p^e)]$ has a lot of extra structure than the $\Sigma\{[\mathbb{Z}(p)]^e\}$, and we discuss below the differences between $\Sigma[GF(p^e)]$ and $\Sigma\{[\mathbb{Z}(p)]^e\}$.

Some of the formulas in this chapter are analogous to those in Chap. 7, with the characters $\omega(\alpha)$ replaced by the characters $\chi(\alpha)$. We present them briefly, and for the proof we refer the reader to the analogous proof in the Chap. 7. In this way the overlap between the present chapter and Chap. 7, is minimal. But we emphasize additional properties like those related to Frobenius transformations, which are a central part of Galois theory, and which were absent in finite quantum systems with variables in $\mathbb{Z}(d)$. For simplicity, and in order to emphasize the analogy, we use in this chapter the same notation for displacement operators and symplectic transformations, as in Chap. 7.

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_9

In the present chapter we use the notation

$$\omega(r) = \exp\left(i\frac{2\pi r}{p}\right); \quad r \in \mathbb{Z}(p)$$
$$\Omega(s) = \exp\left(i\frac{2\pi s}{e}\right); \quad s \in \mathbb{Z}(e) \tag{9.1}$$

9.1 Fourier Transforms in $\Sigma[GF(p^e)]$

The Hilbert space for the system $\Sigma[GF(p^e)]$ is the p^e-dimensional space $H[GF(p^e)]$, of complex wavefunctions $f(m)$, where $m \in GF(p^e)$. A basis in this Hilbert space consists of the position states $|X; m\rangle$ where $m \in GF(p^e)$ (the X in the notation indicates the position basis).

The Fourier transform in $H[GF(p^e)]$ is given in terms of the characters defined in Eq. (8.48) as

$$F = \frac{1}{\sqrt{p^e}} \sum_{m,n \in GF(p^e)} \chi(mn)|X; m\rangle\langle X; n|; \quad F^4 = \mathbf{1}. \tag{9.2}$$

Momentum states are defined as

$$|P; m\rangle = F|X; m\rangle = \frac{1}{\sqrt{p^e}} \sum_{n \in GF(p^e)} \chi(mn)|X; n\rangle. \tag{9.3}$$

If $m = \sum m_i \varepsilon^i$, the bijective map

$$m \quad \leftrightarrow \quad (m_0, ..., m_{e-1}), \tag{9.4}$$

implies that there is a bijective map

$$H[GF(p^e)] \quad \leftrightarrow \quad H[\mathbb{Z}(p)] \otimes \cdots \otimes H[\mathbb{Z}(p)] \tag{9.5}$$

where

$$|X; m_0 + m_1\varepsilon + \cdots + m_{e-1}\varepsilon^{e-1}\rangle \quad \rightarrow \quad |X; m_0\rangle \otimes \cdots \otimes |X; m_{e-1}\rangle. \tag{9.6}$$

We stress that this depends on the chosen basis $\{\varepsilon^i\}$ for $GF(p^e)$, and later (in Eq. (9.17)), we discuss how to change the basis.

Using Eq. (8.49), we express the Fourier transform as

$$F = \frac{1}{\sqrt{p^e}} \sum \omega\left[\sum g_{ij} m_i n_j\right] |X; m_0\rangle\langle X; n_0| \otimes \cdots \otimes |X; m_{e-1}\rangle\langle X; n_{e-1}| \tag{9.7}$$

The momentum states can now be written as:

$$|P; m_0 + m_1\varepsilon + \cdots + m_{e-1}\varepsilon^{e-1}\rangle \quad \rightarrow \quad |P; \overline{m}_0\rangle \otimes \cdots \otimes |P; \overline{m}_{e-1}\rangle. \tag{9.8}$$

We note that the components of m, and the dual components of m (defined in Proposition 8.4), appear in the right hand side of Eqs. (9.6), (9.8), correspondingly.

Example 9.1 As a numerical example, we consider a Galois quantum system which has positions and momenta in $GF(9)$. We choose the irreducible polynomial $P(\varepsilon) = \varepsilon^2 + \varepsilon + 2$, and we will calculate the Fourier transform as a 9×9 matrix with the following order for its elements:

$$(0, 1, 2, \varepsilon, 1 + \varepsilon, 2 + \varepsilon, 2\varepsilon, 1 + 2\varepsilon, 2 + 2\varepsilon). \tag{9.9}$$

We need to calculate the $\mathrm{Tr}(mn)$ for all $m, n \in GF(9)$. If

$$m = m_0 + m_1\varepsilon; \quad n = n_0 + n_1\varepsilon; \quad m_0, m_1, n_0, n_1 \in \mathbb{Z}(3), \tag{9.10}$$

then using the g matrix in Eq. (8.46), we find that

$$\mathrm{Tr}(mn) = \sum_{i,j} m_i g_{ij} n_j = -m_0 n_0 - m_0 n_1 - m_1 n_0. \tag{9.11}$$

Therefore

$$F = \frac{1}{3}\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & a^* & a & a^* & a & 1 & a & 1 & a^* \\
1 & a & a^* & a & a^* & 1 & a^* & 1 & a \\
1 & a^* & a & 1 & a^* & a & 1 & a^* & a \\
1 & a & a^* & a^* & 1 & a & a & a^* & 1 \\
1 & 1 & 1 & a & a & a & a^* & a^* & a^* \\
1 & a & a^* & 1 & a & a^* & 1 & a & a^* \\
1 & 1 & 1 & a^* & a^* & a^* & a & a & a \\
1 & a^* & a & a & 1 & a^* & a^* & a & 1
\end{pmatrix} \tag{9.12}$$

where

$$a = \exp\left(i\frac{2\pi}{3}\right). \tag{9.13}$$

9.1.1 Change of the Basis in $GF(p^e)$

In Sect. 8.4, we have studied the change of basis in $GF(p^e)$, and here we study the implications of this for Galois quantum systems [6]. We replace the basis $\{\varepsilon^i\}$ with the basis $\mathscr{E}_j$ in Eq. (8.54), and let

$$m = \sum m_i \varepsilon^i = \sum M_i \mathscr{E}_i; \quad M_i = \sum_j \mathscr{U}_{ij} m_j. \tag{9.14}$$

$\mathscr{U}$ is an element of the $GL[e, \mathbb{Z}(p)]$ group, as discussed in Sect. 8.4. We also consider the unitary transformations

$$B(\mathscr{U}) = \sum_{m_i} |X; M_0\rangle\langle X; m_0| \otimes \cdots \otimes |X; M_{e-1}\rangle\langle X; m_{e-1}|, \tag{9.15}$$

which form a unitary representation of the $GL[e, \mathbb{Z}(p)]$ group:

$$B(\mathscr{U}_1)B(\mathscr{U}_2) = B(\mathscr{U}_1\mathscr{U}_2); \quad B(\mathbf{1}) = \mathbf{1}. \tag{9.16}$$

Then

$$|X; M_0\rangle \otimes \cdots \otimes |X; M_{e-1}\rangle = B(\mathscr{U})\left[|X; m_0\rangle \otimes \cdots \otimes |X; m_{e-1}\rangle\right]. \tag{9.17}$$

Acting with $B(\mathscr{U})$ on both sides of the Fourier transform in Eq. (9.7), we get the Fourier transform in the basis $\mathscr{E}_j$:

$$B(\mathscr{U})F[B(\mathscr{U})]^T = \frac{1}{\sqrt{p^e}} \sum \omega\left[\sum (g_{\mathscr{U}})_{ij} M_i N_j\right] \times |X; M_0\rangle\langle X; N_0| \otimes \cdots \otimes |X; M_{e-1}\rangle\langle X; N_{e-1}|. \tag{9.18}$$

The $g_{\mathscr{U}}$ is given in Eq. (8.56).

9.1.2 Comparison of the System $\Sigma[GF(p^e)]$ with the System $\Sigma\{[\mathbb{Z}(p)]^e\}$

The Hilbert space of the system $\Sigma\{[\mathbb{Z}(p)]^e\}$ is the p^e-dimensional space

$$H\{[\mathbb{Z}(p)]^e\} = H[\mathbb{Z}(p)] \otimes \cdots \otimes H[\mathbb{Z}(p)], \tag{9.19}$$

of complex wavefunctions $f(m_0, ..., m_{e-1})$, where $(m_0, ..., m_{e-1}) \in [\mathbb{Z}(p)]^e$. We consider the basis of position states $|X; m_0\rangle \otimes \cdots \otimes |X; m_{e-1}\rangle$. The Fourier transform in $H\{[\mathbb{Z}(p)]^e\}$ is given by

$$\mathscr{F} = \bigotimes_{i=1}^{e} \left[\frac{1}{\sqrt{p}} \sum \omega \left(\sum_{m_i, n_i} m_i n_i \right) |X; m_i\rangle\langle X; n_i| \right]; \quad \mathscr{F}^4 = \mathbf{1}. \tag{9.20}$$

Momentum states are defined as

$$\mathscr{F}|X; m_0\rangle \otimes \cdots \otimes |X; m_{e-1}\rangle = |P; m_0\rangle \otimes \cdots \otimes |P; m_{e-1}\rangle \tag{9.21}$$

The Fourier transform is different in the systems $\Sigma[GF(p^e)]$ and $\Sigma\{[\mathbb{Z}(p)]^e\}$, and consequently the dual state (in the Fourier transform sense) to $|X; m_0\rangle \otimes \cdots \otimes |X; m_{e-1}\rangle$ is $|P; \overline{m}_0\rangle \otimes \cdots \otimes |P; \overline{m}_{e-1}\rangle$ in the former case, and $|P; m_0\rangle \otimes \cdots \otimes |P; m_{e-1}\rangle$ in the latter case. This difference propagates into other parts of the formalism, which we do not discuss explicitly (see also Remark 9.1).

9.2 Frobenius Transformations

Frobenius transformations and the Galois group play a central role in Galois theory. Here we study them in the context of Galois quantum systems [4].

The space $H[GF(p^e)]$ can be written as the direct sum of 'Frobenius subspaces':

$$\begin{aligned} H[GF(p^e)] &= \bigoplus_{d \in \mathfrak{d}(e)} \left[\bigoplus_{\kappa=1}^{n(d)} H_{d\kappa} \right] \\ H_{d\kappa} &= \text{span}\{|X; m_{d\kappa}(1)\rangle, |X; m_{d\kappa}(2)\rangle, ..., |X; m_{d\kappa}(d)\rangle\} \end{aligned} \tag{9.22}$$

The space $H_{d\kappa}$ is spanned by all position states labelled with Galois conjugate numbers in the set $S_{d\kappa}$ in Eq. (8.16). d takes values in the set $\mathfrak{d}(e)$ of divisors of e. The bijective map in Eq. (8.17) between the irreducible polynomials and the Frobenius sets of Galois conjugates, is here extended to include the Frobenius subspaces:

$$\mathfrak{P}_{d\kappa} \;\leftrightarrow\; S_{d\kappa} \;\leftrightarrow\; H_{d\kappa}. \tag{9.23}$$

In the special case $d = 1$, the $H_{1\kappa}$ is the one-dimensional space

$$H_{1\kappa} = \{|X; \kappa\rangle\}; \quad \kappa \in \mathbb{Z}(p). \tag{9.24}$$

If $d|e$ then $\mathfrak{d}(d) \subseteq \mathfrak{d}(e)$ and the system $\Sigma[GF(p^d)]$ is a subsystem of $\Sigma[GF(p^e)]$. In this case $H[GF(p^d)]$ is a subspace of $H[GF(p^e)]$:

$$H[GF(p^d)] = \bigoplus_{g \in \mathfrak{d}(d)} \left[\bigoplus_{\kappa=1}^{n(g)} H_{g\kappa} \right] \prec \bigoplus_{g \in \mathfrak{d}(e)} \left[\bigoplus_{\kappa=1}^{n(g)} H_{g\kappa} \right] = H[GF(p^e)] \tag{9.25}$$

This is analogous to Eq. (8.18). The $\prec$ denotes here subspace.

We denote as $\Pi_{d\kappa}$ the projector to $H_{d\kappa}$, and as $\Pi[GF(p^d)]$ the projector to $H[GF(p^d)]$. Then for $d|e$,

$$\Pi[GF(p^d)] = \sum_{g\in\mathfrak{d}(d)} \left[\sum_{\kappa=1}^{n(g)} \Pi_{g\kappa}\right]$$
$$\Pi[GF(p^d)]\Pi[GF(p^e)] = \Pi[GF(p^d)] \tag{9.26}$$

Example 9.2 We consider a Galois quantum system where position and momentum take values in $GF(9)$. Taking into account example 8.2, we find that if we choose the irreducible polynomial $\mathfrak{P}(\varepsilon) = \varepsilon^2 + \varepsilon + 2$, the Frobenius subspaces are

$$\begin{aligned} H_{11} &= \{|X;0\rangle\} \\ H_{12} &= \{|X;1\rangle\} \\ H_{13} &= \{|X;2\rangle\} \\ H_{21} &= \text{span}\{|X;1+2\varepsilon\rangle, |X;2+\varepsilon\rangle\} \\ H_{22} &= \text{span}\{|X;\varepsilon\rangle, |X;2+2\varepsilon\rangle\} \\ H_{23} &= \text{span}\{|X;1+\varepsilon\rangle, |X;2\varepsilon\rangle\}. \end{aligned} \tag{9.27}$$

In this case

$$\begin{aligned} H[\mathbb{Z}(3)] &= H_{11} \oplus H_{12} \oplus H_{13} = \text{span}\{|X;0\rangle, |X;1\rangle, |X;2\rangle\} \\ H[GF(9)] &= H_{11} \oplus H_{12} \oplus H_{13} \oplus H_{21} \oplus H_{22} \oplus H_{23}. \end{aligned} \tag{9.28}$$

If we choose the irreducible polynomial $\mathfrak{P}(\varepsilon) = \varepsilon^2 + 1$, the Frobenius subspaces are

$$\begin{aligned} H_{11} &= \{|X;0\rangle\} \\ H_{12} &= \{|X;1\rangle\} \\ H_{13} &= \{|X;2\rangle\} \\ H_{21} &= \text{span}\{|X;\varepsilon\rangle, |X;2\varepsilon\rangle\} \\ H_{22} &= \text{span}\{|X;1+\varepsilon\rangle, |X;1+2\varepsilon\rangle\} \\ H_{23} &= \text{span}\{|X;2+\varepsilon\rangle, |X;2+2\varepsilon\rangle\}. \end{aligned} \tag{9.29}$$

Definition 9.1 The Frobenius transformations are the unitary transformations:

$$\mathscr{G} = \sum_{d\in\mathfrak{d}(e)} \sum_{\kappa=1}^{n(d)} \sum_{\nu\in\mathbb{Z}(d)} |X; m_{d\kappa}(\nu+1)\rangle\langle X; m_{d\kappa}(\nu)| \tag{9.30}$$

Proposition 9.1 *Let $d|e$. Then [4]:*

(1)

$$\mathscr{G}^e = \mathbf{1} \tag{9.31}$$

and the

$$\mathrm{Gal}(e|1) = \{\mathbf{1}, \mathscr{G}, ..., \mathscr{G}^{e-1}\} \cong \mathbb{Z}(e), \tag{9.32}$$

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

(2) Acting with $\mathscr{G}^j$ where $j \in \mathbb{Z}(e)$ on position and momentum states we get

$$\mathscr{G}^j|X; m\rangle = |X; m^{p^j}\rangle; \qquad \mathscr{G}^j|P; m\rangle = |P; m^{p^j}\rangle \tag{9.33}$$

(3) The Frobenius transform commutes with the Fourier transform:

$$[F, \mathscr{G}] = 0. \tag{9.34}$$

(4) The Frobenius transform commutes with the projection operators $\Pi_{d\kappa}$, and with the $\Pi[GF(p^d)]$:

$$[\mathscr{G}, \Pi_{d\kappa}] = \left[\mathscr{G}, \Pi[GF(p^d)]\right] = 0. \tag{9.35}$$

Consequently the spaces $H_{d\kappa}$ are invariant under Frobenius transforms.

(5) The Frobenius transformation $\mathscr{G}^d$ leaves all the vectors in $H[GF(p^d)]$ fixed:

$$\mathscr{G}^d|X; \kappa\rangle = |X; \kappa\rangle; \quad \kappa \in GF(p^d). \tag{9.36}$$

The Galois group

$$\mathrm{Gal}(e/d) = \{\mathbf{1}, \mathscr{G}^d, ..., \mathscr{G}^{e-d}\} \cong \mathbb{Z}(e/d), \tag{9.37}$$

is a cyclic group of order e/d, and it is a subgroup of $\mathrm{Gal}(e/1)$.

(6) $\mathscr{G}$ can be written in terms of its eigenvalues and eigenprojectors as:

$$\mathscr{G} = \varpi(0) + \Omega(1)\varpi(1) + \cdots + \Omega(e-1)\varpi(e-1) \tag{9.38}$$

$\Omega(s)$ has been defined in Eq. (9.1). $\varpi(r)$ are orthogonal projectors, which can be written in terms of $\mathscr{G}$ as

$$\varpi(r) = \frac{1}{e}\left[\mathbf{1} + \Omega(-r)\mathscr{G} + \Omega(-2r)\mathscr{G}^2 + \cdots + \Omega[-r(e-1)]\mathscr{G}^{e-1}\right]. \tag{9.39}$$

(7) $\mathscr{G}^d$ can be written in terms of its eigenprojectors as:

$$\mathscr{G}^d = \mathfrak{P}(0) + \Omega\left(\frac{e}{d}\right)\mathfrak{P}(1) + \cdots + \Omega\left[(d-1)\frac{e}{d}\right]\mathfrak{P}(d-1) \tag{9.40}$$

$\mathfrak{P}(r)$ are orthogonal projectors to its eigenspaces, given by:

$$\mathfrak{P}(r) = \varpi(r) + \varpi\left(r + \frac{e}{d}\right) + \cdots + \varpi\left[r + (d-1)\frac{e}{d}\right] \tag{9.41}$$

Proof (1) Using the fact that $m^{p^e} = m$ for all $m \in GF(p^e)$, we prove that $\mathscr{G}^e = \mathbf{1}$. Therefore the $\{\mathbf{1}, \mathscr{G}, ..., \mathscr{G}^{e-1}\}$ form a cyclic group of order e.

(2) From Eq. (8.13) it follows that $m_{d\kappa}(\nu + 1) = [m_{d\kappa}(\nu)]^p$. Therefore $\mathscr{G}|X; m\rangle = |X; m^p\rangle$ and from this follows that $\mathscr{G}^j|X; m\rangle = |X; m^{p^j}\rangle$.
For the momentum states, we get

$$\begin{aligned}\mathscr{G}^j|P; m\rangle &= \frac{1}{\sqrt{p^e}} \sum_{n \in GF(p^e)} \chi(mn)\mathscr{G}^j|X; n\rangle \\ &= \frac{1}{\sqrt{p^e}} \sum_{n \in GF(p^e)} \chi(mn)|X; n^{p^j}\rangle.\end{aligned} \tag{9.42}$$

We substitute $n = k^{p^{e-j}}$ and we get

$$\mathscr{G}^j|P; m\rangle = \frac{1}{\sqrt{p^e}} \sum_{k \in GF(p^e)} \chi\left(mk^{p^{e-j}}\right)|X; k\rangle. \tag{9.43}$$

All conjugates have the same trace, and therefore

$$\chi\left(mk^{p^{e-j}}\right) = \chi\left(m^{p^e}k\right). \tag{9.44}$$

Consequently

$$\mathscr{G}^j|P; m\rangle = \frac{1}{\sqrt{p^e}} \sum_{k \in GF(p^e)} \chi\left(m^{p^e}k\right)|X; k\rangle = |P; m^{p^j}\rangle. \tag{9.45}$$

(3) The Fourier operator can be written as

$$F = \sum_m |P; m\rangle\langle X; m|, \tag{9.46}$$

and therefore

$$\mathscr{G}F\mathscr{G}^\dagger = \sum_m \mathscr{G}|P; m\rangle\langle X; m|\mathscr{G}^\dagger = \sum_m |P; m^p\rangle\langle X; m^p| = F. \tag{9.47}$$

Therefore $[F, \mathscr{G}] = 0$.

(4)

$$\Pi_{d\kappa} = \sum_{\nu \in \mathbb{Z}(d)} |X; m_{d\kappa}(\nu)\rangle\langle X; m_{d\kappa}(\nu)|, \tag{9.48}$$

and therefore

$$\begin{aligned} \mathcal{G}\Pi_{d\kappa}\mathcal{G}^{\dagger} &= \sum_{\nu \in \mathbb{Z}(d)} \mathcal{G}|X; m_{d\kappa}(\nu)\rangle\langle X; m_{d\kappa}(\nu)|\mathcal{G}^{\dagger} \\ &= \sum_{\nu \in \mathbb{Z}(d)} \mathcal{G}|X; m_{d\kappa}(\nu+1)\rangle\langle X; m_{d\kappa}(\nu+1)|\mathcal{G}^{\dagger} = \Pi_{d\kappa}. \end{aligned} \tag{9.49}$$

Therefore $[\Pi_{d\kappa}, \mathcal{G}] = 0$. The $\Pi[GF(p^d)]$ is the sum of $\Pi_{g\kappa}$ in Eq. (9.26), and therefore it commutes with $\mathcal{G}$.

(5) For $m \in GF(p^d)$, the $m^{p^d} = m$. This together with Eq. (9.33) proves that for $m \in GF(p^d)$, we get $\mathcal{G}^d|X; m\rangle = |X; m\rangle$. Consequently the $\{\mathbf{1}, \mathcal{G}^d, ..., \mathcal{G}^{e-d}\}$ form a cyclic group of order e/d, which is a subgroup of Gal$(e/1)$.

(6) The fact that $\mathcal{G}^e = \mathbf{1}$ implies Eq. (9.38). We can easily confirm that the operators in Eq. (9.39) are projectors which obey the relation $\mathcal{G}\varpi_r = \Omega(r)\varpi_r$. Therefore they are eigenprojectors of $\mathcal{G}$.

(7) The fact that $(\mathcal{G}^d)^{e/d} = \mathbf{1}$ implies Eq. (9.40). In order to prove Eq. (9.41), we exponentiate both sides of Eq. (9.38), to the power d.

Example 9.3 We consider $GF(9)$ and we choose the irreducible polynomial $\varepsilon^2 + \varepsilon + 2$. In this case $\mathcal{G}$ is given by

$$\mathcal{G} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0 \\ 0&0&0&1&0&0&0&0&0 \end{pmatrix}; \quad \mathcal{G}^2 = \mathbf{1}. \tag{9.50}$$

In this matrix we used the order in Eq. (9.9) for their indices.

9.3 The Heisenberg-Weyl Group $HW[GF(p^e)]$

Definition 9.2 The displacement operators $Z(\alpha)$ and $X(\beta)$ are given by

$$Z(\alpha) = \sum_{n \in GF(p^e)} \chi(\alpha n)|X; n\rangle\langle X; n|; \quad \alpha, \beta \in GF(p^e)$$
$$X(\beta) = FZ(\alpha)F^{\dagger} = \sum_{n \in GF(p^e)} \chi(-\beta n)|P; n\rangle\langle P; n| \tag{9.51}$$

Using Eq. (8.49), they can also be written as

$$Z(\alpha) = \sum \omega_p \left[\sum g_{ij}\alpha_i n_j\right] |X; n_0\rangle\langle X; n_0| \otimes \cdots \otimes |X; n_{e-1}\rangle\langle X; n_{e-1}|$$
$$X(\beta) = \sum \omega_p \left[\sum g_{ij}\beta_i n_j\right] |P; n_0\rangle\langle P; n_0| \otimes \cdots \otimes |P; n_{e-1}\rangle\langle P; n_{e-1}| \tag{9.52}$$

in the basis $\{\varepsilon^i\}$ for $GF(p^e)$.

More general displacement operators are given by

$$D(\alpha, \beta) = Z(\alpha)X(\beta)\chi(-2^{-1}\alpha\beta) \tag{9.53}$$

Lemma 9.1 *(1) The operators $Z(\alpha)$ and $X(\beta)$ act on position and momentum states as follows:*

$$Z(\alpha)|P; m\rangle = |P; m + \alpha\rangle; \qquad Z(\alpha)|X; m\rangle = \chi(\alpha m)]|X; m\rangle$$
$$X(\beta)|P; m\rangle = \chi(-m\beta)]|P; m\rangle; \qquad X(\beta)|X; m\rangle = |X; m + \beta\rangle, \tag{9.54}$$

(2)

$$X(\beta)Z(\alpha) = Z(\alpha)X(\beta)\chi(-\alpha\beta) \tag{9.55}$$

(3)

$$[Z(\alpha)]^p = [X(\beta)]^p = \mathbf{1} \tag{9.56}$$

The $Z(\alpha), X(\beta)$ are $p^e \times p^e$ complex matrices, and they have the $\omega_p(i)$ as eigenvalues (with various multiplicities).

Proof (1) Using the definition of $Z(\alpha)$ in Eq. (9.51) we immediately prove that $Z(\alpha)|X; m\rangle = \chi(\alpha m)]|X; m\rangle$. Also acting with $Z(\alpha)$ on both sides of Eq. (9.3), we prove that $Z(\alpha)|P; m\rangle = |P; m + \alpha\rangle$.

(2) We act with both $X(\beta)Z(\alpha)$ and $Z(\alpha)X(\beta)\chi(-\alpha\beta)$ on $|X; m\rangle$, and using Eq. (9.54) we show that they give the same result.

(3) $[Z(\alpha)]^p = Z(p\alpha) = Z(0) = \mathbf{1}$. Therefore the eigenvalues of $Z(\alpha)$ are $\omega_p(i)$. Analogous result holds for $X(\beta)$.

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

Proposition 9.2 *(1)*

$$D(\alpha, \beta)|X; m\rangle = \chi(2^{-1}\alpha\beta + \alpha m)\ |X; m + \beta\rangle$$
$$D(\alpha, \beta)|P; m\rangle = \chi(-2^{-1}\alpha\beta - \beta m)\ |P; m + \alpha\rangle \tag{9.57}$$

(2)

$$D(\alpha,\beta)D(\gamma,\delta) = D(\alpha+\gamma,\beta+\delta)\ \chi\left[2^{-1}(\alpha\delta-\beta\gamma)\right] \tag{9.58}$$

The $D(\alpha,\beta)\chi(\gamma)$, where $\alpha,\beta,\gamma \in GF(p^e)$ form a representation of the Heisenberg-Weyl $HW[GF(p^e)]$ group.

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

$$[D(\alpha,\beta)]^p = \mathbf{1}, \tag{9.59}$$

They are $p^e \times p^e$ complex matrices, and they have the $\omega_p(i)$ as eigenvalues (with various multiplicities).

(4) For an arbitrary operator θ

$$\frac{1}{p^e}\sum_{\alpha,\beta\in GF(p^e)} D(\alpha,\beta)\ \frac{\theta}{\mathrm{tr}\theta}\ [D(\alpha,\beta)]^\dagger = \mathbf{1} \tag{9.60}$$

This is the resolution of the identity in the present context.

(5) In the context of the isomorphism in Eq. (9.5), the displacement operators acting on $H[GF(p^e)]$ are expressed in terms of the displacement operators $\mathscr{D}$ acting on the various $H[\mathbb{Z}(p)]$ as:

$$D(\alpha,\beta) = D(\overline{\alpha}_0,\beta_0)\otimes\cdots\otimes D(\overline{\alpha}_{e-1},\beta_{e-1}) \tag{9.61}$$

The dual components of α, and the components of β appear in this formula.

Proof (1) This is proved using Eq. (9.54).

(2) This is proved using Eq. (9.55). The proof that the $D(\alpha,\beta)\omega(\gamma)$ form a group, is analogous to the proof of Proposition 4.3 (part 1).

(3) Using Eq. (9.58) we show that

$$[D(\alpha,\beta)]^p = D(p\alpha,p\beta) = D(0,0) = \mathbf{1}. \tag{9.62}$$

Therefore the eigenvalues of $D(\alpha,\beta)$ are $\omega_p(i)$.

(4) The proof is analogous to the one for Proposition 4.4.

(5) We express the displacement operators as

$$D(\alpha,\beta) = \sum_m \chi(2^{-1}\alpha\beta+\alpha m)\ |X;m+\beta\rangle\langle X;m|, \tag{9.63}$$

and then use Eq. (8.49), to prove Eq. (9.61).

Remark 9.1 Displacements in the system $\Sigma\{[\mathbb{Z}(p)]^e\}$ will be

$$D(\alpha_0,\beta_0)\otimes\cdots\otimes D(\alpha_{e-1},\beta_{e-1}). \tag{9.64}$$

Comparison with Eq. (9.61) shows another difference between the systems $\Sigma[GF(p^e)]$ and $\Sigma\{[\mathbb{Z}(p)]^e\}$. The dual components of α appear in Eq. (9.61), in contrast to the components of α which appear in Eq. (9.64).

Remark 9.2 We can define coherent states here, analogous to those in Sect. 4.4, but we do not pursue this direction.

Example 9.4 We consider $GF(9)$ and we choose the irreducible polynomial $\varepsilon^2 + \varepsilon + 2$. In this case, we present some of the $Z(\alpha)$, which in the basis of position states are diagonal 9×9 matrices:

$$\begin{aligned} Z(1) &= \text{diag}\left(1\ \omega(2)\ \omega(1)\ \omega(2)\ \omega(1)\ 1\ \omega(1)\ 1\ \omega(2)\right), \\ Z(2+\varepsilon) &= \text{diag}\left(1\ 1\ 1\ \omega(1)\ \omega(1)\ \omega(1)\ \omega(2)\ \omega(2)\ \omega(2)\right), \\ \omega(r) &= \exp\left(i\frac{2\pi r}{3}\right). \end{aligned} \tag{9.65}$$

We have used the order in Eq. (9.9).

A central aspect of Galois theory is the Frobenius transformations and the Galois groups. It is these transformations in a quantum context, that make the quantum systems in this chapter different from those in Chap. 7. The following proposition studies a group that combines displacements and Frobenius transformations. Later we will study a group that combines symplectic and Frobenius transformations, and also a bigger group that combines displacements, symplectic and Frobenius transformations.

Proposition 9.3 *(1) The Frobenius transform acts on the displacement operators as follows:*

$$\mathscr{G}^j D(\alpha, \beta)(\mathscr{G}^\dagger)^j = D(\alpha^{p^j}, \beta^{p^j}); \quad j = 0, ..., e-1 \tag{9.66}$$

If $d|e$ and α, β belong to the subfield $GF(p^d)$ of $GF(p^e)$, then $[\mathscr{G}^d, D(\alpha, \beta)] = 0$.

(2) The unitary operators

$$\mathscr{D}(j|\alpha, \beta, \gamma) = \mathscr{G}^j D(\alpha, \beta)\chi(\gamma); \quad j \in \mathbb{Z}(e), \tag{9.67}$$

form the 'Heisenberg-Weyl-Galois' group $HWGal[GF(p^e)]$ which is the semi-direct product of the Heisenberg-Weyl group by the Galois group $\text{Gal}(e|1)$*:*

$$HWGal[GF(p^e)] = HW[GF(p^e)] \rtimes \text{Gal}(e|1). \tag{9.68}$$

Proof (1) We calculate the matrix elements

$$\langle X; m|\mathscr{G}^j D(\alpha,\beta)(\mathscr{G}^\dagger)^j|X; n\rangle, \quad \langle X; m|D(\alpha^{p^j},\beta^{p^j})|X; n\rangle,$$

using Eqs. (9.57), (9.33), and we prove that they are identical.
If $\alpha, \beta \in GF(p^d)$, then $\alpha^{p^d} = \alpha$, and similarly for β. In this case $\mathscr{G}^d D(\alpha,\beta)(\mathscr{G}^\dagger)^d = D(\alpha,\beta)$.

(2) There is a closure property of the $\mathscr{D}(j|\alpha,\beta,\gamma)$ under multiplication:

$$\begin{aligned}
&\mathscr{D}(j_1|\alpha_1,\beta_1,\gamma_1)\mathscr{D}(j_2|\alpha_2,\beta_2,\gamma_2) = \mathscr{D}(j_1+j_2|\alpha_3,\beta_3,\gamma_3)\\
&\alpha_3 = \alpha_1^{p^{e-j_2}} + \alpha_2; \quad \beta_3 = \beta_1^{p^{e-j_2}} + \beta_2\\
&\gamma_3 = \gamma_1 + \gamma_2 + 2^{-1}\alpha_1^{p^{e-j_2}}\beta_2 - 2^{-1}\beta_1^{p^{e-j_2}}\alpha_2
\end{aligned} \tag{9.69}$$

The multiplication is associative and the inverse of $\mathscr{D}(j|\alpha,\beta,\gamma)$ is

$$[\mathscr{D}(j|\alpha,\beta,\gamma)]^{-1} = \mathscr{D}(-j|-\alpha^{p^j},-\beta^{p^j},-\gamma) \tag{9.70}$$

Therefore the $\mathscr{D}(j|\alpha,\beta,\gamma)$ form a group, which we denote as $HWGal[GF(p^e)]$. We next show that

$$\begin{aligned}
&HW[GF(p^e)] \triangleleft HWGal[GF(p^e)]\\
&\mathrm{Gal}(e|1) \prec HWGal[GF(p^e)]\\
&HW[GF(p^e)] \bigcap \mathrm{Gal}(e|1) = \{\mathbf{1}\}.
\end{aligned} \tag{9.71}$$

The $\triangleleft$ indicates normal subgroup, and the $\prec$ indicates subgroup. In order to show that $HW[GF(p^e)]$ is a normal subgroup of $HWGal[GF(p^e)]$, we show that:

$$\begin{aligned}
&\mathscr{D}(j|\alpha,\beta,\gamma)\ D(A,B)\chi(\gamma)\ [\mathscr{D}(j|\alpha,\beta,\gamma)]^\dagger\\
&= D(A^{p^j},B^{p^j})\chi(\gamma + B\alpha - A\beta).
\end{aligned} \tag{9.72}$$

We easily prove the other two relations in Eq. (9.71). Therefore $HWGal[GF(p^e)]$ is the semidirect product of the $HW[GF(p^e)]$ by the $\mathrm{Gal}(e|1)$.

9.4 Symplectic Transformations and the $Sp[2, GF(p^e)]$ Group

In this section we study symplectic transformations. We also study the groups that combine displacement and symplectic transformations, and also symplectic and Frobenius transformations. Furthermore we study the group that combines

displacement, symplectic and Frobenius transformations. We use self-explanatory notation for these groups.

Definition 9.3 $S(\kappa, \lambda|\mu, \nu)$ are $p^e \times p^e$ unitary matrices which perform the following transformations on the operators $X(\beta)$, $Z(\alpha)$:

$$\begin{aligned}
&[X(\kappa, \lambda)](\beta) = S(\kappa, \lambda|\mu, \nu)X(\beta)[S(\kappa, \lambda|\mu, \nu)]^\dagger = D(\lambda\beta, \kappa\beta) \\
&[Z(\mu, \nu)](\alpha) = S(\kappa, \lambda|\mu, \nu)Z(\alpha)[S(\kappa, \lambda|\mu, \nu)]^\dagger = D(\nu\alpha, \mu\alpha) \\
&\kappa\nu - \lambda\mu = 1; \quad \kappa, \lambda, \mu, \nu \in GF(p^e).
\end{aligned} \tag{9.73}$$

The following proposition is analogous to 4.9.

Proposition 9.4 *(1) The $p^e \times p^e$ matrices $S(\kappa, \lambda|\mu, \nu)$ form a unitary representation of the $Sp[2, GF(p^e)]$ group.*

(2) The symplectic group $Sp[2, GF(p^e)]$ is a group of outer automorphisms of the Heisenberg-Weyl group $HW[GF(p^e)]$:

$$\begin{aligned}
&S(\kappa, \lambda|\mu, \nu)D(\alpha, \beta)[S(\kappa, \lambda|\mu, \nu)]^\dagger = D(\alpha\nu + \beta\lambda, \alpha\mu + \beta\kappa) \\
&\kappa, \lambda, \mu, \nu, \alpha, \beta \in GF(p^e)
\end{aligned} \tag{9.74}$$

Proof The proof of both parts is analogous to the one for $Sp[2, \mathbb{Z}(d)]$, given in Proposition 4.9.

Proposition 9.5 *The Iwasawa decomposition states that*

$$\begin{aligned}
S(\kappa, \lambda|\mu, \nu) &= S(1, 0|\xi_1, 1)S(1, \xi_2|0, 1)S(\xi_3, 0|0, \xi_3^{-1}) \\
S(1, 0|\xi_1, 1) &= \sum_m \chi(-2^{-1}\xi_1 m^2)|P; m\rangle\langle P; m| \\
S(1, \xi_2|0, 1) &= \sum_m \chi(2^{-1}\xi_2 m^2)|X; m\rangle\langle X; m| \\
S(\xi_3, 0|0, \xi_3^{-1}) &= \sum_n |X; n\rangle\langle X; \xi_3 n| = \sum_n |P; \xi_3^{-1} n\rangle\langle P; n|
\end{aligned} \tag{9.75}$$

where the relationship between $\kappa, \lambda, \mu, \nu$ and ξ_1, ξ_2, ξ_3 is given in Eqs. (3.39), (3.40).

Proof The proof is analogous to the one in Proposition 4.10, for the $Sp[2, \mathbb{Z}(d)]$ group.

The following lemma is the analogue in the present context, of Lemma 4.1:

Lemma 9.2

$$\begin{aligned}
\langle X; r|S(\kappa, \lambda|\mu, \nu)|X; n\rangle = &\frac{1}{p^e} G[-2^{-1}\mu\nu^{-1}; GF(p^e)] \\
&\times \chi\left[2^{-1}\lambda\nu^{-1}n^2 + 2^{-1}\mu^{-1}\nu^{-1}(r\nu - n)^2\right],
\end{aligned} \tag{9.76}$$

where $G[s; GF(p^e)]$ is the Gauss sum in Eq. (8.51).

Proof The proof is analogous to that for Lemma 4.1.

Example 9.5 We consider $GF(9)$ and we choose the irreducible polynomial $\varepsilon^2 + \varepsilon + 2$. Using Eq. (9.76), we calculate the $\langle X; 2|S(1+\varepsilon, 0|\varepsilon, \varepsilon)|X; 1+\varepsilon\rangle$. In this case

$$-2^{-1}\mu\nu^{-1} = -2^{-1}\varepsilon\varepsilon^{-1} = 1. \tag{9.77}$$

Using the matrix g in Eq. (8.46) we find that

$$\mathrm{Tr}[(\alpha_1 + \varepsilon\alpha_2)^2] = -\alpha_1^2 - 2\alpha_1\alpha_2; \quad \alpha_1, \alpha_2 \in \mathbb{Z}(3), \tag{9.78}$$

and therefore the Gauss sum is

$$G[1; GF(9)] = 5 + 2\omega(1) + 2\omega(-1). \tag{9.79}$$

Also

$$\chi\left[2^{-1}\lambda\nu^{-1}n^2 + 2^{-1}\mu^{-1}\nu^{-1}(r\nu - n)^2\right] = \omega(0) = 1 \tag{9.80}$$

and

$$\langle X; 2|S(1+\varepsilon, 0|1+\varepsilon, \varepsilon)|X; 1+\varepsilon\rangle = 5 + 2\omega(1) + 2\omega(-1). \tag{9.81}$$

Here

$$\omega(\alpha) = \exp\left(i\frac{2\pi\alpha}{3}\right). \tag{9.82}$$

Proposition 9.6 *The unitary operators*

$$T(\kappa, \lambda|\mu, \nu|\alpha, \beta, \gamma) = S(\kappa, \lambda|\mu, \nu)D(\alpha, \beta)\chi(\gamma) \tag{9.83}$$

form a group [4] which we denote as $HWSp[GF(p^e)]$, and which is the semidirect product of the $HW[GF(p^e)]$ by the $Sp[2, GF(p^e)]$:

$$HWSp[GF(p^e)] = HW[GF(p^e)] \rtimes Sp[2, GF(p^e)]. \tag{9.84}$$

Proof The proof is analogous to the proof of Proposition 4.11. We first show that the operators $T(\kappa, \lambda|\mu, \nu|\alpha, \beta, \gamma)$ form a group which we denote as $HWSp[GF(p^e)]$. We then show that

$$\begin{aligned} &HW[GF(p^e)] \lhd HWSp[GF(p^e)] \\ &Sp[GF(p^e)] \prec HWSpGal[GF(p^e)] \\ &HW[GF(p^e)] \bigcap Sp[GF(p^e)] = \{\mathbf{1}\}. \end{aligned} \tag{9.85}$$

Proposition 9.7 *(1) The Frobenius transformations act on the symplectic transformations as follows:*

$$\mathscr{G}^i S(\kappa, \lambda|\mu, \nu)(\mathscr{G}^\dagger)^i = S(\kappa^{p^i}, \lambda^{p^i}|\mu^{p^i}, \nu^{p^i}); \quad i = 0, ..., e-1 \tag{9.86}$$

If $\kappa, \lambda, \mu, \nu$ belong to the subfield $GF(p^d)$ of $GF(p^e)$ (where $d|e$) then

$$[\mathscr{G}^d, S(\kappa, \lambda|\mu, \nu)] = 0. \tag{9.87}$$

(2) The unitary operators

$$\mathfrak{s}(j|\kappa, \lambda|\mu, \nu) = \mathscr{G}^j S(\kappa, \lambda|\mu, \nu); \quad j \in \mathbb{Z}(e) \tag{9.88}$$

form a group $SpGal[GF(p^e)]$, which is the semidirect product of the $Sp[2, GF(p^e)]$ by the Galois group $\mathrm{Gal}(e|1)$*:*

$$SpGal[GF(p^e)] = Sp[2, GF(p^e)] \rtimes \mathrm{Gal}(e|1). \tag{9.89}$$

Proof (1) We act with $\mathscr{G}^i$ and $(\mathscr{G}^\dagger)^i$ on the left and right of Eq. (4.66), and using Eq. (9.33) we get

$$\mathscr{G}^i S(\kappa, \lambda|\mu, \nu)(\mathscr{G}^\dagger)^i = \left[\frac{1}{p^e}\sum_m \chi(A)\right] |X; r^{p^i}\rangle\langle X; n^{p^i}|. \tag{9.90}$$

A is given in Eq. (4.66). All conjugates have the same character and taking into account Eq. (8.3), we get

$$\begin{aligned} &\chi(A) = \chi\left(A^{p^i}\right) \\ &A^{p^i} = -2^{-1}MN^{-1}m^{2p^i} + 2^{-1}\Lambda N^{-1}n^{2p^i} - N^{-1}(mn)^{p^i} + (mr)^{p^i} \\ &\Lambda = \lambda^{p^i}; \quad M = \mu^{p^i}; \quad N = \nu^{p^i}. \end{aligned} \tag{9.91}$$

Inserting them into Eq. (9.90), we prove Eq. (9.86).
If the parameters belong to the subfield $GF(p^d)$ of $GF(p^e)$, then $\kappa^{p^d} = \kappa$, and similarly for the other parameters. In this case, Eq. (9.86) gives Eq. (9.87).

(2) There is a closure property of the $\mathfrak{s}(j|\kappa, \lambda|\mu, \nu)$ under multiplication:

$$\begin{aligned}
&\mathfrak{s}(j_1|\kappa_1, \lambda_1|\mu_1, \nu_1)\mathfrak{s}(j_2|\kappa_2, \lambda_2|\mu_2, \nu_2) = \mathfrak{s}(j_1 + j_2|\kappa, \lambda|\mu, \nu) \\
&\kappa = \kappa_2\kappa_1^{p^{e-j_2}} + \lambda_2\mu_1^{p^{e-j_2}}; \quad \lambda = \kappa_2\lambda_1^{p^{e-j_2}} + \lambda_2\nu_1^{p^{e-j_2}} \\
&\mu = \mu_2\kappa_1^{p^{e-j_2}} + \nu_2\mu_1^{p^{e-j_2}}; \quad \nu = \mu_2\lambda_1^{p^{e-j_2}} + \nu_2\nu_1^{p^{e-j_2}}.
\end{aligned} \tag{9.92}$$

The multiplication is associative and the inverse of $\mathfrak{s}(j|\kappa, \lambda|\mu, \nu)$ is

$$[\mathfrak{s}(j|\kappa, \lambda|\mu, \nu)]^{-1} = \mathfrak{s}(-j|\nu^{p^j}, -\lambda^{p^j}| - \mu^{p^j}, \kappa^{p^j}). \tag{9.93}$$

Therefore the $\mathfrak{s}(j|\kappa, \lambda|\mu, \nu)$ form a group, which we denote as $SpGal[GF(p^e)]$. We next show that

$$\begin{aligned}
&Sp[GF(p^e)] \lhd SpGal[GF(p^e)] \\
&\text{Gal}(e|1) \prec SpGal[GF(p^e)] \\
&\text{Gal}(e|1) \bigcap Sp[GF(p^e)] = \{\mathbf{1}\}.
\end{aligned} \tag{9.94}$$

In order to show that the $Sp[2, GF(p^e)]$ is a normal subgroup of $SpGal[GF(p^e)]$, we show that:

$$\begin{aligned}
&\mathfrak{s}(i|\kappa_1, \lambda_1|\mu_1, \nu_1)\ S(\kappa_2, \lambda_2|\mu_2, \nu_2)\ [\mathfrak{s}(i|\kappa_1, \lambda_1|\mu_1, \nu_1)]^\dagger \\
&= \mathscr{G}^i S(\kappa_1, \lambda_1|\mu_1, \nu_1)S(\kappa_2, \lambda_2|\mu_2, \nu_2)S(\nu_1, -\lambda_1| - \mu_1, \kappa_1)\mathscr{G}^{-i} \\
&= \mathscr{G}^i S(\kappa, \lambda|\mu, \nu)\mathscr{G}^{-i} = S(\kappa^{p^i}, \lambda^{p^i}|\mu^{p^i}, \nu^{p^i}).
\end{aligned} \tag{9.95}$$

Here

$$\begin{pmatrix} \kappa & \lambda \\ \mu & \nu \end{pmatrix} = \begin{pmatrix} \nu_1 & -\lambda_1 \\ -\mu_1 & \kappa_1 \end{pmatrix} \begin{pmatrix} \kappa_2 & \lambda_2 \\ \mu_2 & \nu_2 \end{pmatrix} \begin{pmatrix} \kappa_1 & \lambda_1 \\ \mu_1 & \nu_1 \end{pmatrix}. \tag{9.96}$$

We also show the other two relations in Eq. (9.94), and we conclude that the $SpGal[GF(p^e)]$ is the semidirect product of the $Sp[2, GF(p^e)]$ by the $Gal(e|1)$.

The following proposition describes a group that combines displacements, symplectic and Frobenius transformations.

Proposition 9.8 *The unitary operators*

$$\mathscr{G}^i T(\kappa, \lambda|\mu, \nu|\alpha, \beta, \gamma) = T(\kappa^{p^i}, \lambda^{p^i}|\mu^{p^i}, \nu^{p^i}|\alpha^{p^i}, \beta^{p^i}, \gamma)\mathscr{G}^i \tag{9.97}$$

form a group [4] which we denote as $HWSpGal[GF(p^e)]$. It is the semidirect product of the group $HWSp[GF(p^e)]$, by the Galois group Gal$(e|1)$*, and it is isomorphic to the semidirect product of $HW[GF(p^e)]$ by the group $SpGal[GF(p^e)]$:*

$$HWSpGal[GF(p^e)] = HWSp[GF(p^e)] \rtimes \text{Gal}(e|1)$$
$$\cong HW[GF(p^e)] \rtimes SpGal[GF(p^e)]. \tag{9.98}$$

Proof The proof is analogous to the second part of Proposition 9.3, and also to the second part of Proposition 9.7. We first show that the operators in Eq. (9.97) form a group which we denote $HWSpGal[GF(p^e)]$. We then show that

$$HWSp[GF(p^e)] \lhd HWSpGal[GF(p^e)]$$
$$\text{Gal}(e|1) \prec HWSpGal[GF(p^e)]$$
$$HWSp[GF(p^e)] \bigcap \text{Gal}(e|1) = \{\mathbf{1}\}, \tag{9.99}$$

and this proves that the $HWSpGal[GF(p^e)]$ is the semidirect product of $HWSp[GF(p^e)]$ by $\text{Gal}(e|1)$.

We also show that

$$HW[GF(p^e)] \lhd HWSpGal[GF(p^e)]$$
$$SpGal[GF(p^e)] \prec HWSpGal[GF(p^e)]$$
$$HW[GF(p^e)] \bigcap SpGal[GF(p^e)] = \{\mathbf{1}\}. \tag{9.100}$$

and this proves that the $HWSpGal[GF(p^e)]$ is the semidirect product of $HW[GF(p^e)]$ by $SpGal[GF(p^e)]$.

9.5 Parity Operators and Wigner and Weyl Functions

The material in Sects. 4.7 and 4.8 is also valid for Galois quantum systems, if we replace the characters $\omega(\alpha)$ where $\alpha \in \mathbb{Z}(d)$, with $\chi(\alpha)$ where $\alpha \in GF(p^e)$. In this section we complement this, with other properties that involve Frobenius transformations, and which are specific to Galois quantum systems.

Parity operators are defined as in Definition 4.8. Propositions 11.4, 4.13, 4.14, 4.15, also hold here, with the characters ω in $\mathbb{Z}(d)$, replaced here with the characters χ in $GF(p^e)$). The proposition below is specific to Galois quantum systems.

Proposition 9.9 *(1) The parity operators acting on $H[GF(p^e)]$ are expressed in terms of the displacement operators $\mathscr{P}$ acting on the various $H[\mathbb{Z}(p)]$ as:*

$$P(\alpha, \beta) = P(\overline{\alpha}_0, \beta_0) \otimes \cdots \otimes P(\overline{\alpha}_{e-1}, \beta_{e-1}) \tag{9.101}$$

The dual components of α, and the components of β appear in this formula.

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

$$\mathscr{G}^j P(\alpha, \beta)(\mathscr{G}^\dagger)^j = P(\alpha^{p^j}, \beta^{p^j}); \quad j = 0, ..., e-1 \tag{9.102}$$

If $d|e$ and α, β belong to the subfield $GF(p^d)$ of $GF(p^e)$, then $[\mathscr{G}^d, P(\alpha, \beta)] = 0$.

Proof (1) We first show that

$$P(0,0) = F^2 = P(0,0) \otimes \cdots \otimes P(0,0) \tag{9.103}$$

and then use Eq. (9.61) to prove Eq. (9.101).

(2) The Frobenius transform $\mathscr{G}^j$ commutes with the Fourier transform F, and therefore it commutes with the parity operator around the origin $P(0,0) = F^2$. Using Eq. (9.66) we get

$$\begin{aligned} &\mathscr{G}^j P(\alpha,\beta)(\mathscr{G}^\dagger)^j = \mathscr{G}^j D(\alpha,\beta) P(0,0)[D(\alpha,\beta)]^\dagger (\mathscr{G}^\dagger)^j \\ &= D(\alpha^{p^j}, \beta^{p^j}) P(0,0)[D(\alpha^{p^j}, \beta^{p^j})]^\dagger = P(\alpha^{p^j}, \beta^{p^j}). \end{aligned} \tag{9.104}$$

Wigner and Weyl functions are defined as in Definition 4.9. Propositions 4.16, 4.17, 4.18, 4.19, 4.20, also hold here.

9.6 Hamiltonians of Galois Quantum Systems and Time Evolution

Both the Galois quantum system $\Sigma[GF(p^e)]$, and the system $\Sigma\{[\mathbb{Z}(p)]^e\}$ are e-partite systems. The Galois quantum system $\Sigma[GF(p^e)]$, has extra structure related to the properties of Galois fields. It is imperative that its Hamiltonian is compatible with these 'Galois properties', and that it preserves them under time evolution [6].

The analogue of the position and momentum operators in Eq. (4.7), involve here Galois numbers. For Hamiltonians we need matrices of complex numbers. We use characters and define the analogue of $\exp(ix^r)$ and $\exp(ip^r)$ in the harmonic oscillator, as follows:

$$\begin{aligned} &\mathfrak{E}_X(r) = \sum_{m \in GF(p^e)} \chi(m^r)|X; m\rangle\langle X; m|; \quad \alpha, \beta \in GF(p^\ell) \\ &\mathfrak{E}_P(r) = \sum_{m \in GF(p^e)} \chi(m^r)|P; m\rangle\langle P; m| = F\mathfrak{E}_X(\beta)F^\dagger \\ &[\mathfrak{E}_X(r)]^p = [\mathfrak{E}_P(r)]^p = \mathbf{1}. \end{aligned} \tag{9.105}$$

They are $p^e \times p^e$ complex matrices. Their logarithms

$$\begin{aligned} &\mathfrak{X} = i \log \mathfrak{E}_X(1) = i \sum_{m \in GF(p^e)} [\log \chi(m^r)]|X; m\rangle\langle X; m| \\ &\mathfrak{P} = i \log \mathfrak{E}_P(1) = i \sum_{m \in GF(p^e)} [\log \chi(m^r)]|P; m\rangle\langle P; m| = F\mathfrak{X}F^\dagger, \end{aligned} \tag{9.106}$$

can be viewed as the analogues of position and momentum operators which can be used in Hamiltonians $h = h(\mathfrak{X}, \mathfrak{P})$, for practical calculations. The logarithms are multivalued, but we can take the principal values.

As an example we consider the Hamiltonian:

$$h = -i \ln[\mathfrak{E}_X(2)\mathfrak{E}_P(2)] = -i \ln[\mathfrak{E}_X(2) F \mathfrak{E}_X(2) F^\dagger]. \tag{9.107}$$

The evolution operator for the system is then

$$\exp(ith) = [\mathfrak{E}_X(2)\mathfrak{E}_P(2)]^t = [\mathfrak{E}_X(2) F \mathfrak{E}_X(2) F^\dagger]^t \tag{9.108}$$

This is the analogue of $\exp(ix^2)\exp(ip^2)$ in the harmonic oscillator.

9.6.1 Example

As a numerical example, we consider a Galois quantum system which has positions and momenta in $GF(9)$. We choose the irreducible polynomial $P(\varepsilon) = \varepsilon^2 + \varepsilon + 2$, and we will calculate the $\mathfrak{X}$, the $\mathfrak{E}_X(2)$, and the evolution operator in Eq. (9.108). We need to calculate the $\mathrm{Tr}(m)$ and $\mathrm{Tr}(m^2)$ for all $m \in GF(9)$. If $m = m_0 + m_1\varepsilon$ where $m_0, m_1 \in \mathbb{Z}(3)$, then using the g matrix in Eq. (8.46), we find that

$$\begin{aligned} \mathrm{Tr}(m) &= \sum_{i,j} m_i g_{i0} = -m_0 - m_1 \\ \mathrm{Tr}(m^2) &= \sum_{i,j} g_{ij} m_i m_j = -m_0^2 - 2m_0 m_1 \end{aligned} \tag{9.109}$$

Therefore

$$\begin{aligned} \mathfrak{X} = &-\frac{2\pi}{3}|X;1\rangle\langle X;1| + \frac{2\pi}{3}|X;2\rangle\langle X;2| \\ &- \frac{2\pi}{3}|X;\varepsilon\rangle\langle X;\varepsilon| + \frac{2\pi}{3}|X;1+\varepsilon\rangle\langle X;1+\varepsilon| \\ &+ \frac{2\pi}{3}|X;2\varepsilon\rangle\langle X;2\varepsilon| - \frac{2\pi}{3}|X;2+2\varepsilon\rangle\langle X;2+2\varepsilon| \end{aligned} \tag{9.110}$$

and

$$\begin{aligned} \mathfrak{E}_X(2) = &|X;0\rangle\langle X;0| + \omega(-1)|X;1\rangle\langle X;1| + \omega(-1)|X;2\rangle\langle X;2| \\ &+ |X;\varepsilon\rangle\langle X;\varepsilon| + |X;1+\varepsilon\rangle\langle X;1+\varepsilon| + \omega(1)|X;2+\varepsilon\rangle\langle X;2+\varepsilon| \\ &+ |X;2\varepsilon\rangle\langle X;2\varepsilon| + \omega(1)|X;1+2\varepsilon\rangle\langle X;1+2\varepsilon| \\ &+ |X;2+2\varepsilon\rangle\langle X;2+2\varepsilon|, \end{aligned} \tag{9.111}$$

where

$$\omega(\alpha) = \exp\left(i\frac{2\pi\alpha}{3}\right); \quad \alpha \in \mathbb{Z}(3). \tag{9.112}$$

The evolution operator in Eq. (9.108) can be written as a 9×9 matrix (in the order of Eq. (9.9)) as $\exp(ith) = M^t$, where

$$M = \mathfrak{E}_X(2) F \mathfrak{E}_X(2) F^\dagger = \frac{1}{3}\begin{pmatrix} 1 & a & a & 1 & 1 & a^* & 1 & a^* & 1 \\ 1 & a^* & 1 & a & a^* & a^* & a^* & a^* & a \\ 1 & 1 & a^* & a^* & a & a^* & a & a^* & a^* \\ 1 & a^* & 1 & 1 & a & a & 1 & 1 & a^* \\ 1 & 1 & a^* & a & 1 & a & a^* & 1 & 1 \\ 1 & a & a & a^* & a^* & a & a & 1 & a \\ 1 & 1 & a^* & 1 & a^* & 1 & 1 & a & a \\ 1 & a & a & a & a & 1 & a^* & a & a^* \\ 1 & a^* & 1 & a^* & 1 & 1 & a & a & 1 \end{pmatrix} \tag{9.113}$$

Here $a = \omega(1)$.

9.6.2 Galois Systems with Frobenius Symmetry

Definition 9.4 A Galois quantum system has a Frobenius symmetry, when its Hamiltonian h commutes with $\mathscr{G}$, and therefore with all the projectors $\varpi(i)$ in Eq. (9.39):

$$[\mathscr{G}, h] = [\varpi(i), h] = 0; \quad i = 0, ..., e-1. \tag{9.114}$$

Let $\rho(0)$ be the density matrix of a system with Frobenius symmetry, at $t = 0$ (it is a $p^e \times p^e$ matrix). We express it in terms of e^2 matrices $\sigma_{ij}(0)$ (which are not density matrices), as

$$\rho(0) = \sum_{ij} \sigma_{ij}(0); \quad \sigma_{ij}(0) = \varpi(i)\rho(0)\varpi(j). \tag{9.115}$$

Then

$$\begin{aligned} \rho(t) &= \exp(ith)\rho(0)\exp(-ith) = \sum_{ij} \sigma_{ij}(t) \\ \sigma_{ij}(t) &= \exp(ith)\ \sigma_{ij}(0)\ \exp(-ith) \end{aligned} \tag{9.116}$$

It is seen that in the case of Frobenius symmetry, each of the matrices $\sigma_{ij}(t)$ evolves independently.

Another consequence of the Frobenius symmetry is that we have e constants of motion:

$$\mathrm{tr}[\rho(t)\varpi(i)] = \mathrm{tr}[\rho(0)\varpi(i)]. \tag{9.117}$$

9.7 Mutually Unbiased Bases in $H[GF(p^e)]$ and Duality to $GF(p^e) \times GF(p^e)$

In this section we extend our earlier discussion on mutually unbiased bases, to systems with variables in Galois fields. There are $p^e + 1$ mutually unbiased bases in $H[GF(p^e)]$, which we construct explicitly in this section. The construction is analogous to the one in Proposition 5.5, for $H[\mathbb{Z}(p)]$. We first introduce a notation, analogous to Notation 5.2.

Notation 9.1 *In $H[GF(p^e)]$ we consider the p^e orthonormal bases*

$$|\mathscr{X}(v); m\rangle = S(0, -1|1, v)|X; m\rangle; \quad v, m \in GF(p^e) \tag{9.118}$$

where $S(0, -1|1, v)$ are symplectic matrices (discussed in Sect. 9.4). In the case $v = 0$, this is the basis of momentum states:

$$|\mathscr{X}(0); m\rangle = S(0, -1|1, 0)|X; m\rangle = F^{\dagger}|X; m\rangle = |P; -m\rangle. \tag{9.119}$$

We also consider the orthonormal basis of position states, and we use the convention

$$|\mathscr{X}(-1); m\rangle = |X; m\rangle. \tag{9.120}$$

So we have $p^e + 1$ orthonormal bases

$$\mathscr{B}(v) = \{|\mathscr{X}(v); m\rangle | m \in GF(p^e)\}; \quad v \in \{-1\} \cup GF(p^e). \tag{9.121}$$

The $v = -1$ is used as an extra element that indicates position states, and should not be confused with the $p - 1 = -1 \pmod p$ which is an element of $GF(p^e)$.

Proposition 9.10 *For $v \neq v'$,*

$$|\langle \mathscr{X}(v'); n|\mathscr{X}(v); m\rangle|^2 = \frac{1}{p^e}; \quad v, v' \in \{-1\} \cup GF(p^e). \tag{9.122}$$

Therefore they are a set of $p^e + 1$ mutually unbiased bases in $H[GF(p^e)]$.

Proof The proof is very similar to the proof of Proposition 5.5 (which is the special case $e = 1$ of the present proposition). The characters ω become here the characters χ. The Gauss sum $G[\alpha; \mathbb{Z}(p)]$ becomes the Gauss sum $G[\alpha; GF(p^e)]$, which has absolute value $|G[\alpha; GF(p^e)]| = \sqrt{p^e}$, for $\alpha \neq 0$.

Proposition 9.11 *The set of $p^e + 1$ mutually unbiased bases in $H[GF(p^e)]$,*

$$\{\mathscr{B}(\nu) \mid \nu \in \{-1\} \cup GF(p^e)\}, \tag{9.123}$$

is invariant under Frobenius transformations.

Proof We show that

$$\mathscr{G}^j|\mathscr{X}(-1); m\rangle = \mathscr{G}^j|X; m\rangle = |X; m^{p^j}\rangle = |\mathscr{X}(-1); m^{p^j}\rangle, \tag{9.124}$$

and

$$\begin{aligned} &\mathscr{G}^j|\mathscr{X}(\nu); m\rangle = \mathscr{G}^j S(0, -1|1, \nu)|X; m\rangle \\ &= S(0, -1|1, \nu^{p^j})|X; m^{p^j}\rangle = |\mathscr{X}(\nu^{p^j}); m^{p^j}\rangle. \end{aligned} \tag{9.125}$$

We denote this as

$$\begin{aligned} &\mathscr{G}^j\mathscr{B}(-1) = \mathscr{B}(-1) \\ &\mathscr{G}^j\mathscr{B}(\nu) = \mathscr{B}(\nu^{p^j}); \quad \nu \in GF(p^e). \end{aligned} \tag{9.126}$$

This proves the proposition.

9.7.1 The Finite Geometry $GF(p^e) \times GF(p^e)$

The $GF(p^e) \times GF(p^e)$ is a near-linear finite geometry, which is a generalization of the $\mathbb{Z}(p) \times \mathbb{Z}(p)$ geometry, discussed earlier. The new concept here is Frobenius transformations.

The geometry $GF(p^e) \times GF(p^e)$ has the $p^e + 1$ lines through the origin given by

$$L(0, 1) = \mathscr{L}(-1); \quad g(0, -1|1, \nu) \circ L(0, 1) = \mathscr{L}(-1); \quad \nu \in GF(p^e) \tag{9.127}$$

This is analogous to Eqs. (5.13),(5.14), for lines in $\mathbb{Z}(p) \times \mathbb{Z}(p)$.

Under Frobenius transformations a point (α, β) in $GF(p^e) \times GF(p^e)$ transforms as

$$\sigma(\alpha, \beta) \equiv (\sigma(\alpha), \sigma(\beta)) = (\alpha^p, \beta^p), \tag{9.128}$$

and a line as

$$\sigma[L(\alpha,\beta)] \equiv L(\sigma(\alpha),\sigma(\beta)) = L(\alpha^p,\beta^p) \tag{9.129}$$

We use the same notation σ for Frobenius transformations on elements in $GF(p^e)$, on pairs in $GF(p^e)\times GF(p^e)$, and on lines. They obey the relation $\sigma^e = \mathbf{1}$, and form the Galois group $G(e|1) \cong \mathbb{Z}(e)$.

The following proposition is dual to Proposition 9.11.

Proposition 9.12 *The set of p^e+1 lines through the origin in $GF(p^e)\times GF(p^e)$,*

$$\{\mathscr{L}(\nu) \mid \nu \in \{-1\}\cup GF(p^e)\}, \tag{9.130}$$

is invariant under Frobenius transformations.

Proof Acting with Frobenius transformations on the lines through the origin we get

$$\begin{aligned}\sigma^j\mathscr{L}(-1) &= \mathscr{L}(-1)\\ \sigma^j\mathscr{L}(\nu) &= \mathscr{L}(\nu^{p^j});\quad \nu\in GF(p^e).\end{aligned} \tag{9.131}$$

This proves the proposition.

Proposition 9.13 *There is a duality between the p^e+1 mutually unbiased bases in $H[GF(p^e)]$, and the p^e+1 lines through the origin in the finite geometry $GF(p^e)\times GF(p^e)$, where*

$$\mathscr{B}(\nu) \;\leftrightarrow\; \mathscr{L}(\nu). \tag{9.132}$$

Proof Comparison of Propositions 9.11, 9.12, proves the duality. The $\mathscr{G}$ corresponds to σ. The vectors in the basis $\mathscr{B}(\nu)$ correspond to the points in the line $\mathscr{L}(\nu)$.

References

1. Vourdas, A. (2005). *Journal of Physical A*, *38*, 8453.
2. Vourdas, A. (2006). *Acta Applications Mathematics*, *93*, 197.
3. Vourdas, A. (2006). *Journal of Mathematical Physics*, *47*, 092104.
4. Vourdas, A. (2007). *Journal of Physics A*, *40*, R285.
5. Vourdas, A. (2008). *The Journal of Fourier Analysis and Applications*, *14*, 102.
6. Vourdas, A. (2010). *Journal of Mathematical Physics*, *51*, 052102.
7. Chaturvedi, S. (2002). *Physical Review A*, *65*, 044301.
8. Gibbons, K., Hoffman, M. J., & Wootters, W. (2004). *Physical Review A*, *70*, 062101.
9. Bandyopadhyay, S., Boykin, P. O., Roychowdhury, V., & Vatan, F. (2002). *Algorithmica*, *34*, 512.
10. Pittenger, A. O., & Rubin, M. H. (2004). *Linear Algebra and its Applications*, *390*, 255.
11. Saniga, M., Planat, M., & Rosu, H. (2004). *Journal of Optics B-Quantum Semiclassical Optics*, *6*, L19.

12. Klappenecker, A., & Rotteler, M. (2004). *Lecture Notes in Computer Science*, *2948*, 137.
13. Pittenger, A. O., & Rubin, M. H. (2005). *Journal of Physics A*, *38*, 6005.
14. Klimov, A., Sanchez-Soto, L., & de Guise, H. (2005). *Journal of Physics A*, *38*, 2747.
15. Klimov, A., Munoz, C., & Romero, J. L. (2006). *Journal of Physics A*, *39*, 1447.
16. Romero, J. L., Bjork, G., Klimov, A. B., & Sanchez-Soto, L. L. (2005). *Physical Review A*, *72*, 062310.
17. Saniga, M., & Planat, M. (2006). *Journal of Physics A*, *39*, 435.
18. Kibler, M. (2009). *Journal of Physics A*, *42*, 353001.
19. Durt, T., Englert, B. G., Bengtsson, I., & Zyczkowski, K. (2010). *International Journal of Quantum Computing*, *8*, 535.
20. Appleby, D. M., Yadsan-Appleby, H., & Zauner, G. (2013). *Quantum Information and Computation*, *13*, 672.
21. Appleby, D. M., Bengtsson, I., & Dang, H. B. (2015). *Quantum Information and Computation*, *15*, 1261.
22. Berlekamp, E. R. (1968). *Algebraic coding theory*. New York: McGraw-Hill.
23. McClellan, J. H., & Rader, C. M. (1979). *Number theory in digital signal processing*. London: Prentice Hall.
24. Lin, S., & Costello, D. J. (1983). *Error control coding*. New Jersey: Prentice Hall.
25. Blahut, R. E. (1985). *Fast algorithms for digital signal processing*. Reading: Addison Wesley.
26. Pollard, J. M. (1971). *Mathematics of Computation*, *25*, 365.
27. Lima, J. B., & Campello de Souza, R. M. (2012). *Signal Processing*, *92*, 465.

Chapter 10
p-adic Numbers and Profinite Groups

Abstract Profinite groups, inverse and direct limits, and p-adic numbers, are briefly discussed. The material in this chapter is prerequisite for Chaps. 11 and 12.

In this chapter we present some background material on p-adic numbers, inverse and direct limits and profinite groups, which is needed later. The emphasis is on how to do practical calculations with p-adic numbers. General references on p-adic numbers are [1–4], and on profinite groups [5–7].

10.1 The Field $\mathbb{Q}_p$ and the Ring $\mathbb{Z}_p$

Let p be a prime number. The field $\mathbb{Q}_p$ of p-adic numbers, contains elements which can be written as a formal series:

$$a_p = \sum_{v=\text{ord}(a_p)}^{\infty} \overline{a}_v p^v; \qquad \overline{a}_v = 0, ..., p-1 \tag{10.1}$$

We note that:

- The -1 as a p-adic number is:

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + ... \tag{10.2}$$

- Addition and multiplication is the usual addition and multiplication of series, together with the 'carry' operation.
- $\text{ord}(a_p)$ is the ordinal or valuation of a_p (and it is a finite integer).
- The ring $\mathbb{Z}_p$ of p-adic integers contains elements with $\text{ord}(a_p) \geq 0$. More generally the ring $p^n\mathbb{Z}_p$ contains elements with $\text{ord}(a_p) \geq n$. For $n \geq m$,

$$p^m\mathbb{Z}_p / p^n\mathbb{Z}_p \cong \mathbb{Z}(p^{n-m}). \tag{10.3}$$

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_10

- Any integer can be written as a p-adic integer, and we get an inclusion of $\mathbb{Z}$ into $\mathbb{Z}_p$:

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p. \tag{10.4}$$

- Any rational number κ/λ, can be written in a p-adic form as

$$\begin{aligned} &\kappa = p^m \kappa_1; \quad \lambda = p^n \lambda_1 \\ &\frac{\kappa}{\lambda} = p^{m-n} \frac{\kappa_1}{\lambda_1} = p^{m-n}(\overline{a}_0 + \overline{a}_1 p + \overline{a}_2 p^2 + ...) \end{aligned} \tag{10.5}$$

In this way we get an inclusion of $\mathbb{Q}$ into $\mathbb{Q}_p$:

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p. \tag{10.6}$$

Example 10.1 Let $p = 3$, $\kappa = 21$, and $\lambda = 45$. Then

$$\begin{aligned} &21 = p + 2p^2; \quad 45 = 2p^2 + p^3; \\ &\frac{21}{45} = p^{-1} \frac{1 + 2p}{2 + p} = p^{-1}(2 + p + 2p^2 + p^3 + p^5 + ...) \\ &\quad = 2p^{-1} + 1 + 2p + p^2 + p^4 + ... \end{aligned} \tag{10.7}$$

10.1.1 Absolute Values of p-adic Numbers

The metric is non-Archimedean. The absolute value of a_p is

$$|a_p|_p = p^{-\mathrm{ord}(a_p)} \tag{10.8}$$

It satisfies the usual properties of the absolute value, and also the property

$$|a_p + b_p|_p \leq \max(|a_p|_p, |b_p|_p), \tag{10.9}$$

which is stronger than the $|a_p + b_p|_p \leq |a_p|_p + |b_p|_p$.

A neighborhood of a_p in Eq. (10.1) is the set of p-adic numbers

$$T_n = \left\{ \sum_{\nu=\mathrm{ord}(a_p)}^{n} \overline{a}_\nu p^\nu + \sum_{\nu=n+1}^{\infty} \overline{b}_\nu p^\nu \right\}, \tag{10.10}$$

with any $\overline{b}_\nu = 0, ..., p-1$. Indeed, if $c_p \in T_n$ then $|c_p - a_p| < p^{-n}$.

The following proposition is by Ostrowski, and we give it without proof:

Proposition 10.1 (Ostrowski) *For a given $a \in \mathbb{Q}$ with $a \neq 0$, let $\{|a|_p\}$ be the set of all its p-adic absolute values, for all $p \in \Pi$. Also let $|a|_\infty$ be the 'usual' absolute value of α. Then*

$$|a|_\infty \prod_{p \in \Pi} |a|_p = 1. \tag{10.11}$$

10.1.2 Additive Characters

If

$$a_p = \sum_{\nu=\mathrm{ord}(a_p)}^{\infty} \overline{a}_\nu p^\nu \tag{10.12}$$

then the characters are given by

$$\begin{aligned} \nu < 0 \quad &\rightarrow \quad \chi_p(a_p) = \exp\left[i2\pi \left(\frac{\overline{a}_\nu}{p^{-\nu}} + ... + \frac{\overline{a}_{-1}}{p} \right) \right] \\ \nu \geq 0 \quad &\rightarrow \quad \chi_p(a_p) = 1. \end{aligned} \tag{10.13}$$

It is seen that if $a_p \in \mathbb{Z}_p$ then $\chi_p(a_p) = 1$.

10.2 $\mathbb{Q}_p/\mathbb{Z}_p$ as the Pontryagin Dual Group of $\mathbb{Z}_p$

The group $\mathbb{Q}_p/\mathbb{Z}_p$ has as elements cosets, represented by

$$\mathfrak{b}_p = \sum_{\nu=\nu_0}^{-1} \overline{b}_\nu p^\nu \tag{10.14}$$

They are fractional p-adic numbers, defined modulo a p-adic integer.

The product $a_p \mathfrak{b}_p$ where $a_p \in \mathbb{Z}_p$ and $\mathfrak{b}_p \in \mathbb{Q}_p/\mathbb{Z}_p$ is also a coset in $\mathbb{Q}_p/\mathbb{Z}_p$. Additive characters are given by

$$\chi_p(a_p \mathfrak{b}_p) = \exp(i2\pi a_p \mathfrak{b}_p). \tag{10.15}$$

Although $\mathfrak{b}_p$ is defined modulo p-adic integers, the character is uniquely defined, because if $c_p \in \mathbb{Z}_p$ then

$$\chi_p[a_p(\mathfrak{b}_p + c_p)] = \chi_p(a_p \mathfrak{b}_p). \tag{10.16}$$

Example 10.2

$$\begin{aligned} a_p &= \overline{a}_0 + \overline{a}_1 p + \overline{a}_2 p^2 + ... \\ \mathfrak{b}_p &= \overline{b}_{-2} p^{-2} + \overline{b}_{-1} p^{-1}, \end{aligned} \tag{10.17}$$

then

$$\chi_p(a_p \mathfrak{b}_p) = \exp\left[i2\pi \left(\frac{\overline{b}_{-2}\overline{a}_0}{p^2} + \frac{\overline{b}_{-1}\overline{a}_0 + \overline{b}_{-2}\overline{a}_1}{p} \right) \right]. \tag{10.18}$$

Definition 10.1 The Prüfer p-group $C(p^\infty)$ is

$$C(p^\infty) = \{\omega_{p^n}(\alpha) | \alpha \in \mathbb{Z}(p^n), n \in \mathbb{Z}^+\} \cong \mathbb{Q}_p/\mathbb{Z}_p \tag{10.19}$$

The $\mathbb{Q}_p/\mathbb{Z}_p$ is isomorphic to the Prüfer p-group $C(p^\infty)$, and the $\mathfrak{a}_p \in \mathbb{Q}_p/\mathbb{Z}_p$ corresponds to $\exp(i2\pi\,\mathfrak{a}_p) \in C(p^\infty)$.

In Eq. (3.2) we have defined the group $C(d)$ for all $d \in \mathbb{N}$. We have now extended this definition to include the supernatural numbers $d = p^\infty$, for all p. Later we will extend this further, and define the group $C(d)$ for all supernatural numbers.

Proposition 10.2 *The Pontryagin dual group to $\mathbb{Z}_p$, is*

$$\widetilde{\mathbb{Z}_p} \cong C(p^\infty) \cong \mathbb{Q}_p/\mathbb{Z}_p. \tag{10.20}$$

Proof The Pontryagin dual group to $\mathbb{Z}_p$, is the group of its characters. The characters in $\mathbb{Z}_p$, are $\chi_p(a_p \mathfrak{b}_p)$, and they are labeled by $\mathfrak{b}_p \in \mathbb{Q}_p/\mathbb{Z}_p$, because as we explained above if we add a p-adic integer to $\mathfrak{b}_p$ we get the same character.

10.3 The Group $\widehat{\mathbb{Z}}$

$\widehat{\mathbb{Z}}$ is the additive group

$$\widehat{\mathbb{Z}} = \prod_{p \in \Pi} \mathbb{Z}_p. \tag{10.21}$$

with elements

$$a = (a_2, ..., a_p, ...); \quad a_p \in \mathbb{Z}_p; \quad p \in \Pi. \tag{10.22}$$

Addition is performed componentwise.

We get an inclusion of $\mathbb{Z}$ into $\widehat{\mathbb{Z}}$

$$\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}, \tag{10.23}$$

where an integer $n \in \mathbb{Z}$ is represented by $(n_2, n_3, n_5, ...) \in \widehat{\mathbb{Z}}$, where n_p is the integer n in the p-adic form (with $p = 2, 3, 5...$).

Example 10.3 The number $n = 13$ is represented in $\widehat{\mathbb{Z}}$ as

$$(1 + p_2^2 + p_2^3, 1 + p_3 + p_3^2, 3 + 2p_5, 6 + p_7, 2 + p_{11}, p_{13}, 13 + 0p_{17}, ...) \tag{10.24}$$

where $p_2 = 2$, $p_3 = 3$, $p_5 = 5$, etc.

10.4 $\mathbb{Q}/\mathbb{Z}$ as the Pontryagin Dual Group of $\widehat{\mathbb{Z}}$

Proposition 10.3 *The group $\mathbb{Q}/\mathbb{Z}$ of rational numbers on a circle, is isomorphic to*

$$\mathbb{Q}/\mathbb{Z} \cong \sum_{p \in \Pi} \mathbb{Q}_p/\mathbb{Z}_p. \tag{10.25}$$

Here $\sum$ denotes the direct sum.

Proof An element of $\mathbb{Q}/\mathbb{Z}$ can be written as κ/λ where κ, λ are coprime integers and $\kappa < \lambda$. We write κ/λ as

$$\frac{\kappa}{\lambda} = \sum_{p \in \Pi(\lambda)} \frac{\kappa_p}{p^{e_p}}; \quad p \in \Pi(\lambda) \tag{10.26}$$

where $\Pi(\lambda)$ is the finite set of of prime numbers which are divisors of λ. We express κ_p/p^{e_p}, in the p-adic form, and then $\frac{\kappa}{\lambda}$ is represented as

$$\begin{aligned} \frac{\kappa}{\lambda} &\rightarrow (\mathfrak{a}_2, ..., \mathfrak{a}_p, ...); \quad \mathfrak{a}_p \in \mathbb{Q}_p/\mathbb{Z}_p \\ p \in \Pi(\lambda) &\rightarrow \mathfrak{a}_p = p^{-e_p}\kappa_p \\ p \notin \Pi(\lambda) &\rightarrow \mathfrak{a}_p = 0 \end{aligned} \tag{10.27}$$

It is seen that only a finite number of the a_p, are non-zero. We express this, by saying that most $\mathfrak{a}_p$ are equal to zero. The term 'most' means, all except from a finite number. Addition is performed componentwise.

Remark 10.1 The direct sum of a finite number of groups, is the same as the direct product. In the direct sum that involves an infinite number of groups, only a finite number of elements are non-zero, whilst in the direct product we do not have such

restriction. Under Pontryagin duality, a direct product of groups becomes a direct sum of their Pontryagin dual groups. For example under Pontryagin duality

$$\widehat{\mathbb{Z}} = \prod_{p \in \Pi} \mathbb{Z}_p \quad \rightarrow \quad \mathbb{Q}/\mathbb{Z} = \sum_{p \in \Pi} \mathbb{Q}_p/\mathbb{Z}_p. \tag{10.28}$$

The $\mathbb{Q}/\mathbb{Z}$ is the direct sum of $\mathbb{Q}_p/\mathbb{Z}_p$ and its elements are represented as $(\mathfrak{a}_2, ..., \mathfrak{a}_p, ...)$, where most $\mathfrak{a}_p$ are equal to zero. This is important for convergence, later.

Example 10.4 The 2/45 can be written as

$$\frac{2}{45} = -\frac{5}{9} + \frac{3}{5} \tag{10.29}$$

Using the notation $p_3 = 3$ and $p_5 = 5$ we get

$$\begin{aligned} \frac{5}{9} &= 2p_3^{-2} + p_3^{-1} \\ -1 &= 2 + 2p_3 + 2p_3^2 + ... \\ -\frac{5}{9} &= p_3^{-2} + p_3^{-1} + 2 + 2p_3 + 2p_3^2 + ... \end{aligned} \tag{10.30}$$

Also

$$\frac{3}{5} = 3p_5^{-1} \tag{10.31}$$

Therefore

$$\frac{2}{45} = (0, p_3^{-2} + p_3^{-1} + 2 + 2p_3 + 2p_3^2 + ..., 3p_5^{-1}, 0, 0, ...) \tag{10.32}$$

10.4.1 Additive Characters

Let

$$\mathfrak{b} = (\mathfrak{b}_2, ..., \mathfrak{b}_p, ...) \in \mathbb{Q}/\mathbb{Z}; \quad a = (a_2, ..., a_p, ...) \in \widehat{\mathbb{Z}}. \tag{10.33}$$

As we explained earlier only a finite number of the $\mathfrak{b}_p$ is different from zero. The product

$$\mathfrak{b}a = (\mathfrak{b}_2 a_2, ..., \mathfrak{b}_p a_p, ...), \tag{10.34}$$

is an element of $\mathbb{Q}/\mathbb{Z}$. Additive characters in $\mathbb{Q}/\mathbb{Z}$ are given by

$$\chi(a\mathfrak{b}) = \prod_{p\in\Pi} \chi_p(a_p\mathfrak{b}_p) \tag{10.35}$$

This converges because most of the $\mathfrak{b}_p$ are equal to zero.

Proposition 10.4 *The Pontryagin dual group to $\widehat{\mathbb{Z}}$, is $\mathbb{Q}/\mathbb{Z}$.*

Proof The characters in $\widehat{\mathbb{Z}}$, are $\chi(a\mathfrak{b})$, and they are labeled by $\mathfrak{b} \in \mathbb{Q}/\mathbb{Z}$.

10.4.2 The Directed-Complete Partial Order of Subgroups of $\mathbb{Q}/\mathbb{Z}$

We extend previous definitions of $C(n)$, $\mathbb{Z}(n)$, to the case where n is any supernatural number.

We first consider the supernatural number $p_1^\infty p_2^\infty$ and define the group $C(p_1^\infty p_2^\infty)$ as the direct sum $C(p_1^\infty) \oplus C(p_2^\infty)$. The elements of this group are $(\mathfrak{a}_{p_1}, \mathfrak{a}_{p_2})$, and they can also be written as $(0, ..., 0, \mathfrak{a}_{p_1}, 0, ..., 0, \mathfrak{a}_{p_2}, 0, ...)$. The latter representation indicates clearly that $C(p_1^\infty p_2^\infty)$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$.

For the supernatural number Υ in Eq. (2.4), we rewrite Eq. (10.25) as

$$C(\Upsilon) = \sum_{p\in\Pi} C(p^\infty) \cong \sum_{p\in\Pi} \mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Q}/\mathbb{Z}. \tag{10.36}$$

For the supernatural number $\mathscr{E}$ in Eq. (2.3),

$$C(\mathscr{E}) = \sum_{p\in\Pi} \mathbb{Z}(p). \tag{10.37}$$

More generally let

$$n = \prod_{p\in S_1} p^{e_p} \times \prod_{p\in S_2} p^\infty \tag{10.38}$$

Here S_1, S_2 are finite or infinite subsets of the set of prime numbers Π, such that $S_1 \cap S_2 = \emptyset$. S_1 is a set of prime numbers for which the exponent is non-zero but finite, and S_2 is a set of prime numbers for which the exponent is infinite. The group $C(n)$ is the direct sum of the groups

$$C(n) = \sum_{p\in S_1} \mathbb{Z}(p^{e_p}) \oplus \sum_{p\in S_2} \mathbb{Q}_p/\mathbb{Z}_p. \tag{10.39}$$

Table 10.1 Some groups G and their Pontryagin dual groups $\widetilde{G}$. All the $\widetilde{G}$ are subgroups of $\mathbb{Q}/\mathbb{Z}$. S_1, S_2 are finite or infinite subsets of the set of prime numbers Π, such that $S_1 \cap S_2 = \emptyset$.

G	$\widetilde{G}$
$\mathbb{Z}(d)$	$C(d) \cong \mathbb{Z}(d)$
$\mathbb{Z}_p = \mathbb{Z}(p^\infty)$	$\mathbb{Q}_p/\mathbb{Z}_p = C(p^\infty)$
$\mathbb{Z}(\mathscr{E}) = \prod_{p\in\Pi} \mathbb{Z}(p)$	$C(\mathscr{E}) = \sum_{p\in\Pi} \mathbb{Z}(p)$
$\prod_{p\in S_1} \mathbb{Z}(p^{e_p}) \times \prod_{p\in S_2} \mathbb{Z}_p$	$\sum_{p\in S_1} \mathbb{Z}(p^{e_p}) \oplus \sum_{p\in S_2} \mathbb{Q}_p/\mathbb{Z}_p$
$\mathbb{Z}(\Upsilon) = \prod_{p\in\Pi} \mathbb{Z}_p \cong \widehat{\mathbb{Z}}$	$C(\Upsilon) = \sum_{p\in\Pi} \mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Q}/\mathbb{Z}$

We have defined the groups $C(n), \mathbb{Z}(n)$ for all supernatural numbers. We consider the set $\mathbb{N}_S^G$

$$\mathbb{N}_S^G = \{C(n) \mid n \in \mathbb{N}_S\} \cong \mathbb{N}_S \tag{10.40}$$

which is isomorphic to $\mathbb{N}_S$. We use the superfix G in the notation to indicate groups. $\mathbb{N}_S^G$ with the order subgroup, is a directed-complete partial order. The $\mathbb{Q}/\mathbb{Z}$ is the supremum in this directed-complete partial order.

The set of finite groups $C(n)$ with $n \in \mathbb{N}$, is a directed partial order which is not complete. By adding to it, groups like those in the second column in table 10.1, we get the set $\mathbb{N}_S^G$ which is a directed-complete partial order.

We also give the Pontryagin duals to these groups. The Pontryagin dual to $C(\mathscr{E})$ is

$$\mathbb{Z}(\mathscr{E}) = \prod_{p\in\Pi} \mathbb{Z}(p). \tag{10.41}$$

As we explained earlier Pontryagin duality changes the direct sum into direct product. The Pontryagin dual to $C(n)$ in Eq. (10.39), is

$$\mathbb{Z}(n) = \prod_{p\in S_1} \mathbb{Z}(p^{e_p}) \times \prod_{p\in S_2} \mathbb{Z}_p. \tag{10.42}$$

These groups are shown in the first column of Table 10.1.

10.5 Inverse and Direct Limits

In the rest of this chapter we approach the profinite groups as inverse limits and their Pontryagin dual groups as direct limits. General references are [8] on inverse and direct limits, and [5–7] on their use in the context of profinite groups.

We consider the groups $\mathbb{Z}(p^e)$ with $e = 1, 2, ...$ The inverse limit shows that for 'large' e, we get the profinite group $\mathbb{Z}_p$ of p-adic integers. Profinite groups are Hausdorff, compact and totally disconnected topological groups.

We also consider their Pontryagin dual groups $\widetilde{\mathbb{Z}}(p^e) \cong \mathbb{Z}(p^e)$ (these groups are self-dual). The direct limit shows that for 'large' e, we get the group $\mathbb{Q}_p/\mathbb{Z}_p$ of fractional p-adic numbers, which is Pontryagin dual to $\mathbb{Z}_p$. Using both the inverse limit on a sequence of finite groups, and the direct limit on the corresponding sequence of their Pontryagin dual groups, ensures that we get two groups, which are Pontryagin dual to each other. Pontryagin duality is important in our case, because we want to use these groups for positions and momenta in quantum mechanics.

We also consider the groups $\mathbb{Z}(d)$ with $d = 1, 2, ...$ The inverse limit shows that for 'large' d, we get the profinite group $\widehat{\mathbb{Z}}$. The direct limit of their Pontryagin dual groups $\widetilde{\mathbb{Z}}(d) \cong \mathbb{Z}(d)$, shows that for 'large' d, we get the group $\mathbb{Q}/\mathbb{Z}$ of rational numbers on a circle, which is Pontryagin dual to $\widehat{\mathbb{Z}}$.

The formalism leads to a partial order, where smaller groups are embedded into larger groups. These embeddings will be used later to define embeddings of smaller quantum systems into larger ones.

10.6 The Profinite Group $\mathbb{Z}_p$ as Inverse Limit

We consider the set of the groups $\{\mathbb{Z}(p^e)\}$. The exponents e belong to $\mathbb{N}$ which is a chain with the usual order. We regard these groups, as additive topological groups with the discrete topology (i.e. all their subsets are open sets). We use Greek letters α_{p^n}, for the elements of $\mathbb{Z}(p^n)$.

For $k \leq n$ we define the continuous homomorphisms [5–7]:

$$\varphi_{kn} : \mathbb{Z}(p^k) \leftarrow \mathbb{Z}(p^n), \tag{10.43}$$

where

$$\varphi_{kn}(\alpha_{p^n}) = \alpha_{p^k}; \quad \alpha_{p^n} = \alpha_{p^k} (\text{mod } p^k). \tag{10.44}$$

These homomorphisms are compatible:

$$\begin{aligned} &k \leq n \leq r \quad \rightarrow \quad \varphi_{kn} \circ \varphi_{nr} = \varphi_{kr} \\ &\varphi_{kk} = \mathbf{1} \end{aligned} \tag{10.45}$$

The $\{\mathbb{Z}(p^\ell), \varphi_{k\ell}\}$ is an inverse system with inverse limit the $\mathbb{Z}_p$:

$$\varprojlim \mathbb{Z}(p^\ell) = \mathbb{Z}_p. \tag{10.46}$$

The elements of the inverse limit of this inverse system are the sequences

$$a_p = (\alpha_p, \alpha_{p^2}, ...) \tag{10.47}$$

where the α_{p^n} obey Eq. (10.44). Addition and multiplication, are componentwise.

We have seen earlier the following representation of p-adic integers:

$$a_p = \overline{a}_0 + \overline{a}_1 p + \overline{a}_2 p^2 + ... \tag{10.48}$$

The correspondence between the two representations is

$$\begin{aligned} &\alpha_p = \overline{a}_0 \\ &\alpha_{p^2} = \overline{a}_0 + \overline{a}_1 p \\ &\alpha_{p^3} = \overline{a}_0 + \overline{a}_1 p + \overline{a}_2 p^2 \\ &..... \end{aligned} \tag{10.49}$$

These relations define projections ξ_k from $\mathbb{Z}_p$ to $\mathbb{Z}(p^k)$, which are truncations given by

$$a_p \quad \rightarrow \quad \xi_k(a_p) = \alpha_{p^k} = \sum_{\nu=0}^{k-1} \overline{a}_\nu p^\nu. \tag{10.50}$$

The projections are compatible with the homomorphisms φ_{kn}. It is easily seen that

$$k \leq n \quad \rightarrow \quad \varphi_{kn} \circ \xi_n = \xi_k \tag{10.51}$$

Remark 10.2 In the language of inverse limits, the character $\chi_p(c_p)$, is the sequence

$$\begin{aligned} &\chi_p(c_p) = (\omega_p(\gamma_p), \omega_{p^2}(\gamma_{p^2}), ...); \quad \gamma_{p^k} \in \mathbb{Z}(p^k) \\ &c_p = (\gamma_p, \gamma_{p^2}, ...) \in \mathbb{Z}_p \\ &n \geq k \quad \rightarrow \quad \omega_{p^n}(\gamma_{p^n}) = \omega_{p^k}(\gamma_{p^k}). \end{aligned} \tag{10.52}$$

10.6.1 $\mathbb{Z}_p$ as a Compact and Totally Disconnected Topological Group

As a profinite group $\mathbb{Z}_p$ is a Hausdorff, compact and totally disconnected topological group [5–7]. A fundamental system of neighbourhoods of 0 for $\mathbb{Z}_p$ is a

$$\mathbb{Z}_p \succ p\mathbb{Z}_p \succ p^2\mathbb{Z}_p \succ ..., \tag{10.53}$$

where $\prec$ indicates subset. This topology is the same as the topology endowed by the p-adic metric in Eq. (10.8).

10.7 $\mathbb{Q}_p/\mathbb{Z}_p$ as Direct Limit

Above we discussed the inverse limit of the groups $\{\mathbb{Z}(p^n)\}$, and we now discuss the direct limit of their Pontryagin dual groups, which are also $\{\mathbb{Z}(p^n)\}$ (they are self-dual). As in the previous section, we use Greek letters α_{p^k} for the elements of $\mathbb{Z}(p^k)$.

For $k \leq n$ we define the homomorphisms [5–7]:

$$\Phi_{kn} : \mathbb{Z}(p^k) \rightarrow \mathbb{Z}(p^n), \tag{10.54}$$

where

$$\Phi_{kn}(\alpha_{p^k}) = \alpha_{p^n}; \qquad \alpha_{p^n} = p^{n-k}\alpha_{p^k} \tag{10.55}$$

The $\mathbb{Z}(p^k)$ is a subgroup of $\mathbb{Z}(p^n)$, and for a given element in $\mathbb{Z}(p^k)$ the homomorphism defines the corresponding element in $\mathbb{Z}(p^n)$. These homomorphisms are compatible:

$$\begin{aligned} &k \leq n \leq r \quad \rightarrow \quad \Phi_{nr} \circ \Phi_{kn} = \Phi_{kr} \\ &\Phi_{nn} = \mathbf{1}. \end{aligned} \tag{10.56}$$

The $\{\mathbb{Z}(p^n), \Phi_{kn}\}$ is a direct system with direct limit

$$\varinjlim \mathbb{Z}(p^\ell) \cong \mathbb{Q}_p/\mathbb{Z}_p \cong C(p^\infty). \tag{10.57}$$

There exist homomorphisms Ξ_n from $\mathbb{Z}(p^n)$ to $\mathbb{Q}_p/\mathbb{Z}_p$

$$\Xi_n(\alpha_{p^n}) = p^{-n}\alpha_{p^n}, \tag{10.58}$$

which are compatible in the sense that

$$k \leq n \quad \rightarrow \quad \Xi_n \circ \Phi_{kn} = \Xi_k. \tag{10.59}$$

The direct limit is the disjoint union of all $\mathbb{Z}(p^n)$, modulo an equivalence relation $\sim$, which identifies $\alpha_{p^k} \in \mathbb{Z}(p^k)$ with $\alpha_{p^k} p^{n-k} \in \mathbb{Z}(p^n)$:

$$\varinjlim \mathbb{Z}(p^\ell) = \bigsqcup_n \mathbb{Z}(p^n)/\sim \cong \mathbb{Q}_p/\mathbb{Z}_p \cong C(p^\infty). \tag{10.60}$$

As a topological group $\mathbb{Q}_p/\mathbb{Z}_p$ is discrete (because it is Pontryagin dual to the compact group $\mathbb{Z}_p$).

Remark 10.3 If instead of the $\mathbb{Z}(p^k)$, $\mathbb{Q}_p/\mathbb{Z}_p$, we work with the $C(p^k)$, $C(p^\infty)$ which are isomorphic to them, then the homomorphism Φ_{kn} from $C(p^k)$ to $C(p^n)$ becomes

$$\Phi_{kn}[\omega_{p^k}(\alpha_{p^k})] = \omega_{p^n}(\alpha_{p^n}); \quad \omega_{p^n}(\alpha_{p^n}) = \omega_{p^k}(\alpha_{p^k}), \tag{10.61}$$

and the homomorphism Ξ_n from $C(p^n)$ to $C(p^\infty)$, becomes

$$\Xi_n[\omega_{p^n}(\alpha_{p^n})] = \omega_{p^n}(\alpha_{p^n}). \tag{10.62}$$

In this language

$$C(p^\infty) = \bigsqcup_n C(p^n)/\sim, \tag{10.63}$$

where the equivalence relation $\sim$, identifies $\omega_{p^k}(\alpha)$ with $\omega_{p^n}(\beta)$, when they are equal.

10.8 A Complete Chain of Pontryagin Dual Pairs of Groups

We consider the set $\mathbb{N}_S^{(G,\widetilde{G})}(p)$

$$\begin{aligned}\mathbb{N}_S^{(G,\widetilde{G})}(p) &= \{(\mathbb{Z}(p), C(p)), (\mathbb{Z}(p^2), C(p^2)), ..., (\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)\} \\ &\cong \mathbb{N}_S(p)\end{aligned} \tag{10.64}$$

which is isomorphic to $\mathbb{N}_S(p)$ in Eq. (2.6). We use the superfix $(G, \widetilde{G})$ in the notation to indicate Pontryagin dual pairs of groups. The total order divisibility in $\mathbb{N}_S(p)$, induces a total order in $\mathbb{N}_S^{(G,\widetilde{G})}(p)$, and makes it a complete chain of Pontryagin dual pairs of groups. For the second groups in the pairs, this order is 'subgroup':

$$C(p) \prec C(p^2) \prec ... \prec C(p^\infty) \cong \mathbb{Q}_p/\mathbb{Z}_p. \tag{10.65}$$

This endows an order for the first groups in the pairs

$$\mathbb{Z}(p) \prec \mathbb{Z}(p^2) \prec ... \prec \mathbb{Z}_p, \tag{10.66}$$

as discussed in a general context, in Sect. 2.3.

The $(\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)$ is the supremum of this chain. We added it, so that the chain is complete. In this sense the $(\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)$ are the 'universe' for all the $(\mathbb{Z}(p^n), C(p^n))$ with all $p^n \in \mathbb{N}_S(p)$. The inverse and direct limits made rigorous this intuitive concept

of 'universe'. We do need both inverse and direct limit, because they lead to groups which are Pontryagin dual to each other. Later, these pairs of groups will be used for quantum systems with positions in the first group of the pair, and momenta in the second group of the pair.

10.9 The Profinite Group $\widehat{\mathbb{Z}}$ as Inverse Limit

We consider the additive topological groups $\{\mathbb{Z}(n)\}$ with the discrete topology. Here n belongs to $\mathbb{N}$ which is a directed partially ordered set, with divisibility as a partial order. We use the Greek letter α_k for elements of $\mathbb{Z}(k)$.

If k is a divisor of n ($k \prec n$) we define the continuous homomorphisms:

$$\psi_{kn} : \mathbb{Z}(k) \leftarrow \mathbb{Z}(n); \quad k \prec n, \tag{10.67}$$

where

$$\psi_{kn}(\alpha_n) = \alpha_k; \quad \alpha_n = \alpha_k (\text{mod } k); \quad k \prec n. \tag{10.68}$$

These homomorphisms are compatible:

$$\begin{aligned} &k \prec n \prec r \quad \rightarrow \quad \psi_{kn} \circ \psi_{nr} = \psi_{kr} \\ &\psi_{kk} = \mathbf{1}. \end{aligned} \tag{10.69}$$

The $\{\mathbb{Z}(n), \psi_{kn}\}$ is an inverse system and we call $\widehat{\mathbb{Z}}$ its inverse limit

$$\varprojlim \mathbb{Z}(\ell) = \widehat{\mathbb{Z}}. \tag{10.70}$$

Its elements can be represented as sequences

$$a = (\alpha_1, \alpha_2, ...); \quad \alpha_n = \alpha_k (\text{mod } k); \quad k \prec n, \tag{10.71}$$

and addition and multiplication are performed componentwise. We next show that this representation of these elements, is equivalent to the representation in Eq. (10.22).

The Chinese remainder theorem shows that a number is defined uniquely by its remainders (with respect to coprime integers). Since $\alpha_n = \alpha_k (\text{mod } k)$ for $k \prec n$, it follows that the elements with indices which are powers of primes, define uniquely the sequence (the rest of the elements are not needed). We then write the sequence $(\alpha_p, \alpha_{p^2}, ...)$ as a single p-adic integer a_p (see Eq. (10.47)). We do this for all primes, and we get the representation in Eq. (10.22).

There exist projections π_n from $\widehat{\mathbb{Z}}$ to $\mathbb{Z}(n)$, as follows. If

$$n = p_1^{e_1} ... p_r^{e_r}, \tag{10.72}$$

then the $a = (a_2, a_3, a_5, ...) \in \widehat{\mathbb{Z}}$ is mapped into

$$\pi_n(a) = \xi_{e_1}(a_{p_1})...\xi_{e_r}(a_{p_r}). \tag{10.73}$$

The projections (truncations) in Eq. (10.50) are used here. These projections are compatible with the ψ_{nr}:

$$n \prec r \quad \rightarrow \quad \psi_{nr} \circ \pi_r = \pi_n \tag{10.74}$$

Remark 10.4 In the language of inverse limits, the character $\chi(c)$, is the sequence

$$\begin{aligned} &\chi(c) = (\omega_1(\gamma_1), \omega_2(\gamma_2), ...); \quad \gamma_k \in \mathbb{Z}(k) \\ &c = (\gamma_1, \gamma_2, ...) \in \widehat{\mathbb{Z}} \\ &k \prec n \ \rightarrow \ \omega_n(\gamma_n) = \omega_k(\gamma_k). \end{aligned} \tag{10.75}$$

Only the elements with indices which are powers of primes are need to define uniquely these sequences. This follows from the Chinese remainder theorem. Consequently, we rewrite $\chi(c)$, as the sequence

$$\begin{aligned} &\chi(c) = (\chi_2(c_2), \chi_3(c_3), \chi_5(c_5), ...); \quad c = (c_2, c_3, ...) \\ &c \in \widehat{\mathbb{Z}}; \quad c_p \in \mathbb{Z}_p. \end{aligned} \tag{10.76}$$

10.9.1 $\widehat{\mathbb{Z}}$ as a Compact and Totally Disconnected Topological Group

As a profinite group, $\widehat{\mathbb{Z}}$ is Hausdorff, compact and totally disconnected topological group [5–7]. The

$$n\widehat{\mathbb{Z}} \cong \prod_{p \in \Pi} p^{e_p}\mathbb{Z}_p; \quad n = \prod_{p \in \Pi} p^{e_p} \in \mathbb{N}, \tag{10.77}$$

are a fundamental system of neighbourhoods of 0. If n is a divisor of m then $m\widehat{\mathbb{Z}}$ is a subset of $n\widehat{\mathbb{Z}}$:

$$n \prec m \ \rightarrow \ n\widehat{\mathbb{Z}} \succ m\widehat{\mathbb{Z}}; \quad n, m \in \mathbb{N}, \tag{10.78}$$

The $n\widehat{\mathbb{Z}} \cong \prod_{p \in \Pi} p^{e_p}\mathbb{Z}_p$ is a product of an infinite number of topological groups, and it has the product (Tychonoff) topology. If V_p is an open sets in $\mathbb{Z}_p$, then the open sets in $\widehat{\mathbb{Z}}$ are $\prod V_p$ where $V_p = \mathbb{Z}_p$ for most p. This is indeed the case, because most of the e_p are zero. We have explained earlier, that 'most' means 'all except a finite number'.

10.10 $\mathbb{Q}/\mathbb{Z}$ as Direct Limit

Above we discussed the inverse limit of the groups $\{\mathbb{Z}(n)\}$, and we now discuss the direct limit of their Pontryagin dual groups, which are isomorphic to $\{\mathbb{Z}(n)\}$. As above, we use the Greek letter α_n for elements of $\mathbb{Z}(n)$. If k is a divisor of n ($k \prec n$) we define the homomorphisms:

$$\Psi_{kn} : \mathbb{Z}(k) \rightarrow \mathbb{Z}(n); \quad k \prec n, \tag{10.79}$$

where

$$\Psi_{kn}(\alpha_k) = \alpha_n; \quad \alpha_n = \frac{n}{k}\alpha_k. \tag{10.80}$$

The $\mathbb{Z}(k)$ is a subgroup of $\mathbb{Z}(n)$, and for a given element in $\mathbb{Z}(k)$ the homomorphism defines the corresponding element in $\mathbb{Z}(n)$. These homomorphisms are compatible

$$\begin{aligned} &k \prec n \prec r \quad \rightarrow \quad \Psi_{nr} \circ \Psi_{kn} = \Psi_{kr} \\ &\Psi_{kk} = \mathbf{1}. \end{aligned} \tag{10.81}$$

The $\{\mathbb{Z}(k), \Psi_{k\ell}\}$ is a direct system with direct limit

$$\varinjlim \mathbb{Z}(k) = \mathbb{Q}/\mathbb{Z}. \tag{10.82}$$

We next define homomorphisms Π_n from $\mathbb{Z}(n)$ to $\mathbb{Q}/\mathbb{Z}$, where

$$\Pi_n(\alpha_n) = \frac{\alpha_n}{n} = (\mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_5, ...). \tag{10.83}$$

In Eq. (10.27) we have explained how to represent the rational number α_n/n as $(\mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_5, ...)$, and we gave Example 10.4. The Π_n are compatible in the sense that

$$n \prec r \quad \rightarrow \quad \Pi_r \circ \Psi_{nr} = \Pi_n. \tag{10.84}$$

As a topological group $\mathbb{Q}/\mathbb{Z}$ is discrete (because it is Pontryagin dual to the compact group $\widehat{\mathbb{Z}}$).

10.11 A Directed-Complete Partial Order of Pontryagin Dual Pairs of Groups

We consider the set $\mathbb{N}_S^{(G,\widetilde{G})}$

$$\mathbb{N}_S^{(G,\widetilde{G})} = \{(\mathbb{Z}(n), C(n)) \mid n \in \mathbb{N}_S\} \cong \mathbb{N}_S \tag{10.85}$$

which is isomorphic to $\mathbb{N}_S$. We use the superfix $(G, \widetilde{G})$ in the notation to indicate Pontryagin dual pairs of groups. We have defined earlier (in Sect. 10.4.2) the groups $\mathbb{Z}(n)$, $C(n)$ for all supernatural numbers n.

The partial order divisibility in $\mathbb{N}_S$, induces a partial order in $\mathbb{N}_S^{(G,\widetilde{G})}$. For the second groups in the pairs, this order is 'subgroup'. The corresponding order for the first elements of the pairs involves quotients of the annihilators, as discussed in Sect. 2.3.

$\mathbb{N}_S^{(G,\widetilde{G})}$ with this order, is a directed-complete partial order of Pontryagin dual pairs of groups. The $(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})$ is the supremum in this directed-complete partial order.

References

1. Weil, A. (1973). *Basic number theory*. Berlin: Springer.
2. Koblitz, N. (1984). *p-adic numbers, p-adic analysis, and zeta functions*. New York: Springer.
3. Gouvea, F. Q. (1993). *p-adic numbers*. Berlin: Springer.
4. Robert, A. M. (2000). *A course in p-adic analysis*. Berlin: Springer.
5. Ribes, L., & Zalesskii, P. (2000). *Profinite groups*. Berlin: Springer.
6. Wilson, J. (1998). *Profinite groups*. Oxford: Clarendon.
7. Klopsch, B., Nikolov, N., & Voll, C. (2011). *Lectures on profinite topics in group theory*. Cambridge: Cambridge University Press.
8. Bourbaki, N. (1970). *Algebra I*. New York: Springer.

Chapter 11
A Quantum System with Positions in the Profinite Group $\mathbb{Z}_p$

Abstract Quantum systems with positions in $\mathbb{Z}_p$ and momenta in $\mathbb{Q}_p/\mathbb{Z}_p$, are discussed. The Schwartz-Bruhat space of wavefunctions in these systems, is presented. The Heisenberg-Weyl group as a locally compact and totally disconnected topological group, is discussed. Wigner and Weyl functions in this context, are also discussed.

In a mathematical context, there is a lot of work on functional analysis on p-adic numbers[1–6], and on wavelets with p-adic numbers [7–12]. There is also a lot of work on various problems in mathematical physics with p-adic numbers [13–32]. Work on condensed matter with p-adic numbers is discussed in [33–36], on particle physics and string theory in [37–41], and on path-integrals in [22, 42]. The use of p-adic numbers in classical computation is discussed in [43].

In this chapter we discuss the quantum system $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, with positions in the profinite group $\mathbb{Z}_p$, and momenta in its Pontryagin dual group $\mathbb{Q}_p/\mathbb{Z}_p$. Intuitively $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ is the system $\Sigma[\mathbb{Z}(p^e)]$, with $e = \infty$. All finite systems $\Sigma[\mathbb{Z}(p^e)]$, are subsystems of $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$.

The set of the systems $\Sigma[\mathbb{Z}(p^e)]$ where $e \in \mathbb{N}$, with the order subsystem, is a chain. This chain is not complete, but when we add the 'top element' $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, it becomes complete.

This chapter belongs to the general area of p-adic physics, but we approach this area from a novel angle. We use inverse and direct limits and profinite groups, to provide a rigorous approach to study of the systems $\Sigma[\mathbb{Z}(p^e)]$, with very large e.

11.1 Locally Constant Functions with Compact Support

We define the concepts of locally constant functions (at small distances) and functions with compact support (at large distances). They reduce the integrals into finite sums, and ensure convergence.

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_11

Definition 11.1 A complex function $f_p(a_p)$ with $a_p \in \mathbb{Q}_p$, is locally constant with degree n, if $f_p(a_p + b_p) = f_p(a_p)$ for all $|b_p|_p \leq p^{-n}$. Such a function is effectively defined on $\mathbb{Q}_p/p^n\mathbb{Z}_p$. We denote this as

$$\mathbf{LC}[f_p(a_p)] = n. \tag{11.1}$$

Definition 11.2 A complex function $f_p(a_p)$ with $a_p \in \mathbb{Q}_p$, has compact support with degree k, if $f_p(a_p) = 0$ for all $|a_p|_p > p^k$. Such a function is effectively defined on $p^{-k}\mathbb{Z}_p$. We denote this as

$$\mathbf{CS}[f_p(a_p)] = k. \tag{11.2}$$

Notation 11.1 *We use the notation $\mathscr{A}_p(k, n)$ for the set of functions*

$$\mathscr{A}_p(k, n) = \{f_p(a_p) \mid \mathbf{CS}[f_p(a_p)] \leq k \text{ and } \mathbf{LC}[f_p(a_p)] \leq n\}. \tag{11.3}$$

We also use the notation

$$\mathscr{A}_p(k, *) = \bigcup_n \mathscr{A}_p(k, n); \quad \mathscr{A}_p(*, n) = \bigcup_k \mathscr{A}_p(k, n); \quad \mathscr{A}_p = \bigcup_{k,n} \mathscr{A}_p(k, n). \tag{11.4}$$

The star in $\mathscr{A}_p(k, *)$ indicates that n can take any finite value, and similarly for $\mathscr{A}_p(*, n)$.

Clearly $\mathscr{A}_p(k_1, n_1) \subseteq \mathscr{A}_p(k_2, n_2)$ if $k_1 \leq k_2$ and $n_1 \leq n_2$.

Remark 11.1
- All functions $f_p(\mathfrak{a}_p)$ with $\mathfrak{a}_p \in \mathbb{Q}_p/\mathbb{Z}_p$ have $\mathbf{LC}[f_p(a_p)] = 0$, and therefore they belong to $\mathscr{A}_p(*, 0)$. These functions obey the relation $f_p(\mathfrak{a}_p) = f_p(\mathfrak{a}_p + 1)$.
- All functions $f_p(a)$ with $a_p \in \mathbb{Z}_p$ have $\mathbf{CS}[f_p(a_p)] = 0$, and therefore they belong to $\mathscr{A}_p(0, *)$.
- A function with $\mathbf{LC}[f_p(a_p)] = n$ and $\mathbf{CS}[f_p(a_p)] = k$, is effectively defined on $p^{-k}\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}(p^{n+k})$, and it can be represented as a p^{n+k}-dimensional vector.

11.2 Integrals of Complex Functions on $\mathbb{Q}_p$

Integrals of complex functions over $\mathbb{Q}_p$ use the Haar measure, with the normalization:

$$\int_{\mathbb{Z}_p} da_p = 1. \tag{11.5}$$

The integral over $\mathbb{Q}_p$, of a function $f_p(a_p) \in \mathscr{A}_p(k, n)$, is given by

$$\int_{\mathbb{Q}_p} f_p(a_p)da_p = p^{-n}\sum f_p(\overline{a}_{-k}p^{-k} + ... + \overline{a}_{n-1}p^{n-1}). \tag{11.6}$$

The sum is over all $\overline{a}_{-k}, ..., \overline{a}_{n-1}$. It is a finite sum with p^{n+k} terms, and therefore it converges. The fact that $\mathbf{LC}[f_p(a_p)] = n$, ensures that if we truncate the sum at $n + m \geq n$, we get the same result:

$$\begin{aligned} &p^{-(n+m)}\sum f_p(\overline{a}_{-k}p^{-k} + ... + \overline{a}_{n+m-1}p^{n+m-1}) \\ &= p^{-n}\sum f_p(\overline{a}_{-k}p^{-k} + ... + \overline{a}_{n-1}p^{n-1}). \end{aligned} \tag{11.7}$$

The fact that $\mathbf{CS}[f_p(a_p)] = k$, ensures that if we truncate the sum at $k + m > k$, we get the same result :

$$\begin{aligned} &p^{-n}\sum f_p(\overline{a}_{-(k+m)}p^{-(k+m)} + ... + \overline{a}_{n+m-1}p^{n-1}) \\ &= p^{-n}\sum f_p(\overline{a}_{-k}p^{-k} + ... + \overline{a}_{n-1}p^{n-1}). \end{aligned} \tag{11.8}$$

The following proposition is helpful if we want to change variables.

Proposition 11.1 *Let $f_p(a_p)$ where $a_p \in \mathbb{Q}_p$, be a complex function in $\mathscr{A}_p(k, n)$. Also let $F_p(a_p) = f_p(\lambda a_p)$, where $|\lambda|_p = p^s$. Then:*

(1) The function $F_p(a_p)$ belongs to $\mathscr{A}_p(k - s, n + s)$.
(2)

$$\int_{\mathbb{Q}_p} f_p(a_p)da_p = p^s\int_{\mathbb{Q}_p} F_p(a_p)da_p \tag{11.9}$$

If we call $a'_p = \lambda a_p$, then we can express this as

$$da'_p = |\lambda|_p da_p. \tag{11.10}$$

If λ, p are coprime then $da'_p = da_p$. If $\lambda = p$, then $d(pa_p) = p^{-1}da_p$.

Proof (1) The function $f_p(a_p)$ has $\mathbf{LC}[f_p(a_p)] = n$, and therefore

$$F_p(a_p + b_p) = f_p(\lambda a_p + \lambda b_p) = f_p(\lambda a_p) \text{ if } |\lambda b_p|_p \leq p^{-n}. \tag{11.11}$$

This gives $|b_p|_p \leq p^{-n-s}$, and therefore the function $F_p(a_p)$ has $\mathbf{LC}[F_p(a_p)] = n + s$.
The function $f_p(a_p)$ has $\mathbf{CS}[f_p(a_p)] = k$, and therefore

$$F_p(a_p) = f_p(\lambda a_p) = 0 \text{ if } |\lambda a_p|_p > p^k. \tag{11.12}$$

This gives $|a_p|_p > p^{k-s}$. Therefore the function $F_p(a_p)$ has $\mathbf{LC}[F_p(a_p)] = k - s$.

(2) The integral for the function $f_p(a_p) \in \mathscr{A}_p(k, n)$, has the prefactor is p^{-n} in Eq.(11.6). The integral for the function $F_p(a_p) \in \mathscr{A}_p(k-s, n+s)$, has the prefactor is p^{-n-s}, and it needs to be 'corrected' with multiplication by p^s. It is seen that the p^s in Eq.(11.9) (or the $|\lambda|_p$ in Eq.(11.10)), compensate the change in the degrees of local constancy and compact support in the function $F_p(a_p)$, which affects the prefactor in Eq.(11.6).
If λ, p are coprime then $|\lambda|_p = 1$.

Example 11.1 For $p = 3$, we consider the following function in $\mathscr{A}_3(0, 2)$:

$$\begin{aligned}
&f_p(0 + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 1 - i \\
&f_p(1 + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 2 \\
&f_p(2 + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 2 + i \\
&f_p(0 + p + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = -1 \\
&f_p(1 + p + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 0 \\
&f_p(2 + p + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 1 - i \\
&f_p(0 + 2p + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 1 - i \\
&f_p(1 + 2p + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 2 \\
&f_p(2 + 2p + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 2 + i
\end{aligned} \tag{11.13}$$

Also for $\overline{a}_{-k} \neq 0$ with $k > 0$, we get

$$f_p(\overline{a}_{-k} p^{-k} + \overline{a}_{-k+1} p^{-k+1} + \cdots) = 0. \tag{11.14}$$

In this case

$$\int_{\mathbb{Q}_p} f_p(a_p) da_p = \frac{1}{9}(10 - i). \tag{11.15}$$

11.3 Integrals of Complex Functions on $\mathbb{Q}_p/\mathbb{Z}_p$ and Weil Transforms

Let $g_p(\mathfrak{p}_p)$ be a complex function of $\mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p$, with $\mathbf{CS}[g_p(\mathfrak{p}_p)] = k$. We have explained earlier that such a function belongs to $\mathscr{A}_p(k, 0)$. Its integral over $\mathbb{Q}_p/\mathbb{Z}_p$ is

$$\int_{\mathbb{Q}_p/\mathbb{Z}_p} g_p(\mathfrak{p}_p) d\mathfrak{p}_p = \sum g_p \left(\overline{p}_{-k} p^{-k} + \overline{p}_{-k+1} p^{-k+1} + ... + \overline{p}_{-1} p^{-1} \right). \tag{11.16}$$

The counting measure is used here.

The $\mathfrak{p}_p$ are cosets and we represented them with the element that has zero integer part. If we represent them with elements that have non-zero integer part, we get the

same result. Indeed, let $c_p = \mathfrak{p}_p + b_p \in \mathbb{Q}_p$, where $b_p \in \mathbb{Z}_p$. The function $g_p(\mathfrak{p}_p)$ assigns a single complex value to each coset $\mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p$, and this implies that $g_p(\mathfrak{p}_p + b_p) = g_p(\mathfrak{p}_p)$. We rewrite the above integral as an integral over $\mathbb{Q}_p$, as

$$\begin{aligned}\int_{\mathbb{Q}_p} dc_p g_p(c_p) &= \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \int_{\mathbb{Z}_p} db_p\ g_p(\mathfrak{p}_p + b_p)\\ &= \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p\ g_p(\mathfrak{p}_p) \int_{\mathbb{Z}_p} db_p = \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p\ g_p(\mathfrak{p}_p). \qquad (11.17)\end{aligned}$$

The counting measure for integration over $\mathbb{Q}_p/\mathbb{Z}_p$ ensures that this relation holds.

More generally let $g_p(\mathfrak{p}_p)$ be a complex function of $\mathfrak{p}_p \in \mathbb{Q}_p/p^{-s}\mathbb{Z}_p$, with $\mathbf{CS}[g_p(\mathfrak{p}_p)] = k$. Such a function belongs to $\mathscr{A}_p(k, -s)$, and its integral over $\mathbb{Q}_p/p^{-s}\mathbb{Z}_p$, is

$$\begin{aligned}&\int_{\mathbb{Q}_p/p^{-s}\mathbb{Z}_p} g_p(\mathfrak{p}_p)d\mathfrak{p}_p\\ &= p^s \sum g_p\left(\overline{p}_{-k}p^{-k} + \overline{p}_{-k+1}p^{-k+1} + ... + \overline{p}_{-s-1}p^{-s-1}\right)\\ &= \sum g_p\left(\overline{p}_{-k}p^{-k} + \overline{p}_{-k+1}p^{-k+1} + ... + \overline{p}_{-s-1}p^{-s-1} + ... + \overline{p}_{-1}p^{-1}\right) \qquad (11.18)\end{aligned}$$

Here the function g_p does not depend on $\overline{p}_{-s}$, ..., $\overline{p}_{-1}$ and this gives the prefactor p^s in the second expression.

Proposition 11.2 *Change of the variable $\mathfrak{p}_p$ into $\mathfrak{p}'_p = \lambda\mathfrak{p}_p$, is performed with the relation*

$$|\lambda|_p \int_{\mathbb{Q}_p/|\lambda|_p\mathbb{Z}_p} g_p(\lambda\mathfrak{p}_p)d\mathfrak{p}_p = \int_{\mathbb{Q}_p/\mathbb{Z}_p} g_p(\mathfrak{p}'_p)d\mathfrak{p}'_p. \qquad (11.19)$$

Therefore

$$d\mathfrak{p}'_p = |\lambda|_p d\mathfrak{p}_p. \qquad (11.20)$$

If λ, p are coprime then $|\lambda|_p = 1$. If $\lambda = p$, then $d(p\mathfrak{p}_p) = p^{-1}d\mathfrak{p}_p$.

Proof We first point out that if $\mathfrak{p}_p \in \mathbb{Q}_p/|\lambda|_p\mathbb{Z}_p$, then $\mathfrak{p}'_p = \lambda\mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p$. Therefore the domain of integration changes.

Equation (11.19) follows from Eq.(11.18). The $|\lambda|_p$ 'corrects' the prefactor, as already discussed in the proof of Proposition 11.1.

Example 11.2 For $p = 2$, we consider the following function in $\mathscr{A}_2(2, 0)$, which is described with 4 complex values:

$$\begin{aligned} &g_p(p^{-2} + \overline{a}_0 + \overline{a}_1 p + ...) = 1 - i \\ &g_p(p^{-2} + p^{-1} + \overline{a}_0 + \overline{a}_1 p + ...) = 2 \\ &g_p(p^{-1} + \overline{a}_0 + \overline{a}_1 p + ...) = 2 - i \\ &g_p(\overline{a}_0 + \overline{a}_1 p + ...) = -1 \end{aligned} \tag{11.21}$$

Also for $\overline{a}_{-k} \neq 0$ with $k > 2$, we get

$$g_p(\overline{a}_{-k} p^{-k} + \overline{a}_{-k+1} p^{-k+1} + ...) = 0. \tag{11.22}$$

In this example

$$\int_{\mathbb{Q}_p/\mathbb{Z}_p} g_p(\mathfrak{p}_p) d\mathfrak{p}_p = 4 - 2i. \tag{11.23}$$

11.3.1 Weil Transforms

Given a function $F_p(c_p)$ with $c_p \in \mathbb{Q}_p$, which is locally constant and has compact support, we express c_p as $c_p = \mathfrak{p}_p + b_p$, where $\mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p$ and $b_p \in \mathbb{Z}_p$. The Weil transform [44], maps the function $F_p(c_p)$ in $\mathbb{Q}_p$, into the following function in $\mathbb{Q}_p/\mathbb{Z}_p$:

$$f(\mathfrak{p}_p) = \int_{\mathbb{Z}_p} F_p(\mathfrak{p}_p + b_p) db_p. \tag{11.24}$$

We note that for any $e_p \in \mathbb{Z}_p$, we get $f(\mathfrak{p}_p) = f(\mathfrak{p}_p + e_p)$. Then

$$\int_{\mathbb{Q}_p/\mathbb{Z}_p} f(\mathfrak{p}_p) d\mathfrak{p}_p = \int_{\mathbb{Q}_p} F_p(c_p) dc_p. \tag{11.25}$$

Example 11.3 For $p = 2$, we consider the following function on $\mathbb{Q}_p$, which belongs to $\mathscr{A}_2(1, 2)$:

$$\begin{aligned} &F_p(p^{-1} + 1 + p + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 1 \\ &F_p(0p^{-1} + 1 + p + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 2 - i \\ &F_p(p^{-1} + 0 + p + \overline{a}_2 p^2 + \overline{a}_3 p^3 + \cdots) = 3 \end{aligned}$$

$$
\begin{aligned}
&F_p(p^{-1}+1+0p+\overline{a}_2p^2+\overline{a}_3p^3+\cdots)=1-i\\
&F_p(0p^{-1}+0+p+\overline{a}_2p^2+\overline{a}_3p^3+\cdots)=1+i\\
&F_p(0p^{-1}+1+0p+\overline{a}_2p^2+\overline{a}_3p^3+\cdots)=i\\
&F_p(p^{-1}+0+0p+\overline{a}_2p^2+\overline{a}_3p^3+\cdots)=-i\\
&F_p(0p^{-1}+0+0p+\overline{a}_2p^2+\overline{a}_3p^3+)=0
\end{aligned}
\tag{11.26}
$$

Also for $\overline{a}_{-k}\neq 0$ with $k>1$, we get

$$
F_p(\overline{a}_{-k}p^{-k}+\overline{a}_{-k+1}p^{-k+1}+...)=0. \tag{11.27}
$$

The Weil transform of this function is the following function on $\mathbb{Q}_p/\mathbb{Z}_p$, which belongs to $\mathscr{A}_2(1,0)$:

$$
\begin{aligned}
f_p(p^{-1}) &= \int_{\mathbb{Z}_p} F_p(p^{-1}+b_p)db_p=\frac{1}{4}[F_p(p^{-1}+1+p)\\
&+F_p(p^{-1}+0+p)+F_p(p^{-1}+1+0p)+F_p(p^{-1}+0+0p)]\\
&=\frac{1}{4}[5-2i],
\end{aligned}
\tag{11.28}
$$

and

$$
\begin{aligned}
f_p(0) &= \int_{\mathbb{Z}_p} F_p(p^{-1}+b_p)db_p=\frac{1}{4}[F_p(0p^{-1}+1+p)\\
&+F_p(0p^{-1}+0+p)+F_p(0p^{-1}+1+0p)+F_p(0p^{-1}+0+0p)]\\
&=\frac{1}{4}[3+i].
\end{aligned}
\tag{11.29}
$$

In this case

$$
\int_{\mathbb{Q}_p/\mathbb{Z}_p} f(\mathfrak{p}_p)d\mathfrak{a}_p=\int_{\mathbb{Q}_p} F_p(c_p)dc_p=\frac{1}{4}[8-i]. \tag{11.30}
$$

11.3.2 Delta Functions

Delta function in the present context, is a function $\delta_p(x_p)$ where $x_p\in\mathbb{Z}_p$, such that

$$
\int_{\mathbb{Z}_p} dx_p f_p(x_p)\delta_p(x_p-a_p)=f_p(a_p). \tag{11.31}
$$

It is a generalized function. It does not belong to $\mathscr{A}_p$ because it is not locally constant.

We also introduce the following function $\Delta_p(\mathfrak{p}_p)$ where $\mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p$:

$$\begin{aligned}&\Delta_p(0) = 1\\ &\Delta_p(\mathfrak{p}_p) = 0 \ \text{ if } \ \mathfrak{p}_p \neq 0.\end{aligned} \tag{11.32}$$

Then

$$\int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p F_p(\mathfrak{p}_p)\Delta_p(\mathfrak{p}_p - \mathfrak{a}_p) = F_p(\mathfrak{a}_p). \tag{11.33}$$

The following relations are useful later:

$$\begin{aligned}&\int_{\mathbb{Z}_p} dx_p \chi_p(x_p\mathfrak{p}_p) = \Delta_p(\mathfrak{p}_p)\\ &\int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \chi_p(x_p\mathfrak{p}_p) = \delta_p(x_p).\end{aligned} \tag{11.34}$$

11.4 The Quantum System $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$

We define the Schwartz-Bruhat space $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, which is the space of complex wavefunctions for the quantum system $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. The definition [4–6] aims to ensure convergence of the scalar products of the wavefunctions. Below we usually use fraktur letters for elements of $\mathbb{Q}_p/\mathbb{Z}_p$.

Definition 11.3 The Schwartz-Bruhat space $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ consists of functions $f_p(x_p) \in \mathscr{A}_p(0, *)$ where $x_p \in \mathbb{Z}_p$, or equivalently of functions $F_p(\mathfrak{p}_p) \in \mathscr{A}_p(*, 0)$ where $\mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p$. The scalar product is given by

$$(f, g) = \int_{\mathbb{Z}_p} dx_p f_p(x_p) g_p(x_p); \quad (F, G) = \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p F_p(\mathfrak{p}_p) G_p(\mathfrak{p}_p). \tag{11.35}$$

The Fourier transform in this space, is defined as follows:

Definition 11.4 The Fourier transform of a function $f_p(x_p) \in \mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ where $x_p \in \mathbb{Z}_p$ (such a function belongs to $\mathscr{A}_p(0, *)$), is the function

$$(\mathfrak{F}_p f_p)(\mathfrak{p}_p) = \widetilde{f_p}(\mathfrak{p}_p) = \int_{\mathbb{Z}_p} dx_p f_p(x_p) \chi_p(-x_p\mathfrak{p}_p), \tag{11.36}$$

which is defined on $\mathbb{Q}_p/\mathbb{Z}_p$, and belongs to the set $\mathscr{A}_p(*, 0)$.

Proposition 11.3 *(1) The inverse Fourier transform of a complex function* $\widetilde{f}_p(\mathfrak{p}_p) \in \mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, *where* $\mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p$ *(such a function belongs to* $\mathscr{A}_p(*, 0)$*), is*

$$(\mathfrak{F}_p^{-1}\widetilde{f}_p)(x_p) = f_p(x_p) = \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \widetilde{f}_p(\mathfrak{p}_p)\chi_p(x_p\mathfrak{p}_p). \tag{11.37}$$

It is a complex function on $\mathbb{Z}_p$, *which belong to the set* $\mathscr{A}_p(0, *)$.

(2)

$$\mathbf{LC}[\widetilde{f}_p(\mathfrak{p}_p)] = \mathbf{CS}[f_p(x_p)]; \quad \mathbf{CS}[\widetilde{f}_p(\mathfrak{p}_p)] = \mathbf{LC}[f_p(x_p)]. \tag{11.38}$$

Therefore if $f_p(x_p) \in \mathscr{A}_p(k, n)$, *then its Fourier transform* $\widetilde{f}_p(\mathfrak{p}_p) \in \mathscr{A}_p(n, k)$.

(3)

$$\mathfrak{F}_p^4 = \mathbf{1}. \tag{11.39}$$

(4) Parceval's theorem holds:

$$\int_{\mathbb{Z}_p} dx_p f_p(x_p)g_p(x_p) = \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \widetilde{f}_p(\mathfrak{p}_p)\widetilde{g}_p(\mathfrak{p}_p) \tag{11.40}$$

Proof (1) We prove that Eqs.(11.36),(11.37) are compatible using Eq.(11.34).

(2) If the function $f_p(x_p)$ has $\mathbf{LC}[f_p(x_p)] = n$, then for all $|\alpha_p|_p \leq p^{-n}$ we get $f_p(x_p + a_p) - f_p(x_p) = 0$ and we rewrite this as

$$\int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \ \chi_p(x_p\mathfrak{p}_p)\widetilde{f}_p(\mathfrak{p}_p)[1 - \chi_p(\alpha_p\mathfrak{p}_p)] = 0. \tag{11.41}$$

It is seen that the Fourier transform of $\widetilde{f}_p(\mathfrak{p}_p)[1 - \chi_p(\alpha_p\mathfrak{p}_p)]$ is zero. Consequently, $\widetilde{f}_p(\mathfrak{p}_p)[1 - \chi_p(\alpha_p\mathfrak{p}_p)] = 0$. But for $|\alpha_p|_p \leq p^{-n}$ and $|\mathfrak{p}_p| > p^n$ the $1 - \chi_p(\alpha_p\mathfrak{p}_p) \neq 0$ and therefore $\widetilde{f}_p(\mathfrak{p}_p) = 0$. This proves that $\mathbf{CS}[\widetilde{f}_p(\mathfrak{p}_p)] = n$. In a similar way we prove the other relation.

(3) The proof of this is based on Eq.(11.34).

(4) The proof of this is based on Eq.(11.34).

Remark 11.2 Equation (11.34) can be interpreted as follows:

- the Fourier transform of the function $f_p(x_p) = 1$ on $\mathbb{Z}_p$, is the function $\Delta_p(\mathfrak{p}_p)$ on $\mathbb{Q}_p/\mathbb{Z}_p$.
- the Fourier transform of the function $\widetilde{f}_p(\mathfrak{p}_p) = 1$ on $\mathbb{Q}_p/\mathbb{Z}_p$, is the function $\delta_p(x_p)$ on $\mathbb{Z}_p$.

11.5 The Heisenberg-Weyl Group $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$

The phase space of the system $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ is $\mathbb{Z}_p \times (\mathbb{Q}_p/\mathbb{Z}_p)$, and we define displacement operators and the Heisenberg-Weyl group [27].

Definition 11.5 The displacement operators $D_p(\mathfrak{a}_p, b_p)$ where $b_p \in \mathbb{Z}_p$ and $\mathfrak{a}_p \in \mathbb{Q}_p/\mathbb{Z}_p$, are defined by one of the following ways, which are equivalent to each other:

(1) They act on the wavefunctions $f_p(x_p) \in \mathscr{A}_p(0, *)$ where $x_p \in \mathbb{Z}_p$, as follows:

$$[D_p(\mathfrak{a}_p, b_p) f_p](x_p) = \chi_p\left(-\mathfrak{a}_p b_p + 2\mathfrak{a}_p x_p\right) f_p(x_p - b_p). \tag{11.42}$$

(2) They act on the wavefunctions $F_p(\mathfrak{p}_p) \in \mathscr{A}(*, 0)$, where $\mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p$ as follows:

$$[D_p(\mathfrak{a}_p, b_p) F_p](\mathfrak{p}_p) = \chi_p\left(\mathfrak{a}_p b_p - b_p \mathfrak{p}_p\right) F_p(\mathfrak{p}_p - 2\mathfrak{a}_p). \tag{11.43}$$

The equivalence of the definitions, is easily proved with a Fourier transform.

Proposition 11.4 *The displacement operators $D_p(\mathfrak{a}_p, b_p)\chi_p(\mathfrak{c}_p)$ form a representation of the Heisenberg-Weyl group $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ (the notation indicates the sets in whch the variables $\mathfrak{a}_p, b_p, \mathfrak{c}_p$ belong).*

Proof Using the definition in Eq.(11.42), we prove the multiplication rule

$$\begin{aligned} &D_p(\mathfrak{a}_p, b_p) D_p(\mathfrak{a}'_p, b'_p) \\ &= D_p(\mathfrak{a}_p + \mathfrak{a}'_p, b_p + b'_p)\chi_p(\mathfrak{a}_p b'_p - \mathfrak{a}'_p b_p). \end{aligned} \tag{11.44}$$

Taking into account the Definition 4.2, we conclude that the $D_p(\mathfrak{a}_p, b_p)\chi_p(\mathfrak{c}_p)$ form a representation of the Heisenberg-Weyl group.

11.5.1 $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ as a Locally Compact and Totally Disconnected Topological Group

We define the following subgroups of $HW(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)$:

$$\begin{aligned} HW_1(\mathbb{Q}_p/\mathbb{Z}_p) &= \{D_p(\mathfrak{a}_p, 0) \mid \mathfrak{a}_p \in \mathbb{Q}_p/\mathbb{Z}_p\} \cong \mathbb{Q}_p/\mathbb{Z}_p \\ HW_2(p^e\mathbb{Z}_p) &= \{D_p(0, b_p) \mid b_p \in p^e\mathbb{Z}_p\} \cong p^e\mathbb{Z}_p \\ HW_3(\mathbb{Q}_p/\mathbb{Z}_p) &= \{\chi_p(\mathfrak{c}_p) \mid \mathfrak{c}_p \in \mathbb{Q}_p/\mathbb{Z}_p\} \cong \mathbb{Q}_p/\mathbb{Z}_p. \end{aligned} \tag{11.45}$$

If $e_1 \leq e_2$ then $HW_2(p^{e_2}\mathbb{Z}_p) \prec HW_2(p^{e_1}\mathbb{Z}_p)$. The set

$$\mathfrak{N}_p = \{HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]\} \cup \{HW_2(p^e\mathbb{Z}_p) \mid e \in \mathbb{Z}_0^+\} \quad (11.46)$$

with the order subgroup, is a chain.

If A, B are subsets of a group G and $g \in G$, we use the notation:

$$\begin{aligned} gA &= \{ga | a \in A\}; \qquad gAg^{-1} = \{gag^{-1} | a \in A\} \\ AB &= \bigcup_{a \in A} aB; \qquad A^{-1} = \{a^{-1} | a \in A\}. \end{aligned} \quad (11.47)$$

Proposition 11.5 *We regard the set $\mathfrak{N}_p$ in Eq.(11.46), as a fundamental system of open neighborhoods of the identity of $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. Then the $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ becomes a topological group, which is totally disconnected and locally compact.*

Proof We prove that the elements of $\mathfrak{N}_p$, satisfy the following properties of a fundamental system of open neighborhoods of the identity (e.g. Sect. III.1.2 in [45]). These properties ensure compatibility between the group structure and the topology.

- Given any $U \in \mathfrak{N}_p$ there exists $V \in \mathfrak{N}_p$ such that $VV \prec U$. This holds because for $U = HW_2(p^n\mathbb{Z}_p)$, all the $V = HW_2(p^k\mathbb{Z}_p)$ with $k \geq n$ satisfy this.
- Given any $U \in \mathfrak{N}_p$ there exists $V \in \mathfrak{N}_p$ such that $V^{-1} \prec U$. This holds because for $U = HW_2(p^n\mathbb{Z}_p)$ all the $V^{-1} = V = HW_2(p^k\mathbb{Z}_p)$ with $k \geq n$ satisfy this.
- Given any element $D(\mathfrak{a}, b)\chi_p(\mathfrak{c})$ of $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ and any $U \in \mathfrak{N}_p$, there exists $V \in \mathfrak{N}_p$ such that

$$V \prec \left[D(\mathfrak{a}, b)\chi_p(\mathfrak{c})\right] U \left[D(-\mathfrak{a}, -b)\chi_p(-\mathfrak{c})\right]. \quad (11.48)$$

  This holds because for $U = HW_2(p^n\mathbb{Z}_p)$, we get

$$D(\mathfrak{a}, b)\chi_p(\mathfrak{c})\ D(0, b')\ D(-\mathfrak{a}, -b)\chi_p(-\mathfrak{c}) = D(0, b')\chi_p(\mathfrak{a}b'); \quad (11.49)$$

  where $b' \in p^n\mathbb{Z}_p$. Any subgroup $V = HW_2(p^k\mathbb{Z}_p)$ with $k \geq \max(n, -\mathrm{ord}(\mathfrak{a}))$ satisfies Eq.(11.48).

Therefore $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ is a topological group.

We next show that it is totally disconnected and locally compact. $HW_1(\mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Q}_p/\mathbb{Z}_p$ is a discrete locally compact topological group. $HW_2(\mathbb{Z}_p) \cong \mathbb{Z}_p$ is a profinite group, i.e. a totally disconnected compact topological group. Since both of these groups are totally disconnected and locally compact, it follows that the $HW_1(\mathbb{Q}_p/\mathbb{Z}_p) \times HW_2(\mathbb{Z}_p)$ with the product topology, is a totally disconnected and locally compact topological group.

$HW_3(\mathbb{Q}_p/\mathbb{Z}_p)$ is a normal subgroup of $HW(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)$. We consider the quotient group

$$\begin{aligned} &HW(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)/HW_3(\mathbb{Q}_p/\mathbb{Z}_p) \\ &\cong HW_1(\mathbb{Q}_p/\mathbb{Z}_p) \times HW_2(\mathbb{Z}_p). \end{aligned} \tag{11.50}$$

Both the $HW_1(\mathbb{Q}_p/\mathbb{Z}_p) \times HW_2(\mathbb{Z}_p)$ and $HW_3(\mathbb{Q}_p/\mathbb{Z}_p)$ are totally disconnected and locally compact topological groups. Consequently, $HW(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)$ is a totally disconnected and locally compact topological group.

Remark 11.3 For completeness we define another representation of the Heisenberg-Weyl group, although it is not relevant for Physics. This is the profinite Heisenberg-Weyl group $HW(\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p)$, and is different from the $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ (which is not profinite).

The $HW(\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p)$ is defined as the inverse limit of the finite Heisenberg-Weyl groups $HW[\mathbb{Z}(p^e), \mathbb{Z}(p^e), \mathbb{Z}(p^e)]$. For $k \leq n$ we define the homomorphisms

$$\widetilde{\varphi}_{kn} : \quad HW[\mathbb{Z}(p^k), \mathbb{Z}(p^k), \mathbb{Z}(p^k)] \ \leftarrow \ HW[\mathbb{Z}(p^n), \mathbb{Z}(p^n), \mathbb{Z}(p^n)], \tag{11.51}$$

where

$$\begin{aligned} &\widetilde{\varphi}_{kn}[D(\alpha_{p^n}, \beta_{p^n})\omega_{p^n}(\gamma_{p^n})] = D(\alpha_{p^k}, \beta_{p^k})\omega_{p^k}(\gamma_{p^k}) \\ &\alpha_{p^k} = \varphi_{kn}(\alpha_{p^n}); \qquad \beta_{p^k} = \varphi_{kn}(\beta_{p^n}); \qquad \gamma_{p^k} = \varphi_{kn}(\gamma_{p^n}). \end{aligned} \tag{11.52}$$

The map φ_{kn} has been defined in Eq.(10.43). The $\widetilde{\varphi}_{kn}$ are compatible, and the $\{HW[\mathbb{Z}(p^n), \mathbb{Z}(p^n), \mathbb{Z}(p^n)], \widetilde{\varphi}_{kn}\}$ is an inverse system, whose inverse limit we denote as $HW(\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p)$. The elements of this group are $\mathfrak{D}_p(a_p, b_p)\chi_p(c_p)$ where

$$\begin{aligned} &\mathfrak{D}_p(a_p, b_p) = (D(\alpha_p, \beta_p), D(\alpha_{p^2}, \beta_{p^2}), ...) \\ &\chi_p(c_p) = (\omega_p(\gamma_p), \omega_{p^2}(\gamma_{p^2}), ...); \quad a_p, b_p, c_p \in \mathbb{Z}_p \\ &a_p = (\alpha_p, \alpha_{p^2}, ...); \quad b_p = (\beta_p, \beta_{p^2}, ...); \quad c_p = (\gamma_p, \gamma_{p^2}, ...). \end{aligned} \tag{11.53}$$

We stress that the $\mathfrak{D}_p(a_p, b_p)$ where $a_p, b_p \in \mathbb{Z}_p$, is very different from the $D_p(\mathfrak{a}_p, b_p)$ where $\mathfrak{a}_p \in \mathbb{Q}_p/\mathbb{Z}_p$ and $b_p \in \mathbb{Z}_p$ (see also Remark 10.2).

Multiplication of these elements is componentwise, and obeys the rule in the Definition 4.2. Therefore we have a representation of the Heisenberg-Weyl group. But the Pontryagin dual group to $\mathbb{Z}_p$ does not appear here. Consequently, the $HW(\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p)$ cannot be associated with displacements of dual quantum variables, and it is not relevant to quantum mechanics. Pontryagin duality of the groups of positions and momenta is an essential feature of quantum mechanics.

11.6 Wigner and Weyl Functions

In this section we discuss Wigner and Weyl functions in the present context[27, 32]. We point out from the outset, that there are differences between the two cases $p = 2$ and $p \neq 2$. Some of the integrals have domain of integration $\mathbb{Q}_p/|2|_p\mathbb{Z}_p$, and also the prefactor $|2|_p$. This is related to change of variables using Eq.(11.19), and it is analogous to our comment in the context of finite quantum systems earlier, that there are technical differences in the two cases of even or odd dimension. We recall that

$$\begin{aligned} |2|_p &= 1 \ \text{ if } \ p \neq 2 \\ |2|_2 &= \frac{1}{2}. \end{aligned} \tag{11.54}$$

We consider an operator $\theta(x_p, y_p)$ where $x_p, y_p \in \mathbb{Z}_p$, and let

$$\widetilde{\theta}(\mathfrak{p}_p, \mathfrak{p}'_p) = \int_{\mathbb{Z}_p} dx_p \int_{\mathbb{Z}_p} dy_p \theta(x_p, y_p) \chi_p(-x_p\mathfrak{p}_p + y_p\mathfrak{p}'_p), \tag{11.55}$$

where $\mathfrak{p}_p, \mathfrak{p}'_p \in \mathbb{Q}_p/\mathbb{Z}_p$. θ acts on a function $f_p(x_p)$, and its Fourier transform $\widetilde{f}_p(\mathfrak{p}_p)$, as follows:

$$\begin{aligned} (\theta f_p)(x_p) &= \int_{\mathbb{Z}_p} dy_p \theta(x_p, y_p) f_p(y_p) \\ (\theta \widetilde{f}_p)(\mathfrak{p}_p) &= \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p \widetilde{\theta}(\mathfrak{p}_p, \mathfrak{p}'_p) \widetilde{f}_p(\mathfrak{p}'_p) \end{aligned} \tag{11.56}$$

The trace of θ is given by

$$\mathrm{tr}\theta = \int_{\mathbb{Z}_p} dx_p \theta(x_p, x_p) = \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \widetilde{\theta}(\mathfrak{p}_p, \mathfrak{p}_p) \tag{11.57}$$

Definition 11.6 The parity operator with respect to the point $(\mathfrak{a}_p, b_p)$ in the phase space $(\mathbb{Q}_p/\mathbb{Z}_p) \times \mathbb{Z}_p$, is

$$\begin{aligned} P_p(\mathfrak{a}_p, b_p) &= [D_p(\mathfrak{a}_p, b_p)]^\dagger \ \mathfrak{F}_p^2 \ D_p(\mathfrak{a}_p, b_p) \\ &= [D_p(2\mathfrak{a}_p, 2b_p)]^\dagger \ \mathfrak{F}_p^2 = \mathfrak{F}_p^2 \ D_p(2\mathfrak{a}_p, 2b_p) \end{aligned} \tag{11.58}$$

In particular the parity operator with respect to the point $(0, 0)$ is $P_p(0, 0) = \mathfrak{F}_p^2$.

Proposition 11.6 *(1) The parity operator acts on wavefunctions in* $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$*, as follows:*

$$\begin{aligned} P_p(\mathfrak{a}_p, b_p) f_p(x_p) &= \chi_p(-4\mathfrak{a}_p b_p - 4\mathfrak{a}_p x_p) f_p(-x_p - 2b_p) \\ P_p(\mathfrak{a}_p, b_p) \widetilde{f}_p(\mathfrak{p}_p) &= \chi_p(4\mathfrak{a}_p b_p + 2\mathfrak{p}_p b_p) \widetilde{f}_p(-\mathfrak{p}_p - 4\mathfrak{a}_p). \end{aligned} \tag{11.59}$$

(2)

$$[P_p(\mathfrak{a}_p, b_p)]^2 = \mathbf{1}; \quad P_p\left(\mathfrak{a}_p + \frac{1}{4}, b_p\right) = P_p(\mathfrak{a}_p, b_p). \tag{11.60}$$

Proof (1) This is proved using Eqs.(11.42), (11.43).
(2) Using Eq.(11.59) we easily prove that $[P_p(\mathfrak{a}_p, b_p)]^2 = \mathbf{1}$. Also using the second of Eqs.(11.59), we prove that $P_p\left(\mathfrak{a}_p + \frac{1}{4}, b_p\right) = P_p(\mathfrak{a}_p, b_p)$.

Remark 11.4 For $p \neq 2$, the $\frac{1}{4} \in \mathbb{Z}_p$, and for $p = 2$, the $\frac{1}{4} \in 2^{-2}\mathbb{Z}_p$. For any $c_p \in \mathbb{Z}_p$, we get $P_p(\mathfrak{a}_p + c_p, b_p) = P_p(\mathfrak{a}_p, b_p)$. Therefore the $P_p(\mathfrak{a}_p + \frac{1}{4}, b_p) = P_p(\mathfrak{a}_p, b_p)$ is a new result, only for $p = 2$.

Definition 11.7 The Weyl function of an operator θ, is defined as:

$$\widetilde{W}(\mathfrak{a}_p, b_p; \theta) = \mathrm{tr}[D_p(-\mathfrak{a}_p, -b_p)\theta]; \quad \mathfrak{a}_p \in \mathbb{Q}_p/\mathbb{Z}_p; \quad b_p \in \mathbb{Z}_p. \tag{11.61}$$

The Wigner function of an operator θ, is defined as:

$$W(\mathfrak{a}_p, b_p; \theta) = \mathrm{tr}[\theta P_p(\mathfrak{a}_p, b_p)]; \quad \mathfrak{a}_p \in \mathbb{Q}_p/\mathbb{Z}_p; \quad b_p \in \mathbb{Z}_p. \tag{11.62}$$

Proposition 11.7 *(1) The Weyl function is given by*

$$\widetilde{W}(\mathfrak{a}_p, b_p; \theta) = \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \ \chi_p\left(\mathfrak{a}_p b_p + \mathfrak{p}_p b_p\right) \widetilde{\theta}(\mathfrak{p}_p + 2\mathfrak{a}_p, \mathfrak{p}_p) \tag{11.63}$$

(2) The Wigner function is given by

$$W(\mathfrak{a}_p, b_p; \theta) = \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \ \chi_p(-4\mathfrak{a}_p b_p - 2\mathfrak{p}_p b_p)\widetilde{\theta}(\mathfrak{p}_p, -\mathfrak{p}_p - 4\mathfrak{a}_p). \tag{11.64}$$

Proof (1) We act with $D_p(-\mathfrak{a}_p, -b_p)$ on the kernel $\widetilde{\theta}(\mathfrak{p}_p, \mathfrak{p}'_p)$ of the operator θ and we get

$$[D_p(-\mathfrak{a}_p, -b_p)\widetilde{\theta}](\mathfrak{p}_p, \mathfrak{p}'_p) = \chi_p\left(\mathfrak{a}_p b_p + \mathfrak{p}_p b_p\right) \widetilde{\theta}(\mathfrak{p}_p + 2\mathfrak{a}_p, \mathfrak{p}'_p) \tag{11.65}$$

Therefore its trace, which is the Weyl function, is

$$\begin{aligned} \widetilde{W}(\mathfrak{a}_p, b_p; \theta) &= \mathrm{tr}[D_p(-\mathfrak{a}_p, -b_p)\theta] \\ &= \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \ \chi_p\left(\mathfrak{a}_p b_p + \mathfrak{p}_p b_p\right) \widetilde{\theta}(\mathfrak{p}_p + 2\mathfrak{a}_p, \mathfrak{p}_p) \end{aligned} \tag{11.66}$$

(2) We act with $P_p(\mathfrak{a}_p, b_p)$ on the kernel $\widetilde{\theta}(\mathfrak{p}_p, \mathfrak{p}'_p)$ of the operator θ and we get

$$[P_p(\mathfrak{a}_p, b_p)\widetilde{\theta}](\mathfrak{p}_p, \mathfrak{p}'_p) = \chi_p\left(4\mathfrak{a}_p b_p + 2\mathfrak{p}_p b_p\right) \widetilde{\theta}(-\mathfrak{p}_p - 4\mathfrak{a}_p, \mathfrak{p}'_p) \tag{11.67}$$

Therefore its trace, which is the Wigner function, is

$$\begin{aligned} W(\mathfrak{a}_p, b_p; \theta) &= \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p \ \chi_p\left(4\mathfrak{a}_p b_p + 2\mathfrak{p}_p b_p\right) \\ &\times \widetilde{\theta}(-\mathfrak{p}_p - 4\mathfrak{a}, \mathfrak{p}'_p) \Delta_p(\mathfrak{p}_p + \mathfrak{p}'_p + 4\mathfrak{a}_p) \\ &= \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \ \widetilde{\theta}(\mathfrak{p}_p, -\mathfrak{p}_p - 4\mathfrak{a}_p) \chi_p(-4\mathfrak{a}_p b_p - 2\mathfrak{p}_p b_p). \quad (11.68) \end{aligned}$$

Proposition 11.8 *The parity operators are related to the displacement operators through a Fourier transform:*

$$P_p(\mathfrak{a}_p, b_p) = \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{a}'_p \int_{\mathbb{Z}_p} db'_p \ D_p(\mathfrak{a}'_p, b'_p) \chi_p(2\mathfrak{a}'_p b_p - 2\mathfrak{a}_p b'_p). \quad (11.69)$$

Also the Wigner function is related to the Weyl function through a Fourier transform:

$$W(\mathfrak{a}_p, b_p; \theta) = \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{a}'_p \int_{\mathbb{Z}_p} db'_p \ \widetilde{W}(-\mathfrak{a}'_p, -b'_p) \chi_p(2\mathfrak{a}'_p b_p - 2\mathfrak{a}_p b'_p). \quad (11.70)$$

Proof We act with the right hand side of Eq.(11.69) on an arbitrary function $F_p(\mathfrak{p}_p)$, and we get

$$\begin{aligned} &\int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{a}'_p \ \chi_p(2\mathfrak{a}'_p b_p) F_p(\mathfrak{p}_p - 2\mathfrak{a}'_p) \int_{\mathbb{Z}_p} db'_p \ \chi_p[b'_p(\mathfrak{a}'_p - \mathfrak{p}_p - 2\mathfrak{a}_p)] \\ &= \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{a}'_p \ \chi_p(2\mathfrak{a}'_p b_p) F_p(\mathfrak{p}_p - 2\mathfrak{a}'_p) \Delta_p(\mathfrak{a}'_p - \mathfrak{p}_p - 2\mathfrak{a}_p) \\ &= \chi_p(4b_p\mathfrak{a}_p + 2b_p\mathfrak{p}_p) \ F_p(-\mathfrak{p}_p - 4\mathfrak{a}_p) = P_p(\mathfrak{a}, b) F_p(\mathfrak{p}_p). \quad (11.71) \end{aligned}$$

From this we prove Eq.(11.70), using the definitions for the Wigner and Weyl functions.

Proposition 11.9 *Let θ be a trace class operator acting on functions in $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. Then*

(1)

$$|2|_p \int_{\mathbb{Q}_p/|2|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{\mathbb{Z}_p} db_p \ D_p(\mathfrak{a}_p, b_p) \ \theta \ [D_p(\mathfrak{a}_p, b_p)]^\dagger = \mathbf{1}\mathrm{tr}\theta. \quad (11.72)$$

(2) θ can be expanded in terms of displacement operators, with the Weyl function as coefficients:

$$\theta = |2|_p \int_{\mathbb{Q}_p/|2|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{\mathbb{Z}_p} db_p \ D_p(\mathfrak{a}_p, b_p) \widetilde{W}(\mathfrak{a}_p, b_p; \theta). \quad (11.73)$$

Proof (1) We act with $D_p(\mathfrak{a}_p, b_p)\ \theta\ [D_p(\mathfrak{a}_p, b_p)]^\dagger$ on a function $F_p(\mathfrak{p}_p) \in \mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ and we get

$$\begin{aligned}&\left[D_p(\mathfrak{a}_p, b_p)\ \theta\ [D_p(\mathfrak{a}_p, b_p)]^\dagger F_p\right](\mathfrak{p}_p)\\&= \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p\ \chi_p(2\mathfrak{a}_p b_p - \mathfrak{p}_p b_p + \mathfrak{p}'_p b_p)\\&\times\theta(\mathfrak{p}_p - 2\mathfrak{a}_p, \mathfrak{p}'_p)\ F_p(\mathfrak{p}'_p + 2\mathfrak{a}_p).\end{aligned} \tag{11.74}$$

The scalar product of this with an arbitrary function $G_p(\mathfrak{p}_p) \in \mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, gives

$$\begin{aligned}&|2|_p \int_{\mathbb{Q}_p/|2|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{\mathbb{Z}_p} db_p\ \left(G_p, D_p(\mathfrak{a}_p, b_p)\ \theta\ [D_p(\mathfrak{a}_p, b_p)]^\dagger F_p\right)\\&= |2|_p \int_{\mathbb{Q}_p/|2|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{\mathbb{Z}_p} db_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p\ [G_p(\mathfrak{p}_p)]^*\\&\times\chi_p(2\mathfrak{a}_p b_p - \mathfrak{p}_p b_p + \mathfrak{p}'_p b_p)\theta(\mathfrak{p}_p - 2\mathfrak{a}_p, \mathfrak{p}'_p)\ F_p(\mathfrak{p}'_p + 2\mathfrak{a}_p)\\&= |2|_p \int_{\mathbb{Q}_p/|2|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p\ [G_p(\mathfrak{p}_p)]^*\\&\times\Delta_p(2\mathfrak{a}_p - \mathfrak{p}_p + \mathfrak{p}'_p)\theta(\mathfrak{p}_p - 2\mathfrak{a}_p, \mathfrak{p}'_p)\ F_p(\mathfrak{p}'_p + 2\mathfrak{a}_p)\end{aligned} \tag{11.75}$$

We now change the variable $2\mathfrak{a}_p$ into $\mathfrak{a}'_p$, taking into account Eq.(11.19). We get:

$$\int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p\ [G_p(\mathfrak{p}_p)]^*\ F_p(\mathfrak{p}_p) \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p\ \theta(\mathfrak{p}'_p, \mathfrak{p}'_p) = (G_p, F_p)\mathrm{tr}(\theta). \tag{11.76}$$

This proves the proposition.

(2) The operator in Eq.(11.73) acts on an arbitrary function $F_p(\mathfrak{p}_p) \in \mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, as follows (use Eq.(11.63)):

$$\begin{aligned}&|2|_p \int_{\mathbb{Q}_p/|2|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{\mathbb{Z}_p} db_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p\ \chi_p\left(\mathfrak{a}_p b_p + \mathfrak{p}_p b_p\right)\\&\times\widetilde{\theta}(\mathfrak{p}_p + 2\mathfrak{a}_p, \mathfrak{p}_p)\chi_p\left(\mathfrak{a}_p b_p - \mathfrak{p}'_p b_p\right) F_p(\mathfrak{p}'_p - 2\mathfrak{a}_p)\\&= |2|_p \int_{\mathbb{Q}_p/|2|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p\ \widetilde{\theta}(\mathfrak{p}_p + 2\mathfrak{a}_p, \mathfrak{p}_p)\\&\times\Delta_p(2\mathfrak{a}_p + \mathfrak{p}_p - \mathfrak{p}'_p)F_p(\mathfrak{p}'_p - 2\mathfrak{a}_p)\end{aligned} \tag{11.77}$$

We now change the variable $2\mathfrak{a}_p$ into $\mathfrak{a}'_p$, taking into account Eq.(11.19). We get

$$\int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p\ \widetilde{\theta}(\mathfrak{p}'_p, \mathfrak{p}_p)F_p(\mathfrak{p}_p) \tag{11.78}$$

This proves the proposition.

Proposition 11.10 *Let θ be a trace class operator acting on functions in the Schwartz-Bruhat space $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. Then*

(1)

$$|2|_p^3 \int_{\mathbb{Q}_p/|4|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{|2|_p\mathbb{Z}_p} db_p \; P_p(\mathfrak{a}_p, b_p)\; \theta \; P_p(\mathfrak{a}_p, b_p) = \mathbf{1}\mathrm{tr}\theta. \quad (11.79)$$

(2) θ can be expanded in terms of parity operators, with the Wigner function as coefficients:

$$\theta = |2|_p^3 \int_{\mathbb{Q}_p/|4|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{|2|_p\mathbb{Z}_p} db_p \; P_p(\mathfrak{a}_p, b_p) W(\mathfrak{a}_p, b_p; \theta). \quad (11.80)$$

Proof (1) We substitute $\mathfrak{a}_p$ with $2\mathfrak{a}_p$ and b_p with $2b_p$ in Eq.(11.72), and change accordingly the domains of integration. We get

$$|2|_p^3 \int_{\mathbb{Q}_p/|4|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{|2|_p\mathbb{Z}_p} db_p \; D_p(2\mathfrak{a}_p, 2b_p)\; \theta \; [D_p(2\mathfrak{a}_p, 2b_p)]^\dagger = \mathbf{1}\mathrm{tr}\theta. \quad (11.81)$$

Then we multiply each side with $\mathfrak{F}_p^2$ on the left and with $(\mathfrak{F}_p^2)^\dagger$ on the right, and we prove the statement.

(2) We substitute Eq.(11.64) on the right hand side of Eq.(11.80), and act on an arbitrary function $F_p(\mathfrak{p}_p)$, in order to prove that this is the operator θ acting on $F_p(\mathfrak{p}_p)$:

$$(|2|_p)^3 \int_{\mathbb{Q}_p/|4|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{|2|_p\mathbb{Z}_p} db_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p \; \widetilde{\theta}(\mathfrak{p}'_p, -\mathfrak{p}'_p - 4\mathfrak{a}_p) \times \chi_p(-4\mathfrak{a}_p b_p - 2\mathfrak{p}'_p b_p)\chi(4\mathfrak{a}_p b_p + 2\mathfrak{p}_p b_p) F_p(-\mathfrak{p}_p - 4\mathfrak{a}_p) \quad (11.82)$$

Integration over $2b_p$ gives,

$$|4|_p \int_{\mathbb{Q}_p/|4|_p\mathbb{Z}_p} d\mathfrak{a}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'_p \; \widetilde{\theta}(\mathfrak{p}'_p, -\mathfrak{p}'_p - 4\mathfrak{a}_p) \times \Delta_p(\mathfrak{p}_p - \mathfrak{p}'_p) F_p(-\mathfrak{p}_p - 4\mathfrak{a}_p) = |4|_p \int_{\mathbb{Q}_p/|4|_p\mathbb{Z}_p} d\mathfrak{a}_p \; \widetilde{\theta}(\mathfrak{p}_p, -\mathfrak{p}_p - 4\mathfrak{a}_p) F_p(-\mathfrak{p}_p - 4\mathfrak{a}_p) \quad (11.83)$$

Now we change the variable $-\mathfrak{p}_p - 4\mathfrak{a}_p$ into $\mathfrak{q}_p$, taking into account Eq.(11.19). We prove that the right hand side of Eq.(11.80), is equal to the operator θ.

11.7 The Complete Chain of Subsystems of $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$

In sect. 10.8 we studied the complete chain $\mathbb{N}_S^{(G,\widetilde{G})}(p)$ which contains pairs of groups $(\mathbb{Z}(p^k), C(p^k))$ which are Pontryagin dual to each other. To each of these pairs corresponds a quantum system, as follows:

$$\begin{aligned}(\mathbb{Z}(p^k), C(p^k)) &\rightarrow \Sigma[\mathbb{Z}(p^k)]; \quad k \in \mathbb{N} \\ (\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)) &\rightarrow \Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]\end{aligned} \tag{11.84}$$

We denote as $\mathbb{N}_S^Q(p)$, the set of these quantum systems (the superfix Q indicates quantum systems). It is a complete chain

$$\Sigma[\mathbb{Z}(p)] \prec \Sigma[\mathbb{Z}(p^2)] \prec ... \prec \Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)], \tag{11.85}$$

with the order subsystem [32]. $\mathbb{N}_S^Q(p)$ is order isomorphic to $\mathbb{N}_S^{(G,\widetilde{G})}(p)$ and also to $\mathbb{N}_S(p)$:

$$\mathbb{N}_S^Q(p) \cong \mathbb{N}_S^{(G,\widetilde{G})}(p) \cong \mathbb{N}_S(p). \tag{11.86}$$

Below we give some technical details related to the fact that $\Sigma[\mathbb{Z}(p^k)]$ is a subsystem of $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. We define a subspace $\mathscr{B}[\mathbb{Z}(p^k)]$ of $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, and show that it is isomorphic to the space $H[\mathbb{Z}(p^k)]$, which describes the system $\Sigma[\mathbb{Z}(p^k)]$.

Definition 11.8 The subspace $\mathscr{B}[\mathbb{Z}(p^k)]$ of $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ is defined by one of the following ways, which are equivalent to each other:

(1) It contains functions $f_p(x_p) \in \mathscr{A}(0,k)$, where $x_p \in \mathbb{Z}_p$. These functions can be regarded as functions $f(m)$ where $m \in \mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}(p^k)$. The scalar product of Eq.(11.35) reduces to

$$(f,g) = \frac{1}{p^n} \sum_{m \in \mathbb{Z}(p^k)} [f(m)]^* g(m). \tag{11.87}$$

(2) It contains functions $F_p(\mathfrak{p}_p) \in \mathscr{A}(k,0)$, where $\mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p$. These functions can be regarded as functions $F(n)$ where $n \in p^{-k}\mathbb{Z}_p/\mathbb{Z}_p \cong \mathbb{Z}(p^k)$. In this case the scalar product of Eq.(11.35) reduces to

$$(F,G) = \sum_{n \in \mathbb{Z}(p^k)} [F(n)]^* G(n). \tag{11.88}$$

In the subspace $\mathscr{B}[\mathbb{Z}(p^k)]$, the Fourier transform of Eq.(11.36), reduces to the finite Fourier transform used in the space $H[\mathbb{Z}(p^k)]$ for the quantum system $\Sigma[\mathbb{Z}(p^n)]$:

$$F(n) = \frac{1}{p^n} \sum_{m \in \mathbb{Z}(p^n)} f(m)\omega_{p^n}(-mn); \quad m, n \in \mathbb{Z}(p^n). \tag{11.89}$$

Therefore the subspace $\mathscr{B}[\mathbb{Z}(p^k)]$ is isomorphic to the space $H[\mathbb{Z}(p^k)]$, that describes the quantum system $\Sigma[\mathbb{Z}(p^n)]$.

The systems $\Sigma[\mathbb{Z}(p^e)]$ are subsystems of $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. The chain of all $\Sigma[\mathbb{Z}(p^e)]$ with $e \in \mathbb{N}$ is not complete. By adding the 'top element' $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ (which describes regorously the case $e = \infty$), we make it complete.

References

1. Gel'fand, I. M., & Graev, M. I. (1963). *Russian Mathematical Surveys*, *18*, 29–109.
2. Taibleson, M. H. (1975). *Fourier analysis on local fields*. Princeton: Princeton University Press.
3. Vladimirov, V. S. (1988). *Russian Mathematical surveys*, *43*, 19.
4. Gel'fand, I. M., Graev, M. I., & Piatetskii-Shapiro, I. I. (1990). *Representation theory and automorphic functions*. London: Academic.
5. Bump, D. (1998). *Automorphic forms and representations*. Cambridge: Cambridge University Press.
6. Ramakrishnan, D., & Valenza, R. J. (1999). *Fourier analysis on number fields*. Berlin: Springer.
7. Benedetto, J. J., & Benedetto, R. L. (2004). *Journal of Geometric Analysis*, *14*, 423.
8. Benedetto, R. L. (2004). *Contemporary Mathematics*, *435*, 27.
9. Lang, W. C., (1996). *SIAM Journal on Mathematical Analysis*, *27*, 305.
10. Shelkovich, V. M., & Skopina, M. (2009). *Journal of Fourier Analysis and Appllications*, *15*, 366.
11. Khrennikov, A., & Shelkovich, V. M. (2010). *Applied and Computational Harmonic Analysis*, *28*, 1.
12. Albeverio, S., Khrennikov, A., & Shelkovich, V. M. (2010). *Theory of p-adic distributions: Linear and non-linear models*. Cambridge: Cambridge University Press.
13. Vladimirov, V. S., & Volovich, I. V. (1989). *Communications in Mathematical Physics*, *123*, 659.
14. Meurice, Y. (1991). *Communications in Mathematical Physics*, *135*, 303.
15. Haran, S. (1993). *In Annales de l'institut Fourier*, *43*, 997.
16. Zelenov, E. I. (1993). *Communications in Mathematical Physics*, *155*, 489.
17. Vladimirov, V. S., Volovich, I. V., & Zelonov, E. I. (1994). *p-adic analysis and mathematical physics*. Singapore: World Scientific.
18. Dragovoch, B. (1994). *Theoretical and Mathematical Physics*, *101*, 1404.
19. Dragovich, B. (1995). *International Journal of Modern Physics A*, *10*, 2349.
20. Albeverio, S., Cianci, R., & Khrennikov, A. (1997). *Journal of Physics A*, *30*, 881.
21. Albeverio, S., Cianci, R., & Khrennikov, A. (1997). *Journal of Physics A*, *30*, 5767.
22. Varadarajan, V. S. (1997). *Letters in Mathematical Physics*, *39*, 97.
23. Dragovich, B. (1998). *Integral Transforms and Special Functions*, *6*, 197–203.
24. Djordjevic, G. S., Nesic, L. J., & Dragovich, B. (1999). *Modern Physics Letters A*, *14*, 317.
25. Vourdas, A. (2008). *Journal of Physics A*, *41*, 455303.
26. Dragovich, B., Khrenikov, A., Kozyrev, S. V., & Volovich, I. V. (2009). *P-adic Numbers Ultrametic Analysis and Applications*, *1*, 1.

27. Vourdas, A. (2010). *J. Fourier Anal. Appl.*, *16*, 748.
28. Albeverio, S., Khrennikov, A., & Shelkovich, V. M. (2010). *Theory of p-adic distributions*. Cambridge: Cambridge University Press.
29. Vourdas, A. (2011). *Journal of Mathematical Physics*, *52*, 062103.
30. Vourdas, A. (2012). *Journal of Mathematical Analysis and Applications*, *394*, 48.
31. Vourdas, A. (2012). *Journal of Mathematical Physics*, *53*, 122101.
32. Vourdas, A. (2013). *Journal of Physics A*, *46*, 043001.
33. Rammal, R., Toulouse, G., & Virasoro, M. A. (1986). *Reviews of Modern Physics*, *58*, 765.
34. Khrennikov, A Yu., & Kozyrev, S. V. (2006). *Physica A*, *359*, 222.
35. Khrennikov, A Yu., & Kozyrev, S. V. (2006). *Physica A*, *359*, 241.
36. Khrennikov, A Yu., & Kozyrev, S. V. (2007). *Physica A*, *378*, 283.
37. Brekke, L., Freund, P., Olson, M., & Witten, E. (1988). *Nuclear Physics B*, *302*, 365.
38. Aref'eva, I. Y., Dragovich, B., & Volovich, I. V. (1988). *Physics Letters B*, *209*, 445.
39. Brekke, L., & Freund, P. (1993). *Physics Reports*, *233*, 1.
40. Ruelle, Ph, Thiran, E., Verstegen, D., & Weyers, J. (1989). *Journal of Mathematical Physics*, *30*, 2854–2874.
41. Vladimirov, V. S. (2005). *Russian Mathematical Surveys*, *60*, 1077.
42. Zelonov, E. I. (1991). *Journal of Mathematical Physics*, *32*, 147.
43. Hehner, E., & Horspool, R. N. (1979). *SIAM Journal on Computing*, *8*, 124.
44. Weil, A. (1964). *Acta Mathematica*, *111*, 143.
45. Bourbaki, N. (1966). *'General topology', part 1*. Paris: Hermann.

Chapter 12
A Quantum System with Positions in the Profinite Group $\widehat{\mathbb{Z}}$

Abstract Quantum systems with positions in $\hat{\mathbb{Z}}$ and momenta in $\mathbb{Q}/\mathbb{Z}$, are discussed. The Schwartz-Bruhat space of wavefunctions in these systems, is presented. The Heisenberg- Weyl group as a locally compact and totally disconnected topological group, is discussed. Wigner and Weyl functions in this context, are also discussed.

In this chapter we discuss the quantum system $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, with positions in the profinite group $\widehat{\mathbb{Z}}$ and momenta in its Pontryagin dual group $\mathbb{Q}/\mathbb{Z}$. This system is factorized in terms of the systems $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ studied in the previous chapter. This factorization is a generalization of the factorization in Sect. 4.9 for the finite case.

Intuitively, $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ is the system $\Sigma[\mathbb{Z}(d)]$ with $d = \Upsilon$. All finite quantum systems $\Sigma[\mathbb{Z}(d)]$ are subsystems of $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$. Also all systems $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ with all prime values p, are subsystems of $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$.

The set of the systems $\Sigma[\mathbb{Z}(d)]$ where $d \in \mathbb{N}$, with the order subsystem, is a directed partial order. It is not directed-complete partial order, but when we add the $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ (and also some other systems like the $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ with all prime values p), it becomes a directed-complete partial order.

Like the previous chapter, this one also belongs to the general area of p-adic physics. As we explained there, we approach this area from a novel angle, that involves inverse and direct limits and profinite groups, to provide a rigorous approach to study of the systems $\Sigma[\mathbb{Z}(d)]$, with very large d.

Some of the material in this section is based on Refs. [1, 2], by the author. Other general references are [3–13].

12.1 The System $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$

We first discuss the convergence of integrals related to the system $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$. This discussion motivates our definition of the Schwartz-Bruhat space for the system $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, later.

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8_12

The integral of a function

$$f(x) = \prod_{p\in\Pi} f_p(x_p); \quad x \in \widehat{\mathbb{Z}}; \quad f_p(x_p) \in \mathscr{A}_p(0,*); \quad x_p \in \mathbb{Z}_p, \tag{12.1}$$

over $\widehat{\mathbb{Z}}$, is given by the product

$$\int_{\widehat{\mathbb{Z}}} f(x)dx = \prod_{p\in\Pi} \int_{\mathbb{Z}_p} f_p(x_p)dx_p. \tag{12.2}$$

Each of the 'factor integrals' in the product converges because $f_p(x_p) \in \mathscr{A}_p(0,*)$. But the product will converge to a non-zero number, only in the case that most of the integrals in the product are equal 1. As we explained earlier, the term 'most' means, all except a finite number. For this reason, in the definition of the Schwartz-Bruhat space below, we require that most of the factor functions in the product of Eq. (12.1) are $f_p(x_p) = 1$.

Similarly, the integral of a function

$$F(\mathfrak{p}) = \prod_{p\in\Pi} F_p(\mathfrak{p}_p); \quad \mathfrak{p} \in \mathbb{Q}/\mathbb{Z}; \quad F_p(\mathfrak{p}_p) \in \mathscr{A}(*,0); \quad \mathfrak{p}_p \in \mathbb{Q}_p/\mathbb{Z}_p, \tag{12.3}$$

over $\mathbb{Q}/\mathbb{Z}$, is given by the product

$$\int_{\mathbb{Q}/\mathbb{Z}} F(\mathfrak{p})d\mathfrak{p} = \prod_{p\in\Pi} \int_{\mathbb{Q}_p/\mathbb{Z}_p} F_p(\mathfrak{p}_p)d\mathfrak{p}_p. \tag{12.4}$$

Each of the factor integrals in the product converges because $F_p(\mathfrak{p}_p) \in \mathscr{A}_p(*,0)$. But the product will converge to a non-zero number, only in the case that most of the integrals in the product are equal 1. For this reason, in the definition of the Schwartz-Bruhat space below, we require that most of the factor functions in the product of Eq. (12.3) are $F_p(\mathfrak{p}_p) = \Delta_p(\mathfrak{p}_p)$ (defined in Eq. (11.32)), so that the corresponding integrals are equal to 1.

With these comments in mind, we define the Schwartz-Bruhat space for the system $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ as follows:

Definition 12.1 The Schwartz-Bruhat space $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ [6, 9, 10] is defined by one of the following two ways which are related through a Fourier transform, and are equivalent to each other:

(1) It consists of finite linear combinations of complex functions as in Eq. (12.1), where for most prime values p, the $f_p(x_p) = 1$. The scalar product is given by

$$(f, g) = \int_{\widehat{\mathbb{Z}}} [f(x)]^* g(x)dx. \tag{12.5}$$

This integral is defined by a product, analogous to Eq. (12.2).

(2) It consists of finite linear combinations of complex functions as in Eq. (12.3), where for most prime values p, the $F_p(\mathfrak{p}_p) = \Delta_p(\mathfrak{p}_p)$. The scalar product is given by

$$(F, G) = \int_{\mathbb{Q}/\mathbb{Z}} [F(\mathfrak{p})]^* G(\mathfrak{p}) d\mathfrak{p}. \tag{12.6}$$

This integral is defined by a product, analogous to Eq. (12.4).

We note that the requirement in the first definition that most $f_p(x_p) = 1$, is related through a Fourier transform, to the requirement in the second definition that most $F_p(\mathfrak{p}_p) = \Delta_p(\mathfrak{p}_p)$.

The Schwartz-Bruhat space $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, is a subspace of the tensor product of the Schwartz-Bruhat spaces $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$. This is because in $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, we have the extra requirement that in the products of Eq. (12.1) most of the $f_p(x_p) = 1$, and also in the products of Eq. (12.3) most of the $F_p(\mathfrak{p}_p) = \Delta_p(\mathfrak{p}_p)$. The restricted tensor product [9, 10], defined below, is precisely the tensor product with this restriction imposed on it.

Definition 12.2 The restricted tensor product of the spaces $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ is the space of finite linear combinations of complex functions as in Eq. (12.1), with the restriction that most of the factor functions in the product are $f_p(x_p) = 1$. Equivalently, it is the space of finite linear combinations of complex functions as in Eq. (12.3), with the restriction that most of the factor functions in the product are $F_p(\mathfrak{p}_p) = \Delta_p(\mathfrak{p}_p)$. The notation for the restricted tensor product is the usual tensor product notation with a prime:

$$\bigotimes_{p\in\Pi}{}' \mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]. \tag{12.7}$$

It is clear that the Schwartz-Bruhat space $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ is isomorphic to the restricted tensor product of the spaces $\mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$:

$$\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})] \cong \bigotimes_{p\in\Pi}{}' \mathscr{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]. \tag{12.8}$$

12.2 Fourier Transforms

The Fourier transform in $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, is given by

$$[\mathfrak{F} f](\mathfrak{p}) = \widetilde{f}(\mathfrak{p}) = \int_{\widehat{\mathbb{Z}}} dx\ \chi(-x\mathfrak{p}) f(x); \qquad \mathfrak{p} \in \mathbb{Q}/\mathbb{Z}. \tag{12.9}$$

The inverse Fourier transform is

$$[\mathfrak{F}^{-1} \widetilde{f}](x) = \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p} \chi(x\mathfrak{p}) f(\mathfrak{p}); \qquad x \in \widehat{\mathbb{Z}}. \tag{12.10}$$

The Fourier transform is related to the Fourier transforms in the factor systems, as follows:

$$\mathfrak{F} = \bigotimes_{p\in\Pi} \mathfrak{F}_p. \tag{12.11}$$

The usual properties of Fourier transforms, hold here also. For example,

$$\mathfrak{F}^4 = \mathbf{1}; \quad (f, g) = (\widetilde{f}, \widetilde{g}). \tag{12.12}$$

Delta functions in the present context are given by

$$\delta(x) = \prod_{p\in\Pi} \delta_p(x_p); \quad \Delta(\mathfrak{p}) = \prod_{p\in\Pi} \Delta_p(\mathfrak{p}_p). \tag{12.13}$$

$\Delta(\mathfrak{p})$ can also be defined as

$$\begin{aligned} &\Delta(\mathfrak{p}) = 1 \ \text{ if } \ \mathfrak{p} = 0 \\ &\Delta(\mathfrak{p}) = 0 \ \text{ if } \ \mathfrak{p} \neq 0; \quad \mathfrak{p} \in \mathbb{Q}/\mathbb{Z}. \end{aligned} \tag{12.14}$$

We note that the zero in $\mathbb{Q}/\mathbb{Z}$ is the coset with all the integers.

Then

$$\int_{\widehat{\mathbb{Z}}} dx \ f(x)\delta(x-a) = f(a); \quad \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p} \ F(\mathfrak{p})\Delta(\mathfrak{p}-\mathfrak{a}) = F(\mathfrak{a}) \tag{12.15}$$

Also the Fourier transform of the function $f(x) = 1$ is $\Delta(\mathfrak{p})$, and the Fourier transform of the function $F(\mathfrak{p})$ is the function $\delta(x)$:

$$\int_{\widehat{\mathbb{Z}}} dx \ \chi(x\mathfrak{p}) = \Delta(\mathfrak{p}); \quad \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p} \ \chi(x\mathfrak{p}) = \delta(x). \tag{12.16}$$

12.2.1 Change of Variables

From Eqs. (11.10), (11.20), it follows that a change in the variables $x' = \lambda x$ or $\mathfrak{p}' = \lambda\mathfrak{p}$, is performed as follows:

$$\begin{aligned} d(\lambda x) = \prod_{p\in\Pi} d(\lambda x_p) = \prod_{p\in\Pi} |\lambda|_p \, dx_p = \frac{1}{|\lambda|_\infty} dx; \qquad x \in \widehat{\mathbb{Z}}; \\ d(\lambda\mathfrak{p}) = \prod_{p\in\Pi} d(\lambda\mathfrak{p}_p) = \prod_{p\in\Pi} |\lambda|_p \, d\mathfrak{p}_p = \frac{1}{|\lambda|_\infty} d\mathfrak{p}; \qquad \mathfrak{p} \in \mathbb{Q}/\mathbb{Z}. \end{aligned} \tag{12.17}$$

We have used here Ostrowski's theorem (in Eq. (10.11)).

Using Eq. (11.19) with $\lambda = 2$ and all primes, we find that:

$$\frac{1}{2}\int_{\mathbb{Q}/2^{-1}\mathbb{Z}} d\mathfrak{a}\, f(2\mathfrak{a}) = \int_{\mathbb{Q}/\mathbb{Z}} d(2\mathfrak{a})\, f(2\mathfrak{a}) = \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{a}'\, f(\mathfrak{a}') \tag{12.18}$$

Here the $\mathfrak{a}$ takes values in $\mathbb{Q}/2^{-1}\mathbb{Z}$, and therefore the $2\mathfrak{a}$ takes values in $\mathbb{Q}/\mathbb{Z}$.

12.3 The Heisenberg-Weyl Group $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$

The phase space of the system $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ is $\widehat{\mathbb{Z}} \times (\mathbb{Q}/\mathbb{Z})$, and we define displacement operators and the Heisenberg-Weyl group.

Definition 12.3 The displacement operators $D(\mathfrak{a}, b)$ map the functions $f(x)$ and $F(\mathfrak{p})$ in $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, into the following functions in $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$:

$$\begin{aligned} &[D(\mathfrak{a}, b)\, f](x) = \chi\,(-\mathfrak{a}b + 2\mathfrak{a}x)\, f(x - b) \\ &[D(\mathfrak{a}, b) F](\mathfrak{p}) = \chi\,(\mathfrak{a}b - \mathfrak{p}b)\, F(\mathfrak{p} - 2\mathfrak{a}) \\ &\mathfrak{a}, \mathfrak{p} \in \mathbb{Q}/\mathbb{Z}; \qquad b, x \in \widehat{\mathbb{Z}}. \end{aligned} \tag{12.19}$$

We have explained earlier that in the $\mathfrak{a} = (\mathfrak{a}_2, ..., \mathfrak{a}_p, ...) \in \mathbb{Q}/\mathbb{Z}$ most of the $\mathfrak{a}_p$ are equal to zero. The same is true for $\mathfrak{p}$. This is important in proving that the $[D(\mathfrak{a}, b)\, f](x)$ and $[D(\mathfrak{a}, b) F](\mathfrak{p})$ belong to the space $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$.

Definition 12.4 Let $\{G_i | i \in I\}$ be a set of locally compact groups. We denote as g_i the elements of G_i. Also let H_i be a compact subgroup of G_i (for all $i \in I$). The restricted direct product of the groups G_i with respect to their compact subgroups H_i, is the [9, 10]

$$\prod_i{}' G_i = \{(g_1, g_2, ...) \mid g_i \in H_i \text{ for most indices } i \in I\}. \tag{12.20}$$

The restricted direct product of groups, is a subgroup of the direct product of groups (because there is a restriction imposed on it).

Proposition 12.1 *(1) The displacement operators $D(\mathfrak{a}, b)\chi(\mathfrak{c})$ form a representation of the Heisenberg-Weyl group $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ (the notation indicates the sets in which the variables $\mathfrak{a}, b, \mathfrak{c}$ belong).*

(2) The Heisenberg-Weyl group $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ is the restricted direct product of the groups $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$ with respect to their compact subgroups $HW_2(\mathbb{Z}_p) \cong \mathbb{Z}_p$ (defined in Eq. (11.45)):

$$HW[(\mathbb{Q}/\mathbb{Z}),\widehat{\mathbb{Z}},(\mathbb{Q}/\mathbb{Z})]=\prod_{p\in\Pi}{}'HW[(\mathbb{Q}_p/\mathbb{Z}_p),\mathbb{Z}_p,(\mathbb{Q}_p/\mathbb{Z}_p)] \quad (12.21)$$

Proof (1) Using the definition in Eq. (12.19), we prove the multiplication rule

$$D(\mathfrak{a},b)D(\mathfrak{a}',b')=D(\mathfrak{a}+\mathfrak{a}',b+b')\chi(\mathfrak{a}b'-\mathfrak{a}'b) \quad (12.22)$$

Comparison with the Definition 4.2, shows that we have a representation of the Heisenberg-Weyl group.

(2) We use the notation $\mathfrak{a}=(\mathfrak{a}_2,...,\mathfrak{a}_p,...)\in\mathbb{Q}/\mathbb{Z}$, where most $\mathfrak{a}_p$ are equal to zero. We also use a similar notation for the other variables in $\mathbb{Q}/\mathbb{Z}$.
We then consider Eq. (11.42) with all $p\in\Pi$, and multiply all these equations. In this way we prove that

$$D(\mathfrak{a},b)=\prod_{p\in\Pi}D_p(\mathfrak{a}_p,b_p). \quad (12.23)$$

Since most $\mathfrak{a}_p$ are equal to zero, it follows that most $D_p(\mathfrak{a}_p,b_p)=D_p(0,b_p)$ belong to the compact group $HW_2(\mathbb{Z}_p)\cong\mathbb{Z}_p$.
We also prove that

$$\chi\left(\mathfrak{c}+\mathfrak{a}b-\mathfrak{p}b\right)=\prod_{p\in\Pi}\chi_p\left(\mathfrak{c}_p+\mathfrak{a}_pb_p-\mathfrak{p}_pb_p\right). \quad (12.24)$$

Here most of the factors are equal to 1. Combining the above two points proves this part of the proposition.

12.3.1 $HW[(\mathbb{Q}/\mathbb{Z}),\widehat{\mathbb{Z}},(\mathbb{Q}/\mathbb{Z})]$ as a Locally Compact and Totally Disconnected Topological Group

We define the following subgroups of $HW[(\mathbb{Q}/\mathbb{Z}),\widehat{\mathbb{Z}},(\mathbb{Q}/\mathbb{Z})]$:

$$\begin{aligned}&HW_1(\mathbb{Q}/\mathbb{Z})=\{D(\mathfrak{a},0)\mid\mathfrak{a}\in\mathbb{Q}/\mathbb{Z}\}\cong\mathbb{Q}/\mathbb{Z}\\&HW_2(n\widehat{\mathbb{Z}})=\{D(0,b)\mid b\in n\widehat{\mathbb{Z}}\}\cong n\widehat{\mathbb{Z}}\\&HW_3(\mathbb{Q}/\mathbb{Z})=\{\chi(\mathfrak{c})\mid\mathfrak{c}\in\mathbb{Q}/\mathbb{Z}\}\cong\mathbb{Q}/\mathbb{Z}.\end{aligned} \quad (12.25)$$

If n_1 is a divisor of n_2, then $HW_2(n_2\widehat{\mathbb{Z}})\prec HW_2(n_1\widehat{\mathbb{Z}})$. The set

$$\mathfrak{N}=\{HW[(\mathbb{Q}/\mathbb{Z}),\widehat{\mathbb{Z}},(\mathbb{Q}/\mathbb{Z})]\}\cup\{HW_2(n\widehat{\mathbb{Z}})\mid n\in\mathbb{N}\} \quad (12.26)$$

with the order subgroup, is a partially ordered set.

Proposition 12.2 *We regard the set $\mathfrak{N}$ in Eq. (12.26), as a fundamental system of open neighborhoods of the identity of the group $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$. Then the $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ becomes a topological group, which is totally disconnected and locally compact.*

Proof The proof is similar to the proof of Proposition 11.5.

Remark 12.1 In analogy with Remark 11.3, we define another representation of the Heisenberg-Weyl group, although it is not relevant for Physics. This is the profinite Heisenberg-Weyl group $HW(\widehat{\mathbb{Z}}, \widehat{\mathbb{Z}}, \widehat{\mathbb{Z}})$, and is different from the $HW[(\mathbb{Q}/\mathbb{Z}), \widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ (which is not profinite).

The $HW(\widehat{\mathbb{Z}}, \widehat{\mathbb{Z}}, \widehat{\mathbb{Z}})$ is defined as the inverse limit of the finite Heisenberg-Weyl groups $HW[\mathbb{Z}(d), \mathbb{Z}(d), \mathbb{Z}(d)]$. If k is a divisor of n ($k \prec n$), we define the homomorphisms

$$\widetilde{\psi}_{kn} : \quad HW[\mathbb{Z}(k), \mathbb{Z}(k), \mathbb{Z}(k)] \quad \leftarrow \quad HW[\mathbb{Z}(n), \mathbb{Z}(n), \mathbb{Z}(n)], \tag{12.27}$$

where

$$\begin{aligned} &\widetilde{\psi}_{kn}[D(\alpha_n, \beta_n)\omega_n(\gamma_n)] = D(\alpha_k, \beta_k)\omega_k(\gamma_k) \\ &\alpha_k = \psi_{kn}(\alpha_n); \quad \beta_k = \psi_{kn}(\beta_n); \quad \gamma_k = \psi_{kn}(\gamma_n) \end{aligned} \tag{12.28}$$

The map ψ_{kn} has been defined in Eq. (10.67). The $\widetilde{\psi}_{kn}$ are compatible, and the $\{HW[\mathbb{Z}(p^n), \mathbb{Z}(p^n), \mathbb{Z}(p^n)], \widetilde{\psi}_{kn}\}$ is an inverse system, whose inverse limit we denote as $HW(\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p)$.

The elements of this group are $\mathfrak{D}(a, b)\chi(c)$, where

$$\begin{aligned} &\mathfrak{D}(a, b) = (D(\alpha_2, \beta_2), D(\alpha_3, \beta_3), ...) \\ &\chi(c) = (\omega_2(\gamma_2), \omega_3(\gamma_3), ...) \\ &a = (\alpha_2, \alpha_3, ...); \qquad b = (\beta_2, \beta_3, ...); \qquad c = (\gamma_2, \gamma_3, ...) \\ &a, b, c \in \widehat{\mathbb{Z}}; \quad \alpha_k, \beta_k, \gamma_k \in \mathbb{Z}(k) \end{aligned} \tag{12.29}$$

The a, b, c are elements $\widehat{\mathbb{Z}}$ written in the representation of Eq. (10.71) (see also Remark 10.4). Only the elements with indices which are powers of primes are need to define uniquely these sequences. This follows from the Chinese remainder theorem. Consequently

$$\begin{aligned} &\mathfrak{D}(a, b) = (\mathfrak{D}_2(a_2, b_2), \mathfrak{D}_3(a_3, b_3), ...) \\ &\chi(c) = (\chi_2(c_2), \chi_3(c_3), \chi_5(c_5), ...); \quad c = (c_2, c_3, ...) \\ &a, b, c \in \widehat{\mathbb{Z}}; \quad a_p, b_p, c_p \in \mathbb{Z}_p. \end{aligned} \tag{12.30}$$

The $\mathfrak{D}_p(a_p, b_p)$ have been defined in Eq. (11.53). We stress that the $\mathfrak{D}(a, b)$ where $a, b \in \widehat{\mathbb{Z}}$, are very different from the $D(\mathfrak{a}, b)$ where $\mathfrak{a} \in \mathbb{Q}/\mathbb{Z}$, and $b \in \widehat{\mathbb{Z}}$.

The Pontryagin dual group to $\widehat{\mathbb{Z}}$ does not appear in $HW(\widehat{\mathbb{Z}}, \widehat{\mathbb{Z}}, \widehat{\mathbb{Z}})$. Therefore it cannot be associated with displacements of dual quantum variables. It is a representation of the Heisenberg-Weyl group, which is not relevant to quantum mechanics.

12.4 Wigner and Weyl Functions

Many of the results in this section are analogous to those in Sect. 11.6, and we present them without proof [1, 2]. Our notation and presentation aims to make clear this analogy. However, there is a difference in cases where we have to change variables in integrals, because we get different constants.

We consider an operator $\theta(x, y)$ where $x, y \in \widehat{\mathbb{Z}}$, and let

$$\widetilde{\theta}(\mathfrak{p}, \mathfrak{p}') = \int_{\widehat{\mathbb{Z}}} dx_p \int_{\widehat{\mathbb{Z}}} dy \theta(x, y) \chi(-x\mathfrak{p} + y\mathfrak{p}'); \quad \mathfrak{p}, \mathfrak{p}' \in \mathbb{Q}/\mathbb{Z}. \tag{12.31}$$

θ acts on a function $f(x)$, and its Fourier transform $\widetilde{f}(\mathfrak{p})$, as:

$$\begin{aligned} (\theta f)(x) &= \int_{\widehat{\mathbb{Z}}} dy \theta(x, y) f(y) \\ (\theta \widetilde{f})(\mathfrak{p}) &= \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}' \widetilde{\theta}(\mathfrak{p}, \mathfrak{p}') \widetilde{f}(\mathfrak{p}') \end{aligned} \tag{12.32}$$

The trace of θ is given by

$$\mathrm{tr}\theta = \int_{\widehat{\mathbb{Z}}} dx \theta(x, x) = \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p} \widetilde{\theta}(\mathfrak{p}, \mathfrak{p}). \tag{12.33}$$

Definition 12.5 The parity operator with respect to the point $(\mathfrak{a}, b)$ in the phase space $(\mathbb{Q}/\mathbb{Z}) \times \widehat{\mathbb{Z}}$, is

$$P(\mathfrak{a}, b) = [D(\mathfrak{a}, b)]^\dagger \, \mathfrak{F}^2 \, D(\mathfrak{a}, b) = [D(2\mathfrak{a}, 2b)]^\dagger \, \mathfrak{F}^2 = \mathfrak{F}^2 \, D(2\mathfrak{a}, 2b). \tag{12.34}$$

Proposition 12.3 *(1) The parity operator acts on wavefunctions in* $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, *as follows:*

$$\begin{aligned} P(\mathfrak{a}, b) f(x_p) &= \chi(-4\mathfrak{a}b - 4\mathfrak{a}x) f(-x - 2b) \\ P(\mathfrak{a}, b) \widetilde{f}(\mathfrak{p}) &= \chi(4\mathfrak{a}b + 2\mathfrak{p}b) \widetilde{f}(-\mathfrak{p} - 4\mathfrak{a}). \end{aligned} \tag{12.35}$$

(2)

$$[P(\mathfrak{a}, b)]^2 = \mathbf{1}; \quad P\left(\mathfrak{a} + \frac{1}{4}, b\right) = P(\mathfrak{a}, b). \tag{12.36}$$

Proof The proof is analogous to the proof of Proposition 11.6.

Definition 12.6 The Weyl function $\widetilde{W}(\mathfrak{a}, b; \theta)$ and the Wigner function $W(\mathfrak{a}, b; \theta)$ of an operator θ, are given by:

$$\begin{aligned} \widetilde{W}(\mathfrak{a}, b; \theta) &= \mathrm{tr}[D(-\mathfrak{a}, -b)\theta]; \quad \mathfrak{a} \in \mathbb{Q}/\mathbb{Z}; \quad b \in \widehat{\mathbb{Z}} \\ W(\mathfrak{a}, b; \theta) &= \mathrm{tr}[\theta P(\mathfrak{a}, b)]. \end{aligned} \tag{12.37}$$

Proposition 12.4 *(1) The Weyl function is given by*

$$\widetilde{W}(\mathfrak{a}, b; \theta) = \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}\ \chi\ (\mathfrak{a}b + \mathfrak{p}b)\, \widetilde{\theta}(\mathfrak{p} + 2\mathfrak{a}, \mathfrak{p}) \tag{12.38}$$

(2) The Wigner function is given by

$$W(\mathfrak{a}, b; \theta) = \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}\ \chi(-4\mathfrak{a}b - 2\mathfrak{p}b)\widetilde{\theta}(\mathfrak{p}, -\mathfrak{p} - 4\mathfrak{a}). \tag{12.39}$$

Proof The proof is analogous to the proof of Proposition 11.7.

Proposition 12.5 *The parity operators are related to the displacement operators through a Fourier transform:*

$$P(\mathfrak{a}, b) = \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{a}' \int_{\widehat{\mathbb{Z}}} db'\ D(\mathfrak{a}', b')\chi(2\mathfrak{a}'b - 2\mathfrak{a}b'). \tag{12.40}$$

Also the Wigner function is related to the Weyl function through a Fourier transform:

$$W(\mathfrak{a}, b; \theta) = \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{a}' \int_{\mathbb{Z}} db'\ \widetilde{W}(-\mathfrak{a}', -b')\chi(2\mathfrak{a}'b - 2\mathfrak{a}b'). \tag{12.41}$$

Proof The proof is analogous to the proof of Proposition 11.8.

Proposition 12.6 *Let θ be a trace class operator acting on functions in $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$. Then*

(1)

$$\frac{1}{2} \int_{\mathbb{Q}/2^{-1}\mathbb{Z}} d\mathfrak{a} \int_{\widehat{\mathbb{Z}}} db\ D(\mathfrak{a}, b)\ \theta\ [D(\mathfrak{a}, b)]^{\dagger} = \mathbf{1}\mathrm{tr}\theta. \tag{12.42}$$

(2) θ can be expanded in terms of displacement operators, with the Weyl function as coefficients:

$$\theta = \frac{1}{2} \int_{\mathbb{Q}/2^{-1}\mathbb{Z}} d\mathfrak{a} \int_{\widehat{\mathbb{Z}}} db\ D(\mathfrak{a}, b)\widetilde{W}(\mathfrak{a}, b; \theta). \tag{12.43}$$

Proof (1) We act with $D(\mathfrak{a}, b)\ \theta\ [D(\mathfrak{a}, b)]^\dagger$ on a function $F(\mathfrak{p}) \in \mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$ and we get

$$\left[D(\mathfrak{a}, b)\ \theta\ [D(\mathfrak{a}, b)]^\dagger F\right](\mathfrak{p}) = \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}'\ \chi(2\mathfrak{a}b - \mathfrak{p}b + \mathfrak{p}'b) \times \theta(\mathfrak{p} - 2\mathfrak{a}, \mathfrak{p}')\ F(\mathfrak{p}' + 2\mathfrak{a}). \tag{12.44}$$

The scalar product of this with an arbitrary function $G(\mathfrak{p}) \in \mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, gives

$$\begin{aligned}
&\int_{\mathbb{Q}/2^{-1}\mathbb{Z}} d\mathfrak{a} \int_{\mathbb{Z}} db\ \left(G, D(\mathfrak{a}, b)\ \theta\ [D(\mathfrak{a}, b)]^\dagger F\right) \\
&= \int_{\mathbb{Q}/2^{-1}\mathbb{Z}} d\mathfrak{a} \int_{\mathbb{Z}} db \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p} \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}'\ [G(\mathfrak{p})]^* \\
&\times \chi(2\mathfrak{a}b - \mathfrak{p}b + \mathfrak{p}'b)\theta(\mathfrak{p} - 2\mathfrak{a}, \mathfrak{p}')\ F(\mathfrak{p}' + 2\mathfrak{a}) \\
&= \int_{\mathbb{Q}/2^{-1}\mathbb{Z}} d\mathfrak{a} \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p} \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}'\ [G(\mathfrak{p})]^* \\
&\times \Delta(2\mathfrak{a} - \mathfrak{p} + \mathfrak{p}')\theta(\mathfrak{p} - 2\mathfrak{a}, \mathfrak{p}')\ F(\mathfrak{p}' + 2\mathfrak{a})
\end{aligned} \tag{12.45}$$

We now change the variable $2\mathfrak{a}$ into $\mathfrak{a}'$, using Eq. (12.18). We get:

$$\int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}\ [G(\mathfrak{p})]^*\ F(\mathfrak{p}) \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}'\ \theta(\mathfrak{p}', \mathfrak{p}') = (G, F)\mathrm{tr}(\theta). \tag{12.46}$$

This proves the proposition.

(2) The operator in Eq. (12.43) acts on an arbitrary function $F(\mathfrak{p}) \in \mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$, as follows (use Eq. (11.63)):

$$\begin{aligned}
&\int_{\mathbb{Q}/2^{-1}\mathbb{Z}} d\mathfrak{a} \int_{\widehat{\mathbb{Z}}} db \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}_p \int_{\mathbb{Q}_p/\mathbb{Z}_p} d\mathfrak{p}'\ \chi\ (\mathfrak{a}b + \mathfrak{p}b) \\
&\times \widetilde{\theta}(\mathfrak{p} + 2\mathfrak{a}, \mathfrak{p})\chi\left(\mathfrak{a}b - \mathfrak{p}'b\right) F(\mathfrak{p}' - 2\mathfrak{a}) \\
&= \int_{\mathbb{Q}/2^{-1}\mathbb{Z}} d\mathfrak{a} \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p} \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}'\ \widetilde{\theta}(\mathfrak{p} + 2\mathfrak{a}, \mathfrak{p}) \\
&\times \Delta(2\mathfrak{a} + \mathfrak{p} - \mathfrak{p}')F(\mathfrak{p}' - 2\mathfrak{a})
\end{aligned} \tag{12.47}$$

We now change the variable $2\mathfrak{a}$ into $\mathfrak{a}'$, using Eq. (12.18): We get

$$\int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p} \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}'\ \widetilde{\theta}(\mathfrak{p}', \mathfrak{p})F(\mathfrak{p}) \tag{12.48}$$

This proves the proposition.

Proposition 12.7 *Let θ be a trace class operator acting on functions in the Schwartz-Bruhat space $\mathscr{B}[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$. Then*

(1)

$$\frac{1}{8}\int_{\mathbb{Q}/2^{-2}\mathbb{Z}} d\mathfrak{a} \int_{2^{-1}\widehat{\mathbb{Z}}} db\ P(\mathfrak{a}, b)\ \theta\ P(\mathfrak{a}, b) = \mathbf{1}\mathrm{tr}\theta. \tag{12.49}$$

(2) θ can be expanded in terms of parity operators, with the Wigner function as coefficients:

$$\theta = \frac{1}{8}\int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{a} \int_{2^{-1}\widehat{\mathbb{Z}}} db\ P(\mathfrak{a}, b) W(\mathfrak{a}, b; \theta). \tag{12.50}$$

Proof (1) We substitute $\mathfrak{a}$ with $2\mathfrak{a}$ and b with $2b$ in Eq. (12.42), and change accordingly the domains of integration. We also take into account Eq. (12.17). We get

$$\frac{1}{8}\int_{\mathbb{Q}/2^{-2}\mathbb{Z}} d\mathfrak{a} \int_{2^{-1}\mathbb{Z}_p} db\ D(2\mathfrak{a}, 2b)\ \theta\ [D(2\mathfrak{a}, 2b)]^{\dagger} = \mathbf{1}\mathrm{tr}\theta. \tag{12.51}$$

Then we multiply each side with $\mathfrak{F}^2$ on the left and with $[\mathfrak{F}^2]^{\dagger}$ on the right, and we prove the statement.

(2) We substitute Eq. (12.39) on the right hand side of Eq. (12.50), and act on an arbitrary function $F(\mathfrak{p})$:

$$\begin{aligned}&\frac{1}{8}\int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{a} \int_{2^{-1}\widehat{\mathbb{Z}}} db \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}'\ \widetilde{\theta}(\mathfrak{p}', -\mathfrak{p}' - 4\mathfrak{a})\\ &\times \chi(-4\mathfrak{a}b - 2\mathfrak{p}'b)\chi(4\mathfrak{a}b + 2\mathfrak{p}b) F(-\mathfrak{p} - 4\mathfrak{a})\end{aligned} \tag{12.52}$$

Integration over $2b$ gives,

$$\begin{aligned}&\frac{1}{4}\int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{a} \int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{p}'\ \widetilde{\theta}(\mathfrak{p}', -\mathfrak{p}' - 4\mathfrak{a})\\ &\times \Delta_p(\mathfrak{p}_p - \mathfrak{p}'_p) F(-\mathfrak{p} - 4\mathfrak{a})\\ &= \frac{1}{4}\int_{\mathbb{Q}/\mathbb{Z}} d\mathfrak{a}_p\ \widetilde{\theta}(\mathfrak{p}, -\mathfrak{p} - 4\mathfrak{a}) F(-\mathfrak{p} - 4\mathfrak{a})\end{aligned} \tag{12.53}$$

Now we change the variable $-\mathfrak{p} - 4\mathfrak{a}$ into $\mathfrak{q}$, using Eq. (12.17). We get the operator θ acting on the function $F(\mathfrak{p})$. This completes the proof.

Table 12.1 Some finite and profinite quantum systems. All them are subsystem of the $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$. S_1, S_2 are finite or infinite subsets of the set of prime numbers Π, such that $S_1 \cap S_2 = \emptyset$.

$\Sigma[\mathbb{Z}(d)]$
$\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$
$\Sigma[\mathbb{Z}(\mathscr{E}), C(\mathscr{E})]$
$\Sigma\left[\prod_{p\in S_1}\mathbb{Z}(p^{e_p}) \times \prod_{p\in S_2}\mathbb{Z}_p, \sum_{p\in S_1}\mathbb{Z}(p^{e_p}) \oplus \sum_{p\in S_2}\mathbb{Q}_p/\mathbb{Z}_p\right]$
$\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$

12.5 The Directed-Complete Partial Order of Subsystems Of $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$

In Sect. 10.11 we studied the directed-complete partial order $\mathbb{N}_S^{(G,\widetilde{G})}$ which contains pairs of groups $G = \mathbb{Z}(p^k)$ and $\widetilde{G} = C(p^k)$ which are Pontryagin dual to each other. To each of these pairs corresponds a quantum system $\Sigma(G, \widetilde{G})$. The set $\mathbb{N}_S^Q$ of these quantum systems (the superfix Q indicates quantum systems), is a directed-complete partial order, with supremum the $\Sigma[\widehat{\mathbb{Z}}, (\mathbb{Q}/\mathbb{Z})]$. Some examples of systems in $\mathbb{N}_S^Q$ are shown in Table 12.1 (which is based on Table 10.1).

The set of finite quantum systems $\Sigma[\mathbb{Z}(d)]$ with the order subsystem, is a directed partial order. which is not complete. By adding to it, systems like those in Table 12.1, we get the set $\mathbb{N}_S^Q$ which is a directed-complete partial order [2].

12.6 Other Topics

An extension of the system studied in this section, is a quantum system with positions in $\mathbb{Q}$. In this case the Pontryagin dual group is $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$, where $\mathbb{A}_\mathbb{Q}$ is the group of adeles [14]. So the momenta take values in $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$. We have studied this in the context of harmonic analysis in [15]. None of these groups is profinite, and therefore this work is outside the remit of this monograph.

Below are some open questions related to profinite quantum systems:

- The study of mutually unbiased bases for profinite quantum systems.
- The Birkhoff-von Neumann lattice of subspaces, obeys the modularity property in the case of finite-dimensional Hilbert spaces, and violates it in the case of infinite-dimensional Hilbert spaces. Profinite groups are infinite, but inherit many properties from the finite groups. It is interesting to study whether modularity is valid in the lattice of subspaces of the Schwartz-Bruhat space of profinite quantum systems.

References

1. Vourdas, A. (2011). *Journal of Mathematical Physics*, *52*, 062103.
2. Vourdas, A. (2013). *Journal of Physics A*, *46*, 043001.
3. Gel'fand, I. M., & Graev, M. I. (1963). *Russian Mathematical Surveys*, *18*, 29–109.

4. Taibleson, M. H. (1975). *Fourier analysis on local fields*. Princeton: Princeton University Press.
5. Vladimirov, V. S. (1988). *Russian Mathematical Surveys*, *43*, 19.
6. Gel'fand, I. M., Graev, M. I., & Piatetskii-Shapiro, I. I. (1990). *Representation theory and automorphic functions*. London: Academic.
7. Dragovoch, B. (1994). *Theoretical and Mathematical Physics*, *101*, 1404.
8. Dragovich, B. (1995). *International Journal of Modern Physics A*, *10*, 2349.
9. Bump, D. (1998). *Automorphic forms and representations*. Cambridge: Cambridge University Press.
10. Ramakrishnan, D., & Valenza, R. J. (1999). *Fourier analysis on number fields*. Berlin: Springer.
11. Vladimirov, V. S., Volovich, I. V., & Zelonov, E. I. (1994). *p-adic analysis and mathematical physics*. Singapore: World Scientific.
12. Dragovich, B., Khrenikov, A., Kozyrev, S. V., & Volovich, I. V. (2009). P-adic numbers. *Ultrametic Analysis and Applications*, *1*, 1.
13. Albeverio, S., Khrennikov, A., & Shelkovich, V. M. (2010). *Theory of p-adic distributions*. Cambridge: Cambridge U. P.
14. Weil, A. (1973). *Basic number theory*. Berlin: Springer.
15. Vourdas, A. (2012). *Journal of Mathematical Analysis and Applications*, *394*, 48.

Index

A
Analytic representations, 49
Angle states, 93
Angular momentum states, 93

B
Boolean algebras, 77
Boolean rings, 80

C
Coherent density matrices, 30
Coherent projectors of rank n, 31
Coherent states, 29

D
Dedekind psi function, 12
Direct limits, 152
Disjunction in quantum versus classical computation, 83
Duality between finite geometries and weak mutually unbiased bases, 67

F
Finite geometries, 57
Fourier interferometry, 101
Frobenius transformations, 123
Functions with compact support, 161

G
Galois fields, 107
Galois groups, 108

H
Heisenberg-Weyl group $HW[GF(p^e)]$, 127
Heisenberg-Weyl group $HW[(\mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, 170
Heisenberg-Weyl group $HW[\mathbb{Z}(d)]$, 26
$HWSp[GF(p^e)]$, 133
$HWSpGal[GF(p^e)]$ group, 135
$HWSp[GF(p^e)]$ group, 133
$HWSp[\mathbb{Z}(d)]$ group, 36

I
Inverse limits, 152

L
Locally constant functions, 161

M
Modular lattices, 85
Mutually unbiased bases, 64

O
Orbital angular momentum states, 103

P
Padic numbers, 145
Parity operators acting on $H[GF(p^e)]$, 136
Parity operators acting on $H[\mathbb{Z}(d)]$, 37
Parity operators acting on $\mathcal{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, 173
Partial order, 7
Pontryagin duality, 9
Profinite group $\mathbb{Z}_p$, 153

A. Vourdas, *Finite and Profinite Quantum Systems*, Quantum Science and Technology, DOI 10.1007/978-3-319-59495-8

Q
$\mathbb{Q}_p/\mathbb{Z}_p$ as the Pontryagin dual group of $\mathbb{Z}_p$, 147

S
Schwartz-Bruhat space $\mathcal{B}[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, 168
$SpGal[GF(p^e)]$ group, 133
Subsystems of $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, 178
Supernatural (Steinitz) numbers, 8
Symplectic group $Sp[2, \mathbb{Z}(d)]$, 33
Symplectic group $Sp[2, GF(p^e)]$, 131

T
Totient functions, 12
Transpose intervals, 87

W
Weak mutually unbiased bases, 67
Weil transforms, 166
Weyl function for $\Sigma[GF(p^e)]$, 136
Weyl function for $\Sigma[\mathbb{Z}(d)]$, 41
Weyl functions for $\Sigma[\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}]$, 188
Weyl functions for $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, 173
Wigner function for $\Sigma[GF(p^e)]$, 136
Wigner function for $\Sigma[\mathbb{Z}(d)]$, 41
Wigner function for $\Sigma[\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}]$, 188
Wigner functions for $\Sigma[\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p)]$, 173