New R-matrices for small quantum groups

Dissertation
submitted with the aim
of achieving a doctoral degree
at the Faculty of Mathematics, Informatics
and Natural Sciences Department of Mathematics
at University of Hamburg

by

Daniel Nett

Hamburg
2015

Day of oral defense: 2015-03-16

The following evaluators recommend the admission of the dissertation:

Prof. Dr. Christoph Schweigert
Prof. Dr. Ingo Runkel

Table of Contents

Introduction

There is no uniform definition of the term quantum group in the literature, but in most cases, it is used for the class of Hopf algebras that may be roughly described as one-parameter deformations of the enveloping algebras of certain Lie algebras — and so do we in this thesis. They were introduced by Drinfeld [Dri85] and Jimbo [Jim85] in order to supply a solution to the quantum Yang-Baxter equation. Since quantum groups are Hopf algebras, the category of their representations is a tensor (also *monoidal*) category. If the quantum group is in addition quasitriangular, i.e. if an R-matrix exist, then the representation category is braided and in the case of finite-dimensional representations even ribbon. Braided categories have many important applications, especially to low-dimensional topology. In particular, ribbon categories give rise to invariants of knots in the Euclidean space $\mathbb{R}^3$. Under some additional non-degeneracy conditions one gets modular tensor categories which give rise to non-semisimple topological field theories ([KL01]) or in the case of semi-simplicity one can derive the corresponding Reshetikhin-Turaev invariants of 3-manifolds and links in 3-manifolds (cf. [RT91, Tur00, BK01]).

In this thesis we will consider exclusively the so-called small quantum groups $u_q(\mathfrak{g})$. They are quotients of the restricted specialization $U_q(\mathfrak{g})$, with q a root of unity and $\mathfrak{g}$ a finite-dimensional semi-simple complex Lie algebra, and are finite-dimensional Hopf algebras over the field $\mathbb{C}$ (see Definitions 1.3.6 and 1.3.8 for details). However, these quantum groups are in general not quasitriangular. In the present thesis we construct new (universal) R-matrices for these small quantum groups or certain extensions thereof, following an ansatz for the R-matrix by Lusztig. The extensions are constructed in the framework of the Lie theoretic input data due to the Lie algebra $\mathfrak{g}$ and are parametrized by lattices Λ containing the root lattice Λ_R and contained in the weight lattice Λ_W and admit R-matrices in many cases where the original small quantum group does not. We find that the existence of solutions for R-matrices then depends only on the (finite) fundamental group $\pi_1 = \Lambda_W/\Lambda_R$ of $\mathfrak{g}$ and on the order ℓ of the root of unity q. Especially for the series of quantum groups corresponding to the root system A_n a combinatorial theorem about roots of unity was necessary, which is interesting on its own.

Consequently, the cases of quasitriangular small quantum groups offer a source for ribbon categories of their representations.

Before proceeding with a detailed outline of this thesis we give a short overview on the algebraic background for this thesis.

Quasitriangular Hopf algebras and braided categories

A Hopf algebra H over a field k is an associative, unital k-algebra with multiplication μ, unit η and the additional structure of a coassociative comultiplication $\Delta\colon H \to H \otimes H$, a counit $\varepsilon\colon H \to k$ and a k-linear homomorphism $S\colon H \to H$, called the antipode. Standard references on the subject are the books of Abe [Abe80] and Sweedler [Swe69]. There are some compatibility conditions for the datum $(\mu, \eta, \Delta, \varepsilon, S)$, e.g. that Δ and ε are algebra maps. For H-modules U, V one can then define an H-action on the tensor product by

$$H \xrightarrow{\Delta} H \otimes H \xrightarrow{\rho_U \otimes \rho_V} \mathrm{End}(U) \otimes \mathrm{End}(V) \longrightarrow \mathrm{End}(U \otimes V)$$

with H-actions ρ_U, ρ_V on U and V, respectively, and the counit ε equips the ground field k with a trivial H-action. This provides the category $H-$mod of representations of H with the structure of a monoidal category. In addition, one can define an H-module structure on the dual representation V^* of an H-module V by using the antipode. We give two important examples of Hopf algebras. For a group G the group algebra $k[G]$ is a Hopf algebra with coalgebra structure and antipode given by

$$\Delta(g) = g \otimes g, \quad \varepsilon(g) = 1, \quad S(g) = g^{-1}$$

for all $g \in G$. The universal enveloping algebra $U(\mathfrak{g})$ of a Lie algebra $\mathfrak{g}$ is also a Hopf algebra with

$$\Delta(x) = 1 \otimes x \,+\, x \otimes 1, \quad \varepsilon(x) = 0, \quad S(x) = -x$$

on the generators $x \in \mathfrak{g}$.

The structure of a quasitriangular Hopf algebra H is the choice of an R-matrix. This invertible element in $H \otimes H$ is an intertwiner for the comultiplication Δ and the opposed comultiplication Δ^{opp}. We recall the exact definition.

Definition 1.1.1. The structure of an *quasitriangular* Hopf algebra H is the choice of an invertible element $R \in H \otimes H$ such that for all $h \in H$

$$\Delta^{\mathrm{opp}}(h) = R\Delta(h)R^{-1}, \tag{1.1.1}$$
$$(\Delta \otimes id)(R) = R_{13}R_{23}, \tag{1.1.2}$$
$$(id \otimes \Delta)(R) = R_{13}R_{12}, \tag{1.1.3}$$

with $\Delta^{\mathrm{opp}}(h) = \tau \circ \Delta(h)$, where $\tau : H \otimes H \longrightarrow H \otimes H,\ a \otimes b \longmapsto b \otimes a$ and $R_{12} = R \otimes 1,\ R_{23} = 1 \otimes R,\ R_{13} = (\tau \otimes id)(R_{23}) = (id \otimes \tau)(R_{12}) \in H^{\otimes 3}$. Such an element is called *(universal) R-matrix of H* and we write (H, R) for the quasitriangular Hopf algebra with R-matrix R.

The quasitriangular structure of an Hopf algebra is in correspondence with the additional structure of a braiding on the corresponding category of modules, i.e. a coherent natural isomorphism $c\colon \otimes \to \otimes^{\text{opp}}$ between the tensor product and the opposed tensor product (fulfilling the hexagon axioms in the case of a non-strict tensor category). Explicitly, this gives for any pair (V, W) of objects of the category an isomorphism

$$c_{V,W}\colon V \otimes W \to W \otimes V$$

which is compatible with morphism in the category. The notion of braided categories was introduced by Joyal and Street [JS93] and the compatibility axioms of a braided category relate to the so-called braid group, hence the term *braided*. In a strict braided category the following version of the Yang-Baxter equation holds:

$$(c_{V,W} \otimes id_U) \circ (id_V \otimes c_{U,W}) \circ (c_{U,V} \otimes id_W) = (id_W \otimes c_{U,V}) \circ (c_{U,W} \otimes id_V) \circ (id_U \otimes c_{V,W})$$

for objects U, V, W and braiding c. Thus, a representation of the braid group B_n on n strands can be constructed on $V^{\otimes n}$ for every object V in a braided monoidal category. The Yang-Baxter equation was first introduced in physics as a factorization condition of the scattering S-matrix in the many-body problem and in work on exactly solvable models in the field of statistical mechanics. It also played an important role in the work of Faddeev and the Leningrad School for the construction of quantum integrable systems [Fad84], coining the term quantum Yang-Baxter equation. As a consequence of the defining relations (1.1.1)-(1.1.3), an R-matrix R in a quasitriangular Hopf algebra obeys the following equation

$$R_{23}R_{13}R_{12} = R_{12}R_{13}R_{23},$$

which is a version of the quantum Yang-Baxter equation.

Braided categories with two additional structures, duality and twist, are called ribbon categories. In the case of the category $H-$mod of the finite-dimensional representations of a quasitriangular Hopf algebra H the category is ribbon, if a ribbon element $\nu \in H$ exist. Ribbon categories admit a consistent theory of traces of morphisms and dimensions of objects and, in particular, they yield invariants of colored framed graphs and links in the Euclidean space $\mathbb{R}^3$ (see e.g. [Tur00]). As we will see below, the quasitriangular small quantum groups provide a source for ribbon categories.

Quantum groups

The theory of quantum groups was triggered by the work of Drinfeld [Dri85, Dri87] and Jimbo [Jim85] around 1983-85. They may be roughly described as a one parameter deformation $U_q(\mathfrak{g})$ of the universal enveloping algebra $U(\mathfrak{g})$ of a semisimple Lie algebra $\mathfrak{g}$. These deformations yield Hopf algebras that are in general neither commutative nor cocommutative. In this thesis we deal exclusively with the case that the parameter q is specialized to a root of unity of order ℓ and consider the small quantum group: We follow Lusztig's approach ([Lus88, Lus90, Lus93]) and define the *restricted specialization* $U_q(\mathfrak{g})$ over $\mathbb{C}$ by introducing first the rational form over $\mathbb{Q}(q)$, with indeterminate q, and then the integral form over $\mathbb{Z}[q, q^{-1}]$ with divided powers. The small quantum group $u_q(\mathfrak{g})$, a quotient of the restricted specialization $U_q(\mathfrak{g})$ (q specialized to a root of unity), is a finite-dimensional Hopf algebra over $\mathbb{C}$. In contrast to the generic case, here the representation categories are not semi-simple. Also, the category of modules is in general not braided for even ℓ, i.e. $u_q(\mathfrak{g})$ is not quasitriangular in this cases (see e.g. [KS11] for $\mathfrak{g} = \mathfrak{sl}_2$).

In the literature one finds two ways to construct a quasitriangular quantum group, closely related to $u_q(\mathfrak{g})$: One can consider slightly smaller quotients, i.e. $K^e = 1$ for e half the exponent in Lusztig's definition and group-like generators K, where one can obtain indeed an R-matrix if ℓ is prime to the determinant of the Cartan matrix [Ros93]. For some applications however, it is desirable that the quotient is taken precisely with Lusztig's choice (this is the choice $\Lambda' = 2\Lambda_R^{(\ell)}$ in the notion of Definitions 1.2.5 and 1.3.8) and one wishes to focus on the even case. On the other hand, for q an even root of unity, some authors consider R-matrices up to outer automorphism ([Tan92, Res95]), or quadratic extensions of $u_q(\mathfrak{g})$, e.g. explicitly in the case of $u_q(\mathfrak{sl}_2)$ in [RT91, FGST06] and more generally in [GW98] for $u_q(\mathfrak{sl}_n)$. To our knowledge, prior to this thesis, there was no general result for $\mathfrak{g}$ other than $\mathfrak{sl}_n$.

We generalize both approaches (choosing a suitable quotient and constructing an extension) in a Lie theoretic setting and determine all those R-matrices that can be obtained through Lusztig's ansatz. We consider extensions $u_q(\mathfrak{g}, \Lambda, \Lambda')$ of the usual small quantum group $u_q(\mathfrak{g})$ for each choice of a lattice $\Lambda_R \subset \Lambda \subset \Lambda_W$ between root and weight lattice of $\mathfrak{g}$, which corresponds to a choice of a complex connected Lie group associated to the Lie algebra $\mathfrak{g}$, and taking the quotient by the lattice $\Lambda' \subset \Lambda_R$ (cf. Definition 1.3.8). In particular this includes the quadratic extensions mentioned above. Depending on the data $\mathfrak{g}$, q, Λ (and fixed Λ') we determine all R-matrices obtained through Lusztig's ansatz for different variants $u_q(\mathfrak{g}, \Lambda, \Lambda')$ of $u_q(\mathfrak{g})$. In particular we find indeed that for q of even order (or divisible by 4 for multiply-laced $\mathfrak{g}$) we get R-matrices for (mostly extensions of) Lusztig's original quotient. The main calculations in the present thesis are formulated in terms of certain sublattices of the weight lattice Λ_W. These sublattices depend heavily on the Lie algebras and the roots of unity in question.

Due to its special structure, a quasitriangular quantum group is also ribbon, i.e. it exists a so-called ribbon element in the quantum group. Thus the corresponding category of modules is a ribbon category.

In the following, we shall give a detailed outline of this thesis.

Outline and Summary

In the first chapter we provide the basic notions used in this thesis. We start by recalling the definition of an R-matrix and quasitriangular Hopf algebras. In the second section we then introduce the Lie theoretic framework, in particular certain sublattices of the weight lattice Λ_W and root lattice Λ_R of the Lie algebra $\mathfrak{g}$, e.g. the so-called centralizer $\mathrm{Cent}^{[\ell]}(\Lambda_R)$ of Λ_R in Λ_W in respect to an integer ℓ. These sublattices play an important role in the proof of the main Theorem 4.3.1 in Chapter 4. Another essential notion of this thesis is introduced, namely the fundamental group $\pi_1 = \Lambda_W/\Lambda_R$ of a Lie algebra. We then define the finite-dimensional quantum groups $u_q(\mathfrak{g}, \Lambda, \Lambda')$, for a primitive ℓ-th root of unity q, a finite-dimensional complex Lie algebra $\mathfrak{g}$ and sublattices Λ, Λ' of the weight, resp. root lattice. The different choices of lattices Λ give extensions of the usual small quantum group $u_q(\mathfrak{g})$ for $\Lambda = \Lambda_R$ (and fixed Λ') and correspond to choosing a Lie group associated to the Lie algebra $\mathfrak{g}$. The two extreme cases are for $\Lambda = \Lambda_R$ the so-called adjoint form and for $\Lambda = \Lambda_W$ the so-called simply-connected form. The lattice Λ' parametrizes different possible quotients of the restricted specialization $U_q(\mathfrak{g}, \Lambda)$.

In the second chapter we review the R-matrix ansatz by Lusztig and its modification by Müller [Mül98a, Mül98b]. This ansatz introduces a so-called quasi-R-matrix $\Theta \in u_q(\mathfrak{g}, \Lambda, \Lambda')^+ \otimes u_q(\mathfrak{g}, \Lambda, \Lambda')^-$, where $u_q(\mathfrak{g}, \Lambda, \Lambda')^\pm$ are the Borel parts generated by the E's and F's, respectively (cf. Theorem 2.1.2). The element Θ is an intertwiner between the comultiplication Δ and a new comultiplication $\bar{\Delta}$, obtained by conjugating with a certain antilinear involution. This quasi-R-matrix is equal to the R-matrix R of our ansatz except for an element $R_0 = \sum_{\mu,\nu \in \Lambda/\Lambda'} f(\mu,\nu) K_\mu \otimes K_\nu \in \mathbb{C}[\Lambda] \otimes \mathbb{C}[\Lambda]$, thus we have $R = R_0\bar{\Theta}$. This element R_0 is an intertwiner for $\bar{\Delta}$ and the opposed comultiplication Δ^{opp} and has to fulfill some requirements which result from the defining relations (1.1.1)-(1.1.3) of an R-matrix. Müller gives in his dissertation equations for the coefficients $f(\mu,\nu)$ of R_0 and uses the ansatz $R = R_0\bar{\Theta}$ for determining R-matrices for quadratic extensions of $u_q(\mathfrak{sl}_n)$. We develop this ansatz further and get a new set of equations for the coefficients of R_0, which split in two different types. The first type of equations depends only on the fundamental group π_1 of the Lie algebra $\mathfrak{g}$ and will be called *group-equation*. The second type depends on some sublattices of Λ, especially on $\mathrm{Cent}^{[\ell]}(\Lambda_R)$ and is very sensitive to different choices of ℓ. This type of equations will be called *diamond-equations*. In the following chapters we determine all solutions of these equations. To this end, we determine the solutions of the group-equations first and check which of these are solutions to the diamond-equations as well. The solutions of these equations give all R-matrices of $u_q(\mathfrak{g}, \Lambda, \Lambda')$ with arbitrary simple Lie algebra $\mathfrak{g}$, which satisfy the ansatz $R = R_0\bar{\Theta}$.

The third chapter is based on the preprint [LN14a]. Here we give all solutions of the group-equations of the R-matrix ansatz of Chapter 2. For this we need a theorem about roots of unity, which is the main result of this chapter and is of independent interest.

Theorem 3.2.1. *Let U be a non-empty finite set of complex roots of unity and consider for all $k \in \mathbb{Z}$ the power sums $a_k := \sum_{\zeta \in U} \zeta^k$. Then all a_k are non-negative integers iff U is actually a multiplicative group of roots of unity (i.e. all N-th roots of unity for some N).*

Most of Chapter 3 is devoted to the proof of this theorem. First, we introduce a new combinatorial principle and the proof of Theorem 3.2.1 is along these lines. We then give an alternative proof of this theorem which does not need the aforementioned combinatorial principle. This proof was pointed out to us by Mihalis Kolountzakis. As an application of this theorem we then prove a theorem about so-called Fourier pairs of $\{0,1\}$-matrices (over the group $\mathbb{Z}_N \times \mathbb{Z}_N$), i.e. a pair of matrices $(\varepsilon_{ij})_{1\le i,j\le N}$, $(\bar{\varepsilon}_{ij})_{1\le i,j\le N}$ with ε_{ij}, $\bar{\varepsilon}_{ij} \in \{0,1\}$ for all i,j, such that the coefficients ε_{ij} are the discrete Fourier transforms of the $\bar{\varepsilon}_{ij}$ (and vice versa).

Theorem 3.4.4. *All idempotents $e^{(\varepsilon)}$ of the group algebra $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ with $\varepsilon_{ij} \in \{0,1\}$, or equivalently all discrete Fourier pairs $\varepsilon, \bar{\varepsilon}$ of $\{0,1\}$-matrices are either of the form*

$$\varepsilon_{ij} = \delta_{(\frac{N}{d}|i)}\delta_{(d|j-t\frac{i}{N/d})}, \qquad 0 \le i,j < N,$$

for a unique $d \mid N$ and $0 \le t \le d-1$ or they are trivial, i.e. $\varepsilon = \bar{\varepsilon} = 0$.

Since from a solution of the group-equations certain idempotent equations could be derived, these $\{0,1\}$-matrices, or idempotents of the group algebra $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ respectively, occur in the course of determining the solutions of the group-equations for cyclic fundamental group. We work out these solutions in Example 3.5.5 and Theorem 3.5.6. The solutions in the case of fundamental group $\mathbb{Z}_2 \times \mathbb{Z}_2$ are determined by a Maple-calculation which is documented in Appendix A.

The last chapter contains the main results of this thesis and is the gist of the preprint [LN14b]. We first introduce the notion of diamonds of sublattices of Λ_W (the notion refers to their inclusion relations) and the corresponding diamond-equations. We then examine which of the solutions of the group-equations discussed in Chapter 3 are solutions of the diamond-equations as well. For the case of cyclic fundamental group π_1 we determine in Lemma 4.2.1 all possible solutions of the diamond-equations for a given diamond. In Example 4.2.3 we give all possible diamonds, depending on the Lie theoretic input and on ℓ. Again, the case of fundamental group $\mathbb{Z}_2 \times \mathbb{Z}_2$ (for root systems $D_{2m}, m \ge 2$), is done by a direct calculation. The Section 4.3 contains the main theorem of this thesis. We finally give the solutions for each root system and list all R-matrices of the form $R_0\bar{\Theta}$ for chosen Lie algebra $\mathfrak{g}$, root of unity q and suitable sublattices Λ, Λ' of the weight lattice.

Theorem 4.3.1. *Let $\mathfrak{g}$ be a finite-dimensional simple complex Lie algebra with root lattice Λ_R, weight lattice Λ_W and fundamental group $\pi_1 = \Lambda_W/\Lambda_R$. Let q be an ℓ-th root of unity, $\ell \in \mathbb{N}$, $\ell > 2$. Then we have the following R-matrix of the form $R = R_0\bar{\Theta}$, with Θ as above:*

$$R = \left(\frac{1}{|\Lambda/\Lambda'|} \sum_{(\mu,\nu)\in(\Lambda_1/\Lambda' \times \Lambda_2/\Lambda')} q^{-(\mu,\nu)}\omega(\bar{\mu},\bar{\nu})\; K_\mu \otimes K_\nu \right) \cdot \bar{\Theta},$$

for the quantum group $u_q(\mathfrak{g},\Lambda,\Lambda')$ with $\Lambda = \Lambda_W$ and Λ_i the preimage of a certain subgroup $H_i \subset \pi_1$ in Λ_W ($i = 1,2$), a certain group-pairing $\omega\colon H_1 \times H_2 \to \mathbb{C}^\times$ and $\Lambda' = \Lambda_R^{[\ell]}$ as in Def. 1.2.5.

In the following table we list for all root systems the following data, depending on ℓ: Possible choices of H_1, H_2 (in terms of fundamental weights λ_k), the group-pairing ω, *and the number of solutions #. If the number has a superscript ∗, we obtain R-matrices for Lusztig's original choice of Λ'. For $\mathfrak{g} = D_n$, $2 \mid n$, with $\pi_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$ we get the only cases $H_1 \neq H_2$ and denote by $\lambda \neq \lambda' \in \{\lambda_{n-1}, \lambda_n, \lambda_{n-1} + \lambda_n\}$ arbitrary elements of order 2 in π_1.*

$\mathfrak{g}$	ℓ	#	$H_i \cong$	H_i $(i=1,2)$	ω
$A_{n\geq 1}$, $\pi_1 = \mathbb{Z}_{n+1}$	ℓ odd	$*$	$\mathbb{Z}_d$	$\langle \frac{n+1}{d}\lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = \xi_d^k$, if $d \mid (n+1)$, $1 \leq k \leq d$ and $\gcd(n+1, d\ell, k\ell - \frac{n+1}{d}n) = 1$
	ℓ even				
$B_{n\geq 2}$, $\pi_1 = \mathbb{Z}_2$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = (-1)^{n-1}$
	$\ell \equiv 2 \mod 4$	2	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = \pm 1$
		1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$, if n even
	$\ell \equiv 0 \mod 4$, $\ell \neq 4$	2^*	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = \pm 1$
		1^*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$, if n even
$C_{n\geq 3}$, $\pi_1 = \mathbb{Z}_2$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = -1$
	$\ell \equiv 2 \mod 4$	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = (-1)^{n-1}$
	$\ell \equiv 0 \mod 4$, $\ell \neq 4$	2^*	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = \pm 1$
		1^*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$, if n even
$D_{n\geq 4}$, n even, $\pi_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		3	$\mathbb{Z}_2$	$\langle \lambda \rangle$	$\omega(\lambda, \lambda) = -1$
		6	$\mathbb{Z}_2 \neq \mathbb{Z}_2'$	$\langle \lambda \rangle, \langle \lambda' \rangle$	$\omega(\lambda, \lambda') = 1$
		1	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1}, \lambda_n \rangle$	$\omega(\lambda_i, \lambda_j) = 1$
		1	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1}, \lambda_n \rangle$	$\omega(\lambda_i, \lambda_j) = -1$
		2	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1}, \lambda_n \rangle$	$\omega(\lambda_{n-1}, \lambda_{n-1}) = \pm 1$ $\omega(\lambda_{n-1}, \lambda_n) = 1$ $\omega(\lambda_n, \lambda_{n-1}) = 1$ $\omega(\lambda_n, \lambda_n) = \mp 1$
		2	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1}, \lambda_n \rangle$	$\omega(\lambda_{n-1}, \lambda_{n-1}) = -1$ $\omega(\lambda_{n-1}, \lambda_n) = \pm 1$ $\omega(\lambda_n, \lambda_{n-1}) = \mp 1$ $\omega(\lambda_n, \lambda_n) = -1$
	ℓ even	16^*	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1}, \lambda_n \rangle$	$\omega(\lambda_i, \lambda_j) \in \{\pm 1\}$
$D_{n\geq 5}$, n odd, $\pi_1 = \mathbb{Z}_4$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle 2\lambda_n \rangle$	$\omega(2\lambda_n, 2\lambda_n) = -1$
		2	$\mathbb{Z}_4$	$\langle \lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = \pm 1$
	$\ell \equiv 2 \mod 4$	4^*	$\mathbb{Z}_4$	$\langle \lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = c$, $c^4 = 1$

	$\ell \equiv 0 \mod 4$	4^*	$\mathbb{Z}_4$	$\langle \lambda_n \rangle$	$\omega(\lambda_n, \lambda_n) = c,\ c^4 = 1$
E_6 $\pi_1 = \mathbb{Z}_3$	ℓ odd, $3 \nmid \ell$	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		2	$\mathbb{Z}_3$	$\langle \lambda_6 \rangle$	$\omega(\lambda_6, \lambda_6) = 1, \exp(\frac{2\pi i}{3})$
	ℓ even, $3 \nmid \ell$	1^*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		2^*	$\mathbb{Z}_3$	$\langle \lambda_6 \rangle$	$\omega(\lambda_6, \lambda_6) = 1, \exp(2\frac{2\pi i}{3})$
	ℓ odd, $3 \mid \ell$	3	$\mathbb{Z}_3$	$\langle \lambda_6 \rangle$	$\omega(\lambda_6, \lambda_6) = c,\ c^3 = 1$
	ℓ even, $3 \mid \ell$	3^*	$\mathbb{Z}_3$	$\langle \lambda_6 \rangle$	$\omega(\lambda_6, \lambda_6) = c,\ c^3 = 1$
E_7 $\pi_1 = \mathbb{Z}_2$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle \lambda_7 \rangle$	$\omega(\lambda_7, \lambda_7) = 1$
	ℓ even	2^*	$\mathbb{Z}_2$	$\langle \lambda_7 \rangle$	$\omega(\lambda_7, \lambda_7) = \pm 1$
E_8 $\pi_1 = \mathbb{Z}_1$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
	ℓ even	1^*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
F_4 $\pi_1 = \mathbb{Z}_1$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
	$\ell \equiv 2 \mod 4$	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
	$\ell \equiv 0 \mod 4$ $\ell \neq 4$	1^*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
G_2 $\pi_1 = \mathbb{Z}_1$	ℓ odd $\ell \neq 3$	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
	ℓ even $\ell \neq 4, 6$	1^*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$

Remark. We indicate in which sense our results are *not* complete:

- Technically, one could even allow $\Lambda_R \subset \Lambda \subset \Lambda_W^\vee$. Here, the lattice $\Lambda_W^\vee$ has basis $\{\tilde{\lambda}_i := 2\lambda_i/(\alpha_i, \alpha_i) \mid i \in I\}$ with fundamental dominant weights λ_i, thus $(\tilde{\lambda}_i, \alpha_j) = \delta_{ij}$. In this case one could get additional R-matrices for further extensions $u_q(\mathfrak{g}, \Lambda, \Lambda')$, corresponding to Λ with $\Lambda_W \subset \Lambda \subset \Lambda_W^\vee$.
- Our assumption $\Lambda' \subset \mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R$ was to simplify calculations and prove uniqueness. In general $\Lambda' \in \mathrm{Cent}^{[\ell]}(\Lambda)$ would suffice (and could yield more solutions), but one would have to deal with possible 2-cocycles in $H^2(\Lambda/\Lambda', \pi_1)$ in Lemma 2.2.1.
- Then, one could ask in general whether *all* R-matrices are necessarily given by Lusztig's ansatz and hence of our form.
- We also do not answer the question whether different R-matrices give equivalent quasitriangular structures for a given quantum group $u = u_q(\mathfrak{g}, \Lambda, \Lambda')$ in the sense of Definition 1.1.3, nor have we investigated which quasitriangular quantum groups (u, R) and (u', R') might give equivalent braided tensor categories $\mathcal{C}(u, R) \cong \mathcal{C}(u', R')$ of their representations.

This thesis is based on the following preprints:

Chapter 3: S. Lentner and D. Nett. *A theorem on roots of unity and a combinatorial principle*. Preprint (2014), arXiv:1409.5822.

Chapters 2, 4: S. Lentner and D. Nett. *New R-matrices for small quantum groups*. Preprint (2014), arXiv:1409.5824.

Acknowledgments

I am very grateful to my adviser Christoph Schweigert for his excellent supervision and never ending support over the last two-and-a-half years. Through many discussions he helped me get a better understanding of the mathematical subjects of this work and his valuable comments on earlier drafts of this thesis helped improving this text. I am also deeply grateful to my co-author Simon Lentner for his profound mathematical support, his cordial encouragement and the fruitful collaboration from which I gained a lot and which lead to parts of this thesis.

Further thanks goes to my dear colleagues Alexander Barvels, Lukas Buhné, Ralf Holtkamp, Jennifer Maier and Jan Priel for providing such a nice and familiar atmosphere. I would like to thank Christian Steup, Johannes Orlob, Sebastian Dany, Alexander Müller and Birger Frehse for encouraging me in going through with this endeavor. Sincere thanks go to Rani Pohl, for her support and patience, for all the sacrifices involved, for making *this* my best decision, for all.

Chapter 1

Preliminaries and Motivation

In this preliminary chapter we will recall some basic algebraic notions. We start by introducing the notion of an R-matrix and quasitriangular Hopf algebra. The quasitriangular Hopf algebra are in correspondence to the structure of a braiding on their representation categories. In the second section we collect the relevant Lie theoretical prerequisites. These are the main ingredients for defining the quantum groups in the last section. In particular, we introduce some sublattices of the weight lattice of the Lie algebra which play in crucial role in the R-matrix ansatz we choose in this thesis.

1.1. R-matrices and quasitriangular Hopf algebras

We introduce the notion of a quasitriangular Hopf algebra H and the connection to the structure of a braiding on its representation category $H-$mod. For precise definitions of the categorial terms we refer the reader to the Appendix B.

One reason why braided tensor categories are interesting is that in such a category a version of the *Yang-Baxter equation* holds. Let U, V, W be objects in a (strict) braided tensor category. Then the following identity holds:

$$(c_{V,W} \otimes id_U) \circ (id_V \otimes c_{U,W}) \circ (c_{U,V} \otimes id_W) = (id_W \otimes c_{U,V}) \circ (c_{U,W} \otimes id_V) \circ (id_U \otimes c_{V,W}).$$

This leads to the questions what kind of structure in a Hopf algebra H induces the structure of a braiding on its representation category, and hence gives a solution of the Yang-Baxter equation. In the following, $H = (H, \mu, \eta, \Delta, \varepsilon, S)$ is a Hopf algebra with product μ, unit η, coproduct Δ, counit ε and antipode S. We now recall the definition of an (universal) R-matrix and with that the notion of an quasitriangular Hopf algebra.

Definition 1.1.1. The structure of an *quasitriangular* Hopf algebra H is the choice of an invertible element $R \in H \otimes H$ such that for all $h \in H$

$$\Delta^{\text{opp}}(h) = R\Delta(h)R^{-1}, \tag{1.1.1}$$

$$(\Delta \otimes id)(R) = R_{13}R_{23}, \tag{1.1.2}$$

$$(id \otimes \Delta)(R) = R_{13}R_{12}, \tag{1.1.3}$$

with $\Delta^{\mathrm{opp}}(h) = \tau \circ \Delta(h)$, where $\tau : H \otimes H \longrightarrow H \otimes H,\ a \otimes b \longmapsto b \otimes a$ and $R_{12} = R \otimes 1,\ R_{23} = 1 \otimes R,\ R_{13} = (\tau \otimes id)(R_{23}) = (id \otimes \tau)(R_{12}) \in H^{\otimes 3}$. Such an element is called an *(universal) R-matrix of H* and we write (H, R) for the quasitriangular Hopf algebra with R-matrix R.

In Sweedler notation, we write $R = R_{(1)} \otimes R_{(2)}$ and with that $R_{12} = R_{(1)} \otimes R_{(2)} \otimes 1$, and so on. In the following we mean by R-matrix always universal R-matrix and omit the epithet.

The following theorem gives the correspondence between quasitriangular Hopf algebras and their braided representation categories.

Theorem 1.1.2 (cf. [Kas95], Prop. XIII.1.4)**.** *Let $(H, \mu, \nu, \Delta, \varepsilon)$ be a bialgebra (with multiplication μ, unit ν, comultiplication Δ and counit ε). The monoidal category* $H-$mod *is braided, if and only if H is quasitriangular.*

For a quasitriangular Hopf algebra H with R-matrix R, the braiding on $H-$mod is given by

$$\begin{aligned} c^R_{U,V} :\ & U \otimes V \to V \otimes U, \\ & u \otimes v \mapsto \tau_{U,V}(R.(u \otimes v)) = R_{(2)}.v \otimes R_{(1)}.u, \end{aligned} \tag{1.1.4}$$

for all pairs $U, V \in H-$mod. Conversely, if the category $H-$mod is endowed with a braiding c, then the element

$$R := \tau_{H,H}(c_{H,H}(1_H \otimes 1_H)) \in H \otimes H$$

is an R-matrix for H.

For quasitriangular Hopf algebras H, H' with R-matrices R and R' respectively, one can ask when the corresponding representation categories, denoted by $\mathcal{C}(H, R)$ and $\mathcal{C}(H', R')$, are equivalent as braided monoidal categories. This is in general very hard to answer. The following definition introduces a notion of equivalent quasitriangular structures on Hopf algebras.

Definition 1.1.3. (1) If (H, R) and (H', R') are quasitriangular Hopf algebras, then they are *isomorphic as quasitriangular Hopf algebras* if there exists a Hopf algebra isomorphism $f \colon H \to H'$ such that $R' = (f \otimes f)(R)$.

(2) Two quasitriangular structures R, R' on a Hopf algebra H are *equivalent* if $(H, R) \cong (H, R')$ as quasitriangular Hopf algebras.

It is an easy implication that for two isomorphic quasitriangular Hopf algebras (H, R) and (H', R') the corresponding representation categories $\mathcal{C}(H, R)$ and $\mathcal{C}(H', R')$ are equivalent as braided tensor categories.

Finally, we introduce the notion of a factorizable Hopf algebra. For an R-matrix $R = R_{(1)} \otimes R_{(2)} \in H \otimes H$ we define the invertible element

$$Q := \tau(R)R = R_{(2)}R_{(1)} \otimes R_{(1)}R_{(2)}.$$

This element in $H \otimes H$ is called *monodromy element* and we write $Q = Q_{(1)} \otimes Q_{(2)}$.

Definition 1.1.4 (cf. [RSTS88])**.** The quasitriangular Hopf algebra (H, R) is called *factorizable* if the map

$$\Phi_R \colon H^* \to H,\ f \mapsto \mu \circ (id_H \otimes f)(\tau(R)R) = Q_{(1)} f(Q_{(2)})$$

is an isomorphism of vector spaces.

The following remark explains the word factorizable and translates this property of the quasitriangular Hopf algebra into a condition on the R-matrix.

Remark 1.1.5. *Let H be a factorizable quasitriangular Hopf algebra with R-matrix R and monodromy element $Q = \tau(R)R$. Then there exist basis $(b_i)_{i\in I}$ and $(c_i)_{i\in I}$ of H, such that $Q = \sum_{i\in I} b_i \otimes c_i$.*

Again, we do not answer the question, whether the small quantum groups with the R-matrices in Theorem 4.3.1 are factorizable. This problem is of special interest since factorizable quantum groups give rise to modular tensor categories, which play an important role in the Reshetikhin-Turaev construction of three-dimensional extended topological field theories.

1.2. Lie Theory

At first, we will collect the Lie theoretic prerequisites. We assume a general knowledge of Lie theory and always assume the Lie algebra being a finite-dimensional, semisimple complex Lie algebra. As a general reference we refer to the book of Humphreys [Hum72].

Let $\mathfrak{g}$ be a finite-dimensional, semisimple complex Lie algebra with a choice of simple roots α_i, indexed by $i \in I$, $|I| =: n$, set of roots Φ and set of positive roots Φ^+. Denote the *Killing form* by $(\_,\_)$, normalized such that $(\alpha,\alpha) = 2$ for the short roots α. The *Cartan matrix* of $\mathfrak{g}$ is given by

$$a_{ij} = \langle \alpha_i, \alpha_j \rangle = 2\frac{(\alpha_i, \alpha_j)}{(\alpha_i, \alpha_i)}.$$

For a root α we introduce $d_\alpha := (\alpha,\alpha)/2$ with $d_\alpha \in \{1,2,3\}$. Especially, $d_i := d_{\alpha_i}$ and in this notation $(\alpha_i, \alpha_j) = d_i a_{ij}$. The fundamental dominant weights λ_i, $i \in I$, are given by the condition $2(\alpha_i, \lambda_j)/(\alpha_i, \alpha_i) = \delta_{ij}$, hence the Cartan matrix expresses the change of basis from roots to weights. By inverting the Cartan matrix the fundamental weights are expressed in the basis of simple roots. This can be found in [Hum72], Section 13.2, and we will use this in the case-by-case proof of our main result Theorem 4.3.1.

Definition 1.2.1. The *root lattice* $\Lambda_R = \Lambda_R(\mathfrak{g})$ of the Lie algebra $\mathfrak{g}$ is the abelian group with rank $\mathrm{rank}(\Lambda_R) = \mathrm{rank}(\mathfrak{g}) = |I|$, generated by the simple roots α_i, $i \in I$.

Definition 1.2.2. The *weight lattice* $\Lambda_W = \Lambda_W(\mathfrak{g})$ of the Lie algebra $\mathfrak{g}$ is the abelian group with rank $\operatorname{rank}(\Lambda_W) = \operatorname{rank}(\mathfrak{g})$, generated by the fundamental dominant weights λ_i, $i \in I$.

The Killing form induces an integral pairing of abelian groups, turning Λ_R into an *integral lattice*. It is standard fact of Lie theory (cf. [Hum72], Section 13.1) that the root lattice is contained in the weight lattice. Moreover it is known that the pairing on Λ_R can be extended to a integral pairing $(\_,\_)\colon \Lambda_W \times \Lambda_R \to \mathbb{Z}$.

Furthermore, it is an elementary fact about lattices that Λ_W/Λ_R is a finite group. We give a definition for this important abelian group.

Definition 1.2.3. Let Λ_W the weight lattice and Λ_R the root lattice of the Lie algebra $\mathfrak{g}$. The finite abelian group Λ_W/Λ_R is called the *fundamental group* of $\mathfrak{g}$.

Remark 1.2.4. *There is a one-to-one correspondence (up to isomorphism) between the set of semi-simple complex Lie algebras and the set of connected compact Lie groups with trivial center. For a Lie algebra $\mathfrak{g}$, the fundamental group $\pi_1(G)$ of the corresponding Lie group G, i.e. the first homotopy group of G, coincides with the fundamental group π_1 of the Lie algebra $\mathfrak{g}$ as defined in Definition 1.2.3.*

We define some important sublattices of Λ_R and Λ_W.

Definition 1.2.5. Let Λ_R, Λ_W the root, resp. weight lattice of the Lie algebra $\mathfrak{g}$ with generators α_i, resp. λ_i, for $i \in I$.

(i) Following Lusztig, we define $\ell_i := \ell/\gcd(\ell, 2d_i)$, which is the order of q^{2d_i}, where q is a primitive ℓ-th root of unity. More generally, we define for any root $\ell_\alpha := \ell/\gcd(\ell, 2d_\alpha)$. For any positive integer ℓ, the *ℓ-lattice* $\Lambda_R^{(\ell)}$, resp. $\Lambda_W^{(\ell)}$, is defined as
$$\Lambda_R^{(\ell)} = \langle \ell_i\alpha_i,\ i \in I\rangle \quad \text{resp.} \quad \Lambda_W^{(\ell)} = \langle \ell_i\lambda_i,\ i \in I\rangle\,. \tag{1.2.1}$$

(ii) For any positive integer ℓ, the lattice $\Lambda_R^{[\ell]}$, resp. $\Lambda_W^{[\ell]}$, is defined as
$$\Lambda_R^{[\ell]} = \left\langle \frac{\ell}{\gcd(\ell, d_i)}\alpha_i,\ i \in I \right\rangle, \quad \text{resp.} \quad \Lambda_W^{[\ell]} = \left\langle \frac{\ell}{\gcd(\ell, d_i)}\lambda_i,\ i \in I \right\rangle. \tag{1.2.2}$$

Definition 1.2.6. For sublattices $\Lambda_1, \Lambda_2 \subset \Lambda_W$ with $\Lambda_2 \subset \Lambda_1$ we define the sublattice $\operatorname{Cent}^{[\ell]}_{\Lambda_1}(\Lambda_2) = \{\eta \in \Lambda_1 \mid (\eta, \lambda) \in \ell\mathbb{Z}\ \forall \lambda \in \Lambda_2\}$. In the situation $\Lambda_1 = \Lambda_W$ and for a fixed ℓ we simply write $\operatorname{Cent}^{[\ell]}_{\Lambda_W}(\Lambda_2) = \operatorname{Cent}^{[\ell]}(\Lambda_2)$. If ℓ is fixed, we also write $\operatorname{Cent}(\Lambda_2)$.

Especially, the set $\langle K_\eta \mid \eta \in \operatorname{Cent}(\Lambda_R)\rangle$ consists of the central group elements of the quantum group $U_q(\mathfrak{g}, \Lambda_W)$, cf. Section 1.3.

We now calculate the centralizer in two special cases, which become relevant later.

Lemma 1.2.7. *For a Lie algebra $\mathfrak{g}$ we have $\operatorname{Cent}^{[\ell]}(\Lambda_R) = \Lambda_W^{[\ell]}$. We call the elements of $\operatorname{Cent}(\Lambda_R)$ (ℓ-)central weights.*

Proof. Let $\lambda = \sum_{j\in I} m_j\lambda_j \in \Lambda_W$ with fundamental weights λ_i and $m_i \in \mathbb{Z}$. For a simple root α_i we have $(\alpha_i, \lambda) = (\alpha_i, \sum_{j\in I} m_j\lambda_j) = d_i m_i$. Thus, λ is central weight if $\ell \mid d_i m_i$ for all i, hence $(\ell/\gcd(\ell, d_i)) \mid m_i$ for all i. ∎

The same calculation gives the following lemma.

Lemma 1.2.8. *For a Lie algebra* $\mathfrak{g}$ *we have* $\mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R = \Lambda_R^{[\ell]}$.

1.3. Quantum groups

For a primitive ℓ-th root of unity q, a finite-dimensional complex simple Lie algebra $\mathfrak{g}$, lattices Λ, Λ' with $\Lambda_R \subset \Lambda \subset \Lambda_W$ and $2\Lambda_R^{(\ell)} \subset \Lambda' \subset \mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R$, we aim to define the finite-dimensional complex quantum group $u_q(\mathfrak{g}, \Lambda, \Lambda')$, also called small quantum group. Here, we use the term *quantum group* for certain quasitriangular Hopf algebras. Quantum groups were introduced around 1983-1985 by V. Drinfeld and M. Jimbo, [Dri85] and [Jim85], an may be roughly described as one-parameter deformations of the enveloping algebras of semisimple Lie algebras. We construct $u_q(\mathfrak{g}, \Lambda, \Lambda')$ by using rational and integral forms of the deformed universal enveloping algebra $U_q(\mathfrak{g})$ for an indeterminate q. In the following we give the definitions of the quantum groups, following the lines of [Len14]. The different choices of Λ are already in [Lus93], Sec. 2.2. We shall give a dictionary to translate Lusztig's notation to the one used in this thesis.

We start with a technical definition of quantum numbers.

Definition 1.3.1. For q an indeterminate and $n \leq k \in \mathbb{N}_0$ we define

$$[n]_q := \frac{q^n - q^{-n}}{q - q^{-1}} \qquad [n]_q! := [1]_1[2]_q \dots [n]_q \qquad \begin{bmatrix} n \\ k \end{bmatrix}_q := \begin{cases} \frac{[n]_q!}{[k]_q![n-k]_q!}, & 0 \leq k \leq n, \\ 0, & \text{else.} \end{cases}$$

Note, that $[n]_q$ and $\begin{bmatrix} n \\ k \end{bmatrix}_q$ are polynomials in $\mathbb{Q}[q, q^{-1}]$ and we can specialize the indeterminate q to an arbitrary value in $\mathbb{C}^\times$. We now give the definition of the rational form $U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)$ for an indeterminate q, which is a Hopf algebra over the field $\mathbb{Q}(q)$. The different choices of a sublattice Λ between the weight lattice Λ_W and the root lattice Λ_R of $\mathfrak{g}$ corresponds to choosing a Lie group associated to the Lie algebra $\mathfrak{g}$. We call the two extreme cases $\Lambda = \Lambda_W$ the *simply-connected form* and $\Lambda = \Lambda_R$ the *adjoint form*. For this, we refer the reader to [CP94], Section 9.1, or [Lus93]. The classical case $\Lambda = \Lambda_R$ is also in [Jan07] II, H.2 and H.3.

Definition 1.3.2. Let q be an indeterminate. For each abelian group Λ with $\Lambda_R \subset \Lambda \subset \Lambda_W$ we define the *rational form* $U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)$ over the ring of rational functions $\Bbbk = \mathbb{Q}(q)$ as follows:

As an algebra, let $U_q^{\mathbb{Q}(q)}(\mathfrak{g},\Lambda)$ be generated by the group ring $\Bbbk[\Lambda]$, spanned by K_Λ, $\lambda\in\Lambda$, and additional generators E_{α_i}, F_{α_i}, for each simple root α_i, $i\in I$, with relations:

$$K_\lambda E_{\alpha_i} K_\lambda^{-1} = q^{(\lambda,\alpha_i)} E_{\alpha_i}, \tag{1.3.1}$$

$$K_\lambda F_{\alpha_i} K_\lambda^{-1} = q^{-(\lambda,\alpha_i)} F_{\alpha_i}, \tag{1.3.2}$$

$$E_{\alpha_i}F_{\alpha_j} - F_{\alpha_j}E_{\alpha_i} = \delta_{ij}\frac{K_{\alpha_i}-K_{\alpha_i}^{-1}}{q_{\alpha_i}-q_{\alpha_i}^{-1}}, \tag{1.3.3}$$

and Serre relations for any $i\neq j\in I$

$$\sum_{r=0}^{1-a_{ij}} (-1)^r \begin{bmatrix} 1-a_{ij} \\ r \end{bmatrix}_{q_i} E_{\alpha_i}^{1-a_{ij}-r} E_{\alpha_j} E_{\alpha_i}^r = 0, \tag{1.3.4}$$

$$\sum_{r=0}^{1-a_{ij}} (-1)^r \begin{bmatrix} 1-a_{ij} \\ r \end{bmatrix}_{\bar{q}_i} F_{\alpha_i}^{1-a_{ij}-r} F_{\alpha_j} F_{\alpha_i}^r = 0, \tag{1.3.5}$$

where $\bar{q} := q^{-1}$, the q_i are defined by $q_i := q^{d_i}$, i.e. $q^{(\alpha_i,\alpha_j)} = (q^{d_i})^{a_{ij}} = q_i^{a_{ij}}$, and the quantum binomial coefficients as defined in Definition 1.3.1.

To define the structure of a coalgebra, let the coproduct Δ, the counit ε and the antipode S be defined on the group-Hopf-algebra $\Bbbk[\Lambda]$ as usual

$$\Delta(K_\lambda) = K_\lambda\otimes K_\lambda, \qquad \varepsilon(K_\lambda)=1, \qquad S(K_\lambda) = K_\lambda^{-1} = K_{-\lambda},$$

and on the generator $E_{\alpha_i}, F_{\alpha_i}$, for each simple root α_i, $i\in I$ as follows

$$\begin{aligned} \Delta(E_{\alpha_i}) &= E_{\alpha_i}\otimes K_{\alpha_i} + 1\otimes E_{\alpha_i}, & \Delta(F_{\alpha_i}) &= F_{\alpha_i}\otimes 1 + K_{\alpha_i}^{-1}\otimes F_{\alpha_i}, \\ \varepsilon(E_{\alpha_i}) &= 0, & \varepsilon(F_{\alpha_i}) &= 0, \\ S(E_{\alpha_i}) &= -E_{\alpha_i}K_{\alpha_i}^{-1}, & S(F_{\alpha_i}) &= -K_{\alpha_i}F_{\alpha_i}. \end{aligned}$$

This definition can also be found in Lusztig's book [Lus93], Section 3.1. In order to translate Lusztig's notation to the one used here, one has to match the terms in the following way

Lusztig's notation	notation used here
Index set I	simple roots $\{\alpha_i \mid i\in I\}$
X	root lattice Λ_R
Y	a lattice $\Lambda_R\subset\Lambda\subset\Lambda_W$
$i'\in X$	α_i
$i\in Y$	$\frac{\alpha_i}{d_{\alpha_i}} = \alpha_i^\vee$ coroot
$i\cdot j$, $i,j\in\mathbb{Z}[I]$	(α_i,α_j)
$\langle i,j'\rangle = 2\frac{i\cdot j}{i\cdot i}$, $i\in Y, j'\in X$	$\langle\alpha_i,\alpha_j\rangle$
K_i	$K_{\alpha_i^\vee}$
$\tilde{K}_i = K_{\frac{i\cdot i}{2}i}$	K_{α_i}

Theorem 1.3.3 (cf. [Len14], Theorem 3.3)**.** *The rational form $U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)$ of Definition 1.3.2 is a Hopf algebra over the field $\Bbbk = \mathbb{Q}(q)$.*

Moreover, we have a triangular decomposition: Consider the subalgebras $U_q^{\mathbb{Q}(q),+}$, generated by the E_{α_i}, and $U_q^{\mathbb{Q}(q),-}$, generated by the F_{α_i}, and $U_q^{\mathbb{Q}(q),0} = \Bbbk[\Lambda]$, spanned by the K_λ. Then the multiplication in $U_q^{\mathbb{Q}(q)} = U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)$ induces an isomorphism of vector spaces:

$$U_q^{\mathbb{Q}(q),+} \otimes U_q^{\mathbb{Q}(q),0} \otimes U_q^{\mathbb{Q}(q),-} \xrightarrow{\cong} U_q^{\mathbb{Q}(q)}.$$

To obtain from $U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)$ a well-defined Hopf algebra by specializing q to an root of unity in $\mathbb{C}^\times$, we have to define the (restricted) integral form $U_q^{\mathbb{Z}[q,q^{-1}]}(\mathfrak{g}, \Lambda)$ of $U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)$. This is an $\mathcal{A} = \mathbb{Z}[q, q^{-1}]$-subalgebra $U_\mathcal{A}$ of $U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)$, such that the extensions of scalar $U_\mathcal{A} \otimes_{\mathbb{Z}[q,q^{-1}]} \mathbb{Q}(q)$ gives an isomorphism to $U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)$.

Definition 1.3.4. The so-called *restricted integral form* $U_q^{\mathbb{Z}[q,q^{-1}]}(\mathfrak{g}, \Lambda)$ is generated as a $\mathbb{Z}[q, q^{-1}]$-algebra by $K_\lambda^{\pm 1}$, $\lambda \in \Lambda$, and the following elements in $U_q^{\mathbb{Q}(q),\pm}(\mathfrak{g}, \Lambda)$, called *divided powers*:

$$E_\alpha^{(r)} := \frac{E_\alpha^r}{\prod_{s=1}^r \frac{q_\alpha^s - q_\alpha^{-s}}{q_\alpha - q_\alpha^{-1}}}, \quad F_\alpha^{(r)} := \frac{F_\alpha^r}{\prod_{s=1}^r \frac{\bar{q}_\alpha^s - \bar{q}_\alpha^{-s}}{\bar{q}_\alpha - \bar{q}_\alpha^{-1}}}, \quad \text{for all } \alpha \in \Phi^+, r > 0,$$

and by the following elements in $U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)^0$:

$$K_{\alpha_i}^{(r)} = \begin{bmatrix} K_{\alpha_i}; 0 \\ r \end{bmatrix} := \prod_{s=1}^r \frac{K_{\alpha_i} q_{\alpha_i}^{1-s} - K_{\alpha_i}^{-1} q_{\alpha_i}^{s-1}}{q_{\alpha_i}^s - q_{\alpha_i}^{-s}}, \qquad i \in I.$$

Theorem 1.3.5 (cf. [Len14], Theorem 3.7)**.** *The restricted integral form $U_q^{\mathbb{Z}[q,q^{-1}]}(\mathfrak{g}, \Lambda)$ is a Hopf algebra over the ring $\mathbb{Z}[q, q^{-1}]$ and is an integral form for $U_q^{\mathbb{Q}(q)}(\mathfrak{g}, \Lambda)$.*

We now define the *restricted specialization* $U_q(\mathfrak{g}, \Lambda)$, by specializing to a specific choice $q \in \mathbb{C}^\times$. This is a complex Hopf algebra.

Definition 1.3.6. The infinite-dimensional Hopf algebra $U_q(\mathfrak{g}, \Lambda)$ is defined by

$$U_q(\mathfrak{g}, \Lambda) := U_q^{\mathbb{Z}[q,q^{-1}]}(\mathfrak{g}, \Lambda) \otimes_{\mathbb{Z}[q,q^{-1}]} \mathbb{C}_q,$$

where $\mathbb{C}_q = \mathbb{C}$ with the $\mathbb{Z}[q, q^{-1}]$-module structure defined by the specific value $q \in \mathbb{C}^\times$. We call $U_q(\mathfrak{g}, \Lambda)$ the *restricted specialization.*

From now on, q will be a primitive ℓ-th root of unity in $\mathbb{C}^\times$. We make an explicit choice.

Convention 1.3.7. *Let $\ell > 1$. In the following, q is an ℓ-th root of unity in $\mathbb{C}^\times$. We fix $q = \exp(\frac{2\pi i}{\ell})$ and for $a \in \mathbb{R}$ we set $q^a = \exp(\frac{2\pi i a}{\ell})$.*

We finally introduce the small quantum group $u_q(\mathfrak{g}, \Lambda, \Lambda')$. For ℓ odd and not equal to 3 in the case $\mathfrak{g} = G_2$, Lusztig described in [Lus90], Theorem 8.10 a homomorphism of Hopf algebras, which he called *Frobenius homomorphism*:

$$U_q(\mathfrak{g}) \to U(\mathfrak{g}).$$

Here, $U(\mathfrak{g})$ is the classical universal enveloping algebra of $\mathfrak{g}$ and $U_q(\mathfrak{g})$ the restricted specialization (for $\Lambda = \Lambda_R$) from above. The kernel of this homomorphism turned out to be a finite-dimensional Hopf algebra $u_q^{\mathcal{L}}(\mathfrak{g})$, the so-called *Frobenius-Lusztig kernel*. However, this Hopf algebra does not (always) coincide with the usual description of the small quantum group $u_q(\mathfrak{g})$ in terms of generators and relations, which we will give below. In [Len14], Theorem 5.4, the connection between these two Hopf algebras is given. We will use this result later to provide solutions of the R-matrix ansatz in Section 2.1, even in the cases of small order ℓ.

Definition 1.3.8. Let $\mathfrak{g}$ be a finite-dimensional complex simple Lie algebra with root system Φ and assume $\mathrm{ord}(q^2) > d_\alpha$ for all $\alpha \in \Phi$. For lattices Λ, Λ' with $\Lambda_R \subset \Lambda \subset \Lambda_W$ and $2\Lambda_R^{(\ell)} \subset \Lambda' \subset \mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R$, we define the *small quantum group* $u_q(\mathfrak{g}, \Lambda, \Lambda')$ as the algebra $U_q(\mathfrak{g}, \Lambda)$ from Definition 1.3.6, generated by K_λ for $\lambda \in \Lambda$ and E_α, F_α with $\ell_\alpha > 1$, $\alpha \in \Phi^+$ not necessarily simple, together with the relations

$$E_\alpha^{\ell_\alpha} = 0, \quad F_\alpha^{\ell_\alpha} = 0 \quad \text{and} \quad K_\lambda = 1 \text{ for } \lambda \in \Lambda'.$$

The coalgebra structure is again given as in Definition 1.3.2. This is a finite dimensional Hopf algebra of dimension

$$|\Lambda/\Lambda'| \prod_{\alpha \in \Phi^+,\ \ell_\alpha > 1} \ell_\alpha^2.$$

The fact, that this gives a Hopf algebra for $\Lambda' = 2\Lambda_R^{(\ell)}$ is shown in Lusztig, [Lus90], Sec. 8.

We fix the assumption on Λ'.

Assumption 1.3.9. *We assume for the sublattice $\Lambda' \subset \Lambda_W$ in the following that*

$$2\Lambda_R^{(\ell)} \subset \Lambda' \subset \mathrm{Cent}(\Lambda_W) \cap \Lambda_R$$

holds.

Chapter 2

An ansatz for R-matrices

The goal of this thesis is to construct new families of R-matrices for small quantum groups and certain extensions thereof (see Def. 1.3.8). Since in general there is no R-matrix for the small quantum group $u_q(\mathfrak{g}) = u_q(\mathfrak{g}, \Lambda_R, \Lambda')$ we consider extensions $u_q(\mathfrak{g}, \Lambda, \Lambda')$ for a lattice $\Lambda_R \subset \Lambda \subset \Lambda_W$ to remedy this situation. Our starting point is Lusztig's ansatz in [Lus93], Sec. 32.1, for a universal R-matrix of $U_q(\mathfrak{g}, \Lambda)$. This ansatz has been translated by Müller in his Dissertation [Mül98a], resp. in [Mül98b], for the use in the case of small quantum groups, which we will use in the following. Note, that this ansatz has been successfully generalized to general diagonal Nichols algebras in [AY13]. In section 2.2 we will then introduce a function $g\colon \pi_1 \times \pi_1 \to \mathbb{C}$ on the fundamental group $\pi_1 = \Lambda_W/\Lambda_R$ of the Lie algebra $\mathfrak{g}$ and derive equations for g which are under our assumption equivalent to the R-matrix ansatz. The following Chapters 3 and 4 are devoted to finding the solutions of these equations.

2.1. Lusztig's ansatz $R = R_0\bar{\Theta}$

The (universal) R-matrix (see Def. 1.1.1) was introduced originally by Drinfeld as an intertwiner of the comultiplication of the quantum group and its opposed comultiplication. Lusztig introduced in [Lus93] a so-called quasi-R-matrix, which is an intertwiner between the comultiplication Δ and a new comultiplication $\bar{\Delta}$, obtained by conjugating with a certain antilinear involution. This quasi-R-matrix Θ has a simpler characterization as the R-matrix R and is equal to it except for an element $R_0 \in \mathbb{C}[\Lambda] \otimes \mathbb{C}[\Lambda]$, i.e. $R = R_0\bar{\Theta}$, which is an intertwiner of $\bar{\Delta}$ and the opposed comultiplication Δ^{opp}. Here, the diagonal part is given by a suitable sum over terms of the form $K_\mu \otimes K_\nu$, $\mu, \nu \in \Lambda$.

In the following, we will fix the prerequisites of this chapter. For a finite-dimensional, semisimple complex Lie algebra $\mathfrak{g}$, an ℓ-th root of unity q and lattices Λ, Λ' as in Section 1.3, we write $u = u_q(\mathfrak{g}, \Lambda, \Lambda')$ and u^+, u^- for the parts generated by the E_{α_i} and F_{α_i}, respectively. By $\bar{u}$ we denote the small quantum group obtained for q^{-1} instead of q. Then u and $\bar{u}$ can be identified as sets. Let $^{-}\colon u \to \bar{u}$ be the $\mathbb{Q}$-algebra isomorphism defined by $q \mapsto q^{-1}$, $E_{\alpha_i} \mapsto E_{\alpha_i}$, $F_{\alpha_i} \mapsto F_{\alpha_i}$, $i \in I$, and $K_\lambda \mapsto K_{-\lambda}$, $\lambda \in \Lambda$. Then the map $^{-} \otimes {}^{-}\colon u \otimes u \to \bar{u} \otimes \bar{u}$ is a well-defined $\mathbb{Q}$-algebra isomorphism and we can define a $\mathbb{Q}(q)$-algebra morphism $\bar{\Delta}\colon u \to u \otimes u$ given by $\bar{\Delta}(x) = \overline{\Delta(\bar{x})}$ for all $x \in U$. We have in general $\bar{\Delta} \neq \Delta$.

Assume in the following, that

$$\ell_i > 1 \text{ for all } i \in I, \text{ and } \ell_i > -\langle \alpha_i, \alpha_j \rangle \text{ for all } i, j \in I \text{ with } i \neq j. \tag{2.1.1}$$

This assumption does not hold for all root systems and small orders ℓ. The following Theorem provides solutions of the R-matrix ansatz $R = R_0\bar{\Theta}$ for these cases as well.

Theorem 2.1.1 ([Len14])**.** *For a root system Φ of a finite-dimensional simple complex Lie algebra and an ℓ-th root of unity q, the condition (2.1.1) fails only in the cases (Φ, ℓ) listed in table 2.1. In each case, the small quantum group $u_q(\mathfrak{g})$ is described by a different $\tilde{\Phi}$ fulfilling (2.1.1), hence the present work also provides solutions of the R-matrix ansatz $R = R_0\bar{\Theta}$ for these cases by consulting the results for $\tilde{\Phi}$.*

Φ	(all)	B_n	C_n	F_4	G_2	G_2
ℓ	$1, 2$	4	4	4	$3, 6$	4
$\tilde{\Phi}$	(empty)	$\underbrace{A_1 \times \ldots \times A_1}_{n-\text{times}}$	D_n	D_4	A_2	A_3

Table 2.1.: Exceptional cases of (Φ, ℓ)

For sublattices $\Lambda_R \subset \Lambda \subset \Lambda_W$ and $2\Lambda_R^{(\ell)} \subset \Lambda' \subset \mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R$ we will now give the quasi-R-matrix of the small quantum group $u = u_q(\mathfrak{g}, \Lambda, \Lambda')$, cf. Definition 1.3.8. On the Borel parts u^+ and u^- exists a natural $\mathbb{N}_0[\alpha_i \mid i \in I]$-grading with E_{α_i} and F_{α_i} homogeneous of degree α_i for all $i \in I$. For $\nu \in \mathbb{N}_0[\alpha_i \mid i \in I]$ we write $u_\nu^\pm$ for the corresponding homogeneous component. We will quote most of the following results without proofs. Theorem 2.1.2 is essentially in [Lus93] and in this form for the finite-dimensional small quantum groups in [Mül98b]. Note that the roles of E, F will be switched in this thesis to match the usual convention.

Theorem 2.1.2 (cf. [Mül98b], Theorem 8.2)**.** *(a) There is a unique family of elements $\Theta_\nu \in u_\nu^+ \otimes u_\nu^-$, $\nu \in \mathbb{N}_0[\alpha_i \mid i \in I]$, such that $\Theta_0 = 1 \otimes 1$ and $\Theta = \sum_\nu \Theta_\nu \in u \otimes u$ satisfies $\Delta(x)\Theta = \Theta\bar{\Delta}(x)$ for all $x \in u$.*

(b) Let B be a vector space-basis of u^+, such that $B_\nu = B \cap u_\nu^+$ is a basis of u_ν^+ for all ν. Let $\{b^* \mid b \in B_\nu\}$ be the basis of u_ν^- dual to B_ν under the non-degenerate bilinear form $(\,\cdot\,,\,\cdot\,)\colon u^+ \otimes u^- \to \mathbb{C}$ (defined in [Mül98b, Sec. 1.2]). We have

$$\Theta_\nu = (-1)^{\mathrm{tr}\,\nu} q_\nu \sum_{b \in B_\nu} b^+ \otimes b^{*-} \in u_\nu^+ \otimes u_\nu^-, \tag{2.1.2}$$

where $q_\nu = \prod_i q_i^{\nu_i}$, $\mathrm{tr}\,\nu = \sum_i \nu_i \in \mathbb{Z}$ for $\nu = \sum_i \nu_i \alpha_i \in \Lambda_R$, $\nu_i \in \mathbb{Z}$.

Remark 2.1.3 (cf. [Mül98b], Remark 8.3). *(i) The element Θ is called the* quasi-R-matrix *of $u = u_q(\mathfrak{g}, \Lambda, \Lambda')$.*

(ii) Since the element Θ is unique, the expressions $\sum_{b\in B_\nu} b^+ \otimes b^{*-}$ in part (b) of the theorem are independent of the actual choice of the basis B of u^+.

(iii) For example, if $\mathfrak{g} = A_1$, i.e. there is only one simple root $\alpha = \alpha_1$, and generators E_α and F_α of the Borel parts of u. Thus we have

$$\Theta = \sum_{n=0}^{\ell_\alpha - 1} (-1)^n \frac{(q-q^{-1})^n}{[n]_q!} q^{-n(n-1)/2} E_\alpha^n \otimes F_\alpha^n.$$

(iv) The quasi-R-matrix Θ is invertible with inverse $\Theta^{-1} = \bar{\Theta}$, i.e. the expression one gets by changing all q to $\bar{q} = q^{-1}$.

In the following, we will give some properties of the quasi-R-matrix Θ. Here, we again use the notion of Definition 1.1.1, i.e. for an element $P \in u \times u$ we denote $P \otimes 1$, $1 \otimes P$ and $(\tau \otimes id)(P_{23})$ by P_{12}, P_{23} and P_{13}, respectively.

Proposition 2.1.4 (cf. [Mül98b], Prop. 8.4). *We have $\Theta\bar{\Theta} = \bar{\Theta}\Theta = 1 \otimes 1$ in $u \times u$.*

Proposition 2.1.5 (cf. [Mül98b], Prop. 8.5). *For all $\nu \in \mathbb{N}_0[\alpha_i \mid i \in I]$ we have*

$$(\Delta \otimes id)\bar{\Theta}_\nu = \sum_{\nu'+\nu''=\nu} \bar{\Theta}_{\nu',13}(1 \otimes K_{-\alpha'_\nu} \otimes 1)\bar{\Theta}_{\nu'',23},$$
$$(id \otimes \Delta)\bar{\Theta}_\nu = \sum_{\nu'+\nu''=\nu} \bar{\Theta}_{\nu',13}(1 \otimes K_{-\alpha'_\nu} \otimes 1)\bar{\Theta}_{\nu'',12}.$$

We now give the Theorem about the R-matrix ansatz $R = R_0\bar{\Theta}$ and for the convenience of the reader, we reproduce the proof of [Mül98b]. We will modify this ansatz in following section and determine all solutions for R_0 of the form such that $R = R_0\bar{\Theta}$ is an R-matrix in the last two Chapters 3 and 4.

Theorem 2.1.6 (cf. [Mül98b], Thm. 8.11). *Let $\Lambda' \subset \{\mu \in \Lambda \mid K_\mu$ central in $U_q(\mathfrak{g}, \Lambda)\}$ be a subgroup of Λ, and H_1, H_2 be subgroups of Λ/Λ', containing Λ_R/Λ'. In the following, $\mu, \mu_1, \mu_2 \in H_1$ and $\nu, \nu_1, \nu_2 \in H_2$.*

The element $R = R_0\bar{\Theta}$ with $R_0 = \sum_{\mu,\nu} f(\mu,\nu) K_\mu \otimes K_\nu$ is an R-matrix for $u_q(\mathfrak{g}, \Lambda, \Lambda')$, if and only if for all $\alpha \in \Lambda_R$ and μ, ν the following holds:

$$f(\mu+\alpha,\nu) = q^{-(\nu,\alpha)} f(\mu,\nu), \quad f(\mu,\nu+\alpha) = q^{-(\mu,\alpha)} f(\mu,\nu), \tag{2.1.3}$$

$$\sum_{\substack{\nu_1,\nu_2\in H_2\\ \nu_1+\nu_2=\nu}} f(\mu_1,\nu_1) f(\mu_2,\nu_2) = \delta_{\mu_1,\mu_2} f(\mu_1,\nu), \quad \sum_{\substack{\mu_1,\mu_2\in H_1\\ \mu_1+\mu_2=\mu}} f(\mu_1,\nu_1) f(\mu_2,\nu_2) = \delta_{\nu_1,\nu_2} f(\mu,\nu_1), \tag{2.1.4}$$

$$\sum_\mu f(\mu,\nu) = \delta_{\nu,0}, \quad \sum_\nu f(\mu,\nu) = \delta_{\mu,0}. \tag{2.1.5}$$

Before we proceed with the proof we make some remarks.

Remark 2.1.7. *(1) Condition (2.1.5) follows from (2.1.3) and (2.1.4) if there exists $c \in \mathbb{C}^\times$ such that $f(\mu,0) = f(0,\nu) = c$ for all μ,ν.*

(2) There are conditions on the order of q: For all μ,ν for which there exist $\tilde{\mu},\tilde{\nu}$ such that $f(\mu,\tilde{\nu}) \neq 0$, $f(\tilde{\mu},\nu) \neq 0$ we have

$$q^{2l_i(\mu,\alpha_i)} = q^{2l_i(\nu,\alpha_i)} = 1. \tag{2.1.6}$$

If this condition is satisfied then f is well-defined on the preimages of $H_1 \times H_2$ under $\Lambda \to \Lambda/\Lambda'$. In particular, this is the case under our assumption $2\Lambda_W^{(\ell)} \subset \Lambda' \subset \mathrm{Cent}^{[\ell]}(\Lambda_W)$.

Proof of Theorem 2.1.6. Since $2\Lambda_W^{(\ell)} \subset \Lambda'$ and $f(\mu + 2\ell_i\alpha_i,\nu) = q^{-2\ell_i(\nu,\alpha_i)}f(\mu,\nu) = f(\mu,\nu)$ by (2.1.3) and (2.1.6), the function f is well-defined on Λ/Λ'. We will show the equivalence of the R-matrix conditions (1.1.1)-(1.1.3) to the equations in (2.1.3)-(2.1.5).

(1) Condition (1.1.1) states $\Delta^{\mathrm{opp}}(x)R = R\Delta(x)$ for all $x \in u$. With Theorem 2.1.2, this gives $\Delta^{\mathrm{opp}}(x)R_0 = R_0\bar{\Delta}(x)$. Since this equation holds for all group-like elements K_μ we have to show, that it holds for all E_{α_i}, F_{α_i}, $i \in I$. We check the condition for $x = E_{\alpha_i}$:

$$(E_{\alpha_i} \otimes 1 + K_{\alpha_i} \otimes E_{\alpha_i})R_0 = R_0(1 \otimes E_{\alpha_i} + E_{\alpha_i} \otimes K_{-\alpha_i}). \tag{2.1.7}$$

On u exists an grading $u_{(\alpha,\beta)} = (u_\alpha^+ \otimes u^0 \otimes u_\beta^-)$. With respect to this gradation, the elements $(E_{\alpha_i} \otimes 1)R_0$ and $R_0(E_{\alpha_i} \otimes K_{-\alpha_i})$ belong to $u_{(\alpha_i,0)} \otimes u_{(0,0)}$, and $(K_{\alpha_i} \otimes E_{\alpha_i})R_0$ and $R_0(1 \otimes E_{\alpha_i})$ belong to $u_{(0,0)} \otimes u_{(\alpha_i,0)}$. This subspaces intersect in $\{0\}$, hence equation (2.1.7) is equivalent to $(E_{\alpha_i} \otimes 1)R_0 = R_0(E_{\alpha_i} \otimes K_{-\alpha_i})$ and $(K_{\alpha_i} \otimes E_{\alpha_i})R_0 = R_0(1 \otimes E_{\alpha_i})$. Thus,

$$\begin{aligned}
(E_{\alpha_i} \otimes 1)R_0 &= \sum_{\mu,\nu} f(\mu,\nu)q^{-(\mu,\alpha_i)}(K_\mu \otimes K_{\nu+\alpha_i})(E_{\alpha_i} \otimes K_{-\alpha_i}) \\
&= \sum_{\mu,\nu} f(\mu,\nu+\alpha_i)(K_\mu \otimes K_{\nu+\alpha_i})(E_{\alpha_i} \otimes K_{-\alpha_i}) \\
&= R_0(E_{\alpha_i} \otimes K_{-\alpha_i}),
\end{aligned}$$

holds if and only if $f(\mu,\nu+\alpha_i) = f(\mu,\nu)q^{-(\mu,\alpha_i)}$ for all μ,ν. An analogous calculation shows that $(K_{\alpha_i} \otimes E_{\alpha_i})R_0 = R_0(1 \otimes E_{\alpha_i})$ is equivalent to $f(\mu+\alpha_i,\nu) = f(\mu,\nu)q^{-(\nu,\alpha_i)}$ for all μ,ν. The equations for F_{α_i} give the same conditions for f, with α_i replaced by $-\alpha_i$.

(2) Condition (1.1.2) states $(\Delta \otimes id)(R) = R_{13}R_{23}$. With $R = R_0\bar{\Theta}$ and Proposition 2.1.5 we have

$$(\Delta \otimes id)(R) = \sum_{\alpha_1,\alpha_2,\mu,\nu} f(\mu,\nu)(K_\mu \otimes K_{\mu-\alpha_1} \otimes K_\nu)\bar{\Theta}_{\alpha_1,13}\bar{\Theta}_{\alpha_2,23},$$

and

$$\begin{aligned}
R_{13}R_{23} &= \sum f(\mu_1,\nu_1)f(\mu_2,\nu_2)(K_{\mu_1}\otimes K_{\mu_2}\otimes K_{\nu_1+\nu_2})q^{-(\nu_2,\alpha_1)}\bar{\Theta}_{\alpha_1,13}\bar{\Theta}_{\alpha_2,23}\\
&= \sum f(\mu_1,\nu_1)f(\mu_2+\alpha_1,\nu_2)(K_{\mu_1}\otimes K_{\mu_2}\otimes K_{\nu_1+\nu_2})\bar{\Theta}_{\alpha_1,13}\bar{\Theta}_{\alpha_2,23}\\
&= \sum f(\mu_1,\nu_1)f(\mu_2,\nu_2)(K_{\mu_1}\otimes K_{\mu_2-\alpha_1}\otimes K_{\nu_1+\nu_2})\bar{\Theta}_{\alpha_1,13}\bar{\Theta}_{\alpha_2,23}.
\end{aligned}$$

Since the group-like elements are linearly independent, we have equality if and only if for all ν,μ_1,μ_2

$$\sum_{\nu_1+\nu_2=\nu} f(\mu_1,\nu_1)f(\mu_2,\nu_2)=\delta_{\mu_1,\mu_2}f(\mu_1,\nu).$$

The other condition of (2.1.4) is equivalent to (1.1.3), i.e. $(id\otimes\Delta)(R)=R_{13}R_{12}$.

(3) It remains the invertibility of R. Assume conditions (1.1.1)-(1.1.3) for R. We then have the following equivalent conditions (cf. [Kas95], Theorem VIII.2.4, and use that the antipode of u is invertible):

(i) R is invertible

(ii) $(\varepsilon\otimes id)R=1$

(iii) $(id\otimes\varepsilon)R=1$

We have $(\varepsilon\otimes id)\bar{\Theta}=(id\otimes\varepsilon)\bar{\Theta}=1$ because the only non-zero contribution comes from $\bar{\Theta}_0\otimes\bar{\Theta}_0=1\otimes 1$. Direct calculation now shows that $(\varepsilon\otimes id)R=(id\otimes\varepsilon)R=1$ is equivalent to (2.1.5). If in addition there exist a $c\in\mathbb{C}^\times$ such that $f(\mu,0)=f(0,\nu)=c$ for all μ,ν, then (2.1.4) implies for $\mu_2=0$:

$$\sum_{\nu_1+\nu_2=\nu} f(\mu,\nu_1)c=\delta_{\mu,0}f(\mu,\nu)=\delta_{\mu,0}c,$$

and this is equivalent to $\sum_{\nu_1}f(\mu,\nu_1)=\delta_{\mu,0}$. ∎

2.2. Two sets of equations

Let $\mathfrak{g}$ be a finite-dimensional, simple complex Lie algebra, and q a primitive ℓ-th root of unity, both fixed in the following section. Following the ansatz in Theorem 2.1.6, we will now introduce a function $g\colon \pi_1\times\pi_1\to\mathbb{C}$ with $\pi_1=\Lambda_W/\Lambda_R$ the fundamental group of $\mathfrak{g}$ and derive equations for g analogue to equations (2.1.4) and (2.1.5). For this, we will use the quasi-periodicity of equations (2.1.3) and the assumption $\Lambda'\subset\mathrm{Cent}^{[\ell]}(\Lambda_W)$. This leads to two sets of equations, which depend either only on the group π_1 or on certain sublattices of Λ and the order ℓ of the root of unity q. We will call these equations *group-equations* and *diamond-equations*, respectively. In Chapters 3 and 4 we will see that under our assumption on Λ' the solutions of these equations give all solutions of R_0 as in the Theorem 2.1.6, hence we get all possible R-matrices satisfying Lusztig's ansatz $R=R_0\Theta$.

Lemma 2.2.1. *Let $\Lambda \subset \Lambda_W$ a sublattice and $\Lambda' \subset \Lambda$. Assume in addition, $\Lambda' \subset \mathrm{Cent}^{[\ell]}(\Lambda_W)$.*

(i) Let $f : \Lambda/\Lambda' \times \Lambda/\Lambda' \to \mathbb{C}$, satisfying condition (2.1.3) of Theorem 2.1.6. Then

$$g(\bar{\mu}, \bar{\nu}) := |\Lambda_R/\Lambda'| q^{(\mu,\nu)} f(\mu, \nu), \tag{2.2.1}$$

defines a function $\pi_1 \times \pi_1 \to \mathbb{C}$.

(ii) Let f and g as in (i). Then f satisfies conditions (2.1.4)-(2.1.5), if and only if the function g satisfies the following equations:

$$\begin{aligned} \sum_{\bar{\nu}_1+\bar{\nu}_2=\bar{\nu}} \delta_{(\mu_2-\mu_1\in \mathrm{Cent}^{[\ell]}(\Lambda_R))} q^{(\mu_2-\mu_1,\bar{\nu}_1)} g(\bar{\mu}_1, \bar{\nu}_1) g(\bar{\mu}_2, \bar{\nu}_2) &= \delta_{\mu_1,\mu_2} g(\bar{\mu}_1, \bar{\nu}), \\ \sum_{\bar{\mu}_1+\bar{\mu}_2=\bar{\mu}} \delta_{(\nu_2-\nu_1\in \mathrm{Cent}^{[\ell]}(\Lambda_R))} q^{(\nu_2-\nu_1,\bar{\mu}_1)} g(\bar{\mu}_1, \bar{\nu}_1) g(\bar{\mu}_2, \bar{\nu}_2) &= \delta_{\nu_1,\nu_2} g(\bar{\mu}, \bar{\nu}_1), \end{aligned} \tag{2.2.2}$$

$$\begin{aligned} \sum_{\bar{\nu}} \delta_{(\mu\in \mathrm{Cent}^{[\ell]}(\Lambda_R))} q^{-(\mu,\bar{\nu})} g(\bar{\mu}, \bar{\nu}) &= \delta_{\mu,0}, \\ \sum_{\bar{\mu}} \delta_{(\nu\in \mathrm{Cent}^{[\ell]}(\Lambda_R))} q^{-(\nu,\bar{\mu})} g(\bar{\mu}, \bar{\nu}) &= \delta_{\nu,0}. \end{aligned} \tag{2.2.3}$$

Here, the sums range over π_1 and expressions like $\delta_{(\mu\in \mathrm{Cent}^{[\ell]}(\Lambda_R))}$ equals 1 if μ is a central weight and 0 otherwise.

Before we proceed with the proof we will comment on the relevance of this equations and introduce two new notion, see also Definitions 3.5.1 and 4.1.2. For a given Lie algebra $\mathfrak{g}$ with root lattice Λ_R and weight lattice Λ_W the solutions of the $g(\bar{\mu}, \bar{\nu})$-equations give solutions for R_0 in the ansatz $R = R_0\bar{\Theta}$. Hence, we get possible R-matrices for the quantum group $u_q(\mathfrak{g}, \Lambda_W, \Lambda')$.

We divide the equations in two types: For central weight $\zeta = 0$ we call the equations (2.2.2)-(2.2.3) *group-equations*, cf. also Definition 3.5.1:

$$\begin{aligned} g(\bar{\mu}, \bar{\nu}) &= \sum_{\bar{\nu}_1+\bar{\nu}_2=\bar{\nu}} g(\bar{\mu}, \bar{\nu}_1) g(\bar{\mu}, \bar{\nu}_2), \\ g(\bar{\mu}, \bar{\nu}) &= \sum_{\bar{\mu}_1+\bar{\mu}_2=\bar{\mu}} g(\bar{\mu}_1, \bar{\nu}) g(\bar{\mu}_2, \bar{\nu}), \\ 1 &= \sum_{\bar{\nu}} g(0, \bar{\nu}), \\ 1 &= \sum_{\bar{\mu}} g(\bar{\mu}, 0) \end{aligned}$$

with $\bar{\mu}, \bar{\mu}_1, \bar{\mu}_2, \bar{\nu}, \bar{\nu}_1, \bar{\nu}_2 \in \pi_1$. For π_1 of order N this gives us $2N^2 + 2$ group-equations.

For central weight $0 \neq \zeta \in \mathrm{Cent}^{[\ell]}(\Lambda_R) \setminus \Lambda'$, we call the equations (2.2.2)-(2.2.3) *diamond-equations* (for reasons that will become transparent later), cf. also Definition

4.1.2:

$$\begin{aligned}
0 &= \sum_{\bar\nu_1+\bar\nu_2=\bar\nu} q^{(\zeta,\bar\nu_1)} g(\bar\mu,\bar\nu_1) g(\bar\mu+\bar\zeta,\bar\nu_2),\\
0 &= \sum_{\bar\mu_1+\bar\mu_2=\bar\mu} q^{(\zeta,\bar\mu_1)} g(\bar\mu_1,\bar\nu) g(\bar\mu_2,\bar\nu+\bar\zeta),\\
0 &= \sum_{\bar\nu} q^{-(\bar\nu,\zeta)} g(\bar\mu+\bar\zeta,\bar\nu),\\
0 &= \sum_{\bar\mu} q^{-(\bar\mu,\zeta)} g(\bar\mu,\bar\nu+\bar\zeta),
\end{aligned}$$

with $\bar\mu,\bar\mu_1,\bar\mu_2,\bar\nu,\bar\nu_1,\bar\nu_2\in\pi_1$. This gives up to $(|\mathrm{Cent}^{[\ell]}(\Lambda_R)/\Lambda'|-1)(2N^2+2)$ diamond-equations.

Proof of Lemma 2.2.1. (i) Since $\Lambda'\subset\mathrm{Cent}^{[\ell]}(\Lambda_W)$ we have $q^{(\Lambda_W,\Lambda')}=1$ and terms $q^{(\mu,\nu)}$ for $\mu,\nu\in\Lambda/\Lambda'$ do not depend on the residue class representatives modulo Λ'. We check that the function g is well-defined. Let $\mu,\nu\in\Lambda$ and $\lambda'\in\Lambda'$. Thus,

$$\begin{aligned}
g(\mu+\lambda',\nu) &= |\Lambda_R/\Lambda'| q^{(\mu+\lambda',\nu)} f(\mu+\lambda',\nu)\\
&= |\Lambda_R/\Lambda'| q^{(\mu+\lambda',\nu)} q^{-(\lambda',\nu)} f(\mu,\nu) && \text{by eq. (2.1.3)}\\
&= |\Lambda_R/\Lambda'| q^{(\mu,\nu)} f(\mu,\nu)\\
&= g(\mu,\nu),
\end{aligned}$$

and analogously for $g(\mu,\nu+\lambda')$.

(ii) We consider equations (2.1.4). Let $\nu_i,\nu\in\Lambda/\Lambda'$ and write $\nu_i=\bar\nu_i+\alpha_i$ and $\nu=\bar\nu+\alpha$ with $\bar\nu_i,\bar\nu\in\Lambda_W/\Lambda_R$ and $\alpha_i,\alpha\in\Lambda_R$, $i=1,2$. For the sum $\nu=\nu_1+\nu_2$ we get $\bar\nu\equiv\bar\nu_1+\bar\nu_2$ in Λ_W/Λ_R, i.e. there is a cocycle $\sigma(\nu_1,\nu_2)\in\Lambda_R$ with $\bar\nu=\bar\nu_1+\bar\nu_2+\sigma(\nu_1,\nu_2)$ in Λ_W and $\alpha=\alpha_1+\alpha_2-\sigma(\nu_1,\nu_2)$. We will write σ for $\sigma(\nu_1,\nu_2)$.

$$\begin{aligned}
&\sum_{\nu_1+\nu_2=\nu} f(\mu_1,\nu_1) f(\mu_2,\nu_2)\\
&\quad= \sum_{\nu_1+\nu_2=\nu} q^{-(\mu_1,\nu_1)+(\bar\mu_1,\bar\nu_1)-(\mu_2,\nu_2)+(\bar\mu_2,\bar\nu_2)} f(\bar\mu_1,\bar\nu_1) f(\bar\mu_2,\bar\nu_2)\\
&\quad= \sum_{\bar\nu_1+\bar\nu_2=\bar\nu}\ \sum_{\alpha_1+\alpha_2=\alpha+\sigma} q^{-(\mu_1,\bar\nu_1)-(\mu_1,\alpha_1)+(\bar\mu_1,\bar\nu_1)} q^{-(\mu_2,\bar\nu_2)-(\mu_2,\alpha_2)+(\bar\mu_2,\bar\nu_2)} f(\bar\mu_1,\bar\nu_1) f(\bar\mu_2,\bar\nu_2)\\
&\quad= \sum_{\bar\nu_1+\bar\nu_2=\bar\nu} q^{-(\mu_1,\bar\nu_1)+(\bar\mu_1,\bar\nu_1)-(\mu_2,\bar\nu_2)+(\bar\mu_2,\bar\nu_2)} f(\bar\mu_1,\bar\nu_1) f(\bar\mu_2,\bar\nu_2) \sum_{\alpha_1+\alpha_2=\alpha+\sigma} q^{-(\mu_1,\alpha_1)-(\mu_2,\alpha_2)}
\end{aligned} \tag{$*$}$$

Firstly, we consider the second sum over the roots (μ_1,μ_2 are fixed).

$$\begin{aligned}
\sum_{\alpha_1+\alpha_2=\alpha+\sigma} q^{-(\mu_1,\alpha_1)-(\mu_2,\alpha_2)} &= \sum_{\alpha_1\in\Lambda_R/\Lambda'} q^{-(\mu_1,\alpha_1)-(\mu_2,\alpha+\sigma-\alpha_1)}\\
&= q^{-(\mu_2,\alpha+\sigma)} \sum_{\alpha_1\in\Lambda_R/\Lambda'} q^{(\mu_2-\mu_1,\alpha_1)}
\end{aligned}$$

The last sum equals $|\Lambda_R/\Lambda'|$ iff $\ell \mid (\mu_2-\mu_1,\alpha_1)$ for all $\alpha_1 \in \Lambda_R/\Lambda'$, i.e. $\mu_2-\mu_1 \in \mathrm{Cent}^{[\ell]}(\Lambda_R)$, and 0 otherwise. Hence, with $C = |\Lambda_R/\Lambda'| \cdot \delta_{(\mu_2-\mu_1\in\mathrm{Cent}^{[\ell]}(\Lambda_R))}$, the sum $(*)$ simplifies to

$$\begin{aligned}
&C \cdot \sum_{\bar\nu_1+\bar\nu_2=\bar\nu} q^{-(\mu_1,\bar\nu_1)+(\bar\mu_1,\bar\nu_1)-(\mu_2,\bar\nu_2)+(\bar\mu_2,\bar\nu_2)} q^{-(\mu_2,\alpha+\sigma)} f(\bar\mu_1,\bar\nu_1) f(\bar\mu_2,\bar\nu_2)\\
&\quad = C \cdot \sum_{\bar\nu_1+\bar\nu_2=\bar\nu} q^{-(\mu_1,\bar\nu_1)+(\bar\mu_1,\bar\nu_1)+(\bar\mu_2,\bar\nu_2)-(\mu_2,\bar\nu_1+\bar\nu_2+\alpha+\sigma)+(\mu_2,\bar\nu_1)} f(\bar\mu_1,\bar\nu_1) f(\bar\mu_2,\bar\nu_2)\\
&\quad = C \cdot q^{-(\mu_2,\nu)} \sum_{\bar\nu_1+\bar\nu_2=\bar\nu} q^{(\mu_2-\mu_1,\bar\nu_1)} q^{(\bar\mu_1,\bar\nu_1)} f(\bar\mu_1,\bar\nu_1) q^{(\bar\mu_2,\bar\nu_2)} f(\bar\mu_2,\bar\nu_2),
\end{aligned}$$

Comparing this with the right hand side of the first equation of (2.1.4) gives

$$\begin{aligned}
&C \cdot q^{-(\mu_2,\nu)} \sum_{\bar\nu_1+\bar\nu_2=\bar\nu} q^{(\mu_2-\mu_1,\bar\nu_1)} q^{(\bar\mu_1,\bar\nu_1)} f(\bar\mu_1,\bar\nu_1) q^{(\bar\mu_2,\bar\nu_2)} f(\bar\mu_2,\bar\nu_2)\\
&\qquad\qquad = \delta_{\mu_1,\mu_2} q^{-(\mu_2,\nu)+(\bar\mu_2,\bar\nu)} f(\bar\mu_2,\bar\nu),
\end{aligned}$$

and with the definition of $g(\bar\mu,\bar\nu) = |\Lambda_R/\Lambda'| q^{(\mu,\nu)} f(\mu,\nu)$ we get the following equation

$$\sum_{\bar\nu_1+\bar\nu_2=\bar\nu} \delta_{(\mu_2-\mu_1\in\mathrm{Cent}^{[\ell]}(\Lambda_R))} q^{(\mu_2-\mu_1,\bar\nu_1)} g(\bar\mu_1,\bar\nu_1) g(\bar\mu_2,\bar\nu_2) = \delta_{\mu_1,\mu_2} g(\bar\mu_1,\bar\nu).$$

Analogously, we get the equation of the sum over $\bar\mu_1+\bar\mu_2=\bar\mu$.

We now consider the equations (2.1.5). Again, $\nu = \bar\nu+\alpha$ as above.

$$\begin{aligned}
\sum_{\nu\in\Lambda/\Lambda'} f(\mu,\nu) &= \sum_{\nu} q^{-(\mu,\nu)+(\bar\mu,\bar\nu)} f(\bar\mu,\bar\nu)\\
&= \sum_{\bar\nu} q^{(\bar\mu,\bar\nu)} f(\bar\mu,\bar\nu) \sum_{\alpha\in\Lambda_R/\Lambda'} q^{-(\mu,\bar\nu+\alpha)}\\
&= \sum_{\bar\nu} q^{-(\mu-\bar\mu,\bar\nu)} f(\bar\mu,\bar\nu) \sum_{\alpha\in\Lambda_R/\Lambda'} q^{-(\mu,\alpha)}\\
&= \delta_{(\mu\in\mathrm{Cent}^{[\ell]}(\Lambda_R))} |\Lambda_R/\Lambda'| \sum_{\bar\nu} q^{-(\mu-\bar\mu,\bar\nu)} f(\bar\mu,\bar\nu)\\
&= \delta_{(\mu\in\mathrm{Cent}^{[\ell]}(\Lambda_R))} \sum_{\bar\nu} q^{-(\mu,\bar\nu)} g(\bar\mu,\bar\nu)\\
&= \delta_{\mu,0}.
\end{aligned}$$

Again, we get the equations for the sum over $\bar\mu$ analogously. ∎

Chapter 3

A theorem about roots of unity and solutions of the group-equations

The goal of this chapter is to give all solutions of the group-equations in Definition 3.5.1. To this end, we will prove a main theorem about roots of unity which characterizes subsets U of complex roots of unity with the property that all power sums over the roots are non-negative integers, as subgroups in $\mathbb{C}^\times$. We first introduce a combinatorial principle, which is the blueprint of the proof of this theorem. We then give an alternative proof of this theorem which does not need the aforementioned combinatorial principle. As an application of the theorem about roots of unity, we then prove a theorem about Fourier pairs of $\{0,1\}$-matrices, and this gives eventually the theorem about the solutions of the group-equations.

3.1. A combinatorial principle

Before we turn to the main Theorem 3.2.1 about roots of unity we prove the following apparently new combinatorial principle. It shows that the main Theorem does not depend on specific properties of prime numbers, but is combinatorial in nature. It also gives the blueprint for the proof of the main Theorem 3.2.1.

Theorem 3.1.1. *Let N be finite set, $\mathcal{P}(N)$ denote the power set of N and $\mathcal{E} \subset \mathcal{P}(N)$. Let $\mu\colon \mathcal{P}(N) \to [0,\infty)$ be a measure on $\mathcal{P}(N)$, such that $\mu(A) > 0$ for all non-empty $A \subset N$. Then the following is equivalent:*

(i) $a_C := (-1)^{|N|} \sum_{D\in\mathcal{E}} (-1)^{|C\cup D|} e^{\mu(C-D)} \geq 0$ *for all $C \subset N$.*

(ii) $\mathcal{E} = \{D \subset N \mid D \supset A\}$ *for some $A \subset N$. Such a set $\mathcal{E}$ is called a* principal filter *on N (see e.g. [Bou66, Chapter I, §6], we also allow the case of $A = \varnothing$).*

The remainder of this section is devoted to the proof of this theorem.

A straightforward calculation gives the values of the a_C if $\mathcal{E}$ is a filter. It shows immediately the implication $(ii) \Rightarrow (i)$, but the precise value will also be crucial to the proof of the converse. For subsets $\{p\} \subset N$, $p \in N$, we write shortly $\mu(p)$ instead of $\mu(\{p\})$.

Lemma 3.1.2. *Let $\mathcal{E}$ be a filter, i.e. $\mathcal{E} = \{D \subset N \mid D \supset A\}$ for some $A \subset N$. Then for any $C \subset N$ we have*

$$a_C = \begin{cases} e^{\mu(N\setminus A)} \prod_{p\in N\setminus A} \left(1 + e^{-\mu(p)}\right), & C \cup A = N, \\ 0, & \textit{else}. \end{cases}$$

Proof.

$$\begin{aligned} a_C &= (-1)^{|N|} \sum_{A\subset D\subset N} (-1)^{|C\cup D|} e^{\mu(C\setminus D)} \\ &= (-1)^{|N|} \sum_{D'\subset N\setminus A} (-1)^{|C\cup A\cup D'|} e^{\mu((C\setminus A)\setminus D')} \\ &= (-1)^{|N\setminus A|} \sum_{D'\subset N\setminus A} (-1)^{|(C\setminus A)\cup D'|} e^{\mu((C\setminus A)\setminus D')} \end{aligned}$$

This shows that the value of a_C for the filter generated by A in N is equal to the value of $a_{C\setminus A}$ for the filter generated by $\varnothing$ in $N \setminus A$. Thus it suffices to show the claim for the filter $\mathcal{E} = \mathcal{P}(N)$ generated by $A = \varnothing$:

$$\begin{aligned} a_C &= (-1)^{|N|} \sum_{D\subset N} (-1)^{|C\cup D|} e^{\mu(C\setminus D)} \\ &= (-1)^{|N|} \sum_{D_1\subset C, D_2\subset N\setminus C} (-1)^{|C|+|D_2|} e^{\mu(C)-\mu(D_1)} \\ &= (-1)^{|N|+|C|} e^{\mu(C)} \left(\sum_{D_2\subset N\setminus C} (-1)^{|D_2|} \right) \left(\sum_{D_1\subset C} e^{-\mu(D_1)} \right) \\ &\overset{(\sharp)}{=} (-1)^{|N|+|C|} e^{\mu(C)} \left(\prod_{p\in N\setminus C} (1-1) \right) \left(\prod_{p\in C} \left(1 + e^{-\mu(p)}\right) \right) \\ &= \begin{cases} e^{\mu(N)} \prod_{p\in N} \left(1 + e^{-\mu(p)}\right), & C = N, \\ 0, & \textit{else}. \end{cases} \end{aligned}$$

Assume the factors in the second last row labeled by elements of $N \setminus C$ and C, respectively. Then, equality $(\sharp)$ holds since there is for each subset D_2 of $N \setminus C$ exactly one possibility of choosing $|D_2|$ factors -1 in the product, and similar for the second product together with the σ-additivity of the measure μ. The general formula for arbitrary A follows by again replacing N with $N \setminus A$ and C by $C \setminus A$. ∎

We use this result to show that if $\mathcal{E}$ is a small modification of a filter, the main assumption $a_C \geq 0$ for all $C \subset N$ usually fails to be true.

Lemma 3.1.3. *Assume $|N| > 1$.*

(a) Let $\mathcal{E} \neq \mathcal{P}(N)$ be a filter in N, then $\mathcal{E} \cup \{\varnothing\}$ gives $a_C < 0$ for some $C \subset N$.

(b) Let $\mathcal{E} = \mathcal{P}(N)$ in N, then $\mathcal{E} \setminus \{\varnothing\}$ gives $a_C < 0$ for some $C \subset N$.

Note that on the other hand for $|N| = 1$ and $\mathcal{E}$ the only filter $\mathcal{E} \neq \mathcal{P}(N)$ we have that both $\mathcal{E} \cup \varnothing$ and $\mathcal{P}(N) \setminus \{\varnothing\}$ are filters (namely $\mathcal{P}(N)$ and $\mathcal{E}$).

Proof. (a) By assumption $\mathcal{E}$ is a filter generated by some $A \neq \varnothing$ for $|N| > 1$. We wish to find a negative value of some $\tilde{a}_C$ for the set system $\tilde{\mathcal{E}} := \mathcal{E} \cup \{\varnothing\}$: Suppose first that also $A \neq N$ and choose some $p \in N \setminus A$, then $a_{N\setminus\{p\}} = 0$ by Lemma 3.1.2 and thus:

$$\begin{aligned}
\tilde{a}_{N\setminus\{p\}} &= (-1)^{|N|} \sum_{D\in\mathcal{E}\cup\{\varnothing\}} (-1)^{|N\setminus\{p\}\cup D|} e^{\mu((N\setminus\{p\})\setminus D)} \\
&= a_{N\setminus\{p\}} + (-1)^{|N|+|N\setminus\{p\}|} e^{\mu(N\setminus\{p\})} \\
&= -e^{\mu(N\setminus\{p\})} < 0.
\end{aligned}$$

Suppose now that $A = N$ and choose some $q \in N$, then again by Lemma 3.1.2:

$$\begin{aligned}
\tilde{a}_{N\setminus\{q\}} &= (-1)^{|N|} \sum_{D\in\mathcal{E}\cup\{\varnothing\}} (-1)^{|N\setminus\{q\}\cup D|} e^{\mu((N\setminus\{q\})\setminus D)} \\
&= a_{N\setminus\{q\}} + (-1)^{|N|+|N\setminus\{q\}|} e^{\mu(N\setminus\{q\})} \\
&= 1 - e^{\mu(N\setminus\{q\})} < 0.
\end{aligned}$$

(b) By assumption $\mathcal{E} = \mathcal{P}(N)$ for $|N| > 1$, so $\mathcal{E}$ is the filter generated by $A = \varnothing$. Then again by Lemma 3.1.2 $a_C = 0$ for $C \neq N$. Choose any $p \neq q \in N$, then we calculate $\tilde{a}_{N\setminus\{p,q\}}$ for the filter $\tilde{\mathcal{E}} := \mathcal{E} \setminus \{\varnothing\}$:

$$\begin{aligned}
\tilde{a}_{N\setminus\{p,q\}} &= (-1)^{|N|} \sum_{D\in\mathcal{E}\setminus\{\varnothing\}} (-1)^{|N\setminus\{p,q\}\cup D|} e^{\mu((N\setminus\{p,q\})\setminus D)} \\
&= a_{N\setminus\{p,q\}} - (-1)^{|N|+|N\setminus\{p,q\}|} e^{\mu(N\setminus\{p,q\})} \\
&= 0 - e^{\mu(N\setminus\{p,q\})} < 0.
\end{aligned}$$

∎

We now proceed by introducing the induction step along $|N|$:

Definition 3.1.4. Let $\mathcal{E}$ be any system of subsets in N and $p \in N$, then we define a new set system for $N \setminus \{p\}$ by

$$\mathcal{E}_p = \{D \setminus \{p\} \mid p \in D, D \in \mathcal{E}\}$$

For $C \subset N \setminus \{p\}$ we denote by $a_C^{\{p\}}$ the corresponding sum over $\mathcal{E}_p$, i.e.

$$a_C^{\{p\}} = (-1)^{|N\setminus\{p\}|} \sum_{D\in\mathcal{E}_p} (-1)^{|C\cup D|} e^{\mu(C\setminus D)}$$

We will in the following only consider $\mathcal{E}_p$ for all p, such that there exists a $D \in \mathcal{E}$ with $p \in D$, so $\mathcal{E}_p$ is not empty.

We first wish to prove that our main assumption $a_C \geq 0$ implies $a_C^{\{p\}} \geq 0$ in $\mathcal{E}_p$:

Lemma 3.1.5. *For any $p \in N$ we get for all $C \in \mathcal{E}_p$ (note that $p \notin C$):*

$$a_C^{\{p\}} = \frac{e^{\mu(p)}}{1+e^{\mu(p)}} a_C + \frac{1}{1+e^{\mu(p)}} a_{C\cup\{p\}}$$

In particular, $a_C \geq 0$ for all $C \in \mathcal{E}$ implies $a_C^{\{p\}} \geq 0$ for all $C \in \mathcal{E}_p$.

Proof. We calculate the right hand side by splitting the sum over all $D \in \mathcal{E}$ into two summands for all $p \notin D$ resp. $p \in D$ and use $p \notin C$. The latter set of D then correspond to $D' = D \setminus \{p\}$ in $\mathcal{E}_p$:

$$\begin{aligned}
&\frac{e^{\mu(p)}}{1+e^{\mu(p)}} a_C + \frac{1}{1+e^{\mu(p)}} a_{C\cup\{p\}} \\
&\qquad = (-1)^{|N|} \frac{e^{\mu(p)}}{1+e^{\mu(p)}} \sum_{p\in D\in\mathcal{E}} (-1)^{|C\cup D|} e^{\mu(C\setminus\{D\})} \\
&\qquad + (-1)^{|N|} \frac{1}{1+e^{\mu(p)}} \sum_{p\in D\in\mathcal{E}} (-1)^{|C\cup\{p\}\cup D|} e^{\mu((C\cup\{p\})\setminus D)} \\
&\qquad + (-1)^{|N|} \frac{e^{\mu(p)}}{1+e^{\mu(p)}} \sum_{p\notin D\in\mathcal{E}} (-1)^{|C\cup D|} e^{\mu(C\setminus\{D\})} \\
&\qquad + (-1)^{|N|} \frac{1}{1+e^{\mu(p)}} \sum_{p\notin D\in\mathcal{E}} (-1)^{|C\cup\{p\}\cup D|} e^{\mu((C\cup\{p\})\setminus D)} \\
&\qquad = (-1)^{|N|} \frac{e^{\mu(p)}}{1+e^{\mu(p)}} \sum_{p\in D\in\mathcal{E}} (-1)^{|C\cup D|} e^{\mu(C\setminus D)} \\
&\qquad + (-1)^{|N|} \frac{1}{1+e^{\mu(p)}} \sum_{p\in D\in\mathcal{E}} (-1)^{|C\cup D|} e^{\mu(C\setminus D)} \\
&\qquad + (-1)^{|N|} \frac{e^{\mu(p)}}{1+e^{\mu(p)}} \sum_{p\notin D\in\mathcal{E}} (-1)^{|C\cup D|} e^{\mu(C\setminus D)} \\
&\qquad + (-1)^{|N|} \frac{1}{1+e^{\mu(p)}} \sum_{p\notin D\in\mathcal{E}} (-1)^{|C\cup D|+1} e^{\mu(C\setminus D)+\mu(p)} \\
&\qquad = \left(\frac{e^{\mu(p)}}{1+e^{\mu(p)}} + \frac{1}{1+e^{\mu(p)}}\right) \cdot (-1)^{|N|} \sum_{p\in D\in\mathcal{E}} (-1)^{|C\cup D|} e^{\mu(C\setminus D)} \\
&\qquad + \left(\frac{e^{\mu(p)}}{1+e^{\mu(p)}} - \frac{1}{1+e^{\mu(p)}} \cdot e^{\mu(p)}\right) \cdot (-1)^{|N|} \sum_{p\notin D\in\mathcal{E}} (-1)^{|C\cup D|} e^{\mu(C\setminus D)} \\
&\qquad = (-1)^{|N|} \sum_{p\in D\in\mathcal{E}} (-1)^{|C\cup D|} e^{\mu(C\setminus D)} \\
&\qquad = (-1)^{|N\setminus\{p\}|} \sum_{D'\in\mathcal{E}_p} (-1)^{|C\cup D'|} e^{\mu(C\setminus D')} = a_C^{\{p\}}.
\end{aligned}$$

∎

Thus if all $a_C \geq 0$ by induction hypothesis all $\mathcal{E}_p$ are filters. We now conclude by induction that $\mathcal{E}$ is a filter if all possible reductions $\mathcal{E}_p$ are filters. As induction step, we use the following lemma.

Lemma 3.1.6. *Let $\mathcal{E}$ be a set system for N such that all $\mathcal{E}_p$ are filters generated by sets $A_p \subset N - p$. Then either there exists $p \in N$ with $p \in A_q$ for all $q \neq p$ or for all $p \in N$ we have $A_p = \varnothing$.*
In the first case we show that $\mathcal{E}$ is the filter generated by $\{p\} \cup A_p$ or $\mathcal{E}$ is the set system consisting of this filter together with $D = \varnothing$. In the second case we show $\mathcal{E} = \mathcal{P}(N)$ or $\mathcal{E} = \mathcal{P}(N) \setminus \{\varnothing\}$.

Proof. Assume there exists q' with $A_{q'} \neq \varnothing$ and let $p \in A_{q'}$, then we claim $p \in A_q$ for all $q \neq p$. We prove this by contradiction. If $p \notin A_q$ for some q we consider $\{q'\} \cup A_q \in \mathcal{E}_q$ (since $\mathcal{E}_q$ is a filter) and hence $\{q\} \cup \{q'\} \cup A_q \in \mathcal{E}$ (by definition of $\mathcal{E}_q$). But then $\{q\} \cup A_q \in \mathcal{E}_{q'}$ and $A_{q'} \subset q \cup A_q$ (since $\mathcal{E}_{q'}$ is a filter). But this contradicts $p \notin A_q$, which shows the first part of the Lemma.

We now prove the consequences in the two cases. In the first case we assume it exists $p \in A_q$ for all $q \neq p$. Let $D \supset \{p\} \cup A_p$ then $D \in \mathcal{E}_p$ (since $\mathcal{E}_p$ is a filter) and $D \in \mathcal{E}$ (by definition of $\mathcal{E}_p$). Let now conversely be $D \in \mathcal{E}$. If $p \in D$ then we have $D \setminus \{p\} \in \mathcal{E}_p$ (by definition of $\mathcal{E}_p$) and hence also $D \supset A_p$ (since $\mathcal{E}_p$ is a filter), implying $D \supset \{p\} \cup A_p$. If $p \notin D$ then either $D = \varnothing$ or some $q \in D$. In the latter case $D \setminus \{q\} \in \mathcal{E}_q$, hence $D \setminus \{q\} \supset A_q \ni p$ which is a contradiction. So either $D \supset \{p\} \cup A_p$ or $D = \varnothing$ as asserted.
In the second case we assume $A_p = \varnothing$ for all $p \in N$, hence any for any set $D \neq \varnothing$ we may choose some $p \in D$ and obtain $D \setminus \{p\} \in \mathcal{E}_p$ and hence $D \in \mathcal{E}_q$. Hence any set with the possible exception of $D = \varnothing$ is in $\mathcal{E}$ as asserted. ∎

We can now conclude the inductive proof of the implication (i)⇒(ii) in Theorem 3.1.1: For $|N| = 0$ the only set system is $\mathcal{E} = \{\varnothing\}$ and is a filter. Let $|N| \geq 1$ and $\mathcal{E}$ such that all $a_C \geq 0$, then $a_C^{\{p\}} \geq 0$ for all $p \in N$ by Lemma 3.1.5. Thus by induction hypothesis all $\mathcal{E}_p$ are filters. Then by Lemma 3.1.6 we have that either $\mathcal{E}$ is a filter (in which case the induction step is finished) or some filter $\mathcal{E} \neq \mathcal{P}(N)$ together with $\varnothing$ or $\mathcal{E} = \mathcal{P}(N) \setminus \{\varnothing\}$. By Lemma 3.1.3 these two cases can only fulfill $a_C \geq 0$ for $|N| = 1$ where both are filters. This concludes the proof of Theorem 3.1.1.

3.2. A theorem about roots of unity

The following theorem is the main result of this chapter. It will be used to prove Theorem 3.4.4 about Fourier pairs of $\{0, 1\}$-matrices and hence to find all solutions of the group-equations. The proof of the theorem is along the lines of the proof of Theorem 3.1.1.

Theorem 3.2.1. *Let U be a non-empty finite set of complex roots of unity and consider for all $k \in \mathbb{Z}$ the power sums $a_k := \sum_{\zeta \in U} \zeta^k$. Then all a_k are non-negative integers iff*

U is actually a multiplicative group of roots of unity (i.e. all N-th roots of unity for some N).

The remainder of this section is devoted to the proof of this theorem.

Since U is finite, we may assume some integer N such that $U \subset \Sigma_N = \{\zeta \in \mathbb{C} \mid \zeta^N = 1\}$. For $k \in \mathbb{N}$ we denote by ξ_k the primitive k-th root of unity $\xi_k = \exp(2\pi i/k)$. We first prove the "$\Leftarrow$" implication of Theorem 3.2.1. In the following, we write shortly (a, b) for the greatest common divisor $\gcd(a, b)$ of two integers a and b.

Lemma 3.2.2. *Let U be a finite group of roots of unity in $\mathbb{C}^\times$, i.e. $U = \Sigma_N$ for some $N \in \mathbb{N}$. Then $a_k = \sum_{\zeta\in U} \zeta^k$ is a non-negative integer for all $k \in \mathbb{Z}$.*

Proof. Write $U = \Sigma_N = \{\xi_N^i \mid 0 \le i < N\}$ with the primitive N-th root of unity ξ_N. For k with $(k, N) = 1$ we have $\operatorname{ord}(\xi_N^k) = \operatorname{ord}(\xi_N) = N$, hence $\sum_{i=0}^{N-1} \xi_N^{ik} = 0$. If $(k, N) = N$, we have $\sum_{i=0}^{N-1} \xi_N^{ik} = \sum_{i=0}^{N-1} 1 = N$. For $1 < (k, N) = d < N$, the power ξ_N^k is a primitive (N/d)-th root of unity, namely $\xi_{N/d}$. Thus we get

$$\sum_{i=0}^{N-1} \xi_N^{ik} = d \sum_{i=0}^{N/d-1} \xi_{N/d}^i = 0. \qquad \blacksquare$$

We will now deal with the converse statement of Theorem 3.2.1. In the following, let U be a non-empty finite set of complex roots of unity. We start with the observation, that the set U is a union of orbits of the Galois group $\mathrm{Gal}(\xi_N)$, acting on Σ_N. Here, $\mathrm{Gal}(\xi_N)$ is the Galois group of the field extension $\mathbb{Q}(\xi_N)/\mathbb{Q}$ which permutes the N-th roots of unity.

Lemma 3.2.3. *Let $U \subset \Sigma_N$ and $a_k = \sum_{\zeta\in U} \zeta^k$ be a non-negative integer for all $k \in \mathbb{Z}$. Then U is invariant under the Galois group $G = \mathrm{Gal}(\xi_N)$, i.e. it is a union of orbits of G acting on Σ_N. Each orbit consist of all primitive roots of unity for some divisor of N and hence a_k only depends on the greatest common divisor (k, N).*

Proof. Let $p(x) = \prod_{\zeta\in U}(x - \zeta) \in \mathbb{C}[x]$, i.e. $p(\zeta) = 0$ for all $\zeta \in U$. Denote $t = |U|$ and $U = \{\zeta_1, \ldots, \zeta_t\}$. For $0 \le k \le t$ let $\sigma_k(x_1, \ldots, x_t) = \sum_{1\le j_1<\ldots<j_k\le t} x_{j_1} \cdot \ldots \cdot x_{j_k}$ be the elementary symmetric polynomials. Then $p(x) = \sum_{k=0}^{t}(-1)^{t-k}\sigma_{t-k}(\zeta_1, \ldots, \zeta_t)x^k$. Let $s_k(x_1, \ldots, x_t) = \sum_{i=1}^{t} x_i^k$, then we have in particular, $a_k = s_k(\zeta_1, \ldots, \zeta_t)$. By the Newton identities, the $\sigma_k(x_1, \ldots, x_t)$ can be expressed as sums of powers of the s_k with rational coefficients, e.g. $\sigma_2 = \frac{1}{2}s_1^2 - \frac{1}{2}s_2$. Thus, we have that the coefficients of $p(x)$, the $\sigma_k(\zeta_1, \ldots, \zeta_k)$, are sums of integers with rational coefficients, hence $p(x) \in \mathbb{Q}[x]$. (In fact, we have $p(x) \in \mathbb{Z}[x]$, since the $\sigma_k(\zeta_1, \ldots, \zeta_t)$ are algebraic integers in $\mathbb{Q}$, hence in $\mathbb{Z}$.) Thus we get that the Galois group G permutes the roots of $p(x)$, i.e. U consists of orbits of G. $\blacksquare$

Definition 3.2.4. Let $N \in \mathbb{N}$. The set $\mathcal{D}(N) = \{d \in \mathbb{N} \mid d \mid N\}$ is the *set of all divisors of N*. We call a set $\mathcal{E} \subset \mathcal{D}(N)$ a *filter in $\mathcal{D}(N)$* if there exist an $e \mid N$ such that $\mathcal{E} = e\mathcal{D}(N/e) = \{d \mid N \mid e \mid d\}$. In this case we write $\mathcal{E} = (e)_N$ or shortly (e) for the filter in $\mathcal{D}(N)$.

Note, that we again use, under slight abuse of notation, the term *filter*. This should be seen as an analogy to the set-theoretic term *filter on a set* N, used in Section 3.1, although the set $\mathcal{E}$ of divisors is not a filter on $\mathcal{D}(N)$ in this (set-theoretical) sense. From now on, by filter we mean the newly defined term in respect to divisibility.

By Lemma 3.2.3, the set U is of the form $U = \bigcup_{d\in\mathcal{E}}\{\xi_N^i \mid (N,i) = d\}$ for a set $\mathcal{E} \subset \mathcal{D}(N)$. We wish to prove that $\mathcal{E}$ is a filter in $\mathcal{D}(N)$ and consequently U a subgroup of $\mathbb{C}^\times$. For $c \mid N$ we have

$$a_c = \sum_{\zeta\in U} \zeta^c = \sum_{d\in\mathcal{E}} \sum_{(i,N)=d} \xi_N^{ic}.$$

The sum $\sum_{(i,N)=d} \xi_N^{ic}$ is essentially a so-called *Ramanujan-sum*. A straightforward calculation gives the values of the a_c.

Lemma 3.2.5. *For $N \in \mathbb{N}$ and $c \in \mathcal{D}(N)$, we have*

$$a_c = \sum_{d\in\mathcal{E}} \frac{\varphi(N/d)}{\varphi(N/(N,dc))}\mu\left(\frac{N}{(N,dc)}\right).$$

Here, $\varphi\colon \mathbb{N} \to \mathbb{N}$ is the Euler φ-function, given by $\varphi(\prod_{i=1}^t p_i^{r_i}) = \prod_{i=1}^t (p_i - 1)p_i^{r_i-1}$ for mutually different prime numbers p_i, and $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ is the Moebius function, defined by $\mu(n) = 1$ if n is square-free and has an even number of prime factors, $\mu(n) = -1$ if n is square-free and has an odd number of prime factors and $\mu(n) = 0$ if n has a squared prime factor.

Proof. It is an elementary number theoretical fact that for an primitive N-th root of unity ξ we have

$$\sum_{\substack{i=1\\(i,N)=1}}^{N} \xi^i = \mu(N)$$

with the Moebius function μ. For $d \mid N$ we have

$$\sum_{\substack{i=1\\(i,N)=d}}^{N} \xi_N^i = \sum_{\substack{i=1\\(i,N/d)=1}}^{N/d} \xi_{N/d}^i = \mu(N/d)$$

with primitive (N/d)-th root of unity $\xi_{N/d}$. For $c \mid N$ we get

$$\sum_{\substack{i=1\\(i,N)=d}}^{N} \xi_N^{ic} = \sum_{\substack{i=1\\(i,N/d)=1}}^{N/d} \xi_{N/d}^{ic} = \sum_{\substack{i=1\\(i,N/d)=1}}^{N/d} \xi_{N/(N,dc)}^{i} = \frac{\varphi(N/d)}{\varphi(N/(N,dc))}\mu\left(\frac{N}{(N,dc)}\right),$$

since the last sum has $\varphi(N/d)$ summands which contain $\varphi(N/(N,dc))$-times all primitive $N/(N,dc)$-th roots of unity and their sum gives $\mu(N/(N,dc))$. ∎

Next, we calculate the a_c explicitly in the case $\mathcal{E}$ is a filter in $\mathcal{D}(N)$, which is essentially already done in Lemma 3.2.2.

Lemma 3.2.6. *Let $c \mid N$ and $\mathcal{E} = (e)$ be a filter for some $e \mid N$. Then*

$$a_c = \begin{cases} N/e, & c \in (N/e)_e = (N/e)\mathcal{D}(e), \\ 0, & \textit{else.} \end{cases}$$

Especially, for a $\mathcal{E}$ being a filter, we have $a_c \geq 0$ for all $c \in \mathcal{D}(N)$.

Proof. We calculate a_c for all $c \in \mathcal{D}(N)$:

$$\begin{aligned} a_c &= \sum_{d \in \mathcal{E}} \frac{\varphi(N/d)}{\varphi(N/(N,dc))} \mu\left(\frac{N}{(N,dc)}\right) \\ &= \sum_{d' \in \mathcal{D}(N/e)} \frac{\varphi(N'e/d'e)}{\varphi(N'e/(N'e,d'ec))} \mu\left(\frac{N'e}{(N'e,d'ec)}\right) \qquad (N' = N/e,\ d' = d/e) \\ &= \sum_{d' \in \mathcal{D}(N/e)} \frac{\varphi(N'/d')}{\varphi(N'/(N',d'c))} \mu\left(\frac{N'}{(N',d'c)}\right) \end{aligned}$$

Thus, we can assume $\mathcal{E} = \mathcal{D}(N)$ and omit the superscript $'$. Since φ and μ are multiplicative functions, we may assume $N = p^{N_p}$, $N_p > 0$, for a prime p and $d = p^{d_p}$, $c = p^{c_p}$ for $d, c \mid N$ and $0 \leq d_p, c_p \leq N_p$. Then

$$\begin{aligned} a_c &= \sum_{d \in \mathcal{D}(N)} \frac{\varphi(N/d)}{\varphi(N/(N,dc))} \mu\left(\frac{N}{(N,dc)}\right) \\ &= \sum_{d \in \mathcal{D}(N)} \frac{\varphi(p^{N_p - d_p})}{\varphi(p^{N_p - \min\{d_p + c_p, N_p\}})} \mu\left(p^{N_p - \min\{d_p + c_p, N_p\}}\right) \\ &= \sum_{i=0}^{N_p} \frac{\varphi(p^{N_p - i})}{\varphi(p^{N_p - \min\{i + c_p, N_p\}})} \mu\left(p^{N_p - \min\{i + c_p, N_p\}}\right) \end{aligned}$$

Since the μ-term equals 0 if $i + c_p < N_p - 1$, is equal to -1 if $i + c_p = N_p - 1$ and $+1$ otherwise, we get

$$\begin{aligned} a_c &= \sum_{i=0}^{N_p - 1} (p-1)p^{N_p - i - 1} + 1 \\ &= (p-1)p^{N_p - 1} \frac{p^{-N_p} - 1}{p^{-1} - 1} + 1 \\ &= p^{N_p} - 1 + 1 = p^{N_p} = N, \end{aligned}$$

for $c_p = N_p$, and

$$
\begin{aligned}
a_c &= \sum_{i=N_p-c_p-1}^{N_p-1} \frac{\varphi(p^{N_p-i})}{\varphi(p^{N_p-\min\{i+c_p,N_p\}})}\mu\left(p^{N_p-\min\{i+c_p,N_p\}}\right) + 1 \\
&= -\frac{(p-1)p^{N_p-(N_p-c_p-1)-1}}{(p-1)p^{N_p-(N_p-c_p-1+c_p)-1}} + \sum_{i=N_p-c_p}^{N_p-1} (p-1)p^{N_p-i-1} + 1 \\
&= -p^{c_p} + (p-1)p^{N_p-1}p^{-(N_p-c_p)} \sum_{i=0}^{c_p-1} p^{-i} + 1 \\
&= -p^{c_p} - (1-p^{c_p}) + 1 = 0,
\end{aligned}
$$

for $0 \leq c_p < N_p$. Thus, in the general case $\mathcal{E} = (e)$, we have $a_c = N' = N/e$ for $c = N/e$ and all multiples, hence the lemma is proven. ∎

We use this result to show that if $\mathcal{E}$ is a small modification of a filter, the main assumption $a_c \geq 0$ for all $c \in \mathcal{D}(N)$ usually fails to be true.

Lemma 3.2.7.

(a) Let $\mathcal{E} = (e) \neq \mathcal{D}(N)$ be a filter, but not (p) for $N = p^n$ a prime power. Then $\mathcal{E} \cup \{1\}$ gives $a_c < 0$ for some c. If $N = p^n$ for some prime number p, $n \in \mathbb{N}$, and $\mathcal{E} = (p)$ a filter, then $\mathcal{E} \cup \{1\}$ is a filter as well.

(b) Let $\mathcal{E} = (1) = \mathcal{D}(N)$ and N be not a prime power. Then $\mathcal{E} \setminus \{1\}$ gives $a_c < 0$ for some c. In the case $N = p^n$, the set $\mathcal{E} \setminus \{1\}$ is a also a filter, namely (p).

Proof. (a) Assume at first, that $N = \prod_{p|N} p^{N_p}$, $N_p \geq 1$ for all p, is not a prime power. If $p \nmid e$ for a prime divisor $p \mid N$, we have $N/e \nmid N/p$, and therefore $a_{N/p} = 0$ by Lemma 3.2.6. We calculate the value $\tilde{a}_{N/p}$ for $\tilde{\mathcal{E}} = \mathcal{E} \cup \{1\}$:

$$
\begin{aligned}
\tilde{a}_{N/p} &= \sum_{d \in \mathcal{E} \cup \{1\}} \frac{\varphi(N/d)}{\varphi(N/(N,d(N/p)))}\mu(N/(N,d(N/p))) \\
&= a_{N/p} + \frac{\varphi(N)}{\varphi(p)}\mu(p) = 0 + \frac{\varphi(N)}{p-1}(-1) < 0.
\end{aligned}
$$

Let $e = \prod_{p|N} p^{e_p}$ with primes p. If $e_p \geq 1$ for all p we have $N/e \leq N/(\prod_{p|N} p) = \prod_{p|N} p^{N_p-1}$. We calculate $\tilde{a}_{N/q}$ for $q = \min\{p \mid p \text{ prime divisor of } N\}$, i.e. $p > q \geq$

2 for all $q \neq p \mid N$, and $\tilde{\mathcal{E}} = \mathcal{E} \cup \{1\}$:

$$\begin{aligned}\tilde{a}_{N/q} &= a_{N/q} + \frac{\varphi(N)}{\varphi(q)}\mu(q)\\ &\leq \prod_{p|N} p^{N_p-1} - \frac{\prod_{p|N}(p-1)p^{N_p-1}}{q-1}\\ &= \prod_{p|N} p^{N_p-1}\left(1 - \prod_{p\neq q}(p-1)\right) < 0.\end{aligned}$$

Assume now, $N = p^n$ and $e = p^k$ for $1 < k \leq n$, thus $a_c = p^{n-k}$ for all $c = p^{n-k+l}$ for $0 \leq l \leq k$. We calculate $\tilde{a}_{p^{n-1}}$ for $\tilde{\mathcal{E}} = \mathcal{E} \cup \{1\}$:

$$\tilde{a}_{p^{n-1}} = a_{p^{n-1}} + \frac{\varphi(p^n)}{\varphi(p)}\mu(p) = p^{n-k} - p^{n-1} < 0.$$

If $N = p^n$ and $\mathcal{E} = (p)$, we have $\mathcal{E} \cup \{1\} = \mathcal{D}(N)$, hence it is a filter.

(b) If $\mathcal{E} = \mathcal{D}(N)$, it is $a_c = N$ for $c = N$ and 0 otherwise by Lemma 3.2.6. Since N is not a prime power, there exist distinct primes $p, q \mid N$. We calculate $\tilde{a}_c$ for $c = N/(pq)$ and $\mathcal{E} \setminus \{1\}$:

$$\begin{aligned}\tilde{a}_c &= a_c - \frac{\varphi(N)}{\varphi(N/(N, N/(pq)))}\mu(N/(N, N/(pq)))\\ &= 0 - \frac{\varphi(N)}{\varphi(pq)}\mu(pq) = -\frac{\varphi(N)}{(p-1)(q-1)} < 0.\end{aligned}$$

∎

The main part of the proof of Theorem 3.2.1 is the following claim, which we show by induction: Let $N \in \mathbb{N}$, $\mathcal{D}(N)$ the set of all divisors of N and $\mathcal{E} \subset \mathcal{D}(N)$. If

$$a_c = \sum_{d\in\mathcal{E}} \frac{\varphi(N/d)}{\varphi(N/(cd, N))}\mu(N/(cd, N)) \geq 0 \tag{3.2.1}$$

for all $c \in \mathcal{D}(N)$, then $\mathcal{E}$ is a filter in $\mathcal{D}(N)$ as is Definition 3.2.4.

Definition 3.2.8. Let $N \in \mathbb{N}$ and $\mathcal{E} \subset \mathcal{D}(N)$. For a prime factor $p \mid N$ we define a new set of divisors of N/p, namely

$$\mathcal{E}_p = \{d/p \mid d \in \mathcal{E},\ p \mid d\} \subset \mathcal{D}(N/p).$$

For $c \in \mathcal{D}(N/p)$ we denote by $a_c^{\{p\}}$ the corresponding sum over $\mathcal{E}_p$, i.e.

$$a_c^{\{p\}} = \sum_{(d/p)\in\mathcal{E}_p} \frac{\varphi\left(\frac{N/p}{d/p}\right)}{\varphi\left(\frac{N/p}{(N/p, cd/p)}\right)}\mu\left(\frac{N/p}{(N/p, cd/p)}\right).$$

We will in the following only consider $\mathcal{E}_p$ for all p, such that there exists an $d \in \mathcal{E}$ with $p|d$, so $\mathcal{E}_p$ is not empty.

We use this as induction step $N/p \mapsto N$. We first wish to prove that $a_c \geq 0$ for $\mathcal{E}$ implies $a_c^{\{p\}} \geq 0$ for $\mathcal{E}_p$ and all $c \in \mathcal{D}(N/p)$.

Lemma 3.2.9. *For any $p|N$ with $\mathcal{E}_p$ we get for all $c \in \mathcal{D}(N/p)$:*

$$a_c^{\{p\}} = \begin{cases} a_c, & \text{if } pc \mid N/p, \\ \frac{1}{p}((p-1)a_c + a_{pc}) & \text{if } pc \nmid N/p. \end{cases}$$

In particular, $a_c \geq 0$ for all $c \in \mathcal{D}(N)$ implies $a_c^{\{p\}} \geq 0$ for all $c \in \mathcal{D}(N/p)$.

Proof. For $\mathcal{E}$ and $p \in \mathcal{D}(N)$ such that p divides at least one $d \in \mathcal{E}$, i.e. the set $\mathcal{E}_p$ is non-empty. We calculate the value of $a_c^{\{p\}}$ for all $c \in \mathcal{D}(N/p)$:

$$\begin{aligned} a_c^{\{p\}} &= \sum_{(d/p)\in\mathcal{E}_p} \frac{\varphi\left(\frac{N/p}{d/p}\right)}{\varphi\left(\frac{N/p}{(N/p,cd/p)}\right)} \mu\left(\frac{N/p}{(N/p,cd/p)}\right) \\ &= \sum_{\substack{d\in\mathcal{E} \\ p|d}} \frac{\varphi\left(\frac{N}{d}\right)}{\varphi\left(\frac{N}{(N,cd)}\right)} \mu\left(\frac{N}{(N,cd)}\right) \\ &= a_c - \underbrace{\sum_{\substack{d\in\mathcal{E} \\ p\nmid d}} \frac{\varphi\left(\frac{N}{d}\right)}{\varphi\left(\frac{N}{(N,cd)}\right)} \mu\left(\frac{N}{(N,cd)}\right)}_{=:a_c^{\{p'\}}}. \end{aligned}$$

For $n \in \mathbb{N}$ and prime number p let $\nu_p(n) \geq 0$ the maximal p-part of n, i.e. $p^{\nu_p(n)} \mid n$ and $p^{\nu_p(n)+1} \nmid n$. Let $k = \nu_p(N)$. If $\nu_p(c) \leq k-2$, i.e. in particular it is $k \geq 2$, then $\nu_p(N/(cd,N)) \geq 2$ for $d \in \mathcal{E}$, $p \nmid d$. Thus, we have $\mu(N/(cd,N)) = 0$ and $a_c^{\{p\}} = a_c$ in the case $pc \mid (N/p)$. For $\nu_p(c) = k-1$ we have

$$\begin{aligned} a_c^{\{p'\}} &= \sum_{\substack{d\in\mathcal{E} \\ p\nmid d}} \frac{\varphi\left(\frac{N}{d}\right)}{\varphi\left(\frac{N}{(N,cd)}\right)} \mu\left(\frac{N}{(N,cd)}\right) \\ &= \sum_{\substack{d\in\mathcal{E} \\ p\nmid d}} \frac{\varphi(p^k)\varphi\left(\frac{N/p^k}{d}\right)}{\varphi(p)\varphi\left(\frac{N/p^k}{(N/p^k,dc/p^{k-1})}\right)} \underbrace{\mu(p)}_{=-1} \mu\left(\frac{N/p^k}{(N/p^k,dc/p^{k-1})}\right) \\ &= -p^{k-1} \underbrace{\sum_{\substack{d\in\mathcal{E} \\ p\nmid d}} \frac{\varphi\left(\frac{N/p^k}{d}\right)}{\varphi\left(\frac{N/p^k}{(N/p^k,dc/p^{k-1})}\right)} \mu\left(\frac{N/p^k}{(N/p^k,dc/p^{k-1})}\right)}_{=:X(c)}. \end{aligned}$$

Assume now $\nu_p(c) = \nu_p(N) = k$. We write $N' = N/p^k$ and $c' = c/p^k$, then we get

$$\begin{aligned}
a_c &= \sum_{d\in\mathcal{E}} \frac{\varphi\left(\frac{N'p^k}{d}\right)}{\varphi\left(\frac{N'p^k}{(N'p^k, c'p^k d)}\right)} \mu\left(\frac{N'p^k}{(N'p^k, c'p^k d)}\right) \\
&= \sum_{\substack{d\in\mathcal{E}\\ p\nmid d}} \frac{\varphi(p^k)\varphi\left(\frac{N'}{d}\right)}{\varphi\left(\frac{N'}{(N',c'd)}\right)} \mu\left(\frac{N'}{(N',c'd)}\right) + \underbrace{\sum_{\substack{d\in\mathcal{E}\\ p\mid d}} \frac{\varphi\left(\frac{N}{d}\right)}{\varphi\left(\frac{N}{(N,cd)}\right)} \mu\left(\frac{N}{(N,cd)}\right)}_{=a^{\{p\}}_{(c'p^{k-1})}} \\
&= (p-1)p^{k-1}X(c) + a^{\{p\}}_{(c'p^{k-1})}.
\end{aligned}$$

We combine the two expressions for a_c, $c = c'p^k$. Then, $c/p = c'p^{k-1} \mid N/p$ and $X(c'p^{k-1}) = X(c'p^k) = X(c)$. Since $xa_{(c'p^{k-1})} + ya_{(c'p^k)} \geq 0$ for $x, y \geq 0$ we get from

$$\begin{aligned}
xa_{(c'p^{k-1})} + ya_{(c'p^k)} &= x\left(a^{\{p\}}_{(c'p^{k-1})} - p^{k-1}X(c)\right) + y\left((p-1)p^{k-1}X(c) + a^{\{p\}}_{(c'p^{k-1})}\right) \\
&= pa^{\{p\}}_{(c'p^{k-1})}, \qquad (x = p-1,\ y = 1)
\end{aligned}$$

and this proves the lemma. ∎

We now conclude by induction that $\mathcal{E}$ is a filter if all possible reductions $\mathcal{E}_p$, $p \mid N$, are filters. Under this assumption, it follows that no $\mathcal{E}_p$ is empty: Let $p \mid N$ such that $p \mid d$ for some $d \in \mathcal{E}$, then $\mathcal{E}_p$ is not empty, hence equals (e_p) for some e_p. Since $\mathcal{E}_p$ is a filter, we have $N/p \in \mathcal{E}_p$, and hence $N = p \cdot N/p \in \mathcal{E}$. As induction step, we use the following lemma.

Lemma 3.2.10. *Let $\mathcal{E} \subset \mathcal{D}(N)$ and for all $p \mid N$ the set $\mathcal{E}_p$, defined as in Definition 3.2.8, a filter, namely $(e_p) = (e_p)_{N/p}$ for some $e_p \mid N/p$. Then either there exist a prime $p \mid N$ with $p \mid e_q$ for all $q \neq p$ or it is $e_p = 1$ for all p.*
In the first case we have $\mathcal{E} = (pe_p)$ or $\mathcal{E} = (pe_p) \cup \{1\}$. In the second case we have $\mathcal{E} = (1) = \mathcal{D}(N)$ or $\mathcal{E} = (1) \setminus \{1\}$.

Proof. Assume, there exist q' with $e_{q'} \neq 1$ and $p \mid e_{q'}$. Then $p \mid e_q$ for all $q \neq p$. We prove this by contradiction, thus assume $p \nmid e_q$ for some q. It is $q'e_q \in \mathcal{E}_q$ (since $\mathcal{E}_q$ is a filter) and hence $qq'e_q \in \mathcal{E}$ (by definition of $\mathcal{E}_q$). Then $qe_q \in \mathcal{E}_{q'}$ and $e_{q'} \mid qe_q$, hence a contradiction to $p \nmid e_q$. This proves the first part of the lemma.

We now prove the consequences in the two cases. Firstly, we assume it exists p with $p \mid e_q$ for all $q \neq p$. Let $x \in (pe_p)$, then $e_p \mid x/p$, and since $\mathcal{E}_p$ is a filter, $x/p \in \mathcal{E}_p$. Thus we have $x = p \cdot x/p \in \mathcal{E}$, i.e. $(pe_p) \subset \mathcal{E}$. Let now $x \in \mathcal{E}$. If $p \mid x$ we have $x/p \in \mathcal{E}_p$, hence $e_p \mid x/p$ and therefore $pe_p \mid x$. If $p \nmid x$, then $x = 1$ or it exists q with $q \mid x$. In this case is $x/q \in \mathcal{E}_q$ and $e_q \mid x/q$, which is a contradiction to $p \nmid x$. This proves $(pe_p) = \mathcal{E} \setminus \{1\}$ (which may be equal to $\mathcal{E}$).
In the case $e_p = 1$ for all p, we have $(p) \subset \mathcal{E}$ for all p. Since it is $\bigcup_{p\in\mathcal{D}(N)}(p) = \mathcal{D}(N) \setminus \{1\}$, this proves the assertion. ∎

We can now conclude the proof of the claim of (3.2.1). Let $\mathcal{E}$ such that

$$a_c = \sum_{d\in\mathcal{E}} \frac{\varphi(N/d)}{\varphi(N/(cd,N))}\mu(N/(cd,N)) \geq 0$$

for all $c \in \mathcal{D}(N)$, then $a_c^{\{p\}} \geq 0$ for all $\mathcal{E}_p$ and $c \in \mathcal{D}(N/p)$ by Lemma 3.2.9. By induction, all $\mathcal{E}_p$ are filters, namely (e_p) for some $e_p \mid N/p$. Then, by Lemma 3.2.10, we have that $\mathcal{E}$ is a filter (e) for some $e \mid N$ or $(e) \cup \{1\}$ for some $e \neq 1$ or $(1) \setminus \{1\}$. By Lemma 3.2.7, the last cases are only possible for $N = p^n$ and $e = p$. In this cases $\mathcal{E}$ is a filter as well. This proves the claim (3.2.1) and hence concludes the proof of Theorem 3.2.1.

3.3. An alternative proof

We now give a direct proof of Theorem 3.2.1, which was pointed out to us by Mihalis Kolountzakis.

Proof of Theorem 3.2.1 [Kol14]. Write $U = \{\exp(2\pi i r/N) \mid r \in E\}$, where $E \subset \mathbb{Z}_N$ the set of exponents of U. The assumption, that all power sums $\sum_{\zeta\in U}\zeta^k$ are non-negative, means exactly that the Fourier transform (on the group $\mathbb{Z}_N$) of the indicator function on E is non-negative:

$$\widehat{\mathbf{1}_E}(k) = \sum_{j\in\mathbb{Z}_N} \mathbf{1}_E(j)\exp(-2\pi i jk/N) \geq 0, \quad \forall\, k \in \mathbb{Z}_N.$$

Write $\widehat{f}(k)$, $k \in \mathbb{Z}_N$, for the non-negative square root of $\widehat{\mathbf{1}_E}(k)$. Hence, $\widehat{f}(k) \in \mathbb{R}_{\geq 0}$ for all k. From the equation $\widehat{\mathbf{1}_E}(k) = \widehat{f}^2(k)$ we derive the convolution identity

$$\mathbf{1}_E(n) = f * f\,(n) = \sum_{j\in\mathbb{Z}_N} f(j)f(n-j) = \sum_{j\in\mathbb{Z}_N} f(j)\overline{f(j-n)}, \tag{3.3.1}$$

where the last identity is due to the fact that $f(x) = \overline{f(-x)}$, which is true as $\widehat{f}$ is real.

By the Cauchy-Schwarz inequality we then have for every $n \in E$ (by assumption, it is $U \neq \emptyset$, and hence $E \neq \emptyset$)

$$1 = \mathbf{1}_E(n) \leq \sum_{j\in\mathbb{Z}_n} \mid f(j) \mid^2 \overset{\dagger}{=} \mathbf{1}_E(0) \overset{\ddagger}{=} 1$$

where the equation (†) is equation (3.3.1) evaluated for $n = 0$, and the equation (‡) follows since $\mathbf{1}_E(0) \leq 1$. Assume now $0 \neq r \in E$. Then

$$1 = \mathbf{1}_E(r) = \sum_{j\in\mathbb{Z}_N} f(j)\overline{f(j-r)},$$

and by the equality case of the Cauchy-Schwarz inequality we conclude that there is a constant c_r with $|c_r| = 1$ such that $f(j) = c_r f(j-r)$ holds for all j, and thus

$$\begin{aligned}\widehat{f}(k) &= \sum_{j\in\mathbb{Z}_N} f(j)\exp(-2\pi ijk/N)\\ &= c_r \sum_{j\in\mathbb{Z}_N} f(j-r)\exp(-2\pi i(j-r)k/N)\exp(-2\pi irk/N)\\ &= c_r \exp(-2\pi irk/N)\widehat{f}(k-r).\end{aligned}$$

Since $\widehat{f}(k)$ is real for all k, it is $\widehat{f}(k) = 0$ except when $c_r = \exp(\pm 2\pi irk/N)$, thus $\widehat{f}$ is periodic with periods all elements $r \in E$, and so is f. Since $\mathbf{1}_E(n) = \sum_{i\in\mathbb{Z}_N} f(j)f(n-j)$, the same is true for $\mathbf{1}_E$, i.e.,

$$\mathbf{1}_E(n-r) = \mathbf{1}_E(n), \quad \forall\, n \in \mathbb{Z}_N, r \in E.$$

In other words: if $n, r \in E$, then $n - r \in E$, i.e. E is an additive group, hence U is a multiplicative group of roots of unity.

The other implication is shown in Lemma 3.2.2. ∎

3.4. Fourier pairs of $\{0, 1\}$-matrices

In the following, we will consider certain idempotents of the group algebra $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$. Recall that an idempotent of a group algebra $\mathbb{C}[G]$ is an element $e \in \mathbb{C}[G]$ with $e^2 = e$. Let g be a generator of $\mathbb{Z}_N$ and $\{g^i \otimes g^j \mid 0 \le i, j < N\}$ a basis of $\mathbb{C}[\mathbb{Z}_N, \mathbb{Z}_N]$. For an idempotent of $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ we write

$$e^{(\varepsilon)} = (1/N)\sum_{i,j} \varepsilon_{ij} g^i \otimes g^j \tag{3.4.1}$$

with matrix $\varepsilon = (\varepsilon_{ij})_{1\le i,j\le N}$. Then the condition $(e^{(\varepsilon)})^2 = e^{(\varepsilon)}$ gives

$$\frac{1}{N^2}\sum_{i',i''}\sum_{j',j''} \varepsilon_{i'j'}\varepsilon_{i''j''}(g^{i'} \otimes g^{j'})(g^{i''} \otimes g^{j''}) = \frac{1}{N}\sum_{i,j} \varepsilon_{ij} g^i \otimes g^j,$$

and by comparing coefficients, we get

$$\frac{1}{N^2}\sum_{i'+i''=i}\sum_{j'+j''=j} \varepsilon_{i'j'}\varepsilon_{i''j''} = \frac{1}{N}\varepsilon_{ij}. \tag{3.4.2}$$

We will be more specifically interested in idempotents such that $\varepsilon_{ij} \in \{0, 1\}$ for all i, j. Let $\xi = \xi_N$ be a primitive N-th root of unity and $\{e_k = 1/N \sum_{r=0}^{N} \xi^{kr} g^r \mid 0 \le k < N\}$ be the set of mutually orthogonal primitive idempotents of the group algebra $\mathbb{C}[\mathbb{Z}_N]$. Then $\{e_k \otimes e_l\}$ is the set of primitive orthogonal idempotents of $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ and we can express $e^{(\varepsilon)}$ as sum of these primitive idempotents: $e^{(\varepsilon)} = \sum_{k,l} \bar{\varepsilon}_{kl} e_k \otimes e_l$ with $\bar{\varepsilon}_{kl} \in \{0,1\}$ for all $0 \le k,l < N$. Comparing the coefficients for these two expressions of $e^{(\varepsilon)}$ leads to

$$\varepsilon_{ij} = \frac{1}{N} \sum_{k,l} \bar{\varepsilon}_{kl} \xi^{ik+jl}, \tag{3.4.3}$$

which means that the matrix ε is the discrete Fourier transform of the matrix $\bar{\varepsilon} = (\bar{\varepsilon}_{ij})_{0 \le i,j < N}$ (over the group $\mathbb{Z}_N \times \mathbb{Z}_N$). We fix two new notions in the following definition.

Definition 3.4.1. Let $N \in \mathbb{N}$ and $\xi = \xi_N$ a primitive N-th root of unity.

(1) Two matrices $A = (a_{ij})_{1 \le i,j \le N}$ and $B = (b_{ij})_{1 \le i,j \le N}$ with $a_{ij}, b_{ji} \in \mathbb{C}$ for all i,j are called a *Fourier pair (of matrices) over the group* $\mathbb{Z}_N \times \mathbb{Z}_N$, if

$$a_{ij} = \frac{1}{N} \sum_{k,l} b_{kl} \xi^{ik+jl} \quad \text{or} \quad b_{ij} = \frac{1}{N} \sum_{k,l} a_{kl} \xi^{ik+jl}.$$

(2) A matrix $\varepsilon = (\varepsilon_{ij})_{1 \le i,j \le N}$ is called $\{0,1\}$-*matrix*, if $\varepsilon_{ij} \in \{0,1\}$ for all i,j.

The considerations above lead to the following problem.

Problem 3.4.2. *We wish to determine all idempotents $e^{(\varepsilon)}$ of $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$, such that ε is $\{0,1\}$-matrix, or equivalent, all Fourier pairs of $\{0,1\}$-matrices ε and $\bar{\varepsilon}$.*

Example 3.4.3. We consider some examples of Fourier transformed matrices, where ε is not necessarily a $\{0,1\}$-matrix.

(i) Let $\bar{\varepsilon}$ the matrix with $\bar{\varepsilon}_{00} = 1$ and $\bar{\varepsilon}_{kl} = 0$ otherwise. Then $\varepsilon_{ij} = 1/N$ for all i,j.

(ii) Let $\bar{\varepsilon}$ the matrix with $\bar{\varepsilon}_{0l} = 1$ for all l and $\bar{\varepsilon}_{kl} = 0$ otherwise. Then $\varepsilon_{i0} = 1$ for all i and $\varepsilon_{ij} = 0$ otherwise.

(iii) Let $\bar{\varepsilon}$ the matrix with $\bar{\varepsilon}_{kk} = 1$ for all k and $\bar{\varepsilon}_{kl} = 0$ otherwise. Then $\varepsilon_{ij} = 1$ for all i,j with $i + j \equiv 0 \mod N$ and $\varepsilon_{ij} = 0$ otherwise. We give the matrices explicitly for $N = 4$:

$$\bar{\varepsilon} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \longrightarrow \quad \varepsilon = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The following theorem completely solves Problem 3.4.2, relying heavily on our main Theorem 3.2.1 about roots of unity:

Theorem 3.4.4. *All idempotents $e^{(\varepsilon)}$ of the group algebra $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ with $\varepsilon_{ij} \in \{0,1\}$, or equivalently all discrete Fourier pairs $\varepsilon, \bar{\varepsilon}$ of $\{0,1\}$-matrices are either of the form*

$$\varepsilon_{ij} = \delta_{(\frac{N}{d}|i)} \delta_{(d|j - t\frac{i}{N/d})}, \quad 0 \le i,j < N, \tag{3.4.4}$$

for a unique $d \mid N$ and $0 \le t \le d-1$ or they are trivial, i.e. $\varepsilon = \bar{\varepsilon} = 0$.

Before we proceed to the proof of the theorem, we give another Example.

Example 3.4.5. Let $N = 12$, $d = 4$ and $t = 2$, then ε as in (3.4.4) is given by

$$\begin{array}{cc}
 & \begin{array}{cccccccccccc} 0 & & t & & d & & & & & & & \end{array} \\
\begin{array}{c} 0 \\ \\ \\ N/d \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} & \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & . & . & . & . & . & .
\end{pmatrix}
\end{array}.$$

Proof. By the Fourier transformation (3.4.3), we have $\varepsilon_{00} = \frac{1}{N}\sum_{k,l}\bar{\varepsilon}_{kl}$. Since ε and $\bar{\varepsilon}$ are $\{0,1\}$-matrices, this gives either $\bar{\varepsilon}_{kl} = 0$ for all k, l or $\sum_{k,l}\bar{\varepsilon}_{kl} = N$. In the first case we have $\varepsilon = 0$ as well. Applying the same argument to the dual Fourier transformation,

$$\bar{\varepsilon}_{kl} = \frac{1}{N}\sum_{i,j}\varepsilon_{ij}\xi^{-(ik+jl)}, \tag{3.4.5}$$

we get $\sum_{i,j}\varepsilon_{ij} = N$ in the second case.

Assume in the following $\varepsilon \neq 0$. We now calculate the row-, resp. column-sums of the matrices ε and $\bar{\varepsilon}$. Let a_k the k-th row-sum of ε and a'_l the l-th column-sum of ε, and $\bar{a}_k$, $\bar{a}'_l$ the according sums of $\bar{\varepsilon}$. Then

$$a_k = \sum_l \varepsilon_{kl} = \frac{1}{N}\sum_{l,i,j}\bar{\varepsilon}_{ij}\xi^{ik+jl} = \frac{1}{N}\sum_i \xi^{ik}\sum_j \bar{\varepsilon}_{ij}\underbrace{\sum_l \xi^{jl}}_{=N\delta_{(j=0)}} = \sum_i \xi^{ik}\bar{\varepsilon}_{i0}.$$

Since the row-sum a_k is a non-negative integer for all k, we get by Theorem 3.2.1, that the set $\{i \mid \bar{\varepsilon}_{i0} = 1\}$ is a subgroup of $\mathbb{Z}_N$, thus it exist $d \mid N$ with $\bar{\varepsilon}_{i0} = \delta_{(d|i)}$. Analogously, we get by calculating the column-sum a'_l that $d' \mid N$ exist, such that $\bar{\varepsilon}_{0j} = \delta_{(d'|j)}$. As a consequence, we get $a_k = N/d$ for k being an N/d-multiple and $a'_l = N/d'$ for l being an N/d'-multiple, and the other row-, resp. column-sums being 0. We now calculate the row- and column-sums of $\bar{\varepsilon}$ using the dual transformation (3.4.5). This gives, again by application of Theorem 3.2.1, that there exist $\bar{d}, \bar{d}' \mid N$ such that $\varepsilon_{i0} = \delta_{(\bar{d}|i)}$ and $\varepsilon_{0j} = \delta_{(\bar{d}'|j)}$, and $\bar{a}_k = N/\bar{d}$ for k being $N/\bar{d}$-multiple and $\bar{a}'_l = N/\bar{d}'$ for l being $N/\bar{d}'$-multiple. Since $N/d = a_0 = \sum_j \varepsilon_{0j} = N/\bar{d}'$, we get $d = \bar{d}'$. Analogously, we get $\bar{d} = d'$. Since only the N/d-th rows have entries 1 and $\varepsilon_{i0} = \delta_{(\bar{d}|i)}$, we get $N/d \mid \bar{d} = d'$, hence $N \mid dd'$.

The case $N = dd'$, i.e. $d' = N/d$ corresponds to the non-shifted solution of (3.4.2), since in this case there are maximal $N/d \cdot N/d' = N$ entries 1.

We consider now a solution with $N < dd'$ and show, that a suitably shifted version of this is also a solution of (3.4.2) with smaller dd'. The claim then follows by induction over dd'. For a solution ε of (3.4.2) the shifted matrix, defined by

$$\varepsilon_{ij}^{[t]} := \begin{cases} \varepsilon_{i,j-t\frac{i}{N/d}}, & N/d \mid i, \\ \varepsilon_{i,j} = 0, & \text{otherwise.} \end{cases}$$

for some $0 \leq t \leq d-1$, is also a solution of (3.4.2). This follows easily by inserting $\varepsilon_{ij}^{[t]}$ in (3.4.2), since the shift gives only a new ordering of the summands. Let now ε be a solution with $N < dd'$. We now want to shift this ε in a way, that no 1 entries in the first column are moved, i.e. the d'-th rows are shifted by multiple of d, and some of the other rows are shifted, such that $\varepsilon^{[t]}$ has at least one 1-entry more in the first column:

Consider the N/d-row. By hypothesis, $N/d < d'$, hence $\varepsilon_{N/d,0} = 0$, but $\varepsilon_{N/d,t} = 1$ for some t, since the row sum $a_{N/d} = N/d > 0$. Since the column sum $a'_t \neq 0$, we have $N/d' \mid t$, hence $d \mid tdd'/N$. Thus the shifted solution $\varepsilon_{ij}^{[-t]}$ has in the 0-column still $\varepsilon_{i0} = 1$ for $d' \mid i$ and it has now additionally $\varepsilon_{N/d,0} = 1$. The expression dd' for $\varepsilon^{[t]}$ has to be strictly smaller than dd' for ε, this reduces the claim by induction to the unshifted case $dd' = N$, which has been solved above. ∎

3.5. Solutions of the group-equations

The following system of equations for an abelian group G arises as a necessary condition on the element $R_0 \in \mathbb{C}[\Lambda/\Lambda'] \otimes \mathbb{C}[\Lambda/\Lambda']$ in Lusztig's ansatz for R-matrices for a quantum group $u_q(\mathfrak{g}, \Lambda, \Lambda')$, cf. Theorem 2.1.6 and Lemma 2.2.1. In this application, the abelian group G is the fundamental group of $\mathfrak{g}$, and hence cyclic except for $\mathfrak{g} = D_{2n}$, see Remark 3.5.4.

Definition 3.5.1. For an abelian group G we define a set of $2|G|^2 + 2$ quadratic equations in $|G|^2$ complex variables $g(x, y)$ indexed by $x, y \in G$:

$$g(x, y) = \sum_{y_1 + y_2 = y} g(x, y_1) g(x, y_2), \tag{3.5.1}$$

$$g(x, y) = \sum_{x_1 + x_2 = x} g(x_1, y) g(x_2, y), \tag{3.5.2}$$

$$1 = \sum_{y \in G} g(0, y), \tag{3.5.3}$$

$$1 = \sum_{x \in G} g(x, 0). \tag{3.5.4}$$

We call these equations *group-equations of G*.

As a side remark, note that these equations are a subset of the equations for a Hopf pairing $g : \mathbb{C}^G \otimes \mathbb{C}^G \to \mathbb{C}$, which are given by

$$\begin{aligned} \delta_{x,x'} g(x,y) &= \sum_{y_1+y_2=y} g(x,y_1)g(x',y_2), \\ \delta_{y,y'} g(x,y) &= \sum_{x_1+x_2=x} g(x_1,y)g(x_2,y'), \\ \delta_{x,0} &= \sum_{y\in G} g(x,y), \\ \delta_{y,0} &= \sum_{x\in G} g(x,y), \end{aligned}$$

where we write by slight abuse of notation x for the element in $\mathbb{C}^G$ which takes the value 1 on the group element $x \in G$ and 0 otherwise. (In $\mathbb{C}^G$ the coproduct structure is given as follows: For $y \in \mathbb{C}^G$ we have $y_{(1)} \otimes y_{(2)} = \sum_{y_1+y_2=y} y_1 \otimes y_2$.) The result of this section is in some sense, that g as in Definition 3.5.1 is still a pairing on a pair of subgroups.

Lemma 3.5.2. *Let G be an abelian group and H_1, H_2 subgroups with equal cardinality $|H_1| = |H_2| = d$ (not necessarily isomorphic!). Let $\omega\colon H_1 \times H_2 \to \mathbb{C}^\times$ be a pairing of groups. (By* group pairing *we denote a bihomomorphism $U \times V \to \mathbb{C}^\times$ of groups U, V.) Here, the group G is written additively and $\mathbb{C}^\times$ multiplicatively, thus we have $\omega(x,y)^d = 1$ for all $x \in H_1, y \in H_2$. Then the assignment*

$$g\colon G \times G \to \mathbb{C},\ (x,y) \mapsto \frac{1}{d}\omega(x,y)\delta_{(x\in H_1)}\delta_{(y\in H_2)} \tag{3.5.5}$$

is a solution of the equations (3.5.1)-(3.5.4) for G.

Proof. The claim follows by straightforward calculations. For $x, y, y_1, y_2 \in G$ we get

$$\begin{aligned} \sum_{y_1+y_2=y} g(x,y_1)g(x,y_2) &= \left(\frac{1}{d}\right)^2 \sum_{y_1+y_2=y} \omega(x,y_1)\omega(x,y_2)\delta_{(x\in H_1)}\delta_{(y_1\in H_2)}\delta_{(y_2\in H_2)} \\ &= \left(\frac{1}{d}\right)^2 \sum_{y_1+y_2=y} \omega(x,y_1+y_2)\delta_{(x\in H_1)}\delta_{(y_1\in H_2)}\delta_{(y_2\in H_2)} \\ &= \left(\frac{1}{d}\right)^2 |H_2|\,\omega(x,y)\delta_{(x\in H_1)}\delta_{(y\in H_2)} = g(x,y). \\ \sum_{y\in G} g(0,y) = \frac{1}{d}\sum_{y\in G}\omega(0,y)\delta_{(y\in H_2)} &= \frac{1}{d}\sum_{y\in H_2} 1 = 1. \end{aligned}$$

And analogously for equations (3.5.2) and (3.5.4). ∎

Question 3.5.3. *Are these all solutions of the equations (3.5.1)-(3.5.4)?*

As an application of Theorems 3.2.1 and 3.4.4 we will below positively answer this question for a **cyclic group** G.

Remark 3.5.4. *For the application in the quantum group framework of Chapter 2, i.e. for quantum groups $u_q(\mathfrak{g}, \Lambda, \Lambda')$ with a finite-dimensional, simple complex Lie algebra $\mathfrak{g}$, the only non-cyclic case of interest is $\mathbb{Z}_2 \times \mathbb{Z}_2$ (the fundamental group of the Lie algebra $\mathfrak{g} = D_{2n}$). Most other simple Lie algebras have $G = \mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$.*

It is quite remarkable that the only highly nontrivial case solved here is hence the Lie algebra A_n with $G = \mathbb{Z}_{n+1}$, which depends highly on the prime divisors of $n+1$. This is due to the unusually large center $\mathbb{Z}_{n+1}$ *of the algebraic group SL_{n+1}, which makes it notoriously hard to deal with (e.g. in Deligne-Lusztig theory). We hope that the technical tools developed here might be useful in addressing such issues.*

Example 3.5.5. Let $G = \mathbb{Z}_N$ and consider for any divisor $d|N$ the unique subgroup $H = \frac{N}{d}\mathbb{Z}_N \cong \mathbb{Z}_d$ of G of order d. By Lemma 3.5.2 we have for any pairing $\omega\colon H \times H \to \mathbb{C}^\times$ the function g as in (3.5.5) as a solution of the equations (3.5.1)-(3.5.4).
We give the solution explicitly: For $H = \langle h \rangle$, $h \in \frac{N}{d}\mathbb{Z}_N$, we define a pairing $\omega\colon H \times H \to \mathbb{C}^\times$ by $\omega(h,h) = \xi$ with ξ a d-th root of unity, not necessarily primitive.
Thus the general solution ansatz in Lemma 3.5.2 translates for cyclic groups G to

$$g\colon \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C},\ (x,y) \mapsto \frac{1}{d}\,\xi^{\frac{xy}{(N/d)^2}}\,\delta_{(\frac{N}{d}|x)}\delta_{(\frac{N}{d}|y)}. \tag{3.5.6}$$

Theorem 3.5.6. *For $G = \mathbb{Z}_N$ the solutions given in Lemma 3.5.2 (and worked out in this case in Example 3.5.5), are in fact all solutions to the system of equations (3.5.1)-(3.5.4).*

Proof. The proof is an application of Theorem 3.4.4, which follows from the main Theorem 3.2.1. Let $g : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C}$ be a solution of the equations (3.5.1)-(3.5.4). We write shortly g_{ij} for $g(i,j)$, $0 \le i,j \le N-1$. Let $\mathbb{Z}_N = \langle x \rangle$, then

$$\sum_{j',j''} (g_{ij'}x^{j'})(g_{ij''}x^{j''}) = \sum_j g_{ij}x^i$$

for all i by (3.5.1), hence $\sum_j g_{ij}x^i$ is an idempotent in $\mathbb{C}[\mathbb{Z}_N]$. Let $\xi = \xi_N$ be a primitive N-th root of unity, then primitive orthogonal idempotents of $\mathbb{C}[\mathbb{Z}_N]$ are all of the form $e_k = \frac{1}{N}\sum_{r=0}^{N-1} \xi^{kr}x^r$ and a general idempotent is a linear combination $e = \sum_k a_k e_k$ with $a_k \in \{0,1\}$ (follows from $e^2 = e$ and $\mathrm{char}(\mathbb{C}) = 0$). Thus, we have $\sum_j g_{ij}x^i = \sum_k \varepsilon_{ik} e_k$ for all i and with $\varepsilon_{ik} \in \{0,1\}$, and therefore

$$g_{ij} = \frac{1}{N}\sum_{k=1}^{N-1} \varepsilon_{ik}\xi^{kj} \tag{3.5.7}$$

for $\{0,1\}$-matrix $\varepsilon = (\varepsilon_{ik})$. By inserting this in (3.5.2), $\sum_{i'+i''=i} g_{i'j}g_{i''j} = g_{ij}$, we get

$$\frac{1}{N^2}\sum_{i'+i''=i}\sum_{k',k''} \varepsilon_{i'k'}\varepsilon_{i''k''}\xi^{(k'+k'')j} = \frac{1}{N}\sum_k \varepsilon_{ik}\xi^{kj}.$$

By comparing the coefficients on both sides we get

$$\frac{1}{N^2}\sum_{i'+i''=i}\sum_{k'+k''=k}\varepsilon_{i'k'}\varepsilon_{i''k''}=\frac{1}{N}\varepsilon_{ik}, \tag{3.5.8}$$

which is equation (3.4.2). Thus, for a generator g of $\mathbb{Z}_N$ the element $e^{(\varepsilon)}=\sum_{i,j}\varepsilon_{ij}g^i\otimes g^j$, defined as in (3.4.1), is an idempotent in $\mathbb{C}[\mathbb{Z}_N\times\mathbb{Z}_N]$ and ε is $\{0,1\}$-matrix and we can apply Theorem 3.4.4. We have

$$\varepsilon_{ij}=\delta_{(\frac{N}{d}|i)}\delta_{(d|j-t\frac{i}{N/d})},$$

for some $d\mid N$ and $0\le t\le d-1$. We insert in (3.5.7):

$$\begin{aligned} g_{ij} &= \frac{1}{N}\sum_{k=0}^{N-1}\delta_{(\frac{N}{d}|i)}\delta_{(d|k-t\frac{i}{N/d})}\xi^{jk} \\ &= \frac{1}{N}\delta_{(\frac{N}{d}|i)}\sum_{k'=0}^{N/d-1}\xi^{j(t\frac{i}{N/d}+dk')} && (k=t\tfrac{i}{N/d}+dk',\ k'=0,\dots,\tfrac{N}{d}-1) \\ &= \frac{1}{d}\left(\xi^{N/d}\right)^{t\frac{i}{N/d}\frac{j}{N/d}}\delta_{(\frac{N}{d}|i)}\underbrace{\frac{1}{N/d}\sum_{k'=0}^{N/d-1}(\xi^d)^{jk'}}_{=\delta_{\frac{N}{d}|j}} \end{aligned}$$

Thus, g is the solution given already in Example 3.5.5, which was the explicitly worked out case of Lemma 3.5.2 for G cyclic. ∎

In the following example, we give all solutions of the group-equations in the case $G=\mathbb{Z}_2\times\mathbb{Z}_2$. It is easy to see, that these maps are solutions of (3.5.1)-(3.5.4). An calculation via Maple shows that these all solutions in this case, see Appendix A.

Example 3.5.7. Let $G=\mathbb{Z}_2\times\mathbb{Z}_2=\langle a,b\rangle$ and $c=a+b$ the third element of order 2 in $\mathbb{Z}_2\times\mathbb{Z}_2$. For $H_1=H_2=G$ there are $2^4=16$ possible parings, since a pairing is given by determining the values of $\omega(x,y)=\pm1$ for $x,y\in\{a,b\}$. In G, there are 3 different subgroups of order 2, hence there are 9 possible pairs (H_1,H_2) of groups H_i of order 2. For each pair, there are two possible choices for $\omega(x,y)=\pm1$, x,y being the generators of H_1, resp. H_2. Thus, we get 18 pairings for subgroups of order $d=2$. For $H_1=H_2=\{0\}$ there is only one pairing, mapping $(0,0)$ to 1. Thus, we have 35 pairings in total.

#	$H_i\cong$	H_1	H_2	ω
16	$\mathbb{Z}_2\times\mathbb{Z}_2$	$\langle a,b\rangle$	$\langle a,b\rangle$	$\omega(x,y)=\pm1$ for $x,y\in\{a,b\}$
9×2	$\mathbb{Z}_2$	$\langle x\rangle$, $x\in\{a,b,c\}$	$\langle y\rangle$, $y\in\{a,b,c\}$	$\omega(x,y)=\pm1$
1	$\mathbb{Z}_1$	$\{0\}$	$\{0\}$	$\omega(0,0)=1$

Chapter 4

Solutions of the diamond-equations and new R-matrices for small quantum groups

In this chapter we will give the solutions of the R-matrix ansatz of Theorem 2.1.6. For this we will consider the equations of Definition 4.1.2, the so-called diamond-equations. Then, we will give some criteria when solutions of the group-equations, as determined in Section 3.5, are also solutions of the diamond-equations. In Section 4.3, we will give our main Theorem 4.3.1 and work out the proof by a case by case argument. We close with an example in the last section.

4.1. Quotient diamonds and equations of diamond type

We introduce the notion of a diamond (of sublattices) and the corresponding diamond-equations and set this in relation to our situation of sublattices Λ, Λ' of the weight lattice Λ_W of a Lie algebra $\mathfrak{g}$ and corresponding quantum group $u_q(\mathfrak{g}, \Lambda, \Lambda')$.

Definition 4.1.1. Let G and A be abelian groups and B, C, D subgroups of A, with $D \subset B \cap C$. We call a tuple $(G, A, B, C, D, \varphi_1, \varphi_2)$ with injective group morphisms $\varphi_1 \colon A/B \to G^* = \mathrm{Hom}(G, \mathbb{C}^\times)$ and $\varphi_2 \colon A/C \to G$ a *diamond for* G. We visualize the situation with the following diagram

$$\begin{tikzcd}[column sep=small]
& & A \arrow[dl, dash] \arrow[dr, dash] & & \\
G^* & B \arrow[l, hook', "\varphi_1"'] \arrow[dr, dash] & & C \arrow[r, hook, "\varphi_2"] \arrow[dl, dash] & G \\
& & D & &
\end{tikzcd}$$

Definition 4.1.2. Let G be a finite abelian group and $(G, A, B, C, D, \varphi_1, \varphi_2)$ be a diamond for G. For $a \in A \setminus (B \cap C)$ we define the following equations in the $|G|^2$

complex variables $g(x,y)$, indexed by $x, y \in G$:

$$0 = \sum_{y_1+y_2=y, y_i \in G} \varphi_1(a)(y_1) g(x, y_1) g(x+\varphi_2(a), y_2), \tag{4.1.1}$$

$$0 = \sum_{x_1+x_2=x, x_i \in G} \varphi_1(a)(x_1) g(x_1, y) g(x_2, y+\varphi_2(a)), \tag{4.1.2}$$

$$0 = \sum_{y \in G} (\varphi_1(a)(y))^{-1} g(\varphi_2(a), y), \tag{4.1.3}$$

$$0 = \sum_{x \in G} (\varphi_1(a)(x))^{-1} g(x, \varphi_2(a)). \tag{4.1.4}$$

Here, $\varphi_i(a)$ denotes the image of $a+B$, resp. $a+C$, for $a \in A$ under φ_1, resp. φ_2. This gives for every $a \in A \setminus (B \cap C)$ a set of $2|G|^2+2$ equations in $|G|^2$ variables with values in $\mathbb{C}$. We call the set of all equations for all possible $a \in A \setminus (B \cap C)$ *diamond-equations* for the diamond of G, which are up to $(|A|-1)(2|G|^2+2)$ equations in total.

We show how these equations arise in the situation of Lemma 2.2.1.

Lemma 4.1.3. *Let $G = \pi_1$, the fundamental group of a root system Φ. Assume Λ' is a sublattice of Λ_R, contained in $\mathrm{Cent}^{[\ell]}(\Lambda_W)$ and $\ell \in \mathbb{N}$. Let $A = \mathrm{Cent}^{[\ell]}(\Lambda_R)/\Lambda'$, $B = \mathrm{Cent}^{[\ell]}(\Lambda_W)/\Lambda'$, $C = \mathrm{Cent}^{[\ell]}(\Lambda_R) \cap \Lambda_R/\Lambda'$ and $D = (\mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R)/\Lambda'$. Then there exist injections $\varphi_1 \colon A/B \to \pi_1^*$ and $\varphi_2 \colon A/C \to \pi_1$, such that $(G, A, B, C, D, \varphi_1, \varphi_2)$ is a diamond for G.*

$$\begin{tikzcd}[column sep=small]
 & \mathrm{Cent}^{[\ell]}(\Lambda_R)/\Lambda' \arrow[dl, dash, "\pi_1^* \hookleftarrow"'] \arrow[dr, dash, "\hookrightarrow \pi_1"] & \\
\mathrm{Cent}^{[\ell]}(\Lambda_W)/\Lambda' \arrow[dr, dash] & & \mathrm{Cent}^{[\ell]}(\Lambda_R) \cap \Lambda_R/\Lambda' \arrow[dl, dash] \\
 & \mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R/\Lambda' &
\end{tikzcd}$$

Proof. Recall from Lemmas 1.2.7 and 1.2.8 that we have $\mathrm{Cent}(\Lambda_R) = \Lambda_W^{[\ell]}$ for the central weights and $\mathrm{Cent}(\Lambda_W) \cap \Lambda_R = \Lambda_R^{[\ell]}$, thus $A/C \cong \Lambda_W^{[\ell]}/(\Lambda_W^{[\ell]} \cap \Lambda_R)$ and $\Lambda_W^{[\ell]} \subset \Lambda_W$.

To show the existence of an injective morphism $\varphi_2 : A/C \to \pi_1$, we define $\tilde{\varphi}_2$ on $\Lambda_W^{[\ell]}$ and calculate the kernel. By Definition 1.2.5, the generators of $\Lambda_W^{[\ell]}$ are $\ell_{[i]}\lambda_i$ for all $i \in I$, with $\ell_{[i]} := \ell/\gcd(\ell, d_i)$. Thus

$$\tilde{\varphi}_2 \colon \Lambda_W^{[\ell]} \to \pi_1, \ \ell_{[i]}\lambda_i \mapsto \ell_{[i]}\lambda_i + \Lambda_R$$

gives a group morphism. Since $\Lambda' \subset \Lambda_R \cap \Lambda_W^{[\ell]} = \ker \tilde{\varphi}_2$, this induces a well-defined map $\varphi_2 \colon A/\Lambda' \to \pi_1$. Obviously, the kernel of this map is $\Lambda_W^{[\ell]} \cap \Lambda_R$, hence the desired injection $\varphi_2\colon A/C \to \pi_1$ exists and is given by taking $\lambda + (\Lambda_W^{[\ell]} \cap \Lambda_R)$ modulo Λ_R, $\lambda \in \Lambda_W^{[\ell]}$.

Now, we show the existence of φ_1. The map

$$f\colon \mathrm{Cent}(\Lambda_R) \to \mathrm{Hom}(\Lambda_W, \mathbb{C}^\times),\ \lambda \mapsto (\Lambda_W \to \mathbb{C}^\times,\ \eta \mapsto q^{(\lambda,\eta)})$$

is a group morphism. We define $g\colon \mathrm{Hom}(\Lambda_W, \mathbb{C}^\times) \to \mathrm{Hom}(\Lambda_W/\Lambda_R, \mathbb{C}^\times)$ by $g(\psi) := \psi \circ p$, where p is the natural projection $\Lambda_W \to \Lambda_W/\Lambda_R$. Thus, the upper right triangle of the following diagram commutes.

$$\begin{tikzcd}
\mathrm{Cent}(\Lambda_R) \arrow[r, "f"] \arrow[d] \arrow[dr, "g \circ f"'] & \mathrm{Hom}(\Lambda_W, \mathbb{C}^\times) \arrow[d, "g"] \\
\mathrm{Cent}(\Lambda_R)/\mathrm{Cent}(\Lambda_W) \arrow[r, "\varphi_1"'] & \mathrm{Hom}(\pi_1, \mathbb{C}^\times)
\end{tikzcd}$$

There exists $\lambda \in \ker g \circ f$, iff $q^{(\lambda,\bar{\eta})} = 1$ for all $\bar{\eta} \in \pi_1$. Since $\lambda \in \mathrm{Cent}(\Lambda_R)$, this is equivalent to $q^{(\lambda,\eta)} = 1$ for all $\eta \in \Lambda_W$, hence $\lambda \in \mathrm{Cent}(\Lambda_W)$. Thus, we get φ_1 as desired, which is well defined as map from $\mathrm{Cent}(\Lambda_R)/\Lambda' \big/ \mathrm{Cent}(\Lambda_W)/\Lambda'$ since $\Lambda' \subset \mathrm{Cent}(\Lambda_W) = \ker f$. ∎

Under our assumptions the choice of the lattice Λ' is unique, as shown in the next Lemma.

Lemma 4.1.4. *Let $(G, A, B, C, D, \varphi_1, \varphi_2)$ be a diamond as in Lemma 4.1.3. If the quotient $(\mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R)/\Lambda' \neq 0$, then none of the solutions of the group-equations (3.5.1)-(3.5.4) are solutions to the diamond-equations (4.1.1)-(4.1.4). Hence under our assumptions 1.3.9, the existence of an R-matrix requires necessarily the choice $\Lambda' = \mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R$.*

Proof. If $(\mathrm{Cent}(\Lambda_W) \cap \Lambda_R)/\Lambda' \neq 0$, then there exist a root $\zeta \in \mathrm{Cent}(\Lambda_W)$, not contained in the kernel Λ'. Thus, there are diamond-equations with $\varphi_1(\zeta) = \mathbf{1}$ and $\varphi_2(\zeta) = 0$, i.e. the set of equations:

$$0 = \sum_{y_1+y_2=y} g(x, y_1) g(x, y_2),$$
$$0 = \sum_{x_1+x_2=x} g(x_1, y) g(x_2, y),$$
$$0 = \sum_{y \in G} g(0, y),$$
$$0 = \sum_{x \in G} g(x, 0).$$

Since this are group-equations as in Definition 3.5.1, but with left-hand side equal to 0, solutions of the group-equations does not solve the diamond-equations in this situation. ∎

Before examining in which case a solution of the group-equations as in Theorem 3.5.2 is also a solution of the diamond-equations (4.1.1)-(4.1.4), we show that it is sufficient to check only the diamond-equations (4.1.3) and (4.1.4).

Lemma 4.1.5. *Let G be an abelian group of order N, H_1, H_2 subgroups with $|H_1| = |H_2| = d$ and $\omega\colon H_1 \times H_2 \to \mathbb{C}^\times$ a group-pairing, such that $g\colon G \times G \to \mathbb{C}$, $(x,y) \mapsto 1/d\ \omega(x,y)\delta_{(x\in H_1)}\delta_{(y\in H_2)}$ is a solution of the group-equations (3.5.1)-(3.5.4), as in Theorem 3.5.2. Then the following holds:*
If g is a solution of the diamond-equations (4.1.1), (4.1.2), then g solves the diamond-equations (4.1.3), (4.1.4) as well.

Proof. Let g be a solution of the group-equations as in Theorem 3.5.2. Assume that g solves (4.1.1) and (4.1.2). Let φ_1, φ_2 as in Definition 4.1.1 and $0 \neq \zeta \in A$ a non-trivial central weight. Then, for $x, y \in G$ we get by inserting g in (4.1.1)

$$
\begin{aligned}
0 &= \sum_{y_1+y_2=y} \varphi_1(\zeta)(y_1)g(x,y_1)g(x+\varphi_2(\zeta),y_2) \\
&= \sum_{y_1+y_2=y} \varphi_1(\zeta)(y_1)\frac{1}{d^2}\omega(x,y_1)\omega(x+\varphi_2(\zeta),y_2)\delta_{(x\in H_1)}\delta_{(y_1\in H_2)}\delta_{(x+\varphi_2(\zeta)\in H_1)}\delta_{(y_2\in H_2)} \\
&= \delta_{(x\in H_1)}\delta_{(y\in H_2)}\delta_{(\varphi_2(\zeta)\in H_1)}\frac{1}{d^2}\sum_{\substack{y_1+y_2=y\\ y_1,y_2\in H_2}} \varphi_1(\zeta)(y_1)\omega(x,y_1)\omega(x,y_2)\omega(\varphi_2(\zeta),y_2) \\
&= \delta_{(x\in H_1)}\delta_{(y\in H_2)}\delta_{(\varphi_2(\zeta)\in H_1)}\frac{1}{d^2}\omega(x,y)\sum_{\substack{y_1+y_2=y\\ y_1,y_2\in H_2}} \varphi_1(\zeta)(y_1)\omega(\varphi_2(\zeta),y_2) \\
&= \delta_{(x\in H_1)}\delta_{(y\in H_2)}\delta_{(\varphi_2(\zeta)\in H_1)}\frac{1}{d^2}\omega(x,y)\sum_{y_2\in H_2} \varphi_1(\zeta)(y-y_2)\omega(\varphi_2(\zeta),y_2) \\
&= \delta_{(x\in H_1)}\delta_{(y\in H_2)}\delta_{(\varphi_2(\zeta)\in H_1)}\frac{1}{d^2}\omega(x,y)\varphi_1(\zeta)(y)\sum_{y_2\in H_2} \varphi_1(\zeta)(y_2)^{-1}\omega(\varphi_2(\zeta),y_2).
\end{aligned}
$$

In particular, this holds for $x = y = 0$, and in this case the expression vanishes iff

$$\delta_{(\varphi_2(\zeta)\in H_1)}\frac{1}{d^2}\sum_{y\in H_2} \varphi_1(\zeta)(y)^{-1}\omega(\varphi_2(\zeta),y) = 0,$$

which is (4.1.3). Analogously, it follows that if g solves (4.1.2) it solves (4.1.4). ∎

4.2. The cyclic case

In the following, G will always be a fundamental group of a simple complex Lie algebra, hence either cyclic or equal to $\mathbb{Z}_2 \times \mathbb{Z}_2$ for the case D_n, n even. In this section, we will derive some results for the cyclic case.

In Example 3.5.5 we have given the solutions of the group-equations for $G = \mathbb{Z}_N$, i.e. for all $d \mid N$ the functions

$$g\colon G \times G \to \mathbb{C},\ (x,y) \mapsto \frac{1}{d}\xi^{\frac{xy}{(N/d)^2}}\,\delta_{(\frac{N}{d}|x)}\delta_{(\frac{N}{d}|y)} \tag{3.5.6}$$

with ξ a d-th root of unity, not necessarily primitive. In the following, we denote by ξ_d the primitive d-th root of unity $\exp(2\pi i/d)$.

Lemma 4.2.1. *Let $l \geq 2$, $m \in \mathbb{N}$ and $G = \langle \lambda \rangle \cong \mathbb{Z}_N$. We consider the following diamonds $(G, A, B, C, D, \varphi_1, \varphi_2)$ with $A = \langle a \rangle \cong \mathbb{Z}_N$ and injections φ_1 and φ_2 given by*

$$\begin{aligned}
&\tilde{\varphi}_1\colon A \to G^*,\ a \mapsto (\xi_N^m)^{(-)}, \quad \textit{with } (\xi_N^m)^{(-)}\colon G \to \mathbb{C}^\times,\ x \mapsto \xi_N^{mx},\\
&\tilde{\varphi}_2\colon A \to G,\ \ a \mapsto l\lambda,
\end{aligned}$$

with primitive N-th root of unity ξ_N, $B = \ker\tilde{\varphi}_1$ and $C = \ker\tilde{\varphi}_2$ and $D = \{0\}$.

Possible solutions of the group-equations (3.5.1)-(3.5.4) are given for any choice of integers $1 \leq k \leq d$ and $d \mid N$ as in Example 3.5.5 by

$$g\colon G \times G \to \mathbb{C},\ (x,y) \mapsto \frac{1}{d}\left(\xi_d^k\right)^{\frac{xy}{(N/d)^2}}\,\delta_{(\frac{N}{d}|x)}\delta_{(\frac{N}{d}|y)}, \tag{4.2.1}$$

with primitive d-th root of unity $\xi_d = \exp(2\pi i/d)$. These are solutions also to the diamond-equations (4.1.1)-(4.1.4), iff $N \mid m, l$ or the following condition hold:

$$\gcd(N, dl, kl - \frac{N}{d}m) = 1. \tag{4.2.2}$$

Proof. For $N \mid m, l$ there is no non-trivial diamond-equation, hence all solutions of the group-equations as in Example 3.5.5 are possible. Assume now that not both $N \mid m$ and $N \mid l$. We insert the function g from (4.2.1) in the diamond-equations (4.1.1)-(4.1.4) and get requirements for d, k, l and N. By Lemma 4.1.5 it is sufficient to consider only equations (4.1.3) and (4.1.4). Since for cyclic G the function g is symmetric we choose equation (4.1.3) for the calculation. In the following we omit the $\tilde{}$ on the maps $\tilde{\varphi}_{1/2}\colon A \to G^*$, resp. G. Let $1 \leq z < N$, a the generator of A and $y \in G$, then

$$\begin{aligned}
\sum_{y=1}^{N} \left(\varphi_1(za)(y)\right)^{-1} g(\varphi_2(za), y) &= \frac{1}{d}\sum_{y=1}^{N} \xi_N^{-zmy}\left(\xi_d^k\right)^{\frac{zly}{(N/d)^2}}\,\delta_{(\frac{N}{d}|zl)}\delta_{(\frac{N}{d}|y)}\\
&= \frac{1}{d}\sum_{y=1}^{N} \xi_d^{-\frac{zmy}{N/d}}\left(\xi_d^{\frac{zkl}{(N/d)}}\right)^{\frac{y}{N/d}}\,\delta_{(\frac{N}{d}|zl)}\delta_{(\frac{N}{d}|y)},\\
&= \frac{1}{d}\sum_{y'=1}^{d}\left(\xi_d^{-zm+\frac{zkl}{(N/d)}}\right)^{y'}\,\delta_{(\frac{N}{d}|zl)},
\end{aligned}$$

with the substitution $y' = y/(N/d)$. This sum equals 0 iff $N/d \nmid zl$ or $d \nmid z(kl/(N/d) - m)$. This is equivalent to $N \nmid zdl$ or $N \nmid z(kl - (N/d)m)$, hence $N \nmid \gcd(zdl, z(kl - (N/d)m)) = z\gcd(dl, kl - (N/d)m)$. Since this condition has to be fulfilled for all z this is equivalent to $\gcd(N, dl, kl - (N/d)m) = 1$. ∎

We spell out the condition for explicit values m and l.

Example 4.2.2. Let $G = \mathbb{Z}_N = \langle \lambda \rangle$, $l \geq 2$, $m \in \mathbb{N}$ and diamond $(G, A, B, C, D, \varphi_1, \varphi_2)$ as in Lemma 4.2.1. Depending on m, l we get the following criteria for solutions of the diamond-equations. Here, we give φ_1 and φ_2 shortly by the generator of its image.

(I) If $N \mid m$ and $N \mid l$ we have diamond $(\mathbb{Z}_N, \mathbb{Z}_N, \mathbb{Z}_N, \mathbb{Z}_N, \mathbb{Z}_1, 1, 0)$ and all solutions of the form (4.2.1) are also solutions to the diamond-equations (4.1.1)-(4.1.4). (Since $B, C = A$ and $D = 1$, there are no non-trivial diamond-equations, and this is not a "real" diamond situation in the sense of Lemma 4.1.3.)

(II) If $N \mid m$ and $N \nmid l$ we have diamond $(\mathbb{Z}_N, \mathbb{Z}_N, \mathbb{Z}_N, \mathbb{Z}_{\gcd(l,N)}, \mathbb{Z}_1, 1, l\lambda)$. In this case the function g as in (4.2.1) is a solution to the diamond-equations (4.1.1)-(4.1.4) if $\gcd(N, dl, kl) = 1$.

(III) If $\gcd(m, N) = 1$ we have diamond $(\mathbb{Z}_N, \mathbb{Z}_N, \mathbb{Z}_1, \mathbb{Z}_{\gcd(l,N)}, \mathbb{Z}_1, \xi_N, l\lambda)$. In this case the function g as in (4.2.1) is a solution to the diamond-equations (4.1.1)-(4.1.4) if

$$\gcd(N, dl, kl - \frac{N}{d}m) = 1. \tag{4.2.2}$$

In most cases, N is prime or equals 1, hence we consider the two special cases

(1) If $d = 1$, (4.2.2) simplifies to $\gcd(N, l, l - Nm) = 1$, which is equivalent to $\gcd(N, l) = 1$.

(2) If $d = N$, (4.2.2) simplifies to $\gcd(N, Nl, kl - m) = 1$, which is equivalent to $\gcd(N, kl - m) = 1$.

Finally, we consider the Lie algebras with cyclic fundamental group in question and determine the values m and l according to the Lie theoretic data and thereby the corresponding diamonds.

Example 4.2.3. Let $G = \mathbb{Z}_N$ be the fundamental group of a simple complex Lie algebra $\mathfrak{g}$, generated by the fundamental dominant weight λ_n. Let $\ell \in \mathbb{N}$, $\ell > 2$, $q = \exp(2\pi i/\ell)$, $\ell_{[n]} = \ell / \gcd(\ell, d_n)$, $m_{[n]} := N(\lambda_n, \lambda_n)/\gcd(\ell, d_n)$ and $(G, A, B, C, D, \varphi_1, \varphi_2)$ be a diamond as in Lemma 4.1.3, such that the corresponding diamond-equations (4.1.1)-(4.1.4) have a solution that is also a solution to the group-equations (3.5.1)-(3.5.4). Then, the diamond is

$$(G, \mathbb{Z}_N, \mathbb{Z}_{\gcd(m_{[n]},N)}, \mathbb{Z}_{\gcd(\ell_{[n]},N)}, \mathbb{Z}_1, \varphi_1, \varphi_2), \tag{4.2.3}$$

with injections

$$\begin{aligned}
&\varphi_1 \colon A \to G^*,\ \ell_{[n]}\lambda_n \mapsto (\xi_N^{m_{[n]}})^{(-)}, \quad \text{with } (\xi_N^{m_{[n]}})^{(-)} \colon G \to \mathbb{C}^\times,\ x \mapsto \xi_N^{m_{[n]}x}, \\
&\varphi_2 \colon A \to G,\ \ \ell_{[n]}\lambda_n \mapsto \ell_{[n]}\lambda_n,
\end{aligned}$$

with primitive N-th root of unity $\xi_N = \exp(2\pi i/N)$. The group $A = \mathrm{Cent}(\Lambda_R)/\Lambda' = \Lambda_W^{[\ell]}/\Lambda_R^{[\ell]}$ is generated by $\ell_{[n]}\lambda_n$ and $q^{(\ell_{[n]}\lambda_n, \lambda_n)} = (\xi_N^N)^{(\lambda_n,\lambda_n)/\gcd(\ell,d_n)}$. Since the order of $\xi_N^{m_{[n]}}$ in $\mathbb{C}^\times$ is $N/\gcd(m_{[n]}, N)$ and the order of $\ell_{[n]}$ in $\mathbb{Z}_N$ is $N/\gcd(\ell_{[n]}, N)$, the injections φ_1, φ_2 determine the diamond (4.2.3).

In the following table, we give the values $\ell_{[n]}$ and $m_{[n]}$ for all root systems of simple Lie algebras with cyclic fundamental group.

$\mathfrak{g}$	$A_{n\geq 1}$	$B_{n\geq 2}$	$C_{n\geq 3}$		$D_{n\geq 5}$ n odd	E_6	E_7	E_8	F_4	G_2	
π_1	$\mathbb{Z}_{n+1}$	$\mathbb{Z}_2$	$\mathbb{Z}_2$		$\mathbb{Z}_4$	$\mathbb{Z}_3$	$\mathbb{Z}_2$	$\mathbb{Z}_1$	$\mathbb{Z}_1$	$\mathbb{Z}_1$	
N	$n+1$	2	2		4	3	2	1	1	1	
d_n	1	1	2		1	1	1	1	1	3	
ℓ	all	all	$2 \nmid \ell$	$2 \mid \ell$	all	all	all	all	all	$3 \nmid \ell$	$3 \mid \ell$
$\gcd(\ell, d_n)$	1	1	1	2	1	1	1	1	1	1	3
(λ_n, λ_n)	$\frac{n}{n+1}$	$\frac{n}{2}$	n		$\frac{n}{4}$	$\frac{4}{3}$	$\frac{3}{2}$	2	1	6	
$\ell_{[n]}$	ℓ	ℓ	ℓ	$\ell/2$	ℓ	ℓ	ℓ	ℓ	ℓ	ℓ	$\ell/3$
$m_{[n]}$	n	n	$2n$	n	n	4	3	2	1	6	2
cases	(III)	(I)-(III)	(II)	(I)-(III)	(III)	(III)	(III)	(I)	(I)	(I)	(I)

In the last row we indicate which cases in Example 4.2.2 apply. This will guide the proof of Theorem 4.3.1. Note that case (II) only appears for B_n, n even and ℓ odd, and for C_n, even n and $\ell \equiv 2 \mod 4$ or odd ℓ.

4.3. Solutions

The following theorem is the main result of this thesis and gives all solutions of R-matrices satisfying Lusztig's ansatz $R = R_0\bar{\Theta}$ of Theorem 2.1.6 under our assumption on Λ', see Lemma 4.1.4.

Theorem 4.3.1. *Let $\mathfrak{g}$ be a finite-dimensional simple complex Lie algebra with root lattice Λ_R, weight lattice Λ_W and fundamental group $\pi_1 = \Lambda_W/\Lambda_R$. Let q be an ℓ-th root of unity, $\ell \in \mathbb{N}$, $\ell > 2$. Then we have the following R-matrix of the form $R = R_0\bar{\Theta}$, with Θ as in Theorem 2.1.2:*

$$R = \left(\frac{1}{|\Lambda/\Lambda'|} \sum_{(\mu,\nu)\in(\Lambda_1/\Lambda' \times \Lambda_2/\Lambda')} q^{-(\mu,\nu)} \omega(\bar{\mu}, \bar{\nu})\ K_\mu \otimes K_\nu \right) \cdot \bar{\Theta},$$

for the quantum group $u_q(\mathfrak{g}, \Lambda, \Lambda')$ with $\Lambda = \Lambda_W$ and Λ_i the preimage of a certain subgroup $H_i \subset \pi_1$ in Λ_W ($i = 1, 2$), a certain group-pairing $\omega\colon H_1 \times H_2 \to \mathbb{C}^\times$ and $\Lambda' = \Lambda_R^{[\ell]}$ as in Def. 1.2.5.

In the following table we list for all root systems the following data, depending on ℓ: Possible choices of H_1, H_2 (in terms of fundamental weights λ_k), the group-pairing ω, and the number of solutions #. If the number has a superscript $*$, we obtain R-matrices for Lusztig's original choice of Λ'. For $\mathfrak{g} = D_n$, $2 \mid n$, with $\pi_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$ we get the only cases $H_1 \neq H_2$ and denote by $\lambda \neq \lambda' \in \{\lambda_{n-1}, \lambda_n, \lambda_{n-1} + \lambda_n\}$ arbitrary elements of order 2 in π_1.

$\mathfrak{g}$	ℓ	#	$H_i \cong$	$H_{i\ (i=1,2)}$	ω
$A_{n\geq 1}$ $\pi_1 = \mathbb{Z}_{n+1}$	ℓ odd		$\mathbb{Z}_d$	$\langle \frac{n+1}{d}\lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = \xi_d^k$, if $d \mid (n+1),\ 1 \leq k \leq d$ and $\gcd(n+1, d\ell, k\ell - \frac{n+1}{d}n) = 1$
	ℓ even	*			
$B_{n\geq 2}$ $\pi_1 = \mathbb{Z}_2$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = (-1)^{n-1}$
	$\ell \equiv 2 \mod 4$	2	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = \pm 1$
		1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$, if n even
	$\ell \equiv 0 \mod 4$ $\ell \neq 4$	2*	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = \pm 1$
		1*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$, if n even
$C_{n\geq 3}$ $\pi_1 = \mathbb{Z}_2$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = -1$
	$\ell \equiv 2 \mod 4$	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = (-1)^{n-1}$
	$\ell \equiv 0 \mod 4$ $\ell \neq 4$	2*	$\mathbb{Z}_2$	$\langle \lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = \pm 1$
		1*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$, if n even
$D_{n\geq 4}$ n even $\pi_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		3	$\mathbb{Z}_2$	$\langle \lambda \rangle$	$\omega(\lambda,\lambda) = -1$
		6	$\mathbb{Z}_2 \neq \mathbb{Z}_2'$	$\langle \lambda \rangle, \langle \lambda' \rangle$	$\omega(\lambda,\lambda') = 1$
		1	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1},\lambda_n \rangle$	$\omega(\lambda_i,\lambda_j) = 1$
		1	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1},\lambda_n \rangle$	$\omega(\lambda_i,\lambda_j) = -1$
		2	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1},\lambda_n \rangle$	$\omega(\lambda_{n-1},\lambda_{n-1}) = \pm 1$ $\omega(\lambda_{n-1},\lambda_n) = 1$ $\omega(\lambda_n,\lambda_{n-1}) = 1$ $\omega(\lambda_n,\lambda_n) = \mp 1$
		2	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1},\lambda_n \rangle$	$\omega(\lambda_{n-1},\lambda_{n-1}) = -1$ $\omega(\lambda_{n-1},\lambda_n) = \pm 1$ $\omega(\lambda_n,\lambda_{n-1}) = \mp 1$ $\omega(\lambda_n,\lambda_n) = -1$
	ℓ even	16*	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\langle \lambda_{n-1},\lambda_n \rangle$	$\omega(\lambda_i,\lambda_j) \in \{\pm 1\}$
$D_{n\geq 5}$ n odd $\pi_1 = \mathbb{Z}_4$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle 2\lambda_n \rangle$	$\omega(2\lambda_n,2\lambda_n) = -1$
		2	$\mathbb{Z}_4$	$\langle \lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = \pm 1$
	$\ell \equiv 2 \mod 4$	4*	$\mathbb{Z}_4$	$\langle \lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = c,\ c^4 = 1$
	$\ell \equiv 0 \mod 4$	4*	$\mathbb{Z}_4$	$\langle \lambda_n \rangle$	$\omega(\lambda_n,\lambda_n) = c,\ c^4 = 1$
E_6	ℓ odd, $3 \nmid \ell$	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		2	$\mathbb{Z}_3$	$\langle \lambda_6 \rangle$	$\omega(\lambda_6,\lambda_6) = 1, \exp(\frac{2\pi i}{3})$
	ℓ even, $3 \nmid \ell$	1*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$

$\pi_1 = \mathbb{Z}_3$		2^*	$\mathbb{Z}_3$	$\langle \lambda_6 \rangle$	$\omega(\lambda_6, \lambda_6) = 1, \exp(2\frac{2\pi i}{3})$
	ℓ odd, $3 \mid \ell$	3	$\mathbb{Z}_3$	$\langle \lambda_6 \rangle$	$\omega(\lambda_6, \lambda_6) = c,\ c^3 = 1$
	ℓ even, $3 \mid \ell$	3^*	$\mathbb{Z}_3$	$\langle \lambda_6 \rangle$	$\omega(\lambda_6, \lambda_6) = c,\ c^3 = 1$
E_7 $\pi_1 = \mathbb{Z}_2$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
		1	$\mathbb{Z}_2$	$\langle \lambda_7 \rangle$	$\omega(\lambda_7, \lambda_7) = 1$
	ℓ even	2^*	$\mathbb{Z}_2$	$\langle \lambda_7 \rangle$	$\omega(\lambda_7, \lambda_7) = \pm 1$
E_8 $\pi_1 = \mathbb{Z}_1$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
	ℓ even	1^*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
F_4 $\pi_1 = \mathbb{Z}_1$	ℓ odd	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
	$\ell \equiv 2 \mod 4$	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
	$\ell \equiv 0 \mod 4$ $\ell \neq 4$	1^*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
G_2 $\pi_1 = \mathbb{Z}_1$	ℓ odd $\ell \neq 3$	1	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$
	ℓ even $\ell \neq 4, 6$	1^*	$\mathbb{Z}_1$	$\{0\}$	$\omega(0,0) = 1$

Table 4.1.: Solutions of R_0-matrices

Proof. We treat the root systems case by case and determine the solutions of the form

$$g\colon G \times G \to \mathbb{C},\ (x,y) \mapsto \frac{1}{d}\omega(x,y)\delta_{(x \in H_1)}\delta_{(y \in H_2)}$$

with subgroups H_1, H_2 of $G = \pi_1$ as in Lemma 3.5.2.
For this, we first determine the lattices $A = \mathrm{Cent}^{[\ell]}(\Lambda_R) = \Lambda_W^{[\ell]},\ B = \mathrm{Cent}^{[\ell]}(\Lambda_W),\ C = \mathrm{Cent}^{[\ell]}(\Lambda_R) \cap \Lambda_R,\ D = \mathrm{Cent}^{[\ell]}(\Lambda_W) \cap \Lambda_R = \Lambda_R^{[\ell]}$, depending on ℓ. For the Lie algebras with cyclic fundamental group (all but for root system D_n with even n), we then determine the values $m_{[n]}$ and $\ell_{[n]}$, depending on ℓ, n and the order of π_1, and thereby the quotient diamonds and which solutions of the group-equations are solutions to the corresponding diamond-equations. In these cases, the ω-part of the solutions to the group-equations are of the form

$$\omega\colon H \times H \to \mathbb{C}^\times,\ (x,y) \mapsto \left(\xi_d^k\right)^{\frac{xy}{(N/d)^2}}$$

for subgroup $H = \frac{N}{d}\mathbb{Z}_N$ of π_1 of order d. We give the solutions by pairs (d,k), which we determine by applying Lemma 4.2.1 and Example 4.2.2. An overview of the possible cases gives Example 4.2.3.
For D_n with even n and fundamental group $\mathbb{Z}_2 \times \mathbb{Z}_2$ we also determine all quotient diamonds (depending on ℓ) and check which solutions of the group-equations solve the diamond-equations in a rather case by case calculation.

A generator of the fundamental group $\pi_1 = \Lambda_W/\Lambda_R$ of the Lie algebra $\mathfrak{g}$ is given by its preimage in Λ_W, i.e. a fundamental weight λ, such that $\bar{\lambda} \in \pi_1$ generates π_1. By slight abuse of notation we will omit the $^-$ in this situation.

(1) For $\mathfrak{g}$ with root system A_n, $n \geq 1$, we have $\pi_1 = \mathbb{Z}_{n+1}$ for all n. The simple roots are $\alpha_1, \ldots, \alpha_n$ and $d_i = 1$ for $1 \leq i \leq n$. The symmetrized Cartan matrix $\tilde{C}$ is given below. The fundamental dominant weights λ_i are given as in [Hum72], Section 13.2, and λ_n is the generator of the fundamental group $\mathbb{Z}_{n+1}$. The matrix id_W^R gives the coefficients of the fundamental dominant weights in the basis $\{\alpha_1, \ldots, \alpha_n\}$.

$$\tilde{C} = \begin{pmatrix} 2 & -1 & 0 & . & . & . & . & 0 \\ -1 & 2 & -1 & 0 & . & . & . & 0 \\ 0 & -1 & 2 & -1 & 0 & . & . & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & . & . & -1 & 2 \end{pmatrix}$$

$$id_W^R = a_{ij} \text{ with } a_{ij} = \begin{cases} \frac{1}{n+1} i(n-j+1), & \text{if } i \leq j, \\ \frac{1}{n+1} j(n-i+1), & \text{if } i > j. \end{cases}$$

The lattice diamonds, depending on ℓ, are:

(i) For even ℓ we have $A = \ell\Lambda_W$, $B = D = \ell\Lambda_R$ and $C = \ell/\gcd(n+1, \ell)\Lambda_R$.

(ii) For odd ℓ: the same lattices as in (i).

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations according to Example 4.2.2.

(i) For odd ℓ it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = n$. Thus, the quotient diamond is given by $(\mathbb{Z}_{n+1}, \mathbb{Z}_{n+1}, \mathbb{Z}_1, \mathbb{Z}_{\gcd(\ell,n+1)}, \mathbb{Z}_1, \xi_{n+1}, \ell\lambda_n)$, hence we are in case (III) of Example 4.2.2. We get solutions (d, k) iff $\gcd(n+1, d\ell, k\ell - \frac{n+1}{d}n) = 1$.

(ii) For odd ℓ it is $\Lambda_R^{[\ell]} = \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = n$. Thus, the quotient diamonds and solutions are as in (i).

(2) For $\mathfrak{g}$ with root system B_n, $n \geq 2$, we have $\pi_1 = \mathbb{Z}_2$ for all n. The long simple roots are $\alpha_1, \ldots, \alpha_{n-1}$ and the short simple root α_n, hence $d_i = 2$ for $1 \leq i \leq n-1$ and $d_n = 1$. The symmetrized Cartan matrix $\tilde{C}$ is given below. The fundamental dominant weights λ_i are given as in [Hum72], Section 13.2. Here, $\lambda_1, \ldots, \lambda_{n-1}$ are roots and λ_n is the generator of the fundamental group $\mathbb{Z}_2$. The matrix id_W^R gives the coefficients of the fundamental dominant weights in the basis $\{\alpha_1, \ldots, \alpha_n\}$.

$$\tilde{C} = \begin{pmatrix} 4 & -2 & 0 & 0 & . & & & 0 \\ -2 & 4 & -2 & 0 & . & & & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & & . & -2 & 4 & -2 \\ 0 & 0 & 0 & & . & 0 & -2 & 2 \end{pmatrix} \qquad id_W^R = \begin{pmatrix} 1 & 1 & . & . & 1 & \frac{1}{2} \\ 1 & 2 & . & . & 2 & 1 \\ . & . & . & . & . & . \\ 1 & 2 & 3 & . & n-1 & \frac{n-1}{2} \\ 1 & 2 & 3 & . & n-1 & \frac{n}{2} \end{pmatrix}$$

The lattice diamonds, depending on ℓ, are:

(i) For odd ℓ we have $A = \ell\Lambda_W$ and $C = D = \ell\Lambda_R$. Since $(\lambda_n, \lambda_n) = n/2$, the group $\mathrm{Cent}(\Lambda_W)$ depends on n. It is $B = \ell\Lambda_W$ for even n and $B = \ell\Lambda_R$ for odd n.

(ii) For even ℓ we have $A = C = \ell\langle \frac{1}{2}\lambda_1, \ldots, \frac{1}{2}\lambda_{n-1}, \lambda_n\rangle$ and $D = \ell\langle \frac{1}{2}\alpha_1, \ldots, \frac{1}{2}\alpha_{n-1}, \alpha_n\rangle$. Again, B depends on n, and we have $B = \ell\langle \frac{1}{2}\lambda_1, \ldots, \frac{1}{2}\lambda_{n-1}, \lambda_n\rangle$ for even n and $B = \ell\langle \frac{1}{2}\lambda_1, \ldots, \frac{1}{2}\lambda_{n-1}, 2\lambda_n\rangle$ for odd n.

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations according to Example 4.2.2.

(i) For odd ℓ it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = n$. In this case, the quotient diamond is given by either $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_1, 1, \lambda_n)$ for even n, or by $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, -1, \lambda_n)$ for odd n. Thus we are either in case (II), or in case (III) of Example 4.2.2. In the first case (even n) we get solutions by $(d, k) = (1, 1)$ and $(2, 1)$. For odd n we get solutions $(d, k) = (1, 1)$ and $(2, 2)$.

(ii.a) For $\ell \equiv 2 \mod 4$ it is $\Lambda_R^{[\ell]} = \ell\langle \frac{1}{2}\alpha_1, \ldots, \frac{1}{2}\alpha_{n-1}, \alpha_n\rangle \neq \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = n$. The quotient diamond is given by either $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, 1, 0)$ for even n, or by $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_1, -1, 0)$ for odd n. Thus we are in either in case (I) or in case (III) of Example 4.2.2. In the first case (even n) we get all possible 3 solutions $(d, k) = (1, 1)$, $(2, 1)$ and $(2, 1)$. For odd n we get solutions $(d, k) = (2, 1)$ and $(2, 2)$.

(ii.b) For $\ell \equiv 0 \mod 4$ it is $\Lambda_R^{[\ell]} = \ell\langle \frac{1}{2}\alpha_1, \ldots \frac{1}{2}\alpha_{n-1}, \alpha_n\rangle = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = n$. Thus the quotient diamonds and solutions are as in (ii.a).

(3) For $\mathfrak{g}$ with root system C_n, $n \geq 3$, we have $\pi_1 = \mathbb{Z}_2$ for all n. The short simple roots are $\alpha_1, \ldots, \alpha_{n-1}$ and the long simple root α_n, hence $d_i = 1$ for $1 \leq i \leq n-1$ and $d_n = 2$. The symmetrized Cartan matrix $\tilde{C}$ is given below. The fundamental dominant weights λ_i are given as in [Hum72], Section 13.2, and λ_n is the generator of the fundamental group $\mathbb{Z}_2$. The matrix id_W^R gives the coefficients of the fundamental dominant weights in the basis $\{\alpha_1, \ldots, \alpha_n\}$.

$$\tilde{C} = \begin{pmatrix} 2 & -1 & 0 & 0 & . & & & 0 \\ -1 & 2 & -1 & 0 & . & & & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & & . & -1 & 2 & -2 \\ 0 & 0 & 0 & & . & 0 & -2 & 4 \end{pmatrix} \qquad id_W^R = \begin{pmatrix} 1 & 1 & . & . & 1 & 1 \\ 1 & 2 & . & . & 2 & 2 \\ . & . & . & . & . & . \\ 1 & 2 & . & . & n-1 & n-1 \\ \frac{1}{2} & 1 & . & . & \frac{n-1}{2} & \frac{n}{2} \end{pmatrix}$$

The lattice diamonds, depending on ℓ, are:

(i) For odd ℓ we have $A = B = \ell\Lambda_W$ and $C = D = \ell\Lambda_R$.

(ii) For $\ell \equiv 2 \mod 4$ we have $A = \ell\langle \lambda_1, \ldots, \lambda_{n-1}, \frac{1}{2}\lambda_n\rangle$ and $C = D = \ell\Lambda_W$. Since

$(\lambda_n, \lambda_n) = n$, $B = \mathrm{Cent}(\Lambda_W)$ depends on n. For odd n it equals $\ell\Lambda_W$ and for even n it is equal to A.

(iii) For $\ell \equiv 0 \mod 4$ we have $A = C = \ell\langle\lambda_1, \ldots, \lambda_{n-1}, \frac{1}{2}\lambda_n\rangle$ and $D = \ell\Lambda_W$. Here again, $B = \mathrm{Cent}(\Lambda_W)$ depends on n. For odd n it equals $\ell\Lambda_W$ and for even n it is equal to A.

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations according to Example 4.2.2.

(i) For odd ℓ it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 2n$. In this case, the quotient diamond is given by $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_1, 1, \lambda_n)$. Thus we are in case (II) of Example 4.2.2, hence the 2 solutions are given by $(d, k) = (1, 1)$ and $(2, 1)$.

(ii) For $\ell \equiv 2 \mod 4$ it is $\Lambda_R^{[\ell]} = \ell\langle\alpha_1, \ldots, \alpha_{n-1}, \frac{1}{2}\alpha_n\rangle \neq \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell/2$ and $m_{[n]} = n$. The quotient diamond is given by either $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_1, 1, \lambda_n)$ for even n, or by $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, -1, \lambda_n)$ for odd n. Thus we are either in case (II) or in case (III) of Example 4.2.2. In the first case (even n) we get solutions $(d, k) = (1, 1)$ and $(2, 1)$. For odd n we get solutions $(d, k) = (1, 1)$ and $(2, 2)$.

(ii) For $\ell \equiv 0 \mod 4$ it is $\Lambda_R^{[\ell]} = \ell\langle\frac{1}{2}\alpha_1, \ldots \frac{1}{2}\alpha_{n-1}, \alpha_n\rangle = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell/2$ and $m_{[n]} = n$. The quotient diamond is given by either $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, 1, 0)$ for even n, or by $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_1, -1, 0)$ for odd n. Thus we are in either in case (I) or in case (III) of Example 4.2.2. In the first case (even n) we get all 3 possible solutions $(d, k) = (1, 1)$, $(2, 1)$ and $(2, 2)$. For odd n we get solutions $(d, k) = (2, 1)$ and $(2, 2)$.

(4) For $\mathfrak{g}$ with root system D_n, $n \geq 4$ even, we have $\pi_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$ for all n. The simple roots are $\alpha_1, \ldots, \alpha_n$ and $d_i = 1$ for $1 \leq i \leq n$. The symmetrized Cartan matrix $\tilde{C}$ is given below. The fundamental dominant weights λ_i are given as in [Hum72], Section 13.2, and λ_{n-1}, λ_n are the generators of the fundamental group $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\lambda_{n-1} + \lambda_n$ is the other element of order 2. The matrix id_W^R gives the coefficients of the fundamental dominant weights in the basis $\{\alpha_1, \ldots, \alpha_n\}$, and since $d_i = 1$ for all i, also the values (λ_i, λ_j) for $1 \leq i, j \leq n$.

$$\tilde{C} = \begin{pmatrix} 2 & -1 & 0 & 0 & . & & & & 0 \\ -1 & 2 & -1 & 0 & . & & . & . & . \\ . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & 2 & -1 & 0 & 0 \\ . & . & . & . & . & -1 & 2 & -1 & -1 \\ 0 & 0 & 0 & & . & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & & . & 0 & -1 & 0 & 2 \end{pmatrix} \qquad id_W^R = \begin{pmatrix} 1 & 1 & 1 & . & 1 & \frac{1}{2} & \frac{1}{2} \\ 1 & 2 & 2 & . & 2 & 1 & 1 \\ 1 & 2 & 3 & . & 3 & \frac{3}{2} & \frac{3}{2} \\ . & . & . & . & . & . & . \\ 1 & 2 & 3 & . & n-2 & \frac{n-2}{2} & \frac{n-2}{2} \\ \frac{1}{2} & 1 & \frac{3}{2} & . & \frac{n-2}{2} & \frac{n}{4} & \frac{n-2}{4} \\ \frac{1}{2} & 1 & \frac{3}{2} & . & \frac{n-2}{2} & \frac{n-2}{4} & \frac{n}{4} \end{pmatrix}$$

The lattice diamonds, depending on ℓ, are:

(i) For odd ℓ we have $A = \ell\Lambda_W$ and $B = C = D = \ell\Lambda_R$.

(ii) For even ℓ we have $A = C = \ell\Lambda_W$ and $B = D = \ell\Lambda_R$.

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations by a case by case calculation.

(i) For odd ℓ it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$. Thus, the quotient diamond is given by $(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \varphi_1, \varphi_2)$ with injections

$$\begin{aligned}
\varphi_1 &\colon \ell\langle \lambda_{n-1}, \lambda_n \rangle \to \pi_1^*,\ \ell\lambda_{n-1} \mapsto q^{\ell(\lambda_{n-1},-)},\ \ell\lambda_n \mapsto q^{\ell(\lambda_n,-)},\\
\varphi_2 &\colon \ell\langle \lambda_{n-1}, \lambda_n \rangle \to \pi_1,\ \ell\lambda_{n-1} \mapsto \lambda_{n-1},\ \ell\lambda_n \mapsto \lambda_n.
\end{aligned}$$

In the following, we will write $a := \lambda_{n-1}$, $b := \lambda_n$ and $c := \lambda_{n-1} + \lambda_n$ for the 3 elements of order 2 of π_1. Since $(\lambda_j, \lambda_j) = n/4$ for $j \in \{n-1, n\}$, and $(\lambda_i, \lambda_j) = (n-2)/4$ for $i \neq j$, $i, j \in \{n-1, n\}$ we get

<table>
<tr><th>φ_1</th><th>0</th><th>a</th><th>b</th><th>c</th><th>n</th></tr>
<tr><td rowspan="2">0</td><td rowspan="2">1</td><td rowspan="2">1</td><td rowspan="2">1</td><td rowspan="2">1</td><td>$n \equiv 0 \mod 4$</td></tr>
<tr><td>$n \equiv 2 \mod 4$</td></tr>
<tr><td rowspan="2">a</td><td rowspan="2">1</td><td>1</td><td>-1</td><td>-1</td><td>$n \equiv 0 \mod 4$</td></tr>
<tr><td>-1</td><td>1</td><td>-1</td><td>$n \equiv 2 \mod 4$</td></tr>
<tr><td rowspan="2">b</td><td rowspan="2">1</td><td>-1</td><td>1</td><td>-1</td><td>$n \equiv 0 \mod 4$</td></tr>
<tr><td>1</td><td>-1</td><td>-1</td><td>$n \equiv 2 \mod 4$</td></tr>
<tr><td rowspan="2">c</td><td rowspan="2">1</td><td rowspan="2">-1</td><td rowspan="2">-1</td><td rowspan="2">1</td><td>$n \equiv 0 \mod 4$</td></tr>
<tr><td>$n \equiv 2 \mod 4$</td></tr>
</table>

Since it suffices to consider the diamond-equations (4.1.3) and (4.1.4) by Lemma 4.1.5, we check which function

$$g\colon G \times G \to \mathbb{C},\ (x, y) \mapsto \frac{1}{d}\omega(x, y)\delta_{(x \in H_1)}\delta_{(y \in H_2)}$$

with subgroups H_i of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ of order d and a pairing ω as in Example 3.5.7 is a solution to these equations. We get the following system of equations for g:

$$\begin{aligned}
1 &= g(0,0)+g(a,0)+g(b,0)+g(c,0)\\
1 &= g(0,0)+g(0,a)+g(0,b)+g(0,c)\\
0 &= g(0,a)\pm g(a,a)\mp g(b,a)-g(c,a)\\
0 &= g(a,0)\pm g(a,a)\mp g(a,b)-g(a,c)\\
0 &= g(0,b)\mp g(a,b)\pm g(b,b)-g(c,b)\\
0 &= g(b,0)\mp g(b,a)\pm g(b,b)-g(b,c)\\
0 &= g(0,c)-g(a,c)-g(b,c)+g(c,c)\\
0 &= g(c,0)-g(c,a)-g(c,b)+g(c,c)
\end{aligned} \tag{4.3.1}$$

where the $\pm,\mp$ possibilities depend on whether $n \equiv 0$ or $2 \mod 4$. It is easy to see that the trivial solution on $H_1 = H_2 = \mathbb{Z}_1$ is a solution. For $H_i \cong \mathbb{Z}_2$ the solution has one of the following two structures. For symmetric solutions $H_1 = H_2 = \langle\lambda\rangle$ we get $\omega(\lambda,\lambda) = -1$. If $H_1 = \langle\lambda\rangle \neq \langle\lambda'\rangle = H_2$ we get $\omega(\lambda,\lambda') = 1$. This give all possible 9 solutions with $H_i \cong \mathbb{Z}_2$. Finally, we check which functions on $G = \mathbb{Z}_2\times\mathbb{Z}_2$ are solutions to the diamond-equations. We get 4 symmetric solutions and 2 non-symmetric solutions, which are given by their values $(\omega(x,y))_{x,y\in\{\lambda_{n-1},\lambda_n\}}$ on generator pairs:

$$\begin{pmatrix}1&1\\1&1\end{pmatrix},\ \begin{pmatrix}-1&-1\\-1&-1\end{pmatrix},\ \begin{pmatrix}1&1\\1&-1\end{pmatrix},\ \begin{pmatrix}-1&1\\1&1\end{pmatrix},\ \begin{pmatrix}-1&1\\-1&-1\end{pmatrix},\ \begin{pmatrix}-1&-1\\1&-1\end{pmatrix}.$$

(ii) For even ℓ it is $\Lambda_R^{[\ell]} = \ell\Lambda_R = 2\Lambda_R^{(\ell)}$. Thus the quotient diamond is given by $(\mathbb{Z}_2\times\mathbb{Z}_2, \mathbb{Z}_2\times\mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_2\times\mathbb{Z}_2, \mathbb{Z}_1, \varphi_1, 0)$ and the injection φ_2 is trivial. We get an analogue block of equations as (4.3.1), but without non-zero "shift" $\varphi_2(x)$, $x \in A$. We can add appropriate equations and get the $1 = 4g(0,0)$, hence only pairings of $H_1 = H_2 = \pi_1$ are solutions. It is now easy to check that all 16 possible parings on $\pi_1 \times \pi_1$ are solutions to the diamond equations.

(5) For $\mathfrak{g}$ with root system D_n, $n \geq 5$ odd, we have $\pi_1 = \mathbb{Z}_4$ for all n. The root and weight data are as for even n in (4). The weight λ_n is the generator of the fundamental group $\mathbb{Z}_2$.

The lattice diamonds, depending on ℓ, are:

(i) For odd ℓ we have $A = \ell\Lambda_W$ and $B = C = D = \ell\Lambda_R$.

(ii) For $\ell \equiv 2 \mod 4$ we have $A = \ell\Lambda_W$, $C = \ell\langle\lambda_1,\ldots,\lambda_{n-2},2\lambda_{n-1},2\lambda_n\rangle$ and $B = D = \ell\Lambda_R$.

(iii) For $\ell \equiv 0 \mod 4$ we have $A = C = \ell\Lambda_W$ and $B = D = \ell\Lambda_R$.

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations according to Example 4.2.2.

(i) For odd ℓ it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = n$. Thus, the quotient diamond is given by $(\mathbb{Z}_4, \mathbb{Z}_4, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \xi_4, \lambda_n)$, hence we are in case (III) of Example 4.2.2. We get solutions $(d, k) = (1, 1)$, $(2, 1)$, $(4, 2)$ and $(4, 4)$.

(ii) For $\ell \equiv 2 \mod 4$ it is $\Lambda_R^{[\ell]} = \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = n$. Thus, the quotient diamond is given by $(\mathbb{Z}_4, \mathbb{Z}_4, \mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_1, \xi_4, 2\lambda_n)$, hence we are in case (III) of Example 4.2.2. We get all 4 solutions $(d, k) = (4, 1)$, $(4, 2)$, $(4, 3)$ and $(4, 4)$ on $H = \mathbb{Z}_4$.

(iii) For $\ell \equiv 0 \mod 4$ it is $\Lambda_R^{[\ell]} = \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = n$. Thus, the quotient diamond is given by $(\mathbb{Z}_4, \mathbb{Z}_4, \mathbb{Z}_1, \mathbb{Z}_4, \mathbb{Z}_1, \xi_4, 0)$, hence we are in case (III) of Example 4.2.2. We get the same 4 solutions as in (ii).

(6) For $\mathfrak{g}$ with root system E_6, we have $\pi_1 = \mathbb{Z}_3$. The simple roots are $\alpha_1, \ldots, \alpha_6$ and $d_i = 1$ for $1 \leq i \leq 6$. The symmetrized Cartan matrix $\tilde{C}$ is given below. The fundamental dominant weights λ_i are given as in [Hum72], Section 13.2, and λ_6 is the generator of the fundamental group $\mathbb{Z}_3$. The matrix id_W^R gives the coefficients of the fundamental dominant weights in the basis $\{\alpha_1, \ldots, \alpha_6\}$, and since $d_i = 1$ for all i, also the values (λ_i, λ_j) for $1 \leq i, j \leq 6$.

$$\tilde{C} = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix} \qquad id_W^R = \begin{pmatrix} \frac{4}{3} & 1 & \frac{5}{3} & 2 & \frac{4}{3} & \frac{2}{3} \\ 1 & 2 & 2 & 3 & 2 & 1 \\ \frac{5}{3} & 2 & \frac{10}{3} & 4 & \frac{8}{3} & \frac{4}{3} \\ 2 & 3 & 4 & 6 & 4 & 2 \\ \frac{4}{3} & 2 & \frac{8}{3} & 4 & \frac{10}{3} & \frac{5}{3} \\ \frac{2}{3} & 1 & \frac{4}{3} & 2 & \frac{5}{3} & \frac{4}{3} \end{pmatrix}$$

The lattice diamonds, depending on ℓ, are:

(i) For $3 \nmid \ell$ we have $A = \ell\Lambda_W$ and $B = C = D = \ell\Lambda_R$.

(ii) For $3 \mid \ell$ we have $A = C = \ell\Lambda_W$ and $B = D = \ell\Lambda_R$.

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations according to Example 4.2.2.

(i.a) For $3 \nmid \ell$ and ℓ odd it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 4$. Thus, the quotient diamond is given by $(\mathbb{Z}_3, \mathbb{Z}_3, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \xi_3, \lambda_6)$, hence we are in case (III) of Example 4.2.2. Since $\ell \equiv 2 \mod 3$ we get solutions $(d, k) = (1, 1)$, $(3, 1)$ and $(3, 3)$.

(i.b) For $3 \nmid \ell$ and ℓ even it is $\Lambda_R^{[\ell]} = \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 4$. Thus, the quotient diamond is given by $(\mathbb{Z}_3, \mathbb{Z}_3, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \xi_3, \lambda_6)$, and we are again in case (III) of Example 4.2.2. Since $\ell \equiv 1 \mod 3$ we get solutions $(d, k) = (1, 1)$, $(3, 2)$ and $(3, 3)$.

(ii.a) For $3 \mid \ell$ and ℓ odd it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 4$.

Thus, the quotient diamond is given by $(\mathbb{Z}_3, \mathbb{Z}_3, \mathbb{Z}_1, \mathbb{Z}_3, \mathbb{Z}_1, \xi_3, 0)$, hence we are in case (III) of Example 4.2.2. We get all 3 solutions $(d, k) = (3, 1)$, $(3, 2)$ and $(3, 3)$ on $\mathbb{Z}_3$.

(ii.b) For $3 \mid \ell$ and ℓ even it is $\Lambda_R^{[\ell]} = \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 4$. Thus, the quotient diamond is given by $(\mathbb{Z}_3, \mathbb{Z}_3, \mathbb{Z}_1, \mathbb{Z}_3, \mathbb{Z}_1, \xi_3, 0)$, and we the same solutions as in (ii.a).

(7) For $\mathfrak{g}$ with root system E_7, we have $\pi_1 = \mathbb{Z}_2$. The simple roots are $\alpha_1, \ldots, \alpha_7$ and $d_i = 1$ for $1 \leq i \leq 7$. The symmetrized Cartan matrix $\tilde{C}$ is given below. The fundamental dominant weights λ_i are given as in [Hum72], Section 13.2, and λ_7 is the generator of the fundamental group $\mathbb{Z}_2$. The matrix id_W^R gives the coefficients of the fundamental dominant weights in the basis $\{\alpha_1, \ldots, \alpha_7\}$, and since $d_i = 1$ for all i, also the values (λ_i, λ_j) for $1 \leq i, j \leq 7$.

$$\tilde{C} = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix} \qquad id_W^R = \begin{pmatrix} 2 & 2 & 3 & 4 & 3 & 2 & 1 \\ 2 & \frac{7}{2} & 4 & 6 & \frac{9}{2} & 3 & \frac{3}{2} \\ 3 & 4 & 6 & 8 & 6 & 4 & 2 \\ 4 & 6 & 8 & 12 & 9 & 6 & 3 \\ 3 & \frac{9}{2} & 6 & 9 & \frac{15}{2} & 5 & \frac{5}{2} \\ 2 & 3 & 4 & 6 & 5 & 4 & 2 \\ 1 & \frac{3}{2} & 2 & 3 & \frac{5}{2} & 2 & \frac{3}{2} \end{pmatrix}$$

The lattice diamonds, depending on ℓ, are:

(i) For odd ℓ we have $A = \ell\Lambda_W$ and $B = C = D = \ell\Lambda_R$.

(ii) For even ℓ we have $A = C = \ell\Lambda_W$ and $B = D = \ell\Lambda_R$.

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations according to Example 4.2.2.

(i) For ℓ odd it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 3$. Thus, the quotient diamond is given by $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \xi_2, \lambda_7)$ and we are in case (III) of Example 4.2.2. We get solutions $(d, k) = (1, 1)$ and $(2, 2)$.

(ii) For ℓ even it is $\Lambda_R^{[\ell]} = \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 3$. Thus, the quotient diamond is given by $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_1, \xi_2, 0)$ and we are again in case (III) of Example 4.2.2. We get all 2 solutions $(d, k) = (2, 1)$ and $(2, 2)$ on $\mathbb{Z}_2$.

(8) For $\mathfrak{g}$ with root system E_8, we have $\pi_1 = \mathbb{Z}_1$. The simple roots are $\alpha_1, \ldots, \alpha_8$ and $d_i = 1$ for $1 \leq i \leq 8$. The symmetrized Cartan matrix $\tilde{C}$ is given below. The fundamental dominant weights λ_i are given as in [Hum72], Section 13.2, and are roots. The matrix id_W^R gives the coefficients of the fundamental dominant weights in the basis $\{\alpha_1, \ldots, \alpha_8\}$, and since $d_i = 1$ for all i, also the values (λ_i, λ_j) for $1 \leq i, j \leq 8$.

$$\tilde{C} = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix} \qquad id_W^R = \begin{pmatrix} 4 & 5 & 7 & 10 & 8 & 6 & 4 & 2 \\ 5 & 8 & 10 & 15 & 12 & 9 & 6 & 3 \\ 7 & 10 & 14 & 20 & 16 & 12 & 8 & 4 \\ 10 & 15 & 20 & 30 & 24 & 18 & 12 & 6 \\ 8 & 12 & 16 & 24 & 20 & 15 & 10 & 5 \\ 6 & 9 & 12 & 18 & 15 & 12 & 8 & 4 \\ 4 & 6 & 8 & 12 & 10 & 8 & 6 & 3 \\ 2 & 3 & 4 & 6 & 5 & 4 & 3 & 2 \end{pmatrix}$$

The lattice diamonds, depending on ℓ, are:

(i) For odd ℓ we have $A = B = C = D = \ell\Lambda_W = \ell\Lambda_R$.

(ii) For even ℓ: same as in (i).

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations according to Example 4.2.2.

(i) For ℓ odd it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 2$. Thus, the quotient diamond is given by $(\mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, 1, 0)$ and we are in case (I) of Example 4.2.2. We get the only solution $(d, k) = (1, 1)$.

(ii) For ℓ even it is $\Lambda_R^{[\ell]} = \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 2$. We get the same diamond and solution as in (i).

(9) For $\mathfrak{g}$ with root system F_4, we have $\pi_1 = \mathbb{Z}_1$. The simple roots α_1, α_2 are long, α_3, α_4 are short, hence $d_1 = d_2 = 2$ and $d_3 = d_4 = 1$. The symmetrized Cartan matrix $\tilde{C}$ is given below. The fundamental dominant weights λ_i are given as in [Hum72], Section 13.2, and are roots. The matrix id_W^R gives the coefficients of the fundamental dominant weights in the basis $\{\alpha_1, \ldots, \alpha_4\}$.

$$\tilde{C} = \begin{pmatrix} 4 & -2 & 0 & 0 \\ -2 & 4 & -2 & 0 \\ 0 & -2 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix} \qquad id_W^R = \begin{pmatrix} 4 & 6 & 4 & 2 \\ 6 & 12 & 8 & 4 \\ 4 & 8 & 6 & 3 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

The lattice diamonds, depending on ℓ, are:

(i) For odd ℓ, we have $A = B = C = D = \ell\Lambda_W = \ell\Lambda_R$.

(ii) For even ℓ, we have $A = B = C = D = \ell\langle \frac{1}{2}\lambda_1, \frac{1}{2}\lambda_2, \lambda_3, \lambda_4 \rangle$.

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations according to Example 4.2.2.

(i) For ℓ odd it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 1$. Thus, the quotient diamond is given by $(\mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, 1, 0)$ and we are in case (I) of Example 4.2.2. We get the only solution $(d, k) = (1, 1)$.

(ii) For $\ell \equiv 2 \mod 4$ it is $\Lambda_R^{[\ell]} = \ell\langle \frac{1}{2}\alpha_1, \frac{1}{2}\alpha_2, \alpha_3, \alpha_4\rangle \neq \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 1$. We get the same diamond and solution as in (i).

(iii) For $\ell \equiv 0 \mod 4$ it is $\Lambda_R^{[\ell]} = \ell\langle \frac{1}{2}\alpha_1, \frac{1}{2}\alpha_2, \alpha_3, \alpha_4\rangle = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 1$. We get the same diamond and solution as in (i).

(10) For $\mathfrak{g}$ with root system G_2, we have $\pi_1 = \mathbb{Z}_1$. The simple root α_1 is short and α_2 is long, hence $d_1 = 1$ and $d_2 = 3$. The symmetrized Cartan matrix $\tilde{C}$ is given below. The fundamental dominant weights λ_i are given as in [Hum72], Section 13.2, and are roots. The matrix id_W^R gives the coefficients of the fundamental dominant weights in the basis $\{\alpha_1, \ldots, \alpha_2\}$.

$$\tilde{C} = \begin{pmatrix} 2 & -3 \\ -3 & 6 \end{pmatrix} \qquad id_W^R = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$$

The lattice diamonds, depending on ℓ, are:

(i) For $3 \nmid \ell$, we have $A = B = C = D = \ell\Lambda_W = \ell\Lambda_R$.

(ii) For $3 \mid \ell$, we have $A = B = C = D = \ell\langle \lambda_1, \frac{1}{3}\lambda_2\rangle$.

We calculate the quotient diamonds for the kernel $\Lambda' = \Lambda_R^{[\ell]}$ and compare it with Lusztig's kernel $2\Lambda_R^{(\ell)}$. We then determine the solutions of the corresponding diamond-equations according to Example 4.2.2.

(i.a) For $3 \nmid \ell$ and ℓ odd it is $\Lambda_R^{[\ell]} = \ell\Lambda_R \neq 2\ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 6$. Thus, the quotient diamond is given by $(\mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, 1, 0)$ and we are in case (I) of Example 4.2.2. We get the only solution $(d, k) = (1, 1)$.

(i.b) For $3 \nmid \ell$ and ℓ even it is $\Lambda_R^{[\ell]} = \ell\Lambda_R = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell$ and $m_{[n]} = 6$. We get the same diamond and solution as in (i.a).

(ii.a) For $3 \mid \ell$ and ℓ odd it is $\Lambda_R^{[\ell]} = \ell\langle \alpha_1, \frac{1}{3}\alpha_2\rangle \neq 2\ell\langle \alpha_1, \frac{1}{3}\alpha_2\rangle = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell/3$ and $m_{[n]} = 2$. We get the same diamond and solution as in (i.a).

(ii.b) For $3 \mid \ell$ and ℓ even it is $\Lambda_R^{[\ell]} = \ell\langle \alpha_1, \frac{1}{3}\alpha_2\rangle = 2\Lambda_R^{(\ell)}$, $\ell_{[n]} = \ell/3$ and $m_{[n]} = 2$. We get the same diamond and solution as in (i.a). ∎

4.4. Example: $u_q(\mathfrak{sl}_2)$

We give an familiar example. For $\mathfrak{g} = \mathfrak{sl}_2$ with root system A_1 the fundamental group is $\pi_1 = \mathbb{Z}_2$. Let α be the simple root, generating the root lattice Λ_R, and $\lambda = \frac{1}{2}\alpha$ the fundamental dominant weight, generating the weight lattice Λ_W. We will give the R-matrices for the quantum groups $u = u_q(\mathfrak{sl}_2, \Lambda_W, \Lambda')$ for ℓ-th root of unity q and lattice $\Lambda' = \Lambda_R^{[\ell]}$, which equals in the simply laced case $\ell\Lambda_R$. The possible subgroups H of π_1 (in the notation of Theorem 4.3.1) are only $\mathbb{Z}_1$ and $\mathbb{Z}_2$ which correspond to their preimage $\Lambda = \Lambda_R$ and Λ_W, respectively.

(1) Following the course of Chapter 2 we first give the quasi-R-matrix of u. The quasi R-matrix Θ depends only on the root lattice and exist in $u^+ \otimes u^-$ with Borel parts $u^\pm$, generated by E_α, F_α. With $\ell_\alpha = \ell/\gcd(\ell, 2d_\alpha) = \ell/\gcd(\ell, 2)$ we have

$$\Theta = \sum_{k=0}^{\ell_{\alpha-1}} (-1)^k \frac{(q-q^{-1})^k}{[k]_q!} q^{-k(k-1)/2} E_\alpha^k \otimes F_\alpha^k$$

and

$$\bar{\Theta} = \sum_{k=0}^{\ell_{\alpha-1}} \frac{(q-q^{-1})^k}{[k]_q!} q^{k(k-1)/2} E_\alpha^k \otimes F_\alpha^k,$$

with q-factorial $[k]_q!$ as in Definition 1.3.1.

(2) The R_0-ansatz of Theorem 2.1.6 and its modification in Lemma 2.2.1 gives the following group-equations for $\pi_1 = \mathbb{Z}_2$.

$$\begin{aligned}
g(0,0) &= g(0,0)g(0,0) + g(0,1)g(0,1), & g(0,0) &= g(0,0)g(0,0) + g(1,0)g(1,0)\\
g(0,1) &= g(0,0)g(0,1) + g(0,1)g(0,0), & g(1,0) &= g(0,0)g(1,0) + g(1,0)g(0,0)\\
g(1,0) &= g(1,0)g(1,0) + g(1,1)g(1,1), & g(0,1) &= g(0,1)g(0,1) + g(1,1)g(1,1)\\
g(1,1) &= g(1,0)g(1,1) + g(1,1)g(1,0), & g(1,1) &= g(0,1)g(1,1) + g(1,1)g(0,1)\\
1 &= g(0,0) + g(0,1), & 1 &= g(0,0) + g(1,0),
\end{aligned}$$

with $\pi_1 = \mathbb{Z}_2 = \{0, 1\}$.

(3) By Lemma 3.5.2, Example 3.5.5 and Theorem 3.5.6, the solutions of these group-equations are all functions

$$g\colon \pi_1 \times \pi_1 \to \mathbb{C},\ \ g(x,y) = \frac{1}{d}\xi^{\frac{xy}{(2/d)^2}} \delta_{(\frac{2}{d}|x)} \delta_{(\frac{2}{d}|y)} \equiv \frac{1}{d}\omega(x,y)\delta_{x\in H}\delta_{y\in H},$$

with $d \mid 2$ $(= N$, the order of $\pi_1)$, $H = (2/d)\mathbb{Z}_2$ the subgroups of order d in $\mathbb{Z}_2$ and ξ a d-th root of unity.

(4) The diamond-equations depend on the sublattices $A = \mathrm{Cent}^{[\ell]}(\Lambda_R) = \Lambda_W^{[\ell]}$, $B = \mathrm{Cent}^{[\ell]}(\Lambda_W)$, $C = \mathrm{Cent}^{[\ell]}(\Lambda_R) \cap \Lambda_R$ and $B \cap C = \Lambda_R^{[\ell]}$, hence on ℓ:

$$0 = \sum_{y_1+y_2=y, y_i\in\mathbb{Z}_2} \varphi_1(a)(y_1) g(x, y_1) g(x + \varphi_2(a), y_2), \tag{4.1.1}$$

$$0 = \sum_{x_1+x_2=x, x_i\in\mathbb{Z}_2} \varphi_1(a)(x_1) g(x_1, y) g(x_2, y + \varphi_2(a)), \tag{4.1.2}$$

$$0 = \sum_{y\in\mathbb{Z}_2} (\varphi_1(a)(y))^{-1}\, g(\varphi_2(a), y), \tag{4.1.3}$$

$$0 = \sum_{x\in\mathbb{Z}_2} (\varphi_1(a)(x))^{-1}\, g(x, \varphi_2(a)) \tag{4.1.4}$$

where, $\varphi_1(a)$ denotes the image of $a+B$ and $\varphi_2(a)$ denotes the image of $a+C$ for $a \in A$. The solutions of the diamond-equations are given by Lemma 4.2.1 and by Example 4.2.2 and Example 4.2.3, one has to check for which $d \mid 2$ and $1 \leq k \leq d$ the condition

$$\gcd(2, d\ell, k\ell - \frac{2}{d}) = 1, \tag{4.2.2}$$

is satisfied.

(5) For odd ℓ we have $A = \ell\Lambda_W$, $B = D = \ell\Lambda_R$ and $C = \ell/\gcd(2,\ell)\Lambda_R = \ell\Lambda_R$. The corresponding quotient diamond is

$$\begin{array}{ccccccc} & & & \mathbb{Z}_2 & & & \\ -1 \overset{\varphi_1}{\hookleftarrow} & & \diagup & & \diagdown & & \overset{\varphi_2}{\mapsto} \lambda_2 \\ & \mathbb{Z}_1 & & & & \mathbb{Z}_1 & \\ & & \diagdown & & \diagup & & \\ & & & \mathbb{Z}_1 & & & \end{array}$$

Condition (4.2.2) is satisfied for $(d,k) = (1,1)$ and $(d,k) = (2,2)$, hence we get the following solutions

$$\begin{aligned} H &= \mathbb{Z}_1, \qquad \omega \colon \mathbb{Z}_1 \times \mathbb{Z}_1 \to \mathbb{C}^\times,\ \omega(0,0) = 1, \\ H &= \mathbb{Z}_2, \qquad \omega \colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{C}^\times,\ \omega(1,1) = 1. \end{aligned}$$

(6) For even ℓ we have $A = \ell\Lambda_W$, $B = D = \ell\Lambda_R$ and $C = \ell/\gcd(2,\ell)\Lambda_R = (\ell/2)\Lambda_R = \ell\Lambda_W$ and the corresponding quotient diamond is

$$\begin{array}{ccccccc} & & & \mathbb{Z}_2 & & & \\ -1 \overset{\varphi_1}{\hookleftarrow} & & \diagup & & \diagdown & & \overset{\varphi_2}{\mapsto} 0 \\ & \mathbb{Z}_1 & & & & \mathbb{Z}_2 & \\ & & \diagdown & & \diagup & & \\ & & & \mathbb{Z}_1 & & & \end{array}$$

Here, condition (4.2.2) simplifies to $\gcd(d\ell, k\ell - 2/d) = 1$, which is satisfied for $(d,k) = (2,1)$ and $(d,k) = (2,2)$, hence we get the following solutions

$$H = \mathbb{Z}_2, \qquad \omega \colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{C}^\times,\ \omega(\lambda,\lambda) = \pm 1.$$

(7) The R_0-part is given by

$$R_0 = \frac{1}{|\Lambda/\Lambda_R^{[\ell]}|} \sum_{\mu,\nu \in \Lambda/\Lambda'} q^{-(\mu,\nu)}\, \omega(\bar{\mu}, \bar{\nu})\, K_\mu \otimes K_\nu,$$

for H and $\omega \colon H \times H \to \mathbb{C}^\times$ as above. We give below the explicit expression for the R-matrices.

(8) For odd ℓ the R-matrices are explicitly given by

$$\begin{aligned}
R &= \left(\frac{1}{\ell}\sum_{i,j=0}^{\ell-1} q^{-(i\alpha,j\alpha)}\, K_\alpha^i \,\otimes\, K_\alpha^j\right)\cdot\bar{\Theta}\\
&= \frac{1}{\ell}\sum_{k=0}^{\ell_\alpha-1}\sum_{i,j=0}^{\ell-1}\frac{(q-q^{-1})^k}{[k]_q!}q^{k(k-1)/2}q^{-2ij}\, K_\alpha^i E_\alpha^k \,\otimes\, K_\alpha^j F_\alpha^k\\
&= \frac{1}{\ell}\sum_{k=0}^{\ell_\alpha-1}\sum_{i,j=0}^{\ell-1}\frac{(q-q^{-1})^k}{[k]_q!}q^{k(k-1)/2+k(j-i)-2ij}\, E_\alpha^k K_\alpha^i \,\otimes\, F_\alpha^k K_\alpha^j
\end{aligned}$$

for the pairing ω on $H=\mathbb{Z}_1$, and

$$\begin{aligned}
R &= \left(\frac{1}{2\ell}\sum_{i,j=0}^{2\ell-1} q^{-(i\lambda,j\lambda)}\, K_\lambda^i \,\otimes\, K_\lambda^j\right)\cdot\bar{\Theta}\\
&= \frac{1}{2\ell}\sum_{k=0}^{\ell_\alpha-1}\sum_{i,j=0}^{2\ell-1}\frac{(q-q^{-1})^k}{[k]_q!}q^{k(k-1)/2}q^{-\frac{ij}{2}}\, K_\lambda^i E_\alpha^k \,\otimes\, K_\lambda^j F_\alpha^k\\
&= \frac{1}{2\ell}\sum_{k=0}^{\ell_\alpha-1}\sum_{i,j=0}^{2\ell-1}\frac{(q-q^{-1})^k}{[k]_q!}q^{k(k-1)/2+k(j-i)-\frac{ij}{2}}\, E_\alpha^k K_\lambda^i \,\otimes\, F_\alpha^k K_\lambda^j
\end{aligned}$$

for the pairing ω on $H=\mathbb{Z}_2$.

(9) For even ℓ the R-matrices are explicitly given by

$$\begin{aligned}
R &= \left(\frac{1}{2\ell}\sum_{i,j=0}^{2\ell-1} q^{-(i\lambda,j\lambda)}\,(\pm1)^{ij}\, K_\lambda^i \,\otimes\, K_\lambda^j\right)\cdot\bar{\Theta}\\
&= \frac{1}{2\ell}\sum_{k=0}^{\ell_\alpha-1}\sum_{i,j=0}^{2\ell-1}\frac{(q-q^{-1})^k}{[k]_q!}q^{k(k-1)/2}q^{-\frac{ij}{2}}\,(\pm1)^{ij}\, K_\lambda^i E_\alpha^k \,\otimes\, K_\lambda^j F_\alpha^k\\
&= \frac{1}{2\ell}\sum_{k=0}^{\ell_\alpha-1}\sum_{i,j=0}^{2\ell-1}\frac{(q-q^{-1})^k}{[k]_q!}q^{k(k-1)/2+k(j-i)-\frac{ij}{2}}\,(\pm1)^{ij}\, E_\alpha^k K_\lambda^i \,\otimes\, F_\alpha^k K_\lambda^j.
\end{aligned}$$

For the sign $+1$ this R-matrix is given in [FGST06, Thm. 4.1.1].

Appendix A

Maple calculation for the case $\pi_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$

For a Lie algebra $\mathfrak{g}$ with root system D_n, n even, the fundamental group $\pi_1 = \Lambda_W/\Lambda_R$ is the non-cyclic group $\mathbb{Z}_2 \times \mathbb{Z}_2$. In this case, the assumptions of Theorem 3.5.6 are not met and we use Maple in this exceptional case to determine all solutions of the group equations, cf. Definition 3.5.1.

$$g(x,y) = \sum_{y_1+y_2=y} g(x,y_1)g(x,y_2), \tag{3.5.1}$$

$$g(x,y) = \sum_{x_1+x_2=x} g(x_1,y)g(x_2,y), \tag{3.5.2}$$

$$1 = \sum_{y \in G} g(0,y), \tag{3.5.3}$$

$$1 = \sum_{x \in G} g(x,0). \tag{3.5.4}$$

To this end, we introduce the following notion. Let a, b, c the three elements of order 2 in $G := \mathbb{Z}_2 \times \mathbb{Z}_2 = \{0, a, b, c\}$. For $x, y \in G$ we write shortly g_{xy} for $g(x,y)$. In the following Maple calculation, we write the $|G|^2 = 16$ equations (3.5.1) in the array `eq1`, and the 16 equations (3.5.2) in `eq2`. We then solve the system of equations consisting of `eq1[i,j]` and `eq2[i,j]` for $1 \leq i, j \leq 4$ and equations (3.5.3) and (3.5.4). We then display the 35 solutions. These are the solutions presented in Example 3.5.7.

```
> i := 0: j := 0: eq1 := Array(1..4,1..4):
  for x in [0, a, b, c] do
    i := i+1: j:= 0:
    for y in [0, a, b, c] do
      j := j+1:
      if y=0 then
        k := 0: l:= a: m := b: n := c:
      elif y=a then
        k := a: l:= 0: m := c: n := b:
      elif y=b then
        k := b: l:= c: m := 0: n := a:
```

```
    elif y=c then
      k := c: l:= b: m := a: n := 0:
    end if:
    eq1[i,j] := cat(‘g_‘,x,y) = cat(‘g_‘,x,‘0‘)*cat(‘g_‘,x,k) +
                                cat(‘g_‘,x,‘a‘)*cat(‘g_‘,x,l) +
                                cat(‘g_‘,x,‘b‘)*cat(‘g_‘,x,m) +
                                cat(‘g_‘,x,‘c‘)*cat(‘g_‘,x,n);
    print(eq1[i,j]);
  end do:
end do:
i := 0: j := 0: eq2 := Array(1..4,1..4):
for x in [0, a, b, c] do
  i := i+1: j:= 0:
  for y in [0, a, b, c] do
    j := j+1:
    if x=0 then
      k := 0: l:= a: m := b: n := c:
    elif x=a then
      k := a: l:= 0: m := c: n := b:
    elif x=b then
      k := b: l:= c: m := 0: n := a:
    elif x=c then
      k := c: l:= b: m := a: n := 0:
    end if:
    eq2[i,j] := cat(‘g_‘,x,y) = cat(‘g_‘,‘0‘,y)*cat(‘g_‘,k,y) +
                                cat(‘g_‘,‘a‘,y)*cat(‘g_‘,l,y) +
                                cat(‘g_‘,‘b‘,y)*cat(‘g_‘,m,y) +
                                cat(‘g_‘,‘c‘,y)*cat(‘g_‘,n,y);
    print(eq2[i,j]);
  end do:
end do:
```

$$g_{00} = g_{00}^2 + g_{0a}^2 + g_{0b}^2 + g_{0c}^2$$
$$g_{0a} = 2g_{00}g_{0a} + 2g_{0b}g_{0c}$$
$$g_{0b} = 2g_{00}g_{0b} + 2g_{0a}g_{0c}$$
$$g_{0c} = 2g_{00}g_{0c} + 2g_{0a}g_{0b}$$
$$g_{a0} = g_{a0}^2 + g_{aa}^2 + g_{ab}^2 + g_{ac}^2$$
$$g_{aa} = 2g_{a0}g_{aa} + 2g_{ab}g_{ac}$$
$$g_{ab} = 2g_{a0}g_{ab} + 2g_{aa}g_{ac}$$
$$g_{ac} = 2g_{a0}g_{ac} + 2g_{aa}g_{ab}$$
$$g_{b0} = g_{b0}^2 + g_{ba}^2 + g_{bb}^2 + g_{bc}^2$$
$$g_{ba} = 2g_{b0}g_{ba} + 2g_{bb}g_{bc}$$

$$
\begin{aligned}
g_{bb} &= 2g_{b0}g_{bb} + 2g_{ba}g_{bc} \\
g_{bc} &= 2g_{b0}g_{bc} + 2g_{ba}g_{bb} \\
g_{c0} &= g_{c0}^2 + g_{ca}^2 + g_{cb}^2 + g_{cc}^2 \\
g_{ca} &= 2g_{c0}g_{ca} + 2g_{cb}g_{cc} \\
g_{cb} &= 2g_{c0}g_{cb} + 2g_{ca}g_{cc} \\
g_{cc} &= 2g_{c0}g_{cc} + 2g_{ca}g_{cb} \\
g_{00} &= g_{00}^2 + g_{a0}^2 + g_{b0}^2 + g_{c0}^2 \\
g_{0a} &= g_{0a}^2 + g_{aa}^2 + g_{ba}^2 + g_{ca}^2 \\
g_{0b} &= g_{0b}^2 + g_{ab}^2 + g_{bb}^2 + g_{cb}^2 \\
g_{0c} &= g_{0c}^2 + g_{ac}^2 + g_{bc}^2 + g_{cc}^2 \\
g_{a0} &= 2g_{00}g_{a0} + 2g_{b0}g_{c0} \\
g_{aa} &= 2g_{0a}g_{aa} + 2g_{ba}g_{ca} \\
g_{ab} &= 2g_{0b}g_{ab} + 2g_{bb}g_{cb} \\
g_{ac} &= 2g_{0c}g_{ac} + 2g_{bc}g_{cc} \\
g_{b0} &= 2g_{00}g_{b0} + 2g_{a0}g_{c0} \\
g_{ba} &= 2g_{0a}g_{ba} + 2g_{aa}g_{ca} \\
g_{bb} &= 2g_{0b}g_{bb} + 2g_{ab}g_{cb} \\
g_{bc} &= 2g_{0c}g_{bc} + 2g_{ac}g_{cc} \\
g_{c0} &= 2g_{00}g_{c0} + 2g_{a0}g_{b0} \\
g_{ca} &= 2g_{0a}g_{ca} + 2g_{aa}g_{ba} \\
g_{cb} &= 2g_{0b}g_{cb} + 2g_{ab}g_{bb} \\
g_{cc} &= 2g_{0c}g_{cc} + 2g_{ac}g_{bc}
\end{aligned}
$$

```
> solutions:=[solve({seq(seq(eq1[i,j],j=1..4),i=1..4),
                     seq(seq(eq2[i,j],j=1..4),i=1..4),
                     1 = g_00 + g_0a + g_0b + g_0c,
                     1 = g_00 + g_a0 + g_b0 + g_c0
                    })]:
> nops(solutions);
```

$$35$$

```
> for i from 1 to 35 do
    print(solutions[i])
  end do;
```

$$
\begin{gathered}
\{g_{00} = 1, g_{0a} = 0, g_{0b} = 0, g_{0c} = 0, g_{a0} = 0, g_{aa} = 0, g_{ab} = 0, g_{ac} = 0, \\
g_{b0} = 0, g_{ba} = 0, g_{bb} = 0, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\} \\
\Big\{g_{00} = \frac{1}{2}, g_{0a} = \frac{1}{0}, g_{0b} = 0, g_{0c} = 0, g_{a0} = \frac{1}{2}, g_{aa} = \frac{1}{2}, g_{ab} = 0, g_{ac} = 0,
\end{gathered}
$$

$$g_{b0} = 0, g_{ba} = 0, g_{bb} = 0, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = \frac{1}{0}, g_{0b} = 0, g_{0c} = 0, g_{a0} = \frac{1}{2}, g_{aa} = -\frac{1}{2}, g_{ab} = 0, g_{ac} = 0,\right.$$
$$g_{b0} = 0, g_{ba} = 0, g_{bb} = 0, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = 0, g_{0b} = \frac{1}{2}, g_{0c} = 0, g_{a0} = \frac{1}{2}, g_{aa} = 0, g_{ab} = \frac{1}{2}, g_{ac} = 0,\right.$$
$$g_{b0} = 0, g_{ba} = 0, g_{bb} = 0, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = 0, g_{0b} = \frac{1}{2}, g_{0c} = 0, g_{a0} = \frac{1}{2}, g_{aa} = 0, g_{ab} = -\frac{1}{2}, g_{ac} = 0,\right.$$
$$g_{b0} = 0, g_{ba} = 0, g_{bb} = 0, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = 0, g_{0b} = 0, g_{0c} = \frac{1}{2}, g_{a0} = \frac{1}{2}, g_{aa} = 0, g_{ab} = 0, g_{ac} = \frac{1}{2},\right.$$
$$g_{b0} = 0, g_{ba} = 0, g_{bb} = 0, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = 0, g_{0b} = 0, g_{0c} = \frac{1}{2}, g_{a0} = \frac{1}{2}, g_{aa} = 0, g_{ab} = 0, g_{ac} = -\frac{1}{2},\right.$$
$$g_{b0} = 0, g_{ba} = 0, g_{bb} = 0, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = \frac{1}{2}, g_{0b} = 0, g_{0c} = 0, g_{a0} = 0, g_{aa} = 0, g_{ab} = 0, g_{ac} = 0,\right.$$
$$\left.g_{b0} = \frac{1}{2}, g_{ba} = \frac{1}{2}, g_{bb} = 0, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\right\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = \frac{1}{2}, g_{0b} = 0, g_{0c} = 0, g_{a0} = 0, g_{aa} = 0, g_{ab} = 0, g_{ac} = 0,\right.$$
$$\left.g_{b0} = \frac{1}{2}, g_{ba} = -\frac{1}{2}, g_{bb} = 0, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\right\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = 0, g_{0b} = \frac{1}{2}, g_{0c} = 0, g_{a0} = 0, g_{aa} = 0, g_{ab} = 0, g_{ac} = 0,\right.$$
$$\left.g_{b0} = \frac{1}{2}, g_{ba} = 0, g_{bb} = \frac{1}{2}, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\right\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = 0, g_{0b} = \frac{1}{2}, g_{0c} = 0, g_{a0} = 0, g_{aa} = 0, g_{ab} = 0, g_{ac} = 0,\right.$$
$$\left.g_{b0} = \frac{1}{2}, g_{ba} = 0, g_{bb} = -\frac{1}{2}, g_{bc} = 0, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\right\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = 0, g_{0b} = 0, g_{0c} = \frac{1}{2}, g_{a0} = 0, g_{aa} = 0, g_{ab} = 0, g_{ac} = 0,\right.$$
$$\left.g_{b0} = \frac{1}{2}, g_{ba} = 0, g_{bb} = 0, g_{bc} = \frac{1}{2}, g_{c0} = 0, g_{ca} = 0, g_{cb} = 0, g_{cc} = 0\right\}$$

$$\left\{g_{00} = \frac{1}{2}, g_{0a} = 0, g_{0b} = 0, g_{0c} = \frac{1}{2}, g_{a0} = 0, g_{aa} = 0, g_{ab} = 0, g_{ac} = 0,\right.$$

$$g_{b0}=\frac{1}{2},g_{ba}=0,g_{bb}=0,g_{bc}=-\frac{1}{2},g_{c0}=0,g_{ca}=0,g_{cb}=0,g_{cc}=0\Big\}$$

$$\Big\{g_{00}=\frac{1}{2},g_{0a}=\frac{1}{2},g_{0b}=0,g_{0c}=0,g_{a0}=0,g_{aa}=0,g_{ab}=0,g_{ac}=0,$$

$$g_{b0}=0,g_{ba}=0,g_{bb}=0,g_{bc}=0,g_{c0}=\frac{1}{2},g_{ca}=\frac{1}{2},g_{cb}=0,g_{cc}=0\Big\}$$

$$\Big\{g_{00}=\frac{1}{2},g_{0a}=\frac{1}{2},g_{0b}=0,g_{0c}=0,g_{a0}=0,g_{aa}=0,g_{ab}=0,g_{ac}=0,$$

$$g_{b0}=0,g_{ba}=0,g_{bb}=0,g_{bc}=0,g_{c0}=\frac{1}{2},g_{ca}=-\frac{1}{2},g_{cb}=0,g_{cc}=0\Big\}$$

$$\Big\{g_{00}=\frac{1}{2},g_{0a}=0,g_{0b}=\frac{1}{2},g_{0c}=0,g_{a0}=0,g_{aa}=0,g_{ab}=0,g_{ac}=0,$$

$$g_{b0}=0,g_{ba}=0,g_{bb}=0,g_{bc}=0,g_{c0}=\frac{1}{2},g_{ca}=0,g_{cb}=\frac{1}{2},g_{cc}=0\Big\}$$

$$\Big\{g_{00}=\frac{1}{2},g_{0a}=0,g_{0b}=\frac{1}{2},g_{0c}=0,g_{a0}=0,g_{aa}=0,g_{ab}=0,g_{ac}=0,$$

$$g_{b0}=0,g_{ba}=0,g_{bb}=0,g_{bc}=0,g_{c0}=\frac{1}{2},g_{ca}=0,g_{cb}=-\frac{1}{2},g_{cc}=0\Big\}$$

$$\Big\{g_{00}=\frac{1}{2},g_{0a}=0,g_{0b}=0,g_{0c}=\frac{1}{2},g_{a0}=0,g_{aa}=0,g_{ab}=0,g_{ac}=0,$$

$$g_{b0}=0,g_{ba}=0,g_{bb}=0,g_{bc}=0,g_{c0}=\frac{1}{2},g_{ca}=0,g_{cb}=0,g_{cc}=\frac{1}{2}\Big\}$$

$$\Big\{g_{00}=\frac{1}{2},g_{0a}=0,g_{0b}=0,g_{0c}=\frac{1}{2},g_{a0}=0,g_{aa}=0,g_{ab}=0,g_{ac}=0,$$

$$g_{b0}=0,g_{ba}=0,g_{bb}=0,g_{bc}=0,g_{c0}=\frac{1}{2},g_{ca}=0,g_{cb}=0,g_{cc}=-\frac{1}{2}\Big\}$$

$$\Big\{g_{00}=\frac{1}{4},g_{0a}=\frac{1}{4},g_{0b}=\frac{1}{4},g_{0c}=\frac{1}{4},g_{a0}=\frac{1}{4},g_{aa}=\frac{1}{4},g_{ab}=-\frac{1}{4},g_{ac}=-\frac{1}{4},$$

$$g_{b0}=\frac{1}{4},g_{ba}=\frac{1}{4},g_{bb}=\frac{1}{4},g_{bc}=\frac{1}{4},g_{c0}=\frac{1}{4},g_{ca}=\frac{1}{4},g_{cb}=-\frac{1}{4},g_{cc}=-\frac{1}{4}\Big\}$$

$$\Big\{g_{00}=\frac{1}{4},g_{0a}=\frac{1}{4},g_{0b}=\frac{1}{4},g_{0c}=\frac{1}{4},g_{a0}=\frac{1}{4},g_{aa}=-\frac{1}{4},g_{ab}=-\frac{1}{4},g_{ac}=\frac{1}{4},$$

$$g_{b0}=\frac{1}{4},g_{ba}=\frac{1}{4},g_{bb}=\frac{1}{4},g_{bc}=\frac{1}{4},g_{c0}=\frac{1}{4},g_{ca}=-\frac{1}{4},g_{cb}=-\frac{1}{4},g_{cc}=-\frac{1}{4}\Big\}$$

$$\Big\{g_{00}=\frac{1}{4},g_{0a}=\frac{1}{4},g_{0b}=\frac{1}{4},g_{0c}=\frac{1}{4},g_{a0}=\frac{1}{4},g_{aa}=\frac{1}{4},g_{ab}=\frac{1}{4},g_{ac}=\frac{1}{4},$$

$$g_{b0}=\frac{1}{4},g_{ba}=\frac{1}{4},g_{bb}=-\frac{1}{4},g_{bc}=-\frac{1}{4},g_{c0}=\frac{1}{4},g_{ca}=\frac{1}{4},g_{cb}=-\frac{1}{4},g_{cc}=-\frac{1}{4}\Big\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = -\frac{1}{4}, g_{ab} = \frac{1}{4}, g_{ac} = -\frac{1}{4},\right.$$
$$\left. g_{b0} = \frac{1}{4}, g_{ba} = \frac{1}{4}, g_{bb} = -\frac{1}{4}, g_{bc} = -\frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = -\frac{1}{4}, g_{cb} = -\frac{1}{4}, g_{cc} = \frac{1}{4}\right\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = \frac{1}{4}, g_{ab} = \frac{1}{4}, g_{ac} = \frac{1}{4},\right.$$
$$\left. g_{b0} = \frac{1}{4}, g_{ba} = \frac{1}{4}, g_{bb} = \frac{1}{4}, g_{bc} = \frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = \frac{1}{4}, g_{cb} = \frac{1}{4}, g_{cc} = \frac{1}{4}\right\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = -\frac{1}{4}, g_{ab} = \frac{1}{4}, g_{ac} = -\frac{1}{4},\right.$$
$$\left. g_{b0} = \frac{1}{4}, g_{ba} = \frac{1}{4}, g_{bb} = \frac{1}{4}, g_{bc} = \frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = -\frac{1}{4}, g_{cb} = \frac{1}{4}, g_{cc} = -\frac{1}{4}\right\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = -\frac{1}{4}, g_{ab} = -\frac{1}{4}, g_{ac} = \frac{1}{4},\right.$$
$$\left. g_{b0} = \frac{1}{4}, g_{ba} = -\frac{1}{4}, g_{bb} = -\frac{1}{4}, g_{bc} = \frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = \frac{1}{4}, g_{cb} = \frac{1}{4}, g_{cc} = \frac{1}{4}\right\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = \frac{1}{4}, g_{ab} = -\frac{1}{4}, g_{ac} = -\frac{1}{4},\right.$$
$$\left. g_{b0} = \frac{1}{4}, g_{ba} = -\frac{1}{4}, g_{bb} = -\frac{1}{4}, g_{bc} = \frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = -\frac{1}{4}, g_{cb} = \frac{1}{4}, g_{cc} = -\frac{1}{4}\right\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = -\frac{1}{4}, g_{ab} = \frac{1}{4}, g_{ac} = -\frac{1}{4},\right.$$
$$\left. g_{b0} = \frac{1}{4}, g_{ba} = -\frac{1}{4}, g_{bb} = -\frac{1}{4}, g_{bc} = \frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = \frac{1}{4}, g_{cb} = -\frac{1}{4}, g_{cc} = -\frac{1}{4}\right\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = \frac{1}{4}, g_{ab} = \frac{1}{4}, g_{ac} = \frac{1}{4},\right.$$
$$\left. g_{b0} = \frac{1}{4}, g_{ba} = -\frac{1}{4}, g_{bb} = -\frac{1}{4}, g_{bc} = \frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = -\frac{1}{4}, g_{cb} = -\frac{1}{4}, g_{cc} = \frac{1}{4}\right\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = -\frac{1}{4}, g_{ab} = \frac{1}{4}, g_{ac} = -\frac{1}{4},\right.$$
$$\left. g_{b0} = \frac{1}{4}, g_{ba} = -\frac{1}{4}, g_{bb} = \frac{1}{4}, g_{bc} = -\frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = \frac{1}{4}, g_{cb} = \frac{1}{4}, g_{cc} = \frac{1}{4}\right\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = \frac{1}{4}, g_{ab} = \frac{1}{4}, g_{ac} = \frac{1}{4},\right.$$
$$\left. g_{b0} = \frac{1}{4}, g_{ba} = -\frac{1}{4}, g_{bb} = \frac{1}{4}, g_{bc} = -\frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = -\frac{1}{4}, g_{cb} = \frac{1}{4}, g_{cc} = -\frac{1}{4}\right\}$$

$$\left\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = -\frac{1}{4}, g_{ab} = -\frac{1}{4}, g_{ac} = \frac{1}{4},\right.$$

$$g_{b0} = \frac{1}{4}, g_{ba} = -\frac{1}{4}, g_{bb} = \frac{1}{4}, g_{bc} = -\frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = \frac{1}{4}, g_{cb} = -\frac{1}{4}, g_{cc} = -\frac{1}{4}\Big\}$$

$$\Big\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = \frac{1}{4}, g_{ab} = -\frac{1}{4}, g_{ac} = -\frac{1}{4},$$

$$g_{b0} = \frac{1}{4}, g_{ba} = -\frac{1}{4}, g_{bb} = \frac{1}{4}, g_{bc} = -\frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = -\frac{1}{4}, g_{cb} = -\frac{1}{4}, g_{cc} = \frac{1}{4}\Big\}$$

$$\Big\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = \frac{1}{4}, g_{ab} = -\frac{1}{4}, g_{ac} = -\frac{1}{4},$$

$$g_{b0} = \frac{1}{4}, g_{ba} = \frac{1}{4}, g_{bb} = -\frac{1}{4}, g_{bc} = -\frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = \frac{1}{4}, g_{cb} = \frac{1}{4}, g_{cc} = \frac{1}{4}\Big\}$$

$$\Big\{g_{00} = \frac{1}{4}, g_{0a} = \frac{1}{4}, g_{0b} = \frac{1}{4}, g_{0c} = \frac{1}{4}, g_{a0} = \frac{1}{4}, g_{aa} = -\frac{1}{4}, g_{ab} = -\frac{1}{4}, g_{ac} = \frac{1}{4},$$

$$g_{b0} = \frac{1}{4}, g_{ba} = \frac{1}{4}, g_{bb} = -\frac{1}{4}, g_{bc} = -\frac{1}{4}, g_{c0} = \frac{1}{4}, g_{ca} = -\frac{1}{4}, g_{cb} = \frac{1}{4}, g_{cc} = -\frac{1}{4}\Big\}$$

Appendix B

Category theory

Every quasitriangular Hopf algebra H (cf. Definition 1.1.1) gives rise to a braided monoidal category, namely its representation (or module) category $H-$mod (and vice versa). So, for the convenience of the reader, in the following we recall the definition of these categorial terms. A standard reference for this is [MacL98], we follow the exposition in [Kas95].

Definition B.1. (1) A *category* $\mathcal{C}$ consists

(a) of a class of objects $\mathrm{Obj}(\mathcal{C})$, whose entries are called the *objects* of the category.

(b) a class $\mathrm{Hom}(\mathcal{C})$, whose entries are called *morphisms* of the category.

(c) Maps

$$\begin{aligned} id &: \mathrm{Obj}(\mathcal{C}) \to \mathrm{Hom}(\mathcal{C}), \\ s,\, t &: \mathrm{Hom}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{C}), \\ o &: \mathrm{Hom}(\mathcal{C}) \times_{\mathrm{Obj}(\mathcal{C})} \mathrm{Hom}(\mathcal{C}) \to \mathrm{Hom}(\mathcal{C}), \end{aligned}$$

such that

- $s(id_V) = t(id_V) = V$ for all $V \in \mathrm{Obj}(\mathcal{C})$,
- $id_{t(f)} \circ f = f \circ id_{s(f)} = f$ for all $f \in \mathrm{Hom}(\mathcal{C})$,
- for all $f, g, h \in \mathrm{Hom}(\mathcal{C})$ with $t(f) = s(g)$ and $t(g) = s(h)$, the associativity identity $(h \circ g) \circ f = h \circ (g \circ f)$ holds.

(2) Let $\mathcal{C}$ and $\mathcal{C}'$ be categories. A *functor* $F : \mathcal{C} \to \mathcal{C}'$ consists of two maps:

$$\begin{aligned} F &: \mathrm{Obj}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{C}'), \\ F &: \mathrm{Hom}(\mathcal{C}) \to \mathrm{Hom}(\mathcal{C}'), \end{aligned}$$

such that

- $F(id_V) = id_{F(V)}$ for all objects $V \in \mathrm{Obj}(\mathcal{C})$,
- $s(F(f)) = F(s(f))$ and $t(F(f)) = F(t(f))$ for all morphisms $f \in \mathrm{Hom}(\mathcal{C})$,

- For any pair f, g of composable morphisms, we have

$$F(g \circ f) = F(g) \circ F(f).$$

Two functors $F\colon \mathcal{C} \to \mathcal{C}'$, $G\colon \mathcal{C}' \to \mathcal{C}''$ can be concatenated to a functor $G \circ F\colon \mathcal{C} \to \mathcal{C}''$.

(3) Let $F, G\colon \mathcal{C} \to \mathcal{C}'$ be functors. A *natural transformation*

$$\eta\colon F \to G$$

is a family of morphisms

$$\eta_V\colon F(V) \to G(V)$$

in $\mathcal{C}'$, indexed by $V \in \mathrm{Obj}(\mathcal{C})$, such that for any morphism $f\colon V \to W$ in $\mathcal{C}$ the diagram

$$\begin{tikzcd}
F(V) \arrow[r, "\eta_V"] \arrow[d, "F(f)"'] & G(V) \arrow[d, "G(f)"] \\
F(W) \arrow[r, "\eta_W"'] & G(W)
\end{tikzcd}$$

in $\mathcal{C}'$ commutes.

If η_V is, for each $V \in \mathrm{Obj}(\mathcal{C})$ an isomorphism, then $\eta\colon F \to G$ is called a *natural isomorphism.*

(4) A functor

$$F\colon \mathcal{C} \to \mathcal{D}$$

is called an *equivalence of categories*, if there is a functor

$$G\colon \mathcal{D} \to \mathcal{C}$$

and natural isomorphisms

$$\eta\colon id_{\mathcal{D}} \to FG,$$
$$\theta\colon GF \to id_{\mathcal{C}}.$$

We introduce the notion of a monoidal category and monoidal functor. Before that, we give the definition of the Cartesian product of categories.

Definition B.2. The *Cartesian product* of two categories $\mathcal{C}, \mathcal{D}$ is defined as the category $\mathcal{C} \times \mathcal{D}$ whose objects are pairs $(V, W) \in \mathrm{Obj}(\mathcal{C}) \times \mathrm{Obj}(\mathcal{D})$ and whose morphisms are given by the Cartesian product of sets: $\mathrm{Hom}_{\mathcal{C}\times\mathcal{D}}((V, W), (V'W')) = \mathrm{Hom}_{\mathcal{C}}(V, V') \times \mathrm{Hom}_{\mathcal{D}}(W, W')$.

Definition B.3. (1) Let $\mathcal{C}$ be a category and $\otimes\colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ a functor, called a *tensor product.* This associates to any pair (V, W) of objects an object $V \otimes W$ and to any pair or morphisms (f, g) a morphism $f \otimes g$ with $s(f \otimes g) = s(f) \otimes s(g)$ and $t(f \otimes g) = t(f) \otimes t(g)$. In particular, $id_{V\otimes W} = id_V \otimes id_W$ and for composable morphisms $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$.

(2) A *monoidal category* (or *tensor category*) consists of a category $(\mathcal{C}, \otimes)$ with tensor product, an object $\mathbf{1} \in \mathcal{C}$, called the *tensor unit*, and natural isomorphism, called the *associator*,

$$a\colon \otimes \circ (\otimes \times id) \to \otimes \circ (id \times \otimes)$$

of functors $\mathcal{C} \times \mathcal{C} \times \to \mathcal{C}$ and natural isomorphisms

$$r\colon id \otimes \mathbf{1} \to id \quad \text{and} \quad l\colon \mathbf{1} \otimes id \to id$$

such that the following axioms hold:

- The *pentagon axiom*: for all quadruples of objects $U, V, W, X \in \mathrm{Obj}(\mathcal{C})$ the following diagram commutes

$$\begin{tikzcd}
 & (U \otimes V) \otimes (W \otimes X) \arrow[dr, "a_{U,V,W\otimes X}"] & \\
((U \otimes V) \otimes W) \otimes X \arrow[ur, "a_{U\otimes V,W,X}"] \arrow[d, "a_{U,V,W} \otimes id_X"'] & & U \otimes (V \otimes (W \otimes X)) \\
(U \otimes (V \otimes W)) \otimes X \arrow[rr, "a_{U,V\otimes W,X}"'] & & U \otimes ((V \otimes W) \otimes X) \arrow[u, "id_U \otimes a_{V,W,X}"']
\end{tikzcd}$$

- The *triangle axiom*: for all pairs of objects $V, W \in \mathrm{Obj}(\mathcal{C})$ the following diagram commutes

$$\begin{tikzcd}
(V \otimes \mathbf{1}) \otimes W \arrow[rr, "a_{V,\mathbf{1},W}"] \arrow[dr, "r_V \otimes id_W"'] & & V \otimes (\mathbf{1} \otimes W) \arrow[dl, "id_V \otimes l_W"] \\
 & V \otimes W &
\end{tikzcd}$$

A monoidal (tensor) category is called *strict*, if the natural transformations a, l and r are the identity.

(3) Let $(\mathcal{C}, \otimes_{\mathcal{C}}, \mathbf{1}_{\mathcal{C}}, a_{\mathcal{C}}, l_{\mathcal{C}}, r_{\mathcal{C}})$ and $(\mathcal{D}, \otimes_{\mathcal{D}}, \mathbf{1}_{\mathcal{D}}, a_{\mathcal{D}}, l_{\mathcal{D}}, r_{\mathcal{D}})$ be tensor categories. A *monoidal* (or *tensor*) *functor* from $\mathcal{C}$ to $\mathcal{D}$ is a triple $(F, \varphi_0, \varphi_2)$ consisting of

(a) a functor $F\colon \mathcal{C} \to \mathcal{D}$,

(b) an isomorphism $\varphi_0\colon \mathbf{1}_{\mathcal{D}} \to F(\mathbf{1}_{\mathcal{C}})$ in the category $\mathcal{D}$,

(c) a natural isomorphism $\varphi_2\colon \otimes_{\mathcal{D}} \circ (F \times F) \to F \circ \otimes_{\mathcal{C}}$

of functors $\mathcal{C} \times \mathcal{C} \to \mathcal{D}$. These data have to obey a series of constraints expressed by commuting diagrams:

- Compatibility with the associativity constraint:

$$
\begin{tikzcd}
(F(U) \otimes F(V)) \otimes F(W) \arrow[rr, "a_{F(U),F(V),F(W)}"] \arrow[d, "\varphi_2(U,V) \otimes \mathrm{id}_{F(W)}"'] & & F(U) \otimes (F(V) \otimes F(W)) \arrow[d, "\mathrm{id}_{F(U)} \otimes \varphi_2(V,W)"] \\
F(U \otimes V) \otimes F(W) \arrow[d, "\varphi_2(U \otimes V, W)"'] & & F(U) \otimes F(V \otimes W) \arrow[d, "\varphi_2(U, V \otimes W)"] \\
F((U \otimes V) \otimes W) \arrow[rr, "F(a_{U,V,W})"'] & & F(U \otimes (V \otimes W))
\end{tikzcd}
$$

- Compatibility with the left unit constraint:

$$
\begin{tikzcd}
\mathbf{1}_{\mathcal{D}} \otimes F(U) \arrow[r, "l_{F(U)}"] \arrow[d, "\varphi_0 \otimes \mathrm{id}_{F(U)}"'] & F(U) \\
F(\mathbf{1}_{\mathcal{C}}) \otimes F(U) \arrow[r, "\varphi_2(\mathbf{1}_{\mathcal{C}}, U)"] & F(\mathbf{1}_{\mathcal{C}} \otimes U) \arrow[u, "F(l_U)"']
\end{tikzcd}
$$

- Compatibility with the right unit constraint:

$$
\begin{tikzcd}
F(U) \otimes \mathbf{1}_{\mathcal{D}} \arrow[r, "r_{F(U)}"] \arrow[d, "\mathrm{id}_{F(U)} \otimes \varphi_0"'] & F(U) \\
F(U) \otimes F(\mathbf{1}_{\mathcal{C}}) \arrow[r, "\varphi_2(U, \mathbf{1}_{\mathcal{C}})"] & F(U \otimes \mathbf{1}_{\mathcal{C}}) \arrow[u, "F(r_U)"']
\end{tikzcd}
$$

(4) A *monoidal natural transformation*

$$\eta\colon (F, \varphi_0, \varphi_2) \to (F', \varphi_0', \varphi_2')$$

between tensor functors is a natural transformation $\eta\colon F \to F'$ such that the following diagrams

$$
\begin{tikzcd}
 & F(\mathbf{1}_{\mathcal{C}}) \arrow[dd, "\eta_{\mathbf{1}_{\mathcal{C}}}"] \\
\mathbf{1}_{\mathcal{D}} \arrow[ur, "\varphi_0"] \arrow[dr, "\varphi_0'"'] & \\
 & F'(\mathbf{1}_{\mathcal{C}})
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
F(U) \otimes F(V) \arrow[r, "\varphi_2(U,V)"] \arrow[d, "\eta_U \otimes \eta_V"] & F(U \otimes V) \arrow[d, "\eta_{U \otimes V}"] \\
F'(U) \otimes F'(V) \arrow[r, "\varphi_2'(U,V)"] & F'(U \otimes V)
\end{tikzcd}
$$

commute for all pairs (U, V) of objects.

For a tensor product $\otimes\colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ we define the functor $\otimes^{\mathrm{opp}}$ by $\otimes \circ \tau$, i.e.

$$V \otimes^{\mathrm{opp}} W := W \otimes V \quad \text{and} \quad f \otimes^{\mathrm{opp}} g := g \otimes f$$

for all objects V, W and morphisms f, g in $\mathcal{C}$. This defines a tensor product: For a given associator a for then tensor product $\otimes$ the natural isomorphism $a^{\mathrm{opp}}_{U,V,W} := a^{-1}_{W,V,U}$ is an associator for the tensor product $\otimes^{\mathrm{opp}}$. Similarly, one obtains left and right unit constraints for $\otimes^{\mathrm{opp}}$. We now introduce the notion of a braided category, braided functor and the equivalence of braided categories.

Definition B.4. (1) Let $\mathcal{C}$ be a monoidal category. Assume at first, $\mathcal{C}$ is strict. A *braiding* is is a natural isomorphism

$$c\colon \otimes \to \otimes^{\mathrm{opp}}$$

of functors $\mathcal{C} \times \mathcal{C} \to \mathcal{C}$, such that for all objects U, V, W the compatibility relations

$$\begin{aligned} c_{U,V\otimes W} &= (id_V \otimes c_{U,W}) \circ (c_{U,V} \otimes id_U) \\ c_{U\otimes V,W} &= (c_{U,W} \otimes id_V) \circ (id_U \otimes c_{V,W}) \end{aligned}$$

with the tensor product hold. If the category is not strict, the following two *hexagon axioms* have to hold:

$$\begin{tikzcd}
 & U \otimes (V \otimes W) \arrow[r, "c_{U,V\otimes W}"] & (V \otimes W) \otimes U \arrow[dr, "a_{V,W,U}"] & \\
(U \otimes V) \otimes W \arrow[ur, "a_{U,V,W}"] \arrow[dr, "c_{U,V} \otimes id_W"'] & & & V \otimes (W \otimes U) \\
 & (V \otimes U) \otimes W \arrow[r, "a_{V,U,W}"] & V \otimes (U \otimes W) \arrow[ur, "id_V \otimes c_{U,W}"'] &
\end{tikzcd}$$

and

$$\begin{tikzcd}
 & (U \otimes V) \otimes W \arrow[r, "c_{U\otimes V,W}"] & W \otimes (U \otimes V) \arrow[dr, "a^{-1}_{W,U,V}"] & \\
U \otimes (V \otimes W) \arrow[ur, "a^{-1}_{U,V,W}"] \arrow[dr, "id_U \otimes c_{V,W}"'] & & & (W \otimes U) \otimes V \\
 & U \otimes (W \otimes V) \arrow[r, "a^{-1}_{U,W,V}"] & (U \otimes W) \otimes V \arrow[ur, "c_{U,W} \otimes id_V"'] &
\end{tikzcd}$$

(2) A *braided tensor category* is a tensor category together with the structure of a braiding.

Summary

Quasitriangular Hopf algebras, i.e. Hopf algebras with an (universal) R-matrix, have braided categories of their modules. In particular, quasitriangular quantum groups yield ribbon categories, which have many interesting applications, especially in low-dimensional topology and topological quantum field theories.

In this thesis we construct new universal R-matrices of the small quantum groups $u_q(\mathfrak{g})$ and extensions thereof. Here, $\mathfrak{g}$ is always a finite-dimensional complex, simple Lie algebra and q is an ℓ-th root of unity for an arbitrary integer $\ell > 2$. The first chapter of this thesis provides the necessary algebraic notions and gives the definition of the quantum groups in interest. Since in general the small quantum group is not quasitriangular, i.e. there exist no R-matrix, we consider certain extensions of the usual quantum group $u_q(\mathfrak{g})$, parametrized by a Lie theoretic input datum, namely a lattice Λ, containing the root lattice Λ_R and contained in the weight lattice Λ_W of $\mathfrak{g}$. This leads to the notion of $u_q(\mathfrak{g}, \Lambda, \Lambda')$ for the extension by Λ of the small quantum group $u_q(\mathfrak{g}, \Lambda')$. Here, the lattice $\Lambda' \subset \Lambda_R$ determines a certain quotient in the construction of the quantum group.

In the second chapter we review the ansatz $R = R_0\bar{\Theta}$ for R-matrices by Lusztig. This ansatz introduces a fixed element, the so-called quasi-R-matrix Θ, which is an intertwiner between the comultiplication Δ and a new comultiplication $\bar{\Delta}$, obtained by conjugating with a certain antilinear involution. The free element R_0 is an intertwiner for $\bar{\Delta}$ and the opposed comultiplication Δ^{opp}. Eric Müller gives in his dissertation an ansatz and equations for the coefficients of R_0 in this ansatz and determines R-matrices of the form $R = R_0\bar{\Theta}$ for quadratic extensions of $u_q(\mathfrak{sl}_n)$. In this thesis, we develop this ansatz further and get a new set of equations for the coefficients of R_0, which we split in two different types. The first type of equations depends only on the fundamental group $\pi_1 = \Lambda_W/\Lambda_R$ of the Lie algebra $\mathfrak{g}$ and will be called *group-equations*. The second type depends on some sublattices of Λ and is very sensitive to different choices of ℓ. This type of equations will be called *diamond-equations*.

In Chapter 3 we determine the solutions to the group-equations. For the case of cyclic fundamental group $\pi_1 = \mathbb{Z}_N$, $N \in \mathbb{N}$, (which is the case for all simple root systems but for D_{2m}, $m \geq 2$), a theorem about certain idempotents of the group algebra $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ is required. In order to prove this, we prove a main theorem about roots of unity first, which is of independent interest. The proof of this theorem is carried out along the lines of a new combinatorial principle, which to the best of our knowledge is introduced

in this thesis. The solutions of the group-equations for the case of fundamental group $\pi_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$ are determined by a Maple-calculation which is documented in Appendix A.

In Chapter 4 we determine all solutions of the diamond-equations from the set of the solutions of the group-equations. Again, we consider the case of cyclic fundamental group first and find that the existence of solutions then depends only on the fundamental group π_1 of $\mathfrak{g}$ and on the order ℓ of the root of unity q. Depending on the data $\mathfrak{g}$, q, Λ (and fixed Λ') we then determine in the main theorem all R-matrices obtained through Lusztig's ansatz for different variants $u_q(\mathfrak{g}, \Lambda, \Lambda')$ of $u_q(\mathfrak{g})$.

Zusammenfassung

Quasitrianguläre Hopf Algebren, also Hopf Algebren mit einer (universellen) R-Matrix, haben verzopfte Modul-Kategorien. Insbesondere bringen quasitrianguläre Quantengruppen Ribbon (Band) Kategorien hervor, welche viele interessante Anwendungen haben, vor allem in der niedrig-dimensionalen Topologie und topologischen Quantenfeldtheorien.

In dieser Arbeit konstruieren wir neue (universelle) R-Matrizen der kleinen Quantengruppen $u_q(\mathfrak{g})$ und Erweiterungen derselben. Dabei ist $\mathfrak{g}$ immer eine endlich-dimensionale komplexe, einfache Lie algebra und q eine ℓ-te Einheitswurzel für beliebiges $\ell > 2$. Das erste Kapitel stellt die notwendigen algebraischen Notationen bereit und enthält die Definition der hier betrachteten Quantengruppen. Da im allgemeinen die kleinen Quantengruppen nicht quasitriangulär sind, d.h. keine R-Matrix existiert, betrachten wir Erweiterung der übliche Quantengruppe $u_q(\mathfrak{g})$. Diese sind durch ein Gitter Λ zwischen Wurzelgitter Λ_R und Gewichtsgitter Λ_W der Lie Algebra $\mathfrak{g}$ parametrisiert. Dies führt zur Notation $u_q(\mathfrak{g}, \Lambda, \Lambda')$ für die Erweiterung der kleinen Quantengruppe $u_q(\mathfrak{g}, \Lambda')$ durch Λ. Das Gitter $\Lambda' \subset \Lambda_R$ legt hier einen gewissen Quotienten in der Konstruktion der Quantengruppe fest.

Im zweiten Kapitel verwenden wir Lusztigs Ansatz $R = R_0\bar{\Theta}$ für R-Matrizen. Dieser Ansatz führt ein festes Element, die sogenannte Quasi-R-Matrix Θ, ein. Diese setzt die Komultiplikation Δ mit einer neuen Komultiplikation $\bar{\Delta}$ in Verbindung, welche durch die Konjugation mit einer nicht-linearen Involution erhalten wird. Das freie Element R_0 setzt $\bar{\Delta}$ und die entgegengesetzte Komultiplikation Δ^{opp} miteinander in Verbindung. In seiner Dissertation gibt Eric Müller einen Ansatz und Gleichungen für die Koeffizienten von R_0 an und nutzt diesen zur Bestimmung von R-Matrizen der Form $R = R_0\bar{\Theta}$ für quadratische Erweiterungen von $u_q(\mathfrak{sl}_n)$. Wir entwickeln diesen Ansatz in dieser Arbeit weiter und erhalten ein neues System von Gleichungen für die Koeffizienten von R_0, welche wir in zwei verschiedene Typen aufteilen. Der erste Typ von Gleichungen hängt nur noch von der Fundamentalgruppe $\pi_1 = \Lambda_W/\Lambda_R$ der Lie algebra $\mathfrak{g}$ ab und wird daher *Gruppen-Gleichungen* genannt. Der zweite Typ hängt von gewissen Untergittern von Λ ab und ist sehr sensible auf verschiedene Wahlen von ℓ. Dieser Typ von Gleichungen wird *Diamanten-Gleichungen* genannt.

Im Kapitel 3 bestimmen wir die Lösungen der Gruppen-Gleichungen. Im Fall zyklischer Fundamentalgruppen $\pi_1 = \mathbb{Z}_N$, $N \in \mathbb{N}$ (was für alle einfachen Wurzelsysteme ausser D_{2m}, $m \geq 2$, der Fall ist), benötigen wir einen Satz über gewisse Idempotente der Gruppenalgebra $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$. Um diesen zu beweisen, beweisen wir zuerst einen Hauptsatz über Einheitswurzeln, welcher von unabhängigem Interesse ist. Der Beweis dieses Satzes benutzt ein neues kombinatorisches Prinzip, welches wir ebenfalls einführen. Die Lösungen der Gruppen-Gleichungen im Fall der Fundamentalgruppe $\pi_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$ werden mittels Maple bestimmt. Die Rechnung ist im Anhang A dokumentiert.

Im Kapitel 4 bestimmen wir ausgehend von den Lösungen der Gruppen-Gleichungen alle Lösungen der Diamanten-Gleichungen. Wieder betrachten wir dafür den Fall zyklischer Fundamentalgruppen zuerst und stellen fest, dass die Existenz von Lösungen nur von der Fundamentalgruppe π_1 von $\mathfrak{g}$ und der Ordnung ℓ der Einheitswurzel abhängt. Abhängig von den Daten $\mathfrak{g}$, q, Λ (und festem Λ') bestimmen wir dann im Hauptsatz alle R-Matrizen für verschiedene Varianten $u_q(\mathfrak{g}, \Lambda, \Lambda')$ von $u_q(\mathfrak{g})$, welche Lusztigs Ansatz genügen.

Bibliography

[Abe80] E. Abe. *Hopf algebras*. Cambridge University Press, Cambridge, 2004.

[AY13] I. Angiono and H. Yamane. *The R-matrix of quantum doubles of Nichols algebras of diagonal type*. Preprint (2013), arXiv:1304.5752.

[BK01] B. Balsam and A. Kirillov. *Lectures on Tensor Categories and Modular Functors*. University Lecture Series, Vol. 21, Amer. Math. Soc., Providence, RI, 2001.

[Bou66] N. Bourbaki. *Elements of General Topology Part I*. Hermann, Paris, 1966.

[CP94] V. Chari and A. Pressley. *A guide to quantum groups*. Cambridge Univ. Press, Cambridge, 1994.

[Dri85] V. Drinfeld. *Hopf algebras and the quantum Yang-Baxter equation*. Dokl. Akad. Nauk SSSR, **32**, 254–258 (1985).

[Dri87] V. Drinfeld. *Quantum groups*. Proc. I.C.M. Berkley 1986, Vol. 1, 798–820, Amer. Math. Soc., Providence, RI, 1987.

[Fad84] L.D. Faddeev. *Integrable models in* (1+1)*-dimensional quantum field theory*. Lectures at Les Houches 1982, Elsevier Science Publishers B.V., Amsterdam, New York, 1984.

[FGST06] B. Feigin, A. Gainutdinov, A. Semikhatov, I. Tipunin. *Modular Group Representations and Fusion in Logarithmic Conformal Field Theories and in the Quantum Group Center*. Commun. Math. Ohys, 265, 47–93 (2006).

[GW98] S. Gelaki and S. Westreich. *On the Quasitriangularity of* $U_q(\mathfrak{sl}_n)'$. J. Amer. Math. Soc., **57**(1), 105–125 (1998).

[Hum72] J. E. Humphreys. *Introduction to Lie algebras and representation theory*. Graduate Texts in Mathematics, Vol. 9, Springer, New York, 1972.

[Jan07] J. C. Jantzen. *Representations of algebraic groups*. Mathematical surveys and monographs, Vol. 107, Amer. Math. Soc., Providence, RI, 2007.

[Jim85] M. Jimbo. *A q-difference analogue of* $U(\mathfrak{g})$ *and the Yang-Baxter equation*. Lett. Math. Phys., **10**(1), 63–69 (1985).

[JS93] A. Joyal and R. Street. *Braided tensor categories*. Adv. Math., **102**(1), 20–78 (1993).

[Kas95] C. Kassel. *Quantum groups.* Graduate Texts in Mathematics, Vol. 155, Springer, New York, 1995.

[KL01] T. Kerler and V.V. Lyubashenko. *Non-Semisimple Topological Qunatum Field Theories for 3-Manifolds with Corners.* Lecture Note in Mathematics, Vol. 1765, Springer, Berling, 2001.

[Kol14] M. Kolountzakis. Private communication, 2014.

[KS11] H. Kondo and Y. Saito. *Indecomposable decomposition of tensor products of modules over the restricted quantum universal enveloping algebra associated to $\mathfrak{sl}_2$.* J. Algebra, **330**(1), 103–129, 2011.

[KRT97] C. Kassel, M. Rosso and V. Turaev. *Quantum groups and knot invariants.* Panoramas et Synthèses, Vol. 5, Société Mathématique de France, Paris, 1997.

[Len14] S. Lentner. *A Frobenius homomorphism for Lusztig's quantum groups over arbitrary roots of unity.* Preprint (2014), arXiv:1406.0865.

[LN14a] S. Lentner and D. Nett. *A theorem on roots of unity and a combinatorial principle.* Preprint (2014), arXiv:1409.5822.

[LN14b] S. Lentner and D. Nett. *New R-matrices for small quantum groups.* Preprint (2014), arXiv:1409.5824.

[Lus88] G. Lusztig. *Quantum deformations of certain simple modules over enveloping algebras.* Adv. Math., **70**(2), 237–249 (1988).

[Lus90] G. Lusztig. *Quantum groups at roots of 1.* Geometriae Dedicata, **35**(1), 89–113, 1990.

[Lus93] G. Lusztig. *Introduction to Quantum Groups.* Progress in Mathematics, Vol. 110, Birkhäuser, Boston, 1993.

[MacL98] S. Mac Lane. *Categories for the Working Mathematician.* Graduate Texts in Mathematics, Vol. 5, Springer, New York, 1998.

[Mül98a] E. Müller. *Quantengruppen im Einheitswurzelfall.* Dissertation, LMU, München, 1998, http://www.mathematik.uni-muenchen.de/~algebra/Dissertationen/Mueller/doktor.ps

[Mül98b] E. Müller. *Some topics on Frobenius–Lusztig kernels I, II.* J. Algebra, **206**(2), 624–681 (1998).

[Res95] N. Reshetikhin. *Quasitriangularity of quantum groups at roots of 1.* Commun. Math. Phys., **170**(1), 79–99 (1995).

[Ros93] M. Rosso. *Quantum Groups at a Root of 1 and Tangle Invariants.* Int. J. Mod. Phys. B, **07**(20n21), 3715–3726 (1993).

[RT91] N. Reshetikhin and V.G. Turaev. *Invariants of 3-manifolds via link polynomials and quantum groups.* Invent. Math., **103**, 547–597 (1991).

[RSTS88] N. Reshetikhin and M. Semenov-Tian-Shansky. *Quantum R-matrices and *factorization problems.* J. Geom. Phys., **5**(4), 533–550 (1988).

[Sch12] C. Schweigert. *Hopf algebras, quantum groups and topological field theory.* Lecture notes (2012), http://www.math.uni-hamburg.de/home/schweigert/ws12/hskript.pdf

[Swe69] M. Sweedler. *Hopf algebras.* W.A. Benjamin, Inc., New York, 1969.

[Tan92] T. Tanisaki. *Killing forms, Harish-Chandra homomorphisms and universal R-matrices for quantum algebras.* Int. J. Mod. Phys. A, **07**(supp01b), 941–962 (1992).

[Tur00] V.G. Turaev. *Quantum Invariants of Knots and 3-Manifolds.* Studies in Mathematics, Vol. 18, de Gruyter, Berlin, 2010.

Declaration on oath/Eidesstatliche Erklärung

I hereby declare, on oath, that I have written the present dissertation by my own and have not used other than the acknowledged resources and aids.

Hiermit erklare ich an Eides statt, dass ich die vorliegende Dissertationsschrift selbst verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Hamburg, 2015-02-05 Signature