Hopf Algebras and Congruence Subgroups

Yorck Sommerhäuser   Yongchang Zhu

Abstract

We prove that the kernel of the natural action of the modular group on the center of the Drinfel'd double of a semisimple Hopf algebra is a congruence subgroup. To do this, we introduce a class of generalized Frobenius-Schur indicators and endow it with an action of the modular group that is compatible with the original one.

Contents

Introduction

At least since the work of J. L. Cardy in 1986, the importance of the role of the modular group has been emphasized in conformal field theory, and it has been extensively investigated since then.[1] This importance stems from the fact that the characters of the primary fields, which depend on a complex parameter, are equivariant with respect to the action of the modular group on the upper half plane on the one hand and a linear representation of the modular group on the other hand, which is finite-dimensional in the case of a rational conformal field theory. It was soon noticed in the course of this development that under quite general assumptions a frequently used generator of the modular group has finite order in this representation.[2] Since this generator and one of its conjugates together generate the modular group, this leads naturally to the conjecture that the kernel of the before-mentioned representation is a congruence subgroup. After an intense investigation, this conjecture was finally established by P. Bantay.[3]

In a different line of thought, Y. Kashina observed, while investigating whether the antipode of a finite-dimensional Yetter-Drinfel'd Hopf algebra over a semisimple Hopf algebra has finite order, that certain generalized powers associated with the semisimple Hopf algebra tend to become trivial after a certain number of steps.[4] She established this fact in several cases and conjectured that in general this finite number after which the generalized powers become trivial, which is now called the exponent of the Hopf algebra, divides the dimension of the Hopf algebra. This conjecture is presently still open. However, P. Etingof and S. Gelaki, realizing the connection between these two lines of thought, were able to establish the finiteness of the exponent and showed that it divides at least the third power of the dimension.[5] They also explained the connection of the exponent to the order of the generator of the modular group by showing that the exponent of the Hopf algebra is equal to the order of the Drinfel'd element of the Drinfel'd double of the Hopf algebra. In this context, it should be noted that this connection between Hopf algebras and conformal field theory has been intensively investigated by many authors; we only mention here the modular Hopf algebras and modular categories of N. Reshetikhin and V. G. Turaev on the one hand and the modular transformations considered by V. Lyubashenko and his coauthors on the other hand.[6]

It is the purpose of the present work to unite these two lines of thought further by establishing an analogue of Bantay's results for semisimple Hopf algebras. We will show in Theorem 9.3 that the kernel of the action of the modular group on the center of the Drinfel'd double of a semisimple Hopf algebra is a congruence subgroup of level N, where N is the exponent of the Hopf algebra discussed above. The proof of this theorem becomes possible by the use of a new tool, a further generalization of the higher Frobenius-Schur indicators studied earlier by Y. Kashina and the authors.[7] These new indicators, which we call equivariant Frobenius-Schur indicators, are functions on the center of the

Drinfel'd double and carry an action of the modular group that is equivariant with respect to the action of the modular group on the center. This equivariance in particular connects, via the action of the Verlinde matrix that arises from the other frequently used generator of the modular group, the first formula for the higher Frobenius-Schur indicators with the second resp. third formula, whose interplay is crucial for the proof of Cauchy's theorem for Hopf algebras.[8]

The Drinfel'd double is an example of a factorizable Hopf algebra, and the results for the Drinfel'd double can be partially generalized to this more general class. However, in the case of a factorizable semisimple Hopf algebra, the modular group acts in general only projectively on the center of the Hopf algebra. This phenomenon also occurs in conformal field theory, and also in the general framework of modular categories, of which the representation category of a semisimple factorizable Hopf algebra is an example.[9] But it is still possible to talk about the kernel of the projective representation, i.e., the subgroup of the modular group that acts as the identity on the associated projective space of the center. We will also show, in Paragraph 9.4, that in this more general case this so-called projective kernel is a congruence subgroup of level N.

However, if the Drinfel'd element of the factorizable Hopf algebra has the same trace as its inverse in the regular representation, then the projective representation just discussed is in fact an ordinary linear representation. This happens in particular in the case of a Drinfel'd double, where both of these traces are equal to the dimension of the doubled Hopf algebra. If these traces coincide, it is therefore meaningful to talk about the kernel of the linear representation, and we show in Theorem 12.3 that this kernel is also a congruence subgroup of level N.

The article is organized as follows: In Section 1, after briefly recalling some facts about the modular group, we describe a relation that characterizes the orbits of the principal congruence subgroups and plays an important role in the proof of the orbit theorem in Paragraph 8.4. In Section 2, we recall some basic facts about quasitriangular Hopf algebras and the Drinfel'd double construction, and prove some lemmas about the Drinfel'd element and the evaluation form. In Section 3, we prove some facts about factorizable Hopf algebras that are important for the equivariance properties that we will discuss later. In Section 4, we construct the action of the modular group on the center of a factorizable Hopf algebra. It must be emphasized that this construction is not new; on the contrary, it is discussed in abundance in the literature we have already quoted, especially in V. G. Turaev's monograph on the one hand and in two closely related articles V. Lyubashenko on the other hand.[10] What we do in this section is to translate Lyubashenko's graphical proof of the modular identities into the language of quasitriangular Hopf algebras, thereby offering a presentation of these results that is not yet available in the literature in this form.[11]

In Section 5, we specialize to the semisimple case. We can then use the centrally primitive idempotents as a basis and therefore get explicit matrices for the action of the modular group constructed in Section 4. In the case of a Drinfel'd double, there is a different construction for the action of the modular group based on the evaluation form and using a slightly less frequently used set of generators of the modular group. This description of the action, which is crucial for the proof of the equivariance theorem in Paragraph 8.3, is given in Section 6.

For two modules V and W of a semisimple Hopf algebra H, the modules $V \otimes W$ and $W \otimes V$ are in general not isomorphic. However, as we show in Section 7, the corresponding induced modules of the Drinfel'd double $D(H)$ are isomorphic. The constructed isomorphism is the essential element for the definition of the equivariant Frobenius-Schur indicators $I_V((m,l),z)$ in Section 8, which depend on an H-module V, two integers m and l, and a central element z in the Drinfel'd double $D(H)$. We then prove the equivariance theorem $I_V((m,l)g,z) = I_V((m,l),g.z)$ for an element g of the modular group. In Paragraph 8.4, we prove the orbit theorem, which asserts that the equivariant indicators only depend on the orbit of (m,l) under the principal congruence subgroup determined by the exponent. This is applied in Section 9 to prove the congruence subgroup theorem, which asserts that $g.z = z$ for all z in the center of the Drinfel'd double $D(H)$ and all g in the principal congruence subgroup. Note that the orbit theorem is an immediate consequence of the equivariance theorem and the congruence subgroup theorem. Finally, in the case of an arbitrary factorizable Hopf algebra, we prove the projective congruence subgroup theorem, which asserts that the kernel of the projective representation is a congruence subgroup.

The Wedderburn components of the character ring of a semisimple factorizable Hopf algebra are isomorphic to subfields of the cyclotomic field determined by the exponent.[12] As in conformal field theory,[13] we therefore get an action of the Galois group of the cyclotomic field on the character ring. As we explain in Section 10, this linear action of the Galois group arises naturally as the composition of the two semilinear actions that preserve the characters resp. the primitive idempotents of the character ring. In Section 11, we relate these actions of the Galois group to the equivariant Frobenius-Schur indicators, which enables us to show in Theorem 11.5 that in the case of a Drinfel'd double the action of the Galois group coincides with the action of the diagonal matrices in the reduced modular group $\mathrm{SL}(2,\mathbb{Z}_N)$. This is again confirming the parallels with conformal field theory, where the analogous result was known in many cases.[14] However, this theorem does not hold for a general semisimple factorizable Hopf algebra, as we see in Section 12: Under the assumption that the character of the regular representation takes the same value on the Drinfel'd element and on its inverse, which happens for Drinfel'd doubles, the action of the modular group, which is in general only projective, becomes an ordinary linear representation. Generalizing the congruence subgroup theorem from Paragraph 9.3, we show in Theorem 12.3 that the kernel of this linear representation is again a congruence subgroup of level N, so that we again get an action of the reduced modular group $\mathrm{SL}(2,\mathbb{Z}_N)$. But this time the action of the Galois group may differ from the action of the diagonal matrices by a certain Dirichlet character, which, as it generalizes the Jacobi symbol to Hopf algebras, we call the Hopf symbol.

Throughout the whole exposition, we consider an algebraically closed base field that is denoted by K. From Section 5 on until the end, we assume in addition that K has characteristic zero. All vector spaces considered are defined over K, and all tensor products without subscripts are taken over K. The dual of a vector space V is denoted by $V^* := \mathrm{Hom}_K(V,K)$, and the transpose of a linear map $f : V \to W$ is denoted by $f^* : W^* \to V^*$. Unless stated otherwise, a module is a left module. Also, we use the so-called Kronecker symbol δ_{ij}, which is equal to 1 if $i = j$ and zero otherwise. The set of natural numbers is the set $\mathbb{N} := \{1, 2, 3, \ldots\}$; in particular, 0 is not a natural number. The symbol $\mathbb{Q}_m$ denotes the m-th cyclotomic field, and not the field of m-adic numbers, and $\mathbb{Z}_m$ denotes the set $\mathbb{Z}/m\mathbb{Z}$ of integers modulo m, and not the ring of m-adic integers. The greatest common divisor of two integers m and l is denoted by $\gcd(m,l)$ and is always chosen to be nonnegative.

Furthermore, H denotes a Hopf algebra of finite dimension n with coproduct Δ, counit ε, and antipode S. We will use the same symbols to denote the corresponding structure elements of the dual Hopf algebra H^*, except for the antipode, which is denoted by S^*. The opposite Hopf algebra, in which the multiplication is reversed, is denoted by H^{op}, and the coopposite Hopf algebra, in which the comultiplication is reversed, is denoted by H^{cop}. If $b_1, \ldots, b_n$ is a basis of H with dual basis $b_1^*, \ldots, b_n^*$, we have the formulas[15]

$$\sum_{i=1}^{n} b_i^* \otimes b_{i(1)} \otimes b_{i(2)} \otimes \ldots \otimes b_{i(m)} = \sum_{i_1, i_2, \ldots, i_m = 1}^{n} b_{i_1}^* b_{i_2}^* \cdots b_{i_m}^* \otimes b_{i_1} \otimes b_{i_2} \otimes \ldots \otimes b_{i_m}$$

and

$$\sum_{i=1}^{n} b_{i(1)}^* \otimes b_{i(2)}^* \otimes \ldots \otimes b_{i(m)}^* \otimes b_i = \sum_{i_1, i_2, \ldots, i_m = 1}^{n} b_{i_1}^* \otimes b_{i_2}^* \otimes \ldots \otimes b_{i_m}^* \otimes b_{i_1} b_{i_2} \cdots b_{i_m}$$

which we will refer to as the dual basis formulas. We use the letter A instead of H if the Hopf algebra under consideration is quasitriangular. With respect to enumeration, we use the convention that propositions, definitions, and similar items are referenced by the paragraph in which they occur; they are only numbered separately if this reference is ambiguous.

The essential part of the present work was carried out when the first author held a visiting research position at the Hong Kong University of Science and Technology. He thanks the university, and in particular his host, for the hospitality.

He also thanks the University of Cincinnati for a follow-on visiting position during which part of the manuscript was written. The second author would like to express his appreciation for the support by the RGC Competitive Earmarked Research Grant HKUST 6059/04.

1 The modular group

1.1 In this article, the modular group is defined as the group $\Gamma := SL(2;\mathbb{Z})$ of 2×2-matrices with integer entries and determinant 1; note that many authors define it as the quotient group $PSL(2;\mathbb{Z})$ instead. The modular group is generated by the two matrices[16]

$$s := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad t := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

It is easy to see that these matrices satisfy the relations

$$s^4 = 1 \qquad (ts)^3 = s^2$$

however, it is a nontrivial result that these are defining relations for the modular group.[17]

It is possible to replace the generator s by the generator

$$r := t^{-1}s^{-1}t^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

The generators r and t satisfy the relations

$$trt = rtr \qquad (rt)^6 = 1$$

and it follows from the corresponding result for the preceding generators that this also constitutes a presentation of the modular group in terms of generators and relations. From this, we get that $s^{-1}r = trtr = ts^{-1}$, which means that $r = sts^{-1}$, so that the generators r and t are conjugate.

The matrix

$$a := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

is not contained in Γ, but conjugation by a induces an automorphism of Γ, for which we introduce the following notation:

Definition For $g \in \Gamma$, we define $\tilde{g} := aga^{-1} = aga$.

Note that we have

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}$$

so that $\tilde{g} = g^{-1}$ whenever $a = d$. In particular, we find for the special matrices that we have used above as generators that

$$\tilde{s} = s^{-1} \qquad \tilde{t} = t^{-1} \qquad \tilde{r} = r^{-1}$$

1.2 If N is a natural number, the quotient map from $\mathbb{Z}$ to $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$ induces a group homomorphism

$$SL(2,\mathbb{Z}) \to SL(2,\mathbb{Z}_N)$$

by applying the quotient map to every component of the matrix. The kernel of this map is denoted by $\Gamma(N)$ and called the principal congruence subgroup of level N. In other words, we have

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \mid a \equiv d \equiv 1, \; b \equiv c \equiv 0 \pmod N \right\}$$

In particular, we have $\Gamma(1) = \Gamma$. A subgroup of the modular group is called a congruence subgroup if it contains $\Gamma(N)$ for a suitable N, and the smallest such N is called the level of the congruence subgroup.

The modular group acts naturally on the lattice $\mathbb{Z}^2 := \mathbb{Z} \times \mathbb{Z}$. The orbits of the principal congruence subgroups can be described as follows:

Proposition Two nonzero lattice points $(m,l),(m',l') \in \mathbb{Z}^2$ are in the same $\Gamma(N)$-orbit if and only if $t := \gcd(m,l) = \gcd(m',l')$ and

$$m/t \equiv m'/t \pmod N \qquad l/t \equiv l'/t \pmod N$$

Proof. If (m,l) and (m',l') are in the same $\Gamma(N)$-orbit, so that

$$\begin{pmatrix} m' \\ l' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} m \\ l \end{pmatrix}$$

then we have for the ideals of $\mathbb{Z}$ generated by m,l resp. m',l' that

$$(m',l') = (am + bl, cm + dl) \subset (m,l) = (t)$$

and vice versa, so that the first assertion holds. If we divide the above relation by t, we see that $(m/t, l/t)$ and $(m'/t, l'/t)$ are still in the same $\Gamma(N)$-orbit, and if we reduce this relation modulo N, we see that they are componentwise congruent.

For the converse, we can assume that $t = 1$. If now two pairs (m,l) and (m',l') of relatively prime integers are componentwise congruent modulo N, this also holds for the pairs $g(m,l)$ and $g(m',l')$ for any $g \in \Gamma$, and if we can show that $g(m,l)$ and $g(m',l')$ are in the same $\Gamma(N)$-orbit, then this also holds for the original pair (m,l) and (m',l'), as $\Gamma(N)$ is a normal subgroup.

Now as m and l are relatively prime, we can find integers n and k satisfying $mn + lk = 1$, so that

$$\begin{pmatrix} m \\ l \end{pmatrix} = \begin{pmatrix} m & -k \\ l & n \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

In other words, $(m;l)$ and $(1;0)$ are in the same Γ-orbit, so that we can in fact assume $(m;l) = (1;0)$. This means that we only have to show that a pair $(m';l')$ of relatively prime integers of the form $(m';l') = (1+aN;bN)$ is in the same $\Gamma(N)$-orbit as $(1;0)$. But this means that we have to find integers $c;d \in \mathbb{Z}$ so that

$$\begin{pmatrix} m' \\ l' \end{pmatrix} = \begin{pmatrix} 1+aN & cN \\ bN & 1+dN \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

subject to the determinant condition

$$1 = (1+aN)(1+dN) - (bN)(cN) = 1 + aN + dN + adN^2 - bcN^2$$

or alternatively

$$0 = a + d(1+aN) - bcN = a + dm' - cl'$$

As m' and l' are relatively prime, this equation is solvable. □

Note that this proposition shows that the condition to be componentwise congruent modulo N is not sufficient for two lattice points to be in the same $\Gamma(N)$-orbit, as the pairs $(2;4)$ and $(5;7)$ illustrate for $N = 3$. Furthermore, it should be noted that in the case $N = 1$ it yields the following fact:

Corollary Two nonzero lattice points $(m;l);(m';l') \in \mathbb{Z}^2$ are in the same Γ-orbit if and only if $\gcd(m;l) = \gcd(m';l')$.

1.3 The group homomorphism from $SL(2;\mathbb{Z})$ to $SL(2;\mathbb{Z}_N)$ discussed at the beginning of Paragraph 1.2 is surjective. The proof of this fact uses the following lemma, which we will use below for a different purpose:[18]

Lemma Suppose that m, l, and N are relatively prime integers and that $l \neq 0$. Then there exists an integer $k \in \mathbb{Z}$ such that $m + kN$ is relatively prime to l.

We need to introduce another subgroup of the modular group. We denote by $\tilde{\Gamma}(N)$ the subgroup of Γ that is generated by all conjugates gt^Ng^{-1} of t^N for $g \in \Gamma$. This subgroup is obviously normal, and it follows from the discussion in Paragraph 1.1 that it contains r^N. Since $\Gamma(N)$ is a normal subgroup that contains t^N, we have that $\tilde{\Gamma}(N)$ is contained in $\Gamma(N)$. However, $\tilde{\Gamma}(N)$ is strictly smaller than $\Gamma(N)$ if $N \geq 6$, and it is not even a congruence subgroup in this case.[19] To deal with this difficulty, we adapt the following notion from the theory of monoids to our situation:[20]

Definition An equivalence relation on the lattice $\mathbb{Z}^2$ is called a congruence relation if, for all $g \in \Gamma$, the lattice points $g.(m;l)$ and $g.(n;k)$ are equivalent whenever the lattice points $(m;l)$ and $(n;k)$ are equivalent.

From every normal subgroup of the modular group, we get a congruence relation by defining that two lattice points are equivalent if they are in the same orbit under the action of the normal subgroup. In this way, both $\Gamma(N)$ and $\Gamma'(N)$ give rise to congruence relations.

Considering relations as sets of pairs, one can show as in the case of monoids that the intersection of congruence relations is again a congruence relation.[21] Therefore, for every relation there is a smallest congruence relation that contains this relation, namely the intersection of all congruence relations that contain the given relation. In this sense, we now consider the smallest congruence relation $\sim$ on the lattice $\mathbb{Z}^2$ that has the following two properties:

1. We have $(m,l) \sim t^N.(m,l)$.
2. We have $(m,l) \sim (m,kl)$ for every $k \in \mathbb{Z}$ that satisfies $k \equiv 1 \pmod N$ and $\gcd(m,kl) = \gcd(m,l)$.

The second property appears to be asymmetrical with respect to the two components. This is, however, not the case, because if k satisfies $k \equiv 1 \pmod N$ and $\gcd(km,l) = \gcd(m,l)$, we have

$$\begin{pmatrix} m \\ l \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} l \\ m \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} l \\ km \end{pmatrix} = \begin{pmatrix} km \\ l \end{pmatrix}$$

so that $(m,l) \sim (km,l)$.

We will need another property of the congruence relation $\sim$:

Proposition For every integer $n \in \mathbb{Z}$, we have $(nm,nl) \sim (nm',nl')$ whenever $(m,l) \sim (m',l')$.

Proof. This is obvious if $n = 0$, so let us assume that $n \neq 0$. Suppose that $\approx$ is an arbitrary congruence relation that satisfies the two defining properties of $\sim$, i.e., that satisfies $(m,l) \approx t^N.(m,l)$ and $(m,l) \approx (m,kl)$ for every $k \in \mathbb{Z}$ with the properties $k \equiv 1 \pmod N$ and $\gcd(m,kl) = \gcd(m,l)$. Recall that $\sim$ is the intersection of all such congruence relations. We define a new relation $\approx_n$ by setting

$$(m,l) \approx_n (m',l') :\Leftrightarrow (nm,nl) \approx (nm',nl')$$

It is immediate that this is again a congruence relation. It also satisfies the first defining property, namely that $(m,l) \approx_n t^N.(m,l)$. For the second property, note that if $k \in \mathbb{Z}$ satisfies $k \equiv 1 \pmod N$ and $\gcd(m,kl) = \gcd(m,l)$, it also satisfies $\gcd(nm,knl) = \gcd(nm,nl)$, so that $(nm,nl) \approx (nm,knl)$ and therefore $(m,l) \approx_n (m,kl)$.

This shows that $(m,l) \sim (m',l')$ implies $(m,l) \approx_n (m',l')$, which means that $(nm,nl) \approx (nm',nl')$. As this holds for all such congruence relations $\approx$, we get $(nm,nl) \sim (nm',nl')$, as asserted. $\square$

It is not hard to see that, if we had dropped the second defining property above, the congruence relation that would have arisen would have been exactly the one determined by the group $\Gamma(N)$ as described above. The following theorem asserts that, by incorporating the second property, we get exactly the congruence relation determined by the group $\Gamma(N)$:

Theorem Two lattice points $(m;l)$ and $(m';l')$ are in the same $\Gamma(N)$-orbit if and only if $(m;l) \sim (m';l')$.

Proof. (1) Let us first show that equivalent lattice points are in the same $\Gamma(N)$-orbit. For this, we need to look at the two defining properties of our congruence relation. For the first property, it is obvious that $(m;l)$ and $t^N.(m;l)$ are in the same $\Gamma(N)$-orbit. For the second property, suppose that $k \in \mathbb{Z}$ satisfies $k \equiv 1 \pmod N$ and $t := \gcd(m;l) = \gcd(m;kl)$. If $(m;l)$ is nonzero, we have that $(m/t;l/t)$ and $(m/t;kl/t)$ are componentwise congruent modulo N. By Proposition 1.2, this implies that $(m;l)$ and $(m;kl)$ are in the same $\Gamma(N)$-orbit. Clearly, this is also the case if $(m;l) = (0;0)$.

This shows that the congruence relation determined by $\Gamma(N)$, for which the equivalence classes are exactly the $\Gamma(N)$-orbits, takes part in the intersection that was used to define the relation $\sim$. In other words, if $(m;l) \sim (m';l')$, then $(m;l)$ and $(m';l')$ are in the same $\Gamma(N)$-orbit.

(2) Now suppose that $(m;l)$ and $(m';l')$ are in the same $\Gamma(N)$-orbit. In the case $N = 1$, we have $\Gamma(N) = \Gamma(N) = \Gamma$, and we have already pointed out above that the two lattice points are then equivalent. We will therefore assume in the sequel that $N > 1$.

We first consider the case where m and l are relatively prime; by Corollary 1.2, we then also have that m' and l' are relatively prime. We need a couple of reductions. The first reduction is that we can assume in addition that all the components m, l, m', and l' are also relatively prime to N. To see this, choose two distinct primes p and q that do not divide N. By Corollary 1.2, we can then find $g \in \Gamma$ such that $g.(m;l) = (p;q)$. If we define $(p';q') := g.(m';l')$, then $(p;q)$ and $(p';q')$ are also in the same $\Gamma(N)$-orbit, because $\Gamma(N)$ is a normal subgroup. By Proposition 1.2, this implies that p' and q' are relatively prime and that

$$p \equiv p' \pmod N \qquad q \equiv q' \pmod N$$

so that in particular also p' and q' are relatively prime to N. But if we could establish that $(p;q)$ and $(p';q')$ are equivalent, then also $(m;l)$ and $(m';l')$ would be equivalent, because $\sim$ is a congruence relation. Therefore, we can assume from the beginning that all the components m, l, m', and l' are also relatively prime to N. Note that this implies in particular that the components are nonzero. This completes our first reduction.

(3) The second reduction is that we can assume in addition that m is relatively prime to l' and that m' is relatively prime to l. Now the numbers m and Nl

are relatively prime, which obviously implies that the numbers m, Nl, and l' are relatively prime. We can therefore apply the lemma stated at the beginning of the paragraph to find an integer $k \in \mathbb{Z}$ such that $m + kNl$ is relatively prime to l'. Note that $m + kNl$ is still relatively prime to N and l, and that $(m + kNl; l) = t^{kN}.(m;l)$ is equivalent to $(m;l)$ even if k is negative. By replacing $(m;l)$ by $(m + kNl; l)$, we can therefore assume from the beginning that in addition m and l' are relatively prime. Using the same argument with the lattice points interchanged, we can furthermore assume that m' and l are relatively prime.

(4) The third reduction is that we can assume in addition that $m = m'$. We have assumed that m' and N are relatively prime, which implies that there is a number $k' \in \mathbb{Z}$ such that $m'k' \equiv 1 \pmod{N}$. The numbers k' and N are then relatively prime, which obviously implies that the numbers k', N, and ll' are relatively prime. As all components are nonzero, we can apply the above lemma again to find an integer $k \in \mathbb{Z}$ such that $n := k' + kN$ is relatively prime to ll'. As we also have $nm' \equiv k'm' \equiv 1 \pmod{N}$, we get by the variant of the second defining property of our congruence relation discussed above that $(m;l) \sim (nm'm;l)$. But $m \equiv m' \pmod{N}$ by Proposition 1.2, so that

$$nm \equiv nm' \equiv 1 \pmod{N}$$

and furthermore nm and l' are relatively prime. Again by the variant of the second defining property, we therefore see that $(m';l') \sim (nmm';l')$. By replacing $(m;l)$ by $(nm'm;l)$ and $(m';l')$ by $(nmm';l')$, we can therefore reduce to the situation where $m = m'$.

(5) We have now two lattice points $(m;l)$ and $(m;l')$ with relatively prime components m and l resp. m and l'. Moreover, all of these components are relatively prime to N, and in particular nonzero. By assumption, they are in the same $\Gamma(N)$-orbit, so that $l \equiv l' \pmod{N}$ by Proposition 1.2. We have to establish that they are equivalent.

For this, we argue as in the preceding step: Choose k such that $kl \equiv 1 \pmod{N}$. Then the numbers k and N are relatively prime, which clearly implies that the numbers k, N, and m are relatively prime. Therefore, again by the above lemma, we can find an integer $n' \in \mathbb{Z}$ such that $n := k + n'N$ is relatively prime to m. We then have $n \equiv k \pmod{N}$ and therefore

$$nl \equiv nl' \equiv 1 \pmod{N}$$

and m and nl resp. nl' are relatively prime. By the second defining property of our congruence relation, we have that $(m;l) \sim (m;nl'l)$, and similarly that $(m;l') \sim (m;nll')$. As equal pairs are clearly equivalent, this finishes the proof in the case of lattice points with relatively prime components.

(6) We now consider the general case, in which we have two lattice points $(m;l)$ and $(m';l')$ in the same $\Gamma(N)$-orbit, but m and l are not necessarily relatively

prime. We have to establish that they are equivalent, and we can clearly assume that they are different from the origin. By Proposition 1.2, we have $t := \gcd(m,l) = \gcd(m',l')$ and

$$m/t \equiv m'/t \pmod{N} \qquad l/t \equiv l'/t \pmod{N}$$

Now m/t and l/t are relatively prime, and m'/t and l'/t are relatively prime as well. Furthermore, $(m/t, l/t)$ and $(m'/t, l'/t)$ are in the same $\Gamma(N)$-orbit. By the facts already established, we therefore get $(m/t, l/t) \sim (m'/t, l'/t)$, which implies $(m,l) \sim (m',l')$ by the above proposition. $\Box$

1.4 The groups $SL(2,\mathbb{Z}_N) = SL(2,\mathbb{Z})/\Gamma(N)$ are obviously generated by the images of the generators under the canonical map, which are

$$s := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad t := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

or alternatively t and

$$r := t^{-1} s^{-1} t^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

However, the defining relations for these generators are not easy to obtain. To write them down, we introduce the abbreviation $d(q) := s t^{q'} s^{-1} t^{q} s t^{q'}$ for $q, q' \in \mathbb{Z}$ such that $qq' \equiv 1 \pmod{N}$. Although we want to understand this expression here as an abbreviation for a word in the generators, it is of course also possible to compute the corresponding matrix in $SL(2,\mathbb{Z}_N)$:

$$\begin{aligned} d(q) &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & q' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & q' \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -1 \\ 1 & q' \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -q \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & q' \end{pmatrix} = \begin{pmatrix} 1 & q \\ -q' & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & q' \end{pmatrix} = \begin{pmatrix} q & 0 \\ 0 & q' \end{pmatrix} \end{aligned}$$

Note also that we have intentionally suppressed the dependence of $d(q)$ on q', on which it, as an abbreviation for a word in the generators, in principle depends.

The following proposition, which is adapted from [11], lists one possible set of defining relations:

Proposition Write $N = 2^e m$, where m is odd. Then the relations

1. $s^4 = 1 \qquad (ts)^3 = s^2 \qquad t^N = 1$
2. $t^{2^e}(s t^m s^{-1}) = (s t^m s^{-1}) t^{2^e}$
3. $d(q)s = s\,d(q)^{-1}$
4. $d(q)t = t^{q^2} d(q)$

for all $q \in \mathbb{Z}$ that are relatively prime to N, are defining relations for $SL(2,\mathbb{Z}_N)$.

Proof. This is proved in [11], §2.2, Lem. 1.c, p. 5, where also further references are given. Note that the generator s is defined differently in [11], namely as our s^{-1}. It is also shown there that the relations 3 and 4 are not necessary for all q that are relatively prime to N, but only for $q = 1 - 2d$, $q = 2 - d$, and $q = 2d + 1$, where d is an integer that satisfies $d \equiv 1 \pmod{2^e}$ and $d \equiv 0 \pmod{m}$. □

2 Quasitriangular Hopf algebras

2.1 Recall that a Hopf algebra A is called quasitriangular[22] if its antipode is invertible and it possesses a so-called R-matrix, which is an invertible element $R = \sum_{i=1}^{m} a_i \otimes b_i \in A \otimes A$ that satisfies $\Delta^{cop}(a) = R\Delta(a)R^{-1}$ as well as

$$(\Delta \otimes \mathrm{id})(R) = \sum_{i,j=1}^{m} a_i \otimes a_j \otimes b_i b_j \qquad (\mathrm{id} \otimes \Delta)(R) = \sum_{i,j=1}^{m} a_i a_j \otimes b_j \otimes b_i$$

Associated with the R-matrix is the Drinfel'd element $u := \sum_{i=1}^{m} S(b_i)a_i$. This is an invertible element that satisfies[23]

$$\Delta(u) = (u \otimes u)(R'R)^{-1} = (R'R)^{-1}(u \otimes u) \qquad S^2(a) = uau^{-1}$$

where $R' := \sum_{i=1}^{m} b_i \otimes a_i$ arises from the R-matrix by interchanging the tensorands. The inverse Drinfel'd element is given by $u^{-1} = \sum_{i=1}^{m} S^{-2}(b_i)a_i$. In this context, it should be noted that the element R'^{-1} always also is an R-matrix for A. The Hopf algebra is called triangular if these two choices for the R-matrices coincide.

2.2 An important source of quasitriangular Hopf algebras is the Drinfel'd double construction.[24] For an arbitrary finite-dimensional Hopf algebra H, the Drinfel'd double $D := D(H)$ is a Hopf algebra whose underlying vector space is $H^* \otimes H$. The coalgebra structure is the tensor product coalgebra structure $H^{*cop} \otimes H$, so that coproduct and counit are given by the formulas

$$\Delta_D(\varphi \otimes h) = (\varphi_{(2)} \otimes h_{(1)}) \otimes (\varphi_{(1)} \otimes h_{(2)}) \qquad \varepsilon_D(\varphi \otimes h) = \varphi(1)\varepsilon(h)$$

The formula for the product is a little more involved; it reads

$$(\varphi \otimes h)(\varphi' \otimes h') = \varphi'_{(1)}(S^{-1}(h_{(3)}))\varphi'_{(3)}(h_{(1)})\,\varphi\varphi'_{(2)} \otimes h_{(2)}h'$$

Finally, the antipode is given by the formula $S_D(\varphi \otimes h) = (\varepsilon \otimes S(h))(S^{-1}(\varphi) \otimes 1)$.

To establish the assertion that the Drinfel'd double is quasitriangular, we have to endow it with an R-matrix, which is explicitly given as follows: If $b_1, \dots, b_n$ is a basis of H with dual basis $b_1^*, \dots, b_n^*$, then the R-matrix is

$$R = \sum_{i=1}^{n} (\varepsilon \otimes b_i) \otimes (b_i^* \otimes 1)$$

The associated Drinfel'd element u_D and its inverse are therefore

$$u_D = \sum_{i=1}^{n} S^{-1}(b_i^*) \otimes b_i \qquad u_D^{-1} = \sum_{i=1}^{n} S^{2}(b_i^*) \otimes b_i$$

The Drinfel'd element has an analogue in the dual D^*, namely the evaluation form

$$e : D^* \to K,\ \varphi \otimes h \mapsto \varphi(h)$$

The evaluation form is a symmetric Frobenius homomorphism.[25] It is invertible with inverse $e^{-1}(\varphi \otimes h) = \varphi(S^{-1}(h))$.

2.3 The integrals of the Drinfel'd double can be described in terms of the integrals of the original Hopf algebra H. If we choose left integrals $\Lambda \in H$ and $\lambda \in H^*$ as well as right integrals $\Gamma \in H$ and $\rho \in H^*$, then

$$\Lambda_D = \rho \otimes \Lambda$$

is a two-sided integral of the Drinfel'd double, which in particular tells that the Drinfel'd double is unimodular.[26] Similarly, the functions λ_D and ρ_D in D^* defined by

$$\lambda_D(\varphi \otimes h) = \varphi(\Gamma)\lambda(h) \qquad \rho_D(\varphi \otimes h) = \varphi(\Lambda)\rho(h)$$

are left resp. right integrals on D. Using the forms of the Drinfel'd element and its inverse given in Paragraph 2.2, we see that

$$\lambda_D(u_D) = \lambda(S^{-1}(\Gamma)) \qquad \lambda_D(u_D^{-1}) = \lambda(S^2(\Gamma))$$
$$\rho_D(u_D) = \rho(S^{-1}(\Lambda)) \qquad \rho_D(u_D^{-1}) = \rho(S^2(\Lambda))$$

Using these integrals, it is possible to relate the Drinfel'd element u_D and the evaluation form e:

Lemma

1. $\Lambda_{D(1)} e(\Lambda_{D(2)}) = e(\Lambda_D) u_D$
2. $e(\Lambda_{D(1)}) \Lambda_{D(2)} = e(\Lambda_D) S_D(u_D)$
3. $e^{-1}(\Lambda_{D(1)}) \Lambda_{D(2)} = e^{-1}(\Lambda_D) u_D^{-1}$
4. $\Lambda_{D(1)} e^{-1}(\Lambda_{D(2)}) = e^{-1}(\Lambda_D) S_D(u_D^{-1})$

Proof. For every $h \in H$, we have

$$\begin{aligned}\rho_{(1)}(\Lambda_{(2)})\rho_{(2)}(h)\Lambda_{(1)} &= \rho(\Lambda_{(2)}h)\Lambda_{(1)} = \rho(\Lambda_{(2)}h_{(3)})\Lambda_{(1)}h_{(2)}S^{-1}(h_{(1)}) \\ &= \rho(\Lambda_{(2)})\Lambda_{(1)}S^{-1}(h) = \rho(\Lambda)S^{-1}(h) = e(\Lambda_D)S^{-1}(h)\end{aligned}$$

Therefore, if $b_1, \ldots, b_n$ is a basis of H with dual basis $b_1^*, \ldots, b_n^*$, we have

$$\begin{aligned}\Lambda_{D(1)} e(\Lambda_{D(2)}) &= \rho_{(2)} \otimes \Lambda_{(1)} e(\rho_{(1)} \otimes \Lambda_{(2)}) = \rho_{(2)} \otimes \Lambda_{(1)}\rho_{(1)}(\Lambda_{(2)}) \\ &= \sum_{i=1}^n b_i^* \otimes \rho_{(2)}(b_i)\Lambda_{(1)}\rho_{(1)}(\Lambda_{(2)}) = e(\Lambda_D)\sum_{i=1}^n b_i^* \otimes S^{-1}(b_i) = e(\Lambda_D)u_D\end{aligned}$$

This proves the first relation. The second relation follows from this by applying the antipode S_D, because Λ_D is invariant under the antipode,[27] and we have $S_D(e) = e$, since

$$\begin{aligned} S_D(e)(\varphi \otimes h) &= e((\varepsilon \otimes S(h))(S^{-1}(\varphi) \otimes 1)) \\ &= e((S^{-1}(\varphi) \otimes 1)(\varepsilon \otimes S(h))) = \varphi(h) \end{aligned}$$

For the third relation, note that

$$\begin{aligned} &\lambda_{(1)}(h)\lambda_{(2)}(S^{-1}(\Lambda_{(1)}))S^{-2}(\Lambda_{(2)}) = \lambda(hS^{-1}(\Lambda_{(1)}))S^{-2}(\Lambda_{(2)}) \\ = {}& \lambda(h_{(2)}S^{-1}(\Lambda_{(1)}))h_{(1)}S^{-1}(\Lambda_{(2)})S^{-2}(\Lambda_{(3)}) = \lambda(h_{(2)}S^{-1}(\Lambda))h_{(1)} \\ = {}& \lambda(S^{-1}(\Lambda))h = e^{-1}(\Lambda_D)h \end{aligned}$$

which implies

$$\begin{aligned} e^{-1}(\Lambda_{D(1)})\Lambda_{D(2)} &= e^{-1}(\lambda_{(2)} \otimes \Lambda_{(1)})\lambda_{(1)} \otimes \Lambda_{(2)} = \lambda_{(2)}(S^{-1}(\Lambda_{(1)}))\lambda_{(1)} \otimes \Lambda_{(2)} \\ &= \sum_{i=1}^{n} \lambda_{(1)}(b_i)\lambda_{(2)}(S^{-1}(\Lambda_{(1)}))b_i \otimes \Lambda_{(2)} \\ &= e^{-1}(\Lambda_D)\sum_{i=1}^{n} b_i \otimes S^2(b_i) = e^{-1}(\Lambda_D)u_D^{-1} \end{aligned}$$

The fourth relation follows as before from the third by applying the antipode. $\square$

We will also need the corresponding result that expresses the evaluation form in terms of the Drinfel'd element:[28]

Proposition

1. $\rho_D(u_D x) = \rho_D(xu_D) = \rho_D(u_D)e(x)$
2. $\rho_D(S_D(u_D^{-1})x) = \rho_D(xS_D(u_D^{-1})) = \rho_D(S_D(u_D^{-1}))e^{-1}(x)$

Proof. We can assume that $x = \varphi \otimes h$. For the first relation, we then have

$$\begin{aligned} \rho_D(u_D x) = \rho_D((S^{-2}(\varphi) \otimes 1)u_D(\varepsilon \otimes h)) &= \sum_{i=1}^{n} \rho_D(S^{-2}(\varphi)S^{-1}(b_i) \otimes b_i h) \\ &= \sum_{i=1}^{n} S^{-2}(\varphi)(\Lambda_{(1)})S^{-1}(b_i)(\Lambda_{(2)})\lambda_{(1)}(b_i)\lambda_{(2)}(h) \\ &= \varphi(S^{-2}(\Lambda_{(1)}))\lambda_{(1)}(S^{-1}(\Lambda_{(2)}))\lambda_{(2)}(h) \\ &= \varphi(S^{-2}(\Lambda_{(1)}))\lambda(S^{-1}(\Lambda_{(2)})h) \\ &= \varphi(S^{-2}(\Lambda_{(1)})S^{-1}(\Lambda_{(2)})h_{(2)})\lambda(S^{-1}(\Lambda_{(3)})h_{(1)}) \\ &= \varphi(h_{(2)})\lambda(S^{-1}(\Lambda)h_{(1)}) = \varphi(h)\lambda(S^{-1}(\Lambda)) = e(x)\rho_D(u_D) \end{aligned}$$

This shows that $\lambda_D(u_D x) = \lambda_D(u_D)e(x)$; if we replace x by $u_D^{-1} x u_D$ and use that e is a symmetric Frobenius homomorphism, we get that also $\lambda_D(x u_D) = \lambda_D(u_D)e(x)$.

For the second relation, we have

$$\begin{aligned}
\lambda_D(S_D(u_D^{-1})x) &= \sum_{i=1}^{n} \lambda_D(S_D(\varepsilon \otimes b_i)S_D(S^2(b_i) \otimes 1)x) \\
&= \sum_{i=1}^{n} \lambda_D((\varepsilon \otimes b_i)(S^2(b_i) \otimes 1)x) \\
&= \sum_{i=1}^{n} \lambda_D((S^2(b_i) \otimes 1)x(\varepsilon \otimes S^{-2}(b_i))) \\
&= \sum_{i=1}^{n} \lambda_D((b_i \otimes 1)x(\varepsilon \otimes b_i)) = \sum_{i=1}^{n} \lambda_D(b_i \varphi \otimes h b_i) \\
&= \sum_{i=1}^{n} b_i(\gamma_{(1)})\varphi(\gamma_{(2)})\rho_{(1)}(h)\rho_{(2)}(b_i) = \varphi(\gamma_{(2)})\rho_{(1)}(h)\rho_{(2)}(\gamma_{(1)}) \\
&= \varphi(\gamma_{(2)})\rho(h\gamma_{(1)}) = \varphi(S^{-1}(h_{(3)})h_{(2)}\gamma_{(2)})\rho(h_{(1)}\gamma_{(1)}) \\
&= \varphi(S^{-1}(h_{(2)}))\rho(h_{(1)}\gamma) = \varphi(S^{-1}(h))\rho(\gamma) = e^{-1}(x)\rho(\gamma)
\end{aligned}$$

For $x = 1$, this yields $\lambda_D(S_D(u_D^{-1})) = \rho(\gamma)$, which we can resubstitute in order to establish one of the claimed identities. The other one follows as before by substituting $S_D(u_D)xS_D(u_D^{-1})$ for x and using the symmetry of e. □

3 Factorizable Hopf algebras

3.1 If A is already a quasitriangular Hopf algebra, it is of course also possible to form its double $D = D(A)$. In this case, there exists a Hopf algebra retraction

$$\pi : D(A) \to A;\ \varphi \otimes a \mapsto (\varphi \otimes \mathrm{id})(R)\,a$$

from the double of A to A itself.[29] Using the alternative R-matrix R'^{-1} mentioned in Paragraph 2.1 instead of R, we get another Hopf algebra retraction π'. As we have[30] $R^{-1} = (S \otimes \mathrm{id})(R) = (\mathrm{id} \otimes S^{-1})(R)$, this map is explicitly given as

$$\pi' : D(A) \to A;\ \varphi \otimes a \mapsto (S \otimes \varphi)(R)\,a = (\mathrm{id} \otimes \varphi)(\mathrm{id} \otimes S^{-1})(R)\,a$$

From these two homomorphisms, we derive the algebra homomorphism

$$\Phi : D(A) \to A \otimes A;\ x \mapsto (\pi \otimes \pi')(\Delta_D(x))$$

where $A \otimes A$ carries the canonical algebra structure. Note that this map is in general not a coalgebra homomorphism with respect to the canonical coalgebra structure on $A \otimes A$. However, it becomes a Hopf algebra homomorphism if we twist the comultiplication[31] by the cocycle $F := 1 \otimes R^{-1} \otimes 1 \in A^{\otimes 4}$. In other words, Φ is a Hopf algebra homomorphism if considered as a map to the Hopf algebra $(A \otimes A)_F$, which has the canonical tensor product algebra structure, but the twisted coproduct

$$\Delta_F(a \otimes b) = F((a_{(1)} \otimes b_{(1)}) \otimes (a_{(2)} \otimes b_{(2)}))F^{-1}$$

The Hopf algebra $(A \otimes A)_F$ even becomes quasitriangular by using the twisted R-matrix[32] $R_F := F_t R_{A \otimes A} F^{-1}$, where

$$R_{A \otimes A} := \sum_{i,j=1}^{m} a_i \otimes b_j \otimes b_i \otimes S(a_j)$$

is an R-matrix for the tensor product Hopf algebra $A \otimes A$ and F_t arises from F by interchanging the first and the third as well as the second and the fourth tensor factor. By using this specific R-matrix, Φ becomes a morphism of quasitriangular Hopf algebras[33] in the sense that it maps the R-matrix of the Drinfel'd double to R_F. This implies that the image of the Drinfel'd element is given as follows:

Lemma $\Phi(u_D) = u \otimes u^{-1}$

Proof. In general, if the coproduct of a Hopf algebra is modified by a cocycle, then the resulting Hopf algebra has the antipode $S_F(a) = w S(a) w^{-1}$, where w arises from $(\mathrm{id} \otimes S)(F)$ by multiplication of the tensorands.[34] From this, we see that

$$S_F^2(a) = x S^2(a) x^{-1}$$

where $x = wS(w^{-1})$, and it can be shown that the Drinfel'd element u_F that arises from the R-matrix $R_F = F_t R F^{-1}$ is related to the original one via the formula $u_F = xu$.

In our case, we find

$$w = \sum_{i=1}^{m} (1 \otimes S(a_i)) S_{A\otimes A}(b_i \otimes 1) = \sum_{i=1}^{m} S(b_i) \otimes S(a_i) = R'$$

This implies in this case that $x = 1$, which means that the Drinfel'd elements of $(A\otimes A)_F$ and $A \otimes A$ coincide. Because Φ is a morphism of quasitriangular Hopf algebras, this element is equal to $\Phi(u_D)$. But for the Drinfel'd element of $A\otimes A$, we find

$$u_{A\otimes A} = \sum_{i,j=1}^{m} S_{A\otimes A}(b_i \otimes S(a_j))(a_i \otimes b_j) = \sum_{i,j=1}^{m} S(b_i)a_i \otimes S^2(a_j)b_j = u \otimes S^2(u^{-1})$$

Because the Drinfel'd element is invariant under the square of the antipode, this implies the assertion. □

Note that by replacing the R-matrix with the alternative R-matrix R'^{-1}, we get a second Hopf algebra homomorphism

$$\Phi' : D(A) \to (A\otimes A)_{F'};\ x \mapsto (\phi' \otimes \phi)(\Delta_D(x))$$

where this time we have to use the cocycle $F' := 1 \otimes R' \otimes 1 \in A^{\otimes 4}$ to twist the comultiplication on the right-hand side. As before, the Hopf algebra $(A \otimes A)_{F'}$ is quasitriangular with respect to the R-matrix $R_{F'} := F'_t R''_{A\otimes A} F'^{-1}$, where

$$R''_{A\otimes A} := \sum_{i,j=1}^{m} b_i \otimes a_j \otimes S(a_i) \otimes b_j$$

is an R-matrix for the tensor product Hopf algebra $A \otimes A$ and F'_t arises from F' by interchanging the first and the third as well as the second and the fourth tensor factor. By using this specific R-matrix, Φ' becomes a morphism of quasitriangular Hopf algebras in the sense that it maps the R-matrix of the Drinfel'd double to $R_{F'}$. Furthermore, the Drinfel'd element arising from the alternative R-matrix R'^{-1} is exactly the inverse u^{-1} of the original one, so that the preceding lemma yields that $\Phi'(u_D) = u^{-1} \otimes u$.

3.2 In the situation of Paragraph 3.1, we have a left action of $A \otimes A$ on A by requiring that the element $a \otimes a' \in A \otimes A$ acts on $b \in A$ by mapping it to $a'bS^{-1}(a)$. Pulling this action back along Φ', we get a left action of $D(A)$ on A given by

$$x \rightharpoonup b = \phi(x_{(2)})bS^{-1}(\phi'(x_{(1)}))$$

If $x = \varphi \otimes a$ and $R = \sum_{i=1}^{m} a_i \otimes b_i$, this action is explicitly given as

$$
\begin{aligned}
(\varphi \otimes a) \rightharpoonup b &= \rho(\varphi_{(1)} \otimes a_{(2)})\,b\,S^{-1}(\rho'(\varphi_{(2)} \otimes a_{(1)})) \\
&= \sum_{i,j=1}^{m} \varphi_{(1)}(a_i) b_i a_{(2)} b S^{-1}(\varphi_{(2)}(b_j) S(a_j) a_{(1)}) \\
&= \sum_{i,j=1}^{m} \varphi(a_i b_j) b_i a_{(2)} b S^{-1}(a_{(1)}) a_j
\end{aligned}
$$

We will use the same notation for the restrictions of this action to A and A^*, i.e., we define

$$
\begin{aligned}
a \rightharpoonup b &:= (\varepsilon \otimes a) \rightharpoonup b = a_{(2)} b S^{-1}(a_{(1)}) \\
\varphi \rightharpoonup b &:= (\varphi \otimes 1) \rightharpoonup b = \sum_{i,j=1}^{m} \varphi(a_i b_j) b_i b a_j
\end{aligned}
$$

Note that the restriction of the action to A is just the left adjoint action of A^{cop} on itself. The space of invariants for this restricted action therefore is exactly the center $Z(A)$ of A.

We also introduce the map

$$
\Phi : A^* \to A,\ \varphi \mapsto (\varphi \otimes 1) \rightharpoonup 1 = \sum_{i,j=1}^{m} \varphi(a_i b_j) b_i a_j = (\mathrm{id} \otimes \varphi)(R'R)
$$

If $C(A)$ denotes the subalgebra

$$
C(A) := \{\chi \in A^* \mid \chi(ab) = \chi(bS^2(a)) \text{ for all } a, b \in A\}
$$

of A^*, it is known[35] that Φ has the following property:

Proposition We have

$$
\Phi(\varphi\chi) = \Phi(\varphi)\Phi(\chi)
$$

for all $\varphi \in A^*$ and all $\chi \in C(A)$. Furthermore, we have

$$
a \rightharpoonup \Phi(\varphi) = \varphi_{(1)}(S^{-1}(a_{(2)}))\varphi_{(3)}(a_{(1)})\,\Phi(\varphi_{(2)})
$$

for all $\varphi \in A^*$ and all $a \in A$. Consequently, Φ restricts to an algebra homomorphism from $C(A)$ to $Z(A)$.

Proof. It is possible to verify these properties by direct computation; however, it is interesting to derive them from our construction of Φ. The second equation holds since

$$
\begin{aligned}
a \rightharpoonup \Phi(\varphi) = (\varepsilon \otimes a)(\varphi \otimes 1) \rightharpoonup 1 &= \varphi_{(1)}(S^{-1}(a_{(3)}))\varphi_{(3)}(a_{(1)})\,(\varphi_{(2)} \otimes a_{(2)}) \rightharpoonup 1 \\
&= \varphi_{(1)}(S^{-1}(a_{(2)}))\varphi_{(3)}(a_{(1)})\,\Phi(\varphi_{(2)})
\end{aligned}
$$

This amounts to saying that Φ is an A-linear map from A^* to A, where A^* is considered as an A-module via $a \otimes \varphi \mapsto \varphi_{(1)}(S^{-1}(a_{(2)}))\varphi_{(3)}(a_{(1)})\varphi_{(2)}$; this action is the left coadjoint action, built with the inverse antipode, and is actually used in the construction of the Drinfel'd double as a double crossproduct.[36] The space $C(A)$ is exactly the space of invariants for this action. As an A-linear map takes invariants to invariants, Φ maps $C(A)$ to the center $Z(A)$.

For the first assertion, note that we clearly have $\varphi \rightharpoonup z = (\varphi \rightharpoonup 1)z$ if $z \in Z(A)$, so that

$$\Phi(\varphi\psi) = (\varphi\psi) \rightharpoonup 1 = \varphi \rightharpoonup (\psi \rightharpoonup 1) = \varphi \rightharpoonup \Phi(\psi) = (\varphi \rightharpoonup 1)\Phi(\psi) = \Phi(\varphi)\Phi(\psi)$$

if $\psi \in C(A)$. Finally, note that it follows from the elementary properties of R-matrices[37] that Φ preserves the unit element. □

In a very similar way, we have a right action of $A \otimes A$ on A by requiring that the element $a \otimes a' \in A \otimes A$ acts on $b \in A$ by mapping it to $S^{-1}(a')ba$. Pulling this action back along π, we get a right action of $D(A)$ on A given by

$$b \leftharpoonup x = S^{-1}(\pi'(x_{(2)}))b\,\pi(x_{(1)})$$

The two actions are related via the formulas

$$S(x \rightharpoonup b) = S(b) \leftharpoonup S_D(x) \quad \text{and} \quad S(b \leftharpoonup x) = S_D(x) \rightharpoonup S(b)$$

If $x = \varphi \otimes a$ and $R = \sum_{i=1}^m a_i \otimes b_i$, this action is explicitly given as

$$\begin{aligned} b \leftharpoonup (\varphi \otimes a) &= S^{-1}(\pi'(\varphi_{(1)} \otimes a_{(2)}))b\,\pi(\varphi_{(2)} \otimes a_{(1)}) \\ &= \sum_{i,j=1}^m S^{-1}(\varphi_{(1)}(b_i)S(a_i)a_{(2)})b\varphi_{(2)}(a_j)b_j a_{(1)} \\ &= \sum_{i,j=1}^m \varphi(b_i a_j)S^{-1}(a_{(2)})a_i b b_j a_{(1)} \end{aligned}$$

As before, we use the same notation for the restrictions of this action to A and A^*, so that

$$\begin{aligned} b \leftharpoonup a &:= b \leftharpoonup (\varepsilon \otimes a) = S^{-1}(a_{(2)})ba_{(1)} \\ b \leftharpoonup \varphi &:= b \leftharpoonup (\varphi \otimes 1) = \sum_{i,j=1}^m \varphi(b_i a_j)a_i b b_j \end{aligned}$$

Note that the restriction of the action to A is just the right adjoint action of A^{cop} on itself, and as for the left adjoint action considered before, the space of invariants is the center $Z(A)$.

We also introduce the map

$$\Psi : A^* \to A, \; \varphi \mapsto (1 \leftharpoonup \varphi) = \sum_{i,j=1}^m \varphi(b_i a_j)a_i b_j = (\varphi \otimes \mathrm{id})(R'R)$$

This map has similar properties as the map Φ: If $C(A)$ denotes the subalgebra

$$C(A) := \{\varphi \in A^* \mid \varphi(ab) = \varphi(bS^2(a)) \text{ for all } a,b \in A\}$$

of A^*, we have

$$\Psi(\psi\varphi) = \Psi(\psi)\Psi(\varphi)$$

for all $\psi \in C(A)$ and all $\varphi \in A^*$. Furthermore, Ψ satisfies

$$\Psi(\varphi) \leftarrow a = \varphi_{(1)}(a_{(2)})\varphi_{(3)}(S^{-1}(a_{(1)}))\,\Psi(\varphi_{(2)})$$

i.e., it is an A-linear map from A^* with the right coadjoint action, built with the inverse antipode, to A with right adjoint action of A^{cop}. The space of invariants of the right coadjoint action is $C(A)$, whereas the space of invariant of the right adjoint action is the center $Z(A)$, so that Ψ restricts to an algebra homomorphism from $C(A)$ to $Z(A)$. These properties can be verified directly[38] or derived from our construction of Ψ in a way similar to the proof of the preceding proposition. It is also possible to derive them from the corresponding properties of Φ, as we have

$$S(\Psi(\varphi)) = S(\varphi \otimes 1) = S(1) \otimes S^{-1}(\varphi) = \Phi(S^{-1}(\varphi))$$

and similarly $S(\Phi(\varphi)) = \Psi(S^{-1}(\varphi))$.

The mappings Φ and Ψ are related in various ways to the Drinfel'd element u. Besides the equations

$$\Phi(\varphi) = (\mathrm{id} \otimes \varphi)((u \otimes u)\Delta(u^{-1})) = (\mathrm{id} \otimes \varphi)(\Delta(u^{-1})(u \otimes u))$$

and

$$\Psi(\varphi) = (\varphi \otimes \mathrm{id})((u \otimes u)\Delta(u^{-1})) = (\varphi \otimes \mathrm{id})(\Delta(u^{-1})(u \otimes u))$$

which are direct consequences of the identity for $\Delta(u)$ stated in Paragraph 2.1, we also have the following relation: The element $g := uS(u^{-1})$ is a grouplike element.[39] If $\chi \in C(A)$, define $\chi' \in A^*$ by $\chi'(a) := \chi(ag^{-1})$. Then $\chi' \in C(A)$, and[40] $\Phi(\chi') = \Psi(\chi)$.

As it turns out,[41] the four conditions that Φ is bijective, that Ψ is bijective, that ι is bijective, and that ι' is bijective, are all equivalent. If these conditions are satisfied, the Hopf algebra A is called factorizable.[42]

3.3 If A is the Drinfel'd double of a finite-dimensional Hopf algebra H, the mapping Φ takes a very simple form. To make this explicit, we decompose the dual of the double in the form $D(H)^* = H \otimes H^*$, where we use the isomorphism

$$H \otimes H^* \to D(H)^*;\; h \otimes \varphi \mapsto (\varphi' \otimes h' \mapsto \varphi'(h)\varphi(h'))$$

From the form of the R-matrix of the Drinfel'd double described in Paragraph 2.2, we see that

$$R'R = \sum_{i,j=1}^{n} (b_j \otimes b_i^*) \otimes (\varepsilon \otimes b_j)(b_i^* \otimes 1)$$

so that $\Phi(h \otimes \varphi) = (h \otimes \varphi \otimes \mathrm{id})(R'R) = (\varepsilon \otimes h)(\varphi \otimes 1)$. A similar formula holds for $\bar\Phi$ under additional restrictions:[43]

Lemma Suppose that $\chi = \sum_j h_j \otimes \varphi_j \in D(H)$.

1. If $\chi \in C(D(H))$, then $\Phi(\chi) = \sum_j S^2(\varphi_j) \otimes h_j$.
2. If $\chi \in C(D(H))$, then $\bar\Phi(\chi) = \sum_j S^{-2}(\varphi_j) \otimes h_j$.

Proof. For the first assertion, we have

$$\begin{aligned}
\Phi(\chi) &= \sum_{i,j=1}^{n} (b_j \otimes b_i)(\chi)\,((\varepsilon \otimes b_j)(b_i \otimes 1)) \\
&= \sum_{i,j=1}^{n} (b_j \otimes b_i)(\chi)\,((b_i \otimes 1)S_D^2(\varepsilon \otimes b_j)) \\
&= \sum_{i,j=1}^{n} (b_j \otimes b_i)(\chi)\,(b_i \otimes S^2(b_j)) = \sum_j S^2(\varphi_j) \otimes h_j
\end{aligned}$$

The proof of the second assertion is very similar. $\Box$

At the end of Paragraph 3.2, we have expressed the mappings Φ and $\bar\Phi$ in terms of the Drinfel'd element. In the case of a Drinfel'd double, we can replace the Drinfel'd element by the evaluation form to get very similar formulas for their inverses:

Proposition Suppose that $D = D(H)$ is the Drinfel'd double of a finite-dimensional Hopf algebra H. Then we have for $x \in D(H)$ that

1. $\Phi^{-1}(x) = ((\mathrm{id}_H \otimes S^2) \circ S_D^{-1})(e^{-1}_{(1)} e)\,(e^{-1}_{(2)} e)(x)$
2. $\bar\Phi^{-1}(x) = (S_D \circ (S^2 \otimes \mathrm{id}))(e e^{-1}_{(2)})\,(e e^{-1}_{(1)})(x)$

Proof. We can assume that $x = \varphi \otimes h$ for $\varphi \in H^*$ and $h \in H$. Suppose that $b_1, \dots, b_n$ is a basis of H with dual basis $b^1, \dots, b^n$. Using the form of the R-matrix given in Paragraph 2.2, we find

$$\begin{aligned}
&(((\mathrm{id}_H \otimes S^2) \circ S_D^{-1})(e^{-1}_{(1)} e))\,(e^{-1}_{(2)} e)(x) \\
&= \sum_{i,j=1}^{n} S_D^{-1}(e^{-1}_{(1)} e)(b_i \otimes S^2(b_j))(\varepsilon \otimes b^i)(b^j \otimes 1)e^{-1}_{(2)}(\varphi_{(2)} \otimes h_{(1)})e(\varphi_{(1)} \otimes h_{(2)}) \\
&= \sum_{i,j=1}^{n} e(b_{i(2)} \otimes S^2(b_{j(1)}))e^{-1}_{(1)}(S_D^{-1}(b_{i(1)} \otimes S^2(b_{j(2)})))(\varepsilon \otimes b^i)(b^j \otimes 1) \\
&\qquad\qquad e^{-1}_{(2)}(\varphi_{(2)} \otimes h_{(1)})\varphi_{(1)}(h_{(2)})
\end{aligned}$$

where we have used the fact that e is invariant under the antipode observed in the proof of Lemma 2.3. Using the definition of e, this becomes

$$(((\mathrm{id}_H \otimes S^2) \otimes S_D^{-1})(e^{-1}_{(1)}e)) \otimes (e^{-1}_{(2)}e)(x) =$$
$$\sum_{i,j=1}^{n} b_{i(2)}(S^2(b_{j(1)}))e^{-1}(S_D^{-1}(b_{i(1)} \otimes S^2(b_{j(2)}))(\varphi_{(2)} \otimes h_{(1)}))\varphi_{(1)}(h_{(2)})$$
$$(\varepsilon \otimes b_i)(b_j \otimes 1) =$$
$$\sum_{i,j=1}^{n} b_{i(2)}(S^2(b_{j(1)}))e^{-1}(S(b_{i(1)})\varphi_{(2)} \otimes h_{(1)}S(b_{j(2)}))\varphi_{(1)}(h_{(2)})(\varepsilon \otimes b_i)(b_j \otimes 1)$$

where, in the last step, we have used that the antipode is antimultiplicative and that e^{-1} is cocommutative. Using the explicit form of e^{-1}, this becomes

$$(((\mathrm{id}_H \otimes S^2) \otimes S_D^{-1})(e^{-1}_{(1)}e)) \otimes (e^{-1}_{(2)}e)(x) =$$
$$\sum_{i,j=1}^{n} b_{i(2)}(S^2(b_{j(1)}))\, S(b_{i(1)})\varphi_{(2)}(b_{j(2)}S^{-1}(h_{(1)}))\varphi_{(1)}(h_{(2)})(\varepsilon \otimes b_i)(b_j \otimes 1) =$$
$$\sum_{i,j=1}^{n} b_{i(2)}(S^2(b_{j(1)}))\varphi_{(1)}(h_{(3)})$$
$$S(b_{i(1)})(b_{j(2)}S^{-1}(h_{(2)}))\varphi_{(2)}(b_{j(3)}S^{-1}(h_{(1)}))(\varepsilon \otimes b_i)(b_j \otimes 1) =$$
$$\sum_{i,j=1}^{n} b_i(h_{(2)}S(b_{j(2)})S^2(b_{j(1)}))\varphi(h_{(3)}b_{j(3)}S^{-1}(h_{(1)}))(\varepsilon \otimes b_i)(b_j \otimes 1)$$

Using the antipode equation, we can cancel two terms to get

$$(((\mathrm{id}_H \otimes S^2) \otimes S_D^{-1})(e^{-1}_{(1)}e)) \otimes (e^{-1}_{(2)}e)(x) =$$
$$\sum_{i,j=1}^{n} b_i(h_{(2)})\varphi(h_{(3)}b_jS^{-1}(h_{(1)}))(\varepsilon \otimes b_i)(b_j \otimes 1) =$$
$$\sum_{j=1}^{n} \varphi(h_{(3)}b_jS^{-1}(h_{(1)}))(\varepsilon \otimes h_{(2)})(b_j \otimes 1) =$$
$$\varphi_{(1)}(h_{(3)})\varphi_{(3)}(S^{-1}(h_{(1)}))(\varepsilon \otimes h_{(2)})(\varphi_{(2)} \otimes 1) = \varphi \otimes h = x$$

This proves the first formula. For the second formula, recall from Paragraph 3.2 that $\Phi^{-1} = S_D \otimes \Phi^{-1} \otimes S_D$, so that we get from the first formula

$$\begin{aligned}\Phi^{-1}(x) &= (S_D \otimes \Phi^{-1} \otimes S_D)(x) = (S_D \otimes (\mathrm{id} \otimes S^2) \otimes S_D^{-1})(e^{-1}_{(1)}e) \otimes (e^{-1}_{(2)}e)(S_D(x)) \\ &= (S_D \otimes (S^2 \otimes \mathrm{id}) \otimes S_D)(e^{-1}_{(1)}e) \otimes (e^{-1}_{(2)}e)(S_D(x)) \\ &= (S_D \otimes (S^2 \otimes \mathrm{id}))(ee^{-1}_{(2)}) \otimes (ee^{-1}_{(1)})(x)\end{aligned}$$

as asserted. $\Box$

Note that, in the case where the antipode of H is an involution, these formulas reduce to

$$^{1}(x) = S_D\ (e_{(1)}^{\ 1}e)\ (e_{(2)}^{\ 1}e)(x) \qquad\qquad {}^{1}(x) = S_D\ (ee_{(2)}^{\ 1})\ (ee_{(1)}^{\ 1})(x)$$

which should be compared with the ones given in Paragraph 3.2 using the Drinfel'd element.

3.4 If $f : A \ ! \ B$ is a morphism of quasitriangular Hopf algebras, then it follows directly from the formulas for and given in Paragraph 3.2 that the diagrams

$$\begin{tikzcd} B \arrow[r, "f"] \arrow[d, "B"'] & A \arrow[d, "A"] \\ B \arrow[r, "f"'] & A \end{tikzcd} \qquad\qquad \begin{tikzcd} B \arrow[r, "f"] \arrow[d, "B"'] & A \arrow[d, "A"] \\ B \arrow[r, "f"'] & A \end{tikzcd}$$

commute, where the index indicates to which Hopf algebra the mapping belongs. Applying this to , we see that the diagrams

$$\begin{tikzcd} (A \quad A)_F \arrow[r] \arrow[d] & D(A) \arrow[d] \\ (A \quad A)_F \arrow[r] & D(A) \end{tikzcd} \qquad\qquad \begin{tikzcd} (A \quad A)_F \arrow[r] \arrow[d] & D(A) \arrow[d] \\ (A \quad A)_F \arrow[r] & D(A) \end{tikzcd}$$

commute. Now we have by definition that $(A \quad A)_F = A \quad A$ as algebras. But these two Hopf algebras have even more things in common:

Lemma We have $C((A \quad A)_F) = C(A \quad A)$ and $C((A \quad A)_F) = C(A \quad A)$ as algebras.

Proof. We have already seen in the proof of Lemma 3.1 that the Drinfel'd elements of $(A \quad A)_F$ and $A \quad A$ coincide. Therefore, the squares of the antipodes coincide, too. This implies the asserted equalities as vector spaces. That the products also agree follows from the fact that $(S^2 \quad S^2)(F) = F$ in our case. 2

From this lemma, we can extract the following information about the restrictions of and :

Proposition The diagrams

$$\begin{tikzcd}
C(A)\otimes C(A) \arrow[rr, "\bar{\ }"] \arrow[d, "(S\otimes\ )"'] & & C(D(A)) \arrow[d] \\
A\otimes A \arrow[rr] & & Z(D(A))
\end{tikzcd}$$

and

$$\begin{tikzcd}
C(A)\otimes C(A) \arrow[rr, "\bar{\ }"] \arrow[d, "(S\otimes\ )"'] & & C(D(A)) \arrow[d] \\
A\otimes A \arrow[rr] & & Z(D(A))
\end{tikzcd}$$

commute.

Proof. From the formula $R_F = F_t R_{A\otimes A} F^{-1}$ for the twisted R-matrix, we get immediately that $R^0_F R_F = F R^0_{A\otimes A} R_{A\otimes A} F^{-1}$. Now we have

$$R^0_{A\otimes A} R_{A\otimes A} = \sum_{i,j,k,l=1}^{m} b_k a_i \otimes S(a_l) b_j \otimes a_k b_i \otimes b_l S(a_j)$$

and therefore

$$R^0_F R_F = \Big(\sum_{p=1}^{m} 1 \otimes S(a_p) \otimes b_p \otimes 1\Big) R^0_{A\otimes A} R_{A\otimes A} \Big(\sum_{q=1}^{m} 1 \otimes a_q \otimes b_q \otimes 1\Big)$$

$$= \sum_{i,j,k,l,p,q=1}^{m} b_k a_i \otimes S(a_p) S(a_l) b_j a_q \otimes b_p a_k b_i b_q \otimes b_l S(a_j)$$

For two elements $\varphi, \psi \in C(A)$, we therefore find

$$(\varphi \otimes \psi) = \sum_{i,j,k,l,p,q=1}^{m} b_k a_i \otimes S(a_p) S(a_l) b_j a_q \varphi(b_p a_k b_i b_q)\, \psi(b_l S(a_j))$$

Now note that

$$\sum_{j,l=1}^{m} S(a_l) b_j\, \psi(b_l S(a_j)) = \sum_{j,l=1}^{m} S(a_l) b_j\, \psi(S(a_j) S^2(b_l)) = \sum_{j,l=1}^{m} a_l b_j\, \psi(S(a_j) S(b_l))$$

$$= \sum_{j,l=1}^{m} S^{-1}(S(b_j) S(a_l))\, \psi(S(a_j) S(b_l))$$

$$= \sum_{j,l=1}^{m} S^{-1}(b_j a_l)\, \psi(a_j b_l) = S^{-1}(\ (\psi))$$

which is a central element by Proposition 3.2. We can therefore rewrite the above expression in the form

$$\Theta(\varphi \otimes \gamma) = \sum_{i,k,p,q=1}^{n} b_k a_i \otimes S(a_p) a_q S^{-1}(\Phi(\gamma)) \varphi(b_p a_k b_i b_q)$$

But in this expression, we can cancel the summation over p and q, as we have

$$\sum_{p,q=1}^{n} S(a_p) a_q \varphi(b_p a_k b_i b_q) = \sum_{p,q=1}^{n} S(a_p) a_q \varphi(a_k b_i b_q S^2(b_p))$$
$$= \sum_{p,q=1}^{n} a_p a_q \varphi(a_k b_i b_q S(b_p)) = \sum_{p,q=1}^{n} a_p a_q \varphi(a_k b_i S(b_p S^{-1}(b_q))) = 1\varphi(a_k b_i)$$

After this cancellation, we get

$$\Theta(\varphi \otimes \gamma) = \sum_{i,k=1}^{n} b_k a_i \otimes S^{-1}(\Phi(\gamma)) \varphi(a_k b_i)$$
$$= \Phi(\varphi) \otimes S^{-1}(\Phi(\gamma)) = \Phi(\varphi) \otimes S(\Phi(\gamma))$$

where the last step follows from the fact that $S^2(\Phi(\gamma)) = u\Phi(\gamma)u^{-1} = \Phi(\gamma)$ since $\Phi(\gamma)$ is central. This shows the commutativity of the first diagram. The commutativity of the second diagram follows from similar computations. $\square$

Note that, in contrast to the factorizable case, it is not true in general that Θ maps the center of $D(A)$ to the center of $A \otimes A$, as the example of a group ring with an R-matrix equal to the unit shows.

In the whole discussion, it is possible to replace the original R-matrix by R'^{-1}. We have already pointed out above that this interchanges Φ and Φ' as well as F and F'. The analogue of Φ is the map that assigns to every $\varphi \in A^*$ the element $(\mathrm{id} \otimes \varphi)(R^{-1}R'^{-1})$. If $\varphi \in C(A)$, this element can be expressed in terms of the original map Φ as follows:

$$(\mathrm{id} \otimes \varphi)(R^{-1}R'^{-1}) = \sum_{i,j=1}^{n} S(a_i) b_j \varphi(b_i S(a_j)) = \sum_{i,j=1}^{n} S(a_i) b_j \varphi(S(a_j) S^2(b_i))$$
$$= S^{-1}\Big(\sum_{i,j=1}^{n} S(b_j) S^2(a_i) \varphi(S(a_j) S^2(b_i))\Big)$$
$$= S^{-1}\Big(\sum_{i,j=1}^{n} b_j a_i \varphi(a_j b_i)\Big) = S^{-1}(\Phi(\varphi)) = S(\Phi(\varphi))$$

where the last step uses the argument from the end of the proof of the preceding proposition. Something similar holds for the analogue of Ψ: If $\varphi \in C(A)$, we have

$$(\varphi \otimes \mathrm{id})(R^{-1}R'^{-1}) = S(\Psi(\varphi))$$

as can be seen by a similar computation. Therefore, the corresponding commutative diagrams for ^{0} are

$$\begin{tikzcd}
C(A) \quad C(A) \arrow[rr, "0"] \arrow[d, "(S \quad)"'] & & C(D(A)) \arrow[d] \\
A \quad A \arrow[rr, "0"'] & & Z(D(A))
\end{tikzcd}$$

and

$$\begin{tikzcd}
C(A) \quad C(A) \arrow[rr, "0"] \arrow[d, "(S \quad)"'] & & C(D(A)) \arrow[d] \\
A \quad A \arrow[rr, "0"'] & & Z(D(A))
\end{tikzcd}$$

3.5 Let us now assume in addition that our quasitriangular Hopf algebra A is also factorizable. It is then nite-dimensional and unimodular,[44] which implies[45] that a right integral $\ 2\ A$ must be contained in $C(A)$. The image of this integral under is again an integral:

Lemma ( ) is a two-sided integral of A.

Proof. It follows from the discussion in Paragraph 3.2 that

$$(\ )\ (')=\ \ (\ ')=\ '(1)\ (\ )=\ "(\ (')) \ (\ )$$

for all $'\ 2\ A$. Because A is factorizable, every $a\ 2\ A$ can be written in the form $a = \ (')$, showing that ( ) is a right integral. It is also a left integral since A is unimodular, or alternatively because ( ) is central, as we saw in Paragraph 3.2. 2

From this lemma, it follows in particular that $(\ (\ ))\ =\ (\quad)(R^0R)\ \neq\ 0$ if $\neq\ 0$, because nonzero integrals do not vanish on nonzero integrals.[46] It also shows that a factorizable Hopf algebra is semisimple if and only if it is cosemisimple, because $(1) = "(\ (\ ))$, and, by Maschke's theorem, A is cosemisimple if and only if $(1)\neq\ 0$, and semisimple if and only if $"(\ (\ ))\neq\ 0$.[47] Finally, it also shows that, for a left integral $\ 2\ A$, the element ( ) is a two-sided integral of A, since we get from Paragraph 3.2 that $S(\ (\ )) = \ (S^{\ 1}\ (\ ))$.

We now discuss how the integrals behave under . It is obvious that is a right integral on the tensor product Hopf algebra A A. Therefore, a general result on the behavior of integrals under twisting,[48] together with the discussion in Lemma 3.1, yields that it is also a right integral on $(A \quad A)_F$. As is a Hopf algebra isomorphism, ( ) must be a right integral on $D(A)$. To make this more precise, we decompose the dual of the double in the form $D(A) = A \quad A$ as described in Paragraph 3.3. We then get the following formulas for the integrals:

Proposition Suppose that $\; 2 A$ is a left integral, that $\; 2 A$ is a right integral, and that $\; 2 A$ is a two-sided integral. Then we have

1. $(\quad) = (\;)$
2. $(\quad) = (\;)$
3. $(\quad) = (\;)$

Proof. (1) To establish the rst assertion, we compute as follows:

$$\begin{aligned}
(\quad) &= (\;_{(2)} \quad _{(1)}) \quad {}^{0}(\;_{(1)} \quad _{(2)}) \\
&= \sum_{i;j=1}^{m} \;_{(2)}(a_i)b_i \;_{(1)} \quad _{(1)}(b_j)S(a_j) \;_{(2)} = \sum_{i;j=1}^{m} (b_j a_i)b_i \;_{(1)} \quad S(a_j) \;_{(2)} \\
&= \sum_{i;j=1}^{m} (b_j a_i)b_i S^2(a_j) \;_{(1)} \quad _{(2)} = \sum_{i;j=1}^{m} (a_i S^2(b_j))b_i S^2(a_j) \;_{(1)} \quad _{(2)} \\
&= \sum_{i;j=1}^{m} (a_i b_j)b_i a_j \;_{(1)} \quad _{(2)} = (\;) \;_{(1)} \quad _{(2)} = (\;)
\end{aligned}$$

where unimodularity is used in particular for the fth equation.

(2) For the second assertion, we get from Proposition 3.4 that

$$(\quad (\quad)) = {}^{1}((\;) \quad S((\;))) = {}^{1}((\;) \quad (\;))$$

since $\; 2 C(A)$. But this gives $(\quad (\quad)) = \quad (\;)$ by the assertion just established. Since $C(D(A))$ and $Z(D(A))$ have the same dimension, it now follows from Lemma 3.3 that[49]

$$(\quad) = {}^{1}(\quad (\;)) = (\;) \quad S^{\;2}(\;) = (\;)$$

(3) For the third assertion, we substitute $(\;)$ for and $S \; (\;)$ for into the rst assertion to get, using another result from Paragraph 3.2, that

$$(S \; (\;) \quad (\;)) = (S \; (\;)) \quad (\;) = S^{\;1}((\;)) \quad (\;) = (\;) \quad (\;)$$

Using the second part of Proposition 3.4 on the right-hand side, this becomes $(S \; (\;) \quad (\;)) = (\quad)(\quad)$, so that

$$S \; (\;) \quad (\;) = (\quad)(\quad)$$

Since the left-hand side is a two-sided integral of D (A), it is invariant under the antipode, so that we can rewrite this equation as

$$
\begin{aligned}
(\quad)(\quad) &= S_D(S(\;)\quad(\;)) = S_D(''\quad(\;))S_D(S(\;)\quad 1) \\
&= (''\quad(\;))(\quad 1) = (\;(\;)\quad)
\end{aligned}
$$

by the discussion in Paragraph 3.3. Now cancelling gives the assertion. 2

4 The action of the modular group

4.1 In our factorizable Hopf algebra A, we now fix a nonzero right integral , and introduce the map

$$:A \to A; a \mapsto (a) := {}_{(1)}(a) {}_{(2)}$$

The fact that is a Frobenius homomorphism[50] implies that is bijective. The fact that $\in C(A)$ implies that is an A-linear map from A with the right adjoint action of A to A with the right coadjoint action, built with the inverse antipode, which we have considered in Paragraph 3.2. In particular, induces an isomorphism between the spaces of invariants of these actions; in other words, it restricts to a bijection between the center $Z(A)$ and the algebra $C(A)$.[51] Following[52] [25], Eq. (2.55), p. 369, we use to introduce the maps $S \in \mathrm{End}(A)$ and $S \in \mathrm{End}(A)$ as

$$S := S \qquad\qquad S := S^{1}$$

It is important to distinguish S from the transpose S of S. Using the form of the R-matrix given in Paragraph 2.1, we have explicitly

$$S(a) = \sum_{i,j=1}^{m} (ab_i a_j) S(a_i b_j)$$

The relationship of these maps is clarified in the following proposition, which also lists some of their basic properties:

Proposition S is an A-linear map from the right adjoint representation of A to itself. In particular, S preserves the center $Z(A)$ of A. Furthermore, the diagrams

$$\begin{tikzcd} A \arrow[r, "S"] \arrow[d] & A \arrow[d] \\ A \arrow[r, "S"'] & A \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "S"] & A \\ A \arrow[r, "S"'] \arrow[u] & A \arrow[u] \end{tikzcd}$$

are commutative, and we have $S \quad S = S \quad S$.

Proof. The composition of A-linear maps is A-linear. From the linearity properties of and discussed so far, we get that is A-linear from the right adjoint representation of A to the right adjoint representation of A^{cop}; i.e., satisfies

$$(\quad)(S(a_{(1)})ba_{(2)}) = S^{1}(a_{(2)})(\quad)(b)a_{(1)}$$

Applying the antipode to this equation gives $S(S(a_{(1)})ba_{(2)}) = S(a_{(1)})S(b)a_{(2)}$, which is the first assertion. The preservation of the center is a direct consequence. The commutativity of the first diagram follows from the equation

$$S \quad = \quad S^{-1} \quad = S \quad = S$$

where we have used the fact that $S \quad = \quad S^{-1}$ established in Paragraph 3.2. To establish the commutativity of the second diagram, we first derive the formula $S \quad = \quad S$. For $' \in A$ and $a \in A$, we have

$$S(')(a) = '(S(a)) = '(S((a)))) = ((a) \quad S('))(R^0R) = (a)((S(')))$$
$$= (a)(S^{-1}((')))= (aS^{-1}((')))= (S((')) a) = (S(('))) (a)$$

where we have used for the second last equality that $\in C(A)$. From this, we immediately get the commutativity of the second diagram, as we now have $S \quad = \quad S \quad = \quad S$. Furthermore, using the results from Paragraph 3.2, we can rewrite the formula for S above in the form $S \quad = \quad S^{1}$, which yields $S \quad S = \quad = S \quad S$. 2

It may be noted that the commutativity of the second diagram is equivalent to the condition $(S(a)b) = (aS(b))$, which is an adjunction property of S with respect to the associative bilinear form determined by the Frobenius homomorphism .

4.2 As we have explained in Paragraph 2.1, $R^{0\,-1}$ is always an alternative choice for the R-matrix of a quasitriangular Hopf algebra. This raises the question how S is modified if one replaces R by $R^{0\,-1}$. The answer to this question is that, up to a scalar multiple, S turns into its inverse:

Proposition $$S^{-1}(a) = \frac{1}{(\quad)(R^0R)} \sum_{i,j=1}^{m} (aa_ib_j)S^2(a_j)b_i$$

Proof. Because A is finite-dimensional, it suffices to prove that

$$\sum_{i,j=1}^{m} (aa_ib_j)S(S^2(a_j)b_i) = (\quad)(R^0R)\,a$$

To see this, we use the identity $(ab_{(1)})S(b_{(2)}) = (a_{(1)}b)a_{(2)}$ to compute

$$\sum_{i,j=1}^{m} (aa_ib_j)S(S^2(a_j)b_i) = \sum_{i,j,k,l=1}^{m} (aa_ib_j)\quad (S^2(a_j)b_ib_ka_l)\,S(a_kb_l)$$
$$= \sum_{i,j,k,l=1}^{m} (aa_ib_j)\quad (b_ib_ka_la_j)\,S(a_kb_l) = \sum_{i,j=1}^{m} (aa_{i(1)}b_{j(1)})\quad (b_ia_j)S(a_{i(2)}b_{j(2)})$$
$$= \sum_{i,j=1}^{m} (a_{(1)}a_ib_j)\quad (b_ia_j)\,a_{(2)} = (a_{(1)}\quad (\quad))\,a_{(2)} = ((\quad))\,a$$

where the last step follows from Lemma 3.5.2

This formula has an interesting consequence for the restriction of S to the center:

Corollary For all $a \in Z(A)$, we have $S^2(a) = (\lambda \otimes \lambda)(R'R)\, S(a)$.

Proof. In this case, we get from the formula in the preceding proposition that

$$(\lambda \otimes \lambda)(R'R)\, S^{-1}(a) = \sum_{i,j=1}^{m} \lambda(a a_i b_j) S^2(a_j) b_i = \sum_{i,j=1}^{m} \lambda(a a_i S^{-2}(b_j)) a_j b_i$$
$$= \sum_{i,j=1}^{m} \lambda(b_j a a_i) a_j b_i = \sum_{i,j=1}^{m} \lambda(a b_j a_i) a_j b_i = S^{-1}(S(a))$$

which becomes the assertion if we insert $S(a)$ for a. $\Box$

By rescaling λ if necessary, we can achieve that $(\lambda \otimes \lambda)(R'R) = 1$, as we saw in Paragraph 3.5 that this expression is nonzero, and in our algebraically closed field every element has a square root. In this case, the formula in the preceding corollary asserts that $S^2(a) = S(a)$ for all $a \in Z(A)$.

4.3 Recall[53] that a ribbon element is a nonzero central element $v \in A$ that satisfies

$$\Delta(v) = (R'R)(v \otimes v) \quad \text{and} \quad S(v) = v$$

It follows[54] that v is an invertible element that satisfies $\varepsilon(v) = 1$ as well as $v^2 = uS(u)$. We use it to define the endomorphism

$$T : A \to A,\ a \mapsto va$$

which is just multiplication by the central element v. The fact that v is central directly yields the equation $\lambda(T(a)b) = \lambda(aT(b))$, which can, as for S in Paragraph 4.1, be expressed by saying that the diagram

$$\begin{tikzcd}
A \arrow[r, "T"] & A \\
A \arrow[u] \arrow[r, "T"'] & A \arrow[u]
\end{tikzcd}$$

is commutative.

The decisive relation between S and T is the following:[55]

Proposition $S \quad T \quad S = \quad (v)\, T^{1} \quad S \quad T^{1}$

Proof. From Proposition 4.2, we have

$$(\; (\;))\,(S^{\;1} \quad T \quad S\,)(a) = \quad ((\;))\sum_{i;j=1}^{m} (ab_i a_j\,) S^{\;1}(vS\,(a_i b_j))$$

$$= \sum_{i;j;k;l=1}^{m} (ab_i a_j\,) \quad (vS\,(a_i b_j\,) a_k\, b_l) S^{2}(a_l) b_k$$

$$= \sum_{i;j;k;l=1}^{m} (ab_i a_j\,) \quad (S^{2}(b_l) vS\,(b_j\,) S\,(a_i\,) a_k\,) S^{2}(a_l) b_k$$

$$= \sum_{i;j;k;l=1}^{m} (aS^{\;1}(b_i) S^{\;1}(a_j\,)) \quad (vb_l b_j a_i a_k\,) a_l b_k$$

$$= \sum_{i;j=1}^{m} (aS^{\;1}(b_{i(2)}) S^{\;1}(a_{j(2)})) \quad (vb_j a_i\,) a_{j(1)} b_{i(1)}$$

Using that $(1 \quad v^{\;1}) \quad (v) = \sum_{i;j=1}^{m} vb_j a_i \quad a_j b_i$, we can write this in the form

$$(\; (\;))\,(S^{\;1} \quad T \quad S\,)(a) = \quad (aS^{1}(v_{(2)}^{\;1} v_{(3)})) \quad (v_{(1)}) v_{(1)}^{\;1} v_{(2)}$$
$$= \quad (aS^{\;1}(v_{(2)}^{\;1})) \quad (v) v_{(1)}^{\;1}$$

On the other hand, we have that

$$(v^{\;1}) = \; (v^{\;1} \quad v^{\;1})(R^{0} R\,)^{\;1} = \sum_{i;j=1}^{m} v^{\;1} a_i b_j \quad v^{\;1} S^{\;1}(b_i) S\,(a_j\,)$$

so that Proposition 4.2 also implies that

$$(\; (\;))\,(T^{\;1} \quad S^{\;1} \quad T^{\;1})(a) = \sum_{i;j=1}^{m} (v^{\;1} a a_i b_j\,) v^{\;1} S^{2}(a_j\,) b_i = \quad (av_{(1)}^{\;1})\, S\,(v_{(2)}^{\;1})$$

Comparing both expressions and using $S\,(v^{\;1}) = v^{\;1}$, we get that

$$(S^{\;1} \quad T \quad S\,)(a) = \quad (v)\,(T^{1} \quad S^{\;1} \quad T^{\;1})(a)$$

which is equivalent to the assertion. 2

The restrictions of S and T to the center of A induce of course also automorphisms of the corresponding projective space $P\,(Z\,(A\,))$ of one-dimensional subspaces of $Z\,(A\,)$, which are even independent of the choice of the integral . It is a consequence of the results above that these automorphisms yield a projective representation of the modular group:

Corollary There is a unique homomorphism from $SL(2;\mathbb{Z})$ to $PGL(Z(A))$ that maps s to the equivalence class of S and t to the equivalence class of T.

Proof. The homomorphism is unique because s and t generate the modular group, as discussed in Paragraph 1.1. For the existence question, recall the defining relations $s^4 = 1$ and $(ts)^3 = s^2$. Because the square of the antipode is given by conjugation with the Drinfel'd element,[56] it restricts to the identity on the center, and therefore Corollary 4.2 implies the first relation needed. The second defining relation $tststs = s^2$ can also be written in the form $sts = t^{-1}st^{-1}$, and therefore it follows from the preceding proposition that this relation is satisfied, too. $\Box$

The proof shows that if $(\quad)(R'R) = 1$ and $(v) = 1$, we even get a linear representation $SL(2;\mathbb{Z}) \to GL(Z(A))$ by assigning S to s and T to t. However, this happens if and only if $(v) = (v^{-1})$, as we see from the following lemma:[57]

Lemma $(\quad)(R'R) = (v)\ (v^{-1})$

Proof. We have seen in Lemma 3.5 that $(\ ) = (v^{-1}v_{(1)})v^{-1}v_{(2)} \in A$ is a two-sided integral. We therefore have

$$(v^{-1}v_{(1)})v_{(2)} = v\ (\ ) = "(v)\ (\ ) = \ (\ )$$

Now there is a grouplike element $g \in A$, called the right modular element, that satisfies $a_{(1)}\ (a_{(2)}) = g\ (a)$ for all $a \in A$, and furthermore $(ag) = (S^{-1}(a))$.[58] The preceding computation therefore yields that

$$\begin{aligned} (\quad)(R'R) &= (\ (\ )) = (v^{-1}v_{(1)})\ (v_{(2)}) \\ &= (v^{-1}g)\ (v) = (S^{-1}(v^{-1}))\ (v) = (v^{-1})\ (v) \end{aligned}$$

as asserted. $\Box$

It may be noted that we have discussed after Lemma 3.5 that this quantity is nonzero if is nonzero. Furthermore, since A is unimodular, the right modular element g that appears in the preceding proof is exactly the grouplike element, also denoted by g, that appeared in the discussion at the end of Paragraph 3.2.[59] It should also be noted that we do not claim that it is impossible to modify the representation so that it becomes linear.[60]

4.4 We have seen in Proposition 3.5 that $_D := (\quad) = (\ )$ is a right integral in $D(A)$. As in the case of A itself, we therefore get an isomorphism

$$_D : D(A) \to D(A)\ ;\ x \mapsto \ _D(x) := \ _{D(1)}(x)\ _{D(2)}$$

Since ${}_D$ is defined as the image of under the Hopf algebra homomorphism, it is obvious that the diagram

$$\begin{tikzcd}
D(A) \arrow[r] & A \otimes A \\
D(A) \arrow[u, "{}_D"] \arrow[r, "\bar{}"] & A \otimes A \arrow[u]
\end{tikzcd}$$

commutes, as we have already pointed out in Paragraph 3.5 that is also a right integral in $(A \otimes A)_F$. Combining this with Proposition 3.4, we get the following commutative diagram:

$$\begin{tikzcd}
Z(D(A)) \arrow[r, "\bar{}"] & Z(A) \otimes Z(A) \\
Z(D(A)) \arrow[u, "{}_D"] \arrow[r, "\bar{}"] & Z(A) \otimes Z(A) \arrow[u, "(\quad)\otimes(S\quad)"']
\end{tikzcd}$$

From the general formula for the antipode of a twist mentioned in the proof of Lemma 3.1, it is immediate that the antipode of $(A \otimes A)_F$ coincides with the antipode of $A \otimes A$ on the center. This implies that the following diagram is also commutative:

$$\begin{tikzcd}
Z(D(A)) \arrow[r, "\bar{}"] & Z(A) \otimes Z(A) \\
Z(D(A)) \arrow[u, "S"] \arrow[r, "\bar{}"] & Z(A) \otimes Z(A) \arrow[u, "S \quad (S \quad S)"']
\end{tikzcd}$$

The ribbon element can be treated in a similar way. It is immediate from the definition that a ribbon element $v \in A$ satisfies

$$(v^{-1}) = (R^{-1}R'^{-1})(v^{-1} \otimes v^{-1})$$

which means that v^{-1} is a ribbon element for A endowed with the alternative R-matrix R'^{-1}. This implies that $v \otimes v^{-1}$ is a ribbon element for $A \otimes A$, endowed with the R-matrix $R_{A \otimes A}$ considered in Paragraph 3.1. It is not difficult to see that a ribbon element stays a ribbon element if the coproduct of the Hopf algebra is twisted, and therefore $v \otimes v^{-1}$ is also a ribbon element for $(A \otimes A)_F$.

This enables us to define a ribbon element v_D of the Drinfel'd double $D(A)$ by setting $v_D := {}^{-1}(v \otimes v^{-1})$. So, if we define $T \in \mathrm{End}(D(A))$ to be the multiplication by v_D, as in Paragraph 4.3, it is obvious that the following diagram is commutative:

$$\begin{tikzcd}
D(A) \arrow[rr] & & A \otimes A \\
D(A) \arrow[u, "T"] \arrow[rr] & & A \otimes A \arrow[u, "T \otimes T^{-1}"']
\end{tikzcd}$$

Note that it follows from Lemma 3.1 that in the case that the ribbon element is the inverse Drinfel'd element, so that $v = u^{-1}$, the arising ribbon element of $D(A)$ is also the inverse Drinfel'd element.

4.5 As we have discussed there, the projective representation of the modular group on the center of A described in Corollary 4.3 is not induced by a linear representation in general. However, the situation is better for a certain tensor product:

Lemma There is a unique homomorphism from $SL(2;\mathbb{Z})$ to $GL(Z(A) \otimes Z(A))$ that maps s to $S \otimes S^{-1}$ and t to $T \otimes T^{-1}$.

Proof. As in the proof of Corollary 4.3, we have to check the defining relations $s^4 = 1$ and $(ts)^3 = s^2$. For the first relation, we have by Corollary 4.2 that

$$(S \otimes S^{-1})^2 = \frac{(\quad)(R'R)}{(\quad)(R'R)} S \otimes S^{-1}$$

which implies the assertion, since $S^2 = \mathrm{id}$ on the center. It should be noted that, in contrast to S, the endomorphism $S \otimes S^{-1}$ is independent of the choice of an integral. The second defining relation can be rewritten in the form $sts = t^{-1}st^{-1}$, as in the proof of Corollary 4.3. This now follows from Proposition 4.3, too, as we have

$$(S \otimes S^{-1}) \circ (T \otimes T^{-1}) \circ (S \otimes S^{-1}) = \frac{(v)}{(v)}(T^{-1} \otimes T) \circ (S \otimes S^{-1}) \circ (T^{-1} \otimes T)$$

and the factors (v) involved now cancel. $\square$

The associated projective representation on the projective space $P(Z(A) \otimes Z(A))$ is the tensor product of two projective representations: The first is the one constructed in Corollary 4.3, and the second is the first one twisted by the conjugation with the matrix a described in Paragraph 1.1. This implies that when $\lambda(v) = \lambda(v^{-1}) = 1$, in which case these two projective representations lift to ordinary linear representations, we can write

$$g.(z \otimes z') = g.z \otimes \tilde{g}.z'$$

This equation holds because it suffices to check it on generators, and for the generators we observed in Paragraph 1.1 that $\tilde{g} = g^{-1}$.

From Corollary 4.3, we also get a projective representation of the modular group on the center of the Drinfel'd double $D(A)$, using the integral $\rho_D = \rho \otimes (\lambda \otimes \lambda)$ and the ribbon element $v_D = \Delta^{-1}(v \otimes v^{-1})$ introduced in Paragraph 4.4. Suppose now that ρ is normalized so that $(\lambda \otimes \lambda)(R'R) = 1$. By Lemma 4.3, we then have

$$\rho_D(v_D) = \lambda(v)\,\lambda(v^{-1}) = (\lambda \otimes \lambda)(R'R) = 1$$

and similarly also that $\rho_D(v_D^{-1}) = 1$. Therefore again by Lemma 4.3, we can conclude for the R-matrix of the Drinfel'd double that $(\rho_D \otimes \rho_D)(R'R) = 1$. By the discussion in Paragraph 4.3, this means that the projective representation on $Z(D(A))$ is induced from an ordinary linear representation. Clearly, Φ is equivariant with respect to this action and the one considered in the preceding lemma:

Proposition For all $g \in \Gamma$ and all $z \in Z(D(A))$, we have $\Phi(g.z) = g.\Phi(z)$.

Proof. It suffices to check this on generators, i.e., in the case $g = s$ and $g = t$. But in these cases the assertion is exactly what we have established in Paragraph 4.4, because $S \otimes S = S^{-1}$ by Corollary 4.2. $\square$

It should be noted that in the case $\lambda(v) = 1$, in which the projective representation on $Z(A)$ lifts to a linear representation, the formula in the proposition can be written as

$$\Phi(g.z) = (g \otimes \tilde{g}).\Phi(z)$$

5 The semisimple case

5.1 Let us now assume that our quasitriangular Hopf algebra A is factorizable, semisimple, and that the base field K is algebraically closed of characteristic zero. In this case, A is also cosemisimple and the antipode is an involution.[61] By Wedderburn's theorem,[62] we can decompose A into a direct sum of simple two-sided ideals:

$$A = \bigoplus_{i=1}^{k} I_i$$

For every $i = 1, \ldots, k$, we can then find a simple module such that the corresponding representation maps I_i isomorphically to $\mathrm{End}(V_i)$ and vanishes on the other two-sided ideals I_j if $j \neq i$. We denote the dimension of V_i by n_i. We can assume that $V_1 = K$, the base field, considered as a trivial module via the counit. We denote the character of V_i by χ_i, so that, for $a \in A$,

$$\chi_i(a) := \mathrm{tr}(a|_{V_i})$$

is the trace of the action of a on V_i. We then have that the character χ_R of the regular representation, i.e., the representation given by left multiplication on A itself, has the form

$$\chi_R(a) = \sum_{i=1}^{k} n_i \chi_i(a)$$

This character is a two-sided integral in A^*.[63]

The subspace of A^* spanned by the characters $\chi_1, \ldots, \chi_k$ is called the character ring of A, and is denoted by $Ch(A)$. It is easy to see that it really is a subalgebra of A^*, which consists precisely of the cocommutative elements. Because the antipode is an involution, this means that the character ring $Ch(A)$ coincides with both of the algebras $C(A)$ and $C(A)$ introduced in Paragraph 3.2, and Proposition 3.2 therefore asserts that Φ induces an isomorphism between the character ring and the center $Z(A)$, which is spanned by the centrally primitive idempotents $e_i \in I_i$. The first idempotent e_1 is then a two-sided integral normalized such that $\varepsilon(e_1) = 1$. Note that it follows from the discussion in Paragraph 3.2 that the restrictions of Φ and Φ' to $Ch(A)$ are equal, because the grouplike element $g := uS(u^{-1})$ is the unit element in this case.[64] The center $Z(A)$ is a commutative semisimple algebra that admits exactly k distinct algebra homomorphisms $\omega_1, \ldots, \omega_k$ to the base field, which are explicitly given as

$$\omega_i : Z(A) \to K, \; z \mapsto \frac{1}{n_i} \chi_i(z)$$

These mappings are called the central characters; they satisfy $\omega_i(e_j) = \delta_{ij}$. Because Φ is an algebra isomorphism between $Ch(A)$ and $Z(A)$, $Ch(A)$ is also a commutative semisimple algebra,[65] whose k distinct algebra homomorphisms $\psi_1, \ldots, \psi_k$ to the base field are given as $\psi_i := \omega_i \circ \Phi$. The primitive idempotents $p_1, \ldots, p_k$ of the character ring are accordingly given as $p_j := \Phi^{-1}(e_j)$

and satisfy $\eta_i(p_j) = \delta_{ij}$. The first primitive idempotent is then proportional to the character of the regular representation; more precisely, we have $\chi_R = np_1$.[66]

Because the pairing between the character ring and the center is nondegenerate, a linear functional on the character ring can be uniquely represented by an element in the center. Therefore, there exist elements[67] $z_1, \ldots, z_k \in Z(A)$ such that $\eta_i(\chi) = \chi(z_i)$ for all $\chi \in Ch(A)$. They are explicitly given as

$$z_i = \sum_{j=1}^{k} \frac{\eta_i(\chi_j)}{n_j} e_j$$

We will call $z_1, \ldots, z_k$ the class sums, as they are related to the normalized conjugacy class sums in the group ring of a finite group. Note that $z_1 = 1$.

For every simple module V_i, its dual V_i^* is again simple. Therefore, there is a unique index $i^* \in \{1, \ldots, k\}$ such that $V_{i^*} \cong V_i^*$. The character of this module will also be denoted by $\chi_i^* := \chi_{i^*}$. The map $i \mapsto i^*$ is an involution on the index set $\{1, \ldots, k\}$. Because the use of the antipode in the definition of the dual module, characters, centrally primitive idempotents, and central characters behave as follows with respect to dualization:

$$\chi_{i^*} = S^*(\chi_i) \qquad e_{i^*} = S(e_i) \qquad \omega_{i^*} = \omega_i \circ S$$

We have derived in Paragraph 3.2 that $S(\iota(\varphi)) = \iota(S^{-1*}(\varphi))$. Since A is involutory and ι and $\bar{\iota}$ agree on the character ring, we get furthermore that

$$\eta_{i^*} = \eta_i \circ S \qquad p_{i^*} = S(p_i)$$

which implies the formula $z_{i^*} = S(z_i)$ for the class sums.

Using duals, we can express the character χ_A of the left adjoint representation in the form[68]

$$\chi_A = \sum_{i=1}^{k} \chi_i \chi_{i^*}$$

This in turn enables to invert the expansion $\chi_j = \sum_{i=1}^{k} \eta_i(\chi_j) p_i$ of the characters in terms of the idempotents:

Proposition For $i = 1, \ldots, k$, we have

$$p_i = \frac{1}{\eta_i(\chi_A)} \sum_{j=1}^{k} \eta_i(\chi_{j^*}) \chi_j$$

Proof. The element $\sum_{j=1}^{k} \chi_j \otimes \chi_{j^*}$ is a Casimir element;[69] i.e., it satisfies

$$\sum_{j=1}^{k} \chi_j \otimes \chi_{j^*} = \sum_{j=1}^{k} \chi_{j^*} \otimes \chi_j$$

for all $\chi \in Ch(A)$. Applying χ_i to the first tensor factor, we get

$$\chi_i(\chi) \sum_{j=1}^{k} \chi_i(\chi_j)\, \chi_j = \chi \sum_{j=1}^{k} \chi_i(\chi_j)\, \chi_j$$

This shows that $\sum_{j=1}^{k} \chi_i(\chi_j)\chi_j$ is proportional to p_i. Since $\chi_i(p_i) = 1$, we find that the proportionality factor is $\chi_i(\sum_{j=1}^{k} \chi_i(\chi_j)\chi_j) = \chi_i(\chi_A)$. This proportionality factor cannot be zero, since the element itself is not zero, so the assertion follows. □

5.2 As A is involutory, u is central.[70] As explained in Paragraph 5.1, u is also invariant under the antipode, and therefore we can in this situation use u^{-1} as a ribbon element. For this ribbon element, the quantum trace coincides with the usual trace,[71] so that the categorical dimensions coincide with the ordinary dimensions n_i introduced above. Clearly, we can expand the Drinfel'd element and its inverse in terms of the centrally primitive idempotents:

$$u = \sum_{i=1}^{k} u_i e_i \qquad u^{-1} = \sum_{i=1}^{k} \frac{1}{u_i} e_i$$

for numbers $u_i \in K$, which are nonzero because the Drinfel'd element is invertible. Using these numbers, we define the diagonal matrix[72]

$$T := \left(\frac{1}{u_i}\delta_{ij}\right)_{i,j=1,\ldots,k}$$

Because for this ribbon element T is the multiplication by u^{-1}, this matrix represents the restriction of T to the center with respect to the basis consisting of the centrally primitive idempotents. Furthermore, we will need an auxiliary matrix, the so-called charge conjugation matrix $C := (\delta_{i,j^*})_{i,j=1,\ldots,k}$, which is the matrix representation of the action of the antipode on the center of A with respect to the basis consisting of the centrally primitive idempotents. It is also the matrix representation of the action of the dual antipode on the character ring with respect to the basis consisting of the irreducible characters.

We define still another matrix, the so-called Verlinde matrix S, which should not be confused with the antipode:[73]

Definition The Verlinde matrix is the matrix $S = (s_{ij})_{i,j=1,\ldots,k}$ with entries

$$s_{ij} := (\chi_i \otimes \chi_j)(R'R) = \chi_i(\Phi(\chi_j))$$

We list some well-known properties of the Verlinde matrix:[74]

Lemma The Verlinde matrix is invertible. Its entries satisfy

1. $s_{ij} = s_{ji}$
2. $s_{ij} = s_{i^* j^*}$
3. $s_{ij} = n_i \eta_i(\chi_j)$

Proof. The first property follows from the trace property of the characters. The second property can be deduced from the fact that $(S \otimes S)(R) = R$. The third property follows from the definitions:

$$\eta_i(\chi_j) = \omega_i(\Phi(\chi_j)) = \frac{1}{n_i}\chi_i(\Phi(\chi_j)) = \frac{1}{n_i}s_{ij}$$

This also shows that the Verlinde matrix is invertible: Expanding the characters in terms of the idempotents, we have $\chi_j = \sum_{i=1}^k \eta_i(\chi_j)p_i$, so that the matrix $(\eta_i(\chi_j))$ is invertible as a base change matrix, and the Verlinde matrix is, by the third property, the product of this matrix and an invertible diagonal matrix. $\square$

In contrast to the matrix T, the Verlinde matrix is not exactly the matrix representation of S with respect to the centrally primitive idempotents, although these two matrices are closely related. To understand this relation, recall that S depends, via Φ, on the choice of an integral $\lambda \in A$. Because the space of integrals is one-dimensional, λ has to be proportional to the character χ_R of the regular representation, so that $\lambda = \nu\chi_R$ for a nonzero number $\nu \in K$. Although it is in principle possible to fix ν by normalizing the integral in some way, we will see that it is convenient not to do that at the moment and to keep ν as a free parameter. With this parameter introduced, let us see how the maps Φ and $\bar{\Phi}$ behave with respect to the new bases introduced in Paragraph 5.1:

Proposition For all $i = 1, \ldots, k$, we have

1. $\Phi(\chi_i) = n_i z_i$
2. $\bar{\Phi}(e_i) = \nu n_i \eta_i$
3. $\bar{\Phi}(z_i) = \nu \chi_i(\Lambda_A) p_i$

Proof. For the first assertion, we note that by the above lemma

$$n_i \eta_i(\chi_j) = s_{ij} = s_{ji} = n_j \eta_j(\chi_i)$$

so that the definition of the class sums from Paragraph 5.1 can be rewritten in the form

$$z_i = \sum_{j=1}^{k} \frac{\eta_i(\chi_j)}{n_j} e_j = \sum_{j=1}^{k} \frac{\eta_j(\chi_i)}{n_i} e_j$$

Expanding $(\ _i)$ in terms of centrally primitive idempotents, we therefore have

$$(\ _i) = \sum_{j=1}^{k} !_j(\ (\ _i))e_j = \sum_{j=1}^{k} \ _j(\ _i)e_j = n_i z_i$$

For the second assertion, we have by definition of that

$$(e_i)(a) = \ _R(e_i a) = \sum_{j=1}^{k} n_j \ _j(e_i a) = n_i \ _i(a)$$

The third assertion follows from the second assertion, together with Proposition 5.1 and the formula for the class sums given in that paragraph. We then find

$$(z_i) = \sum_{j=1}^{k} \frac{\ _i(\ _j)}{n_j} (e_j) = \sum_{j=1}^{k} \frac{\ _i(\ _j)}{n_j} n_j \ _j$$
$$= \sum_{j=1}^{k} \ _i(\ _j)\ _j = \ _i(\ _A)p_i$$

where we have used that $\ _i(\ _j) = \ _i(\ _j)$ and $\ _i(\ _A) = \ _i(\ _A)$. □

From this proposition, we can deduce the precise relation of the Verlinde matrix and the matrix representation of S resp. S . Up to scalar multiples, S maps idempotents to class sums, and vice versa. Similarly, S maps idempotents to multiples of characters and characters to multiples of idempotents:

Corollary

1. $S(z_j) = \ _j(\ _A)e_j = \sum_{i=1}^{k} \frac{n_i}{n_j} s_{ji} z_i$
2. $S(e_j) = n_j^2 z_j = \sum_{i=1}^{k} \frac{n_j}{n_i} s_{j\ i} e_i$
3. $S(\ _j) = n_j\ _j(\ _A)p_j = \sum_{i=1}^{k} s_{ji}\ _i$
4. $S(p_j) = n_j\ _j = \sum_{i=1}^{k} \frac{n_j}{n_i} s_{ij}\, p_i$

Proof. If we apply to the formula in Proposition 5.1 and use the preceding proposition, then we get

$$e_j = \frac{1}{\ _j(\ _A)} \sum_{i=1}^{k} \ _j(\ _i)n_i z_i = \frac{1}{\ _j(\ _A)} \sum_{i=1}^{k} \frac{n_i}{n_j} s_{ji} z_i$$

Since and coincide on the character ring, we get from the definition of S in Paragraph 4.1 that

$$S(z_j) = \quad {}_j(\ {}_A)S(\ (p_j\ )) = \quad {}_j(\ {}_A)e_j$$

Combining these two formulas, we get the first statement. For the second statement, we get from the preceding proposition that

$$S(e_j) = \quad n_j S(\ (\ {}_j)) = \quad n_j^2 z_j \quad = \quad n_j^2 \sum_{i=1}^{k} \frac{{}_j(\ {}_i)}{n_i} e_i$$

For the third statement, recall that by its definition in Paragraph 4.1 we have S = S , so that the preceding proposition gives

$$S\ (\ {}_j) = n_j S\ (\ (z_j)) = \quad n_j\ {}_j(\ {}_A)p_j = \sum_{i=1}^{k} n_j\ {}_j(\ {}_i)\ {}_i = \sum_{i=1}^{k} s_{ji}\ {}_i$$

where the third equation follows from Proposition 5.1. For the fourth statement, we have

$$S\ (p_j) = S\ (\ (e_j)) = \quad n_j\ {}_j \ = \sum_{i=1}^{k} n_j\ {}_i(\ {}_j\ )p_i = \sum_{i=1}^{k} \frac{n_j}{n_i} s_{ij}\, p_i$$

as asserted. 2

5.3 The fact that the matrices S and T are essentially the matrix representations of S and T implies that they essentially satisfy the defining relations of the modular group. More precisely, they satisfy the following relations:[75]

Proposition

$$S^2 = \dim(A)C \qquad\qquad STS = \ {}_R(u^{\ 1})T^{\ 1}SCT^{\ 1}$$

Proof. By Corollary 5.2, we have

$$S^2(e_j) = \sum_{l=1}^{k} \frac{n_j}{n_l} s_{j\,l} S(e_l) = \ {}^2 \sum_{i,l=1}^{k} \frac{n_j}{n_i} s_{j\,l} s_{i\,l} e_i$$

On the other hand, it follows from Corollary 4.2 and Lemma 4.3 that

$$S^2(a) = \quad (u)\ \ (u^{\ 1})S(a)$$

Inserting $a = e_j$ into this equation and comparing it with the preceding one, we find

$$(u)\ \ (u^{\ 1})e_j \ = \ {}^2 \sum_{i,l=1}^{k} \frac{n_j}{n_i} s_{j\,l} s_{i\,l} e_i$$

which implies $(u)\,(u^{1})_{ij} = {}^{2}\frac{n_j}{n_i}\sum_{l=1}^{k} s_{j\,l} s_{i\,l}$ by comparing coe cients. Now note that by Lemma 4.3

$$\frac{1}{{}_2}\,(u)\,(u^{1}) = {}_R(u)\,{}_R(u^{1}) = {}_R(\,(\,{}_R)) = \dim(A)$$

because $(\,{}_R)$ is an integral satisfying $"(\,(\,{}_R)) = \dim(A)$ by Lemma 3.5. This shows that[76]

$$\sum_{l=1}^{k} s_{il} s_{lj} = \dim(A)\,{}_{ij}$$

which is the rst assertion.

For the second assertion, recall that $S \quad T \quad S = (u^{1})\,T^{1} \quad S \quad T^{1}$ by Proposition 4.3. By Corollary 5.2, we have

$$(S \quad T \quad S)(e_j) = \sum_{l=1}^{k} \frac{n_j}{n_l} s_{j\,l} \frac{1}{u_l} S(e_l) = {}^{2}\sum_{i,l=1}^{k} \frac{n_j}{n_i} \frac{s_{j\,l} s_{l\,i}}{u_l} e_i$$

as well as

$$(T^{1} \quad S \quad T^{1})(e_j) = \sum_{i=1}^{k} \frac{n_j}{n_i} u_i u_j s_{j\,i} e_i$$

Comparing coe cients, we nd that[77]

$$\sum_{l=1}^{k} \frac{s_{j\,l} s_{l\,i}}{u_l} = (u^{1})\,u_i u_j s_{j\,i}$$

or alternatively that $\sum_{l=1}^{k} \frac{s_{jl} s_{li}}{u_l} = {}_R(u^{1}) u_i u_j s_{ji}$, which gives the second relation. 2

In the proof of the rst matrix identity above, we have used one of the two formulas for $S(e_j)$ given in Corollary 5.2. Using the other form reveals another interesting identity:

Corollary $\;{}_i(\,{}_A) = \dfrac{\dim(A)}{n_i^2}$

Proof. From Corollary 5.2, we have

$$S^{2}(e_j) = n_j^2 S(z_j) = {}^{2} n_j^2\,{}_j(\,{}_A) e_j$$

But in the proof of the preceding proposition, we have derived that

$$S^{2}(e_j) = (u)\,(u^{1}) e_j$$

and also that $(u)\,(u^{1}) = {}^{2}\dim(A)$. Therefore, the assertion follows by comparing coe cients. 2

It should be noted that $\chi_i(\rho_A)$ is an eigenvalue of the multiplication with the character ρ_A corresponding to the eigenvector p_i, and therefore an algebraic integer. As the corollary shows, it is also a rational number, and therefore an integer. This yields the well-known[78] result that n_i^2 divides $\dim(A)$.

It should furthermore be noted that the preceding corollary can also be used to give a different proof of the equation $S^2 = \dim(A)C$, as we have

$$\sum_{l=1}^{k} s_{il}s_{lj} = \sum_{l=1}^{k} n_i \chi_i(\chi_l) n_j \chi_j(\chi_l) = n_i n_j \chi_j(\rho_A)\chi_i(p_j) = n_j^2 \chi_j(\rho_A)\delta_{ij}$$

where the first equation follows from Lemma 5.2 and the second equation from Proposition 5.1.

5.4 We proceed to carry out a more precise comparison of our setup with the setup in [58]. For this, we need the following lemma:

Lemma $\displaystyle\sum_{i=1}^{k} n_i u_i^{-1} u_j^{-1} s_{ij} = n_j \chi_R(u^{-1})$

Proof. Since $\Delta(u) = (R'R)^{-1}(u \otimes u) = (u \otimes u)(R'R)^{-1}$, we have

$$\sum_{i=1}^{k} n_i u_i^{-1} u_j^{-1} s_{ij} = \sum_{i=1}^{k} n_i u_i^{-1} u_j^{-1} (\chi_i \otimes \chi_j)(R'R) = \sum_{i=1}^{k} n_i (\chi_i \otimes \chi_j)(\Delta(u^{-1}))$$
$$= (\chi_R \otimes \chi_j)(\Delta(u^{-1})) = (\chi_R \chi_j)(u^{-1}) = n_j \chi_R(u^{-1})$$

where the last equality follows from the fact that the character of the regular representation is an integral. □

As we have already pointed out in Paragraph 5.2, categorical dimensions and ordinary dimensions coincide for our choice of a ribbon element, so that the numbers dim(i) introduced in [58], Sec. II.1.4, p. 74 are equal to n_i. Also, since our ribbon element is u^{-1}, it is clear that the numbers v_i and Δ introduced in [58], Sec. II.1.6, p. 76 are equal to $1/u_i$ resp. $\chi_R(u)$. It therefore follows from the preceding lemma that the parameters d_i introduced in [58], Sec. II.3.2, p. 87 are in our case equal to $d_i = n_i/\chi_R(u^{-1})$, which is in accordance with [58], Lem. II.3.2.3, p. 89. For the rank D, we have the two choices $D = \pm\sqrt{\dim(A)}$. The equation $\dim(A) = \chi_R(u)\chi_R(u^{-1})$ observed in Paragraph 5.3 then becomes the equation $\Delta = d_0 D^2$ in [58], Sec. II.3.2, Eq. (3.2.j), p. 89.

5.5 We now illustrate the preceding considerations by inspecting an example given by D. E. Radford.[79] Consider a cyclic group G of order n. Denote the group ring by $A = K[G]$, and fix a generator g of G. As A is cocommutative,

A is certainly quasitriangular with respect to the R-matrix $1 \otimes 1$. However, with respect to this R-matrix, it is not factorizable. Radford has determined all possible R-matrices for A, and shown that A can only be factorizable if n is odd, what we will assume for the rest of this paragraph, and that in this case the R-matrix necessarily has the form

$$R = \frac{1}{n} \sum_{i,j=0}^{n-1} \zeta^{-ij} g^i \otimes g^j$$

where ζ is a primitive n-th root of unity.[80] To follow his convention, we will deviate in this paragraph from the enumeration introduced in Paragraph 5.1 and enumerate the (centrally) primitive idempotents in the form $e_0, \ldots, e_{n-1}$ instead of $e_1, \ldots, e_k$; note that $n = k$ in the present situation. They are then given by the formula[81]

$$e_j = \frac{1}{n} \sum_{i=0}^{n-1} \zeta^{-ij} g^i$$

The irreducible characters are determined by $\chi_i(e_j) = \delta_{ij}$ and therefore satisfy $\chi_i(g) = \zeta^i$. Radford also gives the following formulas for the Drinfel'd element and its inverse:[82]

$$u = \sum_{i=0}^{n-1} \zeta^{-i^2} e_i \qquad\qquad u^{-1} = \sum_{i=0}^{n-1} \zeta^{i^2} e_i$$

He also gives the formula $\Delta(u^{-1}) = \sum_{i,j=0}^{n-1} \zeta^{(i+j)^2} e_i \otimes e_j$ for the coproduct of the inverse Drinfel'd element, from which we get that

$$R'R = (u \otimes u)\Delta(u^{-1}) = \sum_{i,j=0}^{n-1} \zeta^{2ij} e_i \otimes e_j$$

This means that the entries of the Verlinde matrix are given as

$$s_{ij} = (\chi_i \otimes \chi_j)(R'R) = \zeta^{2ij}$$

so that, using Corollary 5.2, we find the expressions

$$S(e_j) = \sum_{i=0}^{n-1} \zeta^{2ij} e_i \qquad\qquad T(e_j) = \zeta^{j^2} e_j$$

for the mappings S and T, since T is the multiplication by u^{-1}.

The reason for mentioning this example is its following feature:

Proposition We have

$$\chi_R(u^{-1}) = \begin{cases} \chi_R(u) & \text{if } n \equiv 1 \pmod 4 \\ -\chi_R(u) & \text{if } n \equiv 3 \pmod 4 \end{cases}$$

Proof. From the form of the inverse Drinfel'd element given above, we see that $_R(u^{\ 1}) = \sum_{i=0}^{n\ 1} {}^{i^2}$ is the quadratic Gaussian sum. As the quadratic Gaussian sum transforms with the Jacobi symbol under change of the root of unity,[83] we have

$$_R(u^{\ 1}) = \frac{1}{n} \ _R(u)$$

The assertion now follows from the rst supplement to Jacobi's reciprocity law.[84] 2

For the discussion in Paragraph 4.3, this result means that the two conditions $(\quad)(R^0 R) = 1$ and $(v) = 1$ can not always be simultaneously satis ed. It also means that Lemma 4.3 can, in a sense, be considered as a generalization of the formula for the absolute value of the quadratic Gaussian sum.[85] We will further elaborate on this analogy in Paragraph 12.1.

6 The case of the Drinfel'd double

6.1 In the case where A is the Drinfel'd double $D = D(H)$ of a semisimple Hopf algebra, it is possible to give another description of the action of the modular group that will play an important role in the sequel. We therefore suppose now that H is a semisimple Hopf algebra over an algebraically closed eld of characteristic zero, and set $A = D(H)$, its Drinfel'd double. First, recall from Paragraph 2.3 that the two-sided integral of the Drinfel'd double has the form $_D =$ for an integral $2 H$ and an integral $2 H$. We can choose these integrals in such a way that "( ) = 1 and ( ) = 1. They are then uniquely determined and satisfy (S( )) = 1 as well as (1) = dim(H).[86] From Paragraph 2.3, we then know that the right integral $_D$ on D given by

$$_D(' \quad h) = '(\ )\ (h)$$

satises $_D(u_D{}^1) = \ _D(u_D) = 1$, which implies that $(_D \quad _D)(R^0 R) = 1$ by Lemma 4.3 and $_D(\ _D) = (\ )^2 = 1$. By comparing normalizations, we see that the character of the regular representation is $_R = \dim(H)\ _D$, so that we have

$$_R(u_D{}^1) = \ _R(u_D) = \dim(H)$$

This means on the one hand that the parameter $= \ _D$, introduced in Paragraph 5.2, is in the case of the Drinfel'd double with these normalizations given by $_D = \frac{1}{\dim(H)}$, and on the other hand means that, as discussed in Paragraph 4.3, the representation of $SL(2;Z)$ on the center is not only a projective representation, but rather is linear.

Recall from Lemma 3.3 that, under the correspondence $H \quad H = D$ described there, the restrictions of and to the character ring are just the interchange of the tensorands. From this, and the fact that the antipode is an involution, it is clear that the evaluation form e introduced in Paragraph 2.2, which is contained in the character ring, is mapped under and to the inverse Drinfel'd element $u_D{}^1$, which, as discussed in Paragraph 5.1, can be used as a ribbon element. Another consequence of these considerations is the following fact:

Lemma Suppose that $z = \sum_j '_j \quad h_j$ is a central element. Then we have also

$$z = \sum_j (" \quad h_j)('_j \quad 1)$$

Proof. Put $:= \ ^1(z)$. By Lemma 3.3, we then have $= \sum_j h_j \quad '_j$. But we have also seen in Paragraph 3.3 that $(\ ) = \sum_j (" \quad h_j)('_j \quad 1)$. Since agrees with on the character ring, the assertion follows. 2

For the right and the left multiplication with the evaluation form, we now introduce the notation T and T. In other words, we dene the endomorphisms T and T of D by

$$T\ (\ ) = \ e \qquad T\ (\ ) = e$$

This notation is justified by the following proposition, which should be compared with Proposition 4.1:

Proposition The diagrams

$$\begin{tikzcd} D \arrow[r, "T"] \arrow[d] & D \arrow[d] \\ D \arrow[r, "T"'] & D \end{tikzcd} \qquad \begin{tikzcd} D \arrow[r, "T"] \arrow[d] & D \arrow[d] \\ D \arrow[r, "T"'] & D \end{tikzcd}$$

are commutative.

Proof. The commutativity of the first diagram follows directly from Proposition 3.2, as we have

$$(T\ (\ )) = \ (\ e) = \ (\ )\ (e) = \ (\ )u_D^{\ 1} = T(\ (\ ))$$

Also in Paragraph 3.2, we saw that $(e\ ) = \ (e)\ (\ ) = u_D^{\ 1}\ (\ )$, which yields the commutativity of the second diagram. 2

This proposition implies that we also get a representation of the modular group on the character ring of the Drinfel'd double by mapping the generator s to the restriction of S and the generator t to the restriction of T . This action is, via , just conjugate to the action on the center constructed in Corollary 4.3. Note that T and T really preserve the character ring, as they are left resp. right multiplication with the character e. As the character ring is commutative, these two endomorphisms in fact coincide on the character ring.

6.2 The second construction of the modular group action alluded to above is based on the following maps R and R , which should not be confused with the R-matrix:

Definition We define the endomorphisms R and R of D by setting

$$R\ (a) := e(a_{(1)})a_{(2)} \qquad R\ (a) := e(a_{(2)})a_{(1)}$$

Furthermore, we define the endomorphism R of D as

$$R\ (\ )(a) = \ (u_D^{\ 1}a)$$

In other words, we set $R = T$, the transpose of T. Note that we also have $R = T$ and $R = T$.

These maps are related in a similar way as the ones considered earlier:

Proposition The diagrams

$$\begin{tikzcd} D \arrow[r, "R"] \arrow[d] & D \arrow[d] \\ D \arrow[r, "R"'] & D \end{tikzcd} \qquad \begin{tikzcd} D \arrow[r, "R"] \arrow[d] & D \arrow[d] \\ D \arrow[r, "R"'] & D \end{tikzcd}$$

are commutative.

Proof. (1) Recall from Paragraph 2.2 the formula $u_D^{\;1} = \sum_{i=1}^n b_i \quad b_i$, where $b_1,\ldots,b_n$ is a basis of H with dual basis $b_1,\ldots,b_n$. Recall further that we have set up in Paragraph 6.1 a correspondence between $H \quad H$ and D, so that we can associate with every $h \in H$ and $\varphi \in H$ an element $\in D$. For this element, we find that

$$\begin{aligned} (\;) &= \sum_{i,j=1}^n (b_i \quad b_j)(\varepsilon \quad b_i)(b_j \quad 1) \\ &= \sum_{i,j=1}^n b_i(h)\varphi(b_j)(\varepsilon \quad b_i)(b_j \quad 1) = (\varepsilon \quad h)(\varphi \quad 1) \end{aligned}$$

which implies that

$$\begin{aligned} R(\;(\;)) &= e((\varepsilon \quad h_{(2)})(\varphi_{(1)} \quad 1))(\varepsilon \quad h_{(1)})(\varphi_{(2)} \quad 1) \\ &= e((\varphi_{(1)} \quad 1)(\varepsilon \quad h_{(2)}))(\varepsilon \quad h_{(1)})(\varphi_{(2)} \quad 1) \\ &= \varphi_{(1)}(h_{(2)})(\varepsilon \quad h_{(1)})(\varphi_{(2)} \quad 1) \end{aligned}$$

(2) On the other hand, for $a = \varphi^0 \quad h^0 \in D$, we have by the centrality of the Drinfel'd element that

$$\begin{aligned} R\;(\;)(a) &= (u_D^{\;1}a) = ((\varphi^0 \quad 1)u_D^{\;1}(\varepsilon \quad h^0)) = \sum_{i=1}^n (\varphi^0 b_i \quad b_i h^0) \\ &= \sum_{i=1}^n (\varphi^0 b_i)(h)\varphi(b_i h^0) = \sum_{i=1}^n \varphi^0(h_{(1)})b_i(h_{(2)})\varphi_{(1)}(b_i)\varphi_{(2)}(h^0) \\ &= \varphi^0(h_{(1)})\varphi_{(1)}(h_{(2)})\varphi_{(2)}(h^0) \end{aligned}$$

This means that $R(\varphi) \in D$ corresponds to $\varphi_{(1)}(h_{(2)})h_{(1)} \otimes \varphi_{(2)} \in H \otimes H^{*}$. By the preceding computation of Θ, we therefore have

$$\Theta(R(\varphi)) = \varphi_{(1)}(h_{(2)})(\varepsilon \otimes h_{(1)})(\varphi_{(2)} \otimes 1) = R(\Theta(\varphi))$$

This establishes the commutativity of the second diagram.

(3) The commutativity of the first diagram is a consequence of the commutativity of the second. As discussed in Paragraph 5.1, we have $S_D(u_D) = u_D$, and therefore $S_D \circ R = R \circ S_D$. From the proof of Lemma 2.3, we have $S_D(e) = e$, which implies that $S_D \circ R = R \circ S_D$. As we saw in Paragraph 3.2, we also have $S_D \circ \Theta = \Theta \circ S_D$ as a consequence of involutivity, so that

$$\begin{aligned} S_D \circ \Theta \circ R &= \Theta \circ S_D \circ R = \Theta \circ R \circ S_D \\ &= R \circ \Theta \circ S_D = R \circ S_D \circ \Theta = S_D \circ R \circ \Theta \end{aligned}$$

After cancelling the antipode, this is the commutativity of the first diagram. □

It is interesting to look at the linearity properties of our new maps:

Lemma For all $a, b \in D$, we have

1. $R(S_D^{-1}(b_{(1)})ab_{(2)}) = S_D^{-1}(b_{(1)})R(a)b_{(2)}$
2. $R(b_{(1)}aS_D^{-1}(b_{(2)})) = b_{(1)}R(a)S_D^{-1}(b_{(2)})$

In particular, R and R both preserve the center of D.

Proof. By the symmetry property of the evaluation form e recorded in Paragraph 2.2, we have

$$\begin{aligned} R(S_D^{-1}(b_{(1)})ab_{(2)}) &= e(S_D^{-1}(b_{(2)})a_{(1)}b_{(3)})S_D^{-1}(b_{(1)})a_{(2)}b_{(4)} \\ &= e(a_{(1)}b_{(3)}S_D^{-1}(b_{(2)}))S_D^{-1}(b_{(1)})a_{(2)}b_{(4)} \\ &= e(a_{(1)})S_D^{-1}(b_{(1)})a_{(2)}b_{(2)} = S_D^{-1}(b_{(1)})R(a)b_{(2)} \end{aligned}$$

For the second assertion, we have similarly that

$$R(b_{(1)}aS_D^{-1}(b_{(2)})) = b_{(1)}a_{(1)}S_D^{-1}(b_{(4)})e(b_{(2)}a_{(2)}S_D^{-1}(b_{(3)})) = b_{(1)}R(a)S_D^{-1}(b_{(2)})$$

These computations do not use that the antipode is an involution; however, this is necessary for the statement about the center, because a is central if and only if $S_D(b_{(1)})ab_{(2)} = \varepsilon_D(b)a$ for all $b \in D$, a relation that is then preserved by R. A similar argument shows that R preserves the center. □

6.3 One important step in the second approach toward the action of the modular group is the following relations between our maps:

Proposition

$$T \quad R \quad T = R \quad T \quad R \qquad\qquad T \quad R \quad T = R \quad T \quad R$$

Proof. As discussed in Paragraph 5.1, we have $S_D(u_D) = u_D$ in our case. It then follows from Proposition 2.3 that $e^{1} = {}_{D(2)}(u_D{}^{1})\ {}_{D(1)}$. We therefore get

$$R^{1}(T^{1}(\ )) = R^{1}(e^{1}\ ) = {}_{D(2)}(u_D{}^{1})R^{1}({}_{D(1)}\ )$$

Since ${}_D$ is an integral, we can rewrite this as[87]

$$\begin{aligned} R^{1}(T^{1}(\ )) &= ({}_{D(2)}S_D(\ ))(u_D{}^{1})R^{1}({}_{D(1)}) \\ &= {}_{D(3)}(u_D{}^{1}{}_{(1)})S_D(\ )(u_D{}^{1}{}_{(2)})\ {}_{D(2)}(u_D)\ {}_{D(1)} \\ &= {}_{D(2)}(u_D u_D{}^{1}{}_{(1)})R\ (S_D(\ ))(u_D u_D{}^{1}{}_{(2)})\ {}_{D(1)} \end{aligned}$$

Using the formula that expresses in terms of the Drinfel'd element given at the end of Paragraph 3.2, this can be written as

$$\begin{aligned} R^{1}(T^{1}(\ )) &= {}_{D(2)}(\ (R\ (S_D(\ ))))\ {}_{D(1)} \\ &= {}_{D(2)}(R(\ (S_D(\ ))))\ {}_{D(1)} = (e\ {}_{D(2)})(\ (S_D(\ )))\ {}_{D(1)} \end{aligned}$$

where the second equality follows from Proposition 6.2. Using the relation between and the Drinfel'd element backwards, this becomes

$$R^{1}(T^{1}(\ )) = (e\ {}_{D(2)})(u_D u_D{}^{1}{}_{(1)})\ S_D(\ )(u_D u_D{}^{1}{}_{(2)})\ {}_{D(1)}$$

Now ${}_D$ is in our case also a left integral, and furthermore we saw in Paragraph 2.3 that e is invariant under the antipode, so that we can rewrite the preceding equation in the form

$$\begin{aligned} R^{1}(T^{1}(\ )) &= {}_{D(2)}(u_D u_D{}^{1}{}_{(1)})\ S_D(\ )(u_D u_D{}^{1}{}_{(2)})\ e\ {}_{D(1)} \\ &= {}_{D(2)}(u_D)\ {}_{D(3)}(u_D{}^{1}{}_{(1)})\ R^{1}(S_D(\ ))(u_D{}^{1}{}_{(2)})\ e\ {}_{D(1)} \\ &= ({}_{D(2)}\ R^{1}(S_D(\ )))(u_D{}^{1})\ eR^{1}({}_{D(1)}) \end{aligned}$$

As discussed in Paragraph 6.2, we have $S_D \quad R = R \quad S_D$, and by using this and the properties of the integral again, we can rewrite this expression as

$$\begin{aligned} R^{1}(T^{1}(\ )) &= ({}_{D(2)}\ S_D(R^{1}(\ )))(u_D{}^{1})\ eR^{1}({}_{D(1)}) \\ &= {}_{D(2)}(u_D{}^{1})\ eR^{1}({}_{D(1)}R^{1}(\ )) \\ &= eR^{1}(e^{1}R^{1}(\ )) = T\ (R^{1}(T^{1}(R^{1}(\ )))) \end{aligned}$$

where the third equation uses Proposition 2.3 again. This proves $R^{1} \quad T^{1} = T \quad R^{1} \quad T^{1} \quad R^{1}$, which is equivalent to the rst assertion. The second assertion follows from the rst by conjugating with the antipode S_D of D, as we have already noted that S_D commutes with R, and $S_D \quad T = T \quad S_D$ holds since S_D is antimultiplicative and preserves e. 2

Instead of using endomorphisms of D , we can use endomorphisms of D. The corresponding relation then has the following form:

Corollary

$$T \quad R \quad T = R \quad T \quad R \qquad\qquad T \quad R \quad T = R \quad T \quad R$$

Proof. Using Proposition 6.1 and Proposition 6.2, this follows by conjugating the rst formula in the preceding proposition by and the second formula in the preceding proposition by . 2

6.4 Corollary 6.3 suggests that we might get a representation of the modular group by assigning T to the generator t and R to the generator r, the two alternative generators described in Paragraph 1.1. The rst de ning relation $trt = rtr$ then follows from this corollary. However, we still need the second de ning relation $(rt)^6 = 1$. This relation only holds for the restrictions of T and R to the center of D. We now proceed not only to verify this relation, but also to check that the representation of the modular group that we construct in this way agrees with the one constructed earlier. To do this, we introduce the following analogue of :

$$: D \ ! \ D ; \quad 7 \quad {}_{D(1)} \ (\ {}_{D(2)})$$

These maps together satisfy the following relations:[88]

$$(\quad)(\ ) = \ {}_D (\ {}_D) S_D (\ ) \qquad (\quad)(x) = {}_D (\ {}_D) S_D (x)$$

With the help of this map, we can deduce the following fact, which relates the two approaches to the representation of the modular group:

Proposition

$$S \quad = T^{1} \quad R^{1} \quad T^{1} = R^{1} \quad T^{1} \quad R^{1}$$

Proof. The second equality is just the inversion of the second identity in Proposition 6.3; it is therefore su cient to show the rst equality. We have the commutation relation $T \quad = \quad R$ because, as discussed in Paragraph 5.1, u_D^{1} is invariant under the antipode, and therefore we have[89]

$$\begin{aligned} T(\ (\ )) &= u_D^{1} \ {}_{D(1)} \ (\ {}_{D(2)}) = \ {}_{D(1)} \ (S_D^{1}(u_D^{1}) \ {}_{D(2)}) \\ &= \ {}_{D(1)} \ (u_D^{1} \ {}_{D(2)}) = \ {}_{D(1)} R \ (\ )(\ {}_{D(2)}) = \ (R \ (\ )) \end{aligned}$$

It follows from Lemma 2.3 that $(e^{1}) = S_D(u_D^{1}) = u_D^{1}$, because $e^{1}(\ {}_D) = (S^{1}(\ )) = 1$ in our case. From the expression for in terms of the Drinfel'd element given in Paragraph 3.2, we therefore get

$$\begin{aligned}(\ ) &= u_D u_{D\,(1)}^{-1} \ (u_D u_{D\,(2)}^{-1}) = T^{-1}(u_{D\,(1)}^{-1})R^{-1}(\ )(u_{D\,(2)}^{-1}) \\ &= T^{-1}(\ _{D\,(1)}) \ R^{-1}(\ )e^{-1} \ (\ _{D\,(2)}) \\ &= T^{-1}(\ _{D\,(1)}) \ T^{-1}(R^{-1}(\ )) \ (\ _{D\,(2)}) \\ &= (T^{-1} \quad T^{-1} \quad R^{-1})(\ ) = (\quad R^{-1} \quad T^{-1} \quad R^{-1})(\ )\end{aligned}$$

so that, by the definition of S in Paragraph 4.1 and the properties of and mentioned above, we have

$$S = S^{-1} \qquad = S^{1} \qquad R^{-1} \quad T^{1} \quad R^{-1} = R^{-1} \quad T^{1} \quad R^{-1}$$

as asserted. 2

It is easy to convert the preceding proposition from a statement about endomorphism of D into a statement about endomorphism of D: If we conjugate the identity by and use Proposition 4.1, Proposition 6.1, and Proposition 6.2, we get

$$S = T^{-1} \quad R^{-1} \quad T^{1} = R^{-1} \quad T^{1} \quad R^{-1}$$

We have proved in Proposition 4.1 that S preserves the center, and this is also true for T by the centrality of the Drinfel'd element. In Lemma 6.2, we have seen that R preserves the center. We use the same symbols for the restrictions of these maps to the center. We then have

Corollary There is a unique homomorphism from SL(2;Z) to GL(Z(D)) that maps r to R and t to T.

Proof. The homomorphism is unique because r and t generate the modular group, as discussed in Paragraph 1.1. For the existence question, recall the defining relations trt = rtr and $(rt)^6 = 1$. The first relation holds by Corollary 6.3. We have $(\ _D \quad _D)(R^0 R) = 1$, and therefore Corollary 4.2 yields that the restriction of S^2 to the center coincides with the antipode. Together with the above considerations, this shows that

$$(R \quad T)^6 = (R \quad T \quad R \quad T \quad R)^2 = S^4 = S_D^{\,2} = \mathrm{id}$$

on the center, which is the second relation needed. 2

Because $s = t^{-1}r^{-1}t^{-1}$, it is clear that this representation of the modular group agrees with the one constructed in Corollary 4.3.

6.5 We have discussed the matrix representations of T and S in Paragraph 5.2. It is possible to give a similar discussion of the matrix representations of R , R , and R :

Proposition

1. $R\ (\ _i) = \frac{1}{u_i}\ _i = \ _i(e)\ _i$

2. $R\,(z_i) = R\,(z_i) = \frac{1}{u_i} z_i = \ _i(e) z_i$

Proof. For the rst assertion, note that

$$R\ (\ _i)(a) = \ _i(u_D{}^{1} a) = \frac{1}{u_i}\ _i(a)$$

which gives the rst equation. The second equation holds since

$$_i(e) = \,!_i(\ (e)) = \,!\ _i(u_D{}^{1}) = \frac{1}{u_i}$$

The second assertion follows by applying to the rst assertion and using Proposition 5.2 and Proposition 6.2; note that we discussed in Paragraph 6.1 that and agree on the character ring. 2

Using this proposition, we can expand the evaluation form explicitly in terms of the irreducible characters:

Corollary

$$e = \frac{1}{\dim(H)} \sum_{i=1}^{k} n_i\ _i(e^{\ 1})\ _i \qquad e^{\ 1} = \frac{1}{\dim(H)} \sum_{i=1}^{k} n_i\ _i(e)\ _i$$

Proof. Since $_R$ is an integral, we can deduce from Proposition 2.3 that

$$R\ (\ _R) = \ _R(u_D{}^{1})e^{\ 1} = \dim(H) e^{\ 1}$$

The second assertion therefore follows from the preceding proposition by applying R to the equation $_R = \sum_{i=1}^{k} n_i\ _i$. The rst assertion follows in a very similar way by applying $R^{\ 1}$, as we have $R^{\ 1}(\ _R) = \dim(H)e$ by Proposition 2.3 and $R^{\ 1}(\ _i) = \ _i(e^{\ 1})\ _i$ by the preceding proposition. 2

It should be pointed out in this context that these two elements are interchanged by S :

Lemma

$$S\ (e) = e^{\ 1} \qquad S\ (e^{\ 1}) = e$$

Proof. It follows from the definition that $R(\varepsilon_D) = \varepsilon_D$. Therefore, we get by Proposition 6.4 that

$$S(e) = (T^{-1} \circ R^{-1} \circ T^{-1})(e) = T^{-1}(R^{-1}(\varepsilon_D)) = T^{-1}(\varepsilon_D) = e^{-1}$$

This proves the first assertion. The second assertion follows from the first by applying S, because we have $S^2(\chi) = S_D(\chi)$ for all $\chi \in Ch(D)$ by Proposition 4.1 and Corollary 4.2, and we have seen in the proof of Lemma 2.3 that $S_D(e) = e$. □

7 Induced modules

7.1 Suppose that H is a semisimple Hopf algebra over an algebraically closed field K of characteristic zero, and consider its Drinfel'd double $D = D(H)$. For an H-module V, we can form the induced D-module:

$$D \otimes_H V = (H^* \otimes H) \otimes_H V = H^* \otimes V$$

where the last isomorphism maps $\varphi \otimes h \otimes_H v$ to $\varphi \otimes h.v$. This isomorphism is D-linear if we consider $H^* \otimes V$ as a D-module via the module structure[90]

$$(\varphi \otimes h).(\varphi' \otimes v) := \varphi'_{(1)}(S(h_{(3)}))\varphi'_{(3)}(h_{(1)})\varphi\varphi'_{(2)} \otimes h_{(2)}.v$$

We will view the induced module from this latter viewpoint in the sequel and therefore write $\mathrm{Ind}(V) := H^* \otimes V$, considered as a D-module with this module structure.

Suppose now that W is another H-module. We introduce the following map:

Definition Suppose that $b_1, \ldots, b_n$ is a basis of H with dual basis $b_1^*, \ldots, b_n^*$. We define

$$\Phi_{V,W}: \mathrm{Ind}(V \otimes W) \to \mathrm{Ind}(W \otimes V),\ \varphi \otimes v \otimes w \mapsto \sum_{i=1}^{n} \varphi b_i^* \otimes w \otimes b_i.v$$

Let us record some first properties of this map:

Lemma $\Phi_{V,W}$ is a D-linear isomorphism. The inverse is given by

$$\Phi_{V,W}^{-1}(\varphi \otimes w \otimes v) = \sum_{i=1}^{n} \varphi b_i^* \otimes S(b_i).v \otimes w$$

Furthermore, we have

$$(\Phi_{W,V} \circ \Phi_{V,W})(x) = u_D^{-1}.x$$

for all $x \in \mathrm{Ind}(V \otimes W)$.

Proof. To establish D-linearity, $\Phi_{V,W}$ has to commute with elements of the form $\varphi \otimes 1$ and elements of the form $\varepsilon \otimes h$. As it clearly commutes with elements of the first form, we can concentrate on elements of the second form. We have

$$(\varepsilon \otimes h).\Phi_{V,W}(\varphi \otimes v \otimes w) =$$
$$\sum_{i=1}^{n} (\varphi_{(1)}b^*_{i(1)})(S(h_{(4)}))(\varphi_{(3)}b^*_{i(3)})(h_{(1)})\varphi_{(2)}b^*_{i(2)} \otimes h_{(2)}.w \otimes h_{(3)}b_i.v =$$
$$\sum_{i=1}^{n} \varphi_{(1)}(S(h_{(6)}))b^*_{i(1)}(S(h_{(5)}))\varphi_{(3)}(h_{(1)})b^*_{i(3)}(h_{(2)})\varphi_{(2)}b^*_{i(2)} \otimes h_{(3)}.w \otimes h_{(4)}b_i.v$$

Using the dual basis formulas stated in the introduction, this becomes

$$
\begin{aligned}
(\varepsilon \otimes h).\theta_{V,W}(\varphi \otimes v \otimes w) = {} & \\
\sum_{i_1,i_2,i_3=1}^{n} \varphi_{(1)}(S(h_{(6)}))b_{i_1}(S(h_{(5)}))\varphi_{(3)}(h_{(1)})b_{i_3}(h_{(2)}) & \\
\varphi_{(2)}b_{i_2} \otimes h_{(3)}.w \otimes h_{(4)}b_{i_1}b_{i_2}b_{i_3}.v & = \\
\sum_{i_2=1}^{n} \varphi_{(1)}(S(h_{(6)}))\varphi_{(3)}(h_{(1)})\,\varphi_{(2)}b_{i_2} \otimes h_{(3)}.w \otimes h_{(4)}S(h_{(5)})b_{i_2}h_{(2)}.v & = \\
\sum_{i=1}^{n} \varphi_{(1)}(S(h_{(4)}))\varphi_{(3)}(h_{(1)})\,\varphi_{(2)}b_i \otimes h_{(3)}.w \otimes b_i h_{(2)}.v &
\end{aligned}
$$

But this is exactly $\theta_{V,W}((\varepsilon \otimes h).(\varphi \otimes v \otimes w))$, which establishes the D-linearity. To establish the form of the inverse, we note that

$$
\begin{aligned}
\theta_{V,W}\Big(\sum_{i=1}^{n} \varphi b_i \otimes S(b_i).v \otimes w\Big) &= \sum_{i,j=1}^{n} \varphi b_i b_j \otimes w \otimes b_j S(b_i).v \\
&= \sum_{i,j=1}^{n} \varphi b_i \otimes w \otimes b_{i(2)}S(b_{i(1)}).v = \varphi \otimes w \otimes v
\end{aligned}
$$

by the dual basis formulas, which establishes that the map stated is a right inverse of $\theta_{V,W}$. It can be shown similarly that it is also a left inverse.

To establish the last property, we can assume that $x = \varphi \otimes v \otimes w$ is decomposable. As discussed in Paragraph 2.2, $u_D^{-1} = \sum_{i=1}^{n} b_i \otimes b_i$ is central, since H is involutory. We therefore have

$$
u_D^{-1}.x = \sum_{i=1}^{n} \varphi b_i \otimes b_{i(1)}.v \otimes b_{i(2)}.w = \sum_{i,j=1}^{n} \varphi b_i b_j \otimes b_i.v \otimes b_j.w
$$

by the dual basis formula. But this is exactly $(\theta_{W,V} \circ \theta_{V,W})(x)$. $\square$

From the point of view of category theory, θ is a natural transformation between the functors $(V,W) \mapsto \mathrm{Ind}(V \otimes W)$ and $(V,W) \mapsto \mathrm{Ind}(W \otimes V)$. The natural transformation θ also satisfies the following coherence properties:

Proposition If U, V, and W are H-modules, the following diagram commutes:

$$
\begin{tikzcd}
\mathrm{Ind}(U \otimes V \otimes W) \arrow[rr, "\theta_{U \otimes V,W}"] \arrow[dr, "\theta_{U,V \otimes W}"'] & & \mathrm{Ind}(W \otimes U \otimes V) \\
& \mathrm{Ind}(V \otimes W \otimes U) \arrow[ur, "\theta_{V,W \otimes U}"'] &
\end{tikzcd}
$$

In addition, the following diagrams also commute:

$$\begin{array}{ccc} \mathrm{Ind}(V\otimes K) & \xrightarrow{\tau_{V,K}} & \mathrm{Ind}(K\otimes V) \\ \Big\downarrow\cong & & \Big\downarrow\cong \\ \mathrm{Ind}(V) & \xrightarrow[w\mapsto u_D^{-1}.w]{} & \mathrm{Ind}(V) \end{array} \qquad \begin{array}{ccc} \mathrm{Ind}(K\otimes V) & \xrightarrow{\tau_{K,V}} & \mathrm{Ind}(V\otimes K) \\ \Big\downarrow\cong & & \Big\downarrow\cong \\ \mathrm{Ind}(V) & \xrightarrow[\mathrm{id}]{} & \mathrm{Ind}(V) \end{array}$$

Here, the vertical maps are induced from the canonical isomorphisms.

Proof. If $\varphi \in H^*$, $u \in U$, $v \in V$, and $w \in W$, we have

$$\begin{aligned}(\tau_{V,W\otimes U}\circ\tau_{U,V\otimes W})(\varphi\otimes u\otimes v\otimes w) &= \tau_{V,W\otimes U}\Big(\sum_{i=1}^n \varphi b_i\otimes v\otimes w\otimes b_i.u\Big)\\ &= \sum_{i,j=1}^n \varphi b_i b_j\otimes w\otimes b_i.u\otimes b_j.v\end{aligned}$$

on the one hand and

$$\tau_{U\otimes V,W}(\varphi\otimes u\otimes v\otimes w) = \sum_{i=1}^n \varphi b_i\otimes w\otimes b_{i(1)}.u\otimes b_{i(2)}.v$$

on the other hand. By the dual basis formula, both expressions agree, proving $\tau_{U\otimes V,W} = \tau_{V,W\otimes U}\circ\tau_{U,V\otimes W}$, which establishes the commutativity of the first diagram. The commutativity of the two remaining diagrams follows directly from the definitions. $\Box$

7.2 For a finite-dimensional module V, it turns out that the induced module of the dual is isomorphic to the dual of the induced module. More generally, suppose that V and V' are two finite-dimensional H-modules endowed with a nondegenerate pairing $\langle\cdot,\cdot\rangle : V\otimes V'\to K$ that satisfies

$$\langle h.v, v'\rangle = \langle v, S(h).v'\rangle$$

for all $v\in V$, $v'\in V'$, and $h\in H$. If we then choose a nonzero integral $\lambda\in H$ and define a pairing $\langle\cdot,\cdot\rangle : \mathrm{Ind}(V)\otimes\mathrm{Ind}(V')\to K$ as

$$\langle\varphi\otimes v, \psi\otimes v'\rangle := (S^*(\varphi)\psi)(\lambda)\langle v, v'\rangle$$

for $\varphi,\psi\in H^*$, $v\in V$, and $v'\in V'$, this pairing has the following properties:

Lemma $\langle\cdot,\cdot\rangle$ is nondegenerate. For $x\in D$, we have

$$\langle x.(\varphi\otimes v), \psi\otimes v'\rangle = \langle\varphi\otimes v, S_D(x).(\psi\otimes v')\rangle$$

Proof. The nondegeneracy follows from the nondegeneracy of the pairing $(\varphi, \psi) \mapsto (S(\varphi)\psi)(\rho)$.[91] To prove the second assertion, it suffices to show this in the cases $x = \varphi' \otimes 1$ and $x = \varepsilon \otimes h$. In the first case, this amounts to the identity

$$(S(\varphi'\varphi)\psi)(\rho)\langle v, v'\rangle = (S(\varphi)S(\varphi')\psi)(\rho)\langle v, v'\rangle$$

In the second case, this amounts to the identity

$$\begin{aligned} &\varphi_{(1)}(S(h_{(3)}))\varphi_{(3)}(h_{(1)})(S(\varphi_{(2)})\psi)(\rho)\langle h_{(2)}.v, v'\rangle \\ &= \psi_{(1)}(h_{(1)})\psi_{(3)}(S(h_{(3)}))(S(\varphi)\psi_{(2)})(\rho)\langle v, S(h_{(2)}).v'\rangle \end{aligned}$$

which by the property of the original pairing will follow from

$$\begin{aligned} &\varphi_{(1)}(S(h_{(3)}))\varphi_{(3)}(h_{(1)})\varphi_{(2)}(S(\rho_{(1)}))\psi(\rho_{(2)})h_{(2)} \\ &= \psi_{(1)}(h_{(1)})\psi_{(3)}(S(h_{(3)}))\varphi(S(\rho_{(1)}))\psi_{(2)}(\rho_{(2)})h_{(2)} \end{aligned}$$

This can be written as

$$\varphi(S(h_{(3)})S(\rho_{(1)})h_{(1)})\psi(\rho_{(2)})h_{(2)} = \varphi(S(\rho_{(1)}))\psi(h_{(1)}\rho_{(2)}S(h_{(3)}))h_{(2)}$$

which is a consequence of the fact that $S(\rho_{(1)}) \otimes \rho_{(2)}$ is a symmetric Casimir element.[92] $\square$

Suppose now that W and W' is another pair of finite-dimensional H-modules endowed with another nondegenerate pairing $\langle \cdot, \cdot \rangle : W \times W' \to K$ that satisfies

$$\langle h.w, w'\rangle = \langle w, S(h).w'\rangle$$

for all $w \in W$, $w' \in W'$, and $h \in H$. We can then form a pairing between the tensor products $V \otimes W$ and $W' \otimes V'$ that has the form

$$\langle v \otimes w, w' \otimes v'\rangle := \langle v, v'\rangle\langle w, w'\rangle$$

This pairing is also nondegenerate and satisfies

$$\langle h.(v \otimes w), w' \otimes v'\rangle = \langle v \otimes w, S(h).(w' \otimes v')\rangle$$

We can therefore invoke the preceding lemma to get a nondegenerate pairing $\langle \cdot, \cdot \rangle$ between $\mathrm{Ind}(V \otimes W)$ and $\mathrm{Ind}(W' \otimes V')$ that has the explicit form

$$\langle \varphi \otimes v \otimes w, \psi \otimes w' \otimes v'\rangle = (S(\varphi)\psi)(\rho)\langle v, v'\rangle\langle w, w'\rangle$$

Interchanging the roles of V and W, we also get a pairing between $\mathrm{Ind}(W \otimes V)$ and $\mathrm{Ind}(V' \otimes W')$, for which we use the same notation and which is explicitly given as

$$\langle \varphi \otimes w \otimes v, \psi \otimes v' \otimes w'\rangle = (S(\varphi)\psi)(\rho)\langle w, w'\rangle\langle v, v'\rangle$$

These pairings are compatible with the morphisms introduced in Paragraph 7.1 in the following way:

Proposition

$$\langle \rho_{V,W}(\varphi \otimes v \otimes w), v' \otimes w' \rangle = \langle \varphi \otimes v \otimes w, \rho_{V',W'}(v' \otimes w') \rangle$$

Proof. On the one hand, we have

$$\begin{aligned}
\langle \rho_{V,W}(\varphi \otimes v \otimes w), v' \otimes w' \rangle &= \sum_{i=1}^{n} \langle \varphi b_i \otimes w \otimes b_i.v, v' \otimes w' \rangle \\
&= \sum_{i=1}^{n} (S(\varphi b_i))()\langle w, w' \rangle \langle b_i.v, v' \rangle \\
&= \sum_{i=1}^{n} (S(b_i)S(\varphi))()\langle w, w' \rangle \langle v, S(b_i).v' \rangle \\
&= \sum_{i=1}^{n} (b_i S(\varphi))()\langle w, w' \rangle \langle v, b_i.v' \rangle
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
\langle \varphi \otimes v \otimes w, \rho_{V',W'}(v' \otimes w') \rangle &= \sum_{i=1}^{n} \langle \varphi \otimes v \otimes w, b_i \otimes w' \otimes b_i.v' \rangle \\
&= \sum_{i=1}^{n} (S(\varphi) b_i)()\langle v, b_i.v' \rangle \langle w, w' \rangle
\end{aligned}$$

Both expressions are equal because δ is cocommutative.[93] □

It is of course possible to choose the dual V^* for V' and the dual W^* for W'. The above discussion then shows that $\mathrm{Ind}(V \otimes W)^* = \mathrm{Ind}(W^* \otimes V^*)$ and also $\mathrm{Ind}(W \otimes V)^* = \mathrm{Ind}(V^* \otimes W^*)$. Using these identifications, it follows from the above proposition that we have

$$\rho_{V,W}^* = \rho_{V^*,W^*}$$

for the transpose of $\rho_{V,W}$.

7.3 As pointed out by D. Nikshych,[94] the natural transformation χ introduced in Definition 7.1 can be related to the categorical center construction. Recall[95] that the category of modules over the Drinfel'd double $D = D(H)$ can be considered as the center of the category of H-modules. This implies in particular that for every D-module U and every H-module V we have the isomorphism

$$c_{V,U}: V \otimes U \to U \otimes V, \quad v \otimes u \mapsto \sum_{i=1}^{n} (b_i \otimes 1).u \otimes b_i.v$$

which consists in the application of the R-matrix followed by interchanging the tensorands. Its inverse is therefore given by

$$c_{V,U}^{-1} : U \otimes V \to V \otimes U;\ u \otimes v \mapsto \sum_{i=1}^{n} S(b_i).v \otimes (b_i^* \otimes 1).u$$

To relate this map to the isomorphism $\tau_{V,W}$, where W is another H-module, note that

$$\mathrm{Hom}_D(\mathrm{Ind}(V \otimes W), U) = \mathrm{Hom}_H(V \otimes W, U)$$

by the Frobenius reciprocity theorem.[96] Therefore, there is a unique isomorphism $\tau'_{V,W,U}$ that makes the diagram

$$\begin{tikzcd}
\mathrm{Hom}_D(\mathrm{Ind}(W \otimes V), U) \arrow[r, "\tau_{V,W}^*"] \arrow[d] & \mathrm{Hom}_D(\mathrm{Ind}(V \otimes W), U) \arrow[d] \\
\mathrm{Hom}_H(W \otimes V, U) \arrow[r, "\tau'_{V,W,U}"'] & \mathrm{Hom}_H(V \otimes W, U)
\end{tikzcd}$$

commutative, where $\tau_{V,W}^*$ denotes the map coming from $\tau_{V,W}$ by composition on the right. The isomorphism $\tau'_{V,W,U}$ is given explicitly as

$$\tau'_{V,W,U}(f)(v \otimes w) = \sum_{i=1}^{n} (b_i^* \otimes 1).f(w \otimes b_i.v)$$

for $f \in \mathrm{Hom}_H(W \otimes V, U)$, as we have

$$(g \circ \tau_{V,W})(\varepsilon \otimes v \otimes w) = g\Big(\sum_{i=1}^{n} b_i^* \otimes w \otimes b_i.v\Big) = \sum_{i=1}^{n} (b_i^* \otimes 1).g(\varepsilon \otimes w \otimes b_i.v)$$

for $g \in \mathrm{Hom}_D(\mathrm{Ind}(W \otimes V), U)$.

Besides the adjunction between induction and restriction that appears in the Frobenius reciprocity theorem, there are two other pairs of adjoint functors that appear in this setting: The composition[97]

$$\mathrm{Hom}_K(W, U \otimes V^*) \to \mathrm{Hom}_K(W \otimes V, U \otimes V^* \otimes V) \to \mathrm{Hom}_K(W \otimes V, U)$$

where the first map takes f to $f \otimes \mathrm{id}_V$ and the second evaluates V^* on V, defines a homomorphism from $\mathrm{Hom}_K(W, U \otimes V^*)$ to $\mathrm{Hom}_K(W \otimes V, U)$. The image $g \in \mathrm{Hom}_K(W \otimes V, U)$ of $f \in \mathrm{Hom}_K(W, U \otimes V^*)$ is given explicitly as

$$g(w \otimes v) = \sum_j \varphi_j(v) u_j$$

if $f(w) = \sum_j u_j \otimes \varphi_j$. This composition is bijective if V is finite-dimensional. Because the evaluation map $V^* \otimes V \to K, \; \varphi \otimes v \mapsto \varphi(v)$ is H-linear, both mappings that appear in the composition preserve the subspace of H-linear maps, so that we can restrict this composition to a map from $\mathrm{Hom}_H(W, U \otimes V^*)$ to $\mathrm{Hom}_H(W \otimes V, U)$, which is an isomorphism in the finite-dimensional case.

Similarly, the composition

$$\mathrm{Hom}_K(W, V^* \otimes U) \to \mathrm{Hom}_K(V \otimes W, V \otimes V^* \otimes U) \to \mathrm{Hom}_K(V \otimes W, U)$$

obtained by tensoring with id_V on the left and then evaluating V^* on V leads to a homomorphism that takes a linear map $f \in \mathrm{Hom}_K(W, V^* \otimes U)$ to the map $g \in \mathrm{Hom}_K(V \otimes W, U)$ that satisfies

$$g(v \otimes w) = \sum_j \varphi_j(v) u_j$$

if $f(w) = \sum_j \varphi_j \otimes u_j$. This time, the second homomorphism in the composition uses the evaluation map

$$V \otimes V^* \to K, \; v \otimes \varphi \mapsto \varphi(v)$$

But as the antipode is an involution, this evaluation map is also H-linear, so that we again get a homomorphism from $\mathrm{Hom}_H(W, V^* \otimes U)$ to $\mathrm{Hom}_H(V \otimes W, U)$ by restriction, which is an isomorphism if V is finite-dimensional.

All these mappings come together in the following proposition:

Proposition The diagram

$$\begin{tikzcd}
\mathrm{Hom}_H(W \otimes V, U) \arrow[r, "\sigma'_{V,W,U}"] & \mathrm{Hom}_H(V \otimes W, U) \\
\mathrm{Hom}_H(W, U \otimes V^*) \arrow[u] \arrow[r, "c^{-1}_{V^*,U*}"'] & \mathrm{Hom}_H(W, V^* \otimes U) \arrow[u]
\end{tikzcd}$$

is commutative, where $c^{-1}_{V^*,U*}$ denotes composition with $c^{-1}_{V^*,U}$ on the left.

Proof. Suppose that $f \in \mathrm{Hom}_H(W, U \otimes V^*)$. The two possible paths in the diagram give two elements of $\mathrm{Hom}_H(V \otimes W, U)$, and we have to prove that they are equal. For this, it suffices to show that they agree for every decomposable tensor $v \otimes w \in V \otimes W$. To see this, write $f(w) = \sum_j u_j \otimes \varphi_j$. Then we have

$$c^{-1}_{V^*,U*}(f(w)) = \sum_j \sum_{i=1}^n S(b_i).\varphi_j \otimes (b_i^* \otimes 1).u_j$$

This means that the homomorphism that arises from composing the lower and the right arrow maps our decomposable tensor $v \otimes w$ to

$$\sum_j \sum_{i=1}^n (S(b_i).\varphi_j)(v)\,(b_i^* \otimes 1).u_j = \sum_j \sum_{i=1}^n \varphi_j(b_i.v)\,(b_i^* \otimes 1).u_j$$

where we have used that the antipode is an involution.

On the other hand, if $g \in \mathrm{Hom}_{H^{op}}(W \otimes V, U)$ is the image of f under the left arrow, then we have $g(w \otimes v) = \sum_j \varphi_j(v) u_j$, so that

$$\theta'_{V,W,U}(g)(v \otimes w) = \sum_{i=1}^n (b_i^* \otimes 1).g(w \otimes b_i.v) = \sum_j \sum_{i=1}^n \varphi_j(b_i.v)\,(b_i^* \otimes 1).u_j$$

which is exactly the result coming from the other path. $\Box$

If we insert the definition of $\theta'_{V,W,U}$ in this diagram, we can extend the vertical arrows by the isomorphisms coming from the Frobenius reciprocity theorem to get the diagram

$$\begin{tikzcd}
\mathrm{Hom}_D(\mathrm{Ind}(W \otimes V), U) \arrow[r, "\sigma_{V,W}"] & \mathrm{Hom}_D(\mathrm{Ind}(V \otimes W), U) \\
\mathrm{Hom}_H(W, U \otimes V) \arrow[u] \arrow[r, "c_{V,U}^{-1}"'] & \mathrm{Hom}_H(W, V \otimes U) \arrow[u]
\end{tikzcd}$$

which exhibits the relation between the natural transformation σ and the categorical center construction.

7.4 The coherence properties of the natural transformation σ stated in Proposition 7.1 can also be related to the coherence properties of the natural transformation c required in the categorical center construction.[98] If V_1 and V_2 are H-modules and U is a D-module, then the natural transformation c makes the triangle

$$\begin{tikzcd}
U \otimes V_2 \otimes V_1 \arrow[rr, "c_{V_2 \otimes V_1, U}^{-1}"] \arrow[dr, "c_{V_2,U}^{-1} \otimes \mathrm{id}_{V_1}"'] & & V_2 \otimes V_1 \otimes U \\
& V_2 \otimes U \otimes V_1 \arrow[ur, "\mathrm{id}_{V_2} \otimes c_{V_1,U}^{-1}"'] &
\end{tikzcd}$$

commutative. If W is another H-module, we therefore have that the diagram

$$\begin{tikzcd}
\mathrm{Hom}_H(W, U \otimes V_2 \otimes V_1) \arrow[rr, "c^{-1}_{V_2 \otimes V_1, U}"] \arrow[dr, "(c^{-1}_{V_2, U} \otimes \mathrm{id}_{V_1})"'] & & \mathrm{Hom}_H(W, V_2 \otimes V_1 \otimes U) \\
& \mathrm{Hom}_H(W, V_2 \otimes U \otimes V_1) \arrow[ur, "(\mathrm{id}_{V_2} \otimes c^{-1}_{V_1, U})"'] &
\end{tikzcd}$$

also commutes, where we have used the circle notation from Paragraph 7.3. To translate this diagram into a diagram for the natural transformation , we need as an intermediate step on the left side the diagram

$$\begin{tikzcd}
\mathrm{Hom}_H(W, U \otimes V_2 \otimes V_1) \arrow[r, "(c^{-1}_{V_2, U} \otimes \mathrm{id}_{V_1})"] \arrow[d] & \mathrm{Hom}_H(W, V_2 \otimes U \otimes V_1) \arrow[d] \\
\mathrm{Hom}_H(W \otimes V_1, U \otimes V_2) \arrow[r, "c^{-1}_{V_2, U}"'] \arrow[d] & \mathrm{Hom}_H(W \otimes V_1, V_2 \otimes U) \arrow[d] \\
\mathrm{Hom}_H(W \otimes V_1 \otimes V_2, U) \arrow[r, "c'_{V_2, W \otimes V_1, U}"'] & \mathrm{Hom}_H(V_2 \otimes W \otimes V_1, U)
\end{tikzcd}$$

where the first diagram commutes because of the naturality of the adjunction and the second diagram commutes by Proposition 7.3. Similarly, we need on the right side the diagram

$$\begin{tikzcd}
\mathrm{Hom}_H(W, V_2 \otimes U \otimes V_1) \arrow[r, "(\mathrm{id}_{V_2} \otimes c^{-1}_{V_1, U})"] \arrow[d] & \mathrm{Hom}_H(W, V_2 \otimes V_1 \otimes U) \arrow[d] \\
\mathrm{Hom}_H(V_2 \otimes W, U \otimes V_1) \arrow[r, "c^{-1}_{V_1, U}"'] \arrow[d] & \mathrm{Hom}_H(V_2 \otimes W, V_1 \otimes U) \arrow[d] \\
\mathrm{Hom}_H(V_2 \otimes W \otimes V_1, U) \arrow[r, "c'_{V_1, V_2 \otimes W, U}"'] & \mathrm{Hom}_H(V_1 \otimes V_2 \otimes W, U)
\end{tikzcd}$$

which commutes for exactly the same reasons. Using this, the commuting triangle for c above translates into the diagram

$$\begin{tikzcd}
\mathrm{Hom}_H(W \otimes V_1 \otimes V_2; U) \arrow[rr, "\sigma'_{V_1 \otimes V_2, W; U}"] \arrow[dr, "\sigma'_{V_2, W \otimes V_1; U}"'] & & \mathrm{Hom}_H(V_1 \otimes V_2 \otimes W; U) \arrow[dl, "\sigma'_{V_1, V_2 \otimes W; U}"] \\
& \mathrm{Hom}_H(V_2 \otimes W \otimes V_1; U) &
\end{tikzcd}$$

where the map at the top has been translated by Proposition 7.3, using the fact that $(V_1 \otimes V_2)^* = V_2^* \otimes V_1^*$ in a way that is compatible with the translation.

Using the adjunction between induction and restriction again, we can translate the last triangle further into the triangle

$$\begin{tikzcd}
\mathrm{Hom}_D(\mathrm{Ind}(W \otimes V_1 \otimes V_2); U) \arrow[rr, "\sigma_{V_1 \otimes V_2, W}"] \arrow[dr, "\sigma_{V_2, W \otimes V_1}"'] & & \mathrm{Hom}_D(\mathrm{Ind}(V_1 \otimes V_2 \otimes W); U) \arrow[dl, "\sigma_{V_1, V_2 \otimes W}"] \\
& \mathrm{Hom}_D(\mathrm{Ind}(V_2 \otimes W \otimes V_1); U) &
\end{tikzcd}$$

which in turn by the Yoneda lemma implies the first coherence property of σ as given in Proposition 7.1. Note that, although all the above diagrams commute in any case, this amounts to a new proof of first coherence property of σ only in the case where V_1 and V_2 are finite-dimensional, because otherwise the commutativity of the second triangle above does not logically imply the commutativity of the third triangle.

7.5 To analyse the relation between σ and c further, we need some preparation. So far in this section, we have basically used two pairs of adjoint functors: The adjunction between induction and restriction and the adjunction between tensoring with a module and tensoring with its dual. These two adjunctions can be related by the following map:

Lemma For an H-module V and a D-module W, the map

$$r_{V,W}: \mathrm{Ind}(V \otimes W) \to \mathrm{Ind}(V) \otimes W;\ x \otimes_H (v \otimes w) \mapsto (x_{(1)} \otimes_H v) \otimes x_{(2)}.w$$

is a D-linear isomorphism.

Proof. First, $r_{V,W}$ is well-defined, as we have

$$\begin{aligned} r_{V,W}(xh \otimes_H (v \otimes w)) &= (x_{(1)}h_{(1)} \otimes_H v) \otimes x_{(2)}h_{(2)}.w \\ &= (x_{(1)} \otimes_H h_{(1)}v) \otimes x_{(2)}h_{(2)}.w = r_{V,W}(x \otimes_H (h_{(1)}.v \otimes h_{(2)}.w)) \end{aligned}$$

The reader should verify at this point that $r_{V,W}$ is D-linear. The bijectivity will follow if we can show that the potential inverse

$$r_{V,W}^{-1} : \mathrm{Ind}(V) \otimes W \to \mathrm{Ind}(V \otimes W);\ (x \otimes_H v) \otimes w \mapsto x_{(1)} \otimes_H (v \otimes S(x_{(2)}).w)$$

is also well-defined. This holds because

$$\begin{aligned} r_{V,W}^{-1}((xh \otimes_H v) \otimes w) &= x_{(1)}h_{(1)} \otimes_H (v \otimes S(x_{(2)}h_{(2)}).w) \\ &= x_{(1)} \otimes_H (h_{(1)}.v \otimes h_{(2)}S(h_{(3)})S(x_{(2)}).w) = x_{(1)} \otimes_H (h.v \otimes S(x_{(2)}).w) \end{aligned}$$

establishing the assertion. □

Note that, under the correspondence of both $\mathrm{Ind}(V \otimes W)$ and $\mathrm{Ind}(V) \otimes W$ to $H^* \otimes V \otimes W$ introduced in Paragraph 7.1, the map $r_{V,W}$ becomes

$$r_{V,W} : H^* \otimes V \otimes W \to H^* \otimes V \otimes W;\ \varphi \otimes v \otimes w \mapsto \varphi_{(2)} \otimes v \otimes (\varphi_{(1)} \otimes 1).w$$

Our claim that $r_{V,W}$ relates the two adjunctions is justified by the following proposition:

Proposition For an H-module V and D-modules W and U, the diagram

$$\begin{tikzcd} \mathrm{Hom}_D(\mathrm{Ind}(V \otimes W), U) \arrow[rr, "\cong"] & & \mathrm{Hom}_H(V \otimes W, U) \\ \mathrm{Hom}_D(\mathrm{Ind}(V) \otimes W, U) \arrow[u, "r^*_{V,W}"] & & \mathrm{Hom}_H(V, U \otimes W^*) \arrow[u] \\ & \mathrm{Hom}_D(\mathrm{Ind}(V), U \otimes W^*) \arrow[ul] & \end{tikzcd}$$

commutes.

Proof. Suppose that $f \in \mathrm{Hom}_D(\mathrm{Ind}(V), U \otimes W^*)$, and consider the image $g \in \mathrm{Hom}_H(V \otimes W, U)$ of f under the left path. Since

$$r_{V,W}(1 \otimes_H (v \otimes w)) = (1 \otimes_H v) \otimes w$$

we have $g(v \otimes w) = \sum_j \varphi_j(w_j)u_j$ iff $f(1 \otimes_H v) = \sum_j u_j \otimes \varphi_j$. But this is exactly the map that arises as the image of f under the right path. □

7.6 As a comparison shows, the coherence condition stated at the beginning of Paragraph 7.4 corresponds to only one of the two conditions that appear in the definition of a quasisymmetry.[99] From the point of view of the center construction, the second condition enters into the definition of the tensor product of two objects. We therefore expect that there is another relation between and c that can be deduced from this second condition by arguing as in Paragraph 7.4. Before we state this relation, we recall the relation between braiding and duality:

Lemma For an H-module V and a D-module U, the diagram

$$\begin{tikzcd}
V^* \otimes U^* \arrow[r, "\cong"] \arrow[d, "c_{V^*,U^*}"'] & (U \otimes V)^* \arrow[d, "c^*_{V,U}"] \\
U^* \otimes V^* \arrow[r, "\cong"] & (V \otimes U)^*
\end{tikzcd}$$

commutes.

Proof. Recall[100] that the top horizontal arrow maps $\varphi \otimes \psi \in V^* \otimes U^*$ to the linear form $u \otimes v \mapsto \varphi(v)\psi(u)$, and the horizontal arrow at the bottom is defined similarly. We therefore have for $\varphi \in V^*$, $\psi \in U^*$, $v \in V$, and $u \in U$ that

$$\begin{aligned}
c_{V^*,U^*}(\varphi \otimes \psi)(v \otimes u) &= \sum_{i=1}^{n} ((b_i \otimes 1).\psi \otimes b_i.\varphi)(v \otimes u) \\
&= \sum_{i=1}^{n} \psi(S_D(b_i \otimes 1).u)\,\varphi(S(b_i).v) \\
&= \sum_{i=1}^{n} \psi((b_i \otimes 1).u)\,\varphi(b_i.v) = (\varphi \otimes \psi)(c_{V,U}(v \otimes u))
\end{aligned}$$

where we have used the notation from Paragraph 2.2 resp. Paragraph 7.4 for the R-matrix. $\square$

With the help of this lemma, we now derive the following additional relation between and c:

Proposition Suppose that V and W are H-modules and that U is a D-module. We assume that V and U are finite-dimensional. Then the diagram

$$
\begin{tikzcd}
\operatorname{Ind}(V\otimes W\otimes U) \arrow[rr, "\Phi_{V,W\otimes U}"] \arrow[d, "r_{V\otimes W,U}"'] & & \operatorname{Ind}(W\otimes U\otimes V) \\
\operatorname{Ind}(V\otimes W)\otimes U \arrow[dr, "\Phi_{V,W}\otimes \mathrm{id}_U"'] & & \operatorname{Ind}(W\otimes V\otimes U) \arrow[u, "\operatorname{Ind}(\mathrm{id}_W\otimes c_{V,U})"'] \\
& \operatorname{Ind}(W\otimes V)\otimes U \arrow[ur, "r^{-1}_{W\otimes V,U}"'] &
\end{tikzcd}
$$

commutes.

Proof. By the Yoneda lemma, it suffices to prove the commutativity of the diagram after the application of the contravariant functor $\operatorname{Hom}_D(\ \cdot\ ;X)$, where X is another D-module. After this application, the diagram takes the form

$$
\begin{tikzcd}
\operatorname{Hom}_D(\operatorname{Ind}(V\otimes W\otimes U);X) & & \operatorname{Hom}_D(\operatorname{Ind}(W\otimes U\otimes V);X) \arrow[ll, "\Phi^*_{V,W\otimes U}"'] \arrow[d, "\operatorname{Ind}(\mathrm{id}_W\otimes c_{V,U})^*"] \\
\operatorname{Hom}_D(\operatorname{Ind}(V\otimes W)\otimes U;X) \arrow[u, "r^*_{V\otimes W,U}"] & & \operatorname{Hom}_D(\operatorname{Ind}(W\otimes V\otimes U);X) \arrow[dl, "r^{-1*}_{W\otimes V,U}"] \\
& \operatorname{Hom}_D(\operatorname{Ind}(W\otimes V)\otimes U;X) \arrow[ul, "(\Phi_{V,W}\otimes \mathrm{id}_U)^*"] &
\end{tikzcd}
$$

Using the defining property of the maps Φ' from Paragraph 7.3 together with Proposition 7.5, we see that the commutativity of this diagram follows from the commutativity of the diagram

$$
\begin{tikzcd}
\operatorname{Hom}_H(V\otimes W\otimes U;X) & & \operatorname{Hom}_H(W\otimes U\otimes V;X) \arrow[ll, "\Phi'_{V,W\otimes U;X}"'] \arrow[d, "(\mathrm{id}_W\otimes c_{V,U})^*"] \\
\operatorname{Hom}_H(V\otimes W;X\otimes U^*) \arrow[u] & & \operatorname{Hom}_H(W\otimes V\otimes U;X) \\
& \operatorname{Hom}_H(W\otimes V;X\otimes U^*) \arrow[ul, "\Phi'_{V,W;X\otimes U^*}"] &
\end{tikzcd}
$$

By taking V and U to the right side in this diagram, we get from Proposition 7.3 that our assertion is equivalent to the commutativity of

$$
\begin{tikzcd}
\mathrm{Hom}_H(W, V \otimes X \otimes U) \arrow[rr, "(c^{-1}_{V,X} \otimes \mathrm{id}_U)_*"] & & \mathrm{Hom}_H(W, X \otimes V \otimes U) \arrow[d, "(\mathrm{id}_X \otimes c_{V,U})_*"] \\
\mathrm{Hom}_H(W, V \otimes X \otimes U) \arrow[u, "\mathrm{id}"] & & \mathrm{Hom}_H(W, X \otimes U \otimes V) \arrow[dl, "\mathrm{id}"] \\
& \mathrm{Hom}_H(W, X \otimes U \otimes V) \arrow[ul, "c^{-1}_{V,X \otimes U}"] &
\end{tikzcd}
$$

where we have used in addition the preceding lemma for the right vertical arrow. But this is now by the Yoneda lemma equivalent to the equation

$$c_{V,X \otimes U} = (\mathrm{id}_X \otimes c_{V,U}) \circ (c_{V,X} \otimes \mathrm{id}_U)$$

that is used to define the tensor product in the center construction.[101] □

It is of course also possible to prove this proposition by direct computation: For $\varphi \in H$, $v \in V$, $w \in W$, and $u \in U$, we have on the one hand

$$
\begin{aligned}
&(r^{-1}_{W \otimes V,U} \circ (\sigma_{V,W} \otimes \mathrm{id}_U) \circ r_{V \otimes W,U})(\varphi \otimes v \otimes w \otimes u) \\
&= (r^{-1}_{W \otimes V,U} \circ (\sigma_{V,W} \otimes \mathrm{id}_U))(\varphi_{(2)} \otimes v \otimes w \otimes (\varphi_{(1)} \otimes 1).u) \\
&= \sum_{i=1}^{n} r^{-1}_{W \otimes V,U}(\varphi_{(2)} b_i \otimes w \otimes b_i.v \otimes (\varphi_{(1)} \otimes 1).u) \\
&= \sum_{i=1}^{n} \varphi_{(3)} b_{i(2)} \otimes w \otimes b_i.v \otimes (S^{-1}(\varphi_{(2)} b_{i(1)}) \otimes 1)(\varphi_{(1)} \otimes 1).u \\
&= \sum_{i=1}^{n} \varphi b_{i(2)} \otimes w \otimes b_i.v \otimes (S^{-1}(b_{i(1)}) \otimes 1).u
\end{aligned}
$$

and on the other hand

$$
\begin{aligned}
&(\mathrm{Ind}(\mathrm{id}_W \otimes c^{-1}_{V,U}) \circ (\sigma_{V,W \otimes U}))(\varphi \otimes v \otimes w \otimes u) \\
&= \sum_{i=1}^{n} \mathrm{Ind}(\mathrm{id}_W \otimes c^{-1}_{V,U})(\varphi b_i \otimes w \otimes u \otimes b_i.v) \\
&= \sum_{i,j=1}^{n} \varphi b_i \otimes w \otimes S(b_j) b_i.v \otimes (b_j \otimes 1).u
\end{aligned}
$$

The assertion therefore would follow from the equation

$$\sum_{i=1}^{n} b_{i(2)} \otimes b_i \otimes S^{-1}(b_{i(1)}) = \sum_{i,j=1}^{n} b_i \otimes S(b_j) b_i \otimes b_j$$

But as we have

$$\begin{aligned}\sum_{i=1}^{n} b_{i(2)}(h)\, b_i\, S^{-1}(b_{i(1)})(h') &= \sum_{i=1}^{n} b_i(S^{-1}(h')h)\, b_i \\ &= S^{-1}(h')h = \sum_{i,j=1}^{n} b_i(h)\, S(b_j) b_i\, b_j(h')\end{aligned}$$

this equation holds.

Besides being substantially simpler, the proof by direct computation also shows that the requirement that V and U be finite-dimensional is unnecessary. We have nonetheless chosen to give the proof above because it exhibits the relation to the second condition in the definition of a quasisymmetry. Note that these conditions also correspond to the equations for $(\Delta \otimes \mathrm{id})(R)$ and $(\mathrm{id} \otimes \Delta)(R)$ that appear in the definition of a quasitriangular Hopf algebra stated in Paragraph 2.1.

8 Equivariant Frobenius-Schur indicators

8.1 We continue to work in the setting of Section 7, which was described in Paragraph 7.1. So, H is a semisimple Hopf algebra over an algebraically closed field K of characteristic zero, and $D = D(H)$ is its Drinfel'd double. For a finite-dimensional H-module V and a positive integer m, we can of course form the m-th tensor power $V^{\otimes m}$ of V, and the Drinfel'd double D acts on its induced module $\mathrm{Ind}(V^{\otimes m})$. We denote the corresponding representation by

$$\rho_m : D \to \mathrm{End}(\mathrm{Ind}(V^{\otimes m}))$$

A further endomorphism of $\mathrm{Ind}(V^{\otimes m})$ is $\vartheta := \sigma_{V,V^{\otimes(m-1)}}$. Using these ingredients, we can now define the following quantities:

Definition For integers $m, l \in \mathbb{Z}$ with $m \geq 1$ and a central element $z \in Z(D)$, we define the (m,l)-th equivariant Frobenius-Schur indicator of V and z as

$$I_V((m,l),z) := \mathrm{tr}(\vartheta^l \circ \rho_m(z))$$

We extend this definition to all integers m as follows: If $m = 1$, we define the indicator by setting $I_V((m,l),z) := \mathrm{tr}(\rho_1(u_D^{-l}) \circ \rho_1(z))$. If $m = 0$, we write $z = \sum_j \varphi_j \otimes h_j$, and define for $l > 0$

$$I_V((0,l),z) := \dim(H) \sum_j \varepsilon(h_j)\varphi_j(\Lambda_{(1)})\chi_V(S^{-1}(\Lambda_{(2)}))$$

where $\Lambda \in H$ is the integral that satisfies $\varepsilon(\Lambda) = 1$. For $l = 0$, we define $I_V((0,0),z) := \dim(H)\sum_j \varepsilon(h_j)\varphi_j(\Lambda)$, whereas we define

$$I_V((0,l),z) := I_V((0,-l),S_D(z))$$

for $l < 0$. In the last case where $m < 0$, we similarly define

$$I_V((m,l),z) = I_V((-m,-l),S_D(z))$$

In the main case where $m \geq 1$, it should be noted that we have $\vartheta^l = \sigma_{V^{\otimes l},V^{\otimes(m-l)}}$ for $l = 1,2,\dots,m-1$. This follows inductively from the coherence property given in Proposition 7.1, because, if we set $U = V^{\otimes l}$ and $W = V^{\otimes(m-l-1)}$ there, we obtain the equation $\sigma_{V^{\otimes(l+1)},V^{\otimes(m-l-1)}} = \sigma_{V,V^{\otimes(m-1)}} \circ \sigma_{V^{\otimes l},V^{\otimes(m-l)}}$. If we interpret the 0-th tensor power as the trivial module $K = V^{\otimes 0}$, then this formula also extends to the cases $l = 0$ and $l = m$, because $\vartheta^0 = \mathrm{id}$ corresponds to $\sigma_{K,V^{\otimes m}}$ by Proposition 7.1, and

$$\vartheta^m(x) = \vartheta(\vartheta^{m-1}(x)) = \sigma_{V,V^{\otimes(m-1)}}(\sigma_{V^{\otimes(m-1)},V}(x)) = u_D^{-1}.x$$

by Lemma 7.1, which corresponds by Proposition 7.1 to $\sigma_{V^{\otimes m},K}$. From this viewpoint, the case $m = 1$ can also be subsumed under the case $m \geq 1$, because then coincides with the action of $u_D^{\ 1}$. It should also be noted that the formula $I_V((\ m;\ l);z) = I_V((m;l);S_D(z))$ holds for all integers m and l by definition; if $m = l = 0$, one needs Lemma 6.1 in addition to see this.

An easy consequence of this definition is the following formula for the indicators of a tensor power:

Lemma $I_{V\ q}((m;l);z) = I_V((qm;ql);z)$

Proof. It is understood here that $q > 0$ is a natural number. We consider the case $m > 1$ first. As just explained, the q-th power of $\ := \ _{V;V\ (qm\ 1)}$ is $\ ^q = \ _{V\ q;V\ (qm\ q)}$, so that

$$I_{V\ q}((m;l);z) = \mathrm{tr}(\ ^{ql}\ \ _{qm}(z)) = I_V((qm;ql);z)$$

The formula also holds in the case $m = 1$ by the explanations above, and in the cases $m = 0$ and $m < 0$ it follows directly from the definitions. 2

Part of the name given above to the quantities $I_V((m;l);z)$ is explained by the following proposition, which relates them to the higher Frobenius-Schur indicators:[102]

Proposition Suppose that $\ 2 H$ and $\ 2 H$ are integrals that are normalized so that $"(\ ) = \ (1) = 1$, and set $\ _D := \ $. If $\ _V$ denotes the character of the H-module V, then we have for its m-th Frobenius-Schur indicator $\ _m(\ _V)$ that

$$\ _m(\ _V) = I_V((m;1);\ _D)$$

for all integers $m > 0$.

Proof. We treat the case $m = 1$ separately. We have seen in Paragraph 2.3 that $\ _D$ is an integral of D; however, the normalization here is different from the one in Paragraph 6.1. By definition, we therefore have

$$I_V((1;1);\ _D) = \mathrm{tr}(\ _1(u_D^{\ 1})\ \ _1(\ _D)) = \mathrm{tr}(\ _1(\ _D))$$

Now we have $\ _1(\ _D)('\ \ v) = '(1)\ \ :v$, so that $\mathrm{tr}(\ _1(\ _D)) = \ _V(\ )$, which is the assertion.

In the case $m > 1$, note that the map

$$(V\ ^m)^H \ ! \ \mathrm{Ind}(V\ ^m)^D;\ w \mapsto \ \ w$$

is an isomorphism between the spaces of invariants,[103] because $\ _m(\ _D)$ is a projection to $\mathrm{Ind}(V\ ^m)^D$ and we have

$$\ _m(\ _D)('\ \ v_1\ \ :::\ \ v_m) = \ \ :('(1)v_1\ \ :::\ \ v_m)$$

Because σ is D-linear, it commutes with $\rho_m(\Lambda_D)$, and therefore preserves the space $\mathrm{Ind}(V^{\otimes m})^D$ of invariants. Similarly, the map

$$\tau : V^{\otimes m} \to V^{\otimes m},\ v_1 \otimes \cdots \otimes v_m \mapsto v_2 \otimes v_3 \otimes \cdots \otimes v_m \otimes v_1$$

preserves[104] the space $(V^{\otimes m})^H$, and the diagram

$$\begin{array}{ccc}
(V^{\otimes m})^H & \xrightarrow{\quad\tau\quad} & (V^{\otimes m})^H \\
{\scriptstyle w \mapsto \varepsilon \otimes w}\Big\downarrow & & \Big\downarrow{\scriptstyle w \mapsto \varepsilon \otimes w} \\
\mathrm{Ind}(V^{\otimes m})^D & \xrightarrow{\quad\sigma\quad} & \mathrm{Ind}(V^{\otimes m})^D
\end{array}$$

is commutative, since we have

$$\begin{aligned}
\sigma(\varepsilon \otimes v_1 \otimes v_2 \otimes \cdots \otimes v_m) &= \sum_{i=1}^{n} b_i \otimes v_2 \otimes \cdots \otimes v_m \otimes b_i^* . v_1 \\
&= \varepsilon \otimes v_2 \otimes \cdots \otimes v_m \otimes v_1 = \varepsilon \otimes \tau(v_1 \otimes v_2 \otimes \cdots \otimes v_m)
\end{aligned}$$

Since the restriction of σ to $\mathrm{Ind}(V^{\otimes m})^D$ is therefore conjugate to the restriction of τ to $(V^{\otimes m})^H$, the traces of these two maps have to coincide, which yields

$$I_V((m,1),\Lambda_D) = \mathrm{tr}(\sigma \circ \rho_m(\Lambda_D)) = \mathrm{tr}(\sigma|_{\mathrm{Ind}(V^{\otimes m})^D}) = \mathrm{tr}(\tau|_{(V^{\otimes m})^H}) = \nu_m(\chi_V)$$

by the first formula for the Frobenius-Schur indicators.[105] $\square$

It should be noted that the normalization for the integral of the Drinfel'd double in the preceding proposition is different from the one used in Paragraph 6.1; we have chosen the normalization in the proposition to avoid the appearance of another proportionality factor. Furthermore, it should be noted that, as a consequence of the preceding argument, the restriction of a power σ^l to $\mathrm{Ind}(V^{\otimes m})^D$ is also conjugate to the restriction of the corresponding power τ^l to $(V^{\otimes m})^H$, so that we get

$$I_V((m,l),\Lambda_D) = \mathrm{tr}(\tau^l|_{(V^{\otimes m})^H})$$

for all $l \in \mathbb{Z}$. This means[106] that $I_V((m,l),\Lambda_D) = \chi_V(\Lambda^{[m,l]})$ if l is relatively prime to m.

8.2 It is possible to express the equivariant Frobenius-Schur indicators in terms of the pairing between induced modules that we introduced in Paragraph 7.2. So, let V be a finite-dimensional H-module with dual V^*. Applying repeatedly the construction described in Paragraph 7.2, we get from the natural pairing $\langle \cdot , \cdot \rangle : V \otimes V^* \to K$ a pairing between $V^{\otimes m}$ and $V^{*\otimes m}$ that is given by

$$\langle v_1 \otimes v_2 \otimes \cdots \otimes v_m, \varphi_m \otimes \cdots \otimes \varphi_2 \otimes \varphi_1 \rangle = \langle v_1, \varphi_1 \rangle \langle v_2, \varphi_2 \rangle \cdots \langle v_m, \varphi_m \rangle$$

and this pairing leads, after we choose a nonzero integral Λ, to a pairing $\langle\cdot,\cdot\rangle$ between $\mathrm{Ind}(V^{\otimes m})$ and $\mathrm{Ind}(V^{*\otimes m})$. We choose an integral satisfying $\varepsilon(\Lambda) = 1$. Then, if $v_1,\ldots,v_d \in V$ is a basis of V with dual basis $v_1^*,\ldots,v_d^* \in V^*$, we get the following formula for the equivariant Frobenius-Schur indicators:

Proposition For all integers $m,l \in \mathbb{Z}$ with $m > 1$ and all central elements $z \in Z(D)$, we have

$$I_V((m,l),z) = \dim(H) \sum_{i_1,\ldots,i_m=1}^{d} \langle (\theta^{l}\rho_m(z))(\varepsilon \otimes v_{i_1} \otimes v_{i_2} \otimes \cdots \otimes v_{i_m}), \varepsilon \otimes v_{i_m}^* \otimes \cdots \otimes v_{i_2}^* \otimes v_{i_1}^* \rangle$$

Proof. If $z = \sum_j \varphi_j \otimes h_j$, we have because z is central that

$$\rho_m(z)(\varphi \otimes v_1 \otimes v_2 \otimes \cdots \otimes v_m) = \sum_j \varphi\varphi_j \otimes h_{j(1)}.v_1 \otimes \cdots \otimes h_{j(m)}.v_m$$

and $\theta(\varphi \otimes v_1 \otimes v_2 \otimes \cdots \otimes v_m) = \sum_{i=1}^{n} \varphi b_i^* \otimes v_2 \otimes \cdots \otimes v_m \otimes b_i.v_1$. This implies that, under the isomorphism $\mathrm{End}(H^* \otimes V^{\otimes m}) \cong \mathrm{End}(H^*) \otimes \mathrm{End}(V^{\otimes m})$, $\theta^{l}\rho_m(z)$ decomposes into a sum of tensor products of right multiplications and endomorphisms of $V^{\otimes m}$. But the trace of the right multiplication by φ on H^* is given by $\dim(H)\varphi(\Lambda)$, and the trace of an endomorphism of $V^{\otimes m}$ can be found by dual bases. Since $S(\Lambda) = \Lambda$, this gives the assertion. $\square$

As a consequence, we can give a formula for the equivariant indicators of the dual module:

Corollary For all $m,l \in \mathbb{Z}$ and all $z \in Z(D)$, we have

$$I_{V^*}((m,l),z) = I_V((m,l),S_D(z))$$

Proof. In the case where $m > 1$, we can argue as in the proof of the preceding proposition to obtain the formula

$$I_{V^*}((m,l),S_D(z)) = n \sum_{i_1,\ldots,i_m} \langle \varepsilon \otimes v_{i_1} \otimes \cdots \otimes v_{i_m}, \theta^{l}(S_D(z).(\varepsilon \otimes v_{i_m}^* \otimes \cdots \otimes v_{i_1}^*))\rangle$$

But by Proposition 7.2 and the discussion after Lemma 7.2, the right-hand side of this formula is equal to the right-hand side of the formula in the preceding proposition, establishing the case where $m > 1$. In the case $m = 1$ the assertion follows directly from the definition, since u_D is invariant under the antipode, and the case $m < 0$ reduces to the cases already treated.

Now suppose that $m = 0$. For $l > 0$, we have

$$I_{V^*}((0,l),z) = \dim(H) \sum_j \varepsilon(h_j)\varphi_j(\Lambda_{(1)})\,\chi_{V^*}^{\,l}(\Lambda_{(2)})$$
$$= \dim(H) \sum_j \varepsilon(h_j)\varphi_j(\Lambda_{(1)})\,\chi_{V}^{\,l}(S(\Lambda_{(2)}))$$

Because Λ is cocommutative and invariant under the antipode,[107] we can rewrite this as

$$I_V((0,l),z) = \dim(H) \sum_j \varepsilon(h_j)\varphi_j(S(\Lambda_{(1)}))\chi_{V^{\otimes l}}(\Lambda_{(2)})$$

But it follows from Lemma 6.1 that $S_D(z) = \sum_j S(\varphi_j) \otimes S(h_j)$, so that the last expression is $I_V((0,l),S_D(z))$. The case $l = 0$ can be established by a very similar reasoning, and the case $l < 0$ reduces as above to the cases already treated. $\Box$

It should be noted that, by comparison with Lemma 8.1 and in view of our definitions, this corollary shows that the dual space behaves with respect to the indicators like a -1-st tensor power of V.

8.3 The other part of the name of the quantities $I_V((m,l),z)$ is explained by the following equivariance theorem:

Theorem For all $g \in SL(2,\mathbb{Z})$, we have $I_V((m,l)g,z) = I_V((m,l),g.z)$.

Proof. (1) It suffices to check this on the generators given in Paragraph 1.1, and begin with the generator t. As this generator acts via T, the assertion then is that $I_V((m,m+l),z) = I_V((m,l),u_D^{-1}z)$. For $m > 1$, this follows from the fact that $\theta^{m} = \rho_m(u_D^{-1})$ as endomorphisms of $H \otimes V^{\otimes m}$, a fact that was already discussed after Definition 8.1. The case $m = 1$ follows directly from the definition, and for $m < 0$ we have

$$\begin{aligned} I_V((m,m+l),z) &= I_V((-m,-m-l),S_D(z)) = I_V((-m,-l),u_D^{-1}S_D(z)) \\ &= I_V((-m,-l),S_D(u_D^{-1}z)) = I_V((m,l),u_D^{-1}z) \end{aligned}$$

In the case $m = 0$ and $l > 0$, write $z = \sum_j \varphi_j \otimes h_j$. Because u_D is central, we then have $u_D^{-1}z = \sum_{i=1}^{n}\sum_j \varphi_j b_i \otimes b_i h_j$ and therefore

$$\begin{aligned} I_V((0,l),u_D^{-1}z) &= \dim(H) \sum_{i=1}^{n}\sum_j \varepsilon(b_i h_j)(\varphi_j b_i)(\Lambda_{(1)})\chi_{V^{\otimes l}}(\Lambda_{(2)}) \\ &= \dim(H) \sum_j \varepsilon(h_j)\varphi_j(\Lambda_{(1)})\chi_{V^{\otimes l}}(\Lambda_{(2)}) = I_V((0,l),z) \end{aligned}$$

The case $m = 0$ and $l = 0$ can be established by a very similar reasoning, and the case $m = 0$ and $l < 0$ reduces as above to the cases already treated.

(2) As the generator r^{-1} acts via R^{-1}, the assertion in this case says that $I_V((m+l,l),z) = I_V((m,l),R^{-1}(z))$. It follows from Proposition 6.2 and the fact, explained in Paragraph 5.1, that λ and Λ agree on the character ring, that we have $R^{-1}(z) = \tilde{R}^{-1}(z) = \sum e^{-1}(z_{(2)})z_{(1)}$ for every central element z.

The assertion therefore can also be written in the form $I_V((m+l,l),R(z)) = I_V((m,l),z)$, which we now establish in the case $m > 0$ and $l > 0$. For this, we write $l = pm + q$, where $0 \le q < m$. If $z = \sum_j \varphi_j \otimes h_j$, we have

$$(\rho_{l+m}(R(z)) \circ \sigma^{l})(\varphi \otimes v_1 \otimes \cdots \otimes v_{l+m}) = \sum_{i_1,\ldots,i_l=1}^{n} \sum_j \varphi_{j(1)}(h_{j(2)})\, \varphi b_{i_1} \cdots b_{i_l} \varphi_{j(2)} \otimes h_{j(1)}.(v_{l+1} \otimes \cdots \otimes v_{l+m} \otimes b^*_{i_1}.v_1 \otimes \cdots \otimes b^*_{i_l}.v_l)$$

By the dual basis formulas stated in the introduction, this means that we have

$$(\rho_{l+m}(R(z)) \circ \sigma^{l})(\varphi \otimes x \otimes w) = \sum_{i=1}^{n} \sum_j \varphi_{j(1)}(h_{j(2)})\, \varphi b_i \varphi_{j(2)} \otimes h_{j(1)}.(w \otimes b^*_i.x)$$

for all $x \in V^{\otimes l}$ and $w \in V^{\otimes m}$. This is a sum of tensor products of right multiplications on H^* and endomorphisms of $V^{\otimes(l+m)}$. If $\Lambda \in H$ is an integral satisfying $\varepsilon(\Lambda) = 1$, the right multiplication by $\varphi \in H^*$ has the trace $n\varphi(\Lambda)$, so that the equivariant Frobenius-Schur indicator $I_V((m+l,l),R(z))$, which is the trace of this map, is n-times the trace of the endomorphism f of $V^{\otimes(l+m)}$ given by

$$f(x \otimes w) = \sum_{i=1}^{n} \sum_j \varphi_{j(1)}(h_{j(2)})(b_i \varphi_{j(2)})(\Lambda)\, h_{j(1)}.(w \otimes b^*_i.x)$$

for $x \in V^{\otimes l}$ and $w \in V^{\otimes m}$, which can be rewritten in the form

$$\begin{aligned} f(x \otimes w) &= \sum_j \varphi_{j(1)}(h_{j(3)})\varphi_{j(2)}(\Lambda_{(2)})\,(h_{j(1)}.w \otimes h_{j(2)}\Lambda_{(1)}.x) \\ &= \sum_j \varphi_{j(1)}(h_{j(3)})\varphi_{j(2)}(S(h_{j(2)})\Lambda_{(2)})\,(h_{j(1)}.w \otimes \Lambda_{(1)}.x) \\ &= \sum_j \varphi_j(\Lambda_{(2)})\,(h_j.w \otimes \Lambda_{(1)}.x) \end{aligned}$$

(3) As we have discussed in Paragraph 8.1, we have on the right-hand side of the assertion that

$$\rho_m(z) \circ \sigma^{l} = \rho_m(z) \circ \sigma^{pm} \circ \sigma^{q} = \rho_m(z u_D^{\,p}) \circ \sigma^{q}$$

so that

$$(\rho_m(z) \circ \sigma^{l})(\varphi \otimes v_1 \otimes \cdots \otimes v_m) = \sum_{i_1,\ldots,i_q=1}^{n} \sum_{j_1,\ldots,j_p=1}^{n} \sum_j \varphi b_{i_1} \cdots b_{i_q} b_{j_1} \cdots b_{j_p} \varphi_j \otimes h_j b^*_{j_p} \cdots b^*_{j_1}.(v_{q+1} \otimes \cdots \otimes v_m \otimes b^*_{i_1}.v_1 \otimes \cdots \otimes b^*_{i_q}.v_q)$$

Using the dual basis formulas as before, we can write this as

$$(\rho_m(z) \circ \ell^{-1})(\varphi \otimes y \otimes t) = \sum_{i=1}^{n} \sum_{j_1,\ldots,j_p=1}^{n} \sum_{j} \varphi(b_i b_{j_1} \cdots b_{j_p} \varphi_j)\, h_j b^*_{j_p} \cdots b^*_{j_1} . (t \otimes b^*_i . y)$$

for $y \in V^{\otimes q}$ and $t \in V^{\otimes (m-q)}$. This is again a sum of tensor products of right multiplications on H^* and endomorphisms of $V^{\otimes m}$, so that we see as before that the equivariant Frobenius-Schur indicator $I_V((m,l),z)$, which is the trace of this map, is n-times the trace of the endomorphism g of $V^{\otimes m}$ given by

$$g(y \otimes t) = \sum_{i=1}^{n} \sum_{j_1,\ldots,j_p=1}^{n} \sum_{j} (b_i b_{j_1} \cdots b_{j_p} \varphi_j)(\Lambda)\, h_j b^*_{j_p} \cdots b^*_{j_1} . (t \otimes b^*_i . y)$$

for $y \in V^{\otimes q}$ and $t \in V^{\otimes (m-q)}$, which can be rewritten in the form

$$g(y \otimes t) = \sum_{j} \varphi_j(\Lambda_{(p+2)})\, h_j \Lambda_{(p+1)} \cdots \Lambda_{(2)} . (t \otimes \Lambda_{(1)} . y)$$

(4) The assertion therefore now is that $\mathrm{tr}_{V^{\otimes (m+l)}}(f) = \mathrm{tr}_{V^{\otimes m}}(g)$. This will hold if we can show that g is the partial trace of f over the last l tensor factors. Let us explain in greater detail what this means. Choose a basis $v_1, \ldots, v_d$ of V with dual basis $v^*_1, \ldots, v^*_d$ of V^*. The assertion then is that

$$g(w) = \sum_{i_1,\ldots,i_l=1}^{d} (\mathrm{id}_{V^{\otimes m}} \otimes v^*_{i_1} \otimes \cdots \otimes v^*_{i_l}) f(w \otimes v_{i_1} \otimes \cdots \otimes v_{i_l})$$

for all $w \in V^{\otimes m}$. To establish this, it is better to use a basis $w_1, \ldots, w_{d^m}$ of $W := V^{\otimes m}$ with dual basis $w^*_1, \ldots, w^*_{d^m}$ of W^* as well as a basis $y_1, \ldots, y_{d^q}$ of $Y := V^{\otimes q}$ with dual basis $y^*_1, \ldots, y^*_{d^q}$ of Y^*, and also to decompose w in the form $w = y \otimes t$ for $y \in V^{\otimes q}$ and $t \in V^{\otimes (m-q)}$. The assertion then becomes

$$g(y \otimes t) = \sum_{j_1,\ldots,j_p=1}^{d^m} \sum_{i=1}^{d^q} (\mathrm{id}_{V^{\otimes m}} \otimes y^*_i \otimes w^*_{j_1} \otimes \cdots \otimes w^*_{j_p}) f(y \otimes t \otimes y_i \otimes w_{j_1} \otimes \cdots \otimes w_{j_p})$$

To see this, we start at the right-hand side:

$$\sum_{j_1,\ldots,j_p=1}^{d^m} \sum_{i=1}^{d^q} (\mathrm{id}_{V^{\otimes m}} \otimes y^*_i \otimes w^*_{j_1} \otimes \cdots \otimes w^*_{j_p}) f(y \otimes t \otimes y_i \otimes w_{j_1} \otimes \cdots \otimes w_{j_p}) =$$

$$\sum_{j_1,\ldots,j_p=1}^{d^m} \sum_{i=1}^{d^q} \sum_{j} \varphi_j(\Lambda_{(p+3)}) (\mathrm{id}_{V^{\otimes m}} \otimes y^*_i \otimes w^*_{j_1} \otimes \cdots \otimes w^*_{j_p})$$

$$(h_j . w_{j_p} \otimes \Lambda_{(1)} . y \otimes \Lambda_{(2)} . t \otimes \Lambda_{(3)} . y_i \otimes \Lambda_{(4)} . w_{j_1} \otimes \cdots \otimes \Lambda_{(p+2)} . w_{j_{p-1}})$$

In this expression, we can carry out the summation over i, in which case it becomes

$$\sum_{j_1,\dots,j_p=1}^{\dim} \sum_j \varphi_j(\;_{(p+3)})(\mathrm{id}_{V^{m}} \; w_{j_1} \; \dots \; w_{j_p})$$
$$(h_j . w_{j_p} \;_{(2)} . t \;_{(3)} \;_{(1)} . y \;_{(4)} . w_{j_1} \; \dots \;_{(p+2)} . w_{j_{p-1}})$$

Next, we carry out the summation over j_p to get

$$\sum_{j_1,\dots,j_{p-1}=1}^{\dim} \sum_j \varphi_j(\;_{(p+3)})(\mathrm{id}_{V^{m}} \; w_{j_1} \; \dots \; w_{j_{p-1}})$$
$$(h_j \;_{(p+2)} . w_{j_{p-1}} \;_{(2)} . t \;_{(3)} \;_{(1)} . y \;_{(4)} . w_{j_1} \; \dots \;_{(p+1)} . w_{j_{p-2}})$$

Continuing to carry out the summations up to j_2, this becomes

$$\sum_{j_1=1}^{\dim} \sum_j \varphi_j(\;_{(p+3)})(\mathrm{id}_{V^{m}} \; w_{j_1})(h_j(\;_{(p+2)} \;_{(4)}) . w_{j_1} \;_{(2)} . t \;_{(3)} \;_{(1)} . y)$$

We can even carry out the summation over j_1 to get

$$\sum_j \varphi_j(\;_{(p+3)}) h_j(\;_{(p+2)} \;_{(4)}) . (\;_{(2)} . t \;_{(3)} \;_{(1)} . y)$$
$$= \sum_j \varphi_j(\;_{(p+2)}) h_j(\;_{(p+1)} \;_{(2)}) . (t \;_{(1)} . y) = g(y \; t)$$

It should be pointed out that this argument needs to be slightly modied in the case $p = 0$, where the summation over $j_1;\dots;j_p$ is empty. In fact, this implies that the computation simplies substantially in this case. Furthermore, the reader is urged to check that this argument also covers the case $m = 1$.

(5) Next, we establish the formula $I_V((m+1;l);z) = I_V((m;l);R^{-1}(z))$ in the case $m > 0$ and $l = 0$, in which it asserts that $\mathrm{tr}(\;_m(z)) = \mathrm{tr}(\;_m(R^{-1}(z)))$. For this, we show that z and $R^{-1}(z)$ have the same trace on every induced module, which corresponds in fact to the case $m = 1$. Now suppose that $z = \sum_j \varphi_j \; h_j \in Z(D)$, and that $\;_V$ is the character of V. We can write $\;_1(z)$ as before as a tensor product of right multiplications on H and an endomorphism of V and get that $\mathrm{tr}(\;_1(z)) = n \sum_j \varphi_j(\;) \;_V(h_j)$. Since

$$R^{-1}(z) = e^{-1}(z_{(1)}) z_{(2)} = \sum_j \varphi_{j(2)}(S(h_{j(1)})) \varphi_{j(1)} \; h_{j(2)}$$

this implies also that

$$\mathrm{tr}(\;_1(R^{-1}(z))) = n \sum_j \varphi_{j(2)}(S(h_{j(1)}))\varphi_{j(1)}(\;) \;_V(h_{j(2)})$$
$$= n \sum_j \varphi_j(\; S(h_{j(1)})) \;_V(h_{j(2)}) = n \sum_j \varphi_j(\;) \;_V(h_j) = \mathrm{tr}(\;_1(z))$$

as asserted.

(6) To establish the assertion $I_V((m+1,l),z) = I_V((m,l),R^{-1}(z))$ in the case $m=0$ and $l>0$, we argue similarly: We have

$$\begin{aligned} I_V((0,l),R^{-1}(z)) &= n \sum_j \varphi_{j(2)}(S(h_{j(1)}))\varepsilon(h_{j(2)})\varphi_{j(1)}(\Lambda_{(1)})\,\chi_{V\,1}(\Lambda_{(2)}) \\ &= n \sum_j \varphi_j(\Lambda_{(1)}S(h_j))\,\chi_{V\,1}(\Lambda_{(2)}) \end{aligned}$$

on the one hand and

$$\begin{aligned} I_V((1,l),z) = \operatorname{tr}(\rho_1(u_D^{-1}z)) &= n \sum_{i=1}^{n} \sum_j (\varphi_j b_i)(\Lambda)\,\chi_{V\,1}(b_i h_j) \\ &= n \sum_j \varphi_j(\Lambda_{(1)})\,\chi_{V\,1}(\Lambda_{(2)}h_j) \end{aligned}$$

on the other hand. Both expressions are equal by the basic Casimir properties of the integral.[108] A very similar reasoning establishes the formula in the case $m=0$ and $l=0$, and for $m=0$ and $l<0$ we have

$$\begin{aligned} I_V((1,l),z) &= I_V((-1,-l),S_D(z)) \\ &= I_V((0,-l),R^{-1}(S_D(z))) = I_V((0,l),R^{-1}(z)) \end{aligned}$$

because R and S_D commute.

(7) We have now established that $I_V((m+1,l),z) = I_V((m,l),R^{-1}(z))$ whenever $m \geq 0$ and $l \geq 0$. Instead of establishing the remaining cases, we use this fact to prove that $I_V((l,m),S(z)) = I_V((m,-l),z)$ if $m>0$ and $l \geq 0$. For this, we write $l = am + b$, where $a \geq 0$ and $0 \leq b < m$, and argue by induction on a. The induction beginning is the case $a=0$, in which we have $l = b < m$. We have seen in Paragraph 1.1 that $s = t^{-1}r^{-1}t^{-1}$, so that by the first step we get

$$\begin{aligned} I_V((l,m),S(z)) &= I_V((l,m),(T^{-1} \circ R^{-1} \circ T^{-1})(z)) \\ &= I_V((l,m-l),(R^{-1} \circ T^{-1})(z)) \end{aligned}$$

Because $m - l > 0$, we can apply the identity established above to rewrite this further as

$$I_V((l,m),S(z)) = I_V((m,m-l),T^{-1}(z)) = I_V((m,-l),z)$$

where we have applied the first step again.

For the induction step, note that it follows from the discussion in Paragraph 1.1 that $rs = st$. By the induction assumption, we have

$$I_V(((a-1)m+b,m),S(z)) = I_V((m,-(a-1)m-b),z)$$

which means that $I_V((am+b,m),R(S(z))) = I_V((m,-am-b),T(z))$. By the preceding commutation relation, this asserts that

$$I_V((l,m),S(T(z))) = I_V((m,-l),T(z))$$

so that the assertion now follows by substituting $T^{-1}(z)$ for z.

(8) Inspection of the preceding argument shows that it also proves the formula $I_V((l,m),S(z)) = I_V((m,-l),z)$ in the case $m = l = 0$. To establish it if $m \geq 0$ and $l > 0$, note that it asserts in this case that

$$I_V((l,m),S(z)) = I_V((-m,l),S_D(z))$$

Since $S_D(z) = S^{-2}(z)$, this is equivalent to $I_V((l,m),z) = I_V((-m,l),S(z))$, a fact that we have just established.

The proof that $I_V((l,m),S(z)) = I_V((m,-l),z)$ if $m \geq 0$ and $l < 0$ is similar: The assertion then is that

$$I_V((-l,-m),S_D(S(z))) = I_V((m,-l),z)$$

If we substitute $S(z)$ for z, this becomes $I_V((-l,-m),z) = I_V((m,-l),S(z))$, which we have obtained already.

Finally, if $m < 0$ and $l \geq 0$, the assertion is that

$$I_V((-l,-m),S_D(S(z))) = I_V((-m,l),S_D(z))$$

which upon substituting $S_D(z)$ for z also reduces to the established case. □

8.4 In our situation, the Drinfel'd element u_D has finite order.[109] This order is called the exponent of H; we denote it by N. It is known that N divides $\dim(H)^3$; however, the original conjecture of Y. Kashina, namely that N divides $\dim(H)$, is still open.[110]

We now consider the cyclotomic field $\mathbb{Q}_N \subset K$ that arises by adjoining to the prime field $\mathbb{Q} \subset K$ all N-th roots of unity that are contained in K. We denote by $Z_{\mathbb{Q}_N}(D)$ the span of the centrally primitive idempotents $e_1,\ldots,e_k$ introduced in Paragraph 5.1 over the subfield $\mathbb{Q}_N$ of K. This space has the following property:

Lemma $Z_{\mathbb{Q}_N}(D)$ is invariant under the action of the modular group.

Proof. It suffices to show that it is invariant under T and S. The fact that u_D has order N means for the expansion $u_D = \sum_{i=1}^k u_i e_i$ considered in Paragraph 5.2 that the coefficients u_i are N-th roots of unity. Since T is the multiplication by u_D^{-1}, we see that $Z_{\mathbb{Q}_N}(D)$ is invariant under T.

To see that $Z_{\mathbb{Q}_N}(D)$ is invariant under S, recall[111] that the entries s_{ij} of the Verlinde matrix are contained in $\mathbb{Q}_N$. Therefore, the assertion follows from the formula $S(e_j) = \frac{1}{\dim(H)} \sum_{i=1}^k \frac{n_j}{n_i} s_{j^* i} e_i$ established, taking Paragraph 6.1 into account, in Corollary 5.2. □

This lemma has the following consequence for the indicators:

Proposition For $z \in Z_{Q_N}(D)$, we have $I_V((m,l),z) \in Q_N$.

Proof. In the case $(m,l) = (0,0)$, it follows easily from the definition that $I_V((m,l),z)$ is the trace of the action of z on the induced module $\mathrm{Ind}(K)$ of the trivial module, which is in Q_N if $z \in Z_{Q_N}(D)$. If $(m,l) \neq (0,0)$, we set $t := \gcd(m,l) > 0$. By Corollary 1.2, we can find $g \in \Gamma$ such that $(m,l) = (t,0)g$. By Theorem 8.3, we then have

$$I_V((m,l),z) = I_V((t,0),g.z) = \mathrm{tr}(\rho_t(g.z))$$

which is in Q_N since $g.z \in Z_{Q_N}(D)$ by the preceding lemma. $\square$

We now consider the principal congruence subgroup $\Gamma(N)$ corresponding to the exponent N. The following orbit theorem asserts that the indicator depends only on the $\Gamma(N)$-orbit of the lattice point:

Theorem Suppose that two lattice points (m,l) and (m',l') are in the same $\Gamma(N)$-orbit. Then we have $I_V((m,l),z) = I_V((m',l'),z)$ for every H-module V and every $z \in Z(D)$.

Proof. (1) We fix an H-module V, and introduce an equivalence relation on the lattice $\mathbb{Z}^2$ by defining $(m,l) \sim (m',l')$ if and only if

$$I_V((m,l),z) = I_V((m',l'),z)$$

for all $z \in Z(D)$. Then $\sim$ is a congruence relation, since, for $g \in \Gamma$, $(m,l) \sim (m',l')$ implies in particular that $I_V((m,l),g.z) = I_V((m',l'),g.z)$, which yields $I_V((m,l)g,z) = I_V((m',l')g,z)$ by Theorem 8.3, so that $(m,l)g \sim (m',l')g$. Note that there is a slight adaption necessary: In Section 1, we have considered the left action of the modular group on the lattice points, considered as columns, whereas we consider here the transposed right action, where the lattice points are considered as rows.

(2) We now want to check that $\sim$ satisfies the two defining properties of the congruence relation listed in Paragraph 1.3. Although the transpose of t^N is r^{-N}, we can also work with t^N in the transposed situation, since t^N and r^N are conjugate and the inverse sign does not matter. For the first property, we therefore have to check that $(m,l) \sim (m,l)t^N$. But this is immediate, since we have $T^N(z) = u_D{}^N z = z$ and therefore

$$I_V((m,l)t^N,z) = I_V((m,l),T^N(z)) = I_V((m,l),z)$$

by Theorem 8.3.

(3) For the second property, we are given $q \in \mathbb{Z}$ that satisfies $q \equiv 1 \pmod{N}$ and $t := \gcd(m,l) = \gcd(m,ql)$, and have to establish that $(m,l) \sim (m,ql)$, in other words, that

$$I_V((m,l),z) = I_V((m,ql),z)$$

for all $z \in Z(D)$. We treat the case $m > 0$ first, where we also have $t > 0$. It is sufficient to establish this in the case where $z = e_i$ is a centrally primitive idempotent.

If we write $m = tm'$, $l = tl'$, we have that q is relatively prime to m'. Consider the cyclotomic field $\mathbb{Q}_{Nm'} \subset K$. Because q is relatively prime to Nm', there is a unique automorphism $\sigma_q \in \mathrm{Gal}(\mathbb{Q}_{Nm'}/\mathbb{Q})$ with the property that

$$\sigma_q(\zeta) = \zeta^q$$

for every Nm'-th root of unity ζ. Because $q \equiv 1 \pmod N$, we have $\sigma_q(\zeta) = \zeta$ if ζ is an N-th root of unity, and therefore even $\sigma_q \in \mathrm{Gal}(\mathbb{Q}_{Nm'}/\mathbb{Q}_N)$. By the preceding proposition, this means that $\sigma_q(I_V((m,l),z)) = I_V((m,l),z)$. On the other hand, we have by definition that $I_V((m,l),z) = \mathrm{tr}(\theta^{-l} \circ \rho_m(z))$, where $\theta = \theta_{V,V^{\otimes(m-1)}}$, properly understood in the case $m = 1$. Now we have

$$(\theta^{-l})^{m'} = \theta^{-tl'm'} = (\theta^{-m})^{l'} = \rho_m(u_D^{-1})^{l'}$$

so that $(\theta^{-l})^{m'N} = \mathrm{id}_{\mathrm{Ind}(V^{\otimes m})}$. Since $z = e_i$, $\rho_m(z)$ is the projection to the isotypical component of V_i in $\mathrm{Ind}(V^{\otimes m})$, so that $\theta^{-l} \circ \rho_m(z)$ coincides with θ^{-l} on this isotypical component and vanishes on the other isotypical components. In particular, the eigenvalues of $\theta^{-l} \circ \rho_m(z)$ are Nm'-th roots of unity, and the eigenvalues of its q-th power $\theta^{-lq} \circ \rho_m(z)$ are the q-th powers of its eigenvalues, so that for the trace we get the formula

$$I_V((m,lq),z) = \mathrm{tr}(\theta^{-lq} \circ \rho_m(z)) = \sigma_q(\mathrm{tr}(\theta^{-l} \circ \rho_m(z))) = \sigma_q(I_V((m,l),z))$$

Combining this with our earlier observation, this establishes the assertion in the case $m > 0$.

(4) The case $m < 0$ reduces immediately to the case just treated, since

$$I_V((m,l),z) = I_V((-m,-l),S_D(z)) = I_V((-m,-ql),S_D(z)) = I_V((m,ql),z)$$

Now suppose that $m = 0$. If also $l = 0$, the assertion is obvious, so that we can assume that $l \neq 0$. In this case, the conditions that $q \equiv 1 \pmod N$ and $\gcd(m,l) = \gcd(m,ql)$ imply that $ql = \pm l$, so that $q = \pm 1$. The case $q = 1$ is obvious, so that we now assume that $q = -1$, which can only happen if $N = 1$ or $N = 2$. A Hopf algebra of exponent 1 is one-dimensional, and for a Hopf algebra of exponent 2 we have $h = h_{(1)}h_{(2)}S(h_{(3)}) = S(h)$, so that the antipode of H is the identity. Then the antipode of H^* is also the identity, so that H is commutative and cocommutative, which implies that D is commutative and cocommutative,[112] so that its antipode is again the identity. We therefore have

$$I_V((0,-l),z) = I_V((0,l),S_D(z)) = I_V((0,l),z)$$

in the case $N = 1$ as well as in the case $N = 2$, and the second defining property is completely established.

(5) In Paragraph 1.3, we have defined the relation $\sim$ as the intersection of all congruence relations that satisfy the two defining properties just verified. Therefore $(m,l) \equiv (m',l')$ implies that $(m,l) \sim (m',l')$. But by Theorem 1.3, $(m,l) \equiv (m',l')$ means that (m,l) and (m',l') are in the same $\Gamma(N)$-orbit, so that this is exactly the assertion. $\square$

We put down one easy special case of this theorem that will be needed later:

Corollary For an H-module V, let χ be the character of $\mathrm{Ind}(V)$. Then we have $\chi(g.z) = \chi(z)$ for all $g \in \Gamma(N)$ and all $z \in Z(D)$.

Proof. We have $\chi(z) = \mathrm{tr}(\rho_1(z)) = I_V((1,0),z)$, so that by Theorem 8.3 the assertion is equivalent to $I_V((1,0)g,z) = I_V((1,0),z)$. But since $(1,0)$ and $(1,0)g$ are obviously in the same $\Gamma(N)$-orbit, this follows directly from the preceding theorem. $\square$

9 The congruence subgroup theorem

9.1 We now will apply the results of Section 8 to prove that the kernel of the projective representation of the modular group on the center of a semisimple factorizable Hopf algebra is a congruence subgroup. Note that the kernel of a group homomorphism consists of those elements that are mapped to the unit element, which in the projective linear group consists of all nonzero scalar multiples of the identity. If therefore a projective representation is induced from an ordinary linear representation, the kernel of the projective representation is in general larger than the kernel of the linear representation.

So, let A be a semisimple factorizable Hopf algebra over our algebraically closed base field K of characteristic zero. The exponent of A will be denoted by N. Otherwise, we will use the notation introduced in Section 5; in particular, we will use the inverse Drinfel'd element u^{-1} as our ribbon element. However, the whole discussion in Section 5 depended on a parameter ζ that was introduced in Paragraph 5.2; we will now dispose of this parameter in the following intricate way: If $\chi_R(u) = \chi_R(u^{-1})$, in which case, as discussed in Paragraph 4.3, our representation is linear, we set $\zeta = \frac{1}{\chi_R(u)}$, so that our integral $\rho \in A^*$ satisfies $\rho(u) = \rho(u^{-1}) = 1$. By Lemma 4.3, this integral also satisfies $(\rho \otimes \rho)(R'R) = 1$. Note that in the case where $A = D(H)$ is the Drinfel'd double of a semisimple Hopf algebra H, we therefore pick here the integral ρ_D from Paragraph 6.1.

If $\chi_R(u) \neq \chi_R(u^{-1})$, in which case our representation is not linear, we choose ζ so that $\zeta^2 = \frac{1}{\dim(A)}$. This obviously only determines ζ up to a sign, but in view of the formula $\chi_R(u)\chi_R(u^{-1}) = \dim(A)$ observed in Paragraph 5.3, implies that $(\rho \otimes \rho)(R'R) = \rho(u)\rho(u^{-1}) = 1$. In particular, the choice of ρ in both cases is compatible, the only difference is that in the first, linear case even the sign of ζ is determined. In any case, this choice of ρ is the one that makes Φ equivariant, as explained in Paragraph 4.5, as it is compatible with the condition that $\rho_D = \Phi(\rho \otimes \rho)$.

Next, we discuss the dual of our projective representation. We denote the morphism that a linear map f induces between the corresponding projective spaces by $P(f)$. By considering the character ring as dual to the center, we can dualize the projective representation of the modular group on the center to a projective representation of the modular group on the character ring as follows: If the group element $g \in SL(2,\mathbb{Z})$ is represented by the equivalence class $P(f) \in PGL(Z(A))$, consider for $\chi \in Ch(A)$ the character $\chi' \in Ch(A)$ that satisfies

$$\chi'(z) = \chi(f^{-1}(z))$$

for all $z \in Z(A)$, and set $g.\chi := \chi'$. This does not depend on the choice of the representative f and gives a projective representation of $SL(2,\mathbb{Z})$ on $P(Ch(A))$.

This construction raises the question whether the isomorphism $P(\Phi)$ that Φ induces between the projective spaces of the center and the character ring is equivariant with respect to the corresponding actions. This is the case only after the action on the center is modified with the help of the automorphism introduced in Definition 1.1:

Proposition For all $g \in$, the diagram

$$\begin{tikzcd}[column sep=huge, row sep=large]
P(Ch(A)) \arrow[r, "\mapsto g."] & P(Ch(A)) \\
P(Z(A)) \arrow[u, "P(\ )"] \arrow[r, "z \mapsto \tilde{g}.z"'] & P(Z(A)) \arrow[u, "P(\ )"']
\end{tikzcd}$$

commutes.

Proof. It suffices to check this for the generators s and t, for which we have seen in Paragraph 1.1 that $\tilde{s} = s^{1}$ and $\tilde{t} = t^{1}$. In the case of s, the assertion therefore follows from Proposition 4.1, and in the case of t it follows from the corresponding diagram given in Paragraph 4.3. $\square$

The analogous question for P( ) can be deduced from this proposition:

Corollary For all $g \in$, the diagram

$$\begin{tikzcd}[column sep=huge, row sep=large]
P(Ch(A)) \arrow[r, "\mapsto g."] \arrow[d, "P(\ )"'] & P(Ch(A)) \arrow[d, "P(\ )"] \\
P(Z(A)) \arrow[r, "z \mapsto (s\tilde{g}s^{1}).z"'] & P(Z(A))
\end{tikzcd}$$

commutes.

Proof. This will follow from the preceding proposition by reversing the vertical arrows if we can verify that $S \quad = \quad {}^{1}$ on the character ring, or equivalently that $\quad = S^{1}$. But as and agree on the character ring, we have from the definition of that $\quad = S \quad S$ on the center, which in view of Corollary 4.2 implies the assertion. $\square$

Note that in the case where we have a linear representation of $SL(2;\mathbb{Z})$ on the center $Z(A)$, we will also get in this way a linear representation on $Ch(A)$, and and will then be equivariant with respect to the linear representations.

9.2 If $\;\in A$ is an integral which satisfies $\varepsilon(\;) = 1$, we define the bilinear form $\langle\;,\;\rangle$ on $Ch(A)$ by the equation

$$\langle\;,\;{}^0\rangle := (\;S(\;{}^0))(\;)$$

Then we have $\langle\;_i,\;_j\rangle = \;_{ij} = \dim \mathrm{Hom}_A(V_i,V_j)$ for the irreducible characters,[113] which shows that this bilinear form is nondegenerate and symmetric.

For $l = 1,\ldots,k$, we denote the character of the induced $D(A)$-module $\mathrm{Ind}(V_l)$ by $\;_l$. Using this, we can express this bilinear form as follows:

Proposition For all $\;,\;{}^0 \in Ch(A)$, we have

$$\langle\;\;{}^0,\;_l\rangle = \frac{1}{\dim(A)}\;_l(\;{}^{1}(\;{}^{1}(\;)\;\;{}^{1}(\;{}^0)))$$

Proof. Because both sides of the equation are bilinear in $\;$ and $\;{}^0$, we can assume that both characters are irreducible, so that $\;=\;_i$ and $\;{}^0 = \;_j$ for some $i,j\;\;k$. The vector space $V_i\;\;V_j$ can be considered as an $A\;\;A$-module by the componentwise action; it is then simple. We can turn it into a $D(A)$-module by pullback along $\;$. We denote this $D(A)$-module by U; since $\;$ is an isomorphism, this module is also simple, and the centrally primitive idempotent in $Z(D(A))$ corresponding to U is $\;{}^{1}(e_i\;\;e_j)$. Because $\;(\varepsilon\;\;a) = \;(a)$, the restriction of U to $A\;\;D(A)$ is the same as the pullback of the $A\;\;A$-module structure along $\;$, which is exactly how the tensor product $V_i\;\;V_j$ of A-modules is formed.

We now have by the Frobenius reciprocity theorem[114] that

$$\begin{aligned}\langle\;_i\;_j,\;_l\rangle &= \dim \mathrm{Hom}_A(V_l,V_i\;\;V_j) = \dim \mathrm{Hom}_{D(A)}(\mathrm{Ind}(V_l),U)\\ &= \dim \mathrm{Hom}_{D(A)}(U,\mathrm{Ind}(V_l)) = \frac{1}{n_in_j}\;_l(\;{}^{1}(e_i\;\;e_j))\end{aligned}$$

By Proposition 5.2, we have $\;(e_i) = \;n_i\;_i$, so that

$$\frac{e_i}{n_i} = \;\;{}^{1}(\;_i)$$

Inserting this into the preceding formula and using $\;{}^2 = \frac{1}{\dim(A)}$, we get the assertion. $\Box$

This proposition has the following consequence:

Corollary Suppose that $\;_R(u) = \;_R(u^{-1})$. Then we have

$$(g:\;)(g:\;{}^0) = \;\;{}^0$$

for all $g \in \;(N)$ and all $\;,\;{}^0 \in Ch(A)$.

Proof. Recall that the assumption implies that the representation of the modular group is linear. By the nondegeneracy of the bilinear form above, it su ces to show that $h(g:)(g: {}^0);\ {}_l i = h\ \ {}^0;\ {}_l i$ for all $l = 1;:::;k$. Now we get from the preceding proposition for $g \in (N)$ that

$$
\begin{aligned}
h(g:)(g: {}^0);\ {}_l i &= \frac{1}{\dim(A)}\ {}_l(\ \ {}^1(\ {}^1(g:)\qquad {}^1(g: {}^0))) \\
&= \frac{1}{\dim(A)}\ {}_l(\ \ {}^1(g: \ {}^1(\ )\quad g: \ {}^1(\ {}^0))) \\
&= \frac{1}{\dim(A)}\ {}_l(g: \ \ {}^1(\ {}^1(\ )\qquad {}^1(\ {}^0))) \\
&= \frac{1}{\dim(A)}\ {}_l(\ \ {}^1(\ {}^1(\ )\qquad {}^1(\ {}^0))) = h\ \ {}^0;\ {}_l i
\end{aligned}
$$

where the second equality follows from Proposition 9.1, the third from Proposition 4.5, and the fourth from Corollary 8.4.2

9.3 We now turn for a moment to the special case where $A = D(H)$, the Drinfel'd double of a semisimple Hopf algebra H, which is denoted by D to distinguish it from the general case. Note that H and D have the same exponent N.[115] In this case, we now prove the following congruence subgroup theorem:

Theorem The kernel of the representation of the modular group on the center of D is a congruence subgroup of level N.

Proof. It follows from Corollary 8.4 that the character of every D-module that is induced from an H-module is invariant under (N). The regular representation of D is induced from the regular representation of H, and therefore its character is invariant under (N). This now implies that the counit is also invariant under (N). To see this, recall that Corollary 5.2 gives in particular that $S\ (p_1) = \frac{1}{\dim(H)}\ {}_1$, which means that $S\ (\ {}_R) = \dim(H)"_D$. In view of Proposition 4.1, this in turn says that $s^{\ 1}: {}_R = \dim(H)"_D$. For an element $g \in (N)$, this gives

$$
g:"_D = \frac{1}{\dim(H)} gs^{\ 1}: {}_R = \frac{1}{\dim(H)} s^{\ 1}(sgs^{\ 1}): {}_R = \frac{1}{\dim(H)} s^{\ 1}: {}_R = "_D
$$

since (N) is a normal subgroup.

If we now substitute $"_D$ for ^{0} in Corollary 9.2, we get that $g: =$ for every character of D and every $g \in (N)$, and since conjugation by a restricts to an automorphism of (N), we see that every character is invariant under (N). But considering how we de ned this action in Paragraph 9.1, this implies that every central element is invariant under (N), since the pairing between the character ring and the center is nondegenerate. In other words, the kernel of the representation contains (N), and therefore is a congruence subgroup.

It remains to be proved that the level of the kernel is exactly N. But if there were some $N' < N$ with the property that (N') would also be contained in the kernel, this would in particular imply that $t^{N'}$ acts trivially on the center, which would mean that $u_D^{N'} = 1$. But as N is by definition the order of u_D, this cannot be the case. □

9.4 Returning to the general case of an arbitrary factorizable semisimple Hopf algebra A, in which the action of the modular group in general is only projective, we can still look at the kernel of the corresponding group homomorphism to $PGL(Z(A))$. For this kernel, the following analogue of Theorem 9.3 holds:

Theorem The kernel of the projective representation of the modular group on the center of A is a congruence subgroup of level N.

Proof. To show that (N) is contained in the kernel, suppose that this is not the case, and choose $g \in (N)$ that is not mapped to the identity in $PGL(Z(A))$. Choose a representative $f \in GL(Z(A))$ for the action of g, and also a representative $\tilde{f}$ for the action of $\tilde{g}$. Because f is not a scalar multiple of the identity, there exists an element $z \in Z(A)$ such that z and $f(z)$ are not proportional, and therefore linearly independent. This implies that $z \quad z$ and $f(z) \quad \tilde{f}(z)$ are not proportional. But we saw in Paragraph 4.5 that the tensor product of our projective representation with its conjugate under a is induced by a linear representation, and that this linear representation is via isomorphic to the representation on $Z(D(A))$, on which g acts trivially by Theorem 9.3. But this means that it acts trivially on $z \quad z$, too, contradicting the fact that $z \quad z$ and $f(z) \quad \tilde{f}(z)$ are not proportional.

As in the proof of Theorem 9.3, it remains to be proved that the level of the kernel is exactly N. Now if there were some $N' < N$ with the property that (N') would also be contained in the kernel, this would in this case only imply that $u_D^{N'}$ acts on the center by multiplication by a scalar. But as u_D always preserves the integral, this scalar has to be 1, which contradicts the definition of N as in the previous case. □

10 The action of the Galois group

10.1 In this section, we will introduce an action of the Galois group of the cyclotomic field determined by the exponent that will turn out to be intimately connected to the action of the modular group. As in Section 9, we consider a semisimple factorizable Hopf algebra A over our algebraically closed base field K of characteristic zero. The exponent of A will be denoted by N. Otherwise, we will use the notation introduced in Section 5; in particular, we will use the inverse Drinfel'd element u^{-1} as our ribbon element. The constant ζ, which determines the normalization of the integral Λ, is chosen as in Paragraph 9.1, and ρ is defined using this integral Λ.

In Paragraph 5.1, we have constructed the algebra homomorphisms $\omega_1, \ldots, \omega_k$ from the character ring to the center. If we denote by $Ch_{\mathbb{Q}}(A)$ the span of the irreducible characters $\chi_1, \ldots, \chi_k$ not over K, but over the rational numbers $\mathbb{Q} \subset K$, it can be shown[116] as in the case of the Drinfel'd double that the images $\omega_i(Ch_{\mathbb{Q}}(A))$ are contained in the cyclotomic field $\mathbb{Q}_N$ determined by the exponent. The restriction of ω_i to $Ch_{\mathbb{Q}}(A)$ is a $\mathbb{Q}$-algebra homomorphism to $\mathbb{Q}_N$, and clearly ω_i is uniquely determined by this restriction. For $\sigma \in Gal(\mathbb{Q}_N/\mathbb{Q})$, the map $\sigma \circ \omega_i$ is again a $\mathbb{Q}$-algebra homomorphism from $Ch_{\mathbb{Q}}(A)$ to $\mathbb{Q}_N$, which must coincide with one of the restrictions of $\omega_1, \ldots, \omega_k$. In this way, we get an action of $Gal(\mathbb{Q}_N/\mathbb{Q})$ on the set $\{1, \ldots, k\}$ so that

$$\sigma \circ \omega_i|_{Ch_{\mathbb{Q}}(A)} = \omega_{\sigma.i}|_{Ch_{\mathbb{Q}}(A)}$$

From this permutation representation, we get an action of the Galois group on the character ring $Ch(A)$ over the full base field K by permuting the characters accordingly, in the sense that

$$\sigma.\chi_i := \chi_{\sigma.i}$$

and extending this action K-linearly.

The following lemma lists some basic properties of this action:

Lemma

1. $n_{\sigma.i} = n_i$
2. $\sigma(s_{ij}) = s_{\sigma.i,j} = s_{i,\sigma^{-1}.j}$
3. $\sigma.\chi_1 = \chi_1$

Proof. For the first assertion, recall the formula $\omega_i(\Lambda_A) = \frac{\dim(A)}{n_i^2}$ established in Corollary 5.3. Using this, we get

$$\frac{\dim(A)}{n_{\sigma.i}^2} = \omega_{\sigma.i}(\Lambda_A) = \sigma(\omega_i(\Lambda_A)) = \sigma(\frac{\dim(A)}{n_i^2}) = \frac{\dim(A)}{n_i^2}$$

from which the first assertion is immediate.

For the second assertion, recall the formula $s_{ij} = n_i \, {}_i({}_j)$ from Lemma 5.2, from which we get

$$(s_{ij}) = n_i \; ({}_i({}_j)) = n_{:i} \; {}_{:i}({}_j) = s_{:i;j}$$

Furthermore, we observed in Lemma 5.2 that the Verlinde matrix is symmetric, from which we see that $(s_{ij}) = (s_{ji}) = s_{:j;i} = s_{i;:j}$.

For the third assertion, note that we have

$${}_1({}_i) = !_1(({}_i)) = "(({}_i)) = n_i$$

so that $({}_1({}_i)) = {}_1({}_i)$. This implies $:1 = 1$. 2

The action on the character ring can also be viewed in a different way: $Ch_Q(A)$ is a commutative semisimple Q-algebra, and therefore by Wedderburn's theorem[117] isomorphic to a direct sum of fields. As in the case of the Drinfel'd double,[118] it can be shown that these fields are subfields of the cyclotomic field Q_N. Since the Galois group of Q_N is abelian, every subfield of the cyclotomic field is normal, and therefore preserved by the action of the Galois group of Q_N. We therefore get an action of this Galois group on $Ch_Q(A)$ as the sum of the actions on the Wedderburn components. The action of the Galois group constructed above is exactly the K-linear extension of this action to $Ch(A) = Ch_Q(A) \; {}_Q K$. To see this, note that the restrictions of ${}_1; \ldots; {}_k$ to $Ch_Q(A)$ arise by projecting to some Wedderburn component and then embedding it into $Q_N \; K$. Because the Galois group is abelian, it does not matter whether we first act on the Wedderburn component and then embed into Q_N, or first embed and then act. In other words, the action on the Wedderburn components satisfies

$${}_i(: {}_j) = ({}_i({}_j))$$

for all $2 \; Gal(Q_N = Q)$. But on the other hand it follows from the preceding lemma that we have ${}_i(\; {}_{:j}) = ({}_i({}_j))$, so that the action constructed before also satisfies this equation, which means that the two actions have to coincide.

If we consider the cyclotomic field Q_N as a subfield of the complex numbers, complex conjugation restricts to an automorphism of the cyclotomic field, which we denote by $2 \; Gal(Q_N = Q)$. It does not depend on the way how the cyclotomic field is embedded into the complex numbers, as it can be characterized by the property that it maps any N-th root of unity to its inverse. As proved in several places in the literature,[119] it acts on $Ch(A)$ via the antipode:

Proposition For all $2 \; Ch(A)$, we have $: = S( )$.

Stated differently, this asserts that $:i = i$, which in particular implies that $:(i) = (:i)$ for all $2 \; Gal(Q_N = Q)$, as the Galois group $Gal(Q_N = Q)$ is abelian. Using this, we can deduce further properties of our action:

Corollary

1. $\dot{p}_i = p_{\ ^{1}:i}$

2. $S(\ (\ )) = \ ^{1}(S(\ ))$

Proof. By Proposition 5.1 and Corollary 5.3, we have

$$p_i = \frac{n_i^2}{\dim(A)} \sum_{j=1}^{k} {}_i(\ _j)\ _j$$

Using the facts just proved, we therefore get

$$\dot{p}_i = \frac{n_i^2}{\dim(A)} \sum_{j=1}^{k} {}_i(\ _j)\ _{:j} = \frac{n_i^2}{\dim(A)} \sum_{j=1}^{k} {}_i(\ ^{1}{:j})\ _j$$
$$= \frac{n^2_{\ ^{1}:i}}{\dim(A)} \sum_{j=1}^{k} {}_{\ ^{1}:i}(\ _j)\ _j = p_{\ ^{1}:i}$$

which is the rst assertion.

It su ces to check the second assertion on a basis, so that we can assume that $= \ _j$. We then have by Corollary 5.2 that

$$S(\ (\ _j)) = S(\ _{:j}) = n_{:j}\ _{:j}(\ _A))p_{:j}$$
$$= n_j\ _j(\ _A))\ ^{1}\dot{p}_j = \ ^{1}(S(\ _j))$$

by the rst assertion and the proof of the preceding lemma. 2

This corollary shows in particular that the Galois group permutes the idempotents, which means that it acts via algebra automorphisms. This fact, however, is also obvious from the second description via the Wedderburn decomposition that we gave above.

10.2 Besides the spaces $Ch(A)$ and $Ch_Q(A)$ that we have considered above, we need to consider a third space that lies in between, namely the space $Ch_{Q_N}(A)$, which we de ne to be the span of the irreducible characters with coe cients in the cyclotomic eld Q_N. From the form of the base change matrix between the irreducible characters and the primitive idempotents of the character ring given in Proposition 5.1, we see that we could alternatively have de ned it as the span of $p_1;:::;p_k$ over the cyclotomic eld Q_N. If we therefore, as in Paragraph 8.4, denote by $Z_{Q_N}(A)$ the span of the centrally primitive idempotents $e_1;:::;e_k$ with coe cients in the cyclotomic eld, we have that $(Ch_{Q_N}(A)) = Z_{Q_N}(A)$.

We use these two di erent bases of the space to de ne two semilinear actions of the Galois group on $Ch_{Q_N}(A)$ as follows:

Definition For $\in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, we define automorphisms $(\ )$ and ${}^0(\ )$ of $\mathrm{Ch}_{\mathbb{Q}_N}(A)$ by

$$(\ )(\sum_{i=1}^{k} {}_i\ {}_i) := \sum_{i=1}^{k} (\ {}_i)\ {}_i \qquad {}^0(\ )(\sum_{i=1}^{k} {}_i p_i) := \sum_{i=1}^{k} (\ {}_i) p_i$$

In other words, $(\ )$ acts on the coefficients in an expansion in terms of the irreducible characters, and ${}^0(\ )$ acts on the coefficients in an expansion in terms of the primitive idempotents. Both of the automorphisms are semilinear in the sense that

$$(\ )(\ \ ) = (\ )\ (\ )(\ ) \qquad {}^0(\ )(\ \ ) = (\ )\ {}^0(\ )(\ )$$

for $\in \mathbb{Q}_N$ and $\in \mathrm{Ch}_{\mathbb{Q}_N}(A)$. Moreover, we have $(\ )(\ {}_i) = \ {}_i$ as well as ${}^0(\ )(p_i) = p_i$ for all $i = 1;:::;k$.

The connection with the action of the Galois group considered in Paragraph 10.1 is given by the following formula:

Proposition For all $\in \mathrm{Ch}_{\mathbb{Q}_N}(A)$, we have

$$: = (\ {}^0(\ )\ \ (\ )^{-1})(\ )$$

Moreover, $(\ )$ and ${}^0(\ )$ commute for all $;\ \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$. If ${}_R(u)$ is rational, we have furthermore that ${}^0(\ ) = S\ \ (\ )\ S^{-1}$.

Proof. For the first assertion, note that ${}^0(\ )\ \ (\ )^{-1}$ is actually $\mathbb{Q}_N$-linear, so that it suffices to prove that $:\ {}_i = (\ {}^0(\ )\ \ (\ )^{-1})(\ {}_i)$. But we have

$$(\ {}^0(\ )\ \ (\ )^{-1})(\ {}_i) = {}^0(\ )(\ {}_i) = {}^0(\ )(\sum_{j=1}^{k} {}_j(\ {}_i)p_j)$$
$$= \sum_{j=1}^{k} (\ {}_j(\ {}_i))p_j = \sum_{j=1}^{k} {}_j(\ {}_{:i})p_j = {}_{:i} = :\ {}_i$$

by Lemma 10.1 and the discussion in Paragraph 5.1.

For the commutativity assertion, note that $(\ )$ obviously commutes with the action of , because the action of is linear and permutes the characters. Also, it clearly commutes with $(\ )$, and therefore also with ${}^0(\ )$ by the result just proved.

For the third assertion, note that the assumption that ${}_R(u)$ is rational implies that ${}_R(u) = (\ {}_R(u)) = {}_R(u^{-1})$, so that by our convention also $= 1 = {}_R(u)$ is rational. To prove that ${}^0(\ )\ \ S = S\ \ (\ )$, we also use that both sides are semilinear, so that it again suffices to check that both sides give the same result on $_i$. But here we have by Corollary 5.2 that

$$^0(\ )(S\ (\ _i)) = \ ^0(\ )(\ n_i\ _i(\ _A)p_i) = \ n_i\ _i(\ _A)p_i = S\ (\ _i) = S\ (\ \ (\ )(\ _i))$$

which implies the assertion. 2

We give a second proof of the fact that $\ :=(\ ^0(\ )\ \ (\ )^{1})(\ )$ from the point of view of the second construction of the action via the Wedderburn decomposition of the character ring, discussed after Lemma 10.1. From Proposition 5.1, we know that the primitive idempotents p_i are already contained in $Ch_{Q_N}(A)$. As we discussed above, a simple ideal of $Ch_Q(A)$ is isomorphic to a subfield L of the cyclotomic field Q_N, and the action on the character ring restricts on these Wedderburn components to the action of the Galois group. In other words, with respect to the isomorphism $Ch_{Q_N}(A) = Ch_Q(A)\ _Q\ Q_N$, we have

$$:(\ \ \ ) = \ (\ )\ \ \ \ \ \ \ \ \ \ (\ )(\ \ \ ) = \ \ \ (\ )$$

for $\ 2\ L$ and $\ 2\ Q_N$. This shows that the formula that we have to prove is $^0(\ )(\ \ \ ) = \ (\ )\ \ (\ )$.

Because L is a Galois extension of the rationals, the map

$$L\ _Q\ Q_N\ !\ Q_N^{Gal(L=Q)};\ \ \ \ \ \ 7\ (\ (\ )\ )_{2\,Gal(L=Q)}$$

is an algebra isomorphism,[120] where the right-hand side is an algebra with respect to componentwise multiplication. Therefore, for every $\ 2\ Gal(Q_N=Q)$ there is a unique element $\sum_j l_j\ \ _j$ such that $\sum_j\ (l_j)\ _j = \ _;$, corresponding to a primitive idempotent of $Q_N^{Gal(L=Q)}$. Because of its uniqueness, we have

$$\sum_j\ (l_j)\ \ (\ _j) = \sum_j l_j\ \ _j$$

for all $\ 2\ Gal(Q_N=Q)$. But this shows that the endomorphism $\ 7\ \ (\ )(\ :\ )$ of $Ch_{Q_N}(A)$ is a semilinear map that preserves primitive idempotents, which is the defining property of $^0(\ )$, establishing the assertion.

10.3 As we have $(Ch(A)) = Z(A)$, we can use to transfer the action of the Galois group on the character ring to an action on the center. In other words, we define an action of $Gal(Q_N=Q)$ on $Z(A)$ by requiring that the diagram

$$\begin{tikzcd}
Ch(A) \arrow[r, "7\ \ :"] \arrow[d] & Ch(A) \arrow[d] \\
Z(A) \arrow[r, "z\ 7\ \ :z"'] & Z(A)
\end{tikzcd}$$

is commutative. With respect to a smaller base field, we can also define representations $\ :\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q}) \to GL(Z_{\mathbb{Q}_N}(A))$ and $\ ^0 : \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q}) \to GL(Z_{\mathbb{Q}_N}(A))$ by requiring that the diagrams

$$
\begin{tikzcd}
\mathrm{Ch}_{\mathbb{Q}_N}(A) \arrow[r, "(\ )"] \arrow[d] & \mathrm{Ch}_{\mathbb{Q}_N}(A) \arrow[d] \\
Z_{\mathbb{Q}_N}(A) \arrow[r, "(\ )"'] & Z_{\mathbb{Q}_N}(A)
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathrm{Ch}_{\mathbb{Q}_N}(A) \arrow[r, "{}^0(\ )"] \arrow[d] & \mathrm{Ch}_{\mathbb{Q}_N}(A) \arrow[d] \\
Z_{\mathbb{Q}_N}(A) \arrow[r, "{}^0(\ )"'] & Z_{\mathbb{Q}_N}(A)
\end{tikzcd}
$$

commute. It is then a direct consequence of Proposition 10.2 that

$$ .z = (\ ^0(\ )\ \ (\ )^{1})(z) $$

Furthermore, $(\ )$ and $^0(\ )$ commute for all $\ ;\ \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, and if $_R(u)$ is rational, we get from Proposition 4.1 that $^0(\ ) = S\ \ (\ )\ S^{1}$. We can also deduce immediately from Proposition 5.2, Corollary 10.1, and the equation $(p_i) = e_i$ that we have

$$ .z_i = z_{\ .i} \qquad .e_i = e_{\ 1.i} $$

Similarly, we have for the semilinear representations that

$$ (\ )(\sum_{i=1}^{k}\ _i z_i) = \sum_{i=1}^{k} (\ _i) z_i \qquad {}^0(\ )(\sum_{i=1}^{k}\ _i e_i) = \sum_{i=1}^{k} (\ _i) e_i $$

for $\ _i \in \mathbb{Q}_N$.

Let us list some basic properties of this action:

Proposition For $\ \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, $\ \in \mathrm{Ch}(A)$, and $z \in Z(A)$, we have

1. $(\ .z) = \ ^1 : (z)$
2. $(\ .z) = (\ :\ )(z)$
3. $S(\ .z) = \ ^1 .S(z)$

Proof. For the first assertion, we have by Proposition 5.2 and Lemma 10.1 that

$$ (\ .e_j) = (e_{\ 1.i}) = n_{\ 1.i}\ \ _{1.i} = n_i\ \ ^1 :\ _i = \ ^1 : (e_j) $$

For the second assertion, we can assume that $\ = \ _j$ and $z = z_i$. We then have by Lemma 5.2 and Lemma 10.1 that

$$ n_i\ _j(\ .z_i) = n_{\ .i}\ _j(z_{\ .i}) = n_{\ .i}\ \ _{.i}(\ _j) = s_{\ .i;j} $$
$$ = s_{i;\ .j} = n_i\ _i(\ \ _{.j}) = n_i\ \ _{.j}(z_i) $$

Alternatively, one can deduce this from the equation $\ _j(e_i) = n_i\ _{ij}$. The third assertion follows from Corollary 10.1 by applying and using Proposition 4.1.2

10.4 Our next goal is to investigate the equivariance properties of the action of the Galois group with respect to the isomorphism Φ introduced in Paragraph 3.1. If V_i and V_j are any two of our simple A-modules, $V_i \otimes V_j$ can be considered as an $A \otimes A$-module by the componentwise action. As Φ is an algebra isomorphism between $D(A)$ and $A \otimes A$, we can introduce a $D(A)$-module structure on $V_i \otimes V_j$ by pullback via Φ. We denote $V_i \otimes V_j$ by V_{ij} if endowed with this $D(A)$-module structure; note that this module was denoted by U in Paragraph 9.2. If χ_{ij} denotes the character of V_{ij}, we have $\chi_{ij} = \Phi^{*}(\chi_i \otimes \chi_j)$. Its degree is $n_{ij} = n_i n_j$, and the corresponding centrally primitive idempotent is $e_{ij} = \Phi^{-1}(e_i \otimes e_j)$.

As described in Paragraph 5.1, from χ_{ij} we can derive several additional quantities: the central characters

$$\omega_{ij} : Z(D(A)) \to K, \; z \mapsto \frac{1}{n_{ij}} \chi_{ij}(z)$$

the idempotents of the character ring $p_{ij} := \rho^{-1}(e_{ij})$, and the corresponding characters

$$\psi_{ij} : Ch(D(A)) \to K, \; \chi \mapsto \omega_{ij}(\rho(\chi))$$

which in turn are used to define the class sums $z_{ij} \in Z(D(A))$ via the requirement that $\chi(z_{ij}) = \psi_{ij}(\chi)$. The following proposition describes how these quantities compare to the corresponding quantities for A:

Proposition For $z \in Z(D(A))$ and $\chi, \chi' \in Ch(A)$, we have

1. $\omega_{ij}(z) = (\omega_i \otimes \omega_j)(\Phi(z))$
2. $p_{i,j} = \Phi^{*}(p_i \otimes p_j)$
3. $\psi_{i,j}(\Phi^{*}(\chi \otimes \chi')) = \psi_i(\chi)\psi_j(\chi')$
4. $z_{i,j} = \Phi^{-1}(z_i \otimes z_j)$

Proof. The first assertion follows directly from the definitions; however, it should be noted that Φ as an algebra isomorphism induces an isomorphism between the centers $Z(D(A))$ and $Z(A \otimes A) = Z(A) \otimes Z(A)$.[121] The second assertion is equivalent to the equation $\rho(p_{i,j}) = \Phi^{-1}(\rho(p_i \otimes p_j))$, which by Proposition 3.4 is equivalent to

$$e_{i,j} = \Phi^{-1}(\rho(p_i) \otimes S(\rho(p_j))) = \Phi^{-1}(e_i \otimes S(e_j))$$

which we have established above. Recall in this context that we have

$$Ch((A \otimes A)_F) = Ch(A \otimes A) = Ch(A) \otimes Ch(A)$$

by Lemma 3.4.

The third assertion follows from the second, because it suffices to check it in the case where $= p_m$ and $^0 = p_l$. But in view of the definition of the class sums, the third assertion can also be written as

$$(\quad ^0)(z_{i;j}) = (z_i) \; ^0(z_j)$$

which implies that $(z_{i;j}) = z_i \quad z_j$, which is the fourth assertion. 2

10.5 In Paragraph 10.1, we have defined the action of the Galois group by first requiring that $_{:i}(\ _j) = (\ _i(\ _j))$ and then defining it on $Ch(A)$ by setting $:\ _i = \quad _{:i}$ and extending linearly. This action is also defined in exactly the same way for $D(A)$; the only difference now is that we have indexed the corresponding quantities for $D(A)$ by pairs. In terms of these pairs, the first equation above reads $_{:(i;j)}(\ _{m\,l}) = (\ _{i;j}(\ _{m\,l}))$. But by Proposition 10.4, this can be rewritten as

$$\begin{aligned} _{:(i;j)}(\ _{m\,l}) &= (\ _{i;j}(\ _{m\,l})) = (\ _{i;j}(\ (\ _m \quad _l))) = (\ _i(\ _m)\ _j\ (\ _l)) \\ &= (\ _i(\ _m))\ (\ _j\ (\ _l)) = \ _{:i}(\ _m)\ \ _{:j}\ (\ _l) = \ _{(\ :i;\ :j)}(\ _{m\,l}) \end{aligned}$$

where we have used the fact that $:(j) = (\ :j)$ discussed after Proposition 10.1. This means that we have $:(i;j) = (\ :i;\ :j)$, which can be restated as follows:

Proposition The map

$$Ch(A) \quad Ch(A) ! \ Ch(D(A)); \qquad ^0 7 \quad (\quad ^0)$$

is $Gal(Q_N=Q)$-equivariant if $Ch(A) \quad Ch(A)$ is endowed with the diagonal action.

Proof. For $2\ Gal(Q_N=Q)$, we have

$$(\ :\ _i \quad :\ _j) = (\ _{:i} \quad _{:j}) = \ _{:i;\ :j} = \ _{:(i;j)} = \ :\ _{ij} = \ :\ (\ _i \quad _j)$$

As the characters $_i \quad _j$ form a basis of $Ch(A) \quad Ch(A)$, this is sufficient. 2

The preceding result can also be understood from the point of view of the Wedderburn decomposition of the character ring, as described after Lemma 10.1. As we pointed out there, the character rings $Ch_Q(A)$ as well as $Ch_Q(D(A))$ decompose into direct sums of subfields of the cyclotomic field Q_N, and the Galois group preserves the Wedderburn components and acts there via restriction to the corresponding subfield. Now is a Hopf algebra isomorphism between $D(A)$ and $(A \quad A)_F$, so that restricts to an isomorphism between the character rings and therefore maps Wedderburn components to Wedderburn components. By Lemma 3.4, we have $Ch_Q((A \quad A)_F) = Ch_Q(A \quad A)$, so that the assertion now will follow if we can justify that the isomorphism $Ch_Q(A \quad A) = Ch_Q(A) \quad Ch_Q(A)$ is equivariant with respect to the diagonal action on the right-hand side.

This now follows from an argument that is similar to the one used at the end of Paragraph 10.2. Let L and M be two subfields of $\mathbb{Q}_N$ that appear as Wedderburn components of $\mathrm{Ch}_{\mathbb{Q}}(A)$, and let P be a subfield of $\mathbb{Q}_N$ that appears as a Wedderburn component of $\mathrm{Ch}_{\mathbb{Q}}(A \otimes A)$. We then have a commutative diagram of the form

$$\begin{tikzcd} L \otimes M \arrow[rr, "f"] \arrow[d] & & P \\ \mathrm{Ch}_{\mathbb{Q}}(A) \otimes \mathrm{Ch}_{\mathbb{Q}}(A) \arrow[r] & \mathrm{Ch}_{\mathbb{Q}}(A \otimes A) \arrow[ur] & \end{tikzcd}$$

where the left vertical arrow is the tensor product of the injections of the Wedderburn components, and the right vertical arrow is the projection to the Wedderburn component. The resulting multiplicative map $f : L \otimes M \to P$ may be zero, in which case it is equivariant. If it is not zero, then $f(1 \otimes 1)$ is a nonzero idempotent in P, which implies that $f(1 \otimes 1) = 1$. Then the map

$$L \to P,\; x \mapsto f(x \otimes 1)$$

is a field homomorphism, and since $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ preserves all subfields and acts on them in a way that is independent of the embedding into $\mathbb{Q}_N$, we get that

$$\sigma(f(x \otimes 1)) = f(\sigma(x) \otimes 1)$$

for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$. Similarly, we $\sigma(f(1 \otimes y)) = f(1 \otimes \sigma(y))$ and therefore

$$\begin{aligned} \sigma(f(x \otimes y)) &= \sigma(f(x \otimes 1)f(1 \otimes y)) = \sigma(f(x \otimes 1))\,\sigma(f(1 \otimes y)) \\ &= f(\sigma(x) \otimes 1)f(1 \otimes \sigma(y)) = f(\sigma(x) \otimes \sigma(y)) \end{aligned}$$

Pasting all the Wedderburn components together, we see that the isomorphism $\mathrm{Ch}_{\mathbb{Q}}(A \otimes A) = \mathrm{Ch}_{\mathbb{Q}}(A) \otimes \mathrm{Ch}_{\mathbb{Q}}(A)$ is equivariant with respect to the diagonal action on the right-hand side.

In Paragraph 10.3, we have transferred the action of the Galois group from the character ring $\mathrm{Ch}(A)$ to the center $Z(A)$ by requiring that Φ be equivariant. As $D(A)$ is also a semisimple factorizable Hopf algebra, this whole discussion applies to $D(A)$ as well, so that we also have an action of $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ on $Z(D(A))$. The formulas obtained in Paragraph 10.3 then give in particular that

$$\sigma.z_{ij} = z_{\sigma.i,\,\sigma.j} \qquad \sigma.e_{ij} = e_{\sigma^{-1}.i,\,\sigma^{-1}.j}$$

where we have used the formula $\sigma.(i,j) = (\sigma.i, \sigma.j)$ obtained earlier.

Now we have already pointed out in the proof of Proposition 10.4 that Φ induces an isomorphism between $Z(D(A))$ and $Z(A) \otimes Z(A)$. The above formulas now imply that this isomorphism is equivariant if we endow $Z(A) \otimes Z(A)$ with the diagonal action of the Galois group:

Corollary For $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ and $z \in Z(D(A))$, we have $\Phi(\sigma.z) = \sigma.\Phi(z)$.

Proof. It suffices to check that we have

$$(\cdot e_{ij}) = (e_{{}^{1}:i;\ {}^{1}:j}) = e_{{}^{1}:i} \quad e_{{}^{1}:j} = \cdot e_i \quad \cdot e_j = : (e_{ij})$$

since the centrally primitive idempotents form a basis of $Z(D(A))$. □

11 Galois groups and indicators

11.1 Before we really begin, we present a little background from the theory of Frobenius algebras. We therefore defer the discussion of the setup of this section to Paragraph 11.2.

Recall that the ring $M(r \times r, K)$ of $r \times r$-matrices is a Frobenius algebra with respect to the ordinary matrix trace function tr as Frobenius homomorphism. The dual basis of matrix units E_{ij} with respect to the bilinear form arising from the trace is again formed by the matrix units E_{ji}, with the indices reversed. The corresponding Casimir element therefore is

$$\sum_{i,j=1}^{r} E_{ij} \otimes E_{ji}$$

Note that this element is symmetric under interchange of the tensorands. The following lemma states that this and its Casimir property characterize it up to proportionality:

Lemma Suppose that $\sum_i A_i \otimes B_i \in M(r \times r, K)^{\otimes 2}$ satisfies

1. $\sum_i A A_i \otimes B_i = \sum_i A_i \otimes B_i A$
2. $\sum_i A_i \otimes B_i = \sum_i B_i \otimes A_i$

Then there is a number $\lambda \in K$ such that $\sum_i A_i \otimes B_i = \lambda \sum_{i,j=1}^{r} E_{ij} \otimes E_{ji}$.

Proof. This verification is left to the reader. $\Box$

If we multiply the tensorands of our Casimir element together, we get a multiple of the unit matrix E_r:

$$\sum_{i,j=1}^{r} E_{ij}E_{ji} = rE_r = r \sum_{i,j=1}^{r} \operatorname{tr}(E_{ij})E_{ji}$$

Multiplying this equation by λ, we see that an element of the form considered in the lemma will also satisfy this equation:

$$\sum_i A_iB_i = r \sum_i \operatorname{tr}(A_i)B_i$$

Note that this discussion applies directly to the Wedderburn components of an arbitrary semisimple algebra, where, however, the number r varies with the Wedderburn component. The algebra that we have in mind is the character ring $Ch(H)$ of a semisimple Hopf algebra, which is a Frobenius algebra.[122] In this application, the element A_i that appears in the lemma will be the Wedderburn component of an irreducible character, and B_i will be the Wedderburn component of the corresponding dual character, so that $\sum_i A_iB_i$ is the Wedderburn component of the character of the adjoint representation.

11.2 It is the aim of this section to discuss how the action of the Galois group relates to the action of the modular group, and again the equivariant Frobenius-Schur indicators that we introduced in Paragraph 8.1 will be our main tool. We assume throughout the section that $A = D := D(H)$, the Drinfel'd double of a semisimple Hopf algebra H. Recall from Paragraph 6.1 that $_R(u_D) = \dim(H)$ is a rational number in this case; furthermore, as pointed out in Paragraph 9.3, D and H have the same exponent N. We will use the notation of Section 10 throughout.

We need a preparatory result about the induced module of the trivial module. As discussed in Paragraph 7.1, the induced D-module $\mathrm{Ind}(K)$ of the trivial H-module K can be realized on the underlying vector space H, and this is the way in which we will look at it in this paragraph. If we denote its character by , the result that we will need is the following:

Proposition For all $z \in Z(D)$ and all $\in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, we have

$$(\ .z) = \ (z)$$

Proof. (1) By linearity, it suffices to check this on a basis of the center, so that we can assume that $z = e_i$ is a centrally primitive idempotent. If m_i denotes the multiplicity of the simple module V_i in $\mathrm{Ind}(K)$, we have $(e_i) = n_i m_i$. We first treat the case where $(e_i) \neq 0$; i.e., the case in which V_i is really a constituent of $\mathrm{Ind}(K)$.

Recall[123] that

$$Ch(H) \to \mathrm{End}_D(H\ ); \quad \mapsto (' \mapsto '\ )$$

is an algebra anti-isomorphism. Since e_i is central, the action of e_i is also a D-endomorphism of H, and therefore must be given by right multiplication with a centrally primitive idempotent $q \in Z(Ch(H))$. Further discussion[124] shows that $q := \mathrm{Res}(p_i)$, where

$$\mathrm{Res} : Ch(D) \to Z(Ch(H))$$

is the restriction map. The fact that $e_i.' = 'q$ for all $' \in H$ implies in particular that $(e_i) = \dim(H\ q)$. Furthermore, the general theory of endomorphism rings of semisimple modules[125] implies that the Wedderburn component of $Ch(H)$ corresponding to q has dimension $\dim(Ch(H)q) = m_i^2$.

(2) Let

$$: Z(Ch(H)) \to K$$

be the central character corresponding to q; i.e., the algebra homomorphism from $Z(Ch(H))$ to K that maps q to 1 and vanishes on all other centrally primitive idempotents of $Ch(H)$. Note that we then have $_i = \ \mathrm{Res}$. Now we know from Lorenz' proof of the class equation,[126] combined with the discussion at the end of Paragraph 11.1, that

$$\frac{m_i \dim(H)}{\dim(H\ q)} = \frac{(\ ^0_A)}{m_i}$$

where ${}^{0}_{A}$ denotes the character of the adjoint representation of H. As we have $\dim(H \quad q) = \quad (e_i) = n_i m_i$, we can rewrite this as

$$m_i \dim(H) = n_i \quad ({}^{0}_{A})$$

(3) If $\quad 2 \; Ch_Q(D)$, we have

$$_{:i}(\quad) = \quad (\;_i(\quad)) = \quad (\;(Res(\quad)))$$

This shows that $_{:i} = \;{}^{0}\; Res$, where ${}^{0}: Ch(H) \,!\, K$ arises by scalar extension of from $Ch_Q(H)$ to $Ch(H)$. If $q^0 \; 2 \; Z(Ch(H))$ is the centrally primitive idempotent that corresponds to ^{0}, in the sense that ${}^{0}(q^0) = 1$, it follows exactly as above that $(e_{:i}) = \dim(H \quad q^0) \not= 0$. Even stronger, by applying the equation obtained in the preceding step to these idempotents and using Lemma 10.1, we get

$$m_{:i} \dim(H) = n_{:i} \;{}^{0}(\;{}^{0}_{A}) = n_i \quad (\;({}^{0}_{A})) = n_i \quad ({}^{0}_{A}) = m_i \dim(H)$$

from which our assertion follows immediately, as we have $(e_{:i}) = n_{:i} m_{:i} = n_i m_i = \quad (e_i)$ by Lemma 10.1 again.

(4) Finally, it remains to consider the case $(e_i) = 0$. But then we must also have $(e_{:i}) = 0$, because otherwise we can replace i by $:i$ and by its inverse in the preceding discussion to get $(e_i) = \quad (e_{\;1\;:i}) \not= 0$, which is obviously a contradiction. 2

In view of Proposition 10.3, this result can be restated by saying that the character of the induced trivial module is invariant under the action of the Galois group:

Corollary For all $\quad 2 \; Gal(Q_N = Q)$, we have $\;:\; = \quad$.

11.3 We now want to relate the action of the Galois group to the equivariant Frobenius-Schur indicators that we introduced in Paragraph 8.1. Recall that for any cyclotomic field Q_m and an integer q relatively prime to m, we have an automorphism $_q \; 2 \; Gal(Q_m = Q)$ with the property that $_q(\quad) = \;{}^{q}$ for every m-th root of unity . Every element of the Galois group is of this form. Although $_q$ depends on the field and therefore on m, this dependence is diminished by the fact that when m^0 divides m, so that $Q_{m^0} \quad Q_m$ and q is also relatively prime to m^0, the restriction of $_q$ to Q_{m^0} coincides with the automorphism defined for this field.

Using this notation, we can now relate the action of the Galois group to the equivariant Frobenius-Schur indicators in the following way:

Proposition Consider an H-module V, a central element $z \in Z_{\mathbb{Q}_N}(D)$, and three integers $m, l, q \in \mathbb{Z}$.

1. If q is relatively prime to N and m, we have
$$\sigma_q(I_V((m,l),z)) = I_V((m,lq), \theta'(\sigma_q)(z))$$
2. If q is relatively prime to N and l, we have
$$\sigma_q(I_V((m,l),z)) = I_V((mq,l), \theta(\sigma_q)(z))$$
3. If q is relatively prime to N, m, and l, we have
$$I_V((m,lq), \sigma_q.z) = I_V((mq,l),z)$$

Proof. (1) Recall that, by Proposition 8.4, we have $I_V((m,l),z) \in \mathbb{Q}_N$, so that the expressions considered are well-defined. We begin by proving the first assertion in the case $m > 0$. For this, we note that both sides of the equation are semilinear in the variable z, so that we can assume that $z = e_i$ for some i. Then we have by definition that $I_V((m,l),z) = \operatorname{tr}(\theta^{l} \circ \rho_m(e_i))$, where $\theta = \theta_{V,V^{(m-1)}}$, properly interpreted in the case $m = 1$. The endomorphism $\theta^{l} \circ \rho_m(e_i)$ coincides with θ^{l} on the isotypical component corresponding to e_i and is zero otherwise. Since $\theta^{mN} = \mathrm{id}$, we see that the eigenvalues of $\theta^{l} \circ \rho_m(e_i)$ are mN-th roots of unity, which are raised to their q-th power by the action of σ_q. But these q-th powers are exactly the eigenvalues of $\theta^{lq} \circ \rho_m(e_i)$, which implies the first assertion in the case $m > 0$.

(2) The first assertion in the case $m < 0$ follows from the case $m > 0$, because we then have by definition that

$$\begin{aligned}\sigma_q(I_V((m,l),z)) &= \sigma_q(I_V((-m,-l),S_D(z))) = I_V((-m,-lq), \theta'(\sigma_q)(S_D(z))) \\ &= I_V((-m,-lq), S_D(\theta'(\sigma_q)(z))) = I_V((m,lq), \theta'(\sigma_q)(z))\end{aligned}$$

where the fact that $\theta'(\sigma_q)$ and S_D commute follows from the fact that S_D permutes the centrally primitive idempotents. The remaining case of the first assertion therefore is the case $m = 0$; however, we leave this case open for a moment.

(3) Instead, we now prove the second assertion in the case $m > 0$ and $q = -1$. In this case, we have that $\sigma_{-1} = \iota$ is the restriction of complex conjugation. In view of the assertion already established, we have to show that

$$I_V((m,-l), \theta'(\iota)(z)) = I_V((-m,l), \theta(\iota)(z))$$

Replacing z by $\theta(\iota)^{-1}(z)$, we get the equivalent assertion that

$$I_V((m,-l), \iota.z) = I_V((m,-l), (\theta'(\iota) \circ \theta(\iota)^{-1})(z)) = I_V((-m,l),z)$$

which follows from the fact that $\iota.z = S(z)$ by Proposition 10.1.

(4) From this, we now deduce the first assertion in the case $m = 0$ and $l > 0$. The condition that q is relatively prime to $m = 0$ then forces that $q = \pm 1$. As the case $q = 1$ is obvious, we can assume that $q = -1$, and this reduces to the case just treated since

$$\begin{aligned} I_V((0,-l),\theta'(\sigma_{-1})(z)) &= I_V((0,-l),(S\circ\theta(\sigma_{-1})\circ S^{-1})(z)) \\ &= I_V((-l,0),(\theta(\sigma_{-1})\circ S^{-1})(z)) \\ &= \sigma_{-1}(I_V((l,0),S^{-1}(z))) = \sigma_{-1}(I_V((0,l),z)) \end{aligned}$$

(5) As in the second step, the case of the first assertion where $m = 0$ and $l < 0$ follows from the case $m = 0$ and $l > 0$ just established by using the antipode. It therefore remains to establish the first assertion in the case where $m = l = 0$. Exploiting semilinearity as in the first step, we can again assume that $z = e_i$. Note that in general $I_V((0,0),z)$ is the trace of the action of z on the induced module $\mathrm{Ind}(K)$; in case $z = e_i$, this is an integer. It is therefore invariant under every Galois automorphism, which establishes the first assertion in this case and therefore completely.

(6) The second assertion follows from the first by a variant of the one we have used in the fourth step:

$$\begin{aligned} I_V((mq,l),\theta(\sigma_q)(z)) &= I_V((mq,l),(S^{-1}\circ\theta'(\sigma_q)\circ S)(z)) \\ &= I_V((-l,mq),(\theta'(\sigma_q)\circ S)(z)) \\ &= \sigma_q(I_V((-l,m),S(z))) = \sigma_q(I_V((m,l),z)) \end{aligned}$$

(7) By comparing the first and the second assertion, we get that

$$I_V((m,lq),\theta'(\sigma_q)(z)) = I_V((mq,l),\theta(\sigma_q)(z))$$

Replacing z by $\theta(\sigma_q)^{-1}(z)$, this becomes

$$I_V((m,lq),\sigma_q.z)) = I_V((m,lq),\theta'(\sigma_q)(\theta(\sigma_q)^{-1}(z))) = I_V((mq,l),z)$$

which is the third assertion. □

For an integer q that is relatively prime to N, we can find another integer q' such that $qq' \equiv 1 \pmod N$, which describes the inverse of the residue class of q in the group of units $\mathbb{Z}_N^\times$. Using it, we can derive the following corollary, which should be viewed as a kind of adjunction relation between the Galois action and an action on the lattice points:

Corollary Suppose that m and l are nonzero integers. Furthermore, suppose that q and q' are relatively prime integers that are both relatively prime to m l. If $qq' \equiv 1 \pmod N$, we have

$$I_V((m,l),\sigma_q.z) = I_V((mq,lq'),z)$$

Proof. Since q is relatively prime to lq', it follows from the preceding proposition that

$$I_V((m,lqq'),{}_q.z) = I_V((mq,lq'),z)$$

As we have $qq' \quad 1 \pmod N$ and $\gcd(m,lqq') = \gcd(m,l)$, it follows from Proposition 1.2 that (m,lqq') and (m,l) are in the same (N)-orbit, so that the assertion follows from Theorem 8.4. 2

11.4 For integers q and q' such that $qq' \quad 1 \pmod N$ as above, we denote the residue classes in $\mathbb{Z}_N$ by q resp. q'. With these numbers, we have associated in Paragraph 1.4 the matrix

$$d(q) = \begin{pmatrix} q & 0 \\ 0 & q' \end{pmatrix} \in SL(2,\mathbb{Z}_N)$$

Because the principal congruence subgroup (N) acts trivially by Theorem 9.3, the action of the modular group factors over the quotient group $SL(2,\mathbb{Z}_N)$, so that in particular the action of $d(q)$ on the center is defined. It has the following basic property:

Proposition $I_V((m,l),{}_q.z) = I_V((m,l),d(q).z)$

Proof. (1) We first prove this in the case where both m and l are nonzero. The numbers q, $ml \neq 0$, and N are relatively prime, because already q and N are relatively prime, and therefore we get from Lemma 1.3 that there is an integer c such that $q + cN$ is relatively prime to ml. Note that $q + cN$ is necessarily nonzero. As the asserted equation only depends on the residue class of q modulo N, we can replace q by $q + cN$ if necessary to achieve that q is relatively prime to ml. Similarly, since q', $mlq \neq 0$, and N are relatively prime, we can again by Lemma 1.3 find an integer c' such that $q' + c'N$ is relatively prime to mlq. If necessary, we can replace q' by $q' + c'N$ to achieve that on the one hand q and q' are relatively prime, on the other hand both of them are relatively prime to $ml \neq 0$.

(2) If q and q' are chosen so that they have these additional properties, it follows from Corollary 11.3 that $I_V((m,l),{}_q.z) = I_V((mq,lq'),z)$. Therefore, our claim will follow if we can establish that

$$I_V((mq,lq'),z) = I_V((m,l),d(q).z)$$

For this, suppose that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$ is a lift of $d(q) \in SL(2,\mathbb{Z}_N)$. By Theorem 8.3 and Theorem 8.4, it then suffices to show that (mq,lq') and $(am + cl, bm + dl)$ are in the same (N)-orbit. But this follows again from Proposition 1.2, as we have

$$t := \gcd(mq,lq') = \gcd(m,l) = \gcd(am + cl, bm + dl)$$

and the two lattice points are by construction componentwise congruent modulo N after division by t.

(3) The case $m \neq 0$, $l = 0$ can be reduced to the case just treated by observing that the lattice points $(m, 0)$ and

$$(m, mN) = (m, 0)\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$$

are in the same $\Gamma(N)$-orbit, so that we get

$$\begin{aligned} I_V((m,0); \sigma_q.z) &= I_V((m,mN); \sigma_q.z) = I_V((m,mN); d(q).z) \\ &= I_V((m,0); d(q).z) \end{aligned}$$

by Theorem 8.4. Similarly, the case $m = 0$, $l \neq 0$ can be reduced to the previous case, as the lattice points $(0, l)$ and

$$(lN, l) = (0, l)\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$$

are in the same $\Gamma(N)$-orbit.

(4) It remains to consider the case $m = l = 0$. In this case, we have in view of Theorem 8.3 that $I_V((0,0); d(q).z) = I_V((0,0); z)$ But on the other hand, this indicator is by definition equal to the character of the induced trivial module, so that the equation $I_V((0,0); \sigma_q.z) = I_V((0,0); z)$ is exactly Proposition 11.2. □

A special case of this proposition leads to an invariance property that will be important later. Recall from Paragraph 5.1 that e_1 is a normalized integral. We now show that it is invariant under the action of the diagonal matrices $d(q)$ considered above. Before we derive this, note a difference in the dualization of the Galois group and the modular group: While the action of the Galois group was carried over from the character ring to the center in Paragraph 10.3 by requiring that ι is equivariant, the action of the modular group on the character ring was introduced in Paragraph 9.1 by regarding the character ring as dual to the center via the canonical pairing.

Corollary If $q \in \mathbb{Z}$ is relatively prime to N, we have $d(q).1 = 1$ as well as $d(q).e_1 = e_1$.

Proof. As we have already used in the proof of Corollary 8.4, the indicators corresponding to the lattice points $(1, 0)$ are exactly the characters of the induced modules. The regular representation of D is induced from the regular representation of H, so that we get as a special case of the above proposition that $\chi_R(\sigma_q.z) = \chi_R(d(q).z)$. If $q' \in \mathbb{Z}$ satisfies $qq' \equiv 1 \pmod N$, this equation, in terms of the action of the modular group on the character ring introduced in Paragraph 9.1, reads

$$\sigma_q . \chi_R = d(q') . \chi_R$$

where we have used Proposition 10.3 in addition. As we have $(1) = {}_R$ by construction, it follows from Proposition 9.1 and Proposition 10.3 that ${}_q{}^{1}.1 = d(q^0).1$. Now it follows from Lemma 10.1 that ${}_q.e_1 = e_1$. Applying S and using Proposition 10.3, we get ${}_q{}^{1}.S(e_1) = S(e_1)$. But $S(e_1) = 1$ by Corollary 5.2, which shows that ${}_q{}^{1}.1 = 1$ and establishes the rst assertion. This equation also shows that the second assertion follows from the rst by applying S^{1} and using the commutation relation

$$\begin{matrix} q & 0 \\ 0 & q^0 \end{matrix} \quad \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} = \begin{matrix} 0 & q \\ q^0 & 0 \end{matrix} = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \quad \begin{matrix} q^0 & 0 \\ 0 & q \end{matrix}$$

between s and the diagonal matrix. 2

11.5 Proposition 11.4 can be substantially strengthened: The following theorem, which is the main result of this section, asserts that the two actions do not only give the same result inside the indicators, but are just equal:

Theorem If $q \in \mathbb{Z}$ is relatively prime to N, then we have ${}_q.z = d(q).z$ for all elements z in the center of $D = D(H)$.

Proof. For this, it su ces to show that $({}_q.z) = (d(q).z)$ for all $\in Ch(D)$. If we rewrite this equation in terms of the action of the Galois group on the character ring introduced in Paragraph 10.1 and of the action of the modular group on the character ring introduced in Paragraph 9.1, it takes by Proposition 10.3 the form ${}_q. = d(q^0).$, where $q^0 \in \mathbb{Z}$ satis es $qq^0 \quad 1 \pmod N$. This is equivalent to the condition

$$h\, {}_q. ;\ {}_1 i = h d(q^0). ;\ {}_1 i$$

for all l, using the bilinear form introduced in Paragraph 9.2. If ${}_1$ denotes the character of the induced $D(D)$-module $\mathrm{Ind}(V_1)$, we can by Proposition 9.2 rewrite this equation in the equivalent form

$${}_1(\ {}^1(\ {}^1({}_q.) \quad {}^1(")))= {}_1(\ {}^1(\ {}^1(d(q^0).) \quad {}^1(")))$$

As we have ${}^1(") = \frac{1}{} e_1$ by Proposition 5.2, we can rewrite this equation further in the form

$${}_1(\ {}^1({}_q{}^1. \ {}^1( ) \quad e_1)) = {}_1(\ {}^1(d(q^0). \ {}^1( ) \quad e_1))$$

where we have used Proposition 9.1 and Proposition 10.3. By Lemma 10.1, we have ${}_q(e_1) = e_1$, which can be used together with the analogous equation in Corollary 11.4 to give with

$${}_1(\ {}^1({}_q{}^1. \ {}^1( ) \quad {}_q{}^1.e_1)) = {}_1(\ {}^1(d(q^0). \ {}^1( ) \quad d(q^0).e_1))$$

still another equivalent version of our condition. This in turn is by Corollary 10.5 and Proposition 4.5 equivalent to

$${}_1({}_q{}^1. \ {}^1(\ {}^1( ) \quad e_1)) = {}_1(d(q^0). \ {}^1(\ {}^1( ) \quad e_1))$$

But as we have $\rho_1(z') = I_{V_1}((1,0), z')$ for all $z' \in Z(D(D))$, this is a special case of Proposition 11.4.2.

This theorem has an interesting consequence for the components u_i of the Drinfel'd element that we introduced in Paragraph 5.2:

Corollary For all $\sigma \in Gal(\mathbb{Q}_N/\mathbb{Q})$, we have $\sigma^2(u_i) = u_{\sigma.i}$.

Proof. Recall that all component u_i of the Drinfel'd element are N-th roots of unity. If $\sigma = \sigma_q$ and $qq' \equiv 1 \pmod N$, it follows from the relation

$$\begin{pmatrix} q' & 0 \\ 0 & q \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} q & 0 \\ 0 & q' \end{pmatrix} .e_i = \begin{pmatrix} 1 & q'^2 \\ 0 & 1 \end{pmatrix} .e_i$$

by the preceding theorem that $\sigma_q^{-1}.(u^{-1}\sigma_q.e_i) = u^{q'^2} e_i$, or alternatively

$$\frac{1}{u_{\sigma_q^{-1}.i}} e_i = \sigma_q^{-1}.\left(\frac{1}{u_{\sigma_q^{-1}.i}} e_{\sigma_q^{-1}.i}\right) = \sigma_q^{-1}.(u^{-1} e_{\sigma_q^{-1}.i}) = u_i^{q'^2} e_i = \sigma_q^{2}\left(\frac{1}{u_i}\right) e_i$$

which establishes the assertion. $\square$

12 Galois groups and congruence subgroups

12.1 In this section, we leave the case of a Drinfel'd double and reconsider an arbitrary semisimple factorizable Hopf algebra A. We will use the notation introduced in Section 5, and for the double $D := D(A)$ we will use the notation introduced in Paragraph 10.4. We first consider a new quantity that will play an important role in the sequel:

Definition For $q \in \mathbb{Z}$, we define the Hopf symbol

$$\left(\frac{q}{A}\right) := \begin{cases} \dfrac{\chi_R(u^q)}{\chi_R(u^{-1})} & : \gcd(q, N) = 1 \\ 0 & : \gcd(q, N) \neq 1 \end{cases}$$

where N is the exponent of A.

The Hopf symbol generalizes the Jacobi symbol: If we take Radford's example, i.e., $A = K[\mathbb{Z}_n]$, the group ring of a cyclic group of odd order n endowed with a modified R-matrix, then it follows from the discussion in Paragraph 5.5 that

$$\left(\frac{q}{K[\mathbb{Z}_n]}\right) = \left(\frac{q}{n}\right)$$

The Hopf symbol should be viewed as a 1-cocycle in the following way:[127] The Galois group $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ acts on the multiplicative group $\mathbb{Q}_N^\times$ of nonzero elements in the cyclotomic field. With the element $\chi_R(u^{-1}) \in \mathbb{Q}_N^\times$, we can therefore associate a 1-coboundary

$$f : \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q}) \to \mathbb{Q}_N^\times, \quad \gamma \mapsto \frac{\gamma(\chi_R(u^{-1}))}{\chi_R(u^{-1})}$$

This is essentially the Hopf symbol: If q is relatively prime to N, we have

$$f(\gamma_q) = \frac{\gamma_q(\chi_R(u^{-1}))}{\chi_R(u^{-1})} = \frac{\chi_R(u^q)}{\chi_R(u^{-1})} = \left(\frac{q}{A}\right)$$

As a 1-coboundary, it is in particular a 1-cocycle, and therefore satisfies

$$\left(\frac{qq'}{A}\right) = \left(\frac{q}{A}\right) \gamma_q\left(\left(\frac{q'}{A}\right)\right)$$

Actually, it follows from a version of Hilbert's theorem 90 that every cocycle is a coboundary in this situation.[128]

From the cocycle equation, we immediately obtain the following:

Proposition The following assertions are equivalent:

1. The Hopf symbol is a Dirichlet character.
2. $\left(\frac{q}{A}\right) \in \mathbb{Q}$ for all $q \in \mathbb{Z}$.

In this case, we even have that $\left(\frac{q}{A}\right) \in \{0, 1, -1\}$ for all $q \in \mathbb{Z}$.

Proof. That the Hopf symbol is a Dirichlet character means by definition[129] that we have
$$\left(\frac{qq'}{A}\right) = \left(\frac{q}{A}\right)\left(\frac{q'}{A}\right)$$
for all $q, q' \in \mathbb{Z}$. Note that this equation is satisfied automatically if q or q' are not relatively prime to N. Comparing this equation to the 1-cocycle equation above, we see that it is equivalent to the condition $\sigma_q\left(\frac{q'}{A}\right) = \left(\frac{q'}{A}\right)$. But that the Hopf symbol is invariant under the Galois group just means that it is a rational number.

If it now happens that the Hopf symbol is a Dirichlet character, then its image
$$\left\{\left(\frac{q}{A}\right) \mid q \in \mathbb{Z}, \gcd(q, N) = 1\right\}$$
is a finite subgroup of the multiplicative group $\mathbb{Q}^\times$. As $\{1, -1\}$ is the largest finite subgroup of $\mathbb{Q}^\times$, it must contain all the Hopf symbols.[130] $\square$

12.2 To find out more about the Hopf symbol, the first step is to note that Corollary 11.5 still holds in this more general situation:

Lemma For all $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, we have $\sigma^2(u_i) = u_{\sigma.i}$.

Proof. The expansion of the Drinfel'd element considered in Paragraph 5.2 takes in the case of $D(A)$ the form
$$u_D = \sum_{i,j=1}^{k} u_{ij} e_{ij}$$
In terms of these components, the equation $(u_D) = u \otimes u^{-1}$ obtained in Lemma 3.1 takes the form
$$\sum_{i,j=1}^{k} u_{ij} e_i \otimes e_j = \sum_{i,j=1}^{k} \frac{u_i}{u_j} e_i \otimes e_j$$
so that $u_{ij} = \frac{u_i}{u_j}$. From Corollary 11.5, we get that $\sigma^2(u_{ij}) = u_{\sigma.i, \sigma.j}$, which translates into
$$\frac{\sigma^2(u_i)}{\sigma^2(u_j)} = \frac{u_{\sigma.i}}{u_{\sigma.j}}$$

so that ${}^2(u_i)/u_{:i} = {}^2(u_j)/u_{:j}$. As we have $u_1 = "(u) = 1$ and $:1 = 1$ by Lemma 10.1, we can insert $j = 1$ into this equation to get ${}^2(u_i)/u_{:i} = 1$, from which the assertion follows immediately. 2

It may be noted that inserting for and using Proposition 10.1, we recover the fact that $u_i = u_i$, which expresses that $S(u) = u$, a fact already pointed out in Paragraph 5.1.

As a consequence, we can derive several facts about the Hopf symbol:

Proposition The Hopf symbol is a root of unity. If N is odd, its order divides 6 and $2N$. If N is even, its order divides 24 and N. Furthermore, we have

$$\frac{q}{A} = 1$$

if q is a square modulo N.

Proof. (1) From Proposition 5.3, we get $STSTST = {}_R(u^{1})\dim(A)C^2$. As C^2 is the unit matrix, this implies by taking determinants that[131]

$$\det(S)^3\det(T)^3 = {}_R(u^{1})^k \dim(A)^k$$

Proposition 5.3 also yields that $\det(S)^2 = \dim(A)^k \det(C) = \dim(A)^k$. Therefore, if q is relatively prime to N, we have ${}_q(\det(S)) = \det(S)$. If we now apply ${}_q$ to the above equation, we get

$$\det(S)^3\ {}_q(\det(T))^3 = {}_R(u^{q})^k \dim(A)^k$$

If we divide the two equations by each other, we therefore get that

$$\frac{q}{A}^{\,k} = \frac{{}_R(u^{q})^k}{{}_R(u^{1})^k} = \frac{{}_q(\det(T))^3}{\det(T)^3}$$

Since $\det(T)$ is an N-th root of unity, we see that $\frac{q}{A}$ is a root of unity. Moreover, it is clear from its definition that $\frac{q}{A}\ 2\ \mathbb{Q}_N$, which implies that $\frac{q}{A}^{2N} = 1$, and actually $\frac{q}{A}^{N} = 1$ if N is even.[132]

(2) It now follows from the preceding lemma and Lemma 10.1 that we have

$${}_R(u^{q^2 1}) = {}^2_q({}_R(u^{1})) = \sum_{i=1}^{k} n_i\ {}^2_q\left(\frac{1}{u_i^1}\right) = \sum_{i=1}^{k} n_{q:i}\frac{1}{u^1_{q:i}} = {}_R(u^{1})$$

Dividing this equation by ${}_R(u^{1})$, this shows that $\frac{lq^2}{A} = \frac{l}{A}$, which shows for $l = 1$ that $\frac{q^2}{A} = 1$. But the computation also shows that

$${}^2_q\left(\frac{1}{A}\right) = \frac{{}^2_q({}_R(u^{1}))}{{}^2_q({}_R(u^{1}))} = \frac{{}_R(u^{1})}{{}_R(u^{1})} = \frac{1}{A}$$

Now if ζ is a primitive N-th root of unity, we have already shown in the first step that we can write $\left(\frac{1}{A}\right) = \zeta^m$ for some m, so that the preceding equation becomes $\zeta^{mq^2} = \zeta^m$, which implies $mq^2 \equiv m \pmod N$ for all q that are relatively prime to N, which means that N divides $m(q^2 - 1)$. If N is odd, we see by taking $q = 2$ that N divides $3m$, so that $\left(\frac{1}{A}\right)^3 = \zeta^{3m} = 1$ and therefore $\left(\frac{1}{A}\right)^6 = 1$.

If N is even, we have seen that we actually have $\left(\frac{1}{A}\right) = \zeta^m$ for some m. If $N = \prod_i p_i^{m_i}$ is the prime factorization of N into powers of distinct primes, we can find by the Chinese remainder theorem a unit q modulo N that satisfies $q \equiv 3 \pmod{p_i^{m_i}}$ if $p_i = 2$ and $q \equiv 2 \pmod{p_i^{m_i}}$ if $p_i \neq 2$. If $p_i = 2$, we therefore get that $p_i^{m_i}$ divides $8m$, and if $p_i \neq 2$, $p_i^{m_i}$ divides $3m$. In any case, $p_i^{m_i}$ divides $24m$, so that N divides $24m$, showing[133] that $\left(\frac{1}{A}\right)^{24} = 1$. □

It may be noted that this proposition asserts in particular that $\chi_R(u) = \chi_R(u^{-1})$ if -1 is a square modulo N. If this happens, we can say even more about the Hopf symbol:

Corollary Suppose that $\chi_R(u) = \chi_R(u^{-1})$. Then the Hopf symbol is a Dirichlet character, and we have $\left(\frac{q}{A}\right) \in \{0, 1, -1\}$ for all $q \in \mathbb{Z}$.

Proof. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ be the restriction of complex conjugation considered in Paragraph 10.1. Using it, we can write the assumption in the form $\sigma(\chi_R(u^{-1})) = \chi_R(u^{-1})$. If q is relatively prime to N, we then also have

$$\sigma(\chi_R(u^{-q})) = \sigma(\sigma_q(\chi_R(u^{-1}))) = \sigma_q(\sigma(\chi_R(u^{-1}))) = \sigma_q(\chi_R(u^{-1})) = \chi_R(u^{-q})$$

because $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ is abelian. Dividing this equation by the preceding one, we obtain $\sigma(\left(\frac{q}{A}\right)) = \left(\frac{q}{A}\right)$. But since $\left(\frac{q}{A}\right)$ is a root of unity by the preceding result, we also have $\sigma(\left(\frac{q}{A}\right)) = 1/\left(\frac{q}{A}\right)$. Therefore $\left(\frac{q}{A}\right)^2 = 1$ and $\left(\frac{q}{A}\right) \in \{1, -1\}$. The remaining assertions follow from Proposition 12.1. □

We have already pointed out that the condition $\chi_R(u) = \chi_R(u^{-1})$ means for the Hopf symbol that $\left(\frac{-1}{A}\right) = 1$. A Dirichlet character with this property is called even.[134]

12.3 We have seen in Paragraph 9.4 that the kernel of the projective representation of the modular group is a congruence subgroup of level N. However, in the case where $\chi_R(u) = \chi_R(u^{-1})$, we have also seen that this projective representation comes from a linear representation. This raises the question whether in this case also the kernel of the linear representation is a congruence subgroup of level N. As we will see now, this in fact holds. Our reasoning is based on the following lemma, which is an adaption of an argument by A. Coste and T. Gannon to our situation:[135]

Lemma Suppose that $q, q' \in \mathbb{Z}$ satisfy $qq' \equiv 1 \pmod{N}$. Then we have

$$(S \circ T^{q'} \circ S^{-1} \circ T^{q} \circ S \circ T^{q'})(e_m) = \tau_R(u^{-q})\, e_{\sigma_q^{-1}.m}$$

Proof. It follows from Proposition 5.3 that

$$STSTST = \tau_R(u^{-1}) \dim(A)\, C^{2}$$

and C^2 is the unit matrix by construction. If we write this out in components, it means that

$$\sum_{j,l=1}^{k} \frac{s_{ij}}{u_j} \frac{s_{jl}}{u_l} \frac{s_{lm}}{u_m} = \tau_R(u^{-1}) \dim(A)\, \delta_{im}$$

If we apply σ_q to this equation, it becomes

$$\sum_{j,l=1}^{k} \frac{s_{i,\sigma_q.j}}{u_j^{q}} \frac{s_{\sigma_q.j,l}}{u_l^{q}} \frac{s_{l,\sigma_q.m}}{u_m^{q}} = \tau_R(u^{-q}) \dim(A)\, \delta_{im}$$

If we replace j by $\sigma_q^{-1}.j$ and m by $\sigma_q^{-1}.m$, this becomes

$$\sum_{j,l=1}^{k} \frac{s_{ij}}{u^{q}_{\sigma_q^{-1}.j}} \frac{s_{jl}}{u_l^{q}} \frac{s_{lm}}{u^{q}_{\sigma_q^{-1}.m}} = \tau_R(u^{-q}) \dim(A)\, \delta_{i,\sigma_q^{-1}.m}$$

But this can by the preceding proposition be written in the form

$$\sum_{j,l=1}^{k} \frac{s_{ij}}{u_j^{q'}} \frac{s_{jl}}{u_l^{q}} \frac{s_{lm}}{u_m^{q'}} = \tau_R(u^{-q}) \dim(A)\, \delta_{i,\sigma_q^{-1}.m}$$

Multiplying e_i/n_i by this scalar and summing over i, this becomes

$$\frac{1}{\lambda} \sum_{j,l=1}^{k} \frac{s_{jl}}{u_l^{q}} \frac{s_{lm}}{u_m^{q'}} (S \circ T^{q'})(\frac{e_j}{n_j}) = \sum_{i,j,l=1}^{k} \frac{s_{ij}}{u_j^{q'}} \frac{s_{jl}}{u_l^{q}} \frac{s_{lm}}{u_m^{q'}} \frac{e_i}{n_i} = \tau_R(u^{-q}) \dim(A) \frac{1}{n_m} e_{\sigma_q^{-1}.m}$$

by Corollary 5.2, and by repeating this argument we get

$$\begin{aligned}
\tau_R(u^{-q}) \frac{\dim(A)}{n_m} e_{\sigma_q^{-1}.m} &= \frac{1}{\lambda^2} \sum_{l=1}^{k} \frac{s_{lm}}{u_m^{q'}} (S \circ T^{q'} \circ S \circ \tilde{T}^{q})(\frac{e_l}{n_l}) \\
&= \frac{1}{\lambda^3} (S \circ T^{q'} \circ S \circ \tilde{T}^{q} \circ S \circ \tilde{T}^{q'})(\frac{e_m}{n_m})
\end{aligned}$$

which gives

$$(S \circ T^{q'} \circ S \circ \tilde{T}^{q} \circ S \circ \tilde{T}^{q'})(e_m) = \lambda^{3}\, \tau_R(u^{-q}) \dim(A)\, e_{\sigma_q^{-1}.m}$$

after substituting m for m. Applying the antipode, which commutes with S and T, we get

$$(S \quad T^{q'} \quad SS \quad T^{q} \quad S \quad T^{q'})(e_m) = \quad {}_R(u^{\;q})(\qquad)(R'R)\, e_{q^{\;1} m}$$

where we have used that $^2 \dim(A) = \;(u)\;(u^{\;1}) = (\qquad)(R'R)$, as observed in Paragraph 5.3. Now the assertion follows from Corollary 4.2.2

From this lemma, we can now deduce the result indicated above:

Theorem Suppose that ${}_R(u) = \;{}_R(u^{\;1})$. Then the kernel of the representation of the modular group on the center of A is a congruence subgroup of level N.

Proof. (1) To begin, recall that we saw in Paragraph 4.3 that the condition ${}_R(u) = \;{}_R(u^{\;1})$, which for the Hopf symbol means that $\frac{1}{A} = 1$, ensures that the representation of the modular group is linear, and not only projective, so that it is meaningful to talk about the kernel. Recall also our convention from Paragraph 9.1 that $= \frac{1}{{}_R(u)}$ in this case. Furthermore, we have just seen in Corollary 12.2 that the Hopf symbol is then a Dirichlet character and takes only the values 0, 1, and 1.

We have to verify the relations listed in Proposition 1.4. The relations $s^4 = 1$, $(ts)^3 = s^2$, and $t^N = 1$ that are listed there rst are clearly satis ed. Next, we verify the second relation, i.e., the relation $t^{2^e}(st^m s^{\;1}) = (st^m s^{\;1})t^{2^e}$, where we have factored the exponent in the form $N = 2^e m$ for m odd. Now, as $t^{2^e}(st^m s^{\;1})t^{\;2^e}(st^{\;m} s^{\;1}) \; 2 \quad (N)$, we know from Theorem 9.4 that there is a scalar $\;2\;K$ such that

$$T^{2^e}(S\,T^m S^{\;1})T^{\;2^e}(S\,T^{\;m} S^{\;1})(z) = \;z$$

for all $z \; 2 \; Z(A)$. Inserting $z = (S\,T^m S^{\;1} T^{2^e})(e_1)$, this becomes

$$(S\,T^m S^{\;1} T^{2^e})(e_1) = T^{2^e}(S\,T^m S^{\;1})(e_1)$$

As e_1 is an integral, and we have $S(1) = S(z_1) = \;\dim(A) e_1$ by Corollary 5.2, this equation can be rewritten as

$$(S\,T^m S^{\;1})(e_1) = \frac{1}{\dim(A)} T^{2^e}(S\,T^m)(1)$$

which implies

$$S(u^{\;m}) = \;(S\,T^m)(1) = T^{2^e}(S\,T^m)(1) = T^{2^e}(S(u^{\;m}))$$

Because $S(u^{\;m}) \neq 0$, we see that is an eigenvalue for T^{2^e}, and therefore an m-th root of unity.

Similarly, we can insert $z = (ST^m S^{-1} T^{2^e})(1)$ into the above equation, which then becomes

$$(ST^m S^{-1} T^{2^e})(1) = T^{2^e}(ST^m S^{-1})(1)$$
$$= \frac{1}{\dim(A)} T^{2^e}(ST^m)(e_1) = \frac{1}{\dim(A)} T^{2^e} S(e_1) = T^{2^e}(1)$$

Applying S^{-1} to both sides and dividing by , this becomes

$$T^m(S^{-1}(u^{2^e})) = \frac{1}{} S^{-1}(u^{2^e})$$

Therefore $1/$ is an eigenvalue for T^m, and therefore a 2^e-th root of unity. But now is both a 2^e-th root of unity and an m-th root of unity, which can only be if $= 1$, which in turn establishes our relation.

(2) The remaining two relations involve the diagonal matrices $d(q)$. Now note that with the help of these matrices the formula in the preceding lemma can be expressed as

$$d(q).e_m = {}_R(u^{q}) e_{q^{-1}.m} = \frac{{}_R(u^{q})}{{}_R(u^{1})} e_{q^{-1}.m} = \frac{q}{A} e_{q^{-1}.m}$$

which shows that $d(q).z = \frac{q}{A} {}_q.z$ for all $z \in Z(A)$. This means that the relation $d(q)s = sd(q)^{-1}$ listed third in Proposition 1.4 reads

$$\frac{q}{A} {}_q.S(z) = \frac{1}{\frac{q}{A}} S({}_q^{-1}.z)$$

But as $\frac{q}{A} = \pm 1$, this amounts to the relation ${}_q.S(z) = S({}_q^{-1}.z)$, which was proved in Proposition 10.3.

(3) Finally, for the fourth relation in Proposition 1.4, we have on the one hand that

$$d(q)t.e_j = \frac{1}{u_j} d(q).e_j = \frac{1}{u_j} \frac{q}{A} e_{q^{-1}.j}$$

and on the other hand

$$t^{q^2} d(q).e_j = \frac{q}{A} t^{q^2}.e_{q^{-1}.j} = \frac{q}{A} \frac{1}{u^{q^2}_{q^{-1}.j}} e_{q^{-1}.j}$$

Both expressions are equal by Lemma 12.2, so that all the required relations are satisfied. This proves that (N) is contained in the kernel, and that the level of the kernel is exactly N follows as in Theorem 9.3.2

The preceding theorem generalizes Theorem 9.3, because in the case where $A = D(H)$ is the Drinfel'd double of a semisimple Hopf algebra H, we saw in Paragraph 6.1 that

$$_R(u_D) = {}_R(u_D{}^{1}) = \dim(H)$$

Applying $_q$ to this formula, we see that also $_R(u_D{}^{q}) = \dim(H)$, so that $\frac{q}{A} = 1$. We therefore see that the formula

$$d(q)z = \frac{q}{A} \; {}_q z$$

that we obtained in the preceding proof reduces to Theorem 11.5. However, one has to keep in mind that all these results were used in the preceding proof.

Notes

1 [10]; [60]; [41].

2 [59].

3 [5]; [11]; [14].

4 [19]; [20].

5 [16], Thm. 4.3, p. 136.

6 [50]; [58]; [25]; [26]; [35]; [36]; [37].

7 [22].

8 [22], Cor. 2.3, p. 17; Prop. 3.2, p. 23; Cor. 6.4, p. 48; Thm. 3.4, p. 26.

9 [6]; [58], Sec. II.3.9, p. 98.

10 [58]; [35]; [36].

11 [25]; [37].

12 [22], Prop. 6.2, p. 44.

13 [9], App. B, p. 302.

14 [11], x 2.3, Thm. 2, p. 7.

15 [49], Prop. 2.3', p. 542.

16 [2], Sec. 2.2, Thm. 2.1, p. 28; [29], x II.2, p. 108.

17 [12], x 7.2, p. 85; [27], x II.9.1, p. 454; [38], Sec. II.1, Thm. 8, p. 53; [39], Thm. 3.1, p. 108.

18 [29], Kap. II, x 3, p. 116.

19 [27], x II.7.5, p. 397; [28], p. 96.

20 [18], Def. 1.4, p. 54.

21 [18], Par. 1.8, Exerc. 8, p. 57.

22 [23], Def. VIII.2.2, p. 173; [40], Def. 10.1.5, p. 180; [58], Sec. XI.2.1, p. 496.

23 [23], Sec. VIII.4, p. 179; [40], Thm. 10.1.13, p. 181; [58], Sec. XI.2.2, p. 498.

24 [23], Chap. IX, p. 199; [40], x 10.3, p. 187; [58], Sec. XI.2.4, p. 499.

25 [25], Prop. 7, p. 366; [21], Par. 2, p. 89.

26 [40], Thm. 10.3.12, p. 192; [46], Thm. 4, p. 303.

27 [48], Prop. 3, p. 590.

28 [25], Prop. 7, p. 366.

29 [13], Prop. 6.2, p. 337; [23], Prop. VIII.2.5, p. 177; [52], Sec. 4, p. 1896; [57], Thm. 1, p. 2.

[30] [23], Thm. VIII.2.4, p. 175; [40], Prop. 10.1.8, p. 180; [58], Lem. XI.2.1.1, p. 497.

[31] [49], Thm. 2.9, p. 546; [52], Thm. 4.3, p. 1897; [57], Thm. 2, p. 2.

[32] [23], Prop. XV.3.6, p. 376.

[33] [40], Def. 10.1.15, p. 183.

[34] [23], Exerc. XV.6.1, p. 381; [52], p. 1897.

[35] [13], Prop. 3.3, p. 327; see also [15], Lem. 1.1; p. 192; [52], Thm. 2.1, p. 1892.

[36] [40], Def. 10.3.1, p. 188.

[37] [23], Thm. VIII.2.4, p. 175; [40], Prop. 10.1.8, p. 180; [58], Lem. XI.2.1.1, p. 497.

[38] [13], Prop. 3.3, p. 327; [25]; Lem. 2, p. 362.

[39] [13], Prop. 3.2, p. 327; [40], Thm. 10.1.13, p. 181.

[40] [13], Prop. 3.4, p. 328.

[41] [49], Thm. 2.9, p. 546; [52], Thm. 4.3, p. 1897.

[42] [49], Def. 2.1, p. 543; see also [15], Lem. 1.1, p. 192; [52], p. 1892.

[43] [22], Par. 6.2, p. 44.

[44] [47], Prop. 3, p. 224; [52], Rem. 4.4, p. 1898.

[45] [48], Thm. 3, p. 594.

[46] [33], Prop. 1, p. 269.

[47] [55], Prop. 4.4, p. 639.

[48] [1], Thm. 3.4, p. 488.

[49] [52], Lem. 2.2, p. 1893; [48], Prop. 3, p. 590.

[50] [40], Thm. 2.1.3, p. 18.

[51] [52], Lem. 2.2, p. 1893.

[52] See also [36], Def. 6.2, p. 320; [37], Thm. 1.1, p. 507.

[53] [58], Sec. XI.3.1, p. 500; note the difference to [23], Def. XIV.6.1, p. 361.

[54] [23], Cor. XIV.6.3, p. 362.

[55] [25], Prop. 13, p. 372; [36], Thm. 6.5, p. 321; [37], Eq. (1), p. 507.

[56] [40], Prop. 10.1.4, p. 179; [58], Sec. XI.2.2, Eq. (2.2.c), p. 498; [23], Prop. VIII.4.1, p. 180.

[57] [47], Cor. 2, p. 226.

[58] [48], Prop. 3, p. 590.

[59] [40], Prop. 10.1.14, p. 183.

[60] [3], Rem. 3.1.9, p. 52; [8], Sec. 4, p. 34.

[61] [33], Thm. 3.3, p. 276; [32], Thm. 4, p. 195.

[62] [17], Thm. 1.11, p. 40.

[63] [33], Prop. 2.4, p. 273.

[64] [13], Prop. 6.2, p. 337; [40], Prop. 10.1.14, p. 183; see also [15], Eq. (3), p. 192.

[65] [63], Lem. 2, p. 55; [22], Prop. 6.2, p. 44.

[66] [54], Prop. 3.3, p. 208.

[67] [62], Eq. (4.1), p. 888.

[68] [54], Subsec. 3.3, p. 208.

[69] [54], Prop. 3.5, p. 211.

[70] [40], Prop. 10.1.4, p. 179; [58], Sec. XI.2.2, Eq. (2.2.c), p. 498; [23], Prop. VIII.4.1, p. 180.

[71] [58], Lem. XI.3.3, p. 501; [23], Prop. XIV.6.4, p. 363.

[72] [58], Sec. II.3.9, p. 98.

[73] [58], Sec. II.1.4, p. 74; note the di erence to [15], p. 192 and [52], Rem. 3.4, p. 1895.

[74] [3], Eq. (3.1.3), p. 48; [52], Rem. 3.4, p. 1895; [58], p. 74f, p. 90.

[75] [58], Sec. II.3.9, p. 98.

[76] [15], Lem. 1.2, p. 193; [52], Rem. 3.4, p. 1895; [58], Sec. II.3.8, Eq. (3.8.a), p. 97.

[77] [58], Sec. II.3.8, Eq. (3.8.c), p. 97.

[78] [15], Thm. 1.4, p. 193; [52], Thm. 3.2, p. 1894; [55], Thm. 5.7, p. 641; [57], Thm. 3, p. 5.

[79] [45], Sec. 3, p. 10; [47], Sec. 2.1, p. 219.

[80] [47], Sec. 2.3, p. 227.

[81] [47], Sec. 1.1, p. 210.

[82] [47], Sec. 1.1, p. 211; Sec. 2.1, p. 219; Sec. 2.3, p. 227.

[83] [42], Chap. V, Exerc. 122, p. 187; [44], Chap. 11, Thm. 38, p. 93.

[84] [30], Chap. I.VI, Thm. 91, p. 66; [42], Chap. IV, Sec. 42, p. 146; [44], Chap. 11, p. 91.

[85] [30], Chap. IV.VI.2, p. 208; [44], Chap. 11, Eq. (11.7), p. 88.

[86] [48], Prop. 1.e, p. 587; Prop. 2.c, p. 589.

[87] [33], Lem. 1.2, p. 270.

[88] [48], p. 588.

[89] [33], Lem. 1.2, p. 270.

[90] [22], Par. 6.4, p. 47.

[91] [40], Thm. 2.1.3, p. 18.

92 [33], Lem. 1.2, p. 270.

93 [33], Prop. 5.4, p. 282.

94 Private communication, Chicago, 2007.

95 [23], Thm. XIII.5.1, p. 333.

96 [31], Chap. XVIII, x 7, p. 689.

97 [23], Prop. XIV.2.2b, p. 343f.

98 [23], Def. XIII.4.1, p. 330.

99 [23], Def. XIII.1.1, p. 315.

100 [23], Prop. XIV.2.2c, p. 343f.

101 [23], Thm. XIII.4.2, Eq. (4.4), p. 330.

102 [22], Def. 2.3, p. 15.

103 [40], x 1.7, Def. 1.7.1, p. 13.

104 [22], Par. 2.3, p. 17.

105 [22], Cor. 2.3, p. 17.

106 [22], Prop. 2.3, p. 17.

107 [48], Prop. 3, p. 590; Thm. 3, p. 594.

108 [33], Lem. 1.2, p. 270.

109 [16], Thm. 2.5, p. 133.

110 [16], Thm. 4.3, p. 136; [19], p. 1261; [20], p. 159.

111 [22], Prop. 6.2, p. 44.

112 [46], Prop. 6, p. 302.

113 [54], Par. 3.5, p. 211.

114 [31], Chap. XVIII, x 7, p. 689.

115 [20], Sec. 3, Thm. 3.4, p. 170; [16], Cor. 3.4, p. 135.

116 [22], Prop. 6.2, p. 44.

117 [17], Thm. 1.11, p. 40.

118 [22], Prop. 6.2, p. 44.

119 [7], x 6, Cor. 6.2; [43], Sec. 2, Rem. 11, p. 1088; [62], Sec. 3, Prop. 3.1, p. 885.

120 [17], Chap. 4, Exerc. 30, p. 140.

121 [17], Chap. 3, Exerc. 22, p. 103.

122 [54], Prop. 3.5, p. 211.

[123] [22], Par. 6.3, p. 45.

[124] [22], Par. 6.3, p. 46.

[125] [17], Prop. 1.8, p. 36.

[126] [34], p. 2843.

[127] [53], Chap. VII, x 3, p. 113.

[128] [53], Chap. X, x 1, Prop. 2, p. 150.

[129] [61], Chap. 3, p. 19.

[130] [30], Chap. II.III.2, Def. 25, p. 114.

[131] [3], Thm. 3.1.19, p. 57f.

[132] [61], Exerc. 2.3, p. 17.

[133] [11], x 2.4, Prop. 3.b, p. 9.

[134] [61], Chap. 3, p. 19.

[135] [11], x 2.3, Thm. 2, p. 7.

Bibliography

[1] E. Aljade / P. Etingof / S. Gelaki / D. Nikshych: On twisting of finite-dimensional Hopf algebras, J. Algebra 256 (2002), 484–501

[2] T. M. Apostol: Modular forms and Dirichlet series in number theory, 2nd ed., Grad. Texts Math., Vol. 41, Springer, Berlin, 1990

[3] B. Bakalov / A. Kirillov Jr.: Lectures on tensor categories and modular functors, Univ. Lect. Ser., Vol. 21, Am. Math. Soc., Providence, 2001

[4] P. Bantay: The Frobenius-Schur indicator in conformal field theory, Phys. Lett. B 394 (1997), 87–88

[5] P. Bantay: The kernel of the modular representation and the Galois action in RCFT, Commun. Math. Phys. 233 (2003), 423–438

[6] P. Bantay: Galois currents and the projective kernel in rational conformal field theory, J. High Energy Phys. 3 (2003), 1–8

[7] A. Beauville: Conformal blocks, fusion rules and the Verlinde formula. In: M. Teicher (ed.): Proceedings of the Hirzebruch 65 conference on algebraic geometry, Isr. Math. Conf. Proc., Vol. 9, Bar-Ilan Univ., Ramat-Gan, 1996, 75–96

[8] F. R. Beyl: The Schur multiplicator of $SL(2,\mathbb{Z}/m\mathbb{Z})$ and the congruence subgroup property, Math. Z. 191 (1986), 23–42

[9] J. de Boer / J. Goeree: Markov traces and II_1 factors in conformal field theory, Commun. Math. Phys. 139 (1991), 267–304

[10] J. L. Cardy: Operator content of two-dimensional conformally invariant theories, Nucl. Phys. B 270 (1986), 186–204

[11] A. Coste / T. Gannon: Congruence subgroups and rational conformal field theory, Preprint, math.QA/9909080, 1999

[12] H. S. M. Coxeter / W. O. J. Moser: Generators and relations for discrete groups, 4th ed., Ergeb. Math. Grenzgeb., Vol. 14, Springer, Berlin, 1984

[13] V. G. Drinfel'd: On almost cocommutative Hopf algebras, St. Petersbg. Math. J. 1 (1990), 321–342

[14] W. Eholzer: On the classification of modular fusion algebras, Commun. Math. Phys. 172 (1995), 623–659

[15] P. Etingof / S. Gelaki: Some properties of finite-dimensional semisimple Hopf algebras, Math. Res. Lett. 5 (1998), 191–197

[16] P. Etingof / S. Gelaki: On the exponent of finite-dimensional Hopf algebras, Math. Res. Lett. 6 (1999), 131–140

[17] B. Farb/R. K. Dennis: Noncommutative algebra, Grad. Texts Math., Vol. 144, Springer, Berlin, 1993

[18] N. Jacobson: Basic algebra I, W. H. Freeman, San Francisco, 1974

[19] Y. Kashina: On the order of the antipode of Hopf algebras in ${}^H_H YD$, Commun. Algebra 27 (1999), 1261–1273

[20] Y. Kashina: A generalized power map for Hopf algebras. In: S. Caenepeel/ F. van Oystaeyen (ed.): Hopf algebras and quantum groups, Lect. Notes Pure Appl. Math., Vol. 209, Dekker, New York, 2000, 159–175

[21] Y. Kashina/Y. Sommerhauser/Y. Zhu: Self-dual modules of semisimple Hopf algebras, J. Algebra 257 (2002), 88–96

[22] Y. Kashina/Y. Sommerhauser/Y. Zhu: On higher Frobenius-Schur indicators, Mem. Am. Math. Soc., Vol. 181, No. 855, Am. Math. Soc., Providence, 2006

[23] C. Kassel: Quantum groups, Grad. Texts Math., Vol. 155, Springer, Berlin, 1995

[24] L. Kau man/D. E. Radford: A necessary and su cient condition for a nite-dimensional Drinfel'd double to be a ribbon Hopf algebra, J. Algebra 159 (1993), 98–114

[25] T. Kerler: Mapping class group actions on quantum doubles, Commun. Math. Phys. 168 (1995), 353–388

[26] T. Kerler/V. Lyubashenko: Non-semisimple topological quantum eld theories for 3-manifolds with corners, Lect. Notes Math., Vol. 1765, Springer, Berlin, 2001

[27] F. Klein/R. Fricke: Vorlesungen uber die Theorie der elliptischen Modulfunktionen, 1. Band, Teubner, Stuttgart, 1890

[28] M. I. Knopp: A note on subgroups of the modular group, Proc. Am. Math. Soc. 14 (1963), 95–97

[29] M. Koecher/A. Krieg: Elliptische Funktionen und Modulformen, Springer, Berlin, 1998

[30] E. Landau: Elementary number theory, 2nd ed., Chelsea, New York, 1966

[31] S. Lang: Algebra, Rev. 3. ed., Grad. Texts Math., Vol. 211, Springer, Berlin, 2002

[32] R. G. Larson/D. E. Radford: Semisimple cosemisimple Hopf algebras, Am. J. Math. 109 (1987), 187–195

[33] R. G. Larson/D. E. Radford: Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple, J. Algebra 117 (1988), 267–289

[34] M. Lorenz: On the class equation for Hopf algebras, Proc. Am. Math. Soc. 126 (1998), 2841–2844

[35] V. Lyubashenko: Tangles and Hopf algebras in braided categories, J. Pure Appl. Algebra 98 (1995), 245–278

[36] V. Lyubashenko: Modular transformations for tensor categories, J. Pure Appl. Algebra 98 (1995), 279–327

[37] V. Lyubashenko/S. Majid: Braided groups and quantum Fourier transform, J. Algebra 166 (1994), 506–528

[38] H. Maa : Lectures on modular functions of one complex variable, Lect. Math. Phys., Math., Tata Inst. Fundam. Res., Vol. 29, Bombay, 1964

[39] W. Magnus: Noneuclidean tesselations and their groups, Pure Appl. Math., Vol. 61, Academic Press, New York, 1974

[40] S. Montgomery: Hopf algebras and their actions on rings, 2nd revised printing, Reg. Conf. Ser. Math., Vol. 82, Am. Math. Soc., Providence, 1997

[41] G. Moore/N. Seiberg: Classical and quantum conformal eld theory, Commun. Math. Phys. 123 (1989), 177–254

[42] T. Nagell: Introduction to number theory, Chelsea, New York, 1964

[43] W. D. Nichols/M. B. Richmond: The Grothendieck algebra of a Hopf algebra I, Commun. Algebra 26 (1998), 1081–1095

[44] H. Rademacher: Lectures on elementary number theory, Blaisdell, New York, 1964

[45] D. E. Radford: On the antipode of a quasitriangular Hopf algebra, J. Algebra 151 (1992), 1–11

[46] D. E. Radford: Minimal quasitriangular Hopf algebras, J. Algebra 157 (1993), 285–315

[47] D. E. Radford: On Kau man's knot invariants arising from nite-dimensional Hopf algebras. In: J. Bergen/S. Montgomery (ed.): Advances in Hopf algebras, Lect. Notes Pure Appl. Math., Vol. 158, Dekker, New York, 1994, 205–266

[48] D. E. Radford: The trace function and Hopf algebras, J. Algebra 163 (1994), 583–622

[49] N. Reshetikhin/M. Semenov-Tian-Shansky: Quantum R-matrices and factorization problems, J. Geom. Phys. 5 (1988), 533–550

[50] N. Reshetikhin/V. G. Turaev: Invariants of 3-manifolds via link polynomials and quantum groups, Invent. Math. 103 (1991), 547–597

[51] H.-J. Schneider: Lectures on Hopf algebras, Universidad de Cordoba Trabajos de Matematica, Serie “B”, No. 31/95, Cordoba, Argentina, 1995

[52] H.-J. Schneider: Some properties of factorizable Hopf algebras, Proc. Am. Math. Soc. 129 (2001), 1891–1898

[53] J. P. Serre: Local fields, Grad. Texts Math., Vol. 67, Springer, Berlin, 1979

[54] Y. Sommerhauser: On Kaplansky's fifth conjecture, J. Algebra 204 (1998), 202–224

[55] M. Takeuchi: Modular categories and Hopf algebras, J. Algebra 243 (2001), 631–643

[56] Y. Tsang: On the Drinfel'd double of a semisimple Hopf algebra, Master's thesis, Hong Kong, 1998

[57] Y. Tsang/Y. Zhu: On the Drinfel'd double of a Hopf algebra, Preprint, Hong Kong, 1998

[58] V. G. Turaev: Quantum invariants of knots and 3-manifolds, de Gruyter Stud. Math., Vol. 18, de Gruyter, Berlin, 1994

[59] C. Vafa: Toward classification of conformal field theories, Phys. Lett. B 206 (1988), 421–426

[60] E. Verlinde: Fusion rules and modular transformations in 2d conformal field theory, Nucl. Phys. B 300 (1988), 360–376

[61] L. C. Washington: Introduction to cyclotomic fields, Grad. Texts Math., Vol. 83, Springer, Berlin, 1982

[62] S. J. Witherspoon: The representation ring and the centre of a Hopf algebra, Can. J. Math. 51 (1999), 881–896

[63] Y. Zhu: Hopf algebras of prime dimension, Int. Math. Res. Not. 1 (1994), 53–59