UNIVERSITÀ DEGLI STUDI DI PADOVA

Sede amministrativa: Università degli Studi di Padova

Dipartimento di Matematica “Tullio Levi Civita”

CORSO DI DOTTORATO DI RICERCA IN SCIENZE MATEMATICHE

CURRICOLO MATEMATICA

CICLO XXXVI

Arithmetic and representation theoretic properties of certain Hopf algebras

Coordinatore del Corso: Ch.mo Prof. Giovanni Colombo
Supervisore: Ch.ma Prof.ssa Giovanna Carnovale
Supervisore esterno: Ch.mo Prof. Juan Cuadra Díaz

Dottoranda: Elisabetta Masut

In 2008:

3. Quali persone attorno a te possono aiutarti a progettare il tuo futuro e perché?

a. insegnante di mate perché il mio sogno è di diventare una matematica

In 2024...

Abstract

This thesis deals with arithmetic and representation theoretic properties of certain semisimple Hopf algebras. It consists of two parts.
The first one is devoted to the study of Hopf orders. The initial goal of this part is to prove that for any finite non-abelian simple group G there is a twist Ω for $\mathbb{C}G$, arising from a 2-cocycle on an abelian subgroup of G, such that $(\mathbb{C}G)_\Omega$ does not admit a Hopf order over any number ring. For showing this we prove the non-existence result for a key family of simple groups G and combine it with two theorems of Thompson and Barry and Ward on minimal simple groups.
In addition, we prove the non-existence of Hopf orders for twists of group algebras of direct products of Frobenius groups, subject to some technical conditions.

The second part of the thesis takes place in the finite W-algebras framework. A finite W-algebra H_ℓ is an algebra constructed from a reductive Lie algebra $\mathfrak{g}$ and a nilpotent element $e \in \mathfrak{g}$. We interpret Goodwin's translation functors as an action of a subcategory of $U(\mathfrak{g})$-representations on the category of finitely generated H_ℓ-modules. This action is obtained by transporting the tensor product of $U(\mathfrak{g})$-modules through Skryabin's equivalence.
Recently, Genra and Juillard studied sufficient conditions to apply the Hamiltonian reduction by stages to finite W-algebras, getting a Skryabin equivalence by stages. We show that the latter is an equivalence of $U(\mathfrak{g})$-module categories.

Riassunto

Questa tesi tratta di proprietà aritmetiche e proprietà concernenti la teoria delle rappresentazioni di alcune algebre di Hopf semisemplici. Si compone di due parti.
La prima è dedicata allo studio degli ordini di Hopf.
L'obiettivo iniziale di questa parte è dimostrare che per qualsiasi gruppo finito semplice e non abeliano G esiste un twist Ω per $\mathbb{C}G$, derivante da un 2-cociclo su un sottogruppo abeliano di G, tale che $(\mathbb{C}G)_\Omega$ non ammette un ordine di Hopf su nessun anello di numeri. Per dimostrare ciò, proviamo il risultato di non-esistenza per una famiglia chiave di gruppi semplici G e lo combiniamo con due teoremi di Thompson e Barry e Ward riguardanti i gruppi semplici minimali.
Inoltre, dimostriamo la non-esistenza di ordini di Hopf per twists di algebre di gruppo di prodotti diretti di gruppi di Frobenius, soggetti ad alcune condizioni tecniche.

La seconda parte della tesi è contestualizzata nella teoria delle W-algebre finite. Una W-algebra finita H_ℓ è un'algebra costruita a partire da un'algebra di Lie riduttiva $\mathfrak{g}$ e da un elemento nilpotente $e \in \mathfrak{g}$. Interpretiamo i funtori di traslazione di Goodwin come un'azione di una sottocategoria delle rappresentazioni di $U(\mathfrak{g})$ sulla categoria di H_ℓ-moduli finitamente generati. Quest'azione è ottenuta trasportando il prodotto tensore di moduli di $U(\mathfrak{g})$ attraverso l'equivalenza di Skryabin.
Recentemente, Genra e Juillard hanno studiato condizioni sufficienti per applicare la riduzione hamiltoniana per fasi alle W-algebre finite, ottenendo un'equivalenza di Skryabin per fasi. Mostriamo che quest'ultima è un'equivalenza di $U(\mathfrak{g})$-modulo categorie.

Contents

Introduction

This thesis consists of two independent parts with Hopf algebras serving as common thread. The first part of the thesis deals with arithmetic properties of certain deformation of group algebras, namely the existence of Hopf orders. The second part involves the Hopf algebra $U(\mathfrak{g})$, for $\mathfrak{g}$ a semisimple Lie algebra. In particular, we are interested in properties of the action of a subcategory of $U(\mathfrak{g})$-mod on the category of finitely generated H_ℓ-modules, where H_ℓ is a finite W-algebra.

1. Hopf orders

Hopf algebras are a variation of an algebraic structure on the cohomolgy rings of certain topological spaces introduced by Heinz Hopf in 1941 ([31]). They provided algebraic tools to understand topological properties of these spaces.
Nowadays, Hopf algebras are defined as algebras with a compatible coalgebra structure and an inverse-like operation called the antipode. Over the years, they have become a topic of great interest in their own right, finding applications in different fields, e.g. condensed-matter physics, quantum field theory, string theory and LHC phenomenology ([1]).
In the late 20th century, the study of Hopf algebras was prompted by the introduction of quantum groups, which are important examples of such algebras and have significant applications in theoretical physics.

A crucial goal in understanding Hopf algebras is their complete classification, which is currently a wide open problem. A natural approach to this issue is to divide them into families, according to their properties. An example of these families consists in Hopf algebras which are semisimple as algebras; the latter can be subdivided by means of invariants and further properties.
One of these properties is the existence of Hopf orders (with the definition to follow below); for this reason we are interested in understanding which semisimple Hopf algebras have this additional structure.

In particular, in this part of the thesis we deal with semisimple Hopf algebras that are obtained by deforming certain group algebras KG -where K is a number field and G a finite group- exploiting a specific twist as devised by Movshev in [54]. The ingredients for the construction of this twist are an abelian subgroup of central type M of G and a non-degenerate 2-cocycle on

the character group $\widehat{M}$ (see Subsections 3.2 and 3.3). This procedure alters the comultiplication and the antipode operation, leaving unchanged the other structures, namely multiplication, unit and counit.
Let H be a Hopf algebra over K and let R be a subring of K. A Hopf order, roughly speaking, is a Hopf algebra over R, such that the extension by scalars is isomorphic to H. There is a well-established theory of Hopf orders for cocommutative Hopf algebras; the theory is less developed for non-commutative and non-cocommutative ones. Hopf orders apart from the Hopf algebra framework have applications in number theory, for instance in Galois module theory (for further details see [12] and [13]).
Our goal is to prove that for some key examples of G and M such deformed group algebras do not admit Hopf orders over the ring of integer of K.
Understanding the (non-)existence of Hopf orders was initially motivated by Kaplansky's sixth conjecture.

1.1. Kaplansky's sixth conjecture. In 1975 Kaplansky, after giving a course on bialgebra in Chicago ([40]), proposed to his students 10 open questions, which are now known as Kaplansky conjectures and have been the focus of a great deal of research. Such problems took inspiration from group theory. Indeed, since finite group algebras are finite-dimensional semisimple Hopf algebras, Kaplansky wondered whether the latter could have similar properties to those of finite groups.
The answer to some of these 10 questions is still unknown; among these the sixth one remains a partially open problem (further details could be found in [61]). The above-mentioned conjecture is a generalization of Frobenius theorem in the framework of representation theory of Hopf algebras. Explicitly, it states that given a finite-dimensional semisimple Hopf algebra H, the dimension of every irreducible representation of H divides the dimension of H.
As already said, Kaplansky sixth conjecture motivated the study of Hopf orders. Specifically, Larson proved in [47] that if a Hopf algebra admits a Hopf order over a number ring then the conjecture holds. The way of proving Larson's result was mimicking the proof of Frobenius theorem. Indeed, the latter is rooted on the fact that -speaking in modern terms- the finite group algebra $\mathbb{C}G$ admits the Hopf order $\mathbb{Z}G$.
At this stage, the problem was to understand if complex semisimple Hopf algebras behave as group algebras, in particular if they admit Hopf orders over a number ring.
In this regard, Cuadra and Meir studied the existence of Hopf orders for several families of semisimple Hopf algebras in [14] and [15]. The Hopf algebras considered are constructed as Drinfeld twists of group algebras through the already mentioned Movshev' strategy.

In this case the validity of Kaplansky's conjecture is given for free. Indeed by definition the representations of a Hopf algebra are the representations of

its underlying algebra; then Frobenius theorem can be applied.
Cuadra and Meir proved that for certain families of groups such deformations of group algebras do not admit Hopf orders over a number ring. This highlighted an important difference between finite semisimple Hopf algebras and finite group algebras, showing that the conjecture can be proven even if the method adopted in the proof of Frobenius theorem for groups fails.

The strategy employed for proving the non-existence of Hopf orders for these families of semisimple Hopf algebras considered by Cuadra and Meir is a sort of verification method; the deep reason for this result to hold is still unclear.
In [15, Section 5] the authors hypothesized a relationship between the simplicity of the twisted group algebras and the non-existence of Hopf orders. In particular, they asked the following:

QUESTION. *Let G be a finite non-abelian group. Let Ω be a non-trivial twist for $\mathbb{C}G$, constructed via Movshev strategy. Suppose that $(\mathbb{C}G)_\Omega$ is simple. Can $(\mathbb{C}G)_\Omega$ admit a Hopf order over a number ring?*

In [10] Giovanna Carnovale, Juan Cuadra and myself gave a partial negative answer to this question when restricting ourselves to finite non-abelian simple groups. Indeed, when G is simple, $(\mathbb{C}G)_\Omega$ is always simple independently of the twist (Corollary 1.3.5).
This part of the thesis recollects the main results obtained in the above paper. In addition, we deal with other simple groups and with several non-simple groups which are direct products of certain Frobenius groups. Frobenius groups are an important family of groups firstly introduced by Frobenius in 1901 ([23]). They have many applications in number theory, representation theory, geometry and physics. A Frobenius group G can be viewed as a semidirect product $D \rtimes_\varphi M$, where $\varphi\colon M \to \mathrm{Aut}(D)$ is subject to specific conditions (see Lemma 3.1.3). In this part of the thesis, we restrict ourselves to the case in which M is an abelian p-group. A basic example of Frobenius groups consists of groups of the form $C_q \rtimes C_p$, where p and q are primes such that $p|q-1$ (see Remark 1.3.6 for the definition). If we consider the family of groups $(C_q \rtimes C_p) \times (C_r \rtimes C_p)$, for p, q and r prime such that $p|q-1$ and $p|r-1$ and a twist arising from $M = C_p \times C_p$, it is known that the associated twisted group algebras are simple ([24, Theorem 4.5]). On the other hand, for a general product of Frobenius groups $\prod_{i=1}^{l} D_i \rtimes_{\varphi_i} M_i$, for M_i an abelian p-group for every $i \in \{1, \dots, l\}$ and $M = \prod_{i=1}^{l} M_i$ of central type, it is not yet clear if the associated twisted group algebras are simple or not.

There are also positive results on the existence of Hopf orders in the literature: Cuadra and Meir gave in [16] some conditions for twisted group algebras to admit a Hopf order over a number ring. In particular, the latter exists if there is a normal abelian subgroup which contains a Lagrangian of M, where M is the abelian subgroup giving rise to the twist ([16, Theorem 4.2]). In addition, under more restrictive assumptions, they also proved the uniqueness of the Hopf order ([16, Theorem 5.1]).

1.2. Organization. We provide a brief overview of the organization of this part of the thesis.

Chapter 1 is devoted to the preliminaries. We give a proof of Frobenius Theorem and we show how this proof can be carried out to prove Larson's theorem. Moreover, we recall the definition and the constructions we need: Drinfeld twist, Movshev strategy, Hopf orders. In addition, we expound the strategy we will use to prove the non-existence of Hopf orders and how this can be applied to finite groups of Lie type.

Chapter 2 aims at proving the non-existence result for deformations of group algebras of simple groups, specifically for $\mathbf{SL}_2(q), \mathbf{PSL}_2(q), \mathbf{SL}_3(q), \mathbf{PSL}_3(q)$, the Suzuki groups and the Janko groups. Here the twists arise from either p-subgroups of central type or subgroups isomorphic to the Klein four group. For this purpose, we describe the abelian subgroups of central type of the groups we are considering.
Finally, in light of some remarkable classification theorems in group theory ([66, Corollary 1, page 388] and [3, Theorem 1]), we deduce a general non-existence result for simple groups.

In Chapter 3, we prove the non existence result for group algebras associated to direct products of some Frobenius groups, namely the ones whose Frobenius complement is an abelian p-group.

Finally in the appendix, we recollect some technical results we need in Chapter 2.

2. W-algebras and $U(\mathfrak{g})$-mod

A finite W-algebra H_ℓ is an algebra constructed from a reductive Lie algebra $\mathfrak{g}$ and a nilpotent element $e \in \mathfrak{g}$.
The first definition of such an algebra dates back to 1978, when Kostant constructed in [45] the algebra H_ℓ starting from a regular nilpotent element e_{reg} and showed that $H_\ell \simeq Z(U(\mathfrak{g}))$.
In [58], Premet gave a general definition of a finite W-algebra, i.e. he generalized Konstant's construction to the case of a general nilpotent element. In particular, when $e = 0$, then $H_\ell \simeq U(\mathfrak{g})$, and when e is regular, then $H_\ell \simeq Z(U(\mathfrak{g}))$. The work in [58] was motivated by the study of representations

of semisimple Lie algebras in positive characteristic.
Roughly speaking, a finite W-algebra is a subquotient of $U(\mathfrak{g})$ which lies between $Z(U(\mathfrak{g}))$ and $U(\mathfrak{g})$, although in general it is not a subalgebra of $U(\mathfrak{g})$. Further contributions to the comprehension of this construction are due to Gan, Ginzburg, Brundan and Goodwin ([7], [8], [25]).

Finite W-algebras captured the attention of mathematicians, but also of physicists. The latter were interested in their connection with affine W-algebras, which are vertex algebras modeling the so called W-Symmetry from conformal field theory (see for instance [5]).
Mathematicians are interested in the representation theory of finite W-algebras, because important information about $U(\mathfrak{g})$-modules and primitive ideals of $U(\mathfrak{g})$ are encoded in the representation theory of H_ℓ ([48]). An important connection was illustrated by Skryabin in the appendix of [58], where he established an equivalence between finitely-generated H_ℓ-modules and a specific subcategory of $U(\mathfrak{g})$-modules. By means of this equivalence, Premet in [59] proved that every finite W-algebra possesses finite dimensional irreducible representations.

In representation theory of Lie algebras, a crucial role is played by the Bernstein-Gelfand-Gelfand category $\mathcal{O}$. This category contains a lot of important modules: e.g. finite-dimensional modules, highest-weight modules, Verma modules.
The category $\mathcal{O}$ is the direct sum of the subcategories $\mathcal{O}_\chi$, called blocks, where χ runs through the set of central characters of $U(\mathfrak{g})$. These blocks are related to each other by means of translation functors; these functors allow us to deduce equivalences between blocks and to understand how representations behave when they are translated from a block to another one in the BGG category $\mathcal{O}$.

In [28], Goodwin introduced an analogous functor for H_ℓ-modules. In particular, he defined the translation of a finitely generated H_ℓ-module by a finite dimensional $U(\mathfrak{g})$-module by transporting the tensor product of $U(\mathfrak{g})$-modules through Skryabin's equivalence. Additionally, he studied the relationship between the translation functors and the category $\mathcal{O}(e)$, which is the analogue of the BGG category in W-algebras setting (for the definition see [8, Subsection 4.4]).
In this part of the thesis, after spelling out the transport of structure procedure for general actions of monoidal categories, we interpret this translation functor as an action of a specific subcategory of $U(\mathfrak{g})$ representations on the category of finitely generated H_ℓ-modules.

2.1. Reduction by stages. By Poincaré-Birkhoff-Witt theorem, the universal enveloping algebra $U(\mathfrak{g})$ is a quantization of the symmetric algebra $S(\mathfrak{g})$. Also, in [58], Premet showed that H_ℓ is a quantization of the Slodowy slice $\mathscr{S}_e$ associated to a nilpotent element $e \in \mathfrak{g}$. For constructing $\mathscr{S}_e$ we need a nilpotent element $e \in \mathfrak{g}$, which, by Jacobson-Morozov Theorem, can be embedded in an $\mathfrak{sl}_2$-triple $\{e, h, f\}$, i.e. h, f are such that $[h, e] = 2e$, $[h, f] = -2f$ and $[e, f] = h$. Then the Slodowy slice is defined as $\mathscr{S}_e = e + \mathfrak{g}^f$, where $\mathfrak{g}^f$ stands for the centralizer of f in $\mathfrak{g}$. Since $\mathfrak{g}^*$ is a Poisson variety, the Slodowy slice inherits its Poisson structure through Hamiltonian reduction. Hence, the finite W-algebra can be seen as a quantum Hamiltonian reduction of $U(\mathfrak{g})$.

Since $U(\mathfrak{g}) \simeq H_\ell$ when $e = 0$, one might ask whether a W-algebra $H_{\ell_{(2)}}$ can be expressed as a quantum Hamiltonian reduction of another W-algebra $H_{\ell_{(1)}}$ in such a way that the following diagram commutes.

$$\begin{tikzcd}
U(\mathfrak{g}) \arrow[rr, dashed, "Q.H.R."] \arrow[dr, dashed, "Q.H.R."'] & & H_{\ell_{(2)}} \\
& H_{\ell_{(1)}} \arrow[ur, dashed, "'Q.H.R'"'] &
\end{tikzcd}$$

The theory of Hamiltonian reduction by stages is a well-developed branch of symplectic geometry. The problem is to find a quantum version of Hamiltonian reduction by stages.
Firstly Morgan in [53], and then Genra and Julliard in [26] worked on this topic. In particular, the latter were interested in this reduction by stages for affine W-algebras and for finite W-algebras; for the first one they made some conjectures, while for the finite ones they found some conditions for which a quantum version of Hamiltonian reduction by stages can be performed.
As a consequence of this construction, they obtained a variant of Skryabin equivalence.
This part of the thesis aims at showing that the above equivalence is compatible with the category action by translation functors.

2.2. Organization. We briefly outline how this part of the thesis is organized.

In the fourth chapter, we recall some notions about category theory. In particular, we recall the definition of a monoidal category, of a left $\mathcal{C}$-module category and of a $\mathcal{C}$-module functor. Then, we spell out how we can construct new $\mathcal{C}$-module categories by means of an equivalence and transport of structure.

In Chapter 5, we recall the definition of a finite W-algebra and of the classical version of Skryabin equivalence.

The goal of Chapter 6 is to spell out how the translation functors introduced by Goodwin are an instance of transport of structure of a natural categorical action. To this aim, we show that the category of Whittaker modules is a $(\mathcal{C}_e, \mathcal{C}_e)$-bimodule category, where $\mathcal{C}_e$ is a subcategory of the category of $U(\mathfrak{g})$-modules, depending on e. Then, by means of Skryabin equivalence, we endow the category of H_ℓ-modules with a $(\mathcal{C}_e, \mathcal{C}_e)$-bimodule structure.

In Chapter 7, we briefly recall from [26] how reduction by stages for finite W-algebras can be performed. Then, we will present the variant of Skryabin equivalence in order to show that the latter is invariant under the action of $\mathcal{C}_e$.

Finally, Chapter 8 aims at showing the exactness of the translation functor for H_ℓ-modules.

CHAPTER 1

Preliminaries

In this Chapter we recollect some definitions and results that will be needed for proving the main results of this part of the thesis.

1. Motivation

As we mentioned in the Introduction, the problem of the non-existence of Hopf orders was motivated by Kaplansky's sixth conjecture, which generalizes Frobenius theorem in the setting of Hopf algebras. For this reason, we start stating and proving this fundamental theorem in the representation theory of finite groups.

Theorem 1.1.1. *Let G be a finite group. Then, the degree of any complex irreducible representation of G divides the order of G.*

Proof. Let $\{V_1, \ldots, V_l\}$ be a set of representatives of the isomorphism classes of the irreducible representations of G. For $i \in \{1, \ldots, l\}$, let $n_i = \dim(V_i)$, let ϕ_i be the character of V_i and let e_{ϕ_i} be the central primitive idempotent orthogonal element of $\mathbb{C}G$ associated with ϕ_i, i.e.

$$\frac{|G|}{n_i} e_{\phi_i} = \sum_{g \in G} \phi_i(g) g^{-1}. \tag{1.1.1}$$

It is well known that for every $i \in \{1, \ldots l\}$, the value $\phi_i(g)$ lies in $\mathbb{Z}[\xi]$, where ξ is a primitive $|G|$-th root of unit ([36] Corollary 3.6). For simplicity, we denote $\mathbb{Z}[\xi]$ by R.
Consider the finitely generated R-module RG. Since R is Noetherian, every R-submodule of a finitely generated R-module is again finitely generated. In particular, taking $x \in RG$, the submodule:

$$R[x] := R\langle 1, x, x^2, \ldots \rangle$$

is finitely generated, where $R\langle 1, x, x^2, \ldots \rangle$ is the R-submodule spanned by all powers of x. This implies that x is a root of a monic polynomial with coefficients in R . Since R is finitely generated as a $\mathbb{Z}$-module and $R[x]$ is finitely generated as an R-module, then $R[x]$ is finitely generated as a $\mathbb{Z}$-module. Given that $\mathbb{Z}$ is Noetherian, then $\mathbb{Z}[x]$ is a finitely generated $\mathbb{Z}$-module. Notice that $\frac{|G|}{n_i} e_{\phi_i} = \sum_{g \in G} \phi_i(g) g^{-1} \in RG$ and by the above considerations it is the root of a monic polynomial with coefficients in $\mathbb{Z}$. Especially, for every

$i \in \{1, \dots, l\}$ there exist $m_i > 0$ and $a_{i,j} \in \mathbb{Z}$, for $j \in \{0, \dots, m_i - 1\}$ such that:

$$\left(\frac{|G|}{n_i} e_{\phi_i}\right)^{m_i} + a_{i,m_i-1}\left(\frac{|G|}{n_i} e_{\phi_i}\right)^{m_i-1} + \cdots + a_{i,1}\frac{|G|}{n_i} e_{\phi_i} + a_{i,0} = 0.$$

Multiplying the latter by e_{ϕ_i} and using the fact that e_{ϕ_i} is idempotent, we obtain that for every $i \in \{1, \dots, l\}$:

$$\left(\left(\frac{|G|}{n_i}\right)^{m_i} + a_{i,m_i-1}\left(\frac{|G|}{n_i}\right)^{m_i-1} + \cdots + a_{i,1}\frac{|G|}{n_i} + a_{i,0}\right) e_{\phi_i} = 0,$$

i.e.

$$\left(\frac{|G|}{n_i}\right)^{m_i} + a_{i,m_i-1}\left(\frac{|G|}{n_i}\right)^{m_i-1} + \cdots + a_{i,1}\frac{|G|}{n_i} + a_{i,0} = 0.$$

Since $\frac{|G|}{n_i} \in \mathbb{Q}$ and it is the root of a monic polynomial with coefficients in $\mathbb{Z}$, then $\frac{|G|}{n_i} \in \mathbb{Z}$, for every $i \in \{1, \dots, l\}$. □

The generalization of the above theorem in the framework of Hopf algebras can be read as:

CONJECTURE 1. *Let H be a complex finite-dimensional semisimple Hopf algebra. Then, the dimension of every irreducible representation of H divides* $\dim(H)$.

Before analyzing the conjecture, we need to recollect some notions, constructions and results in Hopf algebra's theory.

2. Hopf algebras

In this section, we fix notations for Hopf algebras and we recall some important notions.
Our main references for the general theory of Hopf algebras are [52] and [60].

We will work over a ground field K. Vector spaces, linear maps, and unindexed tensor products are over K, unless otherwise specified. Throughout, H is a finite-dimensional Hopf algebra over K. We denote by 1_H its identity element; and by Δ, ε, and S its coproduct, counit, and antipode, respectively. The dual Hopf algebra of H is denoted by H^*.
We recall that an element $t \in H$ is called a left (resp. right) integral if it is invariant under left (resp. right) multiplication, i.e. $ht = \varepsilon(h)t$ (resp. $th = \varepsilon(h)t$) for every $h \in H$.

EXAMPLE 1.2.1. Let G be a finite group. Consider the algebra KG endowed with the usual Hopf algebra structure, i.e. $\Delta(g) = g \otimes g$, $S(g) = g^{-1}$ and $\varepsilon(g) = 1$, for every $g \in G$.
The space of left and of right integrals is generated by $\sum_{g \in G} g$.

We say that a Hopf algebra H is *semisimple* if it is semisimple as an algebra.
Semisimplicity is related to left and right integrals; explicitly, a finite-dimensional Hopf algebra is semisimple if and only if $\varepsilon(t) \neq 0$, for every left (and consequently right) integral t.

REMARK 1.2.1. We stress that the antipode of a finite dimensional semisimple Hopf algebra satisfies $S^2 = \mathrm{id}$ by [60, Theorem 16.1.2].

Symmetrically, we say that a Hopf algebra H is *cosemisimple* if it is a direct sum of simple coalgebras, i.e. coalgebras with no proper subcoalgebras.

EXAMPLE 1.2.2. Let G be a finite group. Call $t = \sum_{g \in G} g$ the generator of left and right integrals. By definition of the counit, $\varepsilon(t) = |G|$. Then KG is semisimple if and only if the characteristic of the field does not divide the order of G. Moreover, KG is cosemisimple since $KG = \bigoplus_{g \in G} Kg$ and Kg is a simple subcoalgebra.

For the notion of a simple Hopf algebra H, we need to define a left action of H on itself, called the left adjoint action. Especially:

$$x.h := \sum h^{(1)} x S(h^{(2)}),$$

for $x, h \in H$.
We say that a Hopf subalgebra is *simple* if there are no normal Hopf subalgebras of H, i.e. Hopf subalgebras which are stable under the adjoint action.

EXAMPLE 1.2.3. Consider the group algebra KG for G a finite non abelian simple group. On the base elements, the left adjoint action defined above is just the conjugation, since by definition $\Delta(g) = g \otimes g$ and $S(g) = g^{-1}$, for every $g \in G$. Since Hopf subalgebras of KG are of the form KN, with N a subgroup of G ([60, Exercise 7.1.3]), then normal Hopf subalgebras of KG are in bijection with normal subgroups of G. Hence, the simplicity of the group G implies the simplicity of KG as a Hopf algebra.

3. Deformation of Hopf algebras

In this section we provide a technique for deforming Hopf algebras. We specify this procedure for group algebras, explaining the so called Movshev's strategy. For this purpose, we briefly present the construction of the second cohomology group of a group G over K and some results about it. Throughout this section K has characteristic zero.

3.1. Drinfeld twist. We succinctly recall here the basics of Drinfeld's deformation procedure of a Hopf algebra. An invertible element
$\Omega := \sum \Omega^{(1)} \otimes \Omega^{(2)} \in H \otimes H$ is called a *twist* for H provided that:

$$(1_H \otimes \Omega)(id \otimes \Delta)(\Omega) = (\Omega \otimes 1_H)(\Delta \otimes id)(\Omega), \quad \text{and}$$
$$(\varepsilon \otimes id)(\Omega) = (id \otimes \varepsilon)(\Omega) = 1_H.$$

The *Drinfeld twist* of H is the new Hopf algebra H_Ω constructed as follows: $H_\Omega = H$ as an algebra, the counit is that of H, and the coproduct and antipode differ from those in H in the following way:

$$\Delta_\Omega(h) = \Omega\Delta(h)\Omega^{-1} \qquad \text{and} \qquad S_\Omega(h) = Q_\Omega S(h) Q_\Omega^{-1} \qquad \forall h \in H.$$

Here, $Q_\Omega := \sum \Omega^{(1)} S(\Omega^{(2)})$ and $Q_\Omega^{-1} = \sum S(\Omega^{-(1)})\Omega^{-(2)}$, where $\Omega^{-(1)}$ and $\Omega^{-(2)}$ are defined by $\Omega^{-1} = \sum \Omega^{-(1)} \otimes \Omega^{-(2)}$.

With the following corollary, we stress that cosemisimplicity is preserved under twisting.

Corollary 1.3.1 (Corollary 3.6 [2]). *If H is a cosemisimple Hopf algebra and $J \in H \otimes H$ is a twist for H, then H_J is again cosemisimple.*

3.2. Cocycles. In order to present Movshev strategy, we need to recall the construction of the second cohomology group together with some of its properties.

Let G be a group. We call $Z^2(G, K^\times)$ the set of all functions $\omega\colon G \times G \to K^\times$ such that for every $x, y, z \in G$, the following identities are satisfied

$$\omega(x, 1_G) = \omega(1_G, x) = 1 \tag{1.3.1}$$

$$\omega(x, y)\omega(xy, z) = \omega(y, z)\omega(x, yz). \tag{1.3.2}$$

The elements of $Z^2(G, K^\times)$ are called 2-cocycles.
The set $Z^2(G, K^\times)$ turns out to be an abelian group with the following operation

$$(\omega\omega')(x, y) := \omega(x, y)\omega'(x, y) \tag{1.3.3}$$

for every $\omega, \omega' \in Z^2(G, K^\times)$ and $x, y \in G$.

Consider a map $\omega'\colon G \to K^\times$ with the property that $\omega'(1_G) = 1$. We define a map $\delta\omega'\colon G \times G \to K^\times$ in the following way

$$(\delta\omega')(x, y) = \omega'(x)\omega'(y)\omega'(xy)^{-1}, \tag{1.3.4}$$

for all $x, y \in G$. Such a map $\delta\omega'$ is called a coboundary. The collection of all coboundaries is denoted by $B^2(G, K^\times)$ and it is a subgroup of $Z^2(G, K^\times)$.
We define the *second cohomology group* of G over K as

$$H^2(G, K^\times) := {Z^2(G, K^\times)}\big/{B^2(G, K^\times)}. \tag{1.3.5}$$

We say that two elements of $Z^2(G, K^\times)$ are cohomologous if they belong to the same cohomology class, i.e. if they represent the same element in $H^2(G, K^\times)$. In particular, for $\omega \in Z^2(G, K^\times)$, we write $[\omega]$ to denote its equivalence class.

From now on in this section, we assume that G is abelian. After recalling the above construction, we need to recollect some properties of $H^2(G, K^\times)$.
For this purpose, consider $\bar{K}$ the algebraic closure of K and denote by P_{as} the set of all anti-symmetric pairings of G into $\bar{K}^\times$, i.e. the set of all maps $\beta\colon G \times G \to \bar{K}^\times$ satisfying the following properties

$$\begin{aligned}
&\beta(gh, g') = \beta(g, g')\beta(h, g'),\\
&\beta(g, hg') = \beta(g, h)\beta(g, g'),\\
&\beta(g, h)^{-1} = \beta(h, g),
\end{aligned}$$

for every $g, h, g' \in G$.
We associate to a 2-cocycle ω the anti symmetric bilinear form

$$\beta_\omega(g, g') := \omega(g, g')/\omega(g', g),$$

for every $g, g' \in G$. Observe that the bilinear form β_ω associated to $\omega \in Z^2(G, \bar{K}^\times)$ depends only on the cohomology class of ω .
The following theorem makes this correspondence more precise.

THEOREM 1.3.2. *[42, Theorem 3.6] Let G be a finite abelian group and let $\bar{K}$ be the algebraic closure of K. The assignment $\omega \mapsto \beta_\omega$ induces an isomorphism between the second cohomology group $H^2(G, \bar{K}^\times)$ and the group of $P_{as}(G, \bar{K}^\times)$ consisting of all anti-symmetric pairings of G into $\bar{K}^\times$.*

This correspondence allows us to shift concepts on bilinear forms to concepts on 2-cocycles and cohomology classes.
For instance for $\omega \in H^2(G, \bar{K}^\times)$, we define the radical of ω as

$$\mathrm{Rad}(\omega) := \{g \in G \ : \ \omega(g, g') = \omega(g', g) \ \forall g' \in G\},$$

that is the radical of its associated anti symmetric bilinear form β_ω. Likewise, we say that a 2-cocycle ω is non-degenerate if $\mathrm{Rad}(\omega) = \{1_G\}$, that is β_ω is non-degenerate.
An important result we will rely on is the following:

LEMMA 1.3.3. *For any 2-cocycle ω' on G there exists, up to coboundary, a unique non-degenerate 2-cocycle ω on $G/Rad(\omega')$, such that $[\omega'] = [\omega \circ (p \times p)]$, where p stands for the projection $p\colon G \to G/Rad(\omega')$, and such that $\omega(g, g')$ lies in a cyclotomic field extension of K for any $g, g' \in G/Rad(\omega')$.*

PROOF. Firstly, we prove that for any 2-cocycle ω' on G there exists, up to coboundary, a unique non-degenerate 2-cocycle ω on $G/\mathrm{Rad}(\omega')$, such that $[\omega'] = [\omega \circ (p \times p)]$.
Let ω' be a degenerate 2-cocycle, i.e. a 2-cocycle such that $\mathrm{Rad}(\omega') \neq \{1_G\}$. Thus, it makes sense to consider the quotient $G/\mathrm{Rad}(\omega')$ and in consequence the projection $p\colon G \to G/\mathrm{Rad}(\omega')$. In addition, there exists a bilinear form β on $G/\mathrm{Rad}(\omega')$, such that the following diagram commutes

$$\begin{tikzcd}
G \times G \arrow[rr, "\beta_{\omega'}"] \arrow[dr, "p\times p"'] & & \bar{K}^{\times} \\
& {G/\mathrm{Rad}(\omega') \times G/\mathrm{Rad}(\omega')}. \arrow[ur, "\beta"'] &
\end{tikzcd}$$

The anti-symmetric bilinear form β is non-degenerate by construction. In light of Theorem 1.3.2 there exists a non-degenerate 2-cocycle ω on $G/\mathrm{Rad}(\omega)$ with values on $\bar{K}^{\times}$ such that $\beta = \beta_{\omega}$. By the commutativity of the above diagram, we get that $\beta_{\omega'} = \beta_{\omega} \circ (p \times p)$. In addition, Theorem 1.3.2 implies that the cohomology class of ω' is related to the one of ω through the equality $[\omega'] = [\omega \circ (p \times p)]$. This concludes this verification.

Finally, by [41, Proposition 2.1.1, p. 14] for any 2-cocycle ω' on G with values in $\bar{K}^{\times}$, there exists a 2-cocycle $\omega \in [\omega']$ with values in the ring of integers of a cyclotomic extension of K. $\square$

We conclude this subsection, presenting the condition on a group M for admitting a non-degenerate 2-cocycle.
Recall from [43, page 366] that M is said to be of symmetric type if $M \simeq E \times E$ for some group E. By [43, Theorems 1.9, 2.8, and 2.11], a group M admits a non-degenerate 2-cocycle if and only if M is of symmetric type. We will use the terminology *central type* instead, which is the standard one nowadays in this setting and applies to arbitrary groups, not necessarily abelian. See, for instance, the introductions of [4] and [27].

3.3. Movshev's strategy. We next describe Movshev's method [54, Section 1] of constructing a twist for the group algebra of a finite group G from a 2-cocycle on an abelian subgroup $M < G$. Actually, Movshev studied and classified all possible twists for a group algebra, but for our purposes, we restrict ourselves to the abelian case.

The group algebra KM is a Hopf subalgebra of KG. Suppose that $\operatorname{char} K$ is coprime with $|G|$ and that K is large enough for KM to split. (Here and below, we use the term *split* in the sense of [17, Definition 7.12]: every irreducible representation -corepresentation when dealing with coalgebras- is absolutely irreducible.) Consider the character group $\widehat{M}$ of M. The Wedderburn decomposition of KM is provided by the complete set of orthogonal primitive idempotents $\{e_{\phi}\}_{\phi \in \widehat{M}}$. If $\omega : \widehat{M} \times \widehat{M} \to K^{\times}$ is a 2-cocycle, then

$$\Omega_{M,\omega} := \sum_{\phi,\psi \in \widehat{M}} \omega(\phi, \psi) e_{\phi} \otimes e_{\psi} \tag{1.3.6}$$

is a twist for KM, and, consequently, for KG. In particular, cohomologous 2-cocycles gives rise to isomorphic twisted group algebras, in virtue of [54, Proposition 3].
Later, we will need to know how a twist of this type is carried under an automorphism $f : G \to G$ (in particular, under conjugation). We can carry ϕ to a character ϕ^f of $f(M)$ and ω to a normalized 2-cocycle ω^f on $\widehat{f(M)}$ in the natural way: $\phi^f = \phi \circ (f|_M)^{-1}$ and $\omega^f = \omega \circ (\widehat{f|_M} \times \widehat{f|_M})$, respectively. For the isomorphism $f : KG \mapsto KG, g \mapsto f(g)$, we have $f(e_\phi) = e_{\phi^f}$ and $(f \otimes f)(\Omega_{M,\omega}) = \Omega_{f(M),\omega^f}$. Then:

Remark 1.3.4. The map $f : KG \mapsto KG$ establishes a Hopf algebra isomorphism between $(KG)_{\Omega_{M,\omega}}$ and $(KG)_{\Omega_{f(M),\omega^f}}$. Similarly, cohomologous 2-cocycles give rise to isomorphic Hopf algebras ([54, Proposition 3]).

We also recall the following proposition, which explains the relationship between the simplicity of the group G and the simplicity of the twisted group algebra $(KG)_{\Omega_{M,\omega}}$.

Corollary 1.3.5. *[55, Corollary 4.3] Let G be a finite simple group and let Ω be any twist for KG. Then $(KG)_\Omega$ is simple as a Hopf algebra.*

Remark 1.3.6. We stress that the converse of Corollary 1.3.5 does not hold. For instance, let G be the symmetric group S_n for $n \geq 5$ and let $M = \langle (12), (34) \rangle$. Moreover, consider the unique non-degenerate cocycle ω on $\widehat{M}$, up to coboundary. Then, by [24, Theorem 3.5], the Hopf algebra $(KS_n)_{\Omega_{M,\omega}}$ is simple, even if the symmetric group S_n is not.
We focus on another interesting example. Let p, q, r be prime numbers such that p divides $q-1$ and $r-1$. Then, there exists an element $s \in \mathbb{F}_q^\times$ and an element $t \in \mathbb{F}_r^\times$ of order p. In consequence, we can define the following action of C_p on C_q

$$xyx^{-1} = y^s,$$

for x and y fixed generators of C_p and C_q, respectively. Likewise, the cyclic group C_p acts on C_r in the following way:

$$zwz^{-1} = w^t,$$

for z and w fixed generators of C_p and C_r, respectively. We can then consider the family of groups $G = (C_q \rtimes C_p) \times (C_r \rtimes C_p)$. Let J be the twist arising from $M = C_p \times C_p$ and let $\omega \in H^2(\widehat{M}, K^\times)$ be any 2-cocycle on $\widehat{M}$. Then, the twisted group algebra $(KG)_{\Omega_{M,\omega}}$ is simple by [24, Theorem 4.5].

Notice that $(KG)_{\Omega_{M,\omega}}$ is cosemisimple by Corollary 1.3.1. The Wedderburn decomposition of $(KG)_{\Omega_{M,\omega}}$ as a coalgebra was described by Etingof and Gelaki in [21, Section 3]. We summarize [21, Propositions 3.1, 4.1, and 4.2] and [15, Propositions 2.1 and 2.2] in the following result.

Proposition 1.3.7. *Let $\{\tau_\ell\}_{\ell=1}^n$ be a set of representatives of the double cosets of M in G and let ω be a 2-cocycle on $\widehat{M}$. Then:*

(i) As a coalgebra, $(KG)_{\Omega_{M,\omega}}$ decomposes as the direct sum of subcoalgebras

$$(KG)_{\Omega_{M,\omega}} = \bigoplus_{\ell=1}^n K(M\tau_\ell M).$$

(ii) Suppose that K is large enough so that $(KG)_{\Omega_{M,\omega}}$ splits as a coalgebra. If $M \cap (\tau_\ell M \tau_\ell^{-1}) = \{1\}$ and ω is non-degenerate, then $K(M\tau_\ell M)$ is isomorphic to a matrix coalgebra of size $|M|$. Moreover, the irreducible cocharacter of $(KG)_{\Omega_{M,\omega}}$ attached to $K(M\tau_\ell M)$ is

$$c_{\tau_\ell} := |M| e_\varepsilon \tau_\ell e_\varepsilon. \tag{1.3.7}$$

The following proposition will be crucial in the proof of our main results:

Proposition 1.3.8. *Keep hypotheses and notation as in Proposition 1.3.7(ii). Set $\tau = \tau_\ell$ for short. Let $\chi : KG \to K$ be the linear extension of a character of G. Then:*

$$(\chi \otimes id)\Delta_\Omega(c_\tau) = \frac{1}{|M|} \sum_{g \in M\tau M} \chi(g) g.$$

Proof. The proof is a variation of that of [15, Proposition 3.1(iii)]. We compute:

$$\begin{aligned}
(\chi \otimes id)\Delta_\Omega(c_\tau) &\overset{①}{=} |M| \sum_{\lambda,\rho \in \widehat{M}} \omega(\lambda,\lambda^{-1})\omega^{-1}(\rho,\rho^{-1})\chi(e_\lambda \tau e_\rho) e_{\lambda^{-1}} \tau e_{\rho^{-1}} \\
&\overset{②}{=} |M| \sum_{\lambda,\rho \in \widehat{M}} \omega(\lambda,\lambda^{-1})\omega^{-1}(\rho,\rho^{-1})\chi(\tau e_\rho e_\lambda) e_{\lambda^{-1}} \tau e_{\rho^{-1}} \\
&\overset{③}{=} |M| \sum_{\lambda \in \widehat{M}} \omega(\lambda,\lambda^{-1})\omega^{-1}(\lambda,\lambda^{-1})\chi(\tau e_\lambda) e_{\lambda^{-1}} \tau e_{\lambda^{-1}} \\
&\overset{③}{=} |M| \sum_{\lambda,\rho \in \widehat{M}} \chi(\tau e_\rho e_\lambda) e_{\lambda^{-1}} \tau e_{\rho^{-1}} \\
&\overset{②}{=} |M| \sum_{\lambda,\rho \in \widehat{M}} \chi(e_\lambda \tau e_\rho) e_{\lambda^{-1}} \tau e_{\rho^{-1}} \\
&\overset{④}{=} (\chi \otimes id)\Delta(|M| e_\varepsilon \tau e_\varepsilon) \\
&= \frac{|M|}{|M|^2} \sum_{u,v \in M} \chi(u\tau v) u\tau v \\
&\overset{⑤}{=} \frac{1}{|M|} \sum_{g \in M\tau M} \chi(g) g.
\end{aligned}$$

Here, we used:

① Definition of Δ_Ω and Equation 2.2 in [15, page 141].

② That χ is a character: $\chi(ab) = \chi(ba)$ for all $a, b \in KG$.
③ That $\{e_\phi\}_{\phi\in\widehat{M}}$ is a complete set of orthogonal idempotents in KM.
④ That $\Delta(e_\phi) = \sum_{\lambda\in\widehat{M}} e_\lambda \otimes e_{\lambda^{-1}\phi}$.
⑤ That $u\tau v$ runs one-to-one all elements of $M\tau M$ since $|M\tau M| = |M|^2$.

□

4. Hopf orders

This section aims at defining Hopf orders and at presenting those results that will play a crucial role on proving our main result.

Let W be a finite-dimensional vector space over K. Let R be a subring of K. A *lattice of W over R* is a finitely generated and projective R-submodule X of W such that the natural map $X \otimes_R K \to W$ is an isomorphism. The submodule X corresponds to the image of $X \otimes_R R$.

A *Hopf order of H over a subring R of K* is a lattice X of H that is closed under the Hopf algebra operations; namely,

$$1_H \in X,\ XX \subseteq X,\ \Delta(X) \subseteq X \otimes_R X,\ \varepsilon(X) \subseteq R,\ S(X) \subseteq X.$$

For the coproduct, $X \otimes_R X$ is naturally identified with an R-submodule of $H \otimes H$. This is equivalent to the requirement that X is a: Hopf algebra over R; finitely generated and projective as an R-module and such that $X \otimes_R K \simeq H$ as Hopf algebras over K.

Example 1.4.4. Let G be a finite group and consider the group algebra $\mathbb{Q}G$. Then, $\mathbb{Z}G$ is a Hopf order of $\mathbb{Q}G$. A Hopf order in a Hopf algebra is not unique in general. Indeed, take for example $G = C_2 \times C_2$ and let $\{g, g'\}$ be a set of generators of such a group. The $\mathbb{Z}$-module generated by $\left\{\frac{1-g}{2}, \frac{1+g}{2}, g'\right\}$ is a Hopf order of $\mathbb{Q}G$ strictly containing $\mathbb{Z}G$.

It is natural to expect that also Hopf orders can be dualized maintaining the property of being isomorphic to their double dual. Firstly, we need to understand the dual of a Hopf order.
Let X be a lattice of H over a subring R of K. We define the *dual* of X as $X^\star := \{\phi \in H^* : \phi(X) \subseteq R\}$.

Then X^* is an R-module via the action $(r.\phi)(x) = \phi(r.x)$, for every $r \in R$, $x \in X$ and $\phi \in X^\star$.

Recall that a representation of a Hopf algebra H is a representation of its underlying algebra, i.e. a vector space V together with a morphism $\phi\colon H \to \mathrm{End}(V)$. The character χ_ϕ of a representation ϕ of H is defined as

$$\chi_\phi(h) := \mathrm{Tr}(\phi(h)),$$

for every $h \in H$, in line with the group algebra case.
In the following three propositions, K is a number field and $R \subset K$ is a Dedekind domain containing $\mathcal{O}_K$, the ring of algebraic integers of K. Under these hypotheses, K is the field of fractions of R. Hopf order means Hopf order over R.

PROPOSITION 1.4.1. *[14, Lemma 1.1] Let X be a Hopf order of H.*

(i) The dual lattice $X^\star := \{\varphi \in H^* : \varphi(X) \subseteq R\}$ is a Hopf order of H^*.
(ii) The natural isomorphism $H \simeq H^{**}$ induces an isomorphism $X \simeq X^{\star\star}$ of Hopf orders.

The proofs of our main results are rooted in the following:

PROPOSITION 1.4.2. *[14, Proposition 1.2] Let X be a Hopf order of H. Then:*

(i) Every character of H belongs to $X^\star$.
(ii) Every character of H^* (cocharacter of H) belongs to X.

The following technical result often eases our task:

PROPOSITION 1.4.3. *[14, Proposition 1.9] Let X be a Hopf order of H.*

(i) If A is a Hopf subalgebra of H, then $X \cap A$ is a Hopf order of A.
(ii) If $\pi : H \to B$ is a surjective Hopf algebra map, then $\pi(X)$ is a Hopf order of B.

5. Larson Theorem

The goal of this section is to prove Larson theorem, generalizing the proof of Frobenius theorem.
For this purpose, we need a formula for the central primitive idempotent elements in a semisimple Hopf algebra.
Let H be a finite-dimensional semisimple Hopf algebra and suppose that K is large enough so that H splits as an algebra and a coalgebra. Applying Wedderburn's theorem, H is isomorphic as an algebra to a product of matrix algebras of finite degree with coefficient in K. Especially,

$$H \simeq \prod_{i=1}^{l} M_{n_i}(K).$$

Moreover, we set V_i to be the natural representation of $M_{n_i}(K)$ and n_i to be its dimension, in particular V_i is irreducible for all $i \in \{1, \dots, l\}$.
Denoting the identity matrix of size n_j by $\mathbb{1}_{n_j}$, we call ϵ_j the element $(0, \dots, \mathbb{1}_{n_j}, \dots, 0)$ in $\prod_{i=1}^{l} M_{n_i}(K)$, where $\mathbb{1}_{n_j}$ is in the j-th position.

By definition,

$$\begin{aligned}&\epsilon_i\epsilon_j = (0,\dots,0) \quad \text{if } i \neq j,\\ &\epsilon_i^2 = \epsilon_i \text{ for every } \; i \in \{1,\dots,l\},\\ &\epsilon_1 + \dots + \epsilon_l = (\mathbb{1}_{n_1}, \mathbb{1}_{n_2}, \dots, \mathbb{1}_{n_l}).\end{aligned}$$

We denote by e_i the image of ϵ_i through the isomorphism $\prod_{i=1}^{l} M_{n_i}(K) \simeq H$. Then

$$e_ie_j = 0 \text{ if } i \neq j,\; e_i^2 = e_i, \text{ for every } \; i \in \{1,\dots,l\}, \text{ and } e_1 + \dots + e_l = 1.$$

Equivalently, the elements $\{e_i\}_{i=1}^{l}$ form a set of orthogonal idempotents in H and they are such that $H = \bigoplus_{i=1}^{l} He_i$, with $He_i \simeq M_{n_i}(K)$, for $i \in \{1,\dots,l\}$.

Let $\lambda \in H^*$ be a left integral, rescaled to ensure that $\langle \lambda, 1_H \rangle = 1$ and let $\Lambda \in H$ be a right integral. Without loss of generality by the semisimplicity of H, we can choose Λ in such a way that $\langle \lambda, \Lambda \rangle = 1$. The following proposition provides a formula for the central primitive idempotent elements.

Proposition 1.5.1. *Let H, Λ and V_i for $i \in \{1,\dots,l\}$ be as above. Let ϕ_i be the character of V_i. Then:*

$$\frac{\dim(H)}{\dim(V_i)} e_i = \sum \Lambda_{(1)} \langle \phi_i, S(\Lambda_{(2)}) \rangle. \tag{1.5.1}$$

We are now in a position to state Larson's theorem.

Theorem 1.5.2. *Let H be a finite-dimensional semisimple Hopf algebra and suppose that K is large enough so that H splits as an algebra and a coalgebra. Suppose that H admits a Hopf order X over a number ring $\mathcal{O}_K$. Then, the dimension of every irreducible representation of H divides* $\dim(H)$.

Proof. By [60, Theorem 16.1.2] the integral Λ is the character of the regular representation; hence, by Proposition 1.4.2, the element Λ lies in X. By the definitions of a Hopf order and of the dual Hopf order and by Proposition 8.0.1, also $\sum \Lambda_{(1)} \langle \phi_i, S(\Lambda_{(2)}) \rangle$ belongs to X, for every $i \in \{1,\dots,l\}$. Consequently, $\frac{\dim(H)}{\dim(V_i)} e_i \in X$ for every $i \in \{1,\dots l\}$. Since X is finitely generated as an $\mathcal{O}_K$-module, arguing as we did in the proof of Frobenius theorem, we obtain that there exist $m_i > 0$ and $r_{i,j} \in \mathbb{Z}$ such that:

$$\left(\frac{\dim H}{\dim V_i} e_i\right)^{m_i} + r_{i,m_i-1}\left(\frac{\dim H}{\dim V_i} e_i\right)^{m_i-1} + \dots + r_{i,1}\left(\frac{\dim H}{\dim V_i} e_i\right) + r_{i,0} = 0,$$

for every $i \in \{1,\dots,l\}$. Multiplying by e_i we obtain

$$\left(\frac{\dim H}{\dim V_i}\right)^{m_i} + r_{i,m_i-1}\left(\frac{\dim H}{\dim V_i}\right)^{m_i-1} + \dots + r_{i,1}\left(\frac{\dim H}{\dim V_i}\right) + r_{i,0} = 0.$$

We conclude that $\frac{\dim H}{\dim V_i}$ is the root of a monic polynomial in $\mathbb{Z}$. Hence $\frac{\dim H}{\dim V_i} \in \mathbb{Z}$, for every $i \in \{1, \ldots, l\}$, i.e. the dimension of V_i divides $\dim H$, for every $i \in \{1, \ldots, l\}$. $\square$

6. Strategy of proof and framework of application

As we mentioned in the introduction, we want to prove the following:

THEOREM. *[10, Corollary 6.4] Let G be a finite non-abelian simple group. Then, there is a twist Ω for $\mathbb{C}G$, as in Subsection 3.3, such that $(\mathbb{C}G)_\Omega$ does not admit a Hopf order over any number ring.*

Apart from the twisted group algebras needed for proving the above result, we will also present other examples of twisted group algebras which do not admit Hopf orders; some of them arise from simple groups and others from the direct product of certain Frobenius groups.

We expound here in general terms the strategy that we will use to prove the non-existence of integral Hopf orders for a twist of several group algebras. This strategy suitably modifies that employed in [15, Section 3] for the alternating groups.

Here K is a number field and R is a Dedekind domain such that $\mathcal{O}_K \subseteq R \subset K$. Consider the Hopf algebra $(KG)_{\Omega_{M,\omega}}$ as in Subsection (3.3), for some abelian subgroup M and some 2-cocycle ω on $\widehat{M}$. Suppose that $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order X over R. The aim will be to prove that for our choice of groups and twists the fraction $\frac{1}{|M|}$ belongs to R. Notice that if $\frac{1}{|M|} \in R$, then the group ring RG is closed under $\Delta_\Omega, \varepsilon_\Omega$ and S_Ω and RG is a Hopf order of $(KG)_{\Omega_{M,\omega}}$ over R. Our result will tell that the condition $\frac{1}{|M|} \in R$ is also necessary for $(KG)_{\Omega_{M,\omega}}$ to admit a Hopf order over R. This implies, in particular, that Hopf orders of $(KG)_{\Omega_{M,\omega}}$ over R do not exist when $R = \mathcal{O}_K$.

For our aim, by Lemma 1.3.3 and by Remark 1.3.4 we can assume first, without loss of generality, that ω is non-degenerate.
We can assume secondly that K is large enough so that $(KG)_{\Omega_{M,\omega}}$ splits as an algebra and as a coalgebra. The reason for this is the following. The Hopf algebra $(KG)_{\Omega_{M,\omega}}$ splits as an algebra and as a coalgebra over a finite field extension L/K. Let $\bar{R}$ denote the integral closure of R in L. Then, $\bar{R}$ is a Dedekind domain, which contains $\mathcal{O}_L$, and if X is a Hopf order of $(KG)_{\Omega_{M,\omega}}$ over R then $X \otimes_R \bar{R}$ is a Hopf order of $(LG)_{\Omega_{M,\omega}}$ over $\bar{R}$. Hence, the non-existence of Hopf orders over $\bar{R}$ implies the non-existence of Hopf orders over R.

We will choose $\tau, \tau' \in G$ such that $M \cap (\tau M \tau^{-1}) = \{1\}$ and $M \cap (\tau' M \tau'^{-1}) = \{1\}$. We will consider the irreducible cocharacters c_τ and $c_{\tau'}$ of $(KG)_{\Omega_{M,\omega}}$ attached to $K(M\tau M)$ and $K(M\tau' M)$ as in (1.3.7) respectively. Assume that X is a Hopf order over R. By Proposition 1.4.2(ii), c_τ and $c_{\tau'}$ belong to X. Using that X is closed under the coproduct, Proposition 1.4.2(i) and Proposition 1.3.8, we obtain that the following elements $y_{\chi,\tau}$ and $y_{\chi',\tau'}$ belong to X:

$$y_{\chi,\tau} := (\chi \otimes id)\Delta_\Omega(c_\tau) = \frac{1}{|M|} \sum_{g \in M\tau M} \chi(g) g, \tag{1.6.1}$$

$$y_{\chi',\tau'} := (\chi' \otimes id)\Delta_\Omega(c_{\tau'}) = \frac{1}{|M|} \sum_{g \in M\tau' M} \chi'(g) g, \tag{1.6.2}$$

for χ and χ' two characters of G. Then, $y_{\chi,\tau}\, y_{\chi',\tau'}$ lies in X as well. Proposition 1.4.2(i) yields that $\chi''(y_{\chi,\tau}\, y_{\chi',\tau'}) \in R$, for any character χ'' of G. We will choose τ, τ', χ, χ' and χ'' in such a way that the fraction $\frac{1}{|M|}$ will appear as a factor of $\chi''(y_{\chi,\tau}\, y_{\chi',\tau'})$ so that we could derive that $\frac{1}{|M|} \in R$ by applying Bezout's identity.

6.1. Strategy for p-groups. In our setting, M will be often a p-group and there will be a Sylow p-subgroup U of G set in advance. Remark 1.3.4 will allow us to assume that M is a subgroup of U. In this case, we will use the strategy presented above with $\chi = \chi' = \chi'' := \mathrm{Ind}_U^G(\mathbb{1}_U)$, where $\mathrm{Ind}_U^G(\mathbb{1}_U)$ stands for the induced character of the trivial representation of U. Set $P = \bigcup_{g \in G} gUg^{-1}$ the set of p-elements in G together with the identity. By construction, χ vanishes outside P. Its values on the identity and on $u \in U$ are:

$$\begin{aligned} \chi(1) &= \frac{|G|}{|U|}, \\ \chi(u) &= \frac{1}{|U|} \sum_{\substack{g \in G \\ gug^{-1} \in U}} \mathbb{1}_U(gug^{-1}) = \frac{1}{|U|} \cdot \#\{g \in G : gug^{-1} \in U\}. \end{aligned} \tag{1.6.3}$$

Next we choose $\tau = \tau' \in G$ such that $M \cap (\tau M \tau^{-1}) = \{1\}$. From now on, we will write y_χ instead of $y_{\chi,\tau}$ to simplify the notation.
The element y_χ^2 reads as:

$$y_\chi^2 = \frac{1}{|M|^2} \sum_{u,u',v,v' \in M} \chi(\tau u' u)\chi(\tau v' v) u\tau u' v \tau v'. \tag{1.6.4}$$

Evaluating χ at this element, we get:

$$\chi(y_\chi^2) = \frac{1}{|M|^2} \sum_{u,u',v,v' \in M} \chi(\tau u'u)\chi(\tau v'v)\chi(\tau u'v\tau v'u). \tag{1.6.5}$$

Let I_χ be the set of fibers of χ of non-zero values; that is,

$$I_\chi = \{\chi^{-1}(\gamma) : \gamma \in \mathrm{Im}(\chi) \text{ and } \gamma \neq 0\}.$$

For $C \in I_\chi$ we write $\chi(C)$ for the value that χ takes at any element in C and we set $M_C = \{v \in M : \tau v \in C\}$. Notice that $C \subseteq P$, for every $C \in I_\chi$.

We now rearrange the subscripts in the sums in (1.6.4) and (1.6.5) as follows. Firstly, we make the substitutions $u'u = x \in M_C$ and $v'v = x' \in M_{C'}$ and eliminate u' and v. Secondly, we replace v' by v^{-1}. Thirdly, we rename $u^{-1}v$ as v in (1.6.5). Thus, we arrive at the following formulas for y_χ^2 and $\chi(y_\chi^2)$:

$$y_\chi^2 = \frac{1}{|M|^2} \sum_{C,C' \in I_\chi} \chi(C)\chi(C') \sum_{\substack{u,v \in M \\ x \in M_C,\, x' \in M_{C'}}} u\tau x x' u^{-1} v \tau v^{-1}, \tag{1.6.6}$$

$$\chi(y_\chi^2) = \frac{1}{|M|} \sum_{C,C' \in I_\chi} \chi(C)\chi(C') \sum_{\substack{v \in M \\ x \in M_C,\, x' \in M_{C'}}} \chi(\tau x x' v \tau v^{-1}). \tag{1.6.7}$$

Then, the calculation of $\chi(y_\chi^2)$ reduces to the following procedure:

(1) Find out $(\tau M) \cap P$ and M_C for every fiber $C \neq \{1\}$ in I_χ.
(2) Detect for which $v \in M, x \in M_C$, and $x' \in M_{C'}$, the element $\tau x x' v \tau v^{-1}$ belongs to P.
(3) For those elements obtained in step (2), calculate $\chi(\tau x x' v \tau v^{-1})$.
(4) Estimate the sum in (1.6.5) to show that $\chi(y_\chi^2) \in \frac{\mathbb{Z}}{|M|} \setminus \mathbb{Z}$.

6.2. Application to finite groups of Lie type. We now explain how to apply the previous strategy to a finite group of Lie type G with defining characteristic p and a twist arising from an abelian p-subgroup M of G of central type. All unexplained notation, notions, properties, and results recalled here can be found in the monograph [49].

Let $\mathbb{G}$ be a simply connected simple algebraic group defined over $\overline{\mathbb{F}_p}$ and F a Steinberg endomorphism; i.e., an endomorphism of the abstract group $\mathbb{G}$ such that the fixed points subgroup $\mathbb{G}^F$ is finite. We will take G to be either the group $\mathbb{G}^F$ or its central quotient $\mathbb{G}^F/Z(\mathbb{G}^F)$. With a few exceptions, $\mathbb{G}^F/Z(\mathbb{G}^F)$ is always simple. All simple groups of Lie type arise in this form, except for the Tits group, and only in very few cases the defining characteristic p is not uniquely determined, see [69, page 3]. For our purpose, any possible realization in this form would work. We denote by $\pi\colon \mathbb{G}^F \to \mathbb{G}^F/Z(\mathbb{G}^F)$ the natural projection. Recall that $\gcd(p, |Z(\mathbb{G}^F)|) = 1$.

In the cases we consider, all elements in $\mathbb{G}$ have finite order. An element in $\mathbb{G}$ is semisimple if and only if its order is coprime with p, while an element

of $\mathbb{G}$ is unipotent if its order is a power of p (p-element). Moreover, central elements are semisimple. A maximal torus $\mathbb{T}$ is a subgroup containing only semisimple elements and maximal for this property.
The group $\mathbb{G}$ contains an F-stable maximal torus $\mathbb{T}$ and two opposite F-stable unipotent subgroups $\mathbb{U}$ and $\mathbb{U}^-$ which are normalized by $\mathbb{T}$ and satisfy $\mathbb{U}\cap\mathbb{U}^- = \{1\}$. The subgroups $\mathbb{U}^F$ and $(\mathbb{U}^-)^F$ are Sylow p-subgroups of $\mathbb{G}^F$. We denote them by U and U^- respectively. The quotient $\pi(U)$, which is isomorphic to U, is in turn a Sylow p-subgroup of $\mathbb{G}^F/Z(\mathbb{G}^F)$. The same holds for U^-. The groups $\mathbb{B} := \langle \mathbb{T}, \mathbb{U}\rangle \simeq \mathbb{T} \ltimes \mathbb{U}$ and $\mathbb{B}^- := \langle \mathbb{T}, \mathbb{U}^-\rangle \simeq \mathbb{T} \ltimes \mathbb{U}^-$ are opposite Borel subgroups of $\mathbb{G}$, i.e. maximal solvable connected subgroups of $\mathbb{G}$. We set $B = \mathbb{B}^F \simeq \mathbb{T}^F \ltimes U$ and $B^- = (\mathbb{B}^-)^F \simeq \mathbb{T}^F \ltimes U^-$. Then, $B \cap B^- = \mathbb{T}^F$. Finally, recall that there is an element $\dot{w}_0 \in N_{\mathbb{G}^F}(\mathbb{T})$ such that $\dot{w}_0\mathbb{U}\dot{w}_0^{-1} = \mathbb{U}^-$, so $\dot{w}_0 U\dot{w}_0^{-1} = U^-$. For any $\sigma \in \dot{w}_0\mathbb{T}^F$ we have $\sigma U\sigma^{-1} = U^-$. The coset $\dot{w}_0\mathbb{T}^F$ is an involution in $N_{\mathbb{G}^F}(\mathbb{T})/\mathbb{T}^F$. Hence, $\sigma^{-1} \in \sigma\mathbb{T}^F$.

Assume that U (or equivalently, $\pi(U)$) contains an abelian subgroup V of central type. Observe that $V \cap (\sigma V\sigma^{-1}) = \{1\}$ for any $\sigma \in \dot{w}_0\mathbb{T}^F$, similarly for $\pi(\sigma)$, because that is a subset of $U \cap U^-$. The double cosets $V\sigma V$ and V are disjoint. Then, $v\sigma v' \neq 1$ for all v, $v' \in V$. Similarly, $\pi(v\sigma v') \neq 1$, since, otherwise, we would have $\sigma \in UZ(\mathbb{G}^F)$, which is impossible because $UZ(\mathbb{G}^F)$ normalizes U.

The next chapter deals mainly with families of groups in the following two scenarios:

(1) The group $\mathbb{G}^F$, the subgroup $M = V$, the element $\tau = \sigma$, and the induced character $\chi = \mathrm{Ind}_U^{\mathbb{G}^F}(\mathbb{1}_U)$.
(2) The group $\mathbb{G}^F/Z(\mathbb{G}^F)$, the subgroup $M = \pi(V)$, the element $\tau = \pi(\sigma)$, and the induced character $\chi = \mathrm{Ind}_{\pi(U)}^G(\mathbb{1}_{\pi(U)})$.

The following remark identifies when an element in P of the form $\tau u'v\tau v'u$ is the identity element. This is necessary in practice for the evaluation of χ, see Equation 1.6.5:

Remark 1.6.1. In the above scenarios, observe that $\tau u'v\tau v'u = 1$ if and only if $u'v = 1$, $v'u = 1$, and $\tau = \tau^{-1}$. For, suppose that $\tau u'v\tau v'u = 1$. Then, $\tau u'v\tau = (v'u)^{-1}$ belongs to $M \cap (\tau M\tau)$. In the first scenario, when dealing with $\mathbb{G}^F$, we have the inclusions

$$M \cap (\tau M\tau) \subseteq M \cap \big(\tau M(\tau^{-1}\mathbb{T}^F)\big) \subseteq U \cap \big(U^-\mathbb{T}^F\big) = \{1\}.$$

Hence, $\tau u'v\tau = 1$ and $v'u = 1$. This implies in turn that $\tau^2 \in M \cap (\tau M\tau)$. Consequently, $\tau^2 = 1$ and $u'v = 1$. For the proof in the second scenario, when dealing with $\mathbb{G}^F/Z(\mathbb{G}^F)$, use in addition that $Z(\mathbb{G}^F) \subseteq \mathbb{T}^F$ and then $\big(UZ(\mathbb{G}^F)\big) \cap \big(U^-\mathbb{T}^F\big) = Z(\mathbb{G}^F) \cap \mathbb{T}^F = Z(\mathbb{G}^F)$.

CHAPTER 2

Non-existence of integral Hopf orders for twists of several simple groups of Lie type

In this chapter, we apply the strategy expounded in Section 6 to several groups, which are either of the form $\mathbb{G}^F$ or $\mathbb{G}^F/Z(\mathbb{G}^F)$, for $\mathbb{G}$ a matrix group.

1. Statement

The aim of this chapter is to establish the following results:

THEOREM 2.1.1. *Let K be a number field and $R \subset K$ a Dedekind domain such that $\mathcal{O}_K \subseteq R$. Let*

- *p be a prime number and $q = p^m$ with $m \geq 1$.*
- *G be one of the following finite quasisimple groups: $\mathbf{SL}_2(q), \mathbf{PSL}_2(q)$, $\mathbf{SL}_3(q)$, $\mathbf{PSL}_3(q)$ and the Suzuki group ${}^2B_2(q)$ (here, $p = 2$ and m is odd).*
- *M be any abelian p-subgroup of central type of G.*
- *$\omega : \widehat{M} \times \widehat{M} \to K^\times$ be any non-degenerate cocycle.*

If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.

PROOF. The proof will be carried out in Section 3. $\square$

THEOREM 2.1.2. *Let K be a number field and $R \subset K$ a Dedekind domain such that $\mathcal{O}_K \subseteq R$. Let*

- *p be a prime number and $q = p^m$ with $m \geq 1$.*
- *G be one of the following finite simple groups: $\mathbf{PSL}_2(q)$ or the Janko group*
- *M be any subgroup isomorphic to the Klein four group.*
- *$\omega : \widehat{M} \times \widehat{M} \to K^\times$ be any non-degenerate cocycle.*

If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.

PROOF. The proof will be carried out in Section 4. $\square$

THEOREM 2.1.3. *Let K be a number field and $R \subset K$ a Dedekind domain such that $\mathcal{O}_K \subseteq R$. Let*

- *p be a prime number and $q = p^m$ with $m \geq 1$.*
- *G be one of the following finite simple groups: $\mathbf{PSL}_2(q)$, the Janko group and the Suzuki group ${}^2B_2(q)$ (here, $p = 2$ and m is odd).*
- *M be any abelian subgroup of central type of G.*
- *$\omega : \widehat{M} \times \widehat{M} \to K^\times$ be any non-degenerate cocycle.*

If the twisted Hopf algebra $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over any number ring contained in K.

Proof. The proof will be carried out in Section 5. □

In light of Remark 1.3.4, we need to classify all abelian p-subgroups of central type up to an automorphism of G for proving Theorem 2.1.1. Similarly, for Theorem 2.1.2 we need to classify all the subgroups of G isomorphic to the Klein four groups $C_2 \times C_2$ up to automorphisms of G. Finally, for Theorem 2.1.3, we need a classification of all abelian subgroups of central type, up to automorphisms of G.

Before tackling the proofs of Theorem 2.1.1, Theorem 2.1.2 and Theorem 2.1.3 we record the following consequence. Its proof is similar to that of [14, Corollary 2.4]. One only has to add the fact that, up to coboundaries, ω can be chosen in such a way that its image is contained in a cyclotomic number field, as we have seen in Subsection 3.2.

Corollary 2.1.4. *Let (G, M, ω) be as Theorem 2.1.1 or as in Theorem 2.1.2. Then, the complex semisimple Hopf algebra $(\mathbb{C}G)_{\Omega_{M,\omega}}$ does not admit a Hopf order over any number ring.*

2. Classification of abelian subgroups of central type

The aim of this section is to classify:

- the abelian p-subgroups of central type the groups listed in Theorem 2.1.1, up to automorphisms;
- the subgroups isomorphic to the Klein four group of the groups listed in Theorem 2.1.2, up to automorphisms;
- all abelian subgroups of central type of the groups listed in Theorem 2.1.3, up to automorphisms.

Throughout these sections, the centralizer of an element g in a group G is denoted by $C(g)$ or by $C_G(g)$, when we need to specify the group we are considering. In the same way, we write $C(L)$ for referring to the centralizer of a subgroup L of G.

2.1. Projective special linear group $\mathbf{PSL}(2,q)$. Let $q = p^m$, with p prime and $m \geq 1$. We denote by $\pi : \mathbf{SL}_2(q) \to \mathbf{PSL}_2(q)$ the natural projection. The classification of all subgroups of $\mathbf{PSL}_2(q)$, which dates from the beginning of last century, can be consulted in [64, Theorem 6.25] or [44, Theorem 2.1]. These theorems bring to light that the only abelian subgroups of central type of $\mathbf{PSL}_2(q)$ are: p-groups of square order or Klein four-groups. In this section we give a self-contained proof of this and we find the relation between these subgroups via conjugation or automorphisms.

We start by recalling some facts about $\mathbf{SL}_2(q)$ that we will draw heavily on in the sequel. We used as references [6, pages 3-9], for q odd, and [37, pages 324-326 and 336], for q even.

We have that

$$U := \{ \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{F}_q \}$$

is a Sylow p-subgroup of $\mathbf{SL}_2(q)$, which is elementary abelian. For $t \in \mathbb{F}_q^\times$ we denote by $d(t)$ the diagonal matrix $\mathrm{diag}(t, t^{-1})$, so that

$$T := \left\{ d(t) : t \in \mathbb{F}_q^\times \right\}.$$

We next fix a non-split torus T' of $\mathbf{SL}_2(q)$. It is constructed by realizing the elements of norm 1 of the field extension $\mathbb{F}_{q^2}/\mathbb{F}_q$ as matrices of size 2 in the following way:

Case q odd. Let $\epsilon \in \mathbb{F}_q$ be a non-square element. Take $\zeta \in \mathbb{F}_{q^2}$ such that $\zeta^2 = \epsilon$. Every element of $\mathbb{F}_{q^2}$ is of the form $a + b\zeta$, with $a, b \in \mathbb{F}_q$. The following map is an algebra morphism:

$$d' : \mathbb{F}_{q^2} \to \mathrm{M}_2(\mathbb{F}_q),\ a + b\zeta \mapsto \left(\begin{smallmatrix} a & b \\ \epsilon b & a \end{smallmatrix}\right).$$

We set:

$$T' = \{ d'(a + b\zeta) : (a + b\epsilon)(a - b\epsilon) = 1 \}.$$

Case q even. Take now $\zeta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then, $\zeta + \zeta^q$ and ζ^{1+q} belong to $\mathbb{F}_q$ and the following map is an algebra morphism:

$$d' : \mathbb{F}_{q^2} \to \mathrm{M}_2(\mathbb{F}_q),\ a + b\zeta \mapsto \left(\begin{smallmatrix} a & b \\ b\zeta^{1+q} & a+b(\zeta+\zeta^q) \end{smallmatrix}\right).$$

We set:

$$T' := \{ d'(a + b\zeta) : (a + b\zeta)(a + b\zeta^q) = 1 \}.$$

We will use the following facts in the proof of the next proposition:

(1) The split and non-split torus T and T' are cyclic groups of orders $q-1$ and $q+1$ respectively.
(2) Every non-central element of $\mathbf{SL}_2(q)$ is conjugate to either $\pm u$, with $u \in U$, an element in T or in T'.
(3) Let $g \in \mathbf{SL}_2(q)$ be non-central. Then, $C(g) = \{\pm 1\}U$ if $g \in \{\pm 1\}U$, if $g \in T$ then $C(g) = T$ and $C(g) = T'$ if $g \in T'$.

(4) Every element of order coprime with p (i.e., semisimple) is conjugate to an element of $T \cup T'$.

To describe the action of $\mathrm{Aut}(\mathbf{PSL}_2(q))$ on the set of subgroups of central type of $\mathbf{PSL}_2(q)$, we view $\mathbf{PSL}_2(q)$ inside $\mathbf{PGL}_2(q)$ as the image of $\mathbf{SL}_2(q)$ through the canonical projection $\mathbf{GL}_2(q) \twoheadrightarrow \mathbf{PGL}_2(q)$. Under this identification, $\mathbf{PSL}_2(q) = \mathbf{PGL}_2(q)$ if q is even, and, if q is odd, $\mathbf{PSL}_2(q)$ is the unique proper normal subgroup of $\mathbf{PGL}_2(q)$, see [63, Section 1]. The action by conjugation of $\mathbf{PGL}_2(q)$ on $\mathbf{PSL}_2(q)$ gives rise to an injective group homomorphism $\mathbf{PGL}_2(q) \to \mathrm{Aut}(\mathbf{PSL}_2(q))$.

Proposition 2.2.1. *Let M be a non-trivial abelian subgroup of central type of $\mathbf{PSL}_2(q)$. Then, M is one of the following subgroups:*

(i) A subgroup of $\pi(U)$ of square order, up to conjugation.

(ii) A subgroup isomorphic to the Klein four group. Moreover, when q is odd, there is a single orbit for the action of $\mathbf{PGL}_2(q)$ (and thus of $\mathrm{Aut}(\mathbf{PSL}_2(q))$) on the set consisting of such subgroups.

Proof. The proof is divided into two parts. In the first part we describe the form of an abelian subgroup of central type. In the second part we deal with the statement about the orbit for the action on the set of subgroups isomorphic to the Klein four group.

1. Description of M. We first show that M must be either a p-group or a 2-group. The justification of this assertion will cover item (i).

Since M is abelian of central type, we know that $M \simeq E \times E$ for some subgroup E. Let r be a prime divisor of $|E|$. We will see that $r = 2$ or $r = p$. Let $\bar{g}, \bar{h}$ be elements of M, one in each copy of E, such that $\mathrm{ord}(\bar{g}) = \mathrm{ord}(\bar{h}) = r$. Then, $\bar{g}$ and $\bar{h}$ commute and $\bar{h} \notin \langle \bar{g} \rangle$. Put $\bar{g} = \pi(g)$ and $\bar{h} = \pi(h)$ for some $g, h \in \mathbf{SL}_2(q)$.

We distinguish two cases:

I. Case q even. Every element of $\mathbf{SL}_2(q)$ is conjugate to an element of U, T or T'. Suppose that g were conjugate to an element of T. We would have that $C(g) = T$ and that g and h generate a non-cyclic subgroup of $C(g)$. This is not possible because T is cyclic. The same argument applies if g were conjugate to an element of T'. Assume that g is conjugate to an element u of U. Then, M is conjugate to a subgroup of $C(u)$. The latter equals U. Hence, $r = 2$ and M is conjugate to a 2-group of square order. This establishes item (i) for q even.

II. Case q odd. Every element of $\mathbf{SL}_2(q)$ is conjugate to an element of the following form: $\pm u$, with $u \in U$, $d(t)$ or $d'(a + b\zeta)$. The elements g and h^2 commute and g is non-central. Proceed as before with these two elements and the subgroup generated by them. Take into account that $C(u)$ is now $\{\pm 1\}U$ for $u \in U$ with $u \neq 1$. We obtain that $h^2 = 1$ or $h^{4p} = 1$. Hence, $r = 2$ or $r = p$.

Suppose that p divides $|E|$. We take $\bar{g}$ and $\bar{h}$ of order p. Then, g is conjugate to u or $-u$, for some $u \in U$, and M is conjugate to a subgroup of

$\pi(C(u))$. As the latter equals $\pi(U)$, item (i) follows for q odd. On the other hand, if p does not divide $|E|$, then, according to the previous paragraph, the only prime divisor of $|E|$ is 2, and every non-trivial element of M has order 2. That is, M is an elementary abelian 2-group.

For the rest of the proof, we assume that p is odd and M is an elementary abelian 2-group. We know that every element of $\mathbf{PSL}_2(q)$ of order 2 is conjugate to an element in $\pi(T \cup T')$. By reason of orders, $\pi(T \cup T')$ has a unique element of order 2. Up to conjugation, we can assume that M contains such an element which we denote again by $\bar{h}$. We now distinguish two cases for q:

A. Case $q \equiv_4 1$. In this case, $\mathbb{F}_q$ has a primitive fourth root of unity, say η. Suppose that $\bar{h} = \pi(d(\eta)) = \pi\left(\begin{smallmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{smallmatrix}\right)$. One can check that the centralizer of $\bar{h}$ is $\pi(T \cup \rho T)$, where $\rho = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then, $\bar{g} = \pi\left(\begin{smallmatrix} 0 & \alpha \\ -\alpha^{-1} & 0 \end{smallmatrix}\right)$, for some $\alpha \in \mathbb{F}_q^\times$. We have that M is contained in the centralizer $C(\langle \bar{g}, \bar{h} \rangle)$ of $\langle \bar{g}, \bar{h} \rangle$. A direct calculation shows the equality $C(\langle \bar{g}, \bar{h} \rangle) = \langle \bar{g}, \bar{h} \rangle$, so $M = \langle \bar{g}, \bar{h} \rangle$ and M is a Klein four group.

B. Case $q \equiv_4 -1$. In this case, -1 is not a square in $\mathbb{F}_q$. We define the non-split torus T' by $\zeta \in \mathbb{F}_{q^2}$ such that $\zeta^2 = -1$. The only element of order 2 in $\pi(T \cup T')$ is now $\bar{h} = \pi(d'(\zeta)) = \pi\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Consider the following subset of $\mathbf{SL}_2(q)$:

$$S := \left\{ \left(\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right) : x, y \in \mathbb{F}_q \text{ and } x^2 + y^2 = -1 \right\}.$$

Notice that $|S| = q + 1$. One can verify that the centralizer of $\bar{h}$ equals $\pi(T' \cup S)$. Then, $\bar{g} = \pi\left(\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right)$, for some $x, y \in \mathbb{F}_q$ as above. The equality $C(\langle \bar{g}, \bar{h} \rangle) = \langle \bar{g}, \bar{h} \rangle$ holds in this case as well. It implies that $M = \langle \bar{g}, \bar{h} \rangle$ and M is a Klein four group.

2. Transitivity of the actions on the Klein four-groups. Let $\mathcal{M}$ denote the set consisting of subgroups of $\mathbf{PSL}_2(q)$ that are isomorphic to the Klein four group. Bear in mind our identification of $\mathbf{PSL}_2(q)$ with a normal subgroup of $\mathbf{PGL}_2(q)$. We will prove that the action by conjugation of $\mathbf{PGL}_2(q)$ on $\mathcal{M}$ is transitive. This will imply that the action of $\mathrm{Aut}(\mathbf{PSL}_2(q))$ is as well. It will suffice to check that the following inequality holds for $M \in \mathcal{M}$:

$$|\mathcal{M}| \leq \frac{|\mathbf{PGL}_2(q)|}{|\mathrm{Stab}(M)|} = \frac{|\mathbf{PGL}_2(q)|}{|\mathrm{N}_{\mathbf{PGL}_2(q)}(M)|}.$$

This will be actually an equality as there will be only one orbit for the action. The cardinality of $\mathcal{M}$ is $\frac{|\mathbf{PSL}_2(q)|}{12}$, see [64, Exercise 5(c), page 417]. With the information available in this proof, this can be deduced from the fact that the centralizer of $\bar{h}$ is isomorphic to a dihedral group of order $q-1$ when $q \equiv_4 1$ and of order $q+1$ when $q \equiv_4 -1$. Hence, we will need to verify that

$$\frac{q(q^2-1)}{24} |\mathrm{N}_{\mathbf{PGL}_2(q)}(M)| \leq q(q^2-1),$$

i.e., that $|\mathrm{N}_{\mathbf{PGL}_2(q)}(M)| \leq 24$. This inequality can be attained in the following way. The action of $\mathrm{N}_{\mathbf{PGL}_2(q)}(M)$ on the set $\{\bar{g}, \bar{h}, \bar{g}\bar{h}\}$ of non-trivial elements in M induces a group homomorphism $\mathrm{N}_{\mathbf{PGL}_2(q)}(M) \to \mathbb{S}_3$ whose kernel is the centralizer $C_{\mathbf{PGL}_2(q)}(M)$ of M in $\mathbf{PGL}_2(q)$. A direct calculation shows that $C_{\mathbf{PGL}_2(q)}(M) = M$. Therefore, $|\mathrm{N}_{\mathbf{PGL}_2(q)}(M)| \leq 4|\mathbb{S}_3| = 24$. This establishes the second part of the statement of (ii) and finishes the proof. $\square$

Remark 2.2.2. The number of conjugacy classes in $\mathbf{PSL}_2(q)$ of subgroups isomorphic to the Klein four group is one if $q \equiv_8 \pm 3$ and two if $q \equiv_8 \pm 1$; see [44, Theorem 2.1, items (j) and (k)] or [64, Exercise 5(d), page 417].

Remark 2.2.3. The group of diagonal matrices in $\mathbf{GL}_2(q)$ acts by conjugation on $\mathbf{SL}_2(q)$, on U, and on the set of subgroups of U of central type. The orbit of any non-trivial such subgroup has a representative containing the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Let M be one of these representatives. Then, $M = \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{E}\}$, where $\mathbb{E}$ is an additive subgroup of $\mathbb{F}_q$ isomorphic to C_p^{2n} for some $n > 0$. Our choice of M ensures that $\mathbb{F}_p \subset \mathbb{E}$.
In addition, since $U \simeq \pi(U)$, an abelian p-subgroup of central type of $\mathbf{PSL}_2(q)$ contained in $\pi(U)$ arises from an abelian p-subgroup of central type of U in $\mathbf{SL}_2(q)$. Hence, we can assume that $\pi(M) = \{\pi\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{E}\}$, where $\mathbb{E}$ is an additive subgroup of $\mathbb{F}_q$ isomorphic to C_p^{2n} for some $n > 0$.

2.2. Special linear group $\mathbf{SL}_3(q)$ and projective special linear group $\mathbf{PSL}_3(q)$. Let $q = p^m$, with p prime and $m \geq 1$. Consider the group $\mathbf{SL}_3(q)$. A Sylow p-subgroup of $\mathbf{SL}_3(q)$ is given by

$$U = \left\{ \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix}\right) : a, b, c \in \mathbb{F}_q \right\}.$$

We consider the following subgroups of U:

$$M_1 = \left\{ \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) : a, b \in \mathbb{F}_q \right\}, \ M_2 = \left\{ \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) : a, b \in \mathbb{F}_q \right\}.$$

The subgroups M_1 and M_2 are maximal abelian p-subgroups of U, since $C(M_1) = M_1$ and $C(M_2) = M_2$. In addition, if p is odd then M_1 and M_2 are elementary abelian; if p is even the subgroup M_1 is elementary abelian, while $M_2 \simeq C_4^m$. The latter isomorphism is obtained by counting the number of elements in M_2 of order 2 and 4.
Moreover, let J be the monomial matrix with 1's on the antidiagonal and consider the automorphism

$$\Psi\colon \mathbf{SL}_3(q) \to \mathbf{SL}_3(q), \ A \mapsto J\,{}^t(A^{-1})J^{-1}, \tag{2.2.1}$$

where ^{t} denotes the tranpose matrix.
Recall that the conjugation through an element in $\mathbf{GL}_3(q)$ induces an automorphism of the group $\mathbf{SL}_3(q)$.
We are in a position to prove the following:

PROPOSITION 2.2.4. *Let $\tilde{M}$ be an abelian p-subgroup of central type of $\mathbf{SL}_3(q)$. Then $\tilde{M}$ is isomorphic through an automorphism of $\mathbf{SL}_3(q)$ to a subgroup of central type of M_1 or M_2.*

PROOF. In virtue of Sylow's theorem, we can assume that $\tilde{M} \leq U$.
Let $\left(\begin{smallmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right) \in \tilde{M}$, for $x, y, z \in \mathbb{F}_q$.
i) If $xz \neq 0$, we can conjugate the above element to $\left(\begin{smallmatrix} 1 & z & zyx^{-1} \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right)$, using the matrix

$$g = \left(\begin{smallmatrix} z & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{smallmatrix}\right) \in N_G(U)$$

in $\mathbf{GL}_3(q)$. Thus we may assume $z = x$. Moreover, since the centralizer of $\left(\begin{smallmatrix} 1 & z & zyx^{-1} \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right)$ is M_2, then $\tilde{M} \leq M_2$.
ii) If $z = 0$ and $xy \neq 0$, then the centralizer of $\left(\begin{smallmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ is M_1 and hence $\tilde{M} \leq M_1$. If $x = 0$ and $yz \neq 0$ then the centralizer of the element $\left(\begin{smallmatrix} 1 & 0 & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right)$ is $\tilde{M}_1 = \left\{\left(\begin{smallmatrix} 1 & 0 & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right), a, b \in \mathbb{F}_q\right\}$, which is mapped to M_1 through the automorphism Ψ of $\mathbf{SL}_3(q)$ defined in (2.2.1).
iii) If each element in $\tilde{M}$ is of the form $\left(\begin{smallmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, then $\tilde{M} \leq M_1 \cap M_2$ and we are done.
If each element in $\tilde{M}$ is of the form $\left(\begin{smallmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, then $\tilde{M} \leq M_1$.
Finally, if each element in $\tilde{M}$ is of the form $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right)$, then $\Psi(\tilde{M}) \leq M_1$. $\square$

REMARK 2.2.5. If $q = 2^m$, then M_2 is of central type if and only if m is even, i.e. if and only if $2^m \equiv_3 1$.

Denote by π the projection $\pi\colon \mathbf{SL}_3(q) \to \mathbf{PSL}_3(q)$. Recall that the kernel of π is trivial if 3 does not divide q and it is isomorphic to C_3 if $q \equiv_3 1$. In particular, if $\ker \pi \neq \{1\}$ then $\mathbb{F}_q$ contains a third root of unit θ that we fix once and for all.

COROLLARY 2.2.6. *Let $\tilde{M}$ be an abelian p-subgroup of central type of $\mathbf{PSL}_3(q)$. Then $\tilde{M}$ is isomorphic through an automorphism of $\mathbf{PSL}_3(q)$ to a subgroup of central type of $\pi(M_1)$ or $\pi(M_2)$.*

PROOF. Since $U \simeq \pi(U)$, then every abelian p-subgroup of central type in $\mathbf{PSL}_3(q)$ is of the form $\pi(N)$, for N an abelian p-subgroup of central type of $\mathbf{SL}_3(q)$. The result follows from Proposition 2.2.4. $\square$

REMARK 2.2.7. Let $\tilde{M} \leq M_1$ and assume $\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in \tilde{M}$, with $ab \neq 0$. Then, there is an automorphism of $\mathbf{SL}_3(q)$ mapping $\tilde{M}$ to a subgroup M of

M_1 containing the element $\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, namely conjugation by $g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -a & 0 \\ 0 & 0 & b \end{pmatrix} \in$ $\mathbf{GL}_3(q)$

REMARK 2.2.8. Let $\tilde{M} \leq M_2$. Assume that $p \neq 2, 3$ and that $\begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \in \tilde{M}$, for some $a \neq 0$. Then, we can conjugate it to the element $\begin{pmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{pmatrix}$ by the element $\begin{pmatrix} \frac{-2a}{3} & -2a+\frac{b}{a} & 0 \\ 0 & 1 & 1 \\ 0 & 0 & \frac{-3}{2a} \end{pmatrix} \in \mathbf{SL}_3(q)$. The automorphism given by conjugation through g preserves U and M_2.
Observe that if $p = 3$ then the element $\begin{pmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{pmatrix}$ is the identity and hence it belongs to $\tilde{M}$.

2.3. The Suzuki group ${}^2B_2(q)$. Before collecting all the necessary information on all abelian subgroups of central type for the Suzuki group ${}^2B_2(q)$, we recall its construction from [62, Section 13]. In this case, $q = 2^{2n+1}$ with $n \geq 1$. Consider the Frobenius automorphism Fr_2 of $\mathbb{F}_q$. Set $\vartheta = \mathrm{Fr}_2^{n+1}$. Then, $\vartheta^2 = \mathrm{Fr}_2$ and the fixed field $(\mathbb{F}_q)^\vartheta$ equals $\mathbb{F}_2$. The following remark is useful to work with Equation (2.2.2) below:

REMARK 2.2.9. Observe that:

(1) If $a \in \mathbb{F}_q$ satisfies $a\vartheta(a) = 1$, then $1 = \vartheta(a)a^2$. Hence, $a = a^2$ and, consequently, $a \in \mathbb{F}_2$.
(2) The map $\Phi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ given by $a \mapsto a\vartheta(a)$, is an isomorphism.

The group ${}^2B_2(q)$ was defined in [62] as a subgroup of $\mathbf{SL}_4(\mathbb{F}_q)$ generated by matrices of a certain type. The first family of such matrices is the following:

$$u(a, b) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ a\vartheta(a) + b & \vartheta(a) & 1 & 0 \\ a^2\vartheta(a) + ab + \vartheta(b) & b & a & 1 \end{pmatrix}, \qquad a, b \in \mathbb{F}_q.$$

These matrices satisfy the multiplication rule:

$$u(a, b)u(a', b') = u(a + a', a\vartheta(a') + b + b').$$

Let U denote the subgroup of $\mathbf{SL}_4(\mathbb{F}_q)$ that they generate. We have that $|U| = q^2$. Moreover, U enjoys the following properties, see [62, Lemma 1]:

(1) U has exponent 4.
(2) The center of U is generated by the elements $u(0, b)$, with $b \in \mathbb{F}_q$. It is an elementary abelian 2-group of order q.
(3) An element of U is an involution if and only if it belongs to $Z(U)$.

The second family of matrices is parameterized by $\kappa \in \mathbb{F}_q^\times$. They are:

$$t_\kappa := \mathrm{diag}(a_1, a_2, a_2^{-1}, a_1^{-1}), \quad \text{with } \vartheta(a_1) = \kappa\vartheta(\kappa) \text{ and } \vartheta(a_2) = \kappa.$$

They form a subgroup T of $\mathbf{SL}_4(\mathbb{F}_q)$, which is isomorphic to $\mathbb{F}_q^\times$. The following formula holds:

$$t_\kappa^{-1} u(a,b) t_\kappa = u(a\kappa, b\kappa\vartheta(\kappa)). \tag{2.2.2}$$

In particular, T normalizes U. The subgroup TU is isomorphic to the semidirect product $T \ltimes U$. Finally, let τ be the monomial matrix with 1's on the antidiagonal. The Suzuki group ${}^2B_2(q)$ is the subgroup of $\mathbf{SL}_4(\mathbb{F}_q)$ generated by U, T, and τ. We have ([62, Theorem 7]):

$$\left|{}^2B_2(q)\right| = q^2(q-1)(q^2+1).$$

The subgroup U is a Sylow 2-subgroup of ${}^2B_2(q)$ by [62, Theorem 7]. Therefore, all non-trivial involutions are conjugate to some $u(0,b)$. By Remark 2.2.9(2) and (2.2.2), all non-trivial involutions are conjugate to $u(0,1)$. By [62, Propositions 1, 2, and 3], the centralizer of a non-trivial element $u(a,b)$ is contained in U.

It can be checked that every element of ${}^2B_2(q)$ leaves invariant the bilinear form defined by τ. This permits to regard ${}^2B_2(q)$ as a subgroup of the symplectic group $\mathbf{Sp}_4(\mathbb{F}_q)$. The description of the Steinberg endomorphism giving rise to ${}^2B_2(q)$ can be found in [56, 57] and [11, Section 12.3].

In this subsection, the data for our setting are: $G = {}^2B_2(q)$, and U and τ as above. The following lemma and Remark 1.3.4 will allow us to take M as a subgroup of $Z(U)$:

LEMMA 2.2.10. *Let M be an abelian 2-subgroup of ${}^2B_2(q)$ of central type. Then, M is conjugate to a subgroup of $Z(U)$. In particular, M is generated by involutions.*

PROOF. By Sylow's theorem, M is conjugate to a subgroup of U. Bear in mind that U has exponent 4. Since M is of central type, $M \simeq E \times E$ for some group E. We next see that E does not have an element of order 4. If it were so, U would contain a subgroup isomorphic to $C_4 \times C_4$. Pick $u(a,b)$ and $u(a',b')$ two generators of such a subgroup. They have order 4, so necessarily $aa' \neq 0$. Furthermore, they commute. This means:

$$u(a'+a, a'\vartheta(a) + b' + b) = u(a+a', a\vartheta(a') + b + b').$$

This gives $a'\vartheta(a) = a\vartheta(a')$. Then, $a'a^{-1} = \vartheta(a'a^{-1})$. Thus, $a'a^{-1} \in \mathbb{F}_2$, which implies $a' = a$. But, then $a + a' = 0$ and the element $u(a,b)u(a',b') = u(0, a\vartheta(a) + b + b')$ has order 2 and not 4, a contradiction. Therefore, M has exponent 2. By the properties of U recalled before, M is conjugate to a subgroup of $Z(U)$. □

The next result shows that there are no other abelian subgroups of central type:

PROPOSITION 2.2.11. *Every non-trivial abelian subgroup of central type M of ${}^2B_2(q)$ is a 2-group.*

Proof. This follows from the knowledge of the structure of the Sylow subgroups of ${}^2B_2(q)$. By [35, Theorem 3.9, page 189], for p odd, every Sylow p-subgroup of ${}^2B_2(q)$ is cyclic. Now, write $M \simeq E \times E$ for some subgroup E. Let r be a prime divisor of $|E|$. Two elements of order r, one in each copy of E, generate a non-cyclic subgroup of order r^2. This is not possible if r is odd, as such a subgroup must be contained in a Sylow r-subgroup of ${}^2B_2(q)$, that is cyclic. □

2.4. The Janko group. We firstly recall the definition of the Janko group from [39] .
Let G be the subgroup of $\mathbf{GL}_7(11)$ generated by the following matrices:

$$A = \begin{pmatrix} 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0 \end{pmatrix} \qquad B = \begin{pmatrix} -3&2&-1&-1&-3&-1&-3\\ -2&1&1&3&1&3&3\\ -1&-1&-3&-1&-3&-3&2\\ -1&-3&-1&-3&-3&2&-1\\ -3&-1&-3&-3&2&-1&-1\\ 1&3&3&-2&1&1&3\\ 3&3&-2&1&1&3&1 \end{pmatrix}.$$

The group G is called the Janko group. We recollect the following properties of G (see [38] and [39]) :

i) G is a simple group;
ii) G has order $11(11^3-1)(11+1) = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$;
iii) G contains an involution t such that $C_G(t) = \langle t \rangle \times F$, where $F \simeq A_5$;
iv) All the involutions of G are conjugate;
v) Any Sylow 2-subgroup of G is elementary abelian of order 8;
vi) For p odd, the p-Sylow subgroups are cyclic;
vii) G has no subgroup of index 2.

In the following proposition, we describe the abelian subgroups of central type of the Janko group.

Proposition 2.2.12. *Let M be a non trivial subgroup of central type of G. Then M is isomorphic to the Klein four group. Moreover, all the subgroups of G isomorphic to the Klein four group form a single orbit for the action of G by conjugation.*

Proof. By properties v) and vi), we deduce that the only abelian subgroups of central type are the Klein four groups. We need to verify that such subgroups are all conjugate.
Let x, y be two involutions such that $x \neq y$ and $xy = yx$. Consider, the subgroup $M_1 = \langle x, y \rangle$. It is enough to prove that M_1 is conjugate to a subgroup $M_2 = \langle t, s \rangle$, with t the involution such that $C_G(t) = \langle t \rangle \times F$ and $s \in F$. Notice that the latter involution t exists by Property iii). Since all involutions are conjugate in G, there exists $g \in G$ such that $gxg^{-1} = t$. Hence $gM_1g^{-1} = \langle t, gyg^{-1} \rangle$. Now, $gyg^{-1} \in C_G(t)$, that is $gyg^{-1} = t^a f$, for some $f \in F$ and for $a \in \{0, 1\}$. Therefore, $gM_1g^{-1} = \langle t, tf \rangle = \langle t, f \rangle$. Since in $F \simeq A_5$ all the involutions are conjugate, there exists $f_1 \in F$ such that

$f_1 f f_1^{-1} = s$. Thus, $f_1 g M_1 g^{-1} f_1^{-1} = \langle f_1 t f_1^{-1}, f_1 f f_1^{-1}\rangle = \langle t, s\rangle$. This concludes the proof. $\square$

3. Proof of Theorem 2.1.1

The goal of this section is to prove Theorem 2.1.1.
Each subsection aims at proving the conclusion of Theorem 2.1.1 for each group listed in there.

3.1. Special linear group $\mathbf{SL}_2(q)$. Retain notation from Subsection 2.1 and let $G = \mathbf{SL}_2(q)$. In light of Remark 2.2.3, we can assume that an abelian subgroup of central type in U is of the form

$$M = \left\{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{E}\right\},$$

where $\mathbb{E}$ is an additive subgroup of $\mathbb{F}_q$ isomorphic to C_p^{2n}, containing $\mathbb{F}_p$.
Recall that $T = \left\{\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) : t \in \mathbb{F}_q^\times\right\}$ and $B = \langle T, U\rangle \simeq T \ltimes U$. Furthermore, we pick the element $\tau = \sigma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ in $N_G(T)$. Using Equation (1.6.3), one can check that the non-zero values of $\chi = \mathrm{Ind}_U^G(\mathbb{1}_U)$ are:

$$\chi(1) = q^2 - 1 \quad \text{and} \quad \chi\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) = q - 1, \quad \text{for } a \neq 0.$$

In this case, the sets P and I_χ particularize to

$$P = \{A \in \mathbf{SL}_2(q) : \mathrm{Tr}(A) = 2\}, \text{ and } I_\chi = \{\{1\}, P \setminus \{1\}\}.$$

Let $P^\bullet = P \setminus \{1\}$. A direct calculation shows that $M_{P^\bullet} = \{1\}$ if $p = 2$ and $M_{P^\bullet} = \{\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)\}$ otherwise. We stress that $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right) \in M$ thanks to our choice of M. Equation (1.6.7) takes the following concrete form:

$$\begin{aligned}
\chi(y_\chi^2) &= \frac{\chi(P^\bullet)^2}{|M|} \sum_{v \in M} \chi\Big(\tau \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)^2 v \tau v^{-1}\Big) \\
&= \frac{(q-1)^2}{p^{2n}} \sum_{a \in \mathbb{E}} \chi\Big(\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -a \\ 0 & 1 \end{smallmatrix}\right)\Big) \\
&= \frac{(q-1)^2}{p^{2n}} \sum_{a \in \mathbb{E}} \chi\left(\begin{smallmatrix} -1 & a \\ 4+a & -1-4a-a^2 \end{smallmatrix}\right).
\end{aligned}$$

Observe that $\left(\begin{smallmatrix} -1 & a \\ 4+a & -1-4a-a^2 \end{smallmatrix}\right) \in P$ if and only if $a = -2$. Then, the only non-zero term in this sum corresponds to $a = -2$. Its value is $q^2 - 1$ if $p = 2$ and $q - 1$ otherwise. Hence:

$$\chi(y_\chi^2) = \frac{(q-1)^3(q+1)}{p^{2n}} \text{ if } p = 2 \quad \text{and} \quad \chi(y_\chi^2) = \frac{(q-1)^3}{p^{2n}} \text{ if } p \neq 2.$$

In both cases, $\chi(y_\chi^2)$ is an irreducible fraction. Propositions 1.4.2 and 1.3.7, together with Bezout's identity, yield $\frac{1}{p^{2n}} = \frac{1}{|M|} \in R$.

This finishes the proof of Theorem 2.1.1 for $\mathbf{SL}_2(q)$. $\square$

3.2. Projective special linear group $\mathbf{PSL}_2(q)$. We assume that p is odd, since otherwise $\mathbf{PSL}_2(q) = \mathbf{SL}_2(q)$ and this case was just treated.
We denote $\mathbf{PSL}_2(q)$ by G. By Let M be an abelian p-subgroup of G of central type. By Remark 2.2.3, we can assume that an abelian p-subgroup of central type M of G is of the form $\{\pi\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{E}\}$, with $\mathbb{E}$ an additive subgroup of $\mathbb{F}_q$ isomorphic to C_p^{2n} and containing $\mathbb{F}_p$.

Our element τ is now $\pi\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. We take $\chi = \mathrm{Ind}_{\pi(U)}^G(\mathbb{1}_{\pi(U)})$. One can check that the non-zero values of χ are:

$$\chi(1) = \frac{q^2-1}{2} \qquad \text{and} \qquad \chi(\pi\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)) = \frac{q-1}{2}, \quad \text{for } a \neq 0.$$

One can also verify that, in this case, $P = \{\pi(A) \in \mathbf{PSL}_2(q) : \mathrm{Tr}(A) = \pm 2\}$. Then, $I_\chi = \{\{1\}, P \setminus \{1\}\}$. Set, as before, $P^\bullet = P \setminus \{1\}$. A direct calculation shows that $M_{P^\bullet} = \{\pi\left(\begin{smallmatrix} 1 & \pm 2 \\ 0 & 1 \end{smallmatrix}\right)\}$. Equation (1.6.7) now reads as:

$$\chi(y_\chi^2) = \frac{(q-1)^2}{4|M|}\left(2\sum_{v\in M}\chi\Big(\pi\Big(\tau v\tau v^{-1}\Big)\Big) + \sum_{v\in M}\chi\Big(\pi\Big(\tau\left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right)v\tau v^{-1}\Big)\Big)\right.$$
$$\left. + \sum_{v\in M}\chi\Big(\pi\Big(\tau\left(\begin{smallmatrix} 1 & -4 \\ 0 & 1 \end{smallmatrix}\right)v\tau v^{-1}\Big)\Big)\right). \tag{2.3.1}$$

We compute the value of the three summands between parentheses:

Firstly, an element of the form

$$\pi\Big(\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)^{-1}\Big) = \pi\left(\begin{smallmatrix} -1 & a \\ a & -1-a^2 \end{smallmatrix}\right)$$

belongs to P if and only if $a = 0$ (i.e., it is the identity element) or $a^2 = -4$. The latter occurs if and only if $\mathbb{E}$ contains a square root of -4. In such a case, both roots are in $\mathbb{E}$ and the corresponding elements of G are non-trivial and distinct. Hence, the value of the first summand is $2\chi(1) = q^2 - 1$ if $\sqrt{-4} \notin \mathbb{E}$ and $2\Big(\chi(1) + 2\chi(\pi\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right))\Big) = q^2 + 2q - 3$ otherwise.

Secondly, an element of the form

$$\pi\Big(\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)^{-1}\Big) = \pi\left(\begin{smallmatrix} -1 & a \\ 4+a & -1-4a-a^2 \end{smallmatrix}\right)$$

belongs to P if and only if $a \in \{0, -2, -4\}$. The three elements of G obtained with these values of a are all non-trivial and distinct. Hence, the second summand equals $\frac{3(q-1)}{2}$.

Finally, and in a similar fashion, an element of the form

$$\pi\Big(\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -4 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)^{-1}\Big) = \pi\left(\begin{smallmatrix} -1 & a \\ -4+a & -1+4a-a^2 \end{smallmatrix}\right)$$

belongs to P if and only if $a \in \{0, 2, 4\}$. The elements of G obtained with these three values of a are all non-trivial and distinct. The third summand equals $\frac{3(q-1)}{2}$ as well.

In total, the value of the sum in (2.3.1) is q^2+3q-4 if $\sqrt{-4}\notin\mathbb{E}$ and q^2+5q-6 otherwise. Therefore, we have:

$$\chi(y_\chi^2)=\frac{(q-1)^3}{4p^{2n}}(q+4)\ \text{ if } \sqrt{-4}\notin\mathbb{E} \quad\text{and}\quad \chi(y_\chi^2)=\frac{(q-1)^3}{4p^{2n}}(q+6)\ \text{ if } \sqrt{-4}\in\mathbb{E}.$$

In both cases, $\chi(y_\chi^2)$ belongs to $\mathbb{Q}\setminus\mathbb{Z}$. It follows from this and Propositions 1.4.2 and 1.3.7 that $\frac{1}{p^{2n}}=\frac{1}{|M|}\in R$.

This finishes the proof of Theorem 2.1.1 for $\mathbf{PSL}_2(q)$.

Remark 2.3.1. For an abelian p-subgroup M of $\mathbf{SL}_2(q)$ of central type, $\pi|_M : M\to\pi(M)$ is an isomorphism. For ω a 2-cocycle on $\widehat{M}$, the natural projection induces a surjective Hopf algebra map $\pi:(K\mathbf{SL}_2(q))_{\Omega_{M,\omega}}\to (K\mathbf{PSL}_2(q))_{\Omega_{\pi(M),\omega^\pi}}$. When q is odd, the statement for $\mathbf{SL}_2(q)$ follows from that for $\mathbf{PSL}_2(q)$ in virtue of Proposition 1.4.3(ii). We preferred to carry out the calculation for $\mathbf{SL}_2(q)$ because it leads the way to the $\mathbf{PSL}_2(q)$ case.

3.3. Special linear group $\mathbf{SL}_3(q)$. Let p be a prime number and $q=p^m$, with $m\geq 1$. Let $G=\mathbf{SL}_3(q)$. Retain notations from Subsection 2.2. Consider the maximal split torus

$$T:=\left\{\begin{pmatrix} s & 0 & 0\\ 0 & t & 0\\ 0 & 0 & t^{-1}s^{-1}\end{pmatrix} : s,t\in\mathbb{F}_q^\times\right\}.$$

Bear in mind that $N_G(U)=B=\langle T,U\rangle\simeq T\ltimes U$.

We first calculate the values at U of the character $\chi=\mathrm{Ind}_U^G(\mathbb{1}_U)$. Every element in U has a Jordan canonical form. There are two possible non-trivial canonical forms: $\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}$ (Jordan type $(2,1)$) and $\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$ (Jordan type (3)).

Lemma 2.3.2. *For $u\in U$ we have:*

$$\chi(u)=\begin{cases}(q^3-1)(q^2-1) & \text{if } u=1,\\ (2q+1)(q-1)^2 & \text{if } u \text{ is of Jordan type } (2,1),\\ (q-1)^2 & \text{if } u \text{ is of Jordan type } (3).\end{cases}$$

Proof. The value at the identity element is straightforward. The proof for the other two values is divided into three steps:

Step 1. Let $u,u'\in U$ be such that $u'=kuk^{-1}$ for some $k\in\mathbf{GL}_3(q)$. We show that $\chi(u')=\chi(u)$. We write $k=e_kd_k$, with $e_k\in G$ and $d_k\in\mathbf{GL}_3(q)$ diagonal. Notice that conjugation by a diagonal matrix in $\mathbf{GL}_3(q)$ stabilizes U. Since χ is a character of G, we get:

$$\chi(u')=\chi(e_kd_kud_k^{-1}e_k^{-1})=\chi(d_kud_k^{-1}).$$

We now compute $\chi(u')$ and $\chi(u)$ by using Equation (1.6.3):

$$\begin{aligned}\chi(u') &= \#\{g \in G : g(d_k u d_k^{-1})g^{-1} \in U\} \cdot |U|^{-1} \\ &= \#\{g \in G : d_k^{-1} g d_k u d_k^{-1} g^{-1} d_k \in U\} \cdot |U|^{-1} \qquad (\text{Put } h = d_k^{-1} g d_k) \\ &= \#\{h \in G : huh^{-1} \in U\} \cdot |U|^{-1} \\ &= \chi(u).\end{aligned}$$

In view of the preceding statement, $\chi(u) = \chi(u_{JF})$, where u_{JF} is the Jordan canonical form of u. In the next steps we calculate the value of χ at the two possible Jordan canonical forms.

Step 2. Set $u = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. We claim that $\chi(u) = (2q+1)(q-1)^2$. Let $Cl(u)$ denote the conjugacy class of u in G. Consider the orbit map $f : G/C(u) \to Cl(u)$, which sends $gC(u)$ to gug^{-1}. Taking the inverse image of $Cl(u) \cap U$ under f, we obtain the following equality:

$$\#\{g \in G : gug^{-1} \in U\} = |C(u)||Cl(u) \cap U|.$$

One can check in a direct way, by computing explicitly $C(u)$, that $|C(u)| = (q-1)q^3$. On the other hand, the Jordan type of a non-trivial element w in U can be detected by calculating the rank of $w - 1$: rank 1 corresponds to type $(2,1)$ and rank 2 to type (3). The set $Cl(u) \cap U$ consists of elements $w \in U$ that are conjugate to u. It can be shown that these are precisely the elements $w \in U$ such that $\mathrm{rk}(w-1) = 1$. There are $(2q+1)(q-1)$ matrices fulfilling this condition. Equation (1.6.3) now applies.

Step 3. Finally, set $u = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. We claim that $\chi(u) = (q-1)^2$. For, one first establishes the equality $\{g \in G : gug^{-1} \in U\} = B$ by direct manipulation with matrices and then applies Equation (1.6.3). $\square$

We can rephrase P as the set consisting of those matrices in G whose characteristic polynomial equals $(1-z)^3$. We already know that χ vanishes outside P. The value of χ at an element $g \in P$ is obtained by determining its Jordan type through the calculation of $\mathrm{rk}(g-1)$ and then applying Lemma 2.3.2. In this case, the set I_χ equals to $\{C_{(1)}, C_{(2,1)}, C_{(3)}\}$, where $C_{(1)} = \{1\}$, and $C_{(2,1)}$ and $C_{(3)}$ are the subsets of P consisting of matrices of type $(2,1)$ and of type (3) respectively.

In virtue of Proposition 2.2.4, up to automorphisms of G the abelian p-subgroups of central type of G are subgroups of M_1 or M_2. Then, for proving Theorem 2.1.1 for G, it is enough to show the non-existence of a Hopf order for cocycles of subgroups M of the following form:

i) $M \leq M_1$ and containing $\left(\begin{smallmatrix} 1 & -1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ by Remark 2.2.7;

ii) $M = \left\{ \left(\begin{smallmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) : b \in \mathbb{E} \right\}$, where $\mathbb{E}$ is an additive subgroup of $\mathbb{F}_q$ isomorphic to C_p^{2n};

iii) $M \leq M_2$, and containing $\left(\begin{smallmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ if q is odd by Remark 2.2.8.

We start then with the following:

Proposition 2.3.3. *Let M be an abelian p-subgroup of central type of M_1 containing $\left(\begin{smallmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ and let $\omega \colon \widehat{M} \times \widehat{M} \to K^{\times}$ be a non-degenerate cocycle. If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.*

Proof. We take the element $\tau = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$ in $N_G(T)$. It can be verified that $M \cap \left(\tau M \tau^{-1}\right) \subseteq M_1 \cap (\tau M_1 \tau^{-1}) = \{1\}$. We have to detect the elements $v \in M$ such that the characteristic polynomial of τv is $(1-z)^3$. This occurs if and only if $v \in \left\{ \left(\begin{smallmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right\}$. In addition, the Jordan type of τv is (3). Hence

$$M_{C_{(3)}} \subseteq \left\{ \left(\begin{smallmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right\},$$

and $M_{C_{(2,1)}} = \emptyset$. Since by assumption $\left(\begin{smallmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$, then also its third power belongs to M. Explicitly, $\left(\begin{smallmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$, so $M_{C_{(3)}} = \left\{ \left(\begin{smallmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right\}$. Notice that $M_{C_{(3)}} = \{1\}$ if $p = 3$.

For simplicity, we write $(a,b) \in M$ to mean that $\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$. Then

$$\begin{aligned}
\chi(y_\chi^2) &= \frac{\chi(C_{(3)})^2}{|M|} \sum_{\substack{v \in M \\ x \in M_{C_{(3)}}}} \chi\left(\tau x^2 v \tau v^{-1}\right) \\
&= \frac{(q-1)^4}{|M|} \sum_{(a,b) \in M} \chi\left(\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)^2 \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & -a & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right) \\
&= \frac{(q-1)^4}{|M|} \sum_{(a,b) \in M} \chi \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & -a & -b \\ b+6 & 1-ab-6a & a-b^2-6-6b \end{smallmatrix} \right).
\end{aligned}$$

The latter element belongs to P if and only if the characteristic polynomial of the above matrix equals $(1-z)^3$, i.e. the pair (a,b) is a solution of the following system of equations

$$\begin{aligned}
-b^2 - 6b - 6 &= 3 \\
a^2 - 6a + 6 &= -3,
\end{aligned}$$

and $\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$.

The unique solution of the above system is $(a,b) = (3,-3)$ and $\left(\begin{smallmatrix} 1 & 3 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$ by assumption. We now divide the treatment into two cases: q odd and q

even.
q odd. Substituting $a = -b = 3$ in the last matrix appearing in $\chi(y_\chi^2)$, we obtain a matrix of Jordan type (3). This yields to:

$$\chi(y_\chi^2) = \frac{(q-1)^6}{|M|}.$$

Since $\gcd(q-1, |M|) = 1$, we have $\frac{1}{|M|} \in R$.

q even. In this case, the last matrix appearing in $\chi(y_\chi^2)$ is of Jordan type $(2,1)$, for $(a,b) = (3,-3)$. We can then conclude that:

$$\chi(y_\chi^2) = \frac{(q-1)^6(2q+1)}{27|M|}.$$

Since $q-1$ and $2q+1$ are odd, we have $\frac{1}{|M|} \in R$. □

Proposition 2.3.4. *Let*

$$M = \left\{ \left(\begin{smallmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \, : \, b \in \mathbb{E} \right\},$$

where $\mathbb{E}$ is an additive subgroup of $\mathbb{F}_q$ isomorphic to C_p^{2k} for some $k > 0$. Let $\omega \colon \widehat{M} \times \widehat{M} \to K^\times$ be a non-degenerate cocycle. If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.

Proof. We consider the element $\tau = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{smallmatrix}\right)$. One can check that $\tau M \tau^{-1} \cap M = \{1\}$. We must find the elements $v \in M$ such that τv is a p-element, i.e. its characteristic polynomial equals to $(1-z)^3$. This happens if and only if v is the identity. Moreover, the Jordan type of τ is (3) and this implies that $M_{C_{(3)}} = \{1\}$. Then,

$$\begin{aligned}
\chi(y_\chi^2) &= \frac{\chi(C_{(3)})^2}{|M|} \sum_{v \in M} \chi\Big(\tau v \tau v^{-1}\Big) \\
&= \frac{(q-1)^4}{|M|} \sum_{b \in \mathbb{E}} \chi\left(\left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right) \\
&= \frac{(q-1)^4}{|M|} \sum_{b \in \mathbb{E}} \chi \left(\begin{smallmatrix} 1+b & b & -b^2 \\ 2+b & 1+b & -b^2-b \\ 3+b & 2+b & -2b-b^2+1 \end{smallmatrix}\right).
\end{aligned}$$

Computing the characteristic polynomial of the above matrix and forcing it to be equal to $(1-z)^3$, we get that b must solve the following equation

$$-b^2 + 3 = 3.$$

In particular, the unique solution is $b = 0$, corresponding to $v = 1$. We now proceed dividing the cases according to the parity of q.

q odd. In this case the Jordan type of $\tau v \tau v^{-1} = \tau^2$ is (3). Hence;

$$\chi(y_\chi^2) = \frac{(q-1)^6}{|M|}.$$

Since $q-1$ and $|M|$ are coprime, then $\frac{1}{|M|} \in R$.
q even. In this case the Jordan type of τ^2 is $(2,1)$. Hence

$$\chi(y_\chi^2) = \frac{(q-1)^6(2q+1)}{|M|}.$$

Since $(q-1)$ and $(2q+1)$ are odd, we have $\frac{1}{|M|} \in R$. □

PROPOSITION 2.3.5. *Let q be odd and let M be an abelian p-subgroup of central type of M_2, containing $\begin{pmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{pmatrix}$. Consider $\omega\colon \widehat{M} \times \widehat{M} \to K^\times$ a non-degenerate cocycle. If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.*

PROOF. We take the element $\tau = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. We can verify that $M_2 \cap \tau M_2 \tau^{-1} = \{1\}$ and hence $M \cap \tau M \tau^{-1} = \{1\}$. We have to find those elements $v \in M_2$ such that τv is a p-element, i.e. its characteristic polynomial is $(1-z)^3$. A direct computation shows that this happens if and only if $v = \begin{pmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{pmatrix}$ and that the Jordan type of τv is (3). This implies that:

$$M_{C_{(3)}} \subseteq \left\{ \begin{pmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

and $M_{C_{(2,1)}} = \emptyset$. Since $\begin{pmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{pmatrix} \in M$, by assumption, then

$$M_{C_{(3)}} = \left\{ \begin{pmatrix} 1 & (-3/2) & 3 \\ 0 & 1 & (-3/2) \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

Also in this case, we say that $(a,b) \in M$ if $\begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \in M$. Then

$$\begin{aligned}
\chi(y_\chi^2) &= \frac{\chi(C_{(3)})^2}{|M|} \sum_{\substack{v \in M \\ x \in M_{C_{(3)}}}} \chi\Big(\tau x^2 v \tau v^{-1}\Big) \\
&= \frac{(q-1)^4}{|M|} \sum_{(a,b) \in M} \chi\left(\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & -a & a^2-b \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{pmatrix} \right) \\
&= \frac{(q-1)^4}{|M|} \sum_{(a,b) \in M} \chi \begin{pmatrix} a-3 & 3a-a^2 & a(a^2-b)-3(a^2-b)+1 \\ 1 & -a & a^2-b \\ b-3a+\frac{33}{4} & 3a^2-ab-\frac{33}{4}a+1 & -3+(a^2-b)(b+\frac{33}{4}-3a) \end{pmatrix}.
\end{aligned}$$

With the usual criterium of the characteristic polynomial, the above element lies in P if and only if (a,b) is a solution of the following system of equations

$$\begin{aligned} &a^2-3a-\tfrac{3}{4}=-3\\ &-6+(a^2-b)(b+\tfrac{33}{4}-3a)=3, \end{aligned}$$

and $(a,b)\in M$.
The unique solution to the system is $(a,b)=(3/2,-3/4)$ and

$$\begin{pmatrix} 1 & 3/2 & -3/4\\ 0 & 1 & 3/2\\ 0 & 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & -3/2 & 3\\ 0 & 1 & -3/2\\ 0 & 0 & 1 \end{pmatrix}^{-1},$$

which belongs to M by assumption. In addition, the Jordan type of $\tau x^2 v\tau v^{-1}$ is (3). Then,

$$\chi(y_\chi^2)=\frac{(q-1)^6}{|M|}.$$

The latter is an irreducible fraction, implying that $\frac{1}{|M|}\in R$. $\square$

Proposition 2.3.6. *Let q be even and let M be an abelian p-subgroup of central type of M_2. Consider $\omega\colon \widehat{M}\times\widehat{M}\to K^\times$ a non-degenerate cocycle. If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|}\in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.*

Proof. In this case we pick the element $\tau=\left(\begin{smallmatrix} 0&0&1\\ 0&1&0\\ 1&0&0 \end{smallmatrix}\right)$. A direct computation shows that $(\tau M_2\tau^{-1})\cap M_2=\{1\}$ and hence $(\tau M\tau^{-1})\cap M=\{1\}$. An element $v\in M$ is such that τv has characteristic polynomial $(1-z)^3$ if and only if $v=1$. In particular,

$$M_{C_{(2,1)}}=\{1\}$$

while $M_{C_{(3)}}=\emptyset$. Then;

$$\begin{aligned} \chi(y_\chi^2)&=\frac{\chi(C_{(2,1)})^2}{|M|}\sum_{v\in M}\chi(\tau v\tau v^{-1})\\ &=\frac{(q-1)^4(2q+1)^2}{|M|}\sum_{(a,b)\in M}\chi\left(\left(\begin{smallmatrix} 0&0&1\\ 0&1&0\\ 1&0&0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1&a&b\\ 0&1&a\\ 0&0&1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0&0&1\\ 0&1&0\\ 1&0&0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1&a&b\\ 0&1&a\\ 0&0&1 \end{smallmatrix}\right)\right)\\ &=\frac{(q-1)^4(2q+1)^2}{|M|}\sum_{(a,b)\in M}\chi\left(\begin{smallmatrix} 1&a&a^2+b\\ a&a^2+1&a+a^3+ab\\ b&a+ab&1+a^2+a^2b+b^2 \end{smallmatrix}\right), \end{aligned}$$

where $(a,b)\in M$ means that $\left(\begin{smallmatrix} 1&a&b\\ 0&1&a\\ 0&0&1 \end{smallmatrix}\right)\in M$. Computing the characteristic polynomial of the above matrix and forcing it to be equal to $(1-z)^3$, we obtain that $(a,b)\in M$ is a 2-element if and only if the pair (a,b) is a solution of the following equation

$$1+a^2b+b^2=1. \tag{2.3.2}$$

The solutions of the above equation are $(a,0)$ for every $a\in\mathbb{F}_q$ and (a,a^2) for every $a\in\mathbb{F}_q^\times$.

If $(a, b) = (0, 0)$, the corresponding matrix showing up in the expression of $\chi(y_\chi^2)$ is the identity.
If $(a, b) = (a, 0)$ or $(a, b) = (a, a^2)$, then the corresponding matrix under consideration is of Jordan type (3) for $a \in \mathbb{F}_q^\times$.
We want to show that the number of solutions (a, b) of system (2.3.2) such that $(a, b) \in M$ is even if $a \neq 0$.
Suppose that $\left(\begin{smallmatrix} 1 & a & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$, for $a \neq 0$. Then, also its third power lies in M, explicitly

$$\left(\begin{smallmatrix} 1 & a & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right)^3 = \left(\begin{smallmatrix} 1 & a & a^2 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right),$$

i.e. $(a, a^2) \in M$.
Call N the number of pairs $(a, b) \neq (0, 0)$ solving the equation (2.3.2) and such that $(a, b) \in M$. By the previous consideration we obtain

$$N = 2 \cdot \#\{(a, 0) \in M \,:\, a \in \mathbb{F}_q^\times\}.$$

For simplicity, denote by N_a the number $\#\{(a, 0) \in M \,:\, a \in \mathbb{F}_q^\times\}$. Hence;

$$\chi(y_\chi^2) = \frac{(q-1)^6(2q+1)^2}{|M|}\Big(2N_a + (q+1)(q^2+q+1)\Big).$$

Since $(q + 1)(q^2 + q + 1)$ is odd, then the number between brackets is odd. Hence, $\frac{1}{|M|} \in R$. □

This concludes the proof of Theorem 2.1.1 for $\mathbf{SL}_3(q)$.

3.4. Projective special linear group $\mathbf{PSL}_3(q)$. Let $q = p^m$, for $m \geq 1$. In this section we assume that $q \equiv_3 1$, since otherwise $\mathbf{PSL}_3(q) = \mathbf{SL}_3(q)$ and this case was just treated. The map $\pi\colon \mathbf{SL}_3(q) \to \mathbf{PSL}_3(q)$ represents the natural projection and G stands for $\mathbf{PSL}_3(q)$. Furthermore, recall that θ is a primitive third root of unit in $\mathbb{F}_q$, which exists since $q \equiv_3 1$.
We retain notation from Subsection 3.3.
In particular, the Sylow p-subgroup we consider is

$$\pi(U) := \left\{\pi\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix}\right) : a, b, c \in \mathbb{F}_q\right\}$$

while the maximal split torus is

$$\pi(T) := \left\{\pi\left(\begin{smallmatrix} s & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & t^{-1}s^{-1} \end{smallmatrix}\right) : s, t \in \mathbb{F}_q^\times\right\}.$$

Moreover, we have that $N_G(\pi(U)) = \pi(B) \simeq \pi(T) \ltimes \pi(U)$.
Firstly, we compute the values of the character $\chi = \mathrm{Ind}_{\pi(U)}^G(\mathbb{1}_{\pi(U)})$ at $\pi(U)$.

LEMMA 2.3.7. *For $\pi(u) \in \pi(U)$ we have:*

$$\chi(\pi(u)) = \begin{cases} \frac{(q^3-1)(q^2-1)}{3} & \text{if } u = 1, \\ \frac{(2q+1)(q-1)^2}{3} & \text{if } u \text{ is of Jordan type } (2,1), \\ \frac{(q-1)^2}{3} & \text{if } u \text{ is of Jordan type } (3). \end{cases}$$

PROOF. The value at the identity element follows from the definition of χ. By [71, Proposition 1.2], for $u \in U$ the following formula holds

$$\mathrm{Ind}_{\pi(U)}^{\mathbf{PSL}_3(q)}(\mathbb{1}_{\pi(U)})(\pi(u)) = \frac{|C_{\mathbf{PSL}_3(q)}(\pi(u))| \cdot |Cl(\pi(u)) \cap \pi(U)|}{|\pi(U)|}.$$

In addition,

$$\mathrm{Ind}_U^{\mathbf{SL}_3(q)}(\mathbb{1}_U)(u) = \frac{|C_{\mathbf{SL}_3(q)}(u)| \cdot |Cl(u) \cap U|}{|U|}.$$

We start proving the following:

(1) $|Cl(u)| = |Cl(\pi(u))|$;
(2) $|Cl(u) \cap U| = |Cl(\pi(u)) \cap \pi(U)|$,

for every $u \in U$.
(1) We first prove that $|Cl(u)| = |\pi(Cl(u))|$, for every $u \in U$. This follows from the fact that the projection π restricted to $Cl(u)$ is injective. In fact if for $u \in U$ and $x, y \in \mathbf{SL}_3(q)$ the conjugates xux^{-1} and yuy^{-1} have the same image via π we must have $xux^{-1} = yuy^{-1}\theta^i$, for $i \in \{0, 1, 2\}$. Since the left hand side of the equation has order p, it follows that $i = 0$. We conclude by observing that $\pi(Cl(u)) = Cl(\pi(u))$ for every $u \in U$, since π is surjective.
(2) For showing this equality, it is enough to prove that

$$|\pi(Cl(u) \cap U)| = |\pi(Cl(u)) \cap \pi(U)|,$$

for every $u \in U$. Indeed, if this is the case we would have

$$|Cl(u) \cap U| = |\pi(Cl(u) \cap U)| = |\pi(Cl(u)) \cap \pi(U)| = |Cl(\pi(u)) \cap \pi(U)|,$$

where the first equality follows from the injectivity of $\pi|_{Cl(u)}$ and the latter one from the fact that $\pi(Cl(u)) = Cl(\pi(u))$.
The inclusion $\pi(Cl(u) \cap U) \subseteq \pi(Cl(u)) \cap \pi(U)$ is trivial, for every $u \in U$. Now let $\pi(z) \in \pi(Cl(u)) \cap \pi(U)$, for $z \in \mathbf{SL}_3(q)$. We have $\pi(z) = \pi(u')$ for some $u' \in U$ and $\pi(z) = \pi(tut^{-1})$, for some $u \in U$ and $t \in \mathbf{SL}_3(q)$. This implies that tut^{-1} and u' have the same projection along π. So we have $tut^{-1} = u'\theta^j$, but again the left hand side has order p, and this forces $j = 0$. So indeed $\pi(z) = \pi(u') \in \pi(\mathrm{Cl}(u) \cap U)$, and we obtain the other inclusion.
The equalities just proven imply that for every $u \in U$

$$|C_{\mathbf{PSL}_3(q)}(\pi(u))| = \frac{|\mathbf{PSL}_3(q)|}{|Cl(\pi(u))|} = \frac{1}{3} \cdot \frac{|\mathbf{SL}_3(q)|}{|Cl(u)|} = \frac{1}{3} \cdot |C_{\mathbf{SL}_3(q)}(u)|,$$

and also that

$$\mathrm{Ind}_{\pi(U)}^{\mathbf{PSL}_3(q)}(\mathbb{1}_{\pi(U)})(\pi(u)) = \frac{1}{3}\cdot \mathrm{Ind}_U^G(\mathbb{1}_U)(u).$$

Finally, by Lemma 2.3.2 we get the desired result. $\square$

In this case, we can view P as the collection of the elements $\pi(g)$, such that the characteristic polynomial of g is $(\theta^i - z)^3$, for some $i \in \{0,1,2\}$.
By definition, the value of the character χ at an element which does not belong to P is equal to zero. If, instead $\pi(g)$ is a p-element in virtue of Lemma 2.3.7 the value of χ depends on the Jordan type of g, which is obtained computing $\mathrm{rk}(g - \theta^i \cdot 1)$, for $i \in \{0,1,2\}$. In particular, we get

$$\begin{aligned} C_{(1)} &= \{\pi(1)\},\\ C_{(2,1)} &= \{\pi(g) \in P\ : g \text{ has Jordan type } (2,1)\},\\ C_{(3)} &= \{\pi(g) \in P\ : g \text{ has Jordan type } (3)\}. \end{aligned}$$

In consequence $I_\chi = \{C_{(1)}, C_{(2,1)}, C_{(3)}\}$.

Remark 2.3.8. Abusing notation, we say that an element $\pi(g) \in G$ is of Jordan type $(2,1)$, respectively (3), if g has 3 equal eigenvalues and is of Jordan type $(2,1)$, respectively (3).

For simplicity, call M_1 and M_2 the subgroups $\pi(M_1)$ and $\pi(M_2)$.
The aim of this section is to prove Theorem 2.1.1 for G. For this purpose, in light of Corollary 2.2.6 and Remarks 2.2.7 and 2.2.8, it is enough to prove the theorem for cocycles associated with subgroups M of the following form:

i) $M \le M_1$, containing $\pi\left(\begin{smallmatrix} 1 & -1 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{smallmatrix}\right)$;
ii) $M = \left\{\pi\left(\begin{smallmatrix} 1 & 0 & b\\ 0 & 1 & 0\\ 0 & 0 & 1\end{smallmatrix}\right)\ :\ b \in \mathbb{E}\right\}$, where $\mathbb{E}$ is an additive subgroup of $\mathbb{F}_q$ isomorphic to C_p^{2n};
iii) $M \le M_2$ containing $\pi\begin{pmatrix} 1 & -3/2 & 3\\ 0 & 1 & -3/2\\ 0 & 0 & 1\end{pmatrix}$, if q is odd.

Hence, the first step is to prove the following:

Proposition 2.3.9. *Let M be an abelian p-subgroup of central type of M_1 containing $\pi\left(\begin{smallmatrix} 1 & -1 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{smallmatrix}\right)$ and let $\omega\colon \widehat{M} \times \widehat{M} \to K^\times$ be a non-degenerate cocycle. If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.*

Proof. We consider the element $\tau = \pi\left(\begin{smallmatrix} 0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{smallmatrix}\right)$ in $N_G(\pi(T))$. One can verify that $M \cap \left(\tau M \tau^{-1}\right) \subseteq M_1 \cap (\tau M_1 \tau^{-1}) = \{\pi(1)\}$. We must find those elements $v \in M$ such that the characteristic polynomial of a lifting of τv is $(\theta^i - z)^3$, for some $i \in \{0,1,2\}$.
This happens if and only if $v \in \left\{\pi\begin{pmatrix} 1 & -3\theta^{2i} & 3\theta^i\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\ :\ i \in \{0,1,2\}\right\}$. Furthermore,

the element τv has Jordan type (3), for every $v \in \left\{\pi\begin{pmatrix} 1 & -3\theta^{2i} & 3\theta^i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : i \in \{0,1,2\}\right\}$.
Hence

$$M_{C_{(3)}} \subseteq \left\{\pi\begin{pmatrix} 1 & -3\theta^{2i} & 3\theta^i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : i \in \{0,1,2\}\right\},$$

and $M_{C_{(2,1)}} = \emptyset$. In addition, $\pi\begin{pmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \pi\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^3 \in M$ by assumption. This implies that $M_{C_{(3)}} \neq \emptyset$.

We now divide the proof according to the size of $M_{C_{(3)}}$.

1) Suppose that $|M_{C_{(3)}}| = 1$. Then $M_{C_{(3)}} = \left\{\begin{pmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right\}$.
For enhancing the readability of some formulas, we write $(a,b) \in M$ to indicate that $\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M$.
Hence,

$$\begin{aligned}
\chi(y_\chi^2) &= \frac{\chi(C_{(3)})^2}{|M|} \sum_{\substack{v \in M \\ x \in M_{C_{(3)}}}} \chi\Big(\tau x^2 v \tau v^{-1}\Big) \\
&= \frac{(q-1)^4}{9|M|} \sum_{(a,b)\in M} \chi\left(\pi\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & -a & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) \qquad (2.3.3) \\
&= \frac{(q-1)^4}{9|M|} \sum_{(a,b)\in M} \chi\left(\pi\begin{pmatrix} 0 & 0 & 1 \\ 1 & -a & -b \\ b+6 & 1-ab-6a & a-b^2-6-6b \end{pmatrix}\right).
\end{aligned}$$

The latter summands are nonzero if and only if the characteristic polynomial of the corresponding matrix equals $(z-\theta^k)^3$ for some $k \in \{0,1,2\}$, i.e. if and only if $(a,b) \in \mathbb{F}_q^2$ is a solution of the following system of equations

$$\begin{aligned} -b^2 - 6b - 6 &= 3\theta^k \\ a^2 - 6a + 6 &= -3\theta^{2k}, \end{aligned} \qquad (2.3.4)$$

and $\pi\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M$.
For $k = 0,1,2$, call N_k the number of solutions of system (2.3.4) satisfying $\pi\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M$.
For $k = 0$ the system (2.3.4) has one solution, namely $(a,b) = (3,-3)$. The corresponding element $\pi\begin{pmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ lies in M, so $N_0 \geq 1$. Moreover, for each $k \in \{1,2\}$, the system has at most four solutions, implying that $1 \leq N_0 + N_1 + N_2 \leq 9$. We proceed treating separately the case q odd and q even.

q odd. The last matrix appearing in the expression of $\chi(y_\chi^2)$ is the matrix in Equation (A.1.2) in the Appendix, with $i = j = 0$; in light of Lemma

A.1.2 it has Jordan type (3). This yields:

$$\chi(y_\chi^2) = \frac{(q-1)^6}{27|M|} \cdot (N_0 + N_1 + N_2).$$

If $|M|$ divides $N_0 + N_1 + N_2$, then $|M| \leq 9$. Since q is odd and satisfies $q \equiv_3 1$ and since $|M|$ is a square, we obtain that $\chi(y_\chi^2)$ is an irreducible fraction, so $\frac{1}{|M|} \in R$.

q even. We consider the matrices appearing in the expression of $\chi(y_\chi^2)$ in (2.3.3). Lemma A.2.1 for $i = j = 0$ states that the latter matrices are of Jordan type $(2, 1)$ if and only if $(a, b) = (\theta^k, \theta^{2k})$ for $k \in \{0, 1, 2\}$. The assumption that $\pi\left(\begin{smallmatrix} 1 & \theta^{2i} & \theta^i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \notin M$ for $i \neq 0$, implies that the only solution (a, b) of system (2.3.4) satisfying $\pi\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$ is $(a, b) = (1, 1)$. We can then conclude that:

$$\chi(y_\chi^2) = \frac{(q-1)^6(2q+1)}{27|M|}.$$

Since $q-1$ and $2q+1$ are odd, we get $\frac{1}{|M|} \in R$.

2) Suppose now that $|M_{C_{(3)}}| > 1$ and $q \equiv_3 1$ is arbitrary with this property.
Firstly, we show that $|M_{C_{(3)}}| \neq 2$. Indeed, fix $i \in \{1, 2\}$ and suppose that the element $\pi\left(\begin{smallmatrix} 1 & -3\theta^i & 3\theta^{2i} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$. The latter together with the assumption $\pi\left(\begin{smallmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$ yields that $\pi\left(\begin{smallmatrix} 1 & -3\theta^{2i} & 3\theta^i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$ since

$$\pi\left(\left(\begin{smallmatrix} 1 & -3\theta^i & 3\theta^{2i} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)\right) = \pi\left(\begin{smallmatrix} 1 & -3\theta^{2i} & 3\theta^i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)^{-1}.$$

Therefore

$$M_{C_{(3)}} = \left\{\pi\left(\begin{smallmatrix} 1 & -3\theta^{2i} & 3\theta^i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \,:\, i \in \{0, 1, 2\}\right\},$$

and so $|\langle M_{C_3}\rangle| = p^2$. Then,

$$\begin{aligned}
\chi(y_\chi^2) &= \frac{\chi(C_{(3)})^2}{|M|} \sum_{\substack{v \in M \\ x, x' \in M_{C_{(3)}}}} \chi\big(\tau x x' v \tau v^{-1}\big) \\
&= \frac{(q-1)^4}{9|M|} \sum_{\substack{(a,b) \in M \\ i,j \in \{0,1,2\}}} \chi\left(\pi\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -3\theta^{2i} & 3\theta^i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -3\theta^{2j} & 3\theta^j \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -a & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)\right) \\
&= \frac{(q-1)^4}{9|M|} \sum_{\substack{(a,b) \in M \\ i,j \in \{0,1,2\}}} \chi\left(\pi\left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & -a & -b \\ b+3(\theta^i+\theta^j) & 1-ab-3a(\theta^i+\theta^j) & a-b^2-3(\theta^{2i}+\theta^{2j})-3b(\theta^i+\theta^j) \end{smallmatrix}\right)\right).
\end{aligned} \tag{2.3.5}$$

The latter summands are nonzero if and only if the characteristic polynomial of the corresponding matrix equals $(\theta^k - z)^3$, for some $k \in \{0,1,2\}$. A computation shows that this holds if and only if the pair $(a,b) \in \mathbb{F}_q^2$ is a solution of the following system of equations:

$$\begin{aligned} &-b^2 - 3b(\theta^i + \theta^j) - 3(\theta^{2i} + \theta^{2j}) = 3\theta^k \\ &a^2 - 3a(\theta^{2i} + \theta^{2j}) + 3(\theta^i + \theta^{2j}) = -3\theta^{2k}, \end{aligned} \tag{2.3.6}$$

for some $k \in \{0,1,2\}$ and a,b such that $\pi\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$.
Let N_k be the number of solutions of the previous system for $k \in \{0,1,2\}$. In this case, as well, we carry out our estimates according to the parity of q.
q odd. For every triple (i,j,k), with $i,j,k \in \{0,1,2\}$ the system (2.3.6) admits at most 4 solutions and so $N_0 + N_1 + N_2 \leq 108$. As in the case $|M_{C_{(3)}}| = 1$, we have at least one solution, i.e. $N_0 + N_1 + N_2 \geq 1$. Since the last matrix appearing in the expression of $\chi(y_\chi^2)$ in Equation (2.3.5) is the matrix in Equation (A.1.2) in the Appendix, Lemma A.1.2 implies that

$$\chi(y_\chi^2) = \frac{(q-1)^6}{27|M|}(N_0 + N_1 + N_2).$$

A necessary condition for $\chi(y_\chi)^2$ to be an integer is that $|M| \leq 108$. Given that $|M| = p^{2l}$, for some $l \in \mathbb{N}$ and that $p \neq 2,3$, this could occur only if $|M| = 49$ or $|M| = 25$.
Let $|M| = 49$. As we have noticed before, $|\langle M_{C_{(3)}} \rangle| = 49$; this forces M to be equal to $\langle M_{C_{(3)}} \rangle$. In this case, the third root of unity θ lies in $\mathbb{F}_7$ and one can verify that $M = \left\{\pi\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) : a,b \in \mathbb{F}_7\right\}$. Lemma A.1.1 together with Lemma A.1.2 imply that

$$\chi(y_\chi^2) = \frac{75(q-1)^6}{27 \cdot 49} \in \mathbb{Q} \setminus \mathbb{Z},$$

leading to $\frac{1}{|M|} \in R$.
If $|M| = 25$, then with the same argument we used for $p = 7$, we obtain that $M = \langle M_{C_{(3)}} \rangle$. Lemma A.1.3 and Lemma A.1.2 yield that

$$\chi(y_\chi^2) = \frac{15(q-1)^6}{27 \cdot 25} \in \mathbb{Q} \setminus \mathbb{Z},$$

implying $\frac{1}{|M|} \in R$.

q even. We denote by $N_{(3)}$ the number of 2-elements in the expression of $\chi(y_\chi^2)$ in Equation (2.3.5) which have Jordan type (3), while $N_{(2,1)}$ stands for the number of 2-elements of Jordan type $(2,1)$ in the expression of $\chi(y_\chi^2)$. We recall that we are looking for the pairs $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$ which solve the following system:

$$\begin{aligned} &b^2 + b(\theta^i + \theta^j) + (\theta^{2i} + \theta^{2j} + \theta^k) = 0 \\ &a^2 + a(\theta^{2i} + \theta^{2j}) + (\theta^i + \theta^{2j} + \theta^{2k}) = 0, \end{aligned} \tag{2.3.7}$$

and satisfy $\pi\left(\begin{smallmatrix}1&a&b\\0&1&0\\0&0&1\end{smallmatrix}\right)\in M$ for some i,j,k running in $\{0,1,2\}$.
If $i=j$, then the solutions of the system are $(a,b)=(\theta^k,\theta^{2k})$, for $k\in\{0,1,2\}$. In the case we are considering, the element $\pi\left(\begin{smallmatrix}1&\theta^k&\theta^{2k}\\0&1&0\\0&0&1\end{smallmatrix}\right)\in M$ for each $k\in\{0,1,2\}$. Moreover for $i=j$, Lemma A.2.1 guarantees that the Jordan type of the corresponding element in the expression of $\chi(y_\chi^2)$ in Equation (2.3.5) is $(2,1)$ and that the only elements of Jordan type $(2,1)$ are those for which $i=j$. Hence, for every $i=j\in\{0,1,2\}$, there are 3 solutions $(a,b)\in\mathbb{F}_q\times\mathbb{F}_q$ of system (2.3.7); explicitly $(a,b)\in\{(1,1),(\theta,\theta^2),(\theta^2,\theta)\}$. Hence, $N_{(2,1)}=9$.
Let $i\neq j$. The solutions of the system (2.3.7) for the pair (i,j) are the same as for the pair (j,i). Thus, $N_{(3)}=2N_{(i,j,k)}$, where $N_{(i,j,k)}$ are the solutions of the system (2.3.7) for the triple (i,j,k), with $i<j$. Hence,

$$\chi(y_\chi^2)=\frac{(q-1)^6}{27|M|}\Big(N_{(3)}+(2q+1)N_{(2,1)}\Big)=\frac{(q-1)^6}{27|M|}\Big(18q+9+2N_{(i,j,k)}\Big).$$

Since the number into brackets is odd, we get that $\frac{1}{|M|}\in R$. $\square$

We now proceed with the following result.

Proposition 2.3.10. *Let*

$$M=\left\{\pi\left(\begin{smallmatrix}1&0&b\\0&1&0\\0&0&1\end{smallmatrix}\right)\,:\,b\in\mathbb{E}\right\},$$

where $\mathbb{E}$ is an additive subgroup of $\mathbb{F}_q$ isomorphic to C_p^{2k} for some $k>0$. Let $\omega\colon\widehat{M}\times\widehat{M}\to K^\times$ be a non-degenerate cocycle. If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|}\in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.

Proof. We take $\tau=\pi\left(\begin{smallmatrix}1&0&0\\1&1&0\\1&1&1\end{smallmatrix}\right)$. One can verify that $\tau M\tau^{-1}\cap M=\{\pi(1)\}$. We must detect for which elements $v\in M$ the characteristic polynomial of a lifting of τv equals $(\theta^i-z)^3$ for some $i\in\{0,1,2\}$. The only element $v\in M$ satisfying this condition is the identity, which clearly belongs to M. Moreover, the Jordan type of τ is (3) and this implies that $M_{C_{(3)}}=\pi(1)$. Then,

$$\begin{aligned}\chi(y_\chi^2)&=\frac{\chi(C_{(3)})^2}{|M|}\sum_{v\in M}\chi\Big(\tau v\tau v^{-1}\Big)\\&=\frac{(q-1)^4}{9|M|}\sum_{b\in\mathbb{E}}\chi\left(\pi\left(\begin{smallmatrix}1&0&0\\1&1&0\\1&1&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0&b\\0&1&0\\0&0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0&0\\1&1&0\\1&1&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0&-b\\0&1&0\\0&0&1\end{smallmatrix}\right)\right)\\&=\frac{(q-1)^4}{9|M|}\sum_{b\in\mathbb{E}}\chi\left(\pi\left(\begin{smallmatrix}1+b&b&-b^2\\2+b&1+b&-b^2-b\\3+b&2+b&-2b-b^2+1\end{smallmatrix}\right)\right).\end{aligned}\tag{2.3.8}$$

Computing the characteristic polynomial of the matrix in the expression of $\chi(y_\chi^2)$ in Equation 2.3.8 and forcing it to be equal to $(\theta^k-z)^3$ for $k\in\{0,1,2\}$

we get that $b \in \mathbb{E}$ must satisfy the following system of equations

$$-3 = -3\theta^{2k}$$
$$-b^2 + 3 = 3\theta^k.$$

In particular, the system admits a solution if and only if $k = 0$, and in this case $b = 0$ is the only solution. We now proceed according to the parity of q.
q odd. In this case the Jordan type of $\tau v \tau v^{-1} = \tau^2$ is (3). Hence;

$$\chi(y_\chi^2) = \frac{(q-1)^6}{27 \cdot |M|}.$$

Since $gcd(q-1, |E|) = 1$, we conclude that $\frac{1}{|M|} \in R$.
q even. In this case the Jordan type of τ^2 is $(2,1)$. Hence

$$\chi(y_\chi^2) = \frac{(q-1)^6(2q+1)}{27 \cdot |M|},$$

which belongs to $\mathbb{Q} \setminus \mathbb{Z}$ since $(q-1)$ and $(2q+1)$ are odd. Thus, $\frac{1}{|M|} \in R$. $\square$

PROPOSITION 2.3.11. *Let q be odd and let M be an abelian p-subgroup of central type of M_2, containing $\pi\begin{pmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{pmatrix}$. Consider $\omega\colon \widehat{M} \times \widehat{M} \to K^\times$ a non-degenerate cocycle. If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.*

PROOF. We pick $\tau = \pi\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. We can verify that $M_2 \cap \tau M_2 \tau^{-1} = \{\pi(1)\}$ and hence $M \cap \tau M \tau^{-1} = \{\pi(1)\}$. We seek those elements $v \in M_2$ such that τv is a p-element, i.e. such that the characteristic polynomial of a lift of it is $(\theta^i - z)^3$, for some $i \in \{0,1,2\}$. A direct computation shows that this occurs if and only if $v \in \left\{\pi\begin{pmatrix} 1 & (-3/2)\theta^{2i} & 3\theta^i \\ 0 & 1 & (-3/2)\theta^{2i} \\ 0 & 0 & 1 \end{pmatrix} : i \in 0,1,2\right\}$ and that in this case the Jordan type of τv is (3). This implies that

$$M_{C_{(3)}} \subseteq \left\{\pi\begin{pmatrix} 1 & (-3/2)\theta^{2i} & 3\theta^i \\ 0 & 1 & (-3/2)\theta^{2i} \\ 0 & 0 & 1 \end{pmatrix} : i \in 0,1,2\right\}$$

and $M_{C_{(2,1)}} = \emptyset$. Bear in mind that $\pi\begin{pmatrix} 1 & (-3/2) & 3 \\ 0 & 1 & (-3/2) \\ 0 & 0 & 1 \end{pmatrix} \in M$, by assumption. We divide the analysis into two cases, according to the size of $M_{C_{(3)}}$.

1) Suppose that $|M_{C_{(3)}}| = 1$. Then $M_{C_{(3)}} = \left\{\pi\begin{pmatrix} 1 & (-3/2) & 3 \\ 0 & 1 & (-3/2) \\ 0 & 0 & 1 \end{pmatrix}\right\}$ and thus M is a proper subgroup of M_2. We write $(a,b) \in M$ to indicate that

$\pi\left(\begin{smallmatrix}1&a&b\\0&1&a\\0&0&1\end{smallmatrix}\right) \in M$ and compute

$$\begin{aligned}\chi(y_\chi^2) &= \frac{\chi(C_{(3)})^2}{|M|} \sum_{\substack{v\in M\\ x\in M_{C_{(3)}}}} \chi\Big(\tau x^2 v\tau v^{-1}\Big)\\ &= \frac{(q-1)^4}{9|M|} \sum_{(a,b)\in M} \chi\left(\pi\left(\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}1&-3/2&3\\0&1&-3/2\\0&0&1\end{smallmatrix}\right)^2\left(\begin{smallmatrix}1&a&b\\0&1&a\\0&0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}0&1&0\\0&0&1\\1&0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}1&-a&a^2-b\\0&1&-a\\0&0&1\end{smallmatrix}\right)\right)\\ &= \frac{(q-1)^4}{9|M|} \sum_{(a,b)\in M} \chi\left(\begin{smallmatrix}a-3 & 3a-a^2 & a(a^2-b)-3(a^2-b)+1\\ 1 & -a & a^2-b\\ b-3a+\frac{33}{4} & 3a^2-ab-\frac{33}{4}a+1 & -3+(a^2-b)(b+\frac{33}{4}-3a)\end{smallmatrix}\right).\end{aligned} \tag{2.3.9}$$

With the usual characteristic polynomial criterium, the summands in the expression of $\chi(y_\chi^2)$ in (2.3.9) are nonzero if and only if $(a,b) \in M$ satisfies the following system of equations

$$\begin{aligned}&a^2 - 3a - \tfrac{3}{4} = -3\theta^{2k}\\ &-6 + (a^2-b)(b + \tfrac{33}{4} - 3a) = 3\theta^k,\end{aligned} \tag{2.3.10}$$

for some $k \in \{0,1,2\}$.
For $k \in \{0,1,2\}$, we call N_k the number of solutions (a,b) such that $(a,b) \in M$. For $k = 0$, there is only one solution to the system, namely $(a,b) = (3/2, -3/4)$. Moreover $\left(\begin{smallmatrix}1&3/2&-3/4\\0&1&3/2\\0&0&1\end{smallmatrix}\right) \in M$, since

$$\begin{pmatrix}1&3/2&-3/4\\0&1&3/2\\0&0&1\end{pmatrix}^{-1} = \begin{pmatrix}1&-3/2&3\\0&1&-3/2\\0&0&1\end{pmatrix} \in M$$

by assumption. Hence $N_0 = 1$. Furthermore, $N_1, N_2 \leq 4$, yielding that $1 \leq N_0 + N_1 + N_2 \leq 9$.
Observe that the matrix appearing in the expression of $\chi(y_\chi^2)$ in (2.3.9) is the matrix in Equation (A.1.3), for $r = w = -3/2$ and $s = y = 3$.
If $p \neq 7, 19$, Lemma A.1.4 implies that

$$\chi(y_\chi^2) = \frac{(q-1)^6}{27|M|} \cdot (N_0 + N_1 + N_2).$$

The above number is an integer if and only if $|M|$ divides $N_0 + N_1 + N_2$. Since $N_0 + N_1 + N_2 \leq 9$ this cannot occur, since the only prime squares less or equal to 9 are 4 and 9, that are discarded because p is odd and $q \equiv_3 1$. Thus, we have $\frac{1}{|M|} \in R$.

Let now N be the number of solutions $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$ of system (2.3.14). Then $N = N_{(3)} + N_{(2,1)}$, where $N_{(3)}$ and $N_{(2,1)}$ stands for the number of solutions (a,b) of system (2.3.14) which are such that the corresponding element in the expression of $\chi(y_\chi)^2$ in Equation (2.3.9) is a p-element of Jordan type (3) and Jordan type $(2,1)$ respectively.

Let $p = 7$. Since $i = j = 0$, by Lemma A.1.4 the element showing up in the expression of $\chi(y_\chi^2)$ in Equation (2.3.9) is a 7-element of Jordan type $(2,1)$ if $k = 2$. Then, $N_{(2,1)} \leq 4$ and $N = N_{(2,1)} + N_{(3)} \leq 9$. Thus

$$\chi(y_\chi^2) = \frac{(q-1)^6}{27|M|}\left(2qN_{(2,1)} + N_{(3)} + N_{(2,1)}\right).$$

Since $M < M_2$ and $|M| = 7^{2l}$, for some $l \geq 1$, then 7^l is a proper divisor of 7^m. Hence, 7^{l+1} divides q. In conclusion, if $|M|$ divides $(2qN_{(2,1)} + N_{(3)} + N_{(2,1)})$ then 7^{l+1} must divide $N_{(2,1)} + N_{(3)} \leq 9$ for some $l \geq 1$, a contradiction.
Let $p = 19$. Lemma A.1.4 implies that $N_{(2,1)} = 0$ because we are assuming $|M_{C_{(3)}}| = 1$ and so $i = j = 0$ in Equation (A.1.3).
Hence;

$$\chi(y_\chi^2) = \frac{(q-1)^6}{27|M|}N_{(3)},$$

where $N_{(3)} \leq 9$; we deduce that $\frac{1}{|M|} \in R$.

2) Assume now that $|M_{C_{(3)}}| > 1$ and that $\pi\begin{pmatrix} 1 & -3/2\theta^2 & 3\theta \\ 0 & 1 & -3/2\theta^2 \\ 0 & 0 & 1 \end{pmatrix} \in M$. Since $\begin{pmatrix} 1 & -3/2 & 3 \\ 0 & 1 & -3/2 \\ 0 & 0 & 1 \end{pmatrix} \in M$, also $\begin{pmatrix} 1 & -3/2\theta & 3\theta^2 \\ 0 & 1 & -3/2\theta \\ 0 & 0 & 1 \end{pmatrix} \in M$. In consequence, $|M_{C_{(3)}}| = 3$, i.e.

$$M_{C_{(3)}} = \left\{\pi\begin{pmatrix} 1 & (-3/2)\theta^{2i} & 3\theta^i \\ 0 & 1 & (-3/2)\theta^{2i} \\ 0 & 0 & 1 \end{pmatrix} \,:\, i \in \{0,1,2\}\right\}.$$

Therefore,

$$\chi(y_\chi^2) = \frac{\chi(C_{(3)})^2}{|M|} \sum_{\substack{v \in M \\ x,x' \in M_{C_{(3)}}}} \chi\left(\tau x x' v \tau v^{-1}\right)$$

$$= \frac{(q-1)^4}{9q^2} \sum_{\substack{(a,b)\in M \\ i,j\in\{0,1,2\}}} \chi\left(\pi\begin{pmatrix} 0&1&0 \\ 0&0&1 \\ 1&0&0 \end{pmatrix}\begin{pmatrix} 1 & (-3/2)\theta^{2i} & 3\theta^i \\ 0 & 1 & (-3/2)\theta^{2i} \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & (-3/2)\theta^{2j} & 3\theta^j \\ 0 & 1 & (-3/2)\theta^{2j} \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1&a&b \\ 0&1&a \\ 0&0&1 \end{pmatrix}\begin{pmatrix} 0&1&0 \\ 0&0&1 \\ 1&0&0 \end{pmatrix}\begin{pmatrix} 1 & -a & a^2-b \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{pmatrix}\right)$$

For simplicity, set $y = 3\theta^i, s = 3\theta^j, w = (-3/2)\theta^{2i}, r = (-3/2)\theta^{2j}$. Then $\chi(y_\chi^2)$ equals to :

$$\frac{(q-1)^4}{9q^2} \sum_{\substack{(a,b)\in M \\ i,j\in\{0,1,2\}}} \chi\left(\pi\begin{pmatrix} a+r+w & -a(a+r+w) & 1+(a^2-b)(a+r+w) \\ 1 & -a & a^2-b \\ b+s+rw+a(r+w)+y & 1-a(b+s+rw+a(r+w)+y) & r+w+(a^2-b)(b+s+rw+a(r+w)+y) \end{pmatrix}\right). \tag{2.3.11}$$

The matrix appearing in Equation (2.3.11) is indeed the matrix C in Equation (A.1.3) in the Appendix.
Computing the characteristic polynomial of C and forcing it to be equal to $(\theta^k - z)^3$, for some $k \in \{0,1,2\}$, we get that C is a p-element if and only if

$(a, b) \in \mathbb{F}_q^2$ is a solution of the following system of equations:

$$\begin{array}{l} a^2 + a(r+w) + s + y - rw - r^2 - w^2 = -3\theta^{2k} \\ 2(r+w) + (a^2 - b)(b + s + rw + y + a(r+w)) = 3\theta^k, \end{array} \tag{2.3.12}$$

for some $k \in \{0, 1, 2\}$ and $\pi \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$.
For each choice of the triple (i, j, k) there are at most 4 pairs (a, b) satisfying the previuos equations. Moreover, for $i = j = k = 0$, the calculations in case 1) imply that $(a, b) = (3/2, -3/4)$ is a solution.
Call N the number of p-elements in the sum. By the previous considerations, we have $1 \leq N \leq 27 \times 4 = 108$.
We now need to establish the Jordan type of the p-elements arising from the solutions of system (2.3.12), for some choice of $i, j, k \in \{0, 1, 2\}$. Let us divide this analysis into three cases, according to the value of p and $|M|$.
i) Let $p \neq 7, 19$. By Lemma A.1.4, the p-elements arising from the solutions of the systems (2.3.12) are all of Jordan type (3). Then,

$$\chi(y_\chi^2) = \frac{(q-1)^6}{27|M|} N.$$

Since q is odd, $q \equiv_3 1$ and $p \neq 7, 19$, then $|M|$ could divide N only if $|M| = 25$. In the other cases we conclude that $\frac{1}{|M|} \in R$. If $|M| = 25$, by order reasons we get $M = \langle M_{C_{(3)}} \rangle$. In light of Lemma A.1.8, we obtain

$$\chi(y_\chi^2) = \frac{(q-1)^6 15}{27 \cdot 25}.$$

Since 25 does not divide 15 we conclude that $\chi(y_\chi^2) \in \mathbb{Q} \setminus \mathbb{Z}$ and in particular that $\frac{1}{|M|} \in R$.
ii) Assume now $p = 7$. Then

$$\chi(y_\chi^2) = \frac{(q-1)^6}{27|M|} (2qN_{(2,1)} + N_{(2,1)} + N_{(3)}),$$

where $N_{(2,1)}$ and $N_{(3)}$ are defined as in case 1). If $M < M_2$ and $|M| = 7^{2l}$, then 7^{l+1} divides q and $|M|$. If $\chi(y_\chi^2) \in \mathbb{Z}$ then 7^{l+1} would divide $N = N_{(2,1)} + N_{(3)}$. This could occur only for $l = 1$, i.e. $|M| = 49$. In this case $M = \langle M_{C_{(3)}} \rangle$ and one can verify that

$$\langle M_{C_{(3)}} \rangle = \left\{ \pi \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \, : \, a, b \in \mathbb{F}_7 \right\}.$$

By Lemma A.1.6, we have that $N_{(2,1)} = 6$ and $N_{(2,1)} + N_{(3)} = 33$. Hence,

$$\chi(y_\chi^2) = \frac{(q-1)^6 (12q + 33)}{27 \cdot 49}.$$

Since 7 divides q but it does not divide 33, the number $\chi(y_\chi^2) \in \mathbb{Q} \setminus \mathbb{Z}$. Thus in the case $p = 7$ and $M < M_2$, we conclude that $\frac{1}{|M|} \in R$.

Assume now $M = M_2$. Then $|M| = q^2$. Moreover, Lemma A.1.5 guarantees that $N_{(2,1)} \leq 12$ and as before $N = N_{(3)} + N_{(2,1)} \leq 108$. If $\chi(y_\chi^2) \in \mathbb{Z}$, then

$$q^2 \leq 2qN_{(2,1)} + (N_{(2,1)} + N_{(3)}) \leq 24q + 108,$$

i.e. $7 \leq q \leq 28$. This forces $q = 7$. In this case, Lemma A.1.6 gives that $N_{(2,1)} = 6$ and $N_{(3)} = 27$. In consequence;

$$\chi(y_\chi^2) = \frac{6^6}{27 \cdot 7^2}(6(14+1) + 27) = \frac{6^6}{27 \cdot 7^2}(117).$$

Since 117 and 7 are coprime, $\chi(y_\chi^2) \in \mathbb{Q} \setminus \mathbb{Z}$. Hence, if $M = M_2$ and $p = 7$ we obtain $\frac{1}{|M|} \in R$.
iii) Finally, assume $p = 19$, Then

$$\chi(y_\chi^2) = \frac{(q-1)^6}{27|M|}(2qN_{(2,1)} + N_{(2,1)} + N_{(3)}),$$

where $N_{(2,1)} \leq 24$ by Lemma A.1.5.
Let $|M| = p^{2l}$, for some $l \geq 1$. If $M < M_2$, then $\chi(y_\chi^2)$ is an integer if p^{l+1} divides $N = N_{(2,1)} + N_{(3)} \leq 108$ for some $l \geq 1$, a contradiction.
If instead $M = M_2$, then $|M| = q^2$. A necessary condition for $\chi(y_\chi^2)$ to be an integer is that $q^2 \leq 48q + 108$, forcing $q = 19$. If this is the case, Lemma A.1.7 implies that

$$\chi(y_\chi^2) = \frac{18^6}{27 \cdot 19^2}(2 \cdot 19 \cdot 12 + 51) = \frac{18^6 \cdot 507}{27 \cdot 19^2} \in \mathbb{Q} \setminus \mathbb{Z}.$$

Also in the case $p = 19$, we conclude that $\frac{1}{|M|} \in R$. $\square$

From now on, let q be even. The last step is proving the following Proposition.

PROPOSITION 2.3.12. *Let q be even and let M be an abelian p-subgroup of central type of M_2. Consider a non-degenerate cocycle $\omega\colon \widehat{M} \times \widehat{M} \to K^\times$. If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.*

PROOF. In this case we take $\tau = \pi\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)$. A direct computation shows that $(\tau M_2 \tau^{-1}) \cap M_2 = \{\pi(1)\}$ and hence $(\tau M \tau^{-1}) \cap M = \{\pi(1)\}$. The elements $v \in M$ such that the characteristic polynomial of a lifting of τv is $(\theta^i - z)^3$ for some $i \in \{0, 1, 2\}$ are $v = \pi(1)$ and $v = \pi\left(\begin{smallmatrix} 1 & 1 & \theta^{2l} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ for $l \in \{1, 2\}$. In particular,

$$M_{C_{(2,1)}} = \pi(1),$$

while

$$M_{C_{(3)}} \subseteq \left\{ \pi\left(\begin{smallmatrix} 1 & 1 & \theta^{2l} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right) \,:\, l = 1, 2 \right\}.$$

We divide the proof into cases, according to the size of $M_{C_{(3)}}$.
Case 1) Suppose that $M_{C_{(3)}} = \emptyset$. We write $(a,b) \in M$ to indicate that $\pi\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$. Then

$$\begin{aligned}
\chi(y_\chi^2) &= \frac{\chi(C_{(2,1)})^2}{|M|} \sum_{v \in M} \chi(\tau v \tau v^{-1}) \\
&= \frac{(q-1)^4(2q+1)^2}{9|M|} \sum_{(a,b)\in M} \chi\left(\pi\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right)\right) \qquad (2.3.13) \\
&= \frac{(q-1)^4(2q+1)^2}{9|M|} \sum_{(a,b)\in M} \chi\left(\pi\left(\begin{smallmatrix} 1 & a & a^2+b \\ a & a^2+1 & a+a^3+ab \\ b & a+ab & 1+a^2+a^2b+b^2 \end{smallmatrix}\right)\right).
\end{aligned}$$

Computing the characteristic polynomial of the matrix in the expression of $\chi(y_\chi^2)$ in (2.3.13) and forcing it to be equal to $(\theta^k - z)^3$ for some $k \in \{0,1,2\}$, we obtain that $(a,b) \in \mathbb{F}_q^2$ must solve the following system of equations

$$\begin{aligned}
1 + a^2b + b^2 &= \theta^k \\
1 + a^2b + b^2 &= \theta^{2k}.
\end{aligned} \qquad (2.3.14)$$

This system has solutions only for $k = 0$. In this case, the solutions are $(a,0)$ for every $a \in \mathbb{F}_q$ and (a,a^2), for every $a \in \mathbb{F}_q^\times$.
If $a = 0$ and $b = 0$, the corresponding matrix showing up in $\chi(y_\chi^2)$ is the identity.
If $a \neq 0$, then by Lemma A.2.2, the corresponding matrix is of Jordan type (3). We want to show that the number of pairs $(a,b) \in \{(a,0),(a,a^2) : a \neq 0\}$ such that $\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$, is even.
Suppose that $\pi\left(\begin{smallmatrix} 1 & a & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$. Then,

$$\left(\begin{smallmatrix} 1 & a & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right)^3 = \left(\begin{smallmatrix} 1 & a & a^2 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M,$$

and so $N_a := \#\{a \in \mathbb{F}_q^\times : (a,0) \in M\} = \#\{a \in \mathbb{F}_q^\times : (a,a^2) \in M\}$.
Hence

$$\chi(y_\chi^2) = \frac{(q-1)^6(2q+1)^2}{27|M|}\Big(2N_a + (q+1)(q^2+q+1)\Big) \in \mathbb{Q} \setminus \mathbb{Z}.$$

So in the case $M_{C_{(3)}} = \emptyset$, we conclude that $\frac{1}{|M|} \in R$.

Case 2) Suppose that $|M_{C_{(3)}}| \neq 0$. Observe that $\pi\left(\begin{smallmatrix} 1 & 1 & \theta \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$ if and only if $\pi\left(\begin{smallmatrix} 1 & 1 & \theta^2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$, since

$$\pi\left(\begin{smallmatrix} 1 & 1 & \theta \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)^3 = \pi\left(\begin{smallmatrix} 1 & 1 & \theta^2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right).$$

Therefore $|M_{C_{(3)}}| \neq 0$ implies

$$M_{C_{(3)}} = \left\{ \pi \left(\begin{smallmatrix} 1 & 1 & \theta^{2l} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix} \right) \, : \, l = 1, 2 \right\}.$$

Hence,

$$\chi(y_\chi^2) = \frac{1}{|M|} \Big[\chi(C_{(2,1)})^2 \sum_{v \in M} \chi\big(\tau v \tau v^{-1}\big) + 2\chi(C_{(2,1)})\chi(C_{(3)}) \sum_{\substack{v \in M \\ x \in M_{C_{(3)}}}} \chi\left(\tau x v \tau v^{-1}\right) +$$

$$+ \chi(C_{(3)})^2 \sum_{\substack{v \in M \\ x, x' \in M_{C_{(3)}}}} \chi\left(\tau x x' v \tau v^{-1}\right) \Big].$$

We aim at showing that the sum between brackets is an odd integer. The first summand was already analyzed in the previous case, while the second one is clearly even. Thus, we are left to study

$$\begin{aligned} &\sum_{\substack{(a,b) \in M \\ x, x' \in M_{C_{(3)}}}} \chi\left(\pi \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix} \right) \left(\begin{smallmatrix} 1 & 1 & \theta^i \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix} \right) \left(\begin{smallmatrix} 1 & 1 & \theta^j \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix} \right) \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix} \right) \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix} \right) \left(\begin{smallmatrix} 1 & -a & a^2-b \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{smallmatrix} \right) \right) \\ &= \sum_{(a,b) \in M} \chi\left(\pi \left(\begin{smallmatrix} 1 & a & a^2+b \\ a & a^2+1 & a(a^2+b+1) \\ b+\theta^{2i}+\theta^{2j}+1 & a(b+\theta^{2i}+\theta^{2j}) & (a^2+b)(b+\theta^{2i}+\theta^{2j})+b+1 \end{smallmatrix} \right) \right). \end{aligned} \tag{2.3.15}$$

By Lemma A.2.3, the matrix appearing in equation (2.3.15) is in P if and only if $(a, b) \in \{(0, 0), (0, 1), (a, 0), (a, a^2), (1, \theta^l)\}$, for l running in $\{1, 2\}$.
Observe that since $\pi \left(\begin{smallmatrix} 1 & 1 & \theta \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix} \right) \in M$, then its square $\pi \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix} \right)$ belongs to M. This implies that $(0, 0), (0, 1), (1, \theta), (1, \theta^2)$ lie in M.
For $i, j \in \{1, 2\}$ such that $i \neq j$ and $k = 0$, by Lemma A.2.3 the matrix appearing in the expression (2.3.15) is in P if and only if $(a, b) = (0, 0)$ and in particular in this case it is the identity thanks to Lemma A.2.4. Then, there are precisely 2 occurrences of the identity in the sum in expression (2.3.15) of $\chi(y_\chi^2)$.
Moreover, for $i = j$ and $k = 0$, in virtue of Lemma A.2.3 the matrix appearing in the expression (2.3.15) is in P if and only if

$$(a, b) \in \{(0, 0), (0, 1), (a, 0), (a, a^2) : a \in \mathbb{F}_q^\times\}$$

and in the cases in which $(a, b) \in \{(0, 0), (0, 1)\}$ the Jordan type of the corresponding matrix in the expression of $\chi(y_\chi^2)$ in (2.3.15) is $(2, 1)$, by Lemma A.2.4. On the other hand, in light of Lemma A.2.4, if $(a, b) \in \{(a, 0), (a, a^2) : a \in \mathbb{F}_q^\times\}$ the Jordan type of the corresponding matrix in the expression of $\chi(y_\chi^2)$ in (2.3.15) is (3). Arguing as in Case 1, we have that $N_a = \#\{a \in \mathbb{F}_q^\times : (a, 0) \in M\} = \#\{a \in \mathbb{F}_q^\times : (a, a^2) \in M\}$. Hence, for $i = j$ and $k = 0$, in the sum in expression (2.3.15), there are four 2-elements of Jordan type $(2, 1)$ and $2N_a$ elements of Jordan type (3).

Finally, for $i = j$ and $k \in \{1, 2\}$, in light of Lemma A.2.3 the summand appearing in the expression (2.3.15) is nonzero if and only if $(a, b) \in \{(1, \theta), (1, \theta^2)\}$ and the Jordan type of the corresponding matrix is $(2, 1)$ thanks to Lemma A.2.4. In consequence, there are eight occurrences of 2-elements of Jordan type $(2, 1)$ in the sum in expression (2.3.15).
Thus, $\chi(y_\chi^2)$ equals

$$\frac{1}{|M|}\Big[\chi(C_{(2,1)})^2\frac{(q-1)^2}{3}\left(2N_a + (q+1)(q^2+q+1)\right) + 2\chi(C_{(2,1)})\chi(C_{(3)})\sum_{\substack{v\in M\\ x\in M_{C_{(3)}}}}\chi\left(\tau x v\tau v^{-1}\right) +$$

$$+\chi(C_{(3)})^2\frac{(q-1)^2}{3}\left(2(q^2+q+1)(q-1) + 12(2q+1) + 2N_a\right)\Big].$$

Since the second and the third summands are even, while the first is odd, we have $\chi(y_\chi^2) \in \mathbb{Q}\setminus\mathbb{Z}$ and so $\frac{1}{|M|} \in R$. $\square$

This concludes the proof of Theorem 2.1.1 for $\mathbf{PSL}_3(q)$.

3.5. The Suzuki group ${}^2B_2(q)$. We retain notations from Subsection 2.3. Here $q = 2^{2n+1}$, where $n \geq 1$. We consider the induced character $\chi = \mathrm{Ind}_U^G(\mathbb{1}_U)$ and the set $P = \bigcup_{g\in G} gUg^{-1}$. We know that χ vanishes outside P. We compute its values at U.We start with a non-trivial involution $u(0, b)$. It is conjugate to $u(0, 1)$ by a certain $t_\kappa \in T$ in view of (2.2.2). Note that $gu(0, 1)g^{-1} \in U$ implies $gu(0, 1)g^{-1} \in Z(U)$. Using (2.2.2) and that $C_G(u(0, 1)) = U$, one can check the equality $\{g \in G : gu(0, 1)g^{-1} \in U\} = TU$. As a consequence of this, and (2.2.2) again, the same equality holds for $u(0, b)$. Now, an arbitrary $u(a, b)$, which is not an involution, has order 4. Then, we have the following chain of inclusions:

$$TU \subseteq \{g \in G : gu(a, b)g^{-1} \in U\} \subseteq \{g \in G : gu(a, b)^2g^{-1} \in U\} = TU.$$

Hence:

$$\chi(1) = \frac{|G|}{|U|} = (q-1)(q^2+1),$$

$$\chi(v) = \frac{|TU|}{|U|} = q-1, \qquad \text{for } v \in U\setminus\{1\}.$$

In this case, the set I_χ particularizes to $I_\chi = \{\{1\}, P\setminus\{1\}\}$. Let $P^\bullet = P\setminus\{1\}$. Clearly, $M_{\{1\}} = \emptyset$. The next step is to find $M_{P^\bullet}$. We analyze when the following product is a 2-element:

$$\tau u(0, b) = \begin{pmatrix} 0&0&0&1\\ 0&0&1&0\\ 0&1&0&0\\ 1&0&0&0 \end{pmatrix}\begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ b&0&1&0\\ \theta(b)&b&0&1 \end{pmatrix} = \begin{pmatrix} \theta(b)&b&0&1\\ b&0&1&0\\ 0&1&0&0\\ 1&0&0&0 \end{pmatrix}.$$

One can see, by looking at the $(4, 3)$-entry, that $(\tau u(0, b))^4 = 1$ if and only if $b = 0$. Then:

$$M_{P^\bullet} = \{v \in M : \tau v \in P^\bullet\} = \{1\}.$$

Equation (1.6.7) now takes the following form. Notice that, in view of the preceding discussion, $(\tau v)^2 \in P$ if and only if $v = 1$. Hence, the only contribution in the second sum occurs when $v = 1$:

$$\begin{aligned}\chi(y_\chi^2) &= \frac{\chi(P^\bullet)^2}{|M|} \sum_{\substack{v\in M \\ x,x'\in M_{P^\bullet}}} \chi\Big(\tau x x' v \tau v^{-1}\Big) \\ &= \frac{\chi(P^\bullet)^2}{|M|} \sum_{v\in M} \chi\Big((\tau v)^2\Big) \\ &= \frac{(q-1)^3(q^2+1)}{|M|}.\end{aligned}$$

This is an irreducible fraction because $|M|$ is a power of 2. As in the previous cases, we can derive from this that $\frac{1}{|M|} \in R$.

This finishes the proof of Theorem 2.1.1. □

4. Proof of Theorem 2.1.2

This section aims at proving Theorem 2.1.2. As in Section 3, we devote each subsection to the proof of the conclusion of Theorem 2.1.2 for the groups listed in there.

4.1. Projective special linear group $\mathbf{PSL}_2(q)$. We will use several characters of $\mathbf{PSL}_2(q)$ in the proof. Composition with the projection $\pi : \mathbf{SL}_2(q) \to \mathbf{PSL}_2(q)$ induces a one-to-one correspondence between characters of $\mathbf{PSL}_2(q)$ and characters of $\mathbf{SL}_2(q)$ with kernel containing $\{\pm 1\}$; see [36, Lemma 2.22]. In particular, if φ is a character of $\mathbf{SL}_2(q)$ such that $\varphi(1) = \varphi(-1)$, then $\tilde{\varphi} : \mathbf{PSL}_2(q) \to \mathbb{C}, \pi(g) \mapsto \varphi(g)$ is a well-defined character of $\mathbf{PSL}_2(q)$.

For convenience, we will work directly with the character table of $\mathbf{SL}_2(q)$. We will use [6, Table 5.4, page 58]. We entirely adopt the notation fixed there, overlooking the clash with our R, which is easily resolved from the context. The necessary information to work with this table can be found in the following parts of [6]. For the conjugacy classes, see: Equation 1.1.9 in page 5, Theorem 1.3.3 in page 8, Table 1.1 in page 9, and Exercise 1.4(d) in page 12. For the irreducible characters, see: Subsection 3.2.3 in page 32, Summary 3.2.5 in page 34, Remark in page 35, Section 4.3 in page 45, Exercise 4.1(c) in page 48, and Proposition 5.3.1 in page 57.

The original description of the character table of $\mathbf{SL}_2(q)$ given by Schur can be found in [19, Theorem 38.1]. The character table of $\mathbf{PSL}_2(q)$ appears, for instance, in [43, Theorems 8.9 and 8.11, pages 280-282]. We stress that its size is $\frac{q+5}{2}$ when q is odd.

Fix a pair $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ such that $x^2 + y^2 = -1$. By Remark 1.3.4

and Proposition 2.2.1(ii) we can assume that M is the subgroup of $\mathbf{PSL}_2(q)$ generated by $r = \pi\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $s = \pi\left(\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right)$. We will use two different characters in the proof according to the following distinction:

A. Case $q \equiv_4 -1$. This case follows the same strategy as that of Subsection 3.2. We take the induced character $\chi = \mathrm{Ind}_{\pi(U)}^{\mathbf{PSL}_2(q)}(\mathbb{1}_{\pi(U)})$ from the Sylow p-subgroup $\pi(U)$ of $\mathbf{PSL}_2(q)$. We know that its non-zero values are:

$$\chi(1) = \frac{q^2-1}{2} \qquad \text{and} \qquad \chi(\pi(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix})) = \frac{q-1}{2}, \quad \text{for } c \neq 0.$$

B. Case $q \equiv_4 1$. Set $\Theta = \{\theta \in \overline{\mu_{q+1}} : R'(\theta)(1) = R'(\theta)(-1)\}$. Here, $\overline{\mu_{q+1}}$ denotes the set parametrizing the family of irreducible characters $R'(\theta)$ of $\mathbf{SL}_2(q)$, see [6, page 45]. We consider the character

$$\varphi = \mathbb{1}_G - \mathrm{St} - 2\sum_{\theta\in\Theta} R'(\theta).$$

Observe that $\varphi(1) = \varphi(-1)$, so we can view $\tilde{\varphi}$ as a character of $\mathbf{PSL}_2(q)$. Its values are given in the following table:

Character \ Conj. classes	$\pi(1)$	$\pi(u_+)$	$\pi(u_-)$	$\pi(d(a))$	$\pi(d'(\xi))$
$\tilde{\varphi}$	$\frac{1-q^2}{2}$	$\frac{q+1}{2}$	$\frac{q+1}{2}$	0	0

The elements $\pi(u_+)$ and $\pi(u_-)$ have order p, whereas the elements of the form $\pi(d(a))$ and $\pi(d'(\xi))$ are semisimple.

As in Subsection 3.2, we write P for the set of elements of order p together with the identity element. Recall that $P = \{\pi(A) \in \mathbf{PSL}_2(q) : \mathrm{Tr}(A) = \pm 2\}$. Define $\psi = \tilde{\varphi}$ if $q \equiv_4 1$ and $\psi = \chi$ if $q \equiv_4 -1$. Observe that ψ vanishes outside P. Define also $n_q = \frac{q+1}{2}$ if $q \equiv_4 1$ and $n_q = \frac{q-1}{2}$ if $q \equiv_4 -1$.

We need to treat separately the first three values of p:

1. Case $p = 3$. Here we assume that $m > 1$ since $\mathbf{PSL}_2(3)$ is not simple. We consider the group associated with the pair $(x, y) = (1, 1)$. Fix $\lambda \in \mathbb{F}_q \setminus \mathbb{F}_3$ and take $\tau = \pi\left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right)$. This choice of λ ensures that $M \cap (\tau M \tau^{-1}) = \{1\}$. We compute the element y_ψ as in (1.6.1):

$$\begin{aligned} y_\psi &= \frac{1}{|M|}\sum_{v,v'\in M}\psi(v\tau v')v\tau v' = \frac{1}{|M|}\sum_{v,v'\in M}\psi(\tau v'v)v\tau v' \\ &= \frac{1}{|M|}\sum_{v,v'\in M}\psi(\tau v')v\tau v'v = \frac{n_q}{4}\sum_{v\in M'} v\tau v. \end{aligned} \tag{2.4.1}$$

In the last step we used that $\psi(\tau v') = 0$ for $v' \neq 1$ and $\psi(\tau) = n_q$. For this, note that the trace of the matrices involved is λ, which is different from ± 2. We now compute $\psi(y_\psi^2)$:

$$\begin{aligned}\psi(y_\psi^2) &= \frac{n_q^2}{16}\sum_{v,v'\in M}\psi(v\tau v v'\tau v') = \frac{n_q^2}{16}\sum_{v,v'\in M}\psi(\tau v v'\tau v v') \\ &= \frac{n_q^2}{4}\sum_{v\in M}\psi\Big((\tau v)^2\Big) = \frac{n_q^3}{4}.\end{aligned} \tag{2.4.2}$$

We used in the final equality that $\psi((\tau v)^2) = 0$ for $v \neq 1$ and $\psi(\tau) = n_q$. Again note that the trace of the matrices involved is different from ± 2 because $\lambda \notin \mathbb{F}_3$.

In light of Propositions 1.4.2 and 1.3.7, we have that $\frac{n_q^3}{4} \in R$. Since $\gcd(n_q, 4) = 1$, we obtain that $\frac{1}{4} \in R$. This establishes the statement for $p = 3$.

To deal with the other values of p, observe that $\mathbf{PSL}_2(p)$ is a subgroup of $\mathbf{PSL}_2(q)$. Recall that we constructed the group M from a pair (x, y) in $\mathbb{F}_p \times \mathbb{F}_p$. Since M is contained in $\mathbf{PSL}_2(p)$, by Proposition 1.4.3(i), it is sufficient to handle $\mathbf{PSL}_2(p)$.

2. Case $p = 5$. This case was discussed in [15, Theorem 3.3] as $\mathbf{PSL}_2(5) \simeq A_5$. Nevertheless, we provide a proof in this context for completeness. We consider the pair $(x, y) = (2, 0)$. Take $\tau = \pi\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$. The condition $M \cap (\tau M \tau^{-1}) = \{1\}$ holds and τ has order 5. Pick a primitive 6th root of unity ν in $\mathbb{C}$. Consider a generator a of $\mathbb{F}_5^\times$ and a generator ξ of $\mathbb{F}_{25}^\times$, so $T = \langle d(a)\rangle \simeq C_4$ and $T' = \langle d'(\xi)\rangle \simeq C_6$. Let $\alpha\colon T \to \mathbb{C}^*$ be the group homomorphism mapping $d(a)$ to -1 and let $\theta\colon T' \to \mathbb{C}^*$ be the group homomorphism mapping $d'(\xi)$ to ν^2. Then $R(\alpha)$ and $R'(\theta)$ are the characters constructed as in [6, Chapter 3.2.1] and [6, Chapter 4.2.1] respectively. We work with the character $\phi = \mathrm{St} + R(\alpha) + R'(\theta)$. Note that $\phi(1) = \phi(-1)$, so ϕ descends to a character $\tilde{\phi}$ of $\mathbf{PSL}_2(5)$. Its values are given in the following table:

Conjugacy class	$\pi(1)$	$\pi(u_+)$	$\pi(u_-)$	$\pi(d(a))$	$\pi(d'(\xi))$
Order of representatives	1	5	5	2	3
$\tilde{\phi}$	15	0	0	-1	0

One can see that τs has order 2, the element τr has order 3, and τ and $\tau r s$ have order 5. Then, $\tilde{\phi}(\tau) = \tilde{\phi}(\tau r) = \tilde{\phi}(\tau r s) = 0$ and $\tilde{\phi}(\tau s) = -1$. We calculate $y_{\tilde{\phi}}$ as in (2.4.1):

$$y_{\tilde{\phi}} = \frac{1}{|M|}\sum_{v,v'\in M}\tilde{\phi}(\tau v')v\tau v' v = -\frac{1}{4}\sum_{v\in M} v(\tau s)v.$$

We now compute $\tilde{\phi}(y_{\tilde{\phi}}^2)$ as in (2.4.2). We get:

$$\begin{aligned}\tilde{\phi}(y_{\tilde{\phi}}^2) &= \frac{1}{16}\sum_{v,v'\in M}\tilde{\phi}\Big(v(\tau s v')^2 v\Big) = \frac{1}{16}\sum_{v,v'\in M}\tilde{\phi}\Big((\tau s v')^2 v^2\Big)\\ &= \frac{1}{4}\sum_{v\in M}\tilde{\phi}\Big((\tau s v)^2\Big) = \frac{15}{4}.\end{aligned}$$

By Propositions 1.4.2 and 1.3.7, we have that $\frac{1}{4}\in R$.

3. Case $p = 7$. The proof of this case follows the lines of the preceding one. We work with the group M associated with the pair $(x, y) = (2, 3)$. As before, we take $\tau = \pi\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$, which satisfies $M \cap (\tau M \tau^{-1}) = \{1\}$ and has order 7. Pick a primitive 6th root of unity η and a primitive 8th root of unity ν in $\mathbb{C}$. Let a be a generator of $\mathbb{F}_7^\times$ and let ξ be a generator of $\mathbb{F}_{49}^\times$, so $T = \langle d(a)\rangle \simeq C_6$ and $T' = \langle d'(\xi)\rangle \simeq C_8$. Consider the group homomorphisms $\alpha\colon T \to \mathbb{C}^*$, mapping $d(a)$ to ν^2 and $\theta\colon T' \to \mathbb{C}^*$ mapping $d'(\xi)$ to η^2. Then $R(\alpha)$ and $R'(\theta)$ are the characters constructed as in [6, Chapter 3.2.1] and [6, Chapter 4.2.1] respectively. The character $\phi = R(\alpha) + R'(\theta)$ of $\mathbf{SL}_2(7)$ descends to a character $\tilde{\phi}$ of $\mathbf{PSL}_2(7)$ because $\phi(1) = \phi(-1)$. Its values are given in the following table:

Conjugacy class	$\pi(1)$	$\pi(u_+)$	$\pi(u_-)$	$\pi(d(a))$	$\pi(d'(\xi))$	$\pi(d'(\xi^2))$
Order of representatives	1	7	7	3	4	2
$\tilde{\phi}$	14	0	0	-1	0	2

One can check that τr has order 3, the element τs has order 4, and τ and $\tau r s$ have order 7. Then, $\tilde{\phi}(\tau) = \tilde{\phi}(\tau s) = \tilde{\phi}(\tau r s) = 0$ and $\tilde{\phi}(\tau r) = -1$. We compute $y_{\tilde{\phi}}$ as in (2.4.1):

$$y_{\tilde{\phi}} = \frac{1}{|M|}\sum_{v,v'\in M}\tilde{\phi}(\tau v')v\tau v' v = -\frac{1}{4}\sum_{v\in M} v(\tau r)v.$$

We now compute $\tilde{\phi}(y_{\tilde{\phi}}^2)$ as in (2.4.2). We get:

$$\tilde{\phi}(y_{\tilde{\phi}}^2) = \frac{1}{16}\sum_{v,v'\in M}\tilde{\phi}\Big((\tau r v')^2 v^2\Big) = \frac{1}{4}\sum_{v\in M}\tilde{\phi}\Big((\tau r v)^2\Big) = \frac{1}{4}.$$

By Propositions 1.4.2 and 1.3.7, we have that $\frac{1}{4}\in R$. This establishes the statement of Theorem 2.1.2 for $p = 7$.

4. Case $p > 7$. We need the following lemma, which will be useful in detecting that certain elements do not belong to P:

Lemma 2.4.1. *Let $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ be such that $x^2 + y^2 = -1$. Then, there is $\lambda \in \mathbb{F}_p^\times$ such that $\lambda, \lambda x$, and λy are all different from ± 2.*

PROOF. Note that at least one among x and y is different from ± 2. Otherwise, we would have $2^2+2^2=-1$, which holds only for $p=3$.

If $x \neq \pm 2$ and $y \neq \pm 2$, then we can take $\lambda = 1$ and we are done. Suppose that $x = \pm 2$ and $y \neq \pm 2$. Then, $-1 = x^2+y^2 = 4+y^2$. This implies $y^2=-5$, and thus $(\lambda y)^2 = -5\lambda^2$. From the latter, we deduce that $\lambda y \neq \pm 2$ if and only if $\lambda^2 \neq -5^{-1}\cdot 4$. We also want $\lambda^2 \neq 4$. So, we must choose λ such that $\lambda^2 \notin \{1, 4, -5^{-1}\cdot 4\}$. The number of squares in $\mathbb{F}_p^\times$ is $\frac{p-1}{2}$, and $\frac{p-1}{2} > 3$ if $p > 7$. This guarantees a choice of λ with the required properties. The same argument can be applied for $x \neq \pm 2$ and $y = \pm 2$. $\square$

We pick $\lambda \in \mathbb{F}_p^\times$ satisfying the conclusion of Lemma 2.4.1. Take $\tau = \pi\left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right)$, so $|\tau| = p$. One can verify that our choice of λ ensures that $M \cap (\tau M \tau^{-1}) = \{1\}$. The cardinality of the set $\big\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : x^2+y^2=-1\big\}$ is $p+1$ if $p \equiv_4 -1$ and $p-1$ if $p \equiv_4 1$. For our purpose, we can assume that the pair (x,y) chosen to define the element s in M satisfies $xy \neq 0$.

Recall that $\psi = \tilde{\varphi}$ if $q \equiv_4 1$ and $\psi = \operatorname{Ind}_{\pi(U)}^{\mathbf{PSL}_2(q)}(\mathbb{1}_{\pi(U)})$ if $q \equiv_4 -1$. Computation of (2.4.1) and (2.4.2) gives:

$$y_\psi = \frac{n_p}{4}\sum_{v \in M} v\tau v \quad \text{ and } \quad \psi(y_\psi^2) = \frac{n_p^3}{4},$$

where $n_p = \frac{p+1}{2}$ if $p \equiv_4 1$ and $n_p = \frac{p-1}{2}$ otherwise.
For the first equality we used that $\psi(\tau) = n_p$ and $\psi(\tau v) = 0$ for $v \neq 1$. The latter holds because the traces of the matrices involved is $\lambda, \lambda x$, and λy, which are different from ± 2 by our choice of λ. In the second equality, we used:

(1) That $\tau^2, (\tau r)^2, (\tau s)^2$, and $(\tau rs)^2$ are different from 1. Note that $(\tau s)^2 = 1$ implies $y = 0$. Similarly, $(\tau rs)^2 = 1$ implies $x = 0$. This would contradict our choice of (x,y).
(2) That ψ vanishes on $(\tau r)^2, (\tau s)^2$, and $(\tau rs)^2$. For this, we argue as follows. If ψ did not vanish on $(\tau r)^2$, then $(\tau r)^2$ would have order p. This would give that τr would have order p. But the trace of the matrix
$$\left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & \lambda \end{smallmatrix}\right)$$
is different from ± 2 by our choice of λ. The same applies to $(\tau s)^2$ and $(\tau rs)^2$ as:
$$\left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & y \\ \lambda x + y & \lambda y - x \end{smallmatrix}\right) \quad \text{ and } \quad \left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -y & x \\ x & y \end{smallmatrix}\right) = \left(\begin{smallmatrix} -y & x \\ -\lambda y + x & \lambda x + y \end{smallmatrix}\right).$$

By Propositions 1.4.2 and 1.3.7, we have that $\psi(y_\psi^2) \in R$. Since $\gcd(n_p, 4) = 1$, we obtain that $\frac{1}{4} \in R$. This finishes the proof of Theorem 2.1.2 for $\mathbf{PSL}_2(q)$. $\square$

REMARK 2.4.2. When $p \equiv_4 -1$ any solution of $x^2+y^2=-1$ in $\mathbb{F}_p \times \mathbb{F}_p$ satisfies $xy \neq 0$. When $p \equiv_4 1$, there are solutions such that $xy = 0$. We can deal directly with this situation by modifying our argument in the following way. At most one of $(\tau s)^2$ and $(\tau rs)^2$ is 1. Then:

$$\psi(y_\psi^2) = \left(\frac{p+1}{4}\right)^2 \sum_{v\in M} \psi\Big((\tau v)^2\Big) = \left(\frac{p+1}{4}\right)^2 \Big(\gamma + \frac{p+1}{2}\Big),$$

where $\gamma \in \left\{0, \frac{1-p^2}{2}\right\}$. We obtain:

$$\psi(y_\psi^2) = \begin{cases} \left(\dfrac{p+1}{4}\right)^3 & \text{if} \quad \gamma = 0, \\ \dfrac{(p+1)^3(2-p)}{32} & \text{if} \quad \gamma = \dfrac{1-p^2}{2}. \end{cases}$$

Since $p \equiv_4 1$, it follows that $\frac{1}{4} \in R$.

This concludes the proof of Theorem 2.1.2 for $\mathbf{PSL}_2(q)$.

4.2. The Janko group. We keep notations from Subsection 2.4. By Proposition 2.2.12, the Klein four groups are all conjugate. Moreover, let t be the involution such that $C_G(t) \simeq \langle t\rangle \times F$. Since $F \simeq A_5 \simeq \mathbf{PSL}_2(5)$, then F contains a subgroup isomorphic to the Klein four group. Therefore, we can choose a subgroup $M \simeq C_2 \times C_2$ in F as a representative. Remark 1.3.4 and Theorem 2.1.2 for $\mathbf{PSL}_2(5)$ imply that Theorem 2.1.1 holds for the Janko group.

□

5. Proof of Theorem 2.1.3

We are left to prove Theorem 2.1.3; this turns out to be a consequence of Theorem 2.1.1 and/or Theorem 2.1.2 and the description of abelian subgroups of central type.

5.1. Projective special linear group $\mathbf{PSL}_2(q)$. By Proposition 2.2.1, the only abelian subgroups of central type of $\mathbf{PSL}_2(q)$ up to automorphisms are Klein four groups and p-subgroups. Hence, Theorem 2.1.1 and Theorem 2.1.2 for $\mathbf{PSL}_2(q)$ imply that Theorem 2.1.3 holds for $\mathbf{PSL}_2(q)$. □

As was the case with Corollary 2.1.4, Theorem 2.1.3 implies the following:

Corollary 2.5.1. *Let Ω be a non-trivial twist of $\mathbb{C}\mathbf{PSL}_2(q)$ arising from a 2-cocycle on an abelian subgroup of $\mathbf{PSL}_2(q)$. Then, the complex semisimple Hopf algebra $(\mathbb{C}\mathbf{PSL}_2(q))_\Omega$ does not admit a Hopf order over any number ring.*

5.2. The Janko group. Proposition 2.2.12 guarantees that the abelian subgroups of central type for the Janko group are all conjugate and isomorphic to the Klein four group. Hence, Theorem 2.1.3 is equivalent to Theorem 2.1.2 for the Janko group. □

Also in this case, we deduce the following:

Corollary 2.5.2. *Let G be the Janko group. Let Ω be a non-trivial twist of $\mathbb{C}G$ arising from a 2-cocycle on an abelian subgroup of G. Then, the complex semisimple Hopf algebra $(\mathbb{C}G)_\Omega$ does not admit a Hopf order over any number ring.*

5.3. The Suzuki group ${}^2B_2(q)$. Proposition 2.2.11 implies that the abelian subgroups of central type of the Suzuki groups are all 2-groups. Hence, Theorem 2.1.3 is equivalent to Theorem 2.1.2 for ${}^2B_2(q)$, concluding the proof.

Corollary 2.5.3. *Let Ω be a non-trivial twist of ${}^2B_2(q)$ arising from a 2-cocycle on an abelian subgroup of ${}^2B_2(q)$. Then, the complex semisimple Hopf algebra $(\mathbb{C}{}^2B_2(q))_\Omega$ does not admit a Hopf order over any number ring.*

6. Twists of finite non-abelian simple groups

Let G be a finite non-abelian simple group and Ω a non-trivial twist for $\mathbb{C}G$ arising from a 2-cocycle on an abelian subgroup of G. In [15, Question 5.1] it was asked whether $(\mathbb{C}G)_\Omega$ can admit a Hopf order over a number ring. We can partially answer this question in the negative building on Theorems 2.1.1 and 2.1.2 and two results on the subgroups structure of finite non-abelian simple groups.

Recall from [66, Section 2] that a *minimal simple group* is a non-abelian simple group all of whose proper subgroups are solvable. The following remarkable classification was established in [66, Corollary 1, page 388]:

Theorem 2.6.1 (Thompson). *Every minimal simple group is isomorphic to one of the following groups:*

(i) $\mathbf{PSL}_2(2^p)$*, with p a prime.*
(ii) $\mathbf{PSL}_2(3^p)$*, with p an odd prime.*
(iii) $\mathbf{PSL}_2(p)$*, with $p > 3$ prime such that 5 divides p^2+1.*
(iv) ${}^2B_2(2^p)$*, with p an odd prime.*
(v) $\mathbf{PSL}_3(3) \simeq \mathbf{SL}_3(3)$.

Relying on this and the classification of the finite simple groups, the following result was proved in [3, Theorem 1]:

Theorem 2.6.2 (Barry-Ward). *Every finite non-abelian simple group contains a minimal simple group as a subgroup.*

Theorems 2.1.1 and 2.1.2 and Proposition 1.4.3(i), reinforced with the previous two results, give as a consequence:

Theorem 2.6.3. *Let K be a number field and G a finite non-abelian simple group. Then, there is a twist Ω for KG, arising from a 2-cocycle on an abelian subgroup of G, such that $(KG)_\Omega$ does not admit a Hopf order over $\mathcal{O}_K$.*

The statement for the complexified group algebra now follows as in Corollary 2.1.4:

Corollary 2.6.4. *Let G be a finite non-abelian simple group. Then, there is a twist Ω for $\mathbb{C}G$, arising from a 2-cocycle on an abelian subgroup of G, such that $(\mathbb{C}G)_\Omega$ does not admit a Hopf order over any number ring.*

For the sporadic groups or the Tits group, Theorem 2.6.3 and Corollary 2.6.4 can be deduced from [15, Theorem 3.3, Remark 3.4, and Corollary 3.5] in view of the following remark:

Remark 2.6.5. Let G be a sporadic group or the Tits group ${}^2F_4(2)'$. Then, G has a subgroup isomorphic to A_5.

This remark can be verified by inspection of the tables of maximal subgroups for the sporadic groups in [70, Section 4] and that for the Tits group in [68, Theorem 1] and [67]. A close look reveals the inclusions as listed below:

Group	Contains
M_{11}	S_5
M_{23}	A_8
J_1	A_5
J_4	M_{22}
Co_1	A_9
Fi_{22}	S_{10}
HS	S_8
Ru	A_6
HN	A_{12}
B	S_5

Group	Contains
M_{12}	S_5
M_{24}	A_8
J_2	A_5
Co_2	M_{23}
Fi_{23}	S_{12}
McL	A_7
Suz	A_7
Ly	M_{11}
$\mathbb{M}$	A_5

Group	Contains
M_{22}	A_7
J_3	A_5
Co_3	S_5
Fi'_{24}	A_5
He	$S_4(4)$
$O'N$	A_7
Th	S_5
${}^2F_4(2)'$	$\mathbf{PSL}_2(5^2)$

For the Tits group, note that $\mathbf{PSL}_2(5^2)$ contains $\mathbf{PSL}_2(5)$, which is isomorphic to A_5; see [64, Theorem 6.26(iv), page 414] for a more general statement.

Remark 2.6.6. One may relax the hypothesis on G being simple in Theorem 2.6.3 and Corollary 2.6.4 provided G contains a non-abelian simple group in light of Proposition 1.4.3(i). Among the groups satisfying this condition we find almost simple groups and some families of primitive groups, see [18, Section 4.8] for more details.

In our way to Corollary 2.6.4 we showed that the complex group algebra of any finite non-abelian simple group can be twisted to produce a simple non-commutative and non-cocommutative Hopf algebra. This was first proved by Hoffman in [30] following a different strategy that does not use minimal simple groups.

CHAPTER 3

Non-existence of Hopf orders for products of certain Frobenius groups

The aim of this Chapter is to prove the non existence of Hopf orders for twisted group algebras of some non-simple groups. The groups we consider are of the form $G = \prod_{i=1}^{l} D_i \rtimes_{\varphi_i} M_i$, where each $D_i \rtimes_{\varphi_i} M_i$ is a Frobenius group and M_i is subject to specific conditions.
We firstly introduce Frobenius groups and we recollect some results on them.

1. Frobenius groups and semi-direct products

A Frobenius group is a type of permutation group studied firstly in ([23]). The original formal definition of such a group is the following:

Definition 3.1.1. A Frobenius group G is a transitive permutation group on a finite set X, such that no non-trivial element of G fixes more than one element in X and some non-trivial element of G fixes an element in X.
A subgroup H of G fixing an element of X is called a *Frobenius complement*.

Let G be a Frobenius group and H a Frobenius complement. In [23, V], Frobenius proved that the set of elements that are not conjugate to an element in H together with the identity is a normal subgroup of G . This result is known as Frobenius Theorem. Such normal subgroup is called the *Frobenius kernel* of G.
These groups captured the attention of many mathematicians, leading to equivalent definitions. For exhibiting the ones we need, we recall the following definition.

Definition 3.1.2. An automorphism φ of a group G is fixed-point-free if φ fixes only the identity of G. A subgroup L of $\mathrm{Aut}(G)$ is said to be fixed-point-free on G if every element φ in $L \setminus \{\mathrm{id}_G\}$ is fixed-point-free.

With the Lemma below, we recollect the most common alternative definitions of a Frobenius group.

Lemma 3.1.3. *[34, Sätze 8.2 and 8.5] Let G be a group. The following are equivalent:*

i) G is a Frobenius group;
ii) G has a non-trivial subgroup M such that $gMg^{-1} \cap M = \{1\}$ for every $g \in G \setminus M$;

iii) $G = D \rtimes_\varphi M$, where φ is injective and $\mathrm{Im}\varphi$ is fixed-point-free.

We briefly explain the implication $ii) \Rightarrow iii)$. The subgroup D in iii) is obtained by ii) as $D = G \setminus \bigcup_{g\in G} g(M \setminus \{1\})g^{-1}$, which is normal by Frobenius theorem.
In this Chapter, we will mainly use condition iii) of Lemma 3.1.3. The standard terminology is inherited from this equivalent definition, so M is called a Frobenius complement, while D is called the Frobenius kernel.
A property we need is the relation between the orders of the Frobenius kernel and of a Frobenius complement.

Proposition 3.1.4. *[34, Satz 8.3] Let $G = D \rtimes_\varphi M$ be a Frobenius group. Then $|M|$ is a divisor of $|D| - 1$.*

In particular, the latter implies that the order of the Frobenius complement M is coprime with the order of the Frobenius kernel D.

Example 3.1.1. A simple example of a Frobenius group is the symmetric group $S_3 = C_3 \rtimes_\varphi C_2$, with

$$\varphi\colon C_2 \to \mathrm{Aut}(C_3),\ x \mapsto \varphi(x)$$

where x is the non-trivial element in C_2 and $\varphi(x)(g) = g^2$, for every $g \in C_3$. Then φ is injective and $\mathrm{Im}\varphi$ is fixed point free.

Example 3.1.2. This example generalizes Example 3.1.1.
Let p, q be prime numbers with q odd and $q \neq p$. Suppose that p^d divides $q-1$ for some $d \in \mathbb{N}$. Consider the cyclic group C_{q^n} of order q^n, for some $n \in \mathbb{N}$. It is well-known that $\mathrm{Aut}(C_{q^n}) \simeq C_{q^{n-1}(q-1)}$, if q is odd (see for example [46, Section 2.2.5 and 2.2.6]). Then, for every k dividing $q^{n-1}(q-1)$, there exists a unique subgroup $M \leq \mathrm{Aut}(C_{q^n})$ of order k and it is cyclic. Moreover, by [50, Proposition 4.1] if $k|q-1$ such subgroup is fixed-point-free. Thus, the group $G = C_{q^n} \rtimes_\varphi C_{p^d}$, with φ an embedding

$$\varphi\colon C_{p^d} \to \mathrm{Aut}(C_{q^n})$$

is a Frobenius group.

Example 3.1.3. This example exhibits a family of Frobenius groups, whose Frobenius complement is non-abelian. We recall it from [51].
Let $q = p^n$ with p prime and $n \in \mathbb{N}$. Consider the group

$$U := \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \ :\ a, b, c \in \mathbb{F}_q \right\}.$$

The group U is non-abelian and it has order p^{3n}. Let $k \in \mathbb{F}_q^\times$ and let $\varphi_k\colon U \to U$ be the conjugation by $\begin{pmatrix} k^2 & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & 1 \end{pmatrix}$ mapping $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ to $\begin{pmatrix} 1 & ka & k^2c \\ 0 & 1 & kb \\ 0 & 0 & 1 \end{pmatrix}$, which is fixed-point-free for every $k \neq \pm 1$.
Let $\mathbb{E}$ be a subgroup of $\mathbb{F}_q^\times$ of odd order r and consider

$$\varphi\colon \mathbb{E} \to \mathrm{Aut}(U),\ k \mapsto \varphi_k.$$

Then φ is injective and $\mathrm{Im}\varphi$ is a cyclic fixed-point-free group of automorphisms. Then $G := U \rtimes_{\varphi} \mathbb{E}$ is a Frobenius group, with non-abelian Frobenius kernel.

We now recollect some properties on semidirect products and Frobenius groups.

LEMMA 3.1.5. *Let $G = D \rtimes_{\varphi} M$. Then the following holds:*

(1) if M is abelian, then $Cl_G(m) \subseteq Dm$.

Assume in addition that G is Frobenius, then:

(2) $C_G(m) \leq M$, for $m \in M \setminus \{1\}$;

(3) if M abelian then $C_G(m) = M$ for any $m \in M \setminus \{1\}$.

PROOF. (1) For $m \in M$ an element in $Cl_G(m)$ is of the form $dm'mm'^{-1}d^{-1}$, for some $d \in D$ and $m' \in M$. Then

$$dm'mm'^{-1}d^{-1} = dmd^{-1} = d\varphi(m)(d^{-1})m \in Dm,$$

i.e. $Cl_G(m) \subseteq Dm$.
(2) Let $m \in M \setminus \{1\}$. For $d \in D$ and $m' \in M$ the element dm' centralizes m if and only if $dm'mm'^{-1}d^{-1} = m \in M$. Then $dm'mm'^{-1}d^{-1} \in M \cap dMd^{-1}$ which is trivial by Lemma 3.1.3 ii) if $d \neq 1$. This implies that $C_G(m) \leq M$.
(3) This statement follows easily from the previous one. □

In the following lemma we summarize some properties of the conjugacy classes of elements of M.

LEMMA 3.1.6. *Let $G = D \rtimes_{\varphi} M$ be a Frobenius group with M abelian. Then for $m \in M$:*

i) $Cl_G(m) \cap M = \{m\}$;

ii) If $m \neq 1$, then

$$|Cl_G(m)| = |D|;$$

iii)

$$|\bigcup_{m \in M \setminus \{1\}} Cl_G(m)| = |M \setminus \{1\}| \cdot |D|.$$

PROOF. i) The first statement follows from Lemma 3.1.5 (1).
ii) We know that

$$|Cl_G(m)| = \frac{|M||D|}{|C_G(m)|}.$$

Lemma 3.1.5 (3) guarantees that $C_G(m) = M$ hence $|Cl_G(m)| = |D|$.
iii) Let $m, m' \in M$, with $m \neq m'$. Then Lemma 3.1.5 (1) gives that

$$Cl_G(m) \cap Cl_G(m') \subseteq Dm \cap Dm' = \emptyset.$$

This together with ii) implies that

$$|\bigcup_{m \in M \setminus \{1\}} Cl_G(m)| = \sum_{m \in M \setminus \{1\}} |Cl_G(m)| = |M \setminus \{1\}| \cdot |D|.$$

□

2. Aim of the chapter

We now focus on direct products of Frobenius groups with an abelian p-group as Frobenius complement, i.e. groups of the form $G = \prod_{i=1}^{l} D_i \rtimes_{\varphi_i} M_i$, where $D_i \rtimes_{\varphi_i} M_i$ is a Frobenius group and M_i is an abelian p-group for every $i \in \{1, \dots, l\}$.
Moreover, we require that $M = \prod_{i=1}^{l} M_i$ is of central type.
Throughout this chapter we say that an element $g \in G$ is a p-element if its order is a positive power of p.
The aim of this chapter is to establish the following result.

THEOREM 3.2.1. *Let K be a number field and $R \subset K$ a Dedekind domain such that $\mathcal{O}_K \subseteq R$. Let*

- *$l \geq 1$.*
- *p be a prime number.*
- *$G_i = D_i \rtimes_{\varphi_i} M_i$ a Frobenius group, where M_i is an abelian p-group for every $i \in \{1, \dots, l\}$.*
- *$G = \prod_{i=1}^{l} G_i$.*
- *$M = \prod_{i=1}^{l} M_i$ and assume it is of central type.*
- *$\omega : \widehat{M} \times \widehat{M} \to K^{\times}$ be any non-degenerate cocycle.*

If $(KG)_{\Omega_{M,\omega}}$ admits a Hopf order over R, then $\frac{1}{|M|} \in R$. Hence, $(KG)_{\Omega_{M,\omega}}$ does not admit a Hopf order over $\mathcal{O}_K$.

For proving this theorem, we firstly need to establish some properties of the groups just described. To simplify the notations, for every $i \in \{1, \dots, l\}$ we write $m_i.d_i$ instead of $\varphi(m_i)(d_i)$ for $m_i \in M_i$ and $d_i \in D_i$. Bear in mind that $m_i.d_i \in D_i$ for every $d_i \in D_i$, for every $m_i \in M_i$ and for every $i \in \{1, \dots, l\}$.
Furthermore, for an element $x \in KG$, for $i \in \{1, \dots, l\}$ we write x_i to indicate the i-th component in KG_i.

We start describing the form of the p-elements in G_i and G.

LEMMA 3.2.2. *With the above assumptions, an element $g_i \in G_i$ is a p-element if and only if $g_i = d_i m_i$, for $d_i \in d_i$ and $m_i \in M_i$, with $m_i \neq 1$, i.e. $g_i \in G_i \setminus D_i$.*

PROOF. Since $\gcd(|D_i|, |M_i|) = 1$, the subgroup M_i is a p-Sylow subgroup. Hence, every p-element is conjugate to some element in M_i. We denote by $P_i^{\bullet}$ the set of p-elements in G_i. Then

$$|P_i^{\bullet}| = |\bigcup_{m_i \in M_i \setminus \{1\}} Cl_G(m_i)|.$$

In particular, by Lemma 3.1.6 iv)

$$|P_i^\bullet| = |\bigcup_{m_i\in M_i\setminus\{1\}} Cl_G(m_i)| = (|M_i|-1)|D_i|.$$

This implies that $|G_i| = |P_i^\bullet| + |D_i|$. Therefore every element $g_i \notin D_i$ is in $P_i^\bullet$, i.e. g_i is a p-element. We conclude that every p-element of G_i is of the form $d_i m_i$, with $m_i \in M_i \setminus \{1\}$ and $d_i \in D_i$. □

As a consequence, we obtain the following:

COROLLARY 3.2.3. *With the above assumptions, let $G = \prod_{i=1}^l G_i$. Then every p-element in G is an l-tuple $(d_1m_1, d_2m_2, \ldots, d_lm_l) \neq (1, 1, \ldots, 1)$, such that d_im_i is a p-element or the identity for every $i \in \{1, \ldots, l\}$.*

Recall that $M = \prod_{i=1}^l M_i$ which is a Sylow p-subgroup of G and let $D = \prod_{i=1}^l D_i$.
We will use $\chi := \mathrm{Ind}_M^G(\mathbb{1}_M)$ and proceed as explained in Section 6. For this purpose we compute $\chi_i := \mathrm{Ind}_{M_i}^{G_i}(\mathbb{1}_{M_i})$, for every $i \in \{1, \ldots, l\}$, since for $g_i \in G_i$ and for $i \in \{1, \ldots, l\}$ there holds

$$\chi(g_1g_2\ldots g_{l-1}g_l) = \prod_{i=1}^l \chi_i(g_i).$$

LEMMA 3.2.4. *Let $i \in \{1, \ldots, l\}$. For $g_i \in G_i$ we have:*

$$\chi_i(m_i) = \begin{cases} |D_i| & \text{if } g_i = 1, \\ 0 & \text{if } g_i \in D_i \setminus \{1\}, \\ 1 & \text{if } g_i \in G_i \setminus D_i. \end{cases}$$

PROOF. The value at the identity is straightforward. The value on $D_i\setminus\{1\}$ follows from Lemma 3.2.2.
Every element in $P_i^\bullet = G_i \setminus D_i$ is conjugate to some element in $M_i \setminus \{1\}$. Let $m_i \in M_i$, then;

$$\chi_i(m_i) = \frac{|C_G(m_i)||Cl_G(m_i)\cap M_i|}{|M_i|} = \frac{|M_i|\cdot 1}{|M_i|} = 1,$$

since $Cl_G(m_i) \cap M_i = \{m_1\}$ by Lemma 3.1.6 i).

□

3. Proof of Theorem 3.2.1

For $i \in \{1, \ldots, l\}$, we fix $\tau_i \in D_i \setminus \{1\}$ and $\tau = \prod_{i=1}^l \tau_i$.
The intersections $M \cap (\tau M \tau^{-1})$ and $M \cap (\tau^{-1} M \tau)$ are trivial by Lemma 3.1.3 ii). We consider

$$y_{\chi,\tau} = \frac{1}{|M|}\sum_{\sigma\in M\tau M}\chi(\sigma)\sigma \quad \text{and} \quad y_{\chi,\tau^{-1}} = \frac{1}{|M|}\sum_{\sigma\in M\tau^{-1}M}\chi(\sigma)\sigma.$$

Since $\tau_i \neq 1$ for every $i \in \{1, \dots, l\}$, by Corollary 3.2.3, the element τm is a p-element if and only if $m_i \neq 1$ for every $i \in \{1, \dots, l\}$. If this is the case, $\chi(\tau m) = \chi_1(\tau_1 m_1) \cdot \dots \cdot \chi_l(\tau_l m_l) = 1$. Hence;

$$y_{\chi,\tau} = \frac{1}{|M|} \sum_{\substack{m,\bar{m} \in M \\ m_i \neq 1,\, i \in \{1,\dots,l\}}} \bar{m}(\tau m)\bar{m}^{-1} = \frac{1}{|M|} \sum_{\substack{m,\bar{m} \in M \\ m_i \neq 1,\, i \in \{1,\dots,l\}}} (\bar{m}.\tau)m.$$

By the same argument we get

$$y_{\chi,\tau^{-1}} = \frac{1}{|M|} \sum_{\substack{n,\bar{n} \in M \\ n_i \neq 1,\, i \in \{1,\dots,l\}}} \bar{n}(\tau^{-1} n)\bar{n}^{-1} = \frac{1}{|M|} \sum_{\substack{n,\bar{n} \in M \\ n_i \neq 1,\, i \in \{1,\dots,l\}}} (\bar{n}.\tau^{-1})n.$$

Multiplying $y_{\chi,\tau}$ by $y_{\chi,\tau^{-1}}$ we get

$$\begin{aligned} y_{\chi,\tau} y_{\chi,\tau^{-1}} &= \frac{1}{|M|^2} \left(\sum_{\substack{m,\bar{m} \in M \\ m_i \neq 1, i \in \{1,\dots,l\}}} (\bar{m}.\tau)m \right) \left(\sum_{\substack{n,\bar{n} \in M \\ n_i \neq 1, i \in \{1,\dots,l\}}} (\bar{n}.\tau^{-1})n \right) \\ &= \frac{1}{|M|^2} \sum_{\substack{m,\bar{m},n,\bar{n} \in M \\ m_i \neq 1, n_i \neq 1 \\ i \in \{1,\dots,l\}}} (\bar{m}.\tau)m(\bar{n}.\tau^{-1})n \\ &= \frac{1}{|M|^2} \sum_{\substack{m,\bar{m},n,\bar{n} \in M \\ m_i \neq 1, n_i \neq 1 \\ i \in \{1,\dots,l\}}} (\bar{m}.\tau)((m\bar{n}).\tau^{-1})mn. \end{aligned}$$

We evaluate χ on $y_{\chi,\tau} y_{\chi,\tau^{-1}}$. To this purpose, we spell out which summands in the expression of $y_{\chi,\tau} y_{\chi,\tau^{-1}}$ are either the identity or a p-element and then we count the number of occurences of them in the sum.

Fix $i \in \{1, \dots, l\}$. The element $(\bar{m}_i.\tau_i)((m_i\bar{n}_i).\tau_i^{-1})m_i n_i \in D_i M_i$ is the identity if and only if $m_i n_i = 1$ and $(\bar{m}_i.\tau_i)((m_i\bar{n}_i).\tau_i^{-1}) = 1$. This is equivalent to $n_i = m_i^{-1}$ and $(\bar{m}_i^{-1} m_i \bar{n}_i).\tau_i^{-1} = \tau_i^{-1}$. The latter, by definition of Frobenius group, implies that $\bar{m}_i^{-1} m_i \bar{n}_i = 1$. In summary, the conditions we found are

$$n_i = m_i^{-1}, \qquad \bar{m}_i^{-1} m_i \bar{n}_i = 1,$$

for $m_i, n_i \in M_i \setminus \{1\}$. Hence for every $m_i, \bar{m}_i \in M_i \setminus \{1\}$, the elements n_i and $\bar{n}_i$ are uniquely determined, so the number of occurrences of the identity on the i-th component is $(|M_i| - 1)|M_i|$. This implies that the number of occurrences of the identity in the expression of $y_{\chi,\tau} y_{\chi,\tau^{-1}}$ is $\prod_{i=1}^{l} |M_i|(|M_i| - 1) = |M| \prod_{i=1}^{l}(|M_i| - 1)$ and so the contribution to $\chi(y_{\chi,\tau} y_{\chi,\tau^{-1}})$ is $\frac{|D|}{|M|} \prod_{i=1}^{l}(|M_i| - 1)$.

We now investigate the number of occurrences of a p-element of the form $(\bar{m}_i.\tau_i)((m_i\bar{n}_i).\tau_i^{-1})m_i n_i$, for $i \in \{1, \dots, l\}$. In this case, the only condition is that $m_i n_i \neq 1$. This implies that for every $m_i \in M_i \setminus \{1\}$, the element $n_i \in M_i \setminus \{1, m_i^{-1}\}$. On the other hand, the elements $\bar{m}_i$ and $\bar{n}_i$ can run freely in M_i. Hence the number of occurrences of a p-element in the i-th component of the expression of $(y_{\chi,\tau} y_{\chi,\tau^{-1}})_i$ is $|M_i|^2(|M_i|-1)(|M_i|-2)$.

Finally, we spell out when $(\bar{m}.\tau)((m\bar{n}).\tau^{-1})mn$ is a p-element. This happens if and only if there exists a subset $\mathcal{L} \neq \emptyset$ of $\{1, \ldots, l\}$ such that $((\bar{m}.\tau)((m\bar{n}).\tau^{-1})mn)_j$ is a p-element for every $j \in \mathcal{L}$ and $((\bar{m}.\tau)((m\bar{n}).\tau^{-1})mn)_k = 1$ for every $k \in \{1, \ldots, l\} \setminus \mathcal{L}$. The character value of each of these elements is an integer depending only on $\mathcal{L}$. Therefore, for every $\mathcal{L} \subseteq \{1, \ldots, l\}$ the contribution to $\chi(y_{\chi,\tau} y_{\chi,\tau^{-1}})$ of the corresponding set of p-elements lies in $\frac{1}{|M|^2} p|M|\mathbb{Z}$, because each $|M_i|$ factor occurs at least once and at least one factor $|M_i|$ occurs as a square. Therefore

$$\chi(y_{\chi,\tau} y_{\chi,\tau^{-1}}) \in \frac{1}{|M|} \left(|D| + p\mathbb{Z}\right).$$

Since $\gcd(|D|, p) = 1$ we have the statement. □

Remark 3.3.1. Notice that if $G = D \rtimes_\varphi M$ is a Frobenius group with M a p-group, then M can not be of central type. Indeed, the Sylow subgroups of a Frobenius complement are either cyclic or generalised quaternion groups ([34, Satz 8.15]). Then for applying Theorem 3.2.1 we need $l > 1$ and, more precisely, even.

Remark 3.3.2. Let $i \in \{1, \ldots, l\}$ and p, q_i be prime numbers with q_i odd and $q_i \neq p$ for every i. Suppose that for every $i \in \{1, \ldots, l\}$ the power p^{d_i} divides $q_i - 1$ for some $d_i \in \mathbb{N}$. Consider $G = \prod_{i=1}^{l} C_{q_i^{n_i}} \rtimes_{\varphi_i} C_{p^{d_i}}$, where $C_{q_i^{n_i}} \rtimes_{\varphi_i} C_{p^{d_i}}$ are as in Example 3.1.2. Hence, Theorem 3.2.1 holds for G when $\prod_{i=1}^{l} C_{p^{d_i}}$ is of central type. This family of examples contains the family of groups $G = (C_q \rtimes C_p) \times (C_q \rtimes C_p)$, described in Remark 1.3.6. For the twisted group algebras associated to such groups the non existence of Hopf orders was already established by Cuadra and Meir in [15] with a different approach. Observe that, as we have seen in Remark 1.3.6, in the case under consideration, the associated twisted Hopf algebra is simple.

For the other families of groups studied in this chapter it is not yet clear if the twisted Hopf algebra is simple or not. This question could be taken into account for future work.

CHAPTER 4

Preliminaries on monoidal categories

In this chapter we recollect some definitions and results on monoidal categories and bi-module categories. Secondly, we spell out transport of structure through an equivalence.

1. Monoidal categories and $\mathcal{C}$-module categories

We start with the definition of a monoidal category that, as the name suggests, is the categorification of the notion of a monoid.

Definition 4.1.1. [22, Definition 2.1] A monoidal category is a sextuple $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1, l, r)$, where $\mathcal{C}$ is a category and $\otimes_{\mathcal{C}} \colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is a bifunctor called the tensor product bifunctor, $a \colon (- \otimes_{\mathcal{C}} -) \otimes_{\mathcal{C}} - \to - \otimes_{\mathcal{C}} (- \otimes_{\mathcal{C}} -)$ is a natural isomorphism:

$$a_{X,Y,Z} \colon (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{C}} Z \simeq X \otimes_{\mathcal{C}} (Y \otimes_{\mathcal{C}} Z) \qquad \text{for all } X, Y, Z \in \mathcal{C},$$

called the associativity constraint, $1 \in \mathcal{C}$ is an object of $\mathcal{C}$, $l, r \colon \mathcal{C} \to \mathcal{C}$ are two natural isomorphisms

$$\begin{aligned} &l_X \colon 1 \otimes_{\mathcal{C}} X \to X, \\ &r_X \colon X \otimes_{\mathcal{C}} 1 \to X \qquad \text{for all } \ X \in \mathcal{C}, \end{aligned}$$

subject to the following axioms.
1. The pentagon axiom. The diagram

$$\begin{tikzcd}
& ((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{C}} Z) \otimes_{\mathcal{C}} W \arrow[dl, "a_{X\otimes_{\mathcal{C}}Y,Z\otimes_{\mathcal{C}}\mathrm{id}_W}"'] \arrow[dr, "a_{X\otimes_{\mathcal{C}}Y,Z,W}"] & \\
(X \otimes_{\mathcal{C}} (Y \otimes_{\mathcal{C}} Z)) \otimes_{\mathcal{C}} W \arrow[d, "a_{X,Y\otimes_{\mathcal{C}}Z,W}"'] & & (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{C}} (Z \otimes_{\mathcal{C}} W) \arrow[d, "a_{X,Y,Z\otimes W}"] \\
X \otimes_{\mathcal{C}} ((Y \otimes_{\mathcal{C}} Z) \otimes_{\mathcal{C}} W) \arrow[rr, "\mathrm{id}_X \otimes_{\mathcal{C}} a_{Y,Z,M}"] & & X \otimes_{\mathcal{C}} (Y \otimes_{\mathcal{C}} (Z \otimes_{\mathcal{C}} W))
\end{tikzcd} \tag{4.1.1}$$

is commutative for all objects $X, Y, Z, W \in \mathcal{C}$.
2. The unit axiom. The diagram

$$
\begin{tikzcd}
(X \otimes_{\mathcal{C}} 1) \otimes_{\mathcal{C}} Y \arrow[rr, "a_{X,1,Y}"] \arrow[dr, "r_X \otimes_{\mathcal{C}} \mathrm{id}_Y"'] & & X \otimes_{\mathcal{C}} (1 \otimes_{\mathcal{C}} Y) \arrow[dl, "\mathrm{id}_X \otimes_{\mathcal{C}} l_Y"] \\
& X \otimes_{\mathcal{C}} Y &
\end{tikzcd}
\tag{4.1.2}
$$

commutes for all $X, Y \in \mathcal{C}$.

Definition 4.1.2. Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1, l, r)$ be a monoidal category. The monoidal category $(\mathcal{C}^{\mathrm{op}}, \otimes_{\mathcal{C}}^{\mathrm{op}}, a^{\mathrm{op}}, 1, l^{\mathrm{op}}, r^{\mathrm{op}})$ opposite to $\mathcal{C}$ is defined as follows. As a category $\mathcal{C}^{\mathrm{op}} = \mathcal{C}$, its tensor product is given by $X \otimes_{\mathcal{C}}^{\mathrm{op}} Y := Y \otimes_{\mathcal{C}} X$, the associativity constraint of $\mathcal{C}^{\mathrm{op}}$ is $a^{\mathrm{op}}_{X,Y,Z} := a^{-1}_{Z,Y,X}$ and $l^{\mathrm{op}} = r$, $r^{\mathrm{op}} = l$.

Definition 4.1.3. Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1, l, r)$ be a monoidal category. Then, $\mathcal{C}$ is called *strict* if $(X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{C}} Z = X \otimes_{\mathcal{C}} (Y \otimes_{\mathcal{C}} Z)$, and $X \otimes_{\mathcal{C}} 1 = X = 1 \otimes_{\mathcal{C}} X$ for all $X, Y, Z \in \mathcal{C}$ and the associativity and the unit constraints are the identity maps.

Example 4.1.1. Let K be a field and consider the category Vec of all vector spaces over K. This category is a monoidal category, where the product is the usual tensor product over K, the associativity constraint is the change of brackets, the unit object is K and l and r are respectively the left and right multiplication by scalars.

Example 4.1.2. Let H be a Hopf algebra over K. Then, the category of H-modules is a monoidal category. By the previous example, its underlying category of vector spaces is a monoidal category. Furthermore, the tensor product of H-modules becomes an H-module by composition with the comultiplication, the unit object K becomes a H-module by means of the counit. Moreover, the compatibility of the associative constraint with the action of H follows from the coassociativity of the comultiplication.

Remark 4.1.4. Abusing notation, we will consider the above category as a strict monoidal category, thanks to Mac Lane's theorem [22, Theorem 2.8.5].

In the following definitions, we suppress the unit constraint l and r unless necessary.

Definition 4.1.5. [22, Definition 2.10.1] Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ be a monoidal category. An object X^* in $\mathcal{C}$ is said to be a left dual of X if there exist morphisms $\mathrm{ev}_X \colon X^* \otimes_{\mathcal{C}} X \to 1$ and $\mathrm{coev}_X \colon 1 \to X \otimes_{\mathcal{C}} X^*$, called the evaluation and coevaluation, such that the compositions

$$X \xrightarrow{\mathrm{coev}_X \otimes_{\mathcal{C}} \mathrm{id}_X} (X \otimes_{\mathcal{C}} X^*) \otimes_{\mathcal{C}} X \xrightarrow{a_{X,X^*,X}} X \otimes_{\mathcal{C}} (X^* \otimes_{\mathcal{C}} X) \xrightarrow{\mathrm{id}_X \otimes_{\mathcal{C}} \mathrm{ev}_X} X$$

$$X^* \xrightarrow{\mathrm{id}_{X^*} \otimes_{\mathcal{C}} \mathrm{coev}_X} X^* \otimes_{\mathcal{C}} (X \otimes_{\mathcal{C}} X^*) \xrightarrow{a^{-1}_{X^*,X,X^*}} (X^* \otimes_{\mathcal{C}} X) \otimes_{\mathcal{C}} X^* \xrightarrow{\mathrm{ev}_X \otimes_{\mathcal{C}} \mathrm{id}_{X^*}} X^*$$

are the identity morphisms.

Definition 4.1.6. [22, Definition 2.10.2] Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ be a monoidal category. An object ${}^*X$ in $\mathcal{C}$ is said to be a right dual of X if there exist morphisms $\mathrm{ev}'_X \colon X \otimes_{\mathcal{C}} {}^*X \to 1$ and $\mathrm{coev}'_X \colon 1 \to {}^*X \otimes_{\mathcal{C}} X$, such that the compositions

$$X \xrightarrow{\mathrm{id}_X \otimes_{\mathcal{C}} \mathrm{coev}'_X} X \otimes_{\mathcal{C}} ({}^*X \otimes_{\mathcal{C}} X) \xrightarrow{a^{-1}_{X,{}^*X,X}} (X \otimes_{\mathcal{C}} {}^*X) \otimes_{\mathcal{C}} X \xrightarrow{\mathrm{ev}'_X \otimes_{\mathcal{C}} \mathrm{id}_X} X$$

$${}^*X \xrightarrow{\mathrm{coev}'_X \otimes_{\mathcal{C}} \mathrm{id}_{{}^*X}} ({}^*X \otimes_{\mathcal{C}} X) \otimes_{\mathcal{C}} {}^*X \xrightarrow{a_{{}^*X,X,{}^*X}} {}^*X \otimes_{\mathcal{C}} (X \otimes_{\mathcal{C}} {}^*X) \xrightarrow{\mathrm{id}_{{}^*X} \otimes_{\mathcal{C}} \mathrm{ev}'_X} X^*$$

are the identity morphisms.

Definition 4.1.7. [22, Definition 2.10.11] A monoidal category $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ is called rigid if every object of $\mathcal{C}$ has left and right duals.

Example 4.1.3. Let $\mathfrak{g}$ be a Lie algebra over $\mathbb{C}$ and let $U(\mathfrak{g})$ be its associated universal enveloping algebra. Let $U(\mathfrak{g})$-mod be the category of $U(\mathfrak{g})$-modules. We recall that $U(\mathfrak{g})$ is a Hopf algebra; explicitly the comultiplication, the antipode and the counit are defined on the generating elements $x \in \mathfrak{g}$ in the following way:

$$\begin{aligned}
&\Delta(x) = 1 \otimes x + x \otimes 1 \\
&S(x) = -x \\
&\varepsilon(x) = 0.
\end{aligned}$$

As a consequence, $U(\mathfrak{g})$-mod is a monoidal category with the structure described in Example 4.1.2. Consider the subcategory $U(\mathfrak{g})\text{-mod}_{\mathrm{fin}}$ of finite dimensional $U(\mathfrak{g})$-modules. This subcategory is closed under the tensor product and hence it is a monoidal category. Moreover, the latter is rigid. Indeed, for a finite dimensional representation V, the dual representation is the usual dual vector space V^*, where $U(\mathfrak{g})$ acts on it in the following way:

$$(x.\phi)(y) = \phi(S(x).y)$$

for every $x \in U(\mathfrak{g})$, $y \in V$ and $\phi \in V^*$.

Once we have defined monoidal categories and rigid monoidal categories, we categorify the notion of morphisms between monoids.

Definition 4.1.8. [22, Definition 2.4.1] Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ and $(\mathcal{D}, \otimes_{\mathcal{D}}, \tilde{a}, \tilde{1})$ be two monoidal categories. A monoidal functor from $\mathcal{C}$ to $\mathcal{D}$ is a pair (F, J), where $F\colon \mathcal{C} \to \mathcal{D}$ is a functor and $J\colon F(-)\otimes_{\mathcal{D}} F(-) \to F(-\otimes_{\mathcal{C}} -)$ a natural isomorphism:

$$J_{X,Y}\colon F(X)\otimes_{\mathcal{D}} F(Y) \to F(X\otimes_{\mathcal{C}} Y), \qquad \text{for all } X,Y\in\mathcal{C}, \tag{4.1.3}$$

such that $\tilde{1} \simeq F(1)$ and the diagram

$$\begin{tikzcd}
(F(X)\otimes_{\mathcal{D}} F(Y))\otimes_{\mathcal{D}} F(Z) \arrow[rr, "\tilde{a}_{F(X),F(Y),F(Z)}"] \arrow[d, "J_{X,Y}\otimes_{\mathcal{D}}\mathrm{id}_{F(Z)}"'] & & F(X)\otimes_{\mathcal{D}} (F(Y)\otimes_{\mathcal{D}} F(Z)) \arrow[d, "\mathrm{id}_{F(X)}\otimes_{\mathcal{D}} J_{Y,Z}"] \\
F(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{D}} F(Z) \arrow[d, "J_{X\otimes_{\mathcal{C}} Y,Z}"'] & & F(X)\otimes_{\mathcal{D}} F(Y\otimes_{\mathcal{C}} Z) \arrow[d, "J_{X,Y\otimes_{\mathcal{C}} Z}"] \\
F((X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{C}} Z) \arrow[rr, "F(a_{X,Y,Z})"'] & & F(X\otimes_{\mathcal{C}} (Y\otimes_{\mathcal{C}} Z))
\end{tikzcd}$$

is commutative for all $X,Y,Z\in\mathcal{C}$.

As monoids act on sets, monoidal categories act on other categories. The categorification of a left action leads to the definition of a left $\mathcal{C}$-module category.

Definition 4.1.9. [22, Definition 7.1.1] Let $(\mathcal{C},\otimes_{\mathcal{C}},a,1)$ be a monoidal category. A left module category over $\mathcal{C}$ is a category $\mathcal{M}$ equipped with an action bifunctor $\otimes_{\mathcal{M}}\colon \mathcal{C}\times\mathcal{M}\to\mathcal{M}$ and a natural isomorphism

$$m_{X,Y,M}\colon (X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} M \xrightarrow{\sim} X\otimes_{\mathcal{M}} (Y\otimes_{\mathcal{M}} M), \qquad X,Y\in\mathcal{C},\ M\in\mathcal{M}, \tag{4.1.4}$$

called module associativity constraint such that the functor $1\otimes_{\mathcal{M}} -\colon \mathcal{M}\to\mathcal{M}$, given by $1\otimes_{\mathcal{M}} M\mapsto M$ is an autoequivalence, and the pentagon diagram:

$$\begin{tikzcd}
& ((X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{C}} Z)\otimes_{\mathcal{M}} M \arrow[dl, "a_{X,Y,Z}\otimes_{\mathcal{M}}\mathrm{id}_M"'] \arrow[dr, "m_{X\otimes_{\mathcal{C}} Y,Z,M}"] & \\
(X\otimes_{\mathcal{C}} (Y\otimes_{\mathcal{C}} Z))\otimes_{\mathcal{M}} M \arrow[d, "m_{X,Y\otimes_{\mathcal{C}} Z,M}"'] & & (X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} (Z\otimes_{\mathcal{M}} M) \arrow[d, "m_{X,Y,Z\otimes_{\mathcal{M}} M}"] \\
X\otimes_{\mathcal{M}} ((Y\otimes_{\mathcal{C}} Z)\otimes_{\mathcal{M}} M) \arrow[rr, "\mathrm{id}_X\otimes_{\mathcal{M}} m_{Y,Z,M}"] & & X\otimes_{\mathcal{M}} (Y\otimes_{\mathcal{M}} (Z\otimes_{\mathcal{M}} M))
\end{tikzcd}$$

is commutative for any $X,Y,Z\in\mathcal{C}$ and $M\in\mathcal{M}$.

Example 4.1.4. Let K be any field and let $\mathcal{C} = \mathrm{Vec}$, the category of all K-vector spaces.
Let G be a finite group and consider $\mathcal{M}$ the category of all G-modules. For $V\in\mathcal{C}$ and $W\in\mathcal{M}$, we define an action of G on $V\otimes_{\mathbb{C}} W$ as follows

$$g.(v\otimes_{\mathbb{C}} w) = v\otimes_{\mathbb{C}} g.w,$$

for every $g \in G$, $v \in V$ and $w \in W$. In this way, $V \otimes_{\mathbb{C}} W$ becomes an object in $\mathcal{M}$ and the category $\mathcal{M}$ endowed with $\otimes_{\mathbb{C}}$ and m the change of brackets results to be a left $\mathcal{C}$-module category.

In a similar way one can define a right $\mathcal{C}$-module category $(\mathcal{M}, \otimes^{\mathcal{M}}, m^r)$. Namely, a right $\mathcal{C}$ module category is the same thing as a left $\mathcal{C}^{\mathrm{op}}$-module category, where $\mathcal{C}^{\mathrm{op}}$ denotes the opposite category (Definition 4.1.2).
We now introduce the notion of a bimodule category over a pair of monoidal categories.

Definition 4.1.10. [22, Definition 7.1.7] Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ and $(\mathcal{D}, \otimes_{\mathcal{D}}, \tilde{a}, \tilde{1})$ be monoidal categories. A $(\mathcal{C}, \mathcal{D})$-bimodule category is a category $\mathcal{M}$ which is a left $\mathcal{C}$-module category $(\mathcal{M}, \otimes_{\mathcal{M}}, m)$ and a right $\mathcal{D}$-module category $(\mathcal{M}, \otimes^{\mathcal{M}}, m^r)$ with module associativity constraints for $X, Y \in \mathcal{C}$, $M \in \mathcal{M}$ and $W, Z \in \mathcal{D}$

$$m_{X,Y,M} \colon (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} M \xrightarrow{\sim} X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} M)$$

and

$$m^r_{M,W,Z} \colon M \otimes^{\mathcal{M}} (W \otimes_{\mathcal{D}} Z) \xrightarrow{\sim} (M \otimes^{\mathcal{M}} W) \otimes^{\mathcal{M}} Z$$

respectively, compatible by a collection of natural isomorphisms for $X \in \mathcal{C}$, $M \in \mathcal{M}$ and $Z \in \mathcal{D}$

$$b_{X,M,Z} \colon (X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} Z \xrightarrow{\sim} X \otimes_{\mathcal{M}} (M \otimes^{\mathcal{M}} Z)$$

called middle associativity constraints such that the diagrams

$$\begin{tikzcd}[column sep=tiny]
& ((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} Z \arrow[dl, "m_{X,Y,M} \otimes^{\mathcal{M}} \mathrm{id}_Z"'] \arrow[dr, "b_{X \otimes_{\mathcal{C}} Y, M, Z}"] & \\
(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} M)) \otimes^{\mathcal{M}} Z \arrow[d, "b_{X, Y \otimes_{\mathcal{M}} M, Z}"'] & & (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} (M \otimes^{\mathcal{M}} Z) \arrow[d, "m_{X,Y,M \otimes^{\mathcal{M}} Z}"] \\
X \otimes_{\mathcal{M}} ((Y \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} Z) \arrow[rr, "\mathrm{id}_X \otimes_{\mathcal{M}} b_{Y,M,Z}"] & & X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} (M \otimes^{\mathcal{M}} Z))
\end{tikzcd} \tag{4.1.5}$$

and

$$\begin{tikzcd}[column sep=tiny]
& X \otimes_{\mathcal{M}} (M \otimes^{\mathcal{M}} (W \otimes_{\mathcal{D}} Z)) \arrow[dl, "\mathrm{id}_X \otimes_{\mathcal{M}} m^r_{M,W,Z}"'] & \\
X \otimes_{\mathcal{M}} ((M \otimes^{\mathcal{M}} W) \otimes^{\mathcal{M}} Z) & & (X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} (W \otimes_{\mathcal{D}} Z) \arrow[ul, "b_{X,M,W \otimes_{\mathcal{D}} Z}"'] \arrow[d, "m^r_{X \otimes_{\mathcal{M}} M, W, Z}"] \\
(X \otimes_{\mathcal{M}} (M \otimes^{\mathcal{M}} W)) \otimes^{\mathcal{M}} Z \arrow[u, "b_{X, M \otimes^{\mathcal{M}} W, Z}"] & & ((X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} W) \otimes^{\mathcal{M}} Z \arrow[ll, "b_{X,M,W} \otimes^{\mathcal{M}} \mathrm{id}_Z"']
\end{tikzcd} \tag{4.1.6}$$

commute for all $X, Y \in \mathcal{C}, Z, W \in \mathcal{D}$ and $M \in \mathcal{M}$.

EXAMPLE 4.1.5. Let $\mathcal{C}$ and $\mathcal{M}$ be the categories considered in Example 4.1.4 and let $\mathcal{D} = \mathcal{C}$. We can define a right action of $\mathcal{C}$ on $\mathcal{M}$, via the tensor product over $\mathbb{C}$. In particular, given $V \in \mathcal{C}$ and $W \in \mathcal{M}$, the tensor product $W \otimes_{\mathbb{C}} V$ becomes a G-module, via the action

$$g.(w \otimes_{\mathbb{C}} v) = g.w \otimes_{\mathbb{C}} v,$$

for every $v \in V, w \in W, g \in G$. In this way, $\mathcal{M}$ results to be a $(\mathcal{C}, \mathcal{C})$-bimodule category, where b is the change of brackets.

An important notion we need to categorify is the notion of equivariant morphisms. This leads to the following definition.

DEFINITION 4.1.11. [22, Definition 7.2.1] Let $(\mathcal{M}, \otimes_{\mathcal{M}}, m)$ and $(\mathcal{N}, \otimes_{\mathcal{N}}, n)$ be two module categories over a monoidal category $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ with associativity constraints m and n, respectively. A $\mathcal{C}$-module functor from $\mathcal{M}$ to $\mathcal{N}$ consists of a functor $F \colon \mathcal{M} \to \mathcal{N}$ and a natural isomorphism

$$s_{X,M} \colon F(X \otimes_{\mathcal{M}} M) \to X \otimes_{\mathcal{N}} F(M), \qquad X \in \mathcal{C},\ M \in \mathcal{M} \tag{4.1.7}$$

such that the following diagrams

$$\begin{tikzcd}
 & F((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} M) \arrow[dl, "F(m_{X,Y,M})"'] \arrow[dr, "s_{X \otimes_{\mathcal{C}} Y, M}"] & \\
F(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} M) \arrow[d, "s_{X, Y \otimes_{\mathcal{M}} M}"'] & & (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{N}} F(M) \arrow[d, "n_{X,Y,F(M)}"] \\
X \otimes_{\mathcal{N}} F(Y \otimes_{\mathcal{M}} M) \arrow[rr, "\mathrm{id}_X \otimes_{\mathcal{N}} s_{Y,M}"] & & X \otimes_{\mathcal{N}} (Y \otimes_{\mathcal{N}} F(M))
\end{tikzcd} \tag{4.1.8}$$

and

$$\begin{tikzcd}
F(1 \otimes_{\mathcal{M}} M) \arrow[rr, "s_{1,M}"] \arrow[dr] & & 1 \otimes_{\mathcal{N}} F(M) \arrow[dl] \\
 & F(M) &
\end{tikzcd} \tag{4.1.9}$$

commute for all $X, Y \in \mathcal{C}$ and $M \in \mathcal{M}$.

DEFINITION 4.1.12. Let $(\mathcal{M}, \otimes_{\mathcal{M}}, m)$ and $(\mathcal{N}, \otimes_{\mathcal{N}}, n)$ be two module categories over a monoidal category $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ with associativity constraints m

and n, respectively. We say that a $\mathcal{C}$-module functor $(F\colon \mathcal{M} \to \mathcal{N}, s)$ is an equivalence of $\mathcal{C}$-module categories if F is an equivalence.

The above definitions have a specular counterpart for right-module categories.

EXAMPLE 4.1.6. Let $\mathcal{C}$ and $\mathcal{M}$ be the categories considered in Example 4.1.4. Let H be a subgroup of G and let $\mathcal{N}$ be the category of H-modules. Then, the restriction functor $\mathrm{Res}^G_H\colon \mathcal{M} \to \mathcal{N}$ is a $\mathcal{C}$-module functor, where $s = \mathrm{id}$.

For the definition of a bimodule functor, we also need a compatibility condition. In particular, [29, Definition 2.10] together with [29, Remark 2.14] gives us the following:

DEFINITION 4.1.13. Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ and $(\mathcal{D}, \otimes_{\mathcal{D}}, \tilde{a}, \tilde{1})$ be two monoidal categories and let $(\mathcal{M}, \otimes_{\mathcal{M}}, \otimes^{\mathcal{M}}, m, m^r, b)$ and $(\mathcal{N}, \otimes_{\mathcal{N}}, \otimes^{\mathcal{N}}, n, n^r, p)$ be two $(\mathcal{C}, \mathcal{D})$-bimodule categories. A $(\mathcal{C}, \mathcal{D})$-bimodule functor from $\mathcal{M}$ to $\mathcal{N}$ consists of a triple (F, s, s^r), where F is a functor from $\mathcal{M}$ to $\mathcal{N}$, (F, s) is a left $\mathcal{C}$-module functor and (F, s^r) is a right $\mathcal{C}$-module functor, such that the following diagram commutes

$$\begin{tikzcd}
F((X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} Y) \arrow[r, "F(b_{X,M,Y})"] \arrow[d, "s^r_{X\otimes_{\mathcal{M}} M, Y}"'] & F(X \otimes_{\mathcal{M}} (M \otimes^{\mathcal{M}} Y)) \arrow[d, "s_{X, M\otimes^{\mathcal{M}} Y}"] \\
F(X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{N}} Y \arrow[d, "s_{X,M} \otimes^{\mathcal{N}} \mathrm{id}_Y"'] & X \otimes_{\mathcal{N}} F(M \otimes^{\mathcal{M}} Y) \arrow[d, "\mathrm{id}_X \otimes_{\mathcal{N}} s^r_{M,Y}"] \\
(X \otimes_{\mathcal{N}} F(M)) \otimes^{\mathcal{N}} Y \arrow[r, "p_{X,F(M),Y}"] & X \otimes_{\mathcal{N}} (F(M) \otimes^{\mathcal{N}} Y)
\end{tikzcd} \tag{4.1.10}$$

for every $M \in \mathcal{M}$, $X \in \mathcal{C}$ and $Y \in \mathcal{D}$.

We conclude this section with a property about $\mathcal{C}$-module functors.

LEMMA 4.1.14. *Let $(\mathcal{M}, \otimes_{\mathcal{M}}, m), (\mathcal{N}, \otimes_{\mathcal{N}}, n)$ and $(\mathcal{P}, \otimes_{\mathcal{P}}, p)$ be module categories over a monoidal category $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$. Let $(F\colon \mathcal{M} \to \mathcal{N}, s)$ and $(G\colon \mathcal{N} \to \mathcal{P}, t)$ be two $\mathcal{C}$-module functors. Then $(G \circ F, u := t_{-,F(-)} \circ G(s))$ is a $\mathcal{C}$-module functor.*

PROOF. Firstly, observe that u has the required source and target, in fact for every $X \in \mathcal{C}$, $M \in \mathcal{M}$

$$u_{X,M}\colon GF(X \otimes_{\mathcal{M}} M) \xrightarrow{G(s_{X,M})} G(X \otimes_{\mathcal{N}} F(M)) \xrightarrow{t_{X,F(M)}} X \otimes_{\mathcal{P}} GF(M).$$

Furthermore, u is a natural isomorphism, since $G(s)$ is a natural isomorphism and u is defined as the composition of natural isomorphisms.
We are left to verify that the following diagrams are commutative

$$
\begin{tikzcd}
 & GF((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} M) \arrow[dl, "GF(m_{X,Y,M})"'] \arrow[dr, "u_{X \otimes_{\mathcal{C}} Y, M}"] & \\
GF(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} M)) \arrow[d, "u_{X, Y \otimes_{\mathcal{M}} M}"'] & & (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{P}} GF(M) \arrow[d, "p_{X,Y,GF(M)}"] \\
X \otimes_{\mathcal{P}} GF(Y \otimes_{\mathcal{M}} M) \arrow[rr, "\mathrm{id}_X \otimes_{\mathcal{N}} u_{Y,M}"] & & X \otimes_{\mathcal{P}} (Y \otimes_{\mathcal{P}} GF(M))
\end{tikzcd}
\tag{4.1.11}
$$

and

$$
\begin{tikzcd}
GF(1 \otimes_{\mathcal{M}} M) \arrow[rr, "u_{1,M}"] \arrow[dr] & & 1 \otimes_{\mathcal{P}} GF(M) \arrow[dl] \\
 & F(M) &
\end{tikzcd}
$$

for all $X, Y \in \mathcal{C}$ and $M \in \mathcal{M}$.
We prove the commutativity of the first diagram. Applying the definition of the natural isomorphism u, the considered diagram is the outer rectangle of the following diagram

$$
\begin{tikzcd}
GF(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} M)) \arrow[d, "G(s_{X,Y \otimes_{\mathcal{M}} M})"'] \arrow[dr, phantom, "\textcolor{red}{A}"] & GF((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} M) \arrow[l, "GF(m_{X,Y,M})"'] \arrow[r, "G(s_{X \otimes_{\mathcal{C}} Y,M})"] & G((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{N}} F(M)) \arrow[d, "t_{X \otimes_{\mathcal{C}} Y,F(M)}"] \arrow[dl, "G(n_{X,Y,F(M)})"'] \\
G(X \otimes_{\mathcal{N}} F(Y \otimes_{\mathcal{M}} M)) \arrow[d, "t_{X,F(Y \otimes_{\mathcal{M}} M)}"'] \arrow[r, "G(\mathrm{id}_X \otimes_{\mathcal{N}} s_{Y,M})"] \arrow[dr, phantom, "\textcolor{red}{B}"] & G(X \otimes_{\mathcal{N}} (Y \otimes_{\mathcal{N}} F(M))) \arrow[d, "t_{X,Y \otimes_{\mathcal{N}} F(M)}"] \arrow[dr, phantom, "\textcolor{red}{C}"] & (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{P}} GF(M) \arrow[d, "p_{X,Y,GF(M)}"] \\
X \otimes_{\mathcal{P}} GF(Y \otimes_{\mathcal{M}} M) \arrow[r, "\mathrm{id} \otimes_{\mathcal{P}} G(s_{Y,M})"] & X \otimes_{\mathcal{P}} G(Y \otimes_{\mathcal{N}} F(M)) \arrow[r, "\mathrm{id}_X \otimes_{\mathcal{P}} t_{Y,F(M)}"] & X \otimes_{\mathcal{P}} (Y \otimes_{\mathcal{P}} GF(M))
\end{tikzcd}
$$

for all $X, Y \in \mathcal{C}, M \in \mathcal{M}$.

Diagrams A and C are commutative since (F, s) and (G, t) are $\mathcal{C}$-module functors. Moreover, the naturality of t implies the commutativity of B. This implies that the outer rectangle is commutative, i.e. that diagram (4.1.11) commutes.
In a similar way, one can prove that diagram (4.1.9) is commutative. $\square$

2. Transport of structure

In the second part of this chapter, we show how we can construct new module categories by means of equivalences and transport of structure.

Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ be a monoidal category. Let $\mathcal{M}$ be a left $\mathcal{C}$-module category, via the action bifunctor $\otimes_{\mathcal{M}} \colon \mathcal{C} \times \mathcal{M} \to \mathcal{M}$ and with module associativity constraint $m_{X,Y,M}$. Let $F \colon \mathcal{M} \to \mathcal{N}$ be an equivalence of categories. Then, there exists a quasi-inverse $G \colon \mathcal{N} \to \mathcal{M}$, i.e. a functor and natural isomorphisms η and ε such that $G \circ F \overset{\varepsilon}{\approx} \mathrm{id}_{\mathcal{M}}$ and $F \circ G \overset{\eta}{\approx} \mathrm{id}_{\mathcal{N}}$.
We can define in a natural way the bifunctor :

$$\begin{aligned} \otimes_{\mathcal{N}} \colon \mathcal{C} \times \mathcal{N} &\to \mathcal{N} \\ (-, \sim) &\mapsto F(- \otimes_{\mathcal{M}} G(\sim)). \end{aligned} \tag{4.2.1}$$

In an analogous way, for every $X, Y \in \mathcal{C}, N \in \mathcal{N}$, we can define the maps

$$n_{X,Y,N} \colon (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{N}} N \to X \otimes_{\mathcal{N}} (Y \otimes_{\mathcal{N}} N)$$

as follows:

$$n_{X,Y,N} := F\Big((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y \otimes_{\mathcal{M}} G(N)}) \circ m_{X,Y,G(N)} \Big). \tag{4.2.2}$$

Remark 4.2.1. The morphism $n \colon (- \otimes_{\mathcal{C}} -) \otimes_{\mathcal{N}} - \to - \otimes_{\mathcal{N}} (- \otimes_{\mathcal{N}} -)$ is a natural isomorphism, because n is the image of a composition of natural isomorphisms through an equivalence.

We are now in a position to prove the following lemma:

Lemma 4.2.2. *Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ be a monoidal category and let $(\mathcal{M}, \otimes_{\mathcal{M}}, m)$ be a left $\mathcal{C}$-module category. Let $F \colon \mathcal{M} \to \mathcal{N}$ be an equivalence of categories, with quasi-inverse $G \colon \mathcal{N} \to \mathcal{M}$ such that $G \circ F \overset{\varepsilon}{\approx} id_{\mathcal{M}}$ and $F \circ G \overset{\eta}{\approx} id_{\mathcal{N}}$. The category $\mathcal{N}$ endowed with $\otimes_{\mathcal{N}}$ as in Equation (4.2.1), and morphisms $n_{X,Y,N}$ for all $X, Y \in \mathcal{C}$, $N \in \mathcal{N}$ as in Equation (4.2.2) is a left $\mathcal{C}$-module category.*

Proof. By definition, $\otimes_{\mathcal{N}}$ is a bifunctor. By Remark 4.2.1 the maps $n_{X,Y,N}$ for $X, Y \in \mathcal{C}$, $N \in \mathcal{N}$ combine to give natural isomorphisms.
Moreover, the functor

$$\begin{aligned} 1 \otimes_{\mathcal{N}} - \colon \mathcal{N} &\to \mathcal{N} \\ N &\mapsto 1 \otimes_{\mathcal{N}} N = F(1 \otimes_{\mathcal{M}} G(N)) \end{aligned}$$

is an autoequivalence, since it is the composition of equivalences.
It remains to verify that the pentagon rule holds, i.e. that the following diagram commutes

$$\begin{tikzcd}
& ((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{C}} Z) \otimes_{\mathcal{N}} N \arrow[dl, "a_{X,Y,Z} \otimes_{\mathcal{N}} \mathrm{id}_N"'] \arrow[dr, "n_{X \otimes_{\mathcal{C}} Y, Z, N}"] & \\
(X \otimes_{\mathcal{C}} (Y \otimes_{\mathcal{C}} Z)) \otimes_{\mathcal{N}} N \arrow[d, "n_{X, Y \otimes_{\mathcal{C}} Z, N}"'] & & (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{N}} (Z \otimes_{\mathcal{N}} N) \arrow[d, "n_{X,Y,Z \otimes_{\mathcal{N}} N}"] \\
X \otimes_{\mathcal{N}} ((Y \otimes_{\mathcal{C}} Z) \otimes_{\mathcal{N}} N) \arrow[rr, "\mathrm{id}_X \otimes_{\mathcal{N}} n_{Y,Z,N}"] & & X \otimes_{\mathcal{N}} (Y \otimes_{\mathcal{N}} (Z \otimes_{\mathcal{N}} N))
\end{tikzcd} \tag{4.2.3}$$

for every $X, Y, Z \in \mathcal{C}$ and $N \in \mathcal{N}$. Using Equation (4.2.1) and Equation (4.2.2), this is equivalent to prove that:

$$\begin{aligned}
&F\big((\mathrm{id}_X \otimes_{\mathcal{M}} GF((\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{Z \otimes_{\mathcal{M}} G(N)}) \circ m_{Y,Z,G(N)})) \circ (\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{(Y \otimes_{\mathcal{C}} Z) \otimes_{\mathcal{M}} G(N)})\big) \circ \\
&\circ F\big(m_{X, Y \otimes_{\mathcal{C}} Z, G(N)} \circ (a_{X,Y,Z} \otimes_{\mathcal{M}} \mathrm{id}_{G(N)})\big) = \\
&F\big((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y \otimes_{\mathcal{M}} (GF(Z \otimes_{\mathcal{M}} G(N)))}) \circ m_{X,Y,GF(Z \otimes_{\mathcal{M}} G(N))} \circ (\mathrm{id}_X \otimes_{\mathcal{C}} \mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{Z \otimes_{\mathcal{M}} G(N)})\big) \circ \\
&\circ F\big(m_{X \otimes_{\mathcal{C}} Y, Z, G(N)}\big).
\end{aligned} \tag{4.2.4}$$

In order to verify that the previous equation holds, we need some commutative diagrams. In particular, by the naturality of ε, the diagrams

$$\begin{tikzcd}
GF((Y \otimes_{\mathcal{C}} Z) \otimes_{\mathcal{M}} G(N)) \arrow[r, "GF(m_{Y,Z,G(N)})"] \arrow[d, "\varepsilon_{(Y \otimes_{\mathcal{C}} Z) \otimes_{\mathcal{M}} G(N)}"'] & GF(Y \otimes_{\mathcal{M}} (Z \otimes_{\mathcal{M}} G(N))) \arrow[d, "\varepsilon_{Y \otimes_{\mathcal{M}} (Z \otimes_{\mathcal{M}} G(N))}"] \\
(Y \otimes_{\mathcal{C}} Z) \otimes_{\mathcal{M}} G(N) \arrow[r, "m_{Y,Z,G(N)}"] & Y \otimes_{\mathcal{M}} (Z \otimes_{\mathcal{M}} G(N))
\end{tikzcd} \tag{4.2.5}$$

and

$$\begin{tikzcd}
GF(Y \otimes_{\mathcal{M}} (Z \otimes_{\mathcal{M}} G(N))) \arrow[r, "\varepsilon_{Y \otimes_{\mathcal{M}} (Z \otimes_{\mathcal{M}} G(N))}"] \arrow[d, "GF(\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{Z \otimes_{\mathcal{M}} G(N)})"'] & Y \otimes_{\mathcal{M}} (Z \otimes_{\mathcal{M}} G(N)) \arrow[d, "\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{Z \otimes_{\mathcal{M}} G(N)}"] \\
GF(Y \otimes_{\mathcal{M}} GF(Z \otimes_{\mathcal{M}} G(N))) \arrow[r, "\varepsilon_{Y \otimes_{\mathcal{M}} GF(Z \otimes_{\mathcal{M}} G(N))}"] & Y \otimes_{\mathcal{M}} GF(Z \otimes_{\mathcal{M}} G(N))
\end{tikzcd} \tag{4.2.6}$$

commute, for every $Y, Z \in \mathcal{C}$ and $N \in \mathcal{N}$.
Furthermore, by the naturality of m with respect to the functors $(- \otimes_{\mathcal{C}} -) \otimes_{\mathcal{M}} -$ and $- \otimes_{\mathcal{M}} (- \otimes_{\mathcal{M}} -)$, the diagram:

$$\begin{tikzcd}
(X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} GF(Z \otimes_{\mathcal{M}} G(N)) \arrow[r, "\mathrm{id}_{X\otimes_{\mathcal{C}} Y} \otimes_{\mathcal{M}} \varepsilon_{Z\otimes_{\mathcal{M}} G(N)}"] \arrow[d, "m_{X,Y,GF(Z\otimes_{\mathcal{M}} G(N))}"'] & (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} (Z \otimes_{\mathcal{M}} G(N)) \arrow[d, "m_{X,Y,Z\otimes_{\mathcal{M}} G(N)}"] \\
X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} GF(Z \otimes_{\mathcal{M}} G(N))) \arrow[r, "\mathrm{id}_X \otimes_{\mathcal{M}} (\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon_{Z\otimes_{\mathcal{M}} G(N)})"] & X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} (Z \otimes_{\mathcal{M}} G(N)))
\end{tikzcd} \tag{4.2.7}$$

is commutative for every $X, Y, Z \in \mathcal{C}$ and $N \in \mathcal{N}$.
Let us consider the left hand-side of equation (4.2.4). The commutativity of diagram (4.2.5) gives:

$$\begin{aligned}
&F\big((\mathrm{id}_X \otimes_{\mathcal{M}} GF((\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{Z\otimes_{\mathcal{M}} G(N)}) \circ m_{Y,Z,G(N)})) \circ (\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{(Y\otimes Z)\otimes_{\mathcal{M}} G(N)})\big) \circ \\
&\circ F\big(m_{X,Y\otimes_{\mathcal{C}} Z,G(N)} \circ (a_{X,Y,Z} \otimes_{\mathcal{M}} \mathrm{id}_{G(N)})\big) \\
&= F\big((\mathrm{id}_X \otimes_{\mathcal{M}} GF(\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{Z\otimes_{\mathcal{M}} G(N)}) \circ \varepsilon^{-1}_{Y\otimes_{\mathcal{M}}(Z\otimes_{\mathcal{M}} G(N)))}) \circ (\mathrm{id}_X \otimes_{\mathcal{M}} m_{Y,Z,G(N)})\big) \circ \\
&\circ F\big(m_{X,Y\otimes_{\mathcal{C}} Z,G(N)} \circ (a_{X,Y,Z} \otimes_{\mathcal{M}} \mathrm{id}_{G(N)})\big).
\end{aligned}$$

Finally by the commutativity of diagram (4.2.6), the above term reads as:

$$\begin{aligned}
&F\big((\mathrm{id}_X \otimes_{\mathcal{M}} (\varepsilon^{-1}_{Y\otimes_{\mathcal{M}}(GF(Z\otimes_{\mathcal{M}} G(N)))} \circ (\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{Z\otimes_{\mathcal{M}} G(N)}))) \circ (\mathrm{id}_X \otimes_{\mathcal{M}} m_{Y,Z,G(N)})\big) \circ \\
&\circ F\big(m_{X,Y\otimes_{\mathcal{C}} Z,G(N)} \circ (a_{X,Y,Z} \otimes_{\mathcal{M}} \mathrm{id}_{G(N)})\big).
\end{aligned} \tag{4.2.8}$$

Consider now the right hand-side of equation (4.2.4). By the commutativity of diagram (A.1.3), the right hand-side becomes:

$$\begin{aligned}
&F\big((\mathrm{id}_X \otimes_{\mathcal{M}} (\varepsilon^{-1}_{Y\otimes_{\mathcal{M}} GF((Z\otimes_{\mathcal{M}} G(N)))} \circ (\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{Z\otimes_{\mathcal{M}} G(N)}))) \circ m_{X,Y,Z\otimes_{\mathcal{M}} G(N)}\big) \circ \\
&\circ F\big(m_{X\otimes_{\mathcal{C}} Y,Z,G(N)}\big).
\end{aligned} \tag{4.2.9}$$

Since $F\big((\mathrm{id}_X \otimes_{\mathcal{M}} (\varepsilon^{-1}_{Y\otimes_{\mathcal{M}}(GF(Z\otimes_{\mathcal{M}} G(N)))} \circ (\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{Z\otimes_{\mathcal{M}} G(N)})))\big)$ is an isomorphism, expression (4.2.8) and expression (4.2.9) are equal if and only if

$$\begin{aligned}
&F\big((\mathrm{id}_X \otimes_{\mathcal{M}} m_{Y,Z,G(N)}) \circ m_{X,Y\otimes_{\mathcal{C}} Z,G(N)} \circ (a_{X,Y,Z} \otimes_{\mathcal{M}} \mathrm{id}_{G(N)})\big) = \\
&F\big(m_{X,Y,Z\otimes_{\mathcal{M}} G(N)} \circ m_{X\otimes_{\mathcal{C}} Y,Z,G(N)}\big).
\end{aligned}$$

This equation holds, since $\mathcal{M}$ is a left $\mathcal{C}$-module category. □

Moreover, we can prove that the functors F and G as above are $\mathcal{C}$-module functors (Definition 4.1.11).

LEMMA 4.2.3. *Let* $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ *be a monoidal category and let* $(\mathcal{M}, \otimes_{\mathcal{M}}, m)$ *be a left* $\mathcal{C}$*-module category. Let* $F\colon \mathcal{M} \to \mathcal{N}$ *be an equivalence, with quasi-inverse* $G\colon \mathcal{N} \to \mathcal{M}$ *such that* $G \circ F \overset{\varepsilon}{\approx} id_{\mathcal{M}}$ *and* $F \circ G \overset{\eta}{\approx} id_{\mathcal{N}}$ *and consider the category* $\mathcal{N}$ *endowed with* $\otimes_{\mathcal{N}}$ *as in Equation* (4.2.1), *with the morphism* $n_{X,Y,N}$ *as in Equation* (4.2.2).
Let $s_{X,M} := F(id_X \otimes_{\mathcal{M}} \varepsilon^{-1}_M)$ *and* $t_{X,N} := \varepsilon_{X\otimes_{\mathcal{M}} G(N)}$, *for every* $X \in \mathcal{C}, M \in \mathcal{M}$

and $N \in \mathcal{N}$. Then the pairs (F, s) and (G, t) are $\mathcal{C}$-module functors, so $\mathcal{M}$ and $\mathcal{N}$ are equivalent as $\mathcal{C}$-module categories.

PROOF. We prove this result for F, for G the proof will be analogous. Firstly, the morphism s has the required source and target, in fact for all $X \in \mathcal{C}$ and $M \in \mathcal{M}$:

$$s_{X,M} \colon F(X \otimes_{\mathcal{M}} M) \xrightarrow{F(\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon_M^{-1})} F(X \otimes_{\mathcal{M}} GF(M)) = X \otimes_{\mathcal{N}} F(M).$$

Furthermore, the morphism s is a natural isomorphism, since it is the composition of a natural isomorphism and an equivalence. We have now to check that Diagrams (4.1.8) and (4.1.9) are commutative.
In particular, Diagram (4.1.8) reduces to

$$\begin{tikzcd}
 & F((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} M) \arrow[dl, "F(m_{X,Y,M})"'] \arrow[dr, "s_{X \otimes_{\mathcal{C}} Y, M}"] & \\
F(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} M)) \arrow[d, "s_{X, Y \otimes_{\mathcal{M}} M}"'] & & F((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} GF(M)) \arrow[d, "n_{X,Y,F(M)}"] \\
F(X \otimes_{\mathcal{M}} GF(Y \otimes_{\mathcal{M}} M)) \arrow[rr, "\mathrm{id}_X \otimes_{\mathcal{N}} s_{Y,M}"] & & F(X \otimes_{\mathcal{M}} GF(Y \otimes_{\mathcal{M}} GF(M)))
\end{tikzcd}$$

for all $X, Y \in \mathcal{C}$ and $M \in \mathcal{M}$. Using the definition of n and s, the previous diagram becomes the outer diagram of the following

$$\begin{tikzcd}
F((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} M) \arrow[r, "F(\mathrm{id}_{X \otimes_{\mathcal{C}} Y} \otimes_{\mathcal{M}} \varepsilon_M^{-1})"] \arrow[d, "F(m_{X,Y,M})"'] & F((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} GF(M)) \arrow[d, "F(m_{X,Y,GF(M)})"] \\
F(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} M)) \arrow[r, "F(\mathrm{id}_X \otimes_{\mathcal{M}} (\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon_M^{-1}))"] \arrow[d, "F(\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y \otimes_{\mathcal{M}} M})"'] & F(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} GF(M))) \arrow[d, "F(\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y \otimes_{\mathcal{M}} GF(M)})"] \\
F(X \otimes_{\mathcal{M}} GF(Y \otimes_{\mathcal{M}} M)) \arrow[r, "F(\mathrm{id}_X \otimes_{\mathcal{M}} GF(\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon_M^{-1}))"] & F(X \otimes_{\mathcal{M}} GF(Y \otimes_{\mathcal{M}} GF(M)))
\end{tikzcd}$$

for all $X, Y \in \mathcal{C}$ and $M \in \mathcal{M}$. By naturality of m, the upper rectangle commutes, while the naturality of ε makes the lower rectangle commutative. As a consequence, we get the commutativity of the outer rectangle.
We are left to prove that Diagram (4.1.9) is commutative, that is the following

$$\begin{tikzcd}
F(1 \otimes_{\mathcal{M}} M) \arrow[r, "F(\mathrm{id}_1 \otimes_{\mathcal{M}} \varepsilon_M^{-1})"] \arrow[d] & F(1 \otimes_{\mathcal{M}} GF(M)) \arrow[d] \\
F(M) \arrow[r, "\varepsilon_M^{-1}"] & FGF(M)
\end{tikzcd}$$

is commutative for any $M \in \mathcal{M}$. This follows from the naturality of ε. $\square$

We can dualize the above construction for a right $\mathcal{C}$-module category.

Let $\mathcal{C}$ be a monoidal category and let $\mathcal{M}$ be a right $\mathcal{C}$-module category, via the action bifunctor $\otimes^{\mathcal{M}}\colon \mathcal{M} \times \mathcal{C} \to \mathcal{M}$ and with module associativity constraint $m^r_{X,Y,M}$. Consider as before, an equivalence $F\colon \mathcal{M} \to \mathcal{N}$ with quasi-inverse G and natural isomorphisms η and ε, such that $G \circ F \overset{\varepsilon}{\approx} \mathrm{id}_{\mathcal{M}}$ and $F \circ G \overset{\eta}{\approx} \mathrm{id}_{\mathcal{N}}$. Then, we have the right-handed version of the definitions given above. We define the bifunctor

$$\begin{aligned} \otimes^{\mathcal{N}}\colon \mathcal{N} \times \mathcal{C} &\to \mathcal{N} \\ (-,\sim) &\mapsto F(G(-)\otimes^{\mathcal{M}} \sim) \end{aligned} \tag{4.2.10}$$

and the maps

$$n^r_{N,X,Y}\colon (N \otimes^{\mathcal{N}} X) \otimes^{\mathcal{N}} Y \to N \otimes^{\mathcal{N}} (X \otimes Y)$$

as

$$n^r_{N,X,Y} := F(m^r_{G(N),X,Y} \circ (\varepsilon_{G(N)\otimes^{\mathcal{M}} X} \otimes^{\mathcal{M}} \mathrm{id}_Y)). \tag{4.2.11}$$

for every $X, Y \in \mathcal{C}$ and $N \in \mathcal{N}$.
In the same way as for the left $\mathcal{C}$-module category, we can prove the right-handed version of Lemma 4.2.2 and Lemma 4.2.3.

Lemma 4.2.4. *Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ be a monoidal category and let $(\mathcal{M}, \otimes^{\mathcal{M}}, m^r)$ be a right $\mathcal{C}$-module category. Let $F\colon \mathcal{M} \to \mathcal{N}$ be an equivalence of categories, with quasi-inverse $G\colon \mathcal{N} \to \mathcal{M}$ and natural isomorphisms η and ε such that $G \circ F \overset{\varepsilon}{\approx} id_{\mathcal{M}}$ and $F \circ G \overset{\eta}{\approx} id_{\mathcal{N}}$. The category $\mathcal{N}$ endowed with $\otimes^{\mathcal{N}}$ as in Equation (4.2.10), with the morphism $n^r_{N,X,Y}$ as in Equation (4.2.11) is a right $\mathcal{C}$-module category.*
Moreover, let $s^r_{X,M} := F(\varepsilon_M^{-1} \otimes^{\mathcal{M}} id_X)$ and let $t^r_{X,N} := \varepsilon_{G(N)\otimes^{\mathcal{M}} X}$, for all $X \in \mathcal{C}, M \in \mathcal{M}$ and $N \in \mathcal{N}$. Then, the pairs (F, s^r) and (G, t^r) are right $\mathcal{C}$-module functors.

It is now natural to expect that the transported structure of a $(\mathcal{C}, \mathcal{D})$-bimodule category by means of an equivalence is again a $(\mathcal{C}, \mathcal{D})$-bimodule category.
Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ and $(\mathcal{D}, \otimes_{\mathcal{D}}, \tilde{a}, \tilde{1})$ be two monoidal categories and let $(\mathcal{M}, m, m^r, b)$ be a $(\mathcal{C}, \mathcal{D})$-bimodule category. Consider $F\colon \mathcal{M} \to \mathcal{N}$ an equivalence, with quasi-inverse G, and natural isomorphisms η and ε such that $G \circ F \overset{\varepsilon}{\approx} \mathrm{id}_{\mathcal{M}}$ and $F \circ G \overset{\eta}{\approx} \mathrm{id}_{\mathcal{N}}$. Using the above notation we define for every $X \in \mathcal{C}, Z \in \mathcal{D}$ and $N \in \mathcal{N}$, the maps

$$p_{X,N,Z}\colon (X \otimes_{\mathcal{N}} N) \otimes^{\mathcal{N}} Z \to X \otimes_{\mathcal{N}} (N \otimes^{\mathcal{N}} Z)$$

as

$$p_{X,N,Z} := F\Big((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ b_{X,G(N),Z} \circ (\varepsilon_{X \otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)\Big). \quad (4.2.12)$$

Remark 4.2.5. Since p is defined as the image of a composition of natural isomorphisms through an equivalence, then it is a natural isomorphism.

We are now in a position to prove the following result.

Lemma 4.2.6. *Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ and $(\mathcal{D}, \otimes_{\mathcal{D}}, \tilde{a}, \tilde{1})$ be monoidal categories and let $(\mathcal{M}, \otimes_{\mathcal{M}}, \otimes^{\mathcal{M}}, m, m^r, b)$ be a $(\mathcal{C}, \mathcal{D})$-bimodule category. Consider $F\colon \mathcal{M} \to \mathcal{N}$ an equivalence, with quasi-inverse G, and natural isomorphisms η and ε such that $G \circ F \overset{\varepsilon}{\approx} id_{\mathcal{M}}$ and $F \circ G \overset{\eta}{\approx} id_{\mathcal{N}}$. The category $\mathcal{N}$ endowed with $\otimes_{\mathcal{N}}$, $\otimes^{\mathcal{N}}$ as in Equation (4.2.1) and Equation (4.2.10), the morphisms $n_{X,Y,N}$, $n^r_{N,X,Y}$ and $p_{X,N,Z}$ for any $X, Y, Z \in \mathcal{C}$ and $N \in \mathcal{N}$ as in Equation (4.2.2), (4.2.11) and in Equation (4.2.12), respectively, is a $(\mathcal{C}, \mathcal{D})$-bimodule category.*
Furthermore, the functors (F, s, s^r) and (G, t, t^r) with s and t as in Lemma 4.2.3 and s^r, t^r as in Lemma 4.2.4 are $(\mathcal{C}, \mathcal{D})$-bimodule functors.

Proof. We first prove that $(\mathcal{N}, \otimes_{\mathcal{N}}, \otimes^{\mathcal{N}}, n, n^r, p)$ is a $(\mathcal{C}, \mathcal{D})$-bimodule category.
By Lemma 4.2.2, Lemma 4.2.4 and Remark 4.2.5, we only need to prove that diagrams (4.1.5) and (4.1.6) commute.
Consider the first diagram. We want to show that the diagram

$$\begin{tikzcd}
 & ((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{N}} N) \otimes^{\mathcal{N}} Z \arrow[dl, "n_{X,Y,N} \otimes^{\mathcal{N}} \mathrm{id}_Z"'] \arrow[dr, "p_{X \otimes_{\mathcal{C}} Y, N, Z}"] & \\
(X \otimes_{\mathcal{N}} (Y \otimes_{\mathcal{N}} N)) \otimes^{\mathcal{N}} Z \arrow[d, "p_{X, Y \otimes_{\mathcal{N}} N, Z}"'] & & (X \otimes_{\mathcal{C}} Y) \otimes^{\mathcal{N}} (N \otimes^{\mathcal{N}} Z) \arrow[d, "n_{X,Y,N \otimes^{\mathcal{N}} Z}"] \\
X \otimes_{\mathcal{N}} ((Y \otimes_{\mathcal{N}} N) \otimes^{\mathcal{N}} Z) \arrow[rr, "\mathrm{id}_X \otimes_{\mathcal{N}} p_{Y,N,Z}"] & & X \otimes_{\mathcal{N}} (Y \otimes_{\mathcal{N}} (N \otimes^{\mathcal{N}} Z))
\end{tikzcd}$$

is commutative for every $X, Y \in \mathcal{C}, Z \in \mathcal{D}$ and $N \in \mathcal{N}$. By Equations (4.2.2) and (4.2.12), this is equivalent to verify that

$$\begin{aligned}
&F(\mathrm{id}_X \otimes_{\mathcal{M}} GF((\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ b_{Y,G(N),Z} \circ (\varepsilon_{Y\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)))\circ\\
&F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{GF(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} \mathrm{id}_Z})\circ b_{X,GF(Y\otimes_{\mathcal{M}} G(N)),Z}\circ(\varepsilon_{X\otimes_{\mathcal{M}} GF(Y\otimes_{\mathcal{M}} G(N))} \otimes^{\mathcal{M}} \mathrm{id}_Z))\circ\\
&F(GF((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y\otimes_{\mathcal{M}} G(N)}) \circ m_{X,Y,G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z) =\\
&F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y\otimes_{\mathcal{M}} GF(G(N)\otimes^{\mathcal{M}} Z)}) \circ m_{X,Y,GF(G(N)\otimes^{\mathcal{M}} Z)} \circ (id_{X\otimes_{\mathcal{C}} Y} \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}))\circ\\
&F(b_{X\otimes_{\mathcal{C}} Y,G(N),Z} \circ (\varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)).
\end{aligned} \tag{4.2.13}$$

We will make use of a series of commutative diagrams. By naturality of ε, the following five diagrams

$$\begin{tikzcd}
GF(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} G(N))) \arrow[r, "\varepsilon_{X\otimes_{\mathcal{M}}(Y\otimes_{\mathcal{M}} G(N))}"] & X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} G(N)) \\
GF((X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} G(N))) \arrow[u, "GF(m_{X,Y,G(N)})"] \arrow[r, "\varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)}"] & (X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} G(N)), \arrow[u, "m_{X,Y,G(N)}"']
\end{tikzcd} \tag{4.2.14}$$

$$\begin{tikzcd}
GF(X \otimes_{\mathcal{M}} GF(Y \otimes_{\mathcal{M}} G(N))) \arrow[r, "\varepsilon_{X\otimes_{\mathcal{M}} GF(Y\otimes_{\mathcal{M}} G(N))}"] \arrow[d, "GF(\mathrm{id}_X\otimes_{\mathcal{M}}\varepsilon_{Y\otimes_{\mathcal{M}} G(N)})"'] & X \otimes_{\mathcal{M}} GF(Y \otimes_{\mathcal{M}} G(N)) \arrow[d, "\mathrm{id}_X\otimes_{\mathcal{M}}\varepsilon_{Y\otimes_{\mathcal{M}} G(N)}"] \\
GF(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} G(N))) \arrow[r, "\varepsilon_{X\otimes_{\mathcal{M}}(Y\otimes_{\mathcal{M}} G(N))}"] & X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} G(N)),
\end{tikzcd} \tag{4.2.15}$$

$$\begin{tikzcd}
GF((Y \otimes_{\mathcal{M}} G(N)) \otimes^{\mathcal{M}} Z) \arrow[r, "\varepsilon_{(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} Z}"] \arrow[d, "GF(b_{Y,G(N),Z})"'] & (Y \otimes_{\mathcal{M}} G(N)) \otimes^{\mathcal{M}} Z \arrow[d, "b_{Y,G(N),Z}"] \\
GF(Y \otimes_{\mathcal{M}} (G(N) \otimes^{\mathcal{M}} Z)) \arrow[r, "\varepsilon_{Y\otimes_{\mathcal{M}}(G(N)\otimes^{\mathcal{M}} Z)}"] & Y \otimes_{\mathcal{M}} (G(N) \otimes^{\mathcal{M}} Z),
\end{tikzcd} \tag{4.2.16}$$

$$\begin{tikzcd}
GF(GF(Y \otimes_{\mathcal{M}} G(N)) \otimes^{\mathcal{M}} Z) \arrow[r, "\varepsilon_{GF(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} Z}"] \arrow[d, "GF(\varepsilon_{Y\otimes_{\mathcal{M}} G(N)}\otimes^{\mathcal{M}}\mathrm{id}_Z)"'] & GF(Y \otimes_{\mathcal{M}} G(N)) \otimes^{\mathcal{M}} Z \arrow[d, "\varepsilon_{Y\otimes_{\mathcal{M}} G(N)}\otimes^{\mathcal{M}}\mathrm{id}_Z"] \\
GF((Y \otimes_{\mathcal{M}} G(N)) \otimes^{\mathcal{M}} Z) \arrow[r, "\varepsilon_{(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} Z}"] & (Y \otimes_{\mathcal{M}} G(N)) \otimes^{\mathcal{M}} Z,
\end{tikzcd} \tag{4.2.17}$$

and

$$\begin{tikzcd}
GF(Y \otimes_{\mathcal{M}} (G(N) \otimes^{\mathcal{M}} Z)) \arrow[r, "\varepsilon_{Y \otimes_{\mathcal{M}} (G(N) \otimes^{\mathcal{M}} Z)}"] \arrow[d, "GF(\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N) \otimes^{\mathcal{M}} Z})"'] & Y \otimes_{\mathcal{M}} (G(N) \otimes^{\mathcal{M}} Z) \arrow[d, "\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N) \otimes^{\mathcal{M}} Z}"] \\
GF(Y \otimes_{\mathcal{M}} GF(G(N) \otimes^{\mathcal{M}} Z)) \arrow[r, "\varepsilon_{Y \otimes_{\mathcal{M}} GF(G(N) \otimes^{\mathcal{M}} Z)}"] & Y \otimes_{\mathcal{M}} GF(G(N) \otimes^{\mathcal{M}} Z)
\end{tikzcd} \tag{4.2.18}$$

commute for every $N \in \mathcal{N}$, $X, Y \in \mathcal{C}$ and $Z \in \mathcal{D}$.
Moreover, by the naturality of m the following diagram:

$$\begin{tikzcd}
(X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} GF(G(N) \otimes^{\mathcal{M}} Z) \arrow[r, "m_{X,Y,GF(G(N) \otimes^{\mathcal{M}} Z)}"] \arrow[d, "\mathrm{id}_{X \otimes_{\mathcal{C}} Y} \otimes_{\mathcal{M}} \varepsilon_{G(N) \otimes^{\mathcal{M}} Z}"'] & X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} GF(G(N) \otimes^{\mathcal{M}} Z)) \arrow[d, "\mathrm{id}_X \otimes_{\mathcal{M}} (\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon_{G(N) \otimes^{\mathcal{M}} Z})"] \\
(X \otimes_{\mathcal{C}} Y) \otimes_{\mathcal{M}} (G(N) \otimes^{\mathcal{M}} Z) \arrow[r, "m_{X,Y,G(N) \otimes^{\mathcal{M}} Z}"] & X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} (G(N) \otimes^{\mathcal{M}} Z))
\end{tikzcd} \tag{4.2.19}$$

commutes for every $X, Y \in \mathcal{C}, Z \in \mathcal{D}$ and $N \in \mathcal{N}$.
Furthermore, by naturality of b the diagram

$$\begin{tikzcd}
(X \otimes_{\mathcal{M}} GF(Y \otimes_{\mathcal{M}} G(N))) \otimes^{\mathcal{M}} Z \arrow[r, "b_{X,GF(Y \otimes_{\mathcal{M}} G(N)),Z}"] \arrow[d, "(\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon_{Y \otimes_{\mathcal{M}} G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z"'] & X \otimes_{\mathcal{M}} (GF(Y \otimes_{\mathcal{M}} G(N)) \otimes^{\mathcal{M}} Z) \arrow[d, "\mathrm{id}_X \otimes_{\mathcal{M}} (\varepsilon_{Y \otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)"] \\
(X \otimes_{\mathcal{M}} (Y \otimes_{\mathcal{M}} G(N))) \otimes^{\mathcal{M}} Z \arrow[r, "b_{X,Y \otimes_{\mathcal{M}} G(N),Z}"] & X \otimes_{\mathcal{M}} ((Y \otimes_{\mathcal{M}} G(N)) \otimes^{\mathcal{M}} Z)
\end{tikzcd} \tag{4.2.20}$$

is commutative for every $X, Y \in \mathcal{C}, Z \in \mathcal{D}$ and $N \in \mathcal{N}$.

Consider the left-hand side of equation (4.2.13). By commutativity of diagram (4.2.14), we get:

$F(\mathrm{id}_X \otimes_{\mathcal{M}} GF((\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ b_{Y,G(N),Z} \circ (\varepsilon_{Y\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)))\circ$
$F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{GF(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} \mathrm{id}_Z}) \circ b_{X,GF(Y\otimes_{\mathcal{M}} G(N)),Z} \circ (\varepsilon_{X\otimes_{\mathcal{M}} GF(Y\otimes_{\mathcal{M}} G(N))} \otimes^{\mathcal{M}} \mathrm{id}_Z))\circ$
$F(GF((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y\otimes_{\mathcal{M}} G(N)}) \circ m_{X,Y,G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z) =$
$F(\mathrm{id}_X \otimes_{\mathcal{M}} GF((\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ b_{Y,G(N),Z} \circ (\varepsilon_{Y\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)))\circ$
$F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{GF(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} \mathrm{id}_Z}) \circ b_{X,GF(Y\otimes_{\mathcal{M}} G(N)),Z} \circ (\varepsilon_{X\otimes_{\mathcal{M}} GF(Y\otimes_{\mathcal{M}} G(N))} \otimes^{\mathcal{M}} \mathrm{id}_Z))\circ$
$F((GF(\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y\otimes_{\mathcal{M}} G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z) \circ ((\varepsilon^{-1}_{X\otimes_{\mathcal{M}}(Y\otimes_{\mathcal{M}} G(N))} \circ m_{X,Y,G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z)\circ$
$F(\varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)).$

The commutativity of diagram (4.2.15) gives:

$F(\mathrm{id}_X \otimes_{\mathcal{M}} GF((\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ b_{Y,G(N),Z} \circ (\varepsilon_{Y\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)))\circ$
$F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{GF(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} \mathrm{id}_Z}) \circ b_{X,GF(Y\otimes_{\mathcal{M}} G(N)),Z} \circ (\varepsilon_{X\otimes_{\mathcal{M}} GF(Y\otimes_{\mathcal{M}} G(N))} \otimes^{\mathcal{M}} \mathrm{id}_Z))\circ$
$F((\varepsilon^{-1}_{X\otimes_{\mathcal{M}} GF(Y\otimes_{\mathcal{M}} G(N))} \circ (\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y\otimes_{\mathcal{M}} G(N)}) \circ m_{X,Y,G(N)} \circ \varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z) =$
$F(\mathrm{id}_X \otimes_{\mathcal{M}} GF((\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ b_{Y,G(N),Z} \circ (\varepsilon_{Y\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)))\circ$
$F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{GF(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} \mathrm{id}_Z}) \circ b_{X,GF(Y\otimes_{\mathcal{M}} G(N)),Z})\circ$
$F(((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y\otimes_{\mathcal{M}} G(N)}) \circ m_{X,Y,G(N)} \circ \varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z)$

By commutativity of (4.2.20), the previous term becomes:

$F(\mathrm{id}_X \otimes_{\mathcal{M}} GF((\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ b_{Y,G(N),Z} \circ (\varepsilon_{Y\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)))\circ$
$F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{GF(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} \mathrm{id}_Z}) \circ (\mathrm{id}_X \otimes_{\mathcal{M}} (\varepsilon^{-1}_{Y\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)) \circ b_{X,Y\otimes_{\mathcal{M}} G(N),Z})\circ$
$F((m_{X,Y,G(N)} \circ \varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z)$

By virtue of commutativity of diagram (4.2.16), the above reads as:

$F(\mathrm{id}_X \otimes_{\mathcal{M}} (GF(\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ (\varepsilon^{-1}_{Y\otimes_{\mathcal{M}}(G(N)\otimes^{\mathcal{M}} Z)} \circ b_{Y,G(N),Z} \circ \varepsilon_{(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} Z})))\circ$
$F(GF(\varepsilon_{Y\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z) \circ (\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{GF(Y\otimes_{\mathcal{M}} G(N))\otimes^{\mathcal{M}} \mathrm{id}_Z}))\circ$
$F((\mathrm{id}_X \otimes_{\mathcal{M}} (\varepsilon^{-1}_{Y\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)) \circ b_{X,Y\otimes_{\mathcal{M}} G(N),Z})\circ$
$F((m_{X,Y,G(N)} \circ \varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z).$

By commutativity of diagram (4.2.17) the previous term becomes:

$$F(\mathrm{id}_X \otimes_{\mathcal{M}} (GF(\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ (\varepsilon^{-1}_{Y\otimes_{\mathcal{M}}(G(N)\otimes^{\mathcal{M}} Z)} \circ b_{Y,G(N),Z})))\circ$$
$$F(b_{X,Y\otimes_{\mathcal{M}} G(N),Z} \circ ((m_{X,Y,G(N)} \circ \varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z)).$$

Finally, by commutativity of diagram (4.2.18) the above equals

$$\begin{aligned} &F(\mathrm{id}_X \otimes_{\mathcal{M}} (\varepsilon^{-1}_{Y\otimes_{\mathcal{M}} GF(G(N)\otimes^{\mathcal{M}} Z)} \circ (\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z}) \circ b_{Y,G(N),Z}))\circ \\ &F(b_{X,Y\otimes_{\mathcal{M}} G(N),Z} \circ ((m_{X,Y,G(N)} \circ \varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)}) \otimes^{\mathcal{M}} \mathrm{id}_Z)).\end{aligned} \tag{4.2.21}$$

Consider now the right hand-side of equation (4.2.13). By commutativity of diagram (4.2.19), it equals

$$F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y\otimes_{\mathcal{M}} GF(G(N)\otimes^{\mathcal{M}} Z)}) \circ (\mathrm{id}_X \otimes_{\mathcal{M}} (\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z})) \circ m_{X,Y,G(N)\otimes^{\mathcal{M}} Z})\circ \\ F(b_{X\otimes_{\mathcal{C}} Y, G(N), Z} \circ (\varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)). \tag{4.2.22}$$

Since $F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{Y\otimes_{\mathcal{M}} GF(G(N)\otimes^{\mathcal{M}} Z)}) \circ (\mathrm{id}_X \otimes_{\mathcal{M}} (\mathrm{id}_Y \otimes_{\mathcal{M}} \varepsilon^{-1}_{G(N)\otimes^{\mathcal{M}} Z})))$ and $(\varepsilon_{(X\otimes_{\mathcal{C}} Y)\otimes_{\mathcal{M}} G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)$ are natural isomorphisms, then equation (4.2.13) is satisfied if and only if :

$$F((\mathrm{id}_X \otimes_{\mathcal{M}} b_{Y,G(N),Z}) \circ b_{X,Y\otimes_{\mathcal{M}} G(N),Z} \circ (m_{X,Y,G(N)} \otimes^{\mathcal{M}} \mathrm{id}_Z)) = \\ F(m_{X,Y,G(N)\otimes^{\mathcal{M}} Z} \circ b_{X\otimes_{\mathcal{C}} Y, G(N), Z}).$$

This equation holds, since $\mathcal{M}$ is a $(\mathcal{C},\mathcal{D})$-bimodule category.
The other diagram is completely analogous to prove.

We now show that (F, s, s^r) is a $(\mathcal{C},\mathcal{D})$-bimodule functor. By Lemma 4.2.3 and Lemma 4.2.4 the pairs (F, s) and (F, s^r) are respectively a left $\mathcal{C}$-module functor and a right $\mathcal{D}$-module functor. We are left to prove the commutativity of Diagram (4.1.10). By the definition of s, s^r and p this is equivalent to verify that the following diagram commutes

$$\begin{tikzcd}
F((X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} Y) \arrow[r, "F(b_{X,M,Y})"] \arrow[d, "F(\varepsilon^{-1}_{X\otimes_{\mathcal{M}} M}\otimes^{\mathcal{M}}\mathrm{id}_Y)"'] & F(X \otimes_{\mathcal{M}} (M \otimes^{\mathcal{M}} Y)) \arrow[d, "F(\mathrm{id}_X \otimes_{\mathcal{M}}\varepsilon^{-1}_{M\otimes^{\mathcal{M}} Y})"] \\
F(GF(X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} Y) \arrow[d, "F(GF(\mathrm{id}_X \otimes_{\mathcal{M}}\varepsilon^{-1}_M)\otimes^{\mathcal{M}}\mathrm{id}_Y)"'] & F(X \otimes_{\mathcal{M}} GF(M \otimes^{\mathcal{M}} Y)) \arrow[d, "F(\mathrm{id}_X \otimes_{\mathcal{M}} GF(\varepsilon^{-1}_M\otimes^{\mathcal{M}}\mathrm{id}_Y))"] \\
F(GF(X \otimes_{\mathcal{M}} GF(M)) \otimes^{\mathcal{M}} Y) \arrow[d, "F(\varepsilon_{X\otimes_{\mathcal{M}} GF(M)}\otimes^{\mathcal{M}}\mathrm{id}_Y)"'] & F(X \otimes_{\mathcal{M}} GF(GF(M) \otimes^{\mathcal{M}} Y)) \\
F((X \otimes_{\mathcal{M}} GF(M)) \otimes^{\mathcal{M}} Y) \arrow[r, "F(b_{X,GF(M),Y})"] & F(X \otimes_{\mathcal{M}} (GF(M) \otimes^{\mathcal{M}} Y)) \arrow[u, "F(\mathrm{id}_X \otimes_{\mathcal{M}}\varepsilon^{-1}_{GF(M)\otimes^{\mathcal{M}} Y})"']
\end{tikzcd} \tag{4.2.23}$$

for every $X \in \mathcal{C}$, $Y \in \mathcal{D}$ and $M \in \mathcal{M}$.
For this purpose, we will use the following diagrams

$$\begin{tikzcd}
F((X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} Y) \arrow[r, "F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon_M^{-1}) \otimes^{\mathcal{M}} \mathrm{id}_Y)"] \arrow[d, "F(\varepsilon^{-1}_{X \otimes_{\mathcal{M}} M} \otimes^{\mathcal{M}} \mathrm{id}_Y)"'] & F((X \otimes_{\mathcal{M}} GF(M)) \otimes^{\mathcal{M}} Y) \arrow[d, "F(\varepsilon^{-1}_{X \otimes_{\mathcal{M}} GF(M)} \otimes^{\mathcal{M}} Y)"] \\
F(GF(X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} Y) \arrow[r, "F(GF(\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon_M^{-1}) \otimes^{\mathcal{M}} \mathrm{id}_Y)"] & F(GF(X \otimes_{\mathcal{M}} GF(M)) \otimes^{\mathcal{M}} Y)
\end{tikzcd} \tag{4.2.24}$$

and

$$\begin{tikzcd}
F(X \otimes_{\mathcal{M}} (M \otimes^{\mathcal{M}} Y)) \arrow[r, "F(\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{M \otimes^{\mathcal{M}} Y})"] \arrow[d, "F(\mathrm{id}_X \otimes_{\mathcal{M}} (\varepsilon_M^{-1} \otimes^{\mathcal{M}} \mathrm{id}_Y))"'] & F(X \otimes_{\mathcal{M}} GF(M \otimes^{\mathcal{M}} Y)) \arrow[d, "F(\mathrm{id}_X \otimes_{\mathcal{M}} GF(\varepsilon_M^{-1} \otimes^{\mathcal{M}} \mathrm{id}_Y))"] \\
F(X \otimes_{\mathcal{M}} (GF(M) \otimes^{\mathcal{M}} Y)) \arrow[r, "F(\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon^{-1}_{GF(M) \otimes^{\mathcal{M}} Y})"] & F(X \otimes_{\mathcal{M}} GF(GF(M) \otimes^{\mathcal{M}} Y))
\end{tikzcd} \tag{4.2.25}$$

which commute for every $X \in \mathcal{C}$, $M \in \mathcal{M}$ and $Y \in \mathcal{D}$ in virtue of the naturality of ε. Thus diagram (4.2.23) reads as

$$\begin{tikzcd}
F((X \otimes_{\mathcal{M}} M) \otimes^{\mathcal{M}} Y) \arrow[r, "F(b_{X,M,Y})"] \arrow[d, "F((\mathrm{id}_X \otimes_{\mathcal{M}} \varepsilon_M^{-1}) \otimes^{\mathcal{M}} \mathrm{id}_Y)"'] & F(X \otimes_{\mathcal{M}} (M \otimes^{\mathcal{M}} Y)) \arrow[d, "F(\mathrm{id}_X \otimes_{\mathcal{M}} (\varepsilon_M^{-1} \otimes^{\mathcal{M}} \mathrm{id}_Y))"] \\
F((X \otimes_{\mathcal{M}} GF(M)) \otimes^{\mathcal{M}} Y) \arrow[r, "F(b_{X,GF(M),Y})"] & F(X \otimes_{\mathcal{M}} (GF(M) \otimes^{\mathcal{M}} Y))
\end{tikzcd}$$

for every $X \in \mathcal{C}$, $M \in \mathcal{M}$ and $Y \in \mathcal{D}$ and it is commutative by the naturality of b.
The proof for (G, t, t^r) is analogous. $\square$

CHAPTER 5

Preliminaries on W-algebras

In this chapter we recall the construction of a finite-dimensional W-algebra. Moreover, we state an important equivalence between categories of modules due to Skryabin.

Let $\mathfrak{g}$ be a finite-dimensional reductive Lie algebra over $\mathbb{C}$ and let $e \in \mathfrak{g}$ be nilpotent. Throughout the next chapters, by a grading on a Lie algebra $\mathfrak{g}$ we mean a Lie algebra grading, i.e. a grading of the vector space $\mathfrak{g} = \bigoplus_{j\in\mathbb{Z}} \mathfrak{g}(j)$ such that $[\mathfrak{g}(i), \mathfrak{g}(j)] \subseteq \mathfrak{g}(i+j)$, for every $i, j \in \mathbb{Z}$.

A $\mathbb{Z}$-grading

$$\mathfrak{g} = \bigoplus_{j\in\mathbb{Z}} \mathfrak{g}(j)$$

of $\mathfrak{g}$ is called a *good grading* for e if

(1) $e \in \mathfrak{g}(2)$;
(2) $\mathfrak{g}^e \subseteq \bigoplus_{j\geq 0} \mathfrak{g}(j)$, where $\mathfrak{g}^e$ stands for the centralizer of e in $\mathfrak{g}$;
(3) $\mathfrak{z}(\mathfrak{g}) \subseteq \mathfrak{g}(0)$, where $\mathfrak{z}(\mathfrak{g})$ denotes the centre of $\mathfrak{g}$.

A classification of such gradings can be found in [20].

Example 5.0.1. Let e be a nilpotent element in $\mathfrak{g}$. By Jacobson-Morozov Theorem, there is an $\mathfrak{sl}_2$-triple (e, h, f), associated to e.
The standard good grading is the one induced by the adjoint action of h, called the Dynkin grading, that is

$$\mathfrak{g}(i) = \{x \in \mathfrak{g} \,|\, [h, x] = ix\}.$$

Remark 5.0.1. Every grading of $\mathfrak{g}$ satisfying $\mathfrak{z}(\mathfrak{g}) \subseteq \mathfrak{g}(0)$ is induced by the adjoint action of a semisimple element. Indeed, let $\mathfrak{s}$ be a semisimple Lie algebra and let $\mathfrak{s} = \bigoplus_{j\in\mathbb{Z}} \mathfrak{s}(j)$ be a grading for $\mathfrak{s}$. We define $\delta\colon \mathfrak{s} \to \mathfrak{s}$ as $\delta(x) = jx$ for $x \in \mathfrak{s}(j)$. One can verify that it is a derivation and since all derivations in $\mathfrak{s}$ are inner ([65, Proposition 20.1.5]), there exists a semisimple element $q \in \mathfrak{s}$, such that $\delta = [q, -]$.
The result follows also for a reductive Lie algebra, since it is the direct sum of a semisimple Lie algebra with an abelian one.

Throughout this chapter, we fix a $\mathbb{Z}$-good grading.
Consider $(\cdot|\cdot)$ a non-degenerate symmetric invariant bilinear form on $\mathfrak{g}$. Define

$\chi \in \mathfrak{g}^*$ in the following way:

$$\chi\colon \mathfrak{g} \to \mathbb{C}, \qquad x \mapsto (e|x).$$

By definition of good grading, $e \in \mathfrak{g}(2)$ and $\chi(x) = (e|x) = 0$ for every $x \in \mathfrak{g}(j)$, unless $j = -2$.
Let $\langle \cdot|\cdot \rangle$ be the non-degenerate alternating bilinear form on $\mathfrak{g}(-1)$ defined by

$$\langle x|y \rangle := \chi([y,x]).$$

Fix ℓ an isotropic subspace of $\mathfrak{g}(-1)$ with respect to $\langle \cdot|\cdot \rangle$.
Let $\ell^\perp = \{x \in \mathfrak{g}(-1) \,|\, \langle x, y\rangle = 0 \text{ for all } y \in \ell\}$, so $\ell \subseteq \ell^\perp$. We define the following subalgebras:

$$\mathfrak{m}_\ell = \ell \oplus \bigoplus_{j<-1} \mathfrak{g}(j), \qquad \mathfrak{n}_\ell = \ell^\perp \oplus \bigoplus_{j<-1} \mathfrak{g}(j),$$

so $\mathfrak{m}_\ell \subseteq \mathfrak{n}_\ell$. The algebras $\mathfrak{n}_\ell$ and $\mathfrak{m}_\ell$ are nilpotent, because they are subalgebras of the nilpotent algebra $\bigoplus_{j<0} \mathfrak{g}(j)$. Moreover, $\mathfrak{m}_\ell$ is a Lie ideal of $\mathfrak{n}_\ell$. Indeed, $[\mathfrak{m}_\ell, \mathfrak{n}_\ell] \subseteq \bigoplus_{j<-1} \mathfrak{g}(j) \subseteq \mathfrak{m}_\ell$.

In order to construct the finite W-algebra H_ℓ, we need to recollect the following facts.

i) The map χ restricts to a character of $\mathfrak{m}_\ell$.
This means that $\chi([x,y]) = ([x,y]|e) = 0$, for every $x, y \in \mathfrak{m}_\ell$. We show that. Since $(z|e) = 0$, for every $z \in \mathfrak{g}(j)$, with $j \neq -2$, then for every $x \in \oplus_{i \leq -2} \mathfrak{g}(i)$ and $y \in \mathfrak{m}_\ell$, $\chi([x,y]) = 0$. It remains to verify that for $x, y \in \ell$, $\chi([y,x]) = 0$. This is a consequence of the isotropy of ℓ.

ii) We can then define

$$Q_\ell := U(\mathfrak{g}) \otimes_{U(\mathfrak{m}_\ell)} \mathbb{C}_\chi,$$

where $\mathbb{C}_\chi$ is the 1-dimensional left $U(\mathfrak{m}_\ell)$-module obtained from the character χ. In particular, $Q_\ell \simeq U(\mathfrak{g})/I_\ell$, where I_ℓ is the left ideal generated by $x - \chi(x)$ for every $x \in \mathfrak{m}_\ell$.

iii) The left multiplication in $U(\mathfrak{g})$ induces an action on Q_ℓ. In particular,

$$x.(y + I_\ell) = xy + I_\ell,$$

for every $x, y \in U(\mathfrak{g})$.

iv) There is an induced $\mathrm{ad}(\mathfrak{n}_\ell)$-action on Q_ℓ, since the ideal I_ℓ is stable under the action of $\mathfrak{n}_\ell$. We show this fact.
We need to verify that $[z, I_\ell] \subseteq I_\ell$, for every $z \in \mathfrak{n}_\ell$. This means that

$$[z, y(x - \chi(x))] = [z,y](x - \chi(x)) + y[z,x]$$

lies in I_ℓ for every $x \in \mathfrak{m}_\ell$, $z \in \mathfrak{n}_\ell$ and $y \in U(\mathfrak{g})$. Since $[z,x] \in \mathfrak{m}_\ell$ and $\chi([z,x]) = 0$, we get the desired inclusion.

Hence, it makes sense to define

$$H_\ell := Q_\ell^{\operatorname{ad}\mathfrak{n}_\ell},$$

that is the subspace of all $x + I_\ell$, with $x \in U(\mathfrak{g})$ such that

$$yx - xy \in I_\ell \qquad \text{for all} \qquad y \in \mathfrak{n}_\ell. \tag{$\clubsuit$}$$

We can define an algebra structure on H_ℓ via

$$(x + I_\ell)(y + I_\ell) = xy + I_\ell,$$

for $x + I_\ell, y + I_\ell \in H_\ell$. We verify that this multiplication is well defined.
Firstly, for any $w \in \mathfrak{m}_\ell$ and $y + I_\ell \in H_\ell$ we have $[w, y] \subset [\mathfrak{m}_\ell, y] \subset [\mathfrak{n}_\ell, y] \subset I_\ell$.
Then, for every $w \in \mathfrak{m}_\ell$ and $y + I_\ell \in H_\ell$, we get that $(w - \chi(w))y \in I_\ell$, since $(w - \chi(w))y = yw - y\chi(w) + [w, y] \in y(w - \chi(w)) + I_\ell \subset I_\ell$. It follows that

$$I_\ell \cdot y \subset I_\ell, \tag{5.0.1}$$

for all $y + I_\ell \in H_\ell$.
Furthermore, the algebra H_ℓ is closed under multiplication because if $z \in \mathfrak{n}_\ell$ and $x+I_\ell, y+I_\ell \in H_\ell$, then $zxy-xyz = (zx-xz)y+x(zy-yz) \in I_\ell y+xI_\ell \subseteq I_\ell$, by Equation (5.0.1).

The algebra H_ℓ is called the *finite W-algebra* associated with e.

Remark 5.0.2. We stress the fact that the finite W-algebra H_ℓ does not depend on the choice of the good grading ([7, Theorem 1]) and neither from the Lagrangian ([25, Theorem 4.1]), but it depends only on the adjoint orbit of e (see [65, Chapter 34] for the definition of the action).

Remark 5.0.3. Notice that Q_ℓ is a $U(\mathfrak{g})$-H_ℓ -bimodule. We mentioned above (iii) that $U(\mathfrak{g})$ acts on Q_ℓ by left multiplication.
The right action of H_ℓ on Q_ℓ is induced by right multiplication. We show that this is indeed an action. Let $y \in U(\mathfrak{g})$ satisfying ($\clubsuit$) and $x \in U(\mathfrak{g})$. We show that

$$(x + I_\ell)(y + I_\ell) \in Q_\ell.$$

Since I_ℓ is a left $U(\mathfrak{g})$-module

$$(x + I_\ell)(y + I_\ell) = xy + xI_\ell + I_\ell y + I_\ell = xy + I_\ell y + I_\ell.$$

By Equation (5.0.1), we get

$$xy + I_\ell y + I_\ell = xy + I_\ell,$$

because y satisfies ($\clubsuit$).
Hence, $(x + I_\ell)(y + I_\ell) \in Q_\ell$ for every $x, y \in U(\mathfrak{g})$, such that $yz - zy \in I_\ell$, for any $z \in \mathfrak{m}_\ell$.
It is straightforward to show that the left action of $U(\mathfrak{g})$ and the right action of H_ℓ are compatible.

REMARK 5.0.4. Notice that

$$(x-\chi(x))y=[x,y]+y(x-\chi(x))=[x,y]+I_\ell, \tag{$\spadesuit$}$$

for every $x\in\mathfrak{m}_\ell$ and $y\in U(\mathfrak{g})$.

In the following we require that ℓ is a Lagrangian subspace of $\mathfrak{g}(-1)$, that is $\ell=\ell^\perp$ so that $\mathfrak{n}_\ell=\mathfrak{m}_\ell$.
Let e, $\mathfrak{n}_\ell=\mathfrak{m}_\ell$ and χ be as above.

From now on $\mathcal{M}$ will denote the category of $U(\mathfrak{g})$-modules on which $x-\chi(x)$ acts locally nilpotently for each $x\in\mathfrak{m}_\ell$. It is called the category of Whittaker modules.
Also, from now on $\mathcal{N}$ will denote the category of finitely-generated H_ℓ-modules. When the good grading for $\mathfrak{g}$ is as in Example 5.0.1, an equivalence between $\mathcal{M}$ and $\mathcal{N}$ was described by Skryabin in [58, Appendix, Theorem 1]. Moreover, under the same assumption, Gan and Ginzburg gave an alternative proof of Skryabin equivalence in [25, Theorem 6.1].
Goodwin in [28, Theorem 3.14] showed that the same equivalence holds also when the grading of $\mathfrak{g}$ is a general good grading. Before exhibiting this equivalence, we put for $M\in\mathcal{M}$

$$\mathrm{Wh}(M):=\{v\in M\,|\,x.v=\chi(x)v\ \text{ for all}\,x\in\mathfrak{m}_\ell\}.$$

REMARK 5.0.5. For $M\in\mathcal{M}$, the subspace $\mathrm{Wh}(M)$ is an H_ℓ-module via the action:

$$(x+I_\ell).m=x.m,$$

for every $m\in\mathrm{Wh}(M)$, $x\in U(\mathfrak{g})$ satisfying ($\clubsuit$).
We show that this is an action. We have to verify that $x.m\in\mathrm{Wh}(M)$, that is $z.(x.m)=\chi(z)x.m$, for every $m\in\mathrm{Wh}(M)$, $z\in\mathfrak{m}_\ell$ and x as above. We can express $z.(x.m)$ in the following way

$$z.(x.m)=(zx).m=[z,x].m+x.(z.m)$$

for every $m\in\mathrm{Wh}(M)$, $z\in\mathfrak{m}_\ell$ and $x\in U(\mathfrak{g})$ satisfying ($\clubsuit$).
Since $[z,x]\in I_\ell$, there exists $u\in U(\mathfrak{g})$ and $w\in\mathfrak{m}_\ell$ such that
$[z,x]=u(w-\chi(w))$, for every $z\in\mathfrak{m}_\ell$ and $x\in U(\mathfrak{g})$ satisfying ($\clubsuit$). Then

$$[z,x].m=(u(w-\chi(w))).m=u.(\chi(w)m-\chi(w)m)=0,$$

for every $m\in\mathrm{Wh}(M)$, $z\in\mathfrak{m}_\ell$ and $x\in U(\mathfrak{g})$ as above. Moreover, since $m\in\mathrm{Wh}(M)$, then $z.m=\chi(z)m$, for every $z\in\mathfrak{m}_\ell$. We can conclude that

$$z.(x.m)=[z,x].m+x.(z.m)=0+x.\chi(z)m,$$

and in particular that $x.m\in\mathrm{Wh}(M)$, for any $m\in\mathrm{Wh}(M)$ and any $x\in U(\mathfrak{g})$ satisfying ($\clubsuit$).

Then, with the usual restriction of morphisms, Wh defines a functor from the category of Whittaker modules $\mathcal{M}$ to the category of finitely generated H_ℓ -modules.
By Remark 5.0.3, we also have a functor

$$Q_\ell \otimes_{H_\ell} - \colon \mathcal{N} \to U(\mathfrak{g})\text{-mod}.$$

Remark 5.0.6. We show that $Q_\ell \otimes_{H_\ell} N$ with $U(\mathfrak{g})$-action by left multiplication is a Whittaker module for every $N \in \mathcal{N}$. Explicitly, we verify that for all $x \in \mathfrak{m}_\ell$ there exists $k \in \mathbb{N}$ such that

$$(x-\chi(x))^k.((y+I_\ell)\otimes_{H_\ell} n) = 0,$$

for all $n \in N$ and $y \in U(\mathfrak{g})$. For simplicity, set $\mathfrak{g}(<j) := \bigoplus_{i<j}\mathfrak{g}(i)$.
We divide this verification into three steps.
Step 1. We first prove the claim for $y + I_\ell \in Q_\ell$, with $y \in \mathfrak{g}(j)$ for $j \in \mathbb{N}$. For every $x \in \mathfrak{m}_\ell$, by (♠) we get

$$(x-\chi(x))((y+I_\ell)\otimes_{H_\ell} N) \subseteq (\mathfrak{g}(<j)+I_\ell)\otimes_{H_\ell} N.$$

Since $\mathfrak{g}$ is finite-dimensional, then for $k >> 0$,
$(x-\chi(x))^k.((\mathfrak{g}(j)+I_\ell)\otimes_{H_\ell} N) = 0$.

Step 2. We consider now an element $y + I_\ell \in Q_\ell$, where $y = y_1 \dots y_l$, with $y_i \in \mathfrak{g}(j_i)$ for $j_i \in \mathbb{N}$ and for $i \in \{1, \dots l\}$. Then for every $x \in \mathfrak{m}_\ell$ we have

$$\begin{aligned}(x-\chi(x))(y_1\dots y_l + I_\ell) &= [x,y_1]y_2\dots y_l + y_1(x-\chi(x))y_2\dots y_l + I_\ell\\ &= \sum_{i=1}^{l} y_1\dots[x,y_i]y_{i+1}\dots y_l + I_\ell.\end{aligned}$$

So for every $x \in \mathfrak{m}_\ell$

$$(x-\chi(x))\left(\left(\prod_{i=1}^{l}\mathfrak{g}(j_i)+I_\ell\right)\otimes_{H_\ell} N\right) \subseteq \sum_{i=1}^{l}\left(\prod_{i=1}^{l}\mathfrak{g}(j_1)\dots\mathfrak{g}(<j_i)\dots\mathfrak{g}(j_l)+I_\ell\right)\otimes_{H_\ell} N,$$

where the product in $U(\mathfrak{g})$ is taken in increasing order.
Since $\mathfrak{g}$ is finite dimensional, then there exists $k \in \mathbb{N}$ such that

$$(x-\chi(x))^k\left(\left(\prod_{i=1}^{l} g(j_i)+I_\ell\right)\otimes_{H_\ell} N\right) = 0.$$

Step 3. We finally consider an element $y + I_\ell \in Q_\ell$, for $y \in U(\mathfrak{g})$. Then, y is a finite sum of elements in $\prod_{i=1}^{l_h}\mathfrak{g}(j_i)$, for $l_h, j_i, h \in \mathbb{N}$. By the previous step, for each summand there exists $k_h \in \mathbb{N}$ such that

$$(x-\chi(x))^{k_h}\left(\prod_{i=1}^{l_h}\mathfrak{g}(j_i)+I_\ell\right)\otimes_{H_\ell} N = 0$$

. Then, taking the maximum among the k_h's we conclude the verification.

We are now in a position to state the following theorem.

THEOREM 5.0.7. *[28, Theorem 3.14] Let $M \in \mathcal{M}$ and $N \in \mathcal{N}$. The functors $M \mapsto Wh(M)$ and $N \mapsto Q_\ell \otimes_{H_\ell} N$ are quasi inverse equivalences between the category of Whittaker modules $\mathcal{M}$ and the category of finitely-generated H_ℓ-modules $\mathcal{N}$.*

REMARK 5.0.8. The natural isomorphism $\varepsilon\colon Q_\ell \otimes_{H_\ell} \mathrm{Wh} \to \mathrm{id}$ is given by

$$\begin{aligned} \varepsilon_M\colon Q_\ell \otimes_{H_\ell} \mathrm{Wh}(M) &\to M \\ (u + I_\ell) \otimes m &\mapsto u.m \end{aligned} \tag{5.0.2}$$

for $M \in \mathcal{M}$ ([28, Theorem 3.14]).

CHAPTER 6

Whittaker modules and H_ℓ-modules as bimodule categories

We retain notation from Chapter 5 and we assume that ℓ is Lagrangian. This chapter aims at endowing the category of H_ℓ-modules with a bimodule structure over a category containing $U(\mathfrak{g})\text{-mod}_{\text{fin}}$. For this purpose, we firstly endow the category of Whittaker modules with a bimodule structure. Then, by means of Skryabin equivalence we will transport this structure to the category of H_ℓ-modules.

Since $U(\mathfrak{g})$ is a Hopf algebra, the category $U(\mathfrak{g})$-mod of $U(\mathfrak{g})$-modules is a monoidal category by Example 4.1.2.
We denote by $\mathcal{C}_e$ the subcategory of $U(\mathfrak{g})$-mod on which $\mathfrak{m}_\ell$ acts locally nilpotently.

Remark 6.0.1. We show that $\mathcal{C}_e$ contains the category $U(\mathfrak{g})\text{-mod}_{\text{fin}}$. Firstly, consider a good grading $\mathfrak{g} = \bigoplus_{i\in\mathbb{Z}} \mathfrak{g}(i)$ for $e \in \mathfrak{g}$. By Remark 5.0.1, it is induced by the adjoint action of a semisimple element q.
Let V be a finite-dimensional $U(\mathfrak{g})$-module. In light of [32, Theorem 6.4], the module V decomposes as

$$V = \bigoplus_{j\in J} V_j,$$

where $V_j := \{v \in V \mid q.v = jv\}$ and $J \subseteq \mathbb{Z}$ is such that $|J| < \infty$.
We need to understand how $\mathfrak{m}_\ell$ acts on each block V_j. Pick an homogeneous element x in $\in \mathfrak{m}_\ell$, say $x \in \mathfrak{g}(i)$ for $i \leq -1$ and let $v \in V_j$ for some j. Then:

$$q.(x.v) = (qx).v = [q, x].v + xq.v = ix.v + jx.v = (i + j)x.v,$$

i.e. $x.v \in V_{i+j}$. Since $i \leq -1$ and $|J| < \infty$, there exists $n_v \in \mathbb{N}$ such that $x^{n_v}.v = 0$ for every $v \in V$ and any homogeneous element x in $\mathfrak{m}_\ell$. Extending the above argument by linearity, the same conclusion holds for every $x \in \mathfrak{m}_\ell$ and thus $\mathfrak{m}_\ell$ acts locally nilpotently on V.

We will firstly show that $\mathcal{C}_e$ is a monoidal category. For this purpose, we need the following result.

LEMMA 6.0.2. *Let $\psi\colon \mathfrak{g} \to \mathbb{C}$ be a linear form. Let X, Z be in $U(\mathfrak{g})$-mod. Then,*

$$(y-\psi(y))^k.(\sum_{i=1}^{I}\sum_{j=1}^{J}\alpha_{i,j}x_i\otimes z_j) = \sum_{i=1}^{I}\sum_{j=1}^{J}\sum_{u=0}^{k}\alpha_{i,j}(y-\psi(y))^u.x_i\otimes y^{k-u}.z_j, \quad (6.0.1)$$

for every $y\in\mathfrak{m}_\ell, x_i\in X, z_j\in Z$, $k\in\mathbb{N}$ and $\alpha_{i,j}\in\mathbb{C}$.

PROOF. First of all, we prove that the equation

$$(y-\psi(y))^k.(x\otimes z) = \sum_{j=0}^{k}\binom{k}{j}(y-\psi(y))^j.x\otimes y^{k-j}.z, \quad (6.0.2)$$

holds for every $y\in\mathfrak{m}_\ell, x\in X$ and $z\in Z$. We proceed by induction on k.
If $k=1$, the above equation is clearly satisfied.
Suppose that for some $k\geq 2$,

$$(y-\psi(y))^k.(x\otimes y) = \sum_{j=0}^{k}\binom{k}{j}(y-\psi(y))^j.x\otimes y^{k-j}.z.$$

By definition of the action:

$$\begin{aligned}(y-\psi(y))^{k+1}.(x\otimes z) &= (y-\psi(y)).\Big((y-\psi(y))^k.(x\otimes z)\Big) = \\ &= (y-\psi(y)).\Big(\sum_{j=0}^{k}\binom{k}{j}(y-\psi(y))^j.x\otimes y^{k-j}.z\Big) = \\ &= \sum_{j=0}^{k}\binom{k}{j}(y-\psi(y))^{j+1}.x\otimes y^{k-j}.z + \\ &+ \sum_{j=0}^{k}\binom{k}{j}(y-\psi(y))^j.x\otimes y^{k+1-j}.z.\end{aligned}$$

Reordering the sum and rescaling the indices the above term equals

$$\begin{aligned}&(y-\psi(y))^{k+1}.x\otimes z + \sum_{j=1}^{k}\binom{k}{j-1}(y-\psi(y))^j.x\otimes y^{k+1-j}.z + \\ &+ \sum_{j=1}^{k}\binom{k}{j}(y-\psi(y))^j.x\otimes y^{k+1-j}.z + x\otimes y^{k+1}.z \\ &= (y-\psi(y))^{k+1}.x\otimes z + x\otimes y^{k+1}.z + \sum_{j=1}^{k}\binom{k+1}{j}(y-\psi(y))^j.x\otimes y^{k+1-j}.z = \\ &\sum_{j=0}^{k+1}\binom{k+1}{j}(y-\psi(y))^j.x\otimes y^{k+1-j}.z.\end{aligned}$$

Hence, Equation (6.0.2) holds for every $y\in\mathfrak{m}_\ell, x\in X$ and $z\in Z$.
Finally, the linearity of the action gives Equation (6.0.1). □

We are now in a position to prove the following.

LEMMA 6.0.3. *The category $\mathcal{C}_e$ endowed with the usual tensor product of modules is a monoidal category.*

PROOF. Since $U(\mathfrak{g})$-mod is monoidal, it is enough to verify that $\mathcal{C}_e$ is closed under the tensor product, i.e. for $X, Z \in \mathcal{C}_e$, we have to show that $\mathfrak{m}_\ell$ acts locally nilpotently on $X \otimes_{\mathbb{C}} Z$. A generic element of $X \otimes Z$ is of the form

$$\sum_{i=1}^{I}\sum_{j=1}^{J}\alpha_{i,j}x_i \otimes z_j,$$

for some $\alpha_{i,j} \in \mathbb{C}$, $x_i \in X$ and $z_j \in Z$. Let $y \in \mathfrak{m}_\ell$. Substituting $\psi = 0$ in Equation (6.0.1), we have

$$y^k.\Big(\sum_{i=1}^{I}\sum_{j=1}^{J}\alpha_{i,j}x_i \otimes z_j\Big) = \sum_{i=1}^{I}\sum_{j=1}^{J}\sum_{u=0}^{k}\alpha_{i,j}y^u.x_i \otimes y^{k-u}.z_j.$$

Since $\mathfrak{m}_\ell$ acts locally nilpotently on X and Z, there exists a sufficient large $k \in \mathbb{N}$, such that one between $y^u.x_i$ and $y^{k-u}.z_j$ vanishes for any $u \in \{0, \dots, k\}$ and any i, j, concluding the proof. □

Recall that $\mathcal{M}$ stands for the category of Whittaker modules, that is the subcategory of $U(\mathfrak{g})$-mod on which $x - \chi(x)$ acts locally nilpotently for each $x \in \mathfrak{m}_\ell$.

REMARK 6.0.4. The category $\mathcal{M}$ does not contain finite-dimensional $U(\mathfrak{g})$-modules if $e \neq 0$. Indeed, let V be a finite-dimensional $U(\mathfrak{g})$-module and suppose that $(x - \chi(x))$ acts locally nilpotently on V for every $x \in \mathfrak{m}_\ell$. This assumption together with Remark 6.0.1 and with the fact that the elements x and $x - \chi(x)$ commute for every $x \in \mathfrak{m}_\ell$ imply that $x - (x - \chi(x)) = \chi(x)$ acts locally nilpotently on V. This condition holds if and only if $\chi(x) = 0$ for every $x \in \mathfrak{m}_\ell$; this would contradict that $(\cdot|\cdot)$ is non degenerate and $\mathfrak{g}(-2) \subseteq \mathfrak{m}_\ell$.

We now define natural left and right actions of $\mathcal{C}_e$ on $U(\mathfrak{g})$-mod by means of the tensor product of modules $\otimes_{\mathbb{C}}$ in $U(\mathfrak{g})$-mod. We set:

$$\begin{aligned} \otimes_{\mathcal{M}} := \otimes_{\mathbb{C}} \colon \mathcal{C}_e \times \mathcal{M} &\to U(\mathfrak{g}) - \mathrm{mod} \\ (-, \sim) &\mapsto - \otimes_{\mathbb{C}} \sim, \end{aligned} \tag{6.0.3}$$

and

$$\begin{aligned} \otimes^{\mathcal{M}} := \otimes_{\mathbb{C}} \colon \mathcal{M} \times \mathcal{C}_e &\to U(\mathfrak{g}) - \mathrm{mod} \\ (-, \sim) &\mapsto - \otimes_{\mathbb{C}} \sim . \end{aligned} \tag{6.0.4}$$

From now on, we will write simply $\otimes$ to denote $\otimes_{\mathbb{C}}$.
We have the following result:

LEMMA 6.0.5. *The category* $\mathcal{M}$ *is a* $(\mathcal{C}_e, \mathcal{C}_e)$*-bimodule category, via the tensor product of* $U(\mathfrak{g})$*-modules, where* $m_{X,Y,Z}, m^r_{X,Y,Z}$ *and* $b_{X,M,Y}$ *are the shift of parentheses.*

PROOF. Firstly, we verify that that $M \otimes X$ is a Whittaker module for every Whittaker module M and for every $U(\mathfrak{g})$-module X on which $\mathfrak{m}_\ell$ acts locally nilpotently, that is we have to show that $y - \chi(y)$ acts locally nilpotently on $M \otimes X$, for every $M \in \mathcal{M}, X \in \mathcal{C}_e$ and $y \in \mathfrak{m}_\ell$. This is equivalent to show that for every $z \in M \otimes X$, there exists $k_z \in \mathbb{N}$ such that $(y - \chi(y))^{k_z}.z = 0$ for every $y \in \mathfrak{m}_\ell$. A generic element z in $M \otimes X$ is of the form

$$\sum_{i=1}^{I} \sum_{j=1}^{J} \alpha_{i,j} m_i \otimes x_j,$$

for some $\alpha_{i,j} \in \mathbb{C}$, $x_j \in X$ and $m_i \in M$. Then, our goal is to show that there exists $k_z \in \mathbb{N}$ such that

$$(y - \chi(y))^{k_z}.\Big(\sum_{i=1}^{I} \sum_{j=1}^{J} \alpha_{i,j} m_i \otimes x_j\Big) = 0,$$

for every $y \in \mathfrak{m}_\ell$ and for $\alpha_{i,j}, m_i$ and x_j as above.
Applying Equation (6.0.1), we get:

$$(y - \chi(y))^k.z = \sum_{i=1}^{I} \sum_{j=1}^{J} \sum_{u=0}^{k} \alpha_{i,j} (y - \chi(y))^u.m_i \otimes y^{k-u}.x_j$$

for $m_i \in M, x_j \in X$ and $\alpha_{i,j} \in \mathbb{C}$ as above and for every $y \in \mathfrak{m}_\ell$. Since M is a Whittaker module and X is a $U(\mathfrak{g})$-module on which $\mathfrak{m}_\ell$ acts locally nilpotently, there exists a sufficient large K_z, such that one between $(y - \chi(y))^u.m_i$ and $y^{K_z - u}.x_j$ vanishes for any $u \in \{0, \dots, K_z\}$ and any i, j.
The proof for the right action is analogous.

Secondly, we have to verify that $\mathcal{M}$ is both a left and a right $\mathcal{C}_e$-module category. Since $m = m^r$ and the associativity constraint of the monoidal category $\mathcal{C}_e$ is identified with the identity as it happens for $U(\mathfrak{g})$-mod (Lemma 6.0.3), the pentagon diagrams reduce to the trivial ones.
For similar reasons, diagrams (4.1.5) and (4.1.6), become the trivial ones. Hence, we conclude that $\mathcal{M}$ is a $(\mathcal{C}_e, \mathcal{C}_e)$-bimodule category. $\square$

Now, our aim is to transpose the $(\mathcal{C}_e, \mathcal{C}_e)$-bimodule structure of $\mathcal{M}$ to $\mathcal{N}$ by means of Skryabin equivalence, following the construction of Chapter 4.
We define the right translation functor and the left translation functor as those given in Definition 4.2.1 and Definition 4.2.10, specializing F to Wh and G to $Q_\ell \otimes_{H_\ell}$.

More precisely, the definition of the right translation functor becomes:

$$\begin{aligned} \otimes^{\mathcal{N}} := \circledast^r \colon \mathcal{N} \times \mathcal{C}_e &\to \mathcal{N} \\ (-, \sim) &\mapsto \mathrm{Wh}((Q_\ell \otimes_{H_\ell} -) \otimes \sim), \end{aligned} \tag{6.0.5}$$

while the left translation functor reads as

$$\begin{aligned} \otimes_{\mathcal{N}} := \circledast \colon \mathcal{C}_e \times \mathcal{N} &\to \mathcal{N} \\ (-, \sim) &\mapsto \mathrm{Wh}(- \otimes (Q_\ell \otimes_{H_\ell} \sim)). \end{aligned} \tag{6.0.6}$$

Moreover, substituting $m = m^r = \mathrm{id}$ and $F = \mathrm{Wh}(-), G = Q_\ell \otimes_{H_\ell} -$ in equations (4.2.2) and (4.2.11), we get, respectively, the left and the right module associativity constraints $n_{X,Y,N}$ and $n^r_{X,Y,N}$, for all $X, Y \in \mathcal{C}_e$ and $N \in \mathcal{N}$.
In particular, for $X, Y \in \mathcal{C}_e$ and $M \in \mathcal{M}$, the module associativity constraint

$$n^r_{X,Y,N} \colon \mathrm{Wh}((Q_\ell \otimes_{H_\ell} (\mathrm{Wh}((Q_\ell \otimes_{H_\ell} M) \otimes X)) \otimes Y) \to \mathrm{Wh}((Q_\ell \otimes_{H_\ell} M) \otimes (X \otimes Y))$$

is the restriction of the following map

$$\begin{aligned} \varphi \colon (Q_\ell \otimes_{H_\ell} (\mathrm{Wh}((Q_\ell \otimes_{H_\ell} M) \otimes X)) \otimes Y &\to (Q_\ell \otimes_{H_\ell} M) \otimes (X \otimes Y) \\ ((u + I_\ell)(((u' + I_\ell) \otimes m) \otimes x)) \otimes y &\mapsto u(((u' + I_\ell) \otimes m) \otimes x) \otimes y. \end{aligned} \tag{6.0.7}$$

REMARK 6.0.6. Let $U(\mathfrak{g})\text{-mod}_{\mathrm{fin}}$ be the category of finite-dimensional $U(\mathfrak{g})$-modules. Then, $U(\mathfrak{g})\text{-mod}_{\mathrm{fin}}$ is a subcategory of $\mathcal{C}_e$, which is closed under the tensor product. Hence, $U(\mathfrak{g})\text{-mod}_{\mathrm{fin}}$ is a monoidal category.
If we restrict the definitions of the right translations functor (6.0.5) and of the module associativity constraint n^r to $U(\mathfrak{g})\text{-mod}_{\mathrm{fin}}$, we get the definition for the translation functors given in [28] and [9].

Furthermore, let $p_{X,N,Z}$ be the compatibility isomorphisms defined as in (4.2.12).
By Lemma 4.2.6, we deduce the following:

THEOREM 6.0.7. *The category* $\mathcal{N}$ *endowed with* $\circledast$, $n_{X,Y,N}$, $\circledast^r$, $n^r_{X,Y,N}$ *and* $p_{X,N,Z}$ *defined above, is a* $(\mathcal{C}_e, \mathcal{C}_e)$*-bimodule category.*

Moreover, by Lemma 4.2.3 we obtain the following.

LEMMA 6.0.8. *Let* ε *be the natural isomorphism* (5.0.2)*, let* $s_{X,M} := Wh(id_X \otimes \varepsilon_M^{-1})$ *and* $t_{X,N} := \varepsilon_{X \otimes (Q_\ell \otimes_{H_\ell} N)}$*, for all* $X \in \mathcal{C}_e, M \in \mathcal{M}$ *and* $N \in \mathcal{N}$*. Then, the pairs* (Wh, s) *and* $(Q_\ell \otimes_{H_\ell}, t)$ *are* $\mathcal{C}_e$*-module functors.*

CHAPTER 7

$\mathcal{C}$-equivariant functors for reduction in stages

In this chapter, we recall the functors Wh_0 and $Q_0 \otimes_{H_0}$ introduced in [26] and we show that they are equivariant under an action of a subcategory of $U(\mathfrak{g})$-mod.

Let $\mathfrak{g}$ be a finite-dimensional simple Lie algebra over $\mathbb{C}$.
For $i = 1, 2$, let $e_i \in \mathfrak{g}$ be nilpotent elements and let χ_i be the associated linear forms constructed as in Chapter 5. For $i = 1, 2$, we denote by (e_i, f_i, h_i) an $\mathfrak{sl}_2$-triple in which e_i is embedded.
We adopt notations from Chapter 5 adding a subscript $_{(i)}$ for referring to the construction related to e_i.
For $i = 1, 2$, let $\mathfrak{g} = \bigoplus_{j\in\mathbb{Z}} \mathfrak{g}(j)_{(i)}$ be a good grading for e_i. By Remark 5.0.1 the good grading $_{(i)}$ is induced by the adjoint action of a semisimple element q_i. Without loss of generality, we can assume that q_1 and q_2 belong to the same Cartan algebra $\mathfrak{h}$. This follows from the fact that all Cartan subalgebras are conjugate under inner automorphisms of the algebra $U(\mathfrak{g})$ and that $H_{\ell_{(i)}}$ depends only on the orbit of e_i for the action of inner automorphisms of $U(\mathfrak{g})$.
Throughout this chapter, we will make the following assumptions:

(1) there is a direct sum decomposition $\mathfrak{m}_{\ell_{(2)}} = \mathfrak{m}_{\ell_{(1)}} \oplus \mathfrak{m}_0$, where $\mathfrak{m}_0$ is a $\mathfrak{h}$-stable Lie subalgebra of $\mathfrak{m}_{\ell_{(2)}}$ and $\mathfrak{m}_{\ell_{(1)}}$ is a Lie ideal of $\mathfrak{m}_{\ell_{(2)}}$,
(2) the element $e_0 := e_2 - e_1$ is nilpotent and e_0 and the Lie algebra $\mathfrak{m}_0$ are contained in $\mathfrak{g}(0)_{(1)}$,
(3) the semisimple element $q_0 := q_2 - q_1$ commutes with e_1.

For simplicity, we denote the above assumptions with $(\diamondsuit)$.

REMARK 7.0.1. Consider the simple Lie algebra

$$\mathfrak{so}_5 := \{x \in \mathfrak{sl}_5 \,|\, x^{\mathrm{T}}K + Kx = 0\}, \text{ for } K := \begin{pmatrix} 0&0&0&0&1\\ 0&0&0&1&0\\ 0&0&1&0&0\\ 0&1&0&0&0\\ 1&0&0&0&0 \end{pmatrix},$$

where x^{T} denotes the transpose of x. We take the symmetric set

$$I_5 := \{-2, -1, 0, 1, 2\}$$

as indexation for the canonical basis of $\mathbb{C}^5$, with the following order

$$v_{-2} = (1, 0, 0, 0, 0),\ v_{-1} = (0, 1, 0, 0, 0),\ \dots, v_2 = (0, 0, 0, 0, 1).$$

We change the numbering of the elementary matrices $e_{i,j}$ to have $i, j \in I_5$ and to respect the order we have chosen for the basis.
Take the regular nilpotent element

$$e_2 := e_{1,0} + e_{2,1} - e_{0,-1} - e_{-1,-2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

We can embed e_2 in a $\mathfrak{sl}_2$-triple $\{e_2, f_2, h_2\}$, where $h_2 := \mathrm{diag}(-4, -2, 0, 2, 4)$ and $f_2 = \begin{pmatrix} 0 & -4 & 0 & 0 & 0 \\ 0 & 0 & -6 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. We consider the Dynkin grading, i.e. the grading induced by h_2.
Take now

$$e_1 := e_{1,0} - e_{0,-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We embed it in a $\mathfrak{sl}_2$ triple $\{e_1, f_1, h_1\}$, where $h_1 = \mathrm{diag}(0, -2, 0, 2, 0)$ and $f_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. Also in this case, we consider the grading induced by the semisimple element h_1. We show that this choice of the gradings does not satisfy the assumptions ($\diamondsuit$). By definition,

$$e_0 = e_2 - e_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Now, h_1 acts on e_0 by means of the adjoint action, in particular

$$[h_1, e_0] = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 \end{pmatrix} = 2e_0.$$

This means that $e_0 \notin \mathfrak{g}(0)_{(1)}$ and hence assumption 2) of ($\diamondsuit$) is not satisfied. If we consider the good grading induced by $q_1 = \mathrm{diag}(-2, -2, 0, 2, 2)$ instead of the Dynkin one, the assumptions are satisfied (see [26, Subsection 4.2]). In this case,

$$\mathfrak{m}_{\ell_{(2)}} = \mathrm{Span}\{e_{i,j} \,|\, i < j\} \cap \mathfrak{so}_5 \qquad \mathfrak{m}_{\ell_{(1)}} = \mathrm{Span}\{e_{i,j} \,|\, i < j \,\text{and}\, i < 1\,,\, j > -1\} \cap \mathfrak{so}_5$$

and in consequence one may take

$$\mathfrak{m}_0 = \mathrm{Span}\{e_{-2,1}, e_{1,2}\} \cap \mathfrak{so}_5.$$

This example justifies the fact that we are considering general good gradings and not only the Dynkin ones.

We stress that throughout this chapter the assumptions ($\diamondsuit$) are satisfied.

We now recall the functors Wh_0 and $Q_0 \otimes_{H_0} -$ from [26]. For this purpose, we recollect some results contained therein.
By [26, Lemma 3.2.1], there is an embedding of $\mathfrak{m}_0$ in $H_{\ell_{(1)}}$, which sends

$y \in \mathfrak{m}_0$ to $y + I_{\ell_{(1)}}$. In consequence, we can define I_0 as the left $H_{\ell_{(1)}}$-ideal spanned by $(y - \chi_2(y)) + I_{\ell_{(1)}}$, $y \in \mathfrak{m}_0$.
Let $Q_0 := H_{\ell_{(1)}}/I_0$. The adjoint action of $\mathfrak{m}_0$ on $H_{\ell_{(1)}}$ descends to Q_0. Then, it makes sense to consider the subspace of invariants $H_0 := Q_0^{\mathrm{ad}(\mathfrak{m}_0)}$. This vector space turns out to be an algebra (see [26, Lemma 3.2.2]), where the multiplication is induced by the one in $H_{\ell_{(1)}}$.
Moreover, in virtue of [26, Theorem 3.2.3], H_0 is isomorphic to $H_{\ell_{(2)}}$.

For $i = 1, 2$, let $\mathcal{C}_i$ be the category of $U(\mathfrak{g})$-modules on which $\mathfrak{m}_{\ell_{(i)}}$ acts locally nilpotently. The category $\mathcal{C}_2$ is a subcategory of $\mathcal{C}_1$ because by assumptions $\mathfrak{m}_{\ell_{(1)}} \subseteq \mathfrak{m}_{\ell_{(2)}}$.
For $i = 1, 2$, we denote with $\mathcal{M}_i$ the category of Whittaker modules with respect to e_i; with $\mathcal{N}_i$ the category of $H_{\ell_{(i)}}$-modules; with $\circledast_{(i)}$ the translation functor and with Wh_i the functor Wh from Chapter 5 defined on $\mathcal{M}_i$.

REMARK 7.0.2. As shown in Chapter 6, the category $\mathcal{M}_i$ is a $(\mathcal{C}_i, \mathcal{C}_i)$-bimodule category. Since $\mathcal{C}_2 \subseteq \mathcal{C}_1$, the category $\mathcal{M}_1$ is also a $(\mathcal{C}_2, \mathcal{C}_2)$-bimodule category. In addition, $\mathcal{M}_2$ is a $(\mathcal{C}_2, \mathcal{C}_2)$-bimodule subcategory of $\mathcal{M}_1$.

Finally, by the embedding of $\mathfrak{m}_0$ in $H_{\ell_{(1)}}$, we can define the category $\mathcal{M}_0$, that is the category of finitely generated $H_{\ell_{(1)}}$-modules on which $y - \chi_2(y)$ acts locally nilpotently, for all $y \in \mathfrak{m}_0$. For $M \in \mathcal{M}_0$, we set

$$\mathrm{Wh}_0(M) := \{m \in M \mid y.m = \chi_2(y)m \text{ for all } y \in \mathfrak{m}_0\}.$$

Before stating the main result of this chapter, we need to recall some facts.

i) By [26, Lemma 5.2.1], for every $M \in \mathcal{M}_0$, the subspace $\mathrm{Wh}_0(M)$ is a left H_0-module with action given by

$$(x + I_0).m = x.m,$$

for every $x + I_0 \in H_0$ and $m \in \mathrm{Wh}_0(M)$. As we recalled before, $H_0 \simeq H_{\ell_{(2)}}$ and hence $\mathrm{Wh}_0(M)$ is a left $H_{\ell_{(2)}}$-module, for every $M \in \mathcal{M}_0$. This implies that, together with restriction on morphisms, Wh_0 gives a functor from the category $\mathcal{M}_0$ to the category $\mathcal{N}_2$.

ii) By [26, Lemma 5.2.2], we have that Q_0 is a $H_{\ell_{(1)}}$-H_0-bimodule, where $H_{\ell_{(1)}}$ acts on Q_0 via left multiplication, while H_0 acts on Q_0 via right multiplication. In consequence, for $N \in \mathcal{N}_2$ the $H_{\ell_{(1)}}$-module $Q_0 \otimes_{H_0} N$ is well defined. The action is given by:

$$(x).((y + I_0) \otimes_{H_0} n) = (xy + I_0) \otimes_{H_0} n,$$

for every $n \in N$ and $x, y \in H_{\ell_{(1)}}$. Furthermore, in virtue of [26, Lemma 5.2.2], the tensor product $Q_0 \otimes_{H_0} N$ lies in $\mathcal{M}_0$ for all $N \in \mathcal{N}_2$.

We are now in a position to state the following.

THEOREM 7.0.3. *[26, Theorem 5.2.3] Let $M \in \mathcal{M}_0$, $N \in \mathcal{N}_2$. Then the functors $M \mapsto Wh_0(M)$ and $N \mapsto Q_0 \otimes_{H_0} N$ are quasi inverse equivalences. Moreover, $Wh_1(-)$ and $Q_{\ell_{(1)}} \otimes_{H_{\ell_{(1)}}} (-)$ induce an equivalence of categories $\mathcal{M}_1 \simeq \mathcal{M}_0$ by restriction and we have $Wh_2 = Wh_0 \circ Wh_1$. In particular, Wh_0 and $Q_0 \otimes_{H_0}$ are exact functors.*

REMARK 7.0.4. By [26, Proposition 5.3.1], the natural isomorphism

$$\mathrm{Wh}_0(Q_0 \otimes_{H_0}) \overset{\varepsilon_0}{\simeq} \mathrm{id}$$

is given by

$$\begin{aligned} (\varepsilon_M^{(0)})^{-1} \colon M &\to \mathrm{Wh}_0(Q_0 \otimes_{H_0} M) \\ m &\mapsto 1 \otimes m, \end{aligned} \tag{7.0.1}$$

for any $M \in \mathcal{M}_0$.

Our final goal is to show that the equivalence just introduced is invariant under the action of the category $\mathcal{C}_2$ and thus also of $U(\mathfrak{g})$-mod$_{\mathrm{fin}}$. To this aim, we firstly need to understand the $\mathcal{C}_2$-module structure of $\mathcal{M}_0$.

LEMMA 7.0.5. *The category $\mathcal{M}_0$ is a $(\mathcal{C}_2, \mathcal{C}_2)$-bimodule category, where the left action bifunctor $\otimes_{\mathcal{M}_0}$ is $\circledast_{(1)\,|_{\mathcal{M}_0}}$, while the right one is $\circledast_{(1)}{}^{r}_{|_{\mathcal{M}_0}}$.*

PROOF. Firstly, recall that $\mathcal{M}_2$ is a $(\mathcal{C}_2, \mathcal{C}_2)$-bimodule category as we observed in Remark 7.0.2.
By Theorem 7.0.3, the functor Wh_1 establishes an equivalence between the categories $\mathcal{M}_2$ and $\mathcal{M}_0$. Hence, by transport of structure, we can endow $\mathcal{M}_0$ with a $\mathcal{C}_2$-module structure following the construction of Chapter 6. In particular, this implies that the left action bifunctor is the restriction to $\mathcal{M}_0$ of $\circledast_{(1)}$, while the right one is the restriction to $\mathcal{M}_0$ of $\circledast^r_{(1)}$. □

The previous lemma together with Lemma 4.2.3 gives the following corollary.

COROLLARY 7.0.6. *The functor $Wh_1|_{\mathcal{M}_2}$ paired with the natural isomorphism $Wh_1|_{\mathcal{M}_2}(\mathrm{id} \otimes \varepsilon^{(1)^{-1}})$ is a $\mathcal{C}_2$-module functor, where $\varepsilon^{(1)}$ is the natural isomorphism defined in Equation* (5.0.2).

Now, we define the following natural isomorphisms

$$u_{X,N_2} \colon \mathrm{Wh}_1 \circ (Q_{\ell_{(2)}} \otimes_{H_{\ell_{(2)}}} (X \circledast_{(2)} N_2)) \to X \circledast_{(1)} \mathrm{Wh}_1 \circ (Q_{\ell_{(2)}} \otimes_{H_{\ell_{(2)}}} N_2)$$

as

$$u_{X,N_2} := \mathrm{Wh}_1\Big((\mathrm{id}_X \otimes \varepsilon^{(1)^{-1}}_{Q_{\ell_{(2)}} \otimes_{H_{\ell_{(2)}}} N_2}) \circ \varepsilon^{(2)}_{X \otimes (Q_{\ell_{(2)}} \otimes_{H_{\ell_{(2)}}} N_2)}\Big) \tag{7.0.2}$$

and

$$v_{X,M_0} \colon \mathrm{Wh}_2 \circ (Q_{\ell_{(1)}} \otimes_{H_{\ell_{(1)}}} (X \circledast_{(1)} M_0)) \to X \circledast_{(2)} \mathrm{Wh}_2 \circ (Q_{\ell_{(1)}} \otimes_{H_{\ell_{(1)}}} M_0)$$

as

$$v_{X,M_0} := \mathrm{Wh}_2\Big((\mathrm{id}_X \otimes \varepsilon^{(2)^{-1}}_{Q_{\ell_{(1)}}\otimes_{H_{\ell_{(1)}}} M_0}) \circ \varepsilon^{(1)}_{X\otimes(Q_{\ell_{(1)}}\otimes_{H_{\ell_{(1)}}} M_0)}\Big). \tag{7.0.3}$$

for every $X \in \mathcal{C}_2, N_2 \in \mathcal{N}_2$ and $M_0 \in \mathcal{M}_0$ and for ε the natural isomorphism defined in Remark 5.0.2.

We are now in a position to prove the main result.

THEOREM 7.0.7. *Let u and v be the natural isomorphisms defined respectively in* (7.0.2) *and* (7.0.3). *Then, the pairs* $(Q_0\otimes_{H_0}, u)$ *and* (Wh_0, v) *are mutually inverse $\mathcal{C}_2$-module equivalences.*

PROOF. We prove the Theorem for the functor $Q_0\otimes_{H_0}$.

Theorem 7.0.3 implies that the following diagram is commutative

$$\begin{tikzcd} \mathcal{M}_2 \arrow[drr, "\mathrm{Wh}_1|_{\mathcal{M}_2}"'] & & \mathcal{N}_2 \arrow[ll, "Q_{\ell_{(2)}}\otimes_{H_{\ell_{(2)}}}"'] \arrow[d, "Q_0\otimes_{H_0}"] \\ & & \mathcal{M}_0. \end{tikzcd}$$

Moreover, by Lemma 6.0.8 the functors Wh_1 and $Q_{\ell_{(2)}}\otimes_{H_{\ell_{(2)}}}$ paired respectively with the natural isomorphisms $\mathrm{Wh}_1(\mathrm{id}_- \otimes \varepsilon^{(1)^{-1}}_-)$ and $\varepsilon^{(2)}_{-\otimes(Q_{\ell_{(2)}}\otimes_{H_{\ell_{(2)}}} -)}$, are $\mathcal{C}_2$-module functors.

Finally, since $Q_0\otimes_{H_0} = Q_{\ell_{(2)}}\otimes_{H_{\ell_{(2)}}} \circ \mathrm{Wh}_1$, we can apply Lemma 4.1.14 obtaining that $(Q_0\otimes_{H_0}, u)$ is a $\mathcal{C}_2$-module functor.

The proof for the functor Wh_0 is analogous. $\square$

CHAPTER 8

Exactness of the tensor product

In this chapter, we study the exactness of the categorical action functor. We start recalling the following general result.

Proposition 8.0.1. *[22, Proposition 7.1.6]. Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ be a rigid monoidal category and let $(\mathcal{M}, \otimes_{\mathcal{M}}, m)$ be a left $\mathcal{C}$-module category. There is a canonical isomorphism*

$$Hom_{\mathcal{M}}(X^* \otimes_{\mathcal{M}} M, M_1) \to Hom_{\mathcal{M}}(M, X \otimes_{\mathcal{M}} M_1) \tag{8.0.1}$$

natural in $X \in \mathcal{C}$ and $M, M_1 \in \mathcal{M}$.

This proposition implies the following.

Corollary 8.0.2. *Let $(\mathcal{C}, \otimes_{\mathcal{C}}, a, 1)$ be a rigid monoidal category and let $(\mathcal{M}, \otimes_{\mathcal{M}}, m)$ be a left $\mathcal{C}$-module category. Then, the endofunctor $X \otimes_{\mathcal{M}} -$ is exact for every $X \in \mathcal{C}$.*

Proof. Proposition 8.0.1 implies that $X \otimes_{\mathcal{M}} -$ is a right adjoint of $X^* \otimes_{\mathcal{M}} -$ and hence it is left exact. Moreover, thanks to Proposition 8.0.1, the endofunctor $X \otimes_{\mathcal{M}} -$ is a left adjoint of ${}^*X \otimes_{\mathcal{M}} -$, and hence it is right exact. $\square$

Consider $U(\mathfrak{g})$-mod$_{\text{fin}}$ the category of finite-dimensional $U(\mathfrak{g})$-modules, which is a rigid monoidal category by Example 4.1.3.
From now on, keep notations as in Chapter 5, 6 and 7. By Corollary 8.0.2, for $i = 1, 2$ the endofunctors

$$X \otimes -\colon \mathcal{M}_i \to \mathcal{M}_i$$

and

$$X \circledast_{(i)} -\colon \mathcal{N}_i \to \mathcal{N}_i$$

are exact functors, for every $X \in U(\mathfrak{g})$-mod$_{\text{fin}}$.
This implies that $X \circledast_{(1)} -\colon \mathcal{M}_0 \to \mathcal{M}_0$ is an exact endofunctor.
The above result has a symmetric counterpart for the right action of $U(\mathfrak{g})$-mod$_{\text{fin}}$ on $\mathcal{M}$ and on $\mathcal{N}$.

CHAPTER A

Appendix

In this appendix we discuss the systems of equations that emerged in Subsection 3.4 when analyzing the number of p-elements occurring in the expression of $\chi(y_\chi^2)$. We collect here the results that were needed to conclude that $\chi(y_\chi^2) \in \mathbb{Q} \setminus \mathbb{Z}$.

A.1. Case $\mathbf{PSL}_3(q)$, q odd

We retain notation from Subsection 3.4, in particular recall that θ is a primitive third root of unity. Moreover, throughout this Section q will be odd. We recall that in Subsection 3.4 we had to estimate the number of pairs (a, b), with $a, b \in \mathbb{F}_q$, which satisfy the following system

$$\begin{aligned} -b^2 - 3b(\theta^i + \theta^j) - 3(\theta^{2i} + \theta^{2j}) &= 3\theta^k \\ a^2 - 3a(\theta^{2i} + \theta^{2j}) + 3(\theta^i + \theta^j) &= -3\theta^{2k}, \end{aligned} \tag{A.1.1}$$

where $i, j, k \in \{0, 1, 2\}$. We denote System (A.1.1) by $E(i, j, k)$, where $i, j, k \in \{0, 1, 2\}$.

LEMMA A.1.1. *Let $q = 7$ and $M = M_1$. Then, the total number of solutions $(a, b) \in \mathbb{F}_7^2$ of each system $E(i, j, k)$ for $i, j, k \in \{0, 1, 2\}$ is 75.*

PROOF. Computing the discriminant of the above equations in b and a respectively, for fixed i, j, k we obtain

$$\begin{aligned} \Delta_1(i, j, k) &= -3(\theta^{2i} + \theta^{2j} + \theta^{i+j} + 4\theta^k) \\ \Delta_2(i, j, k) &= -3(\theta^i + \theta^j + \theta^{2(i+j)} + 4\theta^{2k}). \end{aligned}$$

Notice that $\Delta_1(i, j, k) = \Delta_2(2i, 2j, 2k)$ and $\Delta_2(i, j, k) = \Delta_1(2i, 2j, 2k)$.
Set $\theta = 2$. Then, for each triple (i, j, k) for $i, j, k \in \{0, 1, 2\}$, the values of the discriminants are collected in the following tables:

i	**j**	**k**	Δ_1	Δ_2
0	0	0	0	0
0	0	1	2	6
0	0	2	6	2
1	0	0	2	2
1	0	1	4	1
1	0	2	1	4
2	0	0	2	2
2	0	1	4	1
2	0	2	1	4

i	**j**	**k**	Δ_1	Δ_2
0	1	0	2	2
0	1	1	4	1
0	1	2	1	4
0	2	0	2	2
0	2	1	4	1
0	2	2	1	4
1	1	0	1	5
1	1	1	3	4
1	1	2	0	0

i	**j**	**k**	Δ_1	Δ_2
2	1	0	2	2
2	1	1	4	1
2	1	2	1	4
2	2	0	5	1
2	2	1	0	0
2	2	2	4	3
1	2	0	2	2
1	2	1	4	1
1	2	2	1	4

Bearing in mind that the non-zero squares in $\mathbb{F}_7$ are $1, 2$ and 4, we underlined in green the rows which give rise to four pairs (a, b) solving the system, and in yellow the rows which provide just one solution. Counting them, we get that the total number of solutions of the systems when i, j, k run through $\{1, 2, 3\}$ is 75. $\square$

For simplicity, we call A the matrix

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & -a & -b \\ b+3(\theta^i+\theta^j) & 1-ab-3a(\theta^i+\theta^j) & a-b^2-3(\theta^{2i}+\theta^{2j})-3b(\theta^i+\theta^j) \end{pmatrix}. \tag{A.1.2}$$

LEMMA A.1.2. *Let q be odd. Let $(a, b) \in \mathbb{F}_q^2$ be any solution of the system $E(i, j, k)$ for $i, j, k \in \{0, 1, 2\}$. Then, the rank of $A - \theta^k \cdot 1$ is 2.*

PROOF. Suppose that A is of Jordan type (2,1), i.e. that the rank of

$$A - \theta^k \cdot 1 = \begin{pmatrix} -\theta^k & 0 & 1 \\ 1 & -a-\theta^k & -b \\ b+3(\theta^i+\theta^j) & 1-ab-3a(\theta^i+\theta^j) & a-b^2-3(\theta^{2i}+\theta^{2j})-3b(\theta^i+\theta^j)-\theta^k \end{pmatrix}$$

is one. Then the second column of $A - \theta^k \cdot 1$ must be trivial and the third column must be a multiple of the first one. These conditions lead to the following system of equations:

$$\begin{aligned} &a = -\theta^k \\ &b = \theta^{2k} \\ &3(\theta^i + \theta^j) = -2\theta^{2k} \\ &3(\theta^{2i} + \theta^{2j}) = -2\theta^k. \end{aligned}$$

We analyze the above system, proving that there are no solutions.
1) If $i = j$, then the last two equations of the above system become $3\theta^i = -\theta^{2k}$ and $3\theta^{2i} = -\theta^k$. Multiplying the latter two equations, we get $9 = 1$, a contradiction since p is odd.
2) If $i \neq j$, then there exists $\bar{j} \in \{0, 1, 2\}$, such that $\theta^i + \theta^j + \theta^{\bar{j}} = 0$. Then, the last two equations of the system read as $-3\theta^{\bar{j}} = -2\theta^{2k}$ and $-3\theta^{2\bar{j}} = -2\theta^k$ respectively. Multiplying them, we obtain $9 = 4$, which is satisfied if and only if $p = 5$. If this is the case, the third equation of the initial system becomes $\theta^{\bar{j}} = -\theta^{2k}$, which implies that $1 = -1$, a contradiction. $\square$

LEMMA A.1.3. *Let $p = 5$ and let $M = \left\langle \pi \begin{pmatrix} 1 & -3\theta^{2i} & 3\theta^i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ for } i \in \{0, 1, 2\} \right\rangle$. Then, the number of pairs $(a, b) \in \mathbb{F}_q^2$ for which $\pi \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M$ and*

$$\pi \begin{pmatrix} 0 & 0 & 1 \\ 1 & -a & -b \\ b+3(\theta^i+\theta^j) & 1-ab-3a(\theta^i+\theta^j) & a-b^2-3(\theta^{2i}+\theta^{2j})-3b(\theta^i+\theta^j) \end{pmatrix}$$

is a 5-element for some $i, j \in \{0, 1, 2\}$ is 15.

PROOF. We use the following GAP code to count the number of p-elements.

```
#we call z the zero of F_25, u the unit of F_25 and theta a third root of unit;
z:=Z(25)*0;;
u:=Z(25)^0;;
theta:=Z(25)^8;;
#y denotes the generator of the group of invertible elements in F_25;
y:=Z(25);;
#t stands for \tau
t:=[[z,u,z],[z,z,u],[u,z,z]];;
centre:=[[theta,z,z],[z,theta,z],[z,z,theta]];;
M:=[];;
F25:=[z];;
#we construct F25
for i in [1..24] do
c:=y^i;
Append(F25,[c]);
od;

#we construct M_{C_{(3)}} as a list and we call it L
L:=[];
for l in [1,2,3] do
c:=[[u,-3*theta^l,3*theta^(2*l)],[z,u,z],[z,z,u]];
Append(L,[c]);
od;

#we construct the subgroup M
for j in [1..5] do
for i in [1..5] do
c:=L[1]^i*L[2]^j;
Append(M,[c]);
od;
od;


#we create a list P containing the elements in t*[[u,(y^12)*3*(x^(2*i)),3*(x^i)],[z,u,z],[z,z,u]]*
#[[u,(y^12)*3*(x^(2*j)),3*(x^j)],[z,u,z],[z,z,u]]*m*t*m^(-1) which are 5-elements for m in M
P:=[];;

for i in [1..3] do
for j in [1..3] do
for m in M do
c:=t*[[u,(y^12)*3*(x^(2*i)),3*(x^i)],[z,u,z],[z,z,u]]*
[[u,(y^12)*3*(x^(2*j)),3*(x^j)],[z,u,z],[z,z,u]]*m*t*m^(-1);
if c^5=theta or c^5=theta^2 or c^5=theta^3 then
Append(P,[c]);
fi;
od;
od;
od;
#the length of P gives us the number of 5-elements
```

```
Length(P);
 15
```

□

Let C be the matrix

$$\begin{pmatrix} a+r+w & -a(a+r+w) & 1+(a^2-b)(a+r+w) \\ 1 & -a & a^2-b \\ b+s+rw+a(r+w)+y & 1-a(b+s+rw+a(r+w)+y) & r+w+(a^2-b)(b+s+rw+a(r+w)+y) \end{pmatrix}, \quad \text{(A.1.3)}$$

for $y = 3\theta^i, s = 3\theta^j, w = (-3/2)\theta^{2i}, r = (-3/2)\theta^{2j}$ and $i, j \in \{0, 1, 2\}$.

Lemma A.1.4. *Let $p \neq 7$ and $p \neq 19$. If the characteristic polynomial of C is $(\theta^k - z)^3$, for some $k \in \{0, 1, 2\}$, then the rank of $C - \theta^k \cdot 1$ is 2. Moreover,*

- *If $p = 7$, the rank of $C - \theta^k \cdot 1$ is 1 if and only if*
$$(i, j, k) \in \{(0, 0, 2), (1, 1, 1), (2, 2, 0)\};$$
- *If $p = 19$, the rank of $C - \theta^k \cdot 1$ is 1 if and only if*
$$(i, j, k) \in \{(0, 1, 0), (0, 2, 1), (1, 0, 0), (1, 2, 2), (2, 0, 1), (2, 1, 2)\}.$$

Proof. First of all, observe that for every $k \in \{0, 1, 2\}$ the $(2, 1)$ entry of $C - \theta^k \cdot 1$ is equal to one. This implies that $C \neq \theta^k \cdot 1$.
Assume that $\mathrm{rk}(C - \theta^k \cdot 1) = 1$. Then

$$\det \begin{pmatrix} a+r+w-\theta^k & -a(a+r+w) \\ 1 & -a-\theta^k \end{pmatrix} = 0.$$

This yields that $r + w = \theta^k$, i.e. $-3(\theta^{2i} + \theta^{2j}) = 2\theta^k$. We compute the following table for $k \in \{0, 1, 2\}$, which shows when the above equation admits solutions.

i	**j**	$-3(\theta^{2i} + \theta^{2j}) = 2\theta^k$	$(-3(\theta^{2i} + \theta^{2j}))^3 = 8$	**Solution if**
0	0	$-3 = \theta^k$	$-27 \equiv_p 1$	$p = 2, 7$
0	1	$3\theta = 2\theta^k$	$27 \equiv_p 8$	$p = 19$
0	2	$3\theta^2 = 2\theta^k$	$27 \equiv_p 8$	$p = 19$
1	0	$3\theta = 2\theta^k$	$27 \equiv_p 8$	$p = 19$
1	1	$-3\theta^2 = \theta^k$	$-27 \equiv_p 1$	$p = 2, 7$
1	2	$3 = 2\theta^k$	$27 \equiv_p 8$	$p = 19$
2	0	$3\theta^2 = 2\theta^k$	$27 \equiv_p 8$	$p = 19$
2	1	$3 = 2\theta^k$	$27 \equiv_p 8$	$p = 19$
2	2	$-3\theta = \theta^k$	$-27 \equiv_p 1$	$p = 2, 7$

(A.1.4)

So for q odd and $p \neq 7, 19$, the equation $-3(\theta^{2i} + \theta^{2j}) = 2\theta^k$ is never satisfied. Let $p = 7$ and set $\theta = 2$. By Table A.1.4, the equation $-3(\theta^{2i} + \theta^{2j}) = 2\theta^k$ admits solutions only if $i = j$. It is easy to verify that for each $i \in \{0, 1, 2\}$ there exists a unique $k \in \{0, 1, 2\}$ such that the equation is satisfied. In particular, the triples (i, j, k) which solve the equation are $(0, 0, 2), (1, 1, 1), (2, 2, 0)$.
For $p = 19$ the argument is analogous, with $\theta = 7$. □

We recall that for proving Proposition 2.3.11, we needed to estimate the number of pairs (a, b) which solve the following system:

$$\begin{aligned} &a^2 + a(r + w) + s + y - rw - r^2 - w^2 = -3\theta^{2k} \\ &2(r + w) + (a^2 - b)(b + s + rw + y + a(r + w)) = 3\theta^k. \end{aligned} \tag{A.1.5}$$

for some r, s, y, w and some $k \in \{0, 1, 2\}$.

Lemma A.1.5. *The total number of solutions $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$ of system* (A.1.5) *for which the rank of $C - \theta^k \cdot 1$ is equal to 1 are at most*

i) 12 if $p = 7$;
ii) 24 if $p = 19$.

Proof. i) Let $p = 7$. By Lemma A.1.4, the triples (i, j, k) which satisfy the equation $-3(\theta^{2i} + \theta^{2j}) = 2\theta^k$ are $(0, 0, 2), (1, 1, 1), (2, 2, 0)$.
For each $(i, j, k) \in \{(0, 0, 2), (1, 1, 1), (2, 2, 0)\}$, the first equation of system A.1.5 gives at most two solutions for a and for each a the second equation provides at most two solutions for b. Hence, there at most $4 \cdot 3$ pairs (a, b) solving system A.1.5 and giving rise to 7-elements of Jordan type $(2, 1)$.
ii) Let $p = 19$. In virtue of Lemma A.1.4, the triples (i, j, k) satisfying the equation $-3(\theta^{2i} + \theta^{2j}) = 2\theta^k$ are $(0, 1, 0), (0, 2, 1), (1, 0, 0), (1, 2, 2), (2, 0, 1)$ and $(2, 1, 2)$. Hence, by the same argument we used for the previous case, the solutions of A.1.5 are at most $4 \cdot 6$. □

Lemma A.1.6. *Let $q = 7$. Then, the number of pairs $(a, b) \in \mathbb{F}_7 \times \mathbb{F}_7$ satisfying system* (A.1.5) *is 33. In addition, in exactly 6 cases the corresponding matrix C has Jordan type (2,1).*

Proof. We use the following GAP code for proving the lemma.

```
#for simplicity, we call z the zero of F_7 and u the unity of F_7
z:=Z(7)*0;;
u:=Z(7)^0;;
theta:=Z(7)^2;;
#y stands for the generator of the group of the invertible elements in F_7
y:=Z(7);;
#t stands for \tau
t:=[[z,u,z],[z,z,u],[u,z,z]];;
centre:=[[theta,z,z],[z,theta,z],[z,z,theta]];;
M:=[];
F7:=[z];
#we construct F_7
for i in [1..6] do
c:=y^i;
Append(F7,[c]);
od;
#we construct M_2 and for simplicity we call it M
for a in F7 do
for b in F7 do
c:=[[u,a,b],[z,u,a],[z,z,u]];
```

```
Append(M,[c]);
od;
od;

P:=[];;
#we create a list with all 7-elements in y_chi^2
for i in [1..3] do
for j in [1..3] do
for m in M do
c:=t*[[u,(-3*2^(-1))*(theta^(2*i)),3*(theta^i)],[z,u,(-3*2^(-1))*(theta^(2*i))],[z,z,u]]*
[[u,(-3*2^(-1))*(theta^(2*j)),3*(theta^j)],[z,u,(-3*2^(-1))*(theta^(2*j))],[z,z,u]]*m*t*m^(-1);
if c<> centre^3 and (c^7=centre or c^7=centre^2 or c^7=centre^3) then
Append(P,[c]);
fi;
od;
od;
od;
#we count the number of 7-elements of Jordan type (2,1)
n:=0;;
for p in P do
c:=p-centre;
d:=p-centre^2;
e:=p-centre^3;
if RankMatrix(c)=1 or RankMatrix(d)=1 or RankMatrix(e)=1 then
n:=n+1;
fi;
od;
#the number of 7-elements is the length of P
Length(P);
 33
#n gives the number of 7-elements of Jordan type (2,1)
n;
 6
```

$\square$

LEMMA A.1.7. *Let $q = 19$. Then, the number of pairs $(a, b) \in \mathbb{F}_{19} \times \mathbb{F}_{19}$ satisfying system A.1.5 is 51. Moreover, in exactly 12 cases the corresponding matrix C has Jordan type (2,1).*

PROOF. The following GAP code proves the Lemma.

```
#for simplicity, we call z the zero of F_19 and u the unity of F_19
z:=Z(19)*0;;
u:=Z(19)^0;;
theta:=Z(19)^6;;
#y stands for the generator of the group of the invertible elements in F_19
y:=Z(19);;
#t stands for \tau
t:=[[z,u,z],[z,z,u],[u,z,z]];;
centre:=[[theta,z,z],[z,theta,z],[z,z,theta]];;
```

```
M:=[];
F19:=[z];
#we construct F_19
for i in [1..18] do
c:=y^i;
Append(F19,[c]);
od;
#we construct M_2 and for simplicity we call it M
for a in F19 do
for b in F19 do
c:=[[u,a,b],[z,u,a],[z,z,u]];
Append(M,[c]);
od;
od;

P:=[];;
#we create a list will all 19-elements in y_chi^2
for i in [1..3] do
for j in [1..3] do
for m in M do
c:=t*[[u,(-3*2^(-1))*(theta^(2*i)),3*(theta^i)],[z,u,(-3*2^(-1))*(theta^(2*i))],[z,z,u]]*
[[u,(-3*2^(-1))*(theta^(2*j)),3*(theta^j)],[z,u,(-3*2^(-1))*(theta^(2*j))],[z,z,u]]*m*t*m^(-1);
if c<> centre^3 and (c^19=centre or c^19=centre^2 or c^19=centre^3) then
Append(P,[c]);
fi;
od;
od;
od;
#we count the number of 19-elements of Jordan type (2,1)
n:=0;;
for p in P do
c:=p-centre;
d:=p-centre^2;
e:=p-centre^3;
if RankMatrix(c)=1 or RankMatrix(d)=1 or RankMatrix(e)=1 then
n:=n+1;
fi;
od;
#the number of 19-elements is the length of P
Length(P);
 51
#n gives the number of 19-elements of Jordan type (2,1)
n;
 12
```

□

Lemma A.1.8. *Let $p = 5$ and let*

$$M = \left\langle \pi \begin{pmatrix} 1 & (-3/2)\theta^{2l} & 3\theta^l \\ 0 & 1 & (-3/2)\theta^{2l} \\ 0 & 0 & 1 \end{pmatrix} : l \in \{0, 1, 2\} \right\rangle.$$

The total number of solutions $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$ *of system* (A.1.5) *such that* $\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in M$ *is* 15.

Proof. The proof is given by the following code.

```
#as in the previous codes, we rename the zero, the unit, the third root of unit
z:=Z(25)*0;;
u:=Z(25)^0;;
theta:=Z(25)^8;;
#t stands for tau
t:=[[z,u,z],[z,z,u],[u,z,z]];;
centre:=[[theta,z,z],[z,theta,z],[z,z,theta]];;
#we create a list where we insert two elements from M_{C_{(3)}}
L:=[];;
for i in [1..2] do
c:=[[u,-3*(2^(-1))*theta^i,3*theta^(2*i)],[z,u,-3*(2^(-1))*theta^i],[z,z,u]];
Append(L,[c]);
od;
# the elements in L generates M, so we construct M in the following way
M:=[];;
for i in [1..5] do
for j in [1..5] do
c:=(L[1]^i)*(L[2]^j);
Append(M,[c]);
od;
od;
#we count the number of 5 elements in M
P:=[];;
for i in [1..3] do
for j in [1..3] do
for m in M do
c:=t*[[u,-3*(2^(-1))*(theta^(2*i)),3*(theta^i)],[z,u,-3*(2^(-1))*(theta^(2*i))],[z,z,u]]*
[[u,-3*(2^(-1))*(theta^(2*j)),3*(theta^j)],[z,u,-3*(2^(-1))*(theta^(2*j))],[z,z,u]]*m*t*m^(-1);
if c<> centre^3 and (c^5=centre or c^5=centre^2 or c^5=centre^3) then
Append(P,[c]);
fi;
od;
od;
od;
#the length of P will give us the number of 5-elements
Length(P);
15
```

∎

A.2. Case $\mathbf{PSL}_3(q)$, q even

Here q is even. We retain notation from Section 3.4.
We need to solve the system (2.3.6), which reads as

$$\begin{aligned} b^2 + b(\theta^i + \theta^j) + (\theta^{2i} + \theta^{2j} + \theta^k) = 0 \\ a^2 + a(\theta^{2i} + \theta^{2j}) + (\theta^i + \theta^{2j} + \theta^{2k}) = 0. \end{aligned} \tag{A.2.1}$$

We call $E'(i,j,k)$ the system (A.2.1).
For computing $\chi(y_\chi^2)$, we need to investigate the Jordan type of the p-elements provided by system (A.2.1).

LEMMA A.2.1. *Let q be even. Let $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$ be a solution of system $E'(i,j,k)$, for some $i,j,k \in \{0,1,2\}$. Then, the rank of*

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & -a & -b \\ b+3(\theta^i+\theta^j) & 1-ab-3a(\theta^i+\theta^j) & a-b^2-3(\theta^{2i}+\theta^{2j})-3b(\theta^i+\theta^j) \end{pmatrix} - \theta^k \begin{pmatrix} 1&0&0\\0&1&0\\0&0&1 \end{pmatrix} \tag{A.2.2}$$

is 1 if and only if $i = j$ and $(a,b) = (\theta^k, \theta^{2k})$.

PROOF. Consider the matrix

$$\begin{pmatrix} -\theta^k & 0 & 1 \\ 1 & -a-\theta^k & -b \\ b+3(\theta^i+\theta^j) & 1-ab-3a(\theta^i+\theta^j) & a-b^2-3(\theta^{2i}+\theta^{2j})-3b(\theta^i+\theta^j)-\theta^k \end{pmatrix},$$

for some $i,j,k \in \{0,1,2\}$ and $a,b \in \mathbb{F}_q$.
By a direct calculation one sees that the rank of the above matrix is 1 if and only if

$$\begin{cases} a = -\theta^k \\ b = \theta^{2k} \\ \theta^i + \theta^j = 0 \\ \theta^{2i} + \theta^{2j} = 0. \end{cases}$$

This system is satisfied if and only if $i = j$ and $(a,b) = (\theta^k, \theta^{2k})$. $\square$

LEMMA A.2.2. *Let $v = \pi \left(\begin{smallmatrix} 1&a&b\\0&1&a\\0&0&1 \end{smallmatrix}\right)$ for some $a,b \in \mathbb{F}_q$ and let $\tau = \pi \left(\begin{smallmatrix} 0&0&1\\0&1&0\\1&0&0 \end{smallmatrix}\right)$. Assume $a \neq 0$. If $b = 0$ or $b = a^2$, then the rank of $\tau v \tau v^{-1} - 1$ is 2.*

PROOF. For $a,b \in \mathbb{F}_q$, we have to study the rank of the matrix

$$\begin{pmatrix} 0 & a & a^2+b \\ a & a^2 & a+a^3+ab \\ b & a+ba & a^2+ba^2+b^2 \end{pmatrix}.$$

Subtracting a-times the second column to the third one, we obtain

$$\begin{pmatrix} 0 & a & b \\ a & a^2 & a+ab \\ b & a+ba & b^2 \end{pmatrix}. \tag{A.2.3}$$

If $b = 0$ then the above matrix has rank 2, since $a \neq 0$ by assumption.
If $b = a^2$ the same Gaussian reduction made before leads to the following matrix:

$$\begin{pmatrix} 0 & a & 0 \\ a & a^2 & a \\ a^2 & a+a^3 & a^2 \end{pmatrix},$$

whose rank is 2, since $a \neq 0$ by assumption.

$\square$

LEMMA A.2.3. *Let $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$ and let $i,j \in \{0,1,2\}$. The characteristic polynomial of*

$$\begin{pmatrix} 1 & a & a^2+b \\ a & a^2+1 & a(a^2+b+1) \\ b+\theta^{2i}+\theta^{2j}+1 & a(b+\theta^{2i}+\theta^{2j}) & (a^2+b)(b+\theta^{2i}+\theta^{2j})+b+1 \end{pmatrix}$$

is $(\theta^k - z)^3$ for some $k \in \{0,1,2\}$ if and only if

$$(a,b) \in \{(0,0),(0,1),(a,0),(a,a^2),(1,\theta^{2l})\},$$

for any $a \neq 0$ and for any $l \in \{1,2\}$.
Furthermore, the following table shows for which $(i,j,k) \in \{0,1,2\}^3$ the pair (a,b) is a solution of $E'(i,j,k)$.

(i,j,k)	***Solution (a,b)***
$(i,j,0)$, $i \neq j$	$(0,0)$
$(i,j,0)$, $i \neq j$	$(a,0)$, $a \neq 0$
$(i,j,0)$, $i \neq j$	(a,a^2), $a \neq 0$
$(i,i,0)$	$(0,0)$
$(i,i,0)$	$(0,1)$
(i,i,k), $k \neq 0$	$(1,\theta)$
(i,i,k), $k \neq 0$	$(1,\theta^2)$

(A.2.4)

PROOF. For $x, x' \in M_{2_{C_{(3)}}}$ and $v = \pi \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right)$, we have

$$\begin{aligned} \tau x x' v \tau v^{-1} &= \pi \left(\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 1 & \theta^{2i} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 1 & \theta^{2j} \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right) \right) \\ &= \pi \begin{pmatrix} 1 & a & a^2+b \\ a & a^2+1 & a(a^2+b+1) \\ b+\theta^{2j}+\theta^{2i}+1 & a(b+\theta^{2j}+\theta^{2i}) & (a^2+b)(b+\theta^{2j}+\theta^{2i})+b+1 \end{pmatrix}, \end{aligned}$$

for $i,j \in \{1,2\}$ and $a,b \in \mathbb{F}_q$.
Computing the characteristic polynomial of the matrix

$$\begin{pmatrix} 1 & a & a^2+b \\ a & a^2+1 & a(a^2+b+1) \\ b+\theta^{2j}+\theta^{2i}+1 & a(b+\theta^{2j}+\theta^{2i}) & (a^2+b)(b+\theta^{2j}+\theta^{2i})+b+1 \end{pmatrix}$$

and forcing it to be equal to $(\theta^j - z)^3$, we get the following system of equalities:

$$\begin{aligned} &1 + b(1 + a^2 + \theta^{2j} + \theta^{2i}) + b^2 = \theta^{2k} \\ &1 + b(1 + a^2 + \theta^{2j} + \theta^{2i}) + b^2 + a^2(1 + \theta^{2j} + \theta^{2i}) = \theta^k. \end{aligned}$$

Summing the equations, we obtain $a^2(1 + \theta^{2j} + \theta^{2i}) = \theta^k + \theta^{2k}$. We divide the treatment into cases.
1) Suppose that $i \neq j$, then the equation $a^2(1 + \theta^{2j} + \theta^{2i}) = \theta^k + \theta^{2k}$ reduces to $0 = \theta^k + \theta^{2k}$, i.e. $k = 0$. Substituting $k = 0$ in the first equation we obtain

$a^2b+b^2=0$; in particular, the solutions are $(a,0)$ and (a,a^2) for $a\in\mathbb{F}_q$.
2) Suppose that $i=j$ then the initial system becomes

$$\begin{aligned}&a^2=\theta^k+\theta^{2k}\\&1+b(1+a^2+\theta^k+\theta^{2k})+b^2=\theta^{2k}.\end{aligned}$$

2a) If $k=0$, then $a=0$ and $b+b^2=0$, i.e. the solutions are $(a,b)=(0,0)$ and $(a,b)=(0,1)$.
2b) If $k\neq 0$ then the solution is $(a,b)=(1,\theta^{2k})$.

$\square$

LEMMA A.2.4. *Let $(i,j,k)\in\{1,2\}^2\times\{0,1,2\}$ and $(a,b)\in\mathbb{F}_q^2$ be such that the characteristic polynomial of the matrix*

$$\begin{pmatrix} 1 & a & a^2+b\\ a & a^2+1 & a(a^2+b+1)\\ b+\theta^{2i}+\theta^{2j}+1 & a(b+\theta^{2i}+\theta^{2j}) & (a^2+b)(b+\theta^{2i}+\theta^{2j})+b+1\end{pmatrix}$$

is $(\theta^k-z)^3$. In the following table we list the Jordan type of the above matrices corresponding to each pair (a,b) together with the matching triple $(i,j,k)\in\{1,2\}^2\times\{0,1,2\}$ as in Table (A.2.4).

(i,j,k)	*Solution (a,b)*	*Jordan type*
$(i,j,0)$, $i\neq j$	$(0,0)$	$(1,1,1)$
$(i,j,0)$, $i\neq j$	$(a,0)$, $a\neq 0$	(3)
$(i,j,0)$, $i\neq j$	(a,a^2), $a\neq 0$	(3)
$(i,i,0)$	$(0,0)$	$(2,1)$
$(i,i,0)$	$(0,1)$	$(2,1)$
(i,i,k), $k\neq 0$	$(1,\theta)$	$(2,1)$
(i,i,k), $k\neq 0$	$(1,\theta^2)$	$(2,1)$

(A.2.5)

PROOF. We compute the Jordan type of the matrices corresponding to the terms in table (A.2.4).
1) If $k=0$ and $(a,b)=(0,0)$, we see that the rank of the matrix

$$\begin{pmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 1+\theta^{2j}+\theta^{2i} & 0 & 0\end{pmatrix}$$

is 1 if and only if $i\neq j$ and 0 otherwise.
If $k=0$ and $(a,b)=(0,1+\theta^{2j}+\theta^{2i})$, then we compute the rank of the matrix

$$\begin{pmatrix} 0 & 0 & 1+\theta^{2j}+\theta^{2i}\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix},$$

and proceed as above.
Let $k=0$ and let $(a,b)=(a,0)$ or (a,a^2). Then we evaluate the rank of

$$\begin{pmatrix} 0 & a & a^2+b\\ a & a^2 & a(a^2+b+1)\\ b & a(b+1) & (a^2+b+1)(b+1)\end{pmatrix}.$$

If $a=0$, then it is 0. If $a\neq 0$, then the first two columns are linearly independent and in consequence the rank of the above matrix is 2.

2) If $k \neq 0$ and $i = j$, then $(a, b) = (1, \theta^{2k})$. Hence, we have to determine the rank of the following matrix

$$\begin{pmatrix} \theta^{2k} & 0 & \theta^k \\ 1 & \theta^k & \theta^{2k} \\ \theta^k & \theta^{2k} & 1 \end{pmatrix},$$

which is clearly 2. $\square$

Acknowledgements

Desidero esprimere innanzitutto la mia gratitudine ai miei relatori.
Ringrazio Giovanna Carnovale per avermi accompagnata in questi tre anni di dottorato. Grazie per il supporto, la pazienza e per avermi saputo conoscere, ascoltare e capire, trovando così il modo migliore per incoraggiarmi e spronarmi nei miei momenti di difficoltà. È stato molto stimolante per me avere come relatrice una donna di cui nutro molta stima professionale e personale.
I would like to thank Juan Cuadra for the help, for the suggestions in mathematics (but not only) and for always welcoming me in Almería. I appreciate all the time you invested (even if sometimes it felt wasted) and the care and attention you provided in supervising me. I must say that if I hadn't done my master's thesis in Almería, I wouldn't be here writing this work.
I would also like to thank Ehud Meir for letting me visit him in Aberdeen. Thank you for our stimulating mathematical discussions, which have enriched my comprehension and knowledge of the topic of Hopf orders.
I would also like to thank the people in the math department in Aberdeen for making me feel welcome there, especially, I am grateful to the climbing team: Irakli, Fabian and Julius.
My gratitude also goes to Gastón García, for helping me with GAP and making me able to finish some computations for concluding the proof of Theorem 2.1.1 for $\mathbf{PSL}_3(q)$.
I would also like to thank the referees Fabio Gavarini and César Galindo for reading my thesis and for giving me suggestions to improve this work.
Voglio ringraziare anche il coordinatore del corso di dottorato Giovanni Colombo. Grazie per aver sempre ascoltato e capito le richieste di noi dottorandi e per essere sempre stato disponibile nei nostri confronti.

Penso che questo traguardo raggiunto sia anche il frutto del sostegno e del supporto delle persone che mi circondano. Sono grata e orgogliosa di avere una famiglia e degli amici così speciali.

Bibliography

[1] S. Abreu, R.Britto, C.Duhr and E.Gardi, *Diagrammatic Hopf algebra of cut Feynman integrals: the one-loop case.* J. High Energy Phys. 12 (2017) 090.

[2] E. Aljadeff, P. Etingof, S. Gelaki, and D. Nikshych, *On twisting of finite-dimensional Hopf algebras.* J. Algebra **256** (2002), no. 2, 484-501.

[3] M. J. J. Barry and M. B. Ward, *Simple groups contain minimal simple groups*. Publ. Mat. **41** (1997), 411-415.

[4] N. Ben David and Y. Ginosar, *On groups of central type, non-degenerate and bijective cohomology classes*. Israel J. Math. **172** (2009), 317-335.

[5] R. Blumenhagen and E. Plauschinn,*Introduction to conformal field theory: with applications to string theory*, Lect. Notes Phys. 779 (2009).

[6] C. Bonnafé, Representations of $\mathrm{SL}_2(\mathbb{F}_q)$. *Algebra and Applications* 13. Springer-Verlag London, Ltd., London, 2011.

[7] J. Brundan and S. M. Goodwin, *Good grading polytopes*. Proceedings of the London Mathematical Society, 94(1):155-189,2007.

[8] J. Brundan, S. M. Goodwin and A. Kleshchev, *Highest weight theory for finite W-algebras*, Internat. Math. Res. Notices, 15 (2008), Art. ID rnn051.

[9] J. Brundan and A. Kleshchev, *Representations of shifted Yangians and finite W-algebras*. Mem. Amer. Math. Soc. 196 (2008).

[10] G. Carnovale, J. Cuadra, and E. Masut, *Non-existence of integral Hopf orders for twists of several simple groups of Lie type.* Publicacions Matemàtiques 68 (2024), 73–101.

[11] R. W. Carter, Simple groups of Lie type. Reprint of the 1972 original. *Wiley Classics Library.* John Wiley & Sons, Inc., New York, 1989.

[12] L. N. Childs, *Taming wild extensions with Hopf algebras*. Trans. Amer. Math. Soc. **304** (1987), no. 1, 111-140.

[13] ———, Taming wild extensions: Hopf algebras and local Galois module theory. *Mathematical Surveys and Monographs* 80. Amer. Math. Soc., Providence, RI, 2000.

[14] J. Cuadra and E. Meir, *On the existence of orders in semisimple Hopf algebras*. Trans. Amer. Math. Soc. **368** (2016), no. 4, 2547-2562.

[15] ———, *Non-existence of Hopf orders for a twist of the alternating and symmetric groups*. J. London Math. Soc. (2) **100** (2019), no. 1, 137-158.

[16] ———, *Existence of integral Hopf orders in twists of group algebras*. 2022. arXiv:2211.00097.

[17] C. W. Curtis and I. Reiner, Methods of representation theory. With applications to finite groups and orders. Vol. I. *Pure and Applied Mathematics*. John Wiley & Sons, Inc., New York, 1981.

[18] J. D. Dixon and B. Mortimer, Permutation groups. *Graduate Texts in Mathematics* 163. Springer-Verlag, New York, 1996.

[19] L. Dornhoff, Group representation theory. Part A: Ordinary representation theory. Pure and Applied Mathematics 7. Marcel Dekker, Inc., New York, 1971.

[20] A.G. Elashvili and V.G. Kac, *Classification of good gradings of simple Lie algebras*. Amer. Math. Soc. Transl. Ser. 2, 213 (2005), 85–104.

[21] P. Etingof and S. Gelaki, *The representation theory of cotriangular semisimple Hopf algebras*. Int. Math. Res. Not. 1999, no. 7, 387-394.

[22] P. Etingof, S. Gelaki, D. Nikshych, and V. Ostrik, *Tensor Categories*. Mathematical Surveys and Monographs, 205. American Mathematical Society, 2015

[23] G. Frobenius, *Über auflüsbare Gruppen IV*. Sitz. Akad. Wiss. Berlin (1901), 1216–1230.

[24] C. Galindo and S. Natale, Simple Hopf algebras and deformations of finite groups. Math. Res. Lett. 14 (6) (2007), 943–954.

[25] W.L. Gan and V. Ginzburg, *Quantization of Slodowy slices*. Int. Math. Res. Not., 5 (2002),243-255.

[26] N. Genra and T. Juillard, *Reduction by stages for finite W-Algebras*. ArXiv:2212.06022, v2.

[27] Y. Ginosar and O. Schnabel, *Groups of central-type, maximal connected gradings and intrinsic fundamental groups of complex semisimple algebras*. Trans. Amer. Math. Soc. **371** (2019), no. 9, 6125-6168.

[28] S. M. Goodwin, *Translation for finite W-algebras*. Represent. Theory **15** (2011), 307-346.

[29] J. Greenough, *Monoidal 2-structure of bimodule categories*. J. Algebra 324 (2010), no. 8, 1818–1859.

[30] C. Hoffman, *On some examples of simple quantum groups*. Comm. Algebra **28** (2000), no. 4, 1867-1873.

[31] Heinz Hopf, *Ueber die Topologie der Gruppen–Mannifaltigkeiten und ihrer Verallgemeinerungen*, Ann. Math. **42**, (1941), 22–52.

[32] J.E. Humphreys, *Introduction To Lie Algebras And Representation Theory*. Springer-Verlag, New York, 1972.

[33] B. Huppert, Character Theory of Finite Groups. *De Gruyter expositions in mathematics* 25. Walter de Gruyter, Berlin-New York, 1998.

[34] ______. Endliche Gruppen I. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[35] B. Huppert and N. Blackburn, Finite groups. III. *Grundlehren der Mathematischen Wissenschaften* 243. Springer-Verlag, Berlin-New York, 1982.

[36] I. M. Isaacs, Character theory of finite groups. Corrected reprint of the 1976 original. Dover Publications, Inc., New York, 1994.

[37] G. James and M. Liebeck, Representations and characters of groups. Second edition. Cambridge University Press, New York, 2001.

[38] Z. Janko. *A new finite simple group with abelian 2-Sylow subgroups.* Proc. Nnt. Acnd. Sci. U.S.A., 53 (1965), 657458.

[39] ______, *A new finite simple group with Abelian Sylow 2-subgroups, and its characterization.* J. Algebra, **3**, 147–186 (1966).

[40] I. Kaplansky, Bialgebras, Lecture Notes in Math., Univ. of Chicago, Chicago, 1975.

[41] G. Karpilovsky, The Schur multiplier. *London Mathematical Society Monographs. New Series* 2. The Clarendon Press, Oxford University Press, New York, 1987.

[42] ______, Group representations. Vol. 2. *North-Holland Mathematics Studies* 177. NorthHolland Publishing Co., Amsterdam, 1993.

[43] ______, Group representations. Vol. 3. *North-Holland Mathematics Studies* 180. North-Holland Publishing Co., Amsterdam, 1994.

[44] O. H. King, The subgroup structure of finite classical groups in terms of geometric configurations. *Surveys in combinatorics* 2005, 29-56. London Math. Soc. Lecture Note Ser. 327. Cambridge University Press, Cambridge, 2005.

[45] B. Kostant, *On Whittaker vectors and representation theory.* Invent. Math. 48 (1978), 101–184.

[46] H. Kurzweil and B. Stellmacher, The Theory of Finite Groups: An Introduction. Springer, New York, 2004.

[47] R. G. Larson, *Orders in Hopf algebras.* J. Algebra **22** (1972), 201-210.

[48] I. Losev, *Finite-dimensional representations of W-algebras.* Duke Math. J., 159(1):99– 143, 2011.

[49] G. Malle and D. Testerman, Linear algebraic groups and finite groups of Lie type. *Cambridge Studies in Advanced Mathematics* 133. Cambridge University Press, Cambridge, 2011.

[50] P. Mayr, Finite fixed point free automorphism groups, Master's thesis, Johannes Kepler University Linz, December 1998.

[51] ———, http://www.algebra.uni-linz.ac.at/~stein/papers/nonabex5.pdf.

[52] S. Montgomery, Hopf algebras and their actions on rings. *CBMS Regional Conference Series in Mathematics* 82. Amer. Math. Soc., Providence, RI, 1993.

[53] S. Morgan, *Quantum Hamiltonian reduction of W-algebras and category* $\mathcal{O}$. PhD thesis, University of Toronto, (2014). arXiv:1502.07025

[54] M. Movshev, *Twisting in group algebras of finite groups*. Funct. Anal. Appl. **27** (1994), 240-244.

[55] D. Nikshych, *K_0-rings and twisting of finite-dimensional semisimple Hopf algebras*. Comm. Algebra **26** (1998), 321-342.

[56] T. Ono, *An identification of Suzuki groups with groups of generalized Lie type*. Ann. of Math. (2) **75** (1962), 251-259.

[57] ———, *Correction to "An identification of Suzuki groups with groups of generalized Lie type"*. Ann. of Math. (2) **77** (1963), 413.

[58] A. Premet, *Special transverse slices and their enveloping algebras*, Adv. Math., 170 (2002), 1-55.

[59] ———, *Primitive ideals, non-restricted representations and finite W-algebras*. Moscow Math. J. 7 (2007), 743-762.

[60] D. E. Radford, Hopf algebras. *Series on Knots and Everything* 49. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.

[61] Yorck Sommerhäuser, On Kaplansky's conjectures, Interactions between ring theory and representations of algebras (Murcia), Lecture Notes in Pure and Appl. Math., vol. 210, Dekker, New York, 2000, pp. 393–412.

[62] M. Suzuki, *On a class of doubly transitive groups*. Ann. of Math. (2) **75** (1962), 105-145.

[63] ———, *A characterization of the simple groups* $\mathbf{PSL}_2(q)$. J. Math. Soc. Japan **20** (1968), 342-349.

[64] ———, Group Theory I. Translated from the Japanese by the author. *Grundlehren der mathematischen Wissenschaften* 247. Springer-Verlag, Berlin-New York, 1982.

[65] P. Tauvel and R.W.T. Yu, *Lie algebras and algebraic groups*, Monographs in Mathematics (2005), Springer, Berlin Heidelberg New York.

[66] J. G. Thompson, *Nonsolvable finite groups all of whose local subgroups are solvable.* Bull. Amer. Math. Soc. **74** (1968), 383-437.

[67] K. B. Tchakerian, *The maximal subgroups of the Tits simple group.* Pliska Stud. Math. Bulgar. **8** (1986), 85-93.

[68] R. A. Wilson, *The geometry and maximal subgroups of the simple groups of A. Rudvalis and J. Tits.* Proc. London Math. Soc. (3) **48** (1984), no. 3, 533-563.

[69] ———, The finite simple groups. *Graduate Texts in Mathematics* 251. Springer-Verlag London, Ltd., London, 2009.

[70] ———, *Maximal subgroups of sporadic groups.* In: *Finite simple groups: thirty years of the atlas and beyond*, 57-72. Contemp. Math. 694. Amer. Math. Soc., Providence, RI, 2017.

[71] P. Wright Beaulieu, *New Construction of Subgroup Inducing Isomorphic Representations*, PhD thesis, Louisiana State University, May 1991.