Ghent University
Faculty of Sciences
Department of Mathematics: Algebra and Geometry

Modular representation theory and applications to decomposition algebras

Mathias Stout

Academic year 2020–2021

Promotor: Prof. Dr. Tom De Medts

Dissertation submitted in fulfillment of the requirements for the degree of Master of Sciences: Mathematics

Preface

This work was written during the academic year 2020-2021, a period of isolation and lockdowns due to the ongoing pandemic. As such, I would like to extend special thanks to my promotor Tom De Medts, not only for his invaluable advice and guidance throughout the project (both mathematical and meta-mathematical), but also for organizing regularly-scheduled meetings with us thesis students. These meetings always provided a stimulating environment to discuss our projects, and they helped bring order and structure during uncertain times of a global pandemic.

I would also like to thank Jens Bossaert for providing this beautiful LaTeX-template.

Finally, I am extremely grateful to my parents for their constant support and for providing the warm home where much of this work was written.

Mathias Stout, Ghent, Belgium, May 31 2021

Mathias Stout

Contents

Introduction

Decomposition algebras form a class of nonassaciative algebras. They admit multiple direct sum decompositions, and the multiplication between summands is controlled by a precise fusion law. They generalize the notion of axial algebras ([HRS15b, Definition 3.2]), which are always commutative and require the decompositions to arise as eigenspaces of idempotents. Axial algebras, in turn were motivated by the theory of Majorana algebras ([Iva09]), whose axioms were motivated by certain key features of the Griess algebra: a real 196884-dimensional commutative non-associative algebra which has the Monster group as its automorphism group ([Gri82]).

Contrary to axial algebras, decomposition algebras form a nice category ([DPSV20, Appendix A]). They further have the added advantage that they allow one to subdivide eigenspaces into smaller summands. This turns out to be the natural setting to examine the decomposition structure of the recent explicit construction by Tom De Medts and Michiel Van Couwenberghe of an 3875-dimensional algebra on which the complex Chevalley group of type E_8 acts by automorphisms ([MC20][1]). Moreover, E_8 arises as the *Miyamoto group* of this decomposition algebra: a generating set of automorphisms can be found directly by looking at the decompositions.

In this thesis, we investigate three aspects of decomposition algebras. First, we generalize the idea of a representation fusion law, using the language of modular representation theory. Then, we examine how the category of fusion laws behaves if we allow multi-valued maps between objects. Finally, we describe an axial structure on certain Matsuo algebras, specific to the case of characteristic 2.

In the first chapter, we provide some background material on the topics of representation theory and decomposition algebras. The goal is to fix notation and provide the statements of theorems that will be used in later chapters. We give references to standard sources for more context and complete proofs.

We then apply this knowledge in the second chapter: we examine how the concept of the representation fusion law of a finite group G can be translated to positive characteristic. The formulation in characteristic zero, as given in [DPSV20, Example 2.13 and §7], is based on the character theory of finite groups. We give a reformulation in terms of the Grothendieck ring of G in section 2.2 and an equivalent reformulation in terms of modular characters in section 2.3. Finally, we use this language to understand the natural choice of fusion law on the direct factors of the ring kG in section 2.4. Along the way, we also illustrate how the finest grading of the representation fusion law can be understood in terms of the universal grading fusion rings.

In the third chapter, we examine a new category whose objects are fusion laws and whose morphisms are multi-valued maps. We argue why this is a natural concept and examine the corresponding category. We compare it to the category **Fus**, focusing on the categorical interpretation of the finest group grading of a given fusion law. In **Fus**, this is a categorical universal object, but this is no longer the case in our new category. We make precise why, and by how much, this fails in theorem 3.2.14.

[1] Independently, and near simultaneously, Maurice Chayet and Skip Garibaldi also gave a construction of this algebra in [CG21]

In the fourth and final chapter, we examine certain Matsuo algebras in characteristic 2. Matsuo algebras can be defined from certain finite geometries where all lines have exactly three points. If the defining geometry is a Fischer space[2] and the characteristic is of the base field k is different from 2, then the points of the defining geometry correspond to semisimple idempotents. This choice of axes makes the Matsuo algebra into an axial algebra of Jordan type and they play a central role in the classification of such algebras. When the characteristic is equal to 2, the idempotents corresponding to points are no longer semisimple. Instead, we consider idempotents corresponding to sums of three collinear points. We show that when all planes of the underlying geometry are isomorphic to the dual affine plane, these idempotents generate an axial algebra whose fusion law closely resembles the Jordan fusion law.

[2] A Fischer space is a partial linear space of order two in which every plane is either isomorphic to the affine plane of order three or the dual affine plane of order two.

1 Preliminaries

1.1 Representation theory

In this section, we take the opportunity to recall some of the basic notions and terminology of representation theory. We limit ourselves to the foundations of the representation theory finite groups. Concepts that are specific to modular representation theory will be introduced in chapter 2, as they are used. A comprehensive introduction on the topics mentioned here can be found in [Zim14], except for the exposition on characters (section 1.1.4), which is based on [Ser77, Part I]. Another reference for all topics mentioned here is [CR81].

1.1.1 Modules

We recall some basic facts from the general theory of (finitely generated) modules of algebras over rings. Let k be a commutative ring (associative and unital) and let B be a *associative* and *unital* k-algebra. By a *B-module*, we then mean a *left* B-module. We call a module B-module M

1. *simple* or *irreducible* if it is nonzero and contains no submodules other than 0 and itself.
2. *semisimple* if it is a direct sum of simple submodules.
3. *indecomposable* if it cannot be written as the direct sum of two nonzero submodules.
4. *projective* if every surjection of B-modules onto M splits.
5. *injective* if each injection of B-modules with domain M splits.

Semisimple modules are very well-behaved. For example, Schur's lemma illustrate that morphisms between simple modules can always be understood in terms of isomorphisms between some of the simple summands.

Lemma 1.1.1 (Schur, [Zim14, Lemma 1.4.9]). *Let B be an associative and unital k-algebra. Every B-module homomorphism $f\colon E_1 \to E_2$ between two simple kG modules is either zero or an isomorphism.*

In the general case, we cannot decompose a module into simple summands, we can only hope for a decomposition into indecomposable summands.

Theorem 1.1.2 (Krull-Schmidt, [Zim14, Theorem 1.4.3]). *Let k be a field or a complete discrete valuation ring, and let B be an associative and unital finite-dimensional algebra over k. Then, if M is a finitely generated B-module, we can express M as a finite direct sum of indecomposable R-modules. Moreover, for two any two such direct sums*

$$M = \bigoplus_{i=1}^{r} M_i = \bigoplus_{j=1}^{s} N_j,$$

there exists a bijection

$$\beta\colon \{1, \dots, r\} \to \{1, \dots, s\}$$

and isomorphisms

$$f_i \colon M_i \xrightarrow{\sim} N_{\beta(i)}$$

of B-modules for each $i \in \{1, \ldots, r\}$.

We can also investigate B-modules M by iteratively examining maximal submodules $N \subsetneq M$ and the simple quotients M/N.

Definition 1.1.3. Let M be an R-module. A chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{r-1} \subsetneq M_r = M$$

is a *composition series* of M, if each M_{i-1} is a maximal submodule of M_i, for $i = 1, \ldots, r$. The simple quotients M_i/M_{i-1} are called the *composition factors* of M.

By the Jordan-Hölder theorem below, the set of composition factors is uniquely defined, up to isomorphisms.

Theorem 1.1.4 (Jordan-Hölder, [Zim14, Theorem 1.6.26]). *Suppose that M is a B-module admitting two composition series, with corresponding composition factors*

$$E_1, \ldots, E_n \quad \textit{and} \quad S_1, \ldots, S_m,$$

then there exists a bijection $\beta \colon \{1, \ldots, n\} \to \{1, \ldots, m\}$ such that, for $i = 1, \ldots, n$,

$$E_i \cong S_{\beta(i)}.$$

Thus, if M is an B-module admitting a composition series and E is a simple B-module, the number $[M : E]$ of composition factors of M, isomorphic to E, is well-defined.

1.1.2 Group algebras

For any commutative ring R and group G, we can define the *group algebra RG*, which is a unital, associative algebra over R. It is a free R-module on the basis $\{g \mid g \in G\}$, with multiplication defined by linearly extending the multiplication in G. If $R = k$ is a field of characteristic zero and G is finite, then the modules of this group algebra are well-behaved:

Theorem 1.1.5 (Maschke, [Zim14, Theorem 1.2.8]). *Let G be a finite group and let k be a field. If $\operatorname{char}(k)$ is either zero or coprime to the order of G, then kG is semisimple (i.e. all kG-modules are semisimple).*

The collection of all finitely generated (left) RG-modules forms a category, which we denote by $\operatorname{Rep}_R(G)$. In the case that $R = k$ is a field, and G is a *finite* group, the category $\operatorname{Rep}_k(G)$ consists precisely of the finite-dimensional kG-modules. Note that the Krull-Schmidt and Jordan-Hölder theorems (theorems 1.1.2 and 1.1.4) hold in $\operatorname{Rep}_k(G)$.

We continue in this case where $R = k$, a field and G is a finite group. Then kG is a finite-dimensional algebra over a field. Thus every finitely generated kG-module M has a well-defined *radical* $\operatorname{rad}(M)$, given by the intersection of all maximal submodules of M, and $M/\operatorname{rad}(M)$ is semisimple. Note that when the characteristic of k is either 0 or coprime to the order of G, Maschke's theorem theorem 1.1.5 implies that $\operatorname{rad}(M) = 0$.

A particular instance of the radical is given by the radical of the regular left kG-module: $\operatorname{rad}(kG)$. It is a two-sided ideal of the ring kG and $\operatorname{rad}(kG)M = \operatorname{rad}(M)$ for all finitely generated kG-modules

M. The simple kG-modules are the same as the simple $kG/\operatorname{rad}(kG)$-modules, after identification via the surjection $kG \twoheadrightarrow kG/\operatorname{rad}(kG)$.

For each simple kG-module S, there exists a unique (up to isomorphism) indecomposable projective kG-module P_S which surjects onto S. This is the *projective cover* of S and we have $P_S/\operatorname{rad}(P_S) \cong S$. By the Krull-Schmidt theorem, all finitely generated indecomposable projective modules are given up to isomorphism by the indecomposable summands of kG. An arbitrary finitely generated kG-module M also has a projective cover P_M which surjects onto it, given by the direct sum of the projective covers of the simple summands of $M/\operatorname{rad}(M)$. When $\operatorname{char}(k) = p$ and G is a p-group, then the radical of kG is easily understood.

Proposition 1.1.6 ([Zim14, Proposition 1.6.22]). *Let $\operatorname{char}(k) = p$ and let G be a finite p-group. Then $\operatorname{rad}(kG)$ is $(|G| - 1)$-dimensional and a basis is given by $\{x - 1 \mid x \in G \setminus \{1\}\}$. In particular, the trivial kG-module k is the only simple kG-module, up to isomorphism.*

We close this paragraph with two important constructions and one proposition, which crucially depend on the special algebra structure of kG.

First, as all the basic elements of kG form a group, we can equip the dual of a kG-module with a *left* kG-module structure.

Definition 1.1.7. For a finitely generated (left) kG-module M, we define its *dual* M^* as a kG-module with underlying vector space $\operatorname{Hom}_k(M, k)$. The G-action is given as follows: for each $f \in M^*$ and $g \in G$, we define $(g \cdot f) \in M^*$ as

$$(g \cdot f)\colon M \to k\colon m \mapsto f(g^{-1}m).$$

The operation of taking the dual defines an auto-equivalence of $\operatorname{Rep}_k(G)$. Indeed, as M is finite-dimensional, there is a canonical bijection $(M^*)^* \cong M$ and this is readily seen to be an isomorphism of kG-modules.

The fact that the basis elements of kG form a group can also be used to show that kG is a *symmetric* k-algebra. This implies the following.

Proposition 1.1.8 ([Zim14, Proposition 1.10.26]). *Let G be a finite group and k a field. Then each projective kG-module is injective and vice versa.*

The second important construction is given by the tensor product of kG-modules.

Definition 1.1.9. Let M, N be two kG-modules, we equip the tensor product $M \otimes_k N$ of vector spaces with the G-action given by

$$g \cdot (m \otimes n) = (g \cdot m) \otimes (g \cdot n) \quad \text{for all } g \in G, m \in M, n \in N \ .$$

We denote the resulting *tensor product* of kG-modules by $M \otimes N$.

1.1.3 Induction and restriction

We continue with another special feature of group algebras: the *restriction* and *induction* functors, which relate kG modules to kH-modules, for $H \leq G$.

Let k be a field, G a finite group and M an kG-module. For each subgroup H of G, we can consider M as a kH-module via the inclusion $kH \hookrightarrow kG$. This *restricted module* is denoted by $M{\downarrow}_H^G$. Conversely, out of any kH-module N, we can construct the *induced* kG-module $N{\uparrow}_H^G$, given by

$$N{\uparrow}_H^G = kG \otimes_{kH} N.$$

If φ is an automorphism of G and M is a kG-module, then we let ${}^{\varphi}M$ be the kG-module with the same underlying k-vector space as M, but with G-action given by

$$g \cdot m = \varphi(g)m$$

for all $m \in M$. Each $g \in G$ defines an automorphism $\iota(g) \in \mathrm{Aut}(G)$ by conjugation:

$$h \mapsto h^g = g^{-1}hg.$$

In this case, we will simply write ${}^{g}M$ instead of ${}^{\iota(g)}M$.

If $H \trianglelefteq G$ is a normal subgroup, then $\iota(g)$ restricts to an automorphism of H. Now, for any kG-module M, any kH-submodule $N \leq M{\downarrow}_H^G$ and $g \in G$, it holds that gN is again an kH-submodule, isomorphic to ${}^{g}N$. Indeed, for any $h \in H$, we have

$$h(gm) = (gg^{-1}hg)m = g(h^g m).$$

We can use Clifford's theorem to express (certain) simple kG-modules in terms of simple kH-modules, when $H \trianglelefteq G$ is a normal subgroup.

Theorem 1.1.10 (Clifford, [Zim14, Theorem 2.2.3] and [CR81, Theorem 11.1]). *Let E be a simple kG-module and $H \trianglelefteq G$ be a normal subgroup of G. Take any simple kH-submodule $S \leq E{\downarrow}_H^G$ and denote by $I_G(S)$ the subgroup of G given by the elements*

$$I_G(S) = \{g \in G \mid {}^{g}S \cong S\}.$$

Then

1. *$\widetilde{S} := \sum_{g \in I_G(S)} gS \leq E{\downarrow}_H^G$ is a semisimple kH-module, isomorphic to S^n for some $n \in \mathbb{N}$, and*
2. *$M \cong \widetilde{S}{\uparrow}_{I_G(S)}^G$.*

Corollary 1.1.11. *Let k be a field, E a simple kG-module and $H \trianglelefteq G$ a normal subgroup of G contained in the center of G. Then there exists some simple kH-module S and some $n \in \mathbb{N}$ such that $E{\downarrow}_H^G \cong S^n$. In particular, all simple submodules of kH are isomorphic.*

Proof. As the conjugation action of G on H is trivial, it follows that $I_G(S) = G$, for any simple kH-module S. Then there exists a simple kH-module S and and $n \in N$ for which $E{\downarrow}_H^G \cong S^n$ by theorem 1.1.10. By Schur's lemma (lemma 1.1.1), it follows that all simple submodules of $E{\downarrow}_H^G \cong S^n$ are isomorphic to S. ■

1.1.4 Character theory

When k is a field of characteristic 0, then kG is semisimple by Maschke's theorem (theorem 1.1.5). If $k = \mathbb{C}$ and G is a finite group, we can apply the theory of *characters* to gain an even better understanding of $\mathbb{C}G$. We recall some basic facts about this theory, using [Ser77, Part I] as our main reference.

Consider a finite group G. To each finitely generated $\mathbb{C}G$-module, we can attach a function $\chi_M : G \to \mathbb{C}$, sending each $g \in G$ to the trace of the vector space endomorphism that it defines on M. This is the (complex) *character afforded by* M and it uniquely determines the isomorphism class of M. We call a character *irreducible* if it is afforded by a simple $\mathbb{C}G$-module and write $\mathrm{Irr}(G)$ for the set of all irreducible characters. The following proposition follows straight from the definition.

Proposition 1.1.12 ([Ser77, Propositions 1 (iii),2]). *The characters of G satisfy the following properties:*

1. *The map χ_M is a* class function *on G: for all $g, h \in G$, it holds that $\chi_M(hgh^{-1}) = \chi(g)$.*
2. *If $M = M' \oplus M''$, then $\chi_M = \chi_{M'} + \chi_{M''}$. In particular, every χ_M is the sum of irreducible characters.*
3. *The character of $M_1 \otimes M_2$ is given by the product $\chi_{M_1}\chi_{M_2}$.*

We will also sometimes denote the character of tensor product by $\chi_{M_1} \otimes \chi_{M_2}$. For simple modules E_1, E_2, E_3, we say that χ_{E_3} is a *constituent* of $\chi_{E_1} \otimes \chi_{E_2}$ if E_3 is isomorphic to a simple submodule of $E_1 \otimes E_2$.

As $\mathbb{C}G$ is semisimple, we can make the following definition:

Definition 1.1.13 ([Ser77, §2.6]). Let M be a finitely generated $\mathbb{C}G$-module. Write $M = V_1 \oplus \cdots \oplus V_n$ as a sum of simple submodules and denote by χ_i the character of V_i. Then, for each $\chi \in \mathrm{Irr}(G)$,

$$M_\chi = \bigoplus_{\chi_i = \chi} V_i$$

is the χ-*isotypic component* of M. We call the decomposition

$$M = \bigoplus_{\chi \in \mathrm{Irr}(G)} M_\chi$$

the G-*isotypic decomposition* of M.

Remark 1.1.14. Note that Schur's lemma implies that M_χ is the sum of all simple submodules of M with character χ. In particular, *the* decomposition of M into G-isotypic components is unique.

An important feature of characters is the existence of useful inner product.

Definition 1.1.15. For any two class function ϕ, ψ on G with values in $\mathbb{C}$, we set

$$\langle \phi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \phi(g)\psi(g^{-1}).$$

This defines a bilinear map $\langle \cdot, \cdot \rangle$ from the space of complex-valued class functions on G to $\mathbb{C}$.

Theorem 1.1.16 ([Ser77, Theorem 3]). *Let E_1, E_2 be two simple $\mathbb{C}G$-modules, then*

$$\langle \chi_{E_1}, \chi_{E_2} \rangle = \begin{cases} 1 & \text{if } E_1 \cong E_2, \\ 0 & \text{if } E_1 \ncong E_2. \end{cases}$$

Corollary 1.1.17. *Let E be a simple $\mathbb{C}G$-module and M a finitely generated $\mathbb{C}G$-module, then*

$$[M : E] = \langle \chi_M, \chi_E \rangle.$$

Proof. This follows immediately by combining proposition 1.1.12 (ii) and theorem 1.1.16. ■

For a $\mathbb{C}G$-module M, recall that dual module is given by the action with inverses on $\operatorname{Hom}_k(M, k)$. It is then readily seen that the following proposition holds.

Proposition 1.1.18 ([Ser77, Proposition 1 (ii)]). *For any finitely generated $\mathbb{C}G$-module M and all $g \in G$, it holds that*

$$\chi_{M^*}(g) = \chi_M(g^{-1}) = \overline{\chi_M(g)}.$$

(By $\overline{\chi_M(g)}$ we mean the complex conjugate of $\chi_M(g)$)

For any finite set S and a (permutation) action of G on this set, we can define the corresponding permutation representation $\mathbb{C}S$. The underlying vector space has basis S and the action of G is given by linearly extending the permutation action of G on S. In particular, we can consider the *conjugating representation*: the permutation representation given by the conjugation action of G on itself.

Proposition 1.1.19. *The character ψ of the conjugating representation is given by*

$$\sum_{\chi \in \operatorname{Irr}(G)} \chi\overline{\chi},$$

where the class function $\overline{\chi}$ is given by sending $g \in G$ to the complex conjugate $\overline{\chi(g)}$ of $\chi(g)$.

Proof (sketch). Take some set $\{g_1, \ldots, g_n\}$ of representatives of the conjugacy classes of G. Using the inner product (definition 1.1.15), we may verify that both ψ and $\sum \chi\overline{\chi}$ are equal to

$$\sum_{\chi \in \operatorname{Irr}(G)} (\sum_{i=1}^{n} \chi(g_i))\chi.$$

This follows the proof presented in [Rot71, Theorem 1.2]. ■

We could also have defined characters of KG-modules for any field K of characteristic zero; we write $\operatorname{Irr}_K(G)$ for the corresponding set of irreducible K-characters. If K has 'sufficiently many' roots of unity, then the character theories over K and $\mathbb{C}$ essentially coincide.

Definition 1.1.20. Let G be a finite group and K a field. Denote by m the l.c.m. of the orders of the elements of G (i.e. the *exponent* of G). We call K sufficiently large (relative to G) if K contains all m-th roots of unity.

Theorem 1.1.21 ([Ser77, Theorem 24]). *Let G be a finite group. If K is a field of characteristic zero which is sufficiently large with respect to G, then we may identify the rings $\mathbb{Z}\operatorname{Irr}_K(G)$ and $\mathbb{Z}\operatorname{Irr}_{\mathbb{C}}(G)$.*

Remark 1.1.22. Consider a field K as in the above proposition. Let M be a finitely generated $\overline{K}G$-module, where $\overline{K}$ is the algebraic closure of K. Then a (sketch of a) proof of the above theorem can be given by showing that there exists some KG-module M' such that $\overline{K}G \otimes_{KG} M' \cong M$. Similarly, after an identification $\mathbb{C} \leq \overline{K}$, we find a $\mathbb{C}G$-module M'' such that $\overline{K}G \otimes_{\mathbb{C}G} M'' \cong M$. As extension of scalars does not affect the characters, it follows that M, M', M'' have the same character (up to the identification $\mathbb{C} \leq \overline{K}$). In other words, the identification of K-characters and complex characters is unique up to a choice of identification of the m-th roots of unity.

1.2 Decomposition algebras and axial algebras

Decomposition algebras form a class of non-associative algebras whose definition is the result of successive generalizations. First, Alexander Ivanov introduced the concept of *Majorana algebras* in [Iva09], axiomatizing certain properties of the Griess algebra: a 196884-dimensional algebra which has the Monster as its automorphism group. This concept was then further generalized to *axial algebras* by Jonathan I. Hall, Felix Rehren and Sergey Shpectorov ([HRS15b]). Only recently, Tom De Medts, Simon F. Peacock, Sergey Shpectorov and Michiel Van Couwenberghe generalized this concept further to (axial) decomposition algebras in [DPSV20]. These algebras retain the most important feature of all previous steps: the existence of multiple decomposition and the fact that the multiplication obeys a precise *fusion law*. Their major advantage is that, for a given fusion law, the collection of all decomposition algebras forms a well-behaved category ([DPSV20, Appendix A]).

1.2.1 Fusion laws

We start with the extremely general definition of fusion laws. They are useful as convenient language to talk about the behavior of the multiplication between different direct summands of an algebra.

Definition 1.2.1 ([DPSV20, Definition 2.1, 2.2]). A fusion law is a pair $(X, *)$, where X is a set and $*$ is a map

$$*\colon X \times X \to P(X),$$

where $P(X)$ denotes the powerset of X.

- A fusion law $(X, *)$ is called *symmetric* if $x * y = y * x$ for all $x, y \in X$.
- Let $(X, *)$ be a fusion law. We call an element $e \in X$ a unit, if for each $x \in X$ it holds that $e * x \subseteq \{x\}$ and $x * e \subseteq \{x\}$.

Remark 1.2.2. All the fusion laws considered here will be both symmetric and unital.

Example 1.2.3. Consider the following fusion law on a set $\{e, z, h\}$ of three elements, given by

$*$	e	z	h
e	$\{e\}$	$\emptyset$	$\{h\}$
z	$\emptyset$	$\{z\}$	$\{h\}$
h	$\{h\}$	$\{h\}$	$\{e, z\}$

This is the *Jordan* fusion law. It is symmetric and unital, with units e, z.

Example 1.2.4. The *Ising fusion law* is given by the following table:

$*$	e	z	q	t
e	$\{e\}$	$\emptyset$	$\{q\}$	$\{t\}$
z	$\emptyset$	$\{z\}$	$\{q\}$	$\{t\}$
q	$\{q\}$	$\{q\}$	$\{e, z\}$	$\{t\}$
t	$\{t\}$	$\{t\}$	$\{t\}$	$\{e, z, q\}$

This fusion law is again symmetric and unital, with units e, z. When we take a ring R, with $2 \in R^\times$, then we obtain the *Monster fusion law* by assigning

$$\begin{aligned} e &= 1, \quad z = 0, \\ q &= \tfrac{1}{4}, \quad t = \tfrac{1}{32}. \end{aligned}$$

Definition 1.2.5 ([DPSV20, Definition 2.10]). Let Γ be a group. Then the map

$$*\colon \Gamma \times \Gamma \to P(\Gamma)\colon (g,h) \mapsto \{gh\}$$

defines the *group fusion law* $(\Gamma, *)$.

Remark 1.2.6. As the group structure and fusion law structure of a group practically coincide, we will often just write Γ for the group fusion law associated to the group Γ. More generally, we will sometimes denote a fusion law $(X, *)$ by just its underlying set X. The map $*$ is then implied.

Definition 1.2.7 ([DPSV20, Example 2.13]). Let G be a finite group and $\operatorname{Irr}(G)$ the set of its irreducible complex characters. We define a fusion law on $\operatorname{Irr}(G)$ by setting

$$\chi_3 \in \chi_1 * \chi_2 \iff \chi_3 \text{ is a constituent of } \chi_1 \otimes \chi_2$$

for all $\chi_1, \chi_2, \chi_3 \in \operatorname{Irr}(G)$. This fusion law is unital, with unit given by the trivial character.

Example 1.2.8. Consider the fusion law $\operatorname{Irr}(D_6)$, where

$$D_6 = \langle r, s \mid r^3 = s^2 = 1, srs = r^{-1} \rangle.$$

The character table of D_6 is given below.

	1	r	s
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	$e^{\frac{2\pi i}{3}} + e^{\frac{-2\pi i}{3}}$	0

See, for example, [Ser77, §5.3]. From the above table, we can easily read off that

$*$	χ_1	χ_2	χ_3
χ_1	χ_1	χ_2	χ_3
χ_2	χ_2	χ_1	χ_3
χ_3	χ_3	χ_3	$\chi_1 + \chi_2 + \chi_3$

Here we have used the additive notation $\chi_1 + \chi_2 + \chi_3$, rather than writing $\{\chi_1, \chi_2, \chi_3\}$. This saves on brackets and allows us to record multiplicities.

Definition 1.2.9 ([DPSV20, Definition 2.7]). Let $(X, *)$ and $(Y, *)$ be two fusion laws. A *morphism* from $(X, *)$ to $(Y, *)$ is a map of sets $\xi\colon X \to Y$ such that, for all $x_1, x_2 \in X$,

$$\xi(x_1 * x_2) \subseteq \xi(x_1) * \xi(x_2),$$

where the obvious extensions of ξ to a map $P(X) \to P(Y)$ is again denoted by ξ.

As this condition is stable under composition of maps, the collection of all fusion laws forms a category **Fus**.

Remark 1.2.10 *([DPSV20, Remark 2.11]).* The category **Grp** inbeds into **Fus** as a *full* subcategory. Indeed, if Γ and Δ are groups, then the morphisms in **Fus** from $(\Gamma, *)$ to $(\Delta, *)$ are precisely the group homomorphisms $\Gamma \to \Delta$.

1.2.2 Graded fusion laws

A grading of a fusion law is intuitively given by 'grouping together' elements until the fusion law becomes a group fusion law. The correct mathematical framework for this intuition is given by morphisms of fusion laws to groups.

Definition 1.2.11 ([DPSV20, Definition 3.1]).

1. Let $(X, *)$ be a fusion law and let $(\Gamma, *)$ be a group fusion law. A Γ-grading of $(X, *)$ is a morphism $\gamma\colon (X, *) \to (\Gamma, *)$. We call the grading *abelian* if Γ is an abelian group and we call it *adequate* if $\xi(X)$ generates Γ.

2. Every fusion law admits a grading where Γ is the trivial group. We call this the *trivial* grading.

3. Let $(X, *)$ be a fusion law. We call a Γ-grading γ of $(X, *)$ a *finest* or *universal* grading of $(X, *)$, if every grading of $(X, *)$ factors through γ: for every group G and G-grading α of $(X, *)$, there is a unique map $\tilde{\alpha}$ of (group) fusion laws that makes the following diagram commute:

$$\begin{tikzcd} X \arrow[r, "\gamma"] \arrow[d, "\alpha"'] & \Gamma \arrow[dl, dotted, "\tilde{\alpha}"] \\ G & \end{tikzcd} .$$

   In other words, γ is initial among all gradings of X. Similarly, we define the *finest* or *universal* abelian grading of a fusion law as the initial object among its abelian gradings.

We denote the finest grading of a fusion law $(X, *)$ by $\gamma\colon X \to \Gamma_X$ and call $(X, *)$ *graded* if $\Gamma_X \neq 1$ and *ungraded* otherwise.

By definition, if a fusion law $(X, *)$ has a universal (abelian) grading, then it is unique. The existence question is solved by the proposition below. It is a rigorous formulation of the intuition that the universal grading must be the largest group that adequately grades $(X, *)$.

Proposition 1.2.12 ([DPSV20, Proposition 3.2]). *Every fusion law $(X, *)$ admits a unique universal grading, given by the group with presentation*

$$\Gamma_X := \langle \gamma_x, x \in X \mid \gamma_x\gamma_y = \gamma_z, \text{ whenever } z \in x * y \rangle$$

and with grading map $\gamma\colon (X, *) \to (\Gamma_X, *)\colon x \mapsto \gamma_x$. Similarly, there exists a unique finest abelian grading induced by the abelianization $\Gamma_X/[\Gamma_X, \Gamma_X]$ of Γ_X. Both gradings are adequate.

Example 1.2.13.

1. For any group Γ, its universal grading group is given by itself. The grading map is the identity.

2. Consider the Jordan fusion law from example 1.2.3. This fusion law is $\mathbb{Z}/2$-graded, with $\gamma_e = \gamma_z = 0$ and $\gamma_h = 1$.

3. Similarly, the *Ising fusion law* from example 1.2.4 is $\mathbb{Z}/2$-graded, with $\gamma_e = \gamma_z = \gamma_q = 0$ and $\gamma_t = 1$.

4. The representation fusion law for D_6 (example 1.2.8) is ungraded. Since $\chi_i \in \chi_3 * \chi_3$, for $i = 1, 2, 3$, it follows that (with multiplicative notation for Γ_{D_6}) $\gamma_{\chi_1} = \gamma_{\chi_2} = \gamma_{\chi_3} = 1$. This is consistent with proposition 1.2.15 below.

Remark 1.2.14. Let $(X, *)$ and $(Y, *)$ be two fusion laws and let $\gamma_X \colon X \to \Gamma_X$ and $\gamma_Y \colon Y \to \Gamma_Y$ be their universal gradings. Given a morphism $\xi \colon (X, *) \to (Y, *)$, there exists a unique map $\Gamma_\xi \colon \Gamma_X \to \Gamma_Y$ that makes the following diagram commute

$$\begin{tikzcd} X \arrow[r, "\xi"] \arrow[d, "\gamma_X"'] & Y \arrow[d, "\gamma_Y"] \\ \Gamma_X \arrow[r, "\Gamma_\xi"'] & \Gamma_Y \end{tikzcd} .$$

Indeed, this follows immediately from the definition of the universal grading Γ_X of X as a universal object. The assignment $\xi \mapsto \Gamma_\xi$ preserves the identity and respects composition. Hence, Γ is a functor from **Fus** to **Grp** $\subseteq$ **Fus**. The above diagram then precisely expresses that γ is a natural transformation from the identity functor to Γ. A similar statement holds for the universal abelian grading.

We will again encounter the following proposition in section 2.2.3, where we will show how it can be understood in terms of the *universal grading* of the *fusion category* $\mathrm{Rep}_{\mathbb{C}}(G)$.

Proposition 1.2.15 ([DPSV20, Proposition 3.6]). *Let G be a finite group and let $(X, *)$ be the* representation fusion law *of G. Then the universal grading of $(X, *)$ is given by $\Gamma_X = \mathrm{Irr}(Z(G))$, with grading map $\chi \mapsto \frac{\chi_{Z(G)}}{\chi(1)}$.*

1.2.3 (Axial) decomposition algebras

Let R be a commutative ring (associative and with 1). By an R-algebra, we mean simply mean an R-module A equipped with a bilinear multiplication. In particular, our algebras are not assumed to be commutative, unital or associative, unless otherwise noted.

Definition 1.2.16 ([DPSV20, Definition 4.1, 4.5]). Let R be a commutative ring and let $\mathcal{F} = (X, *)$ be a fusion law.

1. An *$\mathcal{F}$-decomposition* of an R-algebra A is a direct sum decomposition $A = \bigoplus_{x \in X} A_x$ (of R-modules) such that
$$A_x A_y \subseteq A_{x*y} \coloneqq \bigoplus_{z \in x*y} A_z$$
for all $x, y \in X$.
2. An *$\mathcal{F}$-decomposition* algebra is a triple (A, I, Ω), where A is an R-algebra, I is an index set and Ω is a tuple of $\mathcal{F}$-decompositions of A, indexed by I. In other words,
$$\Omega[i] = \big((A^i_x)_{x \in X} \mid i \in I\big)$$
and for each $i \in I$, $A = \bigoplus_{x \in X} A^i_x$, is an $\mathcal{F}$-decomposition.
3. Let (A, I, Ω) and (B, J, Σ) be two $\mathcal{F}$-decomposition algebras. A morphism $(\phi, \psi) \colon (A, I, \Omega) \to (B, J, \Sigma)$ is defined as a pair (ϕ, ψ), where $\phi \colon A \to B$ is an R-algebra morphism and $\psi \colon I \to J$ is a map of sets such that
$$\phi(A^i_x) \subseteq B^{\psi(i)}_x$$
for all $x \in X$ and $i \in I$.

This defines a category $\mathcal{F}$-$\mathbf{Dec}_R$ of *$\mathcal{F}$-decomposition algebras.*

Definition 1.2.17 ([DPSV20, Definition 5.3]). Let $(X, *)$ be a fusion law with a distinguished unit $e \in X$ and let $\lambda\colon X \to R\colon x \mapsto \lambda_x$ be an arbitrary map, called the *evaluation map.* We define a category $(\mathcal{F}, \lambda)$-$\mathbf{AxDec}_R$ whose objects are quadruples (A, I, Ω, α) such that (A, I, Ω) is an $\mathcal{F}$-decomposition algebra and $\alpha\colon I \to A\colon i \mapsto a_i$ is a map such that:

1. $a_i \in A^i_e$ for each $i \in I$ and
2. $a_i \cdot b_x = \lambda_x b_x$ for each $i \in I$ and $b_x \in A^i_x$.

These a_i are then called the *left axes.*

A morphism from (A, I, Ω, α) to (B, J, Σ, β) is given by a morphism of decomposition algebras $(\phi, \psi)\colon (A, I, \Omega) \to (B, J, \Sigma)$, for which additionally $\phi \circ \alpha = \beta \circ \psi$. In other words, ϕ maps the axis a_i to $b_{\psi(i)}$.

We can compare the definition of axial decomposition algebras to the original definition of axial algebras:

Definition 1.2.18 ([HRS15b, Definition 3.2]). Let $\mathcal{F} = (X, *)$ be a fusion law such that $X \subseteq R$. An *$\mathcal{F}$-axis* for a commutative R-algebra A is an idempotent e such that there exists a $\mathcal{F}$-decomposition $A = \bigoplus_{x \in X} A_x$ of A, with $e \cdot b_x = x b_x$ for all $b_x \in A_x$ and $x \in X$. The algebra A is called an *$\mathcal{F}$-axial algebra* if it is generated by its $\mathcal{F}$-axes.

Remark 1.2.19. Note that, since axial algebras are nonassociative, the eigenvalues x can be more than just 0 and 1.

Remark 1.2.20. Each axial algebra can be viewed as an axial decomposition algebra. Indeed, pick a set of axes $\{a_i\}_{i \in I}$ and denote by A^i_x the x-eigenspace of the operator ad_{a_i}, given by left multiplication with a_i. Now set set $\Omega[i] = \bigoplus_{x \in X} A^i_x$. Then (A, I, Ω) has the structure of an $\mathcal{F}$-decomposition algebra. When we let λ be the inclusion $X \hookrightarrow R$ and α the map $i \mapsto a_i$, then (A, I, Ω, α) becomes an object of $(\mathcal{F}, \lambda)$-$\mathbf{AxDec}$.

1.2.4 Miyamoto groups

We now define the Miyamoto group of a Γ-decomposition algebra (A, I, Ω), where Γ is a (finite) group. This group arises naturally from the decompositions of A and acts by algebra automorphisms.

Definition 1.2.21 ([DPSV20, Definition 6.1]). Let $R^\times$ be the multiplicative group of units of the base ring R. Denote by $\mathcal{X}_R(\Gamma)$ the *character group* of Γ: the set of all group homomorphisms $\Gamma \to R^\times$, with group operation induced by the multiplication in R.

Definition 1.2.22 ([DPSV20, Definition 6.2]). Let (A, I, Ω) be a Γ-decomposition algebra.

1. Let $\chi \in \mathcal{X}_R(\Gamma)$. For each $i \in I$, we define a linear map $\tau_{i,\chi}\colon A \to A$ by
$$\tau_{i,\chi}(a) = \chi(g)a \quad \text{for all } a \in A^i_g \text{ and } g \in \Gamma.$$
As the base ring R is commutative, it follows that this map defines an R-algebra automorphism of A. We call $\tau_{i,\chi}$ a *Miyamoto map.*

2. Let $\mathcal{Y}$ be a subgroup of $\mathcal{X}_R(\Gamma)$. We define the *Miyamoto group* with respect to $\mathcal{Y}$ as
$$\operatorname{Miy}_{\mathcal{Y}}(A, I, \Omega) := \langle \tau_{i,\chi} \mid i \in I, \chi \in \mathcal{Y} \rangle.$$
We define seperate notation for the special case $\mathcal{Y} = \mathcal{X}_R(\Gamma)$
$$\operatorname{Miy}(A, I, \Omega) := \operatorname{Miy}_{\mathcal{X}_R(\Gamma)}(A, I, \Omega).$$

3. We call (A, I, Ω) *Miyamoto-closed* with respect to $\mathcal{Y}$ if the Miyamoto-group with respect to $\mathcal{Y}$ permutes the elements of Ω. That is, for each $i \in I$ and $\chi \in \mathcal{Y}$, there exists a permutation $\pi_{i,\chi}$ of I such that $\tau_{i,\chi}$ maps each A_g^j to $A_g^{\pi_{i,\chi}(j)}$. In other words, $(\tau_{i,\chi}, \pi_{i,\chi})$ is an automorphism of $(A, I, \Omega) \in \Gamma\text{-}\mathbf{Dec}_R$.

Remark 1.2.23. If there are repeated decompositions in Ω, then there will be multiple valid choices for some of the $\pi_{i,\chi}$.

1.2.5 An observation on Miyamoto groups of decomposition algebras

We conclude this section on decomposition algebras with something more of an observation than a preliminary. Using the following theorem of Michiel van Couwenberghe, it will be straightforward to see that almost any finite group can be the Miyamoto group of a decomposition algebra.

Theorem 1.2.24 ([Cou20, Theorem 3.3.1]). *Let A be a $\mathbb{C}$-algebra, $H \leq \operatorname{Aut}(A)$ a finite abelian subgroup of its automorphism group and $(g_i)_{i \in I}$ any tuple of elements of $\operatorname{Aut}(A)$. Consider the H-isotypic decomposition*
$$A = \bigoplus_{\chi \in \operatorname{Irr}(H)} A_\chi,$$
and for each $i \in I$, let
$$\Omega[i] = (g_i A_\chi \mid \chi \in \operatorname{Irr}(H)).$$
Then (A, I, Ω) is an $\operatorname{Irr}(H)$-decomposition algebra, and
$$\operatorname{Miy}(A, I, \Omega) = \langle z \mid z \in {}^{g_i}H, i \in I \rangle \leq \operatorname{Aut}(A).$$

Proof. A proof of (a slightly more general statement) can be found in [Cou20, Theorem 3.3.1]. The essence of the argument consists of the following two observations, where we abbreviate ${}^{g_i}H =: H_i$.

1. Each decomposition $\Omega[i]$ is the H_i-isotypic decomposition of A.

2. For each i, every $h_i \in H_i$ defines an element of $\mathcal{X}_k(\operatorname{Irr}(H_i))$, given by $\chi \mapsto \chi(h_i)$. Then, for each $\chi \in \operatorname{Irr}(H_i)$, $h_i \in H_i$ and $a \in (g_i A_\chi)$, we have that $\tau_{i,h_i}(\chi)a = \chi(h_i)a = ha$. Indeed, as H is abelian, it acts by scalars on all simple $\mathbb{C}G$-modules. Hence, $\langle \tau_{i,\chi} \mid \chi \in \operatorname{Irr}(H_i) \rangle = H_i$. ■

Corollary 1.2.25. *Let G be a finite group, generated by conjugates of an abelian subgroup H, i.e. $G = \langle \{ {}^gH \mid g \in G \} \rangle$. Then there exists an $\operatorname{Irr}(H)$-decomposition algebra (A, I, Ω) over $\mathbb{C}$ such that $\operatorname{Miy}(A, I, \Omega) \cong G$.*

Proof. Let A be the regular left kG-module, equipped with the multiplication $gh = \delta_{g,h}g$. Then G (and $H \leq G$) acts on A by algebra automorphisms through left multiplication. By assumption, there exists a set of elements $\{g_i\}_{i\in I}$ such that the conjugates ${}^{g_i}H$ generate G. Then theorem 1.2.24 constructs an $\operatorname{Irr}(H)$-decomposition algebra (A, I, Ω) for which

$$\operatorname{Miy}(A, I, \Omega) \cong \langle z \mid z \in {}^{g_i}H\rangle \cong G. \qquad ■$$

Remark 1.2.26. The above corollary 1.2.25 can also be interpreted in terms of ordinary linear algebra. The case $G = H$ asserts that any finite collection of pairwise commuting permutation matrices[1] over $\mathbb{C}^n$ can be simultaneously diagonalized (which is already implicitly used in theorem 1.2.24).

Example 1.2.27. Particular examples of corollary 1.2.25 include S_n, $n \in \mathbb{N}$, and D_{2n}, when n odd.

When k is instead a field of characteristic p, we cannot hope to recover all groups as Miyamoto groups of decomposition algebras.

Definition 1.2.28. Let G be a group and p a prime number. An element $g \in G$ is called *p-regular* is its order is not divisible by p. We denote the set of all p-regular elements of G by G_{reg}.

Proposition 1.2.29. *Let k be a field of characteristic p. If $\langle G_{reg}\rangle \neq G$, then G can not arise as the Miyamoto group of a decomposition algebra over k.*

Proof. Let H be any group, viewed as a fusion law, and let $(A, I, \Omega) \in \text{H-}\mathbf{Dec}_R$. By definition, $\operatorname{Miy}(A, I, \Omega)$ is generated by the Miyamoto maps $\tau_{i,\chi}$. Take any such map $\tau_{i,\chi}$ and write its order as $p^d m$, with m coprime to p. For every $h \in H$, we now have that

$$\chi(h)^{p^d m} = 1 \implies \chi(h)^m = 1.$$

Hence $d = 0$, and the order of $\tau_{\chi,i}$ equals m. As the $\tau_{i,\chi}$ generate $\operatorname{Miy}(A, I, \Omega)$, it follows that $\operatorname{Miy}(A, I, \Omega)$ is generated by its p-regular elements. As H was arbitrary, the proposition follows. ■

Proposition 1.2.30. *Let G be a finite group with $\langle G_{reg}\rangle = G$ and p either zero or a prime number. If $p > 0$, then let m be the l.c.m. of the orders of all p-regular elements. If $p = 0$, let m be the l.c.m. of the orders of all elements of G (i.e. the exponent of G). Take any field k, with $\operatorname{char}(k) = p$, which contains all m-th roots of unity. Then there exists a group H and an algebra $(A, I, \Omega) \in \text{H-}\mathbf{Dec}_k$ such that $\operatorname{Miy}(A, I, \Omega) = G$.*

Proof. Let $\{r_1, \ldots, r_n\}$ be a generating set of p-regular elements of G. Define

$$H_1 \coloneqq \bigoplus_{i=1}^{n} \langle r_i \rangle$$

and set $H = \hat{H_1}$, its group of characters. Let A be the regular left kG-module, equipped with the multiplication $gh = \delta_{g,h}g$. For each $i \in \{1, \ldots, n\}$, we have an $\operatorname{Irr}(\langle r_i\rangle)$-decomposition

$$A = \bigoplus_{\chi\in\operatorname{Irr}(\langle r_i\rangle)} A^i_\chi,$$

into isotypic components for the action of r_i. Now

$$H \cong \prod_{i=1}^{n} \operatorname{Irr}(\langle r_i\rangle)$$

[1] These are matrices where there is a single 1 in each row and column and all other entries are zero.

(as either groups or group fusion laws) and thus each $\mathrm{Irr}(\langle r_i \rangle)$-decomposition of A is actually a H-decomposition (by adding zero terms). Furthermore,

$$\mathcal{X}_k(H) \cong \prod_{i=1}^{n} \mathcal{X}_k(\mathrm{Irr}(\langle r_i \rangle)) \cong \prod_{i=1}^{n} \langle r_i \rangle.$$

By assumption, all r_i are p-regular and k contains a primitive $\mathrm{o}(r_i)$-th root of unity, where $\mathrm{o}(r_i)$ is the order of r_i. It follows that (as the proof of in theorem 1.2.24), for all $i \in \{1, \dots, n\}$,

$$\langle \tau_{i,\psi} \mid \psi \in \mathcal{X}_k(H) \rangle = \langle r_i \rangle,$$

as subgroups of $\mathrm{Aut}(A)$. Hence, for $I = \{1, \dots, n\}$ and $\Omega[i] = (A^i_\chi)_{\chi \in H}$, it follows that

$$\mathrm{Miy}(A, I, \Omega) \cong G.$$ ■

We conclude that in the very general setting of decomposition algebras, we have almost no restrictions on the possibilities for the Miyamoto group.

2 Modular fusion laws

Motivated by the representation fusion law, we will investigate (known) representation-theoretic notions that help describe the tensor product of modules and their composition factors. We build up the language of the Grothendieck ring of a finite group and modular characters in the first two sections and then examine how these tools relate to the tensor products of blocks.

As in the previous chapter, algebras are not assumed to be commutative, unital or associative, unless otherwise noted.

2.1 Motivation and outline

2.1.1 Motivation and the case $k = \mathbb{C}$

Suppose we have a field k of any characteristic different from 2 and a k-algebra A with a k-vector space decomposition:

$$A = A_0 \oplus A_1.$$

If this is a $\mathbb{Z}/2$-decomposition of the algebra and $A_1 \neq 0$, then we have a nontrivial algebra automorphism τ, given by (linear extension of)

$$\tau(a) = \begin{cases} a & \text{if } a \in A_0, \\ -a & \text{if } a \in A_1. \end{cases}$$

Note that τ is precisely the Miyamoto map τ_χ determined by the unique nontrivial character $\chi\colon \mathbb{Z}/2 \to k$ (as $\operatorname{char}(k) \neq 2$, we have $1 \neq -1 \in k$).

Conversely, if we have a nontrivial involutory automorphism ψ of A, then we have a uniquely determined decomposition

$$A = A_0 \oplus A_1,$$

where

$$\begin{aligned} A_0 &= \{a \in A \mid \psi(a) = a\}, \\ A_1 &= \{a \in A \mid \psi(a) = -a\}. \end{aligned}$$

It is clear that this is a useful correspondence when investigating $\mathbb{Z}/2$-graded fusion laws and this idea is actively used in e.g. [HRS15a].

We can expand on this idea by asking which fusion laws arise from the action of an arbitrary finite group G ([DPSV20, §7]). For $k = \mathbb{C}$, the answer is given by the *representation fusion law* $(\operatorname{Irr}(G), *)$ (definition 1.2.7). Using Schur's lemma, it is straightforward to prove the following proposition.

Proposition 2.1.1 ([DPSV20, Theorem 7.2 (i)]). *Let A be a $\mathbb{C}$-algebra and let G be a finite subgroup of $\operatorname{Aut}(A)$. Then the decomposition of A into isotypic components*

$$A = \bigoplus_{\chi \in \operatorname{Irr}(G)} A_\chi$$

is an $(\operatorname{Irr}(G), *)$-decomposition of A.

This idea does not just give rise to single decompositions, but also to decomposition algebras. Take any subgroup $H \leq G \leq \operatorname{Aut}(A)$ and any tuple of elements $(g_i)_{i\in I}$ of G, for some index set I. For any $i \in I$, we then have a decomposition

$$A = g_i A = \bigoplus_{\chi\in\operatorname{Irr}(H)} g_i A_\chi.$$

As G acts by algebra automorphisms, it follows that

$$(g_i A_\chi)(g_i A_\psi) = g_i(A_\chi A_\psi).$$

Hence, this is again a $(\operatorname{Irr}(H), *)$-decomposition. We have shown the following:

Proposition 2.1.2 ([DPSV20, Theorem 7.2 (iii)]). *Let A be a $\mathbb{C}$-algebra, H a finite subgroup of $\operatorname{Aut}(A)$, and*

$$A = \bigoplus_{\chi\in\operatorname{Irr}(G)} A_\chi$$

the H-isotypic decomposition of A. Take any tuple of elements $(g_i)_{i\in I}$ of $\operatorname{Aut}(A)$ and set, for each $i \in I$,

$$\Omega[i] = (g_i A^i_\chi \mid \chi \in \operatorname{Irr}(H)).$$

Then (A, I, Ω) is an $\operatorname{Irr}(H)$-decomposition algebra.

Thus, even if we are interested in decomposition algebras, it is worthwile to examine single decompositions arising from group actions.

We conclude that the representation theory of finite groups gives rise to a large class of interesting fusion laws. They are well-behaved, due to the fact that they arise from *fusion rings* (section 2.2.3) and can furthermore be easily computed when the character table of G is known.

2.1.2 Towards modular fusion laws

The goal of this chapter is to expand the concept of a representation fusion law to positive characteristic. We wish to construct for any field k and finite group G a sensible fusion law $\mathcal{F}_{G,k}$, even when $\operatorname{char}(k) = p > 0$. Preferably, $\mathcal{F}_{G,k}$ should (just like $(\operatorname{Irr}(G), *)$) satisfy the following properties:

1. It is a generalization of the representation fusion law: when $k = \mathbb{C}$, then $\mathcal{F}_{G,\mathbb{C}} \cong (\operatorname{Irr}(G), *)$.
2. It is straightforward to compute $\mathcal{F}_{G,k}$ (possibly conditional on some knowledge of the representation theory of G).
3. If A is a k-algebra and $G \leq \operatorname{Aut}(A)$, then A admits a canonical $\mathcal{F}_{G,k}$-decomposition.

It turns out that we will be able to fulfill these three requirements simultaneously (conditional on some assumptions on k) by introducing the correct representation-theoretic notions.

To attempt to fulfill the first condition, we start in section 2.2 by giving a reformulation of $(\operatorname{Irr}(G), *)$ in terms of the *Grothendieck* ring of G. This will give rise to a representation fusion law $(S_k(G), *)$ which also makes sense when $\operatorname{char}(k) \neq 0$. Simultaneously, this illustrates the connection between the representation fusion law and the theory of $\mathbb{Z}_+$-rings ([IGNO15]). As a byproduct, we illustrate how to derive the universal grading of $\operatorname{Irr}(G)$ from this theory, following the remark in [DPSV20, Footnote 4].

Conditional on certain assumptions on k, we can associate *modular characters* to finitely generated kG-modules (section 2.3). These give rise to a character table which contains the necessary information to compute $S_k(G)$. Thus $S_k(G)$ also satisfies the second requirement.

The last remaining issue is then that not every k-algebra A will admit a natural $S_k(G)$-decomposition. By instead starting from this last requirement, we arrive in section 2.4 at a second generalization of $\mathrm{Irr}(G)$, which we call the *block fusion law* $(B(kG), *)$. This produces a fusion law that satisfies both our first and third condition. It then follows from representation theory that $(B(kG), *)$ is completely determined by $(S_k(G), *)$ and the knowledge of the composition factors of the projective indecomposable kG-modules. In other words, $(B(kG), *)$ is our desired generalization.

We now turn to introducing the relevant representation-theoretic language and connecting it to fusion laws, as outlined above.

2.2 The fusion law $(S_k(G), *)$

Throughout this section, let k be a field and G be a finite group. We define the *Grothendiek ring* $R_k(G)$ and use it to define the fusion law $S_k(G)$ on the set of isomorphism classes of simple kG-modules. The representation-theoretic results here can be found in references such as [Zim14, CR81, Ser77], often in greater generality.

2.2.1 The Grothendieck ring of a finite group

Definition 2.2.1. We denote by $R_k(G)$ the *Grothendieck group* of the category $\mathrm{Rep}_k(G)$. It is the quotient of the free abelian group on the isomorphism classes $\{M\}$ of finitely generated kG-modules by the relations

$$\{M\} = \{M'\} + \{M''\}$$

for each short exact sequence

$$0 \to M' \to M \to M'' \to 0.$$

For a kG-module M, we denote its image in $R_k(G)$ by $[M]$.

Proposition 2.2.2. *The Grothendieck group $R_k(G)$ is isomorphic to the free abelian group generated by the isomorphism classes $\{E\}$ of the simple kG-modules.*

Proof. This follows, for example from [Zim14, Proposition 2.6.2]. ■

Definition 2.2.3. Denote by $S_k(G)$ the image of isomorphism classes of simple kG-modules in $R_k(G)$:

$$S_k(G) = \{[E] \mid E \text{ is a simple } kG\text{-module}\}.$$

Lemma 2.2.2 precisely expresses that $S_k(G)$ is a basis for the $\mathbb{Z}$-module $R_k(G)$.

Proposition 2.2.4. *The image of any kG-module M in $R_k(G)$ can uniquely be written as a sum of the $[E] \in S_k(G)$:*

$$[M] = \sum_{[E] \in S_k(G)} [M : E][E].$$

Proof. Since $S_k(G)$ is a $\mathbb{Z}$-basis for $R_k(G)$, it suffices to show that the proposed equality holds. If $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_s = M$ is a composition series of some kG-module M, then we have a short exact sequence $0 \to M_{s-1} \to M \to M/M_{s-1} \to 0$. By definition of $R_k(G)$, we thus have $[M] = [M/M_{s-1}] + [M_{s-1}]$. Since $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{s-1}$ is a composition series for M_{s-1}, the result now follows by induction. ■

Lemma 2.2.5. *Let f be a map from the set of isomorphism classes $\{M\}$ of finitely generated kG-modules to some abelian group H. If, for each sort exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

it holds that $f(\{M\}) = f(\{M'\}) + f(\{M''\})$, then f induces a morphism of abelian groups

$$R_k(G) \to H \colon [M] \mapsto f(\{M\}).$$

Proof. This is an immediate consequence of the definition of $R_k(G)$ by generators and relations. ■

Proposition 2.2.6. *The product*

$$[M] \cdot [V] := [M \otimes V]$$

equips $R_k(G)$ with the structure of a commutative, unital ring.

Proof. We need to check that if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of kG-modules, then so is $0 \to M' \otimes V \to M \otimes V \to M'' \otimes V \to 0$. But we can check exactness on the level of vector spaces, where it is clear that $\cdot \otimes_k V$ is exact. Hence $[M \otimes V] = [M' \otimes V] + [M'' \otimes V] \in R_k(G)$.

By lemma 2.2.5, it then follows that $[M] \cdot [V]$ only depends on the class of $[M] \in R_k(G)$ and not on (the isomorphism class of) M. By symmetry, $[M] \cdot [V]$ then also only depends on $[V]$ and not on V. Hence, the product is well-defined, moreover it is bilinear.

Associatitivity and commutativity follow from the corresponding properties for the tensor product. Unitality follows from the fact that $k \otimes M \cong M$ for any module M, where k is the trivial kG-module. ■

The above proposition justifies calling $R_k(G)$ the *Grothendieck ring* of the category $\mathrm{Rep}_k(G)$.

2.2.2 Fusion laws from $\mathbb{Z}_+$-rings

We observe that in $R_k(G)$ the multiplication of two elements of $S_k(G)$ is always a nonnegative linear combination of such elements. This suggests a natural way of extracting a fusion law on $S_k(G)$.

There is actually a general class of rings for which such a procedure is sensible: the $\mathbb{Z}_+$*-rings*. As noted in [DPSV20, Footnote 4], results from this theory can be used to deduce the universal grading on the representation fusion law in characteristic zero.

Definition 2.2.7 ([IGNO15, Definition 3.1.1]). Let R be a ring (associative, but not necessarily unital or commutative) which is free as $\mathbb{Z}$-module.

- A $\mathbb{Z}_+$*-basis* for R is a $\mathbb{Z}$-basis $\{b_i\}_{i \in I}$ for R such that for all $i, j, k \in I$ it holds that $c_{i,j}^k \in \mathbb{Z}_+$, where the $c_{i,j}^k$ are given by
$$b_i b_j = \sum_{k \in I} c_{i,j}^k b_k.$$

- A $\mathbb{Z}_+$*-ring* R is a unital ring R, together with a distinguished $\mathbb{Z}_+$-basis $\{b_i\}_{i\in I}$ such that $1 \in R$ is a $\mathbb{Z}_+$-linear combination of the b_i.
- A *unital* $\mathbb{Z}_+$-ring R is a $\mathbb{Z}_+$-ring where $1 \in R$ is one of the basis elements.

We will use the phrase "a $\mathbb{Z}_+$-ring (R, B)" to refer to a $\mathbb{Z}_+$-ring R with basis $B = \{b_i\}_{i\in I}$.

Example 2.2.8. The Grothendieck ring $R_k(G)$ forms a $\mathbb{Z}_+$-ring with basis $S_k(G)$. Writing $S_k(G) = \{E_i\}_{i\in I}$ for some index set I, we have that

$$[E_i][E_j] = [E_i \otimes E_j] = \sum_{k\in I}[E_i \otimes E_j : E_k][E_k].$$

In other words: $c^k_{i,j} = [E_i \otimes E_j : E_k]$.

Definition 2.2.9. Let R be a $\mathbb{Z}_+$-ring with basis B. We denote by $(B, *)$ the fusion law on the set B obtained by letting $b_k \in b_i * b_j$ if and only if $c^k_{i,j} \neq 0$ in $b_ib_j = \sum_\ell c^\ell_{i,j}b_\ell$. In particular, the $\mathbb{Z}_+$-ring $R_k(G)$ defines a *representation fusion law* $(S_k(G), *)$.

Remark 2.2.10. By definition of $(S_k(G), *)$, we have that $[E] \in [E_1]*[E_2]$ if and only if $[E_1 \otimes E_2 : E] \neq 0$ (see also example 2.2.8).

Example 2.2.11. If G is an abelian group, then all simple $\mathbb{C}G$-modules are one-dimensional. Consequently, the tensor product of two simple modules is again simple and $S_\mathbb{C}(G)$ is a multiplicative subgroup of $R_\mathbb{C}(G)^\times$. Then $(S_\mathbb{C}(G), *)$ is the corresponding group fusion law.

Proposition 2.2.12. *When $k = \mathbb{C}$, the representation fusion law $(S_\mathbb{C}(G), *)$ is isomorphic to the representation fusion law of G as defined in definition 1.2.7.*

Proof. Irreducible modules E correspond to irreducible characters ϕ_E and for two irreducible modules E_1, E_2, the product $\phi_{E_1} \cdot \phi_{E_2}$ is the character of $E_1 \otimes E_2$. Thus the map $S_k(G) \to \mathrm{Irr}(G)\colon [E] \mapsto \phi_E$, sending an isomorphism class of irreducible modules to the corresponding character defines an isomorphism of fusion laws. ■

We now consider a k-algebra A on which G acts by algebra automorphisms. When $\mathrm{char}(k)$ is either zero or coprime to the order of G, then the group algebra kG is semisimple and A decomposes into a direct sum of simple kG-modules. This induces a direct sum decomposition

$$A = \bigoplus_{[E]\in S_k(G)} A_{[E]},$$

where $A_{[E]}$ consists of the sum of all submodules of A that are isomorphic to E (this is similar to the isotypic decomposition from definition 1.1.13). This is an $(S_k(G), *)$-decomposition by the definition of this fusion law.

The language of the Grothendieck ring allows us to extend this observation to the case where $\mathrm{char}(k)$ *does* divide the order of G, as long as we assume that A admits a sufficiently nice decomposition as a kG-module.

Proposition 2.2.13. *Let A be a finite-dimensional k-algebra and $G \leq \mathrm{Aut}(A)$ a finite group of automorphisms of A. Suppose that A admits a kG-module decomposition*

$$A = \bigoplus_{[E]\in S_k(G)} A_{[E]}$$

in such a way that for all $[E] \in S_k(G)$, the composition factors of $A_{[E]}$ are all isomorphic to E. Then this is an $(S_k(G), *)$-decomposition of A.

Proof. Let $[E_1], [E_2] \in S_k(G)$ be arbitrary. Consider the multiplication map $m : A_{[E_1]} \otimes A_{[E_2]} \to A$. By assumption, the multiplication in A is G-equivariant. Hence, m belongs to $\mathrm{Hom}_G(A_{[E_1]} \otimes A_{[E_2]}, A)$. Since $S_k(G)$ is a finite set, we have a natural isomorphism

$$\mathrm{Hom}_G(A_{[E_1]} \otimes A_{[E_2]}, A) \cong \bigoplus_{[E] \in S_{k(G)}} \mathrm{Hom}_G(A_{[E_1]} \otimes A_{[E_2]}, A_{[E]}).$$

Thus it suffices to show that $\mathrm{Hom}_G(A_{[E_1]} \otimes A_{[E_2]}, A_{[E]}) = 0$ whenever $[E] \notin [E_1] * [E_2]$.

So let $[E] \in S_k(G)$ be such that $[E] \notin [E_1] * [E_2]$ and let $f \in \mathrm{Hom}_G(A_{[E_1]} \otimes A_{[E_2]}, A_{[E]})$. We show that $\mathrm{im}(f) = 0$.

We have two short exact sequences:

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{im}(f) \arrow[r] & A_{[E]} \arrow[r] & A_{[E]}/\,\mathrm{im}(f) \arrow[r] & 0 \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r] & \ker(f) \arrow[r] & A_{[E_1]} \otimes A_{[E_2]} \arrow[r] & \mathrm{im}(f) \arrow[r] & 0 \end{tikzcd}$$

These sequences respectively imply that in $R_k(G)$

1. $[\mathrm{im}(f)] = [\mathrm{im}(f) : E][E]$, and
2. $[A_{[E_1]} \otimes A_{[E_2]}] = [\mathrm{im}(f)] + [\ker(f)]$.

If $[\mathrm{im}(f)] \neq 0$, then $[E]$ would appear with a nonzero coefficient in the expansion of $[A_{[E_1]} \otimes A_{[E_2]}]$ with respect to the basis $S_k(G)$. Since $[A_{[E_1]} \otimes A_{[E_2]}]$ is a scalar multiple of $[E_1 \otimes E_2]$, this contradicts the assumption $[E] \notin [E_1] * [E_2]$. Thus $[\mathrm{im}(f)] = 0$, and hence also $\mathrm{im}(f) = 0$. ■

Remark 2.2.14. The assumption of proposition 2.2.13 requires that A admits a kind of 'isotypic decomposition'. Such a decomposition can certainly exist even when A is not semisimple as a kG-module.

Consider, for example, a field k of characteristic p and a direct product $G = C_q \times H$ with q a power of p and the order of H coprime to p. Then, as $kG \cong kC_q \otimes_k kH$ as k-algebras, it is readily seen that the projective indecomposable kG-modules are given by $kC_q \otimes E$, where E is a simple kH-module. As $kC_q \cong k[x]/(x^q - 1) \cong k[y]/(y^q)$ is uniserial, so are the kG-modules $kC_q \otimes_k E$. All their composition factors are then isomorphic to $k \otimes_k E$. Hence

$$A = \bigoplus_{[E] \in S_k(H)} kC_q \otimes_k E,$$

satisfies the hypothesis of the above proposition 2.2.13 (for any choice of multiplication), but is not semisimple.

On the other hand, if $G = C_q \rtimes H$ and this product is not direct, then a decomposition as in proposition 2.2.13 can only exist if A is semisimple kG-module. This will follow from propositions 2.4.13 and 2.4.15, two representation-theoretic facts that we will also use when examining the block fusion law in section 2.4.

2.2.3 Universal grading of a fusion ring

As an immediate application of the language of the Grothendieck ring, we illustrate how the universal grading of the representation fusion law in characteristic zero can be derived from the theory of *fusion categories*, as indicated in [DPSV20, Footnote 4]. The essential ingredient is [GN08, Theorem 3.5], which describes the universal grading of a *fusion ring*. It turns out that $R_{\mathbb{C}}(G)$ indeed has the structure of a fusion ring, and from this we derive a conceptual proof of the universal grading of $(S_{\mathbb{C}}(G), *)$.

This section follows the original arguments given in [GN08], but uses the terminology of the textbook [IGNO15]. The main difference is that the former requires *based rings* to be of finite rank, while the latter calls these *multifusion rings*.

As in section 2.2.2, we will use (R, B) to denote a $\mathbb{Z}_+$-ring R with fixed basis $B = \{b_i\}_{i \in I}$ (definition 2.2.7).

Definition 2.2.15 ([GN08, §2]). Let R be a $\mathbb{Z}_+$-ring with basis $\{b_i\}_{i \in I}$. Define the *inner product* $(\cdot, \cdot)$ on R by $\mathbb{Z}$-linearly extending

$$(b_i, b_j) = \delta_{i,j},$$

were $\delta_{i,j}$ is the Kronecker delta. For $b_i \in B$ and a $\mathbb{Z}_+$-linear combination of basis elements $a \in R$, we say that "b_i is contained in a" when $(b_i, a) > 0$.

Definition 2.2.16 ([GN08, Definition 2.1]). A $\mathbb{Z}_+$-ring (R, B) is called a *based ring* if

1. there exists some finite subset $I_0 \subseteq I$ such that $1 = \sum_{i \in I_0} b_i$, and
2. there exists an involution $*\colon I \to I$, such that for the map $*\colon R \to R$, induced by $b_i \mapsto b_{i^*}$, it holds that
$$(x, zy^*) = (xy, z) = (y, x^* z).$$

A based ring is

- *unital* if it is unital as a $\mathbb{Z}_+$-ring: $1 \in B$.
- a *multifusion ring* if it is of finite $\mathbb{Z}$-rank.
- a *fusion ring* if it is a unital multifusion ring.

Lemma 2.2.17. *The map $*$ as defined in definition 2.2.16 is an anti-involution of the ring R.*

Proof. For all $x, y \in R$ and $b_i \in B$ it holds that

$$(b_{i^*}, y^* x^*) = (xy, b_i) = (b_{i^*}, (xy)^*).$$ ■

Definition 2.2.18 ([GN08, §2]). A *(left) $\mathbb{Z}_+$-module* over a $\mathbb{Z}_+$-ring (R, B) consists of an R-module M, free over $\mathbb{Z}$, together with a $\mathbb{Z}$-basis $\{m_j\}_{j \in J}$ such that when

$$b_i m_j = \sum_{k \in J} d_{i,j}^k m_k,$$

then $d_{i,j}^k \in \mathbb{Z}_+$, for all $i \in I$ and $j, k \in J$.

If (R, B) is additionally a based ring, then the $\mathbb{Z}_+$-module M is a *based module* over R if

$$d_{i,j}^k = d_{i^*,k}^j$$

for all $i \in I$ and $j, k \in J$. In other words, the action of b_{i^*} is given by the transpose of the action of b_i.

Remark 2.2.19. Note that a based ring is a based module over itself. Indeed, we have

$$c_{i,j}^{k} = (b_i b_j, b_k) = (b_j, b_i^* b_k) = c_{i^*,k}^{j}.$$

Definition 2.2.20 ([GN08, §2]). Let (R, B) be a $\mathbb{Z}_+$-ring and M a $\mathbb{Z}_+$-module over R, with basis $\{m_j\}_{j\in J}$.

- A ($\mathbb{Z}_+$-)*submodule* N of M is a free $\mathbb{Z}$-submodule of M, with $\mathbb{Z}$-basis $\{m_k\}_{k\in J_1} \subseteq \{m_j\}_{j\in J}$ such that $RN \subseteq N$.
- A nonzero R-module M is called *simple* or *irreducible* if it has no $\mathbb{Z}_+$-submodules other than 0 and itself.
- Given a set of submodules $\{N_s\}_{s\in S}$ of M with bases $\{B_s\}_{s\in S}$, we say that M is the *direct sum* of the N_s if B is the disjoint union of the B_s. We write $M = \bigoplus_{s\in S} N_s$
- As for $\mathbb{Z}_+$-rings, write $(\cdot,\cdot)$ for the *inner product* on M defined by linear extension of $(m_i, m_j) = \delta_{i,j}$.

Remark 2.2.21. We will prefer the term *irreducible* $\mathbb{Z}_+$*-module* here, as we will want to apply this theory to the Grothendieck ring of a finite group, which is spanned by isomorphism classes of *simple* kG-modules.

Lemma 2.2.22 ([Ost03, Lemma 1]). *Let (R, B) be a based ring. Any based R-module M can be written as a uniquely determined direct sum of its irreducible submodules.*

Proof. We first show that if $N_1 \subseteq M$ is a based submodule with basis $\{m_j\}_{j\in J_1}$, then $M = N_1 \oplus N_2$, with N_2 the free $\mathbb{Z}$-submodule of M with basis $\{m_j\}_{j\in J\setminus J_1}$. Indeed, for all $i \in I$, $j_1 \in J_1$ and $j_2 \in J \setminus J_1$, we have

$$(b_i m_{j_2}, m_{j_1}) = (m_{j_2}, b_{i^*} m_{j_1}) = 0.$$

Existence of a decomposition then follows by a standard application of Zorn's lemma.

We now turn to uniqueness. Take two submodules N_1, N_2 of M, with respective $\mathbb{Z}$-bases $\{m_j\}_{j\in J_1}$ and $\{m_j\}_{j\in J_2}$. Then the free $\mathbb{Z}$-submodule $N_1 \cap N_2$, generated by $\{m_j\}_{j\in J_1\cap J_2}$ is also a based submodule of M. Thus, given any two decompositions into irreducible submodules $\bigoplus_{s\in S} N_s$ and $\bigoplus_{t\in T} V_t$ of M, then also $M = \bigoplus_{(s,t)\in S\times T} N_s \cap V_t$. Let $(s,t) \in S \times T$ be such that $N_s \cap V_t \neq 0$. If $N_s \cap V_t \neq N_s$, then N_s would not be irreducible. Hence N_s and V_t must contain the same basic elements of M and thus $N_s = V_t$. By symmetry in S and T, it follows that there exists a bijection $\beta\colon S \to T$ such that $N_s = V_{\beta(s)}$. ■

Definition 2.2.23 ([GN08, Definition 3.1]). The *adjoint subring* R_{ad} of a fusion ring (R, B) is the smallest based subring which contains all products of the form $b_{i^*} b_i$. Equivalently, define $I(1) := \sum_{i\in I} b_{i^*} b_i$. Then R_{ad} is the $\mathbb{Z}$-linear span of basic elements contained in $I(1)^n$ for some $n \in \mathbb{N}$.

Remark 2.2.24. Let R be a based unital ring. Then R is naturally a left R_{ad}-module and we can consider the deocomposition of R into irreducible left R_{ad}-submodules:

$$R = \bigoplus_{x\in U} R_x.$$

The next part of this section is devoted to showing that U is a group and the above decomposition is the *universal grading* of R.

Definition 2.2.25 ([GN08, §2]). A *grading* of a based ring (R, B) by a group G is a partition $\{B_g\}_{g\in G}$ of B such that, for the $\mathbb{Z}$-submodules R_g generated by B_g, it holds that

1. for all $g, h \in G$: $R_g R_h \subseteq R_{gh}$ and
2. for all $g \in G$: $(R_g)^* = R_{g^{-1}}$.

A grading of (R, B) by G is *universal*, if for each other grading of (R, B) by some group H, there exists a unique morphism $\pi \colon G \to H$ such that

$$B_h = \bigcup_{g\in\pi^{-1}(h)} B_g.$$

Lemma 2.2.26. *The gradings of a fusion ring (R, B) correspond bijectively to those of the fusion law $(B, *)$.*

Proof. If $R = \bigoplus_{g\in G} R_g$ is a grading of G, then we define a grading $\alpha \colon B \to G$ by

$$\alpha(b) = g \text{ if } b \in R_g.$$

Conversely, if $\alpha \colon B \to G$ is a grading of $(B, *)$, then we define a partition $\{B_g\}_{g\in G}$ of B by:

$$B_g = \{b \in B \mid \alpha(b) = g\}.$$

The first condition of a grading is then certainly satisfied. Now take any $g \in G$ and $b \in B_g$. Now $(b, b) = 1$, whence $(bb^*, 1) = 1$. As 1 is a basic element of R, this implies that $1 \in R_1$ is contained in bb^*. Then b^* must belong to $R_{g^{-1}}$. ■

Lemma 2.2.27. *Let R be a fusion ring with basis B. If*

$$R = \bigoplus_{g\in G} R_g$$

is a grading of R, then each R_g is an irreducible (left) R_1-module.

Proof. Let $g \in G$ and take any $b_1, b_2 \in B \cap R_g$. Then $b_1 b_2^* \in R_1$. Hence, there is some $b \in B \cap R_1$ such that $(b_1 b_2^*, b) > 0$. But then $(b_1, bb_2) > 0$, implying that b_1 is contained in the R_1-submodule generated by b_2. As b_1, b_2 were arbitrary, it follows that R_g is an irreducible (left) R_1-module. ■

Lemma 2.2.28 ([GN08, Proposition 3.3]). *Let (R, B) be a multifusion ring. The element $I(1) = \sum_{i\in I} b_{i^*} b_i$ is central in R.*

Proof. We compute that, for all $b_j \in B$,

$$\begin{aligned}
\sum_{i\in I} b_j b_{i^*} b_i &= \sum_{i,k\in I} (b_j b_{i^*}, b_k) b_k b_i \\
&= \sum_{i,k\in I} b_k((b_{k^*} b_j, b_i) b_i) \\
&= \sum_{k\in I} b_k b_{k^*} b_j \\
&= \sum_{k\in I} b_{k^*} b_k b_j.
\end{aligned}$$

The lemma now follows, as R is a free $\mathbb{Z}$-module with basis B. ■

Proposition 2.2.29 ([GN08, Proposition 3.3]). *Each left R_{ad}-submodule of a multifusion ring $(R, B)$is an R_{ad}-subbimodule. In particular, an R_{ad}-subbimodule of R is indecomposable if and only if it is indecomposable as a left R_{ad}-submodule.*

Proof. We first prove that the left R_{ad}-submodules of R are precisely the $\mathbb{Z}$-submodules which are free on a subset of B and that are closed under multiplication with $I(1)^n$, for all $n \in \mathbb{N}$. Let M be a left R_{ad}-submodule of R. Then we have in particular that $I(1)^n M \subseteq M$. Conversely, let $M \subseteq R$ be a $\mathbb{Z}$-submodule spanned by certain basis elements $\{b_j\}_{j \in J}$ and assume $I(1)^n m \in M$ for all $m \in M$ and $n \in \mathbb{N}$. Then also $bb_j \in M$ for all for all basis elements b contained in some $I(1)^n$ and all $j \in J$, as R is a $\mathbb{Z}_+$-ring.

By symmetry, the analogous claim holds for right R_{ad}-modules as well. Thus, to prove the proposition, it now suffices to show that $MI(1)^n \subseteq M$ for any left R_{ad}-submodule M of R. But this follows since $I(1)^n M = MI(1)^n$ by the above lemma 2.2.28. ■

Theorem 2.2.30 ([GN08, Theorem 3.5]). *Let R be a fusion ring with basis $\{b_i\}_{i \in I}$. Let $R = \bigoplus_{x \in U} R_x$ be a direct sum decomposition of R into irreducible R_{ad}-bimodules. Then*

1. *There is an element $1 \in U$ such that $R_1 = R_{ad}$.*
2. *For all $x \in U$, it holds that $R_x(R_x)^* \subseteq R_{ad}$,*
3. *If $x, y \in U$, then there is a unique $z \in U$ such that $R_x R_y \subseteq R_z$.*

Thus the rule

$$xy = z \iff R_x R_y \subseteq R_z$$

defines a group structure on U and $R = \bigoplus_{x \in U} R_x$ is a grading of R.

Proof. 1. Since 1 is a basic element and $1(1^*) = 1$, it follows that $1 \in R_{ad}$. Then also $I(1)^n \in R_{ad}$ for all $n \in \mathbb{N}$. Thus the smallest R_{ad}-submodule of R containing 1, is R_{ad} itself. By unique decomposition of based modules (lemma 2.2.22) it then follows that R_{ad} is an irreducible based module over itself.

2. Let b_i be a basic element of R_x. Consider the $\mathbb{Z}$-module M generated by all the basic elements contained in $I(1)^n b_i$ ($n \in \mathbb{N}$). Since M is a nonzero R_{ad}-submodule of the irreducible module R_x, it follows that $M = R_x$. It thus suffices to check that for all $n, m \in \mathbb{N}$, we have

$$I(1)^n b_{i^*} I(1)^m b_i \in R_{ad}.$$

   This is immediate since $I(1)$ is central in R and $b_{i^*} b_i \in R_{ad}$ by definition.

3. Let $b_i \in R_x$ and $b_j \in R_y$ be basic elements. Suppose we have $b_k \in R_z$ and $b_\ell \in R_v$ with $z \neq v$ and such that both b_k and b_ℓ are contained in $b_i b_j$. Then $(b_i b_j)^*(b_i b_j)$ contains $b_{k^*} b_l$ and hence $b_{k^*} b_l \in R_{ad}$. But this implies that $b_k(b_{k^*} b_\ell) \in R_z$ (as R_z is a right R_{ad}-module). However, we also have $(b_k b_{k^*}) b_\ell \in R_v$ (as R_v is a left R_{ad}-module). Thus $b_k b_{k^*} b_\ell = 0$. We now remark that $1 = (b_k, b_k) = (b_k b_{k^*}, 1)$. Hence, 1 is contained in $b_k b_{k^*}$ (recall that R is a fusion ring and thus $1 \in B$). In particular $b_k b_{k*} b_\ell \neq 0$, a contradiction.

   Hence, $b_i b_j \in R_z$ for a $z \in U$. To see that $R_x R_y \subseteq R_z$, it again suffices to only check products of elements of the form $I(1)^n b_i$ and $I(1)^m b_j$. This follows from the above paragraph, by again using that that $I(1) \in Z(R) \cap R_{ad}$. ■

Corollary 2.2.31 ([GN08, Corollary 3.7]). *For any fusion ring (R, B), the grading constructed in 2.2.30 is universal.*

Proof. Let G be a group such that $\bigoplus_{g\in G} R^g$ is a grading of R and write $R = \bigoplus_{x\in U} R_x$ for the grading constructed in theorem 2.2.30. For each $b_i \in B$, we have $b_{i^*}b_i \in R^1$. Thus $R_{ad} \subseteq R^1$. Since $R^1R^g \subseteq R^g$ for all g, it follows that all R^g are R_{ad}-modules. By the unique decomposition of based modules (lemma 2.2.22), each R_x thus has a unique $R^{\pi(x)}$ of which it is a direct summand. It is then clear that $\pi\colon U \to G$ is the unique morphism of groups for which $R^g = \bigoplus_{x\in\pi^{-1}(g)} R_x$. ■

We now apply this description of the universal grading to the deduce the universal grading of the representation fusion law (proposition 1.2.15).

Lemma 2.2.32. *The $\mathbb{Z}_+$-ring $(R_\mathbb{C}(G), S_\mathbb{C}(G))$ is a fusion ring.*

Proof. It is clear that $(R_\mathbb{C}(G), S_\mathbb{C}(G))$ is of finite $\mathbb{Z}$-rank and unital. We claim that the required involution is given by taking the dual of the underlying modules:

$$[M]^* := [M^*].$$

Let E_1, E_2, E_3 be simple $\mathbb{C}G$-modules. We need to verify that

$$[E_1 \otimes E_2 : E_3] = [E_3 \otimes E_2^* : E_1].$$

Write χ_{E_i} for the character afforded by E_i ($i = 1, 2, 3$). Since $\chi_{E_2^*}(g) = \chi_{E_2}(g^{-1})$ (proposition 1.1.18), it indeed follows that (corollary 1.1.17)

$$\begin{aligned}[E_1 \otimes E_2 : E_3] &= \frac{1}{|G|}\sum_{g\in G}(\chi_{E_1}\chi_{E_2})(g)\chi_{E_3}(g^{-1}) \\ &= \frac{1}{|G|}\sum_{g\in G}(\chi_{E_3}\chi_{E_2^*})(g^{-1})\chi_{E_1}(g) \\ &= [E_3 \otimes E_2^* : E_1].\end{aligned}$$

■

Lemma 2.2.33. $(R_\mathbb{C}(G))_{ad} = R_\mathbb{C}(G/Z(G))$.

Proof. Note that $R_\mathbb{C}(G)_{ad}$ is a subring of $R_\mathbb{C}(G)$ by definition and that $R_\mathbb{C}(G/Z(G))$ can be identified with a subring of $R_\mathbb{C}(G)$ via the surjection $\mathbb{C}G \twoheadrightarrow \mathbb{C}(G/Z(G))$.

As $Z(G)$ is abelian, all simple $\mathbb{C}Z(G)$-modules are one-dimensional and $Z(G)$ acts by by multiplication with a certain root of unity. Then, by Clifford's theorem 1.1.10, $Z(G)$ acts trivially on $E \otimes E^*$ whenever E is a simple $\mathbb{C}G$-module. Hence it follows that $(R_\mathbb{C}(G))_{ad} \subseteq R_\mathbb{C}(G/Z(G))$.

For the converse inclusion, consider the permutation representation V, given by the conjugation action of G on itself. By proposition 1.1.19 this permutation module is given by

$$V \cong \bigoplus_{[E]\in S_k(G)} E \otimes E^*.$$

As this is a faithful representation of $G/Z(G)$, it follows from the Burnside-Brauer theorem ([CR81, Theorem 9.34]) that each finite-dimensional representation of $G/Z(G)$ is contained in a tensor power of V. Hence $R_\mathbb{C}(G/Z(G)) \subseteq (R_\mathbb{C}(G))_{ad}$. ■

Theorem 2.2.34. *The universal grading of $(S_\mathbb{C}(G), *)$ is given by the map*

$$S_\mathbb{C}(G) \to S_\mathbb{C}(Z(G))\colon [E] \mapsto [S] \quad \textit{if } S \textit{ is a simple submodule of } E{\downarrow}^G_{Z(G)}.$$

Proof. Recall that $(S_{\mathbb{C}}(Z(G)), *)$ is a group fusion law, as $Z(G)$ is abelian (example 2.2.11). Write $R = R_{\mathbb{C}}(G)$. For each $[S] \in S_{\mathbb{C}}(Z(G))$, write R_S for the $\mathbb{Z}$-submodule of R spanned by the isomorphism classes of the simple kG-modules E, for which $E{\downarrow}^G_{Z(G)}$ contains a submodule isomorphic to S (each $[E]$ then belongs to a unique R_S by corollary 1.1.11). Then

$$R = \bigoplus_{[S] \in S_{\mathbb{C}}(G)} R_S$$

is an $S_{\mathbb{C}}(G)$-graded decomposition of R. As $R_1 = R(G/Z(G)) = R_{ad}$ by lemma 2.2.33, it follows by lemma 2.2.27 and corollary 2.2.31 that this is the universal grading of R. This implies that the corresponding map $(S_{\mathbb{C}}(G), *) \to (S_{\mathbb{C}}(Z(G)), *)$, identifying the basic elements of R which belong to a common R_S, is indeed the universal grading of $(S_{\mathbb{C}}(G), *)$ (lemma 2.2.26). ■

Remark 2.2.35. It may seem at a first glance that the above proof would also work for, say algebraically closed fields[1] of characteristic $p > 0$. The obstruction to this hides in lemma 2.2.32. There we (crucially) relied on character-theoretic methods to show that $R_{\mathbb{C}}(G)$ is a based ring. When $k \neq \mathbb{C}$, it is possible that there exists some simple kG-module E such that

$$[E \otimes E^* : 1] \neq 1 = [E : E],$$

which means $R_k(G)$ does not satisfy the second condition of definition 2.2.16.

An illustration of this phenomenon can be seen in the examples of the next section, where we compute tensor products using modular characters (examples 2.3.26 and 2.3.28). For example, when $G = D_6$ and $\mathrm{char}(k) = 2$, then it is seen from example 2.3.26 that the unique two-dimensional simple module E has the property that

$$[E \otimes E^* \colon k] = [E \otimes E \colon k] = 2 > 1.$$

On the other hand, $R_k(G)$ *can* still be a fusion ring in certain cases. For example, take $G = D_6$ and $\mathrm{char}(k) = 3$. Then $R_k(G) \cong \mathbb{Z}C_2$ and $(S_k(D_6), *)$ is simply the group fusion law C_2 (example 2.3.27).

2.3 Modular characters

2.3.1 Definition and relation to $R_k(G)$

Theorem 2.2.13 gives an abstract description of the fusion law that exists on an algebra A as soon as it is "close to" a semisimple representation of some finite subgroup G of $\mathrm{Aut}(A)$. However, it leaves open the question of how one could compute the resulting fusion law. In this subsection, we turn to *modular characters* to obtain a more concrete description of tensor products of simple modules and hence of this fusion law in positive characteristic. The exposition in this section is primarily based on that of Serre in [Ser77, Chapter 18]. However, he does not explicitly use the term *p-modular system*, terminology which we borrow from [CR81].

Recall that when $k = \mathbb{C}$, we can associate a *character* to each linear representation of G: a map $G \to k$, constant on each conjugation class of G. Such a character uniquely determines the isomorphism class of the representation. We now fix a prime p. When k is a field of characteristic $p > 0$, a similar statement is possible, conditional on the existence of a good *p-modular system*.

We first recall the definition of a discrete valuation and a discrete valuation ring.

[1] This assumption guarantees that all simple $kZ(G)$-modules are one-dimensional.

Definition 2.3.1. Let K be a field and $K^\times$ its multiplicative group. A *discrete valuation* ν on K is a map

$$\nu\colon K \to \mathbb{Z} \cup \{\infty\}$$

such that $\nu(K^\times) = \mathbb{Z}$ and for all $a, b \in K$

- $\nu(a) = \infty$ if and only if $a = 0$,
- $\nu(ab) = \nu(a) + \nu(b)$ and
- $\nu(a + b) = \min(\nu(a), \nu(b))$,

where we define $a \leq \infty$ and $a + \infty = \infty + a = \infty$ for all $a \in \mathbb{Z}$.

Definition 2.3.2. Let R be a domain, we call R a *discrete valuation ring* if there exists a discrete valuation ν on its field of fractions K such that

$$R = \{a \in K \mid \nu(a) \geq 0\}.$$

We call R a *complete* discrete valuation ring if K is complete with respect to the metric

$$d(a, b) = 2^{-\nu(a-b)}.$$

Any discrete valuation ring R has a unique maximal ideal $\mathfrak{m}$, given by

$$\mathfrak{m} = \{a \in R \mid \nu(a) > 0\}.$$

See also [Zim14, §2.5.1] for more details.

Definition 2.3.3. A *p-modular system* is a triple (K, R, k), where

- R is a discrete valuation ring (DVR) with unique maximal ideal $\mathfrak{m}$, such that
- its fraction field $K = \mathrm{Frac}(R)$ has characteristic zero, and
- its residue field $R/\mathfrak{m} = k$ has characteristic p.

Example 2.3.4. For any prime number p, we can consider the ring $R = \mathbb{Z}_p$ of p-adic integers. Its fraction field is equal to the p-adic numbers $K = \mathbb{Q}_p$ and its quotient field is given by $\mathbb{Z}_p/(p) \cong \mathbb{F}_p$. It can be shown ([CR81, Proposition 16.21]) that for any finite field extension K' of K we have a new p-modular system: (K', R', k'). Concretely, we can extend the valuation ν on K to a valuation ν' on K'. Then R' is simply the valuation ring of K' and $k' = R'/\mathfrak{m}'$, for the unique maximal ideal $\mathfrak{m}'$ of R'. In particular, consider an extension of $\mathbb{Q}_p$ by some m-th root of unity, with m such that $p \nmid m$. Then, by adapting lemma 2.3.5 below, we see that k' is the extension of $\mathbb{F}_p$ by the "same" root of unity.

Note that in all these examples R is *complete*. See also [Zim14, Proposition 2.5.9] which states that for any perfect field k of characteristic p, there exists a p-modular system (K, R, k) such that R is complete.

Lemma 2.3.5. *Let (K, R, k) be a p-modular system and let m be coprime to p. Denote by μ_K (resp. μ_k) the multiplicative group of m-th roots of unity in K (resp. k). Then $\mu_K \subseteq R$ and the quotient map $R \to k$ induces an isomorphism $\mu_K \cong \mu_k$.*

Proof. Denote by ν the valuation map on K and let ζ be an m-th root of unity of K. From $\zeta^m = 1$, it follows that $m\nu(\zeta) = 0$. Hence $\zeta \in R \subseteq K$. Suppose now that ζ_1, ζ_2 are two different m-th roots of unity whose images $\widetilde{\zeta_1}, \widetilde{\zeta_2}$ under $R \mapsto k$ coincide. This would imply that $\zeta_2 - \zeta_1 = a$, for some $a \in R$ with $\nu(a) > 0$ (as $\mathfrak{m} = \{a \in R \mid \nu(a) > 0\}$). Multiplying by ζ_2^{-1}, we may assume $1 - \zeta_1 = a$. The equality

$$(1-a)^m = \zeta_1^m = 1,$$

implies that

$$\sum_{i=0}^{m} (-a)^i \binom{m}{i} = 1.$$

And hence

$$ma = \binom{m}{2}(-a)^2 + \binom{m}{3}(-a)^3 + \cdots + (-a)^m.$$

As $m \in R^\times$, it follows that $\nu(ma) = \nu(a) \in \mathbb{Z}_{>0}$. By applying ν to the right-hand side, it then follows that

$$\nu(a) \geq \min_{i=2}^{m}(i\nu(a)) > \nu(a),$$

a contradiction. ■

Notation 2.3.6. As in the previous sections, we denote by G some finite group. In order to define modular characters, we fix some p-modular system (K, R, k). For simplicity, we will always assume that K is sufficiently large with respect to G.

Remark 2.3.7. Recall that the K-characters of G may be identified with the complex characters of G by theorem 1.1.21 (up to some identification of the roots of unity in K and $\mathbb{C}$). As such, we will not actively distinguish between the two in the rest of this text.

The trick of modular characters is that, for a given p-modular system, we are still able to define useful class functions on a subset of G. Just like complex characters, they characterize the composition series of a given kG-module, but as kG is not semisimple (in general) this information does not (always) determine an isomorphism class of kG-modules.

Definition 2.3.8. An element $g \in G$ is *p-regular* if its order is not divisible by p. The set of all p-regular elements of G is denoted by G_{reg}.

Definition 2.3.9. Let M be a finitely generated kG-module and let $n = \dim_k(M)$. Take any p-regular element $g \in G$. Left multiplication by g induces an automorphism g_M of the vector space M. Since the order of g is coprime to p, it follows that g_M is diagonalizable (see e.g. Maschke's theorem 1.1.5). Let $(\widetilde{\lambda_1}, \ldots, \widetilde{\lambda_n})$ be the eigenvalues of g_M (counted with multiplicities). These scalars all belong to μ_k. Now let $(\lambda_1, \ldots, \lambda_n)$ be their lifts to μ_K (lemma 2.3.5). We set

$$\phi_M(g) = \sum_{i=1}^{n} \lambda_i.$$

This procedure defines a function $\phi_M : G_{\text{reg}} \to R \subseteq K$, which is called the *modular character* or *Brauer character* of M.

Remark 2.3.10. We will illustrate how modular characters can be used to compute the tensor product of kG-modules and hence the fusion law $(S_k(G), *)$. The requirement for there to be a p-modular system (K, R, k), with K sufficiently large with respect to G, may seem restrictive in this regard. However, following example 2.3.4, such a p-modular system (with additionally R complete) exists whenever k is a finite field containing all m-th roots of unity, where m is the l.c.m. of the orders of the p-regular elements of G. Hence they are actually applicable to many situations.

Proposition 2.3.11. *The modular characters of G satisfy the following properties:*

1. *ϕ_M is a* class function *on G_{reg}: for all $g \in G_{reg}$ and $h \in G$, it holds that $\phi_M(hgh^{-1}) = \phi(g)$.*
2. *If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence, then $\phi_M = \phi_{M'} + \phi_{M''}$. In particular, $\phi_M = \sum_{[E] \in S_k(G)} [M : E]\phi_E$.*
3. *The modular character of $M_1 \otimes M_2$ is given by the product $\phi_{M_1}\phi_{M_2}$.*

Proof. The arguments for these facts are given in [Ser77, §18.1]. Also note the similarity with proposition 1.1.12. ■

Corollary 2.3.12. *The map assigning to each $[M] \in R_k(G)$ the modular character ϕ_M determines a morphism of rings to the space of class functions on G_{reg} with values in K.*

Proof. This follows immediately from the above proposition 2.3.11 and the definition of $R_k(G)$ by generators and relations. ■

Theorem 2.3.13. *The tuple $(\phi_E \mid [E] \in S_k(G))$ is a basis of the K-vector space of class functions on G_{reg} with values in K.*

Proof. A proof can be found in [Ser77, Theorem 42]. ■

Corollary 2.3.14. *Each simple kG-module E is characterized, up to isomorphism, by its modular character. Furthermore, two finitely generated modules M and M' have isomorphic composition factors if and only if their modular characters are equal.*

Proof. The first statement follows from the second. From proposition 2.3.11 it follows that two modules with isomorphic composition factors have the same modular character. The converse follows from theorem 2.3.13. ■

We call a modular character ϕ_E *irreducible* when E is a simple kG-module.

Corollary 2.3.15. *Let $\mathrm{Irr}_p(G)$ be the set of all irreducible modular characters of G. Consider the $\mathbb{Z}$-span of $\{\phi_E \mid E$ is a simple kG-module$\}$ in the vector space of class functions on G_{reg} with values in K. This is a $\mathbb{Z}_+$-ring for the basis $\mathrm{Irr}_p(G)$ and the induced fusion law (definition 2.2.9) $(\mathrm{Irr}_p(G), *)$ is isomorphic to $(S_k(G), *)$.*

Proof. We first notice that $\phi_{E_1}\phi_{E_2}$ is a $\mathbb{Z}_+$-linear combination of the elements of $\mathrm{Irr}_p(G)$. Indeed,

$$\phi_{E_1}\phi_{E_2} = \phi_{E_1 \otimes E_2} = \sum_{[E] \in S_k(G)} [E_1 \otimes E_2 : E]\phi_E$$

by proposition 2.3.11. This formula also shows that the bijection $S_k(G) \to \mathrm{Irr}_p(G) : [E] \mapsto \phi_E$ from corollary 2.3.14 extends to an isomorphism of $\mathbb{Z}_+$-rings. In particular, the induced fusion laws $(S_k(G), *)$ and $(\mathrm{Irr}_p(G), *)$ are isomorphic. ■

2.3.2 The Cartan-Brauer triangle

We now introduce the Cartan-Brauer triangle and illustrate how it can be used to extract information on the modular characters from the complex characters. Full proofs and context for the representation-theoretic facts mentioned here can be found in [Ser77, Part III]. Consistent with notation 2.3.6, we denote by (K, R, k) a fixed p-modular system, with K sufficiently large with respect to some fixed finite group G. We write $\mathfrak{m}$ for the unique maximal ideal of R. For this part, we will need R to be a *complete* discrete valuation ring.

Definition 2.3.16. For any ring Λ, denote by $P_\Lambda(G)$ the free abelian group on the isomorphism classes of indecomposable projective ΛG-modules.

Proposition 2.3.17. *If R is complete, then we have an isomorphism $P_R(G) \cong P_k(G)$, induced by sending a projective RG-module P onto its reduction modulo $\mathfrak{m}$, given by $P/\mathfrak{m}P$.*

Proof. A proof can be found in [Ser77, Proposition 42,Corollary 3]. The essence of the proof is that R is a *complete* discrete valuation ring. This allows one to lift the primitive idempotents of kG to RG (and these idempotents are in bijection with isomorphism classes of indecomposable kG-modules). ■

Definition 2.3.18. We define the *Cartan map*

$$c\colon P_k(G) \to R_k(G)\colon [P] \mapsto [P] = \sum_{[E] \in S_k(G)} [P : E][E],$$

induced by mapping (the isomorphism classes of) the projective indecomposable kG-modules to the sum of their composition factors.

Theorem 2.3.19. *Suppose that R is a complete discrete valuation ring. Then there exist two maps d and e that, together with c, form a commutative triangle of abelian groups, called the Cartan-Brauer triangle:*

$$\begin{tikzcd}
P_k(G) \cong P_R(G) \arrow[rr, "c"] \arrow[dr, "e"'] & & R_k(G) \\
& R_K(G) \arrow[ur, "d"'] &
\end{tikzcd},$$

where additionally $E = D^T$, for the matrix representations of e, d with respect to the following bases

- *$\{[P_E] \mid P_E$ is the projective cover of E, for $[E] \in S_k(G)\}$ for $P_k(G)$,*
- *$S_K(G)$ for $R_K(G)$,*
- *$S_k(G)$ for $R_k(G)$.*

Proof. The full arguments are given throughout [Ser77, Chapter 15]. The results quoted here are stated in [Ser77, §15.4]. ■

Remark 2.3.20.

- The map e is induced by sending a projective RG-module P to the KG-module $K[G] \otimes_{R[G]} P$. This last module simply arises by *extension of scalars* from R to K. As P is projective over RG and RG is a free R-module, it follows that $P{\downarrow}_1^G$ is a projective R-module. As R is a PID, P is then free over R. Thus if $e_1, \dots, e_n$ is a basis of P over R, then $1 \otimes e_1, \dots 1 \otimes e_n$ is a basis of $K[G] \otimes_{R[G]} P$ over K. In particular, up to identification $e_i \leftrightarrow 1 \otimes e_i$, the action of G on $K[G] \otimes_{R[G]} P$ is represented by the same matrices as its action on P.
- One can show that any finitely generated KG-module M always contains an RG-submodule N, free as an R-module, for which $KN = M$. Then we define $d(M) = N/\mathfrak{m}N$. It can be shown that the composition factors of the resulting kG-module are independent of N, whence $d([M]) = [d(M)] \in R_k(G)$ is well-defined. Details can be found in [Ser77, Chapter 15].

Remark 2.3.21. Each isomorphism class $[E] \in S_k(G)$ is contained in some $d([M])$, where M is a simple KG-module. Indeed, this follows by the commutativity of the Cartan-Brauer triangle and the fact that $[E]$ is contained in the image of its projective cover $[P_E] \in R_k(G)$.

Remark 2.3.22.

- Any projective RG-module P can be interpreted as a KG-module (by extension of scalars). Thus we can associate a character $\Phi_P \colon P \to K$ to it, which uniquely determines its isomorphism class. We can then identify $P_k(G) \cong P_R(G)$ with the $\mathbb{Z}$-module of class functions on G spanned by $\{\Phi_{P_E}\}_{[E]\in S_k(G)}$.

- Similarly, we can identify each element $[M]$ of $R_K(G)$ with the corresponding $\mathbb{Z}$-linear combination of characters χ_M.

- For $R_k(G)$ too, we can identify each element $[E]$ with the corresponding $\mathbb{Z}$-linear combination of modular characters ϕ_E.

The (currently mysterious) maps from theorem 2.3.19 become very easy when expressed in terms of class functions.

Proposition 2.3.23. *In terms of class functions, the maps c and d are given by restriction, and e is given by inclusion:*

1. *For each $[P] \in P_R(G) : c(\Phi_P) = \Phi_{P|G_{reg}}$.*

2. *For each $[M] \in R_k(G) : d(\chi_M) = \chi_{M|G_{reg}}$.*

3. *For each $[P] \in P_R(G) : e(\Phi_P) = \Phi_P$.*

We also have certain orthogonality relations, which allow for direct computation of products of modular characters $\phi_{E_1}\phi_{E_2}$.

Proposition 2.3.24. *Let E, E' be two simple kG-modules. Denote by Φ_{P_E} the character of the projective cover of E (remark 2.3.22), and let $\phi_{E'}$ be the Brauer character of E'. Then, for*

$$\langle \Phi_{P_E}, \phi_{E'} \rangle \coloneqq \frac{1}{|G|} \sum_{g\in G_{reg}} \Phi_{P_E}(g^{-1})\phi_{E'}(g),$$

it holds that

$$\langle \Phi_{P_E}, \phi_{E'} \rangle = \begin{cases} 1 & \textit{if } E \cong E', \\ 0 & \textit{if } E \ncong E'. \end{cases}$$

Proof. A proof can be found in [Ser77, §18.1]. ■

Proposition 2.3.25. *Let E be a simple KG-module. If the dimension $\dim(E)$ of E is divisible by the largest power p^n of p dividing the order of G, then*

1. *$E = K[G] \otimes_{R[G]} P$ for a projective RG-module, and*

2. *$d(E)$ is a simple and projective kG-module.*

Proof. A proof can be found in [Ser77, Proposition 46]. ■

2.3.3 Examples

We illustrate the use of the Cartan-Brauer triangle and orthogonality relations with three classical examples. Starting from the complex characters, we determine the modular characters and their tensor products (and hence $(S_k(G), *)$).

Example 2.3.26 *([Web16, Appendix B],D_{2m} in even characteristic).* Let m be an odd natural number. Consider the dihedral group D_{2m} on $2m$ elements, given by the presentation

$$\langle r, s \mid r^m = s^2 = 1, srs = r^{-1}\rangle.$$

Denote by ζ a primitive m-th root of unity. Then the ordinary character table of D_{2m} is given by:

	1	s	r	r^2	$\dots$	$r^{\frac{m-1}{2}}$
χ_1	1	1	1	1	$\dots$	1
χ_{-1}	1	-1	1	1	$\dots$	1
χ_{ζ^s}	2	0	$\zeta^s + \zeta^{-s}$	$\zeta^{2s} + \zeta^{-2s}$	$\dots$	$\zeta^{\frac{m-1}{2}s} + \zeta^{\frac{-(m-1)}{2}s}$

There is one character χ_{ζ^s} for each $s = 1, \dots, \frac{m-1}{2}$. As 2 is the highest power of 2 dividing the order of D_{2m}, it follows that each χ_{ζ^s} restricts to an irreducible modular character ϕ_{ζ^s} (proposition 2.3.25). As χ_1 and χ_{-1} are equal everywhere, except on the the conjugation class of s, it follows that they restrict to the same modular charcter ϕ_1. As ϕ_1 is one-dimensional, it is irreducible as well. We have found all irreducible modular characters (remark 2.3.21). Their values on the p-regular classes are given by

	1	r	r^2	$\dots$	$r^{\frac{m-1}{2}}$
χ_1	1	1	1	$\dots$	1
χ_{-1}	1	1	1	$\dots$	1
χ_{ζ^s}	2	$\zeta^s + \zeta^{-s}$	$\zeta^{2s} + \zeta^{-2s}$	$\dots$	$\zeta^{\frac{m-1}{2}s} + \zeta^{\frac{-(m-1)}{2}s}$

They multiply as follows:

$$\begin{cases} \phi_1^2 & = \phi_1, \\ \phi_1 \cdot \phi_{\zeta^s} & = \phi_{\zeta^s}, \\ \phi_{\zeta_1^s} \cdot \phi_{\zeta_2^s} & = \phi_{\zeta^{s_1+s_2}} + \phi_{\zeta^{s_1-s_2}}, \end{cases}$$

as can be immediately read off from the character table.

Example 2.3.27 *(D_{2p}, p odd).* We consider the modular characters of D_{2p} in characteristic p, where p is an *odd* prime. As the only p-regular conjugation class is the one containing s, it immediately follows that that the modular character table is given by

	1	s
ϕ_1	1	1
ϕ_{-1}	1	-1

Notice that, in contrast to the characteristic zero case, the resulting fusion law is $\mathbb{Z}/2$-graded. This is due to the fact that the simple kD_{2p}-modules coincide with the simple kC_2-modules when $\mathrm{char}(k) = 2$.

Example 2.3.28 *([Ser77, §18.6], A_5, $p = 2$).* Consider the group A_5 of even permutations on the elements $\{1, 2, 3, 4, 5\}$, we compute its modular characters and their tensor products for $p = 2$. It has 5 conjugacy classes

$$\{\{1\}, ((12)(34))^G, (123)^G, (12345)^G, (12354)^G\}.$$

Its ordinary character table is given by

	1	(12)(34)	(123)	(12345)	(13254)
χ_1	1	1	1	1	1
χ_2	3	-1	0	$z = \frac{1+\sqrt{5}}{2}$	z'
χ_3	3	-1	0	$z' = \frac{1-\sqrt{5}}{2}$	z
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Both the trivial character χ_1 and χ_4 reduce to irreducible modular characters ϕ_1, ϕ_4 (proposition 2.3.25) We observe that, on G_{reg} we have the equality

$$\chi_2 + \chi_3 = \chi_1 + \chi_5.$$

As χ_1 reduces to an irreducible modular character ϕ_1 this implies that at least one of χ_2 or χ_3 reduces to

$$\begin{aligned} \chi_2 &= \phi_1 + \phi_2 \quad \text{on } G_{\text{reg}}, \\ \chi_3 &= \phi_1 + \phi_3 \quad \text{on } G_{\text{reg}}, \end{aligned}$$

for certain modular characters ϕ_2, ϕ_3. By symmetry in χ_2, χ_3, they must then both reduce to the sum of two modular characters.

Suppose that ϕ_2 is not irreducible: assume that it is the sum of two (necessarily linear) modular characters $\phi_2 = \phi_2' + \phi_2''$. Then, as $\phi_2((123)) = -1$,

$$\begin{aligned} \phi_2'((123)) &= \zeta_3, \\ \phi_2''((123)) &= \zeta_3^2, \end{aligned}$$

for a primitive third root of unity ζ_3. In particular, $\phi_2' \neq \phi_2''$ and $\phi_2', \phi_2'' \neq \phi_1$. Since there are only 4 p-regular conjugacy classes, it follows that $\phi_1, \phi_2', \phi_2'', \phi_4$ are all the irreducible modular characters. As $\phi_3((123)) = -1$, we must then have that $\phi_3 = \phi_2' + \phi_2'' = \phi_2$, a contradiction. Hence ϕ_2 and ϕ_3 are irreducible.

Thus the character table of the modular characters is given by

	1	(123)	(12345)	(12354)
ϕ_1	1	1	1	1
ϕ_2	2	-1	$z-1$	$z'-1$
ϕ_3	2	-1	$z'-1$	$z-1$
ϕ_4	4	1	-1	-1

On G_{reg}, we then have

$$\begin{aligned} \chi_1 &= \phi_1, \\ \chi_2 &= \phi_1 + \phi_2, \\ \chi_3 &= \phi_1 + \phi_3, \\ \chi_4 &= \phi_4, \\ \chi_5 &= \phi_1 + \phi_2 + \phi_3. \end{aligned}$$

Thus the matrix representation D of d is given by

$$D = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

We now compute the matrix representation C of the Cartan map by $C = DD^T$ (theorem 2.3.19):

$$C = \begin{pmatrix} 4 & 2 & 2 & 0 \\ 2 & 2 & 1 & 0 \\ 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

For each ϕ_i, denote the character of the projective cover of the corresponding simple kG-module by Φ_i. Then the above matrix representation of C simply spells out that:

$$\begin{cases} \Phi_1 & = 4\phi_1 \quad +2\phi_2 \quad +2\phi_3, \\ \Phi_2 & = 2\phi_1 \quad +2\phi_2 \quad +\phi_3, \\ \Phi_3 & = 2\phi_1 \quad +\phi_2 \quad +2\phi_3, \\ \Phi_4 & = \phi_4. \end{cases}$$

Using the orthogonality relation from proposition 2.3.24, it is straightforward to compute the decompositions of products of the modular characters.

$\otimes$	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	$2\phi_1 + \phi_3$	ϕ_4	$2\phi_1 + \phi_2 + 2\phi_3$
ϕ_3	ϕ_3	ϕ_4	$2\phi_1 + \phi_2$	$2\phi_1 + 2\phi_2 + \phi_3$
ϕ_4	ϕ_4	$2\phi_1 + \phi_2 + 2\phi_3$	$2\phi_1 + 2\phi_2 + \phi_3$	$4\phi_1 + 2\phi_2 + 2\phi_3 + \phi_4$

Remark 2.3.29. Notice that most of the information we needed could be read of directly from the character table and we only needed a very limited amount of knowledge on the groups themselves. Indeed, the only information we used were their orders and the fact that there is an automorphism of A_5, swapping (12345) with (12354) (which implies the 'symmetry' in ϕ_2 and ϕ_3 that we used in example 2.3.28).

The upshot of this section is that (for many fields k) knowledge of all kG-modules is not required in order to understand $(S_k(G), *)$: it suffices to know the irreducible modular characters.

2.4 Block fusion laws

Until now, we have studied the problem of examining the fusion law on an algebra A arising from a group action, when we already know that A admits a suitable decomposition (as in proposition 2.2.13). Now, we wish to put a decomposition algebra structure on arbitrary algebra A, over a field, for any finite group $G \leq \mathrm{Aut}(A)$.

If kG is a direct product of k-algebras $kG \cong B_1 \times \cdots \times B_n$, then certainly $A = \bigoplus_{i=1}^n B_i A$. The finest such direct product decomposition is given when $B_i = e_i kG$ for the blocks e_i of kG. The desired *block fusion law* is then determined by the blocks B_i appearing as direct summands of the tensor products of the kG-modules $B_i \otimes B_j$.

It turns out that this *block fusion law* $B(kG)$ can be completely described when we know both $S_k(G)$ and the Cartan matrix. We also mention the structure of these blocks in the case that G has a normal Sylow p-subgroup or has a normal subgroup with a Sylow p-subgroup as a complement.

2.4.1 Blocks of group rings

There are many equivalent ways to define the (p-)blocks of G. Following [Web16], we shall opt to identify them with *primitive central idempotents* of kG as this makes it clear how the corresponding decompositions of kG-modules arise. We also mention an equivalent definition in terms of $\mathrm{Rep}_k(G)$, which illustrates how $(S_k(G), *)$ relates to $(B(kG), *)$.

Definition 2.4.1. Let k be a field and B an associative, unital k-algebra. A *block* of B is a *primitive central idempotent* $e \in B$. That is, an element $e \in \mathrm{Z}(B)$ such that $e^2 = e$ and which can not be written as the sum of two nonzero *central* idempotents.

Lemma 2.4.2. *Let k be a field and B a finite-dimensional associative, unital k-algebra. Then $1 \in B$ can be written as a sum of pairwise orthogonal primitive central idempotents*

$$1 = e_1 + \cdots + e_n.$$

The set $\{e_1, \ldots, e_n\}$ is precisely the set of all primitive central idempotents of B.

Equivalently, there is a unique decomposition of B as a direct sum of indecomposable two-sided ideals.

Proof. Note that the two claims are indeed equivalent. When given a decomposition $B = B_1 \oplus B_2$ into two-sided ideals, then the unit $e_1 \in B_1$ is a central idempotent of B for wich $e_1 B = B_1$ and $(1 - e_1)B = B_2$. The lemma now follows from e.g. [Zim14, Proposition 1.9.4], noting that B can only have finitely many indecomposable direct summands. ■

We continue in the setting of a finite-dimensional associative, unital k-algebra B. By the above lemma 2.4.2, this guarantees a unique decomposition of B into blocks. This will pose no essential restriction on our further goals, as we are interested in the case of group algebras of finite groups over a field. We first illustrate a link between blocks and $B\mathbf{-mod}$ with two easy lemmas, the content of which can also be found in [Web16, Proposition 12.1.2].

Lemma 2.4.3. *Let k be a field and B a finite-dimensional associative, unital k-algebra. Let M be an indecomposable B-module. Then there is a unique block e_i of B such that $e_i M = M$. For all other blocks e_j, it holds that $e_j M = 0$.*

Proof. Let $e_1, \ldots, e_n$ be the blocks of R. Then $e_i M \cap \sum_{i \neq j} e_j M = 0$, as $e_i e_i M = e_i M$, but $e_i e_j M = 0$, for all $j \neq i$ (lemma 2.4.2). Hence, we have a direct sum decomposition

$$M = 1 \cdot M = e_1 M \oplus \cdots \oplus e_n M.$$

Since M is indecomposable, only one term $e_i M$ can be nonzero, but then necessarily $e_i M = M$. ■

We say that an indecomposable module M *belongs to* a block e_i if $e_i M = M$.

Lemma 2.4.4. *Let k be a field, and let B be a finite-dimensional associative, unital k-algebra. Let M_1, M_2 be two indecomposable B-modules, belonging to blocks e_1 and e_2, respectively. If $e_1 \neq e_2$, then $\mathrm{Hom}_B(M_1, M_2) = 0$.*

Proof. Let $f \in \mathrm{Hom}_R(M_1, M_2)$. Then, for every $m \in M_1$,

$$f(m) = e_2 f(e_1 m) = (e_2 e_1) f(m) = 0.$$ ■

We could also have defined blocks in terms of properties of $B\mathbf{-mod}$.

Proposition 2.4.5. *Let B be a finite-dimensional algebra over a field k. For two simple B-modules S and T, the following statements are equivalent.*

1. *Both modules S and T belong to the same block.*
2. *There exists a finite sequence of simple B-modules $S = S_0, \dots, S_n = T$ such that S_i, S_{i-1} are both composition factors of the same projective indecomposable module P_i, for $i = 1, \dots, n$.*

Proof. A proof can be found in [Web16, Proposition 12.1.7]. ■

Definition 2.4.6. Let k be a field and G a finite group. Denote by $B(kG)$ the set of all blocks of kG. Define the *block fusion* law $(B(kG), *)$ by letting $e_3 \in e_1 * e_2$ if and only if exist indecomposable modules M_1 and M_2 belonging to e_1 and e_2 respectively such that $M_1 \otimes M_2$ has an indecomposable summand belonging to e_3.

Proposition 2.4.7. *Let A be a k-algebra and let $G \leq \operatorname{Aut}(A)$ be a finite group. Then*

$$\bigoplus_{e_i \in B(kG)} e_i A$$

is a $(B(kG), *)$-decomposition of A.

Proof. The sum is direct by lemma 2.4.3. Then, by lemma 2.4.4 and by the definition of the block fusion law, it follows that

$$(e_i A)(e_j A) \subseteq \bigoplus_{e_\ell \in e_i * e_j} e_\ell A.$$ ■

Theorem 2.4.8. *There is a natural surjective map of fusion laws*

$$\pi \colon S_k(G) \to B(kG),$$

sending the isomorphism class $[E]$ of a simple kG-module to the block e to which it belongs. Furthermore, for all blocks e_1, e_2 it holds that

$$e_1 * e_2 = \pi(\pi^{-1}(e_1) * \pi^{-1}(e_2)).$$

Proof. Let E_1, E_2 be simple modules belonging to certain blocks e_1, e_2 respectively. By definition each indecomposable summand M of $E_1 \otimes E_2$, belongs to one of the blocks $e_3 \in e_1 * e_2$. Then every simple submodule of M must also belong to e_3. Since every simple submodule of of $E_1 \otimes E_2$ is isomorphic to a simple submodule of an indecomposable direct summand, it follows that that $\pi(E_1 * E_2) \subseteq e_1 * e_2$. Hence π is a morphism of fusion laws, and it holds that

$$e_1 * e_2 \supseteq \pi(\pi^{-1}(e_1) * \pi^{-1}(e_2)).$$

For the converse inclusion, we have to show that if a block e_3 is contained in $e_1 * e_2$, then there are simple modules E_i, each belonging to e_i ($i = 1, 2, 3$), such that $[E_3] \in [E_1] * [E_2]$ in $S_k(G)$. By assumption, we have indecomposable modules M_i belonging to each e_i ($i = 1, 2, 3$) such that M_3 is a direct summand of $M_1 \otimes M_2$. In particular, $M_1 \otimes M_2$ has a simple composition factor belonging to e_3. As $[M_1 \otimes M_2] = [M_1][M_2]$, and $R_k(G)$ is a $\mathbb{Z}_+$-ring, it follows that there are composition factors E_1, E_2 of M_1, M_2 respectively such that $[E_1][E_2] = [E_3] \oplus [N]$ for some kG-module N. This is precisely what was left to prove. ■

2.4.2 Groups with normal p-complement

We fix a prime p and consider groups of the form $G = H \rtimes Q$, where Q is a Sylow p-subgroup of G and the order of H is (necessarily) coprime to p. We say that G has a normal *p-complement* (given by H). The following is a known fact about these groups.

Theorem 2.4.9. *Let G be a finite group and k a field of characteristic p. Then G has normal p-complement if and only if for every simple kG-module S, the composition factors of the projective cover P_S are all isomorphic to S.*

Proof. A proof can be found in [Web16, Theorem 8.4.1]. ■

Corollary 2.4.10. *Let G be a finite group and k be a field. Then $(S_k(G), *) \cong (B(kG), *)$ if and only if $\operatorname{char}(k) = 0$ or $\operatorname{char}(k) = p > 0$ and G has a normal p-complement (possibly $1 \leq G$).*

Proof. Using the second characterization of blocks from proposition 2.4.5, it follows from the above theorem 2.4.9 that these are the only cases for which all blocks of kG contain only one simple module. ■

Thus these are the only finite groups for which the fusion law does not change when going from simple modules to blocks.

2.4.3 Groups $G = C_q \rtimes C_m$

Consider a prime number p, a natural number $d \geq 1$ and denote $q = p^d$. We investigate $B(kG)$ when $G \cong C_q \rtimes C_m$, with m coprime to p, and k is a field of characteristic p, sufficiently large with respect to C_m. In particular, the group μ_k consisting of the m-th roots of unity in k has order m.

Lemma 2.4.11. *Let $G = Q \rtimes H$ be such that Q is a p-group and the order of H is coprime to p. Then the simple kG-modules are precisely the simple kH-modules via the surjection $kG \to kH$.*

Proof. Up to isomorphism, the only simple kQ-module is k, equipped with trivial Q-action (proposition 1.1.6). Thus, by Clifford's theorem 1.1.10, it follows that Q acts trivially on all simple kG-modules. Hence, the simple kG-modules are precisely the simple $k(G/Q)$-modules. ■

Notation 2.4.12. Let $\langle y \rangle = C_m$, with m coprime to p. If k is sufficiently large with respect to C_m, then all simple kC_m-modules are 1-dimensional. For any m-th root of unity ζ, denote by k_ζ the one-dimensional kC_m-module on which y acts by multiplication with ζ. In this way, the simple kC_m-modules are parameterized by the m-th roots of unity in k. Also note that $k_\zeta \otimes k_\xi = k_{\zeta\xi}$, for all m-th roots of unity ζ, ξ.

By the above lemma 2.4.11, these modules k_ζ also form the collection of all simple $k(C_q \rtimes C_m)$-modules, up to isomorphism.

As in the case of groups with a normal p-complement, the heavy lifting is done by a known representation-theoretic fact.

Proposition 2.4.13. *Let $G = Q \rtimes H$, where $Q = \langle x \rangle \cong C_q$ and H is a group of order relatively prime to p. Consider the one-dimensional kG-module W, on which Q acts trivially and H acts via its conjugation action on $Q/\langle x^p \rangle$: if $y \in K$ and ${}^y x = x^r$, then $y \cdot w = rw$, for all $w \in W$. If S is any simple kG-module, then its projective cover P_S is uniserial, with successive radical quotients $\operatorname{rad}^i(P_S)/\operatorname{rad}^{i+1}(P_S)$ given by*

$$S, W \otimes S, W^{\otimes 2} \otimes S, \ldots, W^{\otimes(q-1)} \otimes S \cong S.$$

Proof. See, for example, [Web16, Proposition 8.3.3] . ■

Theorem 2.4.14. *Let $G = C_q \rtimes C_m$ where q is a power of p and m is coprime to p. Write $C_q = \langle x \rangle$ and $C_m = \langle y \rangle$ and let $r \in \mathbb{F}_q$ be such that ${}^y x = yxy^{-1} = x^r$. Then $r \in \mathbb{F}_p \subseteq k$ and $r \in \mu_k$. Furthermore, $B(kG) \cong \mu_k/\langle r \rangle$ as (group) fusion laws.*

Proof. As in the statement of the theorem, write $G = Q \rtimes H$, with $Q = \langle x \rangle \cong C_q$ and $H = \langle y \rangle \cong C_m$. Clearly, G is completely determined if we know the value of r in ${}^y x = x^r$, where r is viewed as an element of $\mathbb{F}_q$. Since $y^m = 1$, it follows that $r^m = 1$. However, the order of $r \in \mathbb{F}_q^\times$ must also divide $|\mathbb{F}_q^\times| = p^{d-1}(p-1)$. As m and p are coprime, this implies that $r^{p-1} = 1$. This last equation precisely expresses that $r \in \mathbb{F}_p \subseteq \mathbb{F}_q$.

For the second part, consider a simple kG module k_ζ and its projective cover P_ζ. Note that as $r^m = 1$, we have $r \in \mu_k$ and the module W of the above proposition 2.4.13 is isomorphic to k_r. Thus the radical quotients of P_ζ are given by

$$k_\zeta, k_{r\zeta}, k_{r^2\zeta}, \ldots, k_{r^{q-1}\zeta} \cong k_\zeta.$$

By proposition 2.4.5 it follows that the (isomorphism classes of) all simple modules in the above list all belong to a common block and that all other isomorphism classes of simple modules belong to a different block. Thus the blocks of kG are indexed by the cosets $\zeta\langle r \rangle$ of $\langle r \rangle \leq \mu_k$. The theorem now follows from theorem 2.4.8, using that $[k_\zeta] * [k_\xi] = \{[k_{\zeta\xi}]\}$ in $S_k(G)$. ■

In the current case of $G \cong C_q \rtimes C_m$, we have a good grip on all possible indecomposable modules. This is a special case of the following proposition, using that the projective and injective modules of group rings coincide (proposition 1.1.8).

Proposition 2.4.15. *Let B be a finite-dimensional unital and associative algebra over a field k. Suppose that all projective and all injective indecomposable B-modules are uniserial. Then every indecomposable B-module is the homomorphic image of an indecomposable projective B-module.*

Proof. A proof can be found in [Web16, Proposition 11.2.1]. ■

Remark 2.4.16. Note that proposition 2.4.15 and the proof of theorem 2.4.14 together imply that the composition factors of any indecomposable kG-module can be listed as

$$\{k_{\zeta r^i}, k_{\zeta r^{i+1}}, \ldots, k_{\zeta r^{i+j}}\},$$

for a certain m-th root of unity ζ and $0 \leq i + j < q$. Denote by $\mathrm{o}(r)$ the order of r in the multiplicative group $\mathbb{F}_p^\times$: the minimal natural number $n \geq 1$ for which $r^n = 1$. Note that when $j \leq \mathrm{o}(r)$, these composition factors are pairwise non-isomorphic.

Lemma 2.4.17. *Let $G \cong C_q \rtimes C_m$, with $C_q = \langle x \rangle$ and $C_m = \langle y \rangle$. Let $1 \leq r < p$ be such that ${}^y x = x^r$ and let $\mathrm{o}(r)$ be the order of r in $\mathbb{F}_p^\times$. Suppose that k is algebraically closed and M is an indecomposable kG-module with $\dim(M) \leq \mathrm{o}(r)$. Then $\mathrm{End}_G(M) \cong k$.*

Proof. As $\mathrm{End}_G(M)$ is a finite-dimensional k-algebra and k is algebraically closed, it suffices to prove that all nontrivial endomorphisms of M are in fact automorphisms. From proposition 2.4.15 it follows that M is uniserial; denote by $S = M/\operatorname{rad}(M)$ its simple quotient. Consider a nontrivial map $f \in \mathrm{End}_G(M)$, and suppose that f is not surjective. Then $\mathrm{im}(f) \subsetneq M$, and, because M is uniserial, $\mathrm{im}(f)/\operatorname{rad}(\mathrm{im}(f)) \cong M/\operatorname{rad}(M) = S$. Again, since M is uniserial, this implies that M has two composition factors isomorphic to S. This is a contradiction, since M cannot have repeating composition factors as long as $\dim(M) \leq \mathrm{o}(r)$ (remark 2.4.16). Hence f is surjective. As M is finite-dimensional, it follows that f is an automorphism. ■

The following theorem can be considered as a partial generalization of [DPSV20, Theorem 7.2 (ii)] to characteristic p, specifically for groups $G \cong C_q \rtimes C_m$.

Theorem 2.4.18. *Let k, G and r be as in lemma 2.4.17 and let A be a k-algebra. Suppose that for every block $e \in B(kG)$, the kG-module eA is indecomposable and that $\dim(eA) \leq \mathrm{o}(r)$. Further suppose that for the block e_0, containing the trivial kG-module it holds that $e_0 A \cong k$. Then any nonzero $a \in e_0 A$ is an axis (both left and right) for the $(B(kG), *)$-decomposition*

$$A = \bigoplus_{e \in B(kG)} eA.$$

Proof. Let $a \in e_0 A \setminus \{0\}$. As $e_0 A$ is isomorphic to the trivial kG-module, it holds for each block e that $(e_0 A) \otimes (eA) \cong eA$. Hence, the operator ad_a given by left multiplication with a induces a morphism of kG-modules from eA to A. By lemma 2.4.4, it follows that the image of ad_a is again contained in eA. Then, by lemma 2.4.17, it follows that ad_a must act as a scalar on eA. Clearly, the same holds for right multiplication with a, and the statement is proved. ■

Remark 2.4.19. Consider the situation of the above theorem 2.4.18. Let $H \leq G$ be a subgroup of G, isomorphic to C_m. As m is coprime to p, the group algebra kH is semisimple and we can apply [DPSV20, Theorem 7.2 (ii)]. This theorem states that the corresponding decomposition

$$A = \bigoplus_{[E] \in S_{C_m}(G)} A_{[E]}$$

is axial when each $A_{[E]}$ is either simple or zero. Note that, by theorem 2.4.14 and remark 2.4.16, this implies the condition on dimensions in theorem 2.4.18. By considering the full group $G = C_q \rtimes C_m$ (instead of only H), we then obtain the additional information that the eigenvalue of the axis $a \in e_0 A$ cannot vary between $A_{[E_1]}, A_{[E_2]}$ when both are contained in the same block.

Theorem 2.4.18 illustrates that despite the differences between the representation theory of groups over $\mathbb{C}$ and the theory over fields of positive characteristic, we can still make similar general observations.

3 Fusion laws as algebraic objects

In this chapter, we examine an alternate definition for morphisms between fusion laws: we allow them to be multi-valued. This has has a natural motivation, as explained below. We then investigate an aspect of the corresponding category: to what extent is the finest grading of a fusion law a categorical universal object?

3.1 Motivation

Let k be a field (or, more generally, a commutative ring). Then a k-algebra A is simply a vector space A, equipped with a map $m\colon A \otimes_k A \to A$. Commutativity, associativity and unitality can then be expressed through the existence of certain commutative diagrams. For example, A is associative if and only if the following diagram commutes:

$$\begin{tikzcd}
A \otimes_k A \otimes_k A \arrow[r, "\mathrm{id}_A \otimes m"] \arrow[d, "m \otimes \mathrm{id}_A"'] & A \otimes_k A \arrow[d, "m"] \\
A \otimes_k A \arrow[r, "m"'] & A
\end{tikzcd}$$

Then, for any category $\mathcal{C}$ equipped with a 'tensor product', we can examine the interpretation of such commutative diagrams. For example, the axioms for a unital and associative k-algebra, become the definition of a *monoid* in an arbitrary *monoidal category*[1].

If the category $\mathcal{C}$ is additionally k-linear and abelian (and *locally finite* and *rigid*), $\mathcal{C}$ becomes a *tensor category* ([IGNO15, Definition 4.1.1]) and one can think of the monoids of $\mathcal{C}$ as generalizations of k-algebras[2].

In [CDL06], the authors use this abstract approach to gain a better understanding of the so called *Hopf group-algebras* and *Hopf group-coalgebras* by showing that they are precisely the Hopf algebras of a certain tensor category. It was pointed out to Tom De Medts by Joost Vercruysse that a similar approach might be possible for decomposition algebras.

In a first attempt, we fix a field k and consider the category **Fam** of pairs (X, A), where X is a set and $A = (A_x)_{x\in X}$ is a family of k-vector spaces. The morphisms between two such objects (X, A) and (Y, B) are given by pairs (ψ, ϕ), where ψ is a map of sets $X \to Y$ and $\phi = (\phi_x)_{x\in X}$ is a family of maps $\phi_x\colon A_x \mapsto B_{\psi(x)}$. This category admits a natural tensor product structure[3]

$$(X, A) \otimes (Y, B) = (X \times Y, A \otimes B).$$

[1] A monoidal category is precisely a category equipped with a "tensor product". That is, there is a bifunctor $\cdot \otimes \cdot$ and specific natural transformations, satisfying certain axioms. A precise definition can be found in [IGNO15, Definition 2.1.1]

[2] We will not define tensor categories here, but examples are given by the category of k-vector spaces, the category $\mathrm{Rep}_k(G)$ and the category of finite-dimensional representations of a Lie algebra $\mathfrak{g}$ ([IGNO15, Example 4.1.2]).

[3] This category is in fact the *Zunino Category from [CDL06].*

Where $X \times Y$ is simply the cartesian product and $(A \otimes B)_{(x,y)} = A_x \otimes_k B_y$ is given by the tensor product of vector spaces.

An algebra in this category is then a morphism

$$(*, m)\colon (X, A) \otimes (X, A) \to (X, A).$$

Equivalently, m defines a multiplication map, making

$$\bigoplus_{x \in X} A_x$$

into an algebra in such a way that

$$m(a_x \otimes a_y) \in A_{x*y},$$

for all $x, y \in X$, $a_x \in A_x$ and $a_y \in A_y$.

In other words, the map $*$ defines (by some abuse of notation) a fusion law $(X, *)$, given by

$$*\colon X \times X \to P(X)\colon (x, y) \mapsto \{x * y\},$$

and $\bigoplus_{x \in X} A_x$ is an $(X, *)$-decomposition. In order to allow $(X, *)$ to become any fusion law, we need to allow the maps between sets in the above category to be multi-valued. Concretely, we consider the category[4] $\mathbf{Fam}_P$, whose objects are those in $\mathbf{Fam}$. The morphisms between objects (X, A) and (Y, B) are now given by pairs (ψ, ϕ), where

- $\psi\colon X \to P(Y)$ is a map of sets, and
- ϕ is a family of maps $(\phi_x)_{x \in X}$ of k-vector spaces
$$\phi_x\colon A_x \mapsto \bigoplus_{y \in \psi(x)} A_y.$$

Then, by construction, an algebra in this category consists of a fusion law $(X, *)$, together with an $(X, *)$-decomposition of an algebra $A = \bigoplus_{x \in X} A_x$.

This naturally introduces the idea of multi-valued maps between fusion laws and this is what we study in the rest of this chapter. We focus on determining whether or not the finest grading of $(X, *)$ is a categorical universal property in this new category $\mathbf{Set}_P$.

3.2 The category Set_P

3.2.1 Definition

We consider a category $\mathbf{Set}_P$ whose objects are the same as the category $\mathbf{Set}$ of all sets, but whose maps can be multi-valued. The magmas of this category are precisely the fusion laws; we can thus view fusion laws as algebraic objects. This category could be defined abstractly as the Kleisli category ([ML98, p. 147]) of the powerset monad $X \mapsto P(X)$, but we give an explicit definition[5]

[4] Some (straightforward) arguments are required to show that $\mathbf{Fam}_P$ is indeed a category and that it is still a monoidal category for the same tensor product as in $\mathbf{Fam}$. Abstractly, these are consequences of the fact that $\mathbf{Fam}_P$ is the *Kleisli category* ([ML98, p. 147]) of the monoidal monad (this concept is introduced under the name *Hopf monad on a tensor category* in [Moe02]) P on $\mathbf{Fam}$. This monad P is an extension of the powerset functor to $\mathbf{Fam}$, given by $P(X, A) = (P(X), P(A))$, where $P(X)$ is the powerset of X and $P(A)_S = \bigoplus_{x \in S} A_x$ for any subset S of X. The idea of the category $\mathbf{Fam}_P$ is due to Joost Vercruysse

[5] The general definition is essentially the same, but with an arbitrary monad instead of the powerset monad P.

Definition 3.2.1. Let $\mathbf{Set}_P$ be the category with

- an object X_P for each $X \in \mathbf{Set}$ and
- a morphism $f^\flat : X_P \to Y_P$, for each map $f : X \to P(Y)$ of sets.

The following concepts make it easier to talk about the *category* $\mathbf{Set}_P$:

1. For each map of sets $f \colon X \to Y$, denote by $P(f)$ its natural extension to a map $P(X) \to P(Y)$.
2. Denote by μ the natural transformation of sets defined by taking the union:
$$\mu_X : P^2(X) \to P(X) \colon S \mapsto \bigcup S,$$
for all $X \in \mathbf{Set}$.
3. For maps $f^\flat : X_P \to Y_P$ and $g^\flat : Y_P \to Z_P$ in $\mathbf{Set}_P$, their composition is defined as
$$g^\flat \circ f^\flat := (\mu_Z \circ P(g) \circ f)^\flat.$$
4. The symbol $\{*\}$ denotes an arbitrary (fixed) set with one element.
5. Denote by η the natural transformation
$$\eta_X \colon X \to P(X) \colon x \mapsto \{x\}$$

Remark 3.2.2. With these objects and morphisms, $\mathbf{Set}_P$ indeed defines a category, as follows from the general theory in [ML98, p. 147].

Lemma 3.2.3. *The cartesian product on* $\mathbf{Set}$ *induces a natural bifunctor* $\times$ *on* $\mathbf{Set}_P$*, given by*
$$X_P \times Y_P = (X \times Y)_P.$$
Furthermore, we have natural transformations $a^\flat, r^\flat, l^\flat$*, induced by*
$$\begin{array}{lll} a_{X,Y,Z} & : (X \times Y) \times Z \to P(X \times (Y \times Z)) & : ((x,y),z) \mapsto \{(x,(y,z))\}, \\ l_X & : \{*\} \times X \to P(X) & : (*,x) \mapsto \{x\}, \\ r_X & : X \times \{*\} \to P(X) & : (x,*) \mapsto \{x\}. \end{array}$$

Proof (sketch). Let X, Y, Z, U be sets and $f \colon X \to P(Z)$, $g \colon Y \to P(U)$ be maps of sets. We must construct a natural map
$$f \times g \colon X \times Y \to P(Z \times U).$$
We already have a map
$$X \times Y \to P(Z) \times P(U) \colon (x,u) \mapsto (f(x), g(y)).$$
Then define $f \times g$ as this map, postcomposed with the natural transformation
$$P(Z) \times P(U) \to P(Z \times U) \colon (V, W) \mapsto \{(v,w) \mid v \in V, w \in W\}.$$
It is now straightforward to verify that $\times$ then respects composition and identity in $\mathbf{Set}_P$. The a, l, r are also clearly natural transformations and express that $\times$ satisfies a kind of associativity and a kind of unitality with respect to $\{*\}$. ■

Remark 3.2.4. The above lemma shows that × induces a bifunctor on $\mathbf{Set}_P$ that "behaves like" a tensor product. In the context of monoidal categories, it proves (minus the verification of the *pentagon* and *triangle* axioms) that $\mathbf{Set}_P$ is monoidal, by verifying that P is a *monoidal monad* (also called a Hopf Monad in [Moe02]). A full proof of these facts follows by combining [Moe02, Proposition 1.4] with the fact that the Kleisli category of a monad T embeds in the category of T-algebras ([ML98, p. 139]).

Lemma 3.2.5. *Let X be a nonempty set. A fusion law $(X, *)$ defines the structure of a magma in $X_P \in \mathbf{Set}_P$ and vice versa.*

Proof. Both a fusion law and a magma in $\mathbf{Set}_P$ consist of a set X and a map

$$* : X \times X \to P(X).$$

■

Remark 3.2.6. Let X_P, Y_P be magmas in $\mathbf{Set}_P$. Then a morphism $f^\flat \colon X_P \to Y_P$ of magmas is simply a map in $\mathbf{Set}_P$ that makes the following diagram commute

$$\begin{tikzcd}
X_P \times X_P \arrow[r, "*"] \arrow[d, "f^\flat \times f^\flat"'] & X_P \arrow[d, "f^\flat"] \\
Y_P \times Y_P \arrow[r, "*"] & Y_P
\end{tikzcd}$$

Thus f is a map $X \to P(Y)$ such that

$$f(x_1 * x_2) = f(x_1) * f(x_2),$$

where on the righ-side $*$ is used for its obvious extension to subsets of Y. Compare this to morphisms g in $\mathbf{Fus}$, which are single-valued and instead satisfy

$$g(x_1 * x_2) \subseteq g(x_1) * g(x_1).$$

In particular, the above lemma 3.2.5 does not imply an equivalence of categories between $\mathbf{Fus}$ and the magmas in $\mathbf{Set}_P$.

Example 3.2.7. Let (K, R, k) be a p-modular system, with K sufficiently large with respect to some finite group G. Then the decomposition map $d \colon R_K(G) \to R_k(G)$ is not a morphism in $\mathbf{Fus}$, but it is a morphism of magmas in $\mathbf{Set}_P$. This is easy to see on the level of characters, as d is given by restriction of K-characters to G_{reg}. Let χ_1, χ_2 be two K-characters, then

$$d(\chi_1 \cdot \chi_2) = d(\chi_1) \cdot d(\chi_2).$$

Example 3.2.8. In $\mathbf{Fus}$, the full subcategory of group fusion laws is equivalent to the category of groups in the obvious way (and the equivalence is the identity on morphisms). However, in $\mathbf{Set}_P$ there are quite a bit more morphisms between group fusion laws.

1. Let G be an arbitrary group and $C_2 = \langle g \rangle$ the cyclic group on two elements. Consider the map $\iota^\flat$ in $\mathbf{Set}_P$ between the group fusion laws $(G, *)$ and $(G \times C_2, *)$, given by the map

$$\iota : G \to P(G \times C_2) \colon x \mapsto \{(x, 1), (x, g)\}.$$

Then, for all $x, y \in G$, we indeed have that

$$\iota(x * y) = \{(xy, 1), (xy, g)\} = \iota(x) * \iota(y).$$

2. More generally, let G be a group and $N \trianglelefteq G$ a normal subgroup. The map of sets

   $$\iota : G/N \to P(G) \colon gN \mapsto \{x \mid x \in gN\},$$

   mapping a coset to its set of elements in G, induces a map in $\mathbf{Set}_P$ between the group fusion laws $(G/N, *)$ and $(G, *)$. Indeed, since N is normal, we have for all $x, y \in G$

   $$\iota(xN * yN) = \iota(xyN) = \iota(xN \cdot yN) = \iota(xN) * \iota(yN),$$

   where $xN \cdot yN$ denotes the elementwise product.

   Note that ι has a left inverse π induced by $x \mapsto \{xN\}$. Thus $\iota^\flat$ is a (categorical) monomorphism and $\bigcup_{xN \in G/N} \iota(xN) = G$, but it is not an isomorphism. Compare this to the category **Fus**, where every morphism with these two properties is an isomorphism of group fusion laws.

It turns out that for finite groups, the oddities in the above example are the only ones that can turn up.

Proposition 3.2.9. *Let G, H be two finite groups and $(G, *)$, $(H, *)$ the corresponding group fusion laws, viewed as magmas in $\mathbf{Set}_P$. Let $\phi^\flat : G_P \to H_P$ be a morphism of magmas such that $\bigcup_{x \in G} \phi(x) = H$.*

Then $\phi(1_G) =: N$ is a normal subgroup of H. Furthermore, $\phi^\flat$ factors uniquely over the canonical map $\iota^\flat : (H/N)_P \to H_P$ (from example 3.2.8) in the following sense: there exists a unique morphism of groups $\psi : G \to H/N$ such that the following diagram commutes:

$$\begin{tikzcd}
& (H/N)_P \arrow[d, "\iota^\flat"] \\
G_P \arrow[ur, dashed, "(\eta\circ\psi)^\flat"] \arrow[r, "\phi^\flat"'] & H_P
\end{tikzcd}.$$

Proof. First suppose that $\phi(x) = \emptyset$ for some $x \in G$. Then for every $y \in G$, we have that $\phi(xy) = \phi(x) * \phi(y) = \emptyset$. Since G is a group, xy ranges over all elements of G when y does. Hence $\phi(y) = \emptyset$ for all $y \in G$, contradicting $\bigcup_{x \in G} \phi(x) = H$.

Now note that $|\phi(x)| \leq |\phi(xy)|$, for all $x, y \in G$. Indeed, take any $h \in \phi(y)$, then

$$|\phi(xy)| \geq |\{gh \mid g \in \phi(x)\}| = |\phi(x)|$$

Then also $|\phi((xy)y^{-1})| \geq |\phi(xy)|$. Since x, y were arbitrary and G is a group, it follows that $|\phi(x)|$ is constant as x ranges over G.

Now let $x \in G$ be arbitrary and denote $\phi(x) = \{h_1, \ldots, h_n\}$, with $h_i \neq h_j$ for $i \neq j$. Write the image of the unit as $\phi(1_G) = \{e_1, \ldots, e_n\}$, with $e_i \neq e_j$ for $i \neq j$. Since $\phi(x) = \phi(1_G \cdot x) = \phi(1_G) * \phi(x)$, the left multiplication by any e_i, $1 \leq i \leq n$ induces a permutation of the elements $\{h_1, \ldots, h_n\}$. If $e_i h_1 = e_j h_1$, then $e_i = e_j$. But there are only n possibilities for the value $e_i h_1$, so necessarily $e_i h_1 = h_1$ for some $1 \leq i \leq n$. Without loss of generality $e_1 h_1 = h_1$, whence $e_1 = 1_H$. By further renumbering the e_i, we may additionally assume $e_i h_1 = h_i$, $1 \leq i \leq n$.

Let $i \in \{1, \ldots, n\}$ be arbitrary. Then $e_i h_1 = h_i$ and thus $e_i^{-1} h_i = h_1$. By a similar argument to the preceding paragraph, there must exist some $j \in \{1, .., n\}$ such that $e_j h_i = h_1$. This implies that $e_i^{-1} = e_j$ and $N = \phi(1_G)$ is closed under taking inverses.

Furthermore, for all $i, j \in \{1, \ldots, n\}$, there exists some $k \in \{1, \ldots, n\}$ such that $e_i e_j h_1 = h_k$. Again, because $h_k = e_k h_1$, it follows that $e_i e_j = e_k$ and thus N is a subgroup of G.

We next prove that $N \trianglelefteq H$. By similar argument as above, it holds that right multiplication by any e_i induces a permutation of $\{h_1, \ldots, h_n\}$ We deduce that for any $i, j \in \{1, \ldots, n\}$, there exists some $k \in \{1, \ldots, n\}$ such that $e_i h_j = h_j e_k$.

At this point, it only remains to show that $\phi^\flat$ uniquely factors through $\iota^\flat$ as claimed. For each $x \in G$, choose some $h_x \in \phi(x)$. By the above considerations: $\phi(x) = h_x N$. Then ψ is uniquely determined by $\psi(x) = h_x N \in G/N$ and $\phi^\flat$ factors as claimed. ■

Remark 3.2.10. The above proposition 3.2.9 tells us that the potentially more complicated morphisms in $\mathbf{Set}_P$ between group fusion laws can be described by morphisms ψ in **Fus** plus a group extension of the image of ψ.

3.2.2 Finest grading of a fusion law

It is not clear at this point whether we can recover the universal grading of a fusion law as a categorical property in $\mathbf{Set}_P$. The most naive approach, "just using the universal grading that exists in **Fus**", will not work in general.

Indeed, consider a fusion law X, with universal grading $\gamma\colon X \to \Gamma_X$ in **Fus**. If there exist $x, y \in X$ such that $x * y = \emptyset$, then the corresponding map $(\eta \circ \gamma)^\flat$ in $\mathbf{Set}_P$ is not a morphism of magmas. Indeed, $\{\gamma(x)\gamma(y)\} \neq \gamma(x * y) = \emptyset$. Note that this situation occurs for important fusion laws, such as the Jordan and Ising fusion laws ([DPSV20, Examples 2.4 and 2.5]).

However, when a fusion law $(B, *)$ originates from a fusion ring (R, B), there is a natural connection between B and the universal grading group Γ_B.

Lemma 3.2.11. *Let (R, B) be a fusion ring and $(B, *)$ the corresponding fusion law. Let $\gamma\colon B \to \Gamma_B$ be its universal grading. Then $\Gamma_B = \gamma(B)$ as sets. Furthermore, $\gamma(b_{i^*}) = \gamma(b_i)^{-1}$ for all $b_i \in B$.*

Proof. Let $b_i, b_j \in B$. Because R is a fusion ring, $b_i b_j \neq 0$. Indeed, $(b_i, b_i) = 1$, implying that $(b_{i^*} b_i, 1) = 1$ and since $1 \in B$, this then implies $(b_i^* b_i b_j, b_j) \geq 1$. Hence, $b_i^*(b_i b_j) \neq 0$ and there is some $b_k \in B$ such that $(b_i b_j, b_k) > 0$. Hence, by construction of Γ_B, it holds that $\gamma(b_i)\gamma(b_j) = \gamma(b_k)$. Since $(b_i^* b_i, 1) = 1$, it also holds that $\gamma(b_i^*) = \gamma(b_i)^{-1}$. As Γ_B is generated by the $\gamma(b_i)$, the lemma follows. ■

Lemma 3.2.12. *Let (R, B) be a fusion ring and $(B, *)$ the corresponding fusion law. Then its universal grading $\gamma\colon B \to \Gamma_B$, viewed as a map of magmas in $\mathbf{Set}_P$, has a section δ. That is, there exists a morphism of magmas $\delta^\flat\colon (\Gamma_B)_P \to B_P$ such that $(\eta \circ \gamma)^\flat \circ \delta^\flat = \mathrm{id}_{(\Gamma_B)_P}$.*

Proof. For each $x \in X$, set $\delta(x) = \gamma^{-1}(x)$, the set of preimages. By the above lemma 3.2.11, we have $\gamma(\gamma^{-1}(x)) = x$, for all $x \in \Gamma_B$. It remains to check that for all $x, y \in \Gamma_B$, we have

$$\gamma^{-1}(x) * \gamma^{-1}(y) = \gamma^{-1}(xy).$$

Note that the inclusion "$\subseteq$" holds in for an arbitrary map in **Fus**.

We now check the opposite inclusion "$\supseteq$". Take any $b_i, b_j \in B$ with the properties that $\gamma(b_i) = x$ and $\gamma(b_j) = xy$ (such b_j, b_i exist by lemma 3.2.11). Then $(b_i b_{i^*} b_j, b_j) > 0$, so we can take some $b_k \in B$ with $(b_{i^*} b_j, b_k) > 0$ such that $(b_i b_k, b_j) > 0$. From $(b_{i*} b_j, b_k) > 0$ it follows that that (as in the proof of lemma 3.2.11)

$$y = x^{-1}(xy) = \gamma(b_{i^*})\gamma(b_j) = \gamma(b_k).$$

From $(b_i b_k, b_j) > 0$ it now follows that

$$b_j \in b_i * b_k \subseteq \gamma^{-1}(x) * \gamma^{-1}(y).$$

As $b_j \in \gamma^{-1}(xy)$ was arbitrary, the lemma follows. ■

Notation 3.2.13. To make the following theorem more readable, we make no notational distinction between the objects and morphisms in $\mathbf{Set}_P$ and those in $\mathbf{Fus}$. For example, we write $\alpha\colon B \to G$ instead of $\alpha^\flat\colon B_P \to G_P$ and $\gamma\colon B \to \Gamma_B$ instead of $(\eta \circ \gamma)^\flat\colon B_P \to (\Gamma_B)_P$.

Theorem 3.2.14. *Let (R, B) be a fusion ring and let $(B, *)$ be the corresponding fusion law, with universal grading $\gamma\colon B \to \Gamma_B$. Given a finite group G, viewed as a fusion law and a morphism of magmas $\alpha\colon B \to G$ in $\mathbf{Set}_P$ with $\bigcup_{b\in B} \alpha(b) = G$, there is a canonical choice of normal subgroup $N \trianglelefteq G$ and a unique morphism of groups $\beta\colon \Gamma_B \to G/N$ such that the following diagram of maps in $\mathbf{Set}_P$ commutes:*

$$\begin{tikzcd}
B \arrow[r, "\gamma"] \arrow[d, "\alpha"'] & \Gamma_B \arrow[r, "\delta"] \arrow[d, dotted, "\beta"] & B \arrow[d, "\alpha"] \\
G \arrow[r, "\pi"'] & G/N \arrow[r, "\iota"'] & G
\end{tikzcd},$$

where π, ι are as in example 3.2.8 and γ, δ are as in lemma 3.2.12.

Proof. By lemma 3.2.12, we have a map $\delta\colon \Gamma_B \to B$. Then $\alpha \circ \delta$ is a morphism in $\mathbf{Set}_P$ between two group fusion laws. By assumption, $\bigcup_{x\in\Gamma_B} (\alpha \circ \delta)(x) = G$, so by proposition 3.2.9, there exists a uniquely determined normal subgroup $N \trianglelefteq G$ and a map of groups $\beta\colon \Gamma_B \to G/N$, such that the following diagram commutes:

$$\begin{tikzcd}
\Gamma_B \arrow[r, "\delta"] \arrow[d, dotted, "\beta"] & B \arrow[d, "\alpha"] \\
G/N \arrow[r, "\iota"'] & G
\end{tikzcd}.$$

Then consider the canonical projection $\pi\colon G \to G/N$, and recall that $\pi \circ \iota = \mathrm{id}_{G/N}$. Hence, we have

$$\pi \circ \alpha \circ \delta = \beta.$$

In particular, for all $x \in \Gamma_B$, we have $|(\pi \circ \alpha \circ \delta)(x) = 1|$. As $\delta(\Gamma_B) = B$, it thus follows that $|(\pi \circ \alpha)(b_i)| \leq 1$ for all $b_i \in B$.

Suppose that $(\pi \circ \alpha)(b_i) = \emptyset$ for some $b_i \in B$, then also

$$(\pi \circ \alpha)(b_i * b_i^*) = (\pi \circ \alpha)(b_i) * (\pi \circ \alpha)(b_i^*) = \emptyset.$$

Since (R, B) is a fusion ring, we have $1 \in B$ and $1 \in b_i * b_i^*$. Thus the above equation implies that $(\pi \circ \alpha)(1) = \emptyset$. But then $(\pi \circ \alpha)(b_j) = \emptyset$, for all $b_j \in B$, contradicting $\bigcup_{b\in B} \alpha(b) = G$. We conclude that $(\pi \circ \alpha)(b_i)$ is always a singleton. Thus $\pi \circ \alpha$ can be thought of as a map in $\mathbf{Fus}$. By definition of the universal grading, there is thus a unique map $\tilde{\alpha}$ in $\mathbf{Fus}$ such that the following diagram commutes

$$\begin{tikzcd}
B \arrow[r, "\gamma"] \arrow[d, "\alpha"'] & \Gamma_B \arrow[d, dotted, "\tilde{\alpha}"] \\
G \arrow[r, "\pi"'] & G/N
\end{tikzcd}.$$

As a formula, this becomes

$$\tilde{\alpha} \circ \gamma = \pi \circ \alpha.$$

Hence, as δ is a right inverse to γ,

$$\tilde{\alpha} = \pi \circ \alpha \circ \delta = \beta.$$

■

Remark 3.2.15. In the situation of the above theorem, the universal grading $\gamma\colon B \to \Gamma_B$ "almost" satisfies a universal property in $\mathbf{Set}_P$ as well. If π is the identity map, then it follows that β is the unique map in $\mathbf{Set}_P$ making the following diagram commute

$$\begin{tikzcd} B_P \arrow[r, "\gamma"] \arrow[d, "\alpha"'] & (\Gamma_B)_P \arrow[dl, dotted, "\beta"] \\ G_P & \end{tikzcd} .$$

A necessary condition for such a map β to exist is that $|\alpha(b_i)| = |\alpha(b_j)|$ for all $b_i, b_j \in B$. This is not always the case:

- Consider the fusion law $\mathrm{Irr}(D_6) = \{\chi_1, \chi_2, \chi_3\}$ from example 1.2.8. Then take any nontrivial finite group G and define the following map between the corresponding magmas in $\mathbf{Set}_P$

  $$\alpha\colon \mathrm{Irr}(D_6) \to G\colon \begin{cases} \chi_1 & \mapsto \{1\}, \\ \chi_2 & \mapsto \{1\} \\ \chi_3 & \mapsto G. \end{cases}$$

  This map α can not factor through $\Gamma_{\mathrm{Irr}(D_6)} = 1$.

- Consider the fusion law $\mathrm{Irr}(Q_8) = \{\chi_1, \chi_i, \chi_j, \chi_k, \chi\}$, with $\chi_i\chi_j\chi_k = \chi_1$ and $(\chi_x)^2 = \chi_1$ for $x = i, j, k$ and $\chi^2 = \chi_1 + \chi_i + \chi_j + \chi_k$. Notice that $\{\chi_1, \chi_i, \chi_j, \chi_k\}$ forms a group $N \cong C_2 \times C_2$ under multiplication. Let $G = N \times H$, with $H = \langle g \rangle$ a cyclic group of order two. Then define the following map of magmas in $\mathbf{Set}_P$

  $$\alpha\colon \mathrm{Irr}(Q_8) \to G\colon \begin{cases} \chi_x & \mapsto \{(\chi_x, 1)\} \quad \text{for } x \in \{1, i, j, k\}, \\ \chi & \mapsto N \times \{g\}. \end{cases}$$

  The difference between the cardinalities $|\alpha(\chi_1)|$ and $|\alpha(\chi)|$ prevents α from factoring over $\Gamma_{\mathrm{Irr}(Q_8)} = C_2 \times C_2$.

At the same time, the issue raised in the above remark is essentially the only thing preventing $\gamma\colon B \to \Gamma_B$ from being a categorical universal object. More precisely, α will factor over Γ_B if and only if $|\alpha(1)|$ is "large enough" in the sense that $|\alpha(1)| = |\alpha(\delta(1))|$.

Corollary 3.2.16. *Let (R, B) be a fusion ring and $(B, *)$ the corresponding fusion law. Let G be a finite group, and let $\alpha\colon B \to G$ be a map of magmas in $\mathbf{Set}_P$ such that $G = \bigcup_{b\in B} \alpha(b)$. There exists a unique map $\tilde{\alpha}$ of magmas in $\mathbf{Set}_P$, making the following diagram commute (in $\mathbf{Set}_P$)*

$$\begin{tikzcd} B \arrow[r, "\gamma"] \arrow[d, "\alpha"'] & \Gamma_B \arrow[dl, dotted, "\tilde{\alpha}"] \\ G & \end{tikzcd} ,$$

if and only if $(\alpha \circ \delta)(1) = \alpha(1)$.

Proof. Note that uniqueness is guaranteed by lemma 3.2.12. Indeed, if $\tilde{\alpha} \circ \gamma = \alpha$, then $\tilde{\alpha} = \alpha \circ \delta$. This also shows the "only if" direction.

Now suppose $(\alpha \circ \delta)(1) = \alpha(1)$ and let $N \trianglelefteq G$ be the normal subgroup $(\alpha \circ \delta)(1)$ of G as in theorem 3.2.14. By assumption, it thus holds that $\alpha(1) = N$. Now let $b_i \in B$ be arbitrary, then

$$\alpha(b_i) = \alpha(b_i * 1) = \alpha(b_i)N.$$

Hence $\alpha(b_i)$ is equal to the full coset $(\alpha \circ \delta)(\gamma(b_i))$ of N (see the proof of proposition 3.2.9). Now we can define $\tilde{\alpha}\colon \Gamma_B \to G$ by

$$\tilde{\alpha}(\gamma(b_i)) \coloneqq \alpha(b_i) = \alpha(b_i) \cdot N \quad \text{for all } b_i \in B \ .$$

As $\gamma(B) = \Gamma_B$ by lemma 3.2.12, this completely defines $\tilde{\alpha}$. It is a map of magmas in $\mathbf{Set}_P$ as, for all $b_i, b_j \in B$,

$$\tilde{\alpha}(\gamma(b_i)\gamma(b_j)) = \alpha(b_i b_j)N = (\alpha(b_i)N)(\alpha(b_j)N) = \tilde{\alpha}(\gamma(b_i))\tilde{\alpha}(\gamma(b_j)).$$

The diagram then commutes by construction. ■

We conclude that despite the natural motivation, the magmas in $\mathbf{Set}_P$ are not as well-behaved as the category **Fus**, in the context of decomposition algebras. Besides the issue with the finest grading, it is not completely clear if other concepts, such as (fibered) products exist and give rise to interesting notions in the context of decomposition algebras. It seems that it would be better to consider a (perhaps slightly) different category than $\mathbf{Fam}_P$. Also, the story would not end there, as there is then the question of creating a '**Fam**-like' category out of that category, to allow for multiple different decompositions. We will not delve deeper into these questions here.

4 Matsuo algebras in characteristic 2

4.1 Motivation

Let R be a commutative ring (unital and associative). An *axial algebra of Jordan type* $\alpha \in R$ is an axial algebra over R (definition 1.2.18) for the Jordan fusion law (example 1.2.3), under the assignment $e = 1, z = 0, h = \alpha$. Such an algebra is called *primitive* if each axis generates its own 1-eigenspace. The primitive axial algebras of Jordan type $\alpha \neq \frac{1}{2}$ over fields of characteristic different from 2 were characterized by Hall, Rehren and Shpectorov in [HRS15a, Theorem 6.3] in terms of *Matsuo algebras* arising from 3-transposition groups.

In characteristic 2, we cannot expect many interesting axial algebras of Jordan type α. Indeed, suppose A is such an algebra and a is one of its axes. Let $b \in A$ be another axis and write $b = b_1 + b_0 + b_\alpha$, where each b_x is the projection of b onto the x-eigenspace of a, for $x = 1, 0, \alpha$. Then, as A is commutative,

$$b^2 = (b_1 + b_0 + b_\alpha)^2 = b_1^2 + b_0^2 + b_\alpha^2.$$

By definition of the Jordan fusion law, the expression on the right is contained in the sum of the 0- and 1-eigenspaces of a. Hence we have that $b_\alpha = 0$.

More generally, take any ring R of characteristic two, an axial algebra A over R and a fusion law $X \subseteq R$ such that A is an X-axial algebra. If X is $\mathbb{Z}/2$-graded, then for all $x \in X$ belonging to the non-trivially graded part and all axes a, it holds that the x-eigenspace of a is zero. To avoid a $\mathbb{Z}/2$-grading on the Jordan fusion law, we can modify it by adding that $h \in h * h$. Under the assignment $e = 1, z = 0, h = \alpha$, this gives us the fusion law presented in the table below.

$*$	1	0	α
1	1	$\emptyset$	α
0	$\emptyset$	0	α
α	α	α	$1+0+\alpha$

Interstingly, a class of axial algebras that satisfies this fusion law is again given by certain Matsuo algebras, as we show in this section.

4.2 Definition

Matsuo algebras can be defined from certain geometries, where each line contains exactly three points.

Definition 4.2.1. A *partial triple system* $\Pi = (\mathcal{P}, \mathcal{L})$ is a pair consisting of a set $\mathcal{P}$, called *points* and a set $\mathcal{L}$ of subsets of $\mathcal{P}$, called *lines*, such that the following two conditions are satisfied.

1. Every line contains exactly three points.
2. Every two points are contained in at most one line.

Definition 4.2.2. Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a partial triple system.

1. Two points $x, y \in \mathcal{P}$ are called *collinear* if there exists a line that contains them both. We write $x \sim y$ if they are collinear and $x \not\sim y$ if they are not.
2. Given two collinear points x, y, we denote the third point on the unique line through x and y by $x \wedge y = y \wedge x$.
3. We call a point $x \in \mathcal{P}$ *isolated* if it is not collinear with any other point.
4. A *subspace* $\Pi' = (\mathcal{P}', \mathcal{L}')$ of Π is a pair of subsets $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{L}' \subseteq \mathcal{L}$ of the points and lines, such that each line $l \in \mathcal{L}$ which contains at least two points of $\mathcal{P}'$, is a line of Π. That is, all points of l are contained in $\mathcal{P}'$ and l is an element of $\mathcal{L}'$.
5. The subspace *generated* by a subset of points $\mathcal{P}'$ of $\mathcal{P}$ is the smallest subspace $(\mathcal{P}'', \mathcal{L}'')$ such that $\mathcal{P}' \subseteq \mathcal{P}''$.
6. A subspace generated by the points of two distinct intersecting lines is called a *plane*.
7. A partial triple system $\Pi = (\mathcal{P}, \mathcal{L})$ is said to satisfy *Pasch's axiom* ([Cuy05]) if every plane of Π is isomorphic[1] to the *dual affine plane of order two*: $\mathrm{DA}(2,2)$. The point set of $\mathrm{DA}(2,2)$, may be taken to be $\{a, b, c, x, y, z\}$, with lines

$$\begin{aligned} &\{a,b,c\}, \quad \{a,z,y\},\\ &\{x,z,b\}, \quad \{x,y,c\}. \end{aligned}$$

An illustration is given in fig. 4.1.

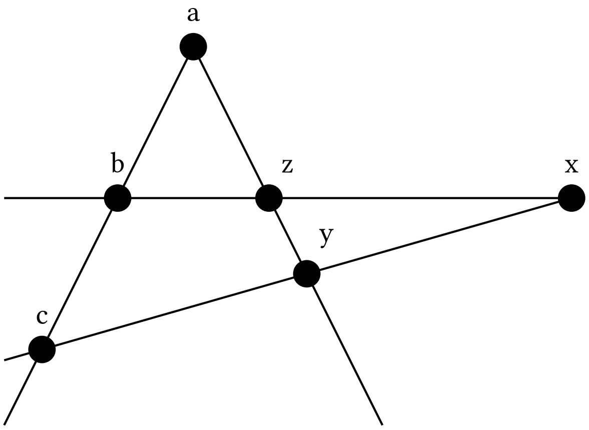


Figure 4.1: The dual affine plane of order two.

Definition 4.2.3. Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a partial triple system. Let k a field and take some $\alpha \in k$. Define the *Matsuo algebra* $M(\Pi, \alpha, k)$ as the vector space with basis $\mathcal{P}$ and multiplication given by linearly extending

$$xy = \begin{cases} x & \text{if } x = y \\ \alpha(x + y - x \wedge y) & \text{if } x \sim y \\ 0 & \text{if } x \not\sim y \end{cases}$$

Note that we make no distinction in notation between a point in a partial triple system Π and the corresponding vector of $M(\Pi, \alpha, k)$. We shall also say that a point p *belongs to* a subset $A \subseteq M(\Pi, \alpha, k)$ if A contains the corresponding vector.

[1] That is, there exists a bijection between the set of points such that the induced map on the set of lines is also a bijection.

Notation 4.2.4. When dealing with the dual affine plane of order two, it will be useful to consistently label the set of points by $\{a,b,c,x,y,z\}$, with the lines

$$\begin{array}{ll} \{a,b,c\}, & \{a,z,y\}, \\ \{x,z,b\}, & \{x,y,c\}, \end{array}$$

as in definition 4.2.2 and fig. 4.1.

4.3 Axiality

We now show that if k is a field of characteristic 2, $\alpha \in k \setminus \{0,1\}$ and Π is a partial triple system satisfying Pasch's axiom, then $M(\Pi,\alpha,k)$ is an axial algebra. This is based on the following lemmas.

Lemma 4.3.1. *Consider the dual affine plane of order two $\Pi = \mathrm{DA}(2,2)$, with labeling of the points as in as in notation 4.2.4, and let k be a field of characteristic 2. Let $\alpha \in k \setminus \{0,1\}$ and consider the Matsuo algebra $A = M(\Pi,\alpha,k)$. Then $e = a+b+c$ is an idempotent of A and the corresponding operator ad_e on A, given by (left) multiplication with e, is semisimple. Its eigenvalues are $1,0,\alpha$, with corresponding eigenspaces A_1, A_0, A_α given by*

$$\begin{aligned} A_1 &= \langle a,b,c\rangle, \\ A_0 &= \langle x+y+z\rangle, \\ A_\alpha &= \langle a+b+\tfrac{\alpha+1}{\alpha}x+\tfrac{\alpha+1}{\alpha}y, a+c+\tfrac{\alpha+1}{\alpha}x+\tfrac{\alpha+1}{\alpha}z\rangle. \end{aligned}$$

Proof. Note that $ax = ay$ and $az = 0$, whence $a(x+y+z) = 0$. Then the equality $(a+b+c)(x+y+z) = 0$ follows by symmetry in a, b and c. A similar calculation shows that a, b and c are three 1-eigenvectors.

Now consider A_α. Using the symmetry of Π, it suffices to verify that $a+b+\frac{\alpha+1}{\alpha}x+\frac{\alpha+1}{\alpha}y$ is an α-eigenvector of e. The lemma will then follow, as A is six-dimensional and we now already know that $A_1 \oplus A_0$ is at least four-dimensional. This last computation is carried out below.

$$\begin{aligned} (a+b+c)(a+b+\frac{\alpha+1}{\alpha}x+\frac{\alpha+1}{\alpha}y) =& [(a+b+c)(a+b)] + \frac{\alpha+1}{\alpha}[(a+b+c)(x+y)] \\ =& [(a+b)+4\alpha(a+b+c)] \\ & + (\alpha+1)[(a+y+z)+(b+x+z)+2(c+x+y)] \\ =& \alpha(a+b+\frac{\alpha+1}{\alpha}x+\frac{\alpha+1}{\alpha}y) \end{aligned}$$ ■

Lemma 4.3.2. *Let $\Pi = (\mathcal{P},\mathcal{L})$ be a partial triple system satisfying Pasch's axiom, k a field of characteristic 2 and $\alpha \in k \setminus \{0,1\}$. Take any line $\{a,b,c\} \in \mathcal{L}$ and consider the corresponding idempotent $e = a+b+c$ of the Matsuo algebra $A = M(\Pi,\alpha,k)$. Then ad_e is semisimple, with eigenvalues 0, 1 and α.*

1. *The 1-eigenspace is spanned by $\{a,b,c\}$.*
2. *The 0-eigenspace is spanned by all vectors $x+y+z$ such that $\{a,b,c,x,y,z\}$ determines a plane in Π, together with all points p, not collinear to any point of $\{a,b,c\}$.*
3. *The α-eigenspace is spanned by all vectors of the form $a+b\frac{\alpha+1}{\alpha}x+\frac{\alpha+1}{\alpha}y$, $a+c+\frac{\alpha+1}{\alpha}x+\frac{\alpha+1}{\alpha}z$ and $b+c+\frac{\alpha+1}{\alpha}y+\frac{\alpha+1}{\alpha}z$, whenever $\{a,b,c,x,y,z\}$ determines a plane in Π, with the lines as in notation 4.2.4.*

Proof. Consider any point p. If p lies in common plane with $\{a, b, c\}$, then p is a linear combination of eigenvectors with eigenvalues $0, 1, \alpha$ by lemma 4.3.1. On the other hand, p does not lie in a common plane with $\{a, b, c\}$, then it is a zero eigenvector. Thus the eigenvectors of ad_e span the whole of A and have the claimed eigenvalues. ■

Definition 4.3.3. Let Π be a partial triple system, k a field of characteristic 2 and $\alpha \in k$. For each line $\{a, b, c\}$, we call $e = a + b + c$ the corresponding *line idempotent* of $M(\Pi, \alpha, k)$.

Lemma 4.3.4. *Let* $\Pi = \mathrm{DA}(2, 2)$ *be the dual affine plane of order two,* k *a field of characteristic* 2 *and* $\alpha \in k \setminus \{0, 1\}$*. The Matsuo algebra* $A = M(\Pi, \alpha, k)$ *is generated by the set of line idempotents.*

Proof. We use the labeling from notation 4.2.4. It suffices to show that a can be written as a linear combination of products of these idempotents. We have the following equality:

$$\begin{aligned}(a + b + c)(a + y + z) &= a + (ay + az) + (ba + ca) + (bz + cy)\\ &= a + \alpha(b + z + c + y),\end{aligned}$$

as $ay + az = ba + ca = 0$. If we add

$$\alpha\left((a + b + c) + (a + z + y)\right)$$

to this last expression, then we indeed obtain a. ■

Lemma 4.3.5. *Let* $\Pi = (\mathcal{P}, \mathcal{L})$ *be a partial triple system satisfying Pasch's axiom,* k *a field of characteristic* 2 *and* $\alpha \in k \setminus \{0, 1\}$*. Consider the subalgebra* A*, of the Matsuo algebra* $M(\Pi, \alpha, k)$*, generated by the line idempotents. Then every point* p *that is contained in some plane of* Π *belongs to* A*.*

Proof. This follows immediately from lemma 4.3.4. ■

It remains to examine the multiplication between the eigenspaces of the line idempotents.

Definition 4.3.6. We use $\mathcal{J}_\alpha$ to denote the fusion law on $\{1, 0, \alpha\}$ given by the following table.

$*$	1	0	α
1	1	$\emptyset$	α
0	$\emptyset$	0	α
α	α	α	$1 + 0 + \alpha$

Lemma 4.3.7. *Let* $\Pi = \mathrm{DA}(2, 2)$ *be the dual affine plane of order two,* k *a field of characteristic* 2 *and* $\alpha \in k \setminus \{0, 1\}$*. The Matsuo algebra* $A = M(\Pi, \alpha, k)$ *is a* $\mathcal{J}_\alpha$*-axial algebra over* k*, with axes given by the line idempotents.*

Proof. This follows from straightforward computations, using lemmas 4.3.1 and 4.3.4. We make some observations for each of the cases. We take a line idempotent $e = a + b + c$ (using the labeling from notation 4.2.4) and observe that:

1. The 1-eigenspace is always commutative, associative subalgebra. In particular, it holds that $A_1 A_1 \subseteq A_1$.
2. The zero eigenspace is contained in the zero eigenspaces of all three points summing to line idempotent. This implies that the rule $1 * 0 = \emptyset$ is satisfied.
3. To check that $1 * \alpha = \{\alpha\}$ is satisfied, it suffices to compute that

$$a(a + b + \frac{\alpha + 1}{\alpha}x + \frac{\alpha + 1}{\alpha}y) = \alpha(b + c + \frac{\alpha + 1}{\alpha}y + \frac{\alpha + 1}{\alpha}z).$$

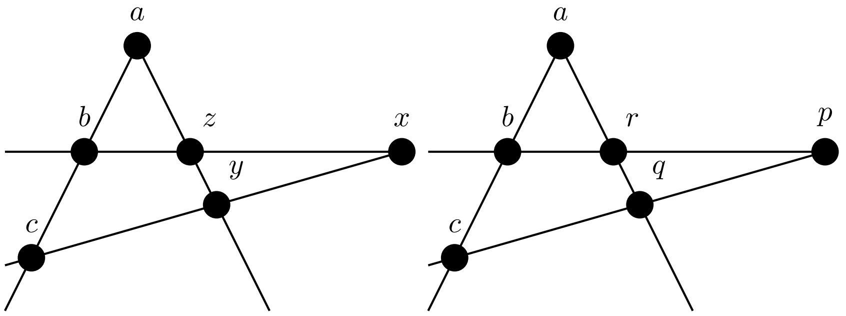
4. To verify that $0 * \alpha = \{\alpha\}$ is satisfied, it suffices to compute that

$$\begin{aligned}(x+y+z)(a+b+\frac{\alpha+1}{\alpha}(x+y)) &= (xb+zb)+(ya+za)\\ &\quad+\frac{\alpha+1}{\alpha}[x+y+(xy+yx)+(zx+zy)]\\ &= \frac{\alpha+1}{\alpha}(x+y)+(\alpha+1)((z+x+b)+(z+y+a))\\ &= (\alpha+1)(a+b+\frac{\alpha+1}{\alpha}x+\frac{\alpha+1}{\alpha}y).\end{aligned}$$

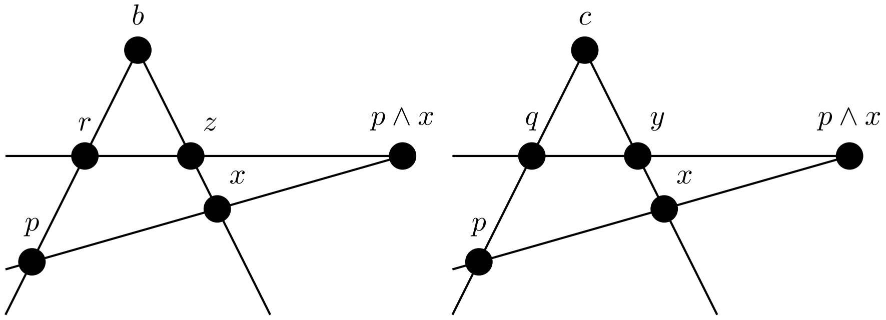
5. Let A_1, A_0, A_α be the $0, 1, \alpha$-eigenspaces with respect to $e = a+b+c$ (labeling as in notation 4.2.4). Then $A_\alpha A_\alpha \subseteq A_{\{1,0,\alpha\}} = A$ is automatic. Note, however, that $\alpha \in \alpha * \alpha$ is necessary, since $A_\alpha \neq 0$ (as we argued in the motivation). Direct computations can also show that $A_\alpha A_\alpha \nsubseteq A_1 + A_\alpha$ and $A_\alpha A_\alpha \nsubseteq A_0 + A_\alpha$. Thus the fusion law $\mathcal{J}_\alpha$ is the "finest" fusion law on A.

Finally, note that A is indeed generated by the line idempotents by the above lemma 4.3.4. ■

Notation 4.3.8. In the following lemmas, we examine the multiplication between points that are both collinear to a point of a certain line $\{a, b, c\}$, but do not lie in the same plane through that line. We thus consider two different planes, intersecting in a line. We will label the points of these two plane by $\{a, b, c, x, y, z\}$ and $\{a, b, c, p, q, r\}$, respectively, with the lines as in the illustration below.



Lemma 4.3.9. *Let* Π *be a partial triple system satisfying Pasch's axiom and consider two planes intersecting in a line* $\{a, b, c\}$*, as in notation 4.3.8. If* $p \sim x$*, then the planes spanned by* $\{p, r, b, z, x\}$ *and* $\{p, q, c, y, x\}$ *are given by the following configurations.*



In particular, it holds that

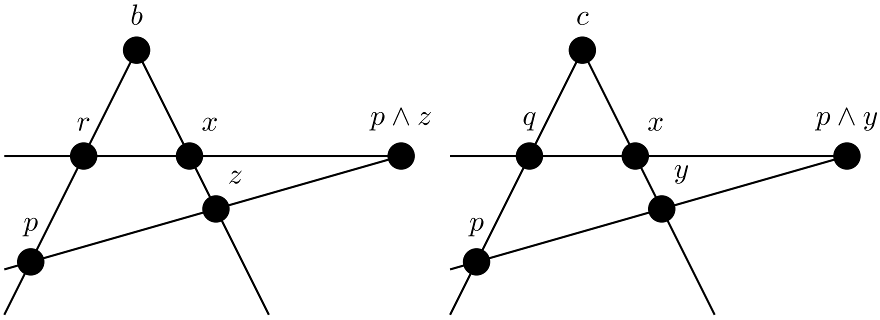
$$p \wedge x = q \wedge y = r \wedge z.$$

Moreover, it holds that

$$q \not\sim z \text{ and } r \not\sim y.$$

Proof. The plane spanned by the intersecting lines $\{b, r, p\}$ and $\{b, z, x\}$ is isomorphic to the dual affine plane of order two, and is thus completely determined by $p \sim x$. Furthermore, since $r \sim a$ and $r \sim z$, it follows that $r \not\sim y$, as r can only be collinear with at most two points of the line $\{a, y, z\}$. By similar reasoning, it holds that the plane spanned by $\{p, q, c\}$ and $\{c, y, x\}$ is given by the plane in the illustration and $q \not\sim z$. ■

Lemma 4.3.10. *Let Π be a partial triple system satisfying Pasch's axiom and consider two planes intersecting in a line $\{a, b, c\}$, as in notation 4.3.8. If $p \not\sim x$, then the planes spanned by $\{p, r, b, z, x\}$ and $\{p, q, c, y, x\}$ are given by the following configurations.*



Moreover, it holds that

$$q \sim z, r \sim y \text{ and } q \wedge z = r \wedge y,$$

and that

$$\{a, q \wedge x, r \wedge x\}.$$

is a line in Π.

Proof. As in the previous lemma, the plane spanned by the lines $\{c, q, p\}$ and $\{c, x, y\}$ (resp. the plane spanned by $\{b, r, p\}$ and $\{b, x, z\}$) is uniquely determined by the knowledge that $p \not\sim x$. This implies that $q \not\sim y$. But as $q \sim a$, it follows that q must be collinear with a second point on the line $\{a, y, z\}$, whence $q \sim z$. Similarly, it holds that $r \sim y$. By considering the plane spanned by the lines $\{a, y, z\}$ and $\{a, q, r\}$, we then see that $q \wedge z = r \wedge y$. For the the last statement, take the plane spanned by $\{a, q, r\}$ and $\{x, q, q \wedge x\}$. The fact that this plane is isomorphic to the dual affine plane of order two then forces that $\{a, q \wedge x, r \wedge x\}$ is a line in Π. ■

Lemma 4.3.11. *Let Π be a partial triple system satisfying Pasch's axiom and consider two planes intersecting in a line, as in notation 4.3.8. Write e for the line idempotent $e = a + b + c$. Then the product $(p + q + r)(x + y + z)$ is again a zero eigenvector for ad_e.*

Proof. First assume that we are in the situation of lemma 4.3.9. Then we have $px = \alpha(p + x + p \wedge x)$ and $p \wedge x = q \wedge y = r \wedge z$. It follows that

$$(p + q + r)(x + y + z) = \alpha(p + q + r + x + y + z + 3(p \wedge x)).$$

As, in this situation, $p \wedge x$ is not collinear with any of point of $\{a, b, c\}$, it follows from the description of the zero eigenspace (lemma 4.3.2) that this product again belongs to the zero eigenspace.

Now consider the situation of lemma 4.3.10. We compute that

$$\begin{aligned}(p+q+r)(x+y+z) &= (py+pz)+(qx+qz)+(rx+ry)\\ &= \alpha((p\wedge y+p\wedge z)+(q\wedge x+q\wedge z)+(r\wedge x+r\wedge y))\\ &= \alpha((p\wedge y+p\wedge z)+(p\wedge y+q\wedge z)+(p\wedge z+q\wedge z))\\ &= 0.\end{aligned}$$

To go from the second to the third line, observe that p, q, r, x, y, z all appear exactly twice in this sum and thus cancel out. ■

Lemma 4.3.12. *Let Π be a partial triple system satisfying Pasch's axiom and consider two planes intersecting in a line, as in notation 4.3.8. Write e for the line idempotent $e = a+b+c$. Then the product $(b+c+\frac{\alpha+1}{\alpha}q+\frac{\alpha+1}{\alpha}r)(x+y+z)$ is an α-eigenvector of ad_e.*

Proof. We again start by considering the case $p \sim x$, as in lemma 4.3.9, and compute the product

$$\begin{aligned}(b+c+\frac{\alpha+1}{\alpha}(q+r))(x+y+z) &= (b+c)(x+y+z)+\frac{\alpha+1}{\alpha}(q+r)(x+y+z)\\ &= (\alpha+1)((q+y+q\wedge y)+(r+z+r\wedge z))\\ &= \alpha(b+c+\frac{\alpha+1}{\alpha}(y+z))+\alpha(b+c+\frac{\alpha+1}{\alpha}(q+r)).\end{aligned}$$

This last expression is contained in the α-eigenspace of ad_e by lemma 4.3.2. The second equality follows from $1 * 0 = \emptyset$, by lemma 4.3.7. In the final step, we have used that $q \wedge y = r \wedge z$.

Now consider the case $p \not\sim x$, as in lemma 4.3.10. Then we have that

$$\begin{aligned}(b+c+\frac{\alpha+1}{\alpha}(q+r))(x+y+z) &= (b+c)(x+y+z)+\frac{\alpha+1}{\alpha}[(qx+qz)+(rx+ry)]\\ &= (\alpha+1)(y+z+q\wedge x+q\wedge z+r\wedge x+r\wedge y)\\ &= (\alpha+1)(y+z+q\wedge x+r\wedge x)\\ &= \alpha(b+c+\frac{\alpha+1}{\alpha}(y+z))+\alpha(b+c+\frac{\alpha+1}{\alpha}(q\wedge x+r\wedge x)).\end{aligned}$$

As $\{a, q\wedge x, r\wedge x\}$ is a line in Π and both $b \not\sim r\wedge x$ and $c \not\sim q\wedge x$, the two summands in the last line are α-eigenvectors of ad_e by lemma 4.3.2. For the second to last equality, we used that $q\wedge z = r\wedge y$. ■

Theorem 4.3.13. *Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a partial triple system, k a field of characteristic 2 and $\alpha \in k\setminus\{0,1\}$. Let A be the subalgebra of the Matsuo algebra $M(\Pi, \alpha, k)$, generated by the set of all line idempotents. Then A is a $\mathcal{J}_\alpha$-axial algebra and every point p which belongs to some plane in Π is contained in A.*

Proof. The line idempotents are semisimple, with eigenspaces given by lemma 4.3.2. The fact that the corresponding eigenspaces satisfy the fusion law $\mathcal{J}_\alpha$ follows from lemmas 4.3.7, 4.3.11 and 4.3.12. The last claim follows from lemma 4.3.5. ■

Remark 4.3.14. In the context of axial algebras of Jordan type, the interesting Matsuo algebras are defined by *Fischer spaces*. These spaces arise from 3-transposition groups: pairs (G, D) of a group G and a normal generating set of involutions D such that the order of the product of two elements of D is at most 3. To a 3-transposition group, we can associate a geometry $g(G, D)$, whose points are the elements of D and where $\{a, b, c\}$ is a line if and only if $a^b = c$. The corresponding geometries are *Fischer spaces*: partial triple systems where every plane is either isomorphic to the dual affine plane of order two or the affine plane of order three. When k is a field not of characteristic 2, then all axial algebras of Jordan type $\eta \neq \frac{1}{2}$ are of the form $(\bigoplus_{i \in I} k) \oplus M$, where M is a quotient of a Matsuo algebra defined by a Fischer space ([HRS15a, Theorem 5.4,Theorem 6.3]).

If we allow all Fischer spaces in our setting here, where $\mathrm{char}(k) = 2$, then the corresponding line idempotents are no longer semisimple. Indeed, if Π is the dual affine plane of order three, then the line idempotents are no longer semisimple. They still have eigenvalues $0, 1, \alpha$, but the dimension of the 0-eigenspace is 1, while the algebraic multiplicity of 0 is 2. When we consider the generalized eigenspaces, the same fusion law seems to hold. However, to verify this for an arbitrary Fischer space, the approach used here would require many case distinctions.

In that case, a more systematic approach would be desirable. Another question that could also be addressed further consists of analyzing the ideals and quotients of the algebras presented here.

5 Conclusion

We conclude this thesis with a short summary of the main ideas. We have examined three main questions, each connecting to different areas of mathematics, but all motivated by the single goal of better understanding decomposition algebras in positive characteristic.

First, we started from the representation fusion law of a finite group G: the fusion law on the set of irreducible complex characters $\mathrm{Irr}(G)$, given by examining tensor products of characters. By replacing 'irreducible characters' with 'isomorphism classes of simple modules', we (trivially) obtained a reformulation which can also be stated in positive characteristic. This fusion law can be derived from the corresponding Grothendieck ring of kG. The elegant description of the universal grading of this fusion law when $k = \mathbb{C}$ can then be traced back to the observation that the Grothendieck ring of $\mathbb{C}G$ admits the structure of a fusion ring.

Although the definition of the Grothendieck ring is very abstract, its structure can be explicitly determined from the modular characters of the finite group. We then applied this knowledge to understand the tensor product of blocks of the group ring kG. As every kG-module admits a direct sum decomposition indexed by these blocks, this provides a fusion law on any k-algebra A with $G \leq \mathrm{Aut}(A)$. It turns out that this block fusion law is completely determined when we know both the Grothendieck ring and the composition factors of the projective indecomposable kG-modules.

We then examined a possible new category of fusion laws which admitted multi-valued homomorphisms. This category arises naturally when we try to consider fusion laws as (categorical) algebraic objects in an appropriate category. Despite its natural motivation, this category fails to explain the finest grading of a fusion law as a universal property. For the fusion laws obtained from fusion rings, such a property still almost holds, as made precise in theorem 3.2.14.

Finally, we examined a class of Matsuo algebras in characteristic 2. Usually, these algebras are defined over fields with characteristic different from 2 and they play a central role in the classification of axial algebras of Jordan type. When we interpret their definition in characteristic 2, some of these algebras still have generating set of semisimple idempotents, corresponding to lines in the defining geometry. The eigenspaces all have a geometric interpretation and we used this to verify that a fusion law close to the Jordan fusion law is satisfied.

A Summary (Dutch)

Deze thesis behandelt decompositie-algebra's, met een focus algebras over een veld met positieve karakteristiek.

Decompositie-algebra's vormen een klasse van niet-associatieve algebra's. Bij definitie laat zo een algebra verschillende (minstens één) directe som-decomposities toe. Bij elk van deze decomposities wordt de vermenigvuldiging tussen twee verschillende sommanden gecontroleerd door een fusiewet. Een belangrijke klasse van fusiewetten, wordt gegeven door de representatiefusiewetten van eindige groepen. Deze worden bepaald door het tensorproduct van de complexe karakters van de groep. Een tweede link met groepentheorie wordt gegeven door de Miyamotogroep. Dit is een (typisch grote) groep van automorfismen van de decompositie-algebra die bestaan wanneer de fusiewet gegradeerd is. In het eerste hoofdstuk worden deze concepten precies gedefinieerd en geven we een overzicht van een aantal basisbegrippen uit de theorie van decompositie-algebra's en de representatietheorie.

In het tweede hoofdstuk focussen we ons dan op het concept van de representatiefusiewet van een eindige groep. Deze is in eerste instantie slechts gedefinieerd in karakteristiek nul gezien ze leeft op de verzameling van complexe karakters van de groep. We buigen ons over de vraag of we een soortgelijke fusiewet kunnen formuleren in positieve karakteristiek. Dit is inderdaad zo, en relatief eenvoudig eens we de juiste concepten uit de representatietheorie ingevoerd hebben. Concreet bouwen we een fusiewet op de blokken van de groepsalgebra kG. De Grothendieck ring van de groepsalgebra kG en de daaraan gelinkte modulaire karakters van G helpen dan om deze fusiewet te begrijpen. Ondertussen betrekken we ook het concept van fusieringen in en presenteren we de afleiding van de universele gradering van de representatiefusiewet in deze context.

Fusieringen zijn gelinkt aan het abstract concept van tensorcategorieëen. In zo een categorie kunnen we het concept van 'een algebra' volledig in categorische termen uitdrukken. We beginnen het derde hoofdstuk met de volgende observatie: als we een categorie wensen te bekomen waarvan de algebra's juist de decompositie-algebra's zijn, dan is het natuurlijk om een categorie van fusiewetten te onderzoeken waar meerwaardige afbeeldingen tussen fusiewetten toegelaten zijn. We tonen aan dat, ondanks de natuurlijke motivatie, de universele gradering van een fusiewet dan niet langer een universeel categorisch object is. Voor fusiewetten afgeleid uit fusieringen geven we exact aan tot op welke hoogte dit fout loopt.

In het vierde en laatste hoofdstuk bespreken we Matsuo algebra's over velden van karakteristiek 2. In karakteristiek verschillend van 2 spelen deze algebra's, afkomstig van meetkundes met drie punten per rechte, een hoofdrol in de classificatie van axiale algebra's van Jordan-type [HRS15a, Theorems 6.3,6.4]. We observeren dat in karakteristiek gelijk aan twee een subklasse van deze algebra's nog steeds een axiale structuur heeft. Specifiek bekijken we algebra's uit meetkundes waar elk vlak isomorf is aan het duaal affien vlak van orde twee. We tonen aan dat bepaalde deelalgebra's dan nog steeds een axiale structuur hebben. De voortbrengende idempotenten (assen) corresponderen met lijnen in de onderliggende meetkunde. De eigenruimten van deze idempotenten vermenigvuldigen volgens een fusiewet die bijna gelijk is aan de Jordan fusiewet.

Bibliography

[CDL06] S. Caenepeel and M. De Lombaerde. A categorical approach to Turaev's Hopf group-coalgebras. *Comm. Algebra*, 34(7):2631–2657, 2006.

[CG21] Maurice Chayet and Skip Garibaldi. A class of continuous non-associative algebras arising from algebraic groups including E_8. *Forum Math. Sigma*, 9:Paper No. e6, 22, 2021.

[Cou20] Michiel Van Couwenberghe. *Decomposition algebras and axial algebras.* PhD thesis, Ghent University, sep 2020.

[CR81] Charles W. Curtis and Irving Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons, Inc., New York, 1981. With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[Cuy05] Hans Cuypers. Lie algebras and cotriangular spaces. *Bull. Belg. Math. Soc. Simon Stevin*, 12(2):209–221, 2005.

[DPSV20] Tom De Medts, Simon F. Peacock, Sergey Shpectorov, and Michiel Van Couwenberghe. Decomposition algebras and axial algebras. *Journal of Algebra*, 556:287 – 314, 2020.

[GN08] Shlomo Gelaki and Dmitri Nikshych. Nilpotent fusion categories. *Advances in Mathematics*, 217(3):1053–1071, 2008.

[Gri82] Robert L. Griess, Jr. The friendly giant. *Invent. Math.*, 69(1):1–102, 1982.

[HRS15a] J. I. Hall, F. Rehren, and S. Shpectorov. Primitive axial algebras of Jordan type. *J. Algebra*, 437:79–115, 2015.

[HRS15b] J.I. Hall, F. Rehren, and S. Shpectorov. Universal axial algebras and a theorem of sakuma. *Journal of Algebra*, 421:394–424, 2015. Special issue in memory of Ákos Seress.

[IGNO15] Pavel I. Etingof, Shlomo Gelaki, Dmitri Nikshych, and Victor Ostrik. *Tensor Categories.* The American Mathematical Society, Providence, Rhode Island, 2015.

[Iva09] A. A. Ivanov. *The Monster group and Majorana involutions*, volume 176 of *Cambridge Tracts in Mathematics.* Cambridge University Press, Cambridge, 2009.

[MC20] Tom De Medts and Michiel Van Couwenberghe. Non-associative frobenius algebras for simply laced chevalley groups, 2020.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edtition edition, 1998.

[Moe02] I. Moerdijk. Monads on tensor categories. *Journal of Pure and Applied Algebra*, 168(2):189–208, 2002. Category Theory 1999: selected papers, conference held in Coimbra in honour of the 90th birthday of Saunders Mac Lane.

[Ost03] Viktor Ostrik. Module categories, weak hopf algebras and modular invariants. *Transformation Groups*, 8:177–206, jun 2003.

[Rot71] Richard L. Roth. On the conjugating representation of a finite group. *Pacific J. Math.*, 36:515–521, 1971.

[Ser77] Jean-Pierre Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977.

[Web16] Peter Webb. *A course in finite group representation theory*, volume 161 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2016.

[Zim14] Alexander Zimmermann. *Representation theory*, volume 19 of *Algebra and Applications*. Springer, Cham, 2014. A homological algebra point of view.