universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

„Principal indecomposable modules for the Alternating group on five symbols in modular characteristic“

Verfasser

Felix Leditzky

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag.rer.nat.)

Wien, 2012

Studienkennzahl lt. Studienblatt:	A 405
Studienrichtung lt. Studienblatt:	Mathematik
Betreuer:	Ao. Univ.-Prof. Dr. Joachim Mahnkopf

Contents

Acknowledgments

I first encountered the subject of representation theory in a lecture held by Joachim Mahnkopf, where he briefly touched the field of modular representation theory and pointed out its interesting features. Upon approaching him with the request to write a thesis about representation theory, he assigned me with the task of classifying the principal indecomposable representations of the Alternating group on five symbols, the smallest non-abelian simple group. Working on this subject proved to be a great way to familiarize myself with modular representation theory and lay a solid foundation for further studies. Therefore, I would like to thank Joachim Mahnkopf for acquainting me with the topic as well as supervising me in a most uncomplicated and helpful way.

For thorough proofreading and checking the mathematical consistency of the text, I want to thank my colleague Christoph Harrach. Furthermore, I also thank my good friend András Bárány for making numerous suggestions regarding linguistic issues and layout problems. Special thanks go to my colleague Hongyi Chu for his tireless willingness to discuss mathematical problems I encountered while working on this thesis.

I am grateful to my parents for giving me the financial opportunity to pursue my studies. Last but not least, I feel very much obliged to thank Nadja Buisman, not only for correcting grammatical and linguistic errors in the text but also for her patience without cease and understanding during the time-consuming process of writing. Without her support, I would not have been able to finish this thesis.

Introduction

The theory of modular representations assumes that the group order is divisible by the characteristic of the field. The subject was first investigated by L.E. Dickson in the early 20th century in a series of papers, where he demonstrated that the theory produced results entirely different from ordinary representation theory. However, modular representation theory was not developed thoroughly until the German-American mathematician Richard Brauer acquired a new position at the University of Toronto in 1935. Together with his PhD student Cecil J. Nesbitt he introduced the concepts of modular characters (later named after him) and blocks, which helped them prove fundamental theorems of modular representation theory about the number of irreducible modular representations and the relationship between Cartan invariants and decomposition numbers. Soon it became clear to Brauer that many results of modular representation theory could be profitably applied to the investigation of the structure of finite groups. Indeed, it turned out later that his work was substantial to the classification of finite simple groups.

The purpose of this thesis is to give a comprehensive analysis of the principal indecomposable representations of the Alternating group A_5 on five symbols. After providing the necessary algebraic background, we develop the main ideas of modular representation theory such as Brauer characters, decomposition numbers and Cartan numbers. Furthermore, an introduction to block theory is given, containing the few but necessary results used throughout the remaining part. Our main result is a classification of the principal indecomposable modules (hereafter abbreviated 'PIMs') for the group A_5, in particular providing detailed information about the structure of the group algebra kA_5. For this purpose we compute the primitive orthogonal idempotents of the group algebra as well as the radical series of the PIMs.

In the first chapter the main algebraic results relevant for modular representation theory are presented. We prove the Krull-Schmidt theorem and the Jordan-Hölder theorem for modules of finite length and investigate the radical of both Artinian rings and modules over Artinian rings. The following sections deal with PIMs of algebras over a field, which are central objects in modular representation theory. Before determining the decomposition of an algebra into a direct sum of PIMs, we also take a short detour into the realm of projective and injective modules and prove that every principal indecomposable module is projective. The chapter concludes with a discussion of the Meataxe algorithm and its most common variant, the Holt-Rees algorithm, which serves as an irreducibility test for modules. Its implementation in the computer program `GAP` is used extensively in the third chapter.

The object of the second chapter is to provide an introduction to modular representation theory. To begin with, we discuss p-modular systems (K, R, k) for a group G, where K is a certain field of characteristic 0, R its ring of integers and k the residue field of R of modular characteristic p. In this context, modular characteristic means that the prime p divides the order of G. The p-modular systems allow for the techniques of lifting idempotents and choosing integral representations, which make the simultaneous investigation of ordinary representations over K, integral representations over R and modular representations over k feasible. The discussion of modular representations starts with the definition of decomposition numbers and Cartan numbers via module-theoretic considerations and the examination of their relationship. We then develop the theory of Brauer characters, a concept in modular representation theory which is analogous to ordinary character theory, and state the meaning of the Decomposition matrix D and the Cartan matrix C in terms of Brauer characters. Finally, a short introduction to block theory provides a few basic results about block decompositions and block idempotents.

The third chapter contains the actual results of this thesis. Since the order of A_5 is divisible by the primes 2, 3 and 5, the following procedure is carried out for each of these three cases. Having fixed a p-modular system for A_5, we decompose the group algebra kA_5 into blocks and compute the corresponding block idempotents. This block decomposition facilitates the determination of irreducible Brauer characters and PIMs by establishing a categorization of these objects into blocks. We then start with the classification of the irreducible modular representations by computing the p-Brauer characters. To this end we reduce the irreducible ordinary characters of A_5 and determine the decomposition numbers d_{ij}. Gathering these numbers in the decomposition matrix D, we immediately get the p-Brauer character table as well as the Cartan matrix C. Both the decomposition matrix and the Cartan matrix allow us to determine the dimensions of the PIMs and their socles, thus constituting an important part of the structure of the group algebra kA_5. After having identified the irreducible modular representations and the PIMs of kA_5, we investigate how to relate them to ordinary representations over K and integral representations over R. In the final section we use the previously obtained theoretical results to compute the primitive orthogonal idempotents corresponding to the decomposition of the group algebra into PIMs. More precisely, a primitive orthogonal idempotent is associated to the direct sum of all submodules of kG which are isomorphic to a given PIM, much like the isotypic component of an irreducible representation in characteristic 0. The idea is to decompose a block B of kG into a direct sum of such 'isotypic' components of PIMs and compute the projection of the block idempotent ε_B with respect to this decomposition. We use the computer algebra system `GAP` as a tool to carry out the computations, particularly resorting to `GAP`'s implementation of the Meataxe algorithm. Furthermore, we also determine the radical series of each PIM.

Appendix A provides results from ordinary representation theory which are needed during the calculations in the third chapter. The second appendix provides an uncommented listing of the results of Chapter 3 and serves as a concise reference guide to modular representation theory of the group A_5.

The reader is assumed to be familiar with ordinary representation theory. Otherwise, [Bur65] and [Wei03] provide a comprehensible introduction into the subject. A more thorough treatise can be found in [CR62] and [LP10], the latter specializing in the computational aspects of representation theory. Of course, the most comprehensive and complete account on the subject is the standard work [CR81]. All books mentioned contain at least an introductory chapter on modular representation theory; for a self-contained account of the theory, refer to [DP77] and [Alp86]. Finally, [Ser77] provides an elegant approach to both ordinary and modular representation theory, although its composition may seem unconventional.

1. Algebraic prerequisites

In this chapter we develop the algebraic prerequisites that are needed to deal with modular representations of finite groups. Clearly, the path we are going to take is tailored to modular representation theory; nevertheless, the presented results have widespread applications throughout the various branches of algebra and deserve to be treated separately. Particularly the theory of projective and injective modules, introduced in Section 1.2.2, is a fundamental concept. Note however, that in some situations we only concentrate on special cases relevant to our applications, e.g., certain results about modules over a group algebra instead of a general ring.

First we discuss modules over Artinian rings and define the radical of a module (respectively a ring), a central object in the non-semisimple case. Then we turn to algebras over a field K and investigate their decompositions by analyzing modules over an algebra. The last section introduces the Meataxe algorithm, which provides an irreducibility test for modules.

The reasoning in Sections 1.1 and 1.2 mainly follows [CR62] and [JS06], with the second section also incorporating material from [Alp86] and [Bur65]. Section 1.3 is based on [HR94] and results from [LP10]. The reader may be reminded that this chapter is not intended as a comprehensive account on the algebraic concepts involved. Rather, it collects the results needed to develop modular representation theory in Chapter 2. Particularly Section 1.2.2 only touches the subject of projective and injective modules.

The following conventions will be adhered to: A ring R always has a unity element 1_R, and the terms ideal and module are short for left ideal and left module, respectively. Unless otherwise specified, throughout the whole chapter, R is a ring, K a field with arbitrary characteristic, G a finite group, and KG the group algebra over K. Arbitrary algebras over fields are always assumed to be finite-dimensional.

1.1. Modules over Artinian rings

1.1.1. Modules of finite length

In the study of the representations of a finite group G, one of the main tasks is the decomposition of a KG-module M into a direct sum of indecomposable submodules. The existence of such a decomposition is assured if the module is Artinian or Noetherian. However, this result is only useful for the study of representation theory if the decomposition is also unique. It turns out that modules of finite length admit such a unique decomposition into indecomposable submodules, which is subject of the Krull-Schmidt theorem. Representation theory is also interested in finding composition series of these indecomposable modules, and again, modules of finite length are of interest because such modules always have a composition series. In this situation the Jordan-Hölder theorem ensures uniqueness of a composition series in the sense that any two series of a module of finite length are equivalent.

These results show the importance of the property of finite length; therefore, the first part of this treatment is dedicated to examining modules with this property. Let us first establish the existence of a decomposition mentioned above.

Theorem 1.1.1. *Let M be an Artinian R-module. Then there are indecomposable submodules $M_1, \dots, M_t$ of M such that $M = M_1 \oplus \cdots \oplus M_t$.*

Proof. Let X be the set of all non-zero submodules of M which cannot be decomposed into a direct sum of a finite number of indecomposable submodules of M, and suppose that $X \neq \emptyset$. Since M is Artinian, X contains a minimal element $U \neq 0$ which is decomposable (otherwise, it would be the trivial direct sum of one indecomposable submodule of M). Thus, there are submodules S and T of M with $U = S \oplus T$. But S and T are submodules of U, and U is a minimal element of X; therefore, both S and T cannot lie in X. This means that there are indecomposable submodules $S_1, \dots, S_m$ and $T_1, \dots T_n$ of M with

$$S = S_1 \oplus \cdots \oplus S_m \quad \text{and} \quad T = T_1 \oplus \cdots \oplus T_n$$

It follows that $U = S_1 \oplus \cdots \oplus S_m \oplus T_1 \oplus \cdots \oplus T_n$ is expressible as a direct sum of indecomposable submodules of M, a contradiction to $U \in X$. Therefore, $X = \emptyset$, so clearly $M \notin X$, and the theorem is proved. □

For a different proof assuming a Noetherian module see [JS06, p. 200, Thm. 7.4]. A decomposition into a direct sum of indecomposable submodules can also be characterized by endomorphisms with certain properties or (in the case of an R-algebra) by orthogonal idempotents.

Proposition 1.1.2.

(i) *Let $M = M_1 \oplus \cdots \oplus M_t$ be a decomposition of an R-module M into a direct sum of submodules. Then there are projections $\pi_1, \ldots, \pi_t \in \operatorname{End}_R(M)$ with*

$$\begin{aligned} \mathrm{id} &= \pi_1 + \cdots + \pi_t \\ \pi_i^2 &= \pi_i \qquad \textit{for } 1 \leq i \leq t \\ 0 &= \pi_i \circ \pi_j \qquad \textit{for } i \neq j \end{aligned}$$

That is, the projections $\pi_1, \ldots, \pi_t$ are a set of orthogonal idempotents in $\operatorname{End}_R(M)$. Moreover, a summand M_i is indecomposable if and only if π_i is primitive.

(ii) *Let $A = A_1 \oplus \cdots \oplus A_t$ be a decomposition of an R-algebra A into a direct sum of submodules. Then there are elements $e_1, \ldots, e_t \in A$ with*

$$\begin{aligned} 1_A &= e_1 + \cdots + e_t \\ e_i^2 &= e_i \qquad \textit{for } 1 \leq i \leq t \\ 0 &= e_i e_j \qquad \textit{for } i \neq j \end{aligned}$$

That is, the elements $e_1, \ldots, e_t \in A$ are a set of orthogonal idempotents, and we have $A_i = Ae_i$. Moreover, a summand A_i is indecomposable if and only if the idempotent e_i is primitive.

Proof. (i) For $x \in M$ we can write $x = m_1 + \cdots + m_t$ with unique $m_i \in M_i$. Define $\pi_i \in \operatorname{End}_R(M)$ as $\pi_i(x) := m_i$ for $1 \leq i \leq t$. It is easy to see that these endomorphisms fulfill the desired properties.

Clearly, if a summand M_i is decomposable, i.e., $M_i = M_i' \oplus M_i''$, and both M_i' and M_i'' are non-trivial, then $\pi_i = \pi_i' + \pi_i''$, where π_i' and π_i'' are defined analogously. Furthermore, π_i' and π_i'' are unequal to the trivial idempotents, and π_i is not primitive. Conversely, suppose an idempotent $\pi_i \in \operatorname{End}_R(M)$ is not primitive, i.e., there are non-trivial idempotents π_i' and π_i'' such that $\pi_i = \pi_i' + \pi_i''$. Define $M_i' := \operatorname{im} \pi_i'$ and $M_i'' := \operatorname{im} \pi_i''$. Then clearly, $M_i' + M_i'' = M_i$. For $x \in M_i' \cap M_i''$ we have $\pi_i(x) = x = \pi_i'(x) + \pi_i''(x) = x + x$, which implies $x = 0$, and hence $M_i = M_i' \oplus M_i''$.

(ii) By (i) there are projections $\pi_1, \ldots, \pi_t$ with $\mathrm{id} = \pi_1 + \cdots + \pi_t$. Define $e_i := \pi_i(1_A)$, then

$$1_A = e_1 + \cdots + e_t \tag{*}$$

Now observe that

$$e_i = e_i 1_A = e_i e_1 + \cdots + e_i^2 + \cdots + e_i e_t$$

which means that $e_i^2 = e_i$ and $e_i e_j = 0$ for $i \neq j$. A similar argument for $x \in A$ shows that $x = xe_1 + \cdots + xe_t$, and hence $A_i = Ae_i$. Moreover, (i) shows that an idempotent e_i is primitive if and only if A_i is indecomposable. □

As we have mentioned before, the decomposition into a direct sum of indecomposable submodules in Theorem 1.1.1 is not unique, and we need to introduce the concept of modules of finite length to remedy this:

Definition 1.1.3. An R-module M has finite length if M is both Artinian and Noetherian.

We will see later that for such modules the Krull-Schmidt theorem guarantees uniqueness of the decomposition in Theorem 1.1.1. The following proposition shows that group algebras always have finite length.

Proposition 1.1.4. *The group algebra KG has finite length.*

Proof. Let $n = |G|$ and recall that KG is a K-algebra with $\dim_K KG = n$. Suppose we have a descending chain

$$KG \supset I_1 \supset I_2 \supset \dots$$

of ideals of KG. Then these ideals can also be viewed as K-subspaces of the K-vector space KG, and $\dim_K I_{i+1} \leq \dim_K I_i \leq n$, which shows that the descending chain ultimately terminates. Thus, KG is Artinian. A similar argument for an ascending chain

$$0 \subset J_1 \subset J_2 \subset \dots$$

shows that KG is also Noetherian. □

To prove the Krull-Schmidt theorem, we need two lemmata, the first of which is a well-known result of Fitting.

Lemma 1.1.5 (Fitting)**.** *Let M be an indecomposable R-module of finite length. Then each $\varphi \in \mathrm{End}_R(M)$ is either bijective or nilpotent.*

Proof. Let $\varphi \in \operatorname{End}_R(M)$ be an endomorphism of M and consider the following chains of submodules:

$$\ker \varphi \subseteq \ker \varphi^2 \subseteq \ker \varphi^3 \subseteq \dots \qquad \operatorname{im} \varphi \supseteq \operatorname{im} \varphi^2 \supseteq \operatorname{im} \varphi^3 \supseteq \dots$$

Since M has finite length, both chains become stationary, i.e., there are integers i and j such that $\ker \varphi^i = \ker \varphi^{i+1} = \dots$ and $\operatorname{im} \varphi^j = \operatorname{im} \varphi^{j+1} = \dots$; we put $k = \max(i, j)$. It follows from $\operatorname{im} \varphi^k = \operatorname{im} \varphi^{2k}$ that for every $x \in M$ there is a $y \in M$ with $\varphi^k(x) = \varphi^{2k}(y)$. This implies $\varphi^k(x - \varphi^k(y)) = 0$ and $x = \varphi^k(y) + (x - \varphi^k(y)) \in \operatorname{im} \varphi^k + \ker \varphi^k$, i.e., $M = \operatorname{im} \varphi^k + \ker \varphi^k$. It further holds that $\operatorname{im} \varphi^k \cap \ker \varphi^k = 0$: Suppose that $x \in \operatorname{im} \varphi^k \cap \ker \varphi^k$, then there is a $y \in M$ with $\varphi^k(y) = x$. But $0 = \varphi^k(x) = \varphi^{2k}(y)$, that is, $y \in \ker \varphi^{2k} = \ker \varphi^k$, and hence $x = \varphi^k(y) = 0$.

Thus, $M = \operatorname{im} \varphi^k \oplus \ker \varphi^k$. But M is indecomposable, so either $\operatorname{im} \varphi^k = 0$, which means that φ is nilpotent or $\ker \varphi^k = 0$, which means that φ is bijective. This proves Fitting's Lemma. □

Lemma 1.1.6. *Let M be a non-zero indecomposable R-module of finite length. Let further $\varphi_1, \dots, \varphi_t \in \operatorname{End}_R(M)$ be endomorphisms of M such that $\varphi_1 + \dots + \varphi_t$ is an automorphism of M. Then there is an i such that φ_i is an automorphism.*

Proof. Let us consider the case $t = 2$, i.e., $\varphi_1 + \varphi_2 =: \psi$ is an automorphism of M. Set $\chi_i = \varphi_i \psi^{-1}$ and observe that $\chi_i \in \operatorname{End}_R(M)$ and $\chi_1 + \chi_2 = \mathrm{id}$. We will show that either χ_1 or χ_2 is an automorphism of M, which proves the claim.

Since $\chi_2 = \mathrm{id} - \chi_1$, we know that χ_1 and χ_2 commute; therefore, the binomial theorem is applicable:

$$\mathrm{id} = (\chi_1 + \chi_2)^n = \sum_{k=0}^{n} \binom{n}{k} \chi_1^k \chi_2^{n-k}$$

Suppose both χ_1 and χ_2 are nilpotent, i.e., there are integers n_1 and n_2 such that $\chi_1^{n_1} = \chi_2^{n_2} = 0$. Choosing $k = n_1 + n_2$ now implies $1 = (\chi_1 + \chi_2)^k = 0$, which is impossible. So either χ_1 or χ_2 is not nilpotent and hence bijective after Lemma 1.1.5. □

Remark. Lemma 1.1.6 is equivalent to saying that the endomorphism ring $\operatorname{End}_R M$ of an indecomposable R-module M is local. A ring R is called local if it fulfills any of the following equivalent conditions:

(i) R has a unique maximal (left or right) ideal.

(ii) The non-units form an ideal (and $1_R \neq 0_R$).

(iii) If a finite sum is a unit, then at least one of the summands is a unit.

We are now ready to prove

Theorem 1.1.7 (Krull-Schmidt)**.** *Let M be an R-module of finite length, and let*

$$M = S_1 \oplus \cdots \oplus S_m = T_1 \oplus \cdots \oplus T_n$$

be two decompositions of M into direct sums of indecomposable submodules. Then $m = n$, and we can rearrange the summands such that $S_i \cong T_i$ for every $i = 1, \dots, m$.

Proof. We assume $m \geq n$ and use induction on m, the case $m = 1$ being trivial. According to Proposition 1.1.2, there are projections $\sigma_1, \dots, \sigma_m$ and $\tau_1, \dots, \tau_n$ associated to the decompositinos $M = S_1 \oplus \cdots \oplus S_m$ and $M = T_1 \oplus \cdots \oplus T_n$, respectively. Since $\mathrm{id} = \sigma_1 + \cdots + \sigma_m = \tau_1 + \cdots + \tau_n$ and $\sigma_i \circ \sigma_j = \tau_i \circ \tau_j = 0$ for $i \neq j$, we have

$$\sigma_1 = \sigma_1 \circ \tau_1 + \cdots + \sigma_1 \circ \tau_n$$

We know from Proposition 1.1.2 that the restriction of σ_1 onto S_1 is the identity, so

$$\mathrm{id}_{S_1} = \sigma_1 \circ \tau_1|_{S_1} + \cdots + \sigma_1 \circ \tau_n|_{S_1}$$

and each $\sigma_1 \circ \tau_i|_{S_1} \in \mathrm{End}_R(S_1)$. By Lemma 1.1.6 there is a j such that $\sigma_1 \circ \tau_j|_{S_1} \in \mathrm{Aut}_R(S_1)$, and we can renumber the modules T_i such that this holds for $\sigma_1 \circ \tau_1|_{S_1}$.

Consider now the diagram

$$S_1 \xrightarrow{\tau_1} T_1 \xrightarrow{\sigma_1} S_1$$

and define $B := \operatorname{im} \tau_1|_{S_1}$ and $K := \ker \sigma_1|_{T_1}$. Since $\sigma_1 \circ \tau_1|_{S_1}$ is an automorphism of S_1, we have $\sigma_1(B) = S_1$. Hence, for $t \in T_1$ there is a $b \in B$ such that $\sigma_1(t) = \sigma_1(b)$, that is, $t - b \in K$. Thus $t = b + (t - b) \in B + K$, so $T_1 = B + K$. Further, let $x \in B \cap K$ then $\sigma_1(x) = 0$. Since σ_1 is injective on B, it follows that $x = 0$ and $T_1 = B \oplus K$. The indecomposability of T_1 now implies $K = \ker \sigma_1 = 0$, and hence $T_1 \cong S_1$.

The last step is to show that $M = S_1 \oplus T_2 \oplus \cdots \oplus T_n$. The preceding paragraph showed that $S_1 \cong T_1$; therefore, $M = S_1 + T_2 + \cdots + T_n$. So suppose that $x \in S_1 \cap (T_2 + \cdots + T_n)$. By Proposition 1.1.2 τ_1 vanishes on T_j for $2 \leq j \leq n$, thus $\tau_1(x) = 0$. But τ_1 is injective on S_1, hence $x = 0$, and the sum is direct. We now have

$$\begin{aligned} M &= S_1 \oplus S_2 \oplus \cdots \oplus S_m \\ &\cong S_1 \oplus T_2 \oplus \cdots \oplus T_n \end{aligned}$$

and factorizing after S_1 gives

$$S_2 \oplus \cdots \oplus S_m \cong T_2 \oplus \cdots \oplus T_n$$

Applying the induction hypothesis now completes the proof. $\square$

So far we have seen that modules of finite length have a unique decomposition into a direct sum of indecomposable submodules. Another important property of modules of finite length is the existence of a unique composition series, which is the subject of the Jordan-Hölder theorem. Let us first recall the definition of a composition series:

Definition 1.1.8 (Composition series)**.** Let M be an R-module. A chain

$$M = M_0 \supset M_1 \supset \cdots \supset M_t = 0$$

of submodules of M is called a composition series if the factors M_i/M_{i+1} are simple R-modules for all $0 \leq i < t$.

If such a series exists, then t is called the length of this chain of submodules. The length of M is defined as the minimum of the length of all chains of submodules.

Proposition 1.1.9. *An R-module M has finite length if and only if it possesses a composition series.*

Proof. Suppose first that M possesses a composition series. We recall a basic result about Artinian and Noetherian modules: If M is a module and N a submodule of M, then M is Artinian (Noetherian) if and only if N and M/N are Artinian (Noetherian). Since simple modules have finite length, we can use induction on the length of the chain to show that M also has finite length.

Conversely, suppose that M has finite length. Let X be the set of all submodules M' of M which possess a composition series, and observe that $(0) \in X$. Since M is Noetherian, there is a maximal element M_0 of X. If $M_0 = M$, the claim is proved.

Otherwise, consider the set $Y = \{M' \leq M \mid M' \supsetneq M_0\}$, which is non-empty since $M \in Y$. Because M is Artinian, there is a minimal element $M_1 \in Y$, and we investigate the factor module M_1/M_0 (which is non-zero). If $\pi : M_1 \to M_1/M_0$ is the canonical projection onto M_1/M_0, then for every submodule N of M_1/M_0 the preimage $\pi^{-1}(N)$ is a submodule of M_1 with $\pi^{-1}(N) \supsetneq M_0$. Due to the minimality of M_1 we have $\pi^{-1}(N) = M_1$, and M_1/M_0 is simple. We can now construct a composition series of M_1 by extending the composition series of M_0 by M_1 (remember that $M_0 \in X$). But this means that $M_1 \in X$, contradicting the maximality of M_0. Therefore, $M_0 = M$, and the result follows. $\square$

Remark. This is the reason for the name 'finite length', and originally modules of finite length were defined by Proposition 1.1.9.

To establish uniqueness of a composition series and prove the Jordan-Hölder theorem we first need a

Definition 1.1.10. Let M be an R-module with composition series

$$\begin{aligned} &M = M_0 \supset M_1 \supset \cdots \supset M_s = 0 \\ \text{and} \quad &M = M_0 \supset M_1' \supset \cdots \supset M_t' = 0 \end{aligned}$$

Then the composition series are equivalent if $s = t$ and there is a renumbering of the modules M_i' such that the factors of both chains are isomorphic, that is, $M_i/M_{i+1} \cong M_i'/M_{i+1}'$ for all $0 \leq i < s$.

We can now prove

Theorem 1.1.11 (Jordan-Hölder)**.** *If M is an R-module of finite length, then any two composition series of M are equivalent.*

Proof. Let M have two composition series

$$M = M_0 \supset M_1 \supset \cdots \supset M_s = 0 \tag{1.1a}$$

$$M = N_0 \supset N_1 \supset \cdots \supset N_t = 0 \tag{1.1b}$$

We assume $s \geq t$ and use induction on s. Suppose that any two composition series of M of length less than s are equivalent. If $M_1 = N_1$, then the claim follows by applying the induction hypothesis. Thus, assume $M_1 \neq N_1$. Since M/M_1 is simple, M_1 is maximal in M, and therefore $M_1 + N_1 = M$. By the fundamental homomorphism theorem for modules we have

$$M/M_1 \cong N_1/(M_1 \cap N_1) \qquad \text{and} \qquad M/N_1 \cong M_1/(M_1 \cap N_1) \tag{1.2}$$

and the simplicity of M/M_1 and M/N_1 again implies that $(M_1 \cap N_1)$ is a maximal submodule of both M_1 and N_1. Now let

$$(M_1 \cap N_1) \supset T_2 \supset \cdots \supset T_l = 0$$

be a composition series for $(M_1 \cap N_1)$ (note that $l < s$), then

$$M = M_0 \supset M_1 \supset (M_1 \cap N_1) \supset T_2 \supset \cdots \supset T_l = 0$$

and

$$M = N_0 \supset N_1 \supset (M_1 \cap N_1) \supset T_2 \supset \cdots \supset T_l = 0$$

are both composition series of M, and by (1.2) the first two factors are isomorphic such that the two series are equivalent. By the induction hypothesis, the first series above is equivalent to (1.1a) since they have the same first term, and analogously the second series is equivalent to (1.1b). Therefore, the series in (1.1a) and (1.1b) are equivalent, and the theorem is proved. $\square$

Corollary 1.1.12. *If M is an R-module of finite length, then any two composition series of M have the same length.*

1.1.2. Radical of a module

We now define the radical and socle of modules and rings and prove the most important results about them. The radical $\operatorname{rad} M$ of a module M provides extensive information about its structure in case M is not semisimple. In our situation the group algebra KG is always non-semisimple, according to the famous

Theorem 1.1.13 (Maschke)**.** *The group algebra KG is semisimple if and only if* $\operatorname{char} K$ *does not divide $|G|$.*

Furthermore, since KG is Artinian as a K-algebra, the radical of Artinian rings deserves special attention and will be investigated as well. We start with a

Definition 1.1.14 (Radical and socle)**.** Let M be an R-module.

(i) The radical $\operatorname{rad} M$ of M is the intersection of all maximal submodules of M. If M does not possess maximal submodules, then $\operatorname{rad} M = M$.

(ii) The socle $\operatorname{soc} M$ of M is the sum of all simple submodules of M.

Proposition 1.1.15. *Let M be an R-module.*

(i) *If M is semisimple, then* $\operatorname{rad} M = 0$.

(ii) *M is semisimple if and only if* $\operatorname{soc} M = M$.

(iii) *If N is a submodule of M with $N \subset \operatorname{rad} M$, then* $\operatorname{rad}(M/N) = \operatorname{rad}(M)/N$*. In particular, the radical of $M/\operatorname{rad} M$ is zero.*

(iv) *Let $(M_i)_{i\in I}$ be a family of R-modules, then*

$$\operatorname{rad}\left(\bigoplus_{i\in I} M_i\right) = \bigoplus_{i\in I} \operatorname{rad} M_i$$
$$\operatorname{soc}\left(\bigoplus_{i\in I} M_i\right) = \bigoplus_{i\in I} \operatorname{soc} M_i$$

Proof. (i) If M is semisimple, there are simple submodules $M_1, \dots, M_t$ of M such that $M = M_1 \oplus \cdots \oplus M_t$, and the maximal submodules of M are the modules $\bigoplus_{i\neq j} M_i$ for a fixed $1 \leq j \leq t$. Consequently, their intersection is empty, and thus $\operatorname{rad} M = 0$.

(ii) is trivial.

(iii) The maximal submodules of M/N arise from maximal submodules M' of M with $M' \supset N$, which are all the maximal submodules of M since we assumed $N \subset \operatorname{rad} M$. The radical of M/N is now the intersection of all M'/N, that is, $\bigcap(M'/N) = (\bigcap M')/N$. For the second claim take $N = \operatorname{rad} M$.

(iv) Every maximal submodule of $\bigoplus_{i\in I} M_i$ is of the form $\cdots \oplus M_{i-1} \oplus M_i' \oplus M_{i+1} \oplus \dots$, where M_i' is a maximal submodule of M_i. Since $M_i \cap M_j = \emptyset$ for $i \neq j$, the first formula follows.

For the socle, suppose S is a simple submodule of $\bigoplus_{i\in I} M_i$. Then clearly $S \leq M_i$ for one i, and $S \cap M_j = \emptyset$ for $j \neq i$. Conversely, any simple submodule of a summand M_i is also a simple submodule of $\bigoplus_{i\in I} M_i$, proving the second formula. □

Definition 1.1.16 (Jacobson radical)**.** The Jacobson radical $J(R)$ of a ring R is the radical $\operatorname{rad}{}_R R$ of the ring viewed as a module over itself.

Proposition 1.1.17. *Let R be a ring, then $J(R)$ is a two-sided ideal and the intersection of the annihilators of all simple R-modules.*

Proof. Let S be a simple R-module, and consider for $x \in S, x \neq 0$ the R-module homomorphism $\varphi_x : R \longrightarrow S, r \longmapsto rx$. Since S is simple and $1_R \cdot x = x$, we have that φ_x is surjective and $\ker \varphi_x = \operatorname{ann}_R(x)$. Therefore, we have $S \cong R/\operatorname{ann}_R(x)$, and $\operatorname{ann}_R(x)$ is a maximal left ideal in R.

Conversely, let I be a maximal left ideal in R, then R/I is a simple R-module which is annihilated by I. We now have

$$\operatorname{rad}{}_R R = \bigcap_{S \text{ simple}} \bigcap_{x\in S} \operatorname{ann}_R(x) = \bigcap_{S \text{ simple}} \operatorname{ann}_R(S)$$

Since the annihilator $\operatorname{ann}_R(S)$ of a simple R-module S is a two-sided ideal, so is the Jacobson radical $J(R)$. □

In the case of Artinian rings R and Artinian modules M, the radical has additional properties. In order to prove them, we have to introduce the concept of a finitely cogenerated module:

Definition 1.1.18. An R-module M is finitely cogenerated if for any family $(M_i)_{i\in I}$ of submodules of M with $\bigcap_{i\in I} M_i = 0$ there is a finite subset $J \subset I$ such that $\bigcap_{i\in J} M_i = 0$.

Remark. If N is a submodule of M, then M/N is finitely cogenerated if and only if for any family $(M_i)_{i\in I}$ of submodules of M with $\bigcap_{i\in I} M_i = N$ there is a finite subset $J \subset I$ such that $\bigcap_{i\in J} M_i = N$.

Recall that a module M is Noetherian if and only if every submodule of M is finitely generated. Being finitely cogenerated is dual to this result in the following sense:

Proposition 1.1.19. *An R-module M is Artinian if and only if every factor module of M is finitely cogenerated.*

Proof. Let N and $(M_i)_{i\in I}$ be submodules of M with $\bigcap_{i\in I} M_i = N$, and consider the set X of all finite intersections $\bigcap_{i\in J} M_i$ for finite $J \subset I$. Since M is Artinian (and X is non-empty), there is a minimal element $P \in X$ with $P \supset N$. Suppose there is no equality, that is, there is a $x \in P$ with $x \notin N$. Because $N = \bigcap_{i\in I} M_i$, there is an $i \in I$ with $x \notin M_i$; therefore, $x \notin P' = \bigcap_{j\in J\cup\{i\}} M_j$. But $P' \in X$ and $P' \subsetneq P$, a contradiction to the minimality of P.

Conversely, let $M_0 \supset M_1 \supset M_2 \supset \dots$ be a descending chain of submodules of M, and set $N = \bigcap_{i\in I} M_i$. Since M/N is finitely cogenerated, there is a finite subset $J \subset I$ with $N = \bigcap_{i\in J} M_i$. But now $N = M_n$ with $n = \max J$, and so $M_i = M_n$ for all $i \geq n$; thus, M is Artinian. □

Corollary 1.1.20. *If M is an Artinian R-module, then $M/\operatorname{rad} M$ is a semisimple R-module.*

Proof. By Proposition 1.1.19 $M/\operatorname{rad} M$ is finitely cogenerated, so there are finitely many submodules $M_1, \dots, M_n$ of M with $\operatorname{rad} M = \bigcap_{i=1}^n M_i$. Consider the monomorphism

$$\begin{aligned} \varphi : M/\operatorname{rad} M &\longrightarrow \bigoplus_{i=1}^n (M/M_i) \\ x + \operatorname{rad} M &\longmapsto \sum_{i=1}^n x + M_i \end{aligned}$$

Since the M/M_i are simple submodules, $M/\operatorname{rad} M$ is isomorphic to a submodule of a semisimple module and therefore itself semisimple. □

We also need the famous Nakayama Lemma, which we state here without proof.

Proposition 1.1.21 (Nakayama Lemma)**.** *Let R be a ring and M be a finitely generated R-module. Then $\operatorname{rad}(R) \cdot M$ is superfluous in M, that is, for every submodule N of M with $\operatorname{rad}(R) \cdot M + N = M$ we have $N = M$.*

Proof. See [JS06, p. 267, Cor. 7.10] □

Now we are able to prove the main results about radicals of Artinian rings.

Proposition 1.1.22. *Let R be an Artinian ring, then the following holds:*

(i) *The ring $R/\operatorname{rad} R$ is semisimple.*

(ii) *The ring R is semisimple if and only if $\operatorname{rad} R = 0$.*

(iii) *If M is an R-module, then $\operatorname{rad} M = \operatorname{rad}(R) \cdot M$.*

(iv) *The radical $\operatorname{rad} R$ is nilpotent.*

Proof. (i) By Corollary 1.1.20 $R/\operatorname{rad} R$ is semisimple as a module over R. From Proposition 1.1.17 follows that $R/\operatorname{rad} R$ is a ring, and obviously, it is also semisimple as a module over itself; hence, $R/\operatorname{rad} R$ is semisimple as a ring.

(ii) The first implication is Proposition 1.1.15(i). For the other implication, use (i) with $\operatorname{rad} R = 0$.

(iii) We first show that $\operatorname{rad}(R) \cdot M \subset \operatorname{rad} M$. Let M' be a maximal submodule of M. Then M/M' is a simple R-module, and by Proposition 1.1.17 we have $\operatorname{rad}(R) \cdot M/M' = 0$, that is, $\operatorname{rad}(R) \cdot M \subset M'$. Thus, the left side is also contained in the intersection of all maximal submodules, and hence $\operatorname{rad}(R) \cdot M \subset \operatorname{rad} M$. Now by (i), $R/\operatorname{rad} R$ is a semisimple ring, so $M/\operatorname{rad}(R)M$ is semisimple as an $R/\operatorname{rad} R$-module and also as an R-module. Therefore, $\operatorname{rad}(M/\operatorname{rad}(R)M) = 0$. On the other hand, by Proposition 1.1.15(iii) we have that

$$0 = \operatorname{rad}(M/\operatorname{rad}(R)M) = \operatorname{rad}(M)/\operatorname{rad}(R)M$$

from which $\operatorname{rad}(R) \cdot M = \operatorname{rad} M$ follows.

(iv) Let $R \supset \operatorname{rad} R \supset (\operatorname{rad} R)^2 \supset \dots$ be a descending chain of ideals in R. Since R is Artinian, there is a $n \in \mathbb{N}$ such that $(\operatorname{rad} R)^m = (\operatorname{rad} R)^n$ for all $m \geq n$. Set $I = (\operatorname{rad} R)^n$ and suppose $I \neq 0$. We show that this leads to a contradiction.

To this end, consider the set X of all ideals J in R with $IJ \neq 0$, and observe that $X \neq \emptyset$ since $I^2 = (\operatorname{rad} R)^{2n} = (\operatorname{rad} R)^n = I \neq 0$. Thus, X contains a minimal element J, and there is an $x \in J$ with $Ix \neq 0$, that is, $IRx \neq 0$ (recall that $\operatorname{rad} R$ is a two-sided ideal by Proposition 1.1.17). Now Rx is an ideal in R, and clearly, $Rx \subset J$, so the minimality of J implies that $J = Rx$. Since $\operatorname{rad}(R)J = J$ contradicts the Nakayama Lemma 1.1.21, we have $\operatorname{rad}(R)J \subsetneq J$, and consequently $IJ \subsetneq J$. But J was a minimal element of X, therefore $I(IJ) = 0$. On the other hand, $I(IJ) = I^2 J = IJ \neq 0$, a contradiction. $\square$

Let us apply these results to the following situation: Let R be an Artinian ring and M an R-module. Then $\operatorname{rad} M$ is also an R-module, and by Proposition 1.1.22(iii) its radical is given by $\operatorname{rad}(\operatorname{rad} M) = \operatorname{rad} R \cdot \operatorname{rad} M = \operatorname{rad}^2(R) \cdot M$. This motivates the definition $\operatorname{rad}^n M := \operatorname{rad}^n(R) \cdot M$ for $n \geq 2$. Note that since R is Artinian, its radical is nilpotent by Proposition 1.1.22(iv); therefore, $\operatorname{rad}^k R = 0$ for some k. This leads to the following

Definition 1.1.23 (Radical series)**.** Let R be an Artinian ring and M an R-module. Then

$$M \geq \operatorname{rad} M \geq \operatorname{rad}^2 M \geq \dots \geq \operatorname{rad}^k M = (0)$$

is called the radical series of M.

Remark. If the ring R is not Artinian, the radical $\operatorname{rad} R$ is not necessarily nilpotent, and an infinite radical series

$$M \geq \operatorname{rad} M \geq \operatorname{rad}^2 M \geq \dots \geq \operatorname{rad}^k M \geq \operatorname{rad}^{k+1} M \geq \dots$$

is possible. Note however, that the radical series is a descending chain of submodules and thus terminates if the R-module M is Artinian.

In Section 3.3.2 we will compute the radical series of the principal indecomposable submodules (cf. Section 1.2.1) of the group algebra kG.

1.2. Algebras

1.2.1. Principal indecomposable modules

We have gathered enough information to define a central object of interest in modular representation theory: the principal indecomposable modules. They are the unique building blocks of an algebra A, and their structure can be described in terms of the radical. This is the main result of the following section.

Definition 1.2.1 (Principal indecomposable modules)**.** Let A be a (finite-dimensional) K-algebra. If

$$A = P_1 \oplus \cdots \oplus P_t$$

is a decomposition of A into a direct sum of indecomposable submodules P_i of A, then P_i is called a principal indecomposable module of A, abbreviated PIM.

Since A is a finite-dimensional K-vector space (see the proof of Proposition 1.1.4), the Krull-Schmidt theorem 1.1.7 justifies Definition 1.2.1 as the summands in the decomposition of A into a direct sum of indecomposable submodules are uniquely determined up to isomorphy and order of appearance. Of course we are actually talking about isomorphy classes of PIMs. Proposition 1.1.2(ii) further implies that to every PIM P of A we can associate a primitive idempotent e with $P = Ae$. The structure of a PIM of an algebra A is revealed in the following

Theorem 1.2.2. *Let K be a field and A a K-algebra, then the following holds:*

(i) *If $P = Ae$ is a PIM of A, where e is the corresponding primitive idempotent, then $\operatorname{rad}(A)e = \operatorname{rad} P$ is the unique maximal submodule of P.*

(ii) *If P and Q are two PIMs of A, then $P \cong Q$ if and only if $P/\operatorname{rad} P \cong Q/\operatorname{rad} Q$.*

Proof. (i) Suppose that M_1 and M_2 are two different maximal submodules of $P = Ae$. Then $P = M_1 + M_2$, and there are $m_1 \in M_1$ and $m_2 \in M_2$ with $e = m_1 + m_2$. Now define $\mu_i \in \operatorname{End}_A(P)$ by $\mu_i : ae \longmapsto aem_i$ for $i = 1, 2$. Then $\mathrm{id}_P = \mu_1 + \mu_2$ and by Lemma 1.1.6 one of the μ_i is an automorphism. But this is impossible since $\operatorname{im} \mu_i = M_i$, and hence neither of the μ_i is surjective. Therefore, $M_1 = M_2$, and $\operatorname{rad}(A)e = \operatorname{rad} P$ is the unique maximal submodule.

(ii) If $P \cong Q$, then trivially $P/\operatorname{rad} P \cong Q/\operatorname{rad} Q$.

Conversely, suppose $P/\operatorname{rad} P \cong Q/\operatorname{rad} Q$ via the A-module isomorphism φ. Then we have a surjective homomorphism

$$\begin{aligned} \psi : P &\longrightarrow Q/\operatorname{rad} Q \\ p &\longmapsto \varphi(p + \operatorname{rad} P) \end{aligned}$$

Let e_P be the idempotent corresponding to P, and choose $q_0 \in Q$ such that $\psi(e_P) = q_0 + \operatorname{rad} Q$. Observe that $q_0 \notin \operatorname{rad} Q$ because otherwise, $\psi(e_P) = 0 \in Q/\operatorname{rad} Q$. Consequently, $\psi(Ae_P) = A\psi(e_P) = 0$, which contradicts the surjectivity of ψ. Define now the A-

homomorphism $\tau : P \longrightarrow Q$, $p \longmapsto pq_0$. Because φ is an A-isomorphism,

$$e_P q_0 + \operatorname{rad} Q = e_P \psi(e_P) = \psi(e_P^2) = q_0 + \operatorname{rad} Q$$

Therefore, $e_P q_0 \in \operatorname{im} \tau$ as well as $e_P q_0 \notin \operatorname{rad} Q$. Hence, $\operatorname{rad} Q \lneqq \operatorname{im} \tau \leq Q$ and (i) implies $\operatorname{im} \tau = Q$. In particular, $\dim_K P \geq \dim_K Q$, and interchanging the roles of P and Q in the above reasoning shows equality. Thus, τ is an isomorphism and $P \cong Q$. □

This theorem shows that a PIM P of an algebra A is uniquely determined by the simple module $P/\operatorname{rad} P$. In fact we know even more:

Corollary 1.2.3. *Every simple A-module S is isomorphic to $P/\operatorname{rad} P$ for some PIM P of A.*

Proof. Let $A = P_1 \oplus \cdots \oplus P_t$ be a decomposition of A into a direct sum of PIMs P_i, then by Proposition 1.1.2(ii) we have a set $\{e_i\}_{i=1}^t$ of primitive orthogonal idempotents with $1_A = e_1 + \cdots + e_t$. Since $1_A S = S$, the idempotents e_i are orthogonal and S is simple, there is exactly one i such that $e_i S \neq 0$. Then $Ae_i s \neq 0$ for some $s \in S$, and since S is simple, $Ae_i s = S$. By considering the homomorphism $\varphi : P_i \longrightarrow S$, $a \longmapsto as$ we have $P_i/\ker \varphi \cong S$, where $\ker \varphi$ is thus a maximal submodule of P_i. Theorem 1.2.2(i) implies $\ker \varphi = \operatorname{rad} P_i$, and the claim follows. □

Corollary 1.2.4. *The number of isomorphy classes of simple A-modules is finite.*

Corollary 1.2.3 shows that for a K-algebra A there is a correspondence between isomorphy classes of PIMs and isomorphy classes of simple A-modules. This result is very important in representation theory, where the classification of indecomposable and irreducible KG-modules is the main object. The setting of group algebras KG has an additional, important property: The simple module $P/\operatorname{rad} P$ coincides with the socle $\operatorname{soc} P$ of P, see Corollary 1.2.16.

1.2.2. Projective and injective modules over group algebras

In this section we discuss projective and injective modules and investigate their interplay in the case of KG-modules. Let us first recall the following fact: A short exact sequence $0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$ of R-modules is said to split if there is an R-homomorphism $s : M \longrightarrow L$ such that $g \circ s = \mathrm{id}_M$.

Proposition 1.2.5. *Let $0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$ be a short exact sequence of R-modules, then the following are equivalent:*

(i) *The sequence splits.*

(ii) *There is an R-homomorphism $t : L \longrightarrow K$ such that $t \circ f = \mathrm{id}_K$.*

(iii) $\ker g$ *is a direct summand of L.*

Proof. See [JS06, p. 196, Prop. 5.1]. □

Definition 1.2.6 (Projective modules)**.** Let M and N be R-modules. An R-module P is called projective, if for every surjective homomorphism $\pi \in \mathrm{Hom}_R(M, N)$ and every homomorphism $\varphi \in \mathrm{Hom}_R(P, N)$ there is a homomorphism $\psi \in \mathrm{Hom}_R(P, M)$ such that $\pi \circ \psi = \varphi$, i.e., the following diagram commutes:

$$\begin{tikzcd} & P \arrow[dl, dotted, "\psi"'] \arrow[d, "\varphi"] & \\ M \arrow[r, "\pi"'] & N \arrow[r] & 0 \end{tikzcd}$$

Projective modules can be characterized by the following

Proposition 1.2.7. *Let P be an R-module, then the following are equivalent:*

(i) *P is projective.*

(ii) *Every short exact sequence $0 \longrightarrow K \longrightarrow L \longrightarrow P \longrightarrow 0$ of R-modules splits.*

(iii) *P is a direct summand of a free module.*

Proof. (i) $\Rightarrow$ (ii) Consider the short exact sequence $0 \longrightarrow K \longrightarrow L \longrightarrow P \longrightarrow 0$, and take $N = P$ and $\varphi = \mathrm{id}_P$ in Definition 1.2.6. Then there is a homomorphism $\psi : P \longrightarrow L$ with $\pi \circ \psi = \mathrm{id}_P$, and by definition the sequence splits.

(ii) $\Rightarrow$ (iii) Since every module is the epimorphic image of a free module, we can assume that there is a free module F and a surjective homomorphism $\varphi : F \longrightarrow P$. Consider now the short exact sequence $0 \longrightarrow \ker\varphi \longrightarrow F \xrightarrow{\varphi} P \longrightarrow 0$, which splits after assumption. Thus, by Proposition 1.2.5(iii) we have $F \cong \ker\varphi \oplus P$, proving (iii).

(iii) $\Rightarrow$ (i) Let P' be an R-module such that $P \oplus P'$ is free, and assume M, N, π and φ as in Definition 1.2.6. Extend $\varphi : P \longrightarrow N$ to a homomorphism $\Phi : P \oplus P' \longrightarrow N$ by setting $\Phi(x, y) := \varphi(x)$ for $x \in P$, $y \in P'$. The claim is proved if we can show that there is a homomorphism $\Psi : P \oplus P' \longrightarrow M$ such that $\pi \circ \Psi = \Phi$, since then $\psi := \Psi(., 0)$ is the desired homomorphism.

To this end, let $F := P \oplus P'$ and $(x_i)_{i \in I}$ be a basis of F. Further, let $n_i := \Phi(x_i)$ be the images of the elements of this basis under Φ, then there are $m_i \in M$ with $\pi(m_i) = n_i$

since π is surjective. Now define $\Psi : F \longrightarrow M$ by $\Psi(x_i) = m_i$ and observe that $\pi \circ \Psi = \Phi$, which proves the claim. □

Remark. If P in Proposition 1.2.7 is assumed to be finitely generated, we can choose the free module F to be finitely generated as well. In this case, there is an R-module P' with $P \oplus P' \cong R^n$ for an $n \in \mathbb{N}$.

If A is a K-algebra, then finitely generated projective A-modules are intimately connected with the PIMs of A. More precisely, we have the following

Proposition 1.2.8. *Let A be a K-algebra. A finitely generated A-module P is projective if and only if it is isomorphic to a direct sum of PIMs of A.*

Proof. If P is a direct sum of PIMs of A, then P is clearly a direct summand of the free A-module A.

Conversely, let P be a finitely generated projective A-module. Then by Proposition 1.2.7(iii) and the remark following the proof, P is a direct summand of a free A-module $F \cong A^n$ for an $n \in \mathbb{N}$. But every copy of A is a direct sum of PIMs, and applying the Krull-Schmidt theorem 1.1.7 proves the claim. □

Proposition 1.2.8 shows that every PIM P of a K-algebra A is projective, and indeed, the term 'PIM' sometimes denotes a projective indecomposable module. In the case of group algebras KG, projective modules have even stronger properties. To show this, we first discuss the dual notion of injective modules.

Definition 1.2.9 (Injective modules)**.** Let L and M be R-modules. An R-module Q is called injective if for every injective homomorphism $\iota \in \mathrm{Hom}_R(L, M)$ and every homomorphism $\varphi \in \mathrm{Hom}_R(L, Q)$ there is a homomorphism $\psi \in \mathrm{Hom}_R(M, Q)$ such that $\psi \circ \iota = \varphi$, i.e., the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "\iota"] \arrow[d, "\varphi"'] & M \arrow[dl, dotted, "\psi"] \\
 & Q &
\end{tikzcd}$$

Proposition 1.2.10. *An R-module Q is injective if and only if every short exact sequence $0 \longrightarrow Q \longrightarrow M \longrightarrow N \longrightarrow 0$ of R-modules splits.*

Proof. To begin with, let Q be injective and take $L = Q$ and $\varphi = \mathrm{id}_Q$ in Definition 1.2.9. Then there is a homomorphism $\psi : M \longrightarrow Q$ with $\psi \circ \iota = \mathrm{id}_Q$ and by Proposition 1.2.5(ii) the sequence splits.

Conversely, suppose that every short exact sequence $0 \longrightarrow Q \longrightarrow M \longrightarrow N \longrightarrow 0$ of R-modules splits, and let L, M, ι and φ be as in Definition 1.2.9. Consider the submodule $S := \{(\varphi(x), -\iota(x)) \mid x \in L\}$ of $Q \oplus M$ (the reason for the minus sign will become apparent at the end of the proof), and let $T := (Q \oplus M)/S$ be the corresponding factor module, $[x, y] \in T$ denoting the class of $(x, y) \in Q \oplus M$. Further, set $N = M/\iota(L)$ and let $\pi : M \longrightarrow N$ be the canonical map. Then the maps $f : Q \longrightarrow T$, $f(x) = [x, 0]$ and $g : T \longrightarrow N$, $g([x, y]) = \pi(y)$ constitute a short exact sequence

$$0 \longrightarrow Q \xrightarrow{f} T \xrightarrow{g} N \longrightarrow 0$$

which splits after assumption. Thus, there is a map $h : T \longrightarrow Q$ such that $h \circ f = \mathrm{id}_Q$. Define now $\psi : M \longrightarrow Q$ as $\psi(x) := h([0, x])$ and observe that for all $x \in L$ we have

$$\begin{aligned}(\psi \circ \iota)(x) &= h([0, \iota(x)]) \\ &= h[(\varphi(x), 0)] \\ &= (h \circ f \circ \varphi)(x) \\ &= \varphi(x)\end{aligned}$$

That is, $\psi \circ \iota = \varphi$. Note that for the second equality sign we need the minus in the definition of S. □

After having defined and characterized projective and injective modules, we now want to investigate the relationship between them in the case of KG-modules. We will see that these two properties are actually equivalent. To understand this we first need to formalize the above mentioned duality between injective and projective modules.

Definition 1.2.11 (Dual module)**.** Let M be a KG-module. Consider the dual (vector) space $M^* = \mathrm{Hom}_K(M, K)$ of the K-vector space M and define for $g \in G$ and $\varphi \in \mathrm{Hom}_K(M, K) = M^*$:

$$\begin{aligned} g\varphi : M &\longrightarrow K \\ v &\longmapsto \varphi(g^{-1}v)\end{aligned}$$

It is easy to verify that this definition turns M^* into a KG-module. M^* is called the dual KG-module of ${}_{KG}M$. If $\rho : M \longrightarrow N$ is a KG-homomorphism from M to N, then the homomorphism $\rho^* : N^* \longrightarrow M^*$ is defined by

$$\rho^*(\psi) : M \longrightarrow K$$

$$v \longmapsto \psi(\rho(v))$$

and it is again readily verified that $g\rho^*(\psi) = \rho^*(g\psi)$ such that ρ^* is a KG-homomorphism from N^* to M^*.

Lemma 1.2.12. *Let M, M_1 and M_2 be KG-modules.*

(i) $M \cong_{KG} M^{**}$

(ii) *Let N be a submodule of M, then N is isomorphic to the dual of a quotient module of M, that is, there is a submodule N' of M^* such that $N' \cong_{KG} (M/N)^*$ and $N^* \cong_{KG} M^*/N'$.*

(iii) $(M_1 \oplus M_2)^* \cong_{KG} M_1^* \oplus M_2^*$

(iv) *If $\varphi : P \to Q$ and $\psi : Q \to R$ are KG-module homomorphisms, then $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.*

(v) *M is simple if and only if M^* is simple.*

Proof. The properties (i)-(iv) carry over directly from the corresponding results about vector spaces.

(v) If M contains a proper submodule N, then by (ii) M^* also contains a proper submodule and is therefore not simple. The same argument applied to M^* together with (i) proves the converse. $\square$

The next lemma is the key stone in our main result and ensures that the dual of a projective module is again projective:

Lemma 1.2.13. *The group algebra KG is selfdual, that is, $KG \cong_{KG} (KG)^*$.*

Proof. For each $g \in G$ define the K-linear functional $\varphi_g : KG \longrightarrow K$ on $x \in G$ by

$$\varphi_g(x) = \begin{cases} 1_K & x = g \\ 0 & x \neq g \end{cases}$$

and extend it by linearity onto KG. Consider now the K-homomorphism $KG \longrightarrow (KG)^*$, $g \longmapsto \varphi_g$, which maps a K-basis of KG onto a K-basis of $(KG)^*$ and is therefore an isomorphism. We see that it is also a KG-homomorphism: For $g, h \in G$ we have

$$(g\varphi_h)(x) = \varphi_h(g^{-1}x)$$

which is 1_K if $h = g^{-1}x$, that is, $x = gh$, and 0 if $h \neq g^{-1}x$, that is, $x \neq gh$. Hence, $g\varphi_h = \varphi_{gh}$, and therefore $KG \cong_{KG} (KG)^*$. $\square$

Corollary 1.2.14. *If M is a free KG-module, then so is M^*.*

Corollary 1.2.15. *The dual of a projective KG-module is projective.*

Lemma 1.2.13 implies another useful result about group algebras which we already pointed out at the end of Section 1.2.1:

Corollary 1.2.16.

$$\operatorname{soc} KG \cong KG/\operatorname{rad} KG$$

In particular, if P is a PIM of KG then $\operatorname{soc} P \cong P/\operatorname{rad} P$.

Proof. We show that for an arbitrary KG-module M we have $(M/\operatorname{rad} M)^* \cong \operatorname{soc} M^*$. Setting $M = KG$ and applying Lemma 1.2.13 then proves the claim.

Consider therefore the KG-module $M/\operatorname{rad} M$. Since the group algebra KG is Artinian, $M/\operatorname{rad} M$ is semisimple by Proposition 1.1.22(i). By Lemma 1.2.12(v) this also holds for the dual $(M/\operatorname{rad} M)^*$. Hence, $(M/\operatorname{rad} M)^*$ is a sum of simple modules and therefore a submodule of $\operatorname{soc} M^*$. On the other hand, suppose S^* is a simple submodule of M^*. Then by Lemma 1.2.12(ii) there is a submodule M' of M such that $S^* \cong (M/M')^*$. Since S^* is simple, by Lemma 1.2.12(v) S is also simple, so M' is maximal in M and $\operatorname{rad} M \leq M'$. Hence, $M'/\operatorname{rad} M$ is a submodule of $M/\operatorname{rad} M$, and by Lemma 1.2.12(ii) there is a submodule T of $(M \operatorname{rad} M)^*$ with $T \cong ((M/\operatorname{rad} M)/(M'/\operatorname{rad} M))^* \cong (M/M')^*$. We see that $S^* \cong T$ is a submodule of $(M/\operatorname{rad} M)^*$. Since S^* was arbitrary, the claim $\operatorname{soc} M^* \cong (M/\operatorname{rad} M)^*$ follows. $\square$

We are now ready to prove

Theorem 1.2.17. *A KG-module M is projective if and only if it is injective.*

Proof. Suppose that M is projective, and consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\iota"] \arrow[d, "\varphi"'] & L \\ & M & \end{tikzcd}$$

where ι and φ are KG-module homomorphisms, ι being injective. We have to show that there is a KG-module homomorphism $\psi : L \longrightarrow M$ such that $\varphi = \psi \circ \iota$.

To this end, take duals in the above situation, resulting in the following diagram:

$$\begin{tikzcd}
0 & N^* \arrow[l] & L \arrow[l, "\iota^*"'] \\
& M^* \arrow[u, "\varphi^*"] &
\end{tikzcd}$$

We first show that ι^* is surjective. Let $\rho \in N^*$, then we can define the homomorphism $\chi : L \longrightarrow N$ on the image $\iota(N)$ in L by $\chi(\iota(n)) := \rho(n)$. This is well-defined since ι is injective. But by Definition 1.2.11, $\iota^*(\chi) = \rho$; hence, $\iota^*(L) = N$.

Since M is projective, it is a direct summand of a free module F by Proposition 1.2.7. Lemma 1.2.12(iii) together with Corollary 1.2.14 then imply that M^* is a direct summand of the free module F^* and hence also projective. Thus, there is a homomorphism $\psi^* : M^* \longrightarrow L^*$ such that $\varphi^* = \iota^* \circ \psi^*$. But by Lemma 1.2.12(iv) we have $\varphi = (\iota^* \circ \psi^*)^* = \psi \circ \iota$. Hence, $\psi : L \longrightarrow M$ is the desired homomorphism, and M is injective.

An entirely analogous argument proves the opposite direction. □

Remark. The proof of Theorem 1.2.17 shows that by taking duals all the arrows in a diagram are reversed. To this extent, projective and injective modules are dual to each other inasmuch as the defining diagram of the former is 'dualized' into the diagram of the latter and vice versa.

1.2.3. Multiplicities of PIMs in decompositions of algebras over a field

In Subsection 1.1.1 we showed that since a K-algebra A has finite length, any decomposition of it into a direct sum of PIMs is unique up to isomorphism and order of appearance. Theorem 1.2.2 in Subsection 1.2.1 further states that on the one hand every PIM P of A possesses a unique submodule $\operatorname{rad} P$, and on the other hand the number of isomorphy classes of PIMs is the same as the number of distinct non-isomorphic simple A-modules. Our next objective is to determine the number of PIMs in each isomorphy class. More precisely, suppose we have a decomposition

$$A = \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{q_i} P_{ij}$$

of the K-algebra A into a direct sum of PIMs, where for fixed i the PIMs P_{ij} are pairwise isomorphic for $1 \leq j \leq q_i$ (to be determined by Theorem 1.2.2(ii)). Then our task is to find q_i for $1 \leq i \leq t$, which can be achieved by deploying intertwining numbers.

Throughout this subsection, let A be a K-algebra. We start with a

Definition 1.2.18. Let M and N be A-modules. The intertwining number $i(M,N)$ is defined by

$$i(M,N) := \dim_K(\mathrm{Hom}_A(M,N))$$

Lemma 1.2.19. *Let M, N_1 and N_2 be A-modules, then the following holds:*

(i) $i(M, N_1 \oplus N_2) = i(M,N_1) + i(M,N_2)$
$i(N_1 \oplus N_2, M) = i(N_1,M) + i(N_2,M)$

(ii) $i(A,M) = \dim_K M$

(iii) *If $e \in A$ is an idempotent, then $i(Ae,M) = \dim_K eM$.*

Proof. (i) The identities follow from the respective identities involving modules of homomorphisms.

(ii) Define the K-homomorphism $\Pi : \mathrm{Hom}(A,M) \longrightarrow M$, $\varphi \longmapsto \varphi(1_A) = m_0 \in M$. Suppose $\Pi(\varphi) = \varphi(1) = 0$. Then $\varphi(a) = \varphi(a1_A) = a\varphi(1_A) = 0$ for all $a \in A$, that is, $\varphi = 0$; hence, Π is injective. Conversely, for $m \in M$ define $\varphi \in \mathrm{Hom}(A,M)$ by $\varphi(a) = am$. Thus, Π is bijective and $\mathrm{Hom}(A,M) \cong M$, from which $i(A,M) = \dim M$ follows.

(iii) In analogy to (ii), define the K-homomorphism $\Psi : \mathrm{Hom}(Ae,M) \longrightarrow M$, $\varphi \longmapsto \varphi(e)$. Then Ψ is injective since $\Psi(\varphi) = 0$ implies $\varphi(ae) = a\varphi(e) = 0$ for all $a \in A$, giving $\varphi = 0$. We claim that $\mathrm{im}\,\Psi = eM$. Since $\Psi(\varphi) = \varphi(e) = \varphi(e^2) = e\varphi(e)$ for all $\varphi \in \mathrm{Hom}(Ae,M)$, we have $\mathrm{im}\,\varphi \subset eM$. Conversely, for $m \in M$ we define $\varphi \in \mathrm{Hom}(Ae,M)$ by $\varphi(ae) := aem$. Then $\Psi(\varphi) = \varphi(e) = em$, implying $\mathrm{im}\,\Psi \supset eM$ and $\mathrm{Hom}(Ae,M) \cong eM$. Now the claim follows. $\square$

In order to prove the main result, we need an important theorem connecting a PIM P of A to A-modules M with composition series. This is in some way a refinement of Corollary 1.2.3.

Theorem 1.2.20. *Let P be a PIM of A and M an A-module with composition series $M = M_0 \supset M_1 \supset \cdots \supset M_r = 0$. Then*

$$i(P,M) = qk$$

where q is the number of factors of M which are isomorphic to $P/\operatorname{rad} P$ and $k = i(P/\operatorname{rad} P, P/\operatorname{rad} P)$.

Proof. Fix an index $0 \leq j < r$ and define the homomorphism

$$\begin{aligned}\Psi : \operatorname{Hom}(P, M_j) &\longrightarrow \operatorname{Hom}(P, M_j/M_{j+1})\\ \tau &\longmapsto \pi \circ \tau\end{aligned}$$

where $\pi : M_j \longrightarrow M_j/M_{j+1}$ is the natural projection onto the factor module. We first show that Ψ is surjective. To this end, abbreviate $R_j := M_j/M_{j+1}$ and let $\sigma \in \operatorname{Hom}(P, R_j)$ and $\pi_P : A \longrightarrow P$ be the projection onto P from Proposition 1.1.2(i). Let $m_0 := \sigma(\pi_P(1_A))$, then there is an $m_1 \in M_j$ with $\pi(m_1) = m_0$. Define $\tau \in \operatorname{Hom}(P, M_j)$ by $\tau(x) = xm_1$, then we have for $x \in P$:

$$\begin{aligned}\sigma(x) = \sigma(\pi_P(x)) &= \sigma(\pi_P(x \cdot 1_A)) = x\sigma(\pi_P(1_A))\\ &= xm_0 = x\pi(m_1) = \pi(xm_1) = \pi(\tau(x))\end{aligned}$$

Hence, $\sigma = \pi \circ \tau$, and Ψ is surjective. The kernel of Ψ is $\operatorname{Hom}(P, M_{j+1})$ and thus,

$$\operatorname{Hom}(P, M_j)/\operatorname{Hom}(P, M_{j+1}) \cong \operatorname{Hom}(P, R_j)$$

and correspondingly,

$$i(P, M_j) - i(P, M_{j+1}) = i(P, R_j)$$

Using Lemma 1.2.19(i) and summing over j in the last equation gives

$$i(P, M) = \sum_{j=0}^{r-1} i(P, R_j) \tag{*}$$

Let us investigate the number $i(P, R_j)$. Either, $i(P, R_j) = 0$ or there is a homomorphism $\tau \in \operatorname{Hom}(P, R_j)$ with $\tau \neq 0$. But since R_j is simple, $\tau(P) = R_j$, $P/\ker\tau \cong R_j$, and by Theorem 1.2.2(i) $\ker\tau = \operatorname{rad} P$, the unique maximal submodule of P. Therefore, τ induces an isomorphism $\overline{\tau} : P/\operatorname{rad} P \longrightarrow M_j/M_{j+1}$. Conversely, suppose we have an isomorphism $\overline{\tau} : P/\operatorname{rad} P \longrightarrow R_j$, then $\tau = \overline{\tau} \circ \pi' \in \operatorname{Hom}(P, R_j)$, where $\pi' : P \longrightarrow P/\operatorname{rad} P$ is the natural projection onto the factor module. Therefore,

$$\operatorname{Hom}(P, R_j) \cong \operatorname{Hom}(P/\operatorname{rad} P, R_j) \cong \operatorname{Hom}(P/\operatorname{rad} P, P/\operatorname{rad} P)$$

and in particular, $i(P, R_j) = i(P/\operatorname{rad} P, P/\operatorname{rad} P)$. Applying this reasoning to (*) proves the claim. $\square$

In total we have gathered much more information about the decomposition of an algebra A:

Theorem 1.2.21. *Let A be a K-algebra with a decomposition*

$$A = \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{q_i} P_{ij}$$

into a direct sum of PIMs P_{ij}, where for fixed i the PIMs P_{ij} are pairwise isomorphic for $1 \leq j \leq q_i$, meaning $P_{ij} \cong P_{kl}$ if and only if $i = k$. Define further the following numbers:

$$\begin{aligned} n &= \dim A & n_i &= \dim(P_{i1}/\operatorname{rad} P_{i1}) \\ d_i &= \dim P_{i1} & k_i &= \dim \operatorname{End}(P_{i1}/\operatorname{rad} P_{i1}) \end{aligned}$$

Then the following identity holds:

$$n = \sum_{i=1}^{t} \frac{n_i}{k_i} d_i$$

Proof. Lemma 1.2.19(ii) implies $i(A, P_{i1}/\operatorname{rad} P_{i1}) = \dim(P_{i1}/\operatorname{rad} P_{i1}) = n_i$. Therefore,

$$\begin{aligned} n_i &= i(A, P_{i1}/\operatorname{rad} P_{i1}) \\ &= i\left(\bigoplus\nolimits_{l=1}^{t} \bigoplus\nolimits_{m=1}^{r_l} P_{lm}, P_{i1}/\operatorname{rad} P_{i1}\right) \\ &= \sum_{l=1}^{t} \sum_{m=1}^{r_l} i(P_{lm}, P_{i1}/\operatorname{rad} P_{i1}) \qquad \text{by Lemma 1.2.19(i)} \end{aligned}$$

Theorem 1.2.20 implies

$$i(P_{lm}, P_{i1}/\operatorname{rad} P_{i1}) = \begin{cases} k_j & \text{if } P_{lm} \cong P_{i1} \\ 0 & \text{else} \end{cases}$$

which means that $n_i = q_i k_i$. Now compare the dimensions on both sides of the decomposition

$$A = \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{q_i} P_{ij}$$

to obtain

$$n = \sum_{i=1}^{t} q_i d_i = \sum_{i=1}^{t} \frac{n_i}{k_i} d_i$$

□

In our applications we can disregard the number k_i by the following

Proposition 1.2.22. *Let A be an algebra over an algebraically closed field K and S be a simple A-module. Then* $\operatorname{End}_A S \cong K$.

Proof. Let $\varphi \in \operatorname{End}_A S$, then also $\varphi \in \operatorname{End}_K(S)$ when treating S as a K-vector space. Since K is algebraically closed, there is an eigenvalue $\lambda \in K$ of φ, and then $\varphi - \lambda \operatorname{id} \in \operatorname{End}_A S$. Since S is simple and $\varphi - \lambda \operatorname{id}$ is singular, $\operatorname{im}(\varphi - \lambda \operatorname{id}) = 0$. Hence $\varphi - \lambda \operatorname{id} \equiv 0$, giving $\varphi = \lambda \operatorname{id}$. □

Remark. Strictly speaking, the assumption that K be algebraically closed is too strong. In fact it suffices to assume that the characteristic polynomial of every $\varphi \in \operatorname{End}_A S$ for every simple A-module S has a root in K. Such fields are called splitting fields for the algebra A and will be dealt with in Section 2.1.1.

1.3. The Meataxe algorithm

Since one of the main tasks of representation theory is to find the irreducible representations of a group G, we are often interested in answering the question whether or not a given KG-module M is simple. Even if the answer is negative, we might find a proper submodule N of M along the way and ask again whether or not N is simple. Moreover, if the field K is a finite field $\mathbb{F}_q$, where $q = p^n$ for some n, and the algebra KG is finite-dimensional over $\mathbb{F}_q$ (which is always the case for finite groups G), the problem is finite. Since we can in principle list all the elements of KG, computations in the group algebra are feasible, especially with computer algebra systems such as `GAP` (cf. Section 3.3).

There is a well known algorithm devised by Richard Parker called the Meataxe to investigate KG-modules M with respect to simplicity. This section explains its key ingredient, Norton's irreducibilty criterion, and presents a widely used extension of Parker's Meataxe, the Holt-Rees algorithm by Derek F. Holt and Sarah Rees.

1.3.1. Norton's irreducibilty criterion

Let us first start with a simple observation from linear algebra:

Lemma 1.3.1. *Let V be a finite-dimensional vector space over K and W be a subspace of V with $\varphi(W) \subset W$ for an endomorphism $\varphi \in \operatorname{End}_K(V)$. Then $\ker_{V^*} \varphi^* \leq W^\circ$ if $W \cap \ker \varphi = (0)$.*

Proof. By definition, $\ker \varphi^* = \{f \in V^* \mid 0 = \varphi^*(f) = f \circ \varphi\} = (\operatorname{im} \varphi)^\circ$. The condition $W \cap \ker \varphi = (0)$ means that $\varphi|_W$ is injective. Thus, W is a subspace of $\operatorname{im} \varphi$, and dually $(\operatorname{im} \varphi)^\circ = \ker \varphi^*$ is a subspace of W°, proving the claim. ☐

Proposition 1.3.2 (Norton's irreducibility criterion)**.** *Let A be a K-algebra and M be an A-module with $\dim_K M < \infty$. Choose further an element $a \in A$ such that $\ker_M a \neq (0)$. Then M is simple if and only if*

(a) *$M = Av$ for all $v \in \ker_M a$.*

(b) *$M^* = wA$ for some $w \in \ker_{M^*} a^*$.*

Proof. If M is simple, then by Proposition 1.2.12(v) both (a) and (b) hold.

Conversely, suppose that both (a) and (b) are true, and let N be a proper submodule of M. Then $\ker_M a \cap N = (0)$, since (a) holds. Lemma 1.3.1 implies $\ker_{M^*} a^* \leq N^\circ \leq M^*$, and by (b) we have $N^\circ = M^*$, so $N = (0)$ and M is simple. ☐

Remark. If M is not simple, a proper submodule is found in (a) or (b). This submodule is of the form Av for some $v \in \ker_M a$ or of the form wA for all $w \in \ker_{M^*} a^*$.

1.3.2. Holt-Rees algorithm

The Holt-Rees algorithm is an extension of the Meataxe algorithm and deploys the computation and factorization of characteristic polynomials of an element $a \in A$. Let us start with a KG-module M which we want to test for simplicity. In our case, $K = \mathbb{F}_q$, the finite field with q elements.

If $g_1, \ldots, g_r$ are generators of the group G and $\rho : G \longrightarrow M_d(K)$ is a representation of G on the vector space $M = K^d$, the matrices $x_1 = \rho(g_1), \ldots, x_r = \rho(g_r)$ define the action of G on the KG-module M. The input is the K-algebra A generated by these matrices, and the algorithm looks as follows:

(1) Choose a random element $a \in A$.

(2) Compute the characteristic polynomial $p_a(x)$ of a.

(3) Factorize $p_a(x)$ into the irreducible factors $f(x)$ and order them by increasing degree. For each $f(x)$ do the following:

(a) Calculate $v = f(a)$.

(b) Calculate $N = \ker_M(v)$. If $\dim N = \deg f$, the factor $f(x)$ of $p_a(x)$ is called a good factor.

(c) Choose a non-zero element $w \in N$ and calculate a basis of the submodule of M generated by this vector under the action of G via the matrices $x_1, \dots, x_r$. If this is a proper submodule of M, return the answer **reducible** and terminate the algorithm.

(d) Calculate $N' = \ker_{M^*}(v^*)$.

(e) Choose a non-zero element $u \in N'$ and calculate a basis of the submodule of M^* generated by this vector under the (right) action of G via the matrices $x_1^T, \dots, x_r^T$. If this is a proper submodule of M^*, return the answer **reducible** and terminate the algorithm.

(f) If $f(x)$ is a good factor, return the answer **irreducible**.

(4) Repeat step (1).

The only major addition to the original Meataxe algorithm is the computation and factorization of the characteristic polynomial $p_a(x)$ of an element $a \in A$. Although one might think that this is a disadvantage, in [HR94, Sect. 1] Holt and Rees state that these computations consume the same amount of time as for example computing the nullspace $\ker_M(v)$ of an element $v \in A$.

The Holt-Rees algorithm is a so-called Las Vegas algorithm, meaning that it is not sure whether or not it terminates. However, if it does terminate, the returned answer is always correct. This is proved in the following

Proposition 1.3.3. *If the Holt-Rees algorithm terminates for the KG-module M, it always returns a correct answer.*

Proof. Since the answer 'reducible' arises from the computation of a proper submodule of M, there is nothing to prove. In order to prove the correctness of the answer 'irreducible', we will show that if M is reducible and contains a proper submodule L, then choosing an element $a \in A$ such that $p_a(x)$ has a good factor $f(x)$ leads to the answer 'reducible'.

So assume L, $a \in A$, $p_a(x)$ and $f(x)$ as above. Let N be as in step (3b) of the algorithm and regard a as an endomorphism of M. Then $a|_N$ has the minimal polynomial $f(x)$ and since $\dim N = \deg f$, the map a is irreducible on N. Therefore, the subspace $L \cap N$, which is fixed by a, is trivial, i.e., either (0) or N. In the latter case the non-zero vector chosen in step (3c) of the algorithm generates a non-trivial submodule S of M contained in L, and the algorithm terminates with the answer 'reducible'.

On the other hand, suppose $L \cap N = (0)$, then Lemma 1.3.1 implies that $N' = \ker_{M^*} v^* \leq L^\circ$. Observe that N' is not zero and $L^\circ \neq M^*$ (since otherwise $L = (0)$, contradicting the assumption). Therefore, step (3e) finds a proper submodule, and the algorithm terminates with the answer 'reducible'. $\square$

2. Modular representation theory

This chapter provides an introduction to modular representation theory. A representation $\rho : G \longrightarrow \mathrm{End}_K(V)$ is called modular if the characteristic of K divides the order of G, so that the group algebra KG is not semisimple by Maschke's theorem 1.1.13. It turns out that in this case a very fruitful approach to investigating the group algebra KG is by working with p-modular systems. They are the subject of the first section and once properly defined, they are used exclusively in the further study of modular representations. In the second part we turn to irreducible modular representations and investigate Cartan numbers, decomposition numbers and Brauer characters. The former relate representations in characteristic zero to modular representations, whereas Brauer characters are the analogue of ordinary characters in the modular case. The last part contains an introduction to the basic tools of block theory and proves the most important structure theorems as well as a formula for the block idempotents.

In this chapter we mostly follow [Bur65, pp. 120, Ch. VI] and [DP77]. Beyond that, Sections 2.1 and 2.2 include results from [LP10] and [Ser77], respectively. Since the last section on block theory only covers the basic results needed for Chapter 3, the interested reader is referred to the bibliography. In particular, [Alp86] and [DP77] are recommended as starting points for block theory.

Let us fix some notation. The conjugacy classes of a finite group G are denoted by $\mathcal{C}_1, \ldots, \mathcal{C}_s$. We also use the standard notation $g^G := \{h^{-1}gh \mid h \in G\}$, i.e., for $g \in \mathcal{C}_i$ we have $g^G = \mathcal{C}_i$.

2.1. p-modular systems

2.1.1. Splitting fields

Consider a K-algebra A, a field extension $L \supset K$ and an A-module M, and construct the tensor products $A_L := L \otimes_K A$ and $M_L := L \otimes_K M$, viewed as an A_L-module. Provided that the A-module M is simple, one might ask if the A_L-module M_L is still simple, which leads to the following

Definition 2.1.1 (Absolutely simple module)**.**

(i) A simple A-module M is called absolutely simple if M_L is simple for every field extension $L \supset K$ of K.

(ii) An irreducible representation $\rho : G \longrightarrow V$ over a K-vector space V is called absolutely irreducible if the corresponding KG-module V is absolutely simple.

If we consider algebraic field extensions of K in Definition 2.1.1, which for finite-dimensional K-algebras such as the group algebra of a finite group is justified by Proposition 2.1.4 below, every simple module over an algebraically closed field K is also absolutely simple. Hence, every irreducible representation $\rho : G \longrightarrow \mathrm{Aut}(\mathbb{C}^n)$ is absolutely irreducible, and this is the reason why ordinary representation theory is usually carried out over $\mathbb{C}$. However, often a smaller (sub-) field already accounts for all the irreducible representations, and one could have restricted the computation of the irreducible representations to this particular field.

Definition 2.1.2 (Splitting field)**.**

(i) A field L is called a splitting field for the K-algebra A if every simple A_L-module M is absolutely simple.

(ii) A field L is called a splitting field for the group G if K is a splitting field for the group algebra KG.

In light of Proposition 1.2.22, splitting fields can be characterized by the following

Proposition 2.1.3. *If K is a splitting field for A, then* $\mathrm{End}_A(M) \cong K$ *for every simple A-module M.*

Proof. Suppose that K is a splitting field for A, and let L be the algebraic closure of K. Then for every simple A-module M the A_L-module M_L is simple, and

$$L \otimes \mathrm{End}_A(M) \cong \mathrm{End}_{A_L}(M_L) \cong L$$

by Proposition 1.2.22. Since A is a finite-dimensional K-algebra, an endomorphism $\varphi \in \mathrm{End}_A(M)$ can be represented by a matrix with entries in K. Hence, the image of $\mathrm{End}_A(M)$ under the above isomorphism is the set of K-multiples of the identity, that is, $\mathrm{End}_A(M) \cong K$. □

Remark. The statement of Proposition 2.1.3 is in fact an equivalence, i.e., if $\operatorname{End}_A(M) \cong K$ for every simple A-module M then K is a splitting field for A. A proof can be found in [DP77, p. 25, Thm. 1.7B].

The next proposition shows that in case of finite-dimensional K-algebras the splitting field can be chosen as an algebraic extension of K.

Proposition 2.1.4. *Let A be a K-algebra with $\dim_K A < \infty$. Then there is a splitting field $L \supset K$ with $[L : K] < \infty$.*

Proof. Let $\{a_1, \ldots, a_n\}$ be a K-basis of A and let $\bar{K}$ be the algebraic closure of K. Further, let $S_1, \ldots, S_m$ be representatives of the isomorphy classes of simple $\bar{K}$-modules (cf. Corollary 1.2.4) and $\mathfrak{b}_i = \{b^i_1, \ldots, b^i_{r_i}\}$ be a $\bar{K}$-basis of S_i for $i = 1, \ldots, m$. Denote by ρ_i the matrix representation afforded by S_i with respect to the basis $\mathfrak{b}_i$, and let L be the field obtained by adjoining to K all entries of the matrices $\rho_i(a_j)$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. We will show that L is a splitting field for A.

Due to the definition of L, the module $S'_i := \langle b^i_1, \ldots, b^i_{r_i} \rangle_L$ is a simple A_L-module, and we observe that $(S'_i)_{\bar{K}} = S_i$, which means that S'_i is absolutely simple. Moreover, for an arbitrary simple L-module S we have for some $i = 1, \ldots, m$ that

$$(0) \neq \operatorname{Hom}_{A_{\bar{K}}}(S_{\bar{K}}, (S'_i)_{\bar{K}}) \cong \bar{K} \otimes_L \operatorname{Hom}_{A_L}(S, S'_i)$$

implying $S \cong S'_i$. Thus, S is absolutely simple, and L is a splitting field for A. □

Corollary 2.1.5. *Let A be a finite-dimensional K-algebra. Then the algebraic closure of K is a splitting field for A.*

Proof. According to Proposition 2.1.4, let L be a splitting field of A with $[L : K] < \infty$. Since the algebraic closure $\bar{K}$ of K contains every algebraic extension of K and hence L, every simple $A_{\bar{K}}$-module is absolutely irreducible. □

Since the group algebra of a finite group is finite-dimensional, Corollary 2.1.5 is the reason why ordinary representation theory of finite groups is usually carried out over the complex numbers $\mathbb{C}$ or another algebraically closed field. However, note that by Proposition 1.2.22 and the remark following Proposition 2.1.3, the algebraic closure $\bar{K}$ is also a splitting field for an infinite-dimensional K-algebra.

The splitting field for a finite group is explicitly known due to a well-known theorem by R. Brauer. Recall that the exponent $\exp G$ of a group G is the least common multiple of the orders of the elements of G.

Theorem 2.1.6 (Brauer)**.** *Let G be a finite group with exponent n and ζ_n be a primitive n-th root of unity. Then $\mathbb{Q}(\zeta_n)$ is a splitting field for G.*

Proof. See [CR81, Vol. I, p. 386, Cor. 15.18] □

This also holds in the case of a (finite) extension of a finite field:

Theorem 2.1.7. *Let G be a finite group with exponent n and K be a splitting field of the polynomial $X^n - 1 \in \mathbb{F}_p[X]$. Then K is also a splitting field for G.*

Proof. See [DP77, p. 58, Thm. 2.7B(ii)] □

2.1.2. Lifting idempotents

The idea of modular representation theory is the investigation of the group algebra kG, where k is a field of characteristic p. Here, we are only considering primes p which divide the order of G, such that Maschke's theorem 1.1.13 does not hold. At first any choice of k seems reasonable, but it turns out that the use of (extensions of) p-adic fields and their corresponding residue fields connects representation theory in characteristic p and ordinary representation theory in characteristic 0 in a satisfactory way. The nature of this connection will become clear when we prove the main result of this section about lifting idempotents.

Let us first define Cauchy sequences for general valuation rings.

Definition 2.1.8. Let (R, ν) be a valuation ring. A sequence $(v_n)_{n\in\mathbb{N}} \in R$ is called a Cauchy sequence if

$$\lim_{n\to\infty} \nu(v_n - v_{n-1}) = \infty$$

and convergent with limit v if

$$\lim_{n\to\infty} \nu(v_n - v) = \infty$$

R is called complete if every Cauchy sequence converges.

We also recall a few facts about p-adic fields which are needed in the following discussion.

Proposition 2.1.9. *Let K be a finite extension of the p-adic numbers $\mathbb{Q}_p$ and R be its ring of integers. Then the following assertions hold:*

(i) $K = \operatorname{Quot} R$ *and* $R \cap \mathbb{Q}_p = \mathbb{Z}_p$

(ii) *R is a free $\mathbb{Z}_p$-module.*

(iii) *The ring R has a unique maximal ideal πR for some uniformizing element $\pi \in R$, and the proper non-zero ideals of R are given by $\pi^n R$, $n = 1, 2, \ldots$.*

(iv) *R is a complete discrete valuation ring for K. The completeness is sometimes restated as*

$$\bigcap_{n=1}^{\infty} \pi^n R = 0$$

(v) *$k := R/\pi R$ is a finite field of characteristic p.*

(vi) *Every finitely generated torsion-free R-module is free.*

Proof. See [DP77, p. 66, Thm. 3.2] or [LP10, pp. 289, Sect. 4.1]. □

Keeping these results in mind we define the setting of our study of modular representations.

Definition 2.1.10 (p-modular systems)**.** Let G be a finite group with exponent n, p be a prime which divides the order of G and $K \supset \mathbb{Q}_p$ with $[K : \mathbb{Q}_p] < \infty$ be a splitting field for the polynomial $X^n - 1$. Let further R be the ring of integers in K and $\pi \in R$ a uniformizing element, i.e., πR is the unique maximal ideal in R. If $k := R/\pi R$ is the residue field of R, then by Theorem 2.1.6 and Theorem 2.1.7 both K and k are splitting fields for G. The system (K, R, k) is called a p-modular system for G.

Note that K, R and k are commutative rings, so the group algebras KG, RG and kG are well defined. The following two theorems show the intimate connection of these three structures.

Theorem 2.1.11 (Lifting idempotents)**.** *Let K, R and k be as in Proposition 2.1.9 and A an R-algebra which is free and finitely generated as an R-module (this is also called an R-order). Set $\bar{A} := A/\pi A$, which is a k-algebra, and write $\bar{x} \in \bar{A}$ for the class of $x \in A$.*

(i) *If e is a non-zero idempotent in A, then $\bar{e}$ is a non-zero idempotent in $\bar{A}$.*

(ii) *If f is an idempotent in $\bar{A}$, there is an idempotent $e \in A$ such that $\bar{e} = f$.*

Proof. (i) Since $^{-} \colon A \longrightarrow \bar{A}$ is an algebra homomorphism, we only have to show that $\bar{e} \neq 0$. Therefore, suppose $\bar{e} = 0$. Then $e \in \pi A$, and for every $n \in \mathbb{N}$ we have $e = e^n \in$

$\pi^n A$. Since A is a free and finitely generated R-module, it holds that $A \cong R^m$, and by Proposition 2.1.9(iv)

$$\bigcap_{n=1}^{\infty} \pi^n A = \bigcap_{n=1}^{\infty} (\pi R)^n A = \left(\bigcap_{n=1}^{\infty} (\pi R)^n \right) A = 0$$

which implies $e = 0$ and proves the claim.

(ii) Given an idempotent $f \in \bar{A}$, we are going to construct an idempotent $e \in A$ with $\bar{e} = f$. To this end, let $e_0 \in A$ be a preimage of f, and define for $n \in \mathbb{N}$ the sequences

$$e_{n+1} = 3e_n^2 - 2e_n^3 \qquad\qquad d_n = e_n^2 - e_n$$

We show by induction on n that $d_n \in \pi^{2^n} A$, from which the rest follows. Since $d_0 = e_0^2 - e_0$ and $\overline{d_0} = \overline{e_0}^2 - \overline{e_0} = f^2 - f = 0$, we have $d_0 \in \pi A$. Assume that the claim holds for n, and observe

$$d_{n+1} = e_{n+1}^2 - e_{n+1} = 9e_n^4 - 12e_n^5 + 4e_n^6 - 3e_n^2 + 2e_n^3 = 4d_n^3 - 3d_n^2$$

Applying the induction hypothesis $d_n \in \pi^{2^n} A$ we get $d_{n+1} \in \pi^{2^{n+1}} A$. Consequently, $e_{n+1} - e_n = d_n(1 - 2e_n) \in \pi^{2^n} A$; therefore, e_n is a Cauchy sequence in A. Since A is a finitely generated R-module, by Proposition 2.1.9(iv) e_n converges to an element $e \in A$. From $d_n \in \pi^{2^n} A$ follows $e^2 - e = \lim_{n\to\infty} \nu(e_n^2 - e_n) = \lim_{n\to\infty} \nu(d_n) = 0$; thus, e is an idempotent in A. Finally, since $e_{n+1} - e_n \in \pi A$ we have

$$e_n - e_0 = e_n - e_{n-1} + e_{n-1} - e_{n-2} + \cdots + e_1 - e_0 \in \pi A$$

for all n, implying $e - e_0 \in \pi A$ and $\bar{e} = f$. □

Remark. Theorem 2.1.11 can in fact be proved for an arbitrary complete discrete valuation ring A, see [LP10, pp. 289, Sect. 4.1].

Corollary 2.1.12. *Let G be a finite group and (K, R, k) be a p-modular system. Then a decomposition of kG into a direct sum of PIMs gives a corresponding decomposition of RG.*

Proof. By Theorem 1.1.2(ii) a decomposition of kG into PIMs corresponds to a complete set of primitive orthogonal idempotents $\{f_1, \ldots, f_m\} \subset kG$. Now apply Theorem 2.1.11. □

So far we have shown that p-modular systems relate representations over R to representations over k. The following theorem illustrates the relationship between representations defined over K and R.

Theorem 2.1.13. *Let (K, R, k) be a p-modular system for the finite group G. If M is a finitely generated KG-module, then there exists an RG-submodule N of the RG-module M and an R-basis of N which is at the same time a K-basis of M. Therefore, $K \otimes N = M$.*

Proof. Let $\{m_1, \dots, m_k\}$ be a K-basis of M and $G = \{g_1, \dots, g_n\}$ be the canonical R-basis of RG. Consider the (finitely generated) RG-module

$$N = \sum_{i=1}^{n} \sum_{j=k}^{n} Rg_i m_j \subset M$$

By Proposition 2.1.9(vi), the R-module N is free since any vector space over K is torsion-free and $R \subset K$. Moreover, every R-basis of N is also a K-basis of M and hence $K \otimes N = M$. $\square$

Corollary 2.1.14. *If (K, R, k) is a p-modular system for a finite group G and $\rho : G \longrightarrow \mathrm{GL}_m(K)$ is a representation defined over K, then ρ is equivalent to a representation $\rho' : G \longrightarrow \mathrm{GL}_m(K)$, where $\rho'(g)$ is defined over R for all $g \in G$.*

Theorems 2.1.11 and 2.1.13 allow us to relate representations over K and k. A detailed explanation of this process is given in Section 2.2.1.

2.2. Irreducible modular representations

For the remainder of our discussion we will stick to a p-modular system (K, R, k) for G as in Definition 2.1.10. We now turn to modular representations, treating the subject first from a module point of view before developing the theory of Brauer characters, which is in many ways analogous to ordinary character theory.

2.2.1. Cartan and decomposition numbers

Given an RG-module M we denote by $\overline{M} := k \otimes_R M$ the kG-module obtained by reducing M modulo π (recall that $k = R/\pi R$). The following denotations will be used throughout this section. Consider the s simple KG-modules $V_1, \dots, V_s$ corresponding to the s irreducible ordinary representations $\sigma_1, \dots, \sigma_s$, where s is the number of conjugacy classes of G. By Theorem 2.1.13 there are RG-modules $U_1, \dots, U_s$ such that $V_i = K \otimes U_i$ for $1 \le i \le s$, and we record the following

Lemma 2.2.1. *With the above denotations and assumptions, the kG-modules $\overline{U}_i$ are indecomposable.*

Proof. Suppose that $\overline{U_i}$ is decomposable, say $\overline{U}_i = \overline{U'} \oplus \overline{U''}$. This corresponds to a sum $e = e' + e''$ of idempotents where e is the idempotent corresponding to U_i. By Theorem 2.1.11 there are idempotents f, f' and f'' such that $f = f' + f''$ and $e = \bar{f} = \bar{f}' + \bar{f}'' = e' + e''$. They correspond to a decomposition $U_i = U' \oplus U''$ of RG-modules, and taking the tensor product with K gives

$$V_i = K \otimes U_i = (K \otimes U') \oplus (K \otimes U'')$$

by Proposition 2.1.9(vi). This contradicts the simplicity of V_i, hence $\overline{U}_i$ is indecomposable. $\square$

Consider further a decomposition of kG into a direct sum of PIMs, $kG = P_1 \oplus \cdots \oplus P_t$. By Theorem 1.2.2 for $1 \le i \le t$ the module P_i is a PIM with the unique maximal submodule $\operatorname{rad} P_i$ such that $S_i := P_i / \operatorname{rad} P_i$ is simple, and every simple kG-module is isomorphic to one of the S_i by Corollary 1.2.3. We make the following

Definition 2.2.2. With the modules $U_1, \dots, U_s$ and $P_1, \dots, P_t$ introduced above the Cartan number c_{ij} and the decomposition number d_{ij} are defined by

$$\begin{aligned} c_{ij} &:= i(P_j, P_i) \\ d_{ij} &:= i(P_j, \overline{U_i}) \end{aligned}$$

We also define the Cartan matrix C and the decomposition matrix D by

$$\begin{aligned} C &:= (c_{ij})_{1 \le i,j \le t} \\ D &:= (d_{ij})_{1 \le i \le s, 1 \le j \le t} \end{aligned}$$

We will prove in Section 2.2.2 (Corollary 2.2.14) that the definition of the decomposition number d_{ij} is independent of the chosen RG-modules U_i.

Theorem 1.2.20 says that $c_{ij} = i(P_j, P_i) = qk$, where q is the number of factors of P_i isomorphic to S_j and $k = i(S_j, S_j)$. A similar statement also holds for d_{ij}. If we consider a p-modular system (K, R, k) for G, then by Proposition 2.1.3 we have $k = 1$, and the numbers c_{ij} and d_{ij} have an immediate interpretation:

Lemma 2.2.3. *Let (K, R, k) be a p-modular system for G and $U_1, \ldots, U_s, P_1, \ldots, P_t$ as above. Then the following holds:*

(i) *The Cartan number c_{ij} is the number of factors of P_i isomorphic to the simple module S_j.*

(ii) *The decomposition number d_{ij} is the number of factors of $\overline{U_i}$ isomorphic to the simple module S_j.*

The definition of the Cartan number c_{ij} suggests that it is a symmetric quantity, and the next theorem indeed affirms this presumption. Let us first introduce the following notation: For a module M of finite length, we write $M \sim \sum_{i=1}^{n} N_i$ to say that up to isomorphy the modules N_i, $1 \leq i \leq n$ are exactly the factors of a composition series of M. The N_i are uniquely determined by the Jordan-Hölder theorem 1.1.11 up to isomorphism and order.

Theorem 2.2.4. *It holds that*

$$C = D^T D$$

In particular, C is a symmetric matrix.

Proof. According to the denotations fixed above, let $f_1, \ldots, f_t$ be the set of primitive orthogonal idempotents corresponding to the PIMs $P_1, \ldots, P_t$. Then by Theorem 2.1.11(ii) these idempotents can be lifted to a set of primitive orthogonal idempotents $e_1, \ldots, e_t$ of RG with $\bar{e_i} = f_i$. We have

$$RGe_i \sim \sum_{j=1}^{s} \lambda_{ij} U_j \tag{$\spadesuit$}$$

and taking the tensor product with K gives:

$$KGe_i = \sum_{j=1}^{s} \lambda_{ij} V_j$$

The equal sign is now justified since KG is completely reducible; therefore, KGe_i is in fact even a direct sum of the simple modules V_j. Analogously to the case of positive characteristic, λ_{ij} is viewed as the number of factors of KGe_i isomorphic to the simple module V_j, that is, $\lambda_{ij} = i(KGe_i, V_j) = \dim e_i V_j$ by Lemma 1.2.19(iii). Since $e_i V_j = K \otimes e_i U_j$ and $e_i U_j \subset U_j$ is a free RG-module by Proposition 2.1.9(vi), we have, again using Lemma 1.2.19(iii),

$$\begin{aligned}\lambda_{ij} &= \dim_K e_i V_j = \operatorname{rank}_R e_i U_j = \dim_k \bar{e}_i \overline{U}_j \\ &= \dim_k f_i \overline{U}_j = i(kGf_i, \overline{U}_j) = i(P_i, \overline{U}_j) \\ &= d_{ji}\end{aligned}$$

Reducing (♠) modulo π and inserting $\lambda_{ij} = d_{ji}$ gives

$$kGf_i = P_i \sim \sum_{j=1}^{s} d_{ji} \overline{U}_j \tag{♣}$$

In the light of Lemma 2.2.3 we can rephrase the meaning of the Cartan number c_{mn} and the decomposition number d_{kl} as

$$P_m \sim \sum_{n=1}^{t} c_{mn} S_n \tag{$\heartsuit$}$$

$$\overline{U}_k \sim \sum_{l=1}^{t} d_{kl} S_l \tag{$\diamondsuit$}$$

These statements follow from Corollary 1.2.3, which states that every simple kG-module is isomorphic to S_i for one i. Inserting ($\diamondsuit$) into (♣) now gives

$$P_i \sim \sum_{j=1}^{s} \sum_{l=1}^{t} d_{ji} d_{jl} S_l$$

and employing ($\heartsuit$) finally leads to

$$c_{il} = \sum_{j=1}^{s} d_{ji} d_{jl}$$

which is the component form of the matrix equation $C = D^T D$. $\square$

In the course of the proof we also showed that $\lambda_{ij} = d_{ji}$, which we record here.

Corollary 2.2.5. *With the above denotations and assumptions, the multiplicity of V_j in the KG-module KGe_i is equal to the number of factors of $\overline{U}_j$ isomorphic to S_i, that is, $\lambda_{ij} = d_{ji}$.*

Finally, we also record the relations between P_i, $\overline{U}_i$ and S_i involving the Cartan numbers c_{ij} and the decomposition numbers d_{ij}:

Corollary 2.2.6. *With the above denotations and assumptions, the following relations hold:*

$$P_j \sim \sum_{i=1}^{s} d_{ij}\overline{U}_i$$
$$P_i \sim \sum_{i=1}^{t} c_{ij}S_j$$
$$\overline{U}_i \sim \sum_{i=1}^{t} d_{ij}S_j$$

Let us clarify the meaning of Corollary 2.2.6. As stated before, the kG-module $\overline{U}_i$ is the reduction of an RG-module U_i such that $K \otimes U_i = V_i$, a simple KG-module. By Lemma 2.2.1, the module $\overline{U}_i$ is indecomposable. Now, the first relation says that a composition series of the PIM P_i consists of the composition series of (some of) the reduced indecomposable kG-modules $\overline{U}_j$, with the decomposition number d_{ij} counting the respective multiplicities. The composition series of the $\overline{U}_i$ in turn comprises the simple kG-modules S_j by the third relation in Corollary 2.2.6. This is exactly the meaning of Theorem 2.2.4. In Section 2.3 it will become clear that in the relation $P_j \sim \sum_{i=1}^{s} d_{ij}\overline{U}_i$ the decomposition number d_{ij} is non-zero if and only if V_j lies in the same block as P_i.

Remark. Although we have $KG = \bigoplus_{i=1}^{s} n_i V_i$, where n_i is the multiplicity of the simple module V_i in KG, it does *not* hold that $RG = \sum_{i=1}^{s} n_i U_i$. In fact, this sum is not even direct, as the preceding discussion shows. We therefore stress that the RG-modules U_i are not isomorphic to the PIMs of the algebra RG, since otherwise they would be projective and hence direct summands in RG.

The procedure explained in this section starts with the simple KG-modules V_i in characteristic 0 and ends with the simple kG-modules S_i in characteristic p. This is in contrast to Section 3.2.4 where we start with a decomposition of kG into a direct sum of kG-PIMs P_i and lift it to a decomposition of RG into a direct sum of RG-PIMs Q_i.

2.2.2. Brauer characters

Consider a k-representation $\rho : G \longrightarrow \mathrm{End}_k(V)$ where $\operatorname{char} k = p$ and $p | \dim_k V$. Then $\chi_\rho(1) = 0$ for the character χ_ρ of ρ. Hence, regardless of whether or not p divides the order of G, ordinary characters lose a great deal of information in case k has positive characteristic. A resort out of this misery is due to R. Brauer, who proposed a slightly different concept of characters for modular representations. These Brauer characters are only defined on certain elements of G:

Definition 2.2.7. Let G be a finite group of order $|G| = p^k q$ where $(p, q) = 1$. An element $g \in G$ is called

- p-regular, if its order is relatively prime to p, that is, $(\operatorname{ord} g, p) = 1$.
- p-singular, if its order is a power of p, that is, $\operatorname{ord} g = p^m$ for some integer $m \in \mathbb{N}$.

A conjugacy class $\mathcal{C}$ of G is called p-regular (resp. p-singular), if every element $g \in \mathcal{C}$ is p-regular (resp. p-singular). The set of all p-regular elements is denoted by $G_{p'}$.

Lemma 2.2.8. *Let $g \in G$ be an element of order $\operatorname{ord} g = p^l r$ where $(p, r) = 1$. Then there are unique elements $a, b \in G$ such that a is p-regular, b is p-singular and $g = ab = ba$. The elements a and b are the p-regular (resp. p-singular) factor of g.*

Proof. Since $(p, r) = 1$, there are integers c, d such that $1 = cp^l + dr$. Set $a = g^{cp^l}$ and $b = g^{dr}$, then $g = ab = ba$. Moreover, $a^r = g^{cp^l r} = (g^{p^l r})^c = 1$, so $\operatorname{ord} a$ divides r; therefore, $(\operatorname{ord} a, p) = 1$. Also, $b^{p^l} = (g^{p^l r})^d = 1$, which implies that $\operatorname{ord} b$ is a power of p.

To show uniqueness, suppose that $g = a_1 b_1 = b_1 a_1$ with a_1 being p-regular and b_1 being p-singular. Let $p^x = \operatorname{ord} b$ and $p^y = \operatorname{ord} b_1^{-1}$, and observe that a, b, a_1 and b_1 commute pairwise, given that they are powers of g. Then $(bb_1^{-1})^{p^{x+y}} = 1 = (a^{-1}a_1)^{p^{x+y}}$ since $ab = g = a_1 b_1$. But the orders of a and a_1 are relatively prime to p and so is the order of $a^{-1}a_1$. Thus, $p^{x+y} = 1$, and consequently, $b = b_1$ and $a = a_1$. □

Proposition 2.2.9. *Let k be a splitting field of G with $\operatorname{char} k = p$ and $\rho : G \longrightarrow \operatorname{End}_k(V)$ be a representation of G. If $g = xy$ is the decomposition of $g \in G$ into the p-regular factor x and the p-singular factor y, then $\rho(g)$ and $\rho(x)$ have the same eigenvalues.*

Proof. Since k is a splitting field for G, we can find bases of V such that $\rho(x)$ and $\rho(y)$ have triangular form with the main diagonal consisting of their eigenvalues. By Lemma 2.2.8 $\rho(x)$ and $\rho(y)$ commute; hence, we can find a basis $\mathfrak{b}$ of V to triangulate both $\rho(x)$ and $\rho(y)$ at the same time. Moreover, $[\rho(g)]_{\mathfrak{b}} = [\rho(x)]_{\mathfrak{b}}[\rho(y)]_{\mathfrak{b}}$, so $[\rho(g)]_{\mathfrak{b}}$ also has triangular form, and its eigenvalues are the products of the respective eigenvalues of $\rho(x)$ and $\rho(y)$. Since y is p-regular, there is an $m \in \mathbb{N}$ such that $\rho(y)^{p^m} = \mathrm{id}$, and consequently, $\zeta^{p^m} = 1_k$ for each eigenvalue ζ of $\rho(y)$. Furthermore, since $\operatorname{char} k = p$ we have $0 = \zeta^{p^m} - 1 = (\zeta - 1)^{p^m}$; therefore, $\zeta = 1$ for every eigenvalue ζ of $\rho(y)$, and the eigenvalues of $\rho(g)$ and $\rho(x)$ are identical. □

We now come to the central definition in this section. Let G be a finite group of order $n = p^l q$ and (K, R, k) be a p-modular system for G with $\operatorname{char} k = p$. Further, let $\rho : G \longrightarrow \mathrm{End}_k(V)$ be a representation of G on the k-vector space V. If x is the p-regular factor of an element $g \in G$, Proposition 2.2.9 implies that the eigenvalues of $\rho(g)$ and $\rho(x)$ are identical. Moreover, $x^q = 1$ by the proof of Lemma 2.2.8; hence, the eigenvalues of $\rho(g)$ are q-th roots of unity in k. Let $\mathcal{E}(\rho, g)$ be the set of eigenvalues of $\rho(g)$ and fix an isomorphism α from the cyclic group of q-th roots of unity in k to the group of q-th roots of unity in K. This isomorphism exists since q is prime to p and reduction modulo π is an inverse mapping to α.

Definition 2.2.10 (Brauer character)**.** Under the above assumptions, the Brauer character φ_V of the k-representation ρ of G on V is defined as

$$\begin{aligned} \varphi_V : G_{p'} &\longrightarrow R \\ g &\longmapsto \sum_{\zeta \in \mathcal{E}(\rho, g)} \alpha(\zeta) \end{aligned}$$

If V is a simple kG-module, then φ_V is called an irreducible Brauer character.

This construction is motivated by the following

Proposition 2.2.11. *Two modular representations have the same Brauer character if and only if they have isomorphic irreducible constituents.*

Proof. Let $\sigma : G \longrightarrow \mathrm{End}_k(V)$ and $\tau : G \longrightarrow \mathrm{End}_k(W)$ be two representations of G on the k-vector spaces V and W. If σ and τ have isomorphic irreducible constituents, then clearly their eigenvalues and hence their Brauer characters are identical.

Conversely, suppose that $\varphi_V = \varphi_W$. For $g \in G$ let $z^{s_1}, \dots, z^{s_a}$ be the eigenvalues of $\sigma(g)$ and $z^{t_1}, \dots, z^{t_b}$ be the eigenvalues of $\tau(g)$. Setting $\zeta := \alpha(z)$ and taking the i-th power of every characteristic root of $\sigma(g)$ and $\tau(g)$ we get the complex identity

$$\zeta^{is_1} + \cdots + \zeta^{is_a} = \zeta^{it_1} + \cdots + \zeta^{it_b} \tag{*}$$

which follows from $\varphi_V(g^i) = \varphi_W(g^i)$ and the definition of Brauer characters. Let H be the cyclic group $\langle g \rangle$ and consider its complex representations

$$\sigma'(g^i) = \begin{pmatrix} \zeta^{is_1} & & \\ & \ddots & \\ & & \zeta^{is_a} \end{pmatrix} \qquad \tau'(g^i) = \begin{pmatrix} \zeta^{it_1} & & \\ & \ddots & \\ & & \zeta^{it_b} \end{pmatrix}$$

Then (*) implies that the ordinary characters of σ' and τ' coincide; thus, their irreducible constituents are isomorphic, giving $\{s_1, \ldots, s_a\} = \{t_1, \ldots, t_a\}$ for $i = 1$, and the claim is proved. $\square$

We immediately get further properties of Brauer characters:

Proposition 2.2.12. *Let $\rho : G \longrightarrow \mathrm{GL}_k(V)$ be a representation of G on the k-vector space V and φ_V its Brauer character. Then the following holds:*

(i) $\varphi_V(1) = \dim_k V$

(ii) *φ_V is a class function on the set $G_{p'}$ of p-regular conjugacy classes.*

(iii) *If W is a kG-submodule of V, then $\varphi_V = \varphi_W + \varphi_{V/W}$.*

(iv) *Let M be a KG-module with the ordinary character χ_M and N be the corresponding RG-module such that $K \otimes N = M$ according to Theorem 2.1.13. Then the Brauer character of $\overline{N}$ is*
$$\varphi_{\overline{N}} = \chi_M|_{G_{p'}}$$

(v) *If $H \leq G$ is a subgroup of G with $p \nmid |H|$ and φ is a Brauer character of G, then $\varphi|_H$ is an ordinary character of H.*

Proof. Properties (i)-(iv) follow directly from Definition 2.2.10. (v) is trivial, since kH is semisimple by Maschke's Theorem 1.1.13. $\square$

We can now prove:

Lemma 2.2.13. *Let M and N be two RG-modules such that $K \otimes M \cong K \otimes N$. Then $\overline{M}$ and $\overline{N}$ have isomorphic composition factors.*

Proof. Let μ and ν be the representations associated with the RG-modules M and N. Since $K \otimes M \cong_K K \otimes N$, the characteristic polynomials of $\mu(g)$ and $\nu(g)$ coincide over K and consequently over R. Hence, $\bar{\mu}(g)$ and $\bar{\nu}(g)$ have the same characteristic roots in k. But then $\varphi_{\overline{M}} = \varphi_{\overline{N}}$, and by Proposition 2.2.11 their composition factors are isomorphic. $\square$

Corollary 2.2.14. *Let V be an irreducible KG-module and U be an RG-module of V such that $V = K \otimes U$. Then the isomorphy classes of composition factors of $\overline{U}$ are determined by V and hence independent of the choice of U.*

As already noted in Section 2.2.1, Corollary 2.2.14 shows that the decomposition number d_{ij} is independent of the choice of the RG-modules U_i.

In modular representation theory, the irreducible Brauer characters are the equivalent of the irreducible ordinary characters, except that the Brauer characters are only defined on the set $G_{p'}$ of p-regular conjugacy classes. Recall that the irreducible ordinary characters defined over the field K constitute a basis of the K-vector space of class functions on G. An analogous result also holds for the irreducible Brauer characters. In order to prove this result, we need the density theorem by Jacobson:

Theorem 2.2.15 (Density theorem). *Let M be a semisimple R-module and set $A = \operatorname{End}_R(M)$. If M is finitely generated as an A-module, then the canonical homomorphism*

$$\begin{aligned} \theta : R &\longrightarrow \operatorname{End}_A(M) \\ r &\longmapsto (\ell_r : m \longmapsto rm) \end{aligned}$$

is surjective.

Proof. See [JS06, p. 217, Cor. 3.2]. □

Theorem 2.2.16. *Let $S_1, \dots, S_t$ be the isomorphy classes of simple kG-modules. Then the irreducible Brauer characters $\varphi_{S_1}, \dots, \varphi_{S_t}$ form a K-basis of the space of class functions on $G_{p'}$.*

Proof. We have to show that the $\varphi_{S_1}, \dots, \varphi_{S_t}$ are linearly independent over K and generate the K-space of class functions on $G_{p'}$. Let us start with the linear independence.

To this end, let us abbreviate $\mathfrak{S}_k := \{S_1, \dots, S_t\}$ and suppose that $\sum_{S \in \mathfrak{S}_k} \lambda_S \varphi_S = 0$ where $\lambda_S \in K$. Multiplying by a proper element of K we can achieve $\lambda_S \in R$ for all $S \in \mathfrak{S}_k$, and by canceling common factors in πR at least one λ_S does not belong to πR. Hence, reduction modulo π gives

$$\sum_{S \in \mathfrak{S}_k} \bar{\lambda}_S \bar{\varphi}_S(x) = 0$$

for all $x \in G_{p'}$ and at least one $\bar{\lambda}_S$ is not zero. This is equivalent to

$$\sum_{S \in \mathfrak{S}_k} \bar{\lambda}_S \operatorname{tr}(\rho_S(x)) = 0$$

for all $x \in G_{p'}$, where ρ_S is the representation of G on S to which φ_S is associated. By Proposition 2.2.9 this equation holds for all $g \in G$ and by linearity of the trace also for all

$v \in kG$. Since k is a splitting field for G, Proposition 1.2.22 implies $A = \operatorname{End}_{kG}(M) \cong k$ for all simple kG-modules M. Hence, from the density theorem 2.2.15 we obtain that the homomorphism $\theta : kG \longrightarrow \bigoplus_{S\in\mathfrak{S}_k} \operatorname{End}_k(S)$ is surjective. Thus, for every $S \in \mathfrak{S}_k$ with $\bar{\lambda}_S \neq 0$ we can choose an element $a \in kG$ such that $\theta(a) = (\psi_T)_{T\in\mathfrak{S}_k}$ with $\operatorname{tr}\psi_S = 1$ and $\psi_T = 0$ for $T \neq S$. Hence $\lambda_S \cdot 1 = 0$, and the $\varphi_{S_1}, \ldots, \varphi_{S_t}$ are linearly independent.

To show that $\varphi_{S_1}, \ldots, \varphi_{S_t}$ generate the space of class functions on $G_{p'}$, let $f : G \longrightarrow K$ be such a function. Extend f to a class function on G and write $f = \sum_{i=1}^{s} \lambda_i \chi_i$ where $\lambda_i \in K$ and $\chi_1, \ldots, \chi_s$ are the irreducible ordinary K-characters. Then $f = \sum_{i=1}^{s} \lambda_i \chi_i|_{G_{p'}}$ and by Proposition 2.2.12(iii) and (iv) the restrictions of χ_i onto $G_{p'}$ are linear combinations of the $\varphi_{S_1}, \ldots, \varphi_{S_t}$, which proves the claim. $\square$

Corollary 2.2.17. *The number of irreducible Brauer characters is equal to the number of p-regular conjugacy classes.*

2.2.3. Modular orthogonality relations

In ordinary representation theory the orthogonality relations for irreducible (ordinary) characters provide a useful way of determining irreducible representations. In this section we will derive analogous statements for the irreducible Brauer characters. For convenience we restate the ordinary orthogonality relations:

Proposition 2.2.18. *For a group G with $n = |G|$ let $\chi_1, \ldots, \chi_s$ be the ordinary irreducible characters of G, $\{g_1, \ldots, g_s\}$ be a set of representatives of the conjugacy classes of G and $h_i = |\mathcal{C}_i|$ be the order of the i-th conjugacy class $\mathcal{C}_i$. Then the following relations holds:*

$$\sum_{k=1}^{s} \chi_k(g_i)\chi_k(g_j^{-1}) = \frac{n}{h_i}\delta_{ij}$$

$$\frac{1}{n}\sum_{k=1}^{s} |\mathcal{C}_k|\chi_i(g_k)\chi_j(g_k^{-1}) = \delta_{ij}$$

Let us fix some notation: $\chi_1, \ldots, \chi_s$ are the irreducible ordinary characters, $\varphi_1, \ldots, \varphi_t$ are the irreducible Brauer characters and $\psi_1, \ldots, \psi_t$ are the characters of the PIMs $P_1, \ldots, P_t$ of kG. We want to formulate the relations involving the Cartan numbers and decomposition numbers in Corollary 2.2.6 as matrix equations in terms of these characters. Replacing the modules in the formulation of Corollary 2.2.6 by characters, the relations read:

$$\psi_j = \sum\nolimits_{i=1}^{s} d_{ij}\chi_i \tag{2.1a}$$

$$\psi_i = \sum\nolimits_{i=1}^{t} c_{ij}\varphi_j \tag{2.1b}$$

$$\chi_i = \sum\nolimits_{i=1}^{t} d_{ij}\varphi_j \tag{2.1c}$$

Strictly speaking it is not correct to mix an ordinary character χ_i and a Brauer character φ_j without specifying the set of group elements on which the relation is defined, so we have to get rid of this inconsistency. Denote by $\mathcal{C}_1, \ldots, \mathcal{C}_s$ the conjugacy classes of G and arrange them such that the first $t \leq s$ of them are p-regular. Further, choose a representative $g_i \in \mathcal{C}_i$ and form the matrices

$$X := (\chi_i(g_j))_{1\leq i\leq s, 1\leq j\leq t}$$
$$\Phi := (\varphi_i(g_j))_{1\leq i,j\leq t}$$
$$\Psi := (\psi_i(g_j))_{1\leq i,j\leq t}$$

Then the relations (2.1) can be expressed in matrix notation as

$$X = D\Phi \tag{2.2a}$$

$$\Psi = C\Phi \tag{2.2b}$$

$$\Psi = D^T X \tag{2.2c}$$

To prove the modular orthogonality relations we first have to introduce a suitable inner product on the space of class functions on $G_{p'}$, paralleling the inner product of the class functions in the ordinary case.

Definition 2.2.19. For class functions ξ, η on $G_{p'}$ define the inner product $\langle ., . \rangle_{G_{p'}}$ by

$$\langle \xi, \eta \rangle_{G_{p'}} = \frac{1}{n} \sum_{g \in G_{p'}} \xi(g)\eta(g^{-1})$$

We finally arrive at the following

Proposition 2.2.20 (Modular orthogonal relations)**.**

(i) *The Cartan matrix C and the Brauer character table Φ are invertible.*

(ii) *With $C^{-1} = (c'_{ij})$ the following relations hold:*

$$\langle \varphi_i, \varphi_j \rangle_{G_{p'}} = c'_{ij}$$
$$\langle \psi_i, \psi_j \rangle_{G_{p'}} = c_{ij}$$

$$\langle \varphi_i, \psi_j \rangle_{G_{p'}} = \delta_{ij}$$

Proof. (i) Define the matrix $M := (\frac{n}{h_i}\delta_{ij})_{1 \le i,j \le t}$ such that the ordinary orthogonal relations from Proposition 2.2.18 can be written as $X^T X = M$. Using the matrix relations (2.2) and $C = D^T D$ we have

$$\Phi^T C \Phi = (D\Phi)^T D\Phi = X^T X = M \tag{*}$$

Since M is invertible, Φ and C are also invertible.

(ii) Using (*) and (2.2) and observing that $M^{-1} = (\frac{h_i}{n}\delta_{ij})$ gives (note that I is the identity matrix)

$$\begin{aligned}
\Phi M^{-1} \Phi^T &= \Phi \Phi^{-1} C^{-1} (\Phi^T)^{-1} \Phi^T = C^{-1} \\
\Psi M^{-1} \Psi^T &= C \Psi M^{-1} \Psi^T C^T = C \\
\Phi M^{-1} \Psi^T &= \Phi M^{-1} \Phi^T C^T = I
\end{aligned}$$

which are the matrix forms of the modular orthogonality relations in the claim. □

2.3. Introduction to block theory

The decomposition of the group algebra kG into a direct sum of PIMs in Section 1.2.1 was derived using the module structure of kG. In this section we investigate the ring structure of the algebra kG by looking at two-sided ideals, the blocks of kG. We will see that every Artinian ring admits a decomposition into such blocks. When viewing a (non-commutative) ring as a module over itself, the notion of a two-sided ideal is stronger than the notion of a (left or right) submodule. Thus, a decomposition into two-sided ideals is much coarser than a decomposition into PIMs. At first glance this seems like a loss of information. However, all necessary data relevant to modular representation theory such as PIMs, simple modules and irreducible characters can be assigned to a certain block, and the block decomposition facilitates both the determination and the structuring of these objects. Throughout this section let (K, R, k) be a p-modular system for G.

2.3.1. Block decomposition

Definition 2.3.1. A two-sided ideal B of kG is called a block if $kG = B \oplus B'$ for some other ideal B' of kG and B cannot be written as a direct sum of two non-trivial two-sided ideals.

Proposition 2.3.2. *The group algebra kG admits a unique decomposition*

$$kG = B_1 \oplus \cdots \oplus B_r$$

into blocks B_i. This block decomposition corresponds to a decomposition

$$1_{kG} = \varepsilon_1 + \cdots + \varepsilon_r$$

of the unity element 1_{kG} into centrally primitive idempotents $\varepsilon_1, \ldots, \varepsilon_r$.

Proof. The existence of the block decomposition $kG = B_1 \oplus \cdots \oplus B_r$ into blocks B_i follows from kG being Artinian by Proposition 1.1.4. To establish uniqueness of the block decomposition, suppose that B is a block of kG. Then $BB_i \subset B \cap B_i$ for $1 \leq i \leq r$ and

$$B = BB_1 + \cdots + BB_r \subset (B \cap B_1) \oplus \cdots \oplus (B \cap B_r) \subset B$$

which implies $B = (B \cap B_1) \oplus \cdots \oplus (B \cap B_r)$. But B is a block ideal and can therefore not be written as a direct sum of nontrivial ideals. Thus, there is a j such that $B \subset B_j$ and $B \cap B_i = \emptyset$ for $i \neq j$. Further, there is an ideal B' such that $kG = B \oplus B'$; hence,

$$B_j = BB_j + B'B_j \subset (B \cap B_j) \oplus (B' \cap B_j) \subset B_j$$

resulting in $B_j = (B \cap B_j) \oplus (B' \cap B_j)$. Again, B_j cannot be written as a direct sum of nontrivial ideals. Since $B \subset B_j$, this gives $B_j = B \cap B_j = B$; hence, every block B is one of the B_j.

By Proposition 1.1.2 the block decomposition $kG = B_1 \oplus \cdots \oplus B_r$ corresponds to a decomposition $1_{kG} = \varepsilon_1 + \cdots + \varepsilon_r$ of the unity element 1_{kG} into idempotents. Let $x \in kG$ and observe that

$$x = x\varepsilon_1 + \cdots + x\varepsilon_r = \varepsilon_1 x + \cdots + \varepsilon_r x$$

Since B_i is a two-sided ideal, it holds for all i that $x\varepsilon_i \in B_i$ as well as $\varepsilon_i x \in B_i$. Hence $x\varepsilon_i = \varepsilon_i x$, and $\varepsilon_i \in Z(kG)$ for all i. $\square$

Definition 2.3.3 (Block decomposition and block idempotents)**.** In Proposition 2.3.2, the unique decomposition $kG = B_1 \oplus \cdots \oplus B_r$ is called the block decomposition of kG. $\varepsilon_1, \ldots, \varepsilon_r$ are called the block idempotents of kG.

Remark. Applying Theorem 2.1.11 to the algebras $Z(RG)$ and $Z(kG) = \overline{Z(RG)}$, we can lift the block idempotents $\varepsilon_1, \ldots, \varepsilon_r$ of kG to RG. More precisely, there is a set of orthogonal idempotents $f_1, \dots, f_r$ such that f_i is centrally primitive and $\bar{f_i} = e_i$. In analogy to Definition 2.3.1, the ideals RGf_i are called the blocks of RG, and

$$RG = RGf_1 \oplus \cdots \oplus RGf_r$$

is called the block decomposition of RG. Note however, that RGf_i is in general not indecomposable in KG and further decomposes into simple components. This is subject of the next section.

2.3.2. Modules and characters lying in a block

The decomposition of kG into blocks allows a classification of the indecomposable modules, simple modules and irreducible (Brauer and ordinary) characters of a group G. We first consider an indecomposable kG-module M. Let $\varepsilon_1, \dots, \varepsilon_r$ be the block idempotents of kG, then

$$M = \varepsilon_1 M \oplus \cdots \oplus \varepsilon_r M$$

as kG-modules, since the ε_i are central. Because M is indecomposable, there exists a j such that $\varepsilon_j M = M$ and $\varepsilon_i M = 0$ for $i \neq j$; thus, M is associated to a single block $B_j = kG\varepsilon_j$. This classifies the PIMs $P_1, \dots, P_t$ of kG and by Corollary 1.2.3 also all simple kG-modules into blocks, hence the following

Definition 2.3.4 (kG-modules lying in blocks)**.** Let $\varepsilon_1, \dots, \varepsilon_r$ be the block idempotents of kG. An indecomposable kG-module M with $\varepsilon_j M = M$ for a unique j, and $\varepsilon_i M = 0$ for $i \neq j$ is said to lie in the block B_j. Further, a simple kG-module S is said to lie in the block B_j if the PIM P with $S \cong P/\operatorname{rad} P$ lies in the block B_j. A Brauer character φ lies in the block B_j if the module affording φ lies in the block B_j.

This shows that a block decomposition provides a classification of kG-modules into blocks via the block idempotents. In order to obtain a similar classification of KG-modules into blocks, we need to be more careful. Given a simple KG-module M we can choose an RG-submodule N of M such that $M = K \otimes N$ and apply Definition 2.3.4 to the kG-module $\overline{N}$. However, using this procedure as a definition for KG-modules lying in blocks only makes sense if attributing M to a block is independent of the particular choice of N:

Lemma 2.3.5. *Let V be a simple KG-module. According to Theorem 2.1.13, choose an RG-submodule U of V such that $V = K \otimes U$ and denote by $\overline{U}$ the corresponding kG-module. Then all the composition factors of $\overline{U}$ lie in the same block B of kG, which does not depend on the choice of the submodule U.*

Proof. According to the remark following Definition 2.3.3 let $\varepsilon_1, \dots, \varepsilon_r$ be the block idempotents of kG and $f_1, \dots, f_r$ be the block idempotents of RG with $\bar{f}_i = \varepsilon_i$ for all i. Write $U = f_1 U \oplus \cdots \oplus f_r U$ and note that since V is irreducible, U is indecomposable by Proposition 2.1.9(vi). Hence, there is a j such that $f_j U = U$ and $f_i U = 0$ for $i \neq j$. Consequently, $\overline{U} = \bar{f}_j \overline{U} = \varepsilon_j \overline{U}$ and $0 = \bar{f}_i \overline{U} = \varepsilon_i \overline{U}$ for $i \neq j$. By Corollary 2.2.14 the composition factors of $\overline{U}$ are completely determined by V, and by the paragraph before Definition 2.3.4, they are isomorphic to the simple kG-modules lying in the block B_j. $\square$

Definition 2.3.6 (KG-modules lying in blocks)**.** Let V be a simple KG-module and U an RG-module of V such that $V = K \otimes U$. Then V is said to lie in the block B in which all the composition factors of $\overline{U}$ lie. An irreducible ordinary character χ lies in the block B if the simple KG-module V affording χ lies in the block B. We set $\mathrm{Irr}(B) := \{\chi \in \mathrm{Irr}(G) \mid \chi \text{ lies in } B\}$.

When classifying irreducible ordinary characters in blocks it is often convenient to consider a special class of characters:

Definition 2.3.7 (Central character)**.** A k-algebra homomorphism $\omega : Z(kG) \longrightarrow k$ is called a central character of k. The same definition also applies to the field K of characteristic zero.

Note that the class sums $\mathcal{C}_i^+ := \sum_{g \in \mathcal{C}_i} g$ form a basis of both $Z(kG)$ and $Z(KG)$. Therefore, a central character is completely determined by its values on $\mathcal{C}_i^+$. In order to demonstrate the usefulness of central characters, let us first analyze the center $Z(kG)$ of kG.

Lemma 2.3.8. *Let $\varepsilon_1, \dots, \varepsilon_r$ be the block idempotents of kG. Then we have a decomposition*

$$Z(kG) = Z(kG)\varepsilon_1 \oplus \cdots \oplus Z(kG)\varepsilon_r$$

of the center $Z(kG)$ of kG into indecomposable $Z(kG)$-modules $Z(kG)\varepsilon_i$. Further, $Z(kG)\varepsilon_i / \operatorname{rad}(Z(kG)\varepsilon_i) \cong k$.

Proof. Set $Z := Z(kG)$. Since the ε_i are central by Proposition 2.3.2, the block decomposition $kG = kG\varepsilon_1 \oplus \cdots \oplus kG\varepsilon_r$ clearly gives a decomposition $Z = Z\varepsilon_1 \oplus \cdots \oplus Z\varepsilon_r$. Moreover, each $Z\varepsilon_i$ is indecomposable as the block idempotent $\varepsilon_i \in Z$ is primitive. The Z-modules $Z\varepsilon_i$ are the PIMs of the k-algebra Z, and Theorem 1.2.2 implies that $Z\varepsilon_i / \operatorname{rad}(Z\varepsilon_i)$ is a simple commutative k-algebra. By the structure theorem for Artinian rings (cf. [AM69, p. 90, Thm. 8.7]) every commutative semisimple Artinian algebra is isomorphic to a direct sum of fields; hence, $Z\varepsilon_i / \operatorname{rad}(Z\varepsilon_i) \cong k$. $\square$

The following result provides a 1:1-correspondence between central characters and blocks of kG.

Proposition 2.3.9. *If $\varepsilon_1, \dots, \varepsilon_r$ are the block idempotents of kG, there are exactly r distinct central characters $\omega_1, \dots, \omega_r$ of kG. They are characterized by*

$$\omega_i(\varepsilon_j) = \delta_{ij}$$

Proof. Once more, abbreviate $Z := Z(kG)$. By Lemma 2.3.8 the k-algebra homomorphism $\omega_i : Z \longrightarrow Z\varepsilon_i \longrightarrow Z\varepsilon_i / \operatorname{rad}(Z\varepsilon_i) \cong k$ defines a central character of kG and $\omega_i(\varepsilon_j) = \delta_{ij}$.

To show that all central characters of kG are given by $\omega_1, \dots, \omega_r$, suppose that $\omega : Z \longrightarrow k$ is an arbitrary central character of kG. Since $\operatorname{rad} Z$ is nilpotent by Proposition 1.1.22(iv), for every $r \in \operatorname{rad} Z$ it holds that $\omega(r)^m = \omega(r^m) = 0$ for some $m \in \mathbb{N}$, giving $\operatorname{rad} Z \subset \ker \omega$. Lemma 2.3.8 implies $Z\varepsilon_i \cong k + \operatorname{rad} Z\varepsilon_i$, which results in the decomposition

$$Z \cong k\varepsilon_1 \oplus \cdots \oplus k\varepsilon_r + \operatorname{rad} Z \tag{*}$$

Now choose i such that $\omega(\varepsilon_i) \neq 0$ and observe that

$$\omega(\varepsilon_i) = \omega(\varepsilon_i \varepsilon_i) = \omega(\varepsilon_i)\omega(\varepsilon_i)$$

giving $\omega(\varepsilon_i) = 1$. Further, for $j \neq i$ we have

$$0 = \omega(\varepsilon_i \varepsilon_j) = \omega(\varepsilon_i)\omega(\varepsilon_j)$$

and hence $\omega(\varepsilon_j) = 0$. In summary, $\omega(\varepsilon_j) = \delta_{ij}$ for i with $\omega(\varepsilon_i) \neq 0$. Thus, $\omega = \omega_i$ on $\varepsilon_1, \dots, \varepsilon_r$ and both have $\operatorname{rad} Z$ in its kernel, so that by (*) they are identical. □

Lemma 2.3.10. *Let V be a simple KG-module affording the irreducible ordinary character χ and ρ be the corresponding representation. Further, define the K-linear map*

$$\begin{aligned} \omega_\chi : Z(KG) &\longrightarrow K \\ \mathcal{C}_i^+ &\longmapsto \frac{|\mathcal{C}_i|\chi(g_i)}{\chi(1)} \end{aligned}$$

for $g_i \in \mathcal{C}_i$. Then $zv = \omega_\chi(z)v$ for all $z \in Z(KG)$ and $v \in V$, that is, the center $Z(KG)$ acts on V via ω_χ. In particular, ω_χ is a central character.

Proof. For $z \in Z(KG)$ the endomorphism $\rho(z)$ lies in the center of $\mathrm{End}(V)$. Therefore, we have $\rho(\mathcal{C}_i^+) = \lambda_i \,\mathrm{id}_V$ with $\lambda_i \in K$, and taking traces gives $|\mathcal{C}_i|\chi(g_i) = \lambda_i\chi(1)$ for a representative $g_i \in \mathcal{C}_i$. Hence, $\lambda_i = \frac{|\mathcal{C}_i|\chi(g_i)}{\chi(1)}$, and $Z(KG)$ acts on V via ω_χ. It follows easily from $zv = \omega_\chi(z)v$ for all $z \in Z(KG)$ and $v \in V$ that ω_χ is a central character. $\square$

Definition 2.3.11. Let χ be an irreducible ordinary character of G. Then

$$\begin{aligned} \omega_\chi : Z(KG) &\longrightarrow K \\ \mathcal{C}_i^+ &\longrightarrow \frac{|\mathcal{C}_i|\chi(g_i)}{\chi(1)} \quad \text{for } g_i \in \mathcal{C}_i \end{aligned}$$

is the canonical central character associated to χ.

To summarize, we have associated a central character of KG to every irreducible ordinary character, and every central character of kG corresponds to a block B. Hence, reducing central characters provides a classification of the irreducible ordinary characters into blocks via the following

Proposition 2.3.12.

(i) *Let S be a simple kG-module and B be a block of G with the corresponding central character ω_B. Then S lies in the block B if and only if $zs = \omega_B(z)s$ for all $z \in Z(kG)$ and $s \in S$.*

(ii) *Two irreducible ordinary characters χ and χ' lie in the same block if and only if for all i*

$$\frac{|g^G|\chi(g_i)}{\chi(1)} \equiv \frac{|g^G|\chi'(g_i)}{\chi'(1)} \mod \pi \quad \textit{for } g_i \in \mathcal{C}_i$$

Proof. (i) Let ρ be the representation associated to the simple kG-module S. For $z \in Z(kG)$ it holds that $\rho(z) \in \mathrm{End}_{kG}(S)$, and by Proposition 2.1.3 the endomorphism ring $\mathrm{End}_{kG}(S)$ is isomorphic to k. Thus, restricting ρ to the center $Z(kG)$ of kG gives a central character $\omega : Z(kG) \longrightarrow k$, and we have $zs = \omega(z)s$ for all $z \in Z(kG)$ and $s \in S$. To prove the claim it therefore suffices to show that $\omega = \omega_B$.

To this end, let ε be the block idempotent corresponding to the block B. Then $\varepsilon s = s$ for all $s \in S$, and also $\varepsilon s = \omega(\varepsilon)s$ for all $s \in S$ by the above paragraph. Hence, $\omega(\varepsilon) = 1$, and by Proposition 2.3.9 the central character ω coincides with the central character ω_B associated to the block B.

(ii) Let V be the simple KG-module affording χ and choose an RG-submodule U of V such that $V = K \otimes U$. Then Lemma 2.3.10 implies

$$zu = \omega_\chi(z)u \quad \text{for all } z \in Z(KG), u \in U \tag{*}$$

Since we know from ordinary representation theory that $\omega_\chi(z) \in R$, we can reduce (*) modulo π. Using (i), this gives

$$zu = \omega_B(z)u \quad \text{for all } z \in Z(kG), u \in \overline{U}$$

where ω_B is the central character of kG corresponding to the block B in which the composition factors of $\overline{U}$ lies. The relation

$$\frac{|g^G|\chi(g_i)}{\chi(1)} \equiv \frac{|g^G|\chi'(g_i)}{\chi'(1)} \mod \pi \quad \text{for } g_i \in \mathcal{C}_i$$

means that $\omega_\chi \equiv \omega_{\chi'} \mod \pi$; therefore, by (i) and Definition 2.3.6 the irreducible ordinary characters χ and χ' lie in the same block. □

Note that given the ordinary character table of a group G, Proposition 2.3.12(ii) provides a simple way of determining the number of blocks in characteristic p.

2.3.3. Block idempotents

The classification of irreducible ordinary characters into blocks gives rise to a famous result by Osima:

Proposition 2.3.13 (Osima). *Let B be a block of kG and denote by $\chi_1, \ldots, \chi_r$ the irreducible ordinary characters lying in B. Then*

$$\sum_{i=1}^{r} \chi_i(x)\chi_i(y) = 0$$

whenever $x \in G_{p'}$ and $y \notin G_{p'}$.

Proof. Let $\chi_1, \ldots, \chi_s$ be the full set of irreducible ordinary characters such that the first r characters lie in the block B and let $\varphi_1, \ldots, \varphi_t$ be the irreducible Brauer characters such that the first m characters lie in B. Then by (2.2) we have $\chi_i = \sum_{j=1}^{t} d_{ij}\varphi_j$.

Moreover, the decomposition matrix D has the form

$$D = \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix}$$

where D_1 is an $r \times m$-matrix and D_2 is an $(s-r) \times (t-m)$-matrix. Let $\mathcal{C}_1, \ldots, \mathcal{C}_t$ be the p-regular conjugacy classes with representatives $g_i \in \mathcal{C}_i$, then by Proposition 2.2.18 we have

$$(\chi_1(y), \ldots, \chi_s(y))X = 0$$

for $y \notin G_{p'}$. Using $X = D\Phi$ from (2.2) and the fact that Φ is invertible gives

$$(\chi_1(y), \ldots, \chi_r(y))D_1 = 0$$

Finally, let $x \in G_{p'}$ and multiply this identity from the right by the column vector $(\varphi_1(x), \ldots, \varphi_m(x))$, giving

$$0 = \sum_{i=1}^{r} \chi_i(y) \sum_{j=1}^{m} d_{ij}\varphi_j(x) = \sum_{i=1}^{m} \chi_i(y)\chi_i(x)$$

which proves the claim. $\square$

In the proof of Proposition 2.3.13 we deployed a block form of the decomposition matrix which was achieved by ordering the irreducible ordinary and Brauer characters accordingly. This is a useful procedure, and we record it here in a separate

Proposition 2.3.14. *Let $B_1, \ldots, B_r$ be the blocks of kG, $\chi_1, \ldots, \chi_s$ be the ordinary irreducible characters and $\varphi_1, \ldots, \varphi_t$ be the irreducible Brauer characters. Renumber the irreducible characters such that the first i_1 ordinary characters lie in B_1, the next i_2 lie in B_2, etc. until the last i_r characters, which lie in B_r. Analogously, the first j_1 Brauer characters lie in B_1, the next j_2 lie in B_2 etc. until the last i_r characters, which lie in B_r. Then the decomposition matrix D and the Cartan matrix C have the form*

$$D = \begin{pmatrix} D_1 & & & 0 \\ & D_2 & & \\ & & \ddots & \\ 0 & & & D_r \end{pmatrix} \qquad C = \begin{pmatrix} C_1 & & & 0 \\ & C_2 & & \\ & & \ddots & \\ 0 & & & C_r \end{pmatrix}$$

where D_k is a $i_k \times j_k$-matrix and C_k is a $j_k \times j_k$-matrix.

The preceding discussion allows us to give explicit formulas of the block idempotents of kG:

Theorem 2.3.15 (Formula for block idempotents)**.** *Let $\chi_1, \dots, \chi_s$ be the irreducible ordinary characters of G. Then the block idempotent ε_B corresponding to B is given by*

$$\varepsilon_B \equiv \sum_{\chi \in \mathrm{Irr}(B)} \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g \mod \pi$$

Proof. By Theorem 2.1.11 we can lift the block idempotent ε_B to an idempotent $f_B \in Z(RG)$ such that $\bar{f}_B = \varepsilon_B$. By ordinary representation theory the irreducible ordinary characters $\chi_1, \dots, \chi_s$ are associated to block idempotents

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g$$

and $e_1, \dots, e_s$ constitute a basis of $Z(KG)$. Let us renumber the irreducible characters such that the first r lie in the block B. Since $Z(RG) \subset Z(KG)$, we can write $f_B = \sum_{i=1}^s \lambda_i e_i$. Observe that $\bar{\omega}_j(\bar{f}_B) = \overline{\omega_j(f_B)} = 1$ for the canonical central character ω_j associated to χ_j by Proposition 2.3.9. We claim that $\omega_j(e_i) = 1$ if $1 \leq j \leq r$ and 0 otherwise. To see this, write

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{l=1}^s \chi_i(g_l^{-1}) \mathcal{C}_l^+$$

where $g_1, \dots, g_l$ are representatives of the conjugacy classes $\mathcal{C}_1, \dots, \mathcal{C}_l$ of G. We then compute

$$\begin{aligned}
\omega_j(e_i) &= \frac{\chi_i(1)}{|G|} \sum_{l=1}^s \chi_i(g_l^{-1}) \omega_j(\mathcal{C}_l^+) \\
&= \frac{\chi_i(1)}{|G|} \sum_{l=1}^s \chi_i(g_l^{-1}) \frac{|\mathcal{C}_l|}{\chi_j(1)} \chi_j(g_l) = \delta_{ij}
\end{aligned}$$

The last equality sign follows from the orthogonality relations of irreducible ordinary characters in Proposition 2.2.18. Hence, we can write $f_B = e_1 + \dots + e_r$, which reduces modulo π to the proposed formula for the block idempotent ε_B. □

Corollary 2.3.16. *In Proposition 2.3.12(ii) it suffices to verify the relation for two irreducible characters χ and χ' to lie in the same block on $G_{p'}$.*

Proof. The proof of Theorem 2.3.15 implies that the block idempotent ε_B of the block B can be written as

$$\varepsilon_B = \sum_{i=1}^{s} \mu_i \mathcal{C}_i^+$$
$$\text{with } \mu_i = \frac{1}{|G|} \sum_{j=1}^{r} \chi_j(1)\chi_j(g_i^{-1})$$

where the irreducible ordinary characters χ_i are again renumbered so that the first r lie in the block B. By Proposition 2.3.13, $\mu_i = 0$ if $\mathcal{C}_i^+$ is a p-singular class. Now let ω_χ be the canonical central character associated to χ, then χ belongs to B if and only if $\bar{\omega}_\chi(\varepsilon_B) = 1$, that is,

$$\sum_{i=1}^{s} \mu_i \omega_\chi(\mathcal{C}_i^+) = \sum_{i=1}^{s} \mu_i \frac{|\mathcal{C}_i|\chi(g_i)}{\chi(1)} \equiv 1 \mod \pi$$

and analogously for χ'. Since the coefficient μ_i is only non-zero on p-regular classes, it suffices to verify the relation $\bar{\omega}_\chi(\varepsilon_B) = 1$ on $G_{p'}$. □

Finally, block theory can be used to obtain a useful result in the process of finding the irreducible Brauer characters of a group G:

Proposition 2.3.17. *Let χ be an irreducible ordinary character belonging to a block B and $p \nmid \frac{|G|}{\chi(1)}$. Then $\mathrm{Irr}(B) = \{\chi\}$, and $\chi|_{G_{p'}}$ is an irreducible Brauer character.*

Proof. The condition $p \nmid \frac{|G|}{\chi(1)}$ means that $\frac{\chi(1)}{|G|} \in R$. Hence, e_χ is a central idempotent in RG and thus the block idempotent of the block B. Consequently, after a suitable renumbering of the irreducible ordinary and Brauer characters, Proposition 2.3.14 implies that the decomposition matrix D_B corresponding to the block B is the 1×1-matrix $D_B = (1)$. Therefore, the restriction of χ to the p-regular conjugacy classes of G is an irreducible Brauer character. □

3. Principal indecomposable modules for the Alternating group A_5

In this chapter we use the methods developed in the preceding sections to analyze the representations of the group A_5 in characteristic p, where the prime p divides the group order $|G|$. Since $|A_5| = 60$, we have to consider the primes $2, 3$ and 5. More precisely, we are trying to understand the structure of the k-algebra kG as a module over itself, where k is a field with $\operatorname{char} k = p$. The kG-module kG is also called the regular representation of G in characteristic p.

In particular we determine (for each characteristic) a set of primitive orthogonal idempotents $\{e_i\}_i$, which corresponds to a decomposition of $kG = \bigoplus_i e_i kG$ into the direct sum of PIMs. The first step in this task is the calculation of the block idempotents and the irreducible p-Brauer characters, the degrees of which are the dimensions of the unique irreducible socles of the PIMs. Knowledge of the p-Brauer characters and the behavior of the ordinary characters under restriction to the p-regular conjugacy classes directly leads to the p-decomposition matrix D_p and the Cartan matrix $C_p = D_p^T D_p$. Those matrices together with the p-Brauer character table provide complete information about the PIMs' dimensions and multiplicities, which in turn facilitates the calculation of the primitive orthogonal idempotents in Section 3.3.1. In addition, we compute the radical series of each PIM in Section 3.3.2.

Let us fix some notations which are going to be used throughout this chapter. We set $G = A_5$ and will use both denotations interchangeably. The decomposition matrix D_p and the Cartan matrix C_p are indexed with the according prime p, which is the characteristic of k. We write $T \sim \tau$ for the correspondence between a kG-module T and the representation τ of G.

3.1. Preliminaries

3.1.1. Ordinary character table of A_5

At first we analyze the ordinary character table of A_5, given in Table 3.1.[1] The group A_5 splits up into five conjugacy classes as follows: $\mathcal{C}_1 = \{e\}$, $\mathcal{C}_2 = (12)(34)^G$, $\mathcal{C}_3 = (123)^G$, $\mathcal{C}_4 = (12345)^G$ and $\mathcal{C}_5 = (12354)^G$, where the group elements are written in cycle notation. The first two lines in the character table display the order of the elements and the cardinality of the corresponding conjugacy class, respectively. The two special values are $a = \frac{1}{2}(1+\sqrt{5})$ and $\bar{a} = \frac{1}{2}(1-\sqrt{5})$.

ord	1	2	3	5	5
#	1	15	20	12	12
	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$
χ_1	1	1	1	1	1
χ_2	3	-1	0	a	$\bar{a}$
χ_3	3	-1	0	$\bar{a}$	a
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Table 3.1.: Ordinary character table of A_5

3.1.2. Choosing a p-modular system

From Section 2.1 we know that the use of p-modular systems (K, R, k) allows for a connection between representations over K in characteristic 0, integral representations over R and p-modular representations over k in characteristic p. First we need to find a splitting field of characteristic 0. Theorem 2.1.6 tells us that a splitting field for A_5 is $K = \mathbb{Q}(\sqrt[u]{1})$ where $u = \exp G$ is the exponent of the group G. From the orders of the elements in G (the first line in the character Table 3.1) we infer that $\exp A_5 = 30$, and consequently, the first candidate for a splitting field is $K' = \mathbb{Q}(\zeta_{30})$ with ζ_{30} a primitive 30-th root of unity. However, the only non-rational values of the ordinary characters are $a = \frac{1}{2}(1+\sqrt{5})$ and $\bar{a} = \frac{1}{2}(1-\sqrt{5})$. Thus, we fix $K = \mathbb{Q}(\frac{1}{2}(1+\sqrt{5})) = \mathbb{Q}(\sqrt{5}) \subset K'$ as a splitting field for A_5 in characteristic 0 and we will embed K in a p-adic field to establish a p-modular system according to Definition 2.1.10. For this, we need a few results from algebraic number theory.[2]

[1] cf. [Wei03] or [Bur65] for a complete deduction.
[2] For a rigorous treatment of the following paragraphs, see [JS06, Ch. 10, pp. 362].

Let $L/\mathbb{Q}$ be an algebraic number field and $\mathcal{O}_L \subset L$ its ring of integers. Further, let $\mathfrak{p} \trianglelefteq \mathcal{O}_L$ be a prime ideal lying over the prime ideal $(p) \trianglelefteq \mathbb{Z}$, that is, $\mathfrak{p} \cap \mathbb{Z} = (p)$, and denote by $\mathbb{F}_\mathfrak{p} := \mathcal{O}_L/\mathfrak{p}$ the residue field.[3] The inertial degree f_p is defined as $f_p = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$.

In our case, $\mathcal{O}_K = \mathcal{O}_5 = \mathbb{Z} \oplus \mathbb{Z}\omega_5$ with $\omega_5 = \frac{1+\sqrt{5}}{2}$. Since $5 \equiv 1 \mod 4$, the discriminant Δ of K equals 5. In quadratic number fields, the inertial degree f_p for a prime p is determined by the Legendre symbol in the following way:

(a) $\left(\frac{\Delta}{p}\right) = 1$: There are distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \subseteq \mathcal{O}_5$ with $p\mathcal{O}_5 = \mathfrak{p}_1\mathfrak{p}_2$. $\mathcal{O}_5/\mathfrak{p}_1 \cong \mathbb{F}_p \cong \mathcal{O}_5/\mathfrak{p}_2$, giving $f_p = 1$. The prime p is said to *split*.

(b) $\left(\frac{\Delta}{p}\right) = 0$: There is a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_5$ with $p\mathcal{O}_5 = \mathfrak{p}^2$. $\mathcal{O}_5/\mathfrak{p} \cong \mathbb{F}_p$, and again $f_p = 1$. The prime p is said to *ramify*.

(c) $\left(\frac{\Delta}{p}\right) = -1$: The ideal $p\mathcal{O}_5$ itself is prime in $\mathcal{O}_5$. $\mathcal{O}_5/p\mathcal{O}_5 \cong \mathbb{F}_{p^2}$, and hence, $f_p = 2$. The prime p is called *inert*.

Consider now the p-adic field $\mathbb{Q}_p$ which is the completion of $\mathbb{Q}$ with respect to the p-adic valuation ν_p. We can extend the valuation ν_p onto $K = \mathbb{Q}(\sqrt{5})$ and complete K with respect to this extended valuation. The resulting completion K_p of K is isomorphic to the extension $\mathbb{Q}_p(\sqrt{5})/\mathbb{Q}_p$ (in symbols: $(\mathbb{Q}(\sqrt{5}))_p \cong \mathbb{Q}_p(\sqrt{5})$) and independent of the chosen extension of the valuation ν_p, which justifies our notation for the modular splitting field fixed above. Since K_p is a local field, there is a unique maximal ideal $\pi\mathcal{O}_{K_p}$ where π is a uniformizing element. Let $k_p = \mathcal{O}_{K_p}/\pi\mathcal{O}_{K_p}$ denote the residue field of K_p. The key observation (cf. [Ser79, §3, Thm. 1(ii)]) is that

$$[k_p : \mathbb{F}_p] = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] = f_p \tag{3.1}$$

or in other words, $k_p \cong \mathbb{F}_\mathfrak{p}$, i.e., the inertial degrees in the global and local field extension are the same. In the light of these considerations we choose the following p-modular system:

- $K_p := \mathbb{Q}_p(\sqrt{5})$, a quadratic extension of the p-adic field $\mathbb{Q}_p$.
- $R := \mathbb{Z}_p[\omega_5]$, the ring of integers of K_p, where $\mathbb{Z}_p$ are the p-adic integers. The unique maximal ideal in R is given by πR with π a uniformizing element of R.
- $k_p := R/\pi R$, the residue field of R. In most cases we will write k for k_p whenever it is clear in which characteristic we are working.

[3] The ring of integers $\mathcal{O}_L$ of an algebraic number field L is a Dedekind ring; therefore, every non-zero prime ideal is maximal. Moreover, $\mathbb{F}_\mathfrak{p}$ is always finite.

Computing the Legendre symbol for the prime numbers dividing $|A_5| = 60$ and applying the above ideas give the corresponding residue fields k_p, which are displayed in Table 3.2.

p	2	3	5
$\left(\frac{5}{p}\right)$	-1	-1	0
$\mathbb{F}_{\mathfrak{p}} = k_p$	$\mathbb{F}_4$	$\mathbb{F}_9$	$\mathbb{F}_5$

Table 3.2.: Residue fields for $p = 2, 3, 5$

3.2. Structure of the group algebra in modular characteristic

3.2.1. Block decomposition and block idempotents

To determine the block structure of kG we first use the character relation formula of Proposition 2.3.12(ii) to find the number of blocks, which we restate here: Two irreducible ordinary characters χ and χ' lie in the same block if and only if

$$\frac{|g^G|\chi(g)}{\chi(1)} \equiv \frac{|g^G|\chi'(g)}{\chi'(1)} \mod \pi \quad \forall g \in G_{p'} \tag{3.2}$$

Here, $G_{p'}$ is the set of all p-regular elements of G as defined in Definition 2.2.7. Once it is clear which characters lie in which block, the corresponding block idempotents can be calculated using

$$\varepsilon_B \equiv \sum_{\chi \in \operatorname{Irr}(B)} \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g \mod \pi \tag{3.3}$$

where $\operatorname{Irr}(B) := \{\chi \in \operatorname{Irr}(G) \mid \chi \text{ lies in } B\}$. Note that the sum is taken over ordinary characters and then reduced modulo π.

Starting with $p = 2$ we apply (3.2) to the irreducible characters from Table 3.1. Since $\operatorname{ord}(g) = 2$ for all $g \in \mathcal{C}_2$, the conjugacy class $\mathcal{C}_2$ of all double transpositions is the only 2-singular conjugacy class and must therefore be discarded in the computation. The result can be seen in Table 3.3, which displays the value of $\frac{|g^G|\chi(g)}{\chi(1)}$ for all characters χ on the 2-regular conjugacy classes.

We infer that there are two blocks B_1 and B_2 with $\operatorname{Irr}(B_1) = \{\chi_1, \chi_2, \chi_3, \chi_5\}$ and $\operatorname{Irr}(B_2) = \{\chi_4\}$, respectively. We will later see that B_2 is a block of defect zero. The block B_1 containing the trivial character is also called the principal block. With this

$\lvert g^G\rvert\chi(g)/\chi(1)$	$\mathcal{C}_1$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$
χ_1	1	0	0	0
χ_2	1	0	0	0
χ_3	1	0	0	0
χ_4	1	1	1	1
χ_5	1	0	0	0

Table 3.3.: Characters in blocks for $p = 2$

knowledge, we are ready to compute the idempotents using (3.3). We set $\mathcal{C}_i^+ := \sum_{g\in\mathcal{C}_i} g$.

$$\begin{aligned}
\varepsilon_{B_1} &= \frac{1}{60}(\mathcal{C}_1^+(1+9+9+25) + \mathcal{C}_3^+(1-5)+ \\
&\quad + \mathcal{C}_4^+(1+3(a+\bar{a})) + \mathcal{C}_5^+(1+3(a+\bar{a}))) \\
&= \frac{1}{60}(44\mathcal{C}_1^+ - 4\mathcal{C}_3^+ + 4\mathcal{C}_4^+ + 4\mathcal{C}_5^+) \\
&= \frac{11}{15}\mathcal{C}_1^+ - \frac{1}{15}\mathcal{C}_3^+ + \frac{1}{15}\mathcal{C}_4^+ + \frac{1}{15}\mathcal{C}_5^+ \\
&\equiv \mathcal{C}_1^+ + \mathcal{C}_3^+ + \mathcal{C}_4^+ + \mathcal{C}_5^+ \mod 2 \qquad (3.4a)\\
\varepsilon_{B_2} &= \frac{1}{60}(16\mathcal{C}_1^+ + 4\mathcal{C}_3^+ - 4\mathcal{C}_4^+ - 4\mathcal{C}_5^+) \\
&= \frac{4}{15}\mathcal{C}_1^+ + \frac{1}{15}\mathcal{C}_3^+ - \frac{1}{15}\mathcal{C}_4^+ - \frac{1}{15}\mathcal{C}_5^+ \\
&\equiv \mathcal{C}_3^+ + \mathcal{C}_4^+ + \mathcal{C}_5^+ \mod 2 \qquad (3.4b)
\end{aligned}$$

As follows from Theorem 2.3.2, it holds that $\varepsilon_{B_1} + \varepsilon_{B_2} = 1$, the identity of the k-algebra kG.

For $p = 3$ we have four 3-regular conjugacy classes, namely $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_4$ and $\mathcal{C}_5$. The distribution of the irreducible characters into blocks can be seen in Table 3.4, where $\lvert g^G\rvert\chi(g)/\chi(1)$ is evaluated for all 3-regular conjugacy classes.

$\lvert g^G\rvert\chi(g)/\chi(1)$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_4$	$\mathcal{C}_5$
χ_1	1	0	0	0
χ_2	1	1	$2+2\sqrt{5}$	$2+\sqrt{5}$
χ_3	1	1	$2+\sqrt{5}$	$2+2\sqrt{5}$
χ_4	1	0	0	0
χ_5	1	0	0	0

Table 3.4.: Characters in blocks for $p = 3$

In characteristic 3, there are three blocks B_1, B_2 and B_3 with $\mathrm{Irr}(B_1) = \{\chi_1, \chi_4, \chi_5\}$ and $\mathrm{Irr}(B_j) = \{\chi_j\}$ for $j = 2, 3$. Similar to the case $p = 2$, the blocks B_2 and B_3 have defect zero, and B_1 is the principal block. The block idempotents are given as

$$\varepsilon_{B_1} \equiv \mathcal{C}_1^+ + \mathcal{C}_2^+ + \mathcal{C}_4^+ + \mathcal{C}_5^+ \mod 3 \tag{3.5a}$$

$$\varepsilon_{B_2} \equiv \mathcal{C}_2^+ + 2a\mathcal{C}_4^+ + 2\bar{a}\mathcal{C}_5^+ \mod 3 \tag{3.5b}$$

$$\varepsilon_{B_3} \equiv \mathcal{C}_2^+ + 2\bar{a}\mathcal{C}_4^+ + 2a\mathcal{C}_5^+ \mod 3 \tag{3.5c}$$

As expected, $\varepsilon_{B_1} + \varepsilon_{B_2} + \varepsilon_{B_3} = 1$ (note that $a + \bar{a} = 1$).

Finally, for $p = 5$ there are only three 5-regular conjugacy classes $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$. The irreducible characters are distributed among the blocks according to Table 3.5.

$\lvert g^G \rvert \chi(g) / \chi(1)$	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$
χ_1	1	0	0
χ_2	1	0	0
χ_3	1	0	0
χ_4	1	0	0
χ_5	1	3	1

Table 3.5.: Characters in blocks for $p = 5$

There are two blocks, the principal block B_1 with $\mathrm{Irr}(B_1) = \{\chi_1, \chi_2, \chi_3, \chi_4\}$ and the block $B_2 = \{\chi_5\}$ of defect zero. The corresponding block idempotents are

$$\varepsilon_{B_1} \equiv \mathcal{C}_1^+ + 2\mathcal{C}_2^+ + 3\mathcal{C}_3^+ \mod 5 \tag{3.6a}$$

$$\varepsilon_{B_2} \equiv 3\mathcal{C}_2^+ + 2\mathcal{C}_3^+ \mod 5 \tag{3.6b}$$

As before, $\varepsilon_{B_1} + \varepsilon_{B_2} = 1$, the identity of kG.

In the further analysis we will always arrange the irreducible ordinary characters according to Proposition 2.3.14 as follows: Suppose we have a block B_1 with the characters χ_1 and χ_3, and a block B_2 with the character χ_2. Then the ordering of the characters in the decomposition matrix (whose rows are indexed by the ordinary irreducible characters) would be

$$\underbrace{1 - 3}_{B_1} - \underbrace{2}_{B_2}$$

The same holds for the irreducible p-Brauer characters: Each corresponds to the unique irreducible socle of a PIM, and according to Definition 2.3.4 each socle lies in one block. Since the columns of the decomposition matrix and the Cartan matrix are labeled by the irreducible Brauer characters, both reorderings ensure the block form of these matrices.

3.2.2. Brauer character table and Decomposition matrix

In this section we want to compute the decomposition matrix D_p and the Brauer character table. Let us fix the notation $\chi' := \chi|_{G_{p'}}$ for the restriction of an ordinary character to the p-regular conjugacy classes. Since the derivation of the 3-Brauer character table is more involved, it is dealt with at the end of this section.

Characteristic 2 and 5

We start by investigating the case $p = 2$. There are four p-regular conjugacy classes, so by Corollary 2.2.17 we are looking for four irreducible Brauer characters. Of course the restriction of the trivial character $\varphi_1 = \chi_1'$ is one of them. Since $2 \nmid \frac{|G|}{\chi_4(1)}$, it follows from Proposition 2.3.17 that $\varphi_4 = \chi_4'$ is another one. Now observe that

$$\chi_2' + \chi_3' = \chi_1' + \chi_5' \tag{3.7}$$

This means that at least one of the characters χ_2', χ_3' contains φ_1 as an irreducible constituent. Since χ_2 and χ_3 are conjugate, this holds for both of them by Proposition A.2.2(ii). It follows that χ_5', which is a character of degree 5, also contains φ_1 as an irreducible constituent. Now 'subtract' φ_1 twice from (3.7). The degree on the right side is now 4, so we see that the remaining irreducible constituents of χ_2' resp. χ_3' have degree 2, i.e. either two constituents of degree 1 or one irreducible constituent of degree 2. From theorem A.1.2 we know that the linear characters of a group G and its abelianization $G^{\text{ab}} = G/[G,G]$ are in 1:1-correspondence. But $[A_5, A_5] = A_5$, which implies that the trivial character χ_1 is the only character of degree 1. In the case of two constituents of degree 1, this leaves $\chi_2' = \chi_3' = 3\chi_1'$ as the only possibility. But comparing the character values on both sides in the ordinary character table 3.1 shows that this cannot be the case. Therefore, χ_2' and χ_3' both contain an irreducible constituent of degree 2, namely φ_2 and φ_3, and they are conjugate and different since χ_2 and χ_3 are conjugate characters. Thus, we have found the two remaining irreducible 2-Brauer characters, and their values on the 2-regular conjugacy classes are determined by (3.7). The 2-Brauer character table is displayed in Table 3.6.

The above discussion also determines the decomposition matrix D_2, which is given by how the ordinary irreducible characters split up into the irreducible Brauer characters. Note the different ordering $1 - 2 - 3 - 5 - 4$ of the irreducible characters according to

	$\mathcal{C}_1$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$
φ_1	1	1	1	1
φ_2	2	-1	$a-1$	$\bar{a}-1$
φ_3	2	-1	$\bar{a}-1$	$a-1$
φ_4	4	1	-1	-1

Table 3.6.: Brauer character table for $p = 2$

their distribution into blocks. Zeros in the decomposition matrix have been replaced by '.' for better readability.

$$\left.\begin{aligned} &\chi_1 \mapsto \varphi_1 \\ &\chi_2 \mapsto \varphi_1 + \varphi_2 \\ &\chi_3 \mapsto \varphi_1 + \varphi_3 \\ &\chi_5 \mapsto \varphi_1 + \varphi_2 + \varphi_3 \\ &\chi_4 \mapsto \varphi_4 \end{aligned}\right\} \qquad D_2 = \begin{pmatrix} 1 & . & . & . \\ 1 & 1 & . & . \\ 1 & . & 1 & . \\ 1 & 1 & 1 & . \\ . & . & . & 1 \end{pmatrix} \tag{3.8}$$

Observe that $X_2 = D_2 \Phi_2$ as in (2.2), where X_2 is the ordinary character table with the column belonging to the 2-singular class $\mathcal{C}_2$ removed and Φ_2 is the 2-Brauer character table.

For $p = 5$ there are three 5-regular conjugacy classes and hence three modular irreducible representations by Corollary 2.2.17. As before, $\chi_1' = \varphi_1$, the trivial representation, and according to Proposition 2.3.17 $\chi_5' = \varphi_3$ is another one since $5 \nmid \frac{|G|}{\chi_5(1)}$.

For the remaining Brauer character, suppose first that $\chi_2' = \chi_3'$ is reducible. Since these characters have degree 3 and the trivial ordinary character χ_1 is the only 1-dimensional character of A_5, a possible option is $\chi_2' = \chi_3' = 3\varphi_1$. However, comparing character values in the ordinary character table 3.1 shows that this is impossible. Hence, in case $\chi_2' = \chi_3'$ is reducible, there must be a 2-dimensional irreducible Brauer character[4] φ_2' with $\varphi_2'(1) = 2$ and

$$\chi_2' = \varphi_1 + \varphi_2' = \chi_3' \tag{3.9}$$

Equation 3.9 determines the character values $\varphi_2'(\mathcal{C}_2) = -2$ and $\varphi_2'(\mathcal{C}_3) = -1$ of the 2-dimensional irreducible Brauer character φ_2'. Now let $\rho : A_5 \to \mathrm{GL}_2(\mathbb{F}_5)$ be the irreducible representation corresponding to φ_2'. Since A_5 is simple and the kernel of a

[4]Note that in this case, the prime does not indicate restriction to p-regular conjguacy classes.

representation is a normal subgroup, we can assume that ρ is injective. For $g \in \mathcal{C}_2$ we have $\operatorname{ord}(g) = \operatorname{ord}(\rho(g)) = 2$; hence, $\rho(g)^2 = \mathrm{id} \neq \rho(g)$ since ρ is injective. Therefore, the minimal polynomial $\mu_{\rho(g)}(T)$ of $\rho(g)$ is either

$$\begin{aligned} &\mu_{\rho(g)}(T) = T^2 - 1 = (T+1)(T-1) \\ \text{or} \quad &\mu_{\rho(g)}(T) = T + 1 \end{aligned}$$

Suppose that the first case is true and $\lambda = \pm 1$ are the possible eigenvalues of $\rho(g)$: Since $\varphi_2'(\mathcal{C}_2) = -2$, the only eigenvalue of $\rho(g)$ is $\lambda = -1$. Due to the choice of the p-modular system in Section 3.1.2, we know that $k = \mathbb{F}_5$ is a splitting field for ρ. Therefore, we can write down the Jordan normal form of $\rho(g)$:

$$\rho(g) = \begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix} \tag{3.10}$$

where $c \in \{0, 1\}$. Since $\rho(g)^2 = \mathrm{id}$, we can exclude $c = 1$; thus, $\rho(g) = -\mathrm{id}$ and $\mu_{\rho(g)}(T) = T+1$. Now $\rho(g) = -\mathrm{id}$ belongs to the center of $\mathrm{GL}_2(\mathbb{F}_5)$ for every $g \in \mathcal{C}_2$. But ρ is injective, and from $\rho(gh) = \rho(g)\rho(h) = \rho(h)\rho(g) = \rho(hg)$ for all $g \in \mathcal{C}_2$ and $h \in A_5$ we infer that $gh = hg$ for all $g \in \mathcal{C}_2$ and $h \in A_5$. In other words, $g \in Z(A_5) = \{e\}$, which is a contradiction to $g \in \mathcal{C}_2$. Therefore, the assumption of the existence of an irreducible Brauer character φ_2' of degree 2 (and hence the reducibility of $\chi_2' = \chi_3'$) was wrong, and $\varphi_2 = \chi_2' = \chi_3'$ is the remaining irreducible Brauer character. This gives the 5-Brauer character table 3.7.

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$
φ_1	1	1	1
φ_2	3	-1	0
φ_3	5	1	-1

Table 3.7.: Brauer character table for $p = 5$

It follows immediately that $\chi_4' = \varphi_1 + \varphi_2$. Note that this time there is no reordering of the irreducible characters. The decomposition matrix D_5 is given as

$$\left.\begin{aligned} \chi_1 &\mapsto \varphi_1 \\ \chi_2 &\mapsto \varphi_2 \\ \chi_3 &\mapsto \varphi_2 \\ \chi_4 &\mapsto \varphi_1+\varphi_2 \\ \chi_5 &\mapsto \varphi_3 \end{aligned}\right\} \qquad D_5 = \begin{pmatrix} 1 & . & . \\ . & 1 & . \\ . & 1 & . \\ 1 & 1 & . \\ . & . & 1 \end{pmatrix} \tag{3.11}$$

Characteristic 3

In characteristic 3 there are four 3-regular conjugacy classes ($\mathcal{C}_3$ being 3-singular), hence four modular irreducible representations by Corollary 2.2.17. Again, $\varphi_1 = \chi_1'$, the trivial representation. Since $3 \nmid \frac{G}{\chi_i(1)}$ for $i = 2, 3$, the characters χ_2 and χ_3 are also irreducible in characteristic 3 by Proposition 2.3.17, and we have found two more irreducible Brauer characters $\varphi_2 = \chi_2'$ and $\varphi_3 = \chi_3'$.

For the remaining irreducible Brauer character let us remember the distribution into blocks of the ordinary characters from Table 3.4. Since χ_2 and χ_3 remain irreducible and in each case form its own block, the remaining irreducible Brauer character has to be a constituent of χ_4 or χ_5. Therefore, consider the ordinary irreducible representation χ_4 which is just the representation of A_5 permuting coordinates in

$$V = \{(x_1, x_2, x_3, x_4, x_5)^T \mid x_1 + \cdots + x_5 = 0\} \leq K^5$$

(cf. [Wei03, Ch. 3, pp. 75]). Reducing this representation modulo 3 gives the k-vector space $V_k \leq k^5$ (remember that $k = \mathbb{F}_9$), and we claim that $\varphi_4 = \chi_4'$ is irreducible and hence the last irreducible Brauer character. This is shown in the following

Lemma 3.2.1. *The restriction $\chi_4' = \chi_4|_{G_{3'}}$ of the ordinary irreducible character χ_4 of A_5 to the 3-regular conjugacy classes remains irreducible and is therefore an irreducible Brauer character.*

Proof. We show that χ_4 cannot be reducible. To begin with, note that the only one-dimensional representation of A_5 is the trivial representation with $g \mapsto \mathrm{id}$ for all $g \in A_5$. Since the coordinates are permuted by elements of the group, the existence of a one-dimensional subspace U on which A_5 acts trivially is only possible if we have $U = \langle (x, x, x, x, x)^T \rangle_k$ for some $0 \neq x \in k$.[5] But the condition $\sum_i x_i = 0$ rules out this

[5] To show this, simply subsequently apply $g = (123), (234), (345)$ to a vector $v = (v_1, v_2, v_3, v_4, v_5)$ with $v_i \in k$. From $gv = v$ follows the stated form of v.

possibility. So in case χ'_4 is reducible modulo 3, we have the following options:

1. $\chi'_4 = 2\varphi'_4$, where φ'_4 is an irreducible Brauer character of degree 2
2. $\chi'_4 = \varphi''_4 + \varphi_1$, where φ''_4 is an irreducible Brauer character of degree 3, and the representation corresponding to φ_1 is a one-dimensional quotient representation in V_k
3. $\chi'_4 = \varphi'''_4 + 2\varphi_1$, where φ'''_4 is an irreducible Brauer character of degree 2, and both representations corresponding to φ_1 are one-dimensional quotient representations in V_k

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_4$	$\mathcal{C}_5$
χ_4	4	0	-1	-1
φ'_4	2	0	$-\frac{1}{2}$	$-\frac{1}{2}$
φ''_4	3	-1	-2	-2
φ'''_4	2	-2	-3	-3

Table 3.8.: Possible choices for φ_4 in characteristic 3

Looking at the ordinary character table 3.1, we can infer the character values of these hypothetical characters, which are listed in Table 3.8. Since $-\frac{1}{2}$ is not an algebraic integer in $R = \mathbb{Z}_p[\omega_5]$, we can directly dismiss φ'_4.[6] We know from Proposition 2.2.12(v) that for a subgroup $H \leq A_5$ with $p \nmid |H|$, the restriction $\varphi|_H$ of a Brauer character φ to H is an ordinary character and therefore in the $\mathbb{Z}$-span of the irreducible ordinary characters of H. We choose for H the dihedral subgroup $D_{10} \leq A_5$ consisting of the conjugacy classes[7]

$$\begin{aligned}
\mathcal{C}_1^H &= \{e\} \\
\mathcal{C}_2^H &= \{(25)(34), (12)(35), (13)(45), (14)(23), (15)(24)\} \\
\mathcal{C}_4^H &= \{(12345), (15432)\} \\
\mathcal{C}_5^H &= \{(13524), (14253)\}
\end{aligned}$$

Table 3.9 is the ordinary character table of D_{10}, where again $a = \frac{1+\sqrt{5}}{2}$.

[6]Remember that Brauer character values are sums of roots of unity and hence integral over $\mathbb{Z}$.
[7]The numbering is adjusted to the 3-regular classes of A_5 to ensure $\mathcal{C}_i^H \subset \mathcal{C}_i$, hence the missing $\mathcal{C}_3$.

	$\mathcal{C}_1^H$	$\mathcal{C}_2^H$	$\mathcal{C}_4^H$	$\mathcal{C}_5^H$
χ_1^H	1	1	1	1
χ_2^H	1	1	1	-1
χ_3^H	2	$-a$	$-\bar{a}$	0
χ_4^H	2	$-\bar{a}$	$-a$	0

Table 3.9.: Ordinary character table of $D_{10} \leq A_5$

We have $\mathcal{C}_i^H \subset \mathcal{C}_i$ for $i = 1, 2, 4, 5$, and the hypothetical restricted Brauer characters $\varphi_4''|_{D_{10}}$ and $\varphi_4'''|_{D_{10}}$ can be written as

$$\varphi_4''|_{D_{10}} = \sum_{i=1}^{4} c_i \chi_i^H \qquad \qquad \varphi_4'''|_{D_{10}} = \sum_{i=1}^{4} d_i \chi_i^H$$

Hence, Tables 3.8 and 3.9 give the following systems of linear equations corresponding to φ_4'' and φ_4''':

$$\begin{aligned} c_1 + c_2 + c_3 + c_4 &= 3 \\ c_1 + c_2 - ac_3 - \bar{a}c_4 &= -1 \\ c_1 + c_2 - \bar{a}c_3 - ac_4 &= -2 \\ c_1 - c_2 &= -2 \end{aligned} \qquad \qquad \begin{aligned} d_1 + d_2 + d_3 + d_4 &= 2 \\ d_1 + d_2 - ad_3 - \bar{a}d_4 &= -2 \\ d_1 + d_2 - \bar{a}d_3 - ad_4 &= -3 \\ d_1 - d_2 &= -3 \end{aligned}$$

The unique solutions of these systems do not lie in $\mathbb{Z}^4$; therefore, neither φ_4'' nor φ_4''' can be irreducible Brauer characters of A_5, and the assumption that χ_4' is reducible is wrong. Hence, $\varphi_4 = \chi_4'$ constitutes the remaining irreducible Brauer character. □

The complete 3-Brauer character table is displayed in Table 3.10.

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_4$	$\mathcal{C}_5$
φ_1	1	1	1	1
φ_4	4	0	-1	-1
φ_2	3	-1	a	$\bar{a}$
φ_3	3	-1	$\bar{a}$	a

Table 3.10.: Brauer character table for $p = 3$

To determine the decomposition matrix D_3, we observe that $\chi_5' = \varphi_1 + \varphi_4$. Therefore, we have:

$$\left.\begin{aligned} \chi_1 &\mapsto \varphi_1 \\ \chi_4 &\mapsto \varphi_4 \\ \chi_5 &\mapsto \varphi_1 + \varphi_4 \\ \chi_2 &\mapsto \varphi_2 \\ \chi_3 &\mapsto \varphi_3 \end{aligned}\right\} \qquad D_3 = \begin{pmatrix} 1 & . & . & . \\ . & 1 & . & . \\ 1 & 1 & . & . \\ . & . & 1 & . \\ . & . & . & 1 \end{pmatrix} \tag{3.12}$$

The ordering of the ordinary irreducible characters (and hence the modular irreducible characters) has been changed to $1-4-5-2-3$ in order to guarantee the block form of D_3.

3.2.3. Cartan matrix and the decomposition of *kG* into PIMs

The modular irreducible characters are collected in the respective Brauer character tables 3.6, 3.10 and 3.7. Using this information we are now able to examine the structure of the regular representation kG.

The most important tool in this process is the Cartan matrix C_p, which according to proposition 2.2.4 is already determined by the decomposition matrix D_p via the formula $C_p = D_p^T D_p$. They are listed in (3.13) for the three cases $p = 2, 3, 5$.

$$C_2 = \begin{pmatrix} 4 & 2 & 2 & 0 \\ 2 & 2 & 1 & 0 \\ 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad C_3 = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad C_5 = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{3.13}$$

Let us recapitulate their implications. At first we restate Lemma 2.2.3(i): The nonnegative entry c_{ij} of C is the multiplicity with which the modular irreducible representation $\overline{\tau}_j$ occurs in the principal indecomposable modular representation $\overline{\partial}_i$. In other words, the rows of C_p are indexed by the PIMs P_i corresponding to the principal indecomposable representations $\overline{\partial}_i$, and the columns are indexed by the (modular) irreducible modules T_j corresponding to the irreducible modular representations $\overline{\tau}_j$. This means that a composition series for P_i contains c_{ij} factors isomorphic to the irreducible module T_j. Furthermore, $\mathrm{soc}(\overline{\partial}_i) \cong T_i \sim \overline{\tau}_i$, and we stress that a PIM is uniquely determined by its socle. If the PIMs indexing the rows of the Cartan matrix C_p and the irreducible Brauer characters indexing the columns are sorted according to their distribution into blocks, then a 1×1-block represents a block of defect zero. In this case, P_i is simple and isomorphic to its socle, $P_i \cong \mathrm{soc}(P_i)$. However, in general the Cartan matrix C_p as well as the decomposition matrix D_p do not have block form, and blocks of defect zero cannot be identified as easily.

The dimensions of the PIMs P_i can be read off from the character table Ψ comprising the characters ψ_i of $\overline{\partial}_i$. According to (2.2) this character table is given by the formula $\Psi_p = C_p \Phi_p$, where Φ is the p-Brauer character table. Moreover, since $\dim(kG) = 60$, simple arithmetic would already determine the multiplicities of P_i in kG. However, Theorem 1.2.21 enables us to derive them theoretically. In our situation it acquires the form of (3.14) with $n_\varphi = \dim \operatorname{soc}(P_\varphi)$ and $k_\varphi = \dim \operatorname{End}(\operatorname{soc}(P_\varphi))$.

$$kG = \bigoplus_{\varphi \in \mathrm{IBr}_p(G)} \frac{n_\varphi}{k_\varphi} P_\varphi \tag{3.14}$$

Note that now the PIMs are indexed by the p-Brauer character associated to the unique socle. Since (K, R, k) is a p-modular system for G, it follows by Proposition 2.1.3 that $\operatorname{End}(S) \cong k$ for every simple kG-module S, so $k_\varphi = 1$. Thus, the multiplicity of P_φ is equal to the dimension of its unique socle $\operatorname{soc}(P_\varphi)$.

These considerations lead to the structure of kG. The results as well as the necessary data for the PIMs are listed in Table 3.11 for all three cases. Compare this also with the Brauer character tables 3.6, 3.10 and 3.7 for the dimensions of $\operatorname{soc}(P_i)$.

char = 2	P_1	P_2	P_3	P_4
dim	12	8	8	4
dim(soc)	1	2	2	4

$$kG = \underbrace{P_1 \oplus 2P_2 \oplus 2P_3}_{B_1} \oplus \underbrace{4P_4}_{B_2}$$

char = 3	P_1	P_2	P_3	P_4
dim	6	9	3	3
dim(soc)	1	4	3	3

$$kG = \underbrace{P_1 \oplus 4P_2}_{B_1} \oplus \underbrace{3P_3}_{B_2} \oplus \underbrace{3P_4}_{B_3}$$

char = 5	P_1	P_2	P_3
dim	5	10	5
dim(soc)	1	3	5

$$kG = \underbrace{P_1 \oplus 3P_2}_{B_1} \oplus \underbrace{5P_3}_{B_2}$$

Table 3.11.: Structure of kG

Remark. According to Proposition 1.1.2, the decomposition of $kG = \bigoplus P_i$ into a direct sum of PIMs corresponds to a set $\{e_i\}$ of primitive orthogonal idempotents. Every PIM P_i is then given as the principal (left or right) ideal $P_i \cong e_i kG$ generated by the respective idempotent e_i. This is the subject of Section 3.3.1.

3.2.4. Reducing the irreducible ordinary representations

So far we have completely determined the irreducible modular representations of G via their corresponding Brauer characters (cf. Section 3.2.2) and decomposed the group algebra kG into the indecomposable components, i.e., the PIMs (cf. Section 3.2.3). However, we already know the irreducible ordinary representations in characteristic 0 (see Table 3.1) from ordinary representation theory. This is the semisimple case where the group algebra KG is completely reducible and has the following decomposition:

$$KG = R_1 \oplus 3R_2 \oplus 3R_3 \oplus 4R_4 \oplus 5R_5 \tag{3.15}$$

where R_i is the irreducible and indecomposable KG-module affording the irreducible character χ_i from Table 3.1.[8] Theorem 2.1.13 shows that the corresponding representations σ_i are equivalent to representations defined over R. However, the situation is a little bit more involved since we want to turn decomposition (3.15) into a decomposition over R, in order to reduce it modulo π and work in the modular case.

To this end we start with a decomposition

$$kG = P_1 \oplus \cdots \oplus P_t$$

of kG into PIMs according to Table 3.11. Theorem 2.1.11 implies that this decomposition corresponds to a decomposition

$$RG = Q_1 \oplus \cdots \oplus Q_t \tag{3.16}$$

of RG into indecomposable RG-modules. To see that the sum of the lifted PIMs Q_i is in fact all of RG, assume the contrary, i.e., $RG = Q_1 \oplus \cdots \oplus Q_t \oplus Q$ with $Q \neq 0$. Since the idempotents f_i corresponding to the PIMs Q_i for $1 \leq i \leq t$ are primitive orthogonal, their sum $f_1 + \cdots + f_t$ is again an idempotent, and $f_Q := 1 - (f_1 + \cdots + f_t) \neq 0$ is the idempotent of Q. But by Theorem 2.1.11(i), the reduction of f_Q is not zero, and since f_Q is orthogonal to every f_i, the same holds for the respective reductions, contradicting the decomposition $kG = P_1 \oplus \cdots \oplus P_t$.

Now take the tensor product with K in (3.16). Since the summands Q_i are finitely generated, torsion-free R-modules (and hence free), by Proposition 2.1.9(vi) the $K \otimes Q_i$ are also free having the same rank as the Q_i, and comparing dimensions shows that in

[8] Recall that in the semisimple case the properties 'irreducible' and 'indecomposable' coincide.

fact

$$KG = (K \otimes Q_1) \oplus \cdots \oplus (K \otimes Q_t) \tag{3.17}$$

But the group algebra KG is semisimple because of char $K = 0$; therefore, (3.17) decomposes into simple summands, and the resulting decomposition is isomorphic to (3.15).

Identifying the decompositions of the group algebra over K and over R by the above reasoning, we can now ask how the PIMs P_i arise when reducing the integral regular representation RG modulo a uniformizing element π of R. We can reformulate this question in terms of representations as follows: Given a PIM $P_i \sim \overline{\partial}_i$ in characteristic p, we choose a representation ∂_i of RG such that $\overline{\partial}_i \sim P_i$. Then we take the tensor product[9] $K \otimes \partial_i$ to obtain a K-representation such that $K \otimes \partial_i$ decomposes into the irreducible K-representations, and we can write

$$K \otimes \partial_i = \sum_j \lambda_{ij} \sigma_j$$

Our goal is to compute the coefficients λ_{ij}. Corollary 2.2.5 states that $\lambda_{ij} = d_{ji}$, i.e., the coefficients λ_{ij} of σ_j for the i-th representation ∂_i can be read off the i-th column of the decomposition matrix D_p. In characteristic 2, the representations ∂_i of KG whose reductions correspond to the PIMs P_i are listed in (3.18a).

$$KG \sim \partial_1 + 2\partial_2 + 2\partial_3 + 4\partial_4 \qquad \text{with} \quad \begin{aligned} \partial_1 &= \sigma_1 + \sigma_2 + \sigma_3 + \sigma_5 \\ \partial_2 &= \sigma_2 + \sigma_5 \\ \partial_3 &= \sigma_3 + \sigma_5 \\ \partial_4 &= \sigma_4 \end{aligned} \tag{3.18a}$$

For $p = 3$, the result is displayed in (3.18b).

$$KG \sim \partial_1 + 4\partial_2 + 3\partial_3 + 3\partial_4 \qquad \text{with} \quad \begin{aligned} \partial_1 &= \sigma_1 + \sigma_5 \\ \partial_2 &= \sigma_4 + \sigma_5 \\ \partial_3 &= \sigma_2 \\ \partial_4 &= \sigma_3 \end{aligned} \tag{3.18b}$$

[9]This is a symbolic notation for the representation afforded by the module $K \otimes Q_i$, where Q_i is the RG-module affording ∂_i.

Finally, in characteristic 5 we have the decomposition (3.18c).

$$KG \sim \partial_1 + 3\partial_2 + 5\partial_3 \qquad \text{with} \quad \begin{aligned} \partial_1 &= \sigma_1 + \sigma_4 \\ \partial_2 &= \sigma_2 + \sigma_3 + \sigma_4 \\ \partial_3 &= \sigma_5 \end{aligned} \tag{3.18c}$$

Observe that the decompositions (3.18a), (3.18b) and (3.18c) are just shuffled versions of the decomposition (3.15), where the irreducible modules R_i have been regrouped to form the modules corresponding to the representations ∂_j.

3.3. Determining Idempotents and radical series of the PIMs

In the following section we are going to use the theoretical results from the previous sections to calculate the primitive orthogonal idempotents corresponding to the PIMs and their radical series. The computations are carried out by the program `GAP` (Groups, Algorithms and Programming), which can be obtained freely from the website `http://www.gap-system.org`. We will also use the `GAP`-package `reps`, authored by Peter Webb,[10] which is a set of routines designed to handle group representations in positive characteristic and can be downloaded from `http://www.math.umn.edu/~webb/GAPfiles/reps`.

3.3.1. Computation of the idempotents

As stated in Proposition 1.1.2(ii) and at the end of Section 3.2.3, the decomposition of $kG = \bigoplus P_i$ into a direct sum of PIMs corresponds to a set $\{e_i\}$ of primitive orthogonal idempotents with $P_i \cong e_i kG$ as kG-right ideals. The objective of this subsection is to compute these idempotents using `GAP` and the Meataxe algorithm. In order to avoid extensive repetition of `GAP`-code, the only case we will examine thoroughly is $\operatorname{char} k = 5$. For characteristic 2 and 3 we will merely state the results. This way the reader will become familiar with the relevant `GAP`-techniques without getting bored.

We are going to pursue the following strategy: From Table 3.11 we know that a block B is the direct sum of the PIMs corresponding to the irreducible p-Brauer characters belonging to this block:

$$B = \bigoplus_{\varphi \in \mathrm{IBr}_p(B)} n_\varphi P_\varphi \tag{3.19}$$

[10] School of Mathematics, University of Minnesota, `webb@math.umn.edu`

Here $\mathrm{IBr}_p(B) := \{\varphi \in \mathrm{IBr}_p(G) \mid \varphi \text{ belongs to } B\}$, and n_φ is the multiplicity of P_φ in the decomposition of B as a direct sum. In the language of idempotents (3.19) reads

$$\varepsilon_B = \sum_{\varphi \in \mathrm{IBr}_p(B)} e_\varphi \tag{3.20}$$

where ε_B is the block idempotent corresponding to the block B, and e_φ are the primitive orthogonal idempotents corresponding to the PIMs P_φ. To compute the e_φ we find a basis $\mathfrak{b}_\varphi$ of $n_\varphi P_\varphi$ for each $\varphi \in \mathrm{IBr}_p(B)$. Equation (3.19) then says that $\{\mathfrak{b}_\varphi\}_{\varphi \in \mathrm{IBr}_p(B)}$ is a basis for B and $e_\varphi = \mathcal{P}_\varphi \varepsilon_B$, where $\mathcal{P}_\varphi$ is the projection onto $n_\varphi P_\varphi$ with respect to decomposition (3.19). Therefore, we repeat the following algorithm in `GAP` for each block B:

(1) Initialize the necessary objects (group, group algebra, regular representation) in `GAP`.

(2) Decompose the regular representation with the routine `Decompose` from the `GAP`-package `reps`, which uses the Meataxe algorithm.

(3) In the output of `Decompose`, identify the correct PIMs of decomposition (3.19) by comparing their dimensions to Table 3.11. This may be ambiguous, so it might become necessary to compute the socle of a summand in doubt, in order to uniquely determine the PIM. If the socle $\operatorname{soc} P$ of a summand P turns out to be reducible, then by Corollary 1.2.16 and Proposition 1.1.15(iv) P is decomposable, and the `GAP` routine could not separate the PIMs.[11]

(4) Collect the bases of each copy of P_φ to construct a basis $\{\mathfrak{b}_\varphi\}_{\varphi \in \mathrm{IBr}_p(B)}$ of the block B adapted to its decomposition.

(5) Create the block B and the submodules $n_\varphi P_\varphi$ for each $\varphi \in \mathrm{IBr}_p(B)$ as the linear spaces spanned by the bases found in (4).

(6) Create the block idempotent ε_B via the formulae (3.6) computed in Section 3.2.1.

(7) Compute the coefficients of ε_B with respect to the basis $\{\mathfrak{b}_\varphi\}_{\varphi \in \mathrm{IBr}_p(B)}$ constructed in step (4).

(8) Compute the idempotents e_φ for each $\varphi \in \mathrm{IBr}_p(B)$.

(9) Verify the results.

[11] This happens quite frequently with Meataxe routines and always has to be accounted for.

Remark. We stress once again that in order to compute the idempotents we heavily depend on theoretical results derived in previous sections. Above all we require knowledge about the structure of kG (found in Table 3.11) and the formulae (3.6) of the block idempotents in characteristic 5. Moreover, identifying PIMs via their dimension is only possible since in our situation, where $G = A_5$, the PIMs P_i belonging to a block B (of defect unequal to zero) either have distinct dimensions ($p = 3, 5$) or are conjugate and hence have isomorphic factors ($p = 2$). For arbitrary (and especially more complicated) groups we would need to deploy other techniques to identify the correct PIMs.

Before we start with the computation, let us first recall the structure of kG in characteristic 5 from Table 3.11:

$$kG = \underbrace{P_1 \oplus 3P_2}_{B_1} \oplus \underbrace{5P_3}_{B_2} \tag{3.21}$$

Since B_2 is a block of defect zero (and therefore indecomposable), we concentrate on B_1 and try to find bases for P_1 and $3P_2$. Let us start with the computation in `GAP` (note that a double semicolon `;;` suppresses the output of a command):

(1)
```
gap> G:=AlternatingGroup(5);;
gap> A:=GroupRing(GF(5),G);;
gap> o:=Embedding(G,A);;
gap> b:=Basis(A);
CanonicalBasis( <algebra-with-one over GF(5), with 2 generators> )
gap> Read("reps");
gap> R:=RegularRep(G,GF(5));;
```

The definitions are rather self-explanatory. In `GAP` the group algebra kG is referred to as group ring and `GF(5)` $= \mathbb{F}_5$. The last lines load the package **`reps`** and create the regular representation ${}_{kG}kG$.

(2)
```
gap> dec:=Decompose(R);;
gap> List(dec,x->Size(x));
[ 5, 5, 5, 10, 5, 10, 10, 10 ]
```

This is the crucial part of our computation. The command `Decompose` invokes the Meataxe algorithm (cf. 1.3) and tries to decompose the regular representation `R` into summands of a direct sum. Since the full output of `Decompose` is rather long, we omit it at this point and merely note that it finds 8 summands with the dimensions printed via the `List` command. However, Table 3.11 tells us that there should be 9 PIMs. We investigate the last summand:

(3)
```
gap> P:=SubmoduleRep(R,dec[8]);;
gap> S:=SubmoduleRep(P,SocleRep(P));;
gap> IsAbsolutelyIrreducibleRep(S);
false
gap> S.dimension;
10
```

As suspected, the eighth summand is really the direct sum $P_3 \oplus P_3$. We will skip the verification that the other summands of dimension 10 are indeed indecomposable and identify the list entries with the corresponding PIMs:

```
[  5,  5,  5, 10,  5, 10, 10, 10 ] =
[ P3, P3, P3, P2, P1, P2, P2, P3 + P3 ]
```

Note that in order to distinguish P_1 and P_3 it is necessary to compute the socle of the entries 1, 2, 3 and 5 in `dec` and compare their dimensions to Table 3.11. For P_1 this computation is done in the next step, the rest is omitted for the sake of clarity. We gather the basis vectors of $3P_2$ (entries 4,6 and 7 in `dec`) in a list `p2` (`Decompose` outputs the basis vectors as coefficients with respect to the basis `b` defined above, hence the command `LinearCombination`):

(4)
```
gap> p2:=[];;
gap> for i in dec[4] do
> Add(p2,LinearCombination(b,i));
> od;
gap> for i in dec[6] do
> Add(p2,LinearCombination(b,i));
> od;
gap> for i in dec[7] do
> Add(p2,LinearCombination(b,i));
> od;
```

The list `p2` now contains a basis of $3P_2$. For P_1 we identify the fifth entry in `dec` as the right summand by computing the socle:

```
gap> Q1:=SubmoduleRep(R,dec[5]);;
```

```
gap> S1:=SubmoduleRep(Q1,SocleRep(Q1));;
gap> IsAbsolutelyIrreducibleRep(S1);
true
gap> S1.dimension;
1
```

We write the basis of P_1 into the list `p2`.

```
gap> p1:=[];;
gap> for i in dec[5] do
> Add(p1,LinearCombination(b,i));
> od;
```

Let us create the submodules `P1` $= P_1$ and `P2` $= 3P_2$ via the bases `p1` and `p2`:

(5)
```
gap> P1:=Subspace(A,p1);
<vector space over GF(5), with 5 generators>
gap> P2:=Subspace(A,p2);
<vector space over GF(5), with 30 generators>
```

Now we deal with the block B_1. We construct it by merging the bases `p1` and `p2`:

```
gap> b1:=[];;
gap> Append(b1,p1);Append(b1,p2);
gap> B1:=Subspace(A,b1);
<vector space over GF(5), with 35 generators>
gap> B:=Basis(B1,b1);;
```

The last command is a technical necessity and ensures that `GAP` is able to compute coefficients with respect to the basis of `B1`. Next we define the block idempotent ε_{B_1} according to (3.6a). `GAP` represents the elements of a finite field $\mathbb{F}_q$ by choosing a generator for the cyclic group of unit elements. In our case $q = 5$, `0*Z(5)` $= 0$ and $<$ `Z(5)` $>= \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. We use addition instead of multiplication in the finite field to facilitate recognizing the formula (3.6a) for the block idempotent.

(6)
```
gap> e:=()^o;;
gap> for i in ConjugacyClass(G,(1,2)(3,4)) do
> e:=e+i^o+i^o;
> od;
```

```
gap> for i in ConjugacyClass(G,(1,2,3)) do
> e:=e+i^o+i^o+i^o;
> od;
gap> e in B1;
true
```

The last line verifies that `e` $= \varepsilon_{B_1}$ indeed lies in the block `B1` $= B_1$. We are now ready to compute the coefficients of the block idempotent with respect to the basis `B`:

(7)
```
gap> coef:=Coefficients(B,e);
[ Z(5)^3, 0*Z(5), 0*Z(5), 0*Z(5), 0*Z(5), Z(5)^2, Z(5)^2, 0*Z(5),
  0*Z(5), Z(5)^0, 0*Z(5), Z(5)^2, Z(5), 0*Z(5), Z(5)^0, Z(5)^2,
  Z(5)^2, 0*Z(5), 0*Z(5), 0*Z(5), Z(5)^2, Z(5)^3, Z(5)^3, Z(5)^0,
  0*Z(5), 0*Z(5), Z(5)^2, Z(5)^2, 0*Z(5), 0*Z(5), Z(5)^2, 0*Z(5),
  Z(5)^0, Z(5), Z(5)^0 ]
```

In the list `coef` the first 5 elements correspond to the basis of the subspace `P1`, the other to the basis of the subspace `P2`. Let us now compute the idempotents:

(8)
```
gap> x:=()^o-()^o;;
gap> y:=x;;
gap> for i in [1..5] do
> x:=x+coef[i]*B[i];
> od;
gap> for i in [6..35] do
> y:=y+coef[i]*B[i];
> od;
```

We want to check that we have indeed found a set of primitive orthogonal idempotents for the block B_1, i.e., the following must hold: $e_\varphi^2 = e_\varphi$ for $\varphi \in \mathrm{IBr}_p(B_1)$, $e_\varphi e_\psi = e_\psi e_\varphi = 0$ for $\varphi, \psi \in \mathrm{IBr}_p(B_1), \varphi \neq \psi$ and $\sum_{\varphi \in \mathrm{IBr}_p(B_1)} = \varepsilon_{B_1}$:

(9)
```
gap> x*x=x;
true
gap> y*y=y;
true
gap> x*y; y*x;
<zero> of ...
<zero> of ...
```

```
gap> x+y=e;
true
gap> P1=RightIdeal(A,[x]);
true
gap> P2=RightIdeal(A,[y]);
true
```

The last two commands check that the idempotents `x` and `y` indeed generate the subspaces `P1` and `P2` as right ideals.

Thus, we have found the primitive orthogonal idempotents in characteristic 5. The computations in characteristic 2 and 3 are analogous, and we state all results in the following

Theorem 3.3.1 (Primitive orthogonal idempotents)**.** *Let $G = A_5$ be the Alternating group on five symbols and (K, R, k) be the p-modular system for G defined in section* 3.1.2*. Then the primitive orthogonal idempotents corresponding to the PIMs P_φ for $\varphi \in \mathrm{IBr}_p(G)$ in decomposition* (3.14) *are*

(i) $p = 2$*:*

$$\begin{aligned} e_{\varphi_1} &= \mathrm{id} + (345) + (354) + (123) + (12345) + (12354) + (12453) + (124) \\ &\quad + (12435) + (12543) + (125) + (12534) + (132) + (13452) + (13542) \\ &\quad + (14532) + (142) + (14352) + (15432) + (152) + (15342) \\ e_{\varphi_2} &= (245) + (24)(35) + (254) + (25)(34) + (124) + (12435) + (125) \\ &\quad + (12534) + (132) + (13542) + (134) + (135) + (13)(25) + (13254) \\ &\quad + (14523) + (14)(23) + (14253) + (14)(25) + (15432) + (15342) \\ &\quad + (154) + (15)(34) + (15423) + (15234) \\ e_{\varphi_3} &= (234) + (235) + (243) + (24)(35) + (253) + (25)(34) + (124) \\ &\quad + (12435) + (125) + (12534) + (132) + (13542) + (13245) + (13524) \\ &\quad + (13)(25) + (13425) + (143) + (145) + (14)(23) + (14235) + (14325) \\ &\quad + (14)(25) + (15432) + (15342) + (153) + (15)(34) + (15243) + (15324) \\ e_{\varphi_4} &= \mathcal{C}_3^+ + \mathcal{C}_4^+ + \mathcal{C}_5^+ \end{aligned}$$

Note that $e_{\varphi_4} = \varepsilon_{B_2}$, the block idempotent of the defect-zero block B_2.

(ii) $p = 3$:

$$
\begin{aligned}
e_{\varphi_1} = {} & \mathrm{id} + \overline{2}(345) + \overline{2}(354) + (23)(45) + \overline{2}(234) + \overline{2}(235) + \overline{2}(243) + \overline{2}(245) \\
& + (24)(35) + \overline{2}(253) + \overline{2}(254) + (25)(34) + \overline{2}(12)(35) + \overline{2}(12345) + \overline{2}(124) \\
& + \overline{2}(12543) + \overline{2}(13452) + \overline{2}(135) + \overline{2}(13)(24) + \overline{2}(13254) + \overline{2}(142) + \overline{2}(14)(35) \\
& + \overline{2}(14523) + \overline{2}(14325) + \overline{2}(15432) + \overline{2}(153) + \overline{2}(15234) + \overline{2}(15)(24) \\
e_{\varphi_2} = {} & (345) + (354) + (234) + (235) + (243) + (245) + (253) + (254) + (12)(45) \\
& + (12)(34) + \overline{2}(12)(35) + \overline{2}(12345) + (12354) + (12453) + (124) + (12435) \\
& + \overline{2}(12543) + (12534) + \overline{2}(13452) + (13542) + (13)(45) + (135) + \overline{2}(13)(24) \\
& + (13245) + (13524) + (13)(25) + \overline{2}(13254) + (13425) + (14532) + (142) \\
& + (14352) + \overline{2}(14)(35) + \overline{2}(14523) + (14)(23) + (14235) + (14253) + \overline{2}(14325 \\
& + (14)(25) + \overline{2}(15432) + (15342) + (153) + (15)(34) + (15423) + (15)(23) \\
& + \overline{2}(15234) + (15243) + (15324) + \overline{2}(15)(24) \\
e_{\varphi_3} = {} & \mathcal{C}_2^+ + 2a\mathcal{C}_4^+ + 2\bar{a}\mathcal{C}_5^+ \\
e_{\varphi_4} = {} & \mathcal{C}_2^+ + 2\bar{a}\mathcal{C}_4^+ + 2a\mathcal{C}_5^+
\end{aligned}
$$

Again, $e_{\varphi_3} = \varepsilon_{B_2}$ and $e_{\varphi_4} = \varepsilon_{B_3}$, and both blocks B_2 and B_3 are blocks of defect zero.

(iii) $p = 5$:

$$
\begin{aligned}
e_{\varphi_1} = {} & \overline{3}\,\mathrm{id} + \overline{3}(345) + \overline{3}(354) + \overline{3}(23)(45) + \overline{3}(234) + \overline{3}(235) + \overline{3}(243) + \overline{3}(245) \\
& + \overline{3}(24)(35) + \overline{3}(253) + \overline{3}(254) + \overline{3}(25)(34) \\
e_{\varphi_2} = {} & \overline{3}\,\mathrm{id} + \overline{4}(23)(45) + \overline{4}(24)(35) + \overline{4}(25)(34) + \overline{2}(12)(45) + \overline{2}(12)(34) + \overline{2}(12)(35) \\
& + \overline{3}(123) + \overline{3}(124) + \overline{3}(125) + \overline{3}(132) + \overline{2}(13)(45) + \overline{3}(134) + \overline{3}(135) + \overline{2}(13)(24) \\
& + \overline{2}(13)(25) + \overline{3}(142) + \overline{3}(143) + \overline{3}(145) + \overline{2}(14)(35) + \overline{2}(14)(23) + \overline{2}(14)(25) \\
& + \overline{3}(152) + \overline{3}(153) + \overline{3}(154) + \overline{2}(15)(34) + \overline{2}(15)(23) + \overline{2}(15)(24) \\
e_{\varphi_3} = {} & \overline{3}\mathcal{C}_2^+ + \overline{2}\mathcal{C}_3^+
\end{aligned}
$$

As before, $e_{\varphi_3} = \varepsilon_{B_2}$ is the block idempotent of the defect-zero block B_2.

Remark. Let us stress that a primitive orthogonal idempotent in kG corresponding to a PIM P generates the subspace which consists of the direct sum of all submodules isomorphic to P. For example, in characteristic 3 we have $kGe_{\varphi_2} = 4P_2$ for the primitive orthogonal idempotent e_{φ_2} corresponding to the PIM P_2.

3.3.2. Radical series of the PIMs

Since the regular representation module ${}_{kG}kG$ has finite length by Proposition 1.1.4, the radical series $P \geq \operatorname{rad} P \geq \operatorname{rad}^2 P \geq ... \geq \operatorname{rad}^k P = 0$ of the PIM P defined in Definition 1.1.23 in Section 1.1.2 is finite. In this subsection we are going to compute the radical series by using the program `GAP`. Again, we will use the package **`reps`** by Peter Webb. The computation consists of the following steps:

(1) Initialize the necessary objects.

(2) Decompose the regular representation using `Decompose` from the `GAP`-package **`reps`** and identify the correct PIM P_i of decomposition (3.19).

(3) Compute the radical $\operatorname{rad} P_i$ using the package **`reps`**.

(4) Repeat step (3) until $\operatorname{rad}^k P_i = 0$.

Analogously to the computation of the idempotents in 3.3.1, we are going to investigate the case $\operatorname{char} k = 5$ and only state the results for $\operatorname{char} k = 2, 3$. As we saw in Section 3.2.3 and in (3.21), we have to investigate the PIMs P_1 and P_2 in characteristic 5. Let us first prepare the necessary objects:

(1)
```
gap> G:=AlternatingGroup(5);;
gap> Read("/home/felix/reps");
gap> R:=RegularRep(G,GF(5));;
```

(2) Once again we use the command `Decompose` from the package **`reps`** to decompose the regular representation into direct summands. We already know from Subsection 3.3.1 that the fifth entry corresponds to P_1 with $\dim \operatorname{soc}(P_1) = 1$.

```
gap> dec:=Decompose(R);;
gap> List(dec,x->Size(x));
[ 5, 5, 5, 10, 5, 10, 10, 10 ]
gap> P1:=SubmoduleRep(R,dec[5]);;
gap> S1:=SubmoduleRep(P1,SocleRep(P1));;
gap> S1.dimension;
1
```

(3) Now we compute the radical of P_1, which is provided by the command `RadicalRep` from **`reps`** and essentially uses the Meataxe algorithm.[12]

[12] Computing the radical can also be achieved by using an equivalent command already implemented in GAP.

```
gap> radP1:=SubmoduleRep(P1,RadicalRep(P1));;
gap> radP1.dimension;
4
```

(4) To produce the radical series we iterate this process and compute $\operatorname{rad}^2 P_1$:

```
gap> rad2P1:=SubmoduleRep(radP1,RadicalRep(radP1));;
gap> rad2P1.dimension;
1
gap> rad2P1=S1;
true
```

We see that $\operatorname{rad}^2 P_1 = \operatorname{soc} P_1$. Since $\operatorname{rad}\operatorname{soc} P_1 = 0$, the radical series ends with the second term.

For the other PIM P_2 of the block B_1 we repeat step 3 and 4. We may choose any of the three copies of P_2 with dimension 10 (recall that P_2 has multiplicity 3) which we already identified in Subsection 3.3.1.

```
gap> P2:=SubmoduleRep(R,dec[4]);;
gap> S2:=SubmoduleRep(P2,SocleRep(P2));;
gap> S2.dimension;
3
gap> radP2:=SubmoduleRep(P2,RadicalRep(P2));;
gap> radP2.dimension;
7
gap> rad2P2:=SubmoduleRep(radP2,RadicalRep(radP2));;
gap> rad2P2.dimension;
3
gap> rad2P2=S2;
true
```

The radical series terminates at the fourth term since $\operatorname{rad}^2 P_2 = \operatorname{soc} P_2$; therefore, $\operatorname{rad}^3 P_2 = 0$. We have thus found the radical series for the PIMs P_1 and P_2 in characteristic 5, which are shown in Table 3.12.

By comparing the dimensions of the factors in the radical series for P_2 (which are 3, 4 and 3) with the entries in the Cartan matrix C_5 in (3.13) we see that the radical series is not a composition series for P_2.

	$P_1 \geq$	$\operatorname{rad} P_1 \geq$	$\operatorname{rad}^2 P_1 \geq$	(0)
dim	5	4	1	
	$P_2 \geq$	$\operatorname{rad} P_2 \geq$	$\operatorname{rad}^2 P_2 \geq$	(0)
dim	10	7	3	

Table 3.12.: Radical series of the PIMs in characteristic 5

We list the radical series for the PIMs in characteristic 2 and 3 in Table 3.13 and 3.14 respectively. Note that for $p = 2$, the PIMs P_2 and P_3 are conjugate; therefore, their radical series are isomorphic by Proposition A.2.2(ii).

	$P_1 \geq$	$\operatorname{rad} P_1 \geq$	$\operatorname{rad}^2 P_1 \geq$	$\operatorname{rad}^3 P_1 \geq$	$\operatorname{rad}^4 P_1 \geq$	(0)
dim	12	11	7	5	1	
	$P_2 \geq$	$\operatorname{rad} P_2 \geq$	$\operatorname{rad}^2 P_2 \geq$	$\operatorname{rad}^3 P_2 \geq$	$\operatorname{rad}^4 P_2 \geq$	(0)
dim	8	6	5	3	2	

Table 3.13.: Radical series of the PIMs in characteristic 2

	$P_1 \geq$	$\operatorname{rad} P_1 \geq$	$\operatorname{rad}^2 P_1 \geq$	(0)
dim	6	5	1	
	$P_2 \geq$	$\operatorname{rad} P_2 \geq$	$\operatorname{rad}^2 P_2 \geq$	(0)
dim	9	5	4	

Table 3.14.: Radical series of the PIMs in characteristic 3

A. Results from ordinary representation theory

A.1. Linear characters

Definition A.1.1. Let G be a finite group. A linear character is a representation $\chi : G \longrightarrow K$ of degree 1.

Proposition A.1.2. *Let G be a finite group, K a splitting field for G and $[G, G]$ be the commutator subgroup generated by the commutators $aba^{-1}b^{-1}$ with $a, b \in G$. Then the linear characters of G and its abelianization $G^{\mathrm{ab}} = G/[G, G]$ are in 1:1-correspondence. The number of linear characters of G equals the index $[G : [G, G]]$ of the commutator subgroup $[G, G]$ in G.*

Proof. Suppose that χ^{ab} is a linear character of G^{ab}. Define $\chi(g) := \chi^{\mathrm{ab}}(g[G, G])$ for $g \in G$ and observe that

$$\chi(gh) = \chi^{\mathrm{ab}}(gh[G, G]) = \chi^{\mathrm{ab}}(g[G, G])\chi^{\mathrm{ab}}(h[G, G]) = \chi(g)\chi(h)$$

for all $g, h \in G$; hence, χ is a linear character of G. Conversely, suppose that χ is a linear character of G and define $\chi^{\mathrm{ab}}(g[G, G]) = \chi(g)$ for $g \in G$. We have to check that χ^{ab} is well defined, that is, $\chi(x) = 1$ for $x \in [G, G]$:

$$\chi(ghg^{-1}h^{-1}) = \chi(g)\chi(h)\chi(g)^{-1}\chi(h)^{-1} = 1 \quad \text{for } g, h \in G$$

The last equality sign holds since χ is a linear character, which implies that its values in K commute.

We have thus established a 1:1-correspondence between linear characters of G and G^{ab}. Since G^{ab} is abelian and K is a splitting field for G, the number of linear characters equals its order, which is the index of $[G, G]$ in G. □

A.2. Conjugate representations

Let A be a K-algebra and L/K be a Galois extension with Galois group $\mathrm{Gal}(L/K)$. For a K-basis $\{a_1, \dots, a_m\}$ of A and $\sigma \in \mathrm{Gal}(L/K)$ define the ring automorphism

$$\begin{aligned} \sigma \otimes \mathrm{id} : A_L &\longrightarrow A_L \\ l \otimes a_i &\longmapsto \sigma(l) \otimes a_i \end{aligned}$$

Note that $(\sigma \otimes \mathrm{id})(\lambda x) = \sigma(\lambda)(\sigma \otimes \mathrm{id})(x)$ for $\lambda \in L$ and $x \in A_L$; hence, $\sigma \otimes \mathrm{id}$ is not an algebra automorphism of A_L. We can now define the action of a Galois automorphism $\sigma \in \mathrm{Gal}(L/K)$ on representations and their corresponding modules:

Definition A.2.1 (Conjugate representations and conjugate modules)**.**

(i) For a matrix representation $\rho : A_L \to M_n(L)$ the conjugate representation ${}^{\sigma}\rho$ is defined by
$${}^{\sigma}\rho = \sigma_{M_n(L)} \circ \rho \circ (\sigma^{-1} \otimes \mathrm{id})$$
where the matrix $\sigma_{M_n(L)}(A)$ is obtained by applying σ to the entries of $A \in M_n(L)$.

(ii) If the A_L-module M affords the representation ρ, the conjugate module ${}^{\sigma}M$ is defined as the A_L-module affording the conjugate representation ${}^{\sigma}\rho$.

Remark. Note that in the case of a group algebra KG and a Galois extension L/K, the ring automorphism $\sigma^{-1} \otimes \mathrm{id}$ acts trivially on $g \in LG$. Therefore, ${}^{\sigma}\rho = \sigma_{M_n(L)} \circ \rho$ on LG.

We immediately get the following properties of conjugate representations and modules:

Proposition A.2.2. *Let M be a A_L-module and $\sigma, \tau \in \mathrm{Gal}(L/K)$:*

(i) ${}^{\tau}({}^{\sigma}M) = {}^{\tau\sigma}M$

(ii) *M is simple if and only if ${}^{\sigma}M$ is simple. Thus, the conjugacy operation ${}^{\sigma}$ permutes the simple A_L-modules.*

(iii) *Let $A = KG$ be the group algebra, L/K a Galois extension, $\sigma \in \mathrm{Gal}(L/K)$ a Galois automorphism and $\rho : G \longrightarrow \mathrm{GL}_n(L)$ a representation of G. Then for all $g \in G$ we have ${}^{\sigma}\rho(g) = \sigma_{M_n(L)}(\rho(g))$. That is, the conjugate representation is obtained by applying the Galois automorphism to the entries of the representation matrices.*

Proof. Properties (i)-(iii) follow immediately from Definition A.2.1. □

B. Collected results

The following pages provide an uncommented summary of the results from Chapter 3. For an explanation of the denotations used, see the respective sections in that chapter. We set $a = \frac{1}{2}(1+\sqrt{5})$ and $\bar{a} = \frac{1}{2}(1-\sqrt{5})$.

Blocks

$$
\begin{array}{lll}
p = 2: & \mathrm{Irr}(B_1) = \{\chi_1, \chi_2, \chi_3, \chi_5\} & \varepsilon_{B_1} = \mathcal{C}_1^+ + \mathcal{C}_3^+ + \mathcal{C}_4^+ + \mathcal{C}_5^+ \\
 & \mathrm{Irr}(B_2) = \{\chi_4\} & \varepsilon_{B_2} = \mathcal{C}_3^+ + \mathcal{C}_4^+ + \mathcal{C}_5^+ \\
p = 3: & \mathrm{Irr}(B_1) = \{\chi_1, \chi_4, \chi_5\} & \varepsilon_{B_1} = \mathcal{C}_1^+ + \mathcal{C}_2^+ + \mathcal{C}_4^+ + \mathcal{C}_5^+ \\
 & \mathrm{Irr}(B_2) = \{\chi_2\} & \varepsilon_{B_2} = \mathcal{C}_2^+ + 2a\mathcal{C}_4^+ + 2\bar{a}\mathcal{C}_5^+ \\
 & \mathrm{Irr}(B_3) = \{\chi_3\} & \varepsilon_{B_3} = \mathcal{C}_2^+ + 2\bar{a}\mathcal{C}_4^+ + 2a\mathcal{C}_5^+ \\
p = 5: & \mathrm{Irr}(B_1) = \{\chi_1, \chi_2, \chi_3, \chi_4\} & \varepsilon_{B_1} = \mathcal{C}_1^+ + 2\mathcal{C}_2^+ + 3\mathcal{C}_3^+ \\
 & \mathrm{Irr}(B_2) = \{\chi_5\} & \varepsilon_{B_2} = 3\mathcal{C}_2^+ + 2\mathcal{C}_3^+
\end{array}
$$

Brauer character tables

$p = 2:$

	$\mathcal{C}_1$	$\mathcal{C}_3$	$\mathcal{C}_4$	$\mathcal{C}_5$
φ_1	1	1	1	1
φ_2	2	-1	$a-1$	$\bar{a}-1$
φ_3	2	-1	$\bar{a}-1$	$a-1$
φ_4	4	1	-1	-1

$p = 3:$

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_4$	$\mathcal{C}_5$
φ_1	1	1	1	1
φ_4	4	0	-1	-1
φ_2	3	-1	a	$\bar{a}$
φ_3	3	-1	$\bar{a}$	a

$p = 5:$

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$
φ_1	1	1	1
φ_2	3	-1	0
φ_3	5	1	-1

Decomposition matrices and Cartan matrices

$$D_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad D_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad D_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 4 & 2 & 2 & 0 \\ 2 & 2 & 1 & 0 \\ 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad C_3 = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad C_5 = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Structure of *kG*

$p = 2:$

PIMs	P_1	P_2	P_3	P_4
dim	12	8	8	4
dim(soc)	1	2	2	4

$p = 3:$

P_1	P_2	P_3	P_4
6	9	3	3
1	4	3	3

$p = 5:$

P_1	P_2	P_3
5	10	5
1	3	5

Lifting of PIMs from characteristic *p* to characteristic 0

$p = 2:$ $\quad KG \sim \partial_1 + 2\partial_2 + 2\partial_3 + 4\partial_4$ $\quad$ with

$$\partial_1 = \sigma_1 + \sigma_2 + \sigma_3 + \sigma_5$$
$$\partial_2 = \sigma_2 + \sigma_5$$
$$\partial_3 = \sigma_3 + \sigma_5$$
$$\partial_4 = \sigma_4$$

$p = 3:$ $\quad KG \sim \partial_1 + 4\partial_2 + 3\partial_3 + 3\partial_4$ $\quad$ with

$$\partial_1 = \sigma_1 + \sigma_5$$
$$\partial_2 = \sigma_4 + \sigma_5$$
$$\partial_3 = \sigma_2$$
$$\partial_4 = \sigma_3$$

$p = 5:$ $\quad KG \sim \partial_1 + 3\partial_2 + 5\partial_3$ $\quad$ with

$$\partial_1 = \sigma_1 + \sigma_4$$
$$\partial_2 = \sigma_2 + \sigma_3 + \sigma_4$$
$$\partial_3 = \sigma_5$$

Primitive orthogonal idempotents

Characteristic 2:

$$\begin{aligned}
e_{\varphi_1} &= \mathrm{id} + (345) + (354) + (123) + (12345) + (12354) + (12453) + (124) \\
&\quad + (12435) + (12543) + (125) + (12534) + (132) + (13452) + (13542) \\
&\quad + (14532) + (142) + (14352) + (15432) + (152) + (15342) \\
e_{\varphi_2} &= (245) + (24)(35) + (254) + (25)(34) + (124) + (12435) + (125) \\
&\quad + (12534) + (132) + (13542) + (134) + (135) + (13)(25) + (13254) \\
&\quad + (14523) + (14)(23) + (14253) + (14)(25) + (15432) + (15342) \\
&\quad + (154) + (15)(34) + (15423) + (15234) \\
e_{\varphi_3} &= (234) + (235) + (243) + (24)(35) + (253) + (25)(34) + (124) \\
&\quad + (12435) + (125) + (12534) + (132) + (13542) + (13245) + (13524) \\
&\quad + (13)(25) + (13425) + (143) + (145) + (14)(23) + (14235) + (14325) \\
&\quad + (14)(25) + (15432) + (15342) + (153) + (15)(34) + (15243) + (15324) \\
e_{\varphi_4} &= \mathcal{C}_3^+ + \mathcal{C}_4^+ + \mathcal{C}_5^+
\end{aligned}$$

Characteristic 3:

$$\begin{aligned}
e_{\varphi_1} &= \mathrm{id} + \overline{2}(345) + \overline{2}(354) + (23)(45) + \overline{2}(234) + \overline{2}(235) + \overline{2}(243) + \overline{2}(245) \\
&\quad + (24)(35) + \overline{2}(253) + \overline{2}(254) + (25)(34) + \overline{2}(12)(35) + \overline{2}(12345) + \overline{2}(124) \\
&\quad + \overline{2}(12543) + \overline{2}(13452) + \overline{2}(135) + \overline{2}(13)(24) + \overline{2}(13254) + \overline{2}(142) + \overline{2}(14)(35) \\
&\quad + \overline{2}(14523) + \overline{2}(14325) + \overline{2}(15432) + \overline{2}(153) + \overline{2}(15234) + \overline{2}(15)(24) \\
e_{\varphi_2} &= (345) + (354) + (234) + (235) + (243) + (245) + (253) + (254) + (12)(45) \\
&\quad + (12)(34) + \overline{2}(12)(35) + \overline{2}(12345) + (12354) + (12453) + (124) + (12435) \\
&\quad + \overline{2}(12543) + (12534) + \overline{2}(13452) + (13542) + (13)(45) + (135) + \overline{2}(13)(24) \\
&\quad + (13245) + (13524) + (13)(25) + \overline{2}(13254) + (13425) + (14532) + (142) \\
&\quad + (14352) + \overline{2}(14)(35) + \overline{2}(14523) + (14)(23) + (14235) + (14253) + \overline{2}(14325 \\
&\quad + (14)(25) + \overline{2}(15432) + (15342) + (153) + (15)(34) + (15423) + (15)(23) \\
&\quad + \overline{2}(15234) + (15243) + (15324) + \overline{2}(15)(24) \\
e_{\varphi_3} &= \mathcal{C}_2^+ + 2a\mathcal{C}_4^+ + 2\bar{a}\mathcal{C}_5^+ \\
e_{\varphi_4} &= \mathcal{C}_2^+ + 2\bar{a}\mathcal{C}_4^+ + 2a\mathcal{C}_5^+
\end{aligned}$$

Characteristic 5:

$$\begin{aligned}
e_{\varphi_1} &= \overline{3}\,\mathrm{id} + \overline{3}(345) + \overline{3}(354) + \overline{3}(23)(45) + \overline{3}(234) + \overline{3}(235) + \overline{3}(243) + \overline{3}(245) \\
&\quad + \overline{3}(24)(35) + \overline{3}(253) + \overline{3}(254) + \overline{3}(25)(34) \\
e_{\varphi_2} &= \overline{3}\,\mathrm{id} + \overline{4}(23)(45) + \overline{4}(24)(35) + \overline{4}(25)(34) + \overline{2}(12)(45) + \overline{2}(12)(34) + \overline{2}(12)(35) \\
&\quad + \overline{3}(123) + \overline{3}(124) + \overline{3}(125) + \overline{3}(132) + \overline{2}(13)(45) + \overline{3}(134) + \overline{3}(135) + \overline{2}(13)(24) \\
&\quad + \overline{2}(13)(25) + \overline{3}(142) + \overline{3}(143) + \overline{3}(145) + \overline{2}(14)(35) + \overline{2}(14)(23) + \overline{2}(14)(25) \\
&\quad + \overline{3}(152) + \overline{3}(153) + \overline{3}(154) + \overline{2}(15)(34) + \overline{2}(15)(23) + \overline{2}(15)(24) \\
e_{\varphi_3} &= \overline{3}\mathcal{C}_2^+ + \overline{2}\mathcal{C}_3^+
\end{aligned}$$

Radical series of the PIMs

$p = 2:$

	P_1	$\geq \operatorname{rad} P_1$	$\geq \operatorname{rad}^2 P_1$	$\geq \operatorname{rad}^3 P_1$	$\geq \operatorname{rad}^4 P_1$	$\geq (0)$
dim	12	11	7	5	1	
	P_2	$\geq \operatorname{rad} P_2$	$\geq \operatorname{rad}^2 P_2$	$\geq \operatorname{rad}^3 P_2$	$\geq \operatorname{rad}^4 P_2$	$\geq (0)$
dim	8	6	5	3	2	

$p = 3:$

	P_1	$\geq \operatorname{rad} P_1$	$\geq \operatorname{rad}^2 P_1$	$\geq (0)$
dim	6	5	1	
	P_2	$\geq \operatorname{rad} P_2$	$\geq \operatorname{rad}^2 P_2$	$\geq (0)$
dim	9	5	4	

$p = 5:$

P_1	$\geq \operatorname{rad} P_1$	$\geq \operatorname{rad}^2 P_1$	$\geq (0)$
5	4	1	
P_2	$\geq \operatorname{rad} P_2$	$\geq \operatorname{rad}^2 P_2$	$\geq (0)$
10	7	3	

List of Tables

Bibliography

[Alp86] Jonathan L. Alperin. *Local Representation Theory.* Cambridge University Press, Cambridge, New York, Melbourne, 1986.

[AM69] Michael F. Atiyah and Ian G. MacDonald. *Introduction to Commutative Algebra.* Addison-Wesley Publishing Company, Reading, Menlo Park, London, Don Mills, 1969.

[Bur65] Martin Burrow. *Representation Theory of Finite Groups.* Academic Press Inc., New York, 1965.

[CR62] Charles W. Curtis and Irving Reiner. *Representation Theory of Finite Groups and Associative Algebras.* John Wiley & Sons, New York, London, Sydney, 1962.

[CR81] Charles W. Curtis and Irving Reiner. *Methods of Representation Theory - with Applications to Finite Groups and Orders.* John Wiley & Sons, New York, Chichester, Brisbane, Toronto, 1981.

[Cur99] Charles W. Curtis. *Pioneers of Representation Theory: Frobenius, Burnside, Schur, and Brauer.* American Mathematical Society, Providence, 1999.

[DP77] John D. Dixon and B.M. Puttaswamaiah. *Modular Representations of Finite Groups.* Academic Press Inc., New York, San Francisco, London, 1977.

[HR94] Derek F. Holt and Sarah Rees. Testing modules for irreducibility. *Journal of the Australian Mathematical Society (Series A)*, 57(1):1–16, 1994.

[JS06] Jens Carsten Jantzen and Joachim Schwermer. *Algebra.* Springer, Berlin, Heidelberg, 2006.

[LP10] Klaus Lux and Herbert Pahlings. *Representations of Groups - a Computational Approach.* Cambridge University Press, Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, Sao Paulo, Delhi, Dubai, Tokyo, 2010.

[Ser77] Jean-Pierre Serre. *Linear Representations of Finite Groups.* Springer, New York, Berlin, Heidelberg, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 1977.

[Ser79] Jean-Pierre Serre. *Local Fields.* Springer, New York, Heidelberg, Berlin, 1979.

[Wei03] Steven H. Weintraub. *Representation Theory of Finite Groups: Algebra and Arithmetic.* American Mathematical Society, Providence, Rhode Island, 2003.

Abstract (German)

In dieser Arbeit werden die prinzipal unzerlegbaren Darstellungen der alternierenden Gruppe in fünf Symbolen in modular Charakteristik bestimmt. Wir ermitteln die irreduziblen modularen Darstellungen und die mod p-Reduktionen der irreduziblen Darstellungen in Charakteristik 0 und berechnen mit Hilfe dieser Resultate ein System von primitiven orthogonalen Idempotenten.

Das erste Kapitel stellt die algebraischen Resultate bereit, die für die Entwicklung der modularen Darstellungstheorie notwendig sind, darunter Moduln endlicher Länge, das Radikal eines Moduls und die prinzipal unzerlegbaren Moduln von Algebren über einem Körper. Das Kapitel schließt mit einer kurzen Behandlung projektiver und injektiver Moduln über Gruppenalgebren und erläutert den Meataxe-Algorithmus, der Moduln bezüglich Einfachheit testet.

Kapitel 2 führt die wichtigsten Konzepte der modularen Darstellungstheorie ein: p-modulare Systeme, Brauercharaktere, Zerlegungszahlen und Cartanzahlen. Weiters werden die modularen Orthogonalitätsrelationen für Brauercharaktere bewiesen. Der letzte Abschnitt ist einer kurzen Einführung in Blocktheorie gewidmet.

Das dritte Kapitel benutzt die Resultate der vorherigen Kapitel zur Bestimmung der prinzipal unzerlegbaren Darstellungen der alternierenden Gruppe in fünf Symbolen in Charakteristik 2, 3 und 5. Dazu berechnen wir die Blockzerlegung und die Blockidempotenten der Gruppenalgebra kG, die Brauercharaktertafeln, die Zerlegungszahlen und die Cartanzahlen. Diese Resultate beinhalten schon wesentliche Informationen über die Struktur der Gruppenalgebra und ihre prinzipal unzerlegbaren Moduln. Der letzte Schritt ist die Berechnung eines Systems von primitiven orthogonalen Idempotenten unter Verwendung der bisher gewonnen Ergebnisse aus der Darstellungstheorie der A_5, wobei das Computeralgebrasystem `GAP` als Hilfsmittel dient. In diesem Zusammenhang ermitteln wir auch die mod p-Reduktionen der irreduziblen Darstellungen in Charakteristik 0 und die Radikalreihen der PIMs.

Abstract (English)

This thesis determines the principal indecomposable representations of the Alternating group on five symbols in modular characteristic. We calculate the irreducible modular representations and the mod p-reductions of the irreducible representations in characteristic 0 and use these results to compute a system of primitive orthogonal idempotents.

The first chapter provides the algebraic results needed to develop modular representation theory. After covering modules of finite lengths and the radical of a module, it examines the principal indecomposable modules of algebras over a field. We also give an account of projective and injective modules over group algebras. The chapter concludes with a discussion of the Meataxe algorithm, which tests modules for simplicity.

Chapter 2 treats the most important concepts of modular representation theory: p-modular systems, Brauer characters, Cartan numbers and decomposition numbers. Furthermore, we prove the modular orthogonality relations for Brauer characters. The last section is dedicated to a short introduction to block theory.

The third chapter uses the results developed in the previous chapters to determine the principal indecomposable representations of the Alternating group on five symbols in characteristic 2, 3 and 5. To this end, we calculate the block decomposition and block idempotents of the group algebra kG, the Brauer character tables, the decomposition numbers and the Cartan numbers. These results already encode a great deal of information about the group algebra and its principal indecomposable modules. As a last step we compute a system of primitive orthogonal idempotents on the basis of the results from representation theory of the group A_5, using the computer algebra system `GAP` to carry out the actual computations. In this context we also determine the mod p-reductions of the irreducible representations in characteristic 0 and the radical series of the PIMs.

Curriculum Vitae

Personal information

Name	Felix Leditzky
Date of birth	29.08.1986
Nationality	Austria

Education

Since 10/2006	Diploma studies in Mathematics at the University of Vienna, Austria
Since 10/2006	Diploma studies in Physics at the University of Vienna, Austria
06/2005	Matura (with distinction)
09/1997 – 06/2005	GRg 19, Billrothstraße 26-30, 1190 Vienna, Austria
09/1993 – 06/1997	VS 9, Galileigasse 5, 1090 Vienna, Austria