Department of Mathematics

M4R Project

Modular Representation Theory

Haiping Yang
CID: 00827193

Supervised by
Prof. Alexander Ivanov

March 9, 2018

Abstract

We present the basics of the theory of modular representation theory of finite groups, mainly from a character theoretic point of view. We begin by exposing the relevant aspect of the theory of non-commutative algebra, then specialise to group algebras. Then, we use the results that we have built to relate modular representations with ordinary representations using the so called CDE triangle. We continue by analysing more properties of the CDE triangle, and by tensoring with a certain field K, we move the CDE triangle to the character theoretic level. We finish by providing some examples of modular character tables and prove a generalised version of Burnside's Theorem.

Contents

Introduction

The aim of this project is to introduce and study modular representation theory of finite groups, mainly from a character theoretic point of view. We assume some knowledge of commutative algebras and representations over $\mathbb{C}$. We will also assume some basic understanding of p-adic numbers.

In the first chapter, we develop enough module theoretic results so that we can use them in the following chapters. We firstly talk about what is special about representations over $\mathbb{C}$. It turns out the correct notion to use is called semisimplicity. We then define a measure of the failure to be semisimple, called the radical. We prove the generalised Maschke's Theorem, which tells us a necessary and sufficient condition on when the group algebra is semisimple. Then we prove the Brauer-Nebsitt's Theorem, which relates the number of irreducible representations with the number of p-regular conjugacy classes. Finally we prove the self-injectivity theorem for group algebras, and we use its corollaries in the following chapters.

In the second chapter, we start by introducing how to relate modular representations with regular representations. The tool we will use is called a $(0, p)$-ring for k. It is basically the ring of integers of some extension of $\mathbb{Q}_p$. Then there will be a mod map from ordinary representations to modular representations. By considering projectives, we can make this into a triangle and this is the so called CDE triangle. We will deal with the technical details of the triangle and show it is commutative. Due to the symmetry of the triangle, we will show two of the maps are 'dual' to each other. We continue by using the Brauer's Induction Theorems to show injectivity and surjectivity of the maps. We finish this chapter by tensoring the entire triangle with K, and hence obtain the triangle on the character theoretic level. We explicitly construct the vertices of the triangle to ease the abstraction, and use the injectivity and surjectivity of the maps to show what we constructed is the same as the tensored triangle. Finally we introduce orthogonality and p-defect then compute examples using the 'dual' maps and results from the previous chapter.

In the final chapter, we relate characters to blocks. We can show this is well-defined by using an equivalent notion of belonging to a block. By invoking ideas from central character theory and a stronger notion of orthogonality on blocks we prove a generalised version of Burnside's Theorem.

We mostly follow [Alp86], [Ser77], [Sch13] and [Fen15]. The most original parts of the report are the two proofs from Section 2.5.1 and examples from Section 2.5.2.

Some applications of representation theory over $\mathbb{R}$ and $\mathbb{C}$ can be found in physics, as it is very useful in quantum mechanics and particle physics. However, this application tends to go away in the positive characteristic case. Nonetheless, it is useful in other areas of mathematics.

Unsurprisingly, as we will see in the generalised Burnside's Theorem, modular representation theory was used in the classification of the finite simple groups. The proof of the Brauer-Suzuki Theorem [BS59] depends on the relationship between the ordinary and modular characters using the CDE triangle. Its generalisation, the Z^* Theorem [Gla66], another important result in finite simple groups, also depends on calculations on modular characters.

Results from modular representation theory also appear in geometry. For example, the Adams conjecture is about real vector bundles over CW complexes. But its proof in [Qui71] involves modular representation theory of the finite groups $\mathrm{GL}_n(\mathbb{F}_p)$ and $\mathrm{O}_n(\mathbb{F}_p)$. There are also uses of modular representation theory in number theory, for example in [Ser77, Ch. 19].

I would like to thank, in no particular order, the people who helped me along the way. I would like to thank my friends Thibault Décoppet, Bradley Doyle and Wen Cong (Isla) Lim for their help and feedback. I thank flatmates Adam Davies and Thomas Willers for their motivational support. I also thank Adrian Wong, Asad Chaudhary and Jeremy Wu for proof-reading. I would also like to thank my personal tutor Dr. John Britnell for his genuine help and support throughout the four years. Finally, I would like to thank my M4R supervisor Prof. Alexander Ivanov for providing leadership and guidance in my project.

Plagiarism Declaration: *This is my own unaided work unless stated otherwise.*

Chapter 1

Module Theoretic Approach

In this chapter, we will mainly follow chapters 1 and 2 in [Alp86], and sometimes we will switch to [Ben98a] for more high-tech machinery. We provide some basic definitions and properties, and will sometimes only sketch the proofs and leave others as facts. Throughout, all modules will be finitely generated (f.g.) and all groups will be finite. We sometimes drop the word left/right for modules if it doesn't cause confusion and the property holds in both cases. And if the ring is obvious, we just say 'a module' without mentioning the specific ring.

1.1 Basic Definitions

Definition 1.1.1. The *group algebra* of a finite group G over a field k is defined as $k[G] = \{\sum_{g\in G} a_g g, a_g \in k\}$, with multiplication generated by $g \cdot h = gh$.

Remark 1.1.2. Since G is finite, we see that $k[G]$ is finite dimensional as a vector space over k, therefore it is Artinian (both left and right) as a ring/algebra over k.

Definition 1.1.3.

1. A module is *simple/irreducible* if there are no submodules other than the trivial module $\{0\}$ or itself;
2. A module is *indecomposable* if it can not be written as a direct sum of proper submodules.

We note that irreducible implies indecomposable.

Recall that if A is a ring, M is an A-module and N is an A-submodule of M. Then M is Noetherian (Artinian) if and only if N and M/N are Noetherian (respectively Artinian). As a corollary, any f.g. A-module is Noetherian (respectively Artinian), since it is the quotient of a f.g. free A-module $A^{\oplus n}$, then do induction on n. We also recall the following proposition.

Proposition 1.1.4. For an A-module M the following conditions are equivalent:

1. The module M is both Noetherian and Artinian;
2. The module M has a composition series.

Combine with the next theorem, we see every f.g. module over an Artinian ring has a composition series.

Theorem 1.1.5. Left (respectively right) Artinian implies left (respectively right) Noetherian.

Remark 1.1.6. Since every f.g. module over our group algebra is a homomorphic image of some free module, and that if M is simple, then any non-zero element of M is a generator, so M is a homomorphic image of the $k[G]$ module $k[G]$. And this implies that there are only finitely many simple $k[G]$ modules, up to isomorphism, as the $k[G]$ module $k[G]$ has a composition series of finite length and any simple module is a composition factor.

Definition 1.1.7. A module M is *semisimple* if the following equivalent conditions hold:

1. M is a direct sum of simple modules;
2. Every submodule of M is a direct summand.

An algebra is called semisimple if it is semisimple as a module over itself.

Proposition 1.1.8. If A is semisimple as an algebra, then all modules over A are semisimple.

Proof. ($\Longleftarrow$) This is obvious by definition.
($\Longrightarrow$) We know that a direct sum of semisimple modules is semisimple so any free A-module is semisimple. But any (f.g.) module is a quotient of a free module, so we just need to show quotients of semisimple modules are semisimple. Let Q be a quotient of the semisimple module M, with quotient map $\pi : M \to Q$. Then $ker\pi$ has a complement by semisimplicity of M, which is isomorphic to Q via π. So we need to show any submodule of a semisimple module is semisimple. Let $N \subset M$ be a submodule of a semisimple module. If $U \subset N$, then we have $M = U \oplus V$ by semisimplicity of M. Therefore, $N \cong U \oplus (V \cap N)$. □

Remark 1.1.9. We just proved that submodules and quotient modules of semisimple modules are semisimple.

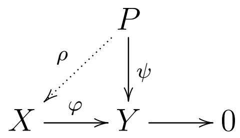
One obvious goal is to decompose a group algebra into a direct sum of indecomposable submodules. In order to do that, we will introduce the notion of projective modules.

Definition 1.1.10. An A module P is said to be *projective* if the following equivalent conditions hold:

1. P is a direct summand of a free module;
2. If φ is a surjective homomorphism from N to P, then the kernel of φ is a direct summand of N; (i.e., every surjection to P has a section)

3. If φ is a surjective homomorphism from X to Y and ψ is a homomorphism from P to Y, then $\exists\ \rho : P \to X$ such that $\varphi \circ \rho = \psi$. (defining property)

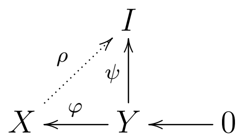
The defining property can be captured into the following commutative diagram.



Similarly, we can define the dual notion of projectivity, the injective modules.

Definition 1.1.11. An A module I is said to be *injective* if the following equivalent conditions hold:

1. If φ is a injective homomorphism from I to N, then the image of φ is a direct summand of N; (i.e., every injection from I has a retract)
2. If φ is a injective homomorphism from Y to X and ψ is a homomorphism from Y to I, then $\exists\ \rho : X \to I$ such that $\varphi \circ \rho = \psi$. (defining property)



We will show later that for group algebras, a module is injective if and only if it is projective.

All omitted proofs can be found in [AM69] and [Lan02].

1.2 Radical and Socle

Not every algebra is semisimple. For example, $\mathbb{F}_2[C_2]$ is not, it has the trivial module as a submodule, but there is no complement for it (see the next section for more discussion on this). We want to measure how much an algebra fails to be semisimple.

Definition 1.2.1. We define the *radical* of A to be $\mathrm{Rad}(A) = \{x \mid x \cdot S = 0$ for all simple modules $S\}$.

We note that if A is semisimple, then $\mathrm{Rad}(A) = 0$. And it is a two-sided ideal of A.

Theorem 1.2.2. The following conditions are equivalent to $\mathrm{Rad}(A)$:

1. The largest nilpotent (two-sided) ideal of A;

2. The intersection of all maximal (left) submodules/ideals of A; (Jacobson radical)

3. The smallest submodule/ideal of A such that the corresponding quotient is semisimple (i.e., the smallest submodule M such that $\mathrm{Rad}(A/M) = 0$);

Proof. 1. If I, J are nilpotent ideals, then it is easy to check that $(I+J)$ is also nilpotent. Thus there is a maximal two-sided nilpotent ideal, call it N. Firstly, $\mathrm{Rad}(A) \subset N$. Indeed, we have a composition series

$$0 = A_m \subset A_{m-1} \subset \cdots \subset A_2 \subset A_1 = A.$$

Since A_i/A_{i+1} is simple, $\mathrm{Rad}(A)$ kills it, so $\mathrm{Rad}(A)A_i \subset A_{i+1}$, so $\mathrm{Rad}(A)^m = 0$. Conversely, if $N \not\subset \mathrm{Rad}(A)$ then $NS = S$ for some simple module S. But then N cannot be nilpotent, because $J^kS = S \implies J^k \neq 0, \forall k$.

2. Let $J = \bigcap \mathfrak{m}_i$ with $\mathfrak{m}_i$ being the maximal left ideals (so J is the Jacobson radical). Note if S is simple, then $S \cong A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. So

$$\mathrm{Rad}(A) = \bigcap_S Ann(S)$$

(where $Ann(S)$ is the annihilator) and $Ann(A/\mathfrak{m}) = \{x \in A \mid xA/\mathfrak{m} = 0\} = \{x \in A \mid xA \subset \mathfrak{m}\}$ is the largest two-sided ideal contained in $\mathfrak{m}$. Thus $\mathrm{Rad}(A) = \bigcap Ann(A/\mathfrak{m}) \subset \bigcap \mathfrak{m} = J$. Conversely, let S be a simple module. We want to show $JS = 0$. Suppose for a contradiction that $JS = S$, take a generator $s \in S$ so that $Js = S$. Then $js = s$ for some $j \in J$, so $(1-j)s = 0$. But this is impossible since it is a unit by usual characterization of the Jacobson radical.

3. We have shown that $\mathrm{Rad}(A) = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$, but recall in an Artinian ring, we only have finitely many maximal ideals. so $\mathrm{Rad}(A) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_N$. Consider the homomorphism $A/\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_N \to A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_N$, it is easy to check this map is injective and since the right hand is semisimple and we have shown any submodule of a semisimple module is semisimple by Remark 1.1.9, this shows $A/\mathrm{Rad}(A)$ is semisimple. On the other hand, suppose M is a submodule such that A/M is semisimple. So say $A/M = X_1/M \oplus \dots X_N/M$ with X_i submodules of A and X_i/M is simple. Let $Y_i = \sum_{j \neq i} X_j$, then $A/Y_i \cong X_i/M$. Since X_i/M is simple, we see that Y_i is maximal. So we have $\mathrm{Rad}(A) = \bigcap \mathfrak{m}_i \subset \bigcap Y_i = M$ by (2).

□

Note that we have showed that the Jacobson radical is nilpotent. It is part of the proof of Theorem 1.1.5.

Now we define the radical of a module.

Definition 1.2.3. If M is an A-module, then we define $\mathrm{Rad}(M)$ to be $\mathrm{Rad}(A)M$.

Proposition 1.2.4. The following conditions are equivalent to $\mathrm{Rad}(M)$:

1. The smallest submodule of M with semisimple quotient;
2. The intersection of all maximal submodules of M.

Proof. 1. Note that $\text{Rad}(A)$ kills $M/\text{Rad}(A)M$, so we can think it as an $A/\text{Rad}(A)$-module. But $A/\text{Rad}(A)$ is semisimple, and modules over semisimple algebras are semisimple by Prop 1.1.8. So $M/\text{Rad}(M)$ is semisimple and an $A/\text{Rad}(A)$-module and therefore as an A-module. It remains to prove that if M/N is semisimple, then $\text{Rad}(M) \subset N$, but this is trivial since $\text{Rad}(A)$ kills M/N by the semisimplicity of M/N.

2. The exact same proof of Theorem 1.2.2 (2) will go through.

□

Remark 1.2.5. Note that if M is any A-module, then M is semisimple if and only if $\text{Rad}(M) = 0$.

Proof. If $\text{Rad}(A)M = 0$ then M is an $A/\text{Rad}(A)$-module, and $A/\text{Rad}(A)$ is semisimple, so M is semisimple by Remark 1.1.9. On the other hand, if M is semisimple, then M is a direct sum of simple A-modules, which are killed by $\text{Rad}(A)$. □

Note that for a module M, $\text{Rad}(M)$ is also a module, we define $\text{Rad}^2(M) := \text{Rad}(\text{Rad}(M)) = \text{Rad}(A)^2M$. And in general $\text{Rad}^n(M) := \text{Rad}(A)^nM$.

Definition 1.2.6. The above is call the radical series of M, it has finite length, since $\text{Rad}(A)$ is nilpotent by Theorem 1.2.2.

Now we discuss the dual notion of radical, the *socle* .

Definition 1.2.7. Let M be an A-module, then $\text{Soc}(M)$ is defined to be the maximal semisimple submodule of M.

Clearly M is semisimple if and only if $\text{Soc}(M) = M$.

Proposition 1.2.8. The following conditions are equivalent to $\text{Soc}(M)$.

1. The sum of all simple submodules of M
2. The set $S = \{m \in M \mid \text{Rad}(A)m = 0\}$

Proof. The first statement is clearly equivalent to the definition of $\text{Soc}(M)$. $\text{Rad}(A)$ kills any semisimple module, so $\text{Soc}(M) \subset S$. It is clear S is a submodule, and since it is killed by $\text{Rad}(A)$, it is semisimple, therefore it has to be the $\text{Soc}(M)$, the biggest one. □

Note that $M/\text{Soc}(M)$ is also a module, let $\text{Soc}^2(M)$ be the preimage of $\text{Soc}(M/\text{Soc}(M))$ under the projection map $M \to M/\text{Soc}(M)$. Note that $\text{Rad}(A)^2\text{Soc}^2(M) = 0$, since $\text{Rad}(A)\text{Soc}^2(M) \subset \text{Soc}(M)$ and $\text{Rad}(A)\text{Soc}(M) = 0$. In fact, this characterizes $\text{Soc}^2(M)$, since $\text{Rad}^2(A)m = 0$ means that $\text{Rad}(M)$ kills $\text{Rad}(M)$, so $\text{Rad}(A)\ m \subset \text{Soc}(M)$ and therefore $\text{Rad}(A)$ kills the coset of $\text{Soc}(M)$ containing m and this means this coset is in $\text{Soc}^2(M)$. Inductively, we define $\text{Soc}^n(M)$ to be the solution set to $\text{Rad}^n(A)m = 0$.

Definition 1.2.9. The series above is called the socle series of M. Since $\text{Rad}(A)$ is nilpotent, it has to terminate with the last term being M.

Next, we prove an exercise in [Alp86, Exercise 3,4 P7]

Proposition 1.2.10. Let M be an A-module, then the radical length and socle length coincide. We call it the *Loewy length.* Moreover, say the length is n, then we have that $\forall$ $0 \leq i \leq n$, $\text{Rad}^i(M) \subset \text{Soc}^{n-i}(M)$.

Proof. This is clear by the equation of how we defined the $\text{Soc}^n(M)$. It remains to show $\text{Rad}^i(M) \subset \text{Soc}^{n-i}(M)$, but this is also clear since $\text{Rad}^{n-i}(A)\text{Rad}^i(M) = \text{Rad}^n(A)M = 0$. □

For future use, we recall Nakayama's lemma from commutative algebra.

Lemma 1.2.11. [1] If $L \subset M$ is a submodule of an A-module M such that M/L is finitely generated, then $L + \text{Rad}(M) = M$ implies that $L = M$.

1.3 Wedderburn and Krull-Schmidt

Next we want to establish some uniqueness statement of decomposition of a group algebra into indecomposables. Let's recall Wedderburn's Theorem.

Theorem 1.3.1 (Wedderburn)**.** If A is a semisimple ring, then A is a direct sum of matrix algebras over division rings.

Corollary 1.3.2. If A is a semisimple algebra over an algebraically closed field k , then A is a direct sum of matrix rings over k.

Remark 1.3.3. Note that $\text{End}_A(M_i)$ is simple and is isomorphic as a direct sum of m simple modules S_i, where m is the rank of the matrix algebra.

We want to prove Krull-Schmidt Theorem, but firstly let's borrow some terminology from commutative algebra.

Definition 1.3.4. Let A be a k algebra. We say that A is local if $A/\text{Rad}(A) \cong k$.

[1] Even though we are in the non-commutative case most of the time, the Nakayama's lemma still holds. The proof is very similar in the commutative case, a full proof can be found on [Isa09, Theorem 13.11, p. 183]

Proposition 1.3.5. A is local if and only if every element is either invertible or nilpotent.

Proof. Suppose A is local, we have proved that $\mathrm{Rad}(A)$ is the largest two-sided nilpotent ideal of A, so if x is not nilpotent then x not be in $\mathrm{Rad}(A)$. Since the quotient by $\mathrm{Rad}(A)$ is k, we write $x = a + b$, where $a \in k$ and $b \in \mathrm{Rad}(A)$. Consider the element

$$a^{-1}(1 - a^{-1}b + a^{-2}b^2 - \dots),$$

as b is nilpotent, this element makes sense, and it is easy to check that it is the inverse of x.

Now suppose the converse it true. We know $A/\mathrm{Rad}(A)$ is semisimple, and therefore by Wedderburn, is isomorphic to a direct sum of matrix algebras. If it consists of more than one matrix algebra, then $(I, 0, \dots, 0)$ is neither invertible nor nilpotent. So $A/\mathrm{Rad}(A) \cong \mathrm{Mat}_n(k)$. But if $n > 1$, then take the matrix $(1, 1)$-th entry to be 1 and 0 for the rest entries, this element is neither nilpotent nor invertible, so we conclude that $n = 1$, which is what we want. $\square$

Proposition 1.3.6. Assume A is an algebra over an algebraically closed field k, then M is an indecomposable A-module if and only if $\mathrm{End}_A(M)$ is local.

Proof. If $M = M_1 \oplus M_2$, then consider the projection to one of them. It is an element in $\mathrm{End}_A(M)$, but it is clearly not invertible, and not nilpotent since the square of it is itself (which is non-zero by assumption).

Suppose M is indecomposable. Let $f \in\mathrm{End}_A(M)$, because k is algebraically closed, we can decompose $M = \bigoplus_\lambda M_\lambda$ (as vector spaces as this moment), where λ are eigenvalues, and M_λ are generalised eigenspaces. Moreover, the M_λ's are submodules. Indeed, if $(f - \lambda I)^n m = 0$ for some n, then $(f - \lambda I)^n am = a(f - \lambda I)^n m = 0$ for any $a \in A$. Since M is indecomposable, we see $M = M_\lambda$. Note that f is nilpotent iff eigenvalue is 0, and is invertible iff 0 is not an eigenvalue. So f is either nilpotent or invertible. $\square$

We now prove Krull-Schmidt Theorem.

Theorem 1.3.7 (Krull-Schmidt)**.** Assume A is an algebra over an algebraically closed field k . Let M be an A-module, suppose that

$$\begin{aligned} M &= U_1 \oplus \dots \oplus U_r \\ &= V_1 \oplus \dots \oplus V_s, \end{aligned}$$

where U_i, V_j are indecomposables, then $r = s$ and $U_i \cong V_j$ up to some permutation.

Proof. Let p_{U_i} be projection to U_i and p_{V_j} be projection to V_j. Consider $p_{U_i} \circ p_{V_j}|_{U_1} \in\mathrm{End}_A U_1$, by the above proposition, it is either invertible or nilpotent. But

$$\sum_j p_{U_1} p_{V_j}|_{U_1} = p_{U_1} \circ 1_M|_{U_1} = 1|_{U_1}.$$

So not all of $p_{U_1}p_{V_j}|_{U_1}$ can be nilpotent, we may assume that $p_{U_1}p_{V_1}|_{U_1}$ is invertible with inverse q. Consider

$$U_1 \xrightarrow{p_{V_1}|_{U_1}} V_1 \xrightarrow{p_{U_1}|_{V_1}} U_1 \xrightarrow{q} U_1.$$

To ease the notation, let $\alpha = p_{V_1}|_{U_1}$ and $\beta = q \circ p_{U_1}|_{V_1}$. We claim that $V_1 = \mathrm{Im}(\alpha) \oplus \ker(\beta)$. If x is in the intersection, then $x = \alpha(y)$, for some $y \in U_1$, and $y = \beta\alpha y = \beta x = 0$, so $x = 0$. And if $z \in V_1$, then write $z = (z - \alpha\beta z) + \alpha\beta z$, and $z - \alpha\beta z \in \ker\beta$, $\alpha\beta z \in \mathrm{Im}\alpha$. Since V_1 is indecomposable and $\mathrm{Im}(\alpha) \neq 0$, we conclude that $\ker(\beta) = 0$ so α, β are isomorphisms and $U_1 \cong V_1$.

We would like to proceed by induction, but we have to check that $U_1 \cap (V_2 \oplus \cdots \oplus V_s) = 0$. Assume it is true, then $M = U_1 \oplus V_2 \oplus \cdots \oplus V_s$, and we will be done by induction and considering the module M/U_1. But if x is in the intersection, then $x = \beta\alpha x$, and $\alpha = p_{V_1}|_{U_1}$ is zero on $V_2, \ldots, V_s$. So $x = 0$ and this completes the proof. □

Remark 1.3.8. Sometimes we will need a stronger result than this. For example, under certain conditions, we can drop the assumption that k is algebraically closed. We will quote the result without proof. For a detailed discussion, see [Sch13, Thm 4.7]

Theorem 1.3.9 (Krull-Remak-Schmidt)**.** The unique decomposition property still hold in the following situations:

1. M is of finite length
2. A is left Artinian and M is finitely generated
3. A is left Noetherian, $A/\mathrm{Rad}(A)$ is left Artinian, any finitely generated A-module is complete, and M is finitely generated
4. A is an A_0-algebra, which is finitely generated as an A_0-module, over a Noetherian complete commutative ring A_0 such that $A_0/\mathrm{Rad}(A_0)$ is Artinian, and M is finitely generated. (We took $A_0 = k$)

Clearly this is the situation we are in. We will sometimes use this theorem without quoting in the future. And we now see that projective indecomposable modules are exactly the indecomposable modules for group algebra $k[G]$.

1.4 Modular Representation

We now fix our Artinian algebra A to be $k[G]$ and $char(k) = p$. So far we haven't touched on how the characteristic of the field k can affect the algebra. It turns out $k[G]$ behaves quite differently depending on whether $char(k) \mid |G|$ or not. When $char(k) \mid |G|$, we say it is *modular representation* , and the other case *ordinary representation.*

Theorem 1.4.1. (Maschke's Theorem) The group algebra $k[G]$ is semisimple if and only if $char(p) \nmid |G|$.

Proof. Let V be a $k[G]$-submodule. It suffices to prove that V is a direct summand. Let π be any k-linear projection from $k[G]$ onto V. Consider the map $\varphi : k[G] \to V$ given by $\varphi(x) = \frac{1}{|G|}\sum_{g\in G} g\cdot\pi(g^{-1}\cdot x)$. Then φ is again a projection: it is clearly K-linear, maps $k[G]$ onto V, and induces the identity on V. Moreover we have:

$$\begin{aligned}\varphi(t\cdot x) &= \frac{1}{|G|}\sum_{s\in G} s\cdot\pi(s^{-1}\cdot t\cdot x)\\ &= \frac{1}{|G|}\sum_{u\in G} t\cdot u\cdot\pi(u^{-1}\cdot x)\\ &= t\cdot\varphi(x),\end{aligned}$$

so φ is in fact $k[G]$-linear. By the splitting lemma, $k[G] = V \oplus \ker\varphi$. Thus $k[G]$ is semisimple.

Conversely, For $x = \sum \lambda_g g \in k[G]$ define $\epsilon(x) = \sum \lambda_g$. Let $I = \ker\epsilon$ (the augmentation ideal). Then I is a $k[G]$-submodule. We claim that for every non-trivial submodule V of $k[G]$, $I \cap V \neq 0$. Let $v = \sum_{g\in G}\mu_g g$ be any non-zero element of V. If $\epsilon(v) = 0$, the claim is immediate. Otherwise, let $s = \sum_{g\in G} g$. Then $\epsilon(s) = |G|\cdot 1 = 0$ so $s \in I$ and $sv = (\sum g)(\sum \mu_g g) = \sum \epsilon(v) g = \epsilon(v)s$ so that sv is an element of both I and V. This proves that V is not a direct complement of I for all V, so $k[G]$ is not semisimple. □

Remark 1.4.2. For the converse, alternatively, it is easy to see that $k[G]/I$ is the trivial module. But $gs = s$ for all $g \in G$. So $\langle s\rangle$ is also trivial, and this contradicts the remark after Wedderburn.

Recall that over $\mathbb{C}$, the number of representations of a group equals the number of conjugacy classes of that group. We want to achieve something similar in the modular case. But we need to establish some basic lemmas.

Definition 1.4.3. Say G is a group. An element g is said to be p-regular if its order is not divisible by p. Otherwise it is called p-unipotent.

Lemma 1.4.4. Let G be a group. Then we can uniquely write $g = xy$ where x and y commute, and x has order p^k and y is p-regular.

Proof. Suppose $g = xy$ with x has order p^k and y is p-regular, choose m large enough so that $x^{p^m} = e$, so we have $g^{p^m} = y^{p^m}$. Since the order of y is coprime to p, we can choose m such that $p^m = 1$ modulo the order of y. Thus $y \in \langle g\rangle$, hence x too, which implies the commutativity since they lie in a cyclic group.

So we reduce to the cyclic case. Write $C_n = C_{p^a}\times C_{{p_1}^{a_1}}\times\cdots\times C_{{p_n}^{a_n}}$. Let $g = (g_0, g_1, \ldots, g_n) \in G$, and then let $x = (g_0, e, \ldots, e)$ and $y = (e, g_1, \ldots, g_n)$. Moreover, this is unique, since x has to have the form $({g'}^i, e, \ldots, e)$, where g' is a generator of C_{p^a}, but then $y = (g_0{g'}^{-i}, g_1, \ldots, g_n)$, this has order coprime to p if and only if $g_0{g'}^{-i} = e$. □

Let A' be the subspace of $k[G]$ generated by commutators $[x, y] = xy - yx$ (i.e., the 'derived algebra'). It is spanned by things of the form $g - hgh^{-1}$. So it consists precisely of things of the form $\sum a_g g$ where the sum of a_g over every conjugacy class vanishes. This clearly implies that the codimension is equal to the number of conjugacy classes.

Let $R = \{x \in A | x^{p^N} \in A' \text{ for some } N\}$, it should be thought as the 'p-radical ideal' of A'. We will use this to prove Brauer-Nesbitt. But let's first prove it is indeed a vector subspace, so that it makes sense to talk about dimensions.

Lemma 1.4.5. If $a, b \in k[G]$ then $a^p + b^p = (a+b)^p$ in $k[G]/A'$.

Proof. Note that $(a+b)^p - a^p - b^p$ is a sum of groups of p terms involving compositions of a and b. We can partition them into things that differ by a cyclic permutation. The commutator $(aaba\dots)x - x(aaba\dots) \in A'$ by definition, so the sum of things in a block is congruent to p times the first term, which is 0. □

Lemma 1.4.6. If $a \in A'$, then so is a^p.

Proof. Indeed, if $a = \sum a_i[x_i, y_i]$ then by the previous lemma $a^p = \sum a_i^p (x_i y_i)^p - a_i^p (y_i x_i)^p$ in $k[G]/A'$. But $(xy)^p - (yx)^p = xz - zx \in A'$, where $z = yxyx\dots y$. □

Lemma 1.4.7. If $a, b \in R$, then so is $a + b$.

Proof. Note that if the $x^{p^n} \in A'$ for some n then it is true for all larger n. Therefore, we may assume that $a^{p^N}, b^{p^N} \in A'$ and then by the first lemma $(a+b)^{p^N} = a^{p^N} + b^{p^N}$ in $k[G]/A'$. □

Now we give the mean theorem:

Theorem 1.4.8 (Brauer-Nesbitt)**.** The number of simple modules for $k[G]$ is the number of p-regular conjugacy classes (conjugacy classes consisting of elements whose order is not divisible by p)

Proof. Let $\{C_i\}$ be the p-regular conjugacy classes and $D_i = \{g \in G \mid p\text{-regular part of } g \in C_i\}$. We claim that $R = \{\sum a_g g \mid \sum a_g = 0 \text{ on each } D_i\}$. Indeed, write $|G| = p^k m$. Choose some $N > k$ such that $p^N = 1 \pmod{m}$. Then raising to the p^N power maps each element $g \in G$ to its p-regular part, and R is the pre-image of A' under this map. So $R = \{f \in k[G] \mid \sum_{g \in C_i} f^{p^N}(g) = 0\} = \{f \in k[G] \mid \sum_{g \in D_i} f(g)^{p^N} = 0\}$, but $\sum_{g \in D_i} f(g)^{p^N} = \sum_{g \in D_i} f(g) \pmod{p}$ (recall the field has characteristic p), and this completes the claim.

Since $\mathrm{Rad}(A)$ is nilpotent, $\mathrm{Rad}(A) \subset R$. Recall we have that $A/\mathrm{Rad}(A) = \bigoplus_i \mathrm{Mat}_{d_i}(k)$. We consider the image of A' or R in $A/\mathrm{Rad}(A)$. In each $\mathrm{Mat}_{d_i}(k)$ the image of A' the subring generated by commutators, which is the trace-zero part. Because R is $\{x | x^{p^N} \in A'\}$, R and A' have the same image ($\mathrm{Tr}(x^{p^N}) = 0$ iff $\mathrm{Tr}(x)^{p^N} = 0$. Indeed it is a consequence of Fermat's little theorem and by considering the algebraic closure). Since $\mathrm{Rad}(A) \subset R$ we see that the codimension of R is equal to both the number of p-regular conjugacy classes, and the number of distinct simple modules. □

Now we get a corollary that is going to be helpful in the next chapter.

Corollary 1.4.9. If G is a p-group, then the trivial $k[G]$-module is the only simple $k[G]$-module.

Proof. The identity element is the only one with order not divisible by p so it is a unique simple module by above. On the other hand, the trivial module is simple. □

1.5 Idempotents and Blocks

In this section, we will take a short detour to idempotents and blocks. We will need them to talk about projective covers in the next section, especially Proposition 1.6.6. This is also the building block of Chapter 3. Also note, blocks are central objects of study in modern group representation theory. And it has many open problems (see Afterword).

Definition 1.5.1. An *idempotent* in A is a non-zero element e such that $e^2 = e$.

Remark 1.5.2. Note if e is an idempotent, then so is $1 - e$. Let Ae be the set $\{ae, a \in A\}$, then this is a left ideal of A. The set $eAe = \{eae, a \in A\}$ is a ring with unity e. And we have ${}_AA = Ae \oplus A(1-e)$. Also note that if M is a left A-module, then eM can be considered as a left eAe module.

Lemma 1.5.3.
1. If M is an (left) A-module and e is an idempotent in A, then $eM \cong \mathrm{Hom}_A(Ae, M)$ (as abelian groups at the moment).
2. We have the ring isomorphism $eAe \cong \mathrm{End}_A(Ae)^o$ (where ^{o} means the opposite ring)

Proof.
1. Define $f_1 : eM \to \mathrm{Hom}_A(Ae, M)$ by $f_1(em) : ae \mapsto aem$, and $f_2 : \mathrm{Hom}_A(Ae, M) \to eM$ by $f_2(\psi) = \psi(e)$. They are clearly inverses of each other.
2. Let $M = Ae$ in 1, we need to check it is compatible with the multiplication and it reverses the order of multiplication on the right hand side. But $ea_1eea_2e = ea_1ea_2e \to (be \mapsto bea_1ea_2e)$, and if $\alpha(be) = bea_1e$ and $\beta(be) = bea_2e$, then $\alpha \circ \beta(be) = \alpha(bea_2e) = bea_2ea_1e$.

□

Definition 1.5.4. Two idempotents e, f are *orthogonal* if $ef = fe = 0$. An idempotent e is said to be *primitive* if it can not be written as $e = e_1 + e_2$, where e_1, e_2 are orthogonal.

Remark 1.5.5. Note there is a bijection between the set of pairwisely orthogonal idempotents $\{e_i\}$ such that $1 = e_1 + \cdots + e_n$, and the direct sum decomposition of modules $A = A_1 \oplus \cdots \oplus A_n$, given by $A_i = Ae_i$ and $e_i = \psi_i(1)$, where ψ_i is the restriction to A_i of the isomorphism $A \cong \bigoplus A_i$. We see that e_i is primitive if and only if A_i is indecomposable. Also note that A is semisimple if and only if every right (or every left) ideal is generated by an idempotent.

Definition 1.5.6. An idempotent is said to be a *central idempotent* if it is an idempotent in the centre of A. A *primitive central idempotent* is an idempotent that is central and primitive.

Remark 1.5.7. There is a bijection between the set of pairwisely central orthogonal idempotents $\{e_i\}$ such that $1 = e_1 + \cdots + e_n$, and the direct sum decomposition $A = B_1 \oplus \cdots \oplus B_n$, where B_i's are two-sided ideals of A. And again, primitive if and only if indecomposable.

Definition 1.5.8. The indecomposable two-sided ideals are call *blocks* of A.

Lemma 1.5.9. This decomposition is unique.

Proof. Say $1 = e_1 + \cdots + e_s = f_1 + \cdots + f_t$. Then $e_i = e_i f_1 + \cdots + e_i f_t$, but e_i is primitive and $e_i f_j$ is either zero or central, we see $e_i = e_i f_j = f_j$ for some j. □

Remark 1.5.10. Let M be an indecomposable A-module. Then $M = e_1 M \oplus \cdots \oplus e_s M$ as left modules (since e_i is central). But M is indecomposable, so we see for some i, $e_i M = M$ and $e_j M = 0$ for $j \neq i$. We say M *belongs to* the block B_i. Clearly if an indecomposable module is in a certain block, then so are all its quotients and submodules.

We will need the following proposition for the next section.

Proposition 1.5.11. Let $I \subset R$ be a two-sided ideal and suppose that every element in I is nilpotent, then for any idempotent $\epsilon \in R/I$ there is an idempotent $e \in R$ such that $e + I = \epsilon$

Remark 1.5.12. We have showed that the $\mathrm{Rad}(A)$ is a two-sided nilpotent ideal, and therefore every element in $\mathrm{Rad}(A)$ is nilpotent.

Proof. Let $\epsilon = a + I$ and $b = 1 - a$. Then $ab = ba = a - a^2 \in I$, and hence $(ab)^m = 0$ for some $m \geq 1$. Since a and b commute, we have

$$1 = (a+b)^{2m} = \sum_{i=0}^{2m} \binom{2m}{i} a^{2m-i} b^i = \sum_{i=0}^{m} \binom{2m}{i} a^{2m-i} b^i + \sum_{i=m+1}^{2m} \binom{2m}{i} a^{2m-i} b^i.$$

We let e be the first term and f be the second term. Since for any $0 \leq i \leq m$ and $m < j \neq 2m$ we have $a^{2m-i} b^i a^{2m-j} b^j = a^m b^m a^{3m-i-j} b^{i+j-m} = (ab)^m a^{3m-i-j} b^{i+j-m} = 0$, we see that $ef = 0$. It follows that $e = e.1 = e(e+f) = e^2$, so e is an idempotent. Finally, $ab \in I$ implies that

$$e + I = a^{2m} + (\sum_{i=1}^{m} \binom{2m}{i} a^{2m-i-1} b^{i-1}) ab + I = a^{2m} + I = \epsilon^{2m} = \epsilon.$$

□

1.6 Self-injectivity

This section is the punchline of this chapter, we will use multiple results in this section in the future chapters. In this section, we will prove a $k[G]$-module is projective if and only if it is injective and some of its consequences. We will use the general notion of so called *symmetric Frobenius algebra* following [Ben98a, Chap1,3]. We sometimes distinguish left and right modules in this section, let M_A be a right module, and ${}_AM$ be a left module. And we denote the dual of M by M^*.

A word on dual: Normally, if we have a left module M, the dual is defined to be the *right* module M^* $=\text{Hom}_A(M, A)$, with the action $(a \cdot f)(m) = f(am)$. This is a right module because $((ba) \cdot f)(m) = f(bam)$, while $(b \cdot (a \cdot f))(m) = (a \cdot f)(bm) = f(abm)$. So following the normal convention, we should write $f \cdot a$ instead of $a \cdot f$. But group algebras are special, they are part of the bigger class call *Hopf algebras*.
A *bialgebra* over k is an algebra with a comultiplication $\Delta : A \to A \otimes_k A$ and a co-unit $\epsilon : A \to k$ satisfying some obvious commutative diagrams. A Hopf algebra is a bialgebra with an k-linear map $S : A \to A$ called the *antipode* such that if $S(a) = \sum_i \mu_i \otimes \nu_i$, then $\sum_i \mu_i S(\nu_i) = \sum_i S(\mu_i)\nu_i = \epsilon(a).1 \in A$. For a group algebra, comultiplication and co-unit is defined as the following: $\Delta(\sum_i r_i g_i) = \sum_i r_i g_i \otimes g_i$ and $\epsilon(\sum_i r_i g_i) = \sum_i r_i$, with usual multiplication and unit defined as $\nabla : A \otimes_k A \to A, \sum_{i,j} r_{i,j} g_i \otimes g_j \mapsto \sum_{i,j} r_{i,j} g_i g_j$ and $\eta : k \to A, x \mapsto xe$, while the antipode is $S(\sum_i r_i g_i) = \sum_i r_i g_i^{-1}$. With this we can view the dual as a *left* module via the antipode $a.m = m.S(a)$ and vice-versa. So from now on, when we have a group algebra, we take the dual to the *left* module with the action $(g \cdot f)(m) = f(g^{-1}m)$ for $g \in G$. (For more details, see [Ben98a, p.51-52])
It is clear that if L is a submodule of M then M^* has a submodule naturally isomorphic to $(M/L)^*$ and the quotient M^* by this submodule is naturally isomorphic to L^*.

Definition 1.6.1. Let A be an algebra over k.

1. We say A is *Frobenius* if there is a k-linear map $\lambda : A \to k$ such that $\ker(\lambda)$ contains no non-zero left or right ideals.
2. We say A is *symmetric* if it is Frobenius and $\lambda(ab) = \lambda(ba)$ for all $a, b \in A$.
3. We say A is *self-injective* if the left module ${}_AA$ is an injective A-module.

Proposition 1.6.2.

1. If A is a finite dimensional Frobenius algebra over k, then $(A_A)^* \cong {}_AA$. In particular, A is self-injective.
2. If A is self-injective, then if M is a (left) f.g. module over A, then the followings are equivalent:
   (a) M is projective
   (b) M is injective
   (c) M^* is projective
   (d) M^* is injective

Proof. 1. We define $\psi : {}_AA \to (A_A)^*$ by $\psi(x) : y \to \lambda(yx)$. This is a module homomorphism because if $z \in A$, then $\psi(zx)(y) = \lambda(yzx) = \psi(x)(yz) = z(\psi(x))y$. This is injective since if it is not, then we have a non-zero x such that $\psi(x)$ is the zero map. I.e., $\lambda(yx) = 0$ for all $y \in A$. So the non-zero ideal generated by x is in the kernel, which is impossible. It is therefore surjective by dimension counting.

2. We first note that (a) and (d) are equivalent by definition. Similarly, (c) and (b) are equivalent. Since A is self-injective, we see that (a) and (c) are equivalent. Hence they are all equivalent.

□

We now specialise to group algebras.

Proposition 1.6.3. The linear map $\lambda : k[G] \to k$ by $\lambda(\sum_{g\in G} r_g g) = r_e$ satisfies the condition of the definition of a symmetric Frobenius algebra.

Proof. Let I be a non-zero left ideal. Say $\sum_{g\in G} r_g g$ is in I with $r_h \neq 0$, then so is $h^{-1}\sum_{g\in G} r_g g$. But if we apply λ to this element, we get a non-zero image. So it is Frobenius. It is clearly symmetric, because

$$\lambda(\sum_{g\in G} r_g g \cdot \sum_{h\in G} s_h h) = \sum_{g\in G} r_g s_{g^{-1}} \overset{g\to g^{-1}}{=\!=\!=} \sum_{g\in G} s_g r_{g^{-1}} = \lambda(\sum_{g\in G} s_g g \cdot \sum_{h\in G} r_h h).$$

□

Theorem 1.6.4. Suppose P is a projective indecomposable module for a symmetric Frobenius algebra A. Then $\mathrm{Soc}(P) \cong P/\mathrm{Rad}(P)$.

Proof. Let e be a primitive idempotent in A with $P \cong Ae$. Let $\lambda : A \to k$ be the map in the definition of the Frobenius algebra A. Since P is projective indecomposable, we see that $\mathrm{Soc}(P)$ is simple and $\mathrm{Soc}(P) = \mathrm{Soc}(P).e$ is a left ideal in A. So there is an $x \in \mathrm{Soc}(P)$ with $\lambda(xe) \neq 0$. But A is symmetric, so $\lambda(ex) \neq 0$ and so $e.\mathrm{Soc}(P) \neq 0$. But by Lemma 1.5.3, $e.\mathrm{Soc}(P) \cong \mathrm{Hom}_A(P, \mathrm{Soc}(P))$, so there is a non-zero homomorphism from P to $\mathrm{Soc}(P)$. By the definition equation of $\mathrm{Soc}(P)$, we see this induces an isomorphism between $P/\mathrm{Rad}(P)$ and $\mathrm{Soc}(P)$. □

We now introduce the concept of projective covers. It will be helpful especially in Section 2.2.3.

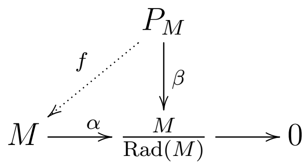
Definition 1.6.5. 1. A homomorphism $f : M \to N$ is called *essential* if it is surjective but $f(L) \neq N$ for any proper submodule L.

2. A *projective cover/envelope* P_M of M is a projective module with an essential map $f : P_M \to M$.

Proposition 1.6.6. If A is Artinian, then projective covers exist for all finitely generated A-modules.

Proof. We can write $1 + \mathrm{Rad}(A) = \epsilon_1 + \cdots + \epsilon_r$ as a sum of pairwise orthogonal primitive idempotents $\epsilon_i \in A/\mathrm{Rad}(A)$. Since $A/\mathrm{Rad}(A)$ is semisimple, we have $A/\mathrm{Rad}(A) = A/\mathrm{Rad}(A)\epsilon_1 + \cdots + A/\mathrm{Rad}(A)\epsilon_r$ is a direct sum of simple $A/\mathrm{Rad}(A)$ modules. Let M be an A-module, then $M/\mathrm{Rad}(M)$ is an $A/\mathrm{Rad}(A)$ module, and write $L_1 \oplus \cdots \oplus L_s$, where L_i's are simple $A/\mathrm{Rad}(A)$ modules. So for each i, we have $L_i \cong A/\mathrm{Rad}(A)\epsilon_{i_j}$ for some i_j. By Prop.1.5.11, we find idempotents $e_1, \ldots, e_r \in R$ such that $e_i + \mathrm{Rad}(A) = \epsilon_i$. So we have the following isomorphism $\bigoplus_{j=1}^{s} Ae_{j_i}/\mathrm{Rad}(A)e_{j_i} \cong \bigoplus_{j=1}^{s} A/\mathrm{Rad}(A)\epsilon_{j_i} \cong \bigoplus_{j=1}^{s} L_j \cong M/\mathrm{Rad}(M)$.

Let $P_M = \bigoplus_{j=1}^{s} Ae_{j_i}$, it has a clear projection to $M/\mathrm{Rad}(M)$ via the above isomorphism. It is clearly a projective module. So we have a diagram.



It remains to show f is essential. Since β is surjective we have $f(P_M) + \mathrm{Rad}(M) = M$, and the Nakayama's lemma 1.2.11 implies that f is surjective. Moreover, $ker(f) \subset \mathrm{Rad}(P_M)$ by construction. Hence if $L \subset P_M$ is a submodule such that $f(L) = M$, then $P_M = L + \ker(f) = L + \mathrm{Rad}(P_M)$, and by Nakayama's lemma again $P_M = L$, so f is essential. □

Proposition 1.6.7. The projective cover is unique up to isomorphism.

Proof. Say P and P' are projective covers of M with maps $f : P \to M$ and $f' : P' \to M$. Then by projectivity there exists $g : P' \to P$ such that $f' = f \circ g$. Since f' is surjective we have $f(g(P')) = M$, and since f is essential we deduce that $g(P') = P$. This shows that g is surjective. Then by an alternative definition of projectivity, there exists a homomorphism $s : P \to P'$ such that $g \circ s = id_P$. We have $f'(s(P)) = f(g(s(P))) = f(P) = M$. Since f' is essential this implies $s(P) = P'$. Hence s and g are isomorphisms. □

Theorem 1.6.8. Suppose k is algebraically closed. There is a bijection between the set of projective indecomposable modules of A and the set of simple modules of A by sending P to $P/rad(P)$. And the inverse is given by taking projective covers.

Proof. Given a simple module S, we see by construction the projective cover is an indecomposable module P such that $P/\mathrm{Rad}(P) = \alpha(f(P))$ in the proof of Prop.1.6.6. But $\mathrm{Rad}(S)= 0$, so we see $P/\mathrm{Rad}(P) = S$. So we see the composition of the two maps described in the theorem is identity on the set of simple modules. For the other direction, we invoke the uniqueness of projective covers by Prop.1.6.7. So by above we need to show $Q/\mathrm{Rad}(Q)$ is simple for all projective indecomposables Q.

We claim that $\mathrm{End}_A(Q/\mathrm{Rad}(Q))$ is a quotient of $\mathrm{End}_A(Q)$ (which we know is local by Prop.1.3.6), hence local. Then $Q/\mathrm{Rad}(Q)$ is semisimple and indecomposable, hence simple. Any endomorphism of Q takes $\mathrm{Rad}(Q)$ into itself, since $\mathrm{Rad}(Q) = \mathrm{Rad}(A)Q$. So there is a map f :$\mathrm{End}(Q) \to \mathrm{End}(Q/\mathrm{Rad}(Q))$. By the lifting property of projective modules, we have a diagram for every $\alpha \in \mathrm{End}(Q/\mathrm{Rad}(Q))$:

$$\begin{array}{ccc} Q & \longrightarrow & \frac{Q}{\mathrm{Rad}(Q)} \\ \vdots {\scriptstyle \bar{\alpha}} & & \downarrow {\scriptstyle \alpha} \\ Q & \longrightarrow & \frac{Q}{\mathrm{Rad}(Q)} \end{array}$$

So the map f is surjective. Therefore by the other implication of Prop.1.3.6, we see that $Q/\mathrm{Rad}(Q)$ is simple. □

The following corollary will be very useful when calculating the decomposition of a group algebra.

Corollary 1.6.9. In the decomposition of A into the direct sum of projective indecomposables, each projective indecomposable occurs as many times as the dimension of simple modules.

Proof. Say $A = P_1 + \cdots + P_s$, multiply by $\mathrm{Rad}(A)$ we get $\mathrm{Rad}(A) = \mathrm{Rad}(P_1) + \cdots + \mathrm{Rad}(P_s)$. Taking quotient we get that $A/\mathrm{Rad}(A) \cong P_1/\mathrm{Rad}(P_1) + \cdots + P_s/\mathrm{Rad}(P_s)$. But $A/\mathrm{Rad}(A)$ is semisimple, so now we use Wedderburn's Theorem and this completes the proof. □

Corollary 1.6.10. Let M be a projective module for G . If $p^m||G|$, then p^m divides $\dim_k M$

Proof. Let $P \subset G$ be a p-Sylow subgroup, and say $|P| = p^m$. If M is a projective indecomposable for G , then M remains projective as a $k[P]$-module, since $k[G] = k[P]^{[G:P]}$ by Lagrange. So M is a direct sum of copies of $k[P]$ as a $k[P]$-module by the $1-1$ correspondence and dimension counting and Corollary 1.4.9, hence it's dimension is a multiple of $\dim_k k[P] = p^m$. □

Remark 1.6.11. Combining Theorem 1.6.8 and Theorem 1.6.4, we see again that $\mathrm{Soc}(P)$ is simple when P is a projective indecomposable module. But note there is a more direct proof without using Theorem 1.6.4 but Prop.1.6.2. Since P is a projective indecomposable, so is P^*. So $P^*/\mathrm{Rad}(P^*)$ is simple. However $\mathrm{Soc}(P)^* \cong P^*/\mathrm{Rad}(P^*)$ (this does not need Theorem 1.6.4, it follows from the last paragraph of the discussion on 'a word on dual' at the start of this section), so $\mathrm{Soc}(P)$, the dual of $\mathrm{Soc}(P)^*$ is also simple.

Chapter 2

Character Theoretic Approach: The CDE Triangle

In this section we will move to character theory and build Brauer characters and relate them to ordinary characters. In particular, we will see the orthogonality relations and some computation examples. We will later use the theory we build in this chapter to prove an important theorem in the next chapter. We will usually follow [Ser77, Part III], but sometimes will switch to [Sch13] or [Fen15] for more details and comprehensible proofs. Throughout, we fix a prime p and $\text{char}(k) = p$.

2.1 The Setup

Again, the problem lies in the possibility that modules can be non-semisimple. But as in any other case, if it is not semisimple, we just force it to be semisimple. And this is the exact idea of the Grothendieck group.

Definition 2.1.1. The *Grothendieck group* consists of the isomorphism classes of $k[G]$-modules modulo the relations $[M] = [M'] + [M'']$ for every short exact sequence

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

We denote by $R_k(G)$ the Grothendieck group of finitely generated modules over the relevant field k, and $P_k(G)$ the Grothendieck group of finitely generated projective modules over k

Remark 2.1.2. Clearly, both $R_k(G)$ and $P_k(G)$ are finitely generated when considered as abelian groups (by adding formal inverses and taking the direct summation as the group operation). The finitely generated aspect was discussed at the beginning of the last chapter, and the well-defined aspect is basically a restatement of the Jordan-Hölder Theorem, where it says the composition factors will be the same no matter what composition series we take. Therefore we have $R_k(G)$ is free abelian and generated by the set of simple modules and $P_k(G)$ is generated by the set of projective indecomposables.

The main technical tool that we will use is a $(0, p)$-ring A for k (following Serre's notation and see [Ser79]), which is a complete local commutative integral domain A such that

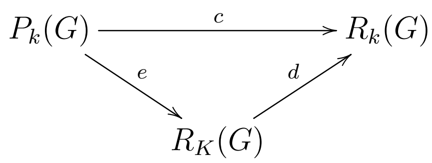
- There is a maximal ideal $\mathfrak{m}$ such that $A/\mathfrak{m} \cong k$.
- The field of fractions of A (which we call K, capitalised) has characteristic zero.

The example to keep in mind is when $k = \mathbb{F}_p$, then the field will be $K = \mathbb{Q}_p$ (p-adic numbers) and the ring of integers will be $A = \mathbb{Z}_p$ (p-adic integers), with the ideal $\mathfrak{m} = p\mathbb{Z}_p$ (the elements with norm $\leq \frac{1}{p}$) and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ (see [Ser79]). For other fields of characteristic p, the field K we get is just some extension of $\mathbb{Q}_p$, and in particular when k is a finite extension of $\mathbb{F}_p$ (so a finite field of characteristic p), the field K will be a finite extension of $\mathbb{Q}_p$.

The idea is to treat the representations of G over K as it is over $\mathbb{C}$, since it has characteristic zero and it behaves nicely when the extension is big enough. And the modular representations (which is what we are after) are linked to the representations of G over K using the map going from K to k.

Remark 2.1.3. Note that $R_K(G) = P_K(G)$ (the Grothendieck group of projective $K[G]$-modules) because $K[G]$-representations are semisimple in characteristic 0, so the simple modules are projective (by Maschke's Theorem).

The main objective is to prove the existence of a commutative triangle.



2.2 The CDE Triangle

The triangle above is called the CDE triangle[1]. We now define the maps separately. We will sometimes write $f(M)$ instead of $f([M])$ for $f = c, d, e$ and an appropriate module M.

2.2.1 The map c

This is the easiest map of the three to define. From the previous section, the set of simple modules $[S_i]$ is a basis of $R_k(G)$ as a finitely generated free abelian group. Also, the set of projective indecomposables $[P_i]$ is a basis of $P_k(G)$. Thus, we can define c to be the map in these bases to be

$$c([P_j]) = \sum_{i,j} c_{ij}[S_i]$$

[1]The letter c is for the Cartan matrix which we will see later, the letter d may stand for 'decomposition', but there might be some historical reasons as well. Nevertheless, it won't bother us.

, where c_{ij} := the multiplicity of S_i in P_j. Again, we had multiple discussions on the well-defined aspect of this. Later we will see that $c_{ij} = c_{ji}$. The matrix C defined as $C_{ij} = c_{ij}$ is called the Cartan matrix. Later we will show it is symmetric.

2.2.2 The map d

This map d is slightly harder to define. Firstly, recall that given a finite-dimensional vector space V over K, a lattice is a finitely-generated A-module $L \subset V$ such that L spans V . This L will be a free module on some basis of V (Recall that A is a PID, and torsion-free).

So to get $d(M)$, where M is an $K[G]$-module, we first take a lattice $L \subset M$ and then map this to $[L/\mathfrak{m}L] \in R_k(G)$.

There can be several issues with this definition. Firstly, we have to choose L such that it is G-stable. This is in fact not too hard to do: just take any L, and form the lattice $\sum_{g \in G} gL$ (recall G is finite), which will be G-stable. A more important question to address is the dependency on the lattice L. The next proposition shows that this construction is in fact independent of L.

Proposition 2.2.1. If $L, L' \subset M$ are G-stable lattices, then $L/\mathfrak{m}L$ and $L'/\mathfrak{m}L'$ have the same composition factors, i.e. $[L/\mathfrak{m}L] = [L'/\mathfrak{m}L']$ in $R_k(G)$.

Proof. Recall that A is a local PID, therefore all ideals are of the form $\mathfrak{m}^n$. So for some n, we have $\mathfrak{m}^n L' \subset L$. Replacing L' by $\mathfrak{m}^n L'$ doesnt change $L'/\mathfrak{m}L'$, so we may assume without loss of generality that $L' \subset L$. Similarly, we have $\mathfrak{m}^N L \subset L'$, hence we have a tower $\mathfrak{m}^N L' \subset \mathfrak{m}^N L \subset L' \subset L$. Now we will prove by induction on N. If $N = 1$, denote $A = L/L'$ and $B = L'/\mathfrak{m}L$, and we have a tower:

$$\begin{array}{c} L \\ \Big| {\scriptstyle A} \\ L' \\ \Big| {\scriptstyle B} \\ \mathfrak{m}L \\ \Big| {\scriptstyle A} \\ \mathfrak{m}L' \end{array}$$

Thus $[L/\mathfrak{m}L] = [A]+[B] = [L'/\mathfrak{m}L']$. For the general case, define $L'' = L'+\mathfrak{m}^{N-1}L$. Then we have $\mathfrak{m}^{N-1}L' \subset \mathfrak{m}^{N-1}L \subset L'' \subset L$ and $\mathfrak{m}L' \subset \mathfrak{m}L'' \subset L' \subset L''$ as $\mathfrak{m}L'' = \mathfrak{m}L'+\mathfrak{m}^N L \subset L'$. By the inductive assumption, $[L/\mathfrak{m}L] \cong [L''/\mathfrak{m}L'']$ from the first tower, and $[L''/\mathfrak{m}L''] \cong [L'/\mathfrak{m}L']$ by the second tower. And this completes the proof. □

2.2.3 The map e

This is the hardest map to define, we first need some preliminary results.

Lemma 2.2.2. Let P be an $A[G]$-module which is projective as an A-module. Then P is projective as an $A[G]$-module if and only if there exists an A-linear map $u : P \to P$ such that $x = \sum_{g \in G} g \cdot u(g^{-1}x)$ for all $x \in P$.

Proof. ($\implies$) If $P = A[G]$, then we can take $u(g) = 1$ if $g = 1$ and 0 otherwise, and this visibly works. Therefore, we can find such a u if $P = A[G]^n$ by writing u in coordinate. Therefore a u exists if P is projective, as we can write $P \oplus P' = A[G]^n$ and compose the u from the free case with the projection to P.

($\impliedby$) We need to show P has the defining property of an $A[G]$-projective module. Let $v : P \to M'$ be a map of $A[G]$-modules, and $M \hookrightarrow M'$ be a surjection. Consider then as A-modules, we get an A-linear map $s : P \to M$ such that $v = fs$. Using the Maschke's Theorem's trick, let $t : P \to M$ be the map $t(x) = \sum_{g \in G} g \cdot u(g^{-1}x)$. This is now an $A[G]$-module homomorphism by construction, and we show it lifts v:

$$\begin{aligned} f(t(x)) &= \sum_{g \in G} g(fsu(g^{-1}x)) \\ &= \sum_{g \in G} g(vu(g^{-1}x)) \\ &= \sum_{g \in G} v(gu(g^{-1}x)) \\ &= v(x) \end{aligned}$$

□

Proposition 2.2.3. If P is an $A[G]$-module that is free as an A-module, then P is projective over $A[G]$ if and only if $P/\mathfrak{m}P$ is projective as a $k[G]$-module.

Proof. ($\implies$) Given a surjection $M \hookrightarrow M'$ and Let $P/\mathfrak{m}P \to M'$, we can compose with the morphism $P \to P/\mathfrak{m}P$, and lift to a map $P \to M$ by considering them and $A[G]$ modules. Since $\mathfrak{m}$ kills M, this lift factors through $P/\mathfrak{m}P$.

($\impliedby$) Suppose that $\bar{P} := P/\mathfrak{m}P$ is projective, and let $\bar{u} : \bar{P} \to \bar{P}$ be an endomorphism as in the lemma. We can lift $\bar{u}$ to a map $u_0 : P \to P$ satisfying $x = \sum_{g \in G} gu_0(g^{-1}x) \pmod{\mathfrak{m}P}$. Then we let $u_1(x) = \sum_{g \in G} gu_0(g^{-1}x)$. As P is a free A-module, the determinant of u_1 is a unit. (A is local, and $\det u_1 = 1 \pmod{\mathfrak{m}}$, so $\det \in A^*$.) So u_1 is invertible (so the determinate is not in the maximal ideal). So we can find $v_1 : P \to P$ such that $u_1 v_1 = \mathrm{Id}_P$. Define $u = u_0 v_1$, then $x = u_1 v_1(x) = \sum_{g \in G} g \cdot u_0(g^{-1} v_1 x) = \sum_{g \in G} u(g^{-1}x)$. Then by the previous lemma, we are done. □

We also want to show that every projective $k[G]$-module is of the form $P/\mathfrak{m}P$ for some projective $A[G]$-module P. Recall that we have shown in the last chapter that the projective envelop always exists and is unique (for group algebras at least).

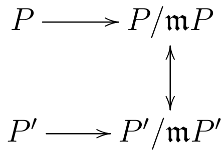
Theorem 2.2.4. If $\bar{P}$ is a projective $k[G]$-module, then $\bar{P} \cong P/\mathfrak{m}P$ for some projective $A[G]$-module P.

Proof. Let $p : P_n \to \bar{P}$ be a projective envelope of $\bar{P}$ as an $(A/\mathfrak{m}^n)[G]$-module. We claim that $\bar{P} \cong P_n/\mathfrak{m}P_n$. The map $P_n \to \bar{P}$ obviously kills $\mathfrak{m}P_n$, so we certainly have a surjection $P_n/\mathfrak{m}P_n \to \bar{P}$. We just have to show this is an isomorphism. There is a ($k[G]$-linear) splitting $s : \bar{P} \to P_n/\mathfrak{m}P_n$ since $\bar{P}$ is projective over $k[G]$. Now $s(\bar{P})$ maps isomorphically onto $\bar{P}$, but since p is essential the image of the splitting must be full: $s(\bar{P}) = P_n/\mathfrak{m}P_n$.

We now take $P = \varprojlim P_n$ (recall that $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$). We only need to show it is projective. Given a surjection $M \hookrightarrow M'$ and a map $P \to M'$. There exists a map $P_n \to M_n$ such that it commutes with the other maps. And glue them together to a map $P = \varprojlim P_n \to M = \varprojlim M_n$.

□

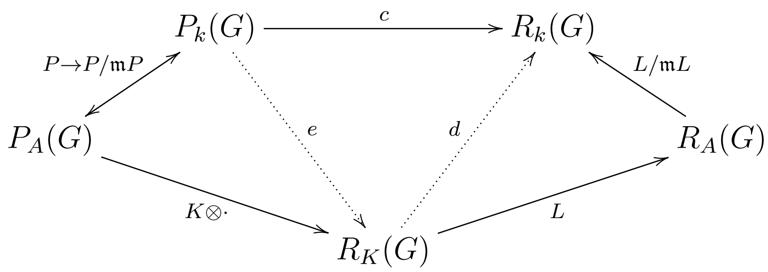
It remains to show uniqueness of this P. Suppose that we have a diagram



So, we have shown that the map $P_A(G) \to P_k(G)$ is an isomorphism. Then we can define the $K[G]$-module $K[G] \otimes_{A[G]} P = K \otimes_A A[G] \otimes_{A[G]} P = K \otimes_A P$. And this defines the map $e : P_k(G) \to R_K(G)$.

We can use projectivity to lift maps $P \to P'$ and $P' \to P$, which are inverse modulo the maximal ideal. This implies that their composition is the identity (as A is a local PID, $\phi(m) = \phi(1)\phi(m)$, so $m = \phi(1)m$ and $\phi(1) = 1$ as it is an ID).

So really, the CDE triangle looks like this



We can see from the diagram that there is some certain symmetry in the maps e and d. In the next section, we will explore this.

2.3 Commutativity and Adjointness

At this stage, it is worth to point out that $L/\mathfrak{m}L \cong A/\mathfrak{m} \otimes L$ in the construction of d. Consider the exact sequence $0 \to \mathfrak{m} \to A \to A/\mathfrak{m} \to 0$ and tensor with L, Because it is right exact, we have $\mathfrak{m} \otimes_A L \to A \otimes_A L \to A/\mathfrak{m} \otimes_A L \to 0$. And since our L is flat, we get the desired isomorphism. (See [AM69, Exercise 2, P31])

Proposition 2.3.1. The CDE triangle is commutative.

Proof. We start at $P_A(G)$. Let P be a projective $A[G]$-module. And let's chase the diagram. Going up we get $c(P/\mathfrak{m}P) = [P/\mathfrak{m}P]$. Going down, we first get $K \otimes P$, but then we have to choose a G-stable lattice, we may just as well choose P (Any finitely generated projective A-module is free), then it goes to $[P/\mathfrak{m}P] \in R_k(G)$. So the triangle is commutative. □

Now we explore the symmetry of the triangle. We introduce two pairings: $P_k(G) \times R_k(G) \to \mathbb{Z}$ and $R_K(G) \times R_K(G) \to \mathbb{Z}$. For $([P],[E])_{k[G]} \in P_k(G) \times R_k(G)$, we define $([P],[E])_{k[G]} = dim_k \mathrm{Hom}_{k[G]}(P, E)$. If $S_1, ..., S_k, P_1, ..., P_k$ are simple modules and the corresponding projective indecomposables, then they form a dual basis since P_i has a homomorphism to $S_i = P_i/\mathrm{Rad}(P_i)$ and to no other S_j for $j \neq i$. The other map is the familiar pairing from ordinary character theory: $([E],[E'])_{K[G]} = dim_K \mathrm{Hom}_{K[G]}(E, E')$, so $([E],[E'])_{K[G]} = \delta_{E,E'}$ if E, E' are simple, where $\delta_{E,E'}$ is the Kronecker Delta (at least when K is big enough).

Proposition 2.3.2. The maps d and e are adjoint with respect to these pairings, i.e. if $[P] \in P_k(G)$ and $[E] \in R_K(G)$, then $(e[P],[E])_{K[G]} = ([P], d[E])_{k[G]}$.

Proof. Let $P = [P'/\mathfrak{m}P']$ for some finitely generated projective $A[G]$-module P'. We pick a G-stable lattice $L \subset E$. The asserted identity then reads

$$dim_k \mathrm{Hom}_{k[G]}(P'/\mathfrak{m}P', L/\mathfrak{m}L) = dim_K \mathrm{Hom}_{K[G]}(K \otimes_A P', E).$$

We have

$$\begin{aligned}\mathrm{Hom}_{k[G]}(P'/\mathfrak{m}P', L/\mathfrak{m}L) &= \mathrm{Hom}_{A[G]}(P', L/\mathfrak{m}L)\\ &= \mathrm{Hom}_{A[G]}(P', L)/\mathrm{Hom}_{A[G]}(P', \mathfrak{m}L)\\ &= \mathrm{Hom}_{A[G]}(P', L)/\mathfrak{m}\mathrm{Hom}_{A[G]}(P', L)\\ &= k \otimes_A \mathrm{Hom}_{A[G]}(P', L),\end{aligned}$$

where the last line follows from the remark at the beginning of this section and the second identity comes from the projectivity of P as an $A[G]$-module.

On the other hand,

$$\begin{aligned}\mathrm{Hom}_{K[G]}(K \otimes_A P', E) &= \mathrm{Hom}_{K[G]}(K \otimes_A P', K \otimes_A L)\\ &= K \otimes_A \mathrm{Hom}_{A[G]}(P', L).\end{aligned}$$

Both P' and L' are free A-modules. Hence $\mathrm{Hom}_A(P', L)$ is a finitely generated free A-module. The ring A is Noetherian, so the A-module $\mathrm{Hom}_{A[G]}(P', L)$ is finitely generated as well. We now deduce from above that the dimensions of two sides are the same.

□

Note that in the previous chapter, we sometimes required the field to be algebraically closed. We now weaken it a bit.

Definition 2.3.3. The field F is called a splitting field for G if for any simple $F[G]$-module V , we have $\mathrm{End}_{F[G]}(V) = F$.

Clearly, If F is algebraically closed then it is a splitting field for G.

Theorem 2.3.4. Let e be the exponent of G (i.e., the lcm of orders of $g \in G$), and suppose that F contains a primitive e-th root of unity; then F is a splitting field for any subgroup of G. In particular, it is splitting for G.

The proof is technical, and is not very related to what we are doing, so we only leave a reference rather than give a full proof.

Proof. [Sch13, Theorem 14.2, p80] □

So we can get a splitting field of G by adding roots to $\mathbb{F}_p$. We now draw attentions to splitting fields. Note for a splitting field K, we have a linear isomorphism $R_K(G) \cong \mathrm{Hom}_{\mathbb{Z}}(R_K(G), \mathbb{Z})$ and similar isomorphisms for $P_k(G)$ and $R_k(G)$. If we fix the bases of the three Grothendieck groups, then with respect to these bases and by the previous proposition, we have $D{=}E^T$. We then have $C = DE = DD^T$. It follows that the Cartan matrix C is symmetric. And in particular it is square, which confirms the result of Theorem 1.6.8. (Note we reproved it, we didn't use it to build the triangle. Although we can not see the isomorphism is canonical.) We will later use this result to compute some characters.

We now consider two extreme examples (in the sense of the p-adic norm of $|G|$). The first one is when $|G|$ is not a multiple of p and the second one is when $|G| = p^m$.

Example 2.3.5. If G has order that is coprime to p, then all maps are identity maps (with respect to the obvious bases).

The map c is the identity map is because of Mashcek's Theorem. Let S be a simple $k[G]$-module. Then it is also projective. By Proposition 2.2.4, there is an $A[G]$-module P such that $P/\mathfrak{m}P \cong S$. Let $S' = K \otimes_A P$, then $d(S') = S$. Obviously, if $K \otimes_A P$ is indecomposable (i.e., simple by Mashcek) then P was indecomposable. Vice versa, if P is indecomposable then the above reasoning says that $P/\mathfrak{m}P$ is simple. Because of $P/\mathfrak{m}P = d(K \otimes_A P)$ it follows that $K \otimes_A P$ must be indecomposable. Visibly, this is the inverse of the map d. Since e is the dual of d, it is an isomorphism too. And obviously, with respect to these bases, they are identity matrices.

Example 2.3.6. If G is a p-group with order p^n. Then by Corollary 1.4.9 and Theorem 2.2.4, we can identify $P_k(G) = \langle k[G] \rangle$ and $R_k(G) = \langle k \rangle$ with $\mathbb{Z}$. Then clearly, the map c is multiplication by p^n. For any $K[G]$-module P and any G-stable lattice L in P, we have $dim_K P = dim_k L/\mathfrak{m}L$. Hence the map d maps P to its dimension as a K vector space.

There is one more example that we can consider: $G = P' \times P$, where P is a p group and P' has order coprime to p. Then, because it is a direct product, we have $k[G] = k[P] \otimes k[P']$.

Lemma 2.3.7. A $k[G]$-module M is semisimple iff P acts trivially on M.

Proof. ($\Longleftarrow$) This follows from that every $k[P']$-module is semisimple and $k[P]$ and $k[P']$ commutes.

($\Longrightarrow$) Assume WLOG M is simple. The subspace M' of M consisting of elements fixed by P is not zero (this is a restatement of Corollary 1.4.9). Since P is normal in G, the subspace M' is stable under G, and thus equal to M, which means that P acts trivially. □

Lemma 2.3.8. A $k[G]$-module P is projective iff it is isomorphic to $F \otimes k[P]$, where F is a $k[P']$-module.

Proof. ($\Longleftarrow$) Since F is a projective $k[P']$-module, $F \otimes k[P]$ is a projective $k[G]$-module (by the universal property of tensor product).

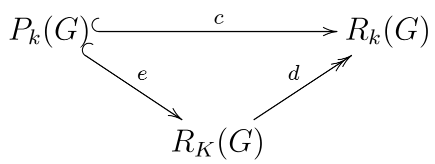
($\Longrightarrow$) Note that F is the largest quotient of $F \otimes k[P]$ such that P acts trivially. By the previous lemma, F is semisimple (as a $k[G]$-module). Via the proof of Proposition 1.6.6, we see that if P is a projective module, and if E is its largest semisimple quotient, then P is a projective envelope for E. Therefore $F \otimes k[P]$ is the projective envelope for F. However, every projective module is the projective envelope of its largest semisimple quotient. Now repeat for all F, we see that every projective module has the form $F \otimes k[P]$. □

The previous lemma shows in particular that the Cartan matrix is the scalar matrix with p^n on the diagonal. Indeed, for $F \otimes k[P]$ to be indecomposable, we need F to be indecomposable. But by Maschke's Theorem, this is the same as being simple. And $[k[P]] = p^n \cdot [k]$. This shows the claim.

We will use these results in the future.

2.4 Brauer's Induction Theorems and More Properties

In this section, we want to prove that c is injective, d is surjective and e is injective. We will need Brauer's induction theorems in order to do it. We will need these properties in the next section (especially Theorem 2.5.14). So the CDE triangle looks like this



But first, let's establish more preliminaries.

Recall that given a subgroup $H \subset G$, we have two maps $\mathrm{Res}_H^G : R_K(G) \to R_K(H)$ and $\mathrm{Ind}_H^G : R_K(H) \to R_K(G)$ (respectively, R_k and P_k). We will take $[V] \cdot [W]$ to be $[V \otimes_k W]$ (respectively, K). This makes these abelian groups into rings.

Remark 2.4.1. $\mathrm{Ind}_H^G(y) \cdot x = \mathrm{Ind}_H^G(y \cdot \mathrm{Res}_H^G(x))$ for any $x \in R_k(G)$ and $y \in R_k(H)$ (respectively, K). This follows from the associativity of tensor products.

It is also absolutely clear that the maps c, d, e will commute with Res_H^G. For the maps c, e, it is also clear that it will commute with Ind_H^G. The map d needs a bit more care.

Lemma 2.4.2. d commutes with Ind_H^G.

Proof. Let W be a $K[H]$-module. We choose an H-stable lattice $L \subset W$. Then

$$\mathrm{Ind}_H^G(d[W]) = \mathrm{Ind}_H^G(d[L/\mathfrak{m}L]) = [k[G] \otimes_{k[H]} (L/\mathfrak{m}L)].$$

Moreover, $K[G] \otimes_{K[H]} L \cong L^{[G:H]}$ is a G-stable lattice in $K[G] \otimes_{K[H]} W \cong W^{[G:H]}$. Hence,

$$\begin{aligned}\mathrm{Ind}_H^G(d[W]) &= [(K[G] \otimes_{K[H]} L)/\mathfrak{m}(K[G] \otimes_{K[H]} L)] \\ &= [K[G] \otimes_{K[H]} L/\mathfrak{m}L].\end{aligned}$$

□

We will work toward the statement of Brauer's Induction Theorem. We will need it to prove the injectivity and surjectivity of the maps.

Definition 2.4.3. Let p be a prime number. A group H is called p-elementary if it is a direct product $H = C \times P$ of a cyclic group C and a p-group P. A group is called elementary if it is p-elementary for some prime p.

Since C is cyclic, we can further assume that C has order coprime to p. Let $\mathcal{H}$ be the family of elementary subgroups of G.

Theorem 2.4.4 (Brauer's Theorem)**.** Suppose that that K is a splitting field for every subgroup of G, then we have

$$\sum_{H \in \mathcal{H}} \mathrm{Ind}_H^G(R_K(H)) = R_K(G).$$

I.e., every representation of G over K is a direct sum of induction representations of elementary subgroups.

Remark 2.4.5. A similar theorem is also true if we don't assume K to be split. Although, we are not going to use it.

At the cost of losing positive linear combinations, we can even assume that the elements of $R_K(H)$ we use are 1-dimensional. This is gathered into the following theorem.

Theorem 2.4.6. Suppose that K is a splitting field for any subgroup of G, and let $x \in R_K(G)$ be any element; then there exist integers $m_1, \cdots, m_r$ (not necessarily positive), elementary subgroups $H_1, \cdots, H_r$, and one dimensional $F[H_i]$-modules W_i such that $x = \sum_{i=1}^r m_i \mathrm{Ind}_{H_i}^G(W_i)$.

The proof of these two theorems are hard (the second one will follow from the first). It uses Clifford theory and Solomon's Theorem. It probably deserves a fourth year project on its own. We will only give the reference to the proof rather than giving a full proof. Also note that the second statement implies that Artin L-functions are meromorphic.

Proof. See either [Ser77, Theorem 27] or [Sch13, Theorem 13.1]. □

Using the above lemma, we get the following:

Theorem 2.4.7. We also have the identities

$$\sum_{H\in\mathcal{H}} \operatorname{Ind}_H^G(R_k(H)) = R_k(G)$$

and

$$\sum_{H\in\mathcal{H}} \operatorname{Ind}_H^G(P_k(H)) = P_k(G).$$

Proof. Let 1_K (i.e., the trivial rep) (respectively 1_k) be the identity element in $R_K(G)$ (respectively $R_k(G)$). By Brauer's Theorem, we can write $1_K = \sum_{H\in\mathcal{H}} \operatorname{Ind}_H^G(x_H)$, where $x_H \in R_K(H)$. It is clear that $d(1_K) = 1_k$. Apply the above lemma to this equation, we get that $1_k = \sum_{H\in\mathcal{H}} \operatorname{Ind}_H^G(x'_H)$, where $x'_H = d(x_H) \in R_k(H)$. Thus for $y \in R_k(G)$ (respectively $P_k(G)$), we get $y = 1_k \cdot y = \sum_{H\in\mathcal{H}} \operatorname{Ind}_H^G(x'_H) \cdot y = \sum_{H\in\mathcal{H}} \operatorname{Ind}_H^G(x'_H \cdot \operatorname{Res}_H^G y)$, by the Remark 2.4.1. And this proves the theorem. □

Now we are ready to talk about the surjectivity of d. As noted above, this is true for all K, but we will only prove for K is a splitting field.

Theorem 2.4.8. The map d is surjective.

Proof. Using the above theorem and the fact that d commutes with Ind_H^G, we just need to show $R_k(H) = d(R_K(H))$ where H is elementary. So we assume G is elementary (for some prime p'). We may as well assume this $p' = p = \operatorname{char}(k)$ (otherwise we will just have Example 2.3.5).

Let $G = P \times C$, where P is a p group and C is a cyclic group with order coprime to p. So we are back in the product case. Since the simple modules form a basis for $R_k(G)$, we may as well assume the $k[G]$-module S is simple. By Corollary 1.4.9, considering S as a P representation, we have the trivial representation is a sub-representation of S. Therefore $S^P := \{s \in S : gs = s, \forall g \in P\} \neq \{0\}$. Since P is a normal, the $k[P]$-submodule S^P in fact is a $k[G]$-submodule of S. S is simple, therefore $S' = S$. So P acts trivially on S. Therefore the action factors through the projection $k[G] \to k[C]$. But C has order coprime to p, so by Example 2.3.5, we can find a lift of S as a $k[C]$-module. Now view it as a $K[G]$-module through the projection $K[G] \to K[H]$ and this is a lift of S as a $K[G]$-module. □

Corollary 2.4.9. The map e is injective.

Proof. Since K is a splitting field, we have that e is the dual of d. Since d is surjective, we have that e is injective. □

Corollary 2.4.10. If P and P' are two projective $A[G]$-modules and $K \otimes_A P$ and $K \otimes_A P'$ are isomorphic, then $P \cong P'$ as $A[G]$-modules.

Proof. This follows directly from the fact that e is injective and $P_A(G) \cong P_k(G)$. □

Lemma 2.4.11. If $|G| = p^n m$, where m is coprime to p. Then every element of $R_k(G)$ divisible by p^n is in the image of c.

Again this is true for all K, but we only prove for splitting fields.

Proof. As in the previous theorem, we can assume that G is elementary. Write $G = P \times C$, which C has order coprime to p. We need to show the cokernel of c is killed by p^n. By the argument at the very end of last section, we see the matrix C is given by multiplication by p^n. Therefore the cokernel is killed by p^n. □

Theorem 2.4.12. c is injective and the cokernel is a finite p group.

Proof. The statement of the cokernel is a finite p group follows directly from the last lemma. Recall that $P_k(G) \cong \mathbb{Z}^r \cong R_k(G)$ as abelian groups, where r is the number of simple modules/projective indecomposables. Since the cokernel is finite, so it has rank 0 and $R_k(G)$ and $im(c)$ has the same rank. So the matrix C is square and is of full rank, so c is injective. □

This has the following obvious corollaries:

Corollary 2.4.13. If two projective $k[G]$-modules have the same composition factors, then they are isomorphic.

Corollary 2.4.14. The determinant of C is a power of p.

2.5 The Brauer Character

Finally, we are ready to discuss the characters for modular representations. These characters are named after its founder and one of the pioneers of modular representation theory at that time, Richard Brauer[2].

Recall that we fix K to be sufficient large, i.e., contains a primitive root of $\text{lcm}_{g\in G}|g|$. Also recall that in Lemma 1.4.4, we showed that for any $g \in G$, there exist uniquely determined elements g_{reg} and g_{uni} in G such that g_{reg} is p-regular, g_{uni} is p-unipotent and $g = g_{\text{reg}}g_{\text{uni}} = g_{\text{uni}}g_{\text{reg}}$. We let the set $G_{\text{reg}} := \{g \in G : g \text{ is } p\text{-regular}\}$. For simplicity, we will assume k to be algebraically closed. We write $\text{Cl}(G, k)$ to be the set of class functions from G taking values in k. We also take an inclusion from K to $\mathbb{C}$ (see [AM69]).

[2] https://en.wikipedia.org/wiki/Richard_Brauer

Definition 2.5.1. Given a $k[G]$-module V and any element $g \in G$, we let $\alpha_{g,i}$ be the eigenvalues of the k-linear endomorphism $g : V \to V$ for $i = 1, \dots, \dim V$ and the k-character is defined as $\chi_V(g) = \alpha_{g,1} + \cdots + \alpha_{g,\dim V}$.

This is the exact same construction as in the case of ordinary characters (over $\mathbb{C}$), and it has lots of the same properties as the ordinary characters, in particular it is constant over conjugacy classes. Since we did not define orthogonal relations for them and Maschke's Theorem does not necessarily hold, linear independence needs a bit more work:

Lemma 2.5.2. The k-characters $\chi_V \in \mathrm{Cl}(G,k)$, where V is simple, are k-linearly independent.

Proof. Consider $A = k[G]/\mathrm{Rad}(k[G])$. By Wedderburn, we have that $A = \prod_{i=1}^{r} \mathrm{End}_k(V_i)$ (k is algebraically closed), where V_i's are simple of both A and $k[G]$ by Theorem 1.6.8. For $1 \le i \le r$, we can pick an element $\phi_i \in \mathrm{End}_k(V_i)$ with $tr(\phi_i) = 1$. Let ψ_i be lifts of them in $k[G]$, then we have $\psi_i : V_j \to V_j = \phi_i$ if $i = j$ and 0 otherwise. Extend by k-linearity, we get $\bar{\chi}_{V_j} : k[G] \to k$ such that $\bar{\chi}_{V_j}(\psi_i) = \mathrm{tr}(a_i; V_j) = 1$ if $i = j$ or 0 otherwise. Then if $\sum c_j \chi_{V_j} = 0$ in $\mathrm{Cl}(G,k)$, we get $\sum c_j \bar{\chi}_{V_j} = 0$ in $\mathrm{Hom}_k(k[G],k)$ and hence $0 = \sum c_j \bar{\chi}_{V_j}(a_i) = c_i$ for all i. □

Thus we have defined an injective map $\mathrm{Tr} : k \otimes_{\mathbb{Z}} R_k(G) \to \mathrm{Cl}(G,k)$. We note that $R_k(G) \to k \otimes_{\mathbb{Z}} R_k(G)$ is not injective (because k has finite characteristic). Next we prove an important observation:

Lemma 2.5.3. Let V be a $k[G]$-module and let $g \in G$, then sequences $\alpha_{g,1}, \dots, \alpha_{g,\dim V}$ and $\alpha_{g_{\mathrm{reg}},1}, \dots, \alpha_{g_{\mathrm{reg}},\dim V}$ coincide up to a reordering; in particular, we have $\chi_V(g) = \chi_V(g_{\mathrm{reg}})$.

Proof. Since the order of g_{reg} is prime to p the vector space $V = V_1 \oplus \cdots \oplus V_t$ decomposes into the different eigenspaces V_j for the linear endomorphism $g_{\mathrm{reg}} : V \to V$. The elements $g_{\mathrm{reg}} g_{\mathrm{uni}} = g_{\mathrm{uni}} g_{\mathrm{reg}}$ commute. Hence g_{uni} respects the eigenspaces of g_{reg}, i.e., $g_{\mathrm{uni}}(V_j) = V_j$ for any $1 \le j \le t$. The cyclic group $\langle g_{\mathrm{uni}} \rangle$ is a p-group. Again, as we saw many times, by Corollary 1.4.9, the only simple $k[\langle g_{\mathrm{uni}} \rangle]$-module is trivial, so the only eigenvalue of $g_{\mathrm{uni}} : V \to V$ is 1. So we can find a basis of V_j such that the matrix $g_{\mathrm{uni}}|_{V_j}$ is upper triangular and with 1's on the diagonal. The matrix of $g_{\mathrm{reg}}|_{V_j}$ is upper triangular and with α_j's on the diagonal, where α_j is the corresponding eigenvalue. The matrix of $g|_{V_j}$ then is still upper triangular and with α_j's on the diagonal. It follows that $g|_{V_j}$ has a single eigenvalue which coincides with the eigenvalue of $g_{\mathrm{reg}}|_{V_j}$.

□

Therefore we have the injective map

$$\mathrm{Tr}_{\mathrm{reg}} : k \otimes_{\mathbb{Z}} R_k(G) \xrightarrow{\mathrm{Tr}} \mathrm{Cl}(G,k) \xrightarrow{\mathrm{Res}} \mathrm{Cl}(G_{\mathrm{reg}},k). \tag{2.1}$$

In order to talk about Brauer characters, we need to discuss some properties of the field K.

Remark 2.5.4. Let $\alpha \in K$ be any root of unity, then $\alpha \in A$. Indeed, recall A is local and the maximal ideal will induce a norm on K. This is even more intuitive in the $\mathbb{Q}_p$ case. Let e denote the exponent of G and let $e = e'p^s$ with p coprime to e'. Let $\mu_{e'}(K)$ and $\mu_{e'}(k)$ be subgroups of $K^\times$ and $k^\times$ consists of all e'-th roots of unity. They are both cyclic of order e' since A is splitting for G and k is algebraically closed of characteristic coprime to e'. Therefore we have a well-defined homomorphism from $\mu_{e'}(K)$ to $\mu_{e'}(k)$, i.e., the mod $\mathfrak{m}$ map. Furthermore, this is an isomorphism. Indeed, we just need to show it is injective since they are the same size, but the polynomial $x^{e'} - 1$ is separable since p is coprime to e'.

Consider the inverse of this map and we can make the following definition:

Definition 2.5.5. For any $k[G]$-module v, we define the Brauer character to be the K-valued class function

$$\begin{aligned} \beta_V : G_{\text{reg}} &\to K \\ g &\mapsto \overline{\alpha_{g,1}} + \cdots + \overline{\alpha_{g,\dim V}}, \end{aligned}$$

where the bars mean taking the inverse map.

Remark 2.5.6. It is important to note that it is from G_{reg} not G. It is a map

$$\begin{aligned} \mathrm{Tr}_B : R_k(G) &\to \mathrm{Cl}(G_{\text{reg}}, K) \\ [V] &\mapsto \beta_V. \end{aligned}$$

Because otherwise we can not necessarily take the lift back. Also note that $\beta_V(g) \equiv \chi_V(g)$ mod $\mathfrak{m}$ for any $g \in G_{\text{reg}}$ by construction.

We will firstly list some very obvious properties that the Brauer characters have:

Lemma 2.5.7.

1. $\beta_V(1) = \dim(V)$
2. β_V is constant on conjugacy classes of G_{reg}
3. If $0 \to A \to B \to C \to 0$ is short exact, then $\beta_B = \beta_A + \beta_C$
4. $\beta_{V \otimes W} = \beta_V \times \beta_W$
5. $\chi(g) \equiv \beta(g_{\text{reg}})$ mod $(\mathfrak{m})$
6. The square in Remark 2.5.9 is commutative

Proof. The proof of $1 - 4$ is exactly the same in the ordinary case, and $5, 6$ are true by construction. ☐

Lemma 2.5.8. The Brauer characters $\beta_V \in \mathrm{Cl}(G, K)$, where V is simple, are K-linearly independent.

Proof. Suppose $\sum c_V \beta_V = 0$. We may assume that all c_V lie in A (by multiplying a high enough power of the generator of the ideal $\mathfrak{m}$). So c_V must lie in $\mathfrak{m}$ (since k-characters are linear independent). So write $c_V = \pi d_V$, where π is the generator of $\mathfrak{m}$ and $d_V \in A$. Then $0 = \sum c_V \beta_V = \pi \sum d_V \beta_V$, so we have $\sum d_V \beta_V = 0$. So $d_V \in \mathfrak{m}$, and we can repeat like this. So we have $c_V \in \cap_{i \geq 0} \mathfrak{m}^i = \{0\}$. □

Remark 2.5.9. Note by construction, we have a commutative diagram

$$\begin{array}{ccc} R_K(G) & \xrightarrow{d} & R_k(G) \\ \downarrow{\scriptstyle \mathrm{Tr}} & & \downarrow{\scriptstyle \mathrm{Tr}_B} \\ \mathrm{Cl}(G, K) & \xrightarrow{\mathrm{Res}} & \mathrm{Cl}(G_{\mathrm{reg}}, K) \end{array}$$

Thus we have a commutative diagram

$$\begin{array}{ccc} K \otimes_{\mathbb{Z}} R_K(G) & \xrightarrow{\mathrm{id} \otimes d} & K \otimes_{\mathbb{Z}} R_k(G) \\ \downarrow{\scriptstyle \mathrm{Tr}} & & \downarrow{\scriptstyle \mathrm{Tr}_B} \\ \mathrm{Cl}(G, K) & \xrightarrow{\mathrm{Res}} & \mathrm{Cl}(G_{\mathrm{reg}}, K) \end{array}$$

We know that the map Tr is an isomorphism by results from ordinary character theory and Res is clearly surjective. Hence Tr_B is also surjective. Furthermore, it is injective by the previous lemma. So we have the map Tr_B is an isomorphism. For convenience, this is captured into the next theorem.

Theorem 2.5.10. The map $\mathrm{Tr_B} : K \otimes_{\mathbb{Z}} R_k(G) \to \mathrm{Cl}(G_{\mathrm{reg}}, K)$ is an isomorphism.

Remark 2.5.11. In particular, they have the same dimension. As a consequence, the number of isomorphism classes of simple $k[G]$-modules coincides with the number of conjugacy classes of p-regular elements in G. Therefore the injective map defined in equation 2.1 is an isomorphism. Also the kernel of d consists of the elements whose character are 0 on G_{reg}.

So far we have characters for $R_k(G)$ (the Brauer characters β) and $R_K(G)$ (the ordinary characters χ). To fully explore the power of the CDE triangle, we need to have something for $P_k(G)$ as well. For a projective module P, we proved it corresponds to an $A[G]$-module M. We define the character η_P to be the ordinary character of $K \otimes_A M$, i.e., the character of $e(P)$.

Proposition 2.5.12. The value $\eta_P(1)$ is a multiple of p^k, where $|G| = mp^k$, m coprime to p, and $\eta_P(g) = 0$ if $g \in G \setminus G_{\mathrm{reg}}$.

Proof. The first assertion following directly by restricting to a Sylow p-subgroup and from Corollary 1.6.10.

Now for the second assertion, write $g = g_{\mathrm{reg}} g_{\mathrm{uni}}$. We want if $g_{\mathrm{uni}} \neq 1$, then $\eta_P(g) = 0$. Consider the cyclic subgroup $\langle g_{\mathrm{uni}} \rangle$. P is free as a module over $k[\langle g_{\mathrm{uni}} \rangle]$ by Corollary 1.6.10 and 1.4.9. Since g_{reg} and g_{uni} commutes with each other, we have a decomposition

$P = \bigoplus P_\alpha$ (as a $k[\langle g_{\mathrm{uni}}\rangle]$-module), where α runs through the eigenvalue of g_{reg} on P, and $P_\alpha = \{x | g_{\mathrm{reg}} x = \alpha x\}$. Therefore each P_α is a free $k[\langle g_{\mathrm{uni}}\rangle]$-module. If $g_{\mathrm{uni}} \neq 1$, then $\mathrm{Tr}(g|_P) = \sum_\alpha \alpha \mathrm{Tr}(g_{\mathrm{uni}}|_{P_\alpha})$. But $\mathrm{Tr}(g_{\mathrm{uni}}|_{P_\alpha}) = 0$ as P_α is free, hence the result. □

Thus we have defined a (unique) map $\mathrm{Tr}_{\mathrm{proj}} : P_k(G) \to \mathrm{Cl}(G_{\mathrm{reg}}, K)$ such that the square

$$\begin{array}{ccc} P_K(G) & \xrightarrow{e} & R_K(G) \\ \downarrow{\scriptstyle \mathrm{Tr}_{\mathrm{proj}}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathrm{Cl}(G_{\mathrm{reg}}, K) & \xrightarrow{\mathrm{Ext}} & \mathrm{Cl}(G, K) \end{array}$$

is commutative.

Remark 2.5.13. As in the case of Remark 2.5.9, we have the following commutative diagram

$$\begin{array}{ccc} K \otimes_{\mathbb{Z}} P_K(G) & \xrightarrow{\mathrm{id}\otimes e} & K \otimes_{\mathbb{Z}} R_K(G) \\ \downarrow{\scriptstyle \mathrm{Tr}_{\mathrm{proj}}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathrm{Cl}(G_{\mathrm{reg}}, K) & \xrightarrow{\mathrm{Ext}} & \mathrm{Cl}(G, K) \end{array}$$

Since e is injective and Tr is bijective, we see that $\mathrm{Tr}_{\mathrm{proj}}$ is injective. But

$$\dim_K K \otimes_{\mathbb{Z}} P_k(G) = \dim_K K \otimes_{\mathbb{Z}} R_k(G) = \dim_K \mathrm{Cl}(G_{\mathrm{reg}}, K)$$

where the first equality follows from Theorem 1.6.8 and the second follows from Brauer-Nesbitt, so $\mathrm{Tr}_{\mathrm{proj}}$ is bijective:

Theorem 2.5.14. The map $\mathrm{Tr}_{\mathrm{proj}} : K \otimes_{\mathbb{Z}} P_k(G) \to \mathrm{Cl}(G_{\mathrm{reg}}, K)$ is an isomorphism.

2.5.1 A bit more theory

Recall the CDE triangle, tensor with K we get the triangle

$$\begin{array}{ccccc} K \otimes_{\mathbb{Z}} P_k(G) & & \xrightarrow{\mathrm{id}\otimes c} & & K \otimes_{\mathbb{Z}} R_k(G) \\ & \searrow^{\mathrm{id}\otimes e} & & \nearrow^{\mathrm{id}\otimes d} & \\ & & K \otimes_{\mathbb{Z}} R_K(G) & & \end{array}$$

But by the previous theorems we can identify them with class functions. So we get the triangle

$$\begin{array}{ccccc} \mathrm{Cl}_0(G, K) & & \xrightarrow{\mathrm{id}\otimes c} & & \mathrm{Cl}(G_{\mathrm{reg}}, K) \\ & \searrow^{\mathrm{id}\otimes e} & & \nearrow^{\mathrm{id}\otimes d} & \\ & & \mathrm{Cl}(G, K) & & \end{array}$$

Here, $\mathrm{Cl}_0(G,K)$ is the set of class functions on G that are zero off G_{reg}. The map $\mathrm{id}\otimes d$ can be identified with the map Res: $\mathrm{Cl}(G,K) \to \mathrm{Cl}(G_{\mathrm{reg}},K)$. The map $\mathrm{id}\otimes e$ can be identified with the map Ext: $\mathrm{Cl}_0(G,K) \to \mathrm{Cl}(G,K)$ which is an inclusion. And The map $\mathrm{id}\otimes c$ is an isomorphism.

And recall that we proved $C = DD^t$.

We want to have orthogonality relations for Brauer characters just like as in the ordinary case. Of course, we are going to do it using the orthogonality relations we have for ordinary characters.

Proposition 2.5.15. Let β_i denote the Brauer character of a simple $k[G]$-module and let η_j denote the character of an indecomposable projective $k[G]$-module. Let $C = (c_{ij})$ and $C^{-1} = (f_{ij})$. Then:

1. $\frac{1}{|G|}\sum_{g\in G_{\mathrm{reg}}} \beta_i(g)\eta_j(g^{-1}) = \delta_{ij}$
2. $\frac{1}{|G|}\sum_{g\in G_{\mathrm{reg}}} \beta_i(g)\beta_j(g^{-1}) = f_{ij}$
3. $\frac{1}{|G|}\sum_{g\in G_{\mathrm{reg}}} \eta_i(g)\eta_j(g^{-1}) = c_{ij}$

We write $\langle\alpha,\beta\rangle$ for the above inner product.

Proof. First note that c is injective and has finite cokernel, therefore C is invertible (over $\mathbb{Q}$).

We know that

$$\chi_j = \sum_i d_{ij}\beta_i \text{ on } G_{\mathrm{reg}} \tag{2.2}$$

$$\eta_i = \sum_j d_{ij}\chi_j \text{ on } G \tag{2.3}$$

$$\eta_j = \sum_i c_{ij}\beta_i \text{ on } G_{\mathrm{reg}}. \tag{2.4}$$

So

$$\begin{aligned}\langle\eta_i,\eta_j\rangle =& \langle\sum_k d_{ik}\chi_k, \sum_m d_{jm}\chi_m\rangle \\ =& \sum_{k,m} d_{ik}d_{jm}\langle\chi_k,\chi_m\rangle \\ =& \sum_{k,m} d_{ik}d_{jm}\delta_{km} \\ =& c_{ij},\end{aligned}$$

where the first equality comes from equation 2.3, the third equality comes from the property of ordinary characters and the final equality comes from $C = DD^T$.

On the other hand, using equation 2.4, we have that

$$\begin{aligned}\langle \eta_i, \eta_j \rangle =& \langle \sum_k c_{ki}\beta_k, \sum_m c_{mj}\beta_m \rangle \\ c_{ij} =& \sum_{k,m} c_{ki}c_{mj}\langle \beta_k, \beta_m \rangle,\end{aligned}$$

where the second equality comes from the above and rearranging. This is an array of $|G_{\mathrm{reg}}|^2$ linear equations. A bit of linear algebra shows that $\langle \beta_k, \beta_m \rangle = f_{ij}$.

Finally,

$$\begin{aligned}\langle \beta_i, \eta_j \rangle =& \langle \beta_i, \sum_k c_{kj}\beta_k \rangle \\ =& \sum_k c_{kj} f_{ik} \\ =& \delta_{ij},\end{aligned}$$

where the first equality is from equation 2.2, the second equality is from the above and the final equality is by definition.

□

Next we need a technical result on a particular class of characters.

Definition 2.5.16. Let χ be an ordinary irreducible character, its p-defect is $\mathrm{val}_p(|G|/\chi(1))$.

Proposition 2.5.17. If χ_i be an ordinary irreducible character with p-defect 0. Then χ_i is in fact a character of $K \otimes_A P$, where P is a projective indecomposable over $A[G]$. Moreover $P/\mathfrak{m}P$ is simple and projective as a $k[G]$-module.

Proof. Let M_i be the module correspond to χ_i. We define $e = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi_i(g^{-1})g \in K[G]$. We claim that e is a idempotent. Indeed, by the orthogonality property of characters, it acts as the identity on the simple module with character χ, and as zero on any simple module with different characters. So applying it twice to any representation is the same as applying it once. So by considering the regular representation, it shows that it's an idempotent. Note that since it has p-defect 0 and the characters are algebraic numbers, e is actually defined over A. Let P_i be the projective indecomposable $A[G]$-module correspond to e and let $k \otimes P_i$ be the corresponding $k[G]$-module. Let η_i be the character for it, we then have that $\langle \eta_i, d(\chi_i) \rangle = \langle \eta_i, \sum_{j=1}^{i} d_{ji}\beta_j \rangle = d_{ji}$ by the above proposition. So in particular M is a summand of say $K \otimes_A P$. So $eP \neq 0$, but $P = eP \oplus (1-e)P$ and P is indecomposable, so $eP = P$. So $K \otimes_A P = \alpha M$ for some positive integer α. So χ must vanish on all singular classes by Proposition 2.5.12. Since the characters of $K \otimes_A P$ form a basis of them and $\alpha \geq 1$, we see $\alpha = 1$ and hence $M = K \otimes_A P$. Moreover, $P/\mathfrak{m}P$ is clearly projective, it remains to show it is also simple. But by the above equation exactly one $d_{ji} \neq 0$ and therefore it must be simple. □

Remark 2.5.18. The construction of the idempotent e seems to be a bit magical. But there is a more general theory behind it (see Chapter 3 and Afterword).

2.5.2 Examples

Example 2.5.19. (C_{p^n})

Recall that all characters of an abelian group are 1 dimensional. If k has characteristic p, then G_{reg} only consists of the identity element. So the only Brauer character is the trivial one, and

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

And $C = DD^t = p^n$, which agrees with Example 2.3.6.

If k has characteristic coprime to p, then the Brauer characters coincide with the ordinary characters, which agrees with Example 2.3.5.

Example 2.5.20. (Cyclic groups)

Let G be an cyclic group, write $G = P_1 \times \cdots \times P_n$, where P_i is a cyclic group of order $p_i^{n_i}$.

Again, all characters are 1 dimensional. If $p \neq p_i$ for all i, then we are back in Example 2.3.5. If $p = p_i$ for some i, then G_{reg} has $\frac{|G|}{{p_i}^{n_i}} = \Pi_{j \neq i} {p_j}^{n_j}$ elements. Recall that the characters of an abelian group of order n is given by the n-th roots of unity. After fixing a generator and listing the elements/conjugacy classes in increasing order, the matrix D looks like the $|G_{\text{reg}}| \times |G|$ matrix

$$\begin{pmatrix} 1 & \dots & 0 & \cdots & \cdots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \cdots & \cdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \cdots & \cdots & 0 & \dots & 1 \end{pmatrix},$$

and C looks like the $|G_{\text{reg}}| \times |G_{\text{reg}}|$ matrix

$$\begin{pmatrix} {p_i}^{n_i} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & {p_i}^{n_i} \end{pmatrix}.$$

This agrees with the result after Lemma 2.3.8. And the determinate is clearly a power of p_i.

Example 2.5.21. (S_3)

Recall the ordinary character table of S_3 is

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Fix $p = 3$, then we can delete the third column and $\text{Res}(\chi_3)$ will be the sum of the first two. So

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

and

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

And the determinate is 3.

Example 2.5.22. (A_5)

Recall the ordinary character table of A_5 is

	1	(12)(34)	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Fix $p = 2$. Note that $\chi_3 + \chi_2 = \chi_1 + \chi_5$ on G_{reg}, hence $\text{Res}(\chi_2)$ and $\text{Res}(\chi_3)$ are not irreducible. We then must have $\chi_2 - \chi_1$ is a Brauer character of a simple $k[G]$-module and so is $\chi_3 - \chi_1$. Note χ_4 has 2-defect 0 (since $60/4 = 15$), and hence is irreducible on G_{reg}. Hence

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

and

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

. And the determinate is $4 = 2^2$

My supervisor is particularly interested in $L_2(7)$, so here it is.

Example 2.5.23. ($L_2(7)$)

Recall the ordinary character table of $L_2(7)$:

Size of Conj. Classes	1	21	56	42	24	24
Ord. of Elements	1	2	3	4	7	7
χ_1	1	1	1	1	1	1
$\chi_3^{(1)}$	3	-1	0	1	ω	ω^*
$\chi_3^{(2)}$	3	-1	0	1	ω^*	ω
χ_6	6	2	0	0	-1	-1
χ_7	7	-1	1	-1	0	0
χ_8	8	0	-1	0	1	1

Here $\omega = \frac{-1+\sqrt{-7}}{2}$ and ω^* is its complex conjugation. ([Wil11, Example 2.7.2])

Fix $p = 2$. If we look at the p-regular part (i.e., ignore the second and fourth columns), we have that $\chi_6 = \chi_3^{(1)} + \chi_3^{(2)}$ and $\chi_7 = \chi_1 + \chi_3^{(1)} + \chi_3^{(2)}$ on G_{reg}. χ_8 has 2-defect 0, since $168/8 = 21$. Therefore the matrix D is:

	β_1	β_3^1	β_3^2	β_8
χ_1	1	0	0	0
$\chi_3^{(1)}$	0	1	0	0
$\chi_3^{(2)}$	0	0	1	0
χ_6	0	1	1	0
χ_7	1	1	1	0
χ_8	0	0	0	1

And the matrix $C = D^T D$ is $\begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 3 & 2 & 0 \\ 1 & 2 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

And the determinate is $8 = 2^3$. In particular we see that the corresponding indecomposable projective module P_8 for S_8 is equal to S_8 and S_8 is projective. And $dimP_1 = 8$, $dimP_3^1 = dimP_3^2 = 16$. By Corollary 1.6.9, we have the decomposition that

$$\overline{\mathbb{F}_2}(L_2(7)) = P_1 \oplus P_3^{1\oplus 3} \oplus P_3^{2\oplus 3} \oplus P_8{}^{\oplus 8}.$$

Also note, from the theory in the final section of chapter 1, we see the radical series for P_1 has top and bottom terms equal to S_1 and P_3^1 and P_3^2 are dual to each other.

Let's also verify some orthogonality relations on this. Note according to the first row of C, then character of P_1 is $(8, 0, 2, 0, 1, 1)$, inner product with β_1 will give us

$$\frac{1}{168}(8 + 56 \times 2 + 24 \times 1 + 24 \times 1) = 1;$$

inner product with β_2 will give us

$$\frac{1}{168}(8 \times 3 + 56 \times 2 \times 0 + 24 \times 1 \times \omega + 24 \times 1 \times \omega^*) = 0;$$

inner product with itself will give us

$$\frac{1}{168}(8 \times 8 + 56 \times 2 \times 2 + 24 \times 1 + 24 \times 1) = 2,$$

which is c_{11}.

Finally β_1 inner product with itself gives

$$\frac{1}{168}(8 + 56 + 24 + 24) = \frac{5}{8}.$$

This is expected since $C^{-1} = \frac{1}{8}\begin{pmatrix} 5 & -1 & -1 & 0 \\ -1 & 5 & -3 & 0 \\ -1 & -3 & 5 & 0 \\ 0 & 0 & 0 & 8 \end{pmatrix}$.

We note that once we know the ordinary character table of a group, then it is not too difficult to find the Brauer characters. However, there is a caveat. The reduction of an irreducible character is not necessarily a sum of reductions of other irreducible characters. We have seen this in the example of A_5, where we had to take a difference. When the group is large, we may run into problems since the difference may not have a small dimension.

Chapter 3

Central Character Theory and Applications

In this chapter, we will develop a little bit more block theory. We will associate characters (both ordinary and Brauer) to blocks. Using some computation, we will be able to apply the theory to group theory and deduce certain conditions on finite simple group. We will follow [Alp86, Chap IV] and [Fen15, Section 12, 13]. For the applications in group theory, we will follow [Fen15, Theorem 13.14].

3.1 More Block Theory

Recall the definitions in Section 1.5 that blocks are indecomposable two-sided ideals in $k[G]$ and a module is said to belong to/lie in the block B_i if $e_iM = M$ and $e_jM = 0$ for all $j \neq i$, where e_i is the idempotent correspond to B_i.

We will need a more careful characterization of notion of modules belonging to a block.

Proposition 3.1.1. If S are T are simple $k[G]$ modules, then the following are equivalent:

1. S and T lie in the same block
2. There are simple modules $S = S_1, \ldots, S_m = T$ such that S_i, S_{i+1} are composition factors of a projective indecomposable.
3. There are simple modules $S = T_1, \ldots, T_n = T$ such that T_i, T_{i+1} are equal or there is a non-split extension of one of them by the other.

Remark 3.1.2. The second statement can be rephrased into 'they are composition factors of the same projective indecomposable.'. And the third statement can be rephrased into $\mathrm{Ext}^1_{k[G]}(S,T) \neq 0$. This is true because we have that $\mathrm{Hom}_{k[G]}(P_i, S_j) = k$ if $i = j$ or 0 otherwise (k is big enough).

We will only use 1 and 2, so we will prove they are equivalent. For a full proof, see [Alp86, Prop 3, p94].

Proof. (2) $\implies$ (1). This is true because submodules and quotient modules of a module belonging to a block also belong to that block.

(1) $\implies$ (2). Let S belong to B, write $B = P_1 \oplus \cdots \oplus P_n \oplus Q$, where the P_i are the projective indecomposables whose composition factors are equivalent to S according to (2) and Q to be the rest. We will show $Q = 0$. Let $P = P_1 \oplus \cdots \oplus P_n$, since Q have no composition factors in common we have $\mathrm{Hom}(P, Q) = 0$. We claim P is a two-sided ideal. Indeed, we just need to show it is closed under right multiplication, If $a \in k[G]$, then right translation followed by projection to Q is in $\mathrm{Hom}(P, Q)$, hence 0 and therefore $Pa \subset P$. Similarly Q is a two-sided ideal as well. But B is indecomposable, which gives a contradiction.

□

We are now going to explain how to associate characters to blocks. For any irreducible ordinary character χ_i, we can associate a simple $K[G]$-module M_i. If all the S_j for which $d_{ij} \neq 0$ belong to the same block, then we just assign the module M_i (and hence the character χ_I) to the block B where S_j belongs to B and $d_{ij} \neq 0$. To make this work, we need the following lemma.

Lemma 3.1.3. If S_i and S_j are in different blocks, then $d_{ij} = 0$.

Proof. We know that the projective indecomposables of $k[G]$ are partitioned into blocks in a way compatible with the partitioning of simple modules by the last proposition. So if S_i is a composition factor of P_i then S_j is not, so $c_{ij} = 0$. But $C = DD^T$, and $0 = c_{ij} = \sum_k d_{ki} d_{kj}$ with all the d_{kj} are non-negative, this implies $d_{ij} = 0$. □

We now see if we order the characters in a way such that the characters correspond to the same blocks are grouped together, then the Cartan matrix will be a matrix with block matrices (not necessarily Jordan blocks) on the diagonal.

For example, in Example 2.5.20, we see there are $|G_{\mathrm{reg}}|$ blocks and each of them has size ${p_i}^{n_i}$. This is expected since $k[C_n]$ is commutative and is isomorphic to $k[x]/(x^n - 1)$. All (left) ideals are automatically two-sided. Let $|G_{\mathrm{reg}}| = q = n/{p_i}^{n_i}$. Since k has characteristic p_i, we have by Frobenius endomorphism that $x^n - 1 = (x^q - 1)^{{p_i}^{n_i}}$. But k is large, so $x^q - 1$ is separable and splits completely. Each ideal is generated by one element (but not necessarily an integral domain). The blocks are exactly the same things as the projective indecomposables, and they correspond to the ideal $(x - \omega)$, where ω is a root, and each smaller ideal $(x - \omega)^i$ correspond to a smaller submodule with $(x - \omega)^{{p_i}^{n_i}}$ is the simple module correspond to the projective indecomposable/block.

In Example 2.5.23, we see that $\overline{\mathbb{F}_2}(L_2(7))$ has only two blocks.

3.2 Central Character Theory

In this section we want to apply the theory we have developed to group theory. We will pick up where we left at the end of the course 'Group Representation Theory' M3P12 ([New16]) and generalise Burnside's Theorem and prove [Fen15, Theorem 13.14].

As the title of the section suggests, we will consider $Z := Z(k[G])$. By Schur's lemma, given a simple $K[G]$-module M, Z acts by scalars. Therefore we have a K-algebra homomorphism $\omega : Z \to K$ such that $\omega(z) \cdot m = \omega(z)m$. This is called the (ordinary) *central character* of M.

Recall that if $\mathcal{C}_1, \ldots, \mathcal{C}_n$ are conjugacy classes of G, then $c_i := \sum_{g \in \mathcal{C}_i} g$ form a basis for Z.

Lemma 3.2.1. For $g \in \mathcal{C}_i$, we have that $\omega(c_i) = \frac{|\mathcal{C}_i|\chi(g)}{\chi(1)}$. Furthermore, it is algebraic.

Proof. Characters are invariant under conjugacy classes, hence c_i has trace $\chi(1)\omega(c_i)$. On the other hand, each $g \in \mathcal{C}_i$ has character $\chi(g)$, but there are $|\mathcal{C}_i|$ of them.

For a proof of the algebraic-ness, see [New16, Prop 4.7]. □

Now we want to link to modular central characters. The idea is the same, since we showed it is algebraic, it is in A, so we can define modulo $\mathfrak{m}$ and this will give us the modular central characters.

More precisely, let M be a simple $K[G]$-module, χ is its character and ω_χ is its central character. Then $\overline{\omega_\chi} := \omega_\chi \bmod \mathfrak{m}$ is the central character attached to the block of $d(M)$. And by Proposition 3.1.1, this is well defined.

Remark 3.2.2. Note that $Z = \oplus Z(B_i)$. By showing each $Z(B_i)$ is local, we can see it is the unique k-algebra homomorphism which is non-trivial on exactly one block. So we can add the condition of having the same central character to the list of equivalent conditions in Proposition 3.1.1. This explains why central characters are 'natural'. Although we don't really need this.

For completeness sake, let's recall Burnside's Theorem ([New16, Thm 4.4, Cor 4.3]).

Theorem 3.2.3. Let p be a prime number, and let $d \geq 1$ be an integer. Suppose G is a finite group with a conjugacy class of size p^d. Then G is not simple.

Corollary 3.2.4. Let p, q be prime numbers and let $a, b \in Z_{\geq 0}$ with $a + b \geq 2$. Suppose G is a finite group with $|G| = p^a q^b$. Then G is not simple.

Now we will work toward a stronger version of Burnside's Theorem ([Fen15, Theorem 13.14]):

Theorem 3.2.5. If G is a non-abelian simple group and $|G| = p^a q^b r$ for distinct primes p, q, r, then if R is an r-Sylow we have $R = \mathrm{Cent}(R)$.

With a bit more work, we can get the following corollary (see [Bra68]):

Corollary 3.2.6. If G is a non-abelian simple group, and $|G| = 5p^a q^b$ for distinct primes $p, q \neq 5$, then $G = A_5, A_6$, or $SO_5(\mathbb{F}_3)$.

Let's begin with some results on the *principal block* (recall the principal block is the block contains the identity).

Proposition 3.2.7. Let G be a non-abelian simple group and χ an irreducible character of G in the principal block. If $\chi(1) = p^k$, then $\chi = 1$.

Proof. Similar to the proof of Theorem 3.2.3, we take g in the center of a p-Sylow subgroup $P \in G$. Then $|\mathcal{C}_g| = |G : \mathrm{Cent}(g)|$ is a factor of $|G : P|$, which is coprime to p. Assume χ is not the trivial character. Since G is simple, by the proof of Theorem 3.2.3 we have that $\chi(g) = 0$.

On the other hand, it is clear that if χ, χ' are in the same block, then $\overline{\omega_\chi} = \overline{\omega'_\chi}$. So we have for any conjugacy class $\mathcal{C}$ and any $g \in \mathcal{C}$,

$$\frac{|\mathcal{C}|\chi(g)}{\chi(1)} = \frac{|\mathcal{C}|\chi'(g)}{\chi'(1)} \bmod \mathfrak{m}.$$

Since the trivial rep is in the principal block, we take $\chi' = 1$. Then we deduce that

$$\frac{|\mathcal{C}|\chi(g)}{\chi(1)} = |G| \bmod \mathfrak{m}.$$

This implies that $\chi(1) = p^k$ and $|\mathcal{C}|$ are coprime. Then $|\mathcal{C}|$ is not in the maximal ideal $\mathfrak{m}$, so we have that $\frac{|\mathcal{C}|\chi(g)}{\chi(1)} = 0$, hence $(g) \neq 0$ and this is a contradiction. □

We will also need:

Lemma 3.2.8. If g is p-regular and h is not, then $\sum_{\chi_i \in B} \chi_i(g)\overline{\chi_i(h)} = 0$.

Proof.

$$\begin{aligned}\sum_{\chi_i \in B} \chi_i(g)\overline{\chi_i(h)} &= \sum_{\chi_i, \beta_j \in B} d_{ij}\beta_j(g)\overline{\chi_i(h)} \\ &= \sum_{\beta_j \in B} \beta_j(g)\overline{\eta_j(h)},\end{aligned}$$

where the equalities follow from the theory of CDE triangle and g is regular. But by Proposition 2.5.12 we have $\eta_j(h) = 0$, hence the result.

□

Remark 3.2.9. Note this is a special case of the more general orthogonality relation called Block Orthogonality (see [Fen15, Theorem 13.8]).

Now we are ready to prove Theorem 3.2.5.

Proof of Theorem 3.2.5. If $\mathrm{Cent}(R) > R$ then by counting, G has an element g of order $p^i r$ or $q^i r$, where $i > 0$. WLOG, assume it is $p^i r$. Let B_0 be the principal block modulo p. We have by the last lemma that $0 = \sum_{\chi \in B_0} \chi(1)\chi(g)$, so $-1 = \sum_{\chi \in B_0, \chi \neq 1} \chi(1)\chi(g)$. We see that there is a $\chi \neq 1$ such that $q \nmid \chi(1)$ and $\chi(g) = 0$ (otherwise will contradict the above equation). Then by Proposition 3.2.7, we must have $r|\chi(1)$. But then the r-defect of χ is 0, which means it comes from a projective $\overline{\mathbb{F}_r}[G]$-module. But then $\chi = \eta_P$ for some projective indecomposable P, and by Proposition 2.5.12, we have $\chi(g) = 0$ as g is not r-regular. And this gives the contradiction.

Afterword

We started with the module theoretic approach, but mainly focused on the character theoretic approach. Some of the notions we introduced lend themselves well to the module theoretic point of view.

For example, we introduced the notion of p-defect in Chapter 2.5.1, it turns out that we can turn it into a definition of p-defected subgroup $D \subset G$ of B by thinking of B as a $k[G \times G]$-module. It has defect 0 when D is the trivial group (see [Alp86, Chap IV]). In fact, the block B is semisimple as an algebra if and only if B has defect 0 (see [Alp86, The 5, p97]). Also note there exists a whole theory for when the defect subgroup is cyclic. We can associate the simple modules of a block to a *Brauer graph* and it turns out if the defect subgroup is cyclic, then the Brauer graph will be a tree (see [Alp86, Chap V]). Note this applies to the special case when it has the trivial defect group.

We also did not touch on Green and Brauer correspondence, which links global structure with local structure. Note that there also exist ring theoretic approaches, which can be found in [Lan83]. And some homological approaches can be found in [Ben98a] and [Ben98b].

Alphabetical Index

Bibliography

[Alp86] J. L. Alperin. *Local representation theory*, volume 11 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. Modular representations as an introduction to the local representation theory of finite groups.

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Ben98a] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1998. Basic representation theory of finite groups and associative algebras.

[Ben98b] D. J. Benson. *Representations and cohomology. II*, volume 31 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1998. Cohomology of groups and modules.

[Bra68] Richard Brauer. On simple groups of order $5 \cdot 3^a \cdot 2^b$. *Bull. Amer. Math. Soc.*, 74(5):900–903, 09 1968.

[BS59] Richard Brauer and Michio Suzuki. On finite groups of even order whose 2-Sylow group is a quaternion group. *Proc. Nat. Acad. Sci. U.S.A.*, 45:1757–1759, 1959.

[Fen15] Tony Feng. Modular Representation Theory. `http://web.stanford.edu/~tonyfeng/mod_rep_theory.pdf/`, 2015. [Lectured BY Dan Bump, typed by Tony Feng. Online; accessed Oct-2016].

[Gla66] George Glauberman. Central elements in core-free groups. *J. Algebra*, 4:403–420, 1966.

[Isa09] I. Martin Isaacs. *Algebra: a graduate course*, volume 100 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009. Reprint of the 1994 original.

[Lan83] P. Landrock. *Finite group algebras and their modules*, volume 84 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[New16] James Newton. M3/4/5P12 GROUP REPRESENTATION THEORY. `https://nms.kcl.ac.uk/james.newton/M3P12/notes.pdf/`, 2016. [Lectured BY James Newton. Online; accessed May-2017].

[Qui71] Daniel Quillen. The Adams conjecture. *Topology*, 10:67–80, 1971.

[Sch13] Peter Schneider. *Modular representation theory of finite groups*. Springer, Dordrecht, 2013.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Wil11] Robert A. Wilson. *Representations of groups: a computational approach* [book review of mr2680716]. *Bull. Lond. Math. Soc.*, 43(5):1031–1033, 2011.