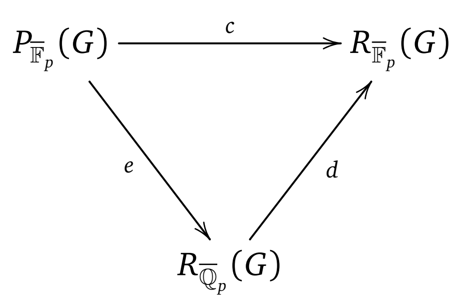
Modular Representation Theory and the CDE Triangle

ARUN DEBRAY



Senior Honors Thesis

Stanford University
Department of Mathematics

May 18, 2015

Contents

Introduction iv

Chapter 1. The Theory Behind Modular Representations 1
1.1. Irreducibility and Indecomposability in Positive Characteristic 1
1.2. Reduction of Representations 3
1.3. Modular Characters 6
1.4. Projective Modules 8
1.5. The CDE Triangle 10
1.6. The CDE Triangle on the Character Level 13

Chapter 2. Modular Representations of Some Small Groups 16
2.1. The Modular Representation Theory of $\mathbb{Z}/p$ 16
2.2. The Modular Representation Theory of S_3 17
2.3. The Modular Representation Theory of S_4 21
2.4. The Modular Representation Theory of A_4 23
2.5. The Modular Representation Theory of S_5 24
2.6. The Modular Representation Theory of $\mathrm{GL}_2(\mathbb{F}_3)$ 31
2.7. The Modular Representation Theory of D_{10} 33
2.8. A Sillier Example: D_8 and Q_8 35

Bibliography 36

Index 37

Introduction

"Representation theory is like a George R.R. Martin novel. There are lots and lots of characters; most of them are complex, and many of them are unfaithful. But everything gets a lot tensor: there are a lot of duals, and some of the characters end up decomposing!"

This paper is my senior honors thesis, written under the direction of Professor Akshay Venkatesh. The senior thesis is a significant part of the requirements for the honors major in mathematics at Stanford, and serves the dual purpose of educating a student on an advanced topic in mathematics and producing an exposition of that topic. My thesis will discuss modular representation theory and a collection of results on modular representations encapsulated in a diagram called the CDE triangle (1.5.1), the figure on the title page. Specifically, in this paper, I will present the background theory of modular representations needed to state and prove these results; then, I will use these results in several explicit examples, calculating modular character tables and the matrices defining the CDE triangle for several groups.

Though this is a senior honors thesis, the prerequisites will be relatively benign. In order to talk about modular representation theory, one of course has to use results from the ordinary, characteristic 0 representation theory of finite groups, and this prerequisite will be pretty important. I will also use some module theory (e.g. projective modules, simple modules, and tensor products) in an important way. Finally, there will also be a few other dependencies from algebra, such as some basic properties of the p-adic numbers; these are less central than having already seen representation theory of finite groups in characteristic 0.

Overview and Major Results. Though representation theory is the study of group actions on vector spaces, the most common choices for these vector spaces are those over fields of characteristic zero, or positive characteristic that doesn't divide the order of the group being studied. Modular representation theory concerns itself with the other choices, where the characteristic of the base field divides the order of the group.

This seemingly small change makes a world of difference, as Maschke's theorem (Theorem 1.1.1), the cornerstone of representation theory in characteristic 0, no longer holds, as explored in Section 1.1. This makes it much more complicated to describe how a representation breaks down into irreducible representations. In order to have a general theory, we need ways of working around this, such as working with semisimplifications (which do decompose cleanly) and with the modular characters discussed in Section 1.3. Then, we can use the CDE triangle to connect the characteristic 0 theory and the characteristic p theory for a particular group G.

This paper is divided into two chapters; Chapter 1 provides an exposition of the theory, and Chapter 2 provides examples of the modular characters and explicit calculations of the morphisms in the CDE triangle.

Here's a summary of the important results contained in the first chapter. Let G be a finite group and p be a prime dividing $|G|$.

(1) Though not all representations in positive characteristic are semisimple, taking the semisimplification, defined in Section 1.1, still provides a lot of information about finitely generated $\overline{\mathbb{F}}_p[G]$-modules. Specifically, the following are equivalent for two such modules M and N.
- M and N have isomorphic semisimplifications.
- For any $g \in G$, the characteristic polynomials for the actions of g on M and N are equal. (Proposition 1.2.7)
- The modular characters of M and N are equal. (Corollary 1.3.5)
- M and N define the same class in the Grothendieck group $R_k(G)$. (Corollary 1.5.2)

(2) Brauer's theorem (Theorem 1.3.4), that the modular characters of the simple $\overline{\mathbb{F}}_p[G]$-modules are a basis for the space of class functions on p-regular elements of G, and therefore (Corollary 1.3.6) there are as many simple $\overline{\mathbb{F}}_p[G]$-modules as there are conjugacy classes of G with order not divisible by p.

(3) The results on the CDE triangle, including:
- Given a representation in characteristic 0, there's a way to produce a representation in characteristic p, called reduction, that's well-defined up to semisimplification (Section 1.2); moreover, reduction induces a surjective morphism on Grothendieck groups (Theorem 1.5.10), which means that every $\overline{\mathbb{F}}_p[G]$-module can be lifted to characteristic zero in the form of a "virtual module," i.e. a linear combination of simple $\overline{\mathbb{Q}}_p[G]$-modules.
- To obtain all of the irreducible modular characters, it suffices to take the irreducible characters in characteristic zero, reduce them mod p, and then decompose them into irreducibles; in this sense, the characteristic 0 theory contains all of the information from characteristic p, and also makes calculating modular character tables much simpler. (Proposition 1.5.14)

Then, in the second chapter, we work this out in several explicit cases: the cyclic group $\mathbb{Z}/p$; the symmetric groups S_3, S_4, and S_5; the alternating group A_4; the dihedral group D_{10}; the group $\mathrm{GL}_2(\mathbb{F}_3)$; and finally p-groups such as D_8 and Q_8. In each of these cases, we use reduction of characters from characteristic 0 to obtain the table of modular characters, and then use this to calculate the three maps in the CDE triangle; in the simpler cases, we can also explicitly describe the projective indecomposable modules, rather than just their characters.

A standard reference for this subject is Serre's *Linear Representations of Finite Groups* [7].

Some Applications. Representation theory over $\mathbb{R}$ or $\mathbb{C}$ is sometimes motivated by its applications to physics, as it is very useful in quantum mechanics and particle physics. However, this application goes away when one passes to positive characteristic, since the symmetries physicists describe with representation theory tend to be as Lie groups acting on Euclidean space. Nonetheless, modular representation theory is useful in several areas of mathematics.

For example, results from modular representation theory are used in the classification of the finite simple groups. The proof of the Brauer-Suzuki theorem [1] rests on the relationship between the ordinary and modular characters through the decomposition homomorphism as well as the linear independence of the modular characters (Theorem 1.3.4). The Z^* theorem [2], another important result in the theory of finite simple groups, also depends on calculations with modular characters.

Results from modular representation theory also appear in algebraic topology: the Adams conjecture is a statement about real vector bundles over CW complexes, and yet its proof in [6] involves the characteristic p representation theory of the finite groups $\mathrm{GL}_n(\mathbb{F}_p)$ and $\mathrm{O}_n(\mathbb{F}_p)$. There are also applications of modular representation theory to number theory, as discussed in [7, Ch. 19].

Notational Conventions. In this paper, we will use the following notational conventions.
- G will always denote a finite group, and $|G|$ will denote its cardinality. p will be a prime number dividing $|G|$, and $G_{\mathrm{reg}}^{(p)}$ is the set of p-regular elements of G, as defined in Section 1.3.
- $\mathbb{Z}/p$ denotes the cyclic group of order p, and $\mathbb{Z}_p$ denotes the p-adic integers.
- S_n denotes the symmetric group on n letters; A_n denotes the alternating group on n letters; D_{2n} denotes the dihedral group with $2n$ elements; and Q_8 denotes the quaternion group.
- K will denote a field of characteristic 0, often $\overline{\mathbb{Q}}_p$, and k will denote a field of characteristic p, often $\overline{\mathbb{F}}_p$. L will be a field of any characteristic.
- The ring of integers of K is denoted $\mathscr{O}_K$. In this paper, $\mathscr{O}_K$ will always be a discrete valuation ring, so $\mathfrak{m}_{\mathscr{O}_K}$ will denote its maximal ideal, and π will denote a uniformizer for $\mathfrak{m}_{\mathscr{O}_K}$.
- Λ will denote a lattice inside K, as defined in Section 1.2.
- If A is a ring, $A[G]$ will denote the group algebra.
- All modules in this paper are left modules, and will usually be denoted M and N, or V and W.
- $R_L(G)$ and $P_k(G)$ are the Grothendieck groups defined in Section 1.5.
- χ will denote the character of a representation in characteristic 0; ϕ_i will be used to denote the modular characters of the simple $k[G]$-modules; and Φ_i will be used for the characters of the projective indecomposable $k[G]$-modules.
- $C\ell(G,K)$ denotes the space of K-valued class functions on G.

Acknowledgements. Modular characters are not the only important characters in bringing this thesis to fruition, and I would like to thank, in no particular order, the many people who played a part in helping me along the way.

I would like to thank my thesis advisor, Professor Akshay Venkatesh. As my pre-major advisor, he met me very early in my time at Stanford. He has provided good advice on courses and on my thesis itself. I have enjoyed talking to him about my thesis and the fascinating topics that lie a little beyond its horizons, and I have enjoyed learning from him in the classroom. Along with my thesis, Professor Venkatesh has influenced the ways I think about mathematics itself. Thank you for working with me!

I would also like to thank my high-school Algebra II/Trig and BC Calculus teacher, Ledya Vakarelov. Under her direction, I first learned what a mathematical proof was, and, more importantly, how to appreciate the art of mathematics. There is no doubt that her class not only made me interested enough in mathematics to continue taking proof-based classes after high school, but also managed to prepare me for the honors freshman math series at Stanford; she is the reason I am a mathematician. Thank you for one of the best classes I took in high school, but also the perspective that brought me to where I am today!

My friends have also been more helpful than they might realize. Many of you have listened to me gripe about the work or stress of preparing this thesis yet even in the same sentence rave about how interesting I find the mathematics of it; thank you for understanding that paradox and listening.

Finally, I would like to thank my family: Mom, Dad, and my sister Reena. For caring so much about what I want to do with my life and advising me along the way; for, from the very beginning, igniting my love of learning; for sharing that common core of things we find important and common sense of humor. I am lucky to have you all.

CHAPTER 1

The Theory Behind Modular Representations

"As much as we often prefer to work over $\mathbb{C}$, modular representation theory has some very positive characteristics."

1.1. Irreducibility and Indecomposability in Positive Characteristic

In representation theory, it's often extremely useful to know how to build a representation out of smaller or less complicated representations. Irreducibility and indecomposability are two basic examples of this.

Definition. Let V be a representation of a group G. Then, a subspace W of V is *G-stable* if the action of G sends W to itself, i.e. $g \cdot w \in W$ for all $g \in G$ and $w \in W$.

Definition.

- A G-representation V is *irreducible* if there are no G-stable subspaces W of V other than 0 and V itself.
- A G-representation V is *indecomposable* if it is not isomorphic to a direct sum of G-representations $W_1 \oplus W_2$.
- A representation that isn't irreducible is called *reducible*, and similarly, one that is not indecomposable is called *decomposable*.

Here are some quick properties.

- Irreducibility implies indecomposability: if $V = W_1 \oplus W_2$ as G-representations, then $W_1 \oplus \{0\} \subsetneq V$ is G-stable.
- An irreducible representation of G over a field L is a *simple* $L[G]$-module (a module whose only submodules are 0 and itself).
- If V is reducible, with W a G-stable subspace, then $0 \to W \to V \to V/W \to 0$ is an exact sequence of G-representations.

Furthermore, in characteristic 0, these two notions of irreducibility and indecomposability are equivalent.

Theorem 1.1.1 (Maschke)**.** *Let G be a finite group and K be a field such that* $\operatorname{char}(K) = 0$ *or* $\operatorname{char}(K) = p \nmid |G|$*. If V is a finite-dimensional representation of G over K and V has a G-stable subspace W, then there exists a representation W' of G over K such that $V = W \oplus W'$ (as G-representations).*

This theorem is proven in [**5**, Ch. XVIII, § 1]; the key step in the proof of this theorem is averaging an action of the elements of G, which involves dividing by $|G|$. Thus, this doesn't work when $\operatorname{char}(K)$ divides $|G|$. Moreover, when $\operatorname{char}(K) = p$ does divide $|G|$, there are representations that are reducible, but indecomposable.

Example 1.1.2. Let V be the two-dimensional representation of $\mathbb{Z}/p = \langle x \rangle$ over $\mathbb{F}_p$, where x^n acts as $\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$; this is a representation because $0 \mapsto I$ and

$$\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ m+n & 1 \end{pmatrix}.$$

Then, the subspace

$$W = \left\{ \begin{pmatrix} 0 \\ y \end{pmatrix} \mid y \in \mathbb{F}_p \right\}$$

is $\mathbb{Z}/p$-stable, but V is not decomposable: if it were, then there would exist some other $\mathbb{Z}/p$-stable subspace W', so that $V = W \oplus W'$, but suppose that

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} cx \\ y \end{pmatrix} = \begin{pmatrix} cx \\ cnx + y \end{pmatrix} = \begin{pmatrix} \lambda cx \\ \lambda y \end{pmatrix}$$

for some $\lambda \in \mathbb{F}_p$ and all $n \in \mathbb{F}_p$; then, since $cx = \lambda cx$, we have $\lambda = 1$, and therefore $cx = 0$ (when $n = 1$), but this means that $c = 0$, so we recover W as the only stable subspace. In particular, this means V is indecomposable, but not irreducible.

This discrepancy between indecomposability and irreducibility is very important in modular representation theory.

Another basic fact about irreducibility is the Jacobson density theorem.

Theorem 1.1.3 (Jacobson density theorem)**.** *Let L be an algebraically closed field and G be a finite group. Then, the $L[G]$-module map*

$$L[G] \longrightarrow \bigoplus_{M \in S_L} \mathrm{End}_L(M),$$

where S_L is the set of isomorphism classes of simple f.g. $L[G]$-modules, is surjective.

For a proof, see [5, Ch. XVII, § 3].

1.1.1. The Semisimplification of a Module. In addition to simple modules, we can also consider *semisimple modules*, which are defined to be those modules isomorphic to direct sums of simple modules. A representation V over a field L is a semisimple $L[G]$-module if every G-stable subspace is a direct summand, i.e. if $W \subseteq V$ is G-stable, then there exists a $W' \subseteq V$ such that $V = W \oplus W'$. Thus, Maschke's theorem informs us that all representations in characteristic zero are semisimple modules, and Example 1.1.2 demonstrates that not all representations over fields of positive characteristic are semisimple.

Nonetheless, if V is any finite-dimensional representation and $W \subset V$ is G-stable, then V/W is also a G-representation, and, assuming W isn't trivial and isn't all of V, then, both have dimension strictly less than V. Thus, these can be thought of as less complicated representations that build together to form V. If one keeps repeating this process on W and V/W, it terminates eventually (since one-dimensional representations are irreducible), providing a finite set of irreducible G-representations known as its *composition factors*.

Lemma 1.1.4. *The composition factors of an f.g. $L[G]$-module V are unique up to isomorphism and reordering.*

Proof. Let $\{M_1, \dots, M_m\}$ and $\{N_1, \dots, N_n\}$ be two sets of composition factors for V. It's sufficient to prove that $M_1 \cong N_j$ for some j; then, induction takes care of the rest.

The key observation is that if M and N are two G-stable subspaces of an $L[G]$-module V, then it doesn't matter whether one quotients by M before $N/(M \cap N)$ or quotients by N followed by $M/(M \cap N)$. Notice that $M \cap N$ is also G-stable, since if $x \in M \cap N$, then $g \cdot x \in M$ and $g \cdot x \in N$ for all $g \in G$, and therefore, e.g. $M/(M \cap N)$ is a G-stable subspace of V/N.

- If we consider M first, the components are M and V/M, so then taking N, which has become $N/(M \cap N)$ in the quotient, we get M, $N/(M \cap N)$, and $(V/M)/(N/(M \cap N))$. Finally, we can decompose M into $M \cap N$ and $M/(M \cap N)$.
- If one chooses N first, the same factors result, but with M and N switched: $M \cap N$, $N/(M \cap N)$, $M/(M \cap N)$, and $(V/N)/(N/(M \cap N))$.

Three of these are the same: $M \cap N$, $M/(M \cap N)$, and $N/(M \cap N)$. The remaining ones are isomorphic as well: by the second isomorphism theorem of modules, $M/(M \cap N) \cong (M + N)/N$, so $(V/M)/(N/(M \cap N)) \cong (V/M)/((M + N)/M) \cong V/(M + N)$ by the third isomorphism theorem of modules, and applying it to the module arising from the other choice (with M and N switched) also produces $V/(M + N)$, so they're isomorphic.

To obtain a set of composition factors of V, one chooses a G-stable submodule M and quotients by it, and then repeats. Without loss of generality, we can assume that M is simple; if not, it contains a simple submodule that the algorithm will eventually get to, and we just showed that order doesn't matter in this algorithm, so we may place the simple submodule first, and get the same answer.

Thus, there's an ordered list of G-stable simple modules which, when one applies this algorithm to it, produces $\{M_1, \dots, M_m\}$, and another such ordered list which yields $\{N_1, \dots, N_n\}$. But we just showed that the order doesn't matter, so we can regard the M_i and N_j are drawn from the same finite set of G-stable simple submodules of V (which is finite because V is finitely generated). But since each of the M_i and N_j are simple, M_1 must be a submodule or a quotient of one of the N_j. If it's a submodule, then $M_1 = N_j$, since N_j is simple, and if it's a quotient, then we proceed one step further in the algorithm, so M_1 must be a submodule or quotient of another $M_{j'}$. Since the algorithm terminates after a finite number of steps, then $M_1 = N_j$ for some j. ⊠

A module M is said to have *finite length* if it has a finite number of composition factors; this is equivalent to every ascending and descending chain of submodules of M stabilizing, because if not, each quotient in the chain would induce another composition factor of M.

Definition. The *semisimplification* of a finitely generated $L[G]$-module is the direct sum of its composition factors.

Lemma 1.1.4 guarantees this is well-defined up to isomorphism. Moreover, since two semisimple modules are isomorphic iff they have isomorphic composition factors, then the semisimplification of a module M is the unique semisimple module that has composition factors isomorphic to those of M. Additionally, we know that if M is a semisimple module, then M is its own semisimplification.

1.2. Reduction of Representations

The simplest way to obtain representations of a group in positive characteristic is from a representation in characteristic zero. We want to take a representation "mod p," which is possible when it's represented by matrices with integer entries, but for anything else there's a problem. Additionally, it'll be better to have a description that is independent of basis. So we need a systematic way of sending representations from an algebraically closed field of characteristic zero to one of characteristic p. This suggests that the base field should be the p-adics $\mathbb{Q}_p$, because it's relatively easy to describe how $\mathbb{Z}_p$ sits inside $\mathbb{Q}_p$, and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Thus, the formal process of reducing a representation looks like this: let G be a finite group, p be a prime dividing $|G|$, and ρ be a complex (finite-dimensional) representation of G. Then, since G is finite, ρ may be realized over $\overline{\mathbb{Q}}$.

Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$; since we have an embedding $\iota : \mathbb{Q} \hookrightarrow \mathbb{Q}_p$, we can take $\overline{\mathbb{Q}}$ to be the algebraic closure of $\mathbb{Q}$ inside $\overline{\mathbb{Q}}_p$ with respect to this embedding. Thus, ρ is also a representation over $\overline{\mathbb{Q}}_p$, i.e. it's a map into $\mathrm{GL}_n(\overline{\mathbb{Q}}_p)$. Since ρ is in fact a representation over a finite extension over $\mathbb{Q}$, it is also a representation over a finite extension of $\mathbb{Q}_p$.

For the rest of this section, let K denote this finite extension of $\mathbb{Q}_p$, and let $\mathscr{O}_K$ denote its ring of integers. Thus, $\mathscr{O}_K$ is a discrete valuation ring, and K is its fraction field; let π be a uniformizer for $\mathscr{O}_K$ (i.e. a generator for its maximal ideal $\mathfrak{m}_{\mathscr{O}_K}$).

Definition. A *lattice* in a K-vector space V is the $\mathscr{O}_K$-span of a K-basis for V.

This is the same idea as a $\mathbb{Z}$-lattice inside a $\mathbb{Q}$-vector space, and the geometric intuition carries over, e.g. given two lattices, there's a common lattice contained in both.

Lemma 1.2.1. *The sum of two lattices is a lattice; that is, if V is a K-vector space and Λ_1 and Λ_2 are lattices in V, then $\Lambda_1 + \Lambda_2 = \{v_1 + v_2 \mid v_1 \in \Lambda_1, v_2 \in \Lambda_2\}$ is also a lattice.*

Proof. Let B_1 (resp. B_2) be the K-basis of V whose $\mathscr{O}_K$-span is Λ_1 (resp. Λ_2), and let $n = \dim_K(V)$. Then, there's a map $M \in \mathrm{GL}(V)$ that sends B_1 to B_2, and therefore $M(\Lambda_1) = \Lambda_2$. In a basis for V, the entries m_{ij} of M are elements of K, and since there are a finite number of them, they have a common denominator, i.e. a nonzero $a \in \mathscr{O}_K$ such that $am_{ij} \in \mathscr{O}_K$ for all i and j. Thus, $aM(\Lambda_1) = a\Lambda_2$, and since the entries of aM are in $\mathscr{O}_K$, then if $v \in \Lambda_1$, then $aM \cdot v \in \Lambda_1$ as well, since it's an $\mathscr{O}_K$-linear combination of the generators of Λ_1. Thus, $a\Lambda_2 \subseteq \Lambda_1$, and, since $a \neq 0$, $\Lambda_2 \subseteq (1/a)\Lambda_1$. Since $\Lambda_1 \subseteq (1/a)\Lambda_1$ as well, then $\Lambda_1 + \Lambda_2 \subseteq (1/a)\Lambda_1$ as well. Since these are abelian groups, we can consider the index of $\Lambda_1 + \Lambda_2$ inside $(1/a)\Lambda_1$; in fact, it must be finite, because $\Lambda_1 \subseteq (1/a)\Lambda_1$ has finite index and $\Lambda_1 \subseteq \Lambda_1 + \Lambda_2 \subseteq (1/a)\Lambda_1$.

Thus, $\Lambda_1 + \Lambda_2$ is an $\mathscr{O}_K$-submodule of $(1/a)\Lambda_1$, which is a free, finitely-generated $\mathscr{O}_K$-module, and therefore $\Lambda_1 + \Lambda_2$ is also a free, finitely-generated $\mathscr{O}_K$-module. Since $\Lambda_1 + \Lambda_2$ is finite-index in $(1/a)\Lambda_1$, then this implies they must have the same rank, so $\Lambda_1 + \Lambda_2$ is an $\mathscr{O}_K$-submodule of V with rank equal to the dimension of V, and therefore is a lattice as well. ⊠

Applying the lemma n times shows that any finite sum of lattices is also a lattice.

Proposition 1.2.2. *G-stable lattices exist over $\mathbb{Q}_p$. That is, if $\rho : G \to \mathrm{GL}(V)$ is a representation over K, then there exists a lattice $\Lambda \subseteq V$ such that $g \cdot \Lambda \subseteq \Lambda$ for all $g \in G$.*

Proof. Let Λ be any lattice in V, and for any $g \in G$, define $g\Lambda = \{gv \mid v \in \Lambda\}$. Since $\rho(g)$ is invertible, then it must have full rank, and in particular sends bases of V to bases of V, so $g\Lambda$ is still a lattice.

Then, let

$$\Lambda' = \sum_{g\in G} g\Lambda.$$

By Lemma 1.2.1, Λ' is a lattice. An arbitrary element of Λ' has the form

$$\ell = \sum_{g\in G} g v_g \text{ for some } v_g \in \Lambda,$$

so

$$h\cdot\ell = \sum_{g\in G}(hg)v_g.$$

Multiplication by h is a (setwise) bijection $G \to G$, so as g ranges over all elements of G, so does hg. In particular, $h\cdot\ell \in \Lambda'$, so Λ' is G-stable. ⊠

Now, returning to ρ and V, choose a G-stable lattice Λ in V. Since Λ is G-stable, the action of ρ on Λ fixes it, which means that ρ is actually a map into $\mathrm{GL}_n(\mathscr{O}_K)$. This means that, in a basis, the entries of the matrices of ρ are in $\mathscr{O}_K$, so, reducing them mod $\mathfrak{m}_{\mathscr{O}_K}$ yields matrices with coefficients in $k = \mathscr{O}_K/\mathfrak{m}_{\mathscr{O}_K}$, which is a finite field extension of $\mathbb{F}_p$. Thus, we have obtained a representation $\overline{\rho} : G \to \mathrm{GL}_n(k)$.

This operation, called *reduction* of a representation mod p, depends on the lattice chosen, and so sometimes it is called the reduction of M with respect to Λ.

Example 1.2.3. Let's explicitly reduce a representation of S_3, the symmetric group on three elements. S_3 acts on 3-tuples of elements of $\mathbb{Q}_3$ by $\sigma\cdot(a_1,a_2,a_3) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)})$. Since this action preserves the sum $a_1+a_2+a_3$, then it preserves the subspace of 3-tuples summing to zero, so restricting to the vector space V of 3-tuples summing to zero, we obtain a two-dimensional representation.

If $v_1 = (1,-1,0)$ and $v_2 = (0,1,-1)$, then $\{v_1, v_2\}$ is a basis for V. In this basis, this representation can be described in terms of matrices.

$$1 \longmapsto \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad (a\ b) \longmapsto \begin{pmatrix}-1 & 1\\ 0 & 1\end{pmatrix} \qquad (a\ b\ c) \longmapsto \begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix} \tag{1.2.1}$$

In particular, $\Lambda_1 = \mathbb{Z}_3\cdot\{v_1, v_2\}$ is a lattice in V. Since the action of each element of S_3 maps v_1 and v_2 to $\mathbb{Z}_3$-linear combinations of v_1 and v_2, then Λ_1 is S_3-stable, so we can reduce.

In order to take the reduction, we simply need to reduce mod 3, so the group elements have the same matrix representations as in (1.2.1), though now the matrices are in $\mathrm{GL}_2(\mathbb{F}_3)$ rather then $\mathrm{GL}_2(\mathbb{Q}_3)$.

However, if one chooses a different lattice, the resulting representation might not be isomorphic. Consider $v_3 = (-2,1,1)$ and $v_4 = (1,-1,0)$. Then, $\{v_3, v_4\}$ is a $\mathbb{Q}_3$-basis for V, so its $\mathbb{Z}_3$-span is a lattice; call it Λ_2. In this basis, our representation takes on the following form.

$$1 \longmapsto \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad (a\ b) \longmapsto \begin{pmatrix}1 & 0\\ 3 & -1\end{pmatrix} \qquad (a\ b\ c) \longmapsto \begin{pmatrix}1 & -1\\ 3 & -2\end{pmatrix} \tag{1.2.2}$$

Just as above, since the coefficients of these matrices are in $\mathbb{Z}_3$, then the action of each element of S_3 sends v_3 and v_4 to $\mathbb{Z}_3$-linear combinations of them, so Λ_2 is S_3-stable. Thus, we may once again reduce mod 3, producing a matrix representation of S_3 over $\mathbb{F}_3$:

$$1 \longmapsto \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad (a\ b) \longmapsto \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \qquad (a\ b\ c) \longmapsto \begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}. \tag{1.2.3}$$

However, it turns out these two representations aren't conjugate, and thus are actually nonisomorphic. If they were, then there would be some 2×2 matrix that simultaneously conjugates the matrices in (1.2.1) into (1.2.3). The identity matrix is preserved by all conjugation, so let's consider the matrices for $(a\ b\ c)$. If we know that

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

then

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

so $b+c=a-b=-d$. Solving these equations in $\mathbb{F}_3$ yields four matrices:

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

Since the sign of the conjugating matrix makes no difference, we really only have two options. Out of these two options, only B conjugates $\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$ to $\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}$. However, it doesn't work for the matrices for $(a\ b)$:

$$\begin{pmatrix}-1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 1 & 1\end{pmatrix}, \qquad \text{but} \qquad \begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}-1 & -1\\ 1 & -1\end{pmatrix}.$$

Thus, there is no matrix that conjugates the first representation to the other, so they're not actually isomorphic.

Though the above representations are nonisomorphic, the characteristic polynomial of the automorphism associated to each group element is independent of the lattice chosen: if $\chi_{1,\sigma}$ denotes the characteristic polynomial of $\sigma\in S_3$ acting as in the first representation, given by the matrices in (1.2.1), and $\chi_{2,\sigma}$ denotes that of the second representation, given by the matrices in (1.2.3), then:

- $1\in S_3$ is sent to the same matrix by each representation, so $\chi_{1,1}=\chi_{2,1}$.
- $\chi_{1,(a\ b)}(\lambda)=(1+\lambda)(1-\lambda)+(0)(1)=1-\lambda^2$, and $\chi_{2,(a\ b)}(\lambda)=(1+\lambda)(1-\lambda)-(0)(0)=1-\lambda^2$, so they're equal.
- $\chi_{1,(a\ b\ c)}(\lambda)=\lambda(\lambda+1)+1=\lambda^2+\lambda+1$, and $\chi_{2,(a\ b\ c)}(\lambda)=(\lambda-1)^2-(1)(0)=\lambda^2-2\lambda+1=\lambda^2+\lambda+1$ in $\mathbb{F}_3$, so they're equal.

This is no accident.

Proposition 1.2.4. *The characteristic polynomial of the reduction of a representation does not depend on the choice of lattice.*

Proof. Let ρ be a representation of G over K, g be an element of G, and Λ be a G-stable lattice. Let $\chi_{g,K}$ denote the characteristic polynomial of the representation over K. Since Λ is G-stable, then in an $\mathscr{O}_K$-basis for Λ, the matrix for $\rho(g)$ has coefficients in $\mathscr{O}_K$, and in particular, the coefficients for $\chi_{g,K}$ are in $\mathscr{O}_K$. However, the coefficients of a characteristic polynomial don't depend on the choice of basis, and therefore don't depend on the choice of lattice. Thus, when the matrix M for g is reduced, the characteristic polynomial is the determinant of $M-\lambda I$, but since this is a polynomial in λ and the entries of M, then when these entries are reduced mod $\mathfrak{m}_{\mathscr{O}_K}$ (i.e. are sent to k by modding out by $\mathfrak{m}_{\mathscr{O}_K}$), the new characteristic polynomial is just the original $\chi_{g,K}$ with all of the coefficients taken mod $\mathfrak{m}_{\mathscr{O}_K}$ as well. This also doesn't depend on the lattice chosen, so the characteristic polynomial of the reduced representation is independent of the lattice chosen. ⊠

In the above proof, we reduced the character of a representation along with the representation itself, by taking the coefficients of the characteristic polynomial modulo $\mathfrak{m}_{\mathscr{O}_K}$. We'll end up using this again.

Proposition 1.2.5. *Let $\chi_1,\dots,\chi_\ell$ be linearly independent class functions for a group G over K, and let $\overline{\chi}_i$ denotes the reduction of χ_i modulo $\mathfrak{m}_{\mathscr{O}_K}$. Then, the $\overline{\chi}_1,\dots,\overline{\chi}_\ell$ are linearly independent over k.*

Proof. Suppose there is a dependence relation between them:

$$\sum_{i=1}^{\ell}\alpha_i\chi_i=0,$$

with $\alpha_i\in K$. Since K is the fraction field of $\mathscr{O}_K$, and there are finitely many α_i, we can find a common denominator c and multiply by it, so that $c\alpha_i\in\mathscr{O}_K$ for each i. Thus, without loss of generality, we can assume that $\alpha_1,\dots,\alpha_n\in\mathscr{O}_K$. Moreover, we can assume at least one isn't in $\mathfrak{m}_{\mathscr{O}_K}$: if all of them are, then divide by the highest power of π that divides all of them.

The next step is to reduce mod $\mathfrak{m}_{\mathscr{O}_K}$; let $\overline{\alpha}_i=\alpha_i \bmod \mathfrak{m}_{\mathscr{O}_K}$, and $\overline{\chi}_i$ denote the function $g\mapsto\chi_i(g)\bmod\mathfrak{m}_{\mathscr{O}_K}$. Since at least one of the α_i isn't in $\mathfrak{m}_{\mathscr{O}_K}$, we still have a nontrivial linear dependence relation as k-valued class functions on G. ⊠

Corollary 1.2.6. *The reductions of the irreducible characters for a group G are linearly independent over k.*

This is because the irreducible characters are linearly independent.

Proposition 1.2.4 tells us that the characteristic polynomial of the reduction is well-defined, but it also completely determines the semisimplification.

Proposition 1.2.7. *Let M and N be f.g. $k[G]$-modules such that for every $g \in G$, the characteristic polynomials for $(g\cdot) \in \operatorname{End}_k(M)$ and $(g\cdot) \in \operatorname{End}_k(N)$ are equal. Then, the semisimplifications of M and N are isomorphic.*

Proof. Let $\{S_i\}_{i\in I}$ denote the set of isomorphism classes of simple f.g. $k[G]$-modules, and assume that there exists some pair of modules M and N whose characteristic polynomials are equal for all $g \in G$, but that are not themselves isomorphic. Then, let m_i be the multiplicity of S_i in the composition factors for M, and n_i be the multiplicity of S_i in the composition factors for N. In particular, choose M and N to be minimal over all such pairs of $k[G]$-modules, as a pair that minimizes $\sum_{i\in I} m_i + n_i$. Since M and N are finitely generated, this is a finite sum, so such a minimum exists.

If $g \in G$, then the characteristic polynomials for the actions of g on M and N are equal, so the characters for M and N are equal. In particular, if $\theta_i(g)$ denotes the characteristic polynomial of g acting on S_i, the characters are

$$\chi_M(g) = \sum_{i\in I} m_i \operatorname{Tr}(\theta_i(g)) = \sum_{i\in I} n_i \operatorname{Tr}(\theta_i(g)) = \chi_N(g).$$

Thus, by Proposition 1.2.5, the irreducible characters are independent, so $n_i \equiv m_i \bmod p$ for each i.

Now, let's look at the characteristic polynomials themselves. Since they're equal, their ratio is 1, i.e. for any $g \in G$, the following is true in k:

$$\prod_{i\in I} \theta_i(g)^{n_i - m_i} = 1.$$

But since $n_i - m_i \equiv 0 \bmod p$, each term in the product is a p^{th} power. And since we're in characteristic p, if f and g are polynomials with $(f(x)/g(x))^p = 1$, then $f(x)/g(x) = 1$ (since there are no other p^{th} roots), and therefore

$$\prod_{i\in I} \theta_i(g)^{(n_i - m_i)/p} = 1.$$

This means that we can choose smaller values for the sum of the m_i and n_i and still have the characteristic polynomials for the resulting M and N be equal, which is a contradiction, because we assumed we chose the minimal pair. ⊠

In summary, reduction is a way of obtaining representations in positive characteristic from ones in characteristic zero. We'll often use $K = \overline{\mathbb{Q}}_p$ and $k = \overline{\mathbb{F}}_p$ after this section, to avoid having to worry about which fields representations are defined over. Reduction will be very useful for our concrete calculations in chapter 2.

1.3. Modular Characters

As in the previous section, let G be a finite group and p be a prime dividing $|G|$. We'll again be interested in reducing representations from $K = \overline{\mathbb{Q}}_p$ to $k = \overline{\mathbb{F}}_p$; thus, all modules in this section will be assumed to be finitely generated.

Definition. An element g of G is *p-regular* if $p \nmid |g|$. Similarly, a conjugacy class is p-regular if its elements are (since they all have the same order). The set of p-regular elements of G is denoted $G^{(p)}_{\text{reg}}$.

Let m denote the least common multiple of the orders of the elements of $G^{(p)}_{\text{reg}}$, and let $\mu_K \subset K$ and $\mu_k \subset k$ denote the sets of m^{th} roots of unity in each respective field. Then, since $p \nmid m$, μ_k and μ_K both have m elements, and reduction mod p is an isomorphism $r : \mu_K \to \mu_k$ of the multiplicative group structures.

If M is an n-dimensional representation of G, then any $g \in G^{(p)}_{\text{reg}}$ defines an action $(g\cdot) \in \operatorname{End}_k(M)$. Its eigenvalues $\lambda_1, \dots, \lambda_n$ must lie in μ_k, as $g^m = \text{id}$, and if λ is an eigenvalue of g, then λ^m must be an eigenvalue of id, i.e. 1. Thus, one can define a function $\phi_M : G^{(p)}_{\text{reg}} \to K$ by the formula

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

Definition. This function ϕ_M is called the *Brauer character* or *modular character* of M.

Here are some quick but important properties.

Proposition 1.3.1.

(1) $\phi_M(1) = \dim_k(M)$.
(2) ϕ_M *is a class function on* $G_{\mathrm{reg}}^{(p)}$*, i.e. if* $g \in G_{\mathrm{reg}}^{(p)}$ *and* $h \in G$*, then* $\phi_M(hgh^{-1}) = \phi_M(g)$.
(3) If $0 \to M' \to M \to M'' \to 0$ *is a short exact sequence of* $k[G]$*-modules, then* $\phi_M = \phi_{M'} + \phi_{M''}$*. Thus, as a special case,* $\phi_{M\oplus N} = \phi_M + \phi_N$ *for* $k[G]$*-modules* M *and* N.
(4) If M *and* N *are* $k[G]$*-modules, then* $\phi_{M\otimes N} = \phi_M \cdot \phi_N$.

Proof. These proofs do not differ significantly from the proofs of the analogous facts for ordinary characters in characteristic 0.

For part (1), 1 acts as the identity map, so all of its eigenvalues are 1, and there are $\dim_k(M)$ of them.

Part (2) follows because the eigenvalues of an endomorphism are invariant under conjugation.

In part (3), it's possible to consider this a short exact sequence of vector spaces, because the eigenvalues are calculated using only the information of each module as a k-vector space. However, a short exact sequence of vector spaces always splits. Thus, if A_M is the matrix of $g \in G$ acting on M, and $A_{M'}$ and $A_{M''}$ are defined similarly, then there is a k-basis for M in which

$$A_M = \begin{pmatrix} A_{M'} & \\ & A_{M''} \end{pmatrix}.$$

Thus, set of eigenvalues of A_M is the union (with multiplicity) of the sets of eigenvalues of $A_{M'}$ and $A_{M''}$, so $\phi_M(g) = \phi_{M'}(g) + \phi_{M''}(g)$.

Part (4) is true because if $g \in G$ and $\lambda_1, \dots, \lambda_m$ are the eigenvalues of g acting on M, and $\nu_1, \dots, \nu_n$ are the eigenvalues of g acting on N, then the eigenvalues of g acting on $M \otimes N$ are $\{\lambda_i \nu_j \mid 1 \le i \le m, 1 \le j \le n\}$. ⊠

Since the list of composition factors of a module is generated by repeatedly taking submodules and quotients, then applying part (3) of the above proposition yields the following.

Corollary 1.3.2. *Let* M *be a* $k[G]$*-module and* $N_1, \dots, N_m$ *be its composition factors. Then,* $\phi_M = \phi_{N_1} + \cdots + \phi_{N_m}$.

Then, there are a few more results which tie these characters more explicitly to representations.

Proposition 1.3.3. *Let* M *be a* $K[G]$*-module with character* χ_M*, and let* $\overline{M}$ *denote a reduction of* M*. Then,* $\phi_{\overline{M}} = \chi_M|_{G_{\mathrm{reg}}^{(p)}}$.

That is, reduction sends ordinary characters to modular characters!

Proof. Let $g \in G_{\mathrm{reg}}^{(p)}$. Then, the action of g in $\mathrm{End}_k(M)$ has trace $\chi_M(g) = \lambda_1 + \cdots + \lambda_n$ for $\lambda_i \in \mu_K$, as per the above discussion.

Thus, $\phi_{\overline{M}}(g) = \chi_M(g) \bmod p$, because the characteristic polynomial for g acting on $\overline{M}$ is just that of g acting on M modulo p. But reduction mod p is an isomorphism $\mu_K \to \mu_k$, so $\phi_{\overline{M}}(g) = \chi_M(g)$. ⊠

Theorem 1.3.4 (Brauer)**.** *The irreducible modular characters* $\{\phi_M \mid M$ *is a simple* $k[G]$*-module*$\}$ *are a basis for the* K*-vector space* $C\ell(G_{\mathrm{reg}}^{(p)}, K)$ *of class functions* $G_{\mathrm{reg}}^{(p)} \to K$.

Proof. First, we must show that they span $C\ell(G_{\mathrm{reg}}^{(p)}, K)$. Given any class function $f : G_{\mathrm{reg}}^{(p)} \to K$, it's possible to extend it to a class function $\widetilde{f} : G \to K$ (e.g. letting $\widetilde{f}(g) = 0$ if $g \notin G_{\mathrm{reg}}^{(p)}$). Since the characters of simple $K[G]$-modules are a basis for $C\ell(G, K)$, there's a linear combination

$$\widetilde{f} = \sum_i \lambda_i \chi_{M_i}$$

where each M_i is a simple $K[G]$-module and $\lambda_i \in K$, and if we restrict to the p-regular conjugacy classes, we get the same relation for f. Reduce each M_i mod p to get a $k[G]$-module $\overline{M}_i$; by Proposition 1.3.3, we now have the relation

$$f = \sum_i \lambda_i \phi_{\overline{M}_i}.$$

For a given i, $\overline{M}_i$ may not be a simple $k[G]$-module, but it has some finite list of composition factors $N_{i,1}, \dots, N_{n,m_i}$, which are simple $k[G]$-modules. Then, by Corollary 1.3.2,

$$f = \sum_i \sum_{j=1}^{m_i} \lambda_i \phi_{N_j},$$

so f is a linear combination of modular characters of simple $k[G]$-modules.

Next, we will show that the irreducible modular characters $\phi_1, \ldots, \phi_\ell$ are linearly independent. Since these are class functions $G^{(p)}_{\text{reg}} \to K$, it's possible to extend each one to a class function $\widetilde{\phi}_i : G \to K$ by letting $\widetilde{\phi}_i(g) = 0$ if $g \notin G^{(p)}_{\text{reg}}$, and $\widetilde{\phi}_i(g) = \phi_i(g)$ otherwise. In particular, the $\widetilde{\phi}_i$ are linearly independent if and only if the ϕ_i are.

By Proposition 1.2.5, the $\widetilde{\phi}_i$ are linearly independent if their reductions $\overline{\phi}_i$ are, so suppose there is a dependence relation between the $\overline{\phi}_i$:

$$\sum_i \alpha_i \overline{\phi}_i = 0,$$

with the $\alpha_i \in k$.

Let j be such that $\alpha_j \neq 0$. By the Jacobson density theorem (Theorem 1.1.3), there exists an $x \in k[G]$ such that $\overline{\phi}_i(x) = 0$ when $i \neq j$ and is nonzero when $i = j$, i.e. x acts as a projection. For this x, the dependence relation is $\alpha_j \overline{\phi}_j(x) = \alpha_j \cdot c_j = 0$ for a nonzero c_j, which is a contradiction. In particular, the $\overline{\phi}_i$ are linearly independent, so the $\widetilde{\phi}_i$ are, and therefore the irreducible modular characters ϕ_i are linearly independent as well. ⊠

In characteristic zero, two representations of the same group G with equal characters are isomorphic. This isn't true in positive characteristic: the two $k[S_3]$-representations from Example 1.2.3 aren't isomorphic, but have equal characteristic polynomials, and therefore their characters are equal. The key is once again semisimplification.

Corollary 1.3.5. *If the modular characters of two $k[G]$-modules M and N are equal, then their semisimplifications are isomorphic.*

Proof. By Theorem 1.3.4, the character of M is a linear combination of the irreducible modular characters in a unique way, the sum of the characters of the composition factors of M. However, since it's equal to the character of N, it is also the sum of the characters of the composition factors of N. These are two ways of writing this character as a linear combination of the irreducible modular characters, so they must have the same coefficients; therefore, the composition factors of M and N must be the same up to isomorphism. In particular, since the semisimplification is the direct sum of the composition factors, the semisimplifications of M and N are isomorphic. ⊠

In particular, when building character tables, the following corollary is extremely useful.

Corollary 1.3.6. *The number of irreducible modular characters, and therefore the number of isomorphism classes of simple $k[G]$-modules, is equal to the number of p-regular conjugacy classes of G.*

Proof. If there are ℓ classes of G that are p-regular, then a class function on $G^{(p)}_{\text{reg}}$ is a choice of ℓ elements of K, and therefore a basis for this space has ℓ elements. ⊠

It'll also be useful to have the following criterion, which is proven in [7, §16.4].

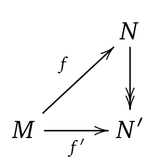
Theorem 1.3.7 (Brauer-Nesbitt). *Let n be the largest power of p dividing $|G|$ and M be a simple $K[G]$-module such that $n \mid \dim(M)$. Then, if $\overline{M}$ is a reduction of M, $\overline{M}$ is a simple $k[G]$-module.*

1.4. Projective Modules

Projective modules are important in modular representation theory: when k has characteristic dividing $|G|$, projective $k[G]$-modules are particularly well-behaved, and if $\text{char}(k) = 0$ or doesn't divide $|G|$, all $k[G]$-modules are projective, so the existence of nonprojective $k[G]$-modules is another important difference that arises in modular representation theory.

First of all, let's recall the definition of projective.

Definition. If A is a ring, then a A-module M is a *projective module* if maps out of M can be lifted across surjections; that is, for every surjection $N \twoheadrightarrow N'$ of A-modules and A-module homomorphism $f' : M \to N'$, there exists an A-linear $f : M \to N$ such that the following diagram commutes.



For example, free modules are projective.

The following equivalent criterion will also be useful.

Lemma 1.4.1. *An A-module M is projective iff it is a direct summand in a free module.*

Proof. First, assume M is projective. It is always possible to find a free module F and a surjection $\pi : F \twoheadrightarrow M$ (e.g. let F be free on the elements of M). Since M is projective, the identity map $\mathrm{id} : M \to M$ lifts to an $f : M \to F$ such that $\pi \circ f = \mathrm{id}$. Thus, in the short exact sequence

$$0 \longrightarrow \ker(\pi) \longrightarrow F \xrightarrow{\pi} M \longrightarrow 0, \tag{1.4.1}$$

f is a section for π, and so (1.4.1) splits. Therefore, $F \cong M \oplus \ker(f)$, and so M is a direct summand in a free module.

In the other direction, let $F = M \oplus M'$, where F is free, and let $\pi : N \twoheadrightarrow N'$ be a surjective map of A-modules. Given an $f' : M \to N'$, we can define a $\widetilde{f}' : F \to N'$ by letting $\widetilde{f}'(m,n) = f(m)$; since F is free and therefore projective, this map lifts to a $\widetilde{f} : F \to N$ such that $\pi(\widetilde{f}(m,n)) = \widetilde{f}(m,n) = f(m)$. Let $f : M \to N$ be given by $f(m) = \widetilde{f}(m,0)$; this defines a lift for f', so M is projective. ⊠

One of the reasons projective $k[G]$-modules are important in modular representation theory is that they correspond closely to projective $\mathscr{O}_K[G]$-modules.

Proposition 1.4.2. *If M is a projective $k[G]$-module, then there is a unique (up to isomorphism) projective $\mathscr{O}_K[G]$-module P such that $P/\mathfrak{m}_{\mathscr{O}_K}P \cong M$.*

For a proof of this result, see [7, §14.4].

Though not all simple $k[G]$-modules are projective, there's a similar notion that will play an important role in later sections.

Definition. A *projective indecomposable* is an f.g. projective $k[G]$-module that is indecomposable (that is, it doesn't split as the direct sum of two $k[G]$-modules).

These are the building blocks of the projective $k[G]$-modules, as Corollary 1.4.6, below, will illustrate. To prove it, though, we need a few preliminary results first.

Lemma 1.4.3 (Fitting)**.** *Let A be a ring and M be an indecomposable A-module of finite length. Then, every $\varphi \in \mathrm{End}_A(M)$ is either an isomorphism or nilpotent.*

Proof. We have chains of submodules of M given by

$$\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \ker(\varphi^3) \subseteq \cdots$$

and

$$\mathrm{Im}(\varphi) \supseteq \mathrm{Im}(\varphi^2) \supseteq \mathrm{Im}(\varphi^3) \supseteq \cdots,$$

but since M has finite length, these must stabilize, so there's an n such that $\ker(\varphi^n) = \ker(\varphi^{n+k})$ and $\mathrm{Im}(\varphi^n) = \mathrm{Im}(\varphi^{n+k})$ when $k \geq 0$.

Suppose $x \in \mathrm{Im}(\varphi^n) \cap \ker(\varphi^n)$. Then, $x = \varphi^n(z)$ for some $z \in M$, and since $x \in \ker(\varphi^n) = \ker(\varphi^{2n})$, then $z \in \ker(\varphi^n)$, so $x = 0$. Thus, $\mathrm{Im}(\varphi^n) \cap \ker(\varphi^n) = 0$. Also, for any $x \in M$, $\varphi^n(x) \in \mathrm{Im}(\varphi^n) = \mathrm{Im}(\varphi^{2n})$, so $\varphi^n(x) = \varphi^{2n}(z)$. Let $y = x - \varphi^n(z)$; then, $\varphi^n(x - \varphi^n(z)) = 0$, or $x = y + \varphi^n(z)$.

Thus, $M = \mathrm{Im}(\varphi^n) \oplus \ker(\varphi^n)$, so since M is indecomposable, either $\ker(\varphi^n) = 0$ and $\mathrm{Im}(\varphi^n) = M$, meaning φ is an isomorphism, or $\ker(\varphi^n) = M$, so φ is nilpotent. ⊠

Corollary 1.4.4. *Let A be a ring, M be an indecomposable A-module of finite length, and $\varphi_1, \dots, \varphi_n \in \mathrm{End}_A(M)$. If $\varphi_1 + \cdots + \varphi_n$ is an isomorphism, then at least one of the φ_i is.*

Proof. First, let $n = 2$ and suppose not. Without loss of generality assume that $\varphi_1 + \varphi_2 = \mathrm{id}$, because if not, we can replace φ_1 with $\varphi_1 \circ (\varphi_1 + \varphi_2)^{-1}$ and φ_2 with $\varphi_2 \circ (\varphi_1 + \varphi_2)^{-1}$. Thus, $\varphi_1 + \varphi_2 = \mathrm{id}$; in particular, this means they commute.

Since both φ_1 and φ_2 aren't isomorphisms, then by Lemma 1.4.3, they're both nilpotent, so there exists an N such that $\varphi_1^N = \varphi_2^N = 0$. But since φ_1 and φ_2 commute, the expansion of $(\varphi_1 + \varphi_2)^{2N}$ has in all of its terms at least one of the φ_i raised to a power at least N, so $(\varphi_1 + \varphi_2)^{2N} = 0$ as well. Thus, $\varphi_1 + \varphi_2$ is nilpotent, so it cannot be an isomorphism.

Finally, apply induction to get this for all n. ⊠

Theorem 1.4.5 (Krull-Schmidt)**.** *If A is a ring and M is an A-module with finite length, there is a unique way to write M as a finite direct sum of indecomposable A-modules, up to isomorphism of the direct-sum factors and reordering.*

Proof. Let $M_1, \dots, M_m$ and $N_1, \dots, N_n$ be A-submodules of M such that

$$M = \bigoplus_{i=1}^{m} M_i = \bigoplus_{j=1}^{n} N_j.$$

Without loss of generality, assume $m \le n$, for if not, the M_i and N_j may be switched.

Let $p_i : M_1 \to N_i$ denote the restriction to M_1 of the canonical projection $M \twoheadrightarrow N_i$ and q_j denote the restriction to N_j of the canonical projection $M \twoheadrightarrow M_1$. Thus, $\psi = \sum_{i=1}^{n} q_i \circ p_i = \mathrm{id}_{M_1}$, as each $x \in M_1$ is dissected into its components $(x_1, \dots, x_n)$ from each of the N_j; then, restricted to each component, ψ is the identity. Thus, by Corollary 1.4.4, one of the $q_i \circ p_i$ must be an isomorphism.

Thus, we have maps $p_i : M_1 \to N_i$ and $q_i : N_i \to M_1$ whose composition is an isomorphism; this means that $M_1 \cong \mathrm{Im}(q_i) \oplus \ker(p_i)$, but since M_1 is indecomposable, the only way for this to happen is for p_i and q_i to be isomorphisms or $p_i = 0$ — but then $q_i \circ p_i = 0$. In particular, $M_1 \cong N_i$, and then the rest of the proof follows by induction.

Finally, we need to show existence of a direct-sum decomposition, but if there's no way to write M as a direct sum of indecomposables, then it's indecomposable, so it is its own decomposition. Thus, there is exactly one such decomposition into indecomposables. ⊠

Corollary 1.4.6. *If M is an f.g. projective $k[G]$-module, then there is a unique way to write $M \cong P_1 \oplus \cdots \oplus P_\ell$ up to isomorphism of the direct-sum factors and reordering, where the P_i are projective indecomposable $k[G]$-modules.*

Proof. M has a finite number of composition factors, as discussed in Section 1.1, so using Theorem 1.4.5, there's a unique way to write $M \cong P_1 \oplus \cdots \oplus P_\ell$ for indecomposable $k[G]$-modules, up to isomorphism of factors and reordering.

By Lemma 1.4.1, M is a direct summand in a free module F, so

$$F \cong M \oplus M' \cong P_1 \oplus \cdots \oplus P_\ell \oplus M',$$

and therefore each P_i is also a projective module, and therefore a projective indecomposable. ⊠

1.5. The CDE Triangle

Some of the most powerful statements in modular representation theory, relating representations in characteristic zero to those in characteristic p, can be encapsulated in a commutative diagram called the CDE triangle.

Most of the tools we've been using have been invariant under semisimplification, including the characteristic polynomial (which actually determines the semisimplification, by Proposition 1.2.7) and the reduction of a $K[G]$-module. Thus, it will be useful for us to identify modules up to their semisimplifications. This motivates the following definition.

Definition.

- Let A be a ring and $\mathscr{C}$ be a full subcategory of the category of finitely generated A-modules. Then, the *Grothendieck group* of $\mathscr{C}$, denoted $\mathrm{GG}(\mathscr{C})$, is the abelian group with the following generators and relations.
  - For each object M in $\mathscr{C}$, there is a generator $[M] \in \mathrm{GG}(\mathscr{C})$.
  - For each short exact sequence $0 \to M' \to M \to M'' \to 0$ in $\mathscr{C}$, add the relation $[M] = [M'] + [M'']$.

  The class of an A-module M in the Grothendieck group is denoted $[M]$.
- If L is a field, G is a group, and $\mathscr{F}_L$ denotes the category of f.g. $L[G]$-modules, the Grothendieck group $\mathrm{GG}(\mathscr{F}_L)$ is denoted $R_L(G)$. If $\mathscr{P}_L$ denotes the category of f.g. projective $L[G]$-modules, the Grothendieck group $\mathrm{GG}(\mathscr{P}_L)$ is denoted $P_L(G)$.

Notice that some elements of $\mathrm{GG}(\mathscr{C})$, such as $-[M]$, aren't classes of modules, though every element is a linear combination of classes of modules.

Lemma 1.5.1. *If $N_1, \dots, N_m$ are the composition factors of an A-module $M \in \mathscr{C}$, then in $\mathrm{GG}(\mathscr{C})$, $[M] = [N_1] + \cdots + [N_m]$.*

Proof. Let's induct on m, the number of composition factors; this is vacuously true if $m = 1$.

More generally, suppose M has m composition factors, where $m > 1$. Then, there exists a nontrivial A-submodule $N \subsetneq M$, and therefore M/N is nontrivial as well. Then, the set of composition factors of M is the union of those of N and those of M/N, and since both N and M/N are nontrivial A-modules, each has strictly fewer composition factors than M does. By induction, the result is true for N and M/N, so $[M] = [N] + [M/N] = [N_1] + \cdots + [N_m]$. ⊠

Corollary 1.5.2. *If two A-modules $M_1, M_2 \in \mathscr{C}$ have the same composition factors up to isomorphism, then $[M_1] = [M_2] \in \mathrm{GG}(\mathscr{C})$.*

Proof. Let $\{N_1, \dots, N_m\}$ be these composition factors; then, $[M_1] = [N_1] + \cdots + [N_m] = [M_2]$. ⊠

Thus, in the Grothendieck group, modules are identified with their semisimplifications.

Finally, it'll be useful to have a criterion for checking when a map is well-defined on a Grothendieck group.

Lemma 1.5.3. *Let H be an abelian group and $\Phi : \mathscr{C} \to H$ be a function. If for every exact sequence $0 \to M' \to M \to M'' \to 0$ we have $\Phi(M) = \Phi(M') + \Phi(M'')$, then there is a unique group homomorphism $\Phi^* : \mathrm{GG}(\mathscr{C}) \to H$ such that $\Phi^*([M]) = \Phi(M)$ for all $M \in \mathscr{C}$.*

In this case, Φ is called *additive*.

Proof. The relations for $\mathrm{GG}(\mathscr{C})$ are all of the form $[M] = [M'] + [M'']$ for such short exact sequences, and so Φ^* as defined in the theorem statement commutes with all relations in $\mathrm{GG}(\mathscr{C})$, and is therefore is well-defined. Thus, such a Φ^* exists; it is unique because it's specified on the basis for $\mathrm{GG}(\mathscr{C})$. ⊠

We will be able to apply these properties of general Grothendieck groups to the specfic cases of $R_L(G)$ and $P_L(G)$, which are necessary for defining the CDE triangle. Let G, K, and k be as in the previous sections.

Proposition 1.5.4. *If L is a field, then $R_L(G)$ is a free $\mathbb{Z}$-module, and the set S_L of isomorphism classes of simple f.g. $L[G]$-modules is a basis for $R_L(G)$.*

Proof. Let R be a free abelian group with S_L as a basis. Then, there's a map $\alpha : R \to R_L(G)$ given by sending a simple module $M \in S_L$ to its class $[M]$.

The assignment sending a module to the sum of its composition factors in R is additive, because if $0 \to N \to M \to M/N \to 0$ is a short exact sequence, then the set of composition factors of M is the union of those of N and of M/N, up to isomorphism. Thus, by Proposition 1.5.3, there exists a unique group homomorphism $\beta : R_L(G) \to R$ such that if M is an $L[G]$-module with composition factors $N_1, \dots, N_n$, then $\beta([M]) = N_1 + \cdots + N_n$.

Finally, α and β are inverses: if $M \in S_L$, then $\beta(\alpha(M))$ is equal to M again, since it's simple, so M is its only composition factor, and if $[M] \in R_L(G)$ has composition factors $N_1, \dots, N_m$, then $[M] = [N_1] + \cdots + [N_m] = \alpha(N_1 + \cdots + N_n) = \alpha(\beta(M))$. ⊠

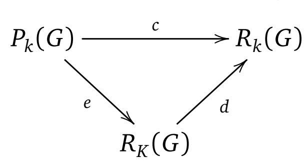
Proposition 1.5.5. *$P_k(G)$ is a free $\mathbb{Z}$-module, and the set S_P of classes of f.g. projective indecomposables is a basis for $P_k(G)$.*

Proof. The proof for Proposition 1.5.4 can be adapted to this case as well; the key is that Corollary 1.4.6 guarantees that there exists a unique decomposition of any f.g. projective $k[G]$-module into projective indecomposables.

Thus, we may let P be the free abelian group with S_P as a basis, and define $\alpha : P \to P_k(G)$ by sending a projective indecomposable $M \in S_P$ to its class $[M]$. Then, there's also a map $\beta : P_k(G) \to P$ defined by decomposing a projective $k[G]$-module M into a direct sum of projective indecomposables $N_1, \dots, N_m$, sending $[M] \mapsto N_1 + \cdots + N_m$, and extending linearly to the whole group. This assignment is again additive, so defines a group homomorphism $\beta : P_k(G) \to P$.

α and β are inverses, because if M decomposes into a direct sum of the projective indecomposables $N_1, \dots, N_m$, then $[M] = [N_1] + \cdots + [N_m]$. ⊠

Now, we can introduce the CDE triangle, which is the following diagram of abelian groups.



(1.5.1)

We already know what the objects are, so now we must define c, d, and e.

1.5.1. Definition of $c : P_k(G) \to R_k(G)$. Let P be an f.g. projective $k[G]$-module; then, sending P to its class in $R_k(G)$, i.e. as an f.g. $k[G]$-module, is additive, because if $0 \to P' \to P \to P'' \to 0$ is short exact, then in $R_k(G)$, $[P] = [P'] + [P'']$. Thus, by Lemma 1.5.3, this defines a group homomorphism $c : P_k(G) \to R_k(G)$; often, it is called the *Cartan homomorphism*.

1.5.2. Definition of $d : R_K(G) \to R_k(G)$. Given an f.g. $K[G]$-module M, i.e. a representation of G in characteristic zero, we defined how to reduce it to a representation in characteristic p, i.e. a $k[G]$-module.

Lemma 1.5.6. *If M is an f.g. $K[G]$-module and Λ_1 and Λ_2 are two G-stable lattices in M, then the semisimplifications of the reductions of M with respect to Λ_1 and Λ_2 are isomorphic.*

Proof. Let N_1 be the reduction of M with respect to Λ_1 and N_2 be that with respect to Λ_2. By Proposition 1.2.4, the characteristic polynomials N_1 and N_2 are equal for any $g \in G$, so by Proposition 1.2.7 the semisimplifications of N_1 and N_2 are isomorphic. ⊠

Thus, reduction defines a function red : {isomorphism classes of f.g. $K[G]$-modules} $\to R_k(G)$.

Lemma 1.5.7. red *is an additive function.*

Proof. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of $K[G]$-modules. Then, M and $M' \oplus M''$ have isomorphic semisimplifications, so for any $g \in G$, the actions of g on M and on $M' \oplus M''$ have equal characteristic polynomials. In the proof of Proposition 1.2.4, we showed that the characteristic polynomial of a reduction is obtained from the characteristic polynomial of the original by reducing the coefficients modulo $\mathfrak{m}_{\mathcal{O}_K}$, so if $\overline{M}$ is a reduction of M and $\overline{N}$ is a reduction of $M' \oplus M''$, then for any $g \in G$, the actions of g on $\overline{M}$ and on $\overline{N}$ have the same characteristic polynomials. But by Proposition 1.2.7, the characteristic polynomial of a $k[G]$-module completely determines its semisimplification, so $\overline{M}$ and $\overline{N}$ have isomorphic semisimplifications, and therefore have the same class in $R_k(G)$. ⊠

Thus, reduction is a homomorphism $d : R_K(G) \to R_k(G)$. This is called the *decomposition homomorphism*.

1.5.3. Definition of $e : P_k(G) \to R_K(G)$. By Proposition 1.4.2, given a projective $k[G]$-module M, there's a unique projective $\mathcal{O}_K[G]$-module P up to isomorphism such that $P/\mathfrak{m}_{\mathcal{O}_K}P \cong M$. Then, $P \otimes_{\mathcal{O}_K} K$ is a $K[G]$-module.

We will check that the assignment $M \mapsto [P \otimes_{\mathcal{O}_K} K] \in R_K(G)$ is additive, and therefore defines a map $e : P_k(G) \to R_K(G)$ sending $[M] \mapsto [P \otimes_{\mathcal{O}_K} K]$ and extending linearly.

Suppose $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of projective $k[G]$-modules; then, $\mathrm{id}_{M''}$ lifts across the surjection $M \twoheadrightarrow M''$ to a section, so the sequence splits and $M \cong M' \oplus M''$. Let P' be the projective $\mathcal{O}_K[G]$-module such that $P'/\mathfrak{m}_{\mathcal{O}_K}P' \cong M'$, and P'' be that for M''; then, $P' \oplus P''$ reduces mod $\mathfrak{m}_{\mathcal{O}_K}$ to M, because

$$(P' \oplus P'')/\mathfrak{m}_{\mathcal{O}_K}(P' \oplus P'') \cong (P'/\mathfrak{m}_{\mathcal{O}_K}P') \oplus (P''/\mathfrak{m}_{\mathcal{O}_K}P'') \cong M' \oplus M'' \cong M.$$

Thus, $e(M) = [(P' \oplus P'') \otimes_{\mathcal{O}_K} K] = [(P' \otimes_{\mathcal{O}_K} K) \oplus (P'' \otimes_{\mathcal{O}_K} K)] = e(M' \oplus M'')$, so it's additive.

1.5.4. Properties of the CDE Triangle.

Theorem 1.5.8. *The CDE diagram* (1.5.1) *commutes.*

Proof. Using the definitions of c, d, and e, the theorem statement is equivalent to stating that if one chooses a projective $k[G]$-module P and lifts it to a $K[G]$-module M as described in Section 1.5.3, the semisimplification of P is isomorphic to the semisimplification of the reduction of M.

P is lifted to M by way of an intermediate $\mathcal{O}_K[G]$-module P', which has the properties that $P' \otimes_{\mathcal{O}_K} K = M$ and $P'/\mathfrak{m}_{\mathcal{O}_K}P' \cong P$. The first property means there's a natural inclusion $i : P' \hookrightarrow M$ of $\mathcal{O}_K[G]$-modules defined by $i(x) = x \otimes 1$, so that $i(P')$ is isomorphic to P'. Furthermore, $i(P')$ is a G-stable lattice in M, since it is an $\mathcal{O}_K[G]$-module that generates all of M when tensored with K.

Thus, we may as well use $i(P')$ as our lattice for reducing M, since the class of the reduction in $R_k(G)$ doesn't depend on the choice of lattice. But $i(P') \cong P'$, so the reduction is just $P'/\mathfrak{m}_{\mathcal{O}_K}P'$, which is isomorphic to P again. Thus, any reduction of M has semisimplification isomorphic to that of P, so the diagram commutes. ⊠

Proposition 1.5.9. *In the bases S_K of $R_K(G)$, S_k of $R_k(G)$, and S_P of $P_k(G)$ defined in Propositions 1.5.4 and 1.5.5, $E = D^{\mathrm{T}}$, and therefore C is a symmetric matrix.*

This is proven in [7, §15.4].

Theorem 1.5.10. *d is surjective.*

This is proven in [7, §17.3].

Corollary 1.5.11. *e is injective.*

Proof. Since $E = D^{\mathrm{T}}$ and D is surjective, then if D is an $m \times n$ matrix, then its rank is m, so E is an $n \times m$ matrix with the same rank. Thus, the dimension of its kernel is $m - \operatorname{rank}(E) = 0$. ⊠

Theorem 1.5.12. *c is injective.*

This is proven in [7, §16.1], and can be restated by applying the definition of the Grothendieck groups.

Corollary 1.5.13. *If two projective $k[G]$-modules have the same composition factors up to isomorphism, they are isomorphic.*

Proof. If two projective $k[G]$-modules M and M' have the same composition factors up to isomorphism, then they define the same class in $P_k(G)$, because c is injective. By Corollary 1.4.6, each can be written as a direct sum of the projective indecomposables $P_1, \dots, P_\ell$ in a unique way:

$$M = (P_1)^{m_1} \oplus (P_2)^{m_2} \oplus \cdots \oplus (P_\ell)^{m_\ell}, \qquad \text{and} \qquad M' = (P_1)^{n_1} \oplus (P_2)^{n_2} \oplus \cdots \oplus (P_\ell)^{n_\ell},$$

where the m_i and n_i denote the multiplicity of P_i in the direct sums for M and M', respectively.

By Proposition 1.5.5, the classes $[P_i]$ of these projective indecomposables are a basis for $P_k(G)$, so since M and M' define the same class, then

$$[M] = \sum_{i=1}^{\ell} m_i [P_i] = [M'] = \sum_{i=1}^{\ell} n_i [P_i],$$

in $P_k(G)$, but this means $m_i = n_i$ for all i, and therefore $M \cong M'$. ⊠

Finally, the following proposition, a corollary of Theorem 1.5.10, is useful for calculations: in order to determine all of the irreducible modular characters for a group, one can start with the characters from characteristic 0, which are well-known, and then reduce and decompose. This will be our primary technique for calculating irreducible characters in Chapter 2.

Proposition 1.5.14. *The set of irreducible characters obtained by reducing every simple f.g. $K[G]$-module and decomposing the character of each reduction into irreducible modular characters is a complete list of the irreducible modular characters.*

Proof. Since d is surjective, then it sends the basis S_K of $R_K(G)$ to a spanning set $\overline{S}_K$ of $R_k(G)$. Then, replacing the class $[M]$ of a module M with the classes of its irreducible components $[N_1], \dots, [N_n]$ in this set cannot make the spanned set smaller, because $[N_1] + \cdots + [N_n] = [M]$, so the spanned set contains all of the elements it did before the replacement. In particular, if one replaces every element in $\overline{S}_K$ with its composition factors, which are irreducible $k[G]$-modules, the result is still a spanning set. Since $\overline{S}_K \subseteq S_k$ (all of the classes of simple $k[G]$-modules), but S_k is a basis and $\overline{S}_K$ is a spanning set, then $\overline{S}_K = S_k$. ⊠

1.6. The CDE Triangle on the Character Level

The Grothendieck groups in the CDE triangle are closely related to spaces of K-valued class functions; for example, $R_K(G)$ has the set of classes of simple $K[G]$-modules as a basis, and the space $C\ell(G, K)$ of class functions $K \to G$ has the characters of these simple $K[G]$-modules as a basis.

This notion can be made formal by tensoring objects and maps in the CDE triangle with K.

Proposition 1.6.1. *The map $\alpha : K \otimes_K R_K(G) \to C\ell(G, K)$ defined by sending a the class $[M]$ of a simple $K[G]$-module to its character χ_M is an isomorphism.*

Proof. Since $R_K(G)$ is $\mathbb{Z}$-free, then its basis S_K is mapped to a K-basis in $K \otimes_K R_K(G)$. Then, α maps this basis into the set of irreducible characters of G in characteristic 0. Since the assignment of a simple $K[G]$-module to its irreducible character defines a bijection of the isomorphism classes of simple $K[G]$-modules and the irreducible characters, then α is a bijection on these bases, and therefore an isomorphism of K-vector spaces. ⊠

Proposition 1.6.2. *The map $\beta : K \otimes_K R_k(G) \to C\ell(G^{(p)}_{\mathrm{reg}}, K)$ defined by sending the class $[M]$ of a simple $k[G]$-module to its modular character ϕ_M is an isomorphism.*

Proof. Since $R_k(G)$ is $\mathbb{Z}$-free, then its basis S_k is mapped to a K-basis in $K \otimes_K R_k(G)$. Then, β maps this basis into the set of irreducible modular characters of G. Since β defines a bijection from simple $k[G]$-modules to the set of irreducible modular characters, then β is a bijection on these bases, and therefore an isomorphism of K-vector spaces. ⊠

Proposition 1.6.3. *The map α defined in Proposition 1.6.1 identifies the image of $\mathrm{id}_K \otimes e : K \otimes_K P_k(G) \to K \otimes_K R_K(G)$ with the subspace W of $C\ell(G, K)$ of class functions that are 0 off of $G^{(p)}_{\mathrm{reg}}$, and $\mathrm{id}_K \otimes e$ with the inclusion $W \hookrightarrow C\ell(G, K)$.*

Proposition 1.6.4. *Under the identifications α and β from the previous three propositions, $\mathrm{id}_K \otimes d$ and $\mathrm{id}_K \otimes c$ are the restriction of class functions from G to $G^{(p)}_{\mathrm{reg}}$.*

For a proof of these two propositions, see [7, §18.3]. They imply in particular that $\mathrm{id}_K \otimes c : W \to C\ell(G^{(p)}_{\mathrm{reg}}, K)$ is an isomorphism.

Thus, after tensoring with K, the CDE triangle corresponds to the following commutative diagram of K-vector spaces.

$$\begin{array}{ccc} W & \xrightarrow[\mathrm{id}_K \otimes c]{\sim} & C\ell(G^{(p)}_{\mathrm{reg}}, K) \\ & {\scriptstyle \mathrm{id}_K \otimes e} \searrow \quad \nearrow {\scriptstyle \mathrm{id}_K \otimes d} & \\ & C\ell(G, K) & \end{array} \tag{1.6.1}$$

The $\mathbb{Z}$-bases for the Grothendieck groups introduced in Propositions 1.5.4 and 1.5.5 carry over to K-bases for these spaces of class functions under the identifications α and β. Let $s_k = |S_k|$ and $s_K = |S_K|$, so that W and $C\ell(G^{(p)}_{\mathrm{reg}}, K)$ are s_k-dimensional, and $C\ell(G, K)$ is s_K-dimensional.

In particular, we may write the morphisms in (1.6.1) as matrices C, D, and E in these bases, coming from $\mathrm{id}_K \otimes c$, $\mathrm{id}_K \otimes d$, and $\mathrm{id}_K \otimes e$, respectively.

- D, the *decomposition matrix*, is an $s_k \times s_K$ matrix sending the class of a module to its reduction mod p, and therefore by Proposition 1.3.3 sends an ordinary character to the modular character of the reduction, which is a linear combination of the irreducible modular characters. In particular, the entry d_{ij} of D is the coefficient of the i^{th} irreducible modular character ϕ_i in this linear combination for the decomposition of the j^{th} irreducible ordinary character χ_j. That is, for any $g \in G^{(p)}_{\mathrm{reg}}$,

$$\chi_j(g) = \sum_{i=1}^{s_k} d_{ij} \phi_i.$$

  Thus, the j^{th} column of D lists off these coordinates, so we can describe all of the χ_j in terms of the ϕ_i as follows:

$$\begin{bmatrix} \chi_1 \\ \vdots \\ \chi_{s_K} \end{bmatrix} = D^{\mathrm{T}} \begin{bmatrix} \phi_1 \\ \vdots \\ \phi_{s_k} \end{bmatrix}.$$

- C, the *Cartan matrix*, is an $s_k \times s_k$ matrix sending the class of a projective module to its class in $R_k(G)$, and therefore sends the character of a projective module to its modular character on $G^{(p)}_{\mathrm{reg}}$. In particular, since the characters of projective indecomposables are a basis for W, but projective indecomposables may have nonprojective composition factors, the entry c_{ij} of C is the coefficient of the i^{th} irreducible modular character ϕ_i in the expression of the character Φ_j of the j^{th} projective indecomposable. That is, for any $g \in G^{(p)}_{\mathrm{reg}}$,

$$\Phi_j(G) = \sum_{i=1}^{s_k} c_{ij} \phi_i.$$

In the same way as for D, we can describe the Φ_j in terms of the ϕ_i using C^{T}, but since C is symmetric by Proposition 1.5.9, we have

$$\begin{bmatrix} \Phi_1 \\ \vdots \\ \Phi_{s_k} \end{bmatrix} = C \begin{bmatrix} \phi_1 \\ \vdots \\ \phi_{s_k} \end{bmatrix}.$$

- Finally, E is an $s_K \times s_k$ matrix whose coefficients e_{ij} describe how the character Φ_j of a projective indecomposable is a linear combination of the irreducible characters χ_i, i.e.

$$\Phi_j = \sum_{i=1}^{s_K} e_{ij} \chi_i,$$

and therefore in the same way as for D,

$$\begin{bmatrix} \Phi_1 \\ \vdots \\ \Phi_{s_k} \end{bmatrix} = E^{\mathrm{T}} \begin{bmatrix} \chi_1 \\ \vdots \\ \chi_{s_K} \end{bmatrix}.$$

Finally, the following lemma will be used several times when calculating character tables, so it'll be useful to prove it here.

Lemma 1.6.5. *The trivial representation is the only one-dimensional representation of $\mathbb{Z}/p$ in characteristic p.*

Proof. Let k be a field of characteristic p. A one-dimensional representation of $\mathbb{Z}/p$ over k is a group homomorphism $\mathbb{Z}/p \to k^\times$, and since $\mathbb{Z}/p$ is generated by 1, such a homomorphism is uniquely determined by a choice of element $x \in k^\times$ with order p, i.e. a root of $x^p - 1$.

However, in characteristic p, this polynomial factors as $(x-1)^p$, and therefore the only solution is $x = 1$. In this case, the homomorphism $\mathbb{Z}/p \to k^\times$ sends everything to 1, and therefore is the trivial representation. ⊠

We have now covered all of the theory we will need for the character table calculations in the next chapter.

CHAPTER 2

Modular Representations of Some Small Groups

"Did you hear the one about the mathematician who lobbied Congress, so that his interest group would have a faithful representation?"

2.1. The Modular Representation Theory of $\mathbb{Z}/p$

Let p be prime. Then $\mathbb{Z}/p$, the cyclic group of order p, has p elements, so its modular representation theory is only interesting over characteristic p.

Character Table in Characteristic Zero. Since $\mathbb{Z}/p$ is abelian, then each element is in its own conjugacy class, so there are p conjugacy classes and p irreducible representations, and each irreducible representation is one-dimensional. Thus, each irreducible representation is determined by sending the generator $1 \in \mathbb{Z}/p$ to a p^{th} root of unity, so the character table is given in Table 1.

	0	1	2	$\cdots$	$p-1$
χ_1	1	1	1	$\dots$	1
χ_2	1	ζ_p	ζ_p^2	$\dots$	ζ_p^{p-1}
χ_3	1	ζ_p^2	ζ_p^4	$\dots$	ζ_p^{2p-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_p	1	ζ_p^{p-1}	ζ_p^{2p-2}	$\dots$	ζ_p

TABLE 1. Character table for $\mathbb{Z}/p$ in characteristic 0, where p is prime and ζ_p is a fixed primitive p^{th} root of unity.

What Happens In Characteristic p. Since the order of every non-identity element in $\mathbb{Z}/p$ is p, then $\{0\}$ is the sole p-regular conjugacy class. Thus, by Corollary 1.3.6, there's only a single irreducible modular character. The trivial representation over k is irreducible, so its character must be the unique irreducible modular character, and all of the irreducible characters in characteristic 0 reduce to the modular character of the trivial representation in characteristic p, because on the sole p-regular class $\{0\}$, they all equal the The character table is given in Table 2.

	0
ϕ	1

TABLE 2. Character table for $\mathbb{Z}/p$ in characteristic p.

We can also calculate the matrices C, D, and E from Section 1.6, and thus describe the CDE triangle. The decomposition matrix is the $1 \times p$ matrix

$$D = \begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} p \end{bmatrix}.$$

Thus, the character of the sole projective indecomposable is

$$\Phi = \chi_1 + \chi_2 + \cdots + \chi_p$$

or in terms of ϕ,

$$\Phi = p\phi.$$

However, we can go one step better and compute the projective indecomposable for $\mathbb{Z}/p$ itself.

Proposition 2.1.1. *The sole projective indecomposable module for $\mathbb{Z}/p$ in characteristic p is the group algebra $k[\mathbb{Z}/p]$.*

Proof. First of all, why is $k[\mathbb{Z}/p]$ indecomposable? As a $k[\mathbb{Z}/p]$-module, it's generated by the identity e of $\mathbb{Z}/p$, so if it's possible to write $f : k[\mathbb{Z}/p] \xrightarrow{\sim} M \oplus N$, then what is $f(e)$? It must be of the form (m, n) where m generates M and n generates N, or else f wouldn't be surjective. Moreover, the orders of m and n must divide the order of e, which is p, so they must be either 1 or p. They can't both be 1 (or $k[\mathbb{Z}/p]$ would be trivial), and if one is 1 and the other is p, then the direct sum is trivial, so both m and n must have order p. If this is the case, however, then $(m, 0)$ isn't generated by (m, n), but (m, n) is supposed to generate all of $M \oplus N$. Thus, $k[\mathbb{Z}/p]$ is indecomposable.

Since $k[\mathbb{Z}/p]$ is free of dimension 1 over itself, then it is a projective $k[\mathbb{Z}/p]$-module. Thus, it is the projective indecomposable; we know there cannot be any more because there is only one p-regular conjugacy class. ⊠

2.2. The Modular Representation Theory of S_3

S_3, the symmetric group on three elements, has 6 elements, so its modular representation theory breaks down into the cases $p = 2$ and $p = 3$.

2.2.1. Character Table in Characteristic Zero. As conjugacy type is equivalent to cycle type in symmetric groups, there are three conjugacy classes, 1, $(a\ b)$, and $(a\ b\ c)$. The character table for S_3 is given in Table 3.

	1	$(a\ b)$	$(a\ b\ c)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Table 3. Character table for S_3 in characteristic zero.

Here, χ_1 is the character of the trivial representation and χ_2 is that of the sign representation. Then, χ_3 can be found by the orthogonality relations (it must be two-dimensional, since $|S_3| = 6 = 1^2 + 1^2 + \chi_3(1)^2$, and its values on the remaining two classes are given by taking dot products); explicitly, it is the permutation representation on three-tuples summing to zero, since that sum is preserved by the action of S_3. Specifically, if $\sigma \in S_3$, $\sigma \cdot (a_1, a_2, a_3) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)})$. The space of 3-tuples whose sum is zero is two-dimensional, and we obtain the irreducible two-dimensional representation whose character is χ_3.

2.2.2. The case $p = 2$. The 2-regular conjugacy classes are 1 and $(a\ b\ c)$; thus, χ_1 and χ_2 coincide on the 2-regular classes of S_3, and reduce to the trivial character ϕ_1. Then, there can be no more irreducible one-dimensional representations in this characteristic, because such a representation must factor through the abelianization of S_3, which is $\mathbb{Z}/2$, but by Lemma 1.6.5, the only one-dimensional representation of $\mathbb{Z}/2$ in characteristic 2 is trivial.

As a consequence, χ_2 is sent to an irreducible modular character in this characteristic, because if it were reducible, then it would decompose as a sum of two one-dimensional modular characters. Since there's only one 1-dimensional representation, and its character is ϕ_1, then $\chi_2((a\ b\ c))$ would have to be $2\phi_1((a\ b\ c)) = 2$, but instead it's -1. Thus, $\chi_2 \neq 2\phi_1$, so χ_2 reduces to an irreducible modular character ϕ_2 in characteristic 2.

Since there are two 2-regular conjugacy classes, this is the complete list of irreducible representations in this characteristic. The modular character table is presented in Table 4.

	1	$(a\ b\ c)$
ϕ_1	1	1
ϕ_2	2	-1

Table 4. Character table for S_3 in characteristic 2.

The decomposition matrix is

$$D = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, the characters of the projective indecomposables are

$$\begin{aligned} \Phi_1 &= \chi_1 + \chi_2, \\ \Phi_2 &= \chi_3, \end{aligned}$$

or in terms of the ϕ_i,

$$\begin{aligned} \Phi_1 &= 2\phi_1. \\ \Phi_2 &= \phi_2. \end{aligned}$$

We can also compute the projective indecomposable modules for S_3 in characteristic 2. Let V be the representation of S_3 on 3-tuples adding to zero, i.e. $\sigma \cdot (a_1, a_2, a_3) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)})$, which is a two-dimensional representation, and let W be the projective indecomposable of $\mathbb{Z}/2$, which has an S_3-action defined by the sign homomorphism $\mathrm{sign} : S_3 \to \mathbb{Z}/2$, in which $\sigma \cdot x = \mathrm{sign}(\sigma) \cdot x$ for an $x \in W$.

Proposition 2.2.1. *V and W are the two projective indecomposables of S_3 in characteristic* 2*.*

Proof. Since ϕ_2 is the modular character for V, then it has modular character equal to that of Φ_2. Let P be the projective indecomposable which has that character; then, since $\Phi_2 = \phi_2$ on $G^{(p)}_{\mathrm{reg}}$, P and V have the same composition factors up to isomorphism. But V is a simple $k[S_3]$-module, so it has exactly one composition factor, which is itself. The composition factors of P are isomorphic to those of V, so P has a single composition factor isomorphic to V, and therefore $P \cong V$, so V is indeed a projective indecomposable.

Next, we will show that W is projective. Let $\pi : N \twoheadrightarrow N'$ and $f' : W \to N'$ be maps of $k[S_3]$-modules, and let $\{0_{\mathbb{Z}/2}, 1_{\mathbb{Z}/2}\}$ denote the two elements of $\mathbb{Z}/2$. We may regard N and N' as $k[\mathbb{Z}/2]$-modules by averaging under the sign homomorphism: specifically, let

$$\begin{aligned} 0_{\mathbb{Z}/2} \cdot x &= (1\ 2) \cdot x + (1\ 3) \cdot x + (2\ 3) \cdot x \\ 1_{\mathbb{Z}/2} \cdot x &= x + (1\ 2\ 3) \cdot x + (1\ 3\ 2) \cdot x \end{aligned}$$

for $x \in N$ or $x \in N'$. This defines a $\mathbb{Z}/2$-action because

$$1_{\mathbb{Z}/2} \cdot (1_{\mathbb{Z}/2} \cdot x) = 3x + 3(1\ 2\ 3)x + 3(1\ 3\ 2)x = x = 0_{\mathbb{Z}/2} x,$$

since we're in characteristic 2, and similarly $0_{\mathbb{Z}/2} \cdot (0_{\mathbb{Z}/2} \cdot x) = 0_{\mathbb{Z}/2} \cdot x$, $1_{\mathbb{Z}/2} \cdot (0_{\mathbb{Z}/2} \cdot x) = 1_{\mathbb{Z}/2} \cdot x$, and $0_{\mathbb{Z}/2} \cdot (1_{\mathbb{Z}/2} \cdot x) = 1_{\mathbb{Z}/2} \cdot x$.

With this action on N and N', π and f' are $k[\mathbb{Z}/2]$-linear, because as $k[S_3]$-linear maps, they commute with the sign homomorphism. Thus, since W is a projective $k[\mathbb{Z}/2]$-module, f' lifts to a $k[\mathbb{Z}/2]$-morphism f such that $\pi \circ f = f'$, and we know that for any $\sigma \in S_3$,

$$f(\sigma \cdot x) = f((\mathrm{sign}\,\sigma) \cdot x) = (\mathrm{sign}\,\sigma) \cdot f(x), \tag{2.2.1}$$

as f is $k[\mathbb{Z}/2]$-linear. (2.2.1) will allow us to prove f is also $k[S_3]$-linear: to check that it commutes with $(1\ 2)$, we have that

$$\begin{aligned} (1\ 2)f(x) &= f((1\ 2)x) + f((1\ 3)x) + f((2\ 3)x) \\ &= f((1\ 2)x) + f(1_{\mathbb{Z}/2} \cdot x) + f(1_{\mathbb{Z}/2} \cdot x) = f((1\ 2)x) \end{aligned}$$

since we're in characteristic 2, and the proof that the actions of $(1\ 3)$ and $(2\ 3)$ commute with f is the same. Then, for $(1\ 2\ 3)$,

$$\begin{aligned} (1\ 2\ 3)f(x) &= f((1\ 2\ 3)x) + f((1\ 3\ 2)x) + f(x) \\ &= f((1\ 2\ 3)x) + f(0_{\mathbb{Z}/2} \cdot x) + f(0_{\mathbb{Z}/2} \cdot x) = f((1\ 2\ 3)x), \end{aligned}$$

and $(1\ 3\ 2)$ is the same. Thus, f is $k[S_3]$-linear, so W is projective.

Then, we will show that W is indecomposable. If there were an isomorphism $u : W \xrightarrow{\sim} M \oplus N$ of $k[S_3]$-modules, then M and N could be made into $k[\mathbb{Z}/2]$-modules by defining $1 \in \mathbb{Z}/2$ to act as $((1\ 2)+(1\ 3)+(2\ 3))/3$ did, since this also has order 2. Under this action, u is $(\mathbb{Z}/2)$-equivariant, and therefore an isomorphism of $k[\mathbb{Z}/2]$-modules, but we know that W is an indecomposable $k[\mathbb{Z}/2]$-module, so this isn't true, and therefore it's indecomposable as a $k[S_3]$-module as well. ⊠

2.2.3. The case $p = 3$. The 3-regular conjugacy classes are 1 and $(a\ b)$, so χ_1 and χ_2 are distinct on the 3-regular elements of S_3. Since they're the characters of one-dimensional representations, their reductions mod 3 are irreducible modular characters, respectively denoted ϕ_1 and ϕ_2. Since there are only two 3-regular conjugacy classes, then these must be all of the irreducible representations (and χ_3 decomposes to $\phi_1 + \phi_2$ on the 3-regular elements), so the character table is given in Table 5.

	1	$(a\ b)$
ϕ_1	1	1
ϕ_2	1	-1

TABLE 5. Character table for S_3 in characteristic 3.

The decomposition matrix is

$$D = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Thus, the characters of the projective indecomposables are

$$\Phi_1 = \chi_1 + \chi_3,$$
$$\Phi_2 = \chi_2 + \chi_3,$$

or in terms of the ϕ_i,

$$\Phi_1 = 2\phi_1 + \phi_2.$$
$$\Phi_2 = \phi_1 + 2\phi_2.$$

We can also compute the two projective indecomposables for S_3 in characteristic 3. Let V denote the permutation representation on k^3, where $\sigma \cdot (a_1, a_2, a_3) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)})$, and let S denote the sign representation, whose modular character is ϕ_2.

Proposition 2.2.2. *The projective indecomposables are V and $V \otimes_k S$.*

PROOF. First, we will show that $V \otimes_k S$ is a projective indecomposable if V is; then, we will prove that V is a projective indecomposable.

Claim. The functor $-\otimes_k S$ defines an equivalence of categories from the category of $k[S_3]$-modules to itself.

PROOF. It suffices to prove the following two things.

1. (1) $-\otimes_k S$ is fully faithful, i.e. that for any $k[S_3]$-modules M and N, $-\otimes \mathrm{id}_S : \mathrm{Hom}_{k[S_3]}(M, N) \to \mathrm{Hom}_{k[S_3]}(M \otimes_k S, N \otimes_k S)$ is an isomorphism.
2. (2) For every $k[S_3]$-module N, there's a $k[S_3]$-module M such that $M \otimes_k S \cong N$.

First, (1). There are natural isomorphisms $i_M : M \otimes_k S \otimes_k S \to M$ and $i_N : N \otimes_k S \otimes_k S \to N$, and these induce an isomorphism $j : \mathrm{Hom}_{k[S_3]}(M \otimes_k S \otimes_k S, N \otimes_k S \otimes_k S) \to \mathrm{Hom}_{k[S_3]}(M, N)$. Let $\Phi : \mathrm{Hom}_{k[S_3]}(M \otimes_k S, N \otimes_k S) \to \mathrm{Hom}_{k[S_3]}(M, N)$ be defined by $\Phi(f) = j(f \otimes \mathrm{id}_S)$ and $\Psi : \mathrm{Hom}_{k[S_3]}(M, N) \to \mathrm{Hom}_{k[S_3]}(M \otimes_k S, N \otimes_k S)$ be given by $\Psi(g) = g \otimes \mathrm{id}_S$. Because $f \otimes \mathrm{id}_S \otimes \mathrm{id}_S = f$ for any morphism f of $k[S_3]$-modules, Φ and Ψ are inverses, so this functor is fully faithful.

For (2), let M be a $k[S_3]$-module; then, since $S \otimes_k S$ is the trivial representation, then $(M \otimes_k S) \otimes_k S \cong M$, so $M \otimes_k S$ is the desired object. ⊠

Since $-\otimes_k S$ is an equivalence of categories, then it sends projective modules to projective modules: the data that a $k[S_3]$-module M is a direct summand in a free module F is an inclusion $i : M \hookrightarrow F$ along with a section $s : F \to M$ such that $s \circ i = \mathrm{id}$, and this is preserved by an equivalence of categories. It also means that $-\otimes_k S$ sends indecomposables to indecomposables, the data that a $k[S_3]$-module M has a direct summand N is also an inclusion $N \hookrightarrow M$ with a section $M \to N$, and this data is preserved by an equivalence of categories. Thus, $-\otimes_k S$ sends projective indecomposables to projective indecomposables, so if V is a projective indecomposable, then $V \otimes_k S$ is as well.

Suppose $\pi : N \twoheadrightarrow N'$ and $f' : V \to N'$ are maps of $k[S_3]$-modules. We want to show that for any $k[S_3]$-module X, there is a setwise bijection

$$\mathrm{Hom}_{k[S_3]}(V, X) \xrightarrow{\sim} \{x \in X \mid (1\ 2)x = x\}. \tag{2.2.2}$$

Lemma 2.2.3. *For any $x \in X$ with $(1\ 2)x = x$, there is a unique $\varphi : V \to X$ such that $\varphi(e_3) = x$.*

Proof. We know $\varphi(e_3) = x$, so let $\varphi(e_1) = (1\ 3)x$ and $\varphi(e_2) = (2\ 3)x$. This defines a linear map, and it commutes with the group action because $(1\ 2)$, $(2\ 3)$, and $(1\ 3)$ generate S_3, and φ already commutes with these three permutations. Thus, there exists such a φ.

This φ is unique because e_3 generates V as a $k[S_3]$-module, so given any $v \in V$, $v = a \cdot e_3$ for an $a \in k[S_3]$, and therefore $\varphi(v) = a \cdot x$. ⊠

Moreover, given a map $\varphi : V \to X$ of $k[S_3]$-modules, $x = \varphi(e_3)$ must be fixed by $(1\ 2)$, since e_3 is, and therefore φ is the unique morphism such that $\varphi(e_3) = x$. Thus, we have established the bijection in (2.2.2), so specifying a map $f : V \to N$ is equivalent to finding an $x \in N$ fixed by $(1\ 2)$. To show $\pi \circ f = f'$, it suffices that $\pi(x) = f'(e_3)$; then, for any other $v \in V$, $v = \sum_{g \in S_3} \lambda_g g \cdot e_3$, so since f is S_3-equivariant, then

$$\pi(f(v)) = \sum_{g \in S_3} \lambda_g g \pi(f(e_3)) = \sum_{g \in S_3} \lambda_g g f'(e_3) = f'(v).$$

Thus, to show that V is projective, it suffices to find an $x \in \pi^{-1}(f(e_3))$ that is fixed by $(1\ 2)$.

Choose any $y \in \pi^{-1}(f(e_3))$ and let $x = (y + (1\ 2)y)/2$, which we can do because we're in characteristic 3. Then, $(1\ 2)x = ((1\ 2)y + y)/2 = x$, and

$$\pi(x) = \frac{\pi(y) + (1\ 2)\pi(y)}{2} = \frac{f(e_3) + (1\ 2)f(e_3)}{2} = \frac{f(e_3) + f(e_3)}{2} = f(e_3),$$

since f' is S_3-equivariant, so $x \in \pi^{-1}(f(e_3))$. Therefore f' lifts, and V is projective.

Finally, we must show that V is indecomposable. We will prove this by finding all of the invariant subspaces, and demonstrating that none of them are direct summands, except 0 and V itself. Since S_3 acts on V by permutation, we only have to consider tuples up to permutations and scalar multiplication, and since this representation is realizable over $\mathbb{F}_3$, then we have the following cases.

- The subspace generated by $(0,0,0)$ is the trivial subspace.
- If W is an S_3-stable subspace containing $(0,0,1)$, then it also contains $(0,1,0)$ and $(1,0,0)$, and therefore is all of V itself.
- If W is an S_3-stable subspace containing $(0,1,1)$, then it also contains $(1,0,1)$ and $(1,1,0)$, so it contains $(-1,1,1)$ and $(1,-1,1)$. Adding these together, W contains $(0,0,1)$, and therefore by the previous case $W = V$.
- If W contains $(1,1,-1)$, then it also contains $(1,0,0)$, and therefore $W = V$ by a previous case.
- The space generated by $(1,1,1)$ is an invariant, one-dimensional subspace containing all tuples of the form (a,a,a).
- The space generated by $(1,-1,0)$ is an invariant, two-dimensional subspace containing all tuples whose sum is zero, since this is unchanged by permutation. In particular, this space contains $(1,1,1)$.

Thus, there are exactly two invariant subspaces other than $\{0\}$ and V itself: $W_1 = \langle(1,1,1)\rangle$ and $W_2 = \langle(1,-1,0)\rangle$, and the latter contains the former. If W_1 is a direct summand, then by the recognition theorem for direct sums, there would have to be another nontrivial $k[S_3]$-submodule of V whose intersection with W_1 is $\{0\}$, but there isn't one, so W_1 isn't a direct summand. Similarly, there is no nontrivial $k[S_3]$-submodule of V whose intersection with W_2 is $\{0\}$, and therefore W_2 cannot be a direct summand either.

Thus, V doesn't have any direct summands other than $\{0\}$ and itself, and therefore is indecomposable. ⊠

2.3. The Modular Representation Theory of S_4

S_4, the symmetric group on four elements, has 24 elements, so its modular representation theory breaks down into the cases $p = 2$ and $p = 3$.

2.3.1. Character Table in Characteristic Zero. As conjugacy type is equivalent to cycle type in symmetric groups, there are five conjugacy classes, 1, $(a\ b)$, $(a\ b)(c\ d)$, $(a\ b\ c)$, and $(a\ b\ c\ d)$. The character table for S_4 is given in Table 6.

	1	$(a\ b)$	$(a\ b)(c\ d)$	$(a\ b\ c)$	$(a\ b\ c\ d)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_4	3	1	-1	0	-1
χ_5	3	-1	-1	0	1

TABLE 6. Character table for S_4 in characteristic zero, as proven in [4, §18.1].

Here, χ_1 is the character for the trivial representation and χ_2 that for the sign representation. χ_4 comes from the representation ρ_4 where S_4 acts on four-tuples summing to zero: $\sigma \cdot (a_1, a_2, a_3, a_4) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, a_{\sigma(4)})$. The set of these tuples is a three-dimensional vector space, so ρ_4 is a three-dimensional representation, and its character is χ_4. Then, χ_5 arises from tensoring ρ_4 with the sign representation; thus, in any characteristic, χ_3 is irreducible iff χ_4 is.

2.3.2. The Case $p = 2$. The 2-regular conjugacy classes are 1 and $(a\ b\ c)$, so by Proposition 1.3.6, there will be two irreducible modular characters.

The trivial representation and the sign representation coincide on the 2-regular classes, providing a one-dimensional irreducible character ϕ_1. Thus, we need only one more representation. There can't be any more one-dimensional ones, because a one-dimensional representation must factor through the abelianization of S_4, which is $\mathbb{Z}/2$. However, by Lemma 1.6.5, the only such representation is the trivial representation, so in particular, any one-dimensional representation of S_4 in characteristic 2 must be trivial.

Suppose that χ_3 doesn't reduce to an irreducible representation in characteristic 2, so that it splits on the 2-regular elements. Since it's two-dimensional, then it must split as the sum of two one-dimensional characters, i.e. twice the trivial character ϕ_1. But then, $\chi_3((1\ 2\ 3)) = -1$ would have to be twice that of $\phi_1((1\ 2\ 3)) = 1$, so it's not $2\phi_1$. Thus, χ_3 reduces to an irreducible ϕ_2.

These are the two irreducible representations in characteristic 2; the character table is presented in Table 7.

	1	$(a\ b\ c)$
ϕ_1	1	1
ϕ_2	2	-1

TABLE 7. Character table for S_4 in characteristic 2.

Now, it's possible to fill in the CDE triangle. The remaining irreducibles from characteristic 0 must decompose as sums of ϕ_1 and ϕ_2 on the 2-regular elements; looking at the character table, one sees that $\chi_1, \chi_2 \mapsto \phi_1$ and $\chi_3 \mapsto \phi_2$, as established, and that $\chi_4, \chi_5 \mapsto \phi_1 + \phi_2$. Thus, the decomposition matrix is

$$D = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 4 & 2 \\ 2 & 3 \end{bmatrix}.$$

Associated to ϕ_1 and ϕ_2 are the characters Φ_1 and Φ_2 of the projective indecomposable $k[S_4]$-modules, which are given by D^{T}:

$$\Phi_1 = \chi_1 + \chi_2 + \chi_4 + \chi_5$$
$$\Phi_2 = \chi_3 + \chi_4 + \chi_5.$$

And after decomposing the χ_i, the characters for the projective indecomposables are expressed in terms of ϕ_1 and ϕ_2 by the matrix C, as

$$\Phi_1 = 4\phi_1 + 2\phi_2$$
$$\Phi_2 = 2\phi_1 + 3\phi_2.$$

2.3.3. The Case $p = 3$**.** The 3-regular conjugacy classes are 1, $(a\ b)$, $(a\ b)(c\ d)$, and $(a\ b\ c\ d)$.

Thus, the trivial and sign representations are distinct in this characteristic (e.g. since they differ on $(a\ b)$), so they are two of the irreducible modular characters: $\chi_1 \mapsto \phi_1$ and $\chi_2 \mapsto \phi_2$; they are irreducible because they are one-dimensional.

Just as with characteristic 2, there can be no more irreducible one-dimensional representations of S_4 in characteristic 3, because they would have to factor through the abelianization $\mathbb{Z}/2$. Once again, a one-dimensional representation of $\mathbb{Z}/2$ is a choice of an element squaring to 1, but in characteristic 3, there are two: 1, corresponding to the trivial representation, and -1, corresponding to the sign representation. But both of these have already been accounted for in S_4, so there can be no others.

On the 3-regular elements, $\chi_3 = \phi_1 + \phi_2$, so χ_3 is reducible.

Since χ_5 is obtained from χ_4 by tensoring with the sign representation, then as stated above one is irreducible iff the other is. Since there are four 3-regular conjugacy classes, then there will be four modular characters, and two have already been accounted for. Thus, if χ_4 and χ_5 reduce to irreducible representations, then we will be done.

We know that $\dim(\rho_4) = \chi_4(1) = 3$. Since $|S_4| = 24$, then $3 \mid 24$, but $3^2 \nmid 24$, and $3 \mid \dim(\rho_4)$. Thus, by Theorem 1.3.7, ρ_4 reduces to an irreducible representation in characteristic 3, and so $\chi_4 \mapsto \phi_3$, the next irreducible modular character. Then, the same argument works for χ_5, so its character on the 3-regular elements is also an irreducible modular character, and will be denoted ϕ_4.

Thus, we have the four irreducible characters in characteristic 3. Table 8 shows the character table.

	1	$(a\ b)$	$(a\ b)(c\ d)$	$(a\ b\ c\ d)$
ϕ_1	1	1	1	1
ϕ_2	1	-1	1	-1
ϕ_3	3	1	-1	-1
ϕ_4	3	-1	-1	1

TABLE 8. Character table for S_4 in characteristic 3.

With the character table in place, the next step is to describe the morphisms in the CDE triangle. To calculate the decomposition matrix, $\chi_1 \mapsto \phi_1$ and $\chi_2 \mapsto \phi_2$ as noted above; then, $\chi_3 \mapsto \phi_1 + \phi_2$, and $\chi_4 \mapsto \phi_3$ and $\chi_5 \mapsto \phi_4$. Thus,

$$D = \begin{bmatrix} 1 & 0 & 1 & & \\ 0 & 1 & 1 & & \\ & & & 1 & 0 \\ & & & 0 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$ as usual, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 2 & 1 & & \\ 1 & 2 & & \\ & & 1 & 0 \\ & & 0 & 1 \end{bmatrix}.$$

Associated to ϕ_1, ϕ_2, ϕ_3, and ϕ_4 are the characters $\Phi_1, \dots, \Phi_4$ of the projective indecomposable $k[S_4]$-modules. Their description in terms of the χ_i is given by D^{T}.

$$\Phi_1 = \chi_1 + \chi_3$$
$$\Phi_2 = \chi_2 + \chi_3$$
$$\Phi_3 = \chi_4$$
$$\Phi_4 = \chi_5,$$

and in terms of the ϕ_i is given by C.

$$\Phi_1 = 2\phi_1 + \phi_2$$
$$\Phi_2 = \phi_1 + 2\phi_2$$
$$\Phi_3 = \phi_3$$
$$\Phi_4 = \phi_4.$$

2.4. The Modular Representation Theory of A_4

A_4, the alternating group on 4 elements, has 12 elements, so its modular representation theory breaks down into two cases, $p = 2$ and $p = 3$.

Character Table in Characteristic Zero. In alternating groups, cycle type does not determine conjugacy class; there are four conjugacy classes, given by 1, $(a\ b)(c\ d)$, and two conjugacy classes of 3-cycles:

$$c_3 = \{(1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\}$$
$$c_4 = \{(1\ 3\ 2), (4\ 1\ 2), (2\ 3\ 4), (3\ 1\ 4)\}.$$

The character table is presented in Table 9.

	1	$(a\ b)(c\ d)$	c_3	c_4
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	0

TABLE 9. Character table for A_4 in characteristic zero. Here, ω is a primitive cube root of unity.

These representations can all be explicitly constructed. Since the abelianization of A_4 is $\mathbb{Z}/3$, then the three one-dimensional representations χ_1, χ_2, and χ_3 of A_4 are the ones corresponding to the three one-dimensional representations of $\mathbb{Z}/3$. Specifically, a one-dimensional representation of $\mathbb{Z}/3$ is a choice of an element whose cube is 1, and there are three of these, corresponding to the three cube roots of unity in K. χ_1 is the trivial representation, and then the two others send $1 \in \mathbb{Z}/3$ to an element of order 3 in $K^\times$, i.e. a cube root of unity. Then, the remaining, three-dimensional representation χ_4 is the restriction of χ_4 for S_4 in Table 6: the action of S_4 on 4-tuples adding to zero is also an action of A_4 on the same space, and is irreducible by the orthogonality relations.

The case $p = 2$. The 2-regular conjugacy classes of A_4 are 1, c_3, and c_4, so there will be 3 modular characters by Corollary 1.3.6. This ends up being relatively easy: all three one-dimensional representations are still distinct on the 2-regular conjugacy classes of A_4, and they must be irreducible, so these are all of them. That's all, folks! See Table 10 for the character table.

	1	c_3	c_4
ϕ_1	1	1	1
ϕ_2	1	ω	ω^2
ϕ_3	1	ω^2	ω

TABLE 10. Character table for A_4 in characteristic 2. Once again, ω is a primitive cube root of unity.

Notationally, we'll let ϕ_i be the reduction of χ_i. Then, χ_4 decomposes as $\phi_1 + \phi_2 + \phi_3$ in this characteristic, because $1 + \omega + \omega^2 = 0$.

Thus, the decomposition matrix is

$$D = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

Thus, the characters of the projective indecomposable $k[A_4]$-modules are given by

$$\Phi_1 = \chi_1 + \chi_4$$
$$\Phi_2 = \chi_2 + \chi_4$$
$$\Phi_3 = \chi_3 + \chi_4,$$

and in terms of the ϕ_i,

$$\Phi_1 = 2\phi_1 + \phi_2 + \phi_3$$
$$\Phi_2 = \phi_1 + 2\phi_2 + \phi_3$$
$$\Phi_3 = \phi_1 + \phi_2 + 2\phi_3.$$

The case $p = 3$. The 3-regular conjugacy classes are 1 and $(a\ b)(c\ d)$. Thus, we should expect two irreducible representations in this characteristic.

However, all three one-dimensional representations coincide on these conjugacy classes; they're all trivial. Thus, $\chi_1, \chi_2, \chi_3 \mapsto \phi_1$, where ϕ_1 denotes the modular character of the trivial representation.

There will be one more representation, but it cannot be one-dimensional: any one-dimensional representation must factor through the abelianization of A_4, which is $\mathbb{Z}/3$. But by Lemma 1.6.5, the only one-dimensional representation of $\mathbb{Z}/3$ in characteristic 3 is trivial. Since this was already accounted for, so $\mathbb{Z}/3$ has no more irreducible representations in this characteristic, and therefore A_4 has no more one-dimensional representations in characteristic 3.

The Brauer-Nesbitt theorem, Theorem 1.3.7, directly proves that χ_4 reduces to an irreducible representation: $|A_4| = 12$, so 3 divides $|A_4|$, but 9 doesn't. Then, $3 \mid \dim(\rho_4) = 3$, so the theorem is satisfied, and $\chi_4 \mapsto \phi_2$, an irreducible modular character. Thus, we've found all of the irreducible modular characters; the character table is given in Table 11.

	1	$(a\ b)(c\ d)$
ϕ_1	1	1
ϕ_2	2	-1

TABLE 11. Character table for A_4 in characteristic 3.

Thus, we've found both irreducibles, so the decomposition matrix is

$$D = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, the characters of the projective indecomposables are

$$\Phi_1 = \chi_1 + \chi_2 + \chi_3$$
$$\Phi_2 = \chi_4,$$

or in terms of ϕ_1 and ϕ_2,

$$\Phi_1 = 3\phi_1$$
$$\Phi_2 = \phi_2.$$

2.5. The Modular Representation Theory of S_5

S_5, the symmetric group on 5 elements, has 60 elements, so its modular representation theory breaks down into the cases $p = 2$, $p = 3$, and $p = 5$.

2.5.1. Character Table in Characteristic Zero. Since conjugacy type is equivalent to cycle type in symmetric groups, there are seven conjugacy classes: 1, $(a\ b)$, $(a\ b\ c)$, $(a\ b\ c\ d)$, $(a\ b\ c\ d\ e)$, $(a\ b)(c\ d)$, and $(a\ b)(c\ d\ e)$. Its character table is given in Table 12.

	1	$(a\ b)$	$(a\ b\ c)$	$(a\ b\ c\ d)$	$(a\ b\ c\ d\ e)$	$(a\ b)(c\ d)$	$(a\ b)(c\ d\ e)$
χ_1	1	1	1	1	1	1	1
χ_2	1	−1	1	−1	1	1	−1
χ_3	4	2	1	0	−1	0	−1
χ_4	4	−2	1	0	−1	0	1
χ_5	5	1	−1	−1	0	1	1
χ_6	5	−1	−1	1	0	1	−1
χ_7	6	0	0	0	1	−2	0

TABLE 12. Character table for S_5 in characteristic 0, as proven in [4, Ch. 19].

Here, χ_1 is the character of the trivial representation and χ_2 is that of the sign representation. χ_3 comes from the representation ρ_3 where S_5 acts on five-tuples summing to zero via the permutation representation

$$\sigma \cdot (a_1, a_2, a_3, a_4, a_5) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, a_{\sigma(4)}, a_{\sigma(5)}).$$

Since the space of 5-tuples summing to zero is four-dimensional, this is a four-dimensional representation, and its character is χ_3. Then, χ_4 is the character of the representation obtained by tensoring ρ_3 with the sign representation. In particular, χ_4 is irreducible in a given characteristic iff χ_3 is (though, as discussed below, it's equal to χ_3 on the 2-regular elements); a similar relationship holds for χ_5 and χ_6.

2.5.2. The Case $p = 2$. The 2-regular conjugacy classes are those with odd order, i.e. 1, $(a\ b\ c)$, and $(a\ b\ c\ d\ e)$. Thus, by Corollary 1.3.6, there should be three irreducible modular characters.

In characteristic 2, the trivial representation and sign representation coincide, to provide an irreducible representation ϕ_1 of dimension 1. Furthermore, by Theorem 1.3.7, since $|S_5| = 60$, 4 divides $|S_5|$ but $8 \nmid |S_5|$, and therefore χ_3 and χ_4 reduce to irreducible representations in characteristic 2, because they are four-dimensional. However, they coincide on the 2-regular elements of S_5, so we get only one more irreducible character, which we'll call ϕ_2.

Since the five-dimensional representations χ_5 and χ_6 came from tensoring with the sign representation, they're also identical in characteristic 2. And on the 2-regular conjugacy classes, $\chi_7 = \chi_5 + \chi_1$, so χ_7 isn't irreducible. Thus, the last irreducible character in characteristic 2 comes either from χ_5 or a component of it.

Proposition 2.5.1. *The five-dimensional representations of S_5 are reducible in characteristic* 2.

This is proven in [3, Ch. 6]. This proposition, along with character computations, allows us to determine the remaining modular character.

Proposition 2.5.2. *On the* 2*-regular elements, $\chi_5 = \phi_1 + \phi_3$, where ϕ_3 is the modular character of an irreducible four-dimensional representation in characteristic* 2.

PROOF. Since ρ_5 is reducible, its character is a sum of at least two irreducible characters. However, since there are three 5-regular conjugacy classes and we've already found two irreducible characters, then there is exactly one more.

Since 5 is prime, then χ_5 cannot split as $n \cdot \phi$ for any ϕ, so one of the characters in its decomposition has to be one of ϕ_1 or ϕ_2 that we've already seen. However, on the 2-regular elements, $\chi_5 - \phi_2$ is a one-dimensional class function distinct from ϕ_1, but every one-dimensional representation of S_5 in characteristic 2 factors through the abelianization $\mathbb{Z}/2$, and by Lemma 1.6.5, ϕ_1 is the only such character, so $\chi_5 - \phi_2$ can't be the character of a simple $k[S_5]$-module.

Thus, the only remaining option is $\chi_5 - \phi_1$, which therefore produces the character ϕ_* of a four-dimensional representation:

	1	$(a\ b\ c)$	$(a\ b\ c\ d\ e)$
	5	−1	0
−	1	1	1
	4	0	−1

This ϕ_* will be our desired character, but we must show that it's irreducible. Since there's exactly one more irreducible character, we know that if ϕ_* is reducible, then either $\phi_* = 2\phi_{**}$, where ϕ_{**} is two-dimensional, or $\phi_* = \phi_1 + \phi_{**}$, where ϕ_{**} is three-dimensional.

In the first case, where ϕ_{**} appears twice in the expression for ϕ_*, its value on $(a\ b\ c\ d\ e)$ is half that of ϕ_*, so $\phi_{**}((a\ b\ c\ d\ e)) = -1/2$. However, since this is a two-dimensional modular character, this means that $-1/2$ is a sum of two m^{th} roots of unity, where m is the least common multiple of the orders of the 2-regular elements of S_5. Thus, $m = 15$, so we want a way to write $1/2$ as a sum of two 15^{th} roots of unity α and β. We can accomplish this in $\overline{\mathbb{Q}}_p$ if and only if we can do this in $\mathbb{C}$, but in $\mathbb{C}$, writing $1/2$ as such a sum means they must both be complex (since 1 is the only real 15^{th} root of unity), and α and β must be conjugates. However, this means $\operatorname{Re}(\alpha) = -1/4$, but there's no 15^{th} root of unity satisfying this, so this ϕ_{**} isn't a modular character, and therefore ϕ_* cannot split in this way.

The other option is that $\phi_* = \phi_1 + \phi_{**}$, with the latter three-dimensional. In this case, $\phi_{**}((a\ b\ c\ d\ e)) = -2$, so we must write -2 as a sum of three 15^{th} roots of unity. We can again do this in $\overline{\mathbb{Q}}_p$ iff it's possible in $\mathbb{C}$, but it's also impossible in $\mathbb{C}$. Either all three of the roots are real (in which case the only choice is 1, and $1+1+1$ certainly isn't equal to -2), or two are complex and one is real, so the latter must be equal to 1. But there are no two 15^{th} roots of unity that sum to -3, so this choice of ϕ_{**} isn't a modular character either.

Thus, ϕ_* is irreducible. ⊠

Let ϕ_3 denote the ϕ_* constructed in the above proof. Since we know all of the irreducible characters, we can write down the character table, and do so in Table 13.

	1	$(a\ b\ c)$	$(a\ b\ c\ d\ e)$
ϕ_1	1	1	1
ϕ_2	4	1	-1
ϕ_3	4	0	-1

TABLE 13. Character table for S_5 in characteristic 2.

Then, we can calculate the maps in the CDE triangle. The decomposition matrix is

$$D = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 8 & 0 & 4 \\ 0 & 2 & 0 \\ 4 & 0 & 3 \end{bmatrix}.$$

Thus, the characters of the projective indecomposable modules are

$$\begin{aligned} \Phi_1 &= \chi_1 + \chi_2 + \chi_5 + \chi_6 + 2\chi_7 \\ \Phi_2 &= \chi_3 + \chi_4 \\ \Phi_3 &= \chi_5 + \chi_6 + \chi_7, \end{aligned}$$

or in terms of the ϕ_i,

$$\begin{aligned} \Phi_1 &= 8\phi_1 + 4\phi_3 \\ \Phi_2 &= 2\phi_2 \\ \Phi_3 &= 4\phi_1 + 3\phi_3. \end{aligned}$$

2.5.3. The Case $p = 3$. In characteristic 3, the trivial representation and the sign representation differ, so χ_1 and χ_2 correspond to distinct irreducible modular representations ϕ_1 and ϕ_2, respectively.

The 3-regular conjugacy classes are 1, $(a\ b)$, $(a\ b\ c\ d)$, $(a\ b\ c\ d\ e)$, and $(a\ b)(c\ d)$, since $(a\ b\ c)$ and $(a\ b)(c\ d\ e)$ have orders divisible by 3.

Since $3 \mid 60$ but $9 \nmid 60$, then by Theorem 1.3.7, whenever $3 \mid \dim(\rho_i)$, where ρ_i is irreducible in characteristic 0, the reduction of ρ_i mod 3 is still irreducible. Thus, χ_7 reduces to an irreducible modular character, as it is six-dimensional.

Since there are five 3-regular conjugacy classes and we've uncovered three irreducible representations, there must be two more.

Claim. χ_3 (and therefore also χ_4) reduces to an irreducible representation in characteristic 3.

Proof. We will prove this by starting with a single vector, and acting on it by group elements in order to generate the entire space.

First, though, recall how χ_3 is defined: since we're not in characteristic 5, it's a permutation action on 5-tuples adding to zero: $\sigma\cdot(a_1,\dots,a_5)=(a_{\sigma(1)},\dots,a_{\sigma(5)})$. This representation is realizable over $\mathbb{F}_3$, so we may take $k=\mathbb{F}_3$ for this proof.

The space of 5-tuples summing to zero is four-dimensional, so take the following basis:

$$e_1=\begin{bmatrix}1\\-1\\0\\0\\0\end{bmatrix},\qquad e_2=\begin{bmatrix}0\\1\\-1\\0\\0\end{bmatrix},\qquad e_3=\begin{bmatrix}0\\0\\1\\-1\\0\end{bmatrix},\qquad\text{and}\qquad e_4=\begin{bmatrix}0\\0\\0\\1\\-1\end{bmatrix}.$$

Thus, $1\in S_5$ acts as the identity; (1 2) sends $e_1\mapsto -e_2$, $e_2\mapsto e_1+e_2$, and fixes e_3 and e_4; (1 2 3) sends $e_1\mapsto e_2$, $e_2\mapsto -e_1-e_2$, $e_3\mapsto e_1+e_2+e_3$, $e_4\mapsto e_4$; and so on.

Since S_5 acts on these tuples by permutation, we only need to consider types of tuples up to reordering, and since we're looking at a k-vector space, scalar multiples come for free; then, given any tuple of a given type, the action of S_5 generates all of the others of that type. In particular, one can ignore sign. Thus, ignoring $(0,0,0,0,0)$, there are four types:

$$e_1=\begin{bmatrix}1\\-1\\0\\0\\0\end{bmatrix},\qquad e_1-e_2+e_3=\begin{bmatrix}1\\1\\-1\\-1\\0\end{bmatrix},\qquad e_1-e_2=\begin{bmatrix}1\\1\\1\\0\\0\end{bmatrix},\qquad\text{and}\qquad e_1-e_2+e_4=\begin{bmatrix}1\\1\\1\\1\\-1\end{bmatrix}.$$

Each of these sums to 0 mod 3, and these must be the only four types, because once you specify the number of 1s, only these types appear: e.g., if there's exactly one 1, it's either $(1,-1,0,0,0)$ or $(1,-1,-1,-1,-1)$, both of which are the same types as above; if there are two, we get the second type; if there are three, we get the third type; and if there are four, the last type is forced.

So we know that if we have any invariant subspace and it contains a given tuple, it must contain all tuples of that type. Thus, the next step is to show that, given any type, we can obtain all of the others; we'll go between the first and the second, between the second and the third, and then between the third and the fourth, so that given a tuple of any type (and therefore all tuples of that type), it's possible to generate all of the others.

Let's start with the first type, e_1. Then, $(1\ 3)(2\ 4)\cdot e_1$ is $(0,0,1,-1,0)$, so $e_1+(1\ 3)(2\ 4)\cdot e_1=(1,-1,1,-1,0)$, so we've gotten the second type. In the other direction, $v_1=(1,1,-1,-1,0)$ and $v_2=(1,-1,1,-1,0)$ are both of the second type, and $v_1+v_2=(-1,0,0,1,0)$ is first type. Thus, if an invariant subspace contains a tuple of either first or second type, it contains all vectors of both types.

If $v_1=(1,1,-1,-1,0)$ and $v_2=(0,-1,-1,1,1)$, so they're both second type, then $v_1+v_2=(1,0,1,0,1)$, which is third type; then, if $w_1=(1,1,1,0,0)$ and $w_2=(1,1,0,1,0)$, then they're both third type, but $w_1+w_2=(-1,-1,1,1,0)$, which is second type. Thus, one can go between the second and third types.

Let $v_1=(1,1,1,0,0)$ and $v_2=(0,0,1,1,1)$, which are both of third type, and $v_1+v_2=(1,1,-1,1,1)$, which is fourth type. Then, if $w_1=(1,1,1,1,-1)$ and $w_2=(1,1,1,-1,1)$, which are both fourth type, then $w_1+w_2=(-1,-1,-1,0,0)$, which is third type. Thus, it's possible to go between the third and fourth types.

Thus, given any tuple, it is possible to generate all tuples of its type, and then to generate the entire space, so any invariant subspace of this representation is equal to the whole space, so it is irreducible. ⊠

Since χ_3 reduces to an irreducible representation, there's a corresponding modular character ϕ_3, and as noted above, χ_4 is irreducible iff χ_3 is, so it gives us another modular character ϕ_4. Thus, we've found all five irreducible characters (since χ_7 is also irreducible, so we've found ϕ_5). This is all the information we need to make the character table, which appears in Table 14.

	1	$(a\ b)$	$(a\ b\ c\ d)$	$(a\ b\ c\ d\ e)$	$(a\ b)(c\ d)$
ϕ_1	1	1	1	1	1
ϕ_2	1	−1	−1	1	1
ϕ_3	4	2	0	−1	0
ϕ_4	4	−2	0	−1	0
ϕ_5	6	0	0	1	−2

TABLE 14. Character table for S_5 in characteristic 3.

Next, the morphisms of the CDE triangle: the decomposition matrix is

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 2 & 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Thus, the characters of the projective indecomposables are

$$\begin{aligned} \Phi_1 &= \chi_1 + \chi_6 \\ \Phi_2 &= \chi_2 + \chi_5 \\ \Phi_3 &= \chi_3 + \chi_5 \\ \Phi_4 &= \chi_4 + \chi_6 \\ \Phi_5 &= \chi_7, \end{aligned}$$

or in terms of the ϕ_i,

$$\begin{aligned} \Phi_1 &= 2\phi_1 + \phi_4 \\ \Phi_2 &= 2\phi_2 + \phi_3 \\ \Phi_3 &= \phi_2 + 2\phi_3 \\ \Phi_4 &= \phi_1 + 2\phi_4 \\ \Phi_5 &= \phi_5. \end{aligned}$$

2.5.4. The Case $p = 5$. The only conjugacy class with order dividing 5 is $(a\ b\ c\ d\ e)$, so the 5-regular conjugacy classes are 1, $(a\ b)$, $(a\ b\ c)$, $(a\ b\ c\ d)$, $(a\ b)(c\ d)$, and $(a\ b)(c\ d\ e)$. There are six conjugacy classes, and therefore six irreducible representations.

Since χ_1 and χ_2 are distinct on the 5-regular classes of S_5, they correspond to distinct irreducibles in characteristic 5, respectively ϕ_1 and ϕ_2.

Since 5 divides $|S_5| = 60$ but 25 doesn't, Theorem 1.3.7 implies that any five-dimensional irreducible representations remain irreducible in characteristic 5; thus, χ_5 and χ_6 remain irreducible.

Claim. χ_3 (and therefore χ_4) are *not* irreducible in characteristic 5.

PROOF. Suppose that they were; then, since there are six 5-regular classes, these would be all of the modular characters in this characteristic. In particular, that means it would be possible to describe the remaining characteristic 0 character, χ_7, in terms of the others on the 5-regular classes.

$(1\ 2)(3\ 4)$ is 5-regular, and for $i = 1, \ldots, 6$, $\chi_i((1\ 2)(3\ 4)) \geq 0$. However, $\chi_7((1\ 2)(3\ 4)) = -2$, so no positive combination of $\chi_1, \ldots, \chi_6$ can create χ_7 on the 5-regular classes, so this is a contradiction. ⊠

The reason the proof given in characteristic 3 doesn't work is that, since we can't divide by 5, this representation isn't on 5-tuples summing to 0; instead, it's the quotient of the permutation representation V' of S_5 by the invariant subspace $W = \{(a,a,a,a,a) \mid a \in k\}$.

In order to classify the representations, we'll need to find an invariant subspace.

Claim. If $V \subseteq V'/W$ denotes the subspace of tuples that sum to 0, V is an irreducible, S_5-stable subspace.

Note that the sum of the entries of a tuple is well-defined, even in the quotient, because all elements of W sum to zero.

Proof. If $v_1, v_2 \in V$, the sum of the entries in $v_1 + v_2$ is the sum of all 10 entries of both v_1 and v_2, i.e. $0 + 0 = 0$, and taking the sum of the entries commutes with scalar multiplication, so the scalar multiple of a $v \in V$ still sums to zero. Thus, V is a subspace. It's S_5-stable because permuting the entries of a tuple doesn't change the sum. Thus, V is invariant.

To show that it's irreducible, we'll once again sort the elements of V into types, and then show that it's possible to go from any type to any other type.

First, it's possible to realize each element of V as a 4-tuple whose entries sum to zero in a unique way, by subtracting off $(1,1,1,1,1)$ times the fifth entry, and then taking only the first four entries; for example $(0,1,2,3,4)$ is represented by $(1,2,3,4,0)$. Thus, since the last entry is zero, the sum of the first four entries is unchanged, so V is realized as those 4-tuples summing to zero.

This space is three-dimensional, with $e_1 = (1,-1,0,0)$, $e_2 = (0,1,-1,0)$, and $e_3 = (0,0,1,-1)$ forming a basis (since any $(a,b,c,-a-b-c)$ can be written as $ae_1 + (a+b)e_2 + (a+b+c)e_3$, and they're linearly independent).

Once again, we'll consider the types of 4-tuples, i.e. equivalence classes under permutation of elements (by S_4) and scalar multiplication. In particular, any nonzero tuple has a nonzero element somewhere, and without loss of generality it can be permuted into the first index, and then by scalar multiplication of the whole tuple, the first element can be made to be a 1.

We end up with the following five types of tuples.

$$\begin{aligned}\tau_1 &= (1,4,0,0)\\ \tau_2 &= (1,1,3,0)\\ \tau_3 &= (1,1,1,2)\\ \tau_4 &= (1,4,1,4)\\ \tau_5 &= (1,4,2,3).\end{aligned}$$

From any type we can get to any other type:

- Since $2\tau_1 = (2,3,0,0)$, then we can go from the first type to the second: $(1,4,0,0) + (0,2,3,0) = (1,1,3,0)$.
- Going from type 2 to type 3: $(1,1,3,0) + (1,0,3,1) = (2,1,1,1)$.
- Going from type 3 to type 4: $(1,1,1,2) + (1,1,2,1) = (2,2,3,3)$; scalar multiplication by 3 turns this into $(1,1,4,4)$.
- Going from type 4 to type 1: $(1,4,1,4) + (1,4,4,1) = (2,3,0,0) = 2\tau_1$.

Thus, everything can be generated from everything else save the last type, which we can also account for.

- Going from type 1 to type 5: $(1,4,0,0) + (0,0,2,3) = (1,4,2,3)$.
- Going from type 5 to type 2: $(1,4,2,3) + (1,2,3,4) = (2,1,0,2)$, which is a scalar multiple of $(1,3,0,1)$.

Thus, every type can generate every other type, so every element of V can generate the entire space from the action of $k[S_5]$. Thus, V must be irreducible. ⊠

When we quotient the original representation (that is, the one reduced from χ_3) by V, the result is therefore a one-dimensional representation; we can figure out which by calculating the character of V. Use the basis e_1, e_2, e_3 from above.

- 1 acts as the identity matrix, and, since this is a three-dimensional representation, has trace 3.
- (1 2) sends $e_1 \mapsto -e_1$, $e_2 \mapsto e_1 + e_2$, and $e_3 \mapsto e_3$. Thus, it has trace 1.
- (1 2 3) sends $e_1 \mapsto e_2$, $e_2 \mapsto -e_1 - e_2$, and $e_3 \mapsto e_1 + e_2 + e_3$. This means its trace is 0.
- (1 2 3 4) sends $e_1 \mapsto e_2$ and $e_2 \mapsto e_3$, but $e_3 \mapsto -e_1 - e_2 - e_3$. Its trace is -1.
- (1 2)(3 4) sends $e_1 \mapsto -e_1$ and $e_3 \mapsto -e_3$, but $e_2 \mapsto e_1 + e_2 + e_3$; thus, its trace is also -1.

- (1 2)(3 4 5) sends $e_1 \mapsto -e_1$ and $e_2 \mapsto e_1 + e_2 + e_3$. However, e_3 is sent to $(0,0,0,1,-1)$, which means we have to fiddle with it to get back to its 4-tuple representation; this is equivalent to $(1,1,1,2,0)$, which is $e_1 + 2e_2 - 2e_3$, so the trace of (1 2)(3 4 5) is -2.

Thus, on the 5-regular elements, $\chi_3 - \chi_V$ must be one of the one-dimensional representations we've already identified. In fact,

	1	$(a\ b)$	$(a\ b\ c)$	$(a\ b\ c\ d)$	$(a\ b)(c\ d)$	$(a\ b)(c\ d\ e)$
	4	2	1	0	0	−1
−	3	1	0	−1	−1	−2
	1	1	1	1	1	1

So then χ_3 decomposes as $\chi_V + \phi_1$ on the 5-regular elements, and since V is irreducible, call its character ϕ_3. Note that ϕ_3 is not invariant under tensoring with the sign representation, so the resulting representation is another irreducible representation in characteristic 5: $\phi_4 = \phi_3 \cdot \phi_1$, so $\chi_4 = \phi_2 + \phi_4$ on the 5-regular elements.

Then, we saw already that χ_5 and χ_6 reduce to irreducible representations, which we will call ϕ_5 and ϕ_6, respectively. And now that we've found ϕ_3 and ϕ_4, we can see that $\chi_7 = \phi_3 + \phi_4$ on the 5-regular elements. We now know enough to write down the character table in characteristic 5, and do so in Table 15.

	1	$(a\ b)$	$(a\ b\ c)$	$(a\ b\ c\ d)$	$(a\ b)(c\ d)$	$(a\ b)(c\ d\ e)$
ϕ_1	1	1	1	1	1	1
ϕ_2	1	−1	1	−1	1	−1
ϕ_3	3	1	0	−1	−1	−2
ϕ_4	3	−1	0	−1	−1	−2
ϕ_5	5	1	−1	−1	1	1
ϕ_6	5	−1	−1	1	1	−1

TABLE 15. Character Table of S_5 in characteristic 5.

The decomposition matrix is

$$D = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Thus, the characters of the projective indecomposables are

$$\begin{aligned} \Phi_1 &= \chi_1 + \chi_3 \\ \Phi_2 &= \chi_2 + \chi_4 \\ \Phi_3 &= \chi_3 + \chi_7 \\ \Phi_4 &= \chi_4 + \chi_7 \\ \Phi_5 &= \chi_5 \\ \Phi_6 &= \chi_6, \end{aligned}$$

or in terms of the ϕ_i,

$$\begin{aligned}
\Phi_1 &= 2\phi_1 + \phi_3\\
\Phi_2 &= 2\phi_2 + \phi_4\\
\Phi_3 &= \phi_1 + 2\phi_3 + \phi_4\\
\Phi_4 &= \phi_2 + \phi_3 + 2\phi_4\\
\Phi_5 &= \phi_5\\
\Phi_6 &= \phi_6.
\end{aligned}$$

2.6. The Modular Representation Theory of $\mathrm{GL}_2(\mathbb{F}_3)$

The general linear group of degree 2 with coefficients in $\mathbb{F}_3$, $\mathrm{GL}_2(\mathbb{F}_3)$ (also written $\mathrm{GL}(2,\mathbb{F}_3)$ or $\mathrm{GL}(2,3)$) is the group of invertible 2×2 matrices with coefficients in $\mathbb{F}_3$. It has 48 elements, so its modular representation theory breaks down into two cases, $p=2$ and $p=3$.

2.6.1. Character Table in Characteristic Zero. $\mathrm{GL}_2(\mathbb{F}_3)$ has eight conjugacy classes.

- The identity I, with order 1.
- $-I$, with order 2.
- c_3, those matrices conjugate to $\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}$, which have order 4.
- c_4, those matrices conjugate to $\begin{pmatrix} 0 & 1\\ 1 & -1\end{pmatrix}$, which have order 8.
- c_5, the matrices conjugate to $\begin{pmatrix} 0 & 1\\ 1 & 1\end{pmatrix}$, which have order 8.
- c_6, the matrices conjugate to $\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}$, which have order 3.
- c_7, the matrices conjugate to $\begin{pmatrix} -1 & 1\\ 0 & -1\end{pmatrix}$, which have order 6.
- c_8, the matrices conjugate to $\begin{pmatrix} 1 & 0\\ 0 & -1\end{pmatrix}$, which have order 2.

The character table for $\mathrm{GL}_2(\mathbb{F}_3)$ is given in Table 16. Notice that $\chi_5 = \chi_4\cdot\chi_2$ and $\chi_7 = \chi_6\cdot\chi_2$.

	I	$-I$	c_3	c_4	c_5	c_6	c_7	c_8
χ_1	1	1	1	1	1	1	1	1
χ_2	1	1	1	-1	-1	1	1	-1
χ_3	2	2	2	0	0	-1	-1	0
χ_4	2	-2	0	$i\sqrt{2}$	$-i\sqrt{2}$	-1	1	0
χ_5	2	-2	0	$-i\sqrt{2}$	$i\sqrt{2}$	-1	1	0
χ_6	3	3	-1	-1	-1	0	0	1
χ_7	3	3	-1	1	1	0	0	-1
χ_8	4	-4	0	0	0	1	1	0

Table 16. Character table for $\mathrm{GL}_2(\mathbb{F}_3)$ in characteristic 0, as proven in [**5**, Ch. XVIII, § 12].

The abelianization of $\mathrm{GL}_2(\mathbb{F}_3)$ is $\langle -I\rangle \cong \mathbb{Z}/2$.

2.6.2. The Case $p=2$. The 2-regular classes of $\mathrm{GL}_2(\mathbb{F}_3)$ are I and c_6. Thus, by Corollary 1.3.6, there are exactly two irreducible modular characters in this characteristic.

The reductions of χ_1 and χ_2 coincide on I and c_6 as the trivial character ϕ_1; then, there can be no more one-dimensional representations in this characteristic, because they would factor through the abelianization $\mathbb{Z}/2$, which has no more one-dimensional representations in this characteristic by Lemma 1.6.5.

This means that the reduction of χ_3 (which coincides with the reductions of χ_4 and χ_5) is also irreducible: if it were reducible, it would have to be the sum of two one-dimensional characters, and therefore would equal $2\phi_1$ on I and c_6. However, $\chi_3(c_6) = -1$ and $\phi_1(c_6) = 1$, so this isn't the case, and χ_3 reduces to an irreducible character ϕ_2.

Thus, that's all of the irreducible modular characters. The character table is given in Table 17.

	I	c_1
ϕ_1	1	1
ϕ_2	2	-1

TABLE 17. Character table for $\mathrm{GL}_2(\mathbb{F}_3)$ in characteristic 2.

The decomposition matrix is

$$D = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 8 & 4 \\ 4 & 6 \end{bmatrix}.$$

Thus, the characters of the projective indecomposables are

$$\Phi_1 = \chi_1 + \chi_2 + \chi_6 + \chi_7 + 2\chi_8$$
$$\Phi_2 = \chi_3 + \chi_4 + \chi_5 + \chi_6 + \chi_7 + \chi_8,$$

or in terms of the ϕ_i,

$$\Phi_1 = 8\phi_1 + 4\phi_2$$
$$\Phi_2 = 4\phi_1 + 6\phi_2.$$

2.6.3. The Case $p = 3$. The 3-regular conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_3)$ are I, $-I$, c_3, c_4, c_5, and c_8. Thus, by Corollary 1.3.6, there are exactly six irreducible modular characters in this characteristic.

The reductions of χ_1 and χ_2 are distinct in this characteristic, and since they're one-dimensional, then they're irreducible, so their reductions ϕ_1 and ϕ_2, respectively, are two irreducible modular characters. However, there can be no more one-dimensional representations, since such a representation would have to factor through the abelianization $\mathbb{Z}/2$, and a one-dimensional representation of $\mathbb{Z}/2$ is given by sending $e \mapsto 1$ and $1 \mapsto \alpha$, where $\alpha^2 = 1$. Thus, $\alpha = \pm 1$, but both of these possibilities have already been accounted for, so there are no more one-dimensional representations of $\mathrm{GL}_2(\mathbb{F}_3)$ in this characteristic.

χ_4 is two-dimensional, so if it were reducible, then on the 3-regular elements, it would be a sum of two one-dimensional characters, which are therefore either ϕ_1 or ϕ_2. Since $\phi_1(-I) = \phi_2(-I) = 1$, this would force $\chi_4(-I) = 2$ (since it would have to decompose as $2\phi_1$, $\phi_1 + \phi_2$, or $2\phi_2$), but instead, $\chi_4(-I) = -2$, so this cannot happen. Thus, χ_4 reduces to an irreducible modular character ϕ_3.

Since χ_5 is two-dimensional, distinct from χ_4 on the 3-regular elements, and has $\chi_5(-I) = -2$, then precisely the same argument works for it; thus, its reduction ϕ_4 is irreducible.

Finally, let's use Theorem 1.3.7. Since 3 divides $|\mathrm{GL}_2(\mathbb{F}_3)| = 48$ but 9 doesn't divide the order of the group, then any three-dimensional representation of $\mathrm{GL}_2(\mathbb{F}_3)$ that's irreducible in characteristic zero reduces to an irreducible representation in characteristic 3. In particular, this means the two three-dimensional characters, χ_6 and χ_7, reduce to irreducible modular characters ϕ_5 and ϕ_6, respectively, and so we've found all six irreducibles. The character table is presented in Table 18.

	I	$-I$	c_3	c_4	c_5	c_8
ϕ_1	1	1	1	1	1	1
ϕ_2	1	1	1	-1	-1	-1
ϕ_3	2	-2	0	$i\sqrt{2}$	$-i\sqrt{2}$	0
ϕ_4	2	-2	0	$-i\sqrt{2}$	$i\sqrt{2}$	0
ϕ_5	3	3	-1	-1	-1	1
ϕ_6	3	3	-1	1	1	-1

TABLE 18. Character table for $\mathrm{GL}_2(\mathbb{F}_3)$ in characteristic 3.

The decomposition matrix is

$$D = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Thus, the characters of the projective indecomposables are

$$\begin{aligned} \Phi_1 &= \chi_1 + \chi_3 \\ \Phi_2 &= \chi_2 + \chi_3 \\ \Phi_3 &= \chi_4 + \chi_8 \\ \Phi_4 &= \chi_5 + \chi_8 \\ \Phi_5 &= \chi_6 \\ \Phi_6 &= \chi_7, \end{aligned}$$

or in terms of the ϕ_i,

$$\begin{aligned} \Phi_1 &= 2\phi_1 + \phi_2 \\ \Phi_2 &= \phi_1 + 2\phi_2 \\ \Phi_3 &= 2\phi_3 + \phi_4 \\ \Phi_4 &= \phi_3 + 2\phi_4 \\ \Phi_5 &= \phi_5 \\ \Phi_6 &= \phi_6. \end{aligned}$$

2.7. The Modular Representation Theory of D_{10}

D_{10}, the dihedral group of 10 elements (symmetries of the regular pentagon), has ten elements, so its modular representation theory breaks down into two cases, $p = 2$ and $p = 5$. Note that if q is an odd prime, the modular representation theory of D_{2q} looks pretty similar to that of D_{10}, laid out below.

2.7.1. Character Table in Characteristic Zero. D_{10} has the presentation $\langle r, s \mid r^5 = s^2 = 1, srs = r^{-1}\rangle$; using this notation, its conjugacy classes are 1, $c_2 = \{r, r^4\}$, $c_3 = \{r^2, r^3\}$, and $c_4 = \{sr^n \mid n = 0, \dots, 4\}$ (i.e. all of the order-2 elements).

Thus, there are four irreducible representations, and the only way to write 10 as a sum of four nonzero squares is $10 = 1^2 + 1^2 + 2^2 + 2^2$, so two are one-dimensional and two are two-dimensional. The two one-dimensional ones are given by the trivial representation and a "sign representation" which sends an $s^m r^n \in D_{10}$ to $(-1)^m$. Then, the two-dimensional representations are the standard action of the dihedral group: r acts by rotation and s by reflection; however, r may rotate through one-fifth of a circle or two-fifths, and these produce the two remaining irreducible representations. Thus, the character table is as in Table 19.

2.7.2. The Case $p = 2$. The 2-regular classes of D_{10} are 1, c_2, and c_3, on which χ_1 and χ_2 coincide as the trivial character ϕ_1. There can be no more one-dimensional representations, as a one-dimensional representation must factor through the abelianization of D_{10}, which is $\mathbb{Z}/2$, and by Lemma 1.6.5, there are no more one-dimensional representations of $\mathbb{Z}/2$.

In particular, this means that χ_3 and χ_4, which are distinct in this characteristic, must remain irreducible: if either were reducible, it would split as a sum of two one-dimensional characters, and therefore as twice the trivial character ϕ_1. However, then $\chi_3(c_2) = 2$, instead of $4\cos(2\pi/5)$, and χ_4 has the same problem: $\chi_4(c_3) \neq 2$. Thus,

	1	c_1	c_2	c_3
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	$2\cos(2\pi/5)$	$2\cos(4\pi/5)$	0
χ_4	2	$2\cos(4\pi/5)$	$2\cos(2\pi/5)$	0

TABLE 19. The character table for D_{10} in characteristic zero.

this doesn't work, so χ_3 and χ_4 reduce to irreducible modular characters in this characteristic, denoted ϕ_2 and ϕ_3 respectively.

Since there are three 2-regular conjugacy classes, and we've described three irreducible representations, then there aren't any more, by Corollary 1.3.6. The character table is presented in Table 20.

	1	c_2	c_3
ϕ_1	1	1	1
ϕ_2	2	$2\cos(2\pi/5)$	$2\cos(4\pi/5)$
ϕ_3	2	$2\cos(4\pi/5)$	$2\cos(2\pi/5)$

TABLE 20. Character table for D_{10} in characteristic 2.

Thus, the decomposition matrix is

$$D = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The characters of the projective indecomposables are

$$\begin{aligned} \Phi_1 &= \chi_1 + \chi_2, \\ \Phi_2 &= \chi_3, \\ \Phi_3 &= \chi_4, \end{aligned}$$

or in terms of the ϕ_i,

$$\begin{aligned} \Phi_1 &= 2\phi_1 \\ \Phi_2 &= \phi_2 \\ \Phi_3 &= \phi_3. \end{aligned}$$

2.7.3. The Case $p = 5$**.** The 5-regular conjugacy classes are 1 and c_4, so by Corollary 1.3.6, there are two irreducible representations in this characteristic. However, χ_1 and χ_2 are distinct one-dimensional characters of D_{10} in characteristic 5, so call them ϕ_1 and ϕ_2, respectively. Thus, we're done, and indeed, χ_3 and χ_4 both split as $\phi_1 + \phi_2$. Table 21 contains the character table.

	1	c_4
ϕ_1	1	1
ϕ_2	1	-1

TABLE 21. Character table for D_{10} in characteristic 5.

The decomposition matrix is

$$D = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix}.$$

Thus, the characters of the projective indecomposables are

$$\Phi_1 = \chi_1 + \chi_3 + \chi_4,$$
$$\Phi_2 = \chi_2 + \chi_3 + \chi_4,$$

or in terms of the ϕ_i,

$$\Phi_1 = 3\phi_1 + 2\phi_2$$
$$\Phi_2 = 2\phi_1 + 3\phi_2.$$

2.8. A Sillier Example: D_8 and Q_8

Just as in characteristic zero, where D_8 and Q_8 have the same character table (though, since they're non-isomorphic as groups, the representations themselves are different), their modular representation theories also behave very similarly.

In fact, there's not very much to say about it in general: since each group is order 8, the only interesting case is $p = 2$; then, the only 2-regular subgroup of either must be the identity. Since there's only one 2-regular class, there's only one irreducible character, which therefore must be trivial. The resulting character table, if one can even call it that, is given in Table 22.

	1
ϕ	1

Table 22. The character table of D_8 or Q_8 in characteristic 2, or more generally, of any p-group in characteristic p.

Nonetheless, we may calculate the matrices for the CDE triangles for these two groups. Since their character tables are the same in characteristic 0 and 2, then the CDE triangles will also be identical. Since D_8 has five conjugacy classes, then it has five irreducible representations over K, and since the sums of the squares of their dimensions must be $|D_8| = 8$, then their dimensions must be 1, 1, 1, 1, and 2. In particular, these are their characters on the identity, even after reducing to characteristic 2, so the decomposition matrix is

$$D = \begin{bmatrix} 1 & 1 & 1 & 1 & 2 \end{bmatrix},$$

and $E = D^{\mathrm{T}}$, so

$$C = DD^{\mathrm{T}} = \begin{bmatrix} 8 \end{bmatrix}.$$

Thus, the character of the lone projective indecomposable $k[D_8]$-module is

$$\Phi = \chi_1 + \chi_2 + \chi_3 + \chi_4 + 2\chi_5,$$

or in terms of ϕ,

$$\Phi = 8\phi,$$

and as noted above, Q_8 has the same CDE triangle.

The reason these examples were uninteresting were because all elements of D_8 and Q_8 are 2-regular save for the identity, and $p = 2$ is the only interesting case; thus, the same can be said for modular representations of any finite p-group: all elements except the identity have order dividing p, so there is only one p-regular conjugacy class, and this is the only interesting positive characteristic. Thus, for any p-group (e.g. D_{16} or the Heisenberg group over $\mathbb{F}_p$), the only irreducible representation will be trivial, and the CDE triangle looks similar to the one above.

Bibliography

[1] B. Brauer and M. Suzuki. "On Finite Groups of Even Order Whose 2-Sylow Group is a Quaternion Group." *PNAS* **45** (1959): 1757-59.

[2] G. Glauberman, "Central Elements in Core-Free Groups." *Journal of Algebra* **4** (1965), 403-20.

[3] G. James and A. Kerber, *The Representation Theory of the Symmetric Group*, Encyclopedia of Mathematics and its Applications **16**, Addison-Wesley, Reading MA, 1981.

[4] G. James and M. Liebeck, *Representations and Characters of Groups*, Cambridge University Press, New York, 2001.

[5] S. Lang, *Algebra* (rev. 3rd ed.), Grad. Texts in Math. **211**, Springer-Verlag, New York, 2002.

[6] D. Quillen, "The Adams Conjecture." *Topology* **10** (1971), 67-80.

[7] J.P. Serre, *Linear Representations of Finite Groups* (trans. L.L. Scott), Grad. Texts in Math. **42**, Springer-Verlag, New York, 1977.

Index

A_4, 23
additive, *11*

Brauer character, *6*
Brauer's theorem, *7*
Brauer-Nesbitt theorem, 8

Cartan homomorphism, *12*
Cartan matrix, *14*
CDE triangle, 10, 11
characteristic polynomial, 5, 8
characters, 5, 7
$C\ell(G, K)$, 7
composition factors, *2*, 7, 10

D_{10}, 33
D_8, 35
decomposable, *1*
decomposition homomorphism, *12*
decomposition matrix, *14*

Fitting lemma, *9*

G-stable subspace, *1*
$GL_2(\mathbb{F}_3)$, 31
$G^{(p)}_{\text{reg}}$, 6
Grothendieck group, *10*

indecomposable, *1*
irreducible, *1*

Jacobson density theorem, 2

Krull-Schmidt theorem, 10

lattice, *3*

Maschke's theorem, 1
modular character, *6*

p-group, 35
p-regular, 6
$P_k(G)$, 10
projective indecomposable, *9*, 11
  of S_3, 18, 19
  of $\mathbb{Z}/p$, 17
projective module, *8*

Q_8, 35

reducible, *1*
reduction, *4*, 12
$R_k(G)$, $R_K(G)$, 10

S_3, 4, 17
S_4, 21
S_5, 24
semisimple modules, *2*
semisimplification, *3*, 6, 8
sign representation, 17, 21, 25
simple, *1*

trivial representation, 17, 21, 23, 25, 33

$\mathbb{Z}/p$, 1, 15, 16