MODULAR REPRESENTATION THEORY

LECTURES BY DAN BUMP
NOTES BY TONY FENG

Contents

Date: Winter 2015, Stanford.

DISCLAIMER

This document is a set of lecture notes that I took from a course taught by Dan Bump at Stanford University in the winter quarter of 2015. I have taken the liberty of editing them, adding explanations or examples where I thought they would be helpful, and pruning some discussions that were confusing (at least to me). There are inevitably errors, which should be entirely attributed to me.

1. Semisimple Modules

We will frequently consider the setup of an algebra A and an artinian A-module M. Some results will require the more restrictive hypothesis that A be a finite-dimensional algebra over k (usually the group ring of a finite group) and M an A-module that is finite-dimensional over k. In any case, that is a useful mental model for the general situation.

Definition 1.1. An A-module M is *simple* if it has no non-trivial (i.e. proper, non-zero) submodules.

Theorem 1.2 (Jordan-Hölder)**.** *M has a filtration*

$$M = M_1 \supset M_2 \supset \ldots \supset M_m = 0, \quad M_i/M_{i+1} \text{ simple}$$

which is called a composition series *for M.*

This is essentially unique in the sense that if $M = M'_1 \supset \ldots \supset M'_n = 0$ is another composition series, then $m = n$ and composition factors of the series are the same up to permutation.

The proof is the same as for groups (see Lang's book).

Definition 1.3. A module M is *semisimple* if it is a direct sum of simple modules.

Definition 1.4. A module M is *complete reducible* if for all submodules $U \subset M$, there exists a complement submodule $V \subset M$ such that $M = U \oplus V$ (i.e. $M = U + V$ and $U \cap V = 0$).

Proposition 1.5. *If M is artinian, then M is semisimple if and only if it is completely reducible.*

Proof. First assume that M is semisimple, and let $M = \bigoplus_{i=1}^{n} M_i$ be a decomposition into simple modules. Let I be a maximal set such that $N \cap \bigoplus_{i\in I} M_i = 0$. We claim that $M = N \oplus \bigoplus_{i\in I} M_i$. If not, then some M_j is not contained in $N \oplus \bigoplus_{i\in I} M_i$. Then we can append j to I to obtain a contradiction: since if any element of M_j lies in $N \oplus \bigoplus_{i\in I} M_i$, then all of M_j does (by simplicity).

The other direction is straightforward.

□

Lemma 1.6. *Submodules and quotient modules of a completely reducible module are completely reducible.*

Proof. Let $N \subset M$ be a submodule of a semisimple module. If $U \subset N$ is a subspace, then we have $M = U \oplus V$ by Proposition 1.5. We claim that $N \cong U \oplus (N \cap V)$. If $n \in N$, then n can be written uniquely as $u + v$ with $u \in U, v \in V$ and $u \in N \implies v \in N$.

Let Q be a quotient of M, with quotient map $\pi \colon M \to Q$. Then $\ker \pi$ admits a complement, which maps isomorphically to Q. This gives a splitting of Q as a submodule of M. □

Definition 1.7. We say a ring A is *semisimple* if it is semisimple as an A-module.

Proposition 1.8. *A is semisimple if and only if all modules over A are semisimple.*

Proof. One direction is automatic. We have to show that if A is semisimple as a module over itself, then all modules over A are semisimple. Since a direct sum of semisimples is semisimple, any free A-module is semisimple. Any module is a quotient of a free module, and a quotient of a semisimple module is semisimple by Proposition 1.6. $\square$

Theorem 1.9 (Wedderburn)**.** *If A is a semisimple ring, then A is a direct sum of matrix algebras over division rings.*

When $k = \overline{k}$, there are no non-trivial division algebras over k, so we have:

Corollary 1.10. *If A is a semisimple algebra over an algebraically closed field k, then A is a direct sum of matrix rings over k.*

♠♠♠ TONY: [as an example, think about (maximal) ideals]

2. The Jacobson radical

2.1. Characterizations of the radical.

Definition 2.1. We define the *radical* of A to be

$$\mathrm{Rad}(A) = \{x \mid xS = 0 \text{ for all simple modules } S\}.$$

This is obviously a two-sided ideal of A.

Theorem 2.2. *(1)* $\mathrm{Rad}(A)$ *is the largest nilpotent (two-sided) ideal.*
(2) It is the intersection of all maximal left (or right) ideals.
(3) It is the smallest left ideal such that $A/\mathrm{Rad}(A)$ *is semisimple.*

Proof. For (1), the key idea is to break things down into composition series. If I_1, I_2 are nilpotent ideals, i.e. $I_1^k = 0$ for some k and $I_2^\ell = 0$ for some ℓ, then $(I_1 + I_2)^{k+\ell} = 0$ (here it is important that we are working with ideals, as A is not necessarily commutative!). Thus there is a maximal two-sided nilpotent ideal. We want to show that it is $\mathrm{Rad}(A)$.

First, let's argue that $\mathrm{Rad}(A)$ actually is nilpotent. We have a composition series

$$A = A_1 \supset A_2 \supset \ldots \supset A_N = 0.$$

Since A_i/A_{i+1} is simple, $\mathrm{Rad}(A)$ annihilates it. That says that $\mathrm{Rad}(A)A_i \subset A_{i+1}$, so $\mathrm{Rad}(A)^N = 0$.

Conversely, if $J \not\subset \mathrm{Rad}(A)$ then $JS = S$ for some simple module S (indeed, $JS = 0$ or S if S is simple). But then J cannot be nilpotent.

(2) Let J' be the intersection of all the maximal left ideals. Observe that if S is simple, then $S \cong A/\mathfrak{m}$ for some maximal left ideal $\mathfrak{m}$. (Take some non-zero $s \in S$, and form the submodule $As \subset S$, which must be all of S. If $\mathfrak{m}$ is the kernel of the action, then $\mathfrak{m}$ is maximal as S has no proper non-zero submodules.) So

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

and $\mathrm{Ann}(A/\mathfrak{m}) = \{x \in A \mid xA \subset \mathfrak{m}\}$ is the largest 2-sided ideal contained in $\mathfrak{m}$. Thus $J = \bigcap \mathrm{Ann}(A/\mathfrak{m}) \subset \bigcap \mathfrak{m}$.

To show that $J' \subset J$, let S be a simple module. We want $J'S = 0$. If not, then $J'S = S$ so there exists some non-zero element $s \in S$ with $J's = S$. Then $xs = s$ for some $x \in J'$, so $(1-x)s = 0$. But we claim that $1-x$ is a unit. This is just the usual proof, with some careful bookkeeping on left ideals. Indeed, $A(1-x)$ is a left ideal, and if it's proper then $A(1-x) \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. But then $x \in \mathfrak{m}$ and $1-x \in \mathfrak{m}$, which is a contradiction.

(3) First let's show that $A/\mathrm{Rad}(A)$ is semisimple. We know that

$$\mathrm{Rad}(A) = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m} = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \ldots \cap \mathfrak{m}_N$$

because A is artinian. We have a homomorphism

$$A/\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_N \to A/\mathfrak{m}_1 \oplus A/\mathfrak{m}_2 \oplus \ldots \oplus A/\mathfrak{m}_n$$

sending $\overline{a} \mapsto (a+m_1, a+m_2, \ldots)$. Since $A/\mathfrak{m}_i$ is evidently semisimple (by the maximality of $\mathfrak{m}_i$), so is the finite direct sum and hence so is any submodule of it.

Next we have to show that $\mathrm{Rad}(A)$ is the minimal ideal with respect to this property, and that will be a consequence of the following more general result. $\square$

Definition 2.3. If M is any A-module, then we define $\mathrm{Rad}(M) := \mathrm{Rad}(A)M$.

Proposition 2.4. *If M is an A-module, then* $\mathrm{Rad}(M)$ *is the smallest submodule such that* $M/\mathrm{Rad}(M)$ *is semisimple, and it is the intersection of all maximal left submodules of M.*

We develop some preliminary results building up to the proof.

Lemma 2.5. *A module M is semisimple if and only if the intersection of all maximal submodules is* 0.

Proof. If M is semisimple, then $M = \bigoplus_{i=1}^n S_i$ with S_i simple. Then $M_i := \sum_{j\neq i} S_j$ is a maximal submodule, and $\bigcap_i M_i = 0$.

In the other direction, if the intersection of all maximal submodules is 0, then we can find *finitely many* maximal ideals $M_1, \ldots, M_n$ such that $\bigcap M_i = 0$ (since M is artinian by assumption) and then we have an inclusion

$$M \hookrightarrow \bigoplus_{i=1}^n (M/M_i).$$

But each M/M_i is simple as M_i is maximal, hence the sum is semi-simple, and a submodule of a semisimple module is semisimple. $\square$

Lemma 2.6. *If N is any A-module, then N is semisimple if and only if* $\mathrm{Rad}(A)N = 0$.

Proof. If $\mathrm{Rad}(A)N = 0$ then N is an $A/\mathrm{Rad}(A)$-module, and $A/\mathrm{Rad}(A)$ is a semisimple so N is semisimple. On the other hand, if N is semisimple, then N is a direct sum of simple A-modules, which are all killed by $\mathrm{Rad}(A)$ (by definition). $\square$

Proof of Proposition 2.4. The module M/Q is semisimple if and only if $\mathrm{Rad}(M/Q) = 0 \iff \mathrm{Rad}(A)M \subset Q$. This shows that $\mathrm{Rad}(M)$ is the smallest submodule whose quotient is semisimple.

To see that this agrees with the third description, note that the intersection of all maximal submodules of M is the smallest submodule Q with the property that the intersection of all the maximal submodules of M/Q is zero.

$\square$

2.2. **The Krull-Schmidt Theorem.** In the rest of the section, we specialize to the case where A is an algebra over an algebraically closed field k, and modules are finite-dimensional k-algebras.

Theorem 2.7 (Krull-Schmidt)**.** *Assume A is an algebra over an algebraically closed field k. Let M be an A-module finite-dimensional over k, and write*

$$M = U_1 \oplus \ldots \oplus U_n \quad U_1, \ldots, U_n \textit{ indecomposable.}$$

If

$$M = V_1 \oplus \ldots \oplus V_m \quad V_1, \ldots, V_m \textit{ indecomposable}$$

then $m = n$ and $U_i \cong V_j$ up to permutation.

Definition 2.8. Let R be a finite-dimensional k-algebra. We say that R is *local* if $R/\operatorname{Rad}(R) \cong k$.

Proposition 2.9. *R is local if and only if every element is either invertible or nilpotent.*

Proof. As $\operatorname{Rad}(R)$ is the largest two-sided nilpotent ideal of R, if $x \in R$ is not nilpotent then $x \notin \operatorname{Rad}(R)$. Let $\overline{x}$ be the image of x in $R/\operatorname{Rad}(R) \cong k$, and $y = \overline{x}^{-1}$ in k. Then $xy = 1 + q$ where $q \in \operatorname{Rad}(R)$, so $(1+q)$ is invertible with inverse $1 - q + q^2 + \ldots$.

The converse is deeper, requiring the classification of simple k-algebras. we know that $R/\operatorname{Rad}(R)$ is semisimple, hence isomorphic to a direct sum of matrix rings. If it is not simple, then each of the summands contributes an idempotent, which is neither nilpotent nor invertible. Thus we reduce to the case $R/\operatorname{Rad}(R) \cong \operatorname{Mat}_n(k)$, and it is again clear that unless $n = 1$, we can produce an idempotent. □

Remark 2.10. From the proof we see that a slightly stronger statement is true: every element is either in $\operatorname{Rad}(R)$ or invertible. Recall that $\operatorname{Rad}(R)$ was defined to be the largest two-sided nilpotent ideal, which could in general fail to contain all nilpotents. For instance, a sum of nilpotents need not be nilpotent in general, but it will be in a local ring.

Proposition 2.11. *M is an indecomposable A-module if and only if $\operatorname{End}_A(M)$ is local.*

Proof. If M is not indecomposable, then $\operatorname{End}_A(M)$ contains an idempotent projection to U, which is neither nilpotent nor invertible.

If M is indecomposable, then we want to show that every element of $\operatorname{End}_A(M)$ is nilpotent or invertible. We are basically going to use Jordan canonical form, which says that $M = \bigoplus_\lambda M_\lambda$ as A-modules. Since M is indecomposable, $M = M_\lambda$, from which the result is obvious. □

Proof of Theorem 2.7. If there are two decompositions

$$\begin{aligned} M &\cong U_1 \oplus \ldots \oplus U_m \\ &\cong V_1 \oplus \ldots \oplus V_n \end{aligned}$$

let $\pi_i \in \operatorname{End}_A(M)$ be the projection onto U_i, and let ρ_j be the projection onto V_j. Then consider $\pi_i \rho_j|_{U_1}$. This is either invertible or nilpotent, but

$$\sum_j \pi_1 \rho_j|_{U_1} = \sum \pi_1 1_M|_{U_1} = 1_{U_1}.$$

As $\pi_1\rho_j|_{U_1} \in \operatorname{End}_A(U_1)$ for each j, and $\operatorname{End}_A(U_1)$ is local, not all of them can be nilpotent. Without loss of generality, we may assume that $\pi_1\rho_1|_{U_1}$ is invertible with inverse $\theta \in \operatorname{End}(U_1)$.

We have the composition

$$\underbrace{U_1 \xrightarrow{\rho_1|_{U_1}} V_1}_{\alpha} \underbrace{\xrightarrow{\pi_1|_{V_1}} U_1 \xrightarrow{\theta}}_{\beta} U_1.$$

Then $\beta \circ \alpha = 1_{U_1}$ by the definition of θ. We claim that $V_1 \cong \mathrm{Im}(\alpha) \oplus \ker(\beta)$. This is just some accounting: if $x \in \mathrm{Im}(\alpha) \cap \ker(\beta)$, then $x = \alpha y$, hence $y = \beta\alpha y = \beta x = 0$. Also, if $z \in V_1$, then we may write

$$z = \underbrace{(z - \alpha\beta z)}_{\in \ker \beta} + \underbrace{\alpha\beta z}_{\in \mathrm{Im}\, \alpha}.$$

Since V_1 is indecomposible and $\mathrm{Im}(\alpha) \neq 0$, we conclude that $\ker(\beta) = 0$ so α, β are isomorphisms $U_1 \cong V_1$.

Now, we claim that $U_1 \cap (V_2 \oplus \ldots \oplus V_m) = 0$. That's because if $x \in U_1 \cap (V_2 + \ldots + V_m)$, then $x = \beta\alpha x$ and α is a restriction of ρ_1, which annihilates $V_2, \ldots, V_m$. Therefore, $M = U_1 + V_2 + \ldots + V_m$ and the sum is direct, and $U_1 \cong V_1$, so $M = U_1 \oplus V_2 \oplus \ldots \oplus V_m$. We are done by induction, considering the decomposition

$$U_2 \oplus \ldots \oplus U_n \cong M/U_1 \cong V_2 \oplus \ldots \oplus V_m.$$

□

3. The Brauer-Nesbitt Theorem

Example 3.1. Consider the group

$$\langle x, y \mid x^7 = y^3 = 1, yxy^{-1} = x^2 \rangle.$$

This has a normal, abelian 7-Sylow subgroup. There are five conjugacy classes, so there are five irreducible *complex* representations.

	$[1]$	$[x](3)$	$[x^{-1}](3)$	$[y](7)$	$[y^2](7)$
χ_1	1	1	1	1	1
χ_2	1	1	1	ρ	ρ^2
χ_3	1	1	1	ρ^2	ρ
χ_4	3	θ	$\overline{\theta}$	0	0
χ_5	3	$\overline{\theta}$	θ	0	0

Here ρ is a primitive cube root of unity , ξ is a primitive 7th root of unity, and $\theta = \xi + \xi^2 + \xi^4$.

What about representations in characteristic p? It turns out that the number of simple modules for $k[G]$ is equal to the number of *p-regular conjugacy classes*, i.e. the number of conjugacy classes consisting of elements whose order is not divisible by p. That is the content of the *Brauer-Nesbitt Theorem*, which we discuss now.

Assume that k is algebraically closed, or at least "sufficiently large." We let $A = k[G]$, where G is a finite group.

Recall that a classical theorem in the representation theory of finite groups over $\mathbb{C}$ says that the number of distinct irreducible representations is equal to the number of conjugacy classes. The goal of this section is to prove the following generalization to fields of positive characteristic.

Theorem 3.2 (Brauer-Nesbitt)**.** *The number of irreducible modules for A is the number of p-regular conjugacy-classes.*

Remark 3.3. Brauer originally proved a the following special case of the theorem: if ch k is 0 or prime to $|G|$, then the number of irreducible modules is the number of conjugacy classes.

Let's recall the proof in the complex case, with the hope of generalizing to positive characteristic.

First proof. The usual proof is to compute $\dim Z(k[G])$ in 2 ways. It is easily checked that $Z(k[G])$ consists of functions on G invariant under conjugation, so it has a basis functions constant on conjugacy classes, and their number is the number of conjugacy classes. On the other hand,

$$k[G] \cong \bigoplus_{V_i \text{ irreducible}} \operatorname{End}(V_i)$$

so $\dim Z(k[G])$ picks up a dimension for each irreducible representation. $\square$

Unfortunately, this proof doesn't generalize so well, so we try to find a different proof that does.

Second proof. We aim to exhibit a submodule of $k[G]$ whose codimension is both the number of irreducibles and the number of conjugacy classes.

Let T be the subspace of $A = k[G]$ generated by commutators $[x, y] = xy - yx$. We claim that this consists precisely of things of the form $\sum a_g g$ where the sum of a_g over *every* conjugacy class vanishes. This clearly implies that the codimension is equal to the number of conjugacy classes.

So why is the claim true? T is spanned by things of the form $[g, h] = gh - hg$, and replacing g by gh^{-1} we see that it's spanned by things of the form $g - hgh^{-1}$, so the characterization is clear.

Now we have to compare the codimension to the number of irreducibles. To compute the codimension of T, we again decompose

$$A = \bigoplus_{V_i \text{ irreducible}} \operatorname{End}(V_i).$$

Clearly the image of T in $\operatorname{End}(V_i) \cong \operatorname{Mat}_{d_i}(k)$ is the subspace spanned by commutators, which is just the subspace with trace 0, which has codimension 1. □

This proof does generalize, so let's pass to the modular case. Let $T = \langle [x, y] \rangle \subset A = k[G]$. This isn't quite the right object anymore, basically because it is not radical, so we consider

$$S = \{x \in A \mid x^{p^N} \in T \text{ for some } N\}.$$

We'll show that this is a vector subspace, and then count its codimension in two different ways.

Lemma 3.4. *If $a, b \in A$ then $a^p + b^p \equiv (a + b)^p \pmod{T}$.*

Proof. Note that $(a + b)^p - a^p - b^p$ is a sum of groups of p terms involving compositions of a and b, e.g. $aababab b\ldots$. We can group things that differ by a cyclic permutation, and it suffices to show that such things are in T. Let's call such a thing an *orbit* .

The commutator $(aaba\ldots)x - x(aaba\ldots) \in T$ by definition, so a whole orbit is congruent to p times the first term, which is 0. □

Lemma 3.5. *If $a \in T$, then so is a^p.*

Proof. Indeed, if $a = \sum_i [u_i, v_i]$ then by the previous lemma

$$a^p \equiv \sum (u_i v_i)^p - (v_i u_i)^p \pmod{T}.$$

But $(uv)^p - (vu)^p = uw - wu \in T$, where $w = vuvu\ldots v$. □

Lemma 3.6. *If $a, b \in S$ then so is $a + b$.*

Proof. From the previous lemma, we see that if the $x^{p^n} \in T$ for some n then it is true for all larger n. Therefore, we may assume that $a^{p^N}, b^{p^N} \in T$ and then by the first lemma (applied many times)

$$(a + b)^{p^N} \equiv a^{p^N} + b^{p^N} \pmod{T}$$

(this uses the second lemma too). □

Before continuing with the proof, let's recall the theory of the p-regular part (which can be thought of as an analogue of Jordan decomposition). Recall that if $g \in G$, then we can *uniquely* write $g = g_p g_{p'}$ where g_p and $g_{p'}$ commute, g_p has order a power of p, and $g_{p'}$ is p-regular. Indeed, given such a decomposition one can raise to a higher power of p to kill g_p, so you get $g^{p^m} = g_{p'}^{p^m}$. For an appropriate choice of m, we can make p^m congruent to 1 modulo the order of $g_{p'}$. Thus $g_{p'} \in \langle g \rangle$, hence g_p too, which implies the commutativity. It then suffices to prove the fact in a cyclic group, which is an easy hands-on exercise.

Now we know that

$$T = \left\{ \sum a_g g \mid \sum a_g = 0 \text{ on each conjugacy class} \right\}.$$

Let $\{C_i\}$ be the p-regular conjugacy classes and $D_i = \{x \mid x_{p'} \in C_i\}$. Then $G = \coprod D_i$ and we claim that

$$S = \left\{ \sum a_g g \mid \sum a_g = 0 \text{ on each } D_i \right\}.$$

To see this, write $|G| = p^k m$. Choose some $N > k$ such that $p^N \equiv 1 \pmod{m}$. Then raising to the p^N power maps each element $g \in G$ to its p-regular part, and S is the pre-image of T under this map. Therefore,

$$S = \{ f \in k[G] \mid \sum_{g \in C_i} f^{p^N}(g) = 0 \} = \{ f \in k[G] \mid \sum_{g \in D_i} f(g)^{p^N} = 0 \}$$

But $\sum_{g \in D_i} f(g)^{p^N} \equiv \sum_{g \in D_i} f(g) \pmod{p}$.

Since $\operatorname{Rad}(A)$ is nilpotent, $\operatorname{Rad}(A) \subset S$. By the classification of semisimple algebras over k,

$$A/\operatorname{Rad}(A) \cong \bigoplus_{\text{simple}} \operatorname{Mat}_{d_i}(k).$$

We can consider the image of S or T in $A/\operatorname{Rad}(A)$ as before, and in each $\operatorname{Mat}_{d_i}(k)$ the image of T the subring generated by commutators, which is the trace-zero part. The image of S is then $\{x \mid x^{p^N} = T\}$, but $\operatorname{Tr}(x^{p^N}) = 0 \iff \operatorname{Tr}(x)^{p^N} = 0$. Thus S and T have the same image in $A/\operatorname{Rad}(A)$, and since $S \supset \operatorname{Rad}(A)$ we see that the codimension of S is equal to both the number of p-regular conjugacy classes, and the number of distinct simple representations.

4. Projective Modules

4.1. **Projective Indecomposables.**

Definition 4.1. A module P is *projective* if and only if P is a summand of a free module.

Equivalently, given any surjective homomorphism $M \xrightarrow{\phi} N \to 0$, and $\theta \colon P \to N$ is any map, then θ can be lifted to a map $\theta' \colon P \to M$ making the diagram commute

$$\begin{tikzcd}
M \arrow[r] & N \\
P \arrow[u, dotted] \arrow[ur] &
\end{tikzcd}$$

Indeed, if P is a free module then this is obvious. Therefore, a direct summand of a free module has this property as well. Conversely, if P has this property then present P as a quotient of a free module.

Theorem 4.2. *If P is a projective indecomposable module, then $P/\operatorname{Rad}(P)$ is simple. The association $P \mapsto P/\operatorname{Rad}(P)$ is a bijection between isomorphism classes of projective indecomposables and simple modules.*

Proof. We claim that $\operatorname{End}(P/\operatorname{Rad}(P))$ is a quotient of $\operatorname{End}(P)$ (which we know is local), hence local. Then $P/\operatorname{Rad}(P)$ is semisimple and indecomposable, hence simple.

Any endomorphism of P takes $\operatorname{Rad}(P)$ into itself, since $\operatorname{Rad}(P) = \operatorname{Rad}(A)P$. So there is a map $\operatorname{End}(P) \to \operatorname{End}(P/\operatorname{Rad}(P))$. We want to show that this is surjective. This is where projectivity comes in to play. Indeed, we have the lifting diagram

$$\begin{tikzcd}
P \arrow[r] \arrow[d, dotted] & P/\operatorname{Rad}(P) \arrow[d] \\
P \arrow[r] & P/\operatorname{Rad}(P)
\end{tikzcd}$$

which attests to the surjectivity.

Now we want to show that if S is simple, then it's a homomorphic image of some projective indecomposable. It is certainly the quotient of some projective module $P = P_1 \oplus \ldots \oplus P_i$ where each P_i is indecomposable and projective. The image of some P_i is all of S, as S is simple. Since $P_i/\operatorname{Rad}(P_i)$ is simple, the kernel must be precisely $\operatorname{Rad}(P_i)$ (it has to contain the radical since the quotient is semisimple, and if it were bigger then the map would be zero).

So it only remains to show that if P, Q are projective indecomposables such that $P/\operatorname{Rad}(P) \cong Q/\operatorname{Rad}(Q)$, then $P \cong Q$. By the lifting property, we can lift both isomorphisms

$$\begin{tikzcd}
P \arrow[r] \arrow[d, dotted, "\alpha"] & P/\operatorname{Rad}(P) \arrow[d] \\
Q \arrow[r] & Q/\operatorname{Rad}(Q)
\end{tikzcd}$$

and

$$\begin{tikzcd} Q \arrow[r] \arrow[d, dotted, "\beta"] & P/\operatorname{Rad}(P) \arrow[d] \\ P \arrow[r] & Q/\operatorname{Rad}(Q) \end{tikzcd}$$

Since $\alpha\beta \in \operatorname{End}_A(Q)$ is not nilpotent (as it descends to an isomorphism on the quotients), it is invertible. □

4.2. **The submodule lattice.**

Example 4.3. Consider $G = S_3 = D_6 = \langle x, y \mid x^3 = y^2 = 1, yxy^{-1} = x^{-1}\rangle$. The character table over characteristic 0 is

	1	x	y
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

If $p = 3$, then there are two p-regular conjugacy classes. We expect then two p-regular Brauer characters (we will define these later, but they are the analogue of the trace of the representation), and they are precisely the 1-dimensional characters.

	1	y
ϕ_1	1	1
ϕ_2	1	-1

Let c_{ij} be the multiple of the ith simple module in the jth projective indecomposable, and set $C = (c_{ij})$. It is a theorem $C = D^t D$ where D is the decomposition matrix, expressing the reductions modulo p of the characteristic 0 irreducibles in terms of simple modules. In this example, we have

$D =$

	ϕ_1	ϕ_2
χ_1	1	0
χ_2	0	1
χ_3	1	1

by inspection of the characteristic 0 character table mod 3.

So $D^t D = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. This predicts that the 2 projective indecomposables have $P_1 = [V_1, V_1, V_2]$ and $P_2 = [V_2, V_2, V_1]$ as the composition factors in a Jordan-Hölder series.

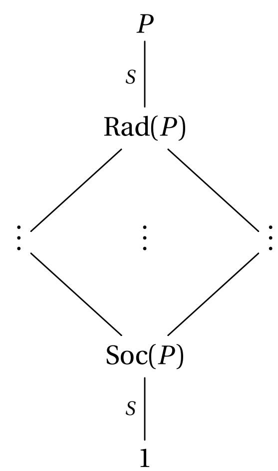
Definition 4.4. The *socle* $\operatorname{Soc}(P)$ of P is the maximal semisimple submodule.

We are interested in studying the structure of the submodule lattice of a projective module P. Let's introduce some useful notation:

$$\begin{tikzcd} U \arrow[d, dash, "M"'] \\ V \end{tikzcd}$$

means that $V \subset U$ and $U/V \cong M$.

In general, for any modular projective indecomposable and any p, G, the submodule lattice looks like



We will prove this later.

In Example 7.8, the two projective indecomposables must have sublattices

$$1 \subset_{V_1} \ldots \subset_{V_1} P_1 \quad \text{and} \quad 1 \subset_{V_2} \ldots \subset_{V_2} P_2.$$

Also, $k[G] = P_1 \oplus P_2$ by inspecting the character table.

Theorem 4.5. *The multiplicity of P_i in A is equal to* $\dim S_i$. *In particular, every projective indecomposable for G appears in A.*

Proof. $A/\operatorname{Rad}(A)$ is a semisimple ring, so every simple (hence semisimple) module for A has its module structured induced from a module structure of $A/\operatorname{Rad}(A)$. So

$$A/\operatorname{Rad}(A) \cong \bigoplus \operatorname{Mat}_{d_i}(k),$$

where $d_i = \dim S_i$, and $\operatorname{Mat}_{d_i}(k)$ is a direct sum as left A-modules of d_i copies of S_i (explicitly, via the columns).

On the other hand, one has by Krull-Schmidt a decomposition $A \cong \bigoplus c_i P_i$. Then

$$A/\operatorname{Rad}(A) \cong \bigoplus c_i P_i/\operatorname{Rad}(P_i) \cong \bigoplus c_i S_i$$

so $c_i = d_i$. □

Example 4.6. Now we analyze the two projective indecomposables of S_3. Write

$$\begin{aligned} a &= (1 + x + x^2)(1 + y), \\ b &= (1 + 2x)(1 + y) = (1 - x)(1 + y) \\ c &= (1 + y) \end{aligned}$$

Considered as elements of $k[G]$, a is the sum of all $g \in G$, so $xa = a$ and $ya = a$. We have the following identities:

$$\begin{aligned} xb &= b - a \\ yb &= -b - a \\ xc &= c - b, \\ yc &= c \end{aligned}$$

Therefore,

$$1 \subset_{V_1} (ka) \subset_{V_2} (ka + kb) \subset_{V_1} (ka + kb + kc)$$

so $ka + kb + kc$ is the projective indecomposable P_1. If one replaces $1 + y$ with $1 - y$ everywhere one gets the other projective indecomposable P_2.

5. Frobenius Algebras

We want to prove the following theorem, which will require us to build up some results on Frobenius algebras.

Theorem 5.1. *P is a projective indecomposable if and only if $P/\operatorname{Rad}(P) \cong \operatorname{Soc}(P)$.*

Definition 5.2. A finite-dimensional algebra is a *Frobenius algebra* if there exists a symmetric bilinear form $\beta \colon A \times A \to k$ which non-degenerate and satisfies $\beta(xy,z) = \beta(x,yz)$.

Remark 5.3. An equivalent definition is that the left and right regular representations on A, A^* are equivalent. Here A^* can be given an A-module structure in the following way: for $\phi \in A^*$, $(a\phi)(x) = \phi(xa)$.

To see the equivalence, given an isomorphism $\theta \colon A \cong A^*$ we can define the bilinear form $\beta(x,y) = \theta(y)(x)$. Then $\beta(xa,y) = \theta(y)(xa) = (a \cdot \theta(y))(x) = \beta(x,ay)$. Conversely, given β then we define θ by the same formula.

The group ring $A = k[G]$ is a Frobenius algebra as follows. Define $\tau \colon A \to k$ by $\tau(g) = 1$ if $g = 1$ and 0 otherwise, and $\beta(x,y) = \tau(xy)$.

Now we choose a slightly different action on the dual: if $\phi \in V^*$ and $g \in G$, then we define $(g\phi)(v) = \phi(g^{-1}v)$.

Lemma 5.4. *If V is projective then so is V^*, and if V is indecomposable then so is V^*.*

Proof. If $k[G]^n \cong V \oplus V'$, then $k[G]^n \cong (k[G]^*)^n \cong V^* \oplus (V')^*$ so V^* is projective. Under this isomorphism $k[G] \to k[G]^*$, $g \longleftrightarrow \delta_g(x) = \mathbf{1}(x = g)$.

If V is indecomposable, then V^* is also indecomposable, as a non-trivial splitting $V^* = W \oplus W'$ gives by duality a non-trivial splitting $V \cong W^* \oplus (W')^*$. □

Remark 5.5. This shows that projectives are also injectives in the category of $k[G]$-modules.

Definition 5.6. If V is a $k[G]$-module, then we define its *socle* to be

$$\operatorname{Soc}(V) = \{x \in V \mid \operatorname{Rad}(A)x = 0\}$$

Lemma 5.7. $\operatorname{Soc}(V)$ *is the maximal semisimple submodule of V.*

Proof. If $U, W \subset V$ are semismple, then so is $U + W$ since $U + W \cong U \oplus W/(U \cap W)$ and $U \oplus W$ is semisimple. Therefore, there is a maximal semisimple submodule, say S.

Observe that $\operatorname{Soc}(V)$ is an $A/\operatorname{Rad}(A)$-module, and $A/\operatorname{Rad}(A)$ is semisimple, so $\operatorname{Soc}(V)$ is semismiple, Therefore, $\operatorname{Soc}(V) \subset S$. The other containment is obvious, as $\operatorname{Rad}(A)$ annihilates any simple module, hence also any semisimple module. □

Remark 5.8. If you dualize our earlier picture of the submodule lattice, then one gets $\operatorname{Soc}(V)^* = V^*/\operatorname{Rad}(V^*)$ and $\operatorname{Soc}(V^*) \cong (V/\operatorname{Rad}(V))^*$.

The following theorem affirms what we mentioned (and observed for S_3) earlier, which is that the top composition factor for V is also isomorphic to $\operatorname{Soc}(V)$.

Theorem 5.9. *If V is a projective indecomposable, then $V/\operatorname{Rad}(V) \cong \operatorname{Soc}(V)$.*

Proof. Write $A \cong Q \oplus R$ where Q is the direct sum of projective indecomposables isomorphic to V, and R is the direct sum of projective indecomposables not isomorphic to V. (At this point, we may not know that this is independent of some presentation of A as a direct sum of projective indecomposables.)

Write $1 = e + f$ where $e \in Q$ and $f \in R$.

Lemma 5.10. *If $x \in Q$, then $xe = x$. If $x \in R$, then $xe = 0$.*

Remark 5.11. This shows that Q is uniquely determined.

Proof. If $x \in Q$, then $x = xe + xf$ so $xf = x - xe$. But $xf \in R$ and $x - xe \in Q$ (since $x \in Q$ and $e \in Q$) so $xf = 0$ and $x = xe$.

If $x \in R$, then we play the same game with $xe = x - xf$. □

Now, we know that $S := V/\operatorname{Rad}(V)$ is simple because V is a projective indecomposable, and $T := \operatorname{Soc}(V) = (V^*/\operatorname{Rad}(V^*))^*$ is also simple because $(V^*/\operatorname{Rad}(V^*))$ is simple. Suppose for the sake of contradiction that $S \ncong T$. Let I be the sum of all simple left ideals of A isomorphic to T.

We claim that I is a two-sided ideal contained in Q. It is clearly a left ideal. If E is a left ideal isomorphic to T and $a \in A$, then either $Ea \cong E$ or $Ea = 0$, as E is simple. So Ia is a sum of left ideals isomorphic to T, verifying that I is also a right ideal.

Why is I contained in Q? Well, I is semisimple, hence $I \subset \operatorname{Soc}(A) = \operatorname{Soc}(Q) \oplus \operatorname{Soc}(R)$, but R has no submodules isomorphic to S since R is the sum of submodules not isomorphic to V. So the projection of I to $\operatorname{Soc}(R)$ is 0, hence $I \subset \operatorname{Soc}(Q) \subset Q$.

Now $I \neq 0$ (for instance, $\operatorname{Soc}(Q)$ is in it), so we can produce a contradiction by showing that $I = 0$. If $a \in I$, then $x \mapsto xa$ is a map $A \to I$, which is zero on R since R is a direct sum of projective indecomposables that do not admit T as a quotient. Therefore, if $f \in R$ then $fa = 0$, so we may write

$$a = ea + fa = ea = ea - ae$$

since $ae = 0$ (by the previous lemma). Since I is a two-sided ideal, this implies that for all $a \in I$ and $b \in A$ (so that $ab \in I$) we can write $a = ae - ea$ and $ab = abe - eab$, hence

$$\begin{aligned} \beta(a,b) &= \tau(ab) \\ &= \tau(abe - eab) \\ &= 0 \end{aligned}$$

Therefore, $\beta(I, A) = 0 \implies I = 0$ since β is non-degenerate.

□

Lemma 5.12. *If H is a p-group, then H has a unique simple module (the trivial one) and every projective module over H is free.*

Proof. Let $z \in Z(H)$. In a representation $\pi \colon H \to \operatorname{End}(V)$, where V is a simple module, $\pi(z)$ has only 1 as an eigenvalue since $z^{p^N} = 1$ and $\operatorname{ch}(k) = p$. So $\{x \in V \mid \pi(z)x = x\}$ is non-trivial, and since V is simple that means $\pi(z)x = x$ for all $x \in V$. So H is a $H/\langle z \rangle$-module, and by induction (there are always non-trivial elements of the center in a p-group) it is trivial.

In particular, there is only one projective indecomposable module $k[G]$-module, and it appears in $k[G]$ with multiplicity 1, so it is $k[G]$. $\square$

Corollary 5.13. *Let P be a projective module for G. If $p^m \mid |G|$, then p^m divides* $\dim_k P$.

Proof. Let $\mathscr{P} \subset G$ be a p-Sylow subgroup, and say $|\mathscr{P}| = p^m$. If P is a projective indecomposable for G, then P remains projective as a $k[\mathscr{P}]$-module, since $k[G] \cong k[\mathscr{P}]^{[G:\mathscr{P}]}$. So P is a direct sum of copies of $k[\mathscr{P}]$ as a $\mathscr{P}$-module, hence its dimension is a multiple of $\dim_k k[\mathscr{P}] = |\mathscr{P}|$. $\square$

6. The CDE Triangle

Let $k = \mathbb{F}_q = \mathbb{F}_{p^n}$, and consider the algebra $k[G]$ for a finite group G. If $S_1, \ldots, S_r$ are the simple modules for $k[G]$ and $P_1, \ldots, P_r$ are the corresponding projective indecomposables, then set $c_{ji} = c_{ij} :=$ the multiplicity of S_i in P_j (in the sense of composition factors). The *Cartan* matrix is defined as

$$C = (c_{ij}).$$

It is a theorem (yet to be proven) that $C = {}^t D \cdot D$, where D describes the decomposition of the characteristic 0 irreducibles in simple modules. What we now discuss is a "categorification" of this relation.

Consider a category of modules over a ring. Our mental model is the ring $k[G]$ where G is a finite group and $k = \mathbb{F}_q$ or $K[G]$ where K is a complete field of characteristic 0 equipped with a discrete valuation, ring of integers $\mathscr{O}$, and maximal ideal $\mathfrak{m}$, e.g. a finite extension of $\mathbb{Q}_p$. Our modules are those induced by finite-dimensional representations, or more specially finite-dimensional projective representations.

Definition 6.1. The *Grothendieck group* consists of the monoid of isomorphism classes of modules in the category modulo the relations $[M] = [M'] + [M'']$ for every short exact sequence

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

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

Remark 6.2. Note that $R_K(G) = P_K(G)$ (the Grothendieck group of *projective* $K[G]$-modules) because $K[G]$-representations are semisimple in characteristic 0, so the simple modules are projective.

The main object of this section is to prove the existence of a commutative triangle

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

whose maps we now discuss (and which encode the Cartan matrix, among other things).

6.1. **The map c.** Here c is the categorical version of the Cartan matrix, sending $[P] \mapsto [P]$.

From the theory before, $[S_i]$ are a basis of $R_k(G)$ as a $\mathbb{Z}$-module (this is a reformulation of the Jordan-Hölder Theorem). Also, $[P_i]$ is a basis of $P_k(G)$ as a $\mathbb{Z}$-module (by the the Krull-Schmidt theorem, and the bijection between projective indecomposables and simple modules). Thus,

$$[P_j] \mapsto \sum_{ij} c_{ij} S_i.$$

6.2. **The map d.** Given a finite-dimensional vector space V over K, a *lattice* is a finitely-generated $\mathcal{O}$-module $L \subset V$ such that L spans V. This L will be a free module on some basis of V, as $\mathcal{O}$ is a DVR.

Example 6.3. If $V = K^n$, then $L = \mathcal{O}^n$ is a lattice.

The idea of the map d is as follows. Choose a $K[G]$-module E representing $[E] \in R_K(G)$. We want to take a lattice $L \subset E$ and map this to $[L/\mathfrak{m}L] \in R_k(G)$.

There are several issues to resolve in order to be assured that this is actually well-defined. For instance, we need to choose L to be G-invariant. But that is easy to arrange by the usual averaging trick: if L is any lattice, then $\sum_{g\in G} gL$ is G-invariant. A more serious issue is whether or not this is independent choice of lattice. Indeed one can obtain distinct $k[G]$-modules, but the key theorem of Brauer-Nesbitt is that they represent the same class in $R_k(G)$.

Theorem 6.4 (Brauer-Nesbitt)**.** *If $L, L' \subset V$ are G-invariant lattices, then $L/\mathfrak{m}L$ and $L'/\mathfrak{m}L'$ have the same composition factors, i.e.*

$$[L/\mathfrak{m}L] = [L'/\mathfrak{m}L'] \text{ in } R_k(G).$$

Proof. For some n, we have $\mathfrak{m}^n L' \subset L$. Replacing L' by $\mathfrak{m}^n L'$ doesn't change $L'/\mathfrak{m}L'$, so we may assume without loss of generality that $L' \subset L$. Similarly, we have $\mathfrak{m}^N L \subset L'$, hence a tower

$$\mathfrak{m}^N L' \subset \mathfrak{m}^N L \subset L' \subset L.$$

We prove the theorem by induction on N.

If $N = 1$, denote $T = L/L'$ and $U = L'/L$, and we have a tower

$$\begin{array}{c} L \\ {\scriptstyle T}\Big| \\ L' \\ {\scriptstyle U}\Big| \\ \mathfrak{m}L \\ {\scriptstyle T}\Big| \\ \mathfrak{m}L' \end{array}$$

Then $[L/\mathfrak{m}L] = [T] + [U] = [L'/\mathfrak{m}L']$.

Now for the general case, define $L'' = L' + \mathfrak{m}^{N-1}L$. Then we have

$$\mathfrak{m}^{N-1}L'' \subset \mathfrak{m}^{N-1}L \subset L'' \subset L$$

and

$$\mathfrak{m}L' \subset \mathfrak{m}L'' \subset L' \subset L''$$

as $\mathfrak{m}L'' = \mathfrak{m}L' + \mathfrak{m}^N L \subset L'$. By induction, $[L/\mathfrak{m}L] \cong [L''/\mathfrak{m}L'']$ from the first tower, and $[L''/\mathfrak{m}L''] \cong [L'/\mathfrak{m}L']$ by the second tower. $\square$

Lemma 6.5. *Let A be a commutative ring and let P be an $A[G]$-module which is projective as an A-module. Then P is projective as an $A[G]$-module if and only if there exists an A-linear map $u\colon P \to P$ such that*

$$x = \sum_{g\in G} g\cdot u(g^{-1}x) \text{ for all } x \in P.$$

This gives a clean criterion to boost P to a projective $A[G]$-module in terms of its A-module structure.

Proof. We first show that this endomorphisms exists if P is projective over $A[G]$. If $P = A[G]$, then we can take $u(g) = 1$ if $g = 1$ and 0 otherwise, and you can check that this works. Therefore, we can find such a u if $P = A[G]^n$ (i.e. P is free). Then we claim that such a u exists if P is projective, as we can write $P \oplus P' = A[G]^n$ and compose the u from the free case with the projection to P.

Now let's prove the converse. Given an $A[G]$-module homomorphism $\tau\colon P \to M$ and an $A[G]$-module surjection $M \xrightarrow{f} M'' \to 0$, we can find an A-module homomorphism $P \to M$ lifting τ.

$$\begin{tikzcd} & P \arrow[dl, dotted, "s"'] \arrow[d, "\tau"] & \\ M \arrow[r, "f"] & M'' \arrow[r] & 0 \end{tikzcd}$$

However, s need not be an $A[G]$-module homomorphism. So we try averaging it: let $\sigma\colon P \to M$ be the map

$$\sigma(x) = \sum_{g\in G} g\cdot su(g^{-1}x).$$

This is now a G-module homomorphism by construction, although we don't know a priori that it lifts τ, so let's compute and see. Applying f to both sides, we get

$$\begin{aligned} f\sigma(x) &= \sum_{g\in G} g(fsu(g^{-1}x)) \\ &= \sum_{g\in G} g(\tau u(g^{-1}x)) \\ &= \sum_{g\in G} \tau(gu(g^{-1}x)) \\ &= \tau(x). \end{aligned}$$

□

Theorem 6.6. *If P is an $\mathcal{O}[G]$-module that is free as an $\mathcal{O}$-module, then P is projective over $\mathcal{O}[G]$ if and only if $P/\mathfrak{m}P$ is projective as a $k[G]$-module.*

Proof. The direction $\Longrightarrow$ is easy. Given a diagram

$$\begin{tikzcd} & P/\mathfrak{m}P \arrow[d] & \\ M' \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

we can compose with the morphism $P \to P/\mathfrak{m}P$, and lift to a map $P \to M'$ by considering the diagram in the category of $\mathscr{O}[G]$-modules.

$$\begin{tikzcd} & P \arrow[d] \arrow[dl, dotted] & \\ & P/\mathfrak{m}P \arrow[d] & \\ M' \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

Since $\mathfrak{m}$ kills M', this lift factors through $P/\mathfrak{m}P$.

The other direction is trickier, and we need to use the preceding lemma. Suppose that $\overline{P} := P/\mathfrak{m}P$ is projective, and let $\overline{u}\colon \overline{P} \to \overline{P}$ be an endomorphism as in the lemma. We can lift $\overline{u}$ to a map $u_0\colon P \to P$ satisfying

$$x \equiv \sum g u_0(g^{-1}x) \pmod{\mathfrak{m}P}.$$

Then we define

$$u_1(x) = \sum_{g \in G} g u_0(g^{-1}x)$$

and we know that u_1 is a G-module homomorphism such that $u_1(x) \equiv x \pmod{\mathfrak{m}P}$. We want to be able to arrange that this be an equality on the nose.

As P is a free $\mathscr{O}$-module of finite rank (by assumption), the determinant of u_1 with respect to some basis is a unit. ($\mathscr{O}$ is a local ring, and $\det u_1 \equiv 1 \pmod{\mathfrak{m}}$, so $\det \in \mathscr{O}^\times$.) This means that u_1 is invertible. Therefore, we can find $v_1\colon P \to P$ such that $u_1 v_1 = 1$ on P, and u_1 being a G-module homomorphism implies that so is v_1. If we define $u = u_0 v_1$, then

$$x = u_1 v_1(x) = \sum_{g \in G} g u_0(g^{-1} v_1 x) = \sum_{g \in G} g u(g^{-1}x).$$

$\square$

6.3. **The map e.** We also want to show that every projective $k[G]$-module is of the form $P/\mathfrak{m}P$ for some projective $\mathscr{O}[G]$-module P. That defines the map $[\overline{P}] \xrightarrow{e} [P]$. So we begin with some preliminaries on projective envelopes.

Definition 6.7. A homomorphism $\phi\colon T \to U$ is *essential* if it is surjective, but ϕ restricted to any proper submodule is not surjective.

A *projective envelope* is an essential homomorphism $\phi\colon P \to M$ where P is projective.

Example 6.8. If U is semi-simple, then it's a direct sum of simples, and for each simple one can take the corresponding projective indecomposable.

Theorem 6.9. *Let A be an artinian ring and M an A-module of finite length. Then M has a projective envelope, which is unique up to isomorphism.*

Proof. Take $M = L/R$ where L is projective. Choose $N \subset R$ minimal (using the Artinian assumption) such that $L/N \to L/R$ is essential ($L \to M$ would be essential if $N = R$). Take Q minimal such that $N + Q = L$.

$$\begin{tikzcd} L \arrow[d, dash, "M"'] \\ R \arrow[d, dash] \\ N \end{tikzcd}$$

We claim that the morphism $Q \hookrightarrow L \to L/N$ is essential. It is clearly surjective, so by projectivity of L we can find a lift

$$\begin{tikzcd} Q \arrow[r, hook] & L \arrow[r] & L/N \\ & & L \arrow[u] \arrow[ull, dotted, "q"] \end{tikzcd}$$

This q satisfies $q(x) \equiv x \pmod N$ (just by the statement that it is a lift). The minimality of Q implies $Q \to L \to L/N$ is essential, as Q is minimal with the property that $Q + N = L$. This also implies that q is surjective, as if the image were a proper submodule then that proper submodule would surject onto L/N.

So at this point we just want to show that Q is projective. Let $N' = \ker q$. We claim that $N' = N$. Indeed, $L/N' = Q \to L/N$ is essential, and $L/N \to L/R$ is essential (it easy to check from the definition that a composite of essential maps is essential) but $N' \subset N$ and we chose N to be *minimal* with respect to this property, so $N' = N$.

Therefore, we can identify $Q = L/\ker(q) = L/N$, so we have a map $\overline{q}\colon L/N \to Q$ and $Q \to L \to L/N$ are inverse isomorphisms. This means that $Q \cap N = 0$ and $L = Q \oplus N$ is a direct sum. Therefore, Q is projective. $\square$

Now we can construct the map e. We proved above that if P is an $\mathscr{O}[G]$-module that is free as an $\mathscr{O}$-module, then P is projective over $\mathscr{O}[G]$ if and only if $P/\mathfrak{m}P$ is projective as a $k[G]$-module. It's also easy to show that if P and P' are projective $\mathscr{O}[G]$-modules such that $P/\mathfrak{m}P \cong P'/\mathfrak{m}P'$, then $P \cong P'$. Indeed, we have a diagram

$$\begin{tikzcd} P \arrow[r] & P/\mathfrak{m}P \arrow[d] \\ P' \arrow[r] & P'/\mathfrak{m}P' \end{tikzcd}$$

and we can use projectivity to lift maps $P \to P'$ and $P' \to P$, which are inverse modulo the maximal ideal. That implies that their composition is invertible, as $\mathscr{O}$ is a DVR.

Theorem 6.10. *If $\overline{P}$ is a projective $k[G]$-module, then $\overline{P} \cong P/\mathfrak{m}P$ for some projective $\mathscr{O}[G]$-module P.*

Proof. Let $p\colon P_n \to \overline{P}$ be a projective envelope of $\overline{P}$ as an $(\mathscr{O}/\mathfrak{m}^N)[G]$-module. We claim that $\overline{P} \cong P_n/\mathfrak{m}P_n$.

The map $P_n \to \overline{P}$ obviously kills $\mathfrak{m}P_n$, so we certainly have a surjection $P_n/\mathfrak{m}P_n \to \overline{P}$. We just have to argue that this is an isomorphism. There is a ($k[G]$-linear) splitting $s\colon \overline{P} \to P_n/\mathfrak{m}P_n$ since $\overline{P}$ is projective over $k[G]$. Now $s(\overline{P})$ maps isomorphically onto $\overline{P}$, but since p is essential the image of the splitting must be full: $s(\overline{P}) = P_n/\mathfrak{m}P_n$.

Then we take $P = \varprojlim P_n$ and this works. This is an $\mathscr{O}[G]$-module, and we only have to argue that it is projective. But given any triangle

$$\begin{tikzcd} & P \arrow[d] \\ M \arrow[r, two heads] & N \end{tikzcd}$$

we have also (by right exactness of tensoring)

$$\begin{tikzcd} & P_n \arrow[d] \arrow[dl, dotted, "\exists"'] \\ M_n \arrow[r, two heads] & N_n \end{tikzcd}$$

and this pieces together to a map

$$\begin{tikzcd} & P = \varprojlim_n P_n \arrow[d] \arrow[dl, dotted, "\exists"'] \\ M = \varprojlim_n M_n \arrow[r, two heads] & N = \varprojlim_n N_n \end{tikzcd}$$

□

6.4. **Adjointness.** There are dual pairings

$$\gamma\colon P_k(G) \times R_k(G) \to \mathbb{Z}$$

and

$$\beta\colon R_K(G) \times R_K(G) \to \mathbb{Z}$$

defined as follows. For $([P],[E]) \in P_k(G) \times R_k(G)$, we define

$$\gamma([P],[E]) = \dim_k \operatorname{Hom}_{k[G]}(P, E).$$

If $S_1, \ldots, S_k, P_1, \ldots, P_k$ are simple and corresponding projective indecomposables, then they form a dual basis since P_i has a homomorphism to $S_i = P_i/\operatorname{Rad}(P_i)$ and to no other S_j.

The map β is the familiar pairing from character theory:

$$\beta([E],[E']) = \dim_K \operatorname{Hom}_{K[G]}(E, E'),$$

so $\beta([E],[E']) = \delta_{E,E'}$ if E, E' are simple.

Proposition 6.11. *The maps d and e are adjoint with respect to these pairings, i.e. if $[P] \in P_k(G)$ and $[E] \in R_K(G)$, then*

$$\beta(e[P],[E]) = \gamma([P], d[E]).$$

Proof. Unraveling the definitions of the maps, this means the following. If $k = \mathbb{F}_q$ and K is the complete field of characteristic 0 with residue field k, then we can find a module P' such that $P'/\mathfrak{m}P' \cong P$. Then $e[P] = [P']$. On the other hand, let L_E be a G-stable lattice in E, so $k \otimes_{\mathscr{O}} L_E$ is $d[E]$. Then we wish to show the equality

$$\dim_K \mathrm{Hom}_{K[G]}(K \otimes_{\mathscr{O}} P', E) = \dim_k \mathrm{Hom}_{k[G]}(P, k \otimes_{\mathscr{O}} E')$$

The left hand side is

$$\dim_K \mathrm{Hom}_{K[G]}(K \otimes_{\mathscr{O}} P', K \otimes_{\mathscr{O}} L_E) = \dim_K K \otimes \mathrm{Hom}_{\mathscr{O}[G]}(P', L_E)$$

and right hand side is

$$\dim_k \mathrm{Hom}_G(k \otimes_{\mathscr{O}} P', k \otimes_{\mathscr{O}} L_E) = \dim_k k \otimes \mathrm{Hom}_{\mathscr{O}[G]}(P', L_E).$$

Since $\mathrm{Hom}_{\mathscr{O}[G]}(P', E')$ is free of a given rank, the dimension in either case is equal to that rank. $\square$

7. Brauer Characters

7.1. **Construction.**

Definition 7.1. A $K[G]$-module M is said to be *absolutely irreducible* over K if $M \otimes_K L$ is irreducible for any field extension L/K, i.e. if

$$L \otimes M = M_1 \oplus M_2$$

then $M_1 = L \otimes M$ or $M_1 = 0$.

Example 7.2. If $G = \mathbb{Z}/2 = \langle \tau \mid \tau^2 = 1 \rangle$ then over $\mathbb{Q}$, the module $E = \mathbb{Q}^2$ with τ acting by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is irreducible but not absolutely irreducible (it splits after extending to $\mathbb{Q}(i)$).

Definition 7.3. If K is a field of characteristic 0, then K is a *splitting field* if every irreducible $K[G]$-module is absolutely irreducible.

Theorem 7.4. *If* $\operatorname{ch} K = 0$*, then K has a finite extension that is a splitting field.*

We will use the following criterion.

Lemma 7.5. *If M is irreducible, then M is absolutely irreducible if and only if* $\operatorname{End}_{K[G]}(M) = K$.

Proof. One direction follows immediately from Schur's Lemma. For the other, observe that by Schur's Lemma, $\operatorname{End}_{K[G]}(M)$ is a division ring. But the assumption of absolute irreducibility implies that after extending scalars to $\overline{K}$, then one obtains just $\overline{K}$, so the division ring must have been K. □

Proof sketch of Theorem 7.4. If $E_1, \ldots, E_r$ are the irreducible modules for $K[G]$, then $\operatorname{End}(E_i)$ is a division ring (by Schur's lemma). If you extend the ground field far enough you can split all the division rings (take a maximal subfield of each such division ring, and then the compositum of all these). □

Remark 7.6. Brauer proved (though we don't need this) that if e is the least common multiple of the orders of the elements of G (so $\mathbb{Q}(\zeta_e)$, $\zeta_e = e^{2\pi i/e}$ contains all the eigenvalues of all complex representations), then $K(\xi_e)$ is a splitting field.

If $k = \overline{\mathbb{F}_p}$, then $k^\times$ is isomorphic to the subgroup of the roots of unity $\mathbb{C}^\times$ consisting of elements of order prime to p. Fix such an isomorphism $\theta \colon k^\times \hookrightarrow \mathbb{C}^\times$.

Let K_1 be a splitting field containing ξ_e, Galois over $\mathbb{Q}$, with ring of integers $\mathcal{O}_1$ and $\mathfrak{p}_1$ a prime lying over p. Then $\mathcal{O}_1/\mathfrak{p}_1 = \mathbb{F}_q$ (Galois implying that this doesn't depend on $\mathfrak{p}_1$). We can arrange θ so that the following diagram commutes

$$\begin{tikzcd} \mu_e \subset \mathcal{O}^\times \arrow[rr, hook] \arrow[dr] & & \overline{K}^\times \\ & \overline{\mu_e} \subset k^\times \arrow[ur, "\theta"] & \end{tikzcd}$$

♠♠♠ TONY: [exercise]

Let M be a $k[G]$-module. Then the associated *Brauer character* is

$$\phi_M(g) = \sum_i \theta(\alpha_i)$$

where $\{\alpha_i\}$ are the eigenvalues of the endomorphism of M induced by g. If g is p-regular, then this is determined by the class of M in $R_k(G)$.

If M is projective, then there is a lift to a $K[G]$-module by the map $e\colon P_k(G) \to R_K(G)$, i.e. a projective $K[G]$-module P such that $P/\mathfrak{m}P \cong M$. This is well-defined in the Grothendieck group, so its usual complex character $\eta_P(g)$ (by picking an inclusion $K \hookrightarrow \mathbb{C}$) is defined for all g.

Theorem 7.7. *The value $\eta_P(1)$ is a multiple of p^k, the order of a p-sylow $\mathscr{P} \subset G$, and $\eta_P(g) = 0$ if g is not p-regular.*

Proof. Restrict P to $k[\mathscr{P}]$. Recall that $\mathscr{P}$ has the trivial module as its only simple module, so $k[\mathscr{P}]$ is a projective indecomposable (hence all projectives are free). Since P is a free $k[\mathscr{P}]$-module, its dimension is a multiple of $p^k = |\mathscr{P}|$. This proves the first part.

Now write $g = g_p g_{p'}$ (the p-regular decomposition). We want that if $g_p \neq 1$, then $\eta(g) = 0$. Well, P remains free when restricted to $\langle g_p \rangle$, and we may assume without loss of generality that $g_p \in \mathscr{P}$. Since $g_{p'}$ commutes with g, we have a decomposition

$$P = \bigoplus P_\alpha$$

where α runs through the eigenvalues of $g_{p'}$ on P and

$$P_\alpha = \{x \mid g_{p'} x = \alpha x\}.$$

Therefore, each P_α is a free module over the cyclic group $\langle g_p \rangle$. If $g_p \neq 1$, then

$$\operatorname{Tr}(g|_P) = \sum_\alpha \alpha \operatorname{Tr}(g_p|_{P_\alpha})$$

but $\operatorname{Tr}(g_p|_{P_\alpha}) = 0$ as P_α is some multiple of the regular representation of $\langle g_p \rangle$. $\square$

Example 7.8. Consider $G = S_3$ and $p = 3$. Then the character table is

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

The p-regular character table is

	1	(12)
ϕ_1	1	1
ϕ_2	1	−1

From this we see by inspection

$D =$

	ϕ_1	ϕ_2
χ_1	1	0
χ_2	0	1
χ_3	1	1

Thus we have

$$C = {}^tD \cdot D = \begin{array}{|c|cc|} \hline & \phi_1 & \phi_2 \\ \hline \eta_1 & 2 & 1 \\ \eta_2 & 1 & 2 \\ \hline \end{array}$$

Let's recall what this predicts. The projective indecomposables P_i form a basis for $P_k(G)$, and the simples S_j form a basis for $R_k(G)$. Then c_{ij} is the multiplicity of S_j in P_i, so if η_i is the Brauer character of $P_k(G)$ and ϕ_j is the Brauer character of S_j, then

$$\eta_i = c_{ij}\phi_j.$$

which only is defined on the p-regular conjugacy classes (as the ϕ_j are only defined on the p-regular conjugacy classes). Also, $\{\eta_i\}$ and $\{\phi_j\}$ form dual bases under the natural pairing (summation over p-regular conjugacy classes).

On the other hand, if χ_k are the complex characters associated to a basis of $R_K(G)$, then

$$\eta_i \mapsto \sum_k d_{ik}\chi_k.$$

So the CDE triangle looks like

$$\begin{tikzcd} \eta_i \arrow[rr, mapsto] \arrow[dr, mapsto] & & c(\eta_i) = \sum c_{ij}\phi_j \\ & \sum d_{ik}\chi_k \arrow[ur, mapsto] & \end{tikzcd}$$

We can deduce the image of the χ_k by the adjointness relations in §6.4. For η_i and χ_k, we have

$$\langle \eta_i, e(\chi_k)\rangle = \langle d(\eta_i), \chi_k\rangle.$$

Using the duality of the bases, this unravels as

$$\langle \eta_i, e(\chi_k)\rangle = \sum_j \langle \eta_i, e_{kj}\phi_j\rangle = e_{ki}.$$

On the other side,

$$\langle d(\eta_i), \chi_k\rangle = \sum_\ell \langle d_{i\ell}\chi_\ell, \chi_k\rangle = d_{ik}.$$

Therefore, we see that $e_{ji} = d_{ij}$, i.e.

$$\chi_k \mapsto \sum_j d_{jk}\phi_j.$$

This gives the identity $C = {}^tD \cdot D$.

We see $\eta_1 = 2\phi_1 + \phi_2$ on p-regular conjugacy classes, and we know that this extends to a true character (of the corresponding characteristic 0 representation under e) which is expected to vanish on (123) (by the theorem), and similarly for η_2. Indeed, this is verified:

	1	(123)	(12)
η_1	3	0	-1
η_2	3	0	-1

7.2. **Orthogonality relations.** Recall from the theory of §6.4 the CDE triangle

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

We defined a pairing

$$P_k(G) \times R_k(G) \to \mathbb{Z}$$

such that

$$\langle [P], [E] \rangle = \dim_k \operatorname{Hom}_{k[G]}(P, E).$$

A natural dual basis consists of the projective indecomposables $\{P_i\} \subset P_k(G)$ and their associated simples $S_i \subset R_k(G)$:

$$\langle [P_i], [S_j] \rangle = \delta_{ij}.$$

For the pairing

$$R_K \times R_K \to \mathbb{Z},$$

similarly defined by

$$\langle [M], [M'] \rangle = \dim_k \operatorname{Hom}_{k[G]}(M, M')$$

the simple modules $[\Pi_i]$ form an orthonormal basis with respect to this pairing.

The maps d, e are adjoint with respect to these pairings: for $[P] \in P_k(G)$ and $M \in R_K(G)$,

$$\langle d[P], [M] \rangle = \langle [P], e[M] \rangle.$$

We denoted $d[\Pi_i] = \sum_j d_{ij}[S_j]$, which implied $e[P_j] = \sum_i d_{ij}[\Pi_i]$ as a formal consequence of adjointness.

This translates into a statement about Brauer characters. Suppose

- ϕ_i is the Brauer character of $[S_i]$ (supported on p-regular conjugacy classes),
- χ_i is the character of Π_i, and
- η_i is the Brauer character of $[P_i]$, i.e. the ordinary character of $e[P_i]$ (which we can extend to all conjugacy classes by declaring them to be 0 off p-regular conjugacy classes).

Then the compatibility of the Brauer character with the relations in the Grothendieck group imply that

$$\boxed{\eta_j(g) = \sum_i d_{ij} \chi_i(g) \text{ for } \textit{all } g,} \tag{1}$$

(all g since both sides vanish if g is not p-regular by Theorem 7.7)

$$\boxed{\chi_i(g) = \sum_j d_{ij} \phi_j(g) \text{ on } p\text{-regular } g} \tag{2}$$

(since the ϕ_j are not defined on g that are not p-regular.)

We now recall the usual inner products from character theory.

- Let $H = \bigoplus \mathbb{Z}\eta_j$ be the Grothendieck group of Brauer characters of projective modules for $k[G]$,

- $B = \bigoplus \mathbb{Z}\phi_i$,
- $X = \bigoplus \mathbb{Z}\chi_i$ (the ordinary characters).

Then we have a pairing

$$X \times X \to \mathbb{Z}$$

defined by

$$\langle \chi_i, \chi_j \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)}.$$

We also define a pairing $H \times B \to \mathbb{Z}$ by

$$\langle \eta_j, \phi_k \rangle = \frac{1}{|G|} \sum_{g \ p\text{-regular}} \eta_j(g)\overline{\phi_k(g)}$$

(which can be interpreted as the sum over all g with the convention that 0 times undefined is 0).

Theorem 7.9. *With these definitions, we have*

$$\langle \phi_j, \eta_k \rangle = \delta_{jk}.$$

Proof. As noted above,

$$\sum_i d_{ij}\chi_i = \eta_j$$

so $d_{ij} = \langle \eta_j, \chi_i \rangle$ as the χ_i form an orthonormal basis of class functions. We also noted that

$$\chi_i(g) = \sum_g d_{ij}\phi_j(g)$$

if g is p-regular. Therefore,

$$\sum_j d_{ij}\langle \phi_j, \eta_k \rangle = \langle \chi_i, \eta_k \rangle = d_{ik} = \sum d_{ij}\delta_{jk}.$$

We would like to conclude the result by multiplying by the inverse of (d_{ij}). Now, the matrix (d_{ij}) is not square, but its rank is equal to the number of p-regular conjugacy classes because $D^t D$ is the Cartan matrix, which has that rank. Therefore D has a *left* inverse, which lets us conclude that $\langle \phi_j, \eta_k \rangle = \delta_{jk}$, as desired. □

Theorem 7.9 implies that the two pairings $P_k(G) \times R_k(G) \to \mathbb{Z}$ we defined (one by Brauer theory, and the other by usual character theory) coincide.

Example 7.10. You can check that the relations hold in the example of S_3, as worked out in Example 7.8.

7.3. **Future applications.** We give a glimpse of some results that we will be able to prove later.

Recall that a *generalized character* (also called *virtual* character) is a difference of two characters, and an *elementary subgroup* is a product of an ℓ-group (ℓ a prime) and a cyclic group.

Theorem 7.11 (Brauer). *If χ is a class function on G and $\chi|_E$ is a generalized character for all elementary subgroups E, then χ is a generalized character.*

This has some interesting consequences. For instance, it can be used to show that the map $R_K(G) \xrightarrow{d} R_k(G)$ is surjective. However, if a class in $R_k(G)$ is not represented by a projective module then you don't know that a representative for the lift can be chosen with no negative coefficients. That means that if χ is any character, then χ restricted to the p-regular conjugacy classes is a linear combination of $\mathbb{Z}$-coefficients (possibly negative) of ϕ_i.

Another consequence proved by Green (used in the classification of irreducible representations of GL_n over a finite field) is that if $\theta\colon k^\times \to \mathbb{C}^\times$ is a character (not necessarily injective) and $\pi\colon G \to \mathrm{GL}(n,k)$ is a representation with $\pi(g)$ having eigenvalues $\alpha_1, \ldots, \alpha_k$, then

$$\chi_\pi(g) = \sum_i \theta(\alpha_i)$$

is a generalized character. Crucially, we are *not* assuming here that g is p-regular.

Yet another interesting consequence is that if $p^k = |\mathscr{P}|$ is the order of a p-Sylow subgroup of G, then $p^k \phi_i$ can be extended to characters. We will see these applications in the future.

8. BLOCKS

The theory of blocks partitions G-modules into equivalence classes.

Let A be a finite-dimensional k-algebra (for our applications, $A = k[G]$). Suppose that we can find *proper* 2-sided ideals A_1, A_2 such that $A = A_1 \oplus A_2$. Writing $1 = e_1 + e_2$ with $e_i \in A_i$. Then A_1, A_2 are themselves rings, as

$$e_1 + e_2 = 1^2 = (e_1 + e_2)^2 = e_1^2 + e_1 e_2 + e_2 e_1 + e_2^2 = e_1^2 + e_2^2.$$

So $e_1 + e_2$ is a central orthogonal idempotent, and e_1, e_2 server as idempotents making A_i into a ring.

Exercise 8.1. Check that $e_1 x = x e_1 = x$ for any $x \in A_1$, and $e_1 x = x e_1 = 0$ if $x \in A_2$.

Definition 8.2. If there is no such decomposition, then we say that A is *indecomposable.*

Lemma 8.3. *There is a unique decomposition of A into indecomposable rings:*

$$A = A_1 \oplus \ldots \oplus A_r.$$

Proof. Let $B = A \otimes A^{\text{opp}}$. Then A is a B-module via $(a \otimes b)x = axb$. The two-sided ideals of A are B-submodules of A, so by the Krull-Schmidt Theorem applied to B, they are unique up to isomorphism. However, the assertion of the lemma is slightly stronger: they unique on the nose.

Suppose we have two different decompositions

$$A_1 \oplus \ldots \oplus A_n \cong A_1' \oplus \ldots \oplus A_n'.$$

If e_1 is the identity element for A_1, then $e_1 \otimes e_1 \in B$ is an idempotent for B, and it preserves A_1 and kills the other A_i. Applying it to A_1', we find that it induces an isomorphism, hence an equality. ☐

Now assume that k is either algebraically closed or “sufficiently large.”

Proposition 8.4. *If A is an indecomposable k-algebra and Z is its center, then Z has a unique k-algebra homomorphism $Z \to k$.*

Example 8.5. Think about $k[\mathscr{P}]$ where $\mathscr{P}$ is an abelian p-group. Then A is abelian, so $A = Z$.

Proof. Take $B = A \otimes A^{\text{opp}}$, so A is an indecomposable B-module. Then $\text{End}_{A \otimes A^{\text{opp}}}(A)$ is local. We have an embedding $Z \to \text{End}_{A \otimes A^{\text{opp}}}(A)$ sending z to $(a \mapsto z \cdot a)$. This is injective because A has a unit, so Z is a subring of a local algebra. Moreover, the property of commuting with A is preserved by inverses, so Z is itself local. Therefore $Z/\text{Rad}(Z) \cong k$. This is the unique k-algebra homomorphism $Z \to k$. (Any homomorphism to k must kill the nilpotents, and so factors through this one). ☐

Now, the idea is that if $A = B_1 \oplus \ldots \oplus B_n$ is a decomposition of $k[G]$ into indecomposable ideals, the composition factors of each B_i will be considered an equivalence class of simple modules, called a *block.*

Example 8.6. If we have a characteristic 0 simple module E, then from the CDE triangle we expect $[E] \in R_K(G)$ to map to a sum of simple modules in $R_k(G)$. We expect that the simple $k[G]$-modules in $d([E])$ are all in the same block and this will be proved later. So E is attached to a unique block B_i. This shows that the notion of blocks are in some sense compatible for different base fields.

Example 8.7. Let $G = D_{10}$, which has character table:

	$[1]$	$[x](2)$	$[x^2](2)$	$[y](5)$
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	α	β	0
χ_4	2	β	α	0

where $\alpha = 2\cos(2\pi/5)$ and $\beta = 2\cos(4\pi/5)$ (the latter two characters are induced from $\mathbb{Z}/5$). Let $p = 5$, so the p-regular conjugacy classes are [1] and $[y]$. Then the decomposition matrix is

$D =$

	ϕ_1	ϕ_2
χ_1	1	
χ_2		1
χ_3	1	1
χ_4	1	1

So $C = {}^t D \cdot D = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$. There's only going to be one block, as P_1 has composition series (S_1, S_2, S_1) and the other projective indecomposable has composition series (S_2, S_1, S_2).

Here is an alternate formulation of blocks. If $A = B_1 \oplus \ldots \oplus B_r$ with each B_i indecomposable, and e_i is the unit of B_i, then e_i acts by 1 on B_i, hence also on any submodule or subquotient of B_i, and by 0 on any composition factor of B_j for $j \neq i$.

Definition 8.8. We say that an A-module M *belongs to the block* B_i if $e_i \cdot M = M$ and $e_j \cdot M = 0$ for $j \neq i$.

Since $M = 1 \cdot M = \bigoplus e_i M = \bigoplus M_i$, we see that any module is a direct sum of modules belonging to the same block. Thus if M is indecomposable, then all submodules belong to some block. So all composition factors of a projective indecomposable belong to the same block.

Remark 8.9. In general, there is a way of ordering the Brauer characters such that the Cartan matrix will decompose into block matrices.

9. Mackey Theory

Mackey theory investigates the relations between representations of G induced from different subgroups. The goal is to calculate intertwining operators between induced representations, or decompose restrictions of inductions of representations.

9.1. **Frobenius Reciprocity.** Let G be a group and $H \subset G$ a subgroup.

Definition 9.1. Let W be a G-representation, i.e. a $k[G]$-module. We define the *restriction of W to H* to be W regarded as an H-representation, i.e. the usual restriction of a module to a subring, and denote it as W_H (or occasionally just W).

Definition 9.2. Let V be an H-representation, i.e. a $k[H]$-module. We define the *induction of V to G* as

$$V^G = \{f : G \to V \mid f(hg) = h \cdot f(g) \text{ for } h \in H\}.$$

with G acting on the right.

This definition generalizes well to infinite-dimensional representations, e.g. of Lie groups, thought it can be a little harder to work with.

Theorem 9.3 (Frobenius Reciprocity). *Let V be an H-representation and W a G-representation. There are H-module homomorphisms $\epsilon : V \to V^G$, and $\delta : V^G \to V$ such that composition with ϵ and δ induce isomorphisms*

$$\mathrm{Hom}_G(V^G, W) \xrightarrow{\epsilon^*} \mathrm{Hom}_H(V, W_H)$$

and

$$\mathrm{Hom}_G(W, V^G) \xrightarrow{\delta^*} \mathrm{Hom}_H(W_H, V)$$

such that $\delta \circ \epsilon = 1_V$.

Proof. First let's consider ϵ. We have to construct a canonical map taking an element $v \in V$ to a function $G \to V$, and a natural candidate is

$$\boxed{\epsilon(v)(g) = \begin{cases} g \cdot v & g \in H, \\ 0 & \text{otherwise.} \end{cases}}$$

On the other ahnd, δ is a natural map from functions $G \to V$ to V, so a natural candidate is $\boxed{\delta(f) = f(1).}$ We will check that these indeed work.

Lemma 9.4. *If $f \in V^G$ then $f = \sum_{\gamma \in G/H} \gamma \epsilon(f(\gamma^{-1}))$.*

Proof. Note that the right hand side is unchanged if we replace $\gamma \mapsto \gamma h$ since ϵ is an H-module homomorphism and the definition of V^G. □

Now we can prove the first isomorphism. Let $T \in \mathrm{Hom}_G(V_H^G, W)$ and $t = T \circ \epsilon$. Then

$$T(f) = \sum_{\gamma \in G/H} \gamma t(f(\gamma^{-1})).$$

This proves that $T \mapsto t$ is injective, as $T(f)$ can be recovered from t. Also, given t this provides a formula for $T(f)$, giving an inverse construction

The second isomorphism is even easier. □

Remark 9.5. This shows that if $k = \mathbb{C}$, and χ_W, χ_V are the characters of W, V, then

$$\langle \chi_{V^G}, \chi_W \rangle_G = \langle \chi_V, \chi_{W_H} \rangle_H.$$

It is illustrative to give a direct proof of this fact. The right hand side is of course

$$\frac{1}{|H|} \sum_{h \in H} \chi_V(h) \chi_W(h).$$

To calculate the left hand side, it is useful to develop a different perspective on the induced representation. Viewing $k[G]$ as functions $G \to k$, we have

$$V^G \cong k[G] \otimes_{k[H]} V$$

with the G-action by right-translation as functions. If we pick left coset representatives

$$G/H = \{\gamma_1 H, \dots, \gamma_n H\}$$

then we can thus identify $V^G \cong \bigoplus_{i=1}^n \gamma_i \cdot V$. Then for $g \in G$, we have $g \cdot \gamma_i \cdot V = \gamma_i \cdot V$ if and only if $g\gamma_i H = \gamma_i H$, i.e. $\gamma_i^{-1} g \gamma^i = h \in H$. Therefore,

$$\chi_{V^G}(g) = \sum_{\gamma_i^{-1} g \gamma_i = h} \chi_V(h)$$

Therefore,

$$\begin{aligned}
\langle \chi_{V^G}, \chi_W \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \chi_{V^G}(g) \chi_W(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_W(g) \#\{i \mid \gamma_i^{-1} g \gamma_i = h\} \cdot \chi_V(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_W(g) \sum_{\gamma_i^{-1} g \gamma_i = h} \chi_V(h) \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_W(h) \chi_V(h) \#\{i \mid \gamma_i^{-1} g \gamma_i = h\} \\
&= \frac{1}{|H|} \sum_{h \in H} \chi_W(h) \chi_V(h)
\end{aligned}$$

as desired.

9.2. **Mackey's Theorem.** Let $H, L < G$ be two subgroups. The problem is to induce an H-module V and restrict to L, and decompose the result into irreducibles. This process is related to another process, obtained by first restricting to some other subgroup and then inducing to L.

$$\begin{tikzcd}
& V^G \arrow[dr, "\mathrm{Res}|_L"] & \\
V \arrow[ur, "\mathrm{Ind}^G"] \arrow[dr, "\mathrm{Res}|_?"'] & & V^G|_L \\
& ?? \arrow[ur, "\mathrm{Ind}^L"'] &
\end{tikzcd}$$

We want to figure out the mystery module ??. It can be thought of as all essentially distinct intersections of conjugates of H with L.

Let $\{\gamma\} \in L\backslash G/H$ be a set of coset representatives. Then Mackey's Theorem asserts that

$$?? = \bigoplus_{\gamma} \gamma H\gamma^{-1} \cap L.$$

Definition 9.6. If V is an H-module and $\gamma \in G$, then let ${}^{(\gamma)}V$ denote the $\gamma H\gamma^{-1}$-module with underlying set is V and action twisted by γ. More precisely, if ${}^{(\gamma)}v \in^{(\gamma)} V$ is the element corresponding to $v \in V$ and $h \in H$, then

$$\gamma h\gamma^{-1} \cdot {}^{(\gamma)}v = {}^{(\gamma)}(h \cdot v).$$

Theorem 9.7 (Mackey)**.** *If $H, L < G$ then*

$$V^G|_L \cong \bigoplus_{\gamma \in L\backslash G/H} \left({}^{(\gamma)}V|_{\gamma H\gamma^{-1}\cap L}\right)^L.$$

Proof. Set $\Omega_\gamma = \{f \in V^G \mid \mathrm{supp}(f) \subset H\gamma^{-1}L\}$. This is closed under translation by L on the right and H on the left, so we have an isomorphism of $k[L]$-modules

$$V^G = \bigoplus_{\gamma \in L\backslash G/H} \Omega_\gamma.$$

We will exhibit an isomorphism of $k[L]$-modules

$$\Omega_\gamma \cong {}^{(\gamma)}V|_{\gamma H\gamma^{-1}\cap L}.$$

If $f \in \Omega_\gamma$ we can define a function $f' \colon L \to {}^{(\gamma)}V$ by

$$f'(x) = {}^{(\gamma)}(f(\gamma^{-1}x)).$$

Note that $\gamma^{-1}x \in H\gamma^{-1}L$. We claim that $f' \in (V|_{L\cap\gamma H\gamma^{-1}})^L$. To see this, we just have to check an invariance property, so let $\gamma h\gamma^{-1} \in L \cap \gamma H\gamma^{-1}$. Then

$$\begin{aligned}
f'(\gamma h\gamma^{-1}x) &= {}^{(\gamma)}(f(h\gamma^{-1}x)) \\
&= \cdot^{(\gamma)}(h \cdot f(\gamma^{-1}x)) \\
&= \gamma h\gamma^{-1} \cdot {}^{(\gamma)}(f'(x))
\end{aligned}$$

So $f \mapsto f'$ is an L-equivariant map. That it is a bijection is clear, because f is completely determined by its values on $\gamma^{-1}L$.

□

Proposition 9.8. *Let V be an H-module and U an L-module. Then*

$$\mathrm{Hom}_G(U^G, V^G) = \bigoplus_{\gamma \in L\backslash G/H} \mathrm{Hom}_{L\cap\gamma H\gamma^{-1}}(U, {}^{(\gamma)}V).$$

Proof. By Frobenius reciprocity,

$$\mathrm{Hom}_G(U^G, V^G) \cong \mathrm{Hom}_L(U, V^G|_L).$$

By Mackey's theorem,

$$\mathrm{Hom}_L(U, V^G|_L) \cong \bigoplus_{L\backslash G/H} \mathrm{Hom}_L(U, ({}^{(\gamma)}V|_{L\cap\gamma H\gamma^{-1}})^L).$$

Finally, by (the other) Frobenius reciprocity

$$\bigoplus_{L\backslash G/H} \mathrm{Hom}_L(U, ({}^{(\gamma)}V|_{L\cap\gamma H\gamma^{-1}})^L) \cong \bigoplus_{L\backslash G/H} \mathrm{Hom}_{L\cap\gamma H\gamma^{-1}}(U, {}^{(\gamma)}V).$$

□

10. Representations of $\mathrm{GL}_n(\mathbb{F}_p)$

Let $G = \mathrm{GL}(n, \mathbb{F}_p)$. We investigate the representation theory of $k[G]$ where $k = \mathbb{F}_p$ or $k = \mathbb{C}$, which was originally worked out by Green. There is a close relationship with the theory of automorphic forms, pointed out by Harish-Chandra in the paper "Eisenstein series over finite fields."

10.1. Parabolic subgroups.

Definition 10.1. A *Borel subgroup* of G is a subgroup conjugate to the upper-triangular matrices. A *parabolic subgroup* is a group containing a Borel subgroup.

The *maximal parabolic* subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$ are conjugate to

$$\left\{ \begin{pmatrix} \boxed{\mathrm{GL}_m} & * \\ 0 & \boxed{\mathrm{GL}_{n-m}} \end{pmatrix} \right\}. \tag{3}$$

A parabolic subgroup is a semidirect product of a semisimple group and a unipotent group.

Example 10.2. $B = TU$ where U is are the superdiagonal matrices, and T is the maximal torus.

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

Example 10.3. The maximal parabolic in (3) has decomposition $M_P \cdot U_P$, where

$$M_P = \left\{ \begin{pmatrix} \boxed{\mathrm{GL}_m} & 0 \\ 0 & \boxed{\mathrm{GL}_{n-m}} \end{pmatrix} \right\} \cong \mathrm{GL}_m \times \mathrm{GL}_{n-m}$$

and

$$U_P \cong \left\{ \begin{pmatrix} 1_m & * \\ 0 & 1_{n-m} \end{pmatrix} \right\}.$$

Now suppose $k = \mathbb{F}_p$. Then U_B is a p-Sylow subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$, with normalizer B.

Definition 10.4. An *irreducible representation* (π, V) is *cuspidal* if it has no fixed vector with respect to the unipotent radical of any parabolic subgroup (it suffices to check the maximal ones).

In other words, for every $P = M_P U_P$, the U_P-coinvariants vanish:

$$V_{U_P} := V / \langle u \cdot v - v \mid u \in U_P \rangle = 0.$$

The general goals are:

(1) Classify the cuspidal representations,
(2) Assemble cuspidal representations of Levi subgroups

The cuspidal representations of Levi subgroups give rise to representations of G by *parabolic induction*, and the result is often irreducible and always has a nice theory of decomposition into irreducibles.

For the second objective, one uses Mackey theory and Hecke algebras. Green's approach was to construct cuspidal representations using "lifts from characteristic p."

10.2. **Cartan subgroups.**

Definition 10.5. A *Cartan subgroup* of G is a maximal torus, and is usually denoted by T.

The Cartan subgroups of G are of the form

$$T(\mathbb{F}_p) \cong \prod_i \mathbb{F}_{p^{\lambda_i}}^\times$$

and the data of the $\{\lambda_i\}$ determine the conjugacy class of the Cartan subgroup.

Example 10.6. For $\mathrm{GL}(2,\mathbb{F}_p)$, the Cartan subgroups are isomorphic either to $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ (of order $(p-1)^2$) or $\mathbb{F}_{p^2}^\times$ (of order p^2-1).

There are two special Cartan subgroups: $\prod \mathbb{F}_p^\times$ (maximal split) and $\mathbb{F}_{p^n}^\times$ (maximal anisotropic). Roughly speaking, irreducible representations are indexed by characters of the maximal tori, and cuspidal representations are indexed by characters of maximal anisotropic torus.

If $G = \mathrm{GL}(2)$ and M_P is a Levi subgroup of G, then there is a parabolic subgroup $P = M_P U_P$ and a quotient map $P \to M_P \cong P/U_P$. Restricting to P and then inducing to G establishes a correspondence between representations of Levi subroups and representations of G, the inverse being given by the Jacquet functor.

For references, see: Tits, Springer, Cartier in AMS Proc Pure Math, Boulder (v.9), Corvallis (v. 33), Borel and Tits (IHES).

Definition 10.7. Let

$$B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

be the standard Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. For two characters $\chi_1, \chi_2 \colon \mathbb{F}_q^\times \to \mathbb{C}^\times$, inducing the character $\chi \colon B \to \mathbb{C}^\times$ via

$$\chi \begin{pmatrix} t_1 & * \\ 0 & t_2 \end{pmatrix} = \chi_1(t_1)\chi_2(t_2),$$

we define the *principal series representation* $B(\chi_1,\chi_2) := \mathrm{Ind}_B^G(\chi)$ (over $k=\mathbb{C}$).

Then $\dim_k B(\chi_1,\chi_2) = [G:B] = p+1$ and we have the following fundamental result.

Theorem 10.8. *If $\chi_1 \neq \chi_2$, then $B(\chi_1,\chi_2)$ is irreducible. All identifications among the principal series are determined by*

$$B(\chi_1,\chi_2) \cong B(\mu_1,\mu_2) \iff \begin{cases} \chi_1 = \mu_1, \chi_2 = \mu_2 \\ \chi_1 = \mu_2, \chi_2 = \mu_1. \end{cases}$$

This produces $\binom{p-1}{2}$ irreducible complex representations of G of dimension $p+1$.

Proof. We shall determine the irreducibility by examining $\dim_k \mathrm{Hom}_G(\chi^G, \mu^G)$. By Mackey's Theorem,

$$\dim_k \mathrm{Hom}_G(\chi^G, \mu^G) = \bigoplus_{B\backslash G/B} \dim_k \mathrm{Hom}_{B\cap \gamma B\gamma^{-1}}(\chi, {}^{(\gamma)}\mu).$$

Now, the Bruhat decomposition says that

$$B\backslash G/B = \coprod_{w\in W} BwB$$

where W is the Weyl group of G, which in the case of GL_2 is simply S_2, identified with the group of permutation matrices. In this case, that means $\gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\gamma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, so the right hand side above is

$$\dim_k \mathrm{Hom}_B(\chi, \mu) + \dim_k \mathrm{Hom}_T(\chi, {}^{(\gamma)}\mu).$$

If $\chi = \mu$ and $\chi_1 \neq \chi_2$, then the first dimension is 1 and the second is 0. Therefore, $\mathrm{Hom}(\chi^G, \chi^G)$ is 1-dimensional, hence χ^G is indecomposable and in characteristic 0, irreducible.

The rest of the accounting is similar. The first dimension can only be non-zero if $\chi = \mu$, i.e. $\chi_i = \mu_i$, while the second can only be non-zero if the characters are swapped. □

Suppose $\chi = \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$ is a character of the split torus, and χ' is a character of the anisotropic torus. We will represent an element of the anisotropic torus as

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix}, \quad \alpha \in \mathbb{F}_{p^2} - \mathbb{F}_p$$

even though such a representatioon only exists after extending scalars. Then we obtain induced representations π, π' by first restricting these to the Borel, and then inducing to G. The resulting characters have the following values:

	1	$\begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix}$	$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix}$
χ	$p+1$	$\chi(t) + \chi(w\cdot t)$	0
χ'	$p-1$	0	$-\chi(\alpha) - \chi(\alpha^p)$

Here $w \cdot t$ denotes the image of t under the nontrivial element w of the Weyl group. This follows from our earlier computation that

$$\chi^G(t) = \sum_{\gamma_i g \gamma_i^{-1} = b} \chi(b)$$

where $\{\gamma_i\}$ form coset representatives for G/B, which we can take to be $\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$ and w.

Roughly speaking, the characters of $\mathrm{GL}(n, \mathbb{F}_q)$ are parametrized by orbits of characters of maximal tori. These orbits are parametrized by partitions of n: if λ is a partition of n, then there is a maximal torus T_λ such that

$$T_\lambda(\mathbb{F}_q) \cong \prod \mathbb{F}_{q^{\lambda_i}}^\times.$$

In particular we have the maximal split torus

$$T_s = T_{(1,\ldots,1)} \cong (\mathbb{F}_q^\times)^n$$

and the maximal anisotropic torus

$$T_a = T_{(n)} = \mathbb{F}_{q^n}^\times.$$

The representations corresponding to characters of T_s are easy to construct by induction (as we just saw). The representations corresponding to characters of T_a are hard to construct - they are called the *cuspidal representations.* So we discuss the problem of constructing them.

Let $\chi\colon \mathbb{F}_{q^n} \to \mathbb{C}^\times$ be a character not factoring through the norm map $\mathbb{F}_{q^n} \to \mathbb{F}_{q^d}$ for any $d < n$. Then there exists an irreducible cuspidal representation indexed by χ, whose character σ_χ has the following description: if g is regular semisimple (i.e. has distinct eigenvalues), then $\sigma_\chi(g) = 0$ unless g is conjugate to an element of T_a, in which case

$$\sigma_\chi(g) = (-1)^{n+1} \sum_{\alpha_i \text{ eigenvalues}} \theta(\alpha_i)$$

where $\theta\colon \overline{F}_q^\times \to \mathbb{C}^\times$ is a fixed character as used in defining the Brauer character.

There are a couple approaches to the construction: one due to Deligne-Lustzig, and the original method of Green. We will discuss the latter.

10.3. Green's theorem.

Theorem 10.9 (Green)**.** *Let $\theta\colon \overline{F}_q^\times \to \mathbb{C}^\times$ be a character (not necessarily injective). Let $S(x_1,\ldots,x_n)$ be a symmetric polynomial with integer coefficients. Let G be some finite group and $\pi\colon G \to \mathrm{GL}(n,\mathbb{F}_q)$ a representation, and $\sigma(g) = S(\theta(\alpha_1),\ldots,\theta(\alpha_n))$ where g has eigenvalues $\alpha_1,\ldots,\alpha_n$. Then σ is a generalized character.*

In particular, if (π, V) is a representation of G over $\mathbb{F}_p$, then the map

$$g \mapsto \sum_{\text{eigenvalues } \alpha_i} \theta(\alpha_i)$$

(which we called a Brauer character when θ was injective) is a generalized character

We'll need to use Brauer's theorem for the proof - see the paper of Brauer and Tate.

Definition 10.10. If ℓ is a prime and E is a direct product of an ℓ-group and a cyclic group, then E is called *ℓ-elementary.*

Theorem 10.11 (Brauer Theorem 1)**.** *If σ is a class function on G and $\sigma|_E$ is a generalized character for every elementary subgroup $E < G$, then σ is a generalized character.*

Theorem 10.12 (Brauer Theorem 2)**.** *Any generalized character is a linear combination of characters induced from one-dimensional representations of elementary subgroups.*

One of the great original applications of this second result was:

Corollary 10.13. *Artin L-functions are meromorphic.*

Proof of Green's Theorem. It is sufficient to assume that θ is injective. Indeed, suppose it is known for an injective character θ_1. Suppose $\mathbb{F}_{q^N}$ is sufficiently large to contain the eigenvalues of $\pi(g)$ for all $g \in G$. Given θ,

$$\theta|_{\mathbb{F}_{q^N}^\times} = \theta_1^r$$

for some r since $\mathbb{F}_{q^n}^\times$ is cyclic. Replacing $S(x_1, \ldots, x_n)$ by $S(x_1^r, \ldots, x_n^r)$ we may work with θ_1. Also, we may work with $S(x_1, \ldots, x_n) = \sum x_i$ because if the theorem is known in this case, then we can replace π by its exterior powers we get the elementary symmetric functions, and these generate the ring of symmetric functions.

So without loss of generality θ is injective and $S(x_1, \ldots, x_n) = \sum x_i$. By Brauer's theorem, we may also assume that G is elementary. (In this case we will find that σ is actually a character, but in general σ is only a generalized character.)

If G is elementary then G is a product of its Sylow subgroups. In particular, $G = P \times H$ where P is a p-group and $p \nmid |H|$. Since $p \nmid |H|$, the Brauer characters of H are ordinary characters.

Let $g = g_p g_H$ where $g_p \in P$ (the p-unipotent part) and $g_H \in H$ (the p-regular part). Then we claim that $\pi(g_p g_H)$ has the same eigenvalues as $\pi(g_H)$. The reason is that over the algebraic closure, we may assume $\pi(g)$ is upper triangular. Then the p-regular part is the usual semisimple part, and the p-unipotent part is the usual unipotent part. So we have that $\sigma(g) = \sigma(g_H)$ is an ordinary character of H. Thus σ factors as

$$\begin{tikzcd} G = P \times H \arrow[r, "p_2"] \arrow[dr, "\sigma"'] & H \arrow[d, "\sigma=\text{ordinary character}"] \\ & \mathbb{C} \end{tikzcd}$$

□

Example 10.14. Let's try to witness Green's Theorem for $\mathrm{GL}(2, \mathbb{F}_q)$. In $\mathrm{GL}(2, \mathbb{F}_q)$ the conjugacy classes are the following:

Type	# of classes	size of class
$\begin{pmatrix} a & \\ & a \end{pmatrix}$	$q-1$	1
$\begin{pmatrix} a & 1 \\ & a \end{pmatrix}$	$q-1$	q^2-1
$\begin{pmatrix} a & \\ & b \end{pmatrix}$ $a \neq b \in \mathbb{F}_q^\times$	$\frac{1}{2}(q-1)(q-2)$	q^2+q
$\begin{pmatrix} \alpha & \\ & \alpha^p \end{pmatrix}$ $\alpha \in \mathbb{F}_{q^2} - \mathbb{F}_q$	$\frac{1}{2}(q^2-q)$	q^2-q

If χ_1, χ_2 are characters of $\mathbb{F}_q^\times$, define $\pi(\chi_1,\chi_2) = \operatorname{Ind}_B^G(\chi_1,\chi_2)$. Let $\chi : \mathbb{F}_{q^2}^\times \to \mathbb{C}^\times$ be a character not factoring through $\mathbb{F}_q^\times$. Then we have the character values:

Type	# classes	class size	$\pi(\chi_1,\chi_2)$	$\pi(\chi)$
$\begin{pmatrix} a & \\ & a \end{pmatrix}$	$q-1$	1		
$\begin{pmatrix} a & 1 \\ & a \end{pmatrix}$	$q-1$	q^2-1		
$\begin{pmatrix} a & \\ & b \end{pmatrix}$ $a \neq b \in \mathbb{F}_q^\times$	$\binom{q-1}{2}$	q^2+q	$\chi_1(a)\chi_2(b)$ $+\chi_2(b)\chi_1(a)$	0
$\begin{pmatrix} \alpha & \\ & \alpha^p \end{pmatrix}$ $\alpha \in \mathbb{F}_{q^2} - \mathbb{F}_q$	$\frac{1}{2}(q^2-q)$	q^2-q	0	$-\chi(\alpha)-\chi(\alpha^p)$

We extend $\chi : \mathbb{F}_{q^2}^\times \to \mathbb{C}^\times$ to a character $\theta : \overline{\mathbb{F}_q}^\times \to \mathbb{C}^\times$ (so $\theta = \chi$ on $\mathbb{F}_{q^2}$).

Now we apply Green's theorem to the standard 2-dimensional representation of $\mathrm{GL}_2(\mathbb{F}_p)$, to obtain a character σ. We'll show that $\langle \sigma, \sigma \rangle = 2$.

Type	# classes	class size	$\pi(\chi_1,\chi_2)$	$\pi(\chi)$	σ
$\begin{pmatrix} a & \\ & a \end{pmatrix}$	$q-1$	1			$2\theta(a)$
$\begin{pmatrix} a & 1 \\ & a \end{pmatrix}$	$q-1$	q^2-1			$2\theta(a)$
$\begin{pmatrix} a & \\ & b \end{pmatrix}$ $a \neq b \in \mathbb{F}_q^\times$	$\binom{q-1}{2}$	q^2+q	$\chi_1(a)\chi_2(b)$ $+\chi_2(b)\chi_1(a)$	0	$\theta(a)+\theta(b)$
$\begin{pmatrix} \alpha & \\ & \alpha^p \end{pmatrix}$	$\frac{1}{2}(q^2-q)$	q^2-q	0	$-\chi(\alpha)-\chi(\alpha^p)$	$\theta(\alpha)+\theta(\alpha^p)$

So what we would like to do is explicitly write down a linear combination of the characters for π and $\pi(\chi_1,\chi_2)$ that looks like σ. It should look like a principal series minus cuspidal. The calculation $\langle \sigma, \sigma \rangle = 2$ will suggest that there are two characters involved. However, we will use a trick to avoid computation.

We have

$$\langle \sigma, \sigma \rangle = \frac{1}{|G|} \sum_{g \in G} |\sigma(g)|^2.$$

Now the possible values for $|\sigma(g)|^2$ are:

Type	# classes	class size	$\lvert\sigma\rvert^2$
$\begin{pmatrix} a & \\ & a \end{pmatrix}$	$q-1$	1	4
$\begin{pmatrix} a & 1 \\ & a \end{pmatrix}$	$q-1$	q^2-1	4
$\begin{pmatrix} a & \\ & b \end{pmatrix}$ $a \neq b \in \mathbb{F}_q^\times$	$\binom{q}{2}$	q^2+q	$2+\theta(a/b)+\theta(b/a)$
$\begin{pmatrix} \alpha & \\ & \alpha^p \end{pmatrix}$ $\alpha \in \mathbb{F}_{q^2} - \mathbb{F}_q$	$\frac{1}{2}(q^2-q)$	q^2-q	$2+\theta(\alpha^{p-1})+\theta(\alpha^{1-p})$

This makes it clear that $\frac{1}{|G|}\sum_{g \in G} |\sigma(g)|^2$ is a polynomial in q. Therefore, to evaluate it we may let $q \to \infty$.

(1) The sum of $|\sigma|^2$ over the first row (central elements) is $O(q-1)$.
(2) The sum over the second row is $O(q^3)$.
(3) The sum over the third row is $q^4 + O(q^3)$.
(4) The sum over the last row is again $q^4 + O(q^3)$.

Since $|G| = q^4 + O(q^3)$, this tells us that $\langle\sigma,\sigma\rangle = 2 + O(1/q) = 2$ for all suffiicently large q.

Now one has to argue further that the difference of the two characters is actually the σ we want.

Example 10.15. The ordinary representation teory of SL(2) is similar to that of GL(2), but there are more conjugacy classes. If $a = \pm 1$, then the conjugacy class of $\begin{pmatrix} a & 1 \\ & a \end{pmatrix}$ splits into two upon restriction to SL(2) (because $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \not\sim \begin{pmatrix} 1 & \epsilon \\ & 1 \end{pmatrix}$ if ϵ is not a square). The $q+1$-dimensional irreducible splits into two irreducibles, with dimensions $\frac{1}{2}(q+1)$ each. The $q-1$-dimensional irreducibles splits into two irreducibles with dimension $\frac{1}{2}(q-1)$ each.

10.4. SL_2 **and the Brauer graph.** We're going to investigate an interesting relationship between the complex representation theory of $\mathrm{SL}_2(\mathbb{F}_q)$ and its modular (characteristic p) representation theory, which will be encoded by the "Brauer graph."

The modular representation theory of algebraic groups is quite similar to that of the corresponding Lie groups. In the case of $\mathrm{SL}(2,\mathbb{C})$ or more generally $G(\mathbb{C})$ where G is a semisimple algebraic group, the irreducible representations are parametrized by *dominant weights*.

If $G = \mathrm{SL}(2,\mathbb{C})$, the *maximal torus* is $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$. We denote by $X^\bullet(T)$ and $X_\bullet(T)$ the *character* and *cocharacter* groups, which are both isomorphic to $\mathbb{Z}$ in this case. The elements of $X^\bullet(T) =: \Lambda$ are called *weights*. With the convention that λ_a is the weight

$$\lambda_a \begin{pmatrix} a & \\ & a \end{pmatrix} = t^a,$$

a dominant weight is one with $a \geq 0$.

There is a partial order on Λ given by $\lambda_a \geq \lambda_b$ if $a > b$. Given a representation π, restriction to T induces a decomposition

$$\pi|_T = \bigoplus_{\mu\in\Lambda} m_\mu \mu.$$

The set of μ such that $m_\mu \neq 0$ are called the *weights*. For irreducible π, there is a unique *highest* weight (this weight λ is dominant with $m_\lambda = 1$), which gives a bijection between irreducible representations and dominant weights. In particular, the dominant weight $k > 0$ for $\mathrm{SL}(2,\mathbb{C})$ corresponds to the irreducible representation $\pi_k := \mathrm{Sym}^k(\mathbb{C}^2)$.

We're going to try to convey the picture in the modular case, without proving all the facts yet. Let $G = \mathrm{SL}(2,\mathbb{F}_q)$. We set $S_k = \mathrm{Sym}^{k-1}\mathbb{F}_q^2$. The eigenvalues of the element of $\mathrm{SL}(2,\mathbb{F}_p)$ conjugate (over an extension) to $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix}$ for $\alpha \in \mathbb{F}_{q^2} - \mathbb{F}_p$ are $\alpha^{k-1}, \alpha^{k-3}, \ldots, \alpha^{1-k}$. If $\theta : \overline{\mathbb{F}_q} \to \mathbb{C}^\times$ is the injective character used to make Brauer characters, then the Brauer character of S_k is

$$\phi_k(g) = \theta(\alpha)^{k-1} + \theta(\alpha^{k-3}) + \ldots + \theta(\alpha)^{1-k}.$$

Theorem 10.16. *If $k \leq p$, then S_k is irreducible.*

Proof. We basically want to imitate the usual Lie algebra proof. Extend the representation to a representation of $\mathrm{Mat}_2(\mathbb{F}_q)$ in the obvious way, and denote

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Suppose $x = (1,0)$ and $y = (0,1)$ is a basis of k^2. Let

$$\begin{aligned} v_{k-1} &= x \vee \ldots \vee x \\ v_{k-3} &= x \vee \ldots \vee x \vee y = (\vee^{k-2} x) \vee y, \\ \vdots &= \qquad\qquad \vdots \\ v_{k-1-2r} &= (\vee^{k-1-r} x) \vee (\vee^r y) \end{aligned}$$

Now you can check that (as usual) e and f are shifts:

$$\begin{aligned} e(y) &= x \\ e(x) &= 0 \\ f(y) &= 0 \\ f(x) &= y \end{aligned}$$

So (up to constants) repeated applications of e take $v_{1-k} \mapsto v_{3-k} \mapsto \ldots$. The key point is that in characteristic p, the chain breaks off at $k = p$! This is easy to see: in $\vee^p y$, there are p different ways of changing y to x, so the coefficient of $e^p(\vee^p y)$ will be divisible by p.

So we have

$$e(\sum c_m v_m) \sim \sum_{m+2 \leq k-1} c_m v_{m+2}$$

If m is the smallest integer such that $c_m \neq 0$, then $e^r(\ldots) = c_m v_{k-1}$. This means that any non-zero submodule contains v_{k-1}. Therefore, applying f shows that it contains all basis vectors, so any non-zero submodule is the full space. That shows irreducibility as an $M_2(\mathbb{F}_p)$-module.

To argue for irreducibility as an $\mathrm{SL}_2(\mathbb{F}_p)$-module, we try to imitate the exponential map. Fortunately, in this case we have $\exp(e), \exp(f) \in \mathrm{SL}_2(\mathbb{F}_p)$ and $\exp(e) - I = e$, $\exp(f) - I = f$. $\square$

Now let's try to unravel the complex representation theory of $\mathrm{SL}(2, \mathbb{F}_q)$. There are $q+4$ conjugacy classes, of which q are p-regular. The $q+4$ irreducible complex representations are comprised of:

- one trivial representation
- two of dimension $\frac{1}{2}(q-1)$ (half-cuspidal),
- two of dimension $\frac{1}{2}(q+1)$ (half-principal series),
- about $q/2$ of dimension $q-1$ (cuspidal),
- one of dimension q (Steinberg), and
- about $q/2$ of dimension $q+1$ (principal series).

Type	# Classes	Class size
$\pm\begin{pmatrix}1 & \\ & 1\end{pmatrix}$	2	1
$\pm\begin{pmatrix}1 & \epsilon \\ & 1\end{pmatrix}$	$2(q-1)$	$2q$
$\begin{pmatrix}t & \\ & t^{-1}\end{pmatrix}, t\in\mathbb{F}_q^\times, t\neq\pm1$	$\frac{1}{2}(q-3)$	
$\begin{pmatrix}\alpha & \\ & \alpha^p\end{pmatrix}, \alpha\in\mathbb{F}_{q^2}-\mathbb{F}_q, N(\alpha)=1$	$\frac{1}{2}(q-1)$	

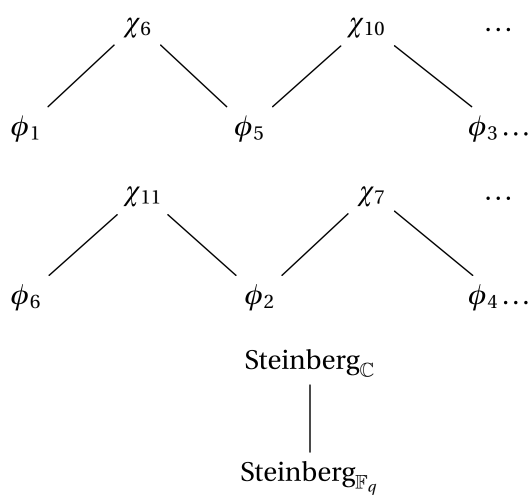
This looks a lot like the theory for $\mathrm{GL}(2,\mathbb{Q}_p)$, except in that case there are infinitely many interesting infinite-dimensional representations.

Definition 10.17. The *Brauer graph* is a graph whose vertices are labelled by the $\{\chi_i\}$ and $\{\phi_j\}$, with the vertices corresponding to χ_i and ϕ_j connected if $d_{ij}\neq 0$.

Proposition 10.18. *The connected components of the Brauer graph of G are precisely the blocks.*

Proof. ♠♠♠ TONY: [TODO] □

Now let's study the Brauer graph. We claim that there are at least three different blocks. If $i\neq j \pmod 2$, then ϕ_i and ϕ_j must lie in different blocks, because $\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$ acts by -1 on $\mathrm{Sym}^{k-1}(\mathbb{F}_q^2)$ if k is even and $+1$ if k is odd. Recall that each block corresponds to one homomorphism $Z(k[G])\to k$. The third component consists of the two Steinberg representations. So the graph looks like



You can compute all this using the decomposition matrix.

In general, for $\mathrm{SL}_2(\mathbb{F}_p)$ the graph is roughly described as follows. By the CDE triangle,

$$c_{ij}=\sum_k d_{ik}d_{jk}$$

is the multiplicity of ϕ_i in η_j. If $d_{ki} \neq 0$ and $d_{kj} \neq 0$, then one will have

$$\begin{tikzcd} & \chi_k \arrow[dl, dash] \arrow[dr, dash] & \\ \phi_i & & \phi_j \end{tikzcd}$$

It turns out that ϕ_i is adjacent to ϕ_{p-1-i} and ϕ_{p+1-i} *except* if $i = 1$ or $p - 1$, in which case one of these doesn't exist. In the middle, i.e. $i = \frac{p-1}{2}, \frac{p+1}{2}$ then we get a self-adjacency. What is the significance of this?

11. The Green Correspondence

11.1. **Review of extensions.**

Definition 11.1. Let M and N be G-modules. An *extension of M by N* is a module E fitting into a short exact sequence

$$E\colon 0 \to N \to E \to M \to 0.$$

We say that $E \equiv E'$ if there exists a G-homomorphism $E \to E'$ making the diagram commute

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d, dotted] & M \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & N \arrow[r] & E' \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

Given G-modules M, N, there is a group structure on the set of equivalence classes of extensions of M by N, which will now be explained.

Choose a projective resolution of M, or more generally just a short exact sequence

$$0 \to Q \to P \to M \to 0$$

where P is projective. Then we get an exact sequence

$$0 \to \mathrm{Hom}(M,N) \to \mathrm{Hom}(P,N) \xrightarrow{i^*} \mathrm{Hom}(Q,N) \to \mathrm{Ext}(M,N).$$

Define Ext to be $\mathrm{Hom}(Q,N)/i^*\mathrm{Hom}(P,N)$, so the above fits into

$$0 \to \mathrm{Hom}(M,N) \to \mathrm{Hom}(P,N) \xrightarrow{i^*} \mathrm{Hom}(Q,N) \to \mathrm{Ext}(M,N)$$

(this can be continued further, but that is not important for us). You can prove that this does not depend on the choice of resolution, using the lifting property for projective modules.

We claim that $\mathrm{Ext}(M,N)$ is in bijection with extensions. Given an extension, the projectivity implies that we can find lifts

$$\begin{tikzcd} 0 \arrow[r] & Q \arrow[r] \arrow[d, "g"'] & P \arrow[r] \arrow[d, "f"'] & M \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & N \arrow[r, "\alpha"'] & E \arrow[r, "\theta"'] & M \arrow[r] & 0 \end{tikzcd}$$

Then $g \in \mathrm{Hom}(Q,N)$ and we claim that the image of $[g]$ in $\mathrm{Ext}(M,N)$ doesn't depend on the choice of f. Indeed, if f and f' are two maps inducing the identity on M, then $\theta(f - f') = 0$ so $f - f'$ has image in $\mathrm{Im}(\alpha) = \ker(\theta)$. Thus $f - f' = \alpha \circ t$ for some $t \in \mathrm{Hom}(P,N)$, i.e. $f - f' \in \mathrm{Im}(i^*)$.

If S, S' are simple then $\mathrm{Ext}(S,S') \neq 0 \implies S, S'$ lie in the same block. Conversely, if S_1, S_2 are in the same block then we can find $S'' = T_1, \ldots, T_n = S_2$ such that either $\mathrm{Ext}(T_i, T_{i+1}) \neq 0$ or $\mathrm{Ext}(T_{i+1}, T_i) \neq 0$. We'll prove this later. The point is that Ext groups detect blocks.

11.2. **Special case of trivial intersections.** Suppose $P < G$ is a p-Sylow subgroup, and if $x \in G - N(P)$ then $xPx^{-1} \cap P = \{1\}$, i.e. for any two p-Sylows P and P' we have $P \cap P' = 1$ or P. This is satisfied for instance when $G = \mathrm{SL}_2(\mathbb{F}_q)$. Let $L = N(P)$.

Theorem 11.2 (Green, special case)**.** *There exists a bijection*

$$\left\{\begin{matrix}\textit{non-projective}\\ \textit{indecomposables}\\ \textit{of } G\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\textit{non-projective}\\ \textit{indecomposables}\\ \textit{of } L\end{matrix}\right\}$$

If $U \longleftrightarrow V$ under this bijection, then $V^G \cong U \oplus X$ where X is projective for G, and $U|_L \cong V \oplus Y$ where Y is projective for L.

Proof. The statement of the theorem makes it clear how to construct the bijection. If U is a non-projective indecomposable of G, then we should consider $U|_L$ and split off a non-projetive indecomposable. Similarly, if V is a non-projective indecomposable of L, then we should consider V^G and split off a non-projective indecomposable of G.

We will need the following useful result.

Lemma 11.3. *Suppose $[G : H]$ is prime to p and U is a G-module such that $U|_H$ is projective. Then U is projective.*

Proof. We have a diagram

$$\begin{tikzcd} & U \arrow[d, "g"] \arrow[dl, dotted, "\theta"'] & \\ M \arrow[r, "f"'] & N \arrow[r] & 0 \end{tikzcd}$$

We want to show that there exists $\theta : U \to M$ with $f \circ \theta = g$. We know that there exists θ_1 that is an H-module homomorphism, as U is projective over H. Then we define

$$\theta(u) = \frac{1}{[G:H]} \sum_{s \in G/H} s\theta_1(s^{-1}u).$$

It is easily checked that this is a G-module homomorphism that does the job. $\square$

Let V be a non-projective indecomposable for L. By Mackey theory,

$$(V^G)_L = \bigoplus_{s \in L\backslash G/L} \mathrm{Ind}^L_{L \cap sLs^{-1}}({}^{(s)}(V)).$$

We claim that if $s \neq 1$, then $\mathrm{Ind}^L_{L\cap sLs^{-1}}(s(V))$ is projective. The key point is that $L \cap sLs^{-1}$ does not contain any subgroup of order p. (P is the only sylow in L, and $sPs^{-1} \cap P = 1$ by assumption.) Since $p \nmid L \cap sLs^{-1}$, *all* modules are projective for $k[L \cap sLs^{-1}]$ (by Maschke's theorem), and induction preserves projectives (since projectivity has to do with exactness of mapping out, and this is controlled by Frobenius reciprocity).

Now if we break up V^G into a direct sum of indecomposables

$$V^G = U_1 \oplus U_2 \oplus \dots \quad \text{(indecomposables)}$$

then we have

$$V^G|_L \cong (U_1)|_L \oplus (U_2)|_L \oplus \dots$$

but also by Mackey theory

$$V^G|_L \cong V \oplus (\text{projective}).$$

This means that exactly one $(U_i)|_L$ has V as a summand and all the others are projective L-modules (hence projective G-modules, by the Lemma). Without loss of generality, we may re-index the summands so that $U_1|_L$ contains V. We know by this discussion that $U_1|_L \cong V \oplus (\text{projective})$. Also, since the restriction of projective is projective (as $k[G]$ is a free $k[H]$-module), we know that U_1 is non-projective for G. □

Proposition 11.4. *If U, U' are G-modules and V, V' are L-modules such that $U \longleftrightarrow V$ and $U' \longleftrightarrow V'$ under the Green correspondence, then*

$$\operatorname{Ext}_{k[G]}(U, U') \cong \operatorname{Ext}_{k[L]}(V, V').$$

Proof. Write

$$\begin{aligned} U|_L &\cong V \oplus Y \\ V^G &\cong U \oplus X \\ U'|_L &\cong V' \oplus Y' \\ (V')^G &\cong U' \oplus X' \end{aligned}$$

Then X, X' are projective G-modules and Y, Y' are projective L-modules, as ensured by the Green correspondence.

Note that if P is projective for $k[G]$, then $\operatorname{Ext}(P, -) = 0$, and also $\operatorname{Ext}(-, P) = 0$ because projectives are automatically also injectives for $k[G]$ by duality.

Choose a resolution

$$0 \to Q \to P \to V \to 0$$

for V where P is projective over L. Then

$$0 \to Q^G \to P^G \to V^G \to 0$$

is a resolution of V^G with P^G projective. The sequence defining $\operatorname{Ext}_{k[L]}(V, V')$ is

$$0 \to \operatorname{Hom}_{k[L]}(V, V') \to \operatorname{Hom}_{k[L]}(P, U') \to \operatorname{Hom}_{k[L]}(Q, U') \to \operatorname{Ext}_{k[L]}(V, V').$$

However, since $U'|_L \cong V' \oplus (\text{projective})$, and projectives being injectives have no higher Ext groups, we can also compute $\operatorname{Ext}_{k[L]}(V, V')$ by using $U'|_L$ in place of V'. Similarly, we can compute $\operatorname{Ext}_{k[G]}(U, U')$ by using $(V')^G$ in place of U'. We then relate these two using Frobenius reciprocity:

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}_{k[L]}(V, U') \arrow[r] \arrow[d, "\cong"'] & \operatorname{Hom}_{k[L]}(P, U') \arrow[r] \arrow[d, "\cong"'] & \operatorname{Hom}_{k[L]}(Q, U') \arrow[r] \arrow[d, "\cong"'] & \operatorname{Ext}_{k[L]}(V, U') \arrow[d, "\cong"'] \\ 0 \arrow[r] & \operatorname{Hom}_{k[G]}(V^G, U') \arrow[r] & \operatorname{Hom}_{k[G]}(P^G, U') \arrow[r] & \operatorname{Hom}_{k[G]}(Q^G, U') \arrow[r] & \operatorname{Ext}_{k[G]}(V^G, U') \end{tikzcd}$$

□

Example 11.5. Let $G = \mathrm{SL}(2, \mathbb{F}_q)$. Then a p-Sylow subgroup is $P = \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$ and its normalizer is the Borel subgroup B. This satisfies the hypothesis of (our version of) the Green correspondence, so we should get a bijection between non-projective indecomposables of P and non-projective indecomposables of B. That means that we can study representations of B to get information about G.

Consider $V = V_\lambda \oplus V_{\lambda-2} \oplus \ldots \oplus V_{\lambda-2k}$, which we found was an irreducible representation of G by studying the maps e and f, which raised and decreased the weights, respectively. When we restrict to a representation of B, we retain only the action of e (via the exponential map).

♠♠♠ TONY: [this was not done clearly (at least that I recorded), both seem to be projective indecomposables?]

12. Back to Blocks

Let $A = k[G]$. We proved that there is a *unique* decomposition

$$A = \bigoplus B_i, \quad B_i \text{ indecomposable 2-sided ideal.}$$

The B_i are called *blocks*. Write

$$1 = \sum e_i$$

where the $e_i \in B_i$ are orthogonal idempotents (the units of the B_i considered as rings). We say that an A-module M "belongs to B_i" if $e_i M = M$ and $e_j M = 0$ for $j \neq i$. We also proved that $Z(B_i)$ has a unique k-algebra homomorphism $\omega_i : Z(B_i) \to k$. We can now give more characterizations of blocks.

Theorem 12.1. *The following four equivalence relations on simple modules are the same.*

(1) $M \sim M'$ if M, M' belong to the same block.
(2) $M \sim M'$ if M, M' are composition factors in the same indecomposable projective.
(3) $M \sim M'$ if $\mathrm{Ext}(M, M') \neq 0$
(4) $M \sim M'$ if M, M' admit the same "central character."

Proof. First, we make some observations concerning the interplay between projective indecomposables and blocks. We claim that every projective indecomposable for A appears as a summand of some B_i.

Let P be a projective indecomposable of A. Then the A-endomorphisms P are local, so in particular the idempotents e_i act invertibly or nilpotently on P. But nilpotent idempotents are 0. Since $\sum e_i = 1$, some e_i acts invertibly. If e_i and e_j both act invertibly, then so does $e_i \cdot e_j$, but that is 0. So P is associated to a unique block.

(2) $\implies$ (1). This is clear from the preceding discussion.

(1) $\implies$ (2). Suppose S is a simple module for A belonging to the block B according to (1). Then we may decompose

$$B = \underbrace{P_1 \oplus P_2 \oplus \ldots}_{P} \oplus Q$$

where the P_i are the projective indecomposables whose composition factors are equivalent to S according to (2), and and Q is the direct sum of the remaining projective indecomposables for B. It suffices to show that $Q = 0$. By definition, $P = \bigoplus_i P_i$ and Q have no composition factors in common, hence $\mathrm{Hom}(P, Q) = 0$.

We produce a contradiction by showing that P and Q are two-sided ideals. Since P is closed under left multiplication by definition, it suffices to show that it is closed under right multiplication. If $\alpha \in A$, then right translation followed by projection to Q is in $\mathrm{Hom}(P, Q)$, hence 0. Therefore, $P\alpha \subset P$. Thus P is a 2-sided ideal, and similarly so is Q, which gives a contradiction.

(3) $\implies$ (2). Suppose $\mathrm{Ext}(M, M') \neq 0$, so we have a non-split extension

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

If we let P be the projective envelope of M, then it has a lift to E:

$$\begin{tikzcd} & & P \arrow[d, dotted, "f"'] \arrow[dr] & & \\ 0 \arrow[r] & M' \arrow[r] & E \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

We claim that f is surjective. If not, then $f(P) \cap M' = 0$ (because M' is simple and $f(P) \cap M'$ must be proper, as otherwise it surjects to M' and M). But that would imply $f(P) \cong M$, and the isomorphism would split the short exact sequence.

Therefore, E is a quotient of P, so M' is a composition factor of P, hence $M \sim M'$ via (2)'s equivalence relation.

(2) $\implies$ (3): It suffices to show that if P is a projective indecomposable with $P/\operatorname{Rad}(P) = M$, and W is a composition factor of P, then $W \sim M$ with respect to the Ext equivalence relation. (In other words, we reduce to the case where one of the modules is at the "top" of the composition series).

Lemma 12.2. *Suppose M is not semisimple, but $\operatorname{Rad}(M)$ is semisimple. If W is a composition factor of $\operatorname{Rad}(M)$, then $\operatorname{Ext}(U, W) \neq 0$ for some composition factor U of $M/\operatorname{Rad}(M)$.*

Proof. We may assume without loss of generality that $W = \operatorname{Rad}(M)$, since if $\operatorname{Rad}(M) = W \oplus W'$ then by passing to M/W', we can arrange this to be the case. So we have

$$0 \to W = \operatorname{Rad}(M) \to M \to M/\operatorname{Rad}(M) \to 0$$

which does not split, as M is not semisimple. Therefore, $\operatorname{Ext}(M/\operatorname{Rad}(M), W) \neq 0$. But as $M/\operatorname{Rad}(M) \cong \bigoplus U_i$, we have

$$\operatorname{Ext}(M/\operatorname{Rad}(M), W) \cong \bigoplus \operatorname{Ext}(U_i, W)$$

so $\operatorname{Ext}(U_i, W) \neq 0$ for some summand U_i of $M/\operatorname{Rad}(M)$.

□

If $M_i = \operatorname{Rad}^i(P)$, then we have

$$P = M_0 \supset M_1 \supset \ldots \supset M_n = 0$$

and $M_0/M_1 = P/\operatorname{Rad}(P) \cong M$. By assumption, W is some composition factor of M_i/M_{i+1} for some i. If $i = 0$ then $M = W$ and there is nothing to show; if $i > 0$, then we have

$$\begin{tikzcd} M_{i-1} \arrow[d, dash] \\ M_i \arrow[d, dash, "W"'] \\ M_{i+1} \end{tikzcd}$$

By the Lemma applied to M_{i-1}/M_{i+1}, W is related (via the Ext relation) to some composition factor U of M_{i-1}/M_i. In this way we can keep "going up the ladder," until $i = 0$.

(1) − (3) $\iff$ (4). If M is simple, then by Schur's lemma $Z(A) = \bigoplus_i Z(B_i)$ acts on M by scalars, i.e. via a homomorphism $\omega_M : Z \to k$ determined by $z \cdot m = \omega_M(z) \cdot m$. Since $e_j \in Z(B_j)$, M belongs to B_i if and only if ω_M is the unique character $Z(A) \to k$ killing e_j for $e_j \neq i$. $\square$

Example 12.3. We now explain why every irreducible characteristic 0 representation is associated with a unique block. This boils down to "block decomposition of the Cartan matrix."

We have the CDE diagram

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

Let $\{P_i\}$ be the projective indecomposables for $k[G]$, $\{V_k\}$ the irreducibles for $K[G]$, and $\{S_j\}$ the simple modules for $k[G]$. Then we know that

$$c[P_i] = \sum_j c_{ij} S_j$$

$$d[P_i] = \sum_k d_{ik} V_k$$

$$e[V_k] = \sum_j d_{kj} S_j$$

There would be a natural assignment of block to V_k if all the S_j for which d_{kj} were non-zero belonged to a single block. Is this the case? Suppose that $d_{kj} \neq 0$. We want to show that if S_j and $S_{j'}$ are in different blocks, then $d_{kj'} = 0$.

We now know that the projective indecomposables of $k[G]$ are partitioned into blocks in a way compatible with the partitioning of simple modules. In particular, S_j is a composition factor of P_j, so $S_{j'}$ is not, i.e. $c_{jj'} = 0$. But we know that

$$c_{jj'} = \sum_k d_{kj} d_{kj'}$$

with all the d_{kj} non-negative, which is a contradiction.

13. Character Theory

13.1. **The central character.** Let $K = \mathbb{C}$, or a sufficiently large (i.e. splitting) field in characteristic 0. Throughout, let (π, V) be an irreducible module for G. Then $Z(G)$ (the center of G) acts by scalars on V by Schur's Lemma. Similarly, the center of the group algebra $Z := Z(k[G])$ acts by scalars, so there is a k-algebra homomorphism $\omega\colon Z \to K$ such that $\omega(z)\cdot v = \omega(z)v$. This is called the *central character* of (π, V).

If $\mathscr{C}_1, \dots, \mathscr{C}_h$ are the conjugacy classes of G, then the $c_i := \sum_{x\in\mathscr{C}_i} x$ for $i = 1, \dots, h$ form a basis for Z. We have

Lemma 13.1. *For $g \in \mathscr{C}_i$, we have*

$$\omega(c_i) = \frac{|\mathscr{C}_i|\chi(g)}{\chi(1)}$$

and this value is an algebraic integer.

Proof. We know that $c_i\colon V \to V$ acts as the scalar $\omega(c_i)$, so the trace of c_i is $\chi(1)\omega(c_i)$. On the other hand, it is evidently equal to $|\mathscr{C}_i|\chi_i(g)$. Comparing these formulas immediately yields the claimed quality.

For algebraicity, write

$$c_i c_j = \sum_k a_{ijk} c_k$$

for some $a_{ijk} \in \mathbb{Z}$. Then applying ω, we have

$$\omega(c_i)\omega(c_j) = \sum_k a_{ijk}\omega(c_k). \tag{4}$$

Therefore, the $\mathbb{Z}$-module spanned by the $\omega(c_i)$ is finitely generated and and faithful and invariant under multiplication by $\omega(c_j)$. Therefore, the $\omega(c_j)$ are algebraic. □

Corollary 13.2. *If χ is the character of an irreducible representation of (π, V) of G, then $\chi(1) \mid |G|$.*

Proof. By the orthogonality of characters, we have

$$|G| = \sum_i |\mathscr{C}_i|\chi(g_i)\overline{\chi(g_i)}$$

where g_i is any representative of $\mathscr{C}_i$, so

$$\frac{|G|}{\chi(1)} = \sum \left(\frac{|\mathscr{C}_i|\chi(g_i)}{\chi(1)}\right)\chi(g_i).$$

The left hand side is clearly rational, and the right hand side is algebraic by Lemma 13.1. □

13.2. **Burnside's Theorem.**

Definition 13.3. For a representation (π, V) define the subgroup

$$Z(\pi) = \{g \mid \pi(g) \text{ acts by a scalar}\}.$$

This is a normal subgroup. If χ is the character of a representation π, then we denote $Z(\chi) = Z(\pi)$.

Proposition 13.4 (Burnside). *If* $\gcd(\chi(1), |\mathscr{C}_i|) = 1$*, then for* $g \in \mathscr{C}_i$ *we have either*

(1) $\chi(g) = 0$ *or*
(2) $|\chi(g)| = \chi(1)$ *and* $g \in Z(\chi)$.

Proof. By hypothesis, there are integers a, b such that

$$a\chi(1) + b|\mathscr{C}_i| = 1.$$

Then we multiply by $\frac{\chi(g)}{\chi(1)}$ to get

$$a\chi(g) + b\frac{\chi(g)}{\chi(1)}|\mathscr{C}_i| = \frac{\chi(g)}{\chi(1)}.$$

The left hand side is manifestly an algebraic integer by Lemma 13.1. The norm of the right hand side down to $\mathbb{Q}$ is the product over conjugates of $\chi(g)/\chi(1)$, and each has norm at most 1 since $\chi(g)$ is a sum of $\chi(1)$ roots of unity. Theefore, the norm of $\chi(g)/\chi(1)$ down to $\mathbb{Q}$ is a rational integer with absolute value at most 1, hence either 0 or ± 1.

If it's 0, then we are in the first case. If it's 1, then the eigenvalues of $\pi(g)$ all have absolute value 1 and their sum has absolute value $\chi(1)$, so they must all be equal. ☐

Theorem 13.5 (Burnside). *If* G *is a non-abelian simple group and* $\mathscr{C} \subset G$ *is a conjugacy class with* $|\mathscr{C}| = p^k$*, then* $C = \{1\}$.

Proof. By the orthogonality relations for characters, we have

$$0 = \sum_{\chi} \chi(1)\chi(g) = 1 + \sum_{\chi \neq 1} \chi(1)\chi(g). \tag{5}$$

For non-trivial χ, we claim that $\chi(g) = 0$ unless $p \mid \chi(1)$. Indeed, if $p \nmid \chi(1)$ then $(|\mathscr{C}|, \chi(1)) = 1$, so Proposition 13.4 implies that $\chi(g) = 0$ or $g \in Z(\chi)$. But $Z(\chi)$ is a normal subgroup of G, hence trivial or all of $|G|$ because G is simple, and the latter case is ruled out for non-trivial irreducible representations because G is non-abelian. (Since G is simple and χ corresponds to a non-trivial irreducible representation π, we have that π is a faithful representation.)

This means that

$$p \mid \sum_{\chi \neq 1} \chi(1)\chi(g)$$

hence $p \mid 1$ by (5), which is absurd. ☐

Theorem 13.6 (Burnside). *If* $|G| = p^a q^b$ *with* $a, b > 0$*, then* G *is not a non-abelian simple group.*

Proof. Let $P < G$ be a p-Sylow subgroup, and take a non-identity element $g \in Z(P)$ (which exists by the standard orbit-stabilizer argument for the conjugation action on P). Let $\mathscr{C}$ be the conjugacy class of g. Then by orbit-stabilizer, we have

$$|\mathscr{C}| = [G : C(g)]$$

By definition $C(g) \supset P$, so $\#\mathscr{C} \mid [G : Z(P)] = q^b$. By Theorem 13.5, $\mathscr{C}$ has size 1, but a simple group cannot have non-trivial center. ☐

13.3. **Blocks.** Let (π, V) be an irreducible representation with character χ over a local field K with residue field k of characteristic p. We have an associated central character $\omega_\chi : Z(K[G]) \to K$ defined by

$$\omega_\chi(C) = \frac{\chi(1)|C|}{\chi(g)}$$

where C is the sum of the conjugates of g, considered as an element of the group algebra. If χ and χ' lie in the same block then they have the same central character, as $K[G] \cong \bigoplus A_i$ and each A_i admits a unique K-algebra homomorphism to K.

Because $\omega_\chi(C)$ is an algebraic integer, it lies in the valuation ring R of K. We can reduce modulo p to get a character of $Z(k[G])$, which is spanned by the reduction $\overline{C}$ of C to k.

Let $\overline{\pi}$ be the image of the representation π under the map

$$d : K[G] - \mathbf{Mod} \to k[G] - \mathbf{Mod}.$$

Then that $\overline{\omega_\chi}$ is the central character attached to the block of $\overline{\pi}$. Indeed, the CDE triangle shows that $\overline{\pi}$ is a sum of simple modules appearing in the composition series of a single projective indecomsable, which by Theorem 12.1 characterizes the blocks. There is a unique k-algebra homomorphism which is non-trivial on exactly one block, and that is the corresponding central character.

Theorem 13.7 (Brauer)**.** *Let G be a non-abelian simple group and χ an irreducible character of G in the principal block. If $\chi(1) = p^k$, then $\chi = 1$.*

Proof. As before, if we take g to be in the center of a p-Sylow subgroup $P < G$, then we have $\#\mathscr{C} = [G : C(g)] \mid [G : P]$, which is coprime to p. Then Burnside's Theorem 13.5 implies that $\chi(g) = 0$ or $g \in Z(\chi)$, but the latter cannot occur since G is non-abelian simple and χ is trivial, so we must have $\chi(g) = 0$.

On the other hand, we have the following general observation. If χ, χ' are in the same block then $\overline{\omega_\chi} = \overline{\omega_{\chi'}}$, so for any conjugacy class $\mathscr{C}$ and any $g \in \mathscr{C}$ we have

$$\frac{|\mathscr{C}|\chi(g)}{\chi(1)} \equiv \frac{|\mathscr{C}|\chi'(g)}{\chi'(1)} \pmod{\mathfrak{m}}.$$

If χ is in the principal block, take $\chi' = 1$. Then we deduce that

$$\frac{|\mathscr{C}|\chi(g)}{\chi(1)} \equiv |\mathscr{C}| \pmod{\mathfrak{m}}.$$

Now take g and $\mathscr{C}$ as before. Recall that we are assuming that $\chi(1)$ is a power of p. This certainly implies that $\chi(1) = p^k$ and $|\mathscr{C}|$ are coprime. Then $|\mathscr{C}|$ is not in the maximal ideal $\mathfrak{m} \subset \mathscr{O}_K$ (as $\mathfrak{m} \cap \mathbb{Z} = p\mathbb{Z}$), so we have a fortiori that $\frac{|\mathscr{C}|\chi(g)}{\chi(1)} \neq 0$ (since it's not even in the maximal ideal), hence $\chi(g) \neq 0$. This is a contradiction. ☐

Theorem 13.8 (Block Orthogonality)**.** *If g and $h \in G$ are such that their p-unipotent parts are not conjugate, then for any block B we have*

$$\sum_{\chi \in B} \chi(g)\overline{\chi(h)} = 0$$

Remark 13.9. This is a refinement of Schur orthogonality, which says that if g, h are not conjugate, then
$$\sum_B \sum_{\chi \in B} \chi(g)\overline{\chi(h)} = 0.$$

We will content ourselves with proving the following special case of block orthogonality:

Proposition 13.10. *If g is p-regular and h is not, then*
$$\sum_{\chi \in B} \chi(g)\overline{\chi(h)} = 0.$$

Proof. Denote, as usual,

- $\{\eta_i\}$ be the Brauer characters of the projective indecomposable $k[G]$-modules,
- $\{\chi_j\}$ the characters of the irreducible $K[G]$-modules, and
- $\{\phi_i\}$ the Brauer characters of the simple $k[G]$-modules.

Recall the relations of the CDE triangle (2) and (1):
$$\chi_i = \sum_j d_{ij}\phi_j$$
on the p-regular conjugacy classes (ϕ_i is undefined on non p-regular conjugacy classes) and
$$\eta_i = \sum_i d_{ij}\chi_j$$
(η_i is defined and identically zero on the non p-regular conjugacy classes).

Setting $\chi = \chi_i$, we have (with the notation in the hypothesis)
$$\begin{aligned}\sum_{i \in B} \chi_i(g)\chi_i(h) &= \sum_{i,j} d_{ij}\phi_j(g)\chi_i(h)\\ &= \sum_j \phi_j(g)\eta_j(h)\end{aligned}$$
but η_j vanishes off of p-regular elements, and in particular on h.

□

Theorem 13.11. *Let χ be an irreducible character and $P < G$ a Sylow p-group. Suppose that $\#P$ divides $\chi(1)$. Then χ lies in a block by itself (i.e. its reduction mod $\mathfrak{m}$ is projective and irreducible).*

Corollary 13.12. *Under the hypothesis of the preceding theorem, χ vanishes off the p-regular elements.*

Example 13.13. Consider S_4. The character table is

	1	(123)	(12)(34)	(12)	(1234)
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	2	-1	2	0	0
χ_4	3	0	-1	1	-1
χ_5	3	0	-1	-1	1

Take $p = 3$. Noting that $\chi_3 = \phi_1 + \phi_2$, the Brauer characters are

	1	(123)	(12)(34)	(12)	(1234)
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_4	3	0	-1	1	-1
χ_5	3	0	-1	-1	1

(We expect that the number of Brauer characters is the same as the number of 3-regular conjugacy classes, which is consistent.) So the decomposition matrix looks like

	ϕ_1	ϕ_2	ϕ_3	ϕ_4
χ_1	1	0	0	0
χ_2	0	1	0	0
χ_3	1	1	0	0
χ_4	0	0	1	0
χ_5	0	0	0	1

Indeed we see that ϕ_3, ϕ_4 are projective irreducible, implying that each of χ_4, χ_5 comprises its own singleton blocks.

Direct proof of Corollary. Define the class function

$$\theta(g) = \begin{cases} \chi(g) & g\ p\text{-regular,} \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$0 < \frac{1}{|G|} \sum_{g\ p\text{-regular}} |\chi(g)|^2 \leq \frac{1}{|G|} \sum_{g} |\chi(g)|^2 = 1$$

Suppose we know that θ is a generalized character. Then $\langle \theta, \chi \rangle \in \mathbb{Z}$ automatically forces $\langle \theta, \chi \rangle = 1$ and $\chi(g) = 0$ off of the p-regular elements.

The idea is to show that $\langle \theta, \psi \rangle_E \in \mathbb{Z}$ for any elementary subgroup E and any irreducible character ψ of E. This will show that θ is a generalized character of E, and then we can invoke Theorem 10.11.

Let P and Q be Sylow subgroups of coprime orders in E. We'll show that $|P|\langle \theta, \psi \rangle_E \in \mathbb{Z}$ and $\frac{|Q|\cdot|G|}{\chi(1)} \langle \theta, \psi \rangle_E \in \mathbb{Z}$. Since $\frac{|Q|\cdot|G|}{\chi(1)}$ is coprime to $|P|$ by assumption, this shows that $\langle \theta, \psi \rangle_E \in \mathbb{Z}$.

Since Q is the subset of p-regular elements of E, we have $\theta|_E = \psi$ on Q and 0 off of Q. So

$$|P|\langle \theta, \psi \rangle_E = \frac{|P|}{|P||Q|} \sum_{g \in Q} \chi(g) \overline{\psi(g)} = \langle \chi, \psi \rangle_Q \in \mathbb{Z}.$$

Note that this shows that $\langle \theta, \psi \rangle_E$ is rational, and hence $\frac{|Q||G|}{\chi(1)} \langle \theta, \psi \rangle_E$, is rational, so it now suffices to show that it is an algebraic integer. To that end, write

$$\frac{|Q||G|}{\chi(1)} \langle \theta, \psi \rangle_E = \sum_{g \in Q} \frac{|G|}{|P|\chi(1)} \chi(g) \overline{\psi(g)}.$$

If $g \in Q$, then $\frac{[G:C(g)]\chi(g)}{\chi(1)}$ is an algebraic integer by Lemma 13.1. Since $C(g) \supset P$, a fortiori $\frac{[G:P]\chi(g)}{\chi(1)}$ is an algebraic integer too. $\square$

Theorem 13.14. *If G is a non-abelian simple group and $|G| = p^a q^b r$ for distinct primes p, q, and r, then if R is an r-Sylow we have $R = C(R)$.*

Proof. If $C(R) > R$ then G has an element g of order pr or qr. Without loss of generality, let's assume that it is pr. Let B^0 be the principal block modulo p. We have

$$0 = \sum_{\chi \in B^0} \chi(1)\chi(g)$$

so

$$-1 = \sum_{\chi \in B^0, \chi \neq 1} \chi(1)\chi(g).$$

It must be the case that $q \nmid \chi(1)$ and $\chi(g) \neq 0$ for some non-trivial χ. We must have $r \mid \chi(1)$, since otherwise $\chi(1)$ is a power of p but χ is *not* the trivial character, which contradicts Theorem 13.7. But now $|R| = r$ divides $\chi(1)$, so $\chi(g) = 0$ as g is not r-regular. This is again a contradiction.

$\square$

Corollary 13.15. *If G is a non-abelian simple group, and $|G| = 5p^a q^b$ for distinct primes $p, q \neq 5$, then $G = A_5, A_6$, or $SO_5(\mathbb{F}_3)$.*