Introduction to Modular Representation Theory *

Zhiyuan Bai

Compiled on November 30, 2022

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part III course *Introduction to Modular Representation Theory* in Michaelmas 2022. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

Contents

0 Ordinary and Modular Representations

The basic procedure of representation theory is the following: We start off with some algebra A, put into some blackbox, and get some information about A-modules and maps between them.

*Based on the lectures under the same name taught by Prof. S. Martin in Michaelmas 2022.

We'll almost always assume that A is an associative k-algebra for some field k. For example, A could be a matrix algebra with coefficients in k, polynomials in several variables over k, etc.. For our purposes, we are mostly interested in the group algebra kG for a (usually finite) group G. And we study them via their actions on k-vector spaces, and the representations of A-modules corresponds to finite-dimensional k-vector spaces with a linear G-action.
The actions depends critically on the relationship between $|G|$ and $\operatorname{char} k$. Recall that Maschke's theorem says that, provided that $\operatorname{char} k \nmid |G|$, all representations are semisimple, i.e. are direct sums of simple modules. Representation theory in this case is called "ordinary representation theory". When $\operatorname{char} k \mid |G|$, the theory is called "modular representation theory". In this case, kG is not even always a semisimple algebra: We'll show later that, if G is a p-group with $p = \operatorname{char} k$, then kG is a local ring and the only irreducible representation is the trivial one. So, how do we start those?

1 Modules, Representations and Reducibility

All rings are assumed to be unital.
Let G be a finite group and k a commutative ring.

Definition 1.1. A representation of G over k is a group homomorphism $\phi : G \to \mathrm{GL}_n(k)$ for some n (the "degree" of the representation).

For a ring R, we write R^{op} to denote the opposite ring whose underlying set is R and whose multiplication is given by $x \circ y = yx$. In particular, a right R-module M is the same as a left R^{op}-module via $r \cdot a = ar$.

Definition 1.2. For rings R, S, supposed an abelian group M is both a left R-module and a right S-module, then it is called an (R, S)-bimodule if $(rm)s = r(ms)$ for all $r \in R, s \in S, m \in M$.

For example, R is an (R, R)-bimodule.

Definition 1.3. An R-module M is finitely generated if all elements of M can be written as a finite R-linear combination of a prescribed finite subset of M.

Definition 1.4. The group algebra kG is the ring with underlying set consisting of formal linear combinations of elements of G with coefficents in k. The addition is given by pointwise addition and the multiplication is given by

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{g\in G} \beta_g g\right) = \sum_{g\in G}\left(\sum_{hh'=g} \alpha_h \beta_{h'}\right) g$$

One easily checks that this is indeed a k-algebra.

Lemma 1.1. *Every left kG-module gives rise to a unique representation of G over k and vice versa.*

Proof. Well-known. □

Example 1.1. If k is a field, then representations of G over k is the same as finite-dimensional left kG-modules.

Definition 1.5. Two representations ϕ, ψ of G over k with degrees n, m are isomorphic (or equivalent, similar, etc.) if $n = m$ and there is some $X \in \mathrm{GL}_n(k)$ such that $X\phi_g X^{-1} = \psi(g)$ for all $g \in G$. This corresponds to the isomorphism of the corresponding kG-modules.
An intertwining operator from ϕ to ψ is an $n \times m$ matrix X such that $\phi(g)X = X\psi(g)$ for all $g \in G$. This corresponds to a homomorphism between the corresponding kG-modules.

Definition 1.6. A representation $\phi : G \to \mathrm{GL}_n(k)$ is reducible if it is similar to a representation ψ with the property that there is some fixed i for each g, $\psi(g)$ can be written in the block form

$$\psi(g) = \begin{pmatrix} A_{i,i} & B_{n-i,i} \\ 0_{i,n-i} & C_{n-i,n-i} \end{pmatrix}$$

So the subspace spanned by the first i basis vectors is a G-invariant subspace ($W \leq V$ is G-invariant if $gw \in W$ for every $w \in W, g \in G$).
We say the representation ϕ is irreducible (or simple) if it is nonzero and not reducible.

Recall that kG-module V is reducible if there is some nonzero proper submodule $0 < W < V$. If k is a field, this corresponds to the reducibility of the representation.

Definition 1.7. A representation ϕ is decomposable if it's similar to a representation ψ with the property that there is some nontrivial block division such that for all g, $\psi(g)$ has the form

$$\psi(g) = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$$

That is, $V = W_1 \oplus W_2$ with W_1, W_2 nonzero G-invariant subspaces.

A kG-module V is decomposable if $V = W_1 \oplus W_2$ with W_1, W_2 nonzero submodules of V. If something is not decomposable, we say it is indecomposable. Any irreducible representation is indecomposable. In ordinary representation theory, indecomposability is the same as irreducibility. Not really the case in modular representation theory, but we'll come to that later.

Example 1.2. Consider $G = S_3 = \langle \sigma = (123), \tau = (12) \rangle$ and $V = \mathbb{C}^2$ with basis $\{e_1, e_2\}$. We can make V a representation of G via

$$\sigma \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \tau = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

This is irreducible, hence also indecomposable.

Definition 1.8. A short exact sequence of kG-modules is a sequence of kG-modules and homomorphisms

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V_3 \longrightarrow 0$$

such that for each pair of composable arrows, the image of the left arrow is the kernel of the right arrow.

In particular, V_1 is isomorphic to a submodule of V_2, whose quotient is isomorphic to V_3. We say V_2 is an extension of V_1 by V_3.

Definition 1.9. A short exact sequence

$$0 \longrightarrow V_1 \xrightarrow{\alpha} V_2 \xrightarrow{\beta} V_3 \longrightarrow 0$$

is split (or splits) if there is a map $\gamma : V_3 \to V_2$ (the "splitting") such that $\beta \circ \gamma = \mathrm{id}_{V_3}$.

In particular, $V_2 = \alpha(V_1) \oplus \gamma(V_3) \cong V_1 \oplus V_3$.

Example 1.3. 1. The short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

is non-split.
2. All short exact sequences of complex vector spaces split.

Theorem 1.2 (Maschke's Theorem)**.** *If $|G| \in k^\times$, then any short exact sequence of kG-modules that splits as a short exact sequence of k-modules also splits as a short exact sequence of kG-modules.*

Proof. Given a k-splitting $\phi : V_3 \to V_2$, we set $\gamma = |G|^{-1} \sum_{g \in G} g^{-1} \phi g$ which as one can check is a kG-splitting. □

Example 1.4. For a field k, kG is semisimple (is a direct sum of irreducibles) if and only if $p = \mathrm{char}\, k \nmid |G|$. The "if" part follows from the preceding theorem. We'll show the "only if" part later.

2 Homs and Tensor Products

Let R be a ring and M a right R-module and N a left R-module. The tensor product $M \otimes_R N = M \otimes N$ is an abelia group generated by symbols $m \times n, m \in M, n \in N$ subject to the usual componentwise linear relations and the relation $(mr) \otimes n = m \otimes (rn)$.

Example 2.1. 1. If R is commuative, given R-modules M, N, we form $M \otimes N$ is again an R-module via $r(m \otimes n) = (rm) \otimes n = m \otimes (rn)$.
2. More generally, if M is an R, S-bimodule, N a left S-module, then $M \otimes_S N$ is a left R-module via $r(m \otimes n) = (rm) \otimes n$.

Definition 2.1. Suppose $H \leq G$ is a subgroup and regard kH as a subring of kG. kG can be considered as a (kG, kH)-bimodule. If M is a kH-module, then the left kG-module $kG \otimes_{kH} M$ is called the induced module $M \uparrow_H^G = M \uparrow^G$ of M from H to G.
If N is a kG-module, we can of course restrict the action to kH, which gives a kH-module $M \downarrow_H^G = M \downarrow_H$ of M from G to H.

Proposition 2.1. *If $R \subset S$ are rings and A is a left S-module, N a left R-module, M a (S, R)-bimodule, then we have a natural isomorphism*

$$\mathrm{Hom}_R(N, \mathrm{Hom}_S(M, A)) \cong \mathrm{Hom}_S(M \otimes_R N, A)$$

Proof. The natural maps $\phi : \mathrm{Hom}_R(N, \mathrm{Hom}_S(M, A)) \to \mathrm{Hom}_S(M \otimes_R N, A)$ via $\phi(\alpha)(m \otimes n) = \alpha(n)(m)$ and $\psi : \mathrm{Hom}_S(M \otimes_R N, A) \to \mathrm{Hom}_R(N, \mathrm{Hom}_S(M, A))$ via $\psi(\beta)(n)(m) = \beta(m \otimes n)$ are mutual inverses. □

In particular, if we take $R = kH$ and $S = kG$ where $H \leq G$ are groups, then this means that for any kH-module U and kG-module V, we have

Corollary 2.2. $\mathrm{Hom}_{kH}(U, \mathrm{Hom}_{kG}(kG, V)) \cong \mathrm{Hom}_{kG}(kG \otimes_{kH} U, V)$.

Observe that $\mathrm{Hom}_{kG}(kG, V) \cong V \downarrow_H$ via $\tau : \mathrm{Hom}_{kG}(kG, V) \to V, \alpha \mapsto \alpha(1)$.

Corollary 2.3 (Frobenius Reciprocity)**.** $\mathrm{Hom}_{kH}(U, V \downarrow_H) \cong \mathrm{Hom}_{kG}(U \uparrow^G, V)$.

If U, V are kG-modules, so are $U \otimes_k V$ (via $g(u \otimes v) = (gu) \otimes (gv)$ and its unique linear extension, notably $(g+h)(u \otimes v) = (gu) \otimes (gv) + (hu) \otimes (hv)$) and $\mathrm{Hom}_k(U, V)$ (via $g(f)(u) = g(f(g^{-1}u))$). If U, V, W are kG-modules, we have $\mathrm{Hom}_k(U, \mathrm{Hom}_k(V, W)) \cong \mathrm{Hom}_k(U \otimes_k V, W)$ is an isomorphism of kG-modules by Theorem 2.1. Taking fixed points under G, we have

$$\mathrm{Hom}_{kG}(U, \mathrm{Hom}_k(V, W)) \cong \mathrm{Hom}_{kG}(U \otimes_k V, W)$$

which is helpful in calculating the decomposition of tensor products (given its semisimplicity) in terms of simple modules.
Let's record some simple algebra facts that follows from easy computation.

Proposition 2.4. *If M is a right R-module and*

$$0 \longrightarrow N \xrightarrow{\alpha} N' \xrightarrow{\beta} N'' \longrightarrow 0$$

is a short exact sequence of left R-modules. Then the sequence

$$M \otimes_R N \xrightarrow{1 \otimes \alpha} M \otimes_R N' \xrightarrow{1 \otimes \beta} M \otimes_R N'' \longrightarrow 0$$

is exact.

Remark. This means that the functor $M \otimes -$ is right-exact. It's not always left-exact.

Proposition 2.5. *Suppose M is a left R-module and*

$$0 \longrightarrow N \longrightarrow N' \longrightarrow N'' \longrightarrow 0$$

is a short exact sequence of left R-modules. Then the sequences

$$0 \longrightarrow \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M, N') \longrightarrow \mathrm{Hom}_R(M, N'')$$

$$0 \longrightarrow \mathrm{Hom}_R(N'', M) \longrightarrow \mathrm{Hom}_R(N', M) \longrightarrow \mathrm{Hom}_R(N, M)$$

Lemma 2.6. *Suppose*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

is a short exact sequence of finite-dimensional kG-modules (with k a field) and $M_2 \cong M_1 \oplus M_3$, then the sequence splits.

Proof. We have the left exact sequence

$$0 \longrightarrow \mathrm{Hom}_{kG}(M_3, M_1) \longrightarrow \mathrm{Hom}_{kG}(M_3, M_2) \longrightarrow \mathrm{Hom}_{kG}(M_3, M_1)$$

But the right-most map must also be surjective by dimension counting, so we in fact have a short exact sequence

$$0 \longrightarrow \mathrm{Hom}_{kG}(M_3, M_1) \longrightarrow \mathrm{Hom}_{kG}(M_3, M_2) \longrightarrow \mathrm{Hom}_{kG}(M_3, M_1) \longrightarrow 0$$

The preimage of id_{M_3} gives a splitting. □

3 The Jacobson Radical

Let R be a (unital) ring.

Definition 3.1. The Jacobson radical $\mathfrak{J}(R)$ of R is the intersection of all maximal left ideals of R.

Example 3.1. $\mathfrak{J}(R) = \bigcap_{p \text{ prime}} p\mathbb{Z} = \{0\}$.

Lemma 3.1.

$$\mathfrak{J}(R) = \bigcap_{M \text{ simple left } R\text{-module}} \mathrm{ann}_R(M) = \bigcap_{I \text{ maximal left ideal}} \mathrm{ann}_R(R/I)$$

where $\mathrm{ann}_R(M) = \{a \in R : aM = 0\}$.

Proof. If $I \leq R$ is a maximal left ideal, then R/m is a simple left R-module and $I = \mathrm{ann}_R(R/I)$. Conversely, if S is a simple module, and $x \in S$ is nonzero, then the map ${}_RR \to S, r \mapsto rx$ is surjective. If I is its kernel, then $S \cong {}_RR/I$. □

Remark. Each $\mathrm{ann}_R(M)$ is a two-sided ideal, hence $\mathfrak{J}(R)$ is a two-sided ideal. We've also seen from the proof that simple left R-modules are in fact quotients of R by left maximal ideals.

Lemma 3.2. $\mathfrak{J}(R) = \{y \in R : \forall a, b \in R : 1 - ayb \text{ has a two-sided inverse}\}$.

Proof. Atiyah-Macdonald. □

Corollary 3.3. $\mathfrak{J}(R)$ *is also the intersection of all maximal right ideals.*

Lemma 3.4 (Nakayama's Lemma)**.** *If M is a finitely generated left R-module and $\mathfrak{J}(R)M = M$, then $M = 0$.*

Proof. Let $m_1, \ldots, m_n$ be a set of generators for M of minimal size. Suppose $n > 0$. Since $\mathfrak{J}(R)M = M$, one can find elements $a_i \in \mathfrak{J}(R)$ such that $m_n = \sum_i a_i m_i$, i.e. $(1 - a_n)m_n = \sum_{i<n} a_i m_i$. Since $a_n \in \mathfrak{J}(R)$, we can find a two-sided inverse b of $1 - a_n$, hence $m_n = \sum_{i<n} b a_i m_i$, contradicting minimality of n. □

Example 3.2. Suppose S is a simple R-module (which is then necessarily finitely generated), then $\mathfrak{J}(R)S = 0$.

Definition 3.2. An R-module M is semisimple (or completely reducible) if M is a (possibly infinite) direct sum of simple R-modules.

Proposition 3.5. *(i) Every submodule of a semisimple module is also semisimple, and is a direct summand.*
(ii) Every quotient of a semisimple module is also semisimple.

Remark. A module M is semisimple iff every submodule of M is a direct summand.

Proof. Webb. □

Theorem 3.6. *Suppose R is Artinian, then the followings are equivalent:*
(i) $\mathfrak{J}(R) = 0$.
(ii) Every R-module is semisimple.
(iii) Every finitely generated R-module is semisimple.

Remark. $\mathfrak{J}(\mathbb{Z}) = 0$, but not all $\mathbb{Z}$-modules are semisimple. Indeed, despite $\mathbb{Z}$ being Noetherian, it is not Artinian.

Proof. Suppose $\mathfrak{J}(R) = 0$. Let $M \subset {}_RR$ be minimal such submodules that it is the intersection of a finite set of maximal left ideals. Thus M must be in every maximal left ideal, hence $M = 0$. Therefore $\bigcap_{i\in I} \mathfrak{m}_i$ for some finite set I.
There is an injection ${}_RR \to \bigoplus_i {}_RR/\mathfrak{m}_i$. Each $S_i = {}_RR/\mathfrak{m}_i$ is a simple module, so ${}_RR$ is semisimple. Note that this is a finite direct sum since R is Artinian.
Suppose now that ${}_RR$ is semisiple, then $\mathfrak{J}(R)$ is a summand of ${}_RR$. Write ${}_RR = \mathfrak{J}(R) \oplus {}_RR/\mathfrak{J}(R)$, so $\mathfrak{J}(R) = \mathfrak{J}(R)\mathfrak{J}(R)$. Since $\mathfrak{J}(R)$ is also a quotient of R, it is finitely generated, so $\mathfrak{J}(R) = 0$ by Lemma 3.4. □

Theorem 3.7 (Wedderburn Structure Theorem)**.** *Let R be a finite-dimensional algebra over a field k with $\mathfrak{J}(R) = 0$. Then*

$$R \cong \prod_i \mathrm{Mat}_{d_i}(\Delta_i)$$

where Δ_i's are finite-dimensional division algberas containing k in their centres.

Proof. For any ring R, we have $R \cong \mathrm{End}_R({}_RR)^{\mathrm{op}}$ (via $r \mapsto (f(x) = xr)$). The regular representation ${}_RR$ is semisimple by the preceding theorem, so we can write ${}_RR = \bigoplus_{i=1}^m d_iS_i$ where the S_i's are pairwise nonisomorphic simple R-modules.
By Schur's lemma, $\mathrm{End}_R(S_i)$ is a divison ring, and we shall denote its opposite ring as Δ_i. The point here is that we have

$$\mathrm{End}_R\left(\bigoplus_{k=1}^m M_k\right) = \mathrm{Mat}_m(\mathrm{Hom}_R(M_i, M_j)_{1\le i,j\le m})$$

We therefore reach

$$\mathrm{End}_R({}_RR) = \prod_{i=1}^m \mathrm{End}(d_iS_i) = \prod_{i=1}^m \mathrm{Mat}_{d_i}(\mathrm{End}_R(S_i)) = \prod_{i=1}^m \mathrm{Mat}_{d_i}(\Delta_i^{\mathrm{op}})$$

Taking opposites gives the result. □

Remark. 1. If k is algebraically closed, we have $\Delta_i = k$. If $k = \mathbb{C}$, then we recover from the theorem that $\mathbb{C}G$ is semisimple and $\mathbb{C}G = \prod_{i=1}^{m} \mathrm{Mat}_{d_i}(\mathbb{C})$.
2. $\mathbb{C}S_3 = \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_2(\mathbb{C})$.
3. If $k = \mathbb{R}$, then there are three possibilities for $\mathbb{R}$-divison algebra, namely $\mathbb{R}, \mathbb{C}, \mathbb{H}$ (Frobenius-Schur indicator).
4. If k is a finite field, each k-divison algbera has to be a finite field as well (Wedderburn's Little Theorem).
5. Let R be the algebra of all upper-triangular matrices over k, one can show that $\mathfrak{J}(R)$ is the set of strictly upper-triangular matrices (i.e. those with zero diagonal).

Note that each $\mathrm{Mat}_n(\mathbb{C})$ has simple modules consisting of column vectors of length n over $\mathbb{C}$.
Returning to the question about the semisimplicity of kG. We shall show that it must not be semisimple when $p = \mathrm{char}\, k \mid |G|$. Assume for the sake of contradiction that kG is semisimple. Then the trivial module k, having dimension 1, would appear once in a direct sum decomposition of kG into a sum of simple kG-modules by the theorem. In particular, in any composition series for kG, there would be exactly one factor isomorphic to k.
Consider the augmentation map $kG \to k, \sum_g \alpha_g g \mapsto \sum_g \alpha_g$, which is a k-algebra homomorphism. Its kernel $\Sigma_G = \{\sum_g \alpha_g g \in kG : \sum_i \alpha_i = 0\}$ is called the augmentation ideal. Note that Σ_G is a submodule of kG, and $kG/\Sigma_G = k$. On the other hand, consider $\sigma = \sum_g g \in \Sigma_G$. It's also clear that $g\sigma = \sigma$ for all $g \in G$, so $k\sigma$ is also a submodule of kG isomorphic to the trivial kG-module k. Thus when we construct a composition series of kG by refining $kG \supsetneq \Sigma_G \supset k\sigma \supsetneq 0$, we get one with at least two factors isomorphic to k, contradiction.

4 Brauer Characters

Definition 4.1. We call a group element $g \in G$ a p-element (or p-singular element, unipotent element, etc.) if its order is a power of p. We call it a p'-element (or p-regular element, semisimple element, etc.) if its order is prime to p (bad notation, I know).

Lemma 4.1. *Let G be a group. Given any $g \in G$, there is a p-element x and a p'-element y such that $g = xy = yx$ and every $h \in G$ with $hg = gh$ has $hx = xh, hy = yh$. Moreover, such x, y are unique.*

x is called the p-part and y the p'-part of $g \in G$.

Proof. Let $n = p^\alpha m, p \nmid m$ be the order of g. There exists $s, t \in \mathbb{Z}$ such that $sp^\alpha + tm = 1$. Thus $g = g^{tm} g^{sp^\alpha}$. Let $x = g^{tm}$ and $y = g^{sp^\alpha}$, which clearly satisfies the conditions.
As for uniqueness, suppose $g = xy = x_1 y_1$ are two such choices, then $x_1^{-1} x = y_1 y^{-1}$, but $x_1 x^{-1}$ is a p-element yet $y_1 y^{-1}$ is a p'-element. So they are both identity, therefore $x = x_1, y = y_1$. □

Let M be a $\mathbb{C}G$-module. There exists a class function $\chi_m : \mathrm{ccls}(G) \to \mathbb{C}$ via $\chi_m(g) = \mathrm{Tr}(g, M)$. This is the ordinary character of M. We know that $\chi_{M_1 \oplus M_2} = \chi_{M_1} + \chi_{M_2}$, $\chi_{M_1 \otimes M_2} = \chi_{M_1} \chi_{M_2}$ and $\chi_M = \chi_{M'}$ iff $M \cong M'$.

We're going to develop a theory of characters $M \mapsto \chi_M$ for modular representations in such a way that the first two properties still hold, and $\chi_M = \chi_{M'}$ iff M, M' have the same composition factors. The problem we're facing is that if the kG-module M is a direct sum of p-copies of M', then we always have $\mathrm{Tr}(-, M) = 0$. This was considered and solved by Brauer. We shall show

Theorem 4.2. *Suppose k has characteristic p, then the follows are equivalent:*
(i) $\mathrm{Tr}(-, M) = \mathrm{Tr}(-, M')$.
(ii) For each simple kG-module S, the multiplicity $[M : S]$ of S as the composition factor of M is congruent to $[M' : S]$ modulo p.

Suppose k has characteristic $p > 0$. For $m = p^\alpha m', p \nmid m'$, we have $X^m - 1 = (X^{m'} - 1)^{p^\alpha}$ in $k[X]$. Hence k contains the m-th roots of unity iff k contains the m'-th roots of unity. The polynomial $X^{m'} - 1$ is separable over k and its roots (in $\bar{k}$) form a a cyclic group generated by some primitive m'-th root of unity. For a group G with order $|G| = p^\alpha m, p \nmid m$, we write $|G|_p = p^\alpha, |G|_{p'} = m$.

Lemma 4.3. *Suppose G is finite and k has* $\operatorname{char} k = p > 0$ *contains all $|G|_{p'}$-th roots of unity. Let $g \in G$ and ϕ a representation of G. Then the eigenvalues of $\phi(g)$ and the eigenvalues of $\phi(y)$, where y is the p'-part y of g, agree.*

Proof. Choose a change-of-basis matrix P such that the matrix $P^{-1}\phi(g)P$ is upper-triangular. Then its diagonals are the eigenvalues λ_i of $\phi(g)$. Let $x = g^t$ be the p-part and y the p' part of g. Suppose x has order p^s for some s, then $I = P^{-1}\phi(x^{p^s})P = P^{-1}\phi(g^{tp^s})P = (P^{-1}\phi(g)P) \cdots (P^{-1}\phi(g)P)$, and we know that the last expression is upper triangular with $\lambda_i^{tp^s}$ on the diagonal. Hence $(\lambda_i^t)^{p^s} = 1$ for all i. Since $\operatorname{char} k = p$, this means that $\lambda_i^t = 1$ for all i. Thus $P^{-1}\phi(x)P$ is unipotent (i.e. upper triangular with 1's on the diagonal), and therefore the eigenvalues of x all equal to 1. Hence $\operatorname{tr} \phi(x)$ is the dimension of the representation. The expression $P^{-1}\phi(g)P = (P^{-1}\phi(x)P)(P^{-1}\phi(y)P)$ gives the result. □

Example 4.1. Let G be a group and $\operatorname{char} k = p > 0, k = \bar{k}$. Given $g \in G$ and a finite-dimensional kG-module M, the k-linear map on M induced by g is annihilated by the polynomial $X^{|G|} - 1$ over k. We know that $(X^{|G|}) - 1 = (X^{|G|_{p'}} - 1)^{|G|_p}$ and $X^{|G|_{p'}} - 1$ is a product of distinct linear factors in $k[X]$. So g has a Jordan canonical form, and its eigenvalues are $|G|_{p'}$-th roots of unity. Suppose

$$\begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \lambda & 1 \\ & & & \lambda \end{pmatrix}$$

is a Jordan block of g. It's conjugate to

$$g_1 = \begin{pmatrix} \lambda & \lambda & & \\ & \lambda & \lambda & \\ & & \lambda & \lambda \\ & & & \lambda \end{pmatrix} = x_1 y_1, x_1 = \begin{pmatrix} 1 & 1 & & \\ & 1 & 1 & \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}, y_1 = \begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & \lambda & \\ & & & \lambda \end{pmatrix}$$

Then it's clear that x_1 is a p-element and y_1 a p'-element. They also commute with any matrix commuting with g_1, as x_1 is a scalar multiple of g_1 and y_1 is in the centre. Thus x_1 is the p-part and y_1 the p'-part of g_1. Hence if $g = xy$ is a

decomposition of g into its p-part x and p'-part y, then the matrix of x has 1's in the diagonal of its Jordan canonical form and the matrix of y is diagonalisable. So $\mathrm{Tr}(g, M) = \mathrm{Tr}(y, M)$ and $\mathrm{Tr}(x, M) = \dim_k M$.

For a finite group G and a field k of characteristic $p > 0$ containing all $|G|_{p'}$-th roots of unity. These roots of unity form a cyclic group $\mu_{|G|_{p'}}(k)$ of order $|G|_{p'}$ under multiplication, and all eigenvalues of $g \in G$ belong to this group. Choose and fix an isomorphism of cyclic groups $\psi : \mu_{|G|_{p'}}(k) \cong \mu_{|G|_{p'}}(\mathbb{C})$. Sometimes this guy is called a lifting.
Suppose M is a finite-dimensional kG-module and g is a p'-element of G. Then the matrix of g is diagonalisable, say with eigenvalues $\lambda_1, \ldots, \lambda_d$ where $d = \dim_k M$.

Definition 4.2. The Brauer character of g on M is $\chi_M(g) = \psi(\lambda_1) + \cdots + \psi(\lambda_d)$.

Remark. $\chi_M(g)$ is a cyclotomic integer. This definition also induces a map χ_M from the set of conjugacy classes of p'-elements of G to $\mathbb{C}$.

Example 4.2. Suppose $k = \mathbb{F}_2$ and $G = \langle x \rangle$ where x has order 3.

$$\rho(x) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

gives a 2-dimensional representation M of G over k. Its characteristic polynomial is $t^2 + t + 1$. The eigenvalues are primitive third roots of unity in $\mathbb{F}_4$. These lift to primitive third roots of unity in $\mathbb{C}$ and so $\chi_M(x) = e^{2\pi i/3} + e^{4\pi i/3} = -1$, which is a surprise since $\mathrm{Tr}(x, M) = 1 \neq -1$.
We might look at a way to fix this somewhere by the end of the course.

Lemma 4.4. *Suppose we are given two modular representations σ, τ of a group G and suppose they have the same Brauer character $\chi_\sigma = \chi_\tau$. Then for every p'-element $g \in G$, $\sigma(g)$ and $\tau(g)$ have the same eigenvalues.*

Proof. Given $\chi_\sigma = \chi_\tau$, let the eigenvalues of $\sigma(g)$ be $\epsilon^{\alpha_1}, \ldots, \epsilon^{\alpha_a}$ and the eigenvalues of $\tau(g)$ be $\epsilon^{\beta_1}, \ldots, \epsilon^{\beta_b}$, where ϵ is a primitive $|G|_{p'}$-th root of unity in k. Raising each of these to the i-th power gives us the characteristic roots $\sigma(g^i)$ and $\tau(g^i)$. Let ζ be a primitive $|G|_{p'}$-root of unity in $\mathbb{C}$ and choose ψ with $\psi(\epsilon) = \zeta$.
Since $\chi_\sigma = \chi_\tau$, we have $\zeta^{i\alpha_1} + \cdots + \zeta^{i\alpha_a} = \zeta^{i\beta_1} + \cdots + \zeta^{i\beta_b}$ for all i. Let's now consider the complex representations $\sigma'(g^i) = \mathrm{diag}(\zeta^{i\alpha_1}, \ldots, \zeta^{i\alpha_a})$ and $\tau'(g^i) = \mathrm{diag}(\zeta^{i\beta_1}, \ldots, \zeta^{i\beta_b})$ of $\langle g \rangle$. They have the same (ordinary) character, therefore they are isomorphic as complex representations. Hence, after possible rearrangements of the indices, we must have $a = b$ and $\alpha_j = \beta_j$ for all j. □

Recall that a composition series of a module M is simply a descending chain $0 = M_0 \subset M_1 \subset \cdots \subset M_l = M$ where the factors M_i/M_{i-1} (known as composition factors of M) are simple. Then any two such series for M are equivalent, in the sense that the composition factors are rearrangements of each other. In particular, the length of the composition series (known as the composition length) is an invariant of M. So every representation has a fixed number of irreducible constituents, which are the composition factors, and they are unique up to rearrangement.
A module M is uniserial if it has a unique composition series. In particular,

it has a unique maximal submodule M', and M/M' has a unique maximal submodule, and so on. In fact, this occurs precisely when the submodules are linearly ordered by inclusion.
Let $\mathcal{B}$ be an ordered basis of M defined by a composition series $0 = M_0 \subset M_1 \subset \cdots \subset M_l = M$, i.e. $B = \{e_1^1, \ldots, e_{n_1}', e_1^2, \ldots, e_{n_2}^2, \ldots, e_1^l, \ldots, e_{n_l}^l\}$ such that $e_1^1, \ldots, e_{n_m}^m$ form a basis for M_m. In other words, the representation can be written in the block form

$$\rho : g \mapsto \begin{pmatrix} \rho_l(g) & & & * \\ & \rho_{l-1}(g) & & \\ & & \ddots & \\ 0 & & & \rho_1(g) \end{pmatrix}$$

Proof of Theorem 4.2. WLOG M, M' are semisimple (look at composition factors I guess).
For the "if" part, let $(S_i)_i$ be the simple factors of M, M', then

$$\operatorname{Tr}(g, M) = \sum_{i=1}^{n} \alpha_i \operatorname{Tr}(g, S_i) = \sum_{i=1}^{n} \beta_i \operatorname{Tr}(g, S_i) = \operatorname{Tr}(g, M')$$

Conversely, suppose $\operatorname{Tr}(g, M) = \operatorname{Tr}(g, M')$ for all $g \in G$, then $\operatorname{Tr}(x, M) = \operatorname{Tr}(x, M')$ for all $x \in kG$. Apply Theorem 3.7 to $kG/\mathcal{J}(kG)$ gives a decomposition $\bigoplus_{i=1}^{r} n_i S_i \cong kG/\mathfrak{J}(kG) = M_{n_1}(\Delta_1) \times \cdots \times M_{n_r}(\Delta_r)$ where $n_i S_i \cong M_{n_i}(\Delta_i)$.
Recall that every simple kG-module S is isomorphic to $kG/\mathfrak{m}$ for some maximal ideal $\mathfrak{m} \leq kG$. Since $\mathfrak{J}(kG)$ contains all such $\mathfrak{m}$, each M, M' is a direct sum of $n_i S_i$'s. Now, any matrix algebra contains a matrix with a 1 in its upper left corner and zeros elsewhere. Let $x_i \in kG$ be the preimage of such a matrix, then $\operatorname{Tr}(x_i, S_j) = \delta_{ij}$. Then $\operatorname{Tr}(x_i, M) = \alpha_i$ is the multiplicity of S_i in M and $\operatorname{Tr}(x_i, M') = \beta_i$ is the multiplicity of S_i in M'. Hence $\alpha_i = \beta_i$ in k, which means that $\alpha_i \equiv \beta_i \pmod{p}$. □

Theorem 4.5 (Brauer)**.** *Let M, M' be finite-dimensional kG-modules, then $\chi_M = \chi_{M'}$ iff the multiplicities of simple modules in their respective composition series agree.*

Proof. Again WLOG M, M' are semisimple.
The "if" part is easy: We've already seen that if the multiplicities of each simple module as composition factors of M, M' are equal then $\chi_M = \chi_{M'}$.
Conversely, suppose $\chi_M = \chi_{M'}$. Suppose we have a counterexample of smallest dimension, then indeed M, M' cannot even share one composition factor, as we'll be able to remove it. As $\chi_M = \chi_{M'}$, we have $\operatorname{Tr}(g, M) = \operatorname{Tr}(g, M')$. Theorem 4.2 shows that the multiplicity of the factors of M, M' are congruent modulo p, so each multiplicity must be a multiple of p. So $M = pN$ and $M' = pN'$ for some N, N', and N, N' must have the same Brauer character, contradicting minimality. □

Example 4.3. Let $G = S_3$. We know the $\mathbb{C}G$-modules are the trivial representation, the sign representation σ and a 2-dimensional representation ϕ given by removing the trivial representation from the permutation representation on three letters. It has ordinary character table

	1	2^1	3^1
k_G	1	1	1
σ	1	-1	1
ϕ	2	0	-1

What about modular characters? If $p = 3$, then G has two conjugacy classes of $3'$-elements, and the irreducible representations are the trivial representation $\bar{k}_G$ and $\bar{\sigma}$ which corresponds to the sign representation. The Brauer character of $\bar{\phi}$ ($\chi(1) = 2, \chi((12)) = 0$) however is a sum of the Brauer characters of $\bar{k}_G$ and $\bar{\sigma}$. By Brauer's theorem, the composition factors of $\bar{\phi}$ are $\bar{k}_G$ and $\bar{\sigma}$.
$p = 2$ is similar. The sign representation becomes trivial, so the remaining simple characters are $\bar{k}_G$ and $\bar{\phi}$. We therefore have the Brauer character tables

$p=2$	1	3
k_G	1	1
$\bar{\phi}$	2	-1

$p=3$	1	2
k_G	1	1
$\bar{\sigma}$	1	-1

5 Character Tables and the Choice of Lifting

Recall that an algebraic integer is a number $\alpha \in \mathbb{C}$ satisfying a nonzero monic polynomial over $\mathbb{Z}$. A number field K is a subfield of $\mathbb{C}$ which is a finite field extension of $\mathbb{Q}$. We write $\mathcal{O}_K$ to denote the ring of algebraic integers inside K (the "ring of integers of K"). It's elementary that for any $x \in K$, there is some $c \in \mathbb{Z} \setminus \{0\}$ such that $cx \in \mathcal{O}_K$.

Definition 5.1. An integral domain R is called a Dedekind domain if it is Noetherian, integrally closed, and every prime ideal of it is maximal.

Example 5.1. $\mathcal{O}_K$ is always a Dedekind domain.

Let $p = \operatorname{char} k > 0$ and G a finite group with $|G| = p^a m, p \nmid m$. Suppose K is sufficiently large to contain all its m-th roots of unity. Let $C, \hat{C}$ be the groups of m-th roots of unity in k and $\mathbb{C}$, respectively. And let $K = \mathbb{Q}(\hat{C})$.

Lemma 5.1. $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Proof. Ask a toddler on the street. □

Take $\mathcal{O}_K$ be the ring of integers of K. Choose a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p (i.e. $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$).

Proposition 5.2. *$\mathcal{O}_K/\mathfrak{p}$ is the smallest finite field containing the m-th roots of unity. If p^r is the smallest power of p such that $m \mid p^r - 1$, then:*
(i) $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^r} \hookrightarrow k$.
(ii) $\hat{C} + \mathfrak{p} \cong C$.
(iii) $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ *is the stabiliser of* $\mathfrak{p}$ *in* $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. Y'all are excellent number theorists. Do it yourselves. □

Example 5.2. Suppose $G = \langle x \rangle = C_n, n = p^a m$. The p'-elements in G are $\{1, x^{p^a}, \ldots, x^{(m-1)p^a}\}$ and the p-elements are $\{1, x^m, x^{2m}, \ldots, x^{(p^a-1)m}\}$. For a group homomorphism $G \to k^\times$, we must have $\rho(x)^n = 1$, so $\rho(x)^m = 1$. So for $i = 0, 1, \ldots, m$ we can define $\rho_i(x) = \omega^i$ where ω is a p-th root of unity in k.
Let's take $n = 12 = 2^2 3$, so the $2'$-elements are $1, x^4, x^8$ and the 2-elements are $1, x^3, x^6, x^9$. Let's construct a table whose columns are indexed by powers of x and rows by ρ_i's.

	1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}
ρ_0	1	1	1	1	1	1	1	1	1	1	1	1
ρ_1	1	ω	ω^2	1	ω	ω^2	1	ω	ω^2	1	ω	ω^2
ρ_2	1	ω^2	ω	1	ω^2	ω	1	ω^2	ω	1	ω^2	ω

Something interesting is happening here: The information on the columns of $2'$-elements is enough for one to capture all the information in the table, e.g. $\rho_i(x) = \rho_i(x^4x^9) = \rho_i(x^4)\rho_i(x^9) = \rho_i(x^4)$. Let's extract those columns.

	1	x^4	x^8
ρ_0	1	1	1
ρ_1	1	ω	ω^2
ρ_2	1	ω^2	ω

Choosing an isomorphism of cyclic groups $\psi : \{|G|_{2'}\text{-th roots of unity in } k\} \to \{|G|_{2'}\text{-th roots of unity in } \mathbb{C}\}$ is the same as choosing a primitive third root of unity in $\mathbb{C}$. So choosing another isomorphism of cyclic group as such is the same as swapping the last two rows (or last two columns) in the smaller table.
The Brauer character table as done here seems to depend on the choice of lift, but not much.

Definition 5.2. The Brauer character table of G modulo $p = \operatorname{char} k > 0$ is a table such that:
(i) The rows are indexed by the simple kG-modules.
(ii) The columns are indexed by conjugacy classes of p'-elements of G.
(iii) The entries are the values of the corresponding Brauer characters.

Once one fix an isomorphism $\psi : C \to \hat{C}$, the tables arising from other isomorphisms $C \to \hat{C}$ are precisely the results of applying the action of $\mathrm{Gal}(K/\mathbb{Q})$ to $\hat{C}$.
So the rows of the Brauer character table are the Brauer characters of simple kG-modules. And we'll see that the columns are the ring homomorphisms from the Grothendieck group of G (defined later) to $\mathbb{C}$. In addition, the irreducible Brauer characters form a basis for class functions on conjugacy classes of p'-elements in $\mathbb{C}$, so the table is necessarily square.

Proposition 5.3. *(i) If we apply an element of* $\mathrm{Gal}(K/\mathbb{Q})$ *to a column of a Brauer character table, we get another column.*
(ii) If we apply an element of the stabiliser of $\mathfrak{p}$ *in* $\mathrm{Gal}(K/\mathbb{Q})$ *to a row, we get another row.*

Hence the Brauer character table is determined by the choice of $\mathfrak{p}$, unique up to permutations of rows and columns.

Remark. If we apply an element of $\mathrm{Gal}(K/\mathbb{Q})$ which does not stabilise $\mathfrak{p}$ to a row of the Brauer character table, we don't necessarily get another row.

Sketch of Proof. (i) Let ζ be a primitive n-th root of unity in $\mathbb{C}$, then $K = \mathbb{Q}(\zeta)$ and an element of $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ sends ζ to ζ^t for some $t \in \mathbb{Z}, \gcd(t, m) = 1$. Then for each p'-element $g \in G$ and each column $\tilde{\chi}$, we must have $\tilde{\chi}^\sigma(g) = \tilde{\chi}(g^t)$, where $\tilde{\chi}(g)$ denote the column corresponding to g.
(ii) σ stabilises $\mathfrak{p}$ precisely when t is a p-power. Let S be a simple kG-module with $\rho : G \to \mathrm{GL}_n(k)$ the corresponding representation, then S^σ is a kG-module with corresponding representation $\rho^\sigma : G \to \mathrm{GL}_n(k) \to \mathrm{GL}_n(k), g \mapsto (\lambda_{ij}(g)) \mapsto (\lambda_{ij}(g)^t)$. □

6 Grothendieck Rings

Let G, k, p as before. We form an abelian group $R(G)$ as follows:

Definition 6.1. $R(G)$ is the abelian group generated by symbols $[M]$, where M is an isomophism class of finite-dimensional kG-modules, subject to the relations $[M_2] = [M_1] + [M_3]$ for every short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

of finite-dimensional kG-modules.

Remark. 1. We are taking isomorphism classes because we'd otherwise run into set-theoretic issues.
2. $R(G)$ is a free abelian group with basis given the isomorphism classes $[S]$ of simple modules, by the Jordan-Hölder theorem.

We can make $R(G)$ a commutative ring by introducing multiplication given by tensor products $[M][N] = [M \otimes_k N]$ (recall that the kG-module structure on $M \otimes_k N$ is given by the diagonal action of G). This is well-defined since everything's flat over a field. It is commutative since tensor products over k are commutative. And the multiplicative identity is given by $[k]$.

Remark. 1. $R(G)$ is sometimes also denoted by $G_0(kG)$.
2. If $k = \mathbb{C}$, $R(G)$ is exactly the ring of virtual characters of $\mathbb{C}G$-modules.
3. In general, every element of $R(G)$ can be expressed in the form $[M] - [N]$.

Let's collect some properties of Brauer characters, 'coz why not.

Lemma 6.1. *(i)* $\chi_M(1) = \dim_k M$.
(ii) χ_M *is a class function on* p'*-elements.*
(iii) $\chi_M(g^{-1}) = \overline{\chi_M(g)} = \chi_{M^*}(g)$.
(iv) If we have a short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

of finite-dimensional kG*-modules, then* $\chi_{M_2} = \chi_{M_1} + \chi_{M_3}$. *In particular,* χ_M *depends only on the isomorphism class of* M.
(v) $\chi_M(g)\chi_N(g) = \chi_{M \otimes_k N}(g)$.

Proof. Exercise. □

Corollary 6.2. *For any conjugacy class of* p'*-elements of* G*, the map* $\tilde{\chi}(g) : R(G) \to \mathbb{C}, [M] \mapsto \chi_M(g)$ *is a well-defined homomorphism of rings.*

Theorem 6.3. *The map*

$$R(G) \to \prod_{\text{conjugacy classes of } p'\text{-elements in } G} \mathbb{C}$$

given by $[M] \mapsto (g \mapsto \chi_M(g))$ *is injective.*

Proof. Suppose $[M] - [N]$ and $[M'] - [N']$ have the same image under this map, then $\chi_M - \chi_N = \chi_{M'} - \chi_{N'}$, so $\chi_{M \oplus N'} = \chi_M + \chi_{N'} = \chi_{M'} + \chi_N = \chi_{M' \oplus N}$, hence $[M] + [N'] = [M \oplus N'] = [M' \oplus N] = [M'] + [N]$, i.e. $[M] - [N] = [M'] - [N']$. □

Theorem 6.4. *The map*

$$\mathbb{C} \otimes_{\mathbb{Z}} R(G) \to \prod_{\text{conjugacy classes of } p'\text{-elements in } G} \mathbb{C}$$

is an isomorphism of $\mathbb{C}$-algebras.

Corollary 6.5 (Brauer)**.** *The number of simple kG-modules equals to the number of conjugacy classes of p'-elements in G.*

Example 6.1. If $p = 0$, then the number of conjugacy classes is the number of ordinary irreducibles. If $p > 0$ and G is a p-group, then the only modular simple kG-module is the trivial module.

Lemma 6.6 (Injectivity Part of Theorem 6.4)**.** *The irreducible Brauer characters χ_{S_i} are $\mathbb{C}$-linearly independent.*

Proof. Let $K \leq \mathbb{C}$ be the field generated over $\mathbb{Q}$ by the $|G|_{p'}$-th roots of unity, $\mathcal{O} = \mathcal{O}_K$ its ring of integers, and $\mathfrak{p} \leq \mathcal{O}$ a prime containing p. Then $\mathcal{O}_{\mathfrak{p}} \subset K$ consists of fractions $x/y, x, y \in \mathcal{O}, y \notin \mathfrak{p}$. Let $\mathfrak{m}_{\mathfrak{p}} = \{x/y \in \mathcal{O}_{\mathfrak{p}} : x \in \mathfrak{p}, y \notin \mathfrak{p}\}$ be its unique maximal ideal. Note that $\mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} \cong \mathcal{O}_{\mathfrak{p}} \hookrightarrow k$ since at some point we assumed that k contains all the $|G|_{p'}$-th roots of unity. Also, $\mathcal{O}_{\mathfrak{p}}$ is a PID, so $\mathfrak{m}_{\mathfrak{p}} = (\pi)$ for some $\pi \in \mathcal{O}_{\mathfrak{p}}$.
Suppose we have a nontrivial linear relation amongst χ_{S_i}'s over $\mathbb{C}$, then there's a nontrivial linear relation over K (which already contains all the character values). Clearing denominators, we get a linear relation now in $\mathcal{O}$. Dividing by a suitable power of π, we may assume that not all coefficients are in $\mathfrak{p}$. Now reducing modulo $\mathfrak{m}_{\mathfrak{p}}$ gives a nontrivial linear relation $\forall x \in kG, 0 = \sum_i \alpha_i \operatorname{Tr}(x, S_j)$ for $\alpha_i \in k$. For each i, there is some $x_i \in kG$ such that $\operatorname{Tr}(x_i, S_j) = \delta_{ij}$, thus forcing $\alpha_i = 0$ for all i. □

Now on to the surjectivity part. For each p'-element $g \in G$, let's try to find an element in $\mathbb{C} \times_{\mathbb{Z}} R(G)$ such that $\tilde{\chi}(g)$ sends them to 1 and $\tilde{\chi}(h)$ sends it to 0 for all h not conjugate to g.
We first try this idea on a cyclic group $G = \langle g \rangle$ with g having order m coprime to p. Irreducible representations of G over k are of the form $g \mapsto \epsilon^j$ where $j \in \mathbb{Z}$ and ϵ is a primitive m-th root of unity in k, corresponding to $e^{2\pi i/m} \in \mathbb{C}$. The irreducible Brauer characters are then $\chi_j(g) = e^{2\pi ij/m}$ corresponding to 1-dimensional simple kG-modules S_j.
We can then consider

$$x_i = \frac{1}{m} \sum_{j=1}^{m} e^{-2\pi ij/m} [S_j] \in \mathbb{C} \otimes_{\mathbb{Z}} R(G)$$

This has Brauer character $g^t \mapsto m^{-1} \sum_j e^{2\pi ij(t-1)/m} = 1_{g^t = g}$, which works (yay).
How do we do this in the general case? We'll take this Brauer character for some cyclic subgroup of G and induce it up. So let's remind ourselves of how induction works.

Lemma 6.7. *Suppose $H \leq G$ and M is a kH-module, then for a p'-element $g \in G$, we have*

$$\chi_{M\uparrow^G}(g) = \chi_M \uparrow^G (g) = \sum_{[h] \subset H, h \sim_G g} [C_G(h) : C_H(h)] \chi_M(h)$$

Here, we write $h \sim_G g$ if h, g are G-conjugates.

Proof. We defined

$$M \uparrow^G = kG \otimes_{kH} M = \bigoplus_{g_i \in G/H} (g_i \otimes M)$$

For $g \in G$ and $m \in M$, we have $g(g_i \otimes m) = g_j \otimes (hm)$ where $gg_i = g_j h$ for some j and $h \in H$. So the matrix representing the actio of g in $M \uparrow^G$ decomposes into blocks corresponding to the G-orbits of G/H. And blocks corresponding to the G-orbits of G/H of length at least 2 are of the form, say,

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

Therefore it has eigenvalue 0. On the other hand, if the singleton $\{g_i\}$ is a G-orbit of G/H, then the corresponding block represents the action of $g_i^{-1} g g_i \in H$ on M. Thus $\chi_{M\uparrow^G}(g) = \sum_{g_i^{-1} g g_i \in H} \chi_M(g_i^{-1} g g_i)$.
For $h \in H$, how many i are there with $g_i^{-1} g g_i \sim_H h$? It's reasonably clear that there are $\#C_G(h)/\#C_H(h)$ of them, hence the result. □

To finish off the proof of surjectivity, if $H \leq G$ is a subgroup, we define $\mathrm{Ind}_H^G : R(H) \to R(G)$ by sending $[M]$ to $[kG \otimes_{kH} M]$. Extending linearly, we get $\mathrm{Ind}_H^G : \mathbb{C} \otimes_{\mathbb{Z}} R(H) \to \mathbb{C} \otimes_{\mathbb{Z}} R(G)$.
Suppose we have a p'-element $g \in G$. Let $H = \langle g \rangle$ and take $x \in \mathbb{C} \otimes_{\mathbb{Z}} R(H)$ such that $\chi_x(g^i) = 1_{g^i = g}$. Then for any $g' \in G$, we can just consider

$$\chi_x \uparrow^G (g') = \sum_{[h] \subset H, h \sim_G g'} [C_G(h) : C_H(h)] \chi_x(h) = \begin{cases} |C_G(g) : \langle g \rangle| & \text{if } g' \sim_G g \\ 0 & \text{otherwise} \end{cases}$$

as in the preceding lemma.

Corollary 6.8. *Every ring homomorphism $R(G) \to \mathbb{C}$ is of the form $\tilde{\chi}(g)$ for some p'-element $g \in G$.*

This follows from the following general lemma.

Lemma 6.9. *Suppose R is a commutative ring and D is an integral domain, then every set of distinct ring homomorphisms $R \to D$ is linearly independent over D.*

Proof. Counterexample of minimal length and all that. □

Proof of Corollary 6.8. Let $\phi : R(G) \to \mathbb{C}$ be a ring homomorphism. Extend linearly, we get a homomorphism of $\mathbb{C}$-algebras $\phi : \mathbb{C} \otimes_{\mathbb{Z}} R(G) \to \mathbb{C}$. Do the same for the $\tilde{\chi}(g)$'s. The algebra homomorphisms $\tilde{\chi}(g_i)$, where g_i runs through representatives of p'-conjugacy classes, form a basis for the space of $\mathbb{C}$-algebra homomorphisms $\mathbb{C} \otimes_{\mathbb{Z}} R(G) \to \mathbb{C}$ over $\mathbb{C}$.
If $\phi \neq \tilde{\chi}(g_i)$ for any i, then the preceding lemma shows that they are linearly independent, contradiction. □

7 Decomposition Numbers and p-Modular Systems

We want to compare representations in characteristic 0 and characteristic $p > 0$. To this end, let's look at representations over $\mathbb{Z}_p$. It's easier than looking at representations over $\mathbb{Z}$, as we have the Krull-Schmidt theorem for $\mathbb{Z}_p$ but not for $\mathbb{Z}$. It's also easier than looking at $\mathbb{Z}_{(p)}$, as we have what's called an idempotent refinement in $\mathbb{Z}_p$ which allows us to "lift" projective indecomposable modules from characteristic p to characteristic 0.
Recall that a DVR is a local PID. If $\mathcal{O}$ is a DVR with maximal ideal $\mathfrak{p} = (\pi)$, we can write any nonzero $x \in \mathcal{O}$ in the form $u\pi^a, u \in \mathcal{O}^\times, a \geq 0$. We then have a valuation on $\mathcal{O}$ given by $v_\mathfrak{p}(x) = a$, which extends to $K = \mathrm{FF}(\mathcal{O})$ in the obvious way.

Definition 7.1. A p-modular system $(K, \mathcal{O}, k)$ consists of a DVR $\mathcal{O}$, $K = \mathrm{FF}(\mathcal{O})$ with characteristic 0 and $k = \mathcal{O}/\mathfrak{p}$ with characteristic p.
A p-modular system is called splitting for G if for every subgroup $H \leq G$, we have $KH \cong \prod_i \mathrm{Mat}_{d_i}(K)$ and $kH/\mathfrak{J}(kH) \cong \prod_j \mathrm{Mat}_{c_j}(k)$ for some d_i, c_j.

Example 7.1. Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers, then $\mathcal{O}$ is integral over $\mathbb{Z}$, so there is a prime (hence maximal) $\mathfrak{p} \leq \mathcal{O}$ lying over (p). Then $(K, \mathcal{O}_\mathfrak{p}, \mathcal{O}/\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p})$ is a p-modular system.
If K contains all the $|G|$-th roots of unity, then the system is splitting for G. Later, we'll require $\mathcal{O}$ to be complete, i.e. the natural map $\mathcal{O} \to \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ is an isomorphism.

Fix a p-modular system $(K, \mathcal{O}, k)$. Let V be an irreducible KG-module. Choose a basis $v_1, \ldots, v_d$ over K. Let W be the $\mathcal{O}$-span of $\{gv_i : 1 \leq i \leq d, g \in G\}$. This a finitely-generated, torsion-free $\mathcal{O}$-module, hence $\mathcal{O}$-free. G also acts on W.
Take a free basis $w_1, \ldots, w_n$ a free $\mathcal{O}$-basis for W. We know that $\{w_i\}_i$ span V over K since W contains the K-basis $v_1, \ldots, v_d$. Furthermore, by clear denominators of any linear relations we conclude that w_i are also linearly independent, so $n = d$ and $\{w_i\}_i$ is a K-basis for V. Changing basis from the v_i's to w_i's, the matrices of the representation V have entries in $\mathcal{O}$, and $V = K \otimes_\mathcal{O} W$.
W is called an $\mathcal{O}$-form for the ordinary irreducible V. Some authors say V is obtained from W by extension of scalars. W is also sometimes called an $\mathcal{O}G$-lattice.
Reducing modulo $\mathfrak{p}$ gives us a kG-module $\bar{W} = k \otimes_\mathcal{O} W = W/\mathfrak{p}W$.

Theorem 7.1. *Assume $(K, \mathcal{O}, k)$ is a splitting p-modular system for G. If W, W' are $\mathcal{O}$-forms for a KG-module V, then the kG-modules $\bar{W}, \bar{W}'$ have the same Brauer characters (hence the same composition factors).*

Proof. The Brauer characters of $\bar{W}$ is just the values on p'-elements of the ordinary characters of V. □

Definition 7.2. The decomposition matrix $D = D_{(p)}$ is defined as follows: List the irreducible KG-modules $V_1, \ldots, V_l$ and find an $\mathcal{O}$-form W_i for each V_i. List also the irreducible kG-modules $S_1, \ldots, S_m$. We then index the rows of D by $V_1, \ldots, V_l$ and columns by $S_1, \ldots, S_m$. And the (i, j)-th entry of D is taken to be $d_{ij} = [k \otimes_\mathcal{O} W_i : S_j]$ (the "(i, j)-th decomposition number").

Remark. 1. The i-th row of D can be interpreted as the modular composition factors of the kG-module $V/\mathfrak{p}V$ where V is the ordinary irreducible KG-module corresponding to the i-th row of the character table.
2. If $p \mid \#G$, then D cannot be square.
3. We'll show later that the composition numbers are independent of choices of W_i's.

Example 7.2. 1. The ordinary character table of $A_5 \cong \mathrm{SL}_2(4), \mathrm{PSL}_2(5)$ is

	1	2	3	5	5
1	1	1	1	1	1
3_1	3	-1	0	$(1+\sqrt{5})/2$	$(1-\sqrt{5})/2$
3_2	3	-1	0	$(1-\sqrt{5})/2$	$(1+\sqrt{5})/2$
4	4	0	1	-1	-1
5	5	1	-1	0	0

What's its 2-modular character table?

	1	3	5	5
1	1	1	1	1
2_1	2	-1	$(-1+\sqrt{5})/2$	$(-1-\sqrt{5})/2$
2_2	2	-1	$(-1-\sqrt{5})/2$	$(-1+\sqrt{5})/2$
4	4	1	-1	-1

So the decomposition matrix is

	1	2_1	2_2	4
1	1	0	0	0
3_1	1	1	0	0
3_2	1	0	1	0
4	0	0	0	1
5	1	1	1	0

2. The decomposition matrices of $S_3 \cong \mathrm{SL}_2(2)$ are

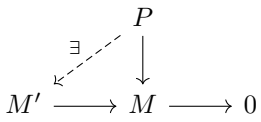
$$D_{(2)} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, D_{(3)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

3. Let G be a p-group. Then there is a unique simple kG-module, so $D_{(p)}$ has a single column, and an entry for each ordinary reducible character giving the degree of that character. For example, $G = C_2$ has decomposition matrix $(1,1)^\top$.
4. (Fong-Swan) Suppose $(K, \mathcal{O}, k)$ is a splitting p-modular system for a p-soluble group G (i.e. there is a series $1 = G_n \lhd \cdots \lhd G_0 = G$ such that G_i/G_{i+1} is either a p-group or a p'-group). Then every irreducible kG-module is a reduction modulo π of some $\mathcal{O}G$-lattice. In particular, D contains the identity matrix as a submatrix of maximal possible size.
5. Suppose $(K, \mathcal{O}, k)$ is a splitting p-modular system for G. Suppose we are in the semisimple case $p \nmid |G|$. Then each simple ordinary representation reduces to a simple modular representation of the same dimension. So reduction gives a one-to-one correspondence between simple KG-modules and simple kG-modules, and D is the identity.
6. (Exercises) Try compute the decomposition matrices of S_4 modulo $2, 3$, and probably also $\mathrm{PSL}_2(p), \mathrm{SL}_2(p)$.

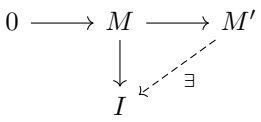
8 Projective Modules

Let R be a unital ring.

Definition 8.1. An R-module P is projective if, for every epimorphism (surjective homomorphism) $M' \to M$ of R-modules and any homomorphism $P \to M$, there is a homomorphism $P \to M'$ making



Dually, an R-module I is injective if, for every monomorphism (injective homomorphism) $M \to M'$ of R-modules and any homomorphism $M \to I$, there is a homomorphism $I \to M'$ making



Lemma 8.1. *The followings are equivalent:*
(i) P is projective.
(ii) Every epimorphism $\lambda : M \to P$ splits, i.e. there is a homomorphism $\epsilon : P \to M$ such that $\lambda \circ \epsilon = \mathrm{id}_P$.
(iii) P is isomorphic to a direct summand of a free R-module.

Proof. Exercise. □

It's clear that direct sums and direct summands of projective modules are projective.

Lemma 8.2. *Suppose k is a field and G a finite group. Then every kG-module M embeds into a free (hence projective) kG-module.*

Proof. Consider the map $\beta : M \to kG \otimes_k M = M\downarrow_{\{1\}}\uparrow^G$ by

$$m \mapsto \sum_{g \in G} g \otimes (g^{-1}m)$$

Note that G acts on $kG \otimes_k M$ is $g'(g \otimes m) = (g'g) \otimes m$. There is a splitting $\psi : kG \otimes_k M \to M$ of β over k given by

$$g \otimes m \mapsto \begin{cases} m & \text{for } g = 1 \\ 0 & \text{for } g \neq 1 \end{cases}$$

So β is injective. For $k \in G, m \in M$, one can check that $\beta(hm) = h\beta(m)$, so ϕ is a kG-homomorphism. Since k is a field, $M\downarrow_{\{1\}}$ is a free k-module, so $kG \otimes_k M$ is a direct sum of copies of kG. Therefore M is embedded in a free kG-module via β. □

Theorem 8.3. *Suppose k is a field, G a finite group and M a kG-module. Then the followings are equivalent:*
(i) M is projective.
(ii) M is injective.
(iii) (Higman's criterion) There is a k-linear map $\lambda : M \to M$ such that

$$\sum_{g\in G} g\lambda g^{-1} = \mathrm{id}_M$$

Proof. (ii) $\implies$ (i): Suppose M is injective. Consider the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{\beta} & kG \otimes_k M \\ & & \| & \swarrow_{\exists\alpha} & \\ & & M & & \end{array}$$

The splitting α of β shows that M is a summand of the free kG-module $kG\otimes_k M$, therefore projective.
(iii) $\implies$ (ii): Suppose we have an injective homomorphism $\beta : M_1 \to M_2$ and suppose $\alpha : M_1 \to M$ is a homomorphism. Choose k-linear γ (not necessarily kG-linear) such that $\gamma\beta = \alpha$. Define $\gamma' = \sum_{g\in G} g(\lambda\gamma)g^{-1}$ which is clearly kG-linear. We have

$$\gamma'\beta = \sum_{g\in G} g(\lambda\gamma)g^{-1}\beta = \sum_{g\in G} g(\lambda\gamma\beta)g^{-1} = \sum_{g\in G} g(\lambda\alpha)g^{-1} = \left(\sum_{g\in G} g\lambda g^{-1}\right)\alpha = \alpha$$

which is what we want.
(i) $\implies$ (iii): If $M = kG$, we take $\lambda(\sum_g \alpha_g g) = \alpha_1 1_G$. So

$$\sum_{h\in G} h\lambda h^{-1} \sum_{g\in G} \alpha_g g = \sum_{h\in G} h\lambda \sum_{g\in G} \alpha_g h^{-1} g = \sum_{h\in G} h\alpha_h 1_G = \sum_{h\in G} \alpha_h h$$

That is, $\sum_{h\in G} h\lambda h^{-1} = \mathrm{id}_{kG}$. If M is free, i.e. a direct sum of copies of kG, we use the same λ but on each factor. If M is a command of a free module F, define $\lambda_M = \pi\lambda_F\iota$ where $\iota : M \to F$ is the split injection and $\pi : F \to M$ is the projection. Then

$$\begin{aligned} \sum_{g\in G} g^{-1}\lambda_M g &= \sum_{g\in G} g(\pi\lambda_F\iota)g^{-1} = \sum_{g\in G} \pi(g\lambda_F g^{-1})\iota \\ &= \pi\left(\sum_{g\in G} g\lambda_F g^{-1}\right)\iota = \pi\,\mathrm{id}_F\,\iota = \mathrm{id}_M \end{aligned}$$

which is what we are after. □

9 Idempotents

First let's quote something from commutative algebra.

Theorem 9.1 (Krull-Schmidt)**.** *Let R be a finite dimensional k-algebra and M a finite R-module. Suppose $M = M_1 \oplus \cdots \oplus M_s = M_1' \oplus \cdots \oplus M_t'$ are two decompositions of M into indecomposable modules. Then $s = t$ and, possibly after reordering, $M_i \cong M_i'$.*

For our purposes, the theorem applies to finite kG-modules.

Remark. The theorem is in fact true if we just assume R to be Artinian. It is also true for finite $\mathcal{O}G$-modules. However, it is false for finite $\mathbb{Z}$-modules.

Corollary 9.2. *Let R be a finite dimensional k-algebra and M a finite indecomposable R-module. If M is a summand of finite indecomposable $M_1 \oplus \cdots \oplus M_s$, then M is a summand of some M_i.*

Corollary 9.3. *Every finite projective indecomposable R-module (where as usual R is a finite dimensional k-algebra) is isomorphic to a summand of ${}_RR$.*

So we can write ${}_RR = P_1 \oplus \cdots \oplus P_s$ as a direct sum of projective indecomposables. Since $R \cong \mathrm{End}_R(R)^{\mathrm{op}}$, the endomorphism $\pi_i : {}_RR \to P_i \to {}_RR$ given by projection followed by inclusion is right multiplication by some $e_i \in R$. Hence $P_i = {}_RRe_i$. Then $1_R = e_1 + \cdots + e_s$. These are idempotents since they come from projections.
We say two idempotents e_i, e_j are orthogonal if $e_ie_j = 0 = e_je_i$ for all $i \neq j$. An idempotent is primitive if it is nonzero and not the sum of two nonzero orthogonal idempotents.
There is a one-to-one correspondence between direct sum decompositions of ${}_RR = P_1 \oplus \cdots \oplus P_s$ with P_i projective indecomposable and expressions of the form $1 = e_1 + \cdots + e_s$ with e_i's primitive orthogonal idempotents.

Example 9.1. 1. For $R = \mathrm{Mat}_n(k)$,

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

is an idempotent conjugate (as will be defined later) to a matrix e_i with 1 at the (i,i)-th entry and zeros elsewhere. Note that $1 = I_n = e_1 + \cdots + e_n$ is a decomposition into primitive idempotents and Re_i consist of matrices all of whose nonzero entries are on the i-th column.
2. Take $R = kG, k = \mathbb{F}_2, G = C_2 = \langle x \rangle$. Consider $M = {}_RR = \{0, 1, x, 1+x\}$ which has no nontrivial idempotents as $x^1 = 1 \neq x, (1+x)^2 = 0$, so ${}_RR$ must be indecomposable.

Recall that Theorem 3.7 says that we have a decomposition

$$R/\mathfrak{J}(R) \cong \prod_{i=1}^{t} \mathrm{Mat}_{d_i}(\Delta_i)$$

for suitable d_i, Δ_i's. If $T_i = \mathrm{Mat}_{d_i}(\Delta_i)$, then ${}_{T_i}T_i$ is a direct sum of column vectors of length d_i with entries in Δ_i, and these are all simple modules all

isomorphic to each other. Let e_{ij} be the $d_i \times d_i$ matrix whose (j,j)-th entry is 1 and zeros elsewhere. Then $1_{T_i} = e_{i1} + \cdots + e_{id_i}$ and hence $1_{R/\mathfrak{J}(R)} = e_{11} + \cdots + e_{1d_1} + e_{21} + \cdots + e_{2d_2} + \cdots + e_{t1} + \cdots + e_{td_t}$.

Lemma 9.4. *If e, e' are idempotents in R, then the followings are equivalent:*
(i) $e \sim e'$ ("e, e' are conjugate") in the sense that $er = re'$ for some $r \in R^\times$.
(ii) $Re \cong Re'$ and $R(1-e) \cong R(1-e')$.

Proof. (i) $\implies$ (ii): We have $Rer = Rre' = Re'$, so $Re \cong Re'$ Since $1-e \sim 1-e'$ we similarly have $R(1-e) \cong R(1-e')$.
(ii) $\implies$ (i): Suppose $\theta : Re \to Re', \phi : R(1-e) \to R(1-e')$ are isomorphisms. Observe that for any R-module M, there is an isomorphism $\psi : \mathrm{Hom}(Re, M) \to eM, \beta \mapsto \beta(e)$. Suppose $\mu_1 \in eRe'$ corresponds $\theta \in \mathrm{Hom}(Re, Re')$, $\mu_2 \in e'Re$ corresponds to θ^{-1}, $\mu_3 \in (1-e)R(1-e')$ corresponds to ϕ and $\mu_4 \in (1-e')R(1-e)$ corresponds to ϕ^{-1}. Then $\mu_1\mu_2 = e, \mu_2\mu_1 = e', \mu_3\mu_4 = 1-e, \mu_4\mu_3 = 1-e'$. Moreover, $(\mu_2+\mu_4)(\mu_1+\mu_3) = 1$, so $\mu_1 + \mu_3 \in R^\times$ with inverse $\mu_2 + \mu_4$.
Set $r = \mu_1 + \mu_3$, then $r^{-1}er = (\mu_2+\mu_4)e(\mu_1\mu_2) = \mu_2 e\mu_1 = \mu_2\mu_1 = e'$. □

Our main is now to find projective indecomposables in ${}_RR$. The idea is to first find those in $R/\mathfrak{J}(R)$ using Theorem 3.7, and then "lift" them back to ${}_RR$. If I is an ideal of R and f is an idempotent in R, then $e = f + I$ is an idempotent in R/I. We say f lifts e.
Conversely, given an idempotent $e \in R/I$, it may or may not be possible to lift it to an idempotent in R.

Definition 9.1. If indeed every idempotent in R/I lifts to an idempotent in R, then we say that we can lift idempotents from R/I to R.

Suppose R is a finite-dimensional algebra over a field. Then $N = \mathfrak{J}(R)$ is an nilpotent of ideal of R (i.e. $N^n = 0$ for some n) since R is Artinian.

Theorem 9.5 (Idempotent Lifting/Idempotent Refinement)**.** *Suppose R is a ring and $N \leq R$ is a nilpotent ideal. Suppose e, e' are idempotents in R/N, then:*
(i) There is a idempotent $f \in R$ such that $f + N = e$. Moreover, if e is primitive, then any lift f of it must be primitive.
(ii) Suppose f, f' are idempotent in R which lift e, e'. Then $e' \sim e$ iff $f \sim f'$.

Proof. (i) We define idempotents $e_i \in R/N^i$ inductively, starting with $e_1 = e$. For $i \geq 2$, one observe that $x + N^{i-1}/N^i \in (R/N^i)/(N^{i-1}/N^i)$ corresponds to some $x' \in R/N^{i-1}$ under the third isomorphism theorem. So suppose ($i \geq 2$ and) e_{i-1} is an idempotent of R/N^{i-1}. Pick any element $a \in R/N^i$ mapping onto e_{i-1}, hence $a^2 - a \in N^{i-1}/N^i$. Since $(N^{i-1})^2 \subset N^i$, we have $(a^2-a)^2 \in N^i$. We then set $e_i = 3a^2 - 2a^3$, which maps onto $e_{i-1} \in R/N^{i-1}$ since $3a^2 - 2a^3 + N^{i-1} = (3a - 2a) + (-2a^2 + a)(a-1) + N^{i-1} = a + N^{i-1}$.
Also, $e_i^2 - e_i = (3a^2 - 2a^3)(3a^2 - 2a^3 - 1) = -(3-2a)(1+2a)(a^2-a)^2 \in N^i$, so indeed e_i is idempotent.
Since N is nilpotent, this procedure eventually gives us a lift to R.
Now suppose f is any lift of e and e is primitive. Suppose $f = f_1 + f_2$ with f_1, f_2 orthogonal idempotents, then $e = e_1 + e_2$ where $e_i = f_i + N$. Since e is primitive, one of e_1, e_2 is zero, so WLOG $f_1 \in N$. But N is nilpotent and f_1 is idempotent, so $f_1 = 0$.
(ii) Suppose $e\mu = \mu e'$ for some $\mu \in R/N$. Let β be any lift of μ to R and set $\nu = f\beta f' + (1-f)\beta(1-f')$. Then ν is invertible and $f\nu = \nu f'$ (exercise). □

Corollary 9.6. *Let $N \leq R$ be a nilpotent ideal and let $1 = e_1 + \cdots + e_s$ be a decomposition of 1 into orthogonal idempotents in R/N. Then there is a decomposition $1 = f_1 + \cdots + f_s$ of 1 into orthogonal idempotents in R such that $f_i + N = e_i$ for all i. Moreover, if the e_i's are primitive, then so are the f_i's.*

Corollary 9.7. *Let f be an idempotent in R and N a nilpotent ideal, then f is primitive iff $f + I$ is primitive in R/I.*

10 Projective Indecomposable Modules (PIMs)

Let R be a finite dimensional k-algebra.
Recall that for a finitely generated R-module M, its radical $\mathfrak{J}(M)$ is

$$\mathfrak{J}(M) = \mathfrak{J}(R)M = \bigcap_{N \leq M \text{ maximal submodule}} N$$

which is the smallest submodule of M with semisimple quotient.
We also set $\mathrm{Soc}(M)$ (the "socle" of M) to be the sum of all simple submodules of M, which is the largest semisimple submodule of M, which is also $\{m \in M : \mathfrak{J}(R)M = 0\}$.
By Theorem 3.7, $R/\mathfrak{J}(R) = \prod_{i=1}^{s} \mathrm{Mat}_{d_i}(\Delta_i)$ for suitable d_i, Δ_i. Note that each $1_{M_{d_i}}$ has a primitive orthogonal decomposition $\bar{e}_{i1} + \cdots + \bar{e}_{id_i}$, corresponding to the simple modules given by the columns. That is, $\bar{e}_{ij}$ is the matrix in $M_{d_i}(\Delta_i)$ with 1 at the (j,j)-th entry and zero elsewhere. And so we have a primitive orthogonal decomposition $1_{R/\mathfrak{J}(R)} = \bar{e}_{11} + \cdots + \bar{e}_{1d_1} + \cdots + \bar{e}_{s1} + \cdots + \bar{e}_{sd_s}$.
Since $\mathfrak{J}(R)$ is nilpotent, we can lift this to get a primitive orthogonal decomposition $1_R = e_{11} + \cdots + e_{1d_1} + \cdots + e_{s1} + \cdots + e_{sd_s}$.
We therefore get a decomposition ${}_RR = Re_{11} \oplus \cdots \oplus Re_{1d_1} \oplus \cdots \oplus Re_{s1} \oplus \cdots \oplus Re_{sd_s}$ into projectives. For each (i,j), $Re_{ij}/\mathfrak{J}(Re_{ij}) = Re_{ij}/(\mathfrak{J}(R)e_{ij}) = (R/\mathfrak{J}(R))\bar{e}_{ij} \cong S_i$ where S_i is a simple R-module. Write $P_{S_i} = P_i$ for a module isomorphic to Re_{ij} for some j. It is called a projective cover of S_i.
We have s isomorphism classes of projective indecomposable R-modules $P_i, 1 \leq i \leq s$, and each P_i has a unique maximal submodule $\mathfrak{J}(P_i)$.

Example 10.1. Suppose $\mathrm{char}\, k = p$ and G is a p-group. Take $R = kG$. Since there is only on p'-class in G, there is a unique simple R-module, namely the trivial R-module. Then $\mathfrak{J}(R)$ is the augmentation ideal and $R/\mathfrak{J}(R) \cong k_G$. Thus there exists a unique projective indecomposable ${}_RR$. Its composition length is $\#G$.

In general, let M be any finite R-module so that $M/\mathfrak{J}(M) \cong \bigoplus_i S_i$. For each i, we let P_i be the projective cover of S_i. Then $\bigoplus_i P_i$ is also projective, so there is some R-linear π such that

$$\begin{array}{ccccc} & & \bigoplus_i P_i & & \\ & \overset{\pi}{\swarrow} & \downarrow & & \\ M & \longrightarrow & M/\mathfrak{J}(M) & \longrightarrow & 0 \end{array}$$

π is surjective as it is surjective modulo $\mathfrak{J}(M)$: Write $N = \pi(\bigoplus_i P_i)$. Since $N + \mathfrak{J}(R)M = M$, we have $M = N$ by Lemma 3.4.

So π induces an isomorphism $(\bigoplus_i P_i)/\mathfrak{J}(\bigoplus_i P_i) \cong M/\mathfrak{J}(M)$. We call $\bigoplus_i P_i$ the projective cover of M. Denote $\Omega(M) = \ker \pi$ (Ω is called the Heller operator). We therefore have the short exact sequence

$$0 \longrightarrow \Omega(M) \longrightarrow \bigoplus_i P_i \longrightarrow M \longrightarrow 0$$

Let $R = kG$. If M is a left R-module, then $M^* = \mathrm{Hom}_k(M, k)$ is a right R-module via $(fr)(m) = f(rm)$. Similarly, if M is a right R-module, then M^* is a left R-module. If M is finite dimensional, then $(M^*)^* \cong M$ canonically.
Since $\mathrm{Hom}_k(-, k)$ is an exact functor from the category of finite left (resp. right) R-modules to the category of finite right (resp. left) R-modules, we have a correspondence between finite projective left (resp. right) R-modules and finite injective right (resp. left) R-modules, given by taking dual. The same functor also gives a correspondence between simple and indecomposable modules.

Remark. Under our running assumption that $R = kG$ for a finite group G, a left R-module is also a right R-module via $mg = g^{-1}m$.

Consequently, if I is an injective R-module, then I has a unique minimal (therefore simple) submodule.
Write I_{S_i} for the injective indecomposable R-module that has S_i as unique simple submodule (i.e. $\operatorname{Soc} I_i = S_i$). I_i is called the injective hull of S_i. In general, if M is a finite R-module, $\operatorname{Soc} M \cong \bigoplus_j S_j$ for simple S_j with injective hulls I_j, respectively. By injectivity of $\bigoplus_j I_j$, there is some $\iota : M \to \bigoplus_j I_j$ such that the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \operatorname{Soc} M & \longrightarrow & M \\ & & \downarrow & \swarrow_{\iota} & \\ & & \bigoplus_j I_j & & \end{array}$$

and we similarly get the injectivity of ι from the injectivity on the socle. So we have an isomorphism $\operatorname{Soc} M \cong \bigoplus_j I_j$. We call $\bigoplus_j I_j$ the injective hull of M. Denote $\mho(M) = \operatorname{coker} \iota$, which gives an exact sequence

$$0 \longrightarrow M \longrightarrow \bigoplus_j I_j \longrightarrow \mho(M) \longrightarrow 0$$

Remark. Sadly, $\Omega, \mho$ are not inverses to each other in the category of finite R-modules, but they are inverses in a certain derived category.

Theorem 10.1. *Suppose G is finite and k is a field. If P is a projective indecomposable kG-module, then $P/\mathfrak{J}(P) \cong \operatorname{Soc}(P)$.*

Proof. Write $P = kGe$ for some primitive idempotent $e \in kG$. Let $x \in \operatorname{Soc}(P)$ be nonzero. So $x = \sum_g \alpha_g g$ and there is some $h \in G$ with $\alpha_h \neq 0$.
Observe that for any $\lambda = \sum_g \lambda_g g, \mu = \sum_g \mu_g g \in kG$, the coefficient of 1_G in $\lambda\mu$ is $\sum_g \lambda_g \mu_{g^{-1}} = \sum_g \lambda_{g^{-1}} \mu_g$, which is the coefficient of 1_G in $\mu\lambda$.
Set $y = h^{-1}x = \sum_g \beta_g g$. Then $\beta_1 \neq 0$ by construction. Since $y = ye$ has nonzero coefficient for 1_G, ey too has nonzero coefficient for 1_G. In particular, $ey \neq 0$ and thus $e \operatorname{Soc}(P) \neq 0$.
We then have $\mathrm{Hom}_{kG}(P, \operatorname{Soc}(P)) = \mathrm{Hom}_{kG}(kGe, \operatorname{Soc}(P)) \cong e \operatorname{Soc}(P) \neq 0$. Recall that P is also an injective indecomposable kG-module, so $\operatorname{Soc}(P)$ is simple. Hence $P/\mathfrak{J}(P) \cong \operatorname{Soc}(P)$. □

Remark. This is a special property enjoyed by so-called symmetrical algebras.

Definition 10.1. $P/\mathfrak{P}$ is often called the head $\mathrm{hd}(P)$ of P.

Recall that Schur's lemma says that if R is a finite-dimensional algebra over a field k with k algebraically closed, then $\mathrm{End}_R(S) \cong k$ for any simple R-module S. We really don't have to assume k to be as big as being algebraically closed. We say k is a splitting field for R if this does happen. Phrased differently,

Definition 10.2. Let R be a finite dimensional F-algebra with F a field (not necessarily algebraically closed). We say a simple R-module S is absolutely irreducible if $E \otimes_F S$ is a irreducible $E \otimes_F R$-module for any field extension E/F.
E/F is a splitting field for R iff every simple $E \otimes_F R$-module is absolutely irreducible. When $R = FG$, we call E/F the splitting field for G.

Example 10.2. 1. Take $G = \langle x \rangle$ with x having order $n \geq 3$. x acts on $\mathbb{C}G$ as the direct sum of 1-dimensional eigenspaces with eigenvalues being powers of $e^{2\pi i/n}$. Since these lie outside $\mathbb{Q}$, the regular representation $\mathbb{Q}G$ is a direct sum of simple modules with some of them having dimension greater than 1. But if we extend to a field K containing $e^{2\pi i/n}$, the simple modules decompose as direct sums of 1-dimensional modules. So $\mathbb{Q}$ is not a splitting field for G but K is (since 1-dimensional simples cannot possibly decompose further).
2. $\mathbb{F}_p$ is a splitting field for any p-group, since there is a unique simple KG-module for any field K with characteristic p.
3. Any field F is a splitting field for $\mathrm{Mat}_n(F)$.

Proposition 10.2. *Suppose S is a simple module for a finite-dimensional F-algebra R. Then the followings are equivalent:*
(i) S is absolutely irreducible.
(ii) $\mathrm{End}_R(S) \cong F$.
(iii) The matrix summands of $R/\mathfrak{J}(R)$ (cf. Theorem 3.7) corresponding to S has the form $\mathrm{Mat}_n(F)$ *where* $n = \dim_F S$.

Proposition 10.3. *R always has a splitting field of finite degree over F. If G is a group and $R = FG$, it has splitting fields that are finite degree extensions of $\mathbb{Q}$ (when* $\mathrm{char}\, F = 0$*) or $\mathbb{F}_p$ (when* $\mathrm{char}\, F = p > 0$*).*
(Brauer) Moreover, if F contains a primitive m-th root of unity where m is the exponent of G, then F is a splitting field for G.

Lemma 10.4. *Let R be a finite dimensional k-algebra. Assume k is a splitting field for R. Then for any finite R-module M, we have* $\dim_k \mathrm{Hom}_R(P_S, M) = [M : S]$ *where P_S is the projective cover of S.*

Proof. Induction on composition length of M. If $M = S'$ is simple, then this is true as k is a splitting field.
If M is not irreducble, choose a maximal (proper) submodule $M' \lneq M$. We have a short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

for M'' simple. As P_S is projective, $\mathrm{Hom}_R(P_S, -)$ is exact, so we have the short exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(P_S, M') \longrightarrow \mathrm{Hom}_R(P_S, M) \longrightarrow \mathrm{Hom}_R(P_S, M'') \longrightarrow 0$$

Taking dimensions finishes the induction step. □

11 Cartan Invariants

Suppose G is finite and k is a field of characteristic p. Irreducible kG-modules S_i corresponds to their projective covers P_{S_i}.

Definition 11.1. The Cartan invariants are $c_{ij} = [P_{S_j}, S_i]$. The matrix $C = (c_{ij})_{i,j}$ is called the Cartan matrix for kG.

Theorem 11.1. *(i) If k is a splitting field for G, then the Cartan matrix for kG is symmetric.*
(ii) If $(K, \mathcal{O}, k)$ is a splitting modular system for G with $\mathcal{O}$ complete, then $c_{ij} = \sum_l d_{li} d_{lj}$.
(iii) $\det C$ is a power of p. In particular, it is nonzero.

We'll sketch the proof of (ii). Part (iii) is not quite easy. In general, the Cartan matrix may be singular if we are not dealing with group algebras.
Recall that $\mathcal{O}$ is a complete DVR with unique maximal ideal $\mathfrak{p}$ such that $\mathcal{O}/\mathfrak{p} = k$. Since the canonical surjection $\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G \to \mathcal{O}G/\mathfrak{p}\mathcal{O}G \cong kG$ has kernel $\mathfrak{p}\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G$, which squares to 0. A primitive orthogonal decomposition $1 = \bar{e}_1 + \cdots + \bar{e}_s$ in kG lifts to a primitive orthogonal decomposition $1 = e_{2,1} + \cdots + e_{2,s}$ in $\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G$. Repeating the process using the surjections $\mathcal{O}G/\mathfrak{p}^3\mathcal{O}G \to \mathcal{O}G/\mathfrak{p}^2\mathcal{O}G$ lifts $1 = e_{2,1} + \cdots + e_{2,s}$ to $1 = e_{3,1} + \cdots + e_{3,s}$ in $\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G$ Continuing this process further gives a decomposition $1 = e_{n,1} + \cdots + e_{n,s}$ in $\mathcal{O}G/\mathfrak{p}^n\mathcal{O}G$ for each n with the property that $e_{n,j} + \mathfrak{p}^{n-1} = e_{n-1,j}$.
Since $\mathcal{O}$ is complete, we have $\mathcal{O}G = \varprojlim_n \mathcal{O}G/\mathfrak{p}^n\mathcal{O}G$. Hence there are $e_j \in \mathcal{O}_G$ such that $e_j + \mathfrak{p}^n = e_{n,j}$ for all n. But then $(e_j^2 + \mathfrak{p}^n)_n$ is the same inverse system of elements as $(e_j + \mathfrak{p}^n)_n$ does, so $e_j^2 = e_j$. Similarly $1 = e_1 + \cdots + e_s$ is a primitive orthogonal decomposition of 1 in $\mathcal{O}G$. In other words,

Theorem 11.2. *If $1 = \bar{e}_1 + \cdots + \bar{e}_s$ is a decomposition of 1 into primitive idempotents in kG, then we can lift it to $1 = e_1 + \cdots + e_s$ in $\mathcal{O}G$. Moreover, if $1 = e_1' + \cdots + e_s'$ is another such lift, then $e_i \sim e_i'$ for all i.*

Consequently, if we decompose kG into projective indecomposables $kG = P_{S_1}^{\oplus d_1} \oplus \cdots \oplus P_{S_n}^{\oplus d_n}$, then they lift to $\mathcal{O}G = \hat{P}_{S_1}^{\oplus d_1} \oplus \cdots \oplus \hat{P}_{S_n}^{\oplus d_n}$.

Proof sketch for Theorem 11.1(ii). Recall that given simple KG-modules $\{V_i\}$, we get $\mathcal{O}$-forms W_i satisfying $V_i = K \otimes_{\mathcal{O}} W_i$. What is the multiplicity of V_i as a factor of $K \otimes_{\mathcal{O}} \hat{P}_{S_j}$? We have

$$\begin{aligned}
[K \otimes_{\mathcal{O}} \hat{P}_{S_j} : V_i] &= \dim_K \operatorname{Hom}_{KG}(K \otimes_{\mathcal{O}} \hat{P}_{S_j}, V_i) \\
&= \dim_K \operatorname{Hom}_{KG}(K \otimes_{\mathcal{O}} \hat{P}_{S_j}, K \otimes_{\mathcal{O}} W_i) \\
&\overset{\text{(a)}}{=} \dim_K \left(K \otimes_{\mathcal{O}} \operatorname{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i) \right) \\
&= \operatorname{rk}_{\mathcal{O}} \operatorname{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i) \\
&\overset{\text{(b)}}{=} \dim_k \operatorname{Hom}_{kG}(P_{S_j}, k \otimes_{\mathcal{O}} W_i) \\
&= [k \otimes_{\mathcal{O}} W_i : S_j] = d_{ij}
\end{aligned}$$

(a) is true because $\mathcal{O}$ is a PID and $\hat{P}_{S_j}, W_i, \operatorname{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i)$ are all $\mathcal{O}$-free. Given any KG-linear $K \otimes_{\mathcal{O}} \hat{P}_{S_j} \to K \otimes_{\mathcal{O}} W_i$, some nonzero multiple of it must

send $\hat{P}_{S_j}$ to W_i by finite generation. Hence the map $K \otimes_{\mathcal{O}} \mathrm{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i) \to \mathrm{Hom}_{KG}(K \otimes_{\mathcal{O}} \hat{P}_{S_j}, K \otimes_{\mathcal{O}} W_i)$ taking $\lambda \otimes \phi$ to $\lambda\phi$ is an isomorphism.
As for (b), $k \otimes_{\mathcal{O}} -$ induces a map $\mathrm{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i) \to \mathrm{Hom}_{kG}(P_{S_j}, \bar{W}_i)$ (where $\bar{W}_i = k \otimes_{\mathcal{O}} W_i$). This is surjective since $\hat{P}_{S_j}$ is projective, and its kernel is $\mathfrak{p}\,\mathrm{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i)$. This – with some technical details skipped – gives (b).
Knowing these, we now have

$$\begin{aligned} c_{ij} &= \dim_k \mathrm{Hom}_{kG}(P_{S_i}, P_{S_j}) = \mathrm{rk}_{\mathcal{O}} \mathrm{Hom}_{\mathcal{O}G}(\hat{P}_{S_i}, \hat{P}_{S_j}) \\ &= \dim_K \mathrm{Hom}_{KG}(K \otimes_{\mathcal{O}} \hat{P}_{S_i}, K \otimes_{\mathcal{O}} \hat{P}_{S_j}) = \sum_l d_{li} d_{lj}. \end{aligned}$$ □

We have a couple of nice consequences.

Remark. 1. Recall that the rows of the decomposition matrix corresponds to multiplicities of modular factors in the modular reductions of ordinary irreducibles. The columns of the decomposition matrix now have an interpretation as well: They are the ordinary factors of the lifts of modular projective indecomposables. This is because $D^\top D = C$ encodes the modular irreducible factors of modular projective indecomposables.
2. The decomposition numbers d_{ij} is independent of choice of $\mathcal{O}$-forms.
3. C is symmetric.