

Modular Representation Theory

Lectured by Professor Stuart Martin

Notes taken by Amy Needham

January 2025

Contents

1 Ordinary and Modular representations	2
2 Representations and Modules	2
2.1 Reducibility and Decomposability	3
3 Homs, Tensors and Exactness	4
3.1 Exactness	5
4 The Jacobson radical	6
5 Brauer Characters	9
6 Character Tables and the Choice of Lifting	15
7 Grothendieck Ring	17
8 Decomposition Numbers and p-Modular Systems	21
8.1 Decomposition Numbers	22
9 Projective Modules	24
10 Idempotents and Principal Indecomposable Modules	27
11 Projective Covers	30
12 Cartan Invariants	34

1 Ordinary and Modular representations

Most theorems and statements left unproven here are in Webb's book. Usually we start with an algebraic object A and we put it into a black box which "does representation theory" and we get modules on which A acts and their morphisms (A category of A -modules). Here A is an associative k -algebra. We could also do things on other structures (eg semigroups, monoids, etc) but we won't

Example 1.1. A could be

1. $n \times n$ matrices with coefficients in a field ($M_n(k)$)
2. Polynomials in k with n variables, $k[x_1, \dots, x_n]$
3. $\text{End}_k(V)$ of endomorphisms of a vector space. If V is finite dimensional over k , this is just example 1 again
4. The group algebra, kG , which is the vector space with basis indexed by G and the obvious multiplication where G is a finite group

We will study $A = kG$ via its actions on vector spaces. An A module representation of A is exactly just a finite dimensional vector space over k with a linear G action.

The actions depend on the relationship between the order of the group and the characteristic of the field. Recall

Theorem 1.1. (*Maschke's Theorem*) If $\text{char}(k) \nmid |G|$ then all reps are semisimple - direct sums of irreducible/simple representations

This case is ordinary representation theory. By modular representation theory we mean the case when $\text{char}(k) \mid |G|$. In this case kG is not a semisimple algebra (proof later)

Example 1.2. Take G to be a p -group and k a field with $\text{char}(k) = p$. Then kG is local, and hence has a unique irreducible representation (the trivial representation)

2 Representations and Modules

Definition 2.1. A **Representation** of a (finite) group G over a commutative unital ring k of coefficients is a group homomorphism $\phi: G \rightarrow GL_n(k)$. The **Degree** of the representation is n

Definition 2.2. The **Group Algebra**, kG , is the k -vector space spanned by the basis G with the obvious addition and multiplication

$$\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g = \sum_{g \in G} (\alpha_g + \beta_g) g$$

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

Check that this is a ring, and is a k algebra if k is a field

Lemma 2.1. *Every left kG module induces a unique representation ϕ of G and conversely*

Proof. Trivial □

Example 2.1. If k is a field, representations of G over k are finite dimensional left kG modules

Remark. A left kG module is just a space V and a homomorphism of algebras $kG \rightarrow \text{End}(V)$. Some authors say a left kG module is a "representation of algebras". (2.1) then says a group representation is an algebra representation of the group algebra

Definition 2.3. Two representations ϕ, ψ of degrees n, m are **isomorphic (equivalent, similar)** if $n = m$ and there is a $X \in GL_n(k)$ such that we have $X\phi(g)X^{-1} = \psi(g)$ for all $g \in G$. This corresponds to an isomorphism of kG modules.

More generally, an **intertwining operator** 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 of kG modules

Example 2.2. There is an example for C_2 in the notes

2.1 Reducibility and Decomposability

Definition 2.4. A representation $\phi: G \rightarrow GL_n(k)$ is **reducible** if it is similar to a representation ψ such that $\psi(g) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$. If A is $i \times i$, then the subspace spanned by the first i basis vectors is an **invariant subspace**, that is, W is invariant if $gw \in W$ for all $w \in W$.

A representation is **irreducible/simple** if it is non-zero and not reducible

Definition 2.5. A representation $\phi: G \rightarrow GL_n(k)$ is **decomposable** if it is similar to a representation ψ such that $\psi(g) = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. In terms of modules, this says $V = W_1 \oplus W_2$ with W_i an invariant subspace.

A representation is **indecomposable** if there is no such similar module.

Example 2.3. We have the following examples of modules and decompositions

1. If $G = \{1, t\}, t^2 = 1, V = \mathbb{C}^2$ with basis $\{e_1, e_2\}$, then

$$V = \langle e_1 + e_2 \rangle \oplus \langle e_1 - e_2 \rangle$$

This fails mod 2

2. If $A = kS_n$, then $V = \{(x_1, \dots, x_n) \in k^n \mid \sum x_i = 0\}$ is a simple A -module
3. Show that the only simple modules for $M_n(k)$ are k^n

Definition 2.6. A **short exact sequence** (abbreviated SES) of kG -modules and kG -module homomorphisms is a sequence of the form

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

such that for every pair of composable arrows, the image of the left one is the kernel of the right one.

In other words, V_1 is isomorphic to a submodule of V_2 with quotient equal to V_3 . We say V_2 is an **extension** of V_1 by V_3 .

A short exact sequence as above **splits** if there is a map $\gamma: V_3 \rightarrow V_2$ such that $\beta \circ \gamma = \text{Id}$ called a **splitting**.

In this case $V_2 = \alpha V_1 \oplus \gamma V_3 \cong V_1 \oplus V_3$

Example 2.4. All SESs of vector spaces over $\mathbb{C}$ split

Theorem 2.2. (*Maschke's Theorem*) If $|G| \in k^\times$, a short exact sequence of kG -modules

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

which splits as a sequence of k -modules then it splits as a sequence of kG -modules

Proof. As in the proof of Maschke's theorem, averaging the k -splitting over G □

3 Homs, Tensors and Exactness

Recall if R is a ring and M is a right R module and N is a left R module we can construct the tensor product $M \otimes_R N$ generated by symbols $m \otimes n$ for $m \in M, n \in N$ with certain relations.

If R is commutative, left and right modules coincide and $M \otimes_R N$ is again an R module via $r(m \otimes n) = rm \otimes n = m \otimes rn$ for $r \in R, n \in N, m \in M$

If R, S are rings then M is an (R, S) -**bimodule** if it is a left R module and a right S module, and $(rm)s = r(ms)$ for $r \in R, s \in S, m \in M$

Given an (R, S) -bimodule M and a left S module N , $M \otimes_S N$ is a left R module via $r(m \otimes n) = rm \otimes n$

Definition 3.1. Regard the ring R as an (R, R) -bimodule. If $S \subset R$, we can regard R as an (R, S) -bimodule. If $H \leq G$, regard kH as a subalgebra of kG and regard kG as a (kG, kH) -bimodule.

If M is a kH module, $kG \otimes_{kH} M$ is a left kG module called the **induced module** denoted $M \uparrow^G$

Definition 3.2. For $S \geq R$ and N a left R module, M a S, R -bimodule, Z a left S -module (for some permutation of the words "left", "right", "S", "R"). We may use the universal property to show

$$\text{Hom}_R(N, \text{Hom}_S(M, Z)) \cong \text{Hom}_S(M \otimes_R N, Z)$$

In particular, $\text{Hom}_{kH}(U, \text{Hom}_{kG}(kG, V)) \cong \text{Hom}_{kG}(kG \otimes_{kH} U, V)$. Viewing kG as a (kG, kH) -bimodule, $\text{Hom}_{kG}(kG, V)$ is just V as a left kH module by **restriction**, denoted $V \downarrow_H$

Corollary 3.0.1. (*Frobenius reciprocity*)

$$\text{Hom}_{kH}(U, V \downarrow_H) = \text{Hom}_{kG}(U \uparrow^G, V)$$

*This is called the **Nakayama isomorphism***

Remark. If U, V are kG -modules, $U \otimes_k V$ becomes a kG module via

$$g(u \otimes v) = gu \otimes gv$$

General elements of the group algebra act via linear extension from this, not necessarily by $r(u \otimes v) = ru \otimes rv$. Similarly, $\text{Hom}(U, V)$ becomes a kG module via

$$(gf)(u) = gf(g^{-1}u), (u \in U, f \in \text{Hom}(U, V), g \in G)$$

Exercise 3.1. If U, V, W are kG modules,

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

3.1 Exactness

Lemma 3.1. If M is a right R -module, and we have

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

an exact sequence of left R -modules, then

$$N \otimes_R M \longrightarrow N' \otimes_R M \longrightarrow N'' \otimes_R M \longrightarrow 0$$

is exact.

If M, N, N', N'' are left R -modules, and we have short exact

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

, then

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

is short exact.
Furthermore if

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

is exact, so is

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

Lemma 3.2. *If*

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

is a short exact sequence of finite dimensional kG -modules and $M_2 \cong M_1 \oplus M_3$, then the sequence splits

Proof. We know

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

is exact. Counting dimensions (using more theory), the right-most map is surjective, then take the preimage of the identity on M_3 . This defines a splitting $\square$

4 The Jacobson radical

Let R be a unital ring.

Definition 4.1. The **Jacobson radical** of R is

$$\mathcal{J}(R) = \bigcap \text{maximal left ideals of } R$$

Example 4.1. $\mathcal{J}(\mathbb{Z}) = \bigcap_{p \text{ prime}} p\mathbb{Z} = \{0\}$

Lemma 4.1.

$$\mathcal{J}(R) = \bigcap_{M \text{ simple left } R \text{ modules}} \operatorname{ann}_R(M) = \bigcap_{\text{maximal left ideals}} \operatorname{ann}_R(R/I)$$

Proof. Exercise. $\square$

Remark. This result shows two things

1. The annihilators are two-sided ideals, and therefore we see that $\mathcal{J}(R)$ is a two-sided ideal
2. Simple left R -modules are quotients of R by maximal left ideals.

Lemma 4.2. $\mathcal{J}(R) = \{y \in R \mid \forall a, b \in R, 1 - ayb \text{ has a two sided inverse}\}$

Proof. Atiyah-Macdonald (commutative case) $\square$

Corollary 4.2.1. $\mathcal{J}(R) = \bigcap \text{maximal right ideals}$

Lemma 4.3. (*Nakayama's Lemma*) If M is a finitely generated R -module and $\mathcal{J}(R)M = M$ then $M = 0$

Proof. Atiyah-Macdonald (commutative case) □

Definition 4.2. An R -module, M , is **semisimple (s.s.)** or **completely reducible** if M is a direct sum of simples

Proposition 4.1. 1. Every submodule of a semi-simple module is semi-simple and a direct summand

2. Every quotient of a semi-simple module is semi-simple

3. M is semi-simple if and only if every submodule is a direct summand

Proof. No Proof □

Theorem 4.4. Suppose R is left Artinian. Then the following are equivalent

1. $\mathcal{J}(R) = 0$

2. Every R -module is semi-simple

3. Every finitely generated R module is semi-simple

Proof. Suppose $\mathcal{J}(R) = 0$ and let $M \subset {}_R R$ be minimal such that it is the intersection of a finite number of maximal left ideals, which we can do as R is Artinian. Then M is in every maximal left ideal, and hence $M = 0$ and furthermore $0 = \bigcap_{i=1}^n \mathfrak{m}_i$. There is therefore an injection ${}_R R \rightarrow \bigoplus_{i=1}^n R/\mathfrak{m}_i$ which is a sum of simples, so ${}_R R$ is semi-simple.

For the converse, suppose ${}_R R$ is semisimple. Then $\mathcal{J}(R)$ is a summand of ${}_R R$, ie ${}_R R = \mathcal{J}(R) \oplus R/\mathcal{J}(R)$. Applying $\mathcal{J}(R)$ to both sides, $\mathcal{J}(R) = \mathcal{J}^2(R)$. Since $\mathcal{J}(R)$ is a quotient of R , it is finitely generated, so is 0 by Nakayama □

Remark. If S is a ring, S^{op} is the opposite ring, with multiplication $a \circ b = ba$

Theorem 4.5. (*Artin-Wedderburn*) Let R be a finite dimensional k -algebra and suppose $\mathcal{J}(R) = 0$ Then

$$R = \prod_{i=1}^m M_{d_i}(\Delta_i)$$

is a product of matrix algebras over finite dimensional division rings Δ_i containing k in their centre

Proof. (Sketch).

1. Take any unital ring R . $R \cong \text{End}_R({}_R R)^{\text{op}}$ via $r \mapsto (s \mapsto sr)$

2. ${}_R R = S_1^{d_1} \oplus \cdots \oplus S_m^{d_m}$ where S_i are non-isomorphic irreducible modules with multiplicities $d_1, \dots, d_m$ in the regular representation (consequence of $\mathcal{J}(R) = 0$)

3. Schur's Lemma: $\text{End}_R(S_i)$ is a division ring
4. If $V = \bigoplus_{i=1}^r V_i$ then $\text{End}_R(V) = M_r(\text{Hom}_R(V_j, V_i))$
5. Conclude (as $\text{Hom}_R(S_i, S_j) = 0$ if $i \neq j$).

□

Remark. We have some corollaries and special cases of this

1. If $k = \bar{k}$ then each $\Delta_i = k$. For example by Maschke's theorem, $\mathbb{C}G$ is semi-simple and

$$\mathbb{C}G = \prod_{i=1}^n M_{d_i}(\mathbb{C})$$

2. For an example of (1), $\mathbb{C}S_3 = \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$
3. The left ideals of any $M_d(\mathbb{C})$ are in 1-1 correspondence with subspaces of $\mathbb{C}^d$ and $M_d(\mathbb{C})$ is a direct sum of its column left ideals
4. If $k = \mathbb{R}$ then the possible division rings are $\mathbb{R}, \mathbb{C}, \mathbb{H}$. This is called the Frobenius-Schur indicator (and is very non-trivial)
5. If k is a finite field then Wedderburn's little theorem says each Δ_i is a finite field (no proof)
6. If $k = \bar{k}$ then there are m isomorphism classes of irreducible modules, with dimensions $d_1, \dots, d_m$ over k (exercise)
7. If $k = \bar{k}$, then $m = \dim_k Z(R)$ as $Z(R) = \prod_1^m Z(M_i(k)) \cong k^m$. Moreover, $\dim_k R = \sum_1^m d_i^2 = \sum_1^m (\dim_k S_i)^2$
8. If $G = \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/9\mathbb{Z}$ and S is a simple $\mathbb{Q}G$ module on which G acts faithfully. Then $\text{End}_{\mathbb{Q}G}(S)$ is 9 dimensional over its centre
9. If $R = U_n(k)$ is the ring of upper triangular matrices and $k = \bar{k}$, then the Jacobson radical $\mathcal{J}(R) = \{A \mid a_{ii} = 0\}$ is the set of strictly upper triangular matrices and $R = \mathcal{J}(R) \oplus D$ where $D =$ diagonal matrices. $\mathcal{J}(D) = 0$ so Artin-Wedderburn applies to D , and actually $D \cong k \oplus \dots \oplus k$.

Example 4.2. $\mathbb{H} = \mathbb{R}\langle i, j, k, \mid i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j \rangle$ is a division algebra, so has no left ideals and is hence simple (hence semisimple) of dimension 4 over $\mathbb{R}$ so if Artin-Wedderburn holds for $\mathbb{R}$ then $\mathbb{H} \cong M_2(\mathbb{R})$ or $\mathbb{H} = \mathbb{R}^4$ which are both false as neither are division rings

5 Brauer Characters

Definition 5.1. A group element is a *p element/unipotent/p singular* if its order is a p th power.

It is a *p' element/p regular/semisimple* if its order is coprime to p

Lemma 5.1. *Let G be a finite group and $g \in G$. We can write $g = xy = yx$ such that*

1. x is a p element
2. y is a p' element
3. Every element of G which commutes with g commutes with x, y

The elements x, y are unique and called the p **part** and p' **part** of g respectively

Proof.

Existence: Let $n = p^\alpha m$ be the order of g where $(p, m) = 1$. Bezout implies there is $s, t \in \mathbb{Z}$ such that $sp^\alpha + tm = 1$. Then $g = g^{tm} g^{sp^\alpha}$ and we claim that $x = g^{tm}, y = g^{sp^\alpha}$ work. But $x^{p^\alpha} = 1$ so $o(x) \mid p^\alpha$ and similarly $o(y) \mid m$ so x, y are a p element/ p' element respectively.

(3) is immediate as x, y are powers of g .

Let $g = x_1 y_1 = y_1 x_1$ be another such decomposition. Then $x_1^{-1} x = y_1 y^{-1}$ but this is an equality of a p element and a p' element, so we are done as the identity is the only such. $\square$

Definition 5.2. Let M be a $\mathbb{C}G$ module. There is a class function of the form $\chi_M: \{\text{conjugacy classes in } G\} \rightarrow \mathbb{C}$ by $g \mapsto \text{Tr}(g, M)$ called the **ordinary character of M** .

Let M, M' be $\mathbb{C}G$ modules. In II Representation Theory we proved:

1. $\chi_{M \oplus M'} = \chi_M + \chi_{M'}$
2. $\chi_{M \otimes M'} = \chi_M \chi_{M'}$
3. $\chi_M = \chi_{M'}$ if and only if $M \cong M'$

We want to try to replicate this for modular representations. We will construct a theory where (1), (2) hold, but (3) will be weakened to (3'): "if and only if the composition series have the same factors".

Problem: If for kG -module M , M is a direct sum of p copies of M' for $p = \text{char}(k)$, then for all g , $\text{Tr}(g, M) = p \text{Tr}(g, M') = 0$. This was resolved by Brauer with "Brauer characters"

If $\text{char}(k) = p$, write $m = p^\alpha m'$ where $p \nmid m'$. In $k[X]$, $X^m - 1 = (X^{m'} - 1)^{p^\alpha}$ hence k will contain the m th roots of unity if and only if k contains the m' th roots of unity. The polynomial $X^{m'} - 1$ is separable over k and its roots form a cyclic group $C_{m'}$ of order m' generated by the primitive m' th roots of unity

Lemma 5.2. *Let G a finite group, $\text{char}(k) = p$ and k contains all the $|G|_{p'}$ th roots of unity (the p' part of the order of G). Let $g \in G$ and let ϕ be a representation of G over k . Then the eigenvalues of $\phi(g)$ and the eigenvalues of $\phi(y)$ coincide where y is the p' part of g*

Proof. By changing basis with matrix P , we may assume $P^{-1}\phi(g)P$ is upper triangular where the eigenvalues, $\lambda_1, \dots, \lambda_n$ are on the diagonal. Let $g = xy$ where x is the p part and y is the p' part. Let the order of x be p^s for some $s \in \mathbb{N}$ and we have $\text{Id} = P^{-1}\phi(x^{p^s})P = P^{-1}\phi(g^{tp^s})P = (P^{-1}\phi(g)P)^{tp^s}$ which has eigenvalues $\lambda_1^{tp^s}, \dots, \lambda_n^{tp^s}$ hence $(\lambda_i^t)^{p^s} = 1$ for all i . So as we are in a field of characteristic p , $\lambda_i^t = 1$. Thus $P^{-1}\phi(x)P$ is upper triangular with 1s on the diagonal. This shows the eigenvalues of x are all 1 and so $\text{Tr}(x) = \dim_k(M)$ where M is the module of the representation ϕ . Now $P^{-1}\phi(g)P = P^{-1}\phi(x)\phi(y)P = P^{-1}\phi(x)PP^{-1}\phi(y)P$ so the eigenvalues of $\phi(y)$ and of $\phi(g)$ are the same $\square$

Definition 5.3. Let G be a finite group, and k a field of characteristic p containing all $|G|_{p'}$ roots of unity. These form a cyclic group of order $|G|_{p'}$ under multiplication and all eigenvalues of $g \in G$ live in this group

Choose an isomorphism ψ from the group of $|G|_{p'}$ roots of unity in k to the $|G|_{p'}$ roots of unity in $\mathbb{C}$. This is sometimes called a **lifting**.

Let M be a finite dimensional kG module. Define the **Brauer character** of g_M , a p' element with eigenvalues $\lambda_1, \dots, \lambda_n$, to be the sum of the images of the eigenvalues of g_M under ψ ie

$$\chi_M(g) = \sum_{i=1}^n \psi(\lambda_i)$$

So $\chi_M(g)$ is a cyclotomic integer and there is a map, as with the ordinary character, $\chi_M: \{p'\text{-order conjugacy classes}\} \rightarrow \mathbb{C}$

Example 5.1. We look at some examples

1. Let G be a group and $k = \bar{k}$ of characteristic p . If $g \in G$ and M a finite dimensional kG modules. Then g induces a k -linear map on M which is annihilated by the polynomial $X^{|G|} - 1$ by multiplication. Since $X^{|G|} - 1 = (X^{|G|_{p'}} - 1)^{|G|_p}$ and $X^{|G|_{p'}} - 1$ is a product of linear factors in $k[x]$, g has a Jordan canonical form and every eigenvalue of g is a $|G|_{p'}$ root of unity

2. Let $\begin{pmatrix} \lambda & 1 & * & * \\ 0 & \lambda & 1 & * \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$ be a Jordan block of g . It is conjugate to the decomposition position $\begin{pmatrix} \lambda & \lambda & 0 & 0 \\ 0 & \lambda & \lambda & 0 \\ 0 & 0 & \lambda & \lambda \\ 0 & 0 & 0 & \lambda \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$ where the

first matrix is the p part, as it is $1 + n$ for n nilpotent and the second matrix is the p' part as λ is not a p th root of unity. Also each is easily seen to commute with any matrix that commutes with the conjugate of g , so these truly are the p, p' parts of g . Hence if $g = xy$ is a decomposition of g into its p, p' parts called x, y respectively, then x_M has only diagonal entries equal to 1 and y_M is diagonalisable. Thus $\text{Tr}(g, M) = \text{Tr}(y, M)$ and $\text{Tr}(x, M) = \dim_k(M)$

3. Let $k = \mathbb{F}_2, G = \langle x \mid x^3 = 1 \rangle$. We have a 2-dimensional representation M of G over k by $x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ with characteristic polynomial $x^2 + x + 1$, eigenvalues the primitive roots of unity in $\mathbb{F}_4$. Lifting these to the primitive third roots of unity in $\mathbb{C}$, we get $\chi(x) = e^{2\pi i/3} + e^{4\pi i/3} = -1$. Note $\text{Tr}(x, M) = 1$ but $\chi_M(g) \neq 1$

Remark. Recall the following. Let μ be a matrix representation of G such that for all $g \in G$, $\mu(g)$ is block upper triangular with two blocks on the diagonal, $\begin{pmatrix} A(g) & * \\ 0 & B(g) \end{pmatrix}$. Defining $\sigma(g) = A(g)$ and $\tau(g) = B(g)$, we said $\mu(g)$ is reducible, and we now say σ, τ are **constituents** of μ . Recall also that if μ is reducible, then the corresponding module M has a non-zero proper submodule, S , which corresponds to σ , and is called the **top constituent** and τ which corresponds to M/S is the **bottom constituent**. If M has no such S , then it (and μ) is irreducible

Lemma 5.3. *Given two modular representations, σ and τ , which have the same Brauer character. Then for all $g \in G$, $\sigma(g), \tau(g)$ have the same eigenvalues*

Proof. We are given $\chi_\sigma = \chi_\tau$. Let $\sigma(g)$ have eigenvalues $\epsilon^{\alpha_1}, \dots, \epsilon^{\alpha_a}$ and $\tau(g)$ have eigenvalues $\epsilon^{\beta_1}, \dots, \epsilon^{\beta_b}$. By taking i th powers of each ϵ^j , we get the characteristic roots of $\sigma(g^i)$ and $\tau(g^i)$. Let ζ be a primitive $|G|_{p'}$ th root of 1 in $\mathbb{C}$ and $\zeta = \psi(\epsilon)$. Then $\zeta^{i\alpha_1} + \dots + \zeta^{i\alpha_a} = \zeta^{i\beta_1} + \dots + \zeta^{i\beta_b}$. Consider the complex representations $\sigma'(g^i) = \text{diag}(\zeta^{i\alpha_1}, \dots, \zeta^{i\alpha_a})$ and $\tau'(g^i) = \text{diag}(\zeta^{i\beta_1}, \dots, \zeta^{i\beta_b})$ of the cyclic group generated by g . We know that $\text{Tr}(g, \sigma') = \text{Tr}(g, \tau')$ so the complex representations σ', τ' are equal hence the irreducible constituents are the same by the ordinary theory. Hence the sets $\{\alpha_1, \dots, \alpha_a\} = \{\beta_1, \dots, \beta_b\}$ are equal $\square$

Recall the Jordan-Holder theorem: A **composition series** of M is a series of submodules

$$0 \subset M_1 \subset \dots \subset M_l = M$$

where M_j/M_{j-1} are non-zero simple. Then any two series for M are equivalent, ie $M_i/M_{i-1} \cong M'_j/M'_{j-1}$ for some reordering of the terms, and in particular the **(composition) length** is invariant, denoted $l(M)$. The irreducible factors correspond to irreducible constituents $\rho_1, \dots, \rho_l$ of the representation ρ which corresponds to M . Therefore every representation has a fixed number of irreducible constituents which are unique up to equivalence and ordering. M is

uniserial if it has a unique composition series

Let $\mathcal{B}$ be an ordered basis of M in the composition series, ie the basis is of the form $\mathcal{B} = \{e_1^1, \dots, e_{n_1}^1, e_1^2, \dots, e_{n_2}^2, \dots, e_1^l, \dots, e_{n_l}^l\}$ where $\{e^i \mid i \leq j\}$ is a basis for M_j . The representation ρ has an upper block triangular form, with the diagonal blocks being the $\rho_i(g)$ corresponding to each M_i/M_{i-1}

Theorem 5.4. *Let $\text{char}(k) = p$ and $k = \bar{k}$. Then each simple kG -module S has the same multiplicity in M, M' modulo p , that is $[M : S] = [M' : S] \pmod{p}$ if and only if for $g \in G$, $\text{Tr}(g, M) = \text{Tr}(g, M')$*

Proof. For the forward direction, without loss of generality, M and M' are semi-simple as we don't care about the off-block-diagonal entries (replace a non-semi-simple module with the sum of its composition factors).

Now

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

where α_i is the multiplicity of S_i in M , and β_i its multiplicity in M' so this direction is done

In the backwards direction, if $\text{Tr}(x, M) = \text{Tr}(x, M') \pmod{p}$ for all $x \in G$ then it holds for all $x \in kG$ by linearity. By Wedderburn applied to $kG/J(kG)$,

$$\bigoplus_{i=1}^r n_i S_i \cong kG/J(kG) \cong M_{n_1}(k) \times \dots \times M_{n_r}(k)$$

where each $n_i S_i \cong M_{n_i}(k)$. Recall that each simple kG module S_i is isomorphic to some $kG/\mathfrak{m}_i$ for some maximal ideal $\mathfrak{m}_i$. Hence we observe that M, M' are direct sums of $m_i S_i$ and $m'_i S_i$. Now any of the matrix algebras contains a matrix of the form $\text{diag}(1, 0, \dots, 0)$. Call its preimage $x_i \in kG$. Then we know that $\text{Tr}(x_i, S_j) = \delta_{ij}$ and so $\text{Tr}(x_i, M) = m_i$ and we are done as $\text{Tr}(x_i, M') = m'_i$ hence $m_i = m'_i \pmod{p}$ $\square$

Theorem 5.5. (*Brauer's Theorem*) *Let M, M' be finite dimensional kG modules. Then $\chi_M = \chi_{M'}$ if and only if the multiplicities of each simple kG -module as composition factors of M, M' are equal*

Proof. We may again assume that M, M' are semisimple for the same reason as 5.4.

For the backwards direction, we've already seen that since the multiplicities of each simple kG module as composition factors are equal, then the characters are equal

In the forwards direction, assume that $\chi_M = \chi_{M'}$ and seek a minimal counterexample in dimension. We may assume M, M' don't share a composition factor in common, as otherwise we may remove it. We know that $\text{Tr}(g, M) = \text{Tr}(g, M')$ so by 5.4, the multiplicities of any composition factor in M, M' are congruent mod p . Write $M = e_1 S_1 \oplus \dots \oplus e_\kappa S_\kappa$ and $M' = e'_1 S_1 \oplus \dots \oplus e'_\kappa S_\kappa$ where we have $e_i = e'_i \pmod{p}$ and at most one of e_i, e'_i is non-zero as M, M' have no factors in common. Therefore $p \mid e_i$ and $p \mid e'_i$ and we can write $e_i = pf_i, e'_i = pf'_i$. We now

	e	(12)	(123)
1	1	1	1
σ	1	-1	1
ψ_v	2	0	-1

Table 1: Ordinary representations of S_3

	1	(123)
$\bar{1}$	1	1
$\bar{V}$	2	-1

Table 2: Representations of S_3 in $\mathbb{F}_2$

have that $M = pM_1$ and $M' = pM'_1$ for some M_1, M'_1 . But $\dim_k M = p \dim_k M_1$ and $\chi_M = p\chi_{M_1}$. Doing the same for the M', M'_1 half, we get a smaller example, contradiction. $\square$

Example 5.2. We have some examples Let $G = S_3$. This has 3 conjugacy classes, represented by $e, (12), (123)$. Over $\mathbb{C}$ we have three representations: the trivial representation, the sign representation, and the representation permuting coordinates in elements of $V = \{(x_1, x_2, x_3)^t \mid x_1 + x_2 + x_3 = 0\}$. We have a basis for V given by $B = \{v_1 = (1, -1, 0), v_2 = (0, 1, -1)\}$. In this basis we have

$$\begin{aligned} (123) &\mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \\ (12) &\mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

So the ordinary character table is as in Table 1

Over $\mathbb{F}_2$ we have two conjugacy classes of $2'$ elements, the 3 cycles and the identity. We will eventually show that the number of irreducible representations over a field of characteristic p is the number of p' conjugacy classes. So we have two irreducible Brauer characters given by the trivial character, $\bar{1}$ and the reduction of V , called $\bar{V}$ with the same matrix as in characteristic 0, but interpreted as $\mathbb{F}_2$ elements. We have Brauer character table as in Table 2

Over $\mathbb{F}_3$ we have again 2 irreducible Brauer characters, namely $\bar{1}$ and $\bar{\sigma}$ as $\bar{V}$ is a sum of these two. The Brauer Character table is Table 3. We say irreducible characters of S_3 in characteristics 2, 3 lift to characteristic 0 (their character tables are sub-tables of the ordinary representations).

	1	(12)
$\bar{1}$	1	1
$\bar{\sigma}$	1	-1

Table 3: Representations of S_3 in $\mathbb{F}_3$

Another fact (that probably won't be proven here): the number of 1d Brauer characters is $[G : [G, G]]$ which is 1 in characteristic 2 and 2 in characteristic 3.

Example 5.3. For cyclic groups of order p^s see Webb.

6 Character Tables and the Choice of Lifting

Recall an **algebraic integer** is an element of $\mathbb{C}$ satisfying a monic polynomial with integer coefficients and a **number field** is a subfield $K \leq \mathbb{C}$ of finite degree over $\mathbb{Q}$. Denote the **ring of integers** in K by $\mathcal{O}_K = K \cap \{\text{algebraic integers}\}$. If $a \in K$, there is some $0 \neq c \in \mathbb{Z}$ such that $ca \in \mathcal{O}_K$.

Definition 6.1. An integral domain R is a **Dedekind domain** if

1. It is integrally closed
2. R is Noetherian
3. Every non-zero prime ideal of R is maximal

It is a fact that for a number field K , $\mathcal{O}_K$ is a Dedekind domain.

Let G be a finite group, k a field of characteristic $p \neq 0$ and $|G| = p^a m$ where $p \nmid m$. Suppose k is sufficiently large as to contain all the m th roots of unity. Let $C, \hat{C}$ be the groups of m th roots of unity in k and $\mathbb{C}$ respectively. Let $K = \mathbb{Q}[\hat{C}]$.

Lemma 6.1. $\text{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^*$

Proof. Trivial □

Take $\mathcal{O}_K$ to be the ring of integers in K . Since $\mathcal{O}_K$ is a Dedekind domain, every prime ideal is maximal, so we want to choose a prime (and hence maximal) ideal, $\mathfrak{p}$, lying over (p) , that is, such that $\mathfrak{p} \cap \mathbb{Z} = (p)$. Then

Proposition 6.1. $\mathcal{O}_K/\mathfrak{p}$ 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

1. $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^r}$
2. $\hat{C} + \mathfrak{p} \cong C$
3. $\text{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) \cong \text{stabiliser of } \mathfrak{p} \text{ in } \text{Gal}(K/\mathbb{Q})$

Proof. Take a primitive m th root of unity, $\zeta \in \mathbb{C}$. $\hat{C} = \langle \zeta \rangle$ and $K = \mathbb{Q}(\zeta)$. We know that $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

1. $\mathcal{O}_K/\mathfrak{p}$ is the extension of $\mathbb{Z}/p\mathbb{Z}$ generated by $\zeta + \mathfrak{p}$
2. Take the polynomial

$$\frac{x^m - 1}{x - 1} = x^{m-1} + \cdots + 1 = \prod_{j=1}^{m-1} (x - \zeta^j)$$

and, letting $x = 1$, the ideal generated by $(1 - \zeta^j) \mid m$ in $\mathcal{O}_K$ for all $j = 1, \dots, m-1$. If $1 - \zeta^j \in \mathfrak{p}$, $m \in \mathfrak{p}$, contradiction as $(m, p) = 1$ and $\mathfrak{p} \cap \mathbb{Z} = (p)$. Therefore $1 - \zeta^j \notin \mathfrak{p}$ for all $1 \leq j \leq m-1$

3. $\zeta + \mathfrak{p}$ is a primitive m th root of unity

□

Example 6.1. Suppose we take $G = C_n$ and $n = p^a m$ where p, m are coprime. The p' elements are $\{1, x^{p^a}, \dots, x^{(m-1)p^a}\}$ and the p elements are the elements $\{1, x^m, \dots, x^{(p^a-1)m}\}$. Now if $\rho: G \rightarrow k^\times$ then $\rho(x)^n = 1$ so $\rho(x)^m = 1$. Define ρ_i for each $i = 0, 1, \dots, m$ by $\rho_i(x) = \omega^i$ where ω is a primitive m th root of unity in k . Take $n = 12 = 2^2 \cdot 3$ and let $p = 2$. The $2'$ elements are $\{1, x^4, x^8\}$ and the 2 elements are $\{1, x^3, x^6, x^9\}$. Construct the table whose columns are indexed by powers of x and rows by the ρ_i , shown as table 4. We actually just need the $2'$ elements to capture all the information, as the 2 elements have $\rho_i(x^j) = 1$. We can therefore construct a smaller table as in table 5. Now choose an isometry of cyclic groups from the m th roots of unity in k to the m th roots of unity in $\mathbb{C}$, call it ψ by sending $\psi(\omega) = \zeta$. Then define the **Brauer character table** (mod 2) by table 6 (left). If we chose the other isomorphism of the cyclic groups, $\psi(\omega) = \zeta^2$ then we would get table 6 (right) and so the Brauer character table depends on the isomorphism ψ

	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

Table 4: Character table of C_{12} modulo 2

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

Table 5: 'Reduced' character table of C_{12} modulo 2

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

Table 6: Brauer character tables of C_{12} modulo 2

Definition 6.2. The **Brauer character table** of $G \bmod p$ is a table where the rows are indexed by the simple kG modules and rows by conjugacy classes of p' elements of G whose entries are the values of the Brauer characters $\chi_S(g)$

We will prove:

Theorem 6.2. *The irreducible Brauer characters form a basis for the class functions on the conjugacy classes of p' elements and hence the Brauer character table is square. The rows of the Brauer character table for G are the irreducible Brauer characters and the columns are homomorphisms for G are ring homomorphisms $\tilde{\chi}(g): R(G) \rightarrow \mathbb{C}$ where $R(G)$ is the Grothendieck ring, which will be defined next chapter*

Remark. After fixing an isomorphism $\psi: C \rightarrow \hat{C}$ all other such isomorphisms $C \rightarrow \hat{C}$ are obtained by applying elements of $\text{Gal}(K/\mathbb{Q})$ to $\hat{C}$

Proposition 6.2.

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

Proof.

1. If ζ is a primitive m th root of unity in $\mathbb{C}$ then $K = \mathbb{Q}(\zeta)$ and an element of the Galois group sends ζ to ζ^t for some t coprime to m and so for all p' elements $g \in G$, $\tilde{\chi}^\sigma(g) = \tilde{\chi}(g^t)$
2. Now σ stabilises $\mathfrak{p}$ if and only if t is a power of p . Let S be a simple module with corresponding representation $\rho: G \rightarrow GL_n(k)$. Then S^σ is a kG -module with corresponding representation $\rho^\sigma: G \rightarrow GL_n(k)$ by $g \mapsto (\lambda_{ij}(g)^t)$

□

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

If ψ, ψ' are two choices of the isomorphism of groups of roots of unity and we change the Brauer character table then columns are preserved and sometimes rows are preserved

Example 6.2. $p = 2, m = 7$. The 7th roots of unity in k have 2 possible minimal polynomials, $x^3 + x^2 + 1$ or $x^3 + x + 1$ so let ζ be a 7th root of unity in $\mathbb{C}$. Then there are two prime ideals in $\mathbb{Z}[\zeta]$ called $\mathfrak{p}_1 = (2, \zeta^3 + \zeta^2 + 1)$ and $\mathfrak{p}_2 = (2, \zeta^3 + \zeta + 1)$ which lie over (2) such that $\mathbb{Z}[\zeta]/\mathfrak{p}_1 \cong \mathbb{F}_8 \cong \mathbb{Z}[\zeta]/\mathfrak{p}_2$.

7 Grothendieck Ring

Let G be a finite group and k a field of characteristic p containing all the $|G|_{p'}$ roots of unity. We form an abelian group $R(G)$ as follows

Definition 7.1. The **Grothedieck group** is the group $R(G)$ generated by symbols $[M]$ where M is an isomorphism class of finite dimensional kG modules with relations $[M_2] = [M_1] + [M_2]$ for every short exact sequence of kG modules

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

Remark. We have the following comments

1. We take isomorphism classes rather than kG modules themselves because the latter collection is not a set
2. $R(G)$ is a free abelian group on the symbols of simple modules by the Jordan-Holder theorem
3. We make $R(G)$ a commutative ring by introducing the natural multiplication $[M][N] = [M \otimes_k N]$ where the kG -module structure of $M \otimes_k N$ is the diagonal action. This is well defined as the modules are flat over k , and is commutative as tensor products are, and the multiplicative identity is k
4. $R(G)$ can be denoted by $G_0(kG)$ as well
5. Every element of $R(G)$ is expressible as a difference, $[M] - [N]$. If $k = \mathbb{C}$ then $R(G)$ is the ring of virtual characters of $\mathbb{C}G$ modules

Lemma 7.1. For N, M, M_i each kG modules, the following hold

1. $\chi_M(1) = \dim_k M$
2. χ_M is a class function on p' conjugacy classes
3. $\chi_M(g^{-1}) = \overline{\chi_M(g)} = \chi_{M^*}(g)$
4. If

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

is a short exact sequence of finite dimensional modules, $\chi_{M_2} = \chi_{M_1} + \chi_{M_3}$, So χ_M depends only on the isomorphism type of M . If M has composition factors S_i each with multiplicity n_i then $\chi_M = \sum_{i=1}^n n_i \chi_{S_i}$

5. $\chi_{M \otimes_k N} = \chi_M \chi_N$

Proof. Trivial □

Corollary 7.1.1. For all conjugacy classes of p' elements $g \in G$, the map $\tilde{\chi}: R(G) \rightarrow \mathbb{C}$ by $[M] \mapsto \chi_M(g)$ is a well defined ring map

Proof. Trivial □

Theorem 7.2. The product of the maps $\tilde{\chi}_M$, which is a map

$$R(G) \rightarrow \prod_{p' \text{ conjugacy classes of } G} \mathbb{C}$$

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

Proof. Suppose that $[M] - [N]$ and $[M'] - [N']$ go to the same place under this map. Then $\chi_M - \chi_N = \chi_{M'} - \chi_{N'}$ so $\chi_M + \chi_{N'} = \chi_N + \chi_{M'}$ and hence $\chi_{M \oplus N'} = \chi_{N \oplus M'}$ so that $[M \oplus N'] = [M' \oplus N]$ hence $[M] + [N'] = [M'] + [N]$ and we are done as then $[M] - [N] = [M'] - [N']$. $\square$

Now we will prove

Theorem 7.3. *The map*

$$\mathbb{C} \otimes_{\mathbb{Z}} R(G) \rightarrow \prod_{p' \text{ conjugacy classes of } G} \mathbb{C}$$

is an algebra isomorphism.

Proof.

Lemma 7.4. *(Injectivity) The irreducible Brauer characters χ_{S_i} are linearly independent over $\mathbb{C}$*

Proof. Let $K \leq \mathbb{C}$ the smallest field containing the $|G|_{p'}$ roots of unity and $\mathcal{O}$ its ring of integers. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}$ containing (p) . Now $\mathcal{O}_{\mathfrak{p}} \leq K$ is the localisation of $\mathcal{O}$ at $\mathfrak{p}$. Let $\mathfrak{m}_{\mathfrak{p}}$ be its unique maximal ideal and we have $\mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p} \hookrightarrow k$. Moreover $\mathcal{O}_{\mathfrak{p}}$ is a principal ideal domain so we write $\mathfrak{m}_{\mathfrak{p}} = (\pi)$. Suppose there is a linear dependence over $\mathbb{C}$ among the irreducible Brauer characters. Then there is also a linear dependence over K as all character values live in K . Clearing denominators, there is a relation over $\mathcal{O}$. If all the coefficients of the relation now lie in $\mathfrak{p}$ we may divide out by a power of π to get a relation where at least one of the coefficients is not in $\mathfrak{p}$, but all are in $\mathcal{O}$. Now reduce everything modulo $\mathfrak{m}_{\mathfrak{p}}$, and we get a linear relation in k between the traces

$$\sum_{i=1}^n \alpha_i \text{Tr}(x, S_j) = 0, \forall x \in kG$$

By Wedderburn (and the previous proof in 5.4), we get some x_i for all $1 \leq i \leq n$ such that $\text{Tr}(x_i, S_j) = \delta_{ij}$ and so all $\alpha_i = 0$. $\square$

We now turn to surjectivity. The idea is, for each a p' element $g \in G$, we will find an element of $\mathbb{C} \otimes_{\mathbb{Z}} R(G)$ such that $\tilde{\chi}(g)$ sends it to something non-zero and $\tilde{\chi}(h)$ sends it to 0 for p' element h not conjugate to g . First take $G = \langle g \rangle$, $|g| = m$ and $(m, p) = 1$. The irreducible representations of G over k are of the form $g \mapsto (\epsilon)$ where $\epsilon^m = 1$ in k . ϵ will be a primitive m th root of unity in k corresponding to $e^{2\pi i/m} \in \mathbb{C}$. So the irreducible Brauer characters are of the form $\chi_j(g) = e^{2\pi i j/m}$ with corresponding 1 dimensional simple kG modules S_j . Then we note that $x = \frac{1}{m} \sum_{j=1}^m e^{-2\pi i j/m} [S_j] \in \mathbb{C} \otimes_{\mathbb{Z}} R(G)$ has Brauer character $\chi_x: g^t \mapsto \frac{1}{m} \sum_{j=1}^m e^{2\pi i j(t-1)/m}$ which is 1 if $g^t = g$ and 0 otherwise. In the general case, we take this Brauer character for some cyclic subgroup of G and induce it up

Lemma 7.5. *Let $H \leq G$ and M a kH -module. Then for all $g \in G$ which are p' ,*

$$\chi_{M \uparrow^G}(g) = \sum_{\text{ccls in } H \text{ such that } h=g_0 g g_0^{-1}} |C_G(h) : C_H(h)| \chi_M(h)$$

Proof. See part II □

To finish, if $H \leq G$ define $\text{Ind}_H^G : R(H) \rightarrow R(G)$ by $[M] \mapsto [kG \otimes_{kH} M]$ and extend it linearly to get $\text{Ind}_H^G : \mathbb{C} \otimes_{\mathbb{Z}} R(H) \rightarrow \mathbb{C} \otimes_{\mathbb{Z}} R(G)$. Given p' element $g \in G$, let $H = \langle g \rangle$ and take $x \in \mathbb{C} \otimes_{\mathbb{Z}} R(H)$ such that $\chi_x(g^i)$ is 1 if $g^i = g$ and 0 otherwise. Then for $g' \in G$, we have $\chi_{x \uparrow^G} = \sum |C_G(h) : C_H(h)| \chi_x(h)$ which is $|C_G(g) : \langle g \rangle|$ if g' is conjugate to g , and 0 otherwise so we are done. □

Immediately, we get

Corollary 7.5.1. *(Brauer) The number of simple kG modules is the number of p' conjugacy classes of G*

Proof. Trivial □

Example 7.1. We have a couple examples

1. If G is a p -group, the only simple kG module is the trivial module
2. If $p = 0$ we get the usual theorem on squareness of the (ordinary) character table

Corollary 7.5.2. *Every ring homomorphism $R(G) \rightarrow \mathbb{C}$ is of the form $\tilde{\chi}(g)$ for some p' element $g \in G$*

We need the following lemma for this

Lemma 7.6. *For a commutative unital ring R and D an integral domain. Then any set of distinct ring homomorphisms $R \rightarrow D$ is linearly independent over D*

Proof. Take a linear relation of smallest size, $\sum_{i=1}^n \lambda_i \phi_i = 0$, $\phi_i : R \rightarrow D$ and $0 \neq \lambda_i \in D$. Choose $r_0 \in R$ such that $\phi_1(r_0) \neq \phi_n(r_0)$. So for all $r \in R$,

$$\sum_{i=1}^n \lambda_i \phi_i(r_0 r) = \sum_{i=1}^n \lambda_i \phi_i(r_0) \phi_i(r) = 0$$

. Multiplying the original relation evaluated at r by $\phi_n(r_0)$ and subtracting, we get a shorter relation

$$\sum_{i=1}^{n-1} \lambda_i (\phi_i(r_0) - \phi_n(r_0)) \phi_i(r) = 0$$

, and the first term isn't zero as D is a domain, contradiction □

Proof. (of the corollary) Let $\phi: R(G) \rightarrow \mathbb{C}$ be a ring homomorphism and extend linearly to an algebra homomorphism $\phi: \mathbb{C} \otimes_{\mathbb{Z}} R(G) \rightarrow \mathbb{C}$. Do the same for the $\tilde{\chi}(g)$. Then we get that the algebra homomorphisms $\tilde{\chi}(g_i)$ with g_i representatives of the p' conjugacy classes form a basis over $\mathbb{C}$ for the space of complex linear maps $\mathbb{C} \otimes R(G) \rightarrow \mathbb{C}$ so we are done by the lemma. $\square$

We want to be able to compare representations in characteristic 0 with those in characteristic p . We use representations over the p -adic integers as an intermediary. This is because

1. It is easier than using $\mathbb{Z}$ as we have Krull Schmidt (Chapter 10)
2. Better than the p -local integers as we have idempotent refinement (Chapter 10) which allows us to lift projective indecomposables from characteristic p (Chapter 11)

8 Decomposition Numbers and p -Modular Systems

Recall that a discrete valuation ring (DVR) is a PID with a unique maximal ideal. If $\mathcal{O}$ is a DVR with maximal ideal $\mathfrak{p} = (\pi)$, we can write any non-zero element x in the form $y\pi^a$ where $a \in \mathbb{N}$ and $y \in \mathcal{O}^\times$: if $x \in \mathfrak{p}$ factorise $x = \pi y_1$ and inductively repeat since $\mathfrak{p}$ is prime, and since $\mathcal{O}$ is a PID, this process terminates with $y_k \notin \mathfrak{p}$. Define $\nu_{\mathfrak{p}}(x) = a$. Let $K = \text{Frac}(\mathcal{O})$ be the field of fractions. Then if $x \in K$, $x = y\pi^a$ for some $a \in \mathbb{Z}$ and $y \in \mathcal{O}^\times$.

Definition 8.1. A p -modular system is a triple $(K, \mathcal{O}, k)$ consisting of

1. A DVR $\mathcal{O}$
2. Its field of fractions K of characteristic 0
3. $k = \mathcal{O}/\mathfrak{p}$ the residue field of characteristic p

A p -modular system $(K, \mathcal{O}, k)$ is **splitting for G** if for any $H \leq G$

1. $KH = \prod_i M_{d_i}(K)$
2. $kH/\mathcal{J}(kH) = \prod_i M_{c_i}(k)$

Example 8.1. Take an algebraic number field K and its ring of integers $\mathcal{O}$. Then $K = \text{Frac}(\mathcal{O})$. Now $\mathcal{O}$ is integral over $\mathbb{Z}$ so there is a prime $\mathfrak{p}$ (which must be maximal) of $\mathcal{O}$ lying over (p) . The localisation $\mathcal{O}_{\mathfrak{p}}$ is a DVR and so we have a p -modular system $(K, \mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}/\mathfrak{p})$.

Remark.

1. If K contains the $|G|$ th roots of unity, then $(K, \mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}/\mathfrak{p} = k)$ is splitting
2. We later require that $\mathcal{O}$ is complete, ie $\mathcal{O} \rightarrow \varprojlim \mathcal{O}/\mathfrak{p}^n$ is an isomorphism

8.1 Decomposition Numbers

Given a p -modular system $(K, \mathcal{O}, k)$, consider V which is an irreducible kG module. Choose a basis $v_1, \dots, v_d$ over K for V . We look at the sub $\mathcal{O}$ module $W = \text{span}_{\mathcal{O}}\{gv_i \mid 1 \leq i \leq d, g \in G\}$. This is a finitely generated torsion free module, hence it is free over $\mathcal{O}$ on which G acts. This $\mathcal{O}$ span W is a subset of V and $\text{Frac}(\mathcal{O}) = K$. Webb calls this an $\mathcal{O}G$ lattice. Take $w_1, \dots, w_n$ an $\mathcal{O}$ -basis of W . The w_i span V over K . If there is a linear relation between the w_i over K , clearing denominators we get an $\mathcal{O}$ -linear combination, so all terms are 0 so there is no non-trivial relation between the w_i over K , and hence $n = d$ as $w_1, \dots, w_n$ is a K basis of V . Changing basis from the v_i to the w_i , all entries in the matrix representation of G are in $\mathcal{O}$ and not just K and $V = K \otimes_{\mathcal{O}} W$.

Definition 8.2. The set W is called an $\mathcal{O}$ -form for the ordinary irreducible KG module V . Some say that V is obtained from W by extending the scalars from $\mathcal{O}$ to K .

In general a module has many non-isomorphic $\mathcal{O}$ -forms, however

Theorem 8.1. Assume $(K, \mathcal{O}, k)$ is a splitting p -modular system. If W, W' are both $\mathcal{O}$ -forms of V , then the kG modules $\overline{W} = k \otimes_{\mathcal{O}} W = W/\mathfrak{p}W$ and $\overline{W'}$ (defined similarly) have the same Brauer character, hence have the same composition factors

Proof. Suppose the ordinary character of V is ϕ_V . If g is a p' element it acts with eigenvalues $\lambda_1, \dots, \lambda_n$ on W , then g acts on $\overline{W}$ with eigenvalues given by $\lambda_1 + (\pi), \dots, \lambda_n + \pi$. Since $\chi_{\overline{W}}(g)$ is the sum of the lifts of these $\lambda_i + (\pi)$, we get $\chi_{\overline{W}}(g) = \lambda_1 + \dots + \lambda_n = \text{Tr}(g, V) = \phi_V(g)$ $\square$

Definition 8.3. List the ordinary irreducible KG modules $V_1, \dots, V_l$. List the $\mathcal{O}$ -forms $W_1, \dots, W_l$ of them, and list the modular irreducible kG modules $S_1, \dots, S_m$. We define the **decomposition matrix** $D \pmod{p}$ has

1. Rows indexed by the irreducible KG modules $\{V_i \mid 1 \leq i \leq s\}$
2. Columns indexed by the irreducible kG modules $\{S_j \mid 1 \leq j \leq m\}$
3. Entries d_{ij} given by choosing an $\mathcal{O}$ -form W_i for V_i and defining the d_{kl} as $d_{ij} = [k \otimes_{\mathcal{O}} W_i : S_j]$, called the **decomposition number**

Remark. If $p \mid |G|$ then D cannot be the identity because it isn't even square (as there are fewer p' conjugacy classes than conjugacy classes)

Example 8.2. We have a few examples

1. $|A_5| = 2^2 \cdot 3 \cdot 5$. $A_5 \cong SL_2(2^2) \cong PSL_2(5)$ has ordinary character table as in table 7. In characteristic 2, we have Brauer character table on the left in table 8 and decomposition matrix on the right. The other primes are in Webb, pages 310-312. If we multiply the decomposition matrix by the Brauer character table, we get X reduced mod 2

2. Let $G = C_2$. In characteristic 2, we only have the trivial irreducible, and the decomposition matrix has one column consisting of a list of dimensions of the ordinary characters
3. $S_3 = SL_2(2)$ has ordinary character table in table 9, Brauer character tables in tables 10, and decomposition matrices in tables 11
4. Try S_4 . $PSL_2(p), SL_2(p)$ are done in Webb, chapter 6, exercise 25
5. If G is a p group and we work in characteristic p , then D_p the decomposition matrix is a column of the dimensions of the ordinary irreducible characters, as in the C_2 case above as G has a unique (trivial) irreducible kG -
6. Let $(K, \mathcal{O}, k)$ be a splitting p -modular system for G and $(|G|, p) = 1$, the semi-simple case. Then each irreducible KG module reduces to an irreducible kG module of the same dimension and $D = I$ (proved in Webb)

A_5	60	(12)(34) 4	(123) 3	(12345) 5	(13524) 5
	1	1	1	1	1
	3_1	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
	3_2	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
	4	0	1	-1	-1
	5	1	-1	0	0

Table 7: Ordinary character table of A_5

A_5	60	(123) 3	(12345) 5	(13524) 5	A_5	1	2_1	2_2	4
	1	1	1	1	1	1	0	0	0
	3_1	-1	$\frac{-1+\sqrt{5}}{2}$	$\frac{-1-\sqrt{5}}{2}$	3_1	1	1	0	0
	3_2	-1	$\frac{-1-\sqrt{5}}{2}$	$\frac{-1+\sqrt{5}}{2}$	3_2	1	0	1	0
	4	1	-1	-1	4	0	0	0	1
	5	1	-1	-1	5	1	1	1	0

Table 8: Brauer character table and decomposition matrix of A_5 mod 2

S_3	1	(12)	(123)
	6	2	3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Table 9: The ordinary character table of S_3

$p = 2$	1	(123)	$p = 3$	1	(12)
ϕ_1	1	1	ϕ_1	1	1
ϕ_2	2	-1	ϕ_2	1	-1

Table 10: The Brauer character tables of S_3 modulo 2, 3

$p = 2$	ϕ_1	ϕ_2	$p = 3$	ϕ_1	ϕ_2
χ_1	1	0	χ_1	1	0
χ_2	1	0	χ_2	0	1
χ_3	0	1	χ_3	1	1

Table 11: The decomposition matrices of S_3 mod 2, 3

Example 8.3. We have one more example

1. (Fong-Swan Theorem) If we have a splitting p -modular system for a p -soluble group G (there is a chain of subgroups of the form

$$1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

such that G_i/G_{i+1} is either a p group or of order prime to p) Then every irreducible kG module is the reduction mod (π) of some $\mathcal{O}G$ lattice. This means that D_p contains the identity matrix as a sub matrix of maximal possible size

Remark. There is a modular atlas of finite groups online, a book by Hiss, Jansen, Lux and Parker "Computational Modular character theory) as well as a book called the atlas of Brauer characters (out of print)

9 Projective Modules

Let M be a (not necessarily finitely generated) R -module where R is a unital ring

Definition 9.1. An R -module P is **projective** if for every surjective homomorphism (epimorphism) $M' \twoheadrightarrow M$ and a homomorphism $P \rightarrow M$ there is a map $P \rightarrow M'$ such that

$$\begin{array}{ccccc} & & P & & \\ & \swarrow \exists & \downarrow & & \\ M' & \twoheadrightarrow & M & \longrightarrow & 0 \end{array}$$

commutes

Definition 9.2. An R -module I is **injective** if for all injective homomorphisms (monomorphisms) $M \hookrightarrow M'$ of R modules and a homomorphism $M \rightarrow I$ there

is a map $M' \rightarrow I$ such that

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \longrightarrow & M' \\ & & \downarrow & \swarrow \exists & \\ & & I & & \end{array}$$

commutes

Lemma 9.1. *The following are equivalent*

1. P is projective
2. Every epimorphism $M \xrightarrow{\lambda} P \rightarrow 0$ splits (there is a homomorphism of the form $\epsilon: P \rightarrow M$ such that $\lambda \circ \epsilon = \text{Id}_P$)
3. P is isomorphic to a direct summand of a free module
4. For all short exact sequences of R modules

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

, the corresponding sequence

$$0 \longrightarrow \text{Hom}_R(P, U) \longrightarrow \text{Hom}_R(P, V) \longrightarrow \text{Hom}_R(P, W) \longrightarrow 0$$

is exact

Proof. See Alperin (it's not hard) □

Remark. It is also clear that direct sums and summands of projective modules are projective. We study indecomposable projective modules for group algebras for the remainder of the course (these are called **principal indecomposable modules**)

Lemma 9.2. *If k is a field and G is a finite group then every kG -module can be embedded into a free kG -module*

Proof. Define a map $\phi: M \rightarrow kG \otimes_k M = M \downarrow_{\{1\}} \uparrow^G$ by

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

. The action of G on $kG \otimes_k M$ by $g'(g \otimes m) = (g'g) \otimes m$. There is a vector space splitting $\psi: kG \otimes_k M \rightarrow M$ of ϕ by $1 \otimes m \mapsto m$, $g \otimes m \mapsto 0$ for any $m \in M, g \in G \setminus \{1\}$, therefore ϕ is injective. Given $h \in G, m \in M$ we can calculate that $\phi(hm) = h\phi(m)$ hence ϕ is a kG homomorphism. As k is a field, $M \downarrow_{\{1\}}$ is a free k -module, and hence $M = \bigoplus_i k$, so that $kG \otimes_k M = \bigoplus_i kG$ and we are done □

Theorem 9.3. Suppose k is a field, G is a finite group and M is a kG -module. Then the following are equivalent

1. M is projective
2. M is injective
3. (Higman's criterion) There is a k -linear map $\lambda: M \rightarrow M$ such that

$$\sum_{g \in G} g \lambda g^{-1} = \text{Id}_M$$

Proof. (ii) implies (i): Suppose that M is injective. Consider

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \longrightarrow & kG \otimes_k M \\ & & \text{Id}_M \downarrow & \nearrow \exists \alpha & \\ & & M & & \end{array}$$

. The splitting α of β shows that M is a summand of the free kG module $kG \otimes_k M$ and so M is projective.

(iii) implies (ii) (the dual proof gives (iii) implies (i)): Take a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M_1 & \xrightarrow{\beta} & M_2 \\ & & \alpha \downarrow & \nearrow \gamma & \\ & & M & & \\ & & \cup & & \\ & & \lambda & & \end{array}$$

where γ is a k -linear map (not necessarily a G -homomorphism) and put

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

. This is a kG -homomorphism and

$$\begin{aligned} \gamma' \beta &= \sum_{g \in G} g(\lambda \gamma)g^{-1} \beta \\ &= \sum_{g \in G} g(\lambda \gamma \beta)g^{-1} \quad \text{as } \beta \text{ is a } kG \text{ map} \\ &= \sum_{g \in G} g(\lambda \alpha)g^{-1} \\ &= \left(\sum_{g \in G} g \lambda g^{-1} \right) \alpha \\ &= \alpha \end{aligned}$$

so we have a splitting and hence M is injective

(i) implies (iii): If $M = kG$, take $\lambda \left(\sum_{g \in G} \alpha_g g \right) = \alpha_1 1_G$. So

$$\begin{aligned} \sum_{h \in G} \left(h \lambda h^{-1} \left(\sum_{g \in G} \alpha_g g \right) \right) &= \sum_{h \in G} \left(h \lambda \left(\sum_{g \in G} \alpha_g h^{-1} g \right) \right) \\ &= \sum_{h \in G} h(\alpha_h 1_G) \\ &= \sum_{h \in G} \alpha_h h \end{aligned}$$

and therefore $\sum_{h \in G} h \lambda h^{-1} = \text{Id}_{kG}$. For $M = \bigoplus_i kG$, use the above lambda on each factor. Suppose that M is a summand of a free module, F (ie M is projective), define $\lambda_M = \pi \lambda_F \iota$ where we have a diagram

$$\lambda_M \curvearrowright M \xrightleftharpoons[\pi]{\iota} F \curvearrowleft \lambda_F$$

Now

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

So we are done, as λ satisfies the Higman criterion □

10 Idempotents and Principal Indecomposable Modules

Theorem 10.1. (*Krull-Schmidt*) Let R be a finite dimensional k algebra and let M be a finitely generated R -module and suppose that

$$\begin{aligned} M &= M_1 \oplus \cdots \oplus M_s \\ M &= M'_1 \oplus \cdots \oplus M'_t \end{aligned}$$

are two indecomposable decompositions of M (ie all the M_i, M'_j are indecomposable). Then $s = t$ and after reordering if necessary, $M_i \cong M'_i$ for all $1 \leq i \leq t = s$

Proof. No Proof □

Example 10.1.

1. Krull-Schmidt applies to finitely generated kG modules. In fact it actually applies to finitely generated modules over any Artinian ring
2. It is also true for finitely generated $\mathcal{O}G$ modules, where $\mathcal{O}$ is a complete DVR
3. Krull-Schmidt is false for finitely generated $\mathbb{Z}G$ modules
4. Note that this doesn't assert existence of decompositions

Corollary 10.1.1. *If M is an indecomposable R -module and M is a summand of $M_1 \oplus \cdots \oplus M_s$ then M is isomorphic to a summand of some M_i*

Proof. Trivial □

Corollary 10.1.2. *Every finitely generated projective indecomposable R -module is isomorphic to a summand of ${}_R R$*

Proof. Trivial □

Write ${}_R R = P_1 \oplus \cdots \oplus P_s$ where the P_i are projective indecomposables. Recall that $R \cong \text{End}({}_R R)^{op}$. Then the endomorphism $\pi_i: {}_R R \rightarrow P_i \hookrightarrow {}_R R$ projecting onto P_i is equal to right multiplication by some element $e_i \in R$ and hence $P_i = Re_i$. Then $1_R = e_1 + \cdots + e_s$ where the e_i are idempotents.

Definition 10.1. We say that idempotents e_i, e_j are **orthogonal** if for all $i \neq j$, $e_i e_j = e_j e_i = 0$. An idempotent e is **primitive** if $e \neq 0$ and e can't be written as the sum of two orthogonal idempotents

As a consequence there is a 1-1 correspondence between direct sum decompositions ${}_R R = P_1 \oplus \cdots \oplus P_s$ with P_i indecomposable and expressions $1 = e_1 + \cdots + e_s$ with the e_i primitive orthogonal idempotents

Example 10.2. 1. If $R = M_n(k)$, then $\text{diag}(1, \dots, 1, 0, \dots, 0)$ is an idempotent, and all the primitive idempotents are conjugate to the matrix with a 1 in the i, i position, and 0s elsewhere. Call this e_i . Note that $1 = e_1 + \cdots + e_n$ is a decomposition into primitive idempotents and Re_i is the matrices with only the i th column non-zero

2. Let $R = kG$ where $k = \mathbb{F}_2$ and $G = C_2 = \langle x \rangle$ and consider the module $M = R = \{0, 1, x, 1 + x\}$. This has no non-trivial idempotents as $x^2 = 1$ and $(1 + x)^2 = 0$. Hence ${}_R R$ is indecomposable

Recall Wedderburn's theorem. We have that $R/\mathcal{J}(R) = \prod_{i=1}^t M_{d_i}(\Delta_i)$. Call each term T_i . We have that ${}_R T_i = \bigoplus \{\text{Column vectors of length } d_i\}$. These are simple and isomorphic to each other. Let e_{ij} be the $d_i \times d_i$ matrix with (j, j) th entry 1 and 0 elsewhere. For the matrix ring T_i we have $1_{T_i} = e_{i,1} + \cdots + e_{i,d_i}$ and hence $1_{R/\mathcal{J}(R)} = \sum_i \sum_j e_{i,j}$. Let $R^\times$ be the group of invertible elements of R

Lemma 10.2. *If e, e' are idempotents in R then the following are equivalent*

1. $e \sim e'$ (is conjugate to) by an element of $R^\times$ (ie $er = re'$ for some $r \in R^\times$)
2. $Re \cong Re'$ and $R(1 - e) \cong R(1 - e')$

Proof. 1 implies 2: If $e \sim e'$, say $re = re'$ for some $r \in R^\times$. Then we have that $Re' \cong Rre'r^{-1} \cong Re$ so $Re \cong Re'$ and the other isomorphism is because $(1 - e)r = r(1 - e')$

2 implies 1: Suppose that $\theta: Re \rightarrow Re'$ and $\phi: R(1 - e) \rightarrow R(1 - e')$ are the isomorphisms. Notice that for any module M there is an isomorphism $\psi: \text{Hom}_R(Re, M) \rightarrow eM$ by $\beta \mapsto \beta(e)$. Let $\mu_1 \in eRe'$ correspond to the isomorphism θ , $\mu_2 \in e'Re$ correspond to θ^{-1} , $\mu_3 \in (1 - e)R(1 - e')$ corresponding to ϕ and $\mu_4 \in (1 - e')R(1 - e)$ corresponding to ϕ^{-1} . Then we have $\mu_1\mu_2 = e$, $\mu_2\mu_1 = e'$, $\mu_3\mu_4 = 1 - e$ and $\mu_4\mu_3 = 1 - e'$. Also $(\mu_1 + \mu_3)(\mu_2 + \mu_4) = 1$ and $(\mu_2 + \mu_4)(\mu_1 + \mu_3) = 1$ so $\mu_1 + \mu_3 \in R^\times$ with two-sided inverse $\mu_2 + \mu_4$. Finally we have that $(\mu_2 + \mu_4)e(\mu_1 + \mu_3) = \mu_2e\mu_1 = \mu_2\mu_1 = e'$ so we are done $\square$

Our aim now is to find the projective indecomposables for ${}_R R$. We first find these in $R/\mathcal{J}(R)$ using Wedderburn, then we need to lift these indecomposables back to R

Definition 10.2. If we take an ideal $I \trianglelefteq R$ and f an idempotent in R , then clearly $e = f + I$ is idempotent in R/I . In this case we say f **lifts** e

Given an idempotent $e \in R/I$, it may or may not be possible to lift it to an idempotent in R . If, for every idempotent $e \in R/I$, it is possible to lift e to an idempotent $f \in R$, then we say we can lift idempotents from R/I to R . Recall that if R is a finite dimensional algebra then $N = \mathcal{J}(R)$ is nilpotent, by taking the descending chain of its powers which must stabilise, so that $N^r = N^{r+1}$, then apply Nakayama

Theorem 10.3. (Idempotent lifting/refinement) *Let R be a ring and N a nilpotent ideal of R . Let e, e' be idempotents in R/N .*

1. *There is an idempotent $f \in R$ such that $\bar{f} = f + N = e$ (f lifts e). If e is primitive then f is primitive*
2. *Suppose f, f' are idempotents in R lifting e, e' respectively. Then $e \sim e'$ if and only if $f \sim f'$*

Proof. (1) Define inductively idempotents $e_i \in R/N^i$ with $e_1 = e$. For $i \geq 2$, the element $e_i + N^{i-1}/N^i \in (R/N^i)/(N^{i-1}/N^i)$ will correspond to $e_{i-1} \in R/N^{i-1}$. Suppose that e_{i-1} is an idempotent in R/N^{i-1} . Pick $a \in R/N^i$ mapping onto e_{i-1} modulo N^{i-1} . Now $a^2 - a \in N^{i-1}/N^i$ but $(N^{i-1})^2 \subset N^i$ hence we know that $(a^2 - a)^2 = 0 \in R/N^i$. Define $e_i = 3a^2 - 2a^3$. Now

$$\begin{aligned} 3a^2 - 2a^3 + N^{i-1} &= (3a - 2a) + (-2a^2 + a)(a - 1) + N^{i-1} \\ &= 3a - 2a + N^{i-1} \\ &= a + N^{i-1} \end{aligned}$$

Hence this maps onto $e_{i-1} \in R/N^{i-1}$ so it lifts e_{i-1} .

$$\begin{aligned} e_i^2 - e_i &= e_i(e_i - 1) \\ &= (3a^2 - 2a^3)(3a^2 - 2a^3 - 1) \\ &= -(3 - 2a)(1 + 2a)(a^2 - a)^2 \\ &= 0 \end{aligned}$$

and so e_i is idempotent and we are done, as if $N^r = 0$, $f = e_r$ is an idempotent lifting e . Suppose e is primitive and that $f = f_1 + f_2$ is a sum of orthogonal idempotents. Then $e = e_1 + e_2$ where $e_i = f_i + N$ is a sum of orthogonal idempotents so without loss of generality $e_1 = 0$, so $f_1 \in N$ so as N is nilpotent $f_1 = 0$

(2) If $e \sim e'$ then there is $\mu \in (R/N)^\times$ such that $e\mu = \mu e'$. Let β be a lift of μ to R and set $\nu = f\beta f' + (1 - f)\beta(1 - f')$. We claim $\nu \in R^\times$ and $f\nu = \nu f'$. The latter statement is obvious: $f\nu = f\beta f' = \nu f'$. Now $\nu + N = \mu$ so if λ is a lift of μ^{-1} to R , then $1 - \nu\lambda \in N$. So $(1 - \nu\lambda)^m = 0$ for some m . Now

$$(1 - (1 - \nu\lambda))(1 + (1 - \nu\lambda) + (1 - \nu\lambda)^2 + \dots) = 1$$

so $\lambda(1 + (1 - \nu\lambda) + (1 - \nu\lambda)^2 + \dots)$ is a right inverse of ν , and similarly it is a left inverse, hence f, f' are conjugate. The other direction of implication is trivial $\square$

Corollary 10.3.1. *(full version of idempotent lifting) Let N be a nilpotent ideal of a ring R and suppose $1 = e_1 + \dots + e_s$ be a decomposition of the identity into orthogonal idempotents modulo N . Then there is a decomposition $1 = f_1 + \dots + f_s$ of 1 into orthogonal idempotents in R such that $f_i + N = e_i$. If the e_i are primitive, then so are the f_i*

Proof. (In Webb) $\square$

Corollary 10.3.2. *Let f be an idempotent in a ring R that has a nilpotent ideal I . Then f is primitive if and only if f_i is primitive*

Proof. Trivial $\square$

11 Projective Covers

Idea: we want to classify the indecomposable projective modules over a finite dimensional algebra as "projective covers" of simple modules.

We work over a finite dimensional algebra R over a field k . Recall that, for some finitely generated R -module M , $\mathcal{J}(M)$ is the intersection of all maximal submodules of M . It is the smallest submodule of M with a semisimple quotient, and is equal to $\mathcal{J}(R)M$. We have the dual notion of the socle, $\text{Soc}(M)$ which is the sum of the simple submodules of M , which is the largest semisimple submodule of M , or $\{m \in M \mid \mathcal{J}(R)m = 0\}$

By Wedderburn, $R/\mathcal{J}(R) \cong \prod_{i=1}^s M_{d_i}(\Delta_i)$ and each term, called M_{d_i} , view as a module over itself is a direct sum of the submodules corresponding to the columns, for Δ_i finite dimensional division algebras over k . Note that each 1_{M_i} has a primitive orthogonal decomposition, $\bar{e}_{i1} + \dots + \bar{e}_{id_i}$ (corresponding to simple modules S_i) and we have a primitive orthogonal decomposition

$$1_{R/\mathcal{J}(R)} = \bar{e}_{11} + \dots + \bar{e}_{1d_1} + \dots + \bar{e}_{s1} + \dots + \bar{e}_{sd_s}$$

where each $\bar{e}_{ij}$ is the matrix in M_i with the only non-zero entry in the (j, j) th position, which is equal to 1. Note that each set $\{\bar{e}_{ij} \mid 1 \leq j \leq d_i\}$ is a conjugacy class of idempotents by Lemma 10.2.

Lifting to R , we get a primitive orthogonal idempotent decomposition

$$1_R = e_{11} + \dots + e_{1d_1} + \dots + e_{s1} + \dots + e_{sd_s}$$

where again our idempotent conjugacy classes are $\{e_{ij} \mid 1 \leq j \leq d_i\}$. Hence we get a decomposition into projectiv indecomposables

$${}_R R = Re_{11} \oplus \dots \oplus Re_{1d_1} \oplus \dots \oplus Re_{s1} \oplus \dots \oplus Re_{sd_s}$$

where each set $\{Re_{ij} \mid 1 \leq j \leq d_i\}$ is an isomorphism class of projective indecomposables.

Now for each i, j we have

$$Re_{ij}/\mathcal{J}(Re_{ij}) = Re_{ij}/\mathcal{J}(R)e_{ij} = (R/\mathcal{J}(R))\bar{e}_{ij} \cong S_i$$

where S_i is a simple R module. Write $P_{S_i} = P_i$ for a module isomorphic to Re_{ij} for some j . Therefore P_i is a projective indecomposable and $P_i/\mathcal{J}(P_i)$ is simple. This is sometimes called the **head** of P_i , and P_i is the **projective cover** of S_i

Example 11.1.

1. Let G be a p -group and $R = kG$ for k of characteristic p . There is a unique simple R -module, k_G , the trivial representation. $\mathcal{J}(R)$ is the augmentation ideal (where the sum of coefficients is 0) and $R/\mathcal{J}(R) \cong k_G$ so there is a unique projective indecomposable, which is kG as a kG -module. This has composition length $|G|$ and all factors are trivial.
2. Let $G = S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, $k = \mathbb{F}_3$ and $R = kG$. There are two simple R modules
 - (a) Trivial = k_G . This has annihilator the augmentation ideal
 - (b) Sign. This has annihilator $\{\sum_{g \in G} \lambda_g g \mid \sum_{g \in G} \text{sgn}(g) \lambda_g\}$

So their intersection is the Jacobson radical,

$$\mathcal{J}(R) = \langle 1 - \sigma, 1 - \sigma^2, \tau - \sigma\tau, \tau - \sigma^2\tau \rangle$$

and

$$R/\mathcal{J}(R) = M_1(k) \oplus M_1(k)$$

where $M_i(k) = \langle -(1 \pm \tau) + J \rangle$ and in fact $e_1 = -1 - \tau, e_2 = -1 + \tau$ are primitive orthogonal idempotents in R . The indecomposable projective modules are

- (a) $P_1 = R(1 + \tau) = \langle 1 + \tau, \sigma(1 + \tau), \sigma^2(1 + \tau) \rangle$
(b) $P_2 = R(1 - \tau)$

which are the projective covers of the trivial and sign representations respectively. The composition series are

$$\begin{aligned} P_1 &\supseteq \mathcal{J}(P_1) = \langle 1 + \tau - \sigma - \sigma\tau, 1 + \tau - \sigma^2 - \sigma^2\tau \rangle \\ &\supseteq T_1 = \langle 1 + \sigma + \sigma^2 + \tau\sigma + \tau + \sigma^2\tau \rangle \\ &\supseteq 0 \end{aligned}$$

with quotients k_G, sgn, k_G respectively, and similarly we can repeat this for P_2 , and we get

$$P_2 \supseteq \mathcal{J}(P_2) \supseteq T_2 \supseteq 0$$

Recall that we have s isomorphism classes of projective indecomposable R modules denoted by P_i , and each P_i has a unique maximal submodule $\mathcal{J}(R)P_i$ whose quotient is S_i . We say that P_i is the **projective cover** of S_i . In general if M is any finitely generated module, we have $M/\mathcal{J}(M) = M/\mathcal{J}(R)M = \bigoplus_j S_j$ for some simple R -modules S_j . Given j , let P_j be the projective cover of S_j . Then by the projectivity of $\bigoplus_j P_j$ we get a commutative diagram of modules

$$\begin{array}{ccccc} & & \bigoplus_j P_j & & \\ & \swarrow \exists \pi & \downarrow & & \\ M & \longrightarrow & M/\mathcal{J}(M) & \longrightarrow & 0 \end{array}$$

We claim that π is surjective. Let $N = \text{Im}(\pi) \leq M$. We know $N + \mathcal{J}(M) = M$ and so $\mathcal{J}(R)(M/N) = (\mathcal{J}(R)M + N)/N = M/N$ and so by Nakayama, we deduce that $M/N = 0$ and so $M = N$.

This induces an isomorphism $\bigoplus_j P_j/\mathcal{J}(\bigoplus_j P_j) \cong M/\mathcal{J}(M)$ and we say that $\bigoplus_j P_j$ is the **projective cover** of M . Let $\Omega M = \ker \pi$ (the **Heller operator**) so we get

$$0 \longrightarrow \Omega M \longrightarrow \bigoplus_j P_j \longrightarrow M \longrightarrow 0$$

Injective modules are the vector space duals of projective modules. If M is a k vector space, then $M^* = \text{Hom}_k(M, k)$ and if M is finite dimensional, $M^{**} \cong M$ naturally.

In fact $\text{Hom}_k(\cdot, k)$ is an exact contravariant endofunctor in the category of finite dimensional vector spaces.

Moreover if R is a finite dimensional k algebra and M is a finitely generated left module, then M^* is a finitely generated right R module with action

$$(f \cdot r)(m) = f(rm) \quad (f \in M^*, m \in M, r \in R)$$

M is a projective left R module if and only if M^* is an injective right R module
 M is indecomposable (respectively simple) if and only if M^* is indecomposable (respectively simple)

Remark. If $R = kG$ for G a finite group, then a left R module M is a right R module by $m \cdot g = g^{-1}m$ for $g \in G, m \in M$

A consequence of this is that if I is an injective R module, then I has a unique minimal (simple) submodule.

Write $I_{S_i} = I_i$ for the injective R -module that has S_i as its unique simple submodule, ie $\text{Soc}(I_i) = S_i$. We call I_i the **injective hull/envelope** of S_i .

In general if M is a finitely generated R module, $\text{Soc}(M) = \bigoplus_j S_j$ for some simple S_j with injective hull I_j . By the injectivity of $\bigoplus_j I_j$, we get a commutative diagram of R modules

$$\begin{array}{ccccc}
 & & \bigoplus_j S_j & & \\
 & & \parallel & & \\
 0 & \longrightarrow & \text{Soc } M & \longrightarrow & M \\
 & & \downarrow & \nwarrow \exists \iota & \\
 & & \bigoplus_j I_j & &
 \end{array}$$

Write $K = \ker(M \xrightarrow{\iota} \bigoplus_j I_j)$, a submodule of M . In fact ι is injective, because it is injective on $\text{Soc}(M)$, as if $K \neq 0$ then $K \cap \text{Soc } M \neq 0$ as K contains a simple submodule, contradiction as we know the map from $\text{Soc}(M)$ to $\bigoplus_j I_j$ is injective.

This induces an isomorphism $\text{Soc } M \cong \text{Soc } \bigoplus_j I_j$. We say that $\bigoplus_j I_j$ is the injective hull of M , and the cokernel of the map $M \rightarrow \bigoplus_j I_j$ is written $\mathcal{U}M$, so we get

$$0 \longrightarrow M \longrightarrow \bigoplus_j I_j \longrightarrow \mathcal{U}M \longrightarrow 0$$

Remark. Note that $\Omega, \mathcal{U}$ are not inverses to each other in the category of finitely generated R modules (although they are inverses “modulo projectives”)

Theorem 11.1. *Let G be a finite group and k a field. If P is a projective indecomposable module for kG , then $P/\mathcal{J}(P) \cong \text{Soc}(P)$*

Proof. Observe that if $x, y \in kG$ with $x = \sum_{g \in G} \lambda_g g$ and $y = \sum_{g \in G} \mu_g g$, then the coefficient of the identity in xy is $\sum_{g \in G} \lambda_g \mu_{g^{-1}} = \sum_{g \in G} \lambda_{g^{-1}} \mu_g$ and the latter is the coefficient of the identity in yx .

Write $P = kG \cdot e$ for some primitive idempotent $e \in kG$. Now take some element $0 \neq x \in \text{Soc}(P)$ and write $x = \sum_{g \in G} \alpha_g g$. There is some $h \in G$ such that $\alpha_h \neq 0$. We set $y = h^{-1}x = \sum_{g \in G} \beta_g g$ so that $\beta_1 \neq 0$

Since $y = ye$ has a non-zero coefficient for the identity, and so by our observation, ey has a non-zero coefficient for the identity. In particular, $ey \neq 0$. We deduce that $e \text{Soc}(P) \neq 0$. Therefore

$$\text{Hom}_{kG}(P, \text{Soc}(P)) = \text{Hom}_{kG}(kGe, \text{Soc}(P)) \cong e \text{Soc}(P) \neq 0$$

Recall that since P is a projective indecomposable kG module, it is also an injective indecomposable kG module, and hence $\text{Soc}(P)$ is simple. Therefore $P/\mathcal{J}(P) \cong \text{Soc}(P)$ as there is some map from P to $\text{Soc}(P)$ $\square$

Remark. This is a special property of symmetric algebras (See Benson, 1.6)

Definition 11.1. If R is a finite dimensional k -algebra, and each Δ_i in the Wedderburn decomposition is equal to k , we say k is a **splitting field** for R . Equivalently, $\text{End}_R(S) = k$ for all simple R modules S

Lemma 11.2. Suppose R is a finite dimensional k -algebra where k is a splitting field for R , and M is a finitely generated R module. Then we have

$$\dim_k \text{Hom}_R(P_S, M) = [M : S]$$

(the composition multiplicity of S as a factor of M , where P_S is the projective cover of S)

Proof. We induct on the length of M .

If $M = S'$ is simple, then this is true as k is a splitting field as

$$\dim_k \text{Hom}_R(P_S, S') = \dim_k \text{Hom}_R(S, S') = [S' : S]$$

If M is not simple then choose a maximal proper submodule M' of M . Then there is a short exact sequence

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

where M'' is the cokernel.

As P_S is projective, $\text{Hom}_{kG}(P_S, \cdot)$ is exact, inducing a short exact sequence

$$0 \longrightarrow \text{Hom}_{kG}(P_S, M') \longrightarrow \text{Hom}_{kG}(P_S, M) \longrightarrow \text{Hom}_{kG}(P_S, M'') \longrightarrow 0$$

. By counting dimensions, and the number of factors isomorphic to S also add so we are done by induction. $\square$

12 Cartan Invariants

Let G be a finite group, k a splitting field of characteristic p . Recall that we denote irreducible kG modules $\{S_i \mid 1 \leq i \leq s\}$ with projective covers $\{P_{S_i} \mid 1 \leq i \leq s\}$

Definition 12.1. Let $c_{ij} = [P_{S_j} : S_i]$ be an $s \times s$ matrix. This is called the **Cartan matrix** of kG

Remark. This is unrelated to the same term from Lie Algebras/Coxeter groups, other than being matrices named after the same person

Remark. Note that $c_{ij} = \dim \text{Hom}_{kG}(P_{S_i}, P_{S_j})$

Theorem 12.1.

1. If k is a splitting field for G , then $c_{ij} = c_{ji}$

2. If $(K, \mathcal{O}, k)$ is a splitting p -modular system, then $c_{ij} = \sum_{l=1}^s d_{li}d_{lj}$
3. $\det(c_{ij})$ is a power of p , and in particular is not zero (Brauer's Theorem)

Proof. We will briefly sketch 2. 1 follows from 2, and 3 is rather involved (see Benson 5.7.2 for a proof using Dress induction or Benson 5.9.3 for another proof due to Kervaire using ψ operators)

The proof of 2 that we will sketch is in Benson 1.9.6, with a different proof in Webb 7.4, 9. For a general finite dimensional associative algebra, the matrix c_{ij} may be singular. An example of such is as follows

Example 12.1. Consider the Quiver Q

$$\bullet \rightleftarrows \bullet$$

and the algebra which is free on the paths (with multiplication given by composition of paths) and consider kQ/I_2 where I_2 is the ideal generated by paths of length 2. This is dimension 4, and the Cartan matrix has all 1s

Example 12.2. If $\mathfrak{g} = sl_2$ over $\bar{\mathbb{F}}_p$ (where p is odd). This has p simples of dimensions $1, 2, \dots, p$ where the dimension p one is called the Steinberg. We have a block (irreducible 2-sided ideal) involving the Steinberg has Cartan number 1. All other blocks have 2 simples in them with 'linked' highest weights. The weights are $0, 1, \dots, p-1$ (with the highest corresponding to the Steinberg) and such blocks correspond to pairs of weights adding up to $p-2$, and so all the Cartan numbers are 2

We start with $\mathcal{O}$ our complete discrete valuation ring with maximal ideal $\mathfrak{p}$ such that $\mathcal{O}/\mathfrak{p} = k$. We have $\mathcal{O}G = \varprojlim_n \mathcal{O}G/\mathfrak{p}^n \mathcal{O}G$. Since the canonical surjection $\mathcal{O}G/\mathfrak{p}^2 \mathcal{O}G \rightarrow \mathcal{O}G/\mathfrak{p} \mathcal{O}G = kG$ has kernel $\mathfrak{p} \mathcal{O}G/\mathfrak{p}^2 \mathcal{O}G$ which squares to 0, a primitive orthogonal decomposition of $1 = \bar{e}_1 + \dots + \bar{e}_s$ in kG lifts to a primitive orthogonal decomposition $1 = e_{21} + \dots + e_{2s}$ in $\mathcal{O}G/\mathfrak{p}^2 \mathcal{O}G$. Similarly via the canonical surjection $\mathcal{O}G/\mathfrak{p}^3 \mathcal{O}G \rightarrow \mathcal{O}G/\mathfrak{p}^2 \mathcal{O}G$ we get a lifting $1 = e_{31} + \dots + e_{3s}$ in $\mathcal{O}G/\mathfrak{p}^3 \mathcal{O}G$ of $1 = e_{21} + \dots + e_{2s}$. Inductively we get a primitive orthogonal decomposition $1 = e_{n1} + \dots + e_{ns}$ in $\mathcal{O}G/\mathfrak{p}^n \mathcal{O}G$ such that $e_{nj} + \mathfrak{p}^{n-1} = e_{(n-1)j}$ for all n, j . By completeness, we get $e_j \in \mathcal{O}G$ such that $e_j + \mathfrak{p}^n = e_{nj}$ for all $n \in \mathbb{N}$. Now e_j^2 defines the same inverse system of elements as e_j so $e_j^2 = e_j$ is idempotent. We can show that $1 = e_1 + \dots + e_s$ is a primitive orthogonal decomposition of the identity in $\mathcal{O}G$ by the following theorem, as given a splitting p -modular system $(K, \mathcal{O}, k)$ we have simple KG modules $\{V_i\}$ and their $\mathcal{O}$ forms $\{W_i\}$. We compute the multiplicity of V_i as a composition factor of $K \otimes \hat{P}_{S_j}$. This is just

$$\begin{aligned} \dim_K \operatorname{Hom}_{KG}(K \otimes \hat{P}_{S_j}, V_i) &= \dim_K \operatorname{Hom}_{KG}(K \otimes \hat{P}_{S_j}, K \otimes_{\mathcal{O}} W_i) \\ &= \dim_K K \otimes_{\mathcal{O}} \operatorname{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i) \\ &= \dots \\ &= [k \otimes W_i : S_j] \\ &= d_{ij} \end{aligned}$$

Then

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

□

Theorem 12.2. *If $1 = \bar{e}_1 + \cdots + \bar{e}_s$ is a decomposition of 1 into primitive orthogonal idempotents in kG , then we can lift to a primitive orthogonal decomposition $1 = e_1 + \cdots + e_s$ in $\mathcal{O}G$. Moreover given another lifting $1 = e'_1 + \cdots + e'_s$ in $\mathcal{O}G$, e'_i is conjugate to e_i*

Proof. Trivial

□

Remark. The decomposition of kG into projective indecomposables, say we have $kG = P_{S_1} \oplus \cdots \oplus P_{S_1} \oplus \cdots \oplus P_{S_n}$ with d_i repetitions of P_{S_i} , can be lifted to $\mathcal{O}G = \hat{P}_{S_1} \oplus \cdots \oplus \hat{P}_{S_1} \oplus \cdots \oplus \hat{P}_{S_n}$ with d_i repetitions of $\hat{P}_{S_i}$

Remark. The decomposition matrix can be read in two ways

1. The rows are the modular composition factors of the modular reductions of ordinary irreducibles
2. The columns are the ordinary composition facts of the lifts of modular projective indecomposables

We know that $D^T D = C$ is the modular irreducible factors of the modular projective indecomposables