Modular Representation Theory

Notes by Eve Pound[*]

Based on lectures by Stuart Martin[†]

0 Informal Chat

The role of modular representation theory is roughly that summarised by the following picture.

Modular representation theory

$$\text{an algebra } A \longrightarrow \boxed{\text{Black box}} \longrightarrow \text{information about } A\text{-modules}$$

Definition. An *algebra* A is a vector space over a field k with a multiplication.

Example 0.1. The group algebra $A = kG = \operatorname{span}\langle g \mid g \in G\rangle$, so the elements of G form a basis and the multiplication is inherited from the group.

An *A-module / representation of A* is a finite dimensional vector space V over k with an A-action. Representation theory tries to break up A-modules into pieces. An A-module module M is *indecomposable* if $M \not\cong M_1 \oplus M_2$ as A-modules where M_1, M_2 are nonzero. An A-module M is *irreducible/simple* if it has no A-submodules except $0, M$.

An algebra A is *semisimple* if the concept of being indecomposable is the same as the concept of being irreducible for A-modules. This is *ordinary representation theory*. The non-semisimple case is *modular representation theory.*

A *composition series* for an A-module M is a sequence

$$M = M_0 \supset M_1 \supset M_2 \supset \ldots \supset M_l = 0$$

where the M_i are submodules of M_{i-1} with M_i/M_{i+1} simple for all i.

Theorem 0.2 (Jordan-Hölder)**.** *Two different composition series for M will always produce the same multiset M_i/M_{i+1} of simple modules.*

Modular representation theory boils down to finding this multiset of *composition factors* of M.

[*]corrections to ep455@cam.ac.uk. All errors are mine.

[†]Lectures for Part III Representation Theory in Lent 2019 at the University of Cambridge.

Remark. If $k = \mathbb{C}$, then $\mathbb{C}G$ is semisimple: this is Maschke's Theorem 1.10.

Questions. Recall the following questions from ordinary representation theory. We might want to ask them similar questions in the modular case.

- What are the irreducible modules?
  - If $k = \mathbb{C}$, there is a correspondence with irreducible characters.
- How many are there?
  - If $k = \mathbb{C}$, the number of conjugacy classes of G
- How do we decompose a representation into a direct sum of irreducibles?
  - Again, in the complex case, we have a handle.

If $k = \overline{\mathbb{F}_p}$ then kG cannot be semisimple if $p \mid G$. (If $p \nmid G$, Maschke's Theorem holds.) Finite dimensional semisimple algebras are described by the Artin-Wedderburn theorem 3.9. In the modular case, the corresponding questions it makes sense to ask are:

- What are the indecomposable modules?
- What are their composition series?
- Compute the irreducible characters: how many are there? It turns out this is the number of *p-regular* conjugacy classes (those with order coprime to p).

Actually the submodules of a given M form a lattice (under inclusion of submodules) which we would like to understand. The lattice is modular: we can imagine each edge of the associated Hasse diagram is labelled by a simple module N_1/N_2 where the N_i are modules on the ends of the edge. So composition series are just maximal chains in the lattice of submodules.

Jordan Hölder implies that every maximal chain in the lattice of submodules for M has the same multiset of labels on its edges: this determines the set of labels.

1 Modules, representations and reducibility

Definition 1.1. If G is a finite group and k a commutative ring of coefficients then a *representation* of G over k is a group homomorphism

$$\varphi : G \to \mathrm{GL}_n(k)$$

for some $n \in \mathbb{N}$. The *degree* of the representation is n.

Examples 1.2 (of modules)**.** (a) $(G, +)$ is an abelian $\mathbb{Z}$-module and the submodules are the subgroups.

(b) A ring R is a right R-module with respect to multiplication, and the submodules are the right ideals.

(c) If R is a ring, R^{op} is the opposite ring with $x \circ y = yx$. Left R-modules are the same things as right R^{op} modules as we can define $x \cdot a = ax$ and $(x \cdot a)b = x(ba) = x(a \circ b)$ for $x \in M, a, b \in R$.

1.3. Let R, S be rings with 1. Suppose an abelian group M is both a left R-module and a right S-module. M is an (R, S)-bimodule if in addition $(rm)s = r(ms)$ for all $r \in R, s \in S, m \in M$.

For example, if $S \subseteq R$, R is an (R, S)-bimodule.

1.4. An R-module M is *finitely generated* if all elements of M can be written as an R-combination of elements of some fixed finite subset of M.

1.5. The *group algebra* kG consists of linear combinations of elements of G with coefficients in k, $\{\sum_g \alpha_g g \mid \alpha_g \in k\}$ with natural addition and multiplication making kG into a ring and k-algebra.

1.6. Every left kG-module induces some (unique) representation φ of G, and conversely.

Proof. Given $\varphi : G \to \mathrm{GL}_n(k)$, let $V = k^n$ a kG-module via, for all $v \in V$,

$$\left(\sum_{g \in G} \alpha_g g\right) \cdot v = \sum_{g \in G} \alpha_g \varphi(g)(v).$$

Conversely, provided a kG-module M when regarded as a k-module via $k \hookrightarrow kG$ is finitely generated and free, we get a representation φ by choosing a basis for M and setting $\varphi(g) \cdot v = g \cdot v$ for all $v \in k^n$. $\square$

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

1.7. Two representations φ, ψ of degree, m, n are *similar* if $m = n$ and there is a nonsingular $x \in \mathrm{GL}_n(k)$ such that $x\varphi(g)x^{-1} = \psi(g)$ for all $g \in G$. The words *conjugate* and *equivalent* are also used. This corresponds to an isomorphism of kG-modules. More generally, a *intertwining operator* is an $n \times m$ matrix X such that $\varphi(g)X = X\psi(g)$ for all $g \in G$. This corrresponds to a homomorphism between the corresponding modules.

Reducibility and Decomposability

1.8. A representation $\varphi : G \to \mathrm{GL}_n(k)$ is *reducible* if it is similar to a representation of the form

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

for all $g \in G$. The subspace spanned by the first i basis vectors is an *invariant* subspace ($W \leq V$ is *invariant* if $gw \in W$ for all $w \in W, g \in G$). The representation is *irreducible* or *simple* if it is nonzero and not reducible.

The representation φ is *decomposable* if it is similar to a representation ψ such that $\psi(g) = \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}$ for all $g \in G$. A kG-module V is *decomposable* if it splits as $V = W_1 \oplus W_2$ with W_1, W_2 nonzero submodules. If V is nonzero and not decomposable, it is *indecomposable*.

Definition 1.9. A short exact sequence of kG-modules is a sequence of kG-modules and kG-homomorphisms of the form

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

such that for each pair of composable arrows, the image of the left arrow is the kernel of the right arrow. That is, V_1 is isomorphic to a submodule of V_2, and $V_3 \cong V_2/V_1$. We say that V_2 is an *extension* of V_1 by V_3. We abbreviate and just write s.e.s. for short exact sequence.

A s.e.s. $0 \longrightarrow V_1 \xrightarrow{\alpha} V_2 \xrightarrow{\beta} V_3 \longrightarrow 0$ is *split* if there is a map (a *splitting*) $\gamma : V_3 \to V_2$ such that $\beta \circ \gamma = \mathrm{Id}_{V_3}$. Thus, $V_2 = \alpha V_1 \oplus \gamma V_3 \cong V_1 \oplus V_3$.

Example. All short exact sequences of $\mathbb{C}$-vector spaces are split.

Theorem 1.10 (Maschke's Theorem)**.** *If $|G| \in k^\times$ and*

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

is a s.e.s. of kG-modules which splits as a sequence of k-modules then it splits as a s.e.s. of kG modules.

Proof. Let $\varphi : V_3 \to V_2$ be a k-splitting and define

$$\gamma = \frac{1}{|G|} \sum_{g \in G} g^{-1} \varphi g.$$

Then

$$\beta \circ \gamma(x) = \beta \left(\frac{1}{|G|} \sum_{g \in G} g^{-1} \varphi g(x) \right) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \beta(\varphi(g(x)))$$

since β is a kG-homomorphism. Since φ is a splitting of k-modules, the above becomes $\frac{1}{|G|} \sum_{g \in G} g^{-1} g(x) = x$. That γ respects addition and multiplication is immediate, so it remains to check it is a kG-homomorphism. We have

$$\gamma \left(\sum_{h \in G} \alpha_h h \cdot x \right) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \varphi g \left(\sum_{h \in G} \alpha_h h \cdot x \right).$$

Since φ is a k-homomorphism this is

$$\frac{1}{|G|}\sum_{g\in G} g^{-1}\varphi\left(\sum_{h\in G}\alpha_h gh\cdot x\right) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\sum_{h\in G}\alpha_h\varphi(gh\cdot x).$$

Swapping the sums and multiplying by hh^{-1} this is equal to

$$\sum_{h\in G}\alpha_h h\frac{1}{|G|}\sum_{g\in G} h^{-1}g^{-1}\varphi(ghx) = \sum_{h\in G}\alpha_h h\cdot\gamma(x),$$

so γ is a kG-homomorphism. $\square$

Example 1.11. Suppose $p \mid |G|$ and $p \mid \mathrm{char}(k)$. Then kG is not semisimple: if it were, the trivial module k would appear once as a summand in a decomposition of kG into simple kG-modules. In particular any composition series of kG has exactly one factor isomorphic to k, c.f. 3.9. The *augmentation map* $kG \to k$ sending, for $\alpha_i \in k, g_i \in g$, $\sum \alpha_i g_i \mapsto \sum \alpha_i$ has kernel $\sum_G = \{\sum \alpha_i g_i \in kG \mid \sum \alpha_i = 0\}$ the *augmentation ideal*. Note that $\sum_G$ is a submodule of the group algebra, and $kG/\sum_G \cong k$ the trivial module. For $g \in kG, 1 \notin \sum_G, g1 = 1 + (g-1) \in 1 + \sum_G$. On the other hand let $\sigma \in kG$ be $\sigma = \sum_{g\in G} g$. Since $p \mid |G|$, $\sigma \in \sum_G$ so the line $k\sigma$ is a submodule of kG also isomorphic to the trivial module. So, when the series $kG \supset \sum_G \supset k\sigma \supset 0$ is refined to a composition series there are at least two factors isomorphic to k, a contradiction.

2 Hom, tensors, exact sequences

Definition. If R is a ring and M a right R-module, N a left R-module, the *tensor product* $M \otimes_R N$ is an abelian group generated by $\{m\otimes n \mid m \in M, n \in N\}$ where $\otimes$ satisfies, for all $m, m' \in M, n, n' \in N, r \in R$:

- $(m + m') \otimes n = (m \otimes n) + (m' \otimes n)$.
- $mr \otimes n = m \otimes rn$.
- $m \otimes (n + n') = m \otimes n + m \otimes n'$.

Examples.

- R commutative implies that left and right modules agree so given two (left) R modules M, N, can form $M \otimes_R N$ an R-module via $r(m \otimes n) = rm \otimes n$.
- If M is an (R, S)-bimodule and N is a left S-module, then $M \otimes_S N$ is a left R module via $r(m \otimes n) = (rm) \otimes n$.
- If M is an (R, S)-bimodule and N is a left S-module then $\mathrm{Hom}_S(M, N)$ is a left R-module via $(rf)(m) = f(mr)$.
- With the hypotheses of the previous point, $\mathrm{Hom}_S(N, M)$ is a right S-module via $(fs)(n) = f(sn)$.

2.1. Let $H \leq G$ and suppose M is a kH-module. Then, $kG \otimes_{kH} M$ is a left kG-module, called the *induced module*, $M\uparrow^G$.

Proposition 2.2. *If $R \leq S$ and A is a left S-module, N a left R-module and M an (S, R)-bimodule then*

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

Proof. (Sketch.) $\varphi(\alpha)(m \otimes n) = \alpha(n)(m)$ and $\psi(\beta)(n)(m) = \beta(m \otimes n)$ are mutually inverse. ☐

Corollary 2.3. $\mathrm{Hom}_{kH}(U, \mathrm{Hom}_{kG}(kG, V)) \cong \mathrm{Hom}_{kG}(kG \otimes_{kH} U, V)$.

Theorem 2.4 (Frobenius Reprocity / Nakayama Isomorphism)**.**

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

Proof. kG is a (kG, kH)-bimodule so by 2.1, $U\uparrow^G = kG \otimes_{kH} U$ so by 2.3,

$$\mathrm{Hom}_{kH}(U, \mathrm{Hom}_{kG}(kG, V)) \cong \mathrm{Hom}_{kG}(U\uparrow^G, V).$$

Hence it suffices to prove that

$$V\downarrow_H \cong \mathrm{Hom}_{kG}(kG, V).$$

To see this, define a map τ from right to left by $\tau(\alpha) = \alpha(1)$, giving $\mathrm{Hom}_{kG}(kG, V)$ the kH structure $(b\alpha)(a) = \alpha(ab)$. Injectivity is immediate since the image at 1 determines the image on kG of a kG-homomorphism. ☐

Now if U, V are kG-modules, they inherit a k-vector space structure and

- $U \otimes_k V$ is a kG-module via $g(u \otimes v) = gu \otimes gv$.
- $\mathrm{Hom}_k(U, V)$ is a kG-module: if $f \in \mathrm{Hom}_k(U, V), g \in G$, then define $(gf)(u) := gf(g^{-1}u)$.

So if U, V, W are kG-modules then by 2.2 there is an isomorphism of kG-modules

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

Taking G-fixed points on both sides we get

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

Proposition 2.5. *If M is a right R-module and*

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

is a s.e.s. of left R-modules,

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

is exact on the left.

Proposition 2.6. *If M, N, N', N'' are left R-modules and*

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

is a s.e.s. of left R-modules, then so are

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

and

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

Lemma 2.7. *If* $0 \longrightarrow M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$ *is a s.e.s. of finite dimensional kG-modules and k is a field, then the sequence splits.*

3 Wedderburn's structure theorem

Let R be a ring with 1.

Definition 3.1. The *Jacobson radical* of R

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

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

If M is any R-module, the *annihilator*

$$\mathrm{ann}_R(M) = \{a \in R : am = 0 \text{ for all } m \in M\}.$$

Recall that simple left R-modules are quotients of R by maximal left ideals. Conversely, if S is a simple left R-module, $0 \neq x \in S$, then the map $R \to S$ given by right multiplication by x is surjective. Let M be the kernel, then we have $S \cong R/M$.

Theorem 3.2.

$$J(R) = \bigcap_{\substack{M \textit{ simple left} \\ R\textit{-module}}} \mathrm{ann}_R(M) = \bigcap_{\substack{M \textit{ max} \\ \textit{left ideal}}} \mathrm{ann}_R(R/M).$$

So, we may conclude that, as each $\mathrm{ann}_R(M)$ is a 2-sided ideal, $J(R)$ is a 2-sided ideal.

Theorem 3.3. $J(R) = \{y \in R : a, b \in R \implies 1 - ayb \textit{ has a 2-sided inverse}\}$.

Corollary 3.4. *$J(R)$ is the intersection of maximal right ideals of R.*

Theorem 3.5 (Nakayama's Lemma)**.** *If M is a finitely generated R-module such that $J(R)M = M$ then $M = 0$.*

The idea of the proof is to take a minimal generating set for M and then use 3.3 to kill a generator off.

Example. If S is a simple R-module, then $J(R)S = 0$.

Definition 3.6. An R module M is semisimple / completely reducible if every R submodule of M is a summand. Equivalently, M is a direct sum of simple modules.

Proposition 3.7. *1. Every submodule of a semisimple module is semisimple, and a direct summand.*

2. Every quotient of a semisimple module is semisimple.

3.8. If R is left Artinian then the following are equivalent:

(i) $J(R) = 0$;

(ii) Every finitely generated R-module is semisimple;

(iii) Every R-module is semisimple.

Proof. If $J(R) = 0$, let $M \subset_R R$ be minimal such that it is the intersection of a finite set of maximal ideals M_i. Then $M = (0)$ since $J(R) = 0$. So, $0 = \bigcap_{i=1}^n M_i$ for some maximal ideals M_i. There is an injection $R \hookrightarrow \bigoplus_{i=1}^n R/M_i = \bigoplus S_i$ for S_i simple so ${}_RR$ is semisimple. Note that we require R to be Artinian to have a finite direct sum.

Now suppose ${}_RR$ is semisimple. Then $J(R)$ is a submodule and therefore a direct summand,

$$ {}_RR = J(R) \oplus_R R/J(R). $$

So

$$ J({}_RR) = J(J(R) \oplus_R R/J(R)). $$

Therefore, $J(R) = J(R)^2$ so $J(R) = 0$ by Nakayama's Lemma. □

In particular, in the semisimple case there is no loss in assuming finite generation.

Theorem 3.9 (Artin-Wedderburn). *Let R be a finite dimensional k-algebra such that $J(R) = 0$. Then*

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

where the Δ_i are division rings with centre containing k, finite dimensional over k.

Remarks. (a) If k is algebraically closed, the only finitely dimensional division rings over k are k itself. For example, since $\mathbb{C}G$ is semisimple and $\mathbb{C}$ is algebraically closed, $\mathbb{C}G = \prod_i M_{n_i}(\mathbb{C})$. For example, $\mathbb{C}S_3 = \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$.

(b) If $k = \mathbb{R}$, then $\Delta_i \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$ the set of all finite dimensional associative division rings (Frobenius' theorem).

(c) If k is finite then each Δ_i is a finite field (Wedderburn's little theorem).

(d) If $R = U_n(k)$ upper triangular matrices (c.f. [Alp86]) then

$$J(R) = \begin{bmatrix} 0 & * & * \\ & \ddots & * \\ & & 0 \end{bmatrix}, \quad R = J(R) \oplus D$$

with D the diagonal matrices. Now $J(D) = 0$ so 3.9 applies and $D = k \oplus k \oplus \cdots \oplus k$. If M_i is the elements of R with 0 in the ith diagonal position then $S_i = U_n(k)/M_i$ is simple.

(e) In general, $J(R/J(R)) = 0$ so 3.9 always applies to $R/J(R)$.

(f) If R is a finite dimension k-algebra and each $\Delta_i = k$ then k is called a *splitting field* for the algebra R.

Proof. See [Web16, 2.1.3]. □

4 Brauer characters

Definition 4.1. For p prime, call an element of G a p-element or p-singular if its order is a power of p. Call it p-regular or a p'-element if its order is coprime to p.

Lemma 4.2. *Given $g \in G$, there is a unique p-element x and a unique p'-element y such that $g = xy$. Moreover, if $h \in G$ commutes with g, then h commutes with x, y.*

Proof. Let $\mathrm{ord}(g) = n = p^\alpha m$ with $(m, p) = 1$. By Euclid's algorithm there are integers s, t such that $sp^\alpha + tm = 1$ so $g = g^{tm} g^{sp^\alpha}$. Let $x = g^{tm}, y = g^{sp^\alpha}$. Then $x^{p^\alpha} = y^m = 1$ so $\mathrm{ord}(x) \mid p^\alpha$ and $\mathrm{ord}(y) \mid m$ so x is a p-element and y is a p'-element. Since x, y are both powers of g any h commuting with g commutes with both x and y. For uniqueness, suppose $x_1 y_1 = x_2 y_2$ are both such decompositions of g. Then $x_2^{-1} x_1 = y_2 y_1^{-1}$ is both a p-element and a p'-element so must be the identity. Hence $x_1 = x_2$ and $y_1 = y_2$. □

Let M be a $\mathbb{C}G$-module. Recall that there is a class function the *ordinary character*

$$\chi_M : \{\text{ccls of } G\} \to \mathbb{C}$$

with $\chi_M(g) = \mathrm{Tr}(g, M)$. We have from complex character theory that $\chi_{M \oplus M'} = \chi_M + \chi_{M'}, \chi_{M \otimes M'} = \chi_M \chi_{M'}$ and $\chi_M = \chi_{M'} \implies M \cong M'$ as $\mathbb{C}G$-modules. In the modular case, the best we can hope for is the first two conditions and $\chi_M = \chi_{M'}$ only if M, M' have the same multiset of composition factors.

The problem is that if M is a sum of p copies of M', then for all $g \in G$, $\mathrm{Tr}(g, M) = p\,\mathrm{Tr}(g, M') = 0$. Our setup to get round this will be as follows. If $\mathrm{char}(k) = p$ then let $m = p^\alpha m'$, $p \nmid n'$. Then in $k[X]$, $X^m - 1 = (X^m - 1)^{p^\alpha}$ so k contains all mth roots of unity if and only if it contains all m'th roots of unity. $X^{m'} - 1$ is separable over k and roots form a cyclic group $C_{m'}$ generated by the primitive m'th roots.

Lemma 4.3. *Assume k contains all $|G|_{p'}$th roots of unity, where $|G|_{p'}$ is the p' part of $|G|$. Let $g \in G$, φ a representation of G. The eigenvalues of $\varphi(g)$ and the eigenvalues of $\varphi(y)$, where y is the p'th part of g, agree.*

Proof. There is a change of basis matrix P such that $P^{-1}\varphi(g)P$ can be written as an upper triangular matrix with the eigenvalues of $\varphi(g)$ on the diagonal,

$$\begin{bmatrix} \lambda_1 & * & * \\ & \ddots & * \\ & & \lambda_n \end{bmatrix}$$

Let x be the p-part of g, $\mathrm{ord}(x) = p^s$. Then, by the proof of Lemma 4.2, $x = g^t$ for some t. So,

$$\mathrm{Id} = P^{-1}\varphi(x^{p^s})P = P^{-1}\varphi(g^{tp^s})P = (P^{-1}\varphi(g)P)^{tp^s}.$$

This is

$$\begin{bmatrix} \lambda_1^{tp^s} & * & * \\ & \ddots & * \\ & & \lambda_n^{tp^s} \end{bmatrix}$$

so $\lambda_i^{tp^s} = 1$ for all i. Modulo p, $(\lambda_i^{tp^s} - 1) = (\lambda_i^t - 1)^{p^s}$ so

$$P^{-1}\varphi(x)P = \begin{bmatrix} 1 & * & * \\ & \ddots & * \\ & & 1 \end{bmatrix}$$

and the eigenvalues are all 1, and the trace is $\dim_k M$. Finally, $P^{-1}\varphi(g)P = P^{-1}\varphi(xy)P = P^{-1}\varphi(x)PP^{-1}\varphi(y)P$ and hence the eigenvalues of g, y coincide. $\square$

Example. If $g \in G$ and M is a kG-module then g induces some linear map on M by $X^{|G|} - 1$ over k. Now, $X^{|G|} - 1 = (X^{|G|_{p'}} - 1)^{|G|_p}$ and $X^{|G|_{p'}} - 1$ is separable and is therefore a product of linear factors in $k[X]$. So g has Jordan canonical form and every eigenvalue of g is a $|G|_{p'}$th root of 1. So a Jordan block of g with λ on the diagonal is conjugate to

$$\begin{aligned} g_1 &= \begin{bmatrix} \lambda & \lambda & & \\ & \lambda & \ddots & \\ & & \ddots & \lambda \\ & & & \lambda \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & & \\ & 1 & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{bmatrix} \begin{bmatrix} \lambda & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \lambda \end{bmatrix} \\ &:= x_1 y_1 \end{aligned}$$

Now, x_1 is a p-element, since it is of the form $\mathrm{Id} + (\text{nilpotent})$ and y_1 is a p'-element since λ is a $|G|_{p'}$ root of unity. So if $g = xy$ is a decomposition as in 4.2 then the action of the p-element has trace $\mathrm{Tr}(x_M, M)$ equal to the dimension. As x_M has entries on the diagonal in Jordan canonical form equal to 1 and y_M is diagonalisable,

$$\mathrm{Tr}(g, M) = \mathrm{Tr}(y, M) \text{ and } \mathrm{Tr}(x, M) = \dim_k(M).$$

Definition 4.4. For G a finite group, k a field containing all $|G|_{p'}$th roots of unity, $\mathrm{char}(k) = p$, the roots form a cyclic $C_{|G|_{p'}}$ under multiplication. All the eigenvalues of elements of G belong to this cyclic group. Fix a *lifting*, an isomorphism of cyclic groups

$$\psi : \left\{ \begin{smallmatrix} |G|_{p'}\text{th roots} \\ \text{of } 1 \text{ in } k \end{smallmatrix} \right\} \longrightarrow \left\{ \begin{smallmatrix} |G|_{p'}\text{th roots} \\ \text{of } 1 \text{ in } \mathbb{C} \end{smallmatrix} \right\}.$$

If g is a p'-element of G and M is a finite dimensional kG-module then $g_M \sim \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{bmatrix}$ where $d = \dim_k M$. The *Brauer character* of g on M is

$$\chi_M(g) = \sum_{i=1}^{d} \psi(\lambda_i) \in \mathbb{C}.$$

In fact, $\chi_M(g)$ is a cyclotomic integer. It is defined on all p'-conjugacy classes of G, and is constant on conjugacy classes.

Example. If $k = \mathbb{F}_2$ and $G = \langle x \rangle = C_3$ and $\rho(x) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ gives a 2-dimensional representation M. The characteristic polynomial of $\rho(x)$ is t^2+t+1 so eigenvalues are primitive 3rd roots. These lift to primitive third roots in $\mathbb{C}$, $\chi_M(x) = e^{\frac{2\pi i}{3}} + e^{\frac{4\pi i}{3}} = -1$. Note that $\mathrm{Tr}(x, M) = 1$ which lifts to 1, but $\chi_M(g) = 1$.

Lemma 4.5. *Given two modular representations σ, τ with the same Brauer character $\chi_\sigma = \chi_\tau$, for all $g \in G$, $\sigma(g)$ and $\tau(g)$ have the same eigenvalues.*

Proof. Let $\sigma(g)$ have eigenvalues $\epsilon^{\alpha_1}, \ldots, \epsilon^{\alpha_a}$ and let τ have eigenvalues $\epsilon^{\beta_1}, \ldots, \epsilon^{\beta_b}$ for some ϵ. By taking powers we get that the characteristic roots of $\sigma(g^i), \tau(g^i)$. Let ζ be a primitive $|G|_{p'}th$ root of unity in $\mathbb{C}$ and let $\zeta = \psi(\epsilon)$. Then,

$$\zeta^{i\alpha_1} + \cdots + \zeta^{i\alpha_a} = \zeta^{i\beta_1} + \cdots + \zeta^{i\beta_b}. \quad (\star)$$

Consider the complex representations

$$\sigma'(g^i) = \begin{bmatrix} \zeta^{i\alpha_1} & & \\ & \ddots & \\ & & \zeta^{i\alpha_a} \end{bmatrix}, \tau(g^i) = \begin{bmatrix} \zeta^{i\beta_1} & & \\ & \ddots & \\ & & \zeta^{i\beta_b} \end{bmatrix}$$

of the cyclic group $\{g^i\}$. By $(\star)$, $\mathrm{Tr}(g, \sigma') = \mathrm{Tr}(g, \tau')$ so the $\mathbb{C}$-characters of τ' and σ' are equal so their irreducible constituents are the same by complex character theory. So $\{\alpha_1, \ldots, \alpha_a\}, \{\beta_1, \ldots, \beta_b\}$ are identical as multisets. $\square$

So, recalling Jordan-Hölder, every representation has a fixed number of constituents and they are unique up to equivalence and order of arrangement. Assume M has a composition series $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_l = M$. Let $\mathcal{B}$ be the ordered basis $\mathcal{B} = \{e_1^1, \ldots, e_{n_1}^1, e_1^2, \ldots, e_{n_2}^2, \ldots, e_1^l, \ldots, e_{n_l}^l\}$ with e_1^1 through to $e_{n_j}^j$ a basis of M_j and l the composition length. Let the matrix representation with respect to $\mathcal{B}$ be given by

$$g \mapsto \begin{bmatrix} \mu_l(g) & * & * & * \\ & \mu_{l-1}(g) & \ddots & \vdots \\ & & \ddots & \vdots \\ & & & \mu_1(g) \end{bmatrix}$$

where the matrix for $\mu_j(g)$ corresponds to the basis for M_j/M_{j-1}. We call $\mu_l(g)$ the top or head, $\mu_1(g)$ the bottom and the other μ_i the heart.

Definition. A module M is *uniserial* if it has a unique composition series. Equivalently, it has a unique minimal submodule M_1, and M/M_1 has a unique minimal submodule, and so on. Equivalently, the submodules are linearly ordered by inclusion. (See [Web16, §6, Ex. 3,6]

Theorem 4.6. *If k is an algebraically closed field of characteristic p, then for $\mathrm{Tr}(g, M) = \mathrm{Tr}(g, M')$ for all $g \in G$ if and only if for all simple kG-modules S, the multiplicities of S as a composition factor of M, M' agree modulo p.*

Proof. Without loss of generality assume M, M' are semisimple. If not, we can replace the submodules with summands to get M, M' with the same trace and composition factors.

($\Longleftarrow$) If S_i is the ith simple summand,

$$\begin{aligned}\mathrm{Tr}(g, M) &= \sum_{i=1}^{n} \alpha_i \,\mathrm{Tr}(g, S_i) \\ &= \sum_{i=1}^{n} \beta_i \,\mathrm{Tr}(g, S_i) \\ &= \mathrm{Tr}(g, M').\end{aligned}$$

($\Longrightarrow$) If $\mathrm{Tr}(g, M) = \mathrm{Tr}(g, M')$ for all $g \in G$ then $\mathrm{Tr}(x, M) = \mathrm{Tr}(x, M')$ for all x in the group algebra kG. By Wedderburn 3.9 on $kG/J(kG)$,

$$\bigoplus_{i=1}^{r} n_i S_i \cong kG/J(kG) = M_{n_1}(\Delta_1) \times \cdots \times M_{n_r}(\Delta_r)$$

with each $n_i S_i \cong M_{n_i}(\Delta_i)$. But every simple S is isomorphic to kG/m for some maximal ideal m. By the semisimplicity of M, M' they are direct sums of the $n_i S_i$. The matrix algebras each contain the matrix

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 \end{bmatrix}.$$

Let $x_i \in kG$ be such that $\mathrm{Tr}(x_i, M) = \delta_{ij}$. Then,

$$\mathrm{Tr}(x_i, M) = \sum_{j} \alpha_j \,\mathrm{Tr}(x, S_j) = \alpha_i$$

and $\mathrm{Tr}(x_i, M') = \beta_i$. So $\alpha_i = \beta_i$ in k for all i so $\alpha_i \equiv \beta_i \mod p$.

□

Theorem 4.7 (Brauer)**.** *Let M, M' be finite dimensional kG-modules. Then, $\chi_m = \chi_{M'}$ if and only if the multiplicities of each kG-module as composition factors of M, M' are equal.*

Proof. As in the proof of 4.6, we may assume without loss of generality that M, M' are semisimple. We have seen that if the multiplicities of simple kG-modules as factors of M, M' are equal then $\chi_M = \chi_{M'}$ so it suffices to prove the converse.

Consider a counterexample of minimal dimension, $\chi_M = \chi_{M'}$ such that the multiplicities of the simple kG-modules as factors of M, M' do not agree. By minimality, M, M' have no composition factor in common. Since $\chi_M = \chi_{M'}$, 4.3 and 4.5 tell us that for all $g \in G$, $\mathrm{Tr}(g, M) = \mathrm{Tr}(g, M')$. Hence, by 4.6

the multiplicities of the simple kG-modules as factors of M, M' agree modulo p. Let

$$M = \bigoplus_{i=1}^{m} \gamma_i S_i, \quad M' = \bigoplus_{i=1}^{m} \gamma' S_i,$$

so $\gamma \equiv \gamma' \pmod p$ and at most one of γ_i and γ_i' is nonzero for each i. So for all i, $p \mid \gamma_i$ and $p \mid \gamma_i'$. Let $\gamma_i = p\delta_i, \gamma_i' = p\delta_i'$. Then $M = pM_1$ and $M' = pM_1'$ where

$$M_1 = \bigoplus_{i=1}^{m} \delta_i S_i, \quad M_1' = \bigoplus_{i=1}^{m} \delta' S_i.$$

Moreover, $\dim_k M = p \dim_k M_1$ so $\dim_k M_1 < \dim_k M$ and $\chi_M = p\chi_{M_1}, \chi_{M'} = p\chi_{M_1'}$. So M_1, M_1' is a counterexample of smaller dimension, a contradiction. $\square$

Example. Let $G = S_3$, having three conjugacy classes: the trivial, the transpositions, and the 3-cycles. We label the conjugacy classes by cycle length. The irreducible $\mathbb{C}G$-modules are the trivial k, sign σ, and the 2-dimensional ψ permuting the co-ordinates of

$$V = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \right\}, \text{ with basis } \mathcal{B} = \left\{ v_1 = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}, v_2 = \begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix} \right\}.$$

That is, $\psi((123))(v_1) = v_2$, $\psi((123))(v_2) = -(v_1 + v_2)$, and $\psi((12))(v_1) = -v_1$, $\psi((12))(v_2) = v_1 + v_2$, so with respect to $\mathcal{B}$ we have

$$\psi((123)) = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \text{ and } \psi((12)) = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}.$$

The ordinary character table for S_3 is given by

	1	2	3
1	1	1	1
σ	1	-1	1
ψ	1	0	2

Later, we will show that the irreducible representations of S_3 lift to characteristic 0 so Brauer characters form tables that can be recovered by ignoring some of the rows and columns of the ordinary table.

When $p = 3$, the conjugacy classes $1, 2$ are $3'$-conjugacy classes and the irreducible representations are $\overline{k}, \overline{\sigma}$. The Brauer character of $\overline{\psi}$ has $\psi_V(1) = 2$, $\psi_V((12)) = 0$ so $\psi_V = \overline{k} + \overline{\sigma}$. By Brauer's theorem, the composition factors of $\overline{\psi}$ are $\overline{\sigma}, \overline{k}$. So modulo 3 the Brauer character table is

	1	2
$\overline{k}$	1	1
$\overline{\sigma}$	1	-1

In characteristic 2, we want the 2′-classes and the irreducible representations are $\overline{k}, \overline{\psi}$ with the same matrices as in characteristic 0 interpreted as being characteristic 2. So the Brauer character table is

	1	3
$\overline{k}$	1	1
$\overline{\psi}$	2	-1

Recall that the abelianisation G_{ab} of a group G determines the number of 1-dimensional representations of G over $\mathbb{C}$: there are $[G : G']$ of them. Brauer gives that there are $[G : G']_{p'}$ in characteristic p, giving one such in characteristic 2, two in characteristic 3.

5 Character tables

Recall an *algebraic integer* is a complex number satisfying a nonzero monic polynomial over $\mathbb{Z}$, and that the set of algebraic integers form a ring. A *number field* is a subfield K of finite degree over $\mathbb{Q}$ and $\mathcal{O}_K$ is the *ring of integers in* K, that is, $K \cap \{\text{algebraic integers}\}$. If $\alpha \in K$, then there is a nonzero $c \in \mathbb{Z}$ such that $c\alpha \in \mathcal{O}_K$. An integral domain R is a *Dedekind domain* if it is integrally closed, Noetherian and every nonzero prime ideal is maximal.

Fact. For every number field K, $\mathcal{O}_K$ is a Dedekind domain.

Now, for G a finite group, let $n = |G| = p^\alpha m$ with $p \nmid m$, and let $\operatorname{char}(k) = p$. If k is large enough in the sense that it contains all mth roots of unity, then these roots of unity form cyclic subgroups $C, \hat{C}$ of the multiplicative groups of $k, \mathbb{C}$ respectively. Let $K = \mathbb{Q}(\hat{C})$.

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

Proof. Let ϵ be a root of the primitive mth cyclotomic polynomial. The Galois group consists of the maps $\epsilon \mapsto \epsilon^i$ for some i coprime to m, and therefore is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$. □

Remark. In general, this group is not cyclic. For example if $m = 8$ then $\mathbb{Z}/m\mathbb{Z} \cong C_2 \times C_2$.

Let $\mathcal{O}_K$ be the ring of integers in K, so $\mathcal{O}_K = \mathbb{Z}[\hat{C}]$ is a Dedekind domain, so in particular, all prime ideals are maximal.

Lemma 5.2. *Choose a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over the prime number p, that is, $\mathfrak{p} \cap \mathbb{Z} = (p)$. If p^r is the smallest p-power 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. $\operatorname{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) \cong \operatorname{Stab}_{K/\mathbb{Q}}(\mathfrak{p}) \cong \mathbb{Z}/r\mathbb{Z}$.

Proof. Exercise. $\square$

Remark. Sine m is coprime to p, $m \mid (p^{\phi(m)} - 1)$ so $r \mid \phi(m)$.

Example 5.3.

Definition 5.4. The *Brauer character table* of G modulo p is the table where:

- rows are indexed by simple kG-modules S;
- columns are indexed by conjugacy classes of p'-elements of G;
- entries are the values of the Brauer characters $\chi_S(g)$.

Once a lift $\psi : C \to \hat{C}$ is fixed, all isomorphisms $C \to \hat{C}$ are obtained by applying elements of $\mathrm{Gal}(K/\mathbb{Q})$ to $\hat{C}$. So, the rows of the Brauer character table are the irreducible Brauer characters χ_S for S simple, and the columns are ring homomorphisms $\widetilde{\chi} : \mathrm{R}(G) \to \mathbb{C}$, where R is the Grothendieck ring (see 6.1). In fact, the irreducible characters form a basis for the class functions from conjugacy classes of p'-elements to $\mathbb{C}$, so the table is square, see 6.5.

Proposition 5.5. *Applying $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ to a column of the Brauer character table gives another column of the Brauer character table. Applying $\tau \in \mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathfrak{p}) \subseteq \mathrm{Gal}(K/\mathbb{Q})$ to a row of the Brauer character table gies another row of the Brauer character table.*

Proof. (Sketch) If ζ is a primitive mth root of unity in $\mathbb{C}$, $K = \mathbb{Q}(\zeta)$, an element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ sends ζ to ζ^t with $(t, m) = 1$. So for each p'-element of G, $\widetilde{\chi}^\sigma(g) = \widetilde{\chi}(g^t)$.

Moreover, σ stabilizes $\mathfrak{p}$ when t is a pth power. Let S be a simple kG-module wit corresponding representation $\rho : G \to \mathrm{GL}_n(k)$. Then S^r is a kG-module with corresponding representation $\rho^\sigma : G \to \mathrm{GL}_n(k) \to \mathrm{GL}_n(K)$ where, if $\rho(g) = (\lambda_{ij}(g))$, $\rho^\sigma(g) = (\lambda_{ij}(g)^t)$. $\square$

Hence the Brauer character table is determined by the choice of $\mathfrak{p}$ up to permuting roots and coumns. Note that if $\tau \notin \mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathfrak{p})$ applied to a row need not give a row.

6 Grothendieck groups

Let G be a finite group, k a field as in §5. We define $\mathrm{R}(G) = G_0(kG)$.

Definition 6.1. $\mathrm{R}(G)$ has generators symbols $[M]$, where M is an isomorphism class of finite dimensional kG-modules, and relations $[M_2] = [M_1] + [M_3]$ if there is a s.e.s. of kG-modules $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$.

Remarks. 1. We have to use isomorphism classes of modules rather than modules themselves in order to obtain a set.

2. R(G) is a free abelian group with basis $[S_i]$, with $[S_i]$ simple by Jordan-Hölder, 0.2.

3. We can make R(G) into a commutative ring by setting $[M][N] = [M \otimes_k N]$.

4. The trivial module $k = k_0$ is expressible as a difference $[M] - [N]$. Note that if $k = \mathbb{C}$, R$[G]$ is the ring of virtual characters of $\mathbb{C}G$-modules.

Lemma 6.2. *The following hold for Brauer characters.*

(i) $\chi_M(1) = \dim_k(M)$.

(ii) χ_M *is a class function of p'-classes.*

(iii) $\chi_M(g^{-1}) = \overline{\chi_M(g)} = \chi_{M^*}(g)$.

(iv) If $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ *is a s.e.s. of finite dimensional kG-modules then $\chi_{M_1} = \chi_{M_2} + \chi_{M_3}$. I particular, χ_M depends only on the isomorphism class of M. If M has composition factors S_j with multiplicities m_j then $\chi_M = \sum_j m_j \chi_{S_j}$.*

(v) $\chi_{M \otimes_k N} = \chi_M \chi_N$.

Proof. Exercise. □

For all p'-elements $g \in G$, the map $\widetilde{\chi}(g) : \mathrm{R}(G) \to \mathbb{C}$ sending $[M]$ to $\chi_M(g)$ is therefore a well defined ring homomorphism.

Theorem 6.3. *The product of these maps*

$$R(G) \longrightarrow \prod_{\substack{ccls\ of\ p'\text{-} \\ elements\ of\ G}} \mathbb{C}$$

$$[M] \longmapsto (g \mapsto \chi_M(g))$$

is injective.

Proof. Suppose that $[M] - [N]$ and $[M'] - [N']$ have the same image, so $\chi_M - \chi_N = \chi_{M'} - \chi_{N'}$, so $\chi_M + \chi_{N'} = \chi_N + \chi_{M'}$. Then, $\chi_{M \oplus N'} = \chi_{N \oplus N'}$ so $[M \oplus N'] = [N \oplus M']$, so $[M] + [N'] = [M'] + [N]$ and $[M] - [N] = [M'] - [N']$. □

Theorem 6.4. *The map* $\mathbb{C} \otimes \mathrm{R}(G) \xrightarrow{\chi} \prod_{\substack{ccls\ of\ p'\text{-} \\ elements\ of\ G}} \mathbb{C}$ *is an algebra isomorphism.*

Corollary 6.5. *The simple kG-modules are in bijection with the p'-conjugacy classes of G.*

We will prove 6.4 in a few steps.

Lemma 6.6 (Injectivity)**.** *The irreducible Brauer charcaters χ_{S_i} are linearly independent over $\mathbb{C}$.*

Proof. Let $K \le \mathbb{C}$ be a field containing $|G|_{p'}$th roots of unity, $\mathcal{O}$ the ring of integers in K, and $\mathfrak{p}$ the prime ideal in $\mathcal{O}$ containing (p). Let $\mathcal{O}_\mathfrak{p}$ be the localisation of $\mathcal{O}$ at $\mathfrak{p}$. Then,

$$m_\mathfrak{p} = \left\{ \frac{x}{y} : x, y \in \mathcal{O}, x \in \mathfrak{p}, y \notin \mathfrak{p} \right\}$$

is the unique maximal ideal of $\mathcal{O}_\mathfrak{p}$, and $\mathcal{O}_p/m_\mathfrak{p} \cong \mathcal{O}/\mathfrak{p} \hookrightarrow k$. Also, $\mathcal{O}\mathfrak{p}$ is a PID so write $m_\mathfrak{p} = (\pi)$. Suppose there is a $\mathbb{C}$-linear relation amongst irreducible Brauer characters. Then there is one over K as all values lie in K, and we can clear denominators to obtain a relation in $\mathcal{O}$. If all coefficients lie in $\mathfrak{p}$, then divide by a suitable power of π until they do not, and reduce modulo p to get a relation between traces

$$\sum \alpha_i \operatorname{Tr}(x_i \delta_j) = 0$$

for all $x \in kG$. By the Wedderburn trick there is an $x \in kG$ such that $\operatorname{Tr}(x_i\delta_j) = \delta_{ij}$ so $\alpha_i = 0$ for all i. □

To get surjectivity, for each p'-element $g \in G$ we find elements x of $\mathbb{C} \otimes_k \mathrm{R}[G]$ such that $\widetilde{\chi}(g)(x) = 1$ and $\widetilde{\chi}(h)(x) = 0$. Let g be an element of order m coprime to p, and let H be cyclic generated by g. The irreducible representations of h over k are of the form $g \mapsto \epsilon$ for ϵ an mth root of unity. The irreducible Brauer characters are of the form $\chi_j(g) = e^{\frac{2\pi i j}{m}}$ with corresponding kG-module S_j. Define

$$x := \frac{1}{m} \sum_{j=1}^{m} e^{\frac{-2\pi i j}{m}} [S_j] \in \mathbb{C} \otimes_k \mathrm{R}[G].$$

This has Brauer character given by

$$g^t \mapsto \frac{1}{m} \sum e^{\frac{2\pi i j (t-1)}{m}} = \begin{cases} 1 & gt = g \\ 0 & gt \neq g \end{cases}.$$

Lemma 6.7. *If $H \le G$ and M is a kH-module, then for $g \in G$,*

$$\chi_{M\uparrow^G} = \sum_{\substack{ccls\ of\ h \in H \\ s.t.\ h \sim g\ in\ G}} |C_G(h) : C_H(h)| \chi_M(h).$$

Proof. $g(g_i \otimes m) = g_j \otimes hm$ where $gg_i = g_j h$, $h \in H$, so the matrix representing the action of g decomposes into blocks corresponding to the g-orbits of G/H. The blocks corresponding to g-orbits of length greater than 1 are of the form

$$\begin{bmatrix} 0 & * & * & * \\ * & 0 & * & * \\ 0 & \ddots & \ddots & * \\ 0 & 0 & * & 0 \end{bmatrix},$$

and the eigenvalues are 0. However, the singleton $\{g_i\}$ is in the orbit of G/H with corresponding block representing the action of $g_j^{-1}gg_i \in H$ on M. Then,

$$\chi_{M\uparrow^G}(g) = \sum_{g_j^{-1}gg_i\in M} \chi_M(g_j^{-1}gg_i).$$

For $h \in H$, counting the number of pairs (g_j, g_i) with $g_j^{-1}gg_i = h$ gives the result. $\square$

Now, if $H \leq G$ define $\mathrm{Ind}_H^G : \mathrm{R}(H) \to \mathrm{R}(G)$, defined on the basis by $[M] \mapsto [kG\otimes M]$ and extending the scalars to get a map $\mathbb{C}\otimes\mathbb{Z}\,\mathrm{R}[H] \to \mathbb{C}\otimes_{\mathbb{Z}}\mathrm{R}(G)$. Given a p-element $g \in G$, let $H \leq \langle g\rangle$ and take $x \in \mathbb{C}\otimes_{\mathbb{Z}}\mathrm{R}(H)$ such that

$$\chi_x(g') = \begin{cases} 1 & g' = g \\ 0 & g' \neq g \end{cases}$$

Then for $g' \in G$,

$$\chi_x\uparrow^G(g') = \sum_{\substack{\text{ccls of } h\in H\\ \text{s.t. } h\sim g'\in G}} |C_G(h) : C_H(h)|\chi_x(h).$$

This is

$$\begin{cases} |C_G(g) : \langle g\rangle| & \text{if } g' \sim_G g \\ 0 & \text{if } g' \not\sim_G g \end{cases}.$$

Corollary 6.8 (of 6.4)**.** *Every ring homomorphism* $\mathrm{R}(G) \to \mathbb{C}$ *is of the form* $\widetilde{\chi}(g)$ *for* g *a* p'*-element of* G*.*

To prove this we need:

6.9. For R a commutative ring with 1, D an integral domain, every set of distinct ring homomorphisms $R \to D$ is linearly independent.

Proof. Take a linearization of minimal size,

$$\sum_{i=1}^n \lambda_i\varphi_i = 0, \text{ where } \varphi_i : R \to D, \lambda_i \in D.$$

Choose $r_0 \in R$ such that $\varphi_1(r_0) \neq \varphi_n(r_0)$, so for all $r \in R$,

$$\sum_{i=1}^n \lambda_i\varphi_i(r_0r) = \sum_{i=1}^n \lambda_i\varphi_i(r_0)\varphi_i(r) = 0 \tag{1}$$

and

$$\sum_{i=1}^n \lambda_i\varphi_n(r_0)\varphi_i(r) = 0. \tag{2}$$

Subtracting (2) from (1) gives that, for all $r \in R$,

$$0 = \sum_{i=1}^{n} \lambda_i(\varphi_i(r_0) - \varphi_n(r_0))\varphi_i(r).$$

Since D is a domain, $\lambda_1(\varphi_1(r_0) - \lambda_n(r_0)) \neq 0$, so this contradicts the minimality. $\square$

Proof of 6.8. Let $\varphi : \mathrm{R}(G) \to \mathbb{C}$ and extend linearly to an algebra homomorphism $\varphi : \mathbb{C} \otimes_{\mathbb{Z}} \mathrm{R}(G) \to \mathbb{C}$. Do the same for the $\widetilde{\chi}(g)$s. Then 6.4 and 6.9 give that $\widetilde{\chi}(g_i)$ form a basis of $\mathbb{C}$-linear maps $\mathbb{C} \otimes \mathrm{R}(G) \to \mathbb{C}$. If φ is not $\widetilde{\chi}(g_i)$ for all i, then by 6.9 $\varphi, \widetilde{\chi}(g_i)$ are linearly independent, a contradiction. $\square$

7 Decomposition matrices and p-modular systems

Definition 7.1. We denote by $\mathcal{O}$ a discrete valuation ring, that is, a PID with a unique nonzero maximal ideal, where the unique maximal ideal $\mathfrak{p} = (\pi)$. A p-modular system is a triple $(K, \mathcal{O}, k)$ where $\mathcal{O}$ is a discrete valuation ring, K the characteristic zero field of fractions of $\mathcal{O}$ and k the residue field $\mathcal{O}/\mathfrak{p}$ of characteristic p. Such a p-modular system is splitting for G if for all subgroups H of G,

1. $KH = \prod M_{a_i}K$ for some a_i;
2. $kH/J(kH) = \prod M_{c_i}(k)$ for some k.

That is, the fields K, k are splitting fields for the semisimple algebras KH and $kH/J(kH)$.

Note that every finitely generated torsion free $\mathcal{O}$-module is free.

Example. If K is an algebraic number field, $\mathcal{O}$ the ring of integers of K so that K is the field of fractions of $\mathcal{O}$ which is integral over $\mathbb{Z}$. There is s $\mathfrak{p}$ prime in $\mathcal{O}$ lying over (p) and the localisation $\mathcal{O}_{\mathfrak{p}}$ at $\mathfrak{p}$ is a discrete valuation ring so $(K, \mathcal{O}_{\mathfrak{p}}, \mathcal{O}/\mathfrak{p})$ is a p-modular system.

Remark. If K contains $|G|$th roots of 1, $(K, \mathcal{O}, \mathcal{O}/\mathfrak{p})$ is a splitting p-modular system for G.

Given a p-modular system, $(K, \mathcal{O}, k)$ V an ordinary finite dimensional KG-module with a K-basis $v_1, \ldots, v_d$, let $W = \mathrm{span}_{\mathcal{O}}\{gv_i \mid 1 \leq i \leq d, g \in G\}$. This is finitely generated and torsion free as an $\mathcal{O}$-module and it is therefore free and a subset of V.

Let $w_1, \ldots, w_n$ be a free $\mathcal{O}$-basis. Then the $\{w_i\}$ span V, and if there is a linear relation between them over K, then since the field of fractions of $\mathcal{O}$ is K we can clear denominators to obtain a relation in $\mathcal{O}$. But since the basis is free no such relation exists, so $\{w_1, \ldots, w_n\}$ is a K-basis fro V and $n = d$. Changing the basis $v_i \to w_i$ ensures that all entries in matrix representations of G are in $\mathcal{O}$, and we may write

$$V = K \otimes_{\mathcal{O}} W$$

W is called an $\mathcal{O}$-form for V (and is not unique).

Theorem 7.2. *If $(K, \mathcal{O}, k)$ is a splitting p-modular system and W, W' are $\mathcal{O}$-forms of V then the kG-modules $k \otimes_{\mathcal{O}} W = \overline{W} = W/\mathfrak{p}W$ and $k \otimes W'$ have the same Brauer character (and therefore the same composition factors by Brauer).*

Proof. The Brauer character of $\overline{W}$ is the values of the p'-elements of the ordinary character of V: suppose the ordinary character is φ_V and g is a p' element with eigenvalues $\lambda_1, \cdots, \lambda_n$ on W then g acts on $\overline{W}$ with eigenvalues $\lambda_i + (\pi)$. The Brauer character is by definition the sum of the lifts of these, and so is $\lambda_1 + \cdots + \lambda_n$. □

Definition 7.3. If $V_1, \ldots, V_l$ are irreducible KG-modules and $W_1, \ldots W_l$ are corresponding $\mathcal{O}$-forms, with $S_1, \ldots S_m$ the irreducible kG-modules then the *decomposition matrix* D has:

- rows indexed by $\{V_i\}$;
- columns indexed by S_j;
- entries d_{ij} given by

  $$d_{ij} = [k \otimes_{\mathcal{O}} W_i : S_j]$$

  the multiplicity with which S_j appears as a composition factor of $k \otimes_{\mathcal{O}} W_i = W_i/\mathfrak{p}W_i$, the *decomposition number*

Examples 7.4. (a) If $G = A_5$ then the ordinary character table is

1	2	3	5	5
1	1	1	1	1
3_1	-1	0	ϕ	$1-\phi$
3_2	-1	0	$1-\phi$	ϕ
4	0	1	-1	-1
5	1	-1	0	0

where $\phi = \frac{1+\sqrt{5}}{2}$. View this as a matrix, X.

If $\mathrm{char}(k) = 2$ then the Brauer character table B is

1	3	5	5
1	1	1	1
2_1	-1	$\phi - 1$	$-\phi$
2_2	-1	$-\phi$	$\phi - 1$
4	1	-1	-1

and the decomposition matrix D is given by

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

where the rows are indexed by $1, 3_1, 3_2, 4, 5$ and the columns by $1, 2_1, 2_2, 4$.

The matrix DB is the 5×4 matrix, which is X with the second column deleted. The ith row of D is the modular composition factors of $\overline{M} = M/\mathfrak{p}M$, M an irreducible kG-module.

(b) If $G = S_3$ in characteristics 2,3, then

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

where the columns are indexed by the trivial and $\overline{\psi}$ and the trivial and $\overline{\sigma}$ respectively.

(c) If G is a p-group and $\text{char}(k) = p$ then D has a single column and the entry for each ordinary irreducible is the degree of the ordinary irreducible, so G has a unique irreducible module modulo p.

(d) (See [Web16, 9.4.11]) If $(K, \mathcal{O}, k)$ is a splitting system for G and $(|G|, p) = 1$ then each simple KG-module reduces to a simple kG-module of the same dimension, and $D = \text{Id}$.

(e) (Fong, Swan, Rukolaine) Take a splitting system $(K, \mathcal{O}, k)$, p-modular for G p-solvable. Every irreducible kG-module is reduction mod (π) of $\mathcal{O}G$-lattice. In particular, D contains Id as a submatrix of maximal possible size.

8 Projective modules

Let R be a ring with 1 and let M be an R-module.

Definition 8.1. An R-module P is *projective* if for all surjective R-module homomorphisms $M' \to M$ and R-module homomorphisms $P \to M$ there is a homomorphism $P \to M'$ such that the following diagram commutes.

$$\begin{tikzcd} & P \arrow[dl, dashed] \arrow[d] & \\ M' \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

I is said to be *injective* if for all injective homomorphisms $M \to M'$ and homomorphisms $M \to I$ there is a homomorphism $M' \to I$ such that the following diagram commutes.

$$\begin{tikzcd}
 & I & \\
M' \arrow[ur, dashed] & M \arrow[l] \arrow[u] & 0 \arrow[l]
\end{tikzcd}$$

Lemma 8.2. *The following are equivalent.*

(i) *P is projective;*

(ii) *Every surjective homomorphism $M \xrightarrow{\lambda} P \longrightarrow 0$ splits, that is, there is an $\epsilon : P \to M$ such that $\lambda \circ \epsilon = \mathrm{Id}_P$;*

(iii) *P is isomorphic to a direct summand of a free module;*

(iv) *For all short exact sequences of R-modules $0 \to U \to V \to W \to 0$ the sequence $0 \to \mathrm{Hom}_R(P, U) \to \mathrm{Hom}_R(P, V) \to \mathrm{Hom}_R(P, W) \to 0$ is exact on the right.*

Lemma 8.3. *If k is a field and G a group, then every kG-module embeds into a free module.*

Proof. Define $\phi : M \to kG \otimes_k M$ by

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

so the target space is the restriction of M to the trivial followed by induction up to G, and the action of G is given by $g'(g \otimes m) = gg' \otimes m$. There is a vector space splitting $\psi : kG \otimes_k M \to M$ with $\psi(g \otimes m) = m$ if g is trivial and 0 otherwise. This shows that ϕ is injective. For $h \in G, m \in M$,

$$\phi(hm) = \sum_{g \in G} g \otimes g^{-1}(hm) = \sum_{g' \in G} hg' \otimes (g')^{-1} m = h \sum_{g' \in G} g' \otimes (g')^{-1} m = h\phi(m)$$

where $g' = h^{-1} g$. So ϕ is a kG-homomorphism. Since k is a field, $M \downarrow_{\{1\}}$ is free (it's a vector space) as a k-module and $M = \bigoplus k$. So $kG \otimes_k M$ is a free kG-module. $\square$

Lemma 8.4. *If M is a kG-module, the following are equivalent:*

(i) *M is projective;*

(ii) *M is injective;*

(iii) *(Higman) There is a k-linear $\lambda : M \to M$ with $\sum_{g \in G} g \lambda g^{-1} = \mathrm{Id}_M$.*

Proof. .

(ii) $\implies$ *(i)*: If M is injective there is an α such that the following diagram commutes:

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\beta"] \arrow[d, "\mathrm{Id}"] & kG \otimes_k M \arrow[dl, dashed, "\alpha"] \\ & M & \end{tikzcd}$$

So, we may realise M as a direct summand of the free module $kG \otimes_k M$, so M is projective.

(iii) $\implies$ *(ii)*: Fix a k-linear map γ not necessarily a kG-homomorphism with $\gamma\beta = \alpha$ below.

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\beta"] \arrow[d, "\alpha"] & M_2 \arrow[dl, dashed, "\gamma"] \\ \lambda \circlearrowright & M & \end{tikzcd}$$

Define $\gamma' = \sum_{g \in G} g(\lambda\gamma)g^{-1}$. This is a kG homomorphism:

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

where we set $g' = hg$. Moreover, since α, β are kG-homomorphisms,

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

This is $\mathrm{Id}_m \circ \alpha = \alpha$. So γ' makes the diagram above commute, so M is injective.

(i) $\implies$ *(iii)*: If $M = kG$ set $\lambda(\sum \alpha_g g) = \alpha_1 1_G$ so that

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

So $\sum_{h \in G} h\lambda h^{-1} = \mathrm{Id}_M$ for $M = kG$. We may apply this construction to any free kG-module M by applying λ to each factor. If M is not free, it is a summand of a free module by projectivity, $F = \oplus kG$ so let $\lambda_M = \pi\lambda_F\iota$, where π, ι are projection and inclusion respectively. Then $M \underset{\pi}{\overset{\iota}{\longleftrightarrow}} F \circlearrowleft \lambda_F$ and we have

$$\sum_{g \in G} g\lambda_m g^{-1} = \sum_{g \in G} g(\pi\lambda_F\iota)g^{-1} = \sum_{g \in G} \pi g\lambda_F g^{-1}\iota = \pi \,\mathrm{Id}_F\, \iota = \mathrm{Id}_M\,.$$

$\square$

9 Idempotents

Theorem 9.1. *(Krull-Schmidt) Let R be a finite-dimensional k-algebra, M a finitely generated R-module, and suppose that $M = \bigoplus_{i=1}^{s} M_i = \bigoplus_{i=1}^{t} M_i'$ are two independent decompositions of M into indecomposables. Then $s = t$ and after reordering $M_i' \cong M_i$.*

Note we can apply this in the cases of finitely generated $\mathcal{O}G$-modules, finitely generated kG-modules, R modules of finite length, but not when R is not artinian, e.g. $\mathbb{Z}G$-modules.

Corollary 9.2. *Under the conditions of Krull-Schmidt,*

1. *If M is indecomposable summand of $M_1 \oplus \cdots \oplus M_r$ with M_i indecomposable, then $M \cong M_i$ for some i.*
2. *Every finitely generated projective indecomposable R-module is isomorphic to a summand of ${}_RR$.*

This is clear: any projective P is a summand of $R \oplus \cdots \oplus R$ so apply (i).

Write ${}_RR = P_1 \oplus \cdots \oplus P_s$, for P_i projective indecomposables.

Fact. $R \cong \mathrm{End}({}_RR)^{op}$ (c.f. proof of Artin-Wedderburn) so the endomorphism

$$\pi :_R R \xrightarrow{project} P_i \xrightarrow{inj} {}_RR$$

is right multiplication by some $e_i \in R$ so $P_i = Re_i$ and $1 = e_1 + \cdots + e_s$, where the e_i are idempotents.

Definition 9.3. Let R be a ring with 1. An *idempotent* is an $e \in R$ such that $e^2 = e$. Note if e is idempotent, then so is $1 - e$, and $e(1 - e) = 0$. Idempotents e, e' are called *orthogonal* if $ee' = e'e = 0$, e is *primitive* if it cannot be written as $e = e' + e''$ for e', e'' nonzero orthogonal idempotents.

There is a 1-1 correspondence

$$\{\text{Direct sum decompositions } {}_RR = P_1 \oplus \cdots \oplus P_s, P_i \text{ projective}\}$$
$$\updownarrow$$
$$\{1 = e_1 + \cdots + e_s \text{ with } e_i \text{ primitive idempotents}\}$$

Recall Artin-Wedderburn: $R/J(R) = \prod_{i=1}^{t} M_{d_i}(\Delta_i)$ for R a finite dimensional k-algebra. If $T_i = M_{d_i}(\Delta_i)$, ${}_{T_i}T_i = \bigoplus(\text{columns of length } d_i) = \bigoplus S_i$. (see sheet 1 question 8) with the S_i simple and isomorphic as isotypical components. Let (e_{ij}) be the $d_i \times d_i$ matrix with the (j, j)th entry 1 and all other entries 0. For the matrix ring T_i,

$$1_{S_i} = e_{i1} + \cdots + e_{id_i}$$

and

$$1_{R/J(R)} = e_{11} + \cdots + e_{1d_1} + e_{21} + \cdots + e_{2d_2} + \cdots + e_{t1} + \cdots e_{td_t}$$

Let $R^\times$ be the group of invertible elements in R.

Example. $R = M_n(k)$, $1 = e_1 + \cdots + e_n$, $e_i = \begin{bmatrix} & & \\ & 1 & \\ & & \end{bmatrix}$ with the 1 in the ith position. Then every projective is of the form $Re_i = \begin{bmatrix} & * & \\ & * & \\ & * & \\ & * & \end{bmatrix}$ and $Re_i \cong Re_j$ even if $i \neq j$.

This motivates the following: define an equivalence relation on idempotents in R by conjugacy: $e \sim e' \iff \exists r \in R^\times$ such that $re = e'r$. Note $e \sim e' \iff (1-e) \sim (1-e')$.

Lemma 9.4. *Let e, e' be idempotents in R. Then $e \sim e'$ if and only if $Re \cong Re'$ and $R(1-e) \cong R(1-e')$.*

Proof. ($\Longrightarrow$) $e \sim e' \implies er = re'$ for some $r \in R^\times$ so $Rer = Rre' = Re'r$ implies $Re \cong Re'$, (multiplication on the right by r). Similarly, $R(1-e)r = Rr(1-e') = R(1-e')$.

($\Longleftarrow$) Let

$$Re \xrightarrow{\cong(\theta)} Re' \qquad \text{and} \qquad R(1-e) \xrightarrow{\cong(\phi)} R(1-e')$$

There is an isomorphism

$$\begin{aligned} \mathrm{Hom}_R(Re, M) &\longrightarrow eM \\ \lambda &\longmapsto \lambda(e) \end{aligned}$$

Since $\lambda(e) = \lambda(ee) = e\lambda(e) \in eM$. Using this, define $\mu_1 \in eRe' \leftrightarrow \theta$, $\mu_2 \in e'Re \leftrightarrow \theta^{-1}$, $\mu_3 \in (1-e)R(1-e') \leftrightarrow \phi$ and $\mu_4 \in (1-e')R(1-e) \leftrightarrow \phi^{-1}$.

Then $\mu_1\mu_2 = e, \mu_2\mu_1 = e', \mu_3\mu_4 = (1-e), \mu_4\mu_3 = (1-e')$. Also, $r = \mu_1 + \mu_3 \in R^\times$ since $(\mu_1+\mu_3)(\mu_2+\mu_4) = e+0+0+(1-e) = (\mu_2+\mu_4)(\mu_1+\mu_3)$.

So, $r^{-1}er = e'$ so $e' \sim e$.

□

So, to find projective indecomposables in ${}_RR$ it suffices to find them in $R/J(R)$ using Wedderburn and lift to R. R a f.d. algebra $\implies N = J(R)$ is a nilpotent ideal (using Nakayama's lemma).

Theorem 9.5 (Idempotent Refinement)**.** *Let R be a ring with 1, N a nilpotent ideal of R and e, e' idempotents in R/N. Then:*

(i) There is an idempotent $f \in R$ such that $\overline{f} = f + N = e$, with f primitive if and only if e is primitive;

(ii) $f \sim f'$ implies that $f + N \sim f' + N$.

Proof. □

Corollary 9.6. *Let N be a nilpotent ideal in a ring R and $1 = e_1 + \cdots + e_s$ a sum of orthogonal idempotents in R/N. Then there is a decomposition $1 = f_1 + \cdots + f_s$ in R into orthogonal idempotents such that $f_i + N = e_i$. If the e_i are primitive, so are the f_i.*

Proof. □

Corollary 9.7. *Let f be idempotent in R, I a nilpotent ideal. The f is primitive if and only if $f + I$ is primitive in R/I.*

Proof. ($\Longrightarrow$) by Theorem 9.5 (i).

($\Longleftarrow$) If $f = f_1 + f_2$ and $f_1 f_2 \in I$ for f_1, f_2 idempotent then $f_1, f_2 \notin I$ so $(f_1 + I)(f_2 + I) = 0$ and $(f_1 + f_2) + I = f + I$ gives the result. □

10 Projective indecomposable modules

Throughout, let R be a finite dimensional k-algebra and k a field. For M an R-module,

$$\begin{aligned} J(M) &= \cap(\text{maximal submodules}) \\ &= (\text{smallest submodule with semisimple quotient}) \\ &= J(R)M \end{aligned}$$

and

$$\begin{aligned} \operatorname{soc}(M) &= \sum(\text{simple summands of } M) \\ &= (\text{largest simple submodule}) \\ &= \{m \in M : J(R)m = 0\}. \end{aligned}$$

By Wedderburn, $R/J(R) = \prod_{i=1}^{s} M_{d_i}(\Delta_i)$ for Δ_i finite dimensional k-division algebras. $1_{M_{d_i}}$ has primitive orthogonal decomposition into idempotents $\overline{e}_{i1} + \cdots + \overline{e}_{id_i}$ corresponding to the simple modules S_i (given by columns). So,

$$1_{R/J(R)} = \overline{e}_{11} + \cdots + \overline{e}_{1d_1} + \cdots + \overline{e}_{s1} + \cdots + \overline{e}_{sd_s}$$

with $\overline{e}_{ij} \in M_{d_i}(\Delta_i)$ having (j,j)th entry 1, and all other entries 0. Lifting to R we get a primitive orthogonal idempotent decomposition

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

where $\overline{e}_{ij} \sim \overline{e}_{kl} \iff e_{ij} \sim e_{kl} \iff i = k$.

Hence we get a decomposition into projective indecomposable modules

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

with $Re_{ij} \cong Re_{kl} \iff k = i$.

Moreover, for each i, j,

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

where S_i is a simple R-module. Write $P_{S_i} = P_i$ for the module isomorphic to Re_{ij} for some j (it does not matter which j we choose). Then P_i is a projective indecomposable and $P_i/J(P_i) \cong S_i$.

So, there are s isomorphism classes of projective indecomposable R-modules P_i for $1 \leq i \leq s$ and each has a unique maximal submodule $J(R)P_i$. We call P_i the projective cover of S_i.

Example 10.1. (i) If k is a field of characteristic p and G is a p-group, $R = kG$ then the unique simple R-module is k. $J(R)$ is the augmentation ideal, $R/J(R) = k$ and the unique projective indecomposable is ${}_RR$ of length $|G|$ with all factors trivial.

(ii) $G = S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}, k = \mathbb{F}_3, R = kG$. There are two simple left kG-modules:

- The trivial k with annihilator the augmentation ideal;
- sign, with annihilator $\{\sum \lambda_g g : \lambda_1 + \lambda_\sigma + \lambda_{\sigma^2} = \lambda_\tau + \lambda_{\sigma\tau} + \lambda_{\sigma^2\tau} = 0\}$.

$J(R)$ is the intersection of the annihilators, which is the annihilator of sign, which has k-basis $\{1-\sigma, 1-\sigma^2, \tau - \sigma\tau, \tau - \sigma^2\tau\}$. So,

$$R/J(R) \cong M_1(k) \oplus M_2(k)$$

where $M_i(k) = \langle -(1 \pm \tau) + J\rangle$. Now, $e_1 = -(1+\tau)$ and $e_2 = -(1-\tau)$ are primitive idempotents in R so the projective indecomposable modules are given by

- Corresponding to e_1,

$$\begin{aligned} P_1 = R(1+\tau) &= \{\sum \lambda_g g : \lambda_1 = \lambda_\tau, \lambda_\sigma = \lambda_{\sigma\tau}, \lambda_{\sigma^2} = \lambda_{\sigma^2\tau}\} \\ &= \langle 1+\tau, \sigma + \sigma\tau, \sigma^2 + \sigma^2\tau\rangle \\ &= \text{ projective cover ot the trivial.} \end{aligned}$$

- Corresponding to e_2,

$$P_2 = R(1-\tau) = \text{ projective cover of sign.}$$

A composition series for P_1 is:

$$\begin{aligned} P_1 &\supseteq JP_1 = \langle 1 + \tau - \sigma - \sigma\tau, 1 + \tau - \sigma^2 - \sigma^2\tau\rangle \\ &\supseteq T_1 = \langle 1 + \sigma + \sigma^2 + \tau + \sigma\tau + \sigma^2\tau\rangle \\ &\supseteq 0 \end{aligned}$$

with P_1/JP_1 and T_1 both trivial R-modules. The action of R on JP_1/T_1 is determined by:

$$\begin{aligned}
\tau\cdot(1+\tau-\sigma-\sigma\tau+T_1) &= \tau+1-\tau\sigma-\tau\sigma\tau+T_1\\
&= 1+\tau-\sigma^2\tau-\sigma^2+T_1\\
&= -(1+\tau-\sigma-\sigma\tau)-(1+\sigma+\sigma^2+\tau+\sigma\tau+\sigma^2\tau)+T_1\\
&= -(1+\tau-\sigma-\sigma\tau)+T_1
\end{aligned}$$

so JP_1/T_1 is the sign R-module so not all factors are trivial. Similarly for P_2,

$$P_2 \supseteq JP_2 \supseteq T_2 \supseteq 0.$$

(iii) $\mathbb{Z}$ has no projective cover for any G.

Let R be a finite dimensional k-algebra for k a field and let M be a finitely generated R-module. Then $M/J(M)$ is semisimple, $\cong \bigoplus_1^N S_j$ for S_j simple R-modules. For each j, let $P_{S_j} = P_j$ be the projective cover. Consider the diagram:

$$\begin{tikzcd}
 & \bigoplus_1^N P_j \arrow[dl, dashed, "\pi"'] \arrow[d] & \\
M \arrow[r] & M/J(M) \cong \bigoplus_1^N S_j \arrow[r] & 0
\end{tikzcd}$$

Since $\bigoplus_1^N P_j$ is projective there is a hom $\pi : \bigoplus_1^N P_j \to M$ such that this commutes. We claim that π is surjective. Let N' be the image of π. Then $N'+J(M) = M$ so $J(R)M/N' = (J(R)M+N')/N' = (J(M)+N')/N' = M/N'$ so by Nakayama's lemma $N' = M$.

We call $\bigoplus_1^N P_j$ the projective cover of M. There is a short exact sequence

$$0 \longrightarrow \Omega M \longrightarrow M \longrightarrow M/J(M) \longrightarrow 0$$

where $\Omega M = \mathrm{Ker}(\pi)$ is called the Heller translate of first syzygy.

Aside on Duality

Let M be a left R-module. $M^* = \mathrm{Hom}_K(M, K)$ is a right R-module with action $(f\cdot r)(m) = f(rm)$ for $f \in M^*, r \in R, m \in M$. Similarly if M is a right R-module, M^* is a left R-module and if M is finite dimensional then $M \cong M^*$. Since $\mathrm{Hom}_K(-, K)$ is an exact contravariant functor from the category of left R-modules to the category of right R-modules and vice versa there is a correspondence

$$\{M \text{ f.g. projective left module}\} \leftrightarrow \{M^* \text{ f.g. injective right module}\}.$$

In the case $R = kG$, G finite, M left $\to M$ right, $mg = g^{-1}m$.

As a consequence of the above, if I is injective decomposable, it has a unique minimal (simple) submodule $\mathrm{soc}(I)$ and every simple R-module S_j has an injective decomposable R-module $I_{S_j} = I_j$ which has S_j as its unique simple submodule, $\mathrm{soc}(I_j) = S_j$.

Definition. I_{S_j} is called the *injective hull* of S_j.

Now let M be a finitely generated R-module. Then we have the following diagram:

$$\begin{tikzcd} & \bigoplus I_j & \\ 0 \arrow[r] & \mathrm{soc}(M) \cong \bigoplus S_j \arrow[u] \arrow[r] & M \arrow[ul, dashed, "\phi"'] \end{tikzcd}$$

where ϕ exists by injectivity of $\bigoplus I_j$. Note that $\phi|_{\mathrm{soc}(M)}$ is injective. Let $N = \mathrm{Ker}(\phi) \leq M$ If $N \neq 0$, $\mathrm{soc}(N) = \mathrm{soc}(N \cap M) = N \cap \mathrm{soc}(M) \neq 0$, a contradiction. Therefore ϕ is injective. Accordingly, we call $\bigoplus I_j$ the *injective hull* of M. We have an isomorphism $\mathrm{soc}(M) \cong \mathrm{soc}\left(\bigoplus I_j\right)$ and a short exact sequence

$$0 \longrightarrow M \longrightarrow \bigoplus I_j \longrightarrow \mho M \longrightarrow 0$$

where $\mho M = \mathrm{coker}(\phi)$. Note that $\Omega, \mho$ are not inverse to one another.

Theorem 10.2. *Let G be a finite group, K a field and P a projective indecomposable KG-module. Then $P/J(P) \cong \mathrm{soc}(P)$.*

Proof. We know $P = KGf$ for f a primitive idempotent. Let $y \in \mathrm{soc}(P)\backslash\{0\}$, $y = \sum_g \alpha_g g$. For any $b = \sum_g \lambda_g g$, $c = \sum_g \mu_g g$ the coefficient of 1 in bc is $\sum_g \lambda_g \mu_{g^{-1}} = \sum_{g^{-1}} \lambda_{g^{-1}} \mu_g$ which is the coefficient of 1 in cb. $y \neq 0$ so there is some $h \in G$ so that $\alpha_h \neq 0$. So, $z = h^{-1}y$ has a nonzero coefficient of the identity. $z \in KGf$ so $zf = z$ so zf has a nonzero coefficient of 1, so fz has a nonzero coefficient of 1 so $fz \neq 0$. Therefore, $f\,\mathrm{soc}(P) \neq 0$.

As seen in Lemma 9.4,

$$\mathrm{Hom}_{KG}(P, \mathrm{soc}(P)) = \mathrm{Hom}_{KG}(KGf, \mathrm{soc}(P)) \cong f\,\mathrm{soc}(P) \neq 0$$

so there is a non-zero homomorphism $\phi : P \to \mathrm{soc}(P)$. P is injective (since it is projective) and indecomposable so $\mathrm{soc}(P)$ is simple. Therefore, $\mathrm{Ker}(\phi)$ is a maximal submodule, so $\mathrm{Ker}(\phi) = J(P)$. The theorem then follows from the first isomorphism theorem. □

Remark. This holds for "symmetric algebras" of which group algebras are an example.

Lemma 10.3. *Let R be a finite-dimensional K-algebra where K is a splitting field for R, that is, $R/J(R) = \prod M_{d_i}(K)$. Let M be a finitely generated R-module. For S simple,* $\dim_K(\mathrm{Hom}_R(P_S, M)) = [M : S]$.

Proof. By induction on the composition length of M. If $M = S'$ then since K is a splitting field,

$$\dim_K \operatorname{Hom}_R(P_S, S') = \dim_K \operatorname{Hom}_R(S, S') = \begin{cases} 1 & S \cong S' \\ 0 & \text{otherwise} \end{cases}$$

by Schur's lemma. If M is not irreducible choose a maximal $M' \subsetneq M$, so there is a short exact sequence

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

As P_S is projective, $\operatorname{Hom}_R(P_S, -)$ is exact so

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

is exact. Dimensions add, as do the number of factors isomorphic to S. $M', M/M'$ have composition length strictly shorter than M so we are done by induction. □

11 Cartan invariants

Throughout, let G be a finite group, k a field of characteristic p, and let the irreducible kG-modules be denoted S_i with their projective covers P_i.

Definition 11.1. Let $c_{ij} = [P_j : S_i]$. The matrix $C = (c_{ij})$ is the *Cartan matrix* and the c_{ij} are called the *Cartan invariants.*

Theorem 11.2. *(i) If k is a splitting field for G, $c_{ji} = c_{ij}$.*

(ii) If $(K, \mathcal{O}, k)$ is a splitting p-modular system for G then

$$c_{ij} = \sum_l d_{li} d_{lj}$$

so $C = D^T D$.

*(iii)** $\det(C)$ *is a power of p, and in particular is nonzero.*

In order to prove this, we need some preparation on idempotent lifting.

Let $\mathcal{O}$ be a complete DVR with unique maximal ideal $\mathfrak{p}$, and $\mathcal{O}/\mathfrak{p} \cong k$. So,

$$\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G = \varprojlim_n \mathcal{O}G/\mathfrak{p}^n\mathcal{O}G. \quad (\star)$$

Since the canonical surjection $\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G \to \mathcal{O}G/\mathfrak{p}\mathcal{O}G$ has kernel $\mathfrak{p}\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G = k\mathcal{O}G$, which squares to zero, a primitive orthogonal decomposition

$$1 = \overline{e}_1 + \cdots + \overline{e}_s \in KG = \operatorname{Im}(\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G \to \mathcal{O}G/\mathfrak{p}\mathcal{O}G) \qquad (3)$$

lifts to

$$1 = e_{21} + \cdots + e_{2s} \in \mathcal{O}G/\mathfrak{p}^2\mathcal{O}G. \tag{4}$$

Similarly, via the canonical surjection $\mathcal{O}G/\mathfrak{p}^3\mathcal{O}G \to \mathcal{O}G/\mathfrak{p}^2\mathcal{O}G$ we get a lift

$$1 = e_{31} + \cdots + e_{3s}. \tag{5}$$

in $\mathcal{O}G/\mathfrak{p}^3\mathcal{O}G$ of (4).

Continuing, we get a primitive orthogonal decomposition up to level n: in $\mathcal{O}G/\mathfrak{p}^n G$ we have

$$1 = e_{n1} + \cdots + e_{ns}$$

such that $e_{nj} + \mathfrak{p}^{n-1} = e_{(n-1)j}$ for all n, j. By ($\star$) this terminates: there is an $e_j \in \mathcal{O}G$ such that $e_j + \mathfrak{p}^n = e_{nj}$ for all n.

Now, e_j^2 defines the same inverse system of elements as e_j does, so $e_j^2 = e_j$. Similarly, we can show

$$1 = e_1 + \cdots + e_s$$

is a primitive orthogonal decomposition of 1 in $\mathcal{O}G$. We have proved the following.

Theorem 11.3. *If $1 = \overline{e_1} + \cdots + \overline{e_s}$ is a decomposition of 1 into primitive orthogonal idempotents in kG then we can lift to a decomposition $1 = e_1 + \cdots + e_s$ in $\mathcal{O}G$. Moreover, conjugation is preserved.*

Consequently, the decomposition of kG into projective indecomposables

$$kG = \underbrace{P_{S_1} \oplus \cdots \oplus P_{S_1}}_{d_1} \oplus \cdots \oplus \underbrace{P_{S_n} \oplus \cdots \oplus P_{S_n}}_{d_n}$$

lifts to a decomposition of $\mathcal{O}G$,

$$\mathcal{O}G = \underbrace{\widehat{P}_{S_1} \oplus \cdots \oplus \widehat{P}_{S_1}}_{d_1} \oplus \cdots \oplus \underbrace{\widehat{P}_{S_n} \oplus \cdots \oplus \widehat{P}_{S_n}}_{d_n}$$

Proof off 11.2(ii). Given $(K, \mathcal{O}, k)$ a splitting p-modular system for G, with simple KG-modules $\{V_i\}$, $\mathcal{O}$-forms $\{W_i\}$, $V_i = K \otimes_{\mathcal{O}} W_i$. Calculating and using 10.3,

$$[K \otimes_{\mathcal{O}} \widehat{P}_{S_j}] = \dim_K \operatorname{Hom}_{KG}(K \otimes_{\mathcal{O}} P_{S_j}, V_i).$$

By the definition of W_i this is

$$\dim_K \operatorname{Hom}_{KG}(K \otimes_{\mathcal{O}} P_{S_j}, K \otimes_{\mathcal{O}} W_i).$$

This is a statement in characteristic zero. We now claim

(a)

$$\begin{aligned}\dim_K \operatorname{Hom}_{KG}(K \otimes_{\mathcal{O}} P_{S_j}, K \otimes_{\mathcal{O}} W_i) &= \dim_K(K \otimes \operatorname{Hom}_{\mathcal{O}G}(\widehat{P}_{S_j}, W_i)) \\ &= \operatorname{rank}_{\mathcal{O}}(\operatorname{Hom}_{\mathcal{O}G}(\widehat{P}_{S_j}, W_i))\end{aligned}$$

(b)

$$\operatorname{rank}_{\mathcal{O}}(\operatorname{Hom}_{\mathcal{O}G}(\widehat{P}_{S_j}, W_i)) = \dim_k \operatorname{Hom}_{kG}(P_{S_j}, k\otimes W_i) = [k\otimes_{\mathcal{O}} W_i : S_j] = d_{ij}$$

(a) holds because $\mathcal{O}$ is a PID, so $\widehat{P}_{S_j}, W_i, \operatorname{Hom}_{\mathcal{O}G}(\widehat{P}_{S_j}, W_i)$ are $\mathcal{O}$-free. Given a KG-homomorphism $K \otimes_{\mathcal{O}} \widehat{P}_{S_j} \to K \otimes_{\mathcal{O}} W_i$, some nonzero multiple sends $\widehat{P}_{S_j}$ into W_i by finite generation and clearing denominators, using $\mathcal{O}$-freeness. So, the map

$$K \otimes \operatorname{Hom}_{\mathcal{O}G}(\widehat{P}_{S_j}, W_i) \to \operatorname{Hom}_{KG}(K \otimes_{\mathcal{O}} P_{S_j}, K \otimes_{\mathcal{O}} W_i)$$

sending $\lambda \otimes \varphi$ to $\lambda\varphi$ is an isomorphism. The second equality follows since $\widehat{P}_{S_j}$ is projective.

(b) holds since $k \otimes -$ induces a map

$$\operatorname{Hom}_{\mathcal{O}G}(\widehat{P}_{S_j}, W_i)) \to \operatorname{Hom}_{kG}(P_{S_j}, k \otimes W_i)$$

which is surjective with kernel $\mathfrak{p} \operatorname{Hom}_{\mathcal{O}G}(\widehat{P}_{S_j}, W_i)$.

Hence,

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

□

Remarks. 1. If R is a finite dimensional k-algebra, k a splitting field, and P a projective indecomposable, then if $k \subset k'$, $k' \otimes P$ is a projective indecomposable $k' \otimes R$-module.

2. The decomposition matrix can be read in two ways:

   - rows are modular composition factors of modular reductions of ordinary irreducibles.
   - columns are ordinary composition factors of lifts of modular projective indecomposables.

   Also, $D^T D = C$ is the modular composition factors of modular projective indecomposables.

3. Decomposition number d_{ij} are independent of the choice of $\mathcal{O}$-form W_i of V_i.

Example. If $G = A_5$ and $p = 2$, the rows of D are indexed by $\chi_1, \chi_{3a}, \chi_{3b}, \chi_4, \chi_5$ and the columns by $1, 2_1, 2_2, 4$,

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

Our new information says that $K \otimes_{\mathcal{O}} \widehat{P}_K = 1 \oplus 3_a \oplus 3_b \oplus 5$.

12 Blocks

Throughout, let G be a finite group, R a commutative ring with 1. The *centre* of the group ring RG, $Z(RG)$ is the free R-module with basis conjugacy class sums in G. That is, $\sum \alpha_g g \in Z(RG)$ if and only if $g \sim g'$ implies that $\alpha_g = \alpha_{g'}$. So, there is a ring homomorphism $Z(\mathcal{O}G) \to Z(kG)$ induced by the canonical surjection $\mathcal{O} \twoheadrightarrow k$. A *central idempotent* in R is an idempotent in $Z(R)$. A *centrally primitive* idempotent is an idempotent in $Z(R)$ which is primitive in $Z(R)$.

Definition 12.1. A *block* of R is an indecomposable two-sided ideal direct factor of R (when R is a direct product).

Krull-Schmidt 9.1 implies that if R is a finite dimensional algebra then $R = B_1 \times \cdots \times B_s$. This decomposition corresponds to

$$1 = e_1 + \cdots + e_s$$

with the e_i orthogonal centrally primitive idempotents. Note $B_i = e_i R$, $e_i \in Z(R)$ since for all $r \in R$,

$$e_i r = e_i(re_1 + \cdots + re_s) = e_i r e_i = (e_1 r + \cdots + e_s r)e_i = re_i,$$

since $e_i r e_j \in B_i B_j$ and is therefore the identity since the product is direct.

Also, if $1 = e_1' + \cdots + e_t'$ with the e_i orthogonal centrally primitive idempotents then

$$e_i = e_i 1 = e_i e_1' + \cdots + e_i e_t'$$

with each $e_i e_j'$ centrally primitive in $Z(R)$:

$$(e_i e_j')(e_i e_l') = e_i e_j' e_i e_l' = e_i^2 e_j' e_l' = \begin{cases} e_i e_j' & j = l \\ 0 & j \neq l. \end{cases}$$

Since e_i is primitive there is a unique j such that $e_i = e_i e_j' = e_j'$, so $s = t$ and $e_i = e_i'$.

Definition 12.2. If M is an R-module then $M = e_1M \oplus \cdots \oplus e_sM$ as R-submodules of M. If M is indecomposable, there is a unique i such that $M = e_iM$ and $e_jM = 0$ for all $j \neq i$. Say M *lies in* or *belongs to* B_i or e_i and write $M \in e_i$ or $M \in B_i$.

In particular, simple modules lie in a block.
Notice that $\mathrm{Hom}_R(e_iM, e_jM) = 0$ if $i \neq j$: if $f : e_iM \to e_jM$ then

$$f(m) = f(e_im) = e_jf(e_im) = e_je_if(m) = 0.$$

So M is in e_i if and only if each of its direct summands belongs to e_i. An indecomposable R-module lies in a unique block, that is, the block e_i such that $e_iM \neq 0$.

Lemma 12.3. *Let e be a block of R. If $0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$ is a s.e.s. of R-modules then $V \in e$ if and only if $U, W \in e$. In other words, submodules and quotients of V belong to e.*

Proof. A module belongs to e if and only if muliplication by e acts as an isomorphism, which holds for V if and only if it holds for both U and W. □

Examples.

1. If R is a finite dimensional semisimple k-algebra then the blocks are matrix summands of R, each block idempotent is the identity of some matrix summand. If $R = \mathbb{C}G$ then the defining idempotents are determined by the ordinary characters.

2. If G is a p-group, $\mathrm{char}(k) = p$ then the regular representation is indecomposable as a module and therefore as a ring. So, the only possible idempotent is the identity, and there is a unique block.

Let $R = kG$ and refine $1 = e_1 + \cdots + e_s$ in $Z(R)$ to $1 = \hat{e}_1 + \cdots + \hat{e}_s$ in $Z(\mathcal{O}G)$. Our indecomposable $\mathcal{O}G$-modules also lie in blocks. If V is an irreducible KG-module, choose an $\mathcal{O}$-form W of V. Then there is a i such that $\hat{e}_iW \neq 0$ and $\hat{e}_jV = 0$ for all $j \neq i$.

Remark. We can think of a block as a bucket into which we put "stuff":

- indecomposable kG-modules;
- indecomposable $\mathcal{O}G$-modules;
- simple KG-modules.

Let V_i be a simple ordinary irreducible and suppose S_j is a simple modular irreducible. If V_i lies in a different block to S_j, then $d_{ij} = 0$. The block to which the trivial module belongs is called the *principal block*. We will now develop a criterion for a simple module to be in a particular block.

Lemma 12.4. *If R is a commutative finite dimensional k-algebra then R is a product of local rings.*

Proof. Wedderburn 3.9 implies that $R/J(R) = \prod M_{d_i}(\Delta_i)$. Since R is commutative, the $\Delta_i = k_i$ are finite extensions of k. We have a decomposition $1 = \overline{e}_1 + \cdots + \overline{e}_s$ in $r/J(R)$. $J(R)$ is nilpotent so we can use idempotent refinement to lift to $1_R = e_1 + \cdots + e_s$, so $R = R_1 \times \cdots \times R_s$ where $R_i = e_i R$. So,

$$R_i/J(R_i) = e_i R/e_i J(R) \cong e_i(R/J(R)) = k_i$$

where k_i is a field. Therefore, $J(R)$ is maximal and is therefore the unique maximal ideal by definition of $J(R)$, so R_i is local. □

If R is a finite dimensional k-algebra and k is a splitting field then there are k-algebra homomorphisms $\lambda : R \to k$ given by projection onto the factors.

Definition 12.5. If R is a finite dimensional k-algebra, a *central character* or *central homomorphism* of R is a ring homomorphism $Z(R) \to k$.

Example. If R is a finite dimensional k-algebra and S is a simple R-module with $\mathrm{End}_R(S) = k$, then if k is a splitting field each $z \in Z(R)$ acts on S by $\lambda_s(z)$ giving a central homomorphism of R.

Proposition 12.6. *Let R be a finite dimensional k-algebra with a block decomposition $1 = e_1 + \cdots + e_s$.*

(i) $Z(R) = e_1 Z(R) \times \cdots \times e_s Z(R)$ is a block decomposition of $Z(R)$. Each $e_i Z(R)$ is a local ring and for each simple R-module S there is an inclusion

$$e_i Z(R)/J(e_i Z(R)) \hookrightarrow \mathrm{End}_R(S)$$

(ii) If R is finite dimensional over a splitting field k, k is a splitting field for $Z(R)$ and $e_i Z(R)/J(e_i Z(R)) \cong k$. There is a 1-1 correspondence between central homomorphisms ω_i and blocks B_i such that $\omega_i(e_j) = \delta_{ij}$.

Proof. (i) A decomposition of 1 as a sum of orthogonal centrally primitive idempotents in R, $Z(R)$ are the same thing, so there is a block decomposition $Z(R) = e_1 Z(R) \times \cdots \times e_s Z(R)$. Also, $e_i Z(R) \cong \mathrm{End}_{Z(R)}(e_i Z(R))$ is a local ring because, for any ring Λ and idempotent e, $e\Lambda e \cong \mathrm{End}_\Lambda(e\Lambda)$. If S is a simple R-module in the ith block then $e_i Z(R)$ acts nontrivially on S as endomorphisms as e_i acts by Id on the relevant block. So there is a nontrivial map $e_i Z(R) \to \mathrm{End}_R(S)$. Since $e_i Z(R)$ is local and $\mathrm{End}_R(S)$ is a division ring, there is an induced injection $e_i Z(R)/J(e_i Z(R)) \hookrightarrow \mathrm{End}_R(S)$.

(ii) If k is a splitting field then there are maps

$$k \hookrightarrow e_i Z(R)/J(e_i Z(R)) \hookrightarrow \mathrm{End}_R(S) \hookrightarrow k$$

which compose to give Id. In other words, $Z(R)/J(Z(R))$ is a direct product of s copies of k and the central homomorphisms ω_i are the s projection operators.

□

Example 12.7. Let K be a splitting field for KG, $\mathrm{char}(K) = 0$. We will construct a central homomorphism of KG with respect to a simple KG-module, V. Let $\{\mathcal{C}_i \mid i \in I\}$ be the set of conjugacy classes of G.

Let $\widehat{\mathcal{C}_i} = \sum_{g \in \mathcal{C}_i} g$. We can calculate $\mathrm{Tr}(\widehat{\mathcal{C}_i}, V)$ in two different ways:

- If $\widehat{\mathcal{C}_i}$ acts via the scalar $\lambda \in K$, $\mathrm{Tr}(\widehat{\mathcal{C}_i}, V) = \lambda \dim_K V$.
- $\chi_V(g) = \chi_V(h)$ if $g \sim h$ so $\mathrm{Tr}(\widehat{\mathcal{C}_i}, V)$ is $|\mathcal{C}_i|\chi_V(g) = |G : C_G(g)|\chi_V(g)$ for any $g \in \mathcal{C}_i$.

So,

$$\lambda = \frac{|G : C_G(g)|\chi_V(g)}{\dim_K(V)}$$

and there is a central homomorphism $\lambda_V : Z(KG) \to K$ defined by

$$\lambda_V(\widehat{\mathcal{C}_i}) = \frac{|G : C_G(g)|\chi_V(g)}{\dim_K(V)}.$$

Theorem 12.8. *The $\lambda_V(\widehat{\mathcal{C}_i})$ are algebraic integers.*

Proof. $Z(\mathbb{Z}G)$ has $\mathbb{Z}$-basis consisting of $\widehat{\mathcal{C}_i}$, so suppose

$$\widehat{\mathcal{C}_i}\widehat{\mathcal{C}_j} = \sum_l a_{ijl}\widehat{\mathcal{C}_l}$$

with $a_{ijl} \in \mathbb{Z}$. Since λ_V is a central homomorphism, it is a homomorphism of rings and

$$\lambda_V(\widehat{\mathcal{C}_i})\lambda_V(\widehat{\mathcal{C}_j}) = \sum_l a_{ijl}\lambda_V(\widehat{\mathcal{C}_l}).$$

So, $\mathrm{Im}(\lambda_V)$ is a subring of K, a finitely generated abelian group. Since $\alpha := \lambda_V(\widehat{\mathcal{C}_i})$ is in the image there is a chain of subgroups

$$\langle 1 \rangle \leq \langle 1, \alpha \rangle \leq \langle 1, \alpha, \alpha^2 \rangle \leq \dots$$

which eventually terminates, so $\alpha^n \in \langle 1, \alpha, \dots, \alpha^{n-1} \rangle$ for some $n \in \mathbb{N}$, so so α is an algebraic integer. □

Recall that for $(K, \mathcal{O}, k)$ a p-modular system, all algebraic integers in K lie in $\mathcal{O}$ so there is a ring homomorphism $\lambda_V : Z(\mathcal{O}G) \to \mathcal{O}$. Reducing mod $\mathfrak{p}$, we get $\overline{\lambda}_V : Z(kG) \to k$. Note if $a_i \in \mathfrak{p}$, then $\sum a_i \lambda_V(\widehat{\mathcal{C}_i})$ is in $\mathfrak{p}$ so $\overline{\lambda}_V$ is well-defined.

If $V \in e$ with $e \in Z(kG)$, $\hat{e} \in Z(\mathcal{O}G)$, $\hat{e}$ acts as the identity on V so $\lambda_V(\hat{e}) = 1$, so $\overline{\lambda}_V(e) = 1$. If W is an $\mathcal{O}$-form then every composition factor of $k \otimes_{\mathcal{O}} W = \overline{W}$, so for example S satisfies $\lambda_{\hat{S}} = \overline{\lambda}_V$, where $\hat{S}$ is S lifted to $\mathcal{O}$.

Theorem 12.9. *Let V, V' be irreducible KG-modules. V, V' are in the same block if and only if $\lambda_V \equiv \lambda_{V'} \pmod{\mathfrak{p}}$. That is, for each $g \in G$,*

$$|G : C_G(g)|\chi_V(g)/\dim_k V \equiv |G : C_G(g)|\chi_{V'}(g)/\dim_k V'.$$

Example. $G = A_5$ has 5 conjugacy classes. Let the representatives be $\sigma_1 = \mathrm{Id}$, $\sigma_2 = (12)(34)$, $\sigma_3 = (123)$, $\sigma_4 = (12345)$, and $\sigma_5 = (12354)$. The corresponding class sizes are 1,15,20,12, and 12. Let $V_1, \ldots V_5$ be representations of non-isomorphic KG-modules. Then, the table with (i,j)th entry

$$\lambda_{V_i}(\widehat{C_G(\sigma_j)}) = \frac{|G : C_G(\sigma_j)|\chi_{V_i}(\sigma_j)}{\dim_k V_i}$$

is

	$\dim_k(V_i)$	σ_1	σ_2	σ_3	σ_4	σ_5
V_1	1	1	15	20	12	12
V_2	3	1	-5	0	$2(1+\sqrt{5})$	$2(1-\sqrt{5})$
V_3	3	1	-5	0	$2(1-\sqrt{5})$	$2(1+\sqrt{5})$
V_4	4	1	0	5	-3	-3
V_5	5	1	3	-4	0	0

The classification into blocks, for $p = 2$ is $V_1, V-2, V_3, V_5; V_4$. For $p = 3$, $V_1, V_4, V_5; V_2; V_3$, and for $p = 5$, $V_1, V_2, V_3, V_4; V_5$.

Remarks. 1. $\overline{\lambda}_V$ is independent of choice of $\mathfrak{p}$ (see [Isa06, 15.8]).

2. V, V' reduced mod $\mathfrak{p}$ have common composition factors if and only if they are in the same block.

13 Defect groups

Let $\mathcal{C}$ be a conjugacy class in G.

Definition 13.1. A *defect group* of $\mathcal{C}$ is a Sylow p-subgroup of $C_G(g)$ for some $g \in \mathcal{C}$. This defines a conjugacy class of p-subgroups associated with $\mathcal{C}$. If P is a p-subgroup of G, $\mathcal{C}$ is *P-defective* if P contains sonce element of $\mathcal{C}$.

Lemma 13.2. *Suppose $\widehat{\mathcal{C}}_i\widehat{\mathcal{C}}_j = \sum_l a_{ijl}\widehat{\mathcal{C}}_l \in Z(\mathbb{Z}G)$. Fix a triple (i,j,l). Then, if $p \nmid a_{ijl}$ and $\mathcal{C}_l$ is P-defective then so are $\mathcal{C}_i, \mathcal{C}_j$.*

Proof. Choose $z \in \mathcal{C}_l$ and suppose z commutes with P. Let

$$\Omega = \{(x,y) \in \mathcal{C}_i \times \mathcal{C}_j \mid xy = z\}.$$

Recall $|\Omega| = a_{ijl}$. Since $p \nmid a_{ijl}$, and a_{ijl} is the sum of the cardinalities of the P-orbits of Ω which are either 1 or divisible by p, there is a fixed point $(x,y) \in \mathcal{C}_i \times \mathcal{C}_j$. That is, $gxg^{-1} = x$ and $gyg^{-1} = y$. Hence both $\mathcal{C}_i$ and $\mathcal{C}_j$ are P-defective. $\square$

If P is a p-subgroup of G, let $Z(\mathcal{O}G)_P$ be the set of all sums $\sum a_i\mathcal{C}_i$ where $a_i \in \mathcal{O}$ and if a defect group of the ith class is not conjugate to a subgroup of P, then $a_i \in \mathfrak{p}$. Note that if $P \leq_G P'$ (that is, P is G-conjugate to a subgroup of P') then $Z(\mathcal{O}G)_P \subseteq Z(\mathcal{O}G)_{P'}$.

Lemma 13.3. *$Z(\mathcal{O}G)_P$ is an ideal of $Z(\mathcal{O}G)$.*

In order to prove the lemma, we will first show the following:

Proposition 13.4. *If P_1, P_2 are p-subgroups of G then*

$$Z(\mathcal{O}G)_{P_1} Z(\mathcal{O}G)_{P_2} \subseteq \sum_{\substack{P \leq_G P_1 \\ P \leq_G P_2}} Z(\mathcal{O}G)_P.$$

Proof. Let I be the right hand side. Since $\mathfrak{p}Z(\mathcal{O}G) \subseteq Z(\mathcal{O}G)_P$ for any p-subgroup P of G, it suffices to show that whenever $\mathcal{C}_i$ is a conugacy class whose defect group is conjugate to a subgroup of P_1 and $\mathcal{C}_j$ is a conjugacy class whose defect group is conjugate to a subgroup of P_2, then $\widehat{\mathcal{C}_i}\widehat{\mathcal{C}_j} \subseteq I$.

Now, $\widehat{\mathcal{C}_i}\widehat{\mathcal{C}_j} = \sum_l a_{ijl}\widehat{\mathcal{C}_l}$. If $a_{ijl} \equiv 0 \pmod p$ then $a_{ijl} \in \widehat{\mathcal{C}_l} \in \mathfrak{p}Z(\mathcal{O}G) \subseteq I$. If $a_{ijl} \not\equiv 0 \pmod p$ then let P be a defect group of $\mathcal{C}_l$. Clearly, $\widehat{\mathcal{C}_l} \in Z(\mathcal{O}G)_P$ and by 13.2 both $\mathcal{C}_i, \mathcal{C}_j$ are P-defective so $P \leq_G P_1$, $P \leq_G P_2$ so $\widehat{\mathcal{C}_l} \in I$. So, $\widehat{\mathcal{C}_i}\widehat{\mathcal{C}_j} \in I$. □

Proof (of 13.3). If $P \in \mathrm{Syl}_p(G)$ then $Z(\mathcal{O}G)_P = Z(\mathcal{O}G)$. So, apply 13.4 with P_1 or P_2 a Sylow p-subgroup. □

Definition 13.5. If e is a block (idempotent) in $Z(\mathcal{O}G)$ then a *defect group of* e is a minimal P-subgroup P of G such that $e \in Z(\mathcal{O}G)_P$.

13.6. The defect groups of any given block are conjugate.

In order to prove this, we will need the following.

Lemma 13.7 (Rosenberg's Lemma)**.** *Let R be a ring and e an idempotent of R. Suppose eRe is local (that is, it has a unique maximal two-sided ideal). We know $eRe = \mathrm{End}_R(R)^{\mathrm{op}}$. If $c \in \sum_\alpha I_\alpha$ where the I_α are two-sided ideals, then there is an α such that $c \in I_\alpha$.*

Proof. Since e is an idempotent and contained in $\sum_\alpha I_\alpha$, $e \in \sum_\alpha eI\alpha e$. Since eRe has a unique maximal 2-sided ideal, $e = \mathrm{Id}_{eRe}$ so not all $eI_\alpha e$ can be in the maximal ideal. So, there is an α such that $eI_alphae = eRe \subseteq I_\alpha$. □

Proof (of 13.6). If $e \in Z(\mathcal{O}G)_{P_1} \cap Z(\mathcal{O}G)_{P_2}$ then by 13.4,

$$e = e^2 \in \sum_{\substack{P \leq_G P_1 \\ P \leq_G P_2}} Z(\mathcal{O}G)_P.$$

So, by 13.7, there is a p-subgroup P of G such that $P \leq_G P_1$, $P \leq_G P_2$ and $e \in Z(\mathcal{O}G)_P$. If P_1, P_2 are minimal then $P_1 \sim_G P$ and $P_2 \sim_G P$ so $P_1 \sim_G P_2$. □

14 Relative projectivity and the transfer map

The transfer map

Let $H \leq G$. G acts on $\mathcal{O}G$ by conjugation. The fixed points are $(\mathcal{O}G)^G = Z(\mathcal{O}G)$, and $(\mathcal{O}G)^H$ has a $\mathcal{O}$-basis consisting of H-conjugacy class sums in G, $\{x \sim_H y$ if and only if $\exists h \in H, hxh^{-1} = y\}$. If $x \in (\mathcal{O}G)^H$ define

$$\operatorname{Tr}_H^G(x) = \sum_{g \in G/H} gxg^{-1}$$

where G/H is a set of representatives of left cosets of H in G. To see that this is independent of choice of coset representatives, let two choices of coset representatives be $\{g_1, \dots, g_t\}$ and $\{g_1h_1, \dots, g_th_t\}$. Then, with respect to the second set,

$$\operatorname{Tr}_H^G(x) = \sum_{i=1}^{t} g_ih_ixh_i^{-1}g_i^{-1} = sum_{i=1}^{t} g_ixg_i^{-1}$$

since x is H-invariant.

We call Tr_H^G the transfer map and denote the image by $(\mathcal{O}G)_H^G$.

Lemma 14.1. *(i) If $H \leq K \leq G$,*

$$\operatorname{Tr}_K^G \operatorname{Tr}_H^K(x) = \operatorname{Tr}_H^G(x).$$

(ii) $\operatorname{Tr}_H^K \operatorname{Res}_H^K$ is multiplication by $[K : H]$.

(iii) $(\mathcal{O}G)^H$ is an ideal of $Z(\mathcal{O}G)$.

Proof. For the third part, let $x \in (\mathcal{O}G)^H$, $y \in (\mathcal{O}G)^G$. Then $\operatorname{Tr}_H^G(x) \cdot y$ is given by $\operatorname{Tr}_H^G(xy)$. For the rest of the proof, see [Web16, 11.3.1, 11.3.2, 11.3.3.] □

Lemma 14.2. *Suppose P is a Sylow p-subgroup of H. Then $(\mathcal{O}G)^H = (\mathcal{O}G)_P^G$.*

Proof. If $x \in (\mathcal{O}G)^H$ then $x = \operatorname{Tr}_P^H\left(\frac{1}{[H:P]}x\right)$ so

$$\operatorname{Tr}_H^G(x) = \operatorname{Tr}_H^G \operatorname{Tr}_P^H\left(\frac{1}{[H:P]}x\right) = \operatorname{Tr}_P^G\left(\frac{1}{[H:P]}x\right).$$

□

Lemma 14.3. *If P is a p-subgroup of G then $Z(\mathcal{O}G)_P = (\mathcal{O}G)_P^G + \mathfrak{p}Z(\mathcal{O}G)$.*

Proof. Take a P-conjugacy class sum in G, and transfer it up to G. If g is in a P-conjugacy class,

$$\operatorname{Tr}_P^G\Big(\sum_{\substack{x \in \text{ reps} \\ \text{of } P/C_P(g)}} xgx^{-1}\Big) = sum_{x \in G/C_P(g)} xgx^{-1} = |C_G(g)C_P(g)|\widehat{\mathcal{C}}_g$$

where $\mathcal{C}_g$ is the G conjugacy class containing g. But $|C_G(g) : C_P(g)$ is not divisible by p if and only if $C_P(g)$ is a defect group of $\mathcal{C}_g$ containing g, which is equivalent to P containing a defect group of $\mathcal{O}g$. □

Lemma 14.4. *If e is a primitive idempotent in $Z(\mathcal{O}G)$ with defect group D, then $e \in (\mathcal{O}G)_D^G$, that is, there is an $x \in (\mathcal{O}G)^D$ such that $e = \sum_{g \in G/D} gxg^{-1}$.*

Proof. Use 14.3 and 13.7. $\square$

Corollary 14.5. *If N is an indecomposable $\mathcal{O}G$-module lying in a block with defect group D there is an endomorphism $\theta \in \mathrm{End}_{\mathcal{O}D}(M)$ such that $\sum_{g \in G/D} g\theta g^{-1} = \mathrm{Id}_M$.*

Proof. Let e be a block idempotent. Then by 14.4, $\sum_{gxg^{-1}} = e$ for some $x \in (\mathcal{O}G)^D$, and e acts on M by the identity whilst x as an $\mathcal{O}D$-endomorphism θ. $\square$

Relative Projectivity

Let R be a commutative ring.

Definition 14.6. Let $H \leq G$, and let M be an RG-module. M is *(relatively) H-projective* if in any diagram of the form below, whenever the dotted arrow exists as an RH-module homomorphism making the diagram commute, it also exists as an RG-module homomorphism making the diagram commute.

$$\begin{tikzcd} & M \arrow[dl, dashed] \arrow[d] & \\ M' \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

Dually, M is said to be *(relatively) H-injective* if in any diagram of the form below, whenever the dotted arrow exists as an RH-module homomorphism making the diagram commute, it also exists as an RG-module homomorphism making the diagram commute.

$$\begin{tikzcd} & M & \\ M_1 \arrow[ur, dashed] & M_2 \arrow[l] \arrow[u] & 0 \arrow[l] \end{tikzcd}$$

Theorem 14.7 (Relative version of 8.4)**.** *Let $H \leq G$, and let M be an RG-module. The following are equivalent.*

(i) M is H-projective;

(ii) M is H-injective;

(iii) (Higman) There is a $\theta \in \mathrm{End}_{RH}(M)$ such that $\sum_{g \in G/H} g\theta g^{-1} = \mathrm{Id}_M$;

(iv) M is isomorphic to a direct summand of $U \uparrow_H^G$ for some RH-module U;

(v) M is isomorphic to a direct summand of $M \downarrow_H \uparrow^G$;

(vi) The natural surjective RG-module homomorphism $M \downarrow_H \uparrow^G \twoheadrightarrow M$ taking $g \otimes m$ to gm splits;

(vii) The natural injective RG-module homomorphism $M \hookrightarrow M \downarrow_H \uparrow^G$ taking m to $\sum_{g \in G/H} g \otimes g^{-1}m$ splits.

Proof. Let $H \leq G$ and let M be an RG-module.

$(vi) + (vii) \implies (v) \implies (iv)$ is immediate.

$(i) \implies (vi)$: the map in (vi) has an H-splitting given by $m \mapsto 1 \otimes m$.

$(ii) \implies (vii)$: the map in (vii) has an H-splitting given by $g \otimes m \mapsto \begin{cases} gm & g \in H \\ 0 & \text{otherwise} \end{cases}$.

$(iii) \implies (i)$ Consider the diagram

$$\begin{tikzcd} & M \arrow[loop left, "\theta"] \arrow[dl, dashed, "\rho"'] \arrow[d, "\gamma"] & \\ M_1 \arrow[r, "\alpha"] & M_2 \arrow[r] & 0 \end{tikzcd}$$

where ρ is an RH-homomorphism such that $\gamma = \alpha\rho$. Set

$$\rho' = \sum_{g \in G/H} g\rho\theta g^{-1}.$$

Then ρ' is an RG-homomorphism with $\alpha\rho' = \gamma$.

$(iii) \implies (ii)$ is similar.

$(iv) \implies (iii)$ If $M = U \uparrow^G$ let $\theta' \in \mathrm{End}_{RH}(M)$ be defined by

$$\theta'(g \otimes m) = \begin{cases} gm & g \in H \\ 0 & \text{otherwise.} \end{cases}$$

If M is a summand of $U \uparrow^G$ then

$$\theta : M \hookrightarrow U \uparrow^G \xrightarrow{\theta'} U \uparrow^G \twoheadrightarrow M$$

works.

$\square$

Examples. If R is commutative then RG is 1-free ($\cong R \uparrow^G$). Projective modules are 1-projective, and over a field the notions of projectivity and 1-projectivity agree. Every RG-module is G-projective.

Consequently, if B is a block of $\mathcal{O}G$ with defect group D and block idempotent e, and if M is an $\mathcal{O}G$-module such that $eM = M$ then M is a direct summand of a module induced from D (14.5) and 14.7 implies that every module with defect group D is D-projective.

15 Examples of blocks 1: defect 0

Recall that a block of G is the specification of a block idempotent e of $\mathcal{O}G$, also the corresponding block of kG, also the modules which belong to these blocks, the KG-modules which belong to these blocks, also the ring direct factors $e\mathcal{O}G$ and $\overline{e}kG$ of kG.

Definition 15.1. If B is a block of $\mathcal{O}G$ or kG with defect group D of order p^a, then we say D is a block of *defect* a.

Suppose B is a block of defect 0, that is, $D = \{1\}$. Let e be a block idempotent. We can ask which kG-modules lie in B. An induced kG-module from $\{1\}$ is free so every kG-module in B is a summand of such a thing, hence is projective.

It is easy to show by induction that ever finitely generated kG-module in B is semisimple. Hence, $J(ekG) = 0$. By Wedderburn 3.9 $ekG \cong \prod M_{n_i}(\Delta_i)$.

Consequently, there is only one isomorphism class of simple kG-modules S, but everything is projective, so S is simple and projective. Since S is a projective kG-module, idempotent refinement 9.5 implies that it lifts uniquely (up to isomorphism) to a projective $\mathcal{O}G$-module, $\widehat{S}$. Then, $K \otimes_{\mathcal{O}} \widehat{S}$ is a simple KG-module. Since the columns of the decomposition matrix give the composition factors of $K \otimes_{\mathcal{O}} \widehat{S}$ it follows that the decomposition and Cartan matrices are (1).

Proposition 15.2. *If B is a block of defect 0, the simple module in B has dimension divisible by the p-part of the group order, $|G|_p$.*

Proof. Let $P \in \mathrm{Syl}_p(G)$. Let S be simple in B. Then $S\downarrow_P$ is a projective kP-module since S is a projective kG-module. But the unique projective indecomposable kP-module is kP. So, $S\downarrow_P$ is a direct sum of copies of kP. In particular, the dimension is divisible by $|P|$. □

Lemma 15.3. *kP has a unique simple module, and hence a unique projective indecomposable.*

Proof. □

We might hope that if $\mathrm{char}(k) = p$ and S is a simple kG-module of dimension divisible by $|G|_p$, then S is necessarily projective, but this turns out to be false. In the 1980s, John Thackray showed that the sporadic simple group McL has a simple module in characteristic two of dimension $2^9 \cdot 7$. This module is not projective, and the 2-part of the group order is 2^7.

The decomposition matrix of kP has only one column with entry $\dim V$ corresponding to the simple KP-module $\dim V$. Let W be an $\mathcal{O}$-form for V. Then the composition factors for $k \otimes_{\mathcal{O}} W$ are k of multiplicity $\dim V$. If E is the decomposition matrix, then

$$E = \begin{bmatrix} \vdots \\ \dim V \\ \vdots \end{bmatrix}$$

so the Cartan matrix $E^T E$ is $(|P|)$ since $|P| = \sum(\dim V)^2$ as V runs over the representations of the simple modules.

15.4 ((Open) problems: local-global conjectures)**.** In 1963, Brauer's Problem 19 appeared: can the number of blocks of defect 0 of a finite group G be described in terms of the group theoretic invariants of G? It was solved by G. Robinson in 1983.

The Alperin-McKay conjecture states that the number of simple kG-modules is given by

$$\sum_{\substack{\text{ccls of } p\text{-subgroups} \\ D \leq G, \text{ including } 1 = D}} |\{\text{blocks of defect 0 of } N_G(D)/D\}|$$

The McKay conjecture (1972) states that there is a count of chaacters of p'-degree, whereas the conjecture above is concerned with characters whose degree has maximal possible p-part. The McKay conjecture says that, for $P \in \mathrm{Syl}_p(G)$, if $\mathrm{Irr}_{p'}(G)$ is the set of irreducible characters χ with $p \nmid \chi(1)$,

$$|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(N_G(p))|.$$

16 Examples of blocks 2: blocks of finite type

For reps of $(\mathbb{Z}/p^n\mathbb{Z})$ in chatacteristic p, consider Jordan canonical form for a generator. For an indecomposable representation there is a single Jordan block. $X^{p^n} - 1 = (X-1)^{p^n}$ so the eigenvalues are all 1. So, the Jordan block has the form

$$J = \underbrace{\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}}_{d}.$$

The order of this matrix is the smallest p-power bigger than d: the entries appearing in J^n are $\binom{n}{i}$ for some $0 \leq i \leq n$ and with n always appearing directly above the diagonal, so the order is p^a for some a. If $p^a < d$ then some entry strictly above the diagonal is 1, so we must have $p^a \geq d$. If $1 \leq d \leq p^a$ then since $p \mid \binom{p}{a}$ for all $1 \leq a \leq p^a - 1$, $J^{p^a} = \mathrm{Id}$. Consequently, there are p^n isomorphism classes of indecomposable $k(\mathbb{Z}/p^n\mathbb{Z})$-modules and they correspond to blocks of size d where $1 \leq d \leq p^n$.

Definition 16.1. Say that a ring A has *finite (representation) type* if there are finitely many isomorphism classes of indecomposable A-modules, otherise say A has *infinite (representation) type.*

Example 16.2. If a block of kG has a cyclic defect group D then there are only a finite number of indecomposable kG-modules lying in the block. (Every indecomposable is a direct summand of (Jordan block for D)$\uparrow^G$ where D is the defect group of the given block.)

Theorem 16.3. *Let $R \in \{\mathcal{O}, k\}$, and let $P \in \mathrm{Syl}_p(G)$. Then, RG has finite representation type if and only if RP has finite representation type.*

Proof. $[G : P]$ is invertible in R so every RG-module M is a summand of some module $U \uparrow_P^G$ (by 14.2). Without loss of generality, we may assume U is indecomposable, for if it splits as $U = U_1 \oplus U_2$, $U \uparrow^G = U_1 \uparrow^G \oplus U_2 \uparrow^G$ and Krull-Schmidt 9.1 applies. So, the indecomposable summands of G are the indecomposable summands of $U_1 \uparrow^G$ together with the indecomposable summands of $U_2 \uparrow^G$.

If RP has finite type then there are only finitely many modules $U \uparrow_P^G$ with U indecomposable, and by Krull-Schmidt 9.1 there are only finitely many isomorphism classes of summands. hence RG is of finite type.

Conversely, every RP-module U is a direct summand of $U \uparrow_P^G \downarrow_P^G$ by 14.7, hence a direct summand of some $V \downarrow_P^G$. If U is indecomposable, we can assume V is indecomposable, and if RG has finite type there are only finitely many possibilities by Krull-Schmidt 9.1, hence RP has finite type. □

Consequently, $(\mathbb{Z}/p^n\mathbb{Z})$ has finite type over a field of characteristic p so by 16.3, groups with cyclic Sylow p-subgroups have finite type. Amazingly, the converse is also true.

Example 16.4. If $G = C_p \times C_p$, suppose it is generated by g, h. Let k be an infinite field of characteristic p. For each $\lambda \in k$ we can construct an indecomposable kG-module M_λ with matrix representation

$$g \mapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ h \mapsto \begin{bmatrix} 1 & \lambda \\ & 1 \end{bmatrix}.$$

If $\lambda \neq \mu$ then it is straightforward to see that $M_\lambda \ncong M_\mu$, so we have an infinite number of indecomposable non-isomorphic kG-modules.

In fact, the group algebra $k(C_p \times C_p)$ has infinitely many indecomposables of any given dimension (see [Web16]).

Theorem 16.5 (D. Higman)**.** *Let* $\mathrm{char}(k) = p$*. Then, kG has finite type if and only if the Sylow p-subgroups of G are cyclic.*

Proof. By 16.3 we may assume that G is a p-group. By the discussion at the start of the chapter, $k(\mathbb{Z}/p^n\mathbb{Z})$ has finite type, so suppose P is a non-cyclic P-group. Then, P has $C_p \times C_p$ as a homomorphic image. To see this, let $\Phi(P)$

be the Frattini subgroup of P, that is, the smallest $N \triangleleft P$ such that P/N is elementary abelian: the group analogue of the Jacobson radical.

So, $P/\Phi(P)$ is elementary abelian isomorphic to $\underbrace{C_p \times \cdots \times C_p}_{d \text{ multiplicands}}$ and P can be generated by d things and no fewer. Since P cannot be generated by a single element, $d \geq 2$.

Hence, we may lift each non-isomorphic indecomposable representations of $C_p \times C_p$ to get an infinite number of indecomposable non-isomorphic kP-modules. $\square$

17 Brauer's First Main Theorem

This section will prove that, for $R \in \{\mathcal{O}, k\}$ there is a 1-1 correspondence between blocks of RG with defect group D, and blocks of $RN_G(D)$ with defect group D. It turns out that it suffices to consider the case $r = k$, because reduction mod $\mathfrak{p}$ preserves D.

Lemma 17.1. *Suppose D is a p-subgroup of G and* $\operatorname{char}(k) = p$. *Then:*

(i) $(kG)^D = kC_G(D) \oplus \sum_{D'<D}(kG)^D_{D'}$*, and*

(ii) $(kG)^{N_G(D)} = (kC_G(D))^{N_G(D)} \oplus \sum_{D \not\leq Q \leq N_G(D)}(kG)^{N_G(D)}_Q$.

In each case this is a direct sum of a subring and a 2-sided ideal.

Proof. For the first, part, let D act by conjugation. The space $(kG)^D$ has basis over k consisting of the D-conjugacy class sums, $\widehat{\mathcal{C}}_{g,D} = \sum_{x \sim_D g} x$. If the orbit has length one then $\widehat{\mathcal{C}}_{g,D} \in kC_G(D)$, otherwise let $D' = C_D(g) < D$, with left coset representatives $\delta_1, \ldots, \delta_s$ of D' in D. So,

$$\widehat{\mathcal{C}}_{g,D} = \sum_{i=1}^{s} \delta_i g \delta_i^{-1} \in (kG)^D_{D'}$$

as $\widehat{\mathcal{C}}_{g,D}$ is precisely the set $\{\delta_1 g \delta_1^{-1}, \ldots, \delta_s g \delta_s^{-1}\}$. Finally, $kC_G(D) \cap \sum_{D'<D}(kG)^D_{D'} = \{0\}$ in characteristic 0 by definition of the transfer map and since $D' < D$ has index p^k for some k.

The second part is left as an exercise. The idea is to split the orbit of $N_G(D)$ into pieces, on some of which the action is trivial and on the remainder of which there are no fixed points. In each case, the right hand side is a 2-sided ideal by 14.1. $\square$

Remarks. (i) follows from a general result about permutation representations, see [Web16, 12.5.3].

The intersection being $\{0\}$ fails over $\mathcal{O}$, but there is a correspondence between blocks of kG and blocks of $\mathcal{O}G$ preserving defect groups, so in counting blocks we can work over k without loss of generality.

Definition 17.2. We define the *Brauer morphism* as the ring homomorphism given by projection $\mathrm{Br}_D : (kG)^D \to kC_G(D)$ given by projection onto the first factor in 17.1(i). Since the second factor is a 2-sided ideal, this *is* a homomorphism.

Remark. In a sense, we are really only interested in the map $\mathrm{Br}_D : Z(kG) \to Z(kC_G(D))$ obtained by restriction, since this is where the central idempotents live. Recall $Z(kG) = (kG)^G \leq (kG)^D$. The point of the more general definition is seen in 17.6.

Theorem 17.3. *Let G be a finite group with a normal p-subgroup D. Then every block idempotent in the centre $Z(kG)$ lies in $kC_G(D)$.*

Proof. Suppose S is a simple kG-module. Then S^D is a nontrivial kG-submodule of S since $S \downarrow^G_D$ contains a copy of the trivial module. So, $S^D = S$ and D acts trivially on S. Now, $kG/J(kG)$ is semisimple so D must act trivially on it. In characteristic p, $kG/J(kG)^D_{D'} = 0$ for any D'¡D, for if $x \in (kG)^{D'}, s \in S$ then

$$\mathrm{Tr}'^D_D(x) \cdot s = \sum_{g \in D/D'} gxg^{-1} \cdot s = \sum_{D/D'} x \cdot s.$$

This is $[D : D']x \cdot s$ and $p \mid [D : D']$ so

$$\sum_{D' < D} (kG)^D_{D'} \leq J(kG).$$

Let e be a block idempotent in kG. Write $e = x + y$ with $x \in kC_G(D), y \in \sum_{D'<D}(kG)^D_{D'}$. Now, $x^2 + xy = xe = ex = x^2 + yx$, so x, y commute so $e = e^{p^n} = (x + y)^{p^n} = x^{p^n} + y^{p^n}$ for all n. Taking n sufficiently large, $y^{p^n} = 0$ since the radical is nilpotent. So, $e = x^{p^n} \in kC_G(D)$. □

Corollary 17.4. *If $C_G(D) \leq D \lhd G$ then kG has only one block.*

Proof. $C_G(D)$ is a p-group since it is a subgroup of D and the group algebra of a p-group has all idempotents either 0 or 1. So, $kC_G(D)$ has only one nonzero idempotent, namely 1 (since 1 simple module means one projective indecomposable). Now apply 17.3. □

If $H \leq G$ such that $DC_G(D) \leq H \leq N_G(D)$ then 17.3 says that every idempotent in $Z(kH)$ lies in $kC_G(D)$. Let $e \in Z(kH)$ be a primitive idempotent corresponding to the direct factor b of kH. Let

$$1 = e_1 + \cdots + e_s$$

be a decomposition into primitive orthogonal idempotents in $Z(kG)$. This corresponds to the block decomposition of

$$kG = B_1 \times \cdots \times B_s.$$

Then, in the centre of kH we have that

$$\begin{aligned} e = e1 = e \operatorname{Br}_D(1) &= e \operatorname{Br}_D(e_1 + \cdots + e_s) \\ &= e \operatorname{Br}_D(e_1) + \cdots + e \operatorname{Br}_d(e_s). \end{aligned}$$

Since e is primitive, $e = e \operatorname{Br}_D(e_i)$ for some I and $e \operatorname{Br}_D(e_j) = 0$ for all $j \neq i$. Define the *Brauer correspondent* b^G of B to be the block B_i of kG. In general the Brauer correspondence just defined is not 1-1 but when $H = N_G(D)$, Brauer's First Main Theorem says that there is a 1-1 correspondence between blocks with defect group D.

Lemma 17.5. *Let* $\operatorname{char}(k) = p$*,* e *be a block of* kG*,* $D \leq G$*. The following are equivalent.*

(i) The block $e \in Z(kG)$ *has defect group* D*;*

(ii) $e \in (kG)^G_D$ *and* $\operatorname{Br}_D(e) \neq 0$*;*

(iii) D *is a maximal subgroup of* G *such that* $\operatorname{Br}_D(e) \neq 0$.

Proof. We first claim that A central idempotent e lies in $(kG)^G_D$ if and only if its defect group De is G-conjugate to a subgroup of D. This follows from the definition of the defect group of e, using that, if $De \leq_G D$,

$$Z(kG)_{De} \subseteq Z(kG)_D.$$

Now suppose e has defect group D. We now claim that $\operatorname{Br}_D(e) \neq 0$. By definition, $e \notin (kG)^D_{D'}$ for all $D' <_G D$. Equivalently, $e \notin \sum_{D <_G D} (kG)^D_{D'}$ by Rosenberg's Lemma 13.7. As

$$\ker \operatorname{Br}_D \cap (kG)^G_D = \sum_{D' < GD} (kG)^D_{D'},$$

we have that $\operatorname{Br}_D(e) \neq 0$. This also shows that $\operatorname{Br}_D(e) = 0$ if $D < De$.

We now claim that $\operatorname{Br}_D(e)$ is a primitive idempotent. The fact that it is an idempotent follows from the fact that Br_D is a ring homomorphism. To see that it is primitive, one way is to use a general form of idempotent refinement,

Lemma. *If* A, B *are finite dimensional* k*-algebras and* I, J *are ideals of* A, B *respectively and* $f : A \to B$ *is an algebra homomorphism such that* $f(I) = J$*, then if we have that* e *is a primitive idempotent of* A *contained in* I *such that* $f(e) \neq 0$ *then* $f(e)$ *is a primitive idempotent of* B.

The proof of this lemma is the same as the proof of idempotent refinement, 9.5.

The map is also injective and surjective by 17.6. $\square$

So D has both minimal and maximal properties.

Remark. Compare 17.5(iii) to 13.5 which says a defect group D is minimal amongst subgroups for which $e \in \operatorname{Tr}^G_D(x)$ for some $x \in (kG)^D$.

Theorem 17.6. *We have a commutative diagram:*

$$\begin{tikzcd}
(kG)^D \arrow[r, two heads, "\mathrm{Br}_D"] \arrow[d, two heads, "\mathrm{Tr}_D^G"] & kC_G(D) \arrow[d, two heads, "\mathrm{Tr}_D^{N_G(D)}"] \\
(kG)_D^G \arrow[r, two heads, "\mathrm{Br}_D"] & kC_G(D)_D^{N_G(D)}
\end{tikzcd}$$

In words, "transfer followed by Brauer is the same as Brauer followed by transfer."

Proof. Observe $(kG)_D^G \subseteq (kG)^G = Z(kG) \subseteq (kG)^D$. Also, $kC_G(D) = (kC_G(D))^D$ and $kC_G(D)_D^{N_G(D)} \subseteq Z(kC_G(D))$.

Let $x \in (kG)^D$,

$$\mathrm{Tr}_D^G(x) = \sum_{g \in D\backslash G/D} \mathrm{Tr}^G_{D\cap gDg^{-1}}(gxg^{-1}),$$

since for each (D, D)-double coset representative $g \in G$, we can take the set of left coset representatives $\delta(g) = \{\delta_{g,1}, \ldots, \delta_{g,n(g)}\}$ of $D \cap gDg^{-1}$ in D, and then we get a set of left coset representatives $\{\delta_{g,i} \cdot g\}$ of D in G, see [Web16, 11.3.1.(4)].

We now have two cases: either $D \cap gDg^{-1}$ is a proper subgroup of D or it is all of D. If $D \cap gDg^{-1}$ is a proper subgroup of D,

$$\mathrm{Br}_D \mathrm{Tr}^D_{D\cap gDg^{-1}}(gxg^{-1}) = 0$$

because we multiply by indices which are p-powers. So, the only terms that contribute have $D \cap gDg^{-1} = D$ which occurs if and only if $g \in N_G(D)$.

So,

$$\begin{aligned}
\mathrm{Br}(\mathrm{Tr}_D^G(x)) &= \sum_{g\in D\backslash N_G(D)/D} \mathrm{Br}_D \mathrm{Tr}_D^D \\
&= \sum_{g\in N_G(D)/D} \mathrm{Br}_D(gxg^{-1})
\end{aligned}$$

by the normality of D in $N_G(D)$.

Now, since $N_G(D)$ acts on both $kC_G(D)$ and $\sum_{D'<D}(kD)_{D'}^D$ respectively so

$$\begin{aligned}
\mathrm{Br}_D(\mathrm{Tr}_D(x)) &= \sum_{g\in N_G(D)/D} g\,\mathrm{Br}_D(x)g^{-1} \\
&= \mathrm{Tr}_D^{N_G(D)}(\mathrm{Br}_D(x))
\end{aligned}$$

and Br_D commutes with $\mathrm{Tr}_D^{N_G(D)}$. The bottom map is surjective by general nonsense. $\square$

Theorem 17.7 (The Brauer Correspondence)**.** Br_D *induces a 1-1 correspondence between block idempotents in* $Z(kG)$ *with defect group* D *and primitive idempotents in* $(kC_G(D))_D^{N_G(D)}$*. The correspondence is given by sending* $e \in (kG)_D^G$ *to* $\mathrm{Br}_D(e)$*.*

Corollary 17.8 (Brauer's First Main Theorem, 1944,1956,1970)**.** *Let* k *be a field of characteristic* p *that is a splitting field for* G *and all of its subgroups. Let* D *be a* p*-subgroup of* G *and let* H *be a subgroup of* G *containing* $N_G(D)$*. Then there is a one-to-one correspondence between the blocks of* kG *with defect group* D *and the blocks of* H *with defect group* D*.*

Proof. Since $N_G(D) \leq H \leq G$, $C_H(D) = C_G(D)$ and $N_H(D) = N_G(D)$. So we have

$$\begin{tikzcd}
 & \left\{\begin{array}{c}\text{block idempotents in}\\ Z(kG)\text{ with defect group } D\end{array}\right\} \arrow[d, leftrightarrow] \arrow[dl, dashed, leftrightarrow] \\
\left\{\begin{array}{c}\text{block idempotents in}\\ Z(kH)\text{ with defect group } D\end{array}\right\} \arrow[r, leftrightarrow] & \left\{\begin{array}{c}\text{primitive idempotents in}\\ kC_G(D)_D^{N_G(D)}=kC_H(D)_D^{N_H(D)}\end{array}\right\}
\end{tikzcd}$$

using 17.7 twice. $\square$

Exercise. Show that if b is a block of $kN_G(D)$ with defect group D then b^G is the corresponding block of kG with defect group D. (See [Web16, 12.6.4].)

An extended version of Brauer's main theorem is the following: there is a correspondence between blocks of $kN_G(D)$ with defect group D, and $N_G(D)$-conjugacy classes of blocks b of $k(DC_G(D)/D)$ of defect 0 such that $p \nmid [\mathrm{Stab}(b) : DC_G(D)]$ under the action of $N_G(D)$ by conjugation.

Brauer's second main theorem says that the Green correspondence is compatible with the Brauer correspondence.

Brauer's third main theorem says that the Brauer correspondent of a block is principal if and only if that block is the principal block.

These are covered in [Ben98, §6], [Alp86] and [Thé95].

On cyclic defect groups, the *Brauer tree algebras* describe the structure of projective indecomposable modules graph theoretically.

References

[Alp86] J. L. Alperin, *Local representation theory*, Cambridge Studies in Advanced Mathematics, vol. 11, Cambridge University Press, Cambridge, 1986. Modular representations as an introduction to the local representation theory of finite groups. MR860771

[Ben98] D. J. Benson, *Representations and cohomology. I*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, Cambridge, 1998. Basic representation theory of finite groups and associative algebras. MR1644252

[Isa06] I. Martin Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. MR2270898

[Sch13] Peter Schneider, *Modular representation theory of finite groups*, Springer, Dordrecht, 2013. MR3012316

[Thé95] Jacques Thévenaz, *G-algebras and modular representation theory*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1995. Oxford Science Publications. MR1365077

[Web16] Peter Webb, *A course in finite group representation theory*, Cambridge Studies in Advanced Mathematics, vol. 161, Cambridge University Press, Cambridge, 2016. MR3617363