MODULAR REPRESENTATION THEORY
AUTUMN SESSION 2007, ABERDEEN

DAVE BENSON
(NOTES BY KAY JIN LIM AND SEJONG PARK)

1. Representations and Modules

Let G be a finite group and let k be a commutative ring of coefficients. A *representation* of G over k is a group homomorphism $G \to \mathrm{GL}(n,k)$ for some n. The *group algebra* kG consists of linear combinations of elements of G with coefficients in k. With addition and multiplication defined as follows

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

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

kG is a ring, even a k-algebra.

Given a representation $\varphi\colon G \to \mathrm{GL}(n,k)$, we make $V = k^n$ into a kG-module via

$$\Big(\sum_{g\in G}\alpha_g g\Big)\cdot v = \sum_{g\in G}\alpha_g\varphi(g)(v), \qquad v\in V.$$

Conversely, provided that a kG-module M, when regarded as a k-module via $k \hookrightarrow kG$, is finitely generated and free, we get a representation $\varphi\colon G \to \mathrm{GL}(n,k)$ by choosing a k-basis for M and setting

$$\varphi(g)(v) = g\cdot v, \qquad g\in G, v\in V.$$

Example 1.1. If k is a field, then representations of G over k correspond to finite dimensional kG-modules.

Given two representations $\varphi\colon G\to\mathrm{GL}(n,k)$, $\psi\colon G\to\mathrm{GL}(m,k)$, they are *similar* if $n=m$ and there exists $X\in\mathrm{GL}(n,k)$ such that $X\varphi(g)X^{-1}=\psi(g)$ for all $g\in G$. This corresponds to an isomorphism of kG-modules. In general, an *intertwining operator* is an $n\times m$ matrix X with the property that

$$\varphi(g)X = X\psi(g) \qquad \forall g\in G.$$

This corresponds to a homomorphism between the corresponding kG-modules.

Example 1.2. For $G=\mathbb{Z}/2=\{1,t\}$, $k=\mathbb{F}_2$, define $\varphi\colon G\to\mathrm{GL}(2,k)$ by

$$\varphi(1)=\begin{pmatrix}1&0\\0&1\end{pmatrix}, \quad \varphi(t)=\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

Date: December 12, 2007.

Then the corresponding kG-module structure is given by

$$(\alpha \cdot 1 + \beta \cdot t)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} (\alpha+\beta)x + \beta y \\ (\alpha+\beta)y \end{pmatrix}, \quad \alpha, \beta, x, y \in k.$$

2. Reducibility and Decomposability

A representation $\varphi\colon G \to \mathrm{GL}(n,k)$ is *reducible* if it is similar to a representation ψ such that

$$\psi(g) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \qquad \forall g \in G.$$

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

A kG-module V is *reducible* if there is a submodule W with $0 \neq W \neq V$. Provided that k is a field, this concept corresponds to the reducibility of the representation. A kG-module is *irreducible* or *simple* if it is nonzero and not reducible.

A representation $\varphi\colon G \to \mathrm{GL}(n,k)$ is *decomposable* if it is similar to a representation ψ such that

$$\psi(g) = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \qquad \forall g \in G.$$

This says $V = W_1 \oplus W_2$, $\dim W_1 = i$, $\dim W_2 = j$ with W_1, W_2 invariant subspaces.

A kG-module is *decomposable* if $V = W_1 \oplus W_2$ with W_1, W_2 nonzero submodules of V. If V is nonzero and not decomposable, then it is *indecomposable.*

A *short exact sequence* of kG-modules is a sequence of kG-modules and kG-module homomorphisms of the form

$$0 \to V_1 \to V_2 \to V_3 \to 0$$

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

Example 2.1. In matrix notation:

$$0 \to (\varphi) \to \begin{pmatrix} (\varphi) & * \\ 0 & (\psi) \end{pmatrix} \to (\psi) \to 0.$$

A short exact sequence $0 \to V_1 \xrightarrow{\alpha} V_2 \xrightarrow{\beta} V_3 \to 0$ is *split* if there is a map $V_3 \xrightarrow{\gamma} V_2$ (a *splitting*) such that $\beta \circ \gamma = \mathrm{id}_{V_3}$. In this case, we have

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

Example 2.2. Example 1.2 gives a nonsplit short exact sequence in which V_1 and V_3 have dimension 1 and V_2 has dimension 2.

Theorem 2.3 (Maschke's Theorem)**.** *If $|G| \in k^\times$ and $0 \to V_1 \xrightarrow{\alpha} V_2 \xrightarrow{\beta} V_3 \to 0$ is a short exact sequence of kG-modules that splits as a sequence of k-modules, then it splits as a short exact sequence of kG-modules.*

Proof. Given a k-splitting $\varphi\colon V_3 \to V_2$, set $\gamma = \frac{1}{|G|}\sum_{g \in G} g^{-1}\varphi g$. If $x \in V_3$,

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

If $h \in G$, then

$$\gamma(hx) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\varphi ghx = h\frac{1}{|G|}\sum_{g\in G}(gh)^{-1}\varphi ghx = h\gamma(x).$$

$\square$

3. Homs and Tensors

Let R be a ring, and let M be a right R-module and N be a left R-module. The abelian group $M \otimes_R N$ has generators the symbols $m \otimes n$, $m \in M$, $n \in N$ and relations:

$$\begin{aligned}(m+m')\otimes n &= m\otimes n + m'\otimes n\\ m\otimes(n+n') &= m\otimes n + m\otimes n'\\ mr\otimes n &= m\otimes rn\end{aligned}$$

where $m \in M$, $n \in N$, $r \in R$.

Let A be an abelian group. A bilinear map $f\colon M \times N \to A$ is called *R-balanced* if it satisfies

$$f(mr,n) = f(m,rn)$$

for $m \in M$, $n \in N$, $r \in R$.

Theorem 3.1 (Universal Property of Tensor Products). *There is a R-balanced bilinear map $\tau\colon M\times N \to M\otimes_R N$ such that given any abelian group A and an R-balanced bilinear map $\alpha\colon M\times N \to A$ we have a unique group homomorphism $\beta\colon M\otimes_R N \to A$*

$$\begin{tikzcd} M\times N \arrow[r, "\alpha"] \arrow[d, "u"'] & A \\ M\otimes_R N \arrow[ur, dashed, "\exists!\beta"'] & \end{tikzcd}$$

such that $\alpha = \beta\circ\tau$.

Example 3.2. If R is a commutative ring, then left and right modules over R are equivalent. Given any two (left) R-modules M, N, we can form $M\otimes_R N$ and this is again an R-module via

$$r(m\otimes n) = rm\otimes n = m\otimes rn, \qquad r\in R, m\in M, n\in N.$$

If R, S are two rings, we say M is an *R-S-bimodule* if it is a left R-module and a right S-module in such a way that

$$(rm)s = r(ms), \qquad m\in M, r\in R, s\in S.$$

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

$$r(m\otimes n) = rm\otimes n, \qquad m\in M, n\in N, r\in R.$$

Example 3.3. If R is a ring, then we can regard R as an R-R-bimodule via left and right multiplication. If S is a subring of R, we can similiarly regard R as an R-S-bimodule.

If H is a subgroup of G, then we regard kH as a subring of kG and look at kG as a kG-kH-bimodule. If M is a kH-module,

$$kG \otimes_{kH} M$$

is a left kG-module called the *induced module* $M{\uparrow}^G$.

$\mathrm{Hom}(N, \mathrm{Hom}(M, A))$ corresponds bijectively to the set of bilinear maps $M \times N \to A$. The right action of R on M gives a left action of R on $\mathrm{Hom}(M, A)$ by $(r\varphi)(m) = \varphi(mr)$ where $\varphi \in \mathrm{Hom}(M, A)$, $m \in M$, $r \in R$. So it makes sense to look at $\mathrm{Hom}_R(N, \mathrm{Hom}(M, A))$. It corresponds bijectively to the set of R-balanced bilinear maps $M \times N \to A$. Hence the universal property of tensor product gives an isomorphism of abelian groups

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

If M is an S-R-bimodule and A is a left S-module, then this isomorphism restricts to

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

In particular, we have

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

Since kG is viewed as a kG-kH-bimodule, $\mathrm{Hom}_{kG}(kG, V)$ is V regarded as a left kH-module by restriction, $V{\downarrow}_H$. Thus we have

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

This is called the *Frobenius reciprocity* or the *Nakayama isomorphism*.

If U and V are two kG-modules, then $U \otimes_k V$ becomes a kG-module via

$$g(u \otimes v) = gu \otimes gv, \qquad g \in G, u \in U, v \in V.$$

Warning. Elements of the group algebra kG acts in a way extended linearly from this:

$$\begin{aligned}(g + h)(u \otimes v) &= gu \otimes gv + hu \otimes hv \\ &\neq (g + h)u \otimes (g + h)v.\end{aligned}$$

where $g, h \in G$, $u \in U$, $v \in V$.

Similarly, $\mathrm{Hom}_k(U, V)$ becomes a kG-module: if $f \in \mathrm{Hom}_k(U, V)$ and $g \in G$,

$$(gf)(u) = gf(g^{-1}u), \qquad u \in U.$$

With these definitions, if U, V, W are kG-modules,

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

is an isomorphism of kG-modules. Taking G-fixed points on both sides, we get

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

4. Exactness

If M is a right R-module and $0 \to N \to N' \to N'' \to 0$ is a short exact sequence of left R-modules, then the sequence

$$M \otimes_R N \to \otimes_R N' \to \otimes_R N'' \to 0$$

is exact.

If M is a left R-module and $0 \to N \to N' \to N'' \to 0$ is a short exact sequence of left R-modules, then the sequences

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

are exact.

Lemma 4.1. *If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of finite dimensional kG-modules (k a field) and $M_2 \cong M_1 \oplus M_3$, then the sequence splits.*

Remark 4.2. The finite dimensional condition is essential.

Proof. $0 \to \mathrm{Hom}_{kG}(M_3, M_1) \to \mathrm{Hom}_{kG}(M_3, M_2) \to \mathrm{Hom}_{kG}(M_3, M_3)$ is exact. Dimensions add, so the rightmost map is surjective. Take a preimage of id_{M_3}. It's a splitting! $\square$

5. The Jacobson Radical

Let R be a ring with 1.

The *Jacobson radical* of R is

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

If m is a maximal left ideal, then R/m is a simple left R-module and m is the annihilator of $[1]$ in R/m. Conversely, if S is simple module and $0 \neq x \in S$, then ${}_RR \to S$ given by $r \mapsto rx$ is surjective. If m is the kernel, then $S \cong R/m$. So

$$J(R) = \bigcap \text{annihilators of simple left } R\text{-modules}$$

A 2-sided ideal I in a ring R is *left primitive* if R/I has a faithful simple left module. The ring R is *left primitive* if (0) is a left primitive ideal of R.

Warning. left primitive is different from right primitive. (Bergman, 1964)

Lemma 5.1. $J(R) = \bigcap$ *left primitive 2-sided ideal*

As a consequence, $J(R)$ is a 2-sided ideal.

Example 5.2. Let V be an infinite dimensional vector space over a field k, $R = \mathrm{End}_k(V)$. This is a (left) primitive ring, but (0) is not maximal because

$$I = \{\text{endomorphisms with finite dimensional image}\}$$

is a nonzero proper ideal. Thus, in general, the concept of maximal ideals is different from that of primitive ideals. They coincide for finitely generated algebras.

Theorem 5.3. $J(R) = \{x \in R \mid \forall a, b \in R, 1 - axb$ *has a 2-sided inverse*$\}$.

Proof. If $x \in J(R)$, then $1-x$ is not in any maximal left ideal, so there exists $t \in R$ such that

$$t(1-x) = 1$$

Then $1 - t = -tx \in J(R)$ so t has a left inverse which must be $1 - x$. Applying this to $axb \in J(R)$ instead of x, $1 - axb$ has a 2-sided inverse.

Conversely, suppose $\forall a, b \in R$, $1 - axb$ has a 2-sided inverse. If $x \notin m$ a maximal left ideal, then there exist a, b with $b \in m$ such that

$$ax + b = 1$$

but then $1 - ax = b \in m$ does not have a 2-sided inverse, so $x \in m$. □

Corollary 5.4. *$J(R) = \bigcap$ maximal right ideals of R*

Lemma 5.5 (Nakayama's Lemma). *If M is a finitely generated R-module and $J(R)M = M$, then $M = 0$.*

Proof. Let $m_1, \dots, m_n$ be generators of M with n minimal. Let

$$m_n = \sum_{j=1}^{n} a_j m_j$$

with $a_j \in J(R)$, then $(1 - a_n)m_n = \sum_{j=1}^{n-1} a_j m_j$. But $1 - a_n$ has a 2-sided inverse $b \in R$, then

$$m_n = b(1 - a_n)m_n = \sum_{j=1}^{n-1} ba_j m_j$$

So $m_1, \dots, m_{n-1}$ generates M, a contradiction. □

Example 5.6. If S is a simple R-module, $J(R)S = 0$. Note that S is necessarily finitely generated.

An R-module M is *semisimple* or *completely reducible* if

$$M = \bigoplus_{\text{possibly infinite}} \text{simples}$$

We also have $J(R)M = 0$ in this case.

Proposition 5.7 (Properties of semisimple modules).

(1) *Every submodule of a semisimple module is semisimple and is a direct summand.*
(2) *Every quotient of a semisimple module is semisimple.*

Remark 5.8. In fact a module M is semisimple if and only if every submodule of M is a direct summand. (For a proof, see Farb and Dennis, *Noncommutative Algebra*, Exercise 17, p. 50.)

Theorem 5.9. *Suppose that R satisfies descending chain condition on left ideals (left Artinian), i.e., if*

$$I_1 \supseteq I_2 \supseteq \dots$$

are left ideals of R, then there exists n such that for all $m \geq n$, $I_m = I_n$. Then the following are equivalent:

(i) $J(R) = 0$
(ii) *Every R-module is semisimple*

(iii) *Every finitely generated R-module is semisimple.*

Remark 5.10. $\mathbb{Z}$, $J(\mathbb{Z}) = 0$, but not all $\mathbb{Z}$-module are semisimple.

Proof. Suppose $J(R) = 0$. Let $M \subseteq {}_RR$ be minimal such that intersection of a finite set of maximal left ideals, we claim M is in every maximal left ideal, if not we can intersect to get a smaller M. So $M = (0)$ since $J(R) = (0)$. Hence

$$(0) = \bigcap_{i=1}^{n} m_i$$

We have an injection

$${}_RR \hookrightarrow \bigoplus_{i=1}^{n} {}_RR/m_i = \bigoplus_{i=1}^{n} S_i$$

so ${}_RR$ is semisimple. Note that we need the Artinian condition to have finite direct sum, instead of infinite direct product.

Conversely, if ${}_RR$ is semisimple, then $J(R)$ considered as a submodule of ${}_RR$ is a direct summand

$${}_RR = J(R) \oplus {}_RR/J(R)$$

apply $J(R)$ to both sides $J(R) = J(R)J(R)$ Since $J(R)$ is a quotient of ${}_RR$, it is finitely generated so by Nakayama's lemma $J(R) = (0)$. □

6. Wedderburn Structure Theorem

In general, $J(R/J(R)) = 0$.

Theorem 6.1. *Let R be a finite dimensional algebra over a field k and suppose that $J(R) = 0$, then*

$$R = \prod_{i=1}^{m} \mathrm{Mat}_{d_i}(\Delta_i)$$

where Δ_i is a division ring containing k in its centre and finite dimensional over k.

Proof. Step 1: For any ring R, $R \cong \mathrm{End}_R({}_RR)^{\mathrm{op}}$ given by $r \mapsto (x \mapsto xr)$.

Step 2: ${}_RR = \bigoplus_{i=1}^{n} d_iS_i$ since $J(R) = 0$, so ${}_RR$ is semisimple.

Step 3: Schur's Lemma: $\mathrm{End}_R(S_i)$ is a division ring ${\Delta_i}^{\mathrm{op}}$.

Step 4: $\mathrm{End}_R\left(\bigoplus_{i=1}^{n} M\right) = \mathrm{Mat}_n(\mathrm{End}_R(M))$

$$\begin{aligned} \mathrm{End}_R({}_RR) &= \prod_{i=1}^{n} \mathrm{End}(d_iS_i) \\ &= \prod_{i=1}^{n} \mathrm{Mat}_{d_i}(\mathrm{End}_R(S_i)) \\ &= \prod_{i=1}^{n} \mathrm{Mat}_{d_i}({\Delta_i}^{\mathrm{op}}) \end{aligned}$$

So $R \cong \prod_{i=1}^{n} \mathrm{Mat}_{d_i}(\Delta_i)$. □

$\mathrm{End}(M_1 \oplus M_2)$ looks like

$$\begin{pmatrix} \mathrm{End}(M_1) & \mathrm{Hom}(M_1, M_2) \\ \mathrm{Hom}(M_2, M_1) & \mathrm{End}(M_2) \end{pmatrix}$$

Remark 6.2. (1) If k is algebraically closed, then each $\Delta_i = k$. For example, $\mathbb{C}G$ is semisimple, so $\mathbb{C}G = \prod \mathrm{Mat}_{n_i}(\mathbb{C})$

$$\mathbb{C}\mathfrak{S}_3 = \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_2(\mathbb{C})$$

(2) If $k = \mathbb{R}$, then $\Delta_i \cong \mathbb{R}, \mathbb{C}, \mathbb{H}$ (Frobenius-Schur Indicator).
(3) If k is a finite field, another theorem of Wedderburn shows that each Δ_i is a finite field.
(4) $|\Delta_i : Z(\Delta_i)|$ is a perfect square.
(5) Take $G = \mathbb{Z}/7 \rtimes \mathbb{Z}/9 = \langle g, h \,|\, g^7 = 1, h^9 = 1, hgh^{-1} = g^2 \rangle$ and let S be a simple $\mathbb{Q}G$-module on which G acts faithfully. Then $\mathrm{End}_{\mathbb{Q}G}(S)$ is 9-dimensional over its centre.

7. Brauer Characters I

Let M be a $\mathbb{C}G$-module. Then we have a class function

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

given by $g \mapsto \mathrm{Tr}(g, M)$.

Proposition 7.1 (Properties of ordinary characters)**.** *Let M, M' be $\mathbb{C}G$-modules.*

(1) $\chi_{M \oplus M'} = \chi_M + \chi_{M'}$
(2) $\chi_{M \otimes M'} = \chi_M \chi_{M'}$
(3) *If $\chi_M = \chi_{M'}$, then $M \cong M'$.*

Goal: Develop character theory for modular representations in such a way that (1) and (2) hold and

(3)' $\chi_M = \chi_{M'}$ if and only if M and M' have the same composition factors with the same multiplicities.

Problem: If M is a direct sum of p-copies of M', then $\forall g \in G$, $\mathrm{Tr}(g, M) = p\mathrm{Tr}(g, M') = 0$.

Theorem 7.2. *Let k be algebraically closed of characteristic p, then the following are equivalent:*

(i) *For any $g \in G$, $\mathrm{Tr}(g, M) = \mathrm{Tr}(g, M')$.*
(ii) *For each simple kG-module S the multiplicity of S as a composition factor of M and of M' are congruent modulo p.*

Proof. For $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$, we have

$$M_2 = \begin{pmatrix} M_1 & * \\ 0 & M_3 \end{pmatrix}$$

so $\mathrm{Tr}(g, M_2) = \mathrm{Tr}(g, M_1) + \mathrm{Tr}(g, M_3)$, and if M, M' have the same composition factors, then $\forall g \in G$,

$$\mathrm{Tr}(g, M) = \mathrm{Tr}(g, M')$$

Without lost of generality, suppose M, M' are semisimple. Since $\mathrm{Tr}(g, p \cdot S) = 0$, then (ii) implies (i).

Conversely, 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 $x \in kG$. Use Wedderburn structure theorem to find elements $x_i \in kG$ such that

$$\mathrm{Tr}(x_i, S_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

So $\mathrm{Tr}(x_i, M) =$ number of copies of S_i as a composition factor of M modulo p $\square$

8. p-elements and p'-elements

A *p-element* is one whose order is p^a for some a and a *p'-element* is one whose order is prime to p.

Lemma 8.1. *Given $g \in G$ we can write $g = xy = yx$ so that*

(i) *x an p-element.*
(ii) *y an p'-element.*
(iii) *every element of G that commutes with g commute with x, y.*

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

Proof. If g has order $n = p^a m$ with $p \nmid m$, choose integers s, t such that $sp^a + tm = 1$, then $g = g^{tm} g^{sp^a}$. $\square$

9. Jordan Canonical Forms

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

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

be a Jordan block of g. It is conjugate to

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

The matrix x_1 is a p-element because it is the sum of the identity matrix I and a nilpotent element u. That is, we have $u^{p^n} = 0$ for some n, and so $x_1^{p^n} = (I+u)^{p^n} = I + u^{p^n} = 0$ because char $k = p$. The matrix y_1 is a p'-element because λ must be a root of $X^{|G|_{p'}} - 1$. Also x_1 and y_1 commute with any matrix commuting with g_1 because x_1 is a scalar multiple of g_1 and y_1 is in the center of the matrix group. Thus x_1 is the p-part and y_1 is the p'-part of g_1. The upshot is that if $g = xy$ is the decomposition of g into its p-part x and p'-part y, then x has all diagonal entries in the Jordan canonical form equal to 1 and y_M is diagonalizable. Therefore we have

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

10. Brauer Characters II

Let G be a finite group and let k be a field of characteristic p. Assume that k has all $|G|_{p'}$-th roots of unity. These form a cyclic group of order $|G|_{p'}$-th under multiplication. All eigenvalues of elements of G belong to this cyclic group. Choose once and for all an isomorphism of cyclic groups

$$\psi\colon \{\, |G|_{p'}\text{-th roots of unity in } k^\times \,\} \to \{\, |G|_{p'}\text{-th roots of unity in } \mathbb{C}^\times \,\}.$$

If g is a p'-element of G and M is a finite dimensional kG-module, then

$$g_M \sim \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{pmatrix}, \qquad d = \dim_k M.$$

Define $\chi_M(g) = \sum_{i=1}^d \psi(\lambda_i)$. Note that $\chi_M(g)$ is a cyclotomic integer. It gives a map

$$\chi_M \colon \{\, \text{conjugacy classes of } p'\text{-elements of } G \,\} \to \mathbb{C}$$

Theorem 10.1 (Brauer)**.** *For finite dimensional kG-modules M and M', the followings are equivalent:*

(1) $\chi_M = \chi_{M'}$.
(2) *The multiplicities of each simple kG-module as composition factors of M and M' are equal.*

Proof. Without loss of generality, we may assume that M, M' are semisimple. (2) $\Rightarrow$ (1) is obvious, so we'll prove (1) $\Rightarrow$ (2). Look at a counterexample of smallest dimension. If M and M' have a composition factor in common, we can remove it and get a smaller example. So assume that they don't. If $\chi_M = \chi_{M'}$, by reducing back to k we have $\mathrm{Tr}(g, M) = \mathrm{Tr}(g, M')$ for all $g \in G$, so the multiplicities are congruent modulo p. So all multiplicities are divisible by p. So we have $M = p.M_1$, $M' = p.M'_1$, and $\chi_M = p\chi_{M_1}$, $\chi_{M'} = p\chi_{M'_1}$. Hence M_1, M'_1 give a smaller counterexample. $\square$

11. Choice of ψ and Brauer Character Table

Let G be a finite group with $|G| = p^a m$, $p \nmid m$ and let k be a field of characteristic p. Suppose that k has all m-th roots of unity. Let C, $\widehat{C}$ be the group of m-th roots of unity in k, $\mathbb{C}$, respective. Let $K = \mathbb{Q}[\widehat{C}]$. Then we have

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Aut}(\widehat{C}) \cong \mathbb{Z}/\varphi(m)$$

where φ denotes the Euler function.

Let $\mathcal{O}_K$ be the ring of integers in K. Then $\mathcal{O}_K = \mathbb{Z}[\widehat{C}]$. Note that $\mathcal{O}_K$ is a Dedekind domain; in particular, every prime ideal in $\mathcal{O}_K$ is maximal. Choose a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p, i.e. $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Then

Proposition 11.1. *$\mathcal{O}_K/\mathfrak{p}$ is the smallest finite field containing the m-th roots of unity: if p^r is the smallest power of p such that $m \mid p^r - 1$, then*

$$\begin{array}{ccll} \mathcal{O}_K/\mathfrak{p} & \cong & \mathbb{F}_{p^r} & \hookrightarrow k \\ \widehat{C} + \mathfrak{p} & \cong & C & \end{array}$$

and

$$\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p) \cong \textit{ Stabilizer of } \mathfrak{p} \textit{ in } \mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/r.$$

Note that since $(m,p)=1$, we have $m \mid p^{\varphi(m)}-1$, and so $r \mid \varphi(m)$.

Proof. Let ζ be a primitive m-th root of unity in $\mathbb{C}$. Then $\mathcal{O}_K/\mathfrak{p}$ is the extension field of $\mathbb{F}_p$ generated by the image $\zeta+\mathfrak{p}$. Since

$$\frac{X^m-1}{X-1} = X^{m-1}+X^{m-2}+\cdots+1 = \prod_{j=1}^{m-1}(X-\zeta^j),$$

setting $X=1$, we see that $1-\zeta^j \mid m$ in $\mathcal{O}_K$ for all $j=1,\ldots,m-1$. Now if $1-\zeta^j \in \mathfrak{p}$, then $m \in \mathfrak{p}\cap\mathbb{Z} = p\mathbb{Z}$, contradicting $(m,p)=1$. Thus $\zeta+\mathfrak{p}$ is a primitive m-th root of unity, so $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^r}$ and $\widehat{C}+\mathfrak{p} \cong C$. □

The *Brauer character table* of G (modulo p) is a table whose rows and columns are indexed by simple kG-modules S and conjugacy classes of p'-elements g of G, respectively, and whose entries are the values of the Brauer characters $\chi_S(g)$.

Note that once fixing an isomorphism $\psi\colon C \to \widehat{C}$, all other isomorphisms $C \to \widehat{C}$ are obtained by applying elements of $\mathrm{Gal}(K/\mathbb{Q})$ to $\widehat{C}$. Rows of the Brauer character table for G are the irreducible Brauer characters

$$\chi_S, \qquad S \text{ a simple } kG\text{-module;}$$

columns of the Brauer character table for G are the ring homomorphisms

$$\chi_-(g)\colon \mathcal{R}(G) \to \mathbb{C}, \qquad g \text{ a } p'\text{-element of } G.$$

Proposition 11.2. (1) *If we apply an element of* $\mathrm{Gal}(K/\mathbb{Q})$ *to a column of the Brauer character table, we get another column.*
(2) *If we apply an element of the stablizer of* $\mathfrak{p}$ *of* $\mathrm{Gal}(K/\mathbb{Q})$ *to a row of the Brauer character table, we get another row.*

Proof. (1) Let ζ be a primitive m-th root of unity in $\mathbb{C}$. Then $K=\mathbb{Q}(\zeta)$ and an element σ of $\mathrm{Gal}(K/\mathbb{Q})$ sends ζ to ζ^t for some t such that $(t,m)=1$. Then for each p'-element g of G, we have $\chi_-^\sigma(g) = \chi_-(g^t)$.

(2) σ stablizes $\mathfrak{p}$ precisely when t is a power of p. Let S be a simple kG-module with corresponding representation $\rho\colon G \to \mathrm{GL}_n(k)$. Then S^σ is a kG-module with corresponding representation

$$\begin{array}{cccccc} \rho^\sigma\colon & G & \xrightarrow{\rho} & \mathrm{GL}_n(k) & \to & \mathrm{GL}_n(k) \\ & g & \mapsto & (\lambda_{ij}(g)) & \mapsto & (\lambda_{ij}(g)^t) \end{array}$$

□

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

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

Example 11.3. Let $p=2$, $m=7$. 7-th roots of unity in k have two possible minimal polynomials X^3+X^2+1, X^3+X+1. Let ζ be a 7-th root of unity in $\mathbb{C}$. Then there are two prime ideals in $\mathbb{Z}[\zeta]$

$$\mathfrak{p}_1 = (2, \zeta^3+\zeta^2+1), \qquad \mathfrak{p}_2 = (2, \zeta^3+\zeta+1)$$

lying over 2 such that

$$\mathbb{Z}[\zeta]/\mathfrak{p}_1 \cong \mathbb{F}_8 \cong \mathbb{Z}[\zeta]/\mathfrak{p}_2.$$

12. Grothendieck Groups I

Given G and k as in the previous section, we form an abelian group $\mathcal{R}(G)$:

- generators: symbols of the form $[M]$ where M is an isomorphism class of finite dimensional kG-modules
- relations: if $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of kG-modules, then
$$[M_2] = [M_1] + [M_3]$$

Remark 12.1. We take equivalence relations over isomorphism classes of finite dimensional kG-modules rather than over all finite dimesional kG-modules because all finite dimensional kG-modules does not form a set.

$\mathcal{R}(G)$ is a free abelian group with basis $[S_i]$, S_i simple, by Jordan-Hölder theorem. We make $\mathcal{R}(G)$ into a commutative ring by introducing the mulitplication

$$[M][N] = [M \otimes_k N]$$

where the kG-module structure of $M \otimes_k N$ is given by diagonal action of G. Note that the multiplication is well defined because over a field k every module is flat; it is commutative because the tensor product over k is commutative. The multiplicative identity element of $\mathcal{R}(G)$ is $[k]$ where k is the trivial kG-module.

Proposition 12.2 (Properties of Brauer characters)**.** (1) *If* $0 \to M_1 \to M_2 \to M_3 \to 0$ *is a short exact sequence of finite dimensinoal kG-modules, then* $\chi_{M_2} = \chi_{M_1} + \chi_{M_3}$.
(2) $\chi_{M \otimes_k N} = \chi_M \chi_N$.

Consequence: for every conjugacy class of p'-element g of G, the map

$$\begin{array}{cccc} \chi_-(g)\colon & \mathcal{R}(G) & \to & \mathbb{C} \\ & [M] & \mapsto & \chi_M(g) \end{array}$$

is a (well-defined) ring homomorphism.

Theorem 12.3. *The product of these maps*

$$\begin{array}{ccc} \mathcal{R}(G) & \to & \prod_{\substack{\text{conj classes of} \\ p'\text{-elts } g \in G}} \mathbb{C} \\ [M] & \mapsto & (g \mapsto \chi_M(g)) \end{array}$$

is injective.

Proof. If $[M] - [N]$ and $[M'] - [N']$ go to the same place, then we have $\chi_M - \chi_N = \chi_{M'} - \chi_{N'}$, so $\chi_M + \chi_{N'} = \chi_{M'} + \chi_N$. Then $\chi_{M \oplus N'} = \chi_{M' \oplus N}$, so $[M \oplus N'] = [M' \oplus N]$. Thus $[M] + [N'] = [M'] + [N]$, and hence $[M] - [N] = [M'] - [N']$. $\square$

13. Grothendieck Groups II

In this section, we show

Theorem 13.1. *The map*

$$\mathbb{C} \otimes_{\mathbb{Z}} \mathcal{R}(G) \xrightarrow{\chi} \prod_{\substack{\text{conj classes of} \\ p'\text{-elements of } G}} \mathbb{C}$$

is an algebra isomorphism.

which yields immediately:

Corollary 13.2. *The number of simple kG-modules is equal to the number of conjugacy classes of p'-elements of G.*

The injectivity of the map follows from

Lemma 13.3. *The irreducible Brauer characters χ_{S_i} are linearly independent over $\mathbb{C}$.*

Proof. Let $K \subseteq \mathbb{C}$ be the field of $|G|_{p'}$-th roots of unity. Let $\mathcal{O}$ be the ring of integers in K. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}$ containing (p). $\mathcal{O}_\mathfrak{p} \subseteq K$ consists of the fractions $\frac{x}{y}$ with $x, y \in \mathcal{O}$, $y \notin \mathfrak{p}$. $\mathfrak{P}_\mathfrak{p}$, consisting of the fractions $\frac{x}{y}$ with $x, y \in \mathcal{O}$, $x \in \mathfrak{p}$, $y \notin \mathfrak{p}$, is the unique maximal ideal in $\mathcal{O}_\mathfrak{p}$ and

$$\mathcal{O}_\mathfrak{p}/\mathfrak{P}_\mathfrak{p} \cong \mathcal{O}/\mathfrak{p} \hookrightarrow k.$$

Moreover, $\mathcal{O}_\mathfrak{p}$ is a PID. Write $\mathfrak{P}_\mathfrak{p} = (\pi)$.

If there is a linear relation over $\mathbb{C}$ among the irreducible Brauer characters, then there's one over K, since all character values are in K. Clear denominators to get a linear relation with coefficients in $\mathcal{O}$. If all the coefficients of the linear relation lie in $\mathfrak{p}$, divide by a suitable power of π so that they don't. Now reduce mod $\mathfrak{P}_\mathfrak{p}$ to get a linear relation in k between the traces:

$$\sum_j \alpha_i \mathrm{Tr}(x, S_j) = 0 \qquad \forall\, x \in kG.$$

By Wedderburn structure theorem, for each i there exists $x_i \in kG$ such that $\mathrm{Tr}(x_i, S_j) = \delta_{ij}$. Therefore $\alpha_i = 0\ \forall\, i$. $\square$

To prove the surjectivity, for each p'-element g of G, we'll find elements of $\mathbb{C} \otimes_\mathbb{Z} \mathcal{R}(G)$ such that $\chi_-(g)$ sends it to 1 and $\chi_-(h)$ sends it to 0 for all $h \nsim_G g$.

First consider the case $G = \langle g \rangle$, $|g| = m$, $(m, p) = 1$. The irreducible representations of G over k are of the form

$$g \mapsto (\varepsilon), \qquad \varepsilon^m = 1 \text{ in } k.$$

So the irreducible Brauer characters are of the form

$$\chi_j(g) = e^{2\pi i j/m}$$

with corresponding simple kG-module S_j for $j = 1, \dots, m$. Then

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

has Brauer character

$$g^t \mapsto \frac{1}{m} \sum_{j=1}^{m} e^{2\pi i j(t-1)/m} = \begin{cases} 1, & \text{if } g^t = g \\ 0, & \text{if } g^t \neq g \end{cases}$$

In the general case, we'll take this Brauer character for some cyclic subgroup of G and induce it up.

Proposition 13.4 (Brauer characters of induced modules)**.** *If $H \leq G$ and M is a kH-module, then for $g \in G$,*

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

Proof. We have
$$M{\uparrow}^G = kG \otimes_{kH} M = \bigoplus_{g_i \in G/H} g_i \otimes M.$$
If $g \in G$, $m \in M$, then $g(g_i \otimes m) = g_j \otimes hm$ where $gg_i = g_j h$, $h \in H$. Thus the matrix representing the action of g on $M{\uparrow}^G$ decomposes into blocks corresponding to G-orbits of G/H, and the blocks corresponding to G-orbits of G/H of length > 1 are of the form
$$\begin{pmatrix} 0 & 0 & 0 & * \\ * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \end{pmatrix},$$
hence their eigenvalues are 0. On the other hand, if the singleton $\{g_i\}$ is a G-orbit of G/H, then the corresponding block represents the action of $g_i^{-1} g g_i \in H$ on M. Thus
$$\chi_{M\uparrow^G}(g) = \sum_{g_i^{-1} g g_i \in H} \chi_M(g_i^{-1} g g_i).$$
If $h \in H$, how many i satisfy $g_i^{-1} g g_i \sim_H h$? Count the pairs
$$\{ (i, h') \mid (g_i h')^{-1} g (g_i h') = h \}$$
to get $|C_G(h)| = \#\, i\text{'s} \cdot |C_H(h)|$. Thus we get the desired equality. $\square$

Now we finish off the proof of surjectivity. If $H \leq G$, define
$$\begin{array}{rccc} \mathrm{Ind}_{H,G}\colon & \mathcal{R}(H) & \to & \mathcal{R}(G) \\ & [M] & \mapsto & [kG \otimes_{kH} M] \end{array}$$
and extend linearly to get
$$\mathrm{Ind}_{H,G}\colon \mathbb{C} \otimes_{\mathbb{Z}} \mathcal{R}(H) \to \mathbb{C} \otimes_{\mathbb{Z}} \mathcal{R}(G).$$
Given any p'-element $g \in G$, let $H = \langle g \rangle$ and take $x \in \mathbb{C} \otimes_{\mathbb{Z}} \mathcal{R}(H)$ such that
$$\chi_x(g^i) = \begin{cases} 1, & \text{if } g^i = g; \\ 0, & \text{if } g^i \neq g. \end{cases}$$
Then for $g' \in G$,
$$\begin{aligned} \chi_{\mathrm{Ind}_{H,G}(x)}(g') &= \sum_{\substack{\text{ccls of } h \in H \\ \text{s.t. } h \sim_G g'}} |C_G(h) : C_H(h)| \chi_x(h) \\ &= \begin{cases} |C_G(g) : \langle g \rangle|, & \text{if } g' \sim_G g; \\ 0, & \text{if } g' \nsim_G g. \end{cases} \end{aligned}$$

We give another corollary of Theorem 13.1:

Corollary 13.5. *Every ring homomorphism $\mathcal{R}(G) \to \mathbb{C}$ is of the form $\chi_-(g)$ for some p'-element $g \in G$.*

For this we need the following lemma.

Lemma 13.6. *Let R be a commutative ring and let D be an integral domain. Then every set of distinct ring homomorphisms $R \to D$ is linearly independent over D.*

Proof. Suppose we have a linear relation of smallest size

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

In particular $\alpha_i \neq 0$ for all $i = 1, \dots, n$. Choose $x_0 \in R$ such that $\varphi_1(x_0) \neq \varphi_n(x_0)$. Then for all $x \in R$

$$\sum_{i=1}^{n} \alpha_i \varphi_i(x_0 x) = \sum_{i=1}^{n} \alpha_i \varphi_i(x_0)\varphi_i(x) = 0.$$

Also for all $x \in R$

$$\sum_{i=1}^{n} \alpha_i \varphi_n(x_0)\varphi_i(x) = 0.$$

Subtract:

$$\sum_{i=1}^{n-1} \alpha_i(\varphi_i(x_0) - \varphi_n(x_0))\varphi_i(x) = 0$$

for all $x \in R$. Since D is an integral domain, $\alpha_i(\varphi_i(x_0) - \varphi_n(x_0)) \neq 0$, a contradiction. □

Proof of Corollary 13.5. Let $\varphi \colon \mathcal{R}(G) \to \mathbb{C}$ be a ring homomorphism. Extend this linearly to get an algebra homomorphism $\varphi \colon \mathbb{C} \otimes_{\mathbb{Z}} \mathcal{R}(G) \to \mathbb{C}$. Do the same thing for $\chi_-(g)$'s. Theorem 13.1 and Lemma 13.6 show that the algebra homomorphisms $\chi_-(g_i)$ where the g_i are representatives of conjugacy classes of p'-elements of G form a $\mathbb{C}$-basis for the space of $\mathbb{C}$-linear maps from $\mathbb{C} \otimes_{\mathbb{Z}} \mathcal{R}(G)$ to $\mathbb{C}$. Now if $\varphi \neq \chi_-(g_i)$ for all i, then by Lemma 13.6 φ, $\chi_-(g_i)$ are linearly independent, contradicting Theorem 13.1. □

14. p-modular system

A *discrete valuation ring* (d.v.r.) is a principal ideal domain with a unique nonzero maximal ideal.

If $\mathcal{O}$ is a d.v.r. with the maximal ideal $\mathfrak{p} = (\pi)$, we can write any nonzero element x as $y\pi^a$ for some $a \in \mathbb{N}$, y a unit: if $x \in \mathfrak{p}$, we can do factorization $x = y_1\pi$. Since π is a prime and $\mathcal{O}$ a principal ideal domain, the factorization terminates. Define $v_p(x) = a$.

If $K = \mathrm{fof}(\mathcal{O})$ is the field of fraction of $\mathcal{O}$, then for any $x \in K$, $x = y\pi^a$ with $a \in \mathbb{Z}$.

A *p-modular system* $(K, \mathcal{O}, k)$ consists of a d.v.r. $\mathcal{O}$, $K = \mathrm{fof}(\mathcal{O})$ of characteristic 0 and $k = \mathcal{O}/\mathfrak{p}$ of characteristic p.

Remark 14.1. Every finitely generated torsion free $\mathcal{O}$-module is free.

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

(i) $KH = \prod \mathrm{Mat}_{d_i}(K)$
(ii) $kH/J(kH) = \prod \mathrm{Mat}_{c_i}(k)$

Example 14.2. Let K be an algebraic number field and $\mathcal{O}$ be the ring of integers in K, then $\mathrm{fof}(\mathcal{O}) = K$. Since $\mathcal{O}$ is integral over $\mathbb{Z}$, then there exists a prime ideal $\mathfrak{p}$ (and hence maximal) of $\mathcal{O}$ that lying above (p), i.e., $\mathfrak{p} \cap \mathbb{Z} = (p)$. The localization $\mathcal{O}_{\mathfrak{p}}$ at $\mathfrak{p}$ is a d.v.r. and hence $(K, \mathcal{O}_{\mathfrak{p}}, \mathcal{O}/\mathfrak{p})$ is a p-modular system.

Remark 14.3. If K contains $|G|$-th roots of unity, then $(K, \mathcal{O}_{\mathfrak{p}}, \mathcal{O}/\mathfrak{p})$ is a splitting p-modular system for G.

Remark 14.4. Later, we will want that $\mathcal{O}$ is complete, i.e.,

$$\mathcal{O} \longrightarrow \varprojlim_{n} \mathcal{O}/\mathfrak{p}^n$$

is an isomorphism.

15. Decomposition Numbers

Let $(K, \mathcal{O}, k)$ be a p-modular system.

Consider an irreducible representation V of G over K. Choose a K-basis $v_1, \ldots, v_d$ for V. Look at the $\mathcal{O}$-span W of

$$\{gv_i \mid 1 \le i \le d, g \in G\}$$

This is a finitely generated torsion free $\mathcal{O}$-module and hence $\mathcal{O}$-free on which G acts: the $\mathcal{O}$-span of W is a subset of V and $\mathrm{fof}(\mathcal{O}) = K$.

If $w_1, \ldots, w_n$ is an $\mathcal{O}$-basis. Clearly, $w_1, \ldots, w_n$ span V: $v_1, \ldots, v_d \in W$. If there is a linear relation between $w_1, \ldots, w_n$ over K, then clearing denominators, there is one over $\mathcal{O}$. So, there is no relation between $w_1, \ldots, w_n$ over K. So, $w_1, \ldots, w_n$ is a K-basis for V and $n = d$.

Changing basis from the v_i's to w_i's, all the entries in the matrix representations of G are in $\mathcal{O}$, not just in K and we have

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

The set W is an $\mathcal{O}$-form for the KG-module V.

Theorem 15.1. *Assume $(K, \mathcal{O}, k)$ is a splitting p-modular system. If W, W' are $\mathcal{O}$-forms of V, then the kG-modules $k \otimes_{\mathcal{O}} W = W/\mathfrak{p}W$ and $k \otimes_{\mathcal{O}} W'$ have the same Brauer character, hence the same composition factors.*

Proof. The Brauer character of $k \otimes_{\mathcal{O}} W$ is just the values on the p'-elements of the ordinary character of V. □

The *decomposition matrix* D has row indexed by the irreducible KG-modules, columns indexed by the irreducible kG-modules. The entry d_{ij} tells you the following: choose an $\mathcal{O}$-form W_i for V_i and

$$d_{ij} = \text{multiplicity of } S_j \text{ as composition factors of } k \otimes_{\mathcal{O}} W_i$$

Example 15.2. The ordinary character table for A_5,

$$X = \begin{array}{|ccccc|} 1 & 2 & 3 & 5 & 5 \\ \hline 1 & 1 & 1 & 1 & 1 \\ 3 & -1 & 0 & \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 3 & -1 & 0 & \frac{1-\sqrt{5}}{2} & \frac{1+\sqrt{5}}{2} \\ 4 & 0 & 1 & -1 & -1 \\ 5 & 1 & -1 & 0 & 0 \end{array}$$

and the modular character table for A_5 when the characteristic of k is 2, we have

$$B = \begin{array}{|cccc|} 1 & 3 & 5 & 5 \\ \hline 1 & 1 & 1 & 1 \\ 2 & -1 & \frac{-1+\sqrt{5}}{2} & \frac{-1-\sqrt{5}}{2} \\ 2 & -1 & \frac{-1-\sqrt{5}}{2} & \frac{-1+\sqrt{5}}{2} \\ 4 & 1 & -1 & -1 \end{array}$$

The decomposition matrix D is

$$D = \begin{array}{|c|cccc|} & 1 & 2 & 2 & 4 \\ \hline 1 & 1 & 0 & 0 & 0 \\ 3 & 1 & 1 & 0 & 0 \\ 3 & 1 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 1 \\ 5 & 1 & 1 & 1 & 0 \end{array}$$

If X_2 is the 5×4-matrix where the second column of X deleted, then we see that

$$DB = X_2$$

The i-th row of D is interpreted as the composition factors of the irreducible kG-module $M/\mathfrak{p}M$ where M is the KG-module corresponding the i-th row of X.

16. Projective and Injective Modules

In this section, M is not necessary a finitely generated R-module assuming R is a ring with 1.

An R-module P is *projective* if for every surjective homomorphism $M' \to M$ of R-modules and homomorphism $P \to M$, there exists a homomorphism $P \to M'$ making the triangle commutes

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

Theorem 16.1. *The following are equivalent:*

(i) *P is projective.*

(ii) *Every surjective homomorphism $M \xrightarrow{\alpha} P \longrightarrow 0$ splits, i.e., there exists a homomorphism $\varepsilon : P \to M$ such that $\alpha \circ \varepsilon = \mathrm{id}_P$.*

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

An R-module I is *injective* if

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

Lemma 16.2. *Let k be a field and G a finite group, then every kG-module embeds into a free kG-module.*

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

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

In this case, the action of G on $kG \otimes_k M$ is $g'(g \otimes m) = g'g \otimes m$.

There is a vector space splitting $\psi : kG \otimes_k M \to M$ of ϕ where

$$\psi(g \otimes m) := \begin{cases} m & ; g = 1 \\ 0 & ; g \neq 1 \end{cases}$$

so ϕ is injective.

Let $h \in G$ and $m \in M$, then

$$\begin{aligned} \phi(hm) &= \sum_{g \in G} g \otimes g^{-1}(hm) \\ &= \sum_{g' \in G} hg' \otimes (g')^{-1}m \\ &= h\left(\sum_{g' \in G} g' \otimes (g')^{-1}m\right) \\ &= h\phi(m) \end{aligned}$$

where we have used $g' = h^{-1}g$ (and hence $(g')^{-1} = g^{-1}h$, $g = hg'$). So ϕ is a kG-homomorphism.

Since k is a field, then $M \downarrow_{\{1\}}$ is a free k-module and we can write $M = \bigoplus k$. So

$$\begin{aligned} kG \otimes_k M &= M \downarrow_{\{1\}}\uparrow^G \\ &= \bigoplus k_{\{1\}} \uparrow^G \\ &= \bigoplus kG \end{aligned}$$

thus M is a free kG-module. □

Theorem 16.3. *Let k be any field, G be a finite group M be a kG-module, then the following are equivalent:*

(i) *M is projective.*
(ii) *M is injective.*
(iii) *(D. Higman's criterion) there exists a k-linear map $\alpha : M \to M$ such that*

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

Proof. (ii)⇒ (i): If M is injective, look at

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

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

(iii)⇒(ii): The proof can be dualised to get (iii)⇒(i)). Consider the diagram

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

Choose a k-linear map γ (not necessary a G-map) such that $\gamma\beta = \alpha$ and set

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

This is a kG-module homomorphism:

$$\begin{aligned} \gamma'\beta &= \sum_{g\in G} g(\theta\gamma)g^{-1}\beta \\ &= \sum_{g\in G} g(\theta\gamma\beta)g^{-1} && \beta \text{ is a } kG\text{-module homomorphism} \\ &= \sum_{g\in G} g(\theta\alpha)g^{-1} \\ &= \left(\sum_{g\in G} g\theta g^{-1}\right)\alpha \\ &= \mathrm{id}_M\alpha = \alpha \end{aligned}$$

(i)⇒(iii): If $M = kG$, take

$$\theta\left(\sum_{g\in G} \alpha_g g\right) := \alpha_1 1_G$$

So

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

So $\sum_{h\in G} h\theta h^{-1} = \mathrm{id}_{kG}$. If $M = \bigoplus kG$, use this θ on each factor. If M is a summand of a free module F, then define $\theta_M = \pi\theta_F\iota$ where

$$\begin{tikzcd} M \arrow[loop left, "\theta_M"] \arrow[r, shift left, "\iota"] & F \arrow[l, shift left, "\pi"] \arrow[loop right, "\theta_F"] \end{tikzcd}$$

We check that θ_M satisfies the desired property:

$$\begin{aligned}\sum_{g\in G} g(\theta_M)g^{-1} &= \sum_{g\in G} g(\pi\theta_F\iota)g^{-1}\\ &= \sum_{g\in G}\pi(g\theta_F g^{-1})\iota\\ &= \pi\left(\sum_{g\in G} g\theta_F g^{-1}\right)\iota\\ &= \pi \mathrm{id}_F\iota = \mathrm{id}_M \quad \square\end{aligned}$$

17. Projective Indecomposable Modules and Idempotents

Theorem 17.1 (Krull-Schmidt Theorem)**.** *Let R be a finite dimensional k-algebra, M be a finitely generated R-module and*

$$M = M_1 \oplus \ldots \oplus M_s = M_1' \oplus \ldots \oplus M_t'$$

be two indecomposable decompositions of M, i..e, M_i's and $M'i$'s are all indecomposable R-modules, then $s = t$ and after reordering if necessary, $M_i \cong M_i'$ for all $1 \le i \le s$.

Remark 17.2. The theorem is also true for finitely generated $\mathcal{O}G$-modules.

Warning. It is not true for finitely generated $\mathbb{Z}G$-modules.

Corollary 17.3. *If M is indecomposable and M is a summand of $M_1 \oplus \ldots \oplus M_s$, then M is isomorphic to a summand of some M_i.*

Corollary 17.4. *Every finitely generated projective indecomposable R-module is isomorphic to a summand of ${}_RR$.*

Write ${}_RR = P_1 \oplus \ldots \oplus P_s$ where P_i's are projective indecomposable. Since $R \cong \mathrm{End}({}_RR)^{\mathrm{op}}$, the endomorphism $\pi_i : {}_RR \twoheadrightarrow P_i \hookrightarrow {}_RR$ projecting onto P_i is a right multiplication by some $e_i \in R$ and hence $P_i = Re_i$, then $1_R = e_1 + \ldots + e_s$. These are *idempotents* ${e_i}^2 = e_i$. Two idempotents e_i, e_j are *orthogonal* if $e_ie_j = 0 = e_je_i$, $i \ne j$. An idempotent e is *primitive* if $e \ne 0$ and we cannot write $e = e' + e''$ with e' orthogonal to e'' and both nonzero.

There is one-to-one correspondence between direct sum decomposition ${}_RR = P_1 \oplus \ldots \oplus P_s$ with P_i's indecomposable and the expression $1 = e_1 + \ldots + e_s$ with e_i's primitive orthogonal idempotents.

Recall Wedderburn theorem:

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

If $T_i = \mathrm{Mat}_{d_i}(\Delta_i)$, then

$${}_{T_i}T_i = \bigoplus \text{columns}$$

and these are simple and isomorphic to each other. Let e_{ij} be the $(d_i \times d_i)$-matrix with (j, j)-entry 1 and zero elsewhere. For the matrix ring T_i, we have

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

and hence

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

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

Lemma 17.5. *If e, e' are idempotents in R, then the following are equivalent:*

(i) *e is conjugate to e' by an element of $R^\times$.*
(ii) *$Re \cong Re'$ and $R(1-e) \cong R(1-e')$.*

Proof. If $e \sim e'$, say $e\mu = \mu e'$ with μ invertible, then $Re\mu = R\mu e' = Re'$ gives $Re \cong Re'$. Similarly, $(1-e)\mu = \mu(1-e')$, so $R(1-e) \cong R(1-e')$.

Conversely, suppose $Re \xrightarrow{\theta\cong} Re'$ and $R(1-e) \xrightarrow{\gamma\cong} R(1-e')$ be the isomorphism. Note that for any R-module M we have

$$\mathrm{Hom}_R(Re, M) \cong^{\phi} eM$$

where $\phi : \beta = \beta(e)$ as $\beta(e) = e\beta(e)$. Let $\mu_1 \in eRe' \cong \mathrm{Hom}_R(Re, Re')$ corresponding to the isomorphism θ; similarly, $\mu_2 \in e'Re$, $\mu_3 \in (1-e)R(1-e')$ and $\mu_4 \in (1-e')R(1-e)$ correspond to the isomorphisms θ^{-1}, γ and γ^{-1} respectively. It is clear that we have

$$\mu_1\mu_2 = e,\ \mu_2\mu_1 = e' \text{ and } \mu_3\mu_4 = 1-e,\ \mu_4\mu_3 = 1-e'$$

Also,

$$(\mu_1 + \mu_3)(\mu_2 + \mu_4) = e + 0 + 0 + (1-e) = 1$$

and similarly, $(\mu_2 + \mu_4)(\mu_1 + \mu_3) = 1$, i.e., $\mu_1 + \mu_3 \in R^\times$ with the two sided inverse $\mu_2 + \mu_4$. Finally,

$$(\mu_2 + \mu_4)e(\mu_1 + \mu_3) = \mu_2 e \mu_1 = \mu_2\mu_1 = e' \quad \square$$

Remark 17.6. For the matrix ring, e_{ir} is conjugate to e_{is} for any $1 \le r, s \le d_i$.

Lemma 17.7. *If R is a finite dimensional algebra, then $J(R)$ is a nilpotent ideal.*

Proof. Look at the descending chain of ideal $J(R), J^2(R), J^3(R), \ldots$, so there exists $n > 0$ such that $J^n(R) = J^{n+1}(R) = J(R)J^n(R)$. By Nakayama's lemma, $J^n(R) = 0$. $\square$

Theorem 17.8 (Idempotent Refinement)**.** *Let R be a ring and N a nilpotent ideal of R, we have*

(i) *if e is an idempotent in R/N, then there exists an idempotent $f \in R$ such that $f + N = e$.*
(ii) *if $e \sim e'$ in R/N, then $f \sim f'$ in R.*

Proof. (i): Without lost of generality, suppose $N^2 = 0$: there is a lift at each stage for the ring R/N^{2^m} and the nilpotent ideal $N^{2^{m-1}}/N^{2^m}$; furthermore, $R/N^{2^n} = R$ for some n. Choose a preimage x of e in R, i.e., $x + N = e$. Set $f = 3x^2 - 2x^3$, then $(3x^2 - 2^3) + N = (3x - 2x) + N = x + N = e$, i.e., f is another lift of e. Also, since $f - 1 = (x-1)^2(-2x-1)$ and $x(x-1) + N = N$, then

$$\begin{aligned} f^2 - f &= f(f-1) \\ &= x^2(3-2x)(x-1)^2(-2x-1) \\ &= (x(x-1))^2(3-2x)(-2x-1) = 0 \end{aligned}$$

as $N^2 = 0$.

Comment on the choice of f: we want

$$f \equiv x \mod (x^2 - x) \text{ and } f \equiv 0 \mod (x-1)^2$$

then use Chinese Remainder theorem.

Comment: if R has characteristic p with p a prime, i.e., $p \cdot 1_R = 0$, then $f = x^p$ will do:

$$f^2 - f = x^{2p} - x^p = (x^2 - x)^p \in N^p$$

(ii): Suppose we are given invertible $\mu \in R/N$ such that $e\mu = \mu e'$. Let β be a lift of μ to R and set

$$\hat{\mu} = f\beta f' + (1-f)\beta(1-f')$$

Claim: $\hat{\mu}$ is invertible and $f\hat{\mu} = \hat{\mu}f'$. We compute $f\hat{\mu} = f\beta f'$ and $\hat{\mu}f' = f\beta f'$ and hence they are equal. Let λ be any lift of μ^{-1} to R, i.e., $1 - \hat{\mu}\lambda \in N$. So, $(1-\hat{\mu}\lambda)^n = 0$ for some n and hence

$$(1 - (1-\hat{\mu}\lambda))(1 + (1-\hat{\mu}\lambda) + (1-\hat{\mu}\lambda)^2 + \dots) = 1$$

So

$$\hat{\mu}\,\underbrace{\lambda(1 + (1-\hat{\mu}\lambda) + (1-\hat{\mu}\lambda)^2 + \dots)}_{\text{right inverse for } \hat{\mu}} = 1$$

Similarly, it is a left inverse of $\hat{\mu}$. □

Remark 17.9. An idempotent in R which lifts any primitive idempotent in R/N is again primitive.

Theorem 17.10 (Idempotent Refinement (full version))**.** *Let N be a nilpotent ideal of R and $1 = e_1 + \ldots + e_s$ be a decomposition of 1 into orthogonal idempotents in R/N, then there is a decomposition $1 = f_1 + \ldots + f_s$ of 1 in orthogonal idempotents in R such that $f_i + N = e_i$ for all $1 \le i \le s$.*

Proof. We inductively define idempotents f_i' in R lifting $e_i + \ldots + e_s$ and then will set $f_i = f_i' - f_{i+1}'$. Let $f_1' = 1_R$ and suppose f_i' is an idempotent in R lifting $e_i + \ldots + e_s$. □

Now we restrict our attention to a finite dimensional algebra R over some field k. Recall that, for a finitely generated R-module M,

$$\begin{aligned} \mathrm{Rad}M &= \text{the intersection of all maximal submodules of } M \\ &= \text{the smallest submodule of } M \text{ with semisimple quotient} \\ &= J(R)M \end{aligned}$$

and

$$\begin{aligned} \mathrm{Soc}M &= \text{the sum of all simple submodules of } M \\ &= \text{the largest semisimple submodule of } M \\ &= \{\, m \in M \mid J(R)m = 0 \,\} \end{aligned}$$

By Wedderburn structure theorem, we have

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

so we have a primitive orthogonal idempotent decomposition

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

where $\bar{e}_{ij}$ is the matrix in $\mathrm{Mat}_{d_i}(\Delta_i)$ whose only nonzero entry is the (j, j)-entry 1. Moreover, idempotents in each brace form a conjugacy class of idempotents. Lifting to R, we get a primitive orthogonal idempotent decomposition

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

where idempotents in each brace form a conjugacy class of idempotents. Thus we get a decomposition into projective indecomposable R-modules

$${}_RR = \underbrace{Re_{11} \oplus \cdots \oplus Re_{1d_1}} \oplus \cdots \oplus \underbrace{Re_{s1} \oplus \cdots \oplus Re_{sd_s}}$$

where projective indecomposables in each brace form an isomorphism class of modules. Moreover, for each i, j,

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

where S_i is a simple R-module. Write $P_{S_i} = P_i$ for a module isomorphic to Re_{ij} for some j.

Consequence: There are s isomorphism classes of projective indecomposable R-modules P_i $(i = 1, \cdots, s)$ and each P_i has a unique maximal submodule $J(R)P_i$.

We say that P_i is the *projective cover* of S_i. In general, if M is any finitely generated R-module, we have $M/\mathrm{Rad}(M) = M/J(R)M \cong \bigoplus_i S_i$. Then by the projectivity of $\bigoplus_i P_i$ we get the following commutative diagram of R-modules

$$\begin{tikzcd} & \bigoplus_i P_i \arrow[dl, dashed] \arrow[d] & \\ M \arrow[r] & M/\mathrm{Rad}(M) \arrow[r] & 0 \end{tikzcd}$$

The map $\bigoplus_i P_i \to M$ is surjective because it is surjective modulo $\mathrm{Rad}(M)$: denoting the image of $\bigoplus_i P_i$ in M by N, we have $N + J(R)M = M$, which implies $N = M$ by Nakayama's lemma. It induces an isomorphism

$$\bigoplus_i P_i/\mathrm{Rad}(\bigoplus_i P_i) \cong M/\mathrm{Rad}(M).$$

We say that $\bigoplus_i P_i$ is the *projective cover* of M. The kernel of the map $\bigoplus_i P_i \to M$ is written $\Omega(M)$:

$$0 \to \Omega(M) \to \bigoplus_i P_i \to M \to 0.$$

On the other hand, injective modules are vector space duals of projective modules.

Duality: If M is a left R-module, then

$$M^* = \mathrm{Hom}_k(M, k)$$

is a right R-module via $(fr)(m) = f(rm)$ for $f \in M^*$, $r \in R$, $m \in M$. Similarly, if M is a right R-module, then M^* is a left R-module. Since $\mathrm{Hom}_k(-, k)$ is an exact functor from the category of finitely generated left(right) R-modules to the category of finitely generated right(left) R-modules, we have

$$M \text{ f.g. proj. left(right) } R\text{-module} \Leftrightarrow M \text{ f.g. inj. right(left) } R\text{-module}$$

Note that, if $R = kG$ for some finite group G, a left R-module M can be made into a right R-module via

$$mg = g^{-1}m, \qquad g \in G, m \in M.$$

Consequence: If I is an injective indecomposable R-module, then I has a unique minimal(i.e. simple) submodule.

Write $I_{S_i} = I_i$ for the injective indecomposable R-module that has S_i as a unique simple submodule; that is, $\mathrm{Soc}(I_i) \cong S_i$. I_i is called the *injective hull* of S_i. In general, if M is any finitely generated R-module, we have $\mathrm{Soc}(M) \cong \bigoplus_i S_i$. Then by the injectivity of $\bigoplus_i I_i$ we get the following commutative diagram of R-modules

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Soc}(M) \arrow[r] \arrow[d] & M \arrow[dl, dashed] \\ & \bigoplus_i I_i & \end{tikzcd}$$

The map $M \to \bigoplus_i I_i$ is injective because it is injective on $\mathrm{Soc}(M)$: if its kernel K is nontrivial, then the intersection $K \cap \mathrm{Soc}(M)$ is nontrivial, contradicting the injectivity of $\mathrm{Soc}(M) \to \bigoplus_i I_i$. It induces an isomorphism

$$\mathrm{Soc}(M) \cong \mathrm{Soc}(\bigoplus_i I_i).$$

We say that I_i is the *injective hull* of M. The cokernel of the map $M \to \bigoplus_i I_i$ is written $\Omega^{-1}(M)$:

$$0 \to M \to \bigoplus_i I_i \to \Omega^{-1}(M) \to 0.$$

Remark 17.11. Ω and Ω^{-1} are not inverse to each other on the category of finitely generated R-modules.

Theorem 17.12. *Let G be a finite group and let k be a field. If P is a projective indecomposable kG-module, then $P/\mathrm{Rad}(P) \cong \mathrm{Soc}(P)$.*

Proof. We have $P = kGe$ for some primitive idempotent e of kG. Let $0 \neq x \in \mathrm{Soc}(P)$, $x = \sum_{g\in G} \alpha_g g$. There exists $h \in G$ such that $\alpha_h \neq 0$. Set $y = h^{-1}x = \sum_{g\in G} \beta_g g$. Then $\beta_1 \neq 0$. Since $y = ye$ has nonzero coefficient for 1_G, so ey has nonzero coefficient for 1_G. In particular, $ey \neq 0$, so $e\mathrm{Soc}(P) \neq 0$. Thus

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

Recall that P is also an injective indecomposable kG-module, so $\mathrm{Soc}(P)$ is a simple kG-module. It follows that $P/\mathrm{Rad}(P) \cong \mathrm{Soc}(P)$. $\square$

Remark 17.13. This is a special property of symmetric algebras.

Lemma 17.14. *Let R be a finite dimensional algebra over a field k. Assume that k be a splitting field for R. Then, for a finitely generated R-module M, we have*

$$\dim_k \mathrm{Hom}_R(P_S, M) = \textit{multiplicity of } S \textit{ as a comp. factor of } M$$

Proof. Induction on composition length of M. If M is simple, this is true because k is a splitting field. If M is not simple, choose a maximal submodule M' of M:

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

Since P_S is projective, $\mathrm{Hom}_R(P_S, -)$ is an exact functor, inducing

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

Dimensions add and number of compostion factors add, so we're done. $\square$

18. The Cartan Matrix

Let G be a finite group and let k be a field of characteristic p. We use the notation in the previous section: simple kG-modules are denoted by S_i and their projective covers by P_{S_i}. Define

$$c_{ij} = \text{multiplicity of } S_i \text{ in } P_{S_j}.$$

The matrix (c_{ij}) is called the *Cartan matrix*. We will show:

Theorem 18.1. (1) *If k is a splitting field for G, then $c_{ij} = c_{ji}$.*
(2) *If $(K, \mathcal{O}, k)$ is a splitting p-modular system for G, then $c_{ij} = \sum_l d_{li} d_{lj}$.*
(3) *$\det(c_{ij})$ is a power of p; in particular it is nonzero.*

We will prove (2) in this section; (1) follows immediately from (2). (3) will be proven later using the *psi operator*.

Lifting to char 0: Let $\mathcal{O}$ be a complete DVR with unique maximal ideal $\mathfrak{p}$ such that $\mathcal{O}/\mathfrak{p} \cong k$. Then we have

$$\mathcal{O}G = \varprojlim_n \mathcal{O}G/\mathfrak{p}^n\mathcal{O}G. \tag{$*$}$$

Since the canonical surjection

$$\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G \twoheadrightarrow \mathcal{O}G/\mathfrak{p}\mathcal{O}G = kG$$

has kernel $\mathfrak{p}\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G$ which squares to zero, a primitive orthogonal decomposition

$$1 = \bar{e}_1 + \cdots + \bar{e}_s$$

in kG lifts to a primitive orthogonal decomposition

$$1 = e_{21} + \cdots + e_{2s}$$

in $\mathcal{O}G/\mathfrak{p}^2\mathcal{O}G$. Similarly, through the canonical surjection

$$\mathcal{O}G/\mathfrak{p}^3\mathcal{O}G \twoheadrightarrow \mathcal{O}G/\mathfrak{p}^2\mathcal{O}G$$

we get a lift

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

in $\mathcal{O}G/\mathfrak{p}^3\mathcal{O}G$ of $1 = e_{21} + \cdots + e_{2s}$. Continuing this way, we get a primitive orthogonal decomposition

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

in $\mathcal{O}G/\mathfrak{p}^n\mathcal{O}G$ such that $e_{nj} + \mathfrak{p}^{n-1} = e_{n-1,j}$ for every n and j. By $(*)$, we get elements $e_j \in \mathcal{O}G$ such that $e_j + \mathfrak{p}^n = e_{nj}$ for every n. e_j^2 defines the same inverse system of elements as e_j does, so $e_j^2 = e_j$. By similar argument one can show that

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

is a primitive orthogonal decomposition of in $\mathcal{O}G$. In summary, we have the following theorem:

Theorem 18.2. *If $1 = \bar{e}_1 + \cdots + \bar{e}_s$ is a decomposition of 1 into primitive orthogonal idempotents in kG, then we can lift to*

$$1 = e_1 + \cdots + e_s \quad \text{in } \mathcal{O}G.$$

Moreover, given another lift $1 = e'_1 + \cdots + e'_s$ in $\mathcal{O}G$, we have $e'_i \sim e_i$ $\forall i$.

It follows that 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 the decomposition of $\mathcal{O}G$ into projective indecomposables

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

Now let us prove part (2) of Theorem 18.1. Let $(K, \mathcal{O}, k)$ be a splitting p-modular system for G and denote the simple KG-modules by V_i and their $\mathcal{O}$-forms by W_i. What is the multiplicity of V_i as a composition factor of $K \otimes_{\mathcal{O}} \hat{P}_{S_j}$? We have

$$\begin{aligned}
&\text{multiplicity of } V_i \text{ as a comp. factor of } K \otimes_{\mathcal{O}} \hat{P}_{S_j} \\
&= \dim_K \operatorname{Hom}_{KG}(K \otimes_{\mathcal{O}} \hat{P}_{S_j}, V_i) \\
&= \dim_K \operatorname{Hom}_{KG}(K \otimes_{\mathcal{O}} \hat{P}_{S_j}, K \otimes_{\mathcal{O}} W_i) \\
&= \dim_K K \otimes_{\mathcal{O}} \operatorname{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i) \qquad (1) \\
&= \operatorname{rank}_{\mathcal{O}} \operatorname{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i) \\
&= \dim_k \operatorname{Hom}_{kG}(P_{S_j}, k \otimes_{\mathcal{O}} W_i) \qquad (2) \\
&= \text{multiplicity of } S_j \text{ as a comp. factor of } k \otimes_{\mathcal{O}} W_i \\
&= d_{ij}.
\end{aligned}$$

(1): Since $\mathcal{O}$ is a PID, $\hat{P}_{S_j}$, W_i, and $\operatorname{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i)$ are all $\mathcal{O}$-free. Moreover, given any KG-homomorphism $K \otimes_{\mathcal{O}} \hat{P}_{S_j} \to K \otimes_{\mathcal{O}} W_i$, some nonzero multiple sends $\hat{P}_{S_j}$ into W_i by finite generation. Thus the map

$$\begin{array}{ccc}
K \otimes_{\mathcal{O}} \operatorname{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i) & \to & \operatorname{Hom}_{KG}(K \otimes_{\mathcal{O}} \hat{P}_{S_j}, K \otimes_{\mathcal{O}} W_i) \\
\lambda \otimes \varphi & \to & \lambda\varphi
\end{array}$$

is an isomorphism.
(2): Taking $k \otimes_{\mathcal{O}} -$ induces the map

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

which is surjective because $\hat{P}_{S_j}$ is projective, and has kernel $\mathfrak{p}\operatorname{Hom}_{\mathcal{O}G}(\hat{P}_{S_j}, W_i)$.
Hence

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

Example 18.3. $G = A_5$, $p = 2$: $K \otimes_{\mathcal{O}} \hat{P}_k = 1 \oplus 3 \oplus 3' \oplus 5$.

19. Blocks

Let G be a finite group and R any commutative ring. Then the center $Z(RG)$ of RG is the free R-module with basis the conjugacy class sums in G: if $\sum \alpha_g g \in Z(RG)$, then whenever $g \sim g'$, $\alpha_g = \alpha_{g'}$. Consequently, the ring homomorphism

$$Z(\mathcal{O}G) \to Z(kG)$$

induced by the canonical surjection $\mathcal{O} \to k$ is surjective.

If R is a ring, a *central idempotent* in R is an idempotent in $Z(R)$. A *centrally primitive idempotent* is an idempotent in $Z(R)$ that is primitive in $Z(R)$. A *block* of R is an indecomposable two sided ideal direct factor of R.

By Krull-Schmidt Theorem, if R is a finite dimensional algebra, we can write R as a product of blocks

$$R = B_1 \times \ldots \times B_s$$

Such a decomposition corresponds to an expression

$$1 = e_1 + \ldots + e_s$$

where the e_i's are orthogonal, centrally primitive idempotents in R: note that $B_i = e_i R$. Those e_i's lie inside the center $Z(R)$: for any $x \in R$, as $e_i x e_j \in B_i, B_j$, then

$$\begin{aligned} e_i x &= e_i(xe_1 + \ldots + xe_s) \\ &= e_i x e_i \\ &= (e_1 x + \ldots + x_s x)e_i \\ &= xe_i \end{aligned}$$

If also $1 = e'_1 + \ldots + e'_t$ where e'_i's orthogonal, centrally primitive idempotents, then

$$e_i = e_i \cdot 1 = e_i e'_1 + \ldots + e_i e'_t$$

where each $e_i e'_j$ is orthogonal, centrally idempotent 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 exists a unique j such that $e_i = e_i e'_j = e'_j$ where the second equality follows from the same reason. So $s = t$ and after reordering, we have $e_i = e'_i$.

If M is any R-module, then $M = e_1 M \oplus \ldots \oplus e_s M$ as submodules of M. If M is indecomposable, then there exists a unique i such that $M = e_i M$ and $e_j M = 0$ if $j \neq i$. We say M "lies in the block B_i". In particular, each simple module lies in some block.

In case $R = kG$, we can refine $1 = e_1 + \ldots + e_s$ in $Z(kG)$ to $1 = \widehat{e_1} + \ldots + \widehat{e_s}$ in $Z(\mathcal{O}G)$. So indecomposable $\mathcal{O}G$-modules also lie in blocks.

If V is an irreducible KG-module, choose an $\mathcal{O}$-form M of V, then there exists a unique i such that $\widehat{e_i} M \neq 0$. Since $\mathcal{O}G \subseteq KG$ we can think of $\widehat{e_i}$ as lying in KG, then $\widehat{e_i} V \neq 0$ and $\widehat{e_j} V = 0$ for $j \neq i$.

Remark 19.1. We can think of a block as a big bucket into which we put:

(i) indecomposable kG-modules
(ii) indecomposable $\mathcal{O}G$-modules
(iii) simple KG-modules

Let V_i be a simple KG-module and S_j a simple kG-module, if V_i lies in a different block to S_j, then $d_{ij} = 0$ where d_{ij} is the corresponding entry in the decomposition matrix.

If e is the block idempotent for V_i, then

$$\widehat{e_i}V_i = V_i, \qquad \widehat{e_i}M_i = M_i, \qquad e(k \otimes_{\mathcal{O}} M_i) = k \otimes_{\mathcal{O}} M_i$$

where M_i is an $\mathcal{O}$-form of V_i.

Lemma 19.2. *If R is a commutative finite dimensional algebra, then R is a product of local rings.*

Proof. By Wedderburn structure theorem, $R/J(R)$ is a product of $\mathrm{Mat}_{d_i}(\Delta_i)$. Since R is commutative, then each $\mathrm{Mat}_{d_i}(\Delta_i)$ is a field, i.e., $R/J(R) = k_1 \times \ldots \times k_s$. We have $1 = \overline{e_1} + \ldots + \overline{e_s}$. As $J(R)$ is a nilpotent ideal, use idempotent refinement in R, then $1 = e_1 + \ldots + e_s$ in R. So $R = R_1 \times \ldots \times R_s$ where $R_i = e_iR$. Also,

$$R_i/J(R_i) = e_iR/e_iJ(R) \cong e_i\left(R/J(R)\right) = k_i$$

so R_i is local ($J(R_i)$ is the maximal ideal of R_i). □

If R is a commutative finite dimensional k-algebra such that k is a splitting field, i.e., $R/J(R) = \prod \mathrm{Mat}_{d_i}(k)$, then

$$R/J(R) = \prod k$$

So we have k-algebra homomorphisms $\lambda_i : R \to k$.

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

Example 19.3. Let R be a finite dimensional k-algebra and S be a simple R-module such that $\mathrm{End}_R(S) = k$ (for instance, k is a splitting field for R), then each element $z \in Z(R)$ acts on S by some scalar $\lambda_S(z)$ and this gives a central character of R.

Theorem 19.4. *If k is a splitting field for R, then k is a splitting field for $Z(R)$.*

Proof. Without lost of generality, we assume R is indecomposable: if R decomposes into indecomposable $R_1 \times \ldots \times R_s$, then k is a splitting field for each R_i, then since we have k is a splitting for $Z(R_i)$, then k is also a splitting field for

$$Z(R) = Z(R_1) \times \ldots \times Z(R_s)$$

Let S be a simple R-module. Since k is a splitting field for R, we have $\mathrm{End}_R(S) = k$. So by the above example we obtain a central character $Z(R) \to k$. □

Example 19.5. Let K be a splitting field for KG, we construct a central character of KG with respect to a simple KG-module. Let $\widehat{\mathcal{C}_i} = \sum_{g \in \mathcal{C}_i} g$, we can calculate $\mathrm{Tr}(\widehat{\mathcal{C}_i}, V)$ in two ways:

- if $\widehat{\mathcal{C}_i}$ acts via multiplication by $\lambda \in K$, then $\mathrm{Tr}(\widehat{\mathcal{C}_i}, V) = \lambda \dim_k V$.
- since $\chi_V(g) = \chi_V(h)$ if $g \sim h$, then $\mathrm{Tr}(\widehat{\mathcal{C}_i}, V) = |\mathcal{C}_i|\chi_V(g) = |G : C_G(g)|\chi_V(g)$ for some $g \in \mathcal{C}_i$.

So $\lambda = |G : C_G(g)|\chi_V(g)/\dim_k V$ and we have the central character $\lambda_V : Z(KG) \to K$ defined by

$$\lambda_V : \widehat{\mathcal{C}_i} \longmapsto \frac{|G : C_G(g)|\chi_V(g)}{\dim_k V}$$

Theorem 19.6. *The numbers $\lambda_V\left(\widehat{\mathcal{C}}\right)$ are algebraic integers.*

Proof. Note that $Z(\mathbb{Z}G)$ has a $\mathbb{Z}$-basis consisting of the class sums $\widehat{\mathcal{C}_i}$. Suppose

$$\widehat{\mathcal{C}_i}\widehat{\mathcal{C}_j} = \sum_k a_{ijk}\widehat{\mathcal{C}_k}$$

with $a_{ijk} \in \mathbb{Z}$. As λ_V is a ring homomorphism, then

$$\lambda_V\left(\widehat{\mathcal{C}_i}\right)\lambda_V\left(\widehat{\mathcal{C}_j}\right) = \sum_k a_{ijk}\lambda_V\left(\widehat{\mathcal{C}_k}\right)$$

So the image of $\lambda_V : Z(\mathbb{Z}G) \to K$ is a subring of K which is finitely generated abelian group.

Since $\alpha = \lambda_V\left(\widehat{\mathcal{C}}\right)$ is in the image of this map, look at the chain of subgroups

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

which eventually terminates and so $\alpha \in \langle 1, \alpha, \dots, \alpha^{n-1}\rangle$ for some $n \in \mathbb{N}$. Thus $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$ with $a_i \in \mathbb{Z}$. □

Recall: Let $(K, \mathcal{O}, k)$ be a p-modular system, then all the algebraic integers in K lie in $\mathcal{O}$. So indeed, we get a ring homomorphism

$$\lambda_V : Z(\mathcal{O}G) \to \mathcal{O}$$

Reducing mod $\mathfrak{p}$, we get $\overline{\lambda_V} : Z(kG) \to k$: if $a_i \in \mathfrak{p}$, then $\sum a_i\lambda_V\left(\widehat{\mathcal{C}_i}\right) \in \mathfrak{p}$ and so $\overline{\lambda_V}$ is well-defined.

If V is in block B with block idempotent $e \in Z(kG)$, $\widehat{e} \in Z(\mathcal{O}G)$, $\widehat{e}$ acts as identity on V, i..e, $\lambda_V(\widehat{e}) = 1$, then $\overline{\lambda_V}(e) = 1$. If M is an $\mathcal{O}$-form of V, then every simple composition factor of $k \otimes_{\mathcal{O}} M$ say S satisfying $\lambda_S = \overline{\lambda_V}$.

Theorem 19.7. *Let V, V' be irreducible KG-modules, then V and V' are in the same block if and only if $\lambda_V \equiv \lambda_{V'} \mod \mathfrak{p}$, i.e., $\overline{\lambda_V} = \overline{\lambda_{V'}}$, i.e., for each $g \in G$, we have*

$$\frac{|G : C_G(g)|\chi_V(g)}{\dim_K V} \equiv \frac{|G : C_G(g)|\chi_{V'}(g)}{\dim_K V'}$$

Example 19.8. We give an example of the previous theorem which $G = A_5$. Note that there are 5 conjugacy classes in A_5, i.e., represented by $g_1 = 1, g_2 = (12)(34), g_3 = (123), g_4 = (12345)$ and $g_5 = (12354)$ respectively. It is not hard to compute the cardinality of each conjugacy class

	g_1	g_2	g_3	g_4	g_5
$\lvert A_5 : C_{A_5}(g_i)\rvert$	1	15	20	12	12

Let $V_1, \dots, V_5$ be representatives of the classes of non-isomorphic simple KG-modules as in Example 15.2, we construct the following table such that its (i, j)-entry is $\lambda_{V_i}\left(\widehat{C_G(g_j)}\right) = |G : C_G(g_j)|\chi_{V_i}(g_j)/\dim_K V_i$

	$\dim_K V_i$	g_1	g_2	g_3	g_4	g_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

For different primes p, V_i's are classified into blocks, for example:

(i) if $p = 2$, then $V_1, V_2, V_3, V_5 \mid V_4$.
(ii) if $p = 3$, then $V_1, V_4, V_5 \mid V_2 \mid V_3$.
(iii) if $p = 5$, then $V_1, V_2, V_3, V_4 \mid V_5$.

Remark 19.9. Note that the function $\overline{\lambda_V}$ is independent of the prime ideal $\mathfrak{p}$ chosen, see Theorem 15.18 [I].

Note that V, V' reduced modulo $\mathfrak{p}$ have a common composition factor if and only if V, V' are in the same block.

20. Defect Groups

If $\mathcal{C}$ is a conjugacy class in G, then 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 associate with $\mathcal{C}$. If P is a p-subgroup of G, we say $\mathcal{C}$ is *P-defective* if P centralises some element of $\mathcal{C}$.

Lemma 20.1. *Suppose $\widehat{\mathcal{C}_i}\widehat{\mathcal{C}_j} = \sum a_{ijk}\widehat{\mathcal{C}_k}$ in $Z(\mathbb{Z}G)$. Fix i, j, k, if $a_{ijk} \not\equiv 0 \mod p$ and $\mathcal{C}_k$ is P-defective, then so are $\mathcal{C}_i$ and $\mathcal{C}_j$.*

Proof. Choose $z \in \mathcal{C}_k$ commuting with P and look at the set

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

This set has a_{ijk} elements. Let P act by conjugation on this set, i.e., $g(x, y) = (gxg^{-1}, gyg^{-1})$ for all $g \in P$ and $(x, y) \in \Omega$. Since $p \nmid a_{ijk}$ and a_{ijk} is the sum of the cardinalities of the P-orbits of Ω, which are divisible by p if it is not 1, there exists a fixed point $(x, y) \in \mathcal{C}_i \times \mathcal{C}_j$, i.e., $gxg^{-1} = x$ and $gyg^{-1} = y$. So both $\mathcal{C}_i$ and $\mathcal{C}_j$ are P-defective. □

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

Lemma 20.2. *$Z(\mathcal{O}G)_P$ is an ideal of $Z(\mathcal{O}G)$.*

This is a consequence of the following proposition.

Proposition 20.3. *If P_1, P_2 are p-subgroups of a group 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 denote 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 conjugacy 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, $\widehat{\mathcal{C}_i}\widehat{\mathcal{C}_i}$ is contained in I. Write

$$\widehat{\mathcal{C}_i}\widehat{\mathcal{C}_j} = \sum_k a_{ijk}\widehat{\mathcal{C}_k}.$$

If $a_{ijk} \equiv 0 \mod p$, then $a_{ijk}\mathcal{C}_k \in \mathfrak{p}Z(\mathcal{O}G) \subseteq I$. If $a_{ijk} \not\equiv 0 \mod p$, let P be a defect group of $\mathcal{C}_k$. Clearly $\mathcal{C}_k \in Z(\mathcal{O}G)_P$; by Lemma 20.1, both $\mathcal{C}_i$ and $\mathcal{C}_j$ are P-defective, and hence $P \leq_G P_1$, $P \leq_G P_2$. So $\mathcal{C}_k \in I$. Therefore $\widehat{\mathcal{C}_i}\widehat{\mathcal{C}_i} \in I$, as desired. □

Proof of Lemma 20.2. If P is a Sylow p-subgroup of G, then $Z(\mathcal{O}G)_P = Z(\mathcal{O}G)$. Now apply Proposition 20.3 with P_1 or P_2 a Sylow p-subgroup of G. $\square$

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

Lemma 20.4. *The defect groups of a block are all conjugate*

To prove this lemma, we need:

Lemma 20.5 (Rosenberg's Lemma)**.** *Let R be a ring and e an idempotent of R such that eRe has a unique maximal 2-sided ideal. (e.g. $R = Z(\mathcal{O}G)$, e a block idempotent) If $e \in \sum_\alpha I_\alpha$ where the I_α are ideals of R, then there exists an α such that $e \in I_\alpha$.*

Proof. Since e is an idempotent, $e \in \sum_\alpha eI_\alpha e$. eRe has a unique maximal 2-sided ideal, so not all the $eI_\alpha e$ can be in it. So there exists an α such that $eI_\alpha e = eRe$. So $e \in I_\alpha$. $\square$

Proof of Lemma 20.4. If $e \in Z(\mathcal{O}G)_{P_1}$, $e \in Z(\mathcal{O}G)_{P_2}$, then by Proposition 20.3,

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

So by Rosenberg's lemma, there exists 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 $P_1 \sim_G P \sim_G P_2$. $\square$

21. The Transfer Map

Let G act by conjugation on $\mathcal{O}G$. The fixed points are $(\mathcal{O}G)^G = Z(\mathcal{O}G)$. If $H \leq G$, then $(\mathcal{O}G)^H$ has an $\mathcal{O}$-basis consisting of the H-conjugacy class sums in G. ($x \sim_H y$ iff $\exists\, h \in H$ s.t. $hxh^{-1} = y$) If $x \in ((\mathcal{O}G)^H$, we define

$$\mathrm{Tr}_{H,G}(x) = \sum_{g \in G/H} gxg^{-1}$$

where G/H denotes a set of representatives of left cosets of H in G; it is independent of the choice of left coset representatives because x is H-invariant. Let

$$(\mathcal{O}G)^G_H = \mathrm{Im}(\mathrm{Tr}_{H,G} \colon (\mathcal{O}G)^H \to (\mathcal{O}G)^G).$$

Lemma 21.1. *$(\mathcal{O}G)^G_H$ is an ideal in $Z(\mathcal{O}G)$.*

Proof. If $x \in (\mathcal{O}G)^H$, $y \in (\mathcal{O}G)^G$, then $\mathrm{Tr}_{H,G}(x)y = \mathrm{Tr}_{H,G}(xy)$. $\square$

Lemma 21.2. *If P is a Sylow p-subgroup of H, then $(\mathcal{O}G)^G_H = (\mathcal{O}G)^G_P$.*

Proof. If $x \in (\mathcal{O}G)^H$, then $x = \mathrm{Tr}_{P,H}\left(\frac{1}{|H:P|}x\right)$, so

$$\mathrm{Tr}_{H,G}(x) = \mathrm{Tr}_{H,G}\mathrm{Tr}_{P,H}\left(\frac{1}{|H:P|}x\right) = \mathrm{Tr}_{P,G}\left(\frac{1}{|H:P|}x\right).$$

$\square$

Theorem 21.3. *If P is a p-subgroup of G, then $Z(\mathcal{O}G)_P = (\mathcal{O}G)^G_P + \mathfrak{p}Z(\mathcal{O}G)$.*

Proof. Take a P-conjugacy class sum in G and transfer to G. If g is an element of the P-conjugacy class,

$$\mathrm{Tr}_{P,G}\left(\sum_{x\in P/C_P(g)} xgx^{-1}\right) = \sum_{x\in G/C_P(g)} xgx^{-1} = |C_G(g):C_P(g)|\widehat{\mathcal{C}}_g$$

where $\mathcal{C}_g$ denotes the G-conjugacy class containing g. Now $|C_G(g):C_P(g)|$ is not divisible by p iff $C_P(g)$ is a defect group of $\mathcal{C}_g$ iff P contains a defect group of $\mathcal{C}_g$. □

Theorem 21.4. *If e is a primitive idempotent in $Z(\mathcal{O}G)$ with defect group D, then*

$$e \in (\mathcal{O}G)^G_D$$

i.e. $\exists\ x \in (\mathcal{O}G)_D$ s.t. $\sum_{g\in G/D} gxg^{-1} = e$.

Proof. This follows from Theorem 21.3 and Rosenberg's lemma. □

Corollary 21.5. *If M is an indecomposable $\mathcal{O}G$-module in a block with defect group D, then $\exists\ \theta \in \mathrm{End}_{\mathcal{O}D}(M)$ s.t.*

$$\sum_{g\in G/D} g\theta g^{-1} = \mathrm{id}_M.$$

Proof. Let e be the block idempotent. By Theorem 21.4, we have

$$\sum_{g\in G/D} gxg^{-1} = e.$$

for some $x \in (\mathcal{O}G)^D$. Now e acts on M as the identity map and x acts on M as an $\mathcal{O}D$-module endomorphism θ. □

22. Relative Projectivity

Let R be any commutative ring. Let $H \le G$ and M an RG-module. We say that M is *relatively H-projective* if

$$\begin{tikzcd} & M \arrow[dl, dashed] \arrow[d] & \\ M_1 \arrow[r] & M_2 \arrow[r] & 0 \end{tikzcd}$$

whenever the dotted arrow exists as an RH-module homomorphism making the diagram commute, then it also exists as an RG-module homomorphism. Dually, M is *relatively H-injective* if

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r] \arrow[d] & M_2 \arrow[dl, dashed] \\ & M & \end{tikzcd}$$

whenever the dotted arrow exists as an RH-module homomorphism making the diagram commute, then it also exists as an RG-module homomorphism.

We have a relative version of Theorem 16.3:

Theorem 22.1. *Let $H \le G$ and M an RG-module. Then the followings are equivalent:*

(1) *M is relatively H-projective;*

(2) *M is relatively H-injective;*
(3) $\exists\ \theta \in \mathrm{End}_{RH}(M)$ *s.t.* $\sum_{g\in G/H} g\theta g^{-1} = \mathrm{id}_M$*;* *(D.Higman's criterion)*
(4) *M is isomorphic to a direct summand of $M'{\uparrow}^G$ for some RH-module M';*
(5) *M is isomorphic to a direct summand of $M{\downarrow}_H{\uparrow}^G$;*
(6) *The natural surjetive RG-module homomorphism*

$$\begin{array}{ccc} M{\downarrow}_H{\uparrow}^G & \twoheadrightarrow & M \\ g\otimes m & \mapsto & gm \end{array}$$

splits;
(7) *The natural injective RG-module homomorphism*

$$\begin{array}{ccc} M & \hookrightarrow & M{\downarrow}_H{\uparrow}^G \\ m & \mapsto & \sum_{g\in G/H} g\otimes g^{-1}m \end{array}$$

splits;

Proof. Clearly $(6),(7) \Rightarrow (5) \Rightarrow (4)$.

$(1) \Rightarrow (6)$: The map in (6) has a H-splitting map

$$\begin{array}{ccc} M & \hookrightarrow & M{\downarrow}_H{\uparrow}^G \\ m & \mapsto & 1\otimes m \end{array}$$

$(2) \Rightarrow (7)$: The map in (7) has a H-splitting map

$$\begin{array}{ccc} M{\downarrow}_H{\uparrow}^G & \twoheadrightarrow & M \\ g\otimes m & \mapsto & \begin{cases} gm, & \text{if } g\in H; \\ 0, & \text{otherwise.} \end{cases} \end{array}$$

$(3) \Rightarrow (1)$: Consider the diagram

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

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

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

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

$(3) \Rightarrow (2)$: Similar.

$(4) \Rightarrow (3)$: If $M = M'{\uparrow}^G$, define $\theta' \in \mathrm{End}_{RH}(M)$ by

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

If $M \mid M'{\uparrow}^G$,

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

does the work. $\square$

Consequence: 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 $e.M = M$, then M is a direct summand of a module induced from D.

23. Blocks of Defect Zero

If B is a block with defect group D and $|D| = p^a$, then we say that B is a block of *defect* a.

Suppose that B is a block of defect zero, i.e. $D = \{1\}$. Look at kG-modules in B; an induced kG-module from $\{1\}$ is a free module, so every kG-module in B is projective. An easy inductive argument shows that every finitely generated kG-module in B is semisimple. So $J(e.kG) = 0$. By Wedderburn structure theorem

$$e.kG \cong \prod_i \mathrm{Mat}_{n_i}(\Delta_i).$$

Since $e.kG$ is indecomposable as an algebra,

$$e.kG \cong \mathrm{Mat}_n(\Delta).$$

Consequently, there's only one isomorphism class of simple kG-module S and S is projective.

Since S is a projective kG-module, the idempotent refinement theorem shows: this 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 column of the decomposition matrix tells us the composition factor of $K \otimes_{\mathcal{O}} \widehat{S}$, it follows that the decomposition matrix is

$$(1).$$

The Cartan matrix is also

$$(1).$$

Theorem 23.1. *If B is a block of defect zero, then the simple modules in B has dimension divisible by the p-part $|G|_p$ of $|G|$.*

Proof. Let P be a Sylow p-subgroup of G and look at $S\downarrow_P$. This is a projective kP-module since S is a projective kG-module. We claim that the only projective indecomposable kP-module is kP itself. So, $S\downarrow_P$ is a direct sum of copies of kP and we get $|P|$ divides $\dim_k S$. □

Lemma 23.2. *kP has only one simple module, i.e., the trivial module k.*

Proof. Let S be a simple kP-module. We claim that P has a nonzero fixed point in S.

Choose $0 \neq x \in S$ and look at the abelian group additively generated by $\{gx \mid g \in P\}$. This is a finite p-group with a P-action. The identity element 0 is fixed, and the remaining orbits have length 1 or divisible by p. So there is a nonzero fixed point. The abelian group additively generated by the fixed points form a submodule of S which is nonzero and has trivial P-action, hence S is the submodule. □

Decomposition matrix D for kP has only one column with each entry $\dim V$ corresponding to the simple KP-module V: let W be an $\mathcal{O}$-form for V, the composition factors for $k \otimes_{\mathcal{O}} W$ is k of multiplicity $\dim V$.

$$D = \begin{pmatrix} \vdots \\ \dim V \\ \vdots \end{pmatrix}$$

So the Cartan matrix D^tD is the 1×1-matrix $(|P|)$ since

$$|P| = \sum (\dim V)^2$$

as V runs over representatives of non-isomorphic classes of simple KP-modules.

Alperin's Conjecture :

$$\# \text{ simple } kG\text{-modules} = \sum_{\substack{\text{conjugacy classes} \\ \text{of } p\text{-subgroups } D \leq G, \\ \text{including } D=1}} \# \text{ blocks of defect zero of } N_G(D)/D$$

24. Blocks with cyclic defect

Representation of $\mathbb{Z}/p^n$ in characteristic p: Look at the Jordon canonical form for a generator. For an indecomposable representation, there is a single Jordon block. Since

$$x^{p^n} - 1 = (x-1)^{p^n}$$

the eigenvalues have to be 1. The Jordon block has the form

$$J = \underbrace{\begin{pmatrix} 1 & 1 & & & \\ & 1 & \ddots & & \\ & & \ddots & & \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}}_{d}$$

The order of this matrix is the smallest $p^a \geq d$: the entries appear in J^n are $\binom{n}{i}$ for some $0 \leq i \leq n$ with n always appears above the diagonal. Hence the order of J is p^a for some a. If $p^a < d$, then some entry strictly above the diagonal is 1. So $p^a \geq d$. Clearly, for any $1 \leq d \leq p^n$, we have $J^{p^n} = 1$. We conclude:

Theorem 24.1. *There are p^n isomorphism classes of indecomposable $k(\mathbb{Z}/p^n)$-module, and they correspond to the Jordon blocks of length d with $1 \leq d \leq p^n$.*

Theorem 24.2. *If a block of kG has cyclic defect group, then there are only a finite number of indecomposable kG-modules in the block.*

Proof. Every indecomposable is a direct summand of (Jordon block for D) $\uparrow^G$ where D is the defect group of the given block. $\square$

Example 24.3. Let $G = \mathbb{Z}/p \times \mathbb{Z}/p = \langle g, h \rangle$ and k be an infinity field. For each $\alpha \in k$, we construct an indecomposable kG-module M_α with a representation

$$g \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \quad h \mapsto \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$$

If $\alpha \neq \beta$, a direct calculation shows that $M_\alpha \ncong M_\beta$. Hence we have infinite number of non-isomorphic indecomposable kG-modules.

25. The Brauer Homomorphism

Goal: Brauer First Main Theorem: There is a natural one-to-one correspondence between blocks of G with defect group D and blocks of $N_G(D)$ with defect group D.

Lemma 25.1. $(kG)^D = kC_G(D) \oplus \displaystyle\sum_{D'<D} (kG)^D_{D'}$ *as a sum of a subring and a 2-sided ideal.*

Proof. $(kG)^D$ has a k-basis consisting of D-conjugacy class sums $\widehat{\mathcal{C}_{g,D}} := \sum_{x \sim_D g} x$. If the orbit has one element, then $\widehat{\mathcal{C}_{g,D}} \in kC_G(D)$; otherwise, let $D' = C_D(g) < D$ with left coset representatives $d_1, \ldots, d_s$ of D/D'. So,

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

as $\mathcal{C}_{g,D}$ is precisely the set $\{d_1 g {d_1}^{-1}, \ldots, d_s g {d_s}^{-1}\}$. In characteristic p, $kC_G(D) \cap \sum_{D'<D} (kG)^D_{D'} = \{0\}$. $\square$

The *Brauer Homomorphism* is the ring homomorphism given by projection

$$\mathrm{Br}_D : (kG)^D \to kC_G(D)$$

Theorem 25.2. *Let G be a finite group with a normal p-subgroup D, then every block idempotent in $Z(kG)$ lies in $kC_G(D)$.*

Proof. If S is a simple kG-module, then S^D is a nontrivial submodule of S: $S\downarrow_D$ has a nontrivial submodule isomorphic to the trivial module k. So $S^D = S$, and hence D acts trivially on S. Since $kG/J(kG)$ is semisimple, then D acts trivially. In characteristic p, we have $(kG/J(kG))^D_{D'} = 0$ for any $D' < D$, i.e., $(kG)^D_{D'} \leq J(kG)$. Let e be a block idempotent in kG, namely $e = x + y$ with $x \in kC_G(D)$ and $y \in \sum_{D'<D} (kG)^D_{D'}$. As

$$x^2 + xy = xe = ex = x^{+}yx$$

then $xy = yx$. So

$$e = e^{p^n} = (x+y)^{p^n} = x^{p^n} + y^{p^n}$$

for all n. For large n, $y^{p^n} = 0$ (as $J(kG)$ is a nilpotent ideal). So $e = x^{p^n} \in kC_G(D)$. $\square$

Corollary 25.3. *If $C_G(D) \leq D \lhd G$, then G has only one block.*

Proof. $C_G(D)$ is a p-group, so $kC_G(D)$ has only one idempotent namely 1 since there is only one projective indecomposable for $kC_G(D)$. The result follows from the previous theorem. $\square$

Theorem 25.4. *The following diagram commutes:*

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

with all arrows are surjective.

Proof. Note that $(kG)_D^G \subseteq (kG)^D$, $kC_G(D) = (kC_G(D))^D$. For any $x \in (kG)^D$,

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

(for each double coset representative g of D, D in G, take a set of left coset representatives $\{\beta_{g,1}, \dots, \beta_{g,n(g)}\}$of $D \cap gDg^{-1}$ in D, then the set $\{\beta_{g,i}g\}$ forms a left coset representatives of D in G). If $D \cap gDg^{-1} < D$, then $\mathrm{Br}_D\mathrm{Tr}_{D\cap gDg^{-1},D}(gxg^{-1}) = 0$. So

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

Since $N_G(D)$ acts on both $kC_G(D)$ and $\sum_{D'<D}(kG)_{D'}^D$ respectively, then $\mathrm{Br}_D(gxg^{-1}) = g\mathrm{Br}_D(x)g^{-1}$ for all $g \in N_G(D)$. So we have

$$\mathrm{Br}_D\mathrm{Tr}_{D,G}(x) = \sum_{g \in N_G(D)/D} g\mathrm{Br}_D(x)g^{-1} = \mathrm{Tr}_{D,N_G(D)}\mathrm{Br}_D(x) \quad \square$$

Theorem 25.5. Br_D *induces a one-to-one correspondence between block idempotents in* $Z(kG)$ *with defect group* D *and primitive idempotents in* $(kC_G(D))_D^{N_G(D)}$.

Proof. The correspondence is given by

$$\left\{\begin{array}{l}\text{block idempotent in}\\ Z(kG) \text{ with defect group } D\end{array}\right\} \leftrightarrow \left\{\begin{array}{l}\text{primitive idempotents}\\ \text{in } kC_G(D)_D^{N_G(D)}\end{array}\right\}$$
$$(kG)_D^G \ni e \quad \mapsto \quad \mathrm{Br}_D(e)$$

Note that a central idempotent e lies in $(kG)_D^G$ if and only if its defect group $D(e) \leq_G D$: follows from the definition of defect group of e and the fact that $Z(kG)_{D(e)} \subseteq Z(kG)_D$ if $D(e) \leq_G D$.

$\underline{\mathrm{Br}_D(e) \neq 0}$: By definition $e \notin (kG)_{D'}^G$ for any $D' <_G D$, it is equivalent to $e \notin \sum_{D'<D}(kG)_{D'}^G$ by Rosenberg's lemma. As $\ker \mathrm{Br}_D \cap (kG)_D^G = \sum_{D'<D}(kG)_{D'}^G$, then $\mathrm{Br}_D(e) \neq 0$. This proves also $\mathrm{Br}_D(e) = 0$ if $D(e) <_G D$.

$\underline{\mathrm{Br}_D(e)\text{ is a primitive idempotent}}$: It is clearly an idempotent since $\mathrm{Br}_D(e) \neq 0$ and Br_D is a ring homomorphism. To show that $\mathrm{Br}_D(e)$ is primitive, we use the idempotent refinement theorem:

Let A, B be finite dimensional k-algebras, I, J be ideals of A, B respectively and $f : A \to B$ be an algebra homomorphism such that $f(I) = J$, we have if 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 contained in J.

The map is injective and it is also surjective by Theorem 25.4. $\square$

Corollary 25.6 (Brauer's first main theorem)**.** *If H is a subgroup of G containing $N_G(D)$, then there is a one-to-one correspondence between blocks of G with defect group D and blocks of H with defect group D.*

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

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

using previous theorem twice. □

26. Module Categories

Let G be a finite group and k a field.

$\mathrm{mod}(kG)$ is a category whose objects are finitely generated kG-modules and whose arrows are kG-module homomorphisms. $\mathrm{Mod}(kG)$ is a category whose objects are all kG-modules and whose arrows are kG-module homomorphisms.

We have a block decomposition

$$\begin{array}{ccccccc} kG & = & B_0 & \times & \cdots & \times & B_s \\ 1 & = & e_0 & + & \cdots & + & e_s \end{array}$$

If M is any kG-module, then

$$M = e_0 M \oplus \cdots \oplus e_s M$$
$$\mathrm{Hom}_{kG}(e_i M, e_j M) = 0 \quad \text{if } i \neq j$$

So

$$\begin{array}{ccccccc} \mathrm{Mod}(kG) & \cong & \mathrm{Mod}(B_0) & \times & \cdots & \times & \mathrm{Mod}(B_s) \\ \mathrm{mod}(kG) & \cong & \mathrm{mod}(B_0) & \times & \cdots & \times & \mathrm{mod}(B_s) \end{array}$$

Warning: In general, tensor products do not preserve blocks.

27. The Stable Module Category

The category $\mathrm{stmod}(kG)$ has the same objects as $\mathrm{mod}(kG)$, but arrows are:

$$\underline{\mathrm{Hom}}_{kG}(M,N) = \mathrm{Hom}_{kG}(M,N)/\mathrm{PHom}_{kG}(M,N)$$

where $\mathrm{PHom}_{kG}(M,N)$ consists of those homomorphisms which factor through some projective module.

Lemma 27.1. *If $P_N \twoheadrightarrow N$ and $M \hookrightarrow I_M$ with P_N, I_M projective(i.e. injective), then the followings are equivalent:*

(1) *$f\colon M \to N$ factors through some projective*
(2) *f factors through $P_N \twoheadrightarrow N$*
(3) *f factors through $M \hookrightarrow I_M$*

Proof. Dashed arrows exist in the following commutative diagram because P is projective(i.e. injective).

$$\begin{tikzcd}
 & & P_N \arrow[d] \\
M \arrow[r] \arrow[d, hook] & P \arrow[r] \arrow[ur, dashed] \arrow[dl, dashed] & N \\
I_M & &
\end{tikzcd}$$

□

As a consequence, we get

Proposition 27.2. *If M, N are finitely generated kG-modules and $f \colon M \to N$ factors through a projective kG-module, then it factors through a finitely generated projective kG-module. Hence the canonical functor*

$$\mathrm{stmod}(kG) \to \mathrm{StMod}(kG)$$

induces an isomorphism on each Hom *sets; in other words, it is a full embedding of categories.*

Warning: There are examples of module homomorphisms which factor through finitely generated modules and also through projective modules, but not through finitely generated projective modules.

Remark 27.3. Projective modules are isomorphic to the zero module in $\mathrm{StMod}(kG)$.

Lemma 27.4 (Schanuel's Lemma)**.** *If we have short exact sequences of kG-modules*

$$0 \to M_1 \to P_1 \to M \to 0$$
$$0 \to M_2 \to P_2 \to M \to 0$$

with P_1, P_2 projective, then $M_1 \oplus P_2 \cong M_2 \oplus P_1$

Consequence: $M_1 \cong M_2$ in $\mathrm{StMod}(kG)$.

Proof. The short exact sequences embed into the following commutative diagram

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & M_2 \arrow[r, equal] \arrow[d] & M_2 \arrow[d] & \\
0 \arrow[r] & M_1 \arrow[r] \arrow[d, equal] & X \arrow[r] \arrow[d] & P_2 \arrow[r] \arrow[d, "\beta"] & 0 \\
0 \arrow[r] & M_1 \arrow[r] & P_1 \arrow[r, "\alpha"] \arrow[d] & M \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 &
\end{tikzcd}$$

where $X = \{\, (a, b) \in P_1 \times P_2 \mid \alpha(a) = \beta(b) \,\}$. Now since P_1, P_2 are projective, the middle row and the middle column split, yielding $M_1 \oplus P_2 \cong X \cong M_2 \oplus P_1$. □

For a kG-module M, let

$$\Omega(M) = \mathrm{Ker}(P \twoheadrightarrow M)$$

for some projective kG-module P. By Schanuel's lemma, $\Omega(M)$ is well-defined up to isomorphism in $\mathrm{StMod}(kG)$. We may define $\Omega(M)$ canonically by choosing P as the free kG-module having M as a basis.

Dually, if

$$0 \to M \to I_1 \to M_1 \to 0$$
$$0 \to M \to I_2 \to M_2 \to 0$$

with I_1, I_2 injective, then $M_1 \oplus I_2 \cong M_2 \oplus I_1$. So if M is a kG-module,

$$\Omega^{-1}(M) = \mathrm{Coker}(M \hookrightarrow I)$$

where I is injective, is well-defined up to isomorphism in $\mathrm{StMod}(kG)$.

Theorem 27.5. *Ω and Ω^{-1} are inverse self-equivalences on the category* $\mathrm{StMod}(kG)$

Proof. In the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \Omega M \arrow[r, "\gamma"] \arrow[d, dashed, shift right] \arrow[d, dashed, shift left] & P_M \arrow[r, "\alpha"] \arrow[d, dashed, shift right, "f"'] \arrow[d, dashed, shift left, "g"] \arrow[dl, dashed, "u"'] & M \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Omega N \arrow[r, "\delta"] & P_N \arrow[r, "\beta"] & N \arrow[r] & 0
\end{tikzcd}$$

we have $\beta(f-g) = 0$, so there exists $u\colon P_M \to \Omega N$ such that $f - g = \delta u$; hence

$$(f-g)|_{\Omega M} = u\gamma.$$

This shows that Ω is a functor on $\mathrm{StMod}(kG)$. Dual argument shows that Ω^{-1} is also a functor and

$$\Omega^{-1}\Omega M \cong M, \qquad \Omega\Omega^{-1} M \cong M$$

in $\mathrm{StMod}(kG)$. $\square$

28. Tate Cohomology

Let M, N be kG-modules. For $i \in \mathbb{Z}$, define the *i-th Tate cohomology group* by

$$\widehat{\mathrm{Ext}}^i_{kG}(M,N) = \underline{\mathrm{Hom}}_{kG}(\Omega^i M, N)$$
$$\widehat{H}^i(G,M) = \widehat{\mathrm{Ext}}^i_{kG}(k,M)$$

Products are given by

$$\begin{array}{ccccc}
\widehat{\mathrm{Ext}}^i_{kG}(M,N) & \times & \widehat{\mathrm{Ext}}^j_{kG}(L,M) & \to & \widehat{\mathrm{Ext}}^{i+j}_{kG}(L,N) \\
(\Omega^i M \xrightarrow{\alpha} N & , & \Omega^{i+j} L \xrightarrow{\beta} \Omega^i M) & \mapsto & \Omega^{i+j} L \xrightarrow{\alpha\beta} N
\end{array}$$

Taking $L = M = N$, we get a graded ring $\widehat{\mathrm{Ext}}^*_{kG}(M,M)$. In particular, if $M = k$

$$\widehat{H}^*(G,k)$$

is called the *Tate cohomology ring*.

Fact: $\widehat{H}^*(G,k)$ is a graded commutative ring: if $x \in \widehat{H}^m(G,k)$, $y \in \widehat{H}^n(G,k)$,

$$yx = (-1)^{mn} xy.$$

Warning: Even if M is simple, there are examples where $\widehat{\mathrm{Ext}}^*_{kG}(M,M)$ surjects onto $\mathrm{Mat}_2(k)$.

For $i \geq 0$, the *i-th (ordinary) cohomology group* is defined by

$$\operatorname{Ext}^i_{kG}(M,N) = \begin{cases} \widehat{\operatorname{Ext}}^i_{kG}(M,N), & \text{if } i > 0 \\ \operatorname{Hom}_{kG}(M,N), & \text{if } i = 0. \end{cases}$$

29. Triangulated Categories

What kind of category $\operatorname{StMod}(kG)$ is? In this category, we can make any homomorphism represented by an injective homomorphism in $\operatorname{Mod}(kG)$:

$$\begin{tikzcd} M \arrow[r] \arrow[d, equal] & M' \arrow[d, "\cong"] \\ M \arrow[r, hook] & I_M \oplus M' \end{tikzcd}$$

or by a surjective homomorphism in $\operatorname{Mod}(kG)$:

$$\begin{tikzcd} M \arrow[r] \arrow[d, "\cong"] & M' \arrow[d, equal] \\ M \oplus P_{M'} \arrow[r, two heads] & M' \end{tikzcd}$$

So $\operatorname{StMod}(kG)$ is not an abelian category. Instead, it is a triangulated category.

A *triangle* in $\operatorname{StMod}(kG)$ is a sequence of objects and maps of the form

$$M \to M' \to M'' \to \Omega^{-1}M.$$

such that the composite of each pair of consecutive maps is zero. Two triangles

$$M \to M' \to M'' \to \Omega^{-1}M$$
$$N \to N' \to N'' \to \Omega^{-1}N$$

are said to be *isomorphic* if there is a commutative diagram

$$\begin{tikzcd} M \arrow[r] \arrow[d] & M' \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & \Omega^{-1}M \arrow[d] \\ N \arrow[r] & N' \arrow[r] & N'' \arrow[r] & \Omega^{-1}N \end{tikzcd}$$

where all the vertical maps are isomorphisms.

Given a morphism $f\colon M \to M'$, there exists a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\alpha"] \arrow[d, "f"'] & I_M \arrow[r] \arrow[d, "\beta"] & \Omega^{-1}M \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & M' \arrow[r, "\gamma"] & M'' \arrow[r] & \Omega^{-1}M \arrow[r] & 0 \end{tikzcd}$$

where $M'' = M' \oplus I_M / \{(f(m), \alpha(m)) \mid m \in M\}$. We have a triangle

$$M \to M' \to M'' \to \Omega^{-1}M.$$

Note that we also have a short exact sequence in $\operatorname{Mod}(kG)$

$$0 \to M \xrightarrow{\begin{pmatrix} \alpha \\ f \end{pmatrix}} I_M \oplus M' \xrightarrow{\begin{pmatrix} \beta, & -\gamma \end{pmatrix}} M'' \to 0.$$

A *distinguished triangle* is a triangle which is isomorphice to one coming from the above construction.

Proposition 29.1 (Properties of the distinguished triangles)**.** (1)

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} \Omega^{-1}A$$

is a distinguished triangle iff

$$B \xrightarrow{g} C \xrightarrow{h} \Omega^{-1}A \xrightarrow{-\Omega^{-1}f} \Omega^{-1}B$$

is a distinguished triangle.

(2) *Every morphism $M \to M'$ can be embedded in a distinguished triangle*

$$M \to M' \to M'' \to \Omega^{-1}M.$$

extends to a map of triangles

(3) *Every commutative diagram in* $\mathrm{StMod}(kG)$

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

extends to a map of triangles

$$\begin{tikzcd} M \arrow[r] \arrow[d, "f"'] & M' \arrow[r] \arrow[d, "g"] & M'' \arrow[r] \arrow[d, "h"] & \Omega^{-1}M \arrow[d, "\Omega^{-1}f"] \\ N \arrow[r] & N' \arrow[r] & N'' \arrow[r] & \Omega^{-1}N \end{tikzcd}$$

(4) *(Oxtahedral Axiom) Given composable maps $A \to B$, $B \to C$, there exists a distinguished triangle $X \to Y \to Z \to \Omega^{-1}X$ which embedds in the following commutative diagram of distinguished triangles*

$$\begin{tikzcd} A \arrow[r] \arrow[drr] & B \arrow[rr] \arrow[dr] & & X \arrow[dd, dashed] \\ & & C \arrow[dr] \arrow[ddr] & \\ & & & Y \arrow[d, dashed] \\ & & & Z \end{tikzcd}$$

(5) *For any M, $M \xrightarrow{\mathrm{id}} M \to 0 \to \Omega^{-1}M$ is a distinguished triangle.*

Remark 29.2. (1) In (3), M'' is determined uniquely but not up to unique isomorphism; in other words, the assignment $M \mapsto M''$ is not functorial.

(2) The oxtahedral axiom is an analogue of the third isomorphism theorem for modules: if $X \cong B/A$, $Y \cong C/A$, and $Z \cong Y/Z$, then $Z \cong C/B$.

A *triangulated category* is an additive category $\mathcal{C}$ with a self-equivalence $\tau \colon \mathcal{C} \to \mathcal{C}$ (e.g. $\tau = \Omega^{-1}$) together with a class of distinguished triangles

$$A \to B \to C \to \tau A$$

such that every triangle isomorphic to a distinguished triangle is distinguished and satisfying (1)–(5) above.

Lemma 29.3. *If M is an object of a triangulated category $(\mathcal{C}, \tau)$ and*

$$A \to B \to C \to \tau A$$

is a distinguished triangle, given a map $M \xrightarrow{f} B$ such that the composite $M \xrightarrow{f} B \to C$ is zero, there exists a map $M \to A$ such that $M \to A \to B$ is zero:

$$\begin{tikzcd} & M \arrow[dl, dashed] \arrow[d, "f"] \arrow[dr, dashed, "0"] & \\ A \arrow[r] & B \arrow[r] & C \end{tikzcd}$$

Proof. By the properties of the distinguished triangles, we have a map of distinguished triangles

$$\begin{tikzcd} M \arrow[r, "\mathrm{id}"] \arrow[d, dashed] & M \arrow[r] \arrow[d, "f"] & 0 \arrow[r] \arrow[d] & \tau M \arrow[d, dashed] \\ A \arrow[r] & B \arrow[r] & C \arrow[r] & \tau A \end{tikzcd}$$

□

Similarly, given a map $B \xrightarrow{g} M$ such that $A \to B \xrightarrow{g} M$ is zero, we can extend to $C \to M$:

$$\begin{tikzcd} A \arrow[r] \arrow[dr, dashed, "0"'] & B \arrow[r] \arrow[d, "g"] & C \arrow[dl, dashed] \\ & M & \end{tikzcd}$$

As a consequence we get:

Corollary 29.4. *Given a distinguished triangle $A \to B \to C \to \tau A$ and an object M, we get exact sequences of* Hom *sets*

$$\cdots \to \mathrm{Hom}_{\mathcal{C}}(M, A) \to \mathrm{Hom}_{\mathcal{C}}(M, B) \to \mathrm{Hom}_{\mathcal{C}}(M, C) \to \mathrm{Hom}_{\mathcal{C}}(M, \tau A) \to \cdots$$
$$\cdots \to \mathrm{Hom}_{\mathcal{C}}(\tau A, M) \to \mathrm{Hom}_{\mathcal{C}}(C, M) \to \mathrm{Hom}_{\mathcal{C}}(B, M) \to \mathrm{Hom}_{\mathcal{C}}(A, M) \to \cdots$$

In $\mathrm{StMod}(kG)$,

$$\widehat{\mathrm{Ext}}^i_{kG}(M, N) = \underline{\mathrm{Hom}}_{kG}(\Omega^i M, N) = \underline{\mathrm{Hom}}_{kG}(M, \Omega^{-i} N).$$

So given a distinguished triangle $A \to B \to C \to \Omega^{-1} A$ and an object M in $\mathrm{StMod}(kG)$, we get long exact sequences

$$\cdots \to \widehat{\mathrm{Ext}}^i_{kG}(M, A) \to \widehat{\mathrm{Ext}}^i_{kG}(M, B) \to \widehat{\mathrm{Ext}}^i_{kG}(M, C) \to \widehat{\mathrm{Ext}}^{i+1}_{kG}(M, A) \to \cdots$$
$$\cdots \to \widehat{\mathrm{Ext}}^i_{kG}(C, M) \to \widehat{\mathrm{Ext}}^i_{kG}(B, M) \to \widehat{\mathrm{Ext}}^i_{kG}(A, M) \to \widehat{\mathrm{Ext}}^{i+1}_{kG}(C, M) \to \cdots$$

In ordinary cohomology, given a short exact sequence $0 \to A \to B \to C \to 0$ and an object in $\mathrm{Mod}(kG)$, we get

$$0 \to \mathrm{Hom}_{kG}(M, A) \to \mathrm{Hom}_{kG}(M, B) \to\to \mathrm{Hom}_{kG}(M, C) \to \mathrm{Ext}^1_{kG}(M, A) \to \cdots$$
$$0 \to \mathrm{Hom}_{kG}(C, M) \to \mathrm{Hom}_{kG}(B, M) \to\to \mathrm{Hom}_{kG}(A, M) \to \mathrm{Ext}^1_{kG}(C, M) \to \cdots$$

Theorem 29.5. *Given any projective resolution of M*

$$\dots \to P_2 \to P_1 \to P_0 \to M \to 0$$

Take homomorphisms $\mathrm{Hom}(-, N)$*:*

$$0 \to \mathrm{Hom}_{kG}(P_0, N) \to \mathrm{Hom}_{kG}(P_1, N) \to \mathrm{Hom}_{kG}(P_2, N) \to \dots$$

This is a complex*, i.e., the composition of any adjacent pair of maps is zero. We have*

$$\mathrm{Ext}^n_{kG}(M, N) \cong \frac{\mathrm{Ker}\,(\mathrm{Hom}_{kG}(P_n, N) \to \mathrm{Hom}_{kG}(P_{n+1}, N))}{\mathrm{Im}\,(\mathrm{Hom}_{kG}(P_{n-1}, N) \to \mathrm{Hom}_{kG}(P_n, N))}$$

Proof. For $n > 0$, consider the diagram

$$\begin{tikzcd}
 & \Omega^{n+1}M \arrow[dr, tail] & & \Omega^n M \arrow[dr, tail] \arrow[ddl, dashed, "f_\alpha"] \arrow[ddr] & \\
P_{n+1} \arrow[ur, two heads] \arrow[rr, "\delta_n"] \arrow[drr, dashed, "0"] & & P_n \arrow[ur, two heads] \arrow[rr] \arrow[d, "\alpha"] & & P_{n-1} \arrow[d, dashed, "\xi"] \\
 & & N & & P \arrow[ll, "\beta"]
\end{tikzcd}$$

Define a map Φ_n as follows: for any $\alpha : P_n \to N$ such that $\alpha\delta_n = 0$, then $\Phi_n(\alpha) = f_\alpha + \mathrm{PHom}_{kG}(\Omega^n M, N)$ where $f_\alpha : \Omega^n M \to N$ is given by $x \mapsto \alpha w$ if $\delta_{n-1} w = x$. If f_α factors through a projective P, then it factors through P_{n-1} as P is also an injective kG-module. So, $\alpha = (\beta\xi)\delta_{n-1} \in \mathrm{Ker}\Phi_n$.
For $n = 0$, we have an exact sequence

$$0 \to \mathrm{Hom}_{kG}(M, N) \to \mathrm{Hom}_{kG}(P_0, N) \to \mathrm{Hom}_{kG}(P_1, N)$$

So $\mathrm{Ext}^0_{kG}(M, N) = \mathrm{Hom}_{kG}(M, N)$. □

Dually, we have

Theorem 29.6. *Given any injective resolution of N*

$$0 \to N \to I_0 \to I_1 \to I_2 \to \dots$$

Take homomorphisms $\mathrm{Hom}(M, -)$*:*

$$0 \to \mathrm{Hom}_{kG}(M, I_0) \to \mathrm{Hom}_{kG}(M, I_1) \to \mathrm{Hom}_{kG}(M, I_2) \to \dots$$

This gives a complex whose cohomology is

$$\mathrm{Ext}^n_{kG}(M, N)$$

We use $\mathrm{Ext}^n_{kG}(M, N) = \underline{\mathrm{Hom}}_{kG}(M, \Omega^{-n} N)$ for the proof of the above theorem instead.

30. Tensor Products

Lemma 30.1. *If P is kG-projective and M is any kG-module, then $P \otimes_k M$ is projective.*

Proof. Without lost of generality, we assume P is free of rank 1, i.e., $P \cong kG$. We claim that there is an isomorphism between the tensor product with diagonal action $kG \otimes_k M$ and the induced module $M\downarrow_k\uparrow^G = kG \otimes M$

$$\phi : kG \otimes_k M \to kG \otimes M$$

given by $x \otimes m \mapsto x \otimes x^{-1}m$ if $x \in G$ and $m \in M$. The action of G on the induced module is $g(x \otimes m) = gx \otimes m$. One can check that ϕ is a kG-homomorphism with the inverse map $\phi^{-1} : x \otimes m \mapsto x \otimes xm$. As a k-module M is a sum of copies of k, so $kG \otimes_k M$ is a sum of copies of kG. □

Lemma 30.2. *For any kG-module M, we have $\Omega(k) \otimes_k M \cong \Omega M$ in* $\mathrm{StMod}(kG)$.

Proof. Take the exact sequence $0 \longrightarrow \Omega(k) \longrightarrow P_k \longrightarrow k \longrightarrow 0$ and tensor with M:

$$0 \longrightarrow \Omega(k) \otimes_k M \longrightarrow P_k \otimes_k M \longrightarrow M \longrightarrow 0$$

It is an exact sequence (tensor product of vector spaces). Since

$$0 \longrightarrow \Omega(M) \longrightarrow P_M \longrightarrow M \longrightarrow 0$$

then by Schanuel's Lemma, we have

$$\Omega(M) \oplus (P_k \otimes_k M) \cong (\Omega(k) \otimes_k M) \oplus P_M \quad \square$$

Consequence: $\Omega^n k \otimes_k M \cong \Omega^n M$ in $\mathrm{StMod}(kG)$ (by induction). Taking $M = \Omega^m k$, then $\Omega^n k \otimes_k \Omega^m k \cong \Omega^{n+m} k$.

Lemma 30.3. *The diagram commutes in* $\mathrm{StMod}(kG)$*:*

$$\begin{tikzcd} \Omega(k) \otimes_k \Omega(k) \arrow[rr, "\tau"] \arrow[dr, "\cong"'] & & \Omega(k) \otimes_k \Omega(k) \arrow[dl, "\cong"] \\ & \Omega^2 k & \end{tikzcd}$$

where $\tau(x \otimes y) = -y \otimes x$ and the isomorphisms are given by the Schanuel's Lemma.

Proof. Consider the chain complex

$$\left(0 \to \Omega(k) \to P_k \xrightarrow{\pi} k \to 0\right) \otimes \left(0 \to \Omega(k) \to P_k \xrightarrow{\pi} k \to 0\right)$$

then we have two rows of exact sequences and ϕ_i's extending id : $x \otimes y \mapsto y \otimes x$ making the diagram commutes

$$\begin{tikzcd} 0 \arrow[r] & \Omega(k) \otimes_k \Omega(k) \arrow[r] \arrow[d, dashed, "\phi_3"] & P_k \otimes_k P_k \arrow[r, "\begin{pmatrix} 1 \otimes \pi \\ -\pi \otimes 1 \end{pmatrix}"] \arrow[d, dashed, "\phi_2"] & \begin{matrix} (P_k \otimes_k k) \\ \oplus (k \otimes_k P_k) \end{matrix} \arrow[r, "(\pi \otimes 1, 1 \otimes \pi)"] \arrow[d, dashed, "\phi_1"] & k \otimes_k k \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ 0 \arrow[r] & \Omega(k) \otimes_k \Omega(k) \arrow[r] & P_k \otimes_k P_k \arrow[r] & \begin{matrix} (P_k \otimes_k k) \\ \oplus (k \otimes_k P_k) \end{matrix} \arrow[r] & k \otimes_k k \arrow[r] & 0 \end{tikzcd}$$

where

$$\begin{aligned} \phi_1 &: (a \otimes 1, 1 \otimes b) \mapsto (b \otimes 1, 1 \otimes a) \\ \phi_2 &: a \otimes b \mapsto -b \otimes a \\ \phi_3 &: a \otimes b \mapsto -b \otimes a \end{aligned}$$

□

Lemma 30.4. *The diagram commutes in* $\mathrm{StMod}(kG)$*:*

$$\begin{tikzcd} \Omega^m \otimes_k \Omega^n k \arrow[rr, "\tau"] \arrow[dr, "\cong"'] & & \Omega^n k \otimes_k \Omega^m k \arrow[dl, "\cong"] \\ & \Omega^{m+n} k & \end{tikzcd}$$

where $\tau : x \otimes y \mapsto (-1)^{mn} y \otimes x$*.*

Proof. Think of $\Omega^m k \otimes_k \Omega^n k$ as

$$\underbrace{(\Omega(k) \otimes_k \ldots \otimes_k \Omega(k))}_{m \text{ copies}} \otimes_k \underbrace{(\Omega(k) \otimes_k \ldots \otimes_k \Omega(k))}_{n \text{ copies}}$$

The results now follows from previous lemma. □

Given a kG-module M, we have a map

$$- \otimes_k \mathrm{id}_M : \widehat{\mathrm{Ext}}^n_{kG}(k,k) \to \widehat{\mathrm{Ext}}^n_{kG}(M,M)$$

as $\underline{\mathrm{Hom}}_{kG}(\Omega^n k \otimes_k M, k \otimes_k M) \cong \underline{\mathrm{Hom}}_{kG}(\Omega^n M, M) = \widehat{\mathrm{Ext}}^n_{kG}(M,M)$. We denote the image of $\zeta \in \widehat{\mathrm{Ext}}^n_{kG}(k,k)$ under the map $- \otimes_k \mathrm{id}_M$ by $\overline{\zeta}$.

Theorem 30.5. *Given a map* $f : \Omega^m M \to N$ *in* $\mathrm{StMod}(kG)$ *we have*

$$\overline{\zeta} f = (-1)^{mn} f \overline{\zeta}$$

for all $\zeta \in \widehat{\mathrm{Ext}}^n_{kG}(k,k)$*, i.e., the following diagram commutes up to the sign* $(-1)^{mn}$

$$\begin{tikzcd} \Omega^{m+n} M \arrow[r, "\Omega^n f"] \arrow[d, "\overline{\zeta}"'] & \Omega^n N \arrow[d, "\overline{\zeta}"] \\ \Omega^m M \arrow[r, "f"] & N \end{tikzcd}$$

Proof. All maps of the following commuting diagram are in $\mathrm{StMod}(kG)$.

$$\begin{tikzcd}
\Omega^{m+n}M \arrow[rrrr, "\Omega^n f"] \arrow[ddddd, "(-1)^{mn}\overline{\zeta}"'] & & & & \Omega^n N \arrow[ddddd, "\overline{\zeta}"] \\
& & \Omega^n k \otimes_k \Omega^m k \otimes_k M \arrow[ull, "\cong"'] \arrow[r, "1\otimes f"] \arrow[dl, "(-1)^{mn}\tau\otimes 1"] \arrow[dd, "\zeta\otimes 1\otimes 1"] & \Omega^n k \otimes_k N \arrow[ur, "\cong"] \arrow[dd, "\zeta\otimes \mathrm{id}_N"] & \\
& \Omega^m k \otimes_k \Omega^n k \otimes_k M \arrow[uul, "\cong"] \arrow[dd, "(-1)^{mn}(1\otimes\zeta\otimes 1)"'] & & & \\
& & k \otimes_k \Omega^m k \otimes_k M \arrow[r, "1\otimes f"] \arrow[dl, "\eta\otimes 1"'] & k \otimes_k N \arrow[ddr, "\cong"] & \\
& \Omega^m k \otimes_k k \otimes_k M \arrow[urr, "f"'] \arrow[dl, "\cong"] & & & \\
\Omega^m M \arrow[rrrr, "f"'] & & & & N
\end{tikzcd}$$

where $\tau(x\otimes y) = y\otimes x$ and $\eta : a\otimes b \mapsto b\otimes a$. □

Consequence: We write $\widehat{H}^*_{kG}(G,k)$ for $\widehat{\mathrm{Ext}}^*_{kG}(k,k)$:

(i) Taking $M = N = k$, then $\widehat{H}^*(G,k)$ is graded commutative, i.e., $xy = (-1)^{|x||y|}yx$ for all $x, y \in \widehat{H}^*(G,k)$.
(ii) The image of the map $- \otimes_k \mathrm{id}_M : \widehat{\mathrm{Ext}}^*_{kG}(k,k) \to \widehat{\mathrm{Ext}}^*_{kG}(M,M)$ lies in the graded centre.

The Centre of a category $\mathcal{C}$:

The *centre* $Z(\mathcal{C})$ *of a category* $\mathcal{C}$ is the natural transformations from the identity functor to itself.

Example 30.6. Let $\mathcal{C} = \mathrm{Mod}(R)$, we claim $Z(\mathcal{C}) = Z(R)$.

Proof. A natural transformation ρ assigns to each object M an arrow $M \xrightarrow{\rho_M} M$ in such a way that if $f : M \to N$, then the diagram commutes

$$\begin{tikzcd} M \arrow[r, "\rho_M"] \arrow[d, "f"'] & M \arrow[d, "f"] \\ N \arrow[r, "\rho_N"] & N \end{tikzcd}$$

If $M = N = {}_RR$, then ρ_R is a right multiplication by an element $r \in R$ such that $r \in Z(R)$ (as $1 \in R$). If M is any module and $m \in M$, then $\rho_M = r\cdot$ by the commuting diagram

$$\begin{tikzcd} {}_RR \arrow[r, "\cdot r"] \arrow[d, "\phi_m"'] & {}_RR \arrow[d, "\phi_m"] \\ M \arrow[r, "\rho_M"] & M \end{tikzcd}$$

where $\phi_m : 1 \mapsto m$. □

Consequence: If $\mathrm{Mod}(R)$ is equivalent to $\mathrm{Mod}(R')$, then $Z(R) \cong Z(R')$.

If $\mathcal{T}$ is a triangulated category with a shift operator τ, define

$$Z^n(\mathcal{T}) = \{\text{natural transformations from } id_{\mathcal{T}} \text{ to } \tau^n\}$$

Example 30.7. Let $\mathcal{T} = \mathrm{StMod}(kG)$ and $\tau = \Omega^{-1}$, then $\rho \in Z^n(\mathrm{StMod}(kG))$ assigns to each M

$$\rho_M : M \to \Omega^{-n}M$$

or equivalently $\Omega^n M \to M$. So we have a ring homomorphism

$$\widehat{\mathrm{Ext}}^*_{kG}(k,k) \to Z^*(\mathrm{StMod}(kG))$$

Explicitly, $\zeta \in \widehat{\mathrm{Ext}}^n_{kG}(k,k)$ is mapped to the natural transformation assigning M the map $\zeta \otimes_k \mathrm{id}_M : \Omega^n M \to M$.

Open Question: What does $Z^*(\mathrm{StMod}(kG))$ look like?

Remark 30.8. There is an injection $H^*(G,k) \rightarrowtail \widehat{H}^*(G,k)$. So $H^*(G,k)$ acting on $H^*(G,M) := \mathrm{Ext}^*_{kG}(M,M)$ via the ring homomorphism

$$\widehat{H}^*(G,k) \xrightarrow{-\otimes_k \mathrm{id}_M} \widehat{\mathrm{Ext}}^*_{kG}(M,M)$$

restricted to its subring $H^*(G,M)$ as $\widehat{\mathrm{Ext}}^*_{kG}(M,M)$ is a graded $\widehat{H}^*(G,k)$-module induced by the ring homomorphism.

Theorem 30.9 (Finite Generation Theorem)**.** *$H^*(G,k)$ is a finitely generated k-algebra. If M is a finitely generated kG-module, then $H^*(G,M)$ is a finitely generated $H^*(G,k)$-module.*

The *nilradical* $\mathrm{Nrad}(R)$ of a ring R is the sum of all the nilpotent 2-sided ideals, i.e.,

$$\mathrm{Nrad}(R) = \{x \in R \,|\, \text{for all } y, z \in R,\ yxz \text{ is nilpotent}\}$$

Lemma 30.10. *If H^* is a graded commutative ring, i.e., $yx = (-1)^{|x||y|}xy$ for all $x, y \in H^*$, then $H^*/\mathrm{Nrad}(H^*)$ is strictly commutative.*

Proof. Let $x \in H^*$, then $xx = (-1)^{|x||x|}xx$. If x has odd degree, then $x^2 = -x^2$, i.e., $2x^2 = 0$. For any $y, z \in R$, $(y \cdot 2x \cdot z)^2 = 0$, so $2x \in \mathrm{Nrad}(H^*)$. Hence

$$x \equiv -x \mod \mathrm{Nrad}(H^*)$$

and so for any $y \in R$ such that $|y|$ is odd, then $xy \equiv -yx \equiv yx \mod \mathrm{Nrad}(H^*)$. If either x or y has even degree, then they already commute. $\square$

So $H^*(G,k)/\mathrm{Nrad}(H^*(G,k))$ is a finitely generated commutative k-algebra and it is isomorphic to $k[x_1, \ldots, x_n]/I$ such that x_i's are homogeneous elements of $H^*(G,k)$.

We define the *variety* V_G corresponding to $H^*(G,k)$ as

$$\begin{aligned} V_G &= \{\text{maximal ideals in } H^*(G,k)\} \\ &= \{\text{maximal ideals in } H^*(G,k)/\mathrm{Nrad}(H^*(G,k))\} \\ &= \{\text{maximal ideals in } k[x_1, \ldots, x_n] \text{ containing the ideal } I\} \\ &\subseteq \{\text{maximal ideals in } k[x_1, \ldots, x_n]\} \end{aligned}$$

where the set of all maximal ideals in $k[x_1, \ldots, x_n]$ has one-to-one correspondence with the set of all points in the affine space $\mathbb{A}^n(k)$ provided k is an algebraically closed field (Hilbert's Nullstellensatz Theorem).

Example 30.11. Let G be the Mathieu group M_{11}, k has characteristic 2. We have $|G| = 7920$ and

$$H^*(G,k) \cong k[x,y,z]/(x^2y - z^2)$$

where $\deg x = 3$, $\deg y = 4$ and $\deg z = 5$. So V_G is the subset of $\mathbb{A}^3(k)$ containing all vectors (v_1, v_2, v_3) such that ${v_1}^2 v_2 = {v_3}^2$ and $\dim V_G = 2$.

Example 30.12. Let G be the cyclic group of order p and the characteristic of k is p.

(i) $p = 2$: $H^*(G,k) = k[x]$ with $\deg x = 1$ and hence $V_G = \mathbb{A}^1(k)$.
(ii) p odd: in the proof of Lemma 30.10 we have seen that odd degree elements square to zero. Indeed $H^*(G,k) = k[x,y]/(x^2)$ with $\deg x = 1$ and $\deg y = 2$. So $V_G = \mathbb{A}^1(k)$.

Example 30.13. If $p \nmid |G|$ and characteristic of k is p, then $H^*(G,k) = k$. So $V_G = \{\text{a point}\}$.

Example 30.14. Let $G = \mathbb{Z}/p \times \mathbb{Z}/p$, then

$$H^*(G,k) = \begin{cases} k[x_1, x_2] & ; p = 2 \\ \Lambda(x_1, x_2) \otimes k[y_1, y_2] & ; p \text{ odd} \end{cases}$$

where in both cases we have $\deg x_i = 1$ and in the second case we have $\deg y_i = 2$ such that ${x_1}^2 = {x_2}^2 = 0$, $x_1x_2 = -x_2x_1$ and $x_iy_j = y_jx_i$. So $V_G = \mathbb{A}^2(k)$ as $\Lambda(x_1, x_2) \subseteq \mathrm{Nrad}(H^*(G, k))$ for p odd.

Example 30.15. Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quarternion group, which lies in the quarternion numbers $\mathbb{H}$. SU(2) is the unit sphere S^3 in $\mathbb{H}$ and Q_8 acts freely on S^3. Cut up S^3 along the 4 "equators" into 16 3-cells permuted by Q_8 and form the complex of cellular chains with coefficients in a field k of characteristic 2:

$$0 \to C_3 \to C_2 \to C_1 \to C_0 \to 0$$

where C_i is the k-vector space with i-cells as basis. Since this complex has nonzero homology k in degrees 0 and 3 and nowhere else, we get an exact sequence

$$0 \to k \to C_3 \to C_2 \to C_1 \to C_0 \to k \to 0.$$

The free action of Q_8 on C_i make it a free kQ_8-module. So by splicing the above exact sequence to itself we get a free resolution of k as a module for kQ_8:

$$\begin{tikzcd}
\cdots \arrow[r] & C_1 \arrow[r] & C_0 \arrow[rr] \arrow[dr] & & C_3 \arrow[r] & C_2 \arrow[r] & C_1 \arrow[r] & C_0 \arrow[r] & k \arrow[r] & 0 \\
& & & k \arrow[ur] \arrow[dr] & & & & & & \\
& & 0 \arrow[ur] & & 0 & & & & &
\end{tikzcd}$$

Theorem 30.16. *Let k be a field of characteristic 2.*

(1) *$H^*(Q_8, k)$ is periodic with period 4*
(2) *There is an element $z \in H^4(Q_8, k)$ such that*
$$\cdot z \colon H^n(Q_8, k) \xrightarrow{\cong} H^{n+4}(Q_8, k)$$
for all $n \geq 0$.
(3) *We have $H^*(Q_8, k)/\langle z \rangle \cong H^*(\mathrm{Hom}_{kQ_8}(C_*, k))$.*

Theorem 30.17. *Suppose that a finite group G acts freely on an n-sphere S^n. Then G has periodic cohomology with any (field) coeffients.*

Corollary 30.18. *$\mathbb{Z}/p \times \mathbb{Z}/p$ cannot act freely on any sphere.*

Corollary 30.19. *If a finite group G acts freely on a sphere, then every abelian subgroup of G is cyclic. More generally, if G acts freely on a compact manifold homotopic equivalent to a sphere, then every abelian subgroup of G is cyclic.*

Example 30.20. Let $G = (\mathbb{Z}/p \times \mathbb{Z}/q) \rtimes Q_8$ where p, q are distinct primes and the action of Q_8 on $(\mathbb{Z}/p \times \mathbb{Z}/q)$ is given as follows: the center Z of Q_8 acts trivially and writing $Q_8/Z = \langle x, y \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, x, y invert the generators of $\mathbb{Z}/p$, $\mathbb{Z}/q$, respectively. One can show that every abelian subgroup of G is cyclic, but that G cannot act freely on S^3. Can G act freely on a homotopy S^3? If so, it provides a counterexample to the Poincaré conjecture.

31. Varieties for Modules

The theory of varieties for modules were developed by Jon Carlson. Let k be an algebraically closed field and let M be a finitely generated kG-module. Consider the map of graded k-algebras

$$H^*(G, k) = \mathrm{Ext}^*_{kG}(k, k) \xrightarrow{-\otimes_k \mathrm{id}_M} \mathrm{Ext}^*_{kG}(M, M).$$

Denote by J_M the kernel of this map. Then we define $V_G(M)$ as the maximal ideal spectrum of $H^*(G,k)/J_M$. Note that $V_G(M)$ is a homogenious subvariety of V_G.

Proposition 31.1. *Let M, M_1, M_2 be finitely generated kG-modules where k is an algebraically closed field. Then*

(1) *M is projective if and only if $V_G(M) = \{0\}$.*
(2) *$V_G(M_1 \oplus M_2) = V_G(M_1) \cup V_G(M_2)$.*
(3) *$V_G(M_1 \otimes_k M_2) = V_G(M_1) \cap V_G(M_2)$. (Avrunin, Scott)*
(4) *$V_G(\Omega M) = V_G(M) = V_G(\Omega^{-1} M)$.*
(5) *$V_G(M^*) = V_G(M)$ where $M^* = \mathrm{Hom}_k(M,k)$.*
(6) *If $0 \neq \zeta \in H^*(G,k) \cong \underline{\mathrm{Hom}}_{kG}(\Omega^n k, k)$ with a short exact sequence*

$$0 \to L_\zeta \to \Omega^n k \xrightarrow{\widehat{\zeta}} k \to 0$$

where $\widehat{\zeta}$ is a representative of ζ in $\underline{\mathrm{Hom}}_{kG}(\Omega^n k, k)$, then $V_G(L_\zeta) = V_G\langle\zeta\rangle$, the hypersurface of V_G where ζ vanishes. Consequently, every closed homogenious subvariety W of V_G is of the form

$$V_G(L_{\zeta_1} \otimes \cdots \otimes L_{\zeta_s}),$$

i.e. W is the subvariety of the ideal generated by $\zeta_1, \ldots, \zeta_s$.
(7) *$V_G(M)$ is 1-dimensional if and only if $M \cong \Omega^n M$ in $\mathrm{stmod}(kG)$ for some $n > 0$. Such M is called a* periodic module*.*
(8) *$\dim V_G(M)$ tells how fast the minimal projective resolution of M grows: if*

$$\cdots \to P_1 \to P_0 \to M \to 0$$

is a minimal projective resolution of M, then there exists $C > 0$ such that

$$\dim P_n \leq C \cdot n^{\dim V_G(M) - 1}$$

for all $n > 0$. Moreover, for every $\varepsilon > 0$ there is no $C > 0$ such that

$$\dim P_n \leq C n^{\dim V_G(M) - 1 - \varepsilon}$$

for all $n > 0$.

Part (8) is a consequence of Hilbert-Serré theorem:

$$p(M,t) = \sum_{n \geq 0} \dim P_n \cdot t^n$$

is a rational function of t and the order of the pole at $t = 1$ is equal to $\dim V_G(M)$.

32. Rank Varieties

Theorem 32.1 (Chouinard)**.** *Let k be any field of characteristic p and let M be any (not necessarily finitely generated) kG-module. Then M is projective if and only if for every elementary abelian p-subgroup E of G, $M\downarrow_E$ is projective.*

More generally, $V_G(M)$ only depends on $V_E(M\downarrow_E)$ for elementary abelian p-subgroups E of G. (Alperin, Evens)

Therefore, to compute $V_G(M)$, the case where $G = E$ is an elementary abelian p-group ($\mathrm{char}\, k = p$) is crucial. Let

$$E = \langle g_1, \cdots, g_r \rangle \cong (\mathbb{Z}/p)^r.$$

Set $x_i = g_i - 1 \in kE$. Then

$$x_i^p = g_i^p - 1 = 0$$
$$x_i x_j = x_j x_i$$

So we have a k-algebra homomorphism

$$\begin{array}{ccc} k[X_1, \cdots, X_r]/(X_1^p, \cdots, X_r^p) & \to & kE \\ X_i & \mapsto & x_i \end{array}$$

Comparing dimension, we see that the above map is in fact an isomorphism.

Now

$$J(kE) = \langle x_1, \cdots, x_r \rangle$$
$$J^2(kE) = \langle x_i^2, x_i x_j \rangle$$

so $J(kE)/J^2(kE)$ has k-basis $x_1 + J^2(kE), \cdots, x_r + J^2(kE)$; in particular it has dimension r. We're going to identify this with V_E.

If $0 \neq \alpha = (\alpha_1, \cdots, \alpha_r) \in \mathbb{A}^r(k)$, look at the element $u_\alpha = 1 + \alpha_1 x_1 + \cdots + \alpha_r x_r$. Then $u_\alpha^p = 1$, so $\langle u_\alpha \rangle$ is a cyclic subgroup of order p in $(kE)^\times$. If M is a finitely generated kE-module, define the *rank variety* of M by

$$V_E^r(M) = \{0 \neq \alpha \in \mathbb{A}^r(k) \mid M\downarrow_{\langle u_\alpha \rangle} \text{ is not a free } k\langle u_\alpha\rangle\text{-module}\} \cup \{0\}.$$

Remark 32.2. A $k\langle u_\alpha \rangle$-module M is free
$\iff$ all Jordan blocks of M have length p
$\iff \dim M^{u_\alpha} = \frac{\dim M}{p}$.

Example 32.3 ("Jon Carlson's favorite example"). Let $E = \langle g_1, g_2, g_3 \rangle \cong (\mathbb{Z}/2)^3$, char $k = 2$. For $a, b, c \in k$, let $M_{a,b,c}$ be a 4-dimensional kE-module given by

$$g_1 \mapsto \begin{pmatrix} 1 & & & \\ & 1 & & \\ 1 & & 1 & \\ & 1 & & 1 \end{pmatrix}, \quad g_2 \mapsto \begin{pmatrix} 1 & & & \\ & 1 & & \\ a & & 1 & \\ & b & & 1 \end{pmatrix}, \quad g_3 \mapsto \begin{pmatrix} 1 & & & \\ & 1 & & \\ & c & 1 & \\ 1 & & & 1 \end{pmatrix}.$$

Then

$$x_1 \mapsto \begin{pmatrix} & & & \\ & & & \\ 1 & & & \\ & 1 & & \end{pmatrix}, \quad x_2 \mapsto \begin{pmatrix} & & & \\ & & & \\ a & & & \\ & b & & \end{pmatrix}, \quad x_3 \mapsto \begin{pmatrix} & & & \\ & & & \\ & c & & \\ 1 & & & \end{pmatrix},$$

and

$$1 + \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 \mapsto \begin{pmatrix} 1 & & & \\ & 1 & & \\ \alpha_1 + a\alpha_2 & c\alpha_3 & 1 & \\ \alpha_3 & \alpha_1 + b\alpha_2 & & 1 \end{pmatrix}.$$

This is non-projective if and only if $(\alpha_1 + a\alpha_2)(\alpha_1 + b\alpha_2) = c\alpha_3^2$. Thus $V_E^r(M_{a,b,c})$ consists of the points (x_1, x_2, x_3) such that

$$(x_1 + ax_2)(x_1 + bx_2) = cx_3^2$$

Lemma 32.4 (Dade). *A finitely generated kE-module M is projective if and only if $V_E^r(M) = \{0\}$.*

Theorem 32.5 (Carlson, Avrunin, Scott). *There is a natural isomorphism $V_E \cong \mathbb{A}^r(k)$ which sends $V_E(M)$ to $V_E^r(M)$ for all finitely generated kE-module M.*

Warning: For p odd, this isomorphism sends $(\alpha_1, \cdots, \alpha_r)$ to $(\alpha_1^p, \cdots, \alpha_r^p)$.

Example 32.6. Let $E = \langle g_1, g_2\rangle \cong (\mathbb{Z}/2)^2$, char $k = 2$. Let $M = k(t) \oplus k(t)$ be a kE-module via

$$g_1 \mapsto \begin{pmatrix} I & 0 \\ I & I \end{pmatrix}, \quad g_2 \mapsto \begin{pmatrix} I & 0 \\ T & I \end{pmatrix}$$

where T denotes multiplication by t. Then

$$1 + \alpha_1(g_1 - 1) + \alpha_2(g_2 - 1) \mapsto \begin{pmatrix} I & 0 \\ \alpha_1 I + \alpha_2 T & I \end{pmatrix}.$$

So

$$V_E^r(M) = \{0\}.$$

Now extend k to $k(x)$. Note $k(t) \otimes_k k(x) \ncong k(t, x)$. Setting $\alpha_1 = x$, $\alpha_2 = 1$, we see that $x + t$ is not invertible in $k(t) \otimes_k k(x)$. Thus

$$V_E^r(k(x) \otimes_k M) \neq \{0\}.$$

Theorem 32.7. *Let M be any (not necessarily finitely generated) kE-module. Then M is projective if and only if for every finitely generated extension K of k and for all shifted subgroup u_α of KE,*

$$(K \otimes_k M)\downarrow_{\langle u_\alpha\rangle}$$

is free.

We have $J(kE)/J^2(kE) \cong H^1(E, k)^*$. If $p = 2$, this is isomorphic to V_E. If p is odd, we have

$$H^*(E, k) \cong \Lambda(x_1, \cdots, x_r) \otimes_k k[y_1, \cdots, y_r]$$

where $\deg x_i = 1$, $\deg y_i = 2$ and the Bokstein map

$$\begin{array}{ccc} H^1(E,k) & \xrightarrow[\cong]{\beta} & H^2(E,k) \\ x_i & \mapsto & y_i \end{array}$$

is semi-linear: $\beta(\lambda x_i) = \lambda^p y_i$ for $\lambda \in k$. Thus

$$H^1(E, k)^* \xleftarrow[\cong]{\beta^*} (H^2/H^1H^1)^{*(p)} \cong V_E^{(p)}.$$

References

[I] I. Martin Isaacs *Chacracter Theory of Finite Groups*, Academic Press, New York, San Francisco, London 1976.