Modular Representation Theory of Finite Groups

Caroline Lassueur
Niamh Farrell
TU Kaiserslautern

WS 2019/20 Part II
(4 hr per week Lecture + 2 hr per week Exercises)

Version: 13th January 2020

Contents

Chapter 8. Splitting p-modular systems and Brauer Reciprocity

The goal of this chapter is to define splitting p-modular systems and to prove Brauer Reciprocity for group algebras. A p-modular system is a triple $(K, \mathcal{O}, k)$ such that K is a field of characteristic 0, $\mathcal{O}$ is a discrete valuation ring contained in K which has unique maximal ideal $J(\mathcal{O})$, and k is a field of characteristic p such that $k \cong \mathcal{O}/J(\mathcal{O})$. We will use p-modular systems and Brauer reciprocity in the subsequent chapters to get information about kG (which is complicated) from KG (which is semisimple and therefore much better understood) via the group algebra $\mathcal{O}G$.

Notation: All modules in this chapter are assumed to be **finitely generated**.

References:

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

[NT89] H. Nagao and Y. Tsushima, *Representations of finite groups*, Translated from the Japenese. Academic Press, Inc., Boston, MA, 1989.

[Rot10] J. J. Rotman, *Advanced modern algebra. 2nd ed.*, Providence, RI: American Mathematical Society (AMS), 2010.

30 Lifting Idempotents

Definition 30.1

A **discrete valuation ring** is a principal ideal domain $\mathcal{O}$ with a surjective valuation map $v : \mathcal{O}\backslash\{0\} \to \mathbb{N}_0$ such that for all $a, b \in \mathcal{O}\backslash\{0\}$,

- $v(a) \geqslant 0$
- $v(ab) = v(a) + v(b)$, and
- $v(a + b) \geqslant \min\{v(a), v(b)\}$,

and $v(0) = \infty$. The map v is called an **exponential valuation**. The ring $\mathcal{O}$ has a maximal ideal $\{a \in \mathcal{O} \mid v(a) \geqslant 1\}$. Since it is the unique maximal ideal of $\mathcal{O}$ it is equal to the Jacobson radical $J(\mathcal{O})$. Note that $\mathcal{O}^\times = \mathcal{O}\backslash J(\mathcal{O})$ so $\mathcal{O}$ is a local ring.

For a more general introduction to valuation rings, see [Web16, Appendix A]. For the rest of this section let $\mathcal{O}$ denote a discrete valuation ring with maximal ideal $J(\mathcal{O})$, and assume that $\mathcal{O}$ is complete with

respect to the valuation v; that is, every sequence in $\mathcal{O}$ which is Cauchy with respect to v converges.

Let $k := \mathcal{O}/J(\mathcal{O})$ be the residue field of $\mathcal{O}$. For a finitely generated free $\mathcal{O}$-algebra A, we write $\overline{A}$ for the k-algebra $A/J(\mathcal{O})A$, and for any $x \in A$ we let $\overline{x}$ denote its image in $\overline{A}$.

Example 30.2 (*Complete discrete valuation ring*)

Let p be a prime and let $\mathcal{O} := \mathbb{Z}_p$ be the ring of p-adic integers – that is,

$$\mathbb{Z}_p = \left\{ \sum_{i=k}^{\infty} a_i p^i \mid k \in \mathbb{Z}_{\geqslant 0} \text{ and } a_i \in \{0, \dots, p-1\} \right\}.$$

Let v denote the exponential p-adic valuation defined by $v(a_i p^i) = i$ for all $a_i \in \{0, \dots, p-1\}$ and $i \geqslant 0$. Then $\mathcal{O}$ is a discrete valuation ring and is complete with respect to v, with maximal ideal $J(\mathcal{O}) = p\mathbb{Z}_p$ and residue field $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

Proposition 30.3

Let A be a finitely generated $\mathcal{O}$-algebra.

(a) For every idempotent $x \in \overline{A}$, there exists an idempotent $e \in A$ such that $\overline{e} = x$.

(b) $A^\times = \{a \in A \mid \overline{a} \in \overline{A}^\times\}$.

(c) If $e_1, e_2 \in A$ are idempotents such that $\overline{e}_1 = \overline{e}_2$ then there is a unit $u \in A^\times$ such that $e_1 = u e_2 u^{-1}$.

(d) The quotient map $^- : A \to \overline{A}$ induces a bijection between the central idempotents of A and the central idempotents of $\overline{A}$.

Proof: (a) Let $x \in \overline{A}$ be an idempotent. Let $x_0 \in A$ be a pre-image of x under the quotient map $A \to \overline{A}$ and define a sequence $(x_n)_n$ in A by $x_{n+1} := 3x_n^2 - 2x_n^3$ for $n \geqslant 0$. We will show that this sequence converges to a limit $e \in A$ which is an idempotent such that $\overline{e} = x$.

For $n \geqslant 0$, define $y_n := x_n^2 - x_n$.

Claim: $y_n \in J(\mathcal{O})^{2^n}$ for all n.

Proof of claim: By induction on n. When $n = 0$ we have $y_0 = x_0^2 - x_0$ and $\overline{y_0} = x^2 - x = 0$ because x is an idempotent. Hence y_0 is in the kernel of the quotient map. In other words, $y_0 \in J(\mathcal{O})$ so the hypothesis holds for $n = 0$. Now suppose that $y_n \in J(\mathcal{O})^{2^n}$. Then

$$y_{n+1} = x_{n+1}^2 - x_{n+1} = 9x_n^4 + 4x_n^6 - 12x_n^5 - 3x_n^2 + 2x_n^3 = 4y_n^3 - 3y_n^2.$$

and this is an element of $J(\mathcal{O})^{2^{n+1}}$ because $y_n \in J(\mathcal{O})^{2^n}$, and the claim is proved.

We have $x_{n+1} - x_n = 3x_n^2 - 2x_n^3 - x_n = y_n(1 - 2x_n) \in J(\mathcal{O})^{2^n}$ because $J(\mathcal{O})^{2^n}$ is an ideal. Hence $(x_n)_n$ is a Cauchy sequence in A. But A is a finitely generated $\mathcal{O}$-module and $\mathcal{O}$ is complete so there exists a limit $e := \lim_{n\to\infty} x_n \in A$.

Now $e^2 - e = \lim_{n\to\infty}(x_n^2 - x_n) = \lim_{n\to\infty}(y_n) = 0$ because $y_n \in J(\mathcal{O})^{2^n}$, so e is an idempotent. Finally, for all $n \geqslant 1$ we have $x_n - x_0 = (x_n - x_{n-1}) + (x_{n-1} - x_{n-2}) + \cdots + (x_2 - x_1) + (x_1 - x_0) \in J(\mathcal{O})$, so $\lim_{n\to\infty}(x_n - x_0) = e - x_0 \in J(\mathcal{O})$ and therefore $\overline{e} = \overline{x}_0 = x$.

(b) Let $u \in A$ such that $\overline{u} \in \overline{A}^\times$ is a unit with inverse $\overline{v}$. Let v be a preimage of $\overline{v}$ under the quotient map. Then $y := 1 - uv \in J(\mathcal{O})$. It follows that $y^n \in J(\mathcal{O})^n$, therefore $\sum_{n=0}^{\infty} y^n$ converges in A and

$$uv \sum_{n=0}^{\infty} y^n = (1 - y) \sum_{n=0}^{\infty} y^n = 1.$$

Hence u has a right inverse in A. Similarly, u has a left inverse in A, so $u \in A^\times$.

The other direction is clear: if $u \in A^\times$ has inverse $v \in A$, then $\overline{u} \in \overline{A}$ has inverse $\overline{v} \in \overline{A}$, so $\overline{u} \in \overline{A}^\times$.

(c) Fix $u := 1 - e_1 - e_2 + 2e_1e_2$. Then $\overline{u} = 1 - 2\overline{e_1} + 2\overline{e_1}^2 = 1$ because e_1 is an idempotent. Hence by part (b), $u \in A^\times$ and furthermore, $e_1u = e_1 - e_1^2 - e_1e_2 + 2e_1^2e_2 = ue_2$ so $e_1 = ue_2u^{-1}$ as required.

(d) Firstly, the image of a central idempotent of A under the quotient map is a central idempotent of $\overline{A}$. It remains to show that the restriction of the quotient map to the central idempotents of A is a bijection.

Suppose that $e_1, e_2 \in A$ are two central idempotents such that $\overline{e}_1 = \overline{e}_2$. Then by part (c), e_1 and e_2 are conjugate in A. But e_1 and e_2 are central so this means that $e_1 = e_2$. Thus the quotient map is injective on central idempotents.

Let $\overline{e} \in \overline{A}$ be a central idempotent. By part (a), there exists a preimage $e \in A$ of $\overline{e}$ under the quotient map which is an idempotent. We will show that e is central. The quotient map sends $(1-e)Ae$ to 0 because $\overline{e}$ is central. Therefore $(1-e)Ae = J(\mathcal{O})(1-e)Ae$ so $(1-e)Ae = 0$ by Nakayama's Lemma (Theorem 9.3). Similarly $eA(1-e) = 0$. Therefore

$$A = (e + 1 - e)A(e + 1 - e) = eAe + (1 - e)A(1 - e),$$

so every element $x \in A$ can be written as $x = eae + (1-e)b(1-e)$ for some $a, b \in A$. In particular, all elements of A commute with e so e is central. ■

We will need the following result for the next corollary.

Exercise 30.4

Lemma 30.5

Let A be a finitely generated algebra over a commutative ring R. Let P be a projective indecomposable A-module. Prove that there exists an idempotent $e \in A$ such that $P \cong Ae$ as A-modules.

Corollary 30.6

(Continue with the notation from before Exercise 30.4.) Let V be a projective $\overline{A}$-module. Then there exists a projective A-module M such that $V \cong M/J(\mathcal{O})M$.

Proof: By Lemma 30.5 there exist idempotents $f_1, \dots, f_r \in \overline{A}$ such that $V \cong \overline{A}f_1 \oplus \cdots \oplus \overline{A}f_r$. It then follows from Proposition 30.3 (a) that we can choose idempotents $e_1, \dots, e_r \in A$ such that e_i is a pre-image of f_i in A for each $1 \leqslant i \leqslant r$. Let $M := Ae_1 \oplus \cdots \oplus Ae_r$. Then M is projective (see Chapter 25 Example 14 (b)) and $M/J(\mathcal{O})M \cong V$. ■

31 Splitting fields

Let R and S be commutative rings and suppose that there exists a ring homomorphism $\varphi : R \to S$. Then there is a right action of R on S given by $s.r := s\varphi(r)$ for all $s \in S$, $r \in R$. This allows us to tensor S by R on the right.

Notation 31.1

Let A be an R-algebra and let U be an A-module. Then $A^S := S \otimes_R A$ is an S-algebra with action of S given by $s.(s' \otimes a) = ss' \otimes a$ for all $s, s' \in S$ and $a \in A$; and $U^S := S \otimes_R U$ is an A^S-module

with action of A^S given by $(s_1 \otimes a).(s_2 \otimes u) = s_1 s_2 \otimes a.u$ for all $s_1, s_2 \in S, a \in A, u \in U$.

Definition 31.2

If R is contained in S and $\varphi : R \hookrightarrow S$ is the inclusion map, then the process above is called **extension of scalars**. We say that the module U^S is **obtained from** U **by the extension of scalars**.

Definition 31.3 (*Splitting field for an algebra*)

Let F be a field and let A be a finite dimensional F-algebra. An extension field E of F is a **splitting field** for A if and only if $\mathrm{End}_{A^E}(S) \cong E$ for all simple A^E-modules S.

Exercise 31.4 (*Splitting fields for an algebra*)

Lemma 31.5

Let F be a field and let A be a finite dimensional F-algebra. Prove the following.

(a) The algebraic closure $\overline{F}$ of F is a splitting field for A.

(b) There is a finite extension $F_1 \mid F$ such that F_1 is a splitting field for A.

Definition 31.6 (*Splitting field for a group*)

Let G be a finite group. A **splitting field for** G is a field F which is a splitting field for the group algebra FG.

Remark 31.7

The character theory of a group over a splitting field of characteristic 0 is the same as the character theory of a group over $\mathbb{C}$, which you may have seen in previous courses.

Example 31.1

Let G be a p-group and suppose that F is a field of characteristic p. Then the trivial module F is the only simple FG-module (see Corollary 17.3) and $\mathrm{End}_{FG}(F) \cong F$, so F is a splitting field for G.

32 $\mathcal{O}$-forms

Definition 32.1

Let $\mathcal{O}$ be a complete discrete valuation ring and let $F := \mathrm{frac}(\mathcal{O})$ be the fraction field of $\mathcal{O}$. Let A be a free $\mathcal{O}$-algebra of finite rank, and let V be an A^F-module. An $\mathcal{O}$-**form** of V is an $\mathcal{O}$-free A-submodule of V which has an $\mathcal{O}$-basis which is also an F-basis of V.

Proposition 32.2

There exists an $\mathcal{O}$-form of V.

Proof: Let $v_1, \ldots, v_r$ be an F-basis of V and let $M := Av_1 + \cdots + Av_r$. Then M is a finitely generated A-module which is torsion free and hence free over $\mathcal{O}$ (since $\mathcal{O}$ is a principal ideal domain). Let $m_1, \ldots, m_t$ be an $\mathcal{O}$-basis of M. Then the m_i span V. We will show that the m_i are also linearly independent over F, and hence $t = r$ and $m_1, \ldots, m_t$ is an F-basis for V, so M is an $\mathcal{O}$-form for V.

Suppose that $\lambda_1 m_1 + \cdots + \lambda_t m_t = 0$ for some $\lambda_i \in F$. Because F is the field of fractions of $\mathcal{O}$, for each $i \in \{1, \ldots, t\}$ we can write $\lambda_i = \frac{a_i}{b_i}$ where $a_i, b_i \in \mathcal{O}$. Therefore $\gamma_1 m_1 + \cdots + \gamma_t m_t = 0$ where $\gamma_i = a_i \prod_{j \in \{1,\ldots,r\} \setminus i} b_j$. Now since $\{m_i\}$ is an $\mathcal{O}$-basis, this implies that $\gamma_i = 0$, and hence $a_i = 0$, for all $1 \leqslant i \leqslant t$. In particular, $\lambda_i = 0$ for all $1 \leqslant i \leqslant t$ and hence the m_i are linearly independent over F. Thus $m_1, \ldots, m_t$ is an F-basis for V. ■

33 Splitting p-modular systems

Definition 33.1 (*p-modular systems*)

(a) A triple $(K, \mathcal{O}, k)$ is a **p-modular system** if

- $\mathcal{O}$ is a complete discrete valuation ring with unique maximal ideal $J(\mathcal{O})$,
- $K := \mathrm{frac}(\mathcal{O})$ is a field of characteristic 0, and
- $k := \mathcal{O}/J(\mathcal{O})$ is a field of characteristic p.

$$K \hookleftarrow \mathcal{O} \twoheadrightarrow k$$

(b) [Splitting p-modular system for an algebra] Let $(K, \mathcal{O}, k)$ be a p-modular system. If A is a free $\mathcal{O}$-algebra of finite rank, K is a splitting field for A^K, and k is a splitting field for $\overline{A}$, then $(K, \mathcal{O}, k)$ is a **splitting p-modular system for** A.

(c) [Splitting p-modular system for a finite group] Let $(K, \mathcal{O}, k)$ be a p-modular system. If G is a finite group and $(K, \mathcal{O}, k)$ is a splitting p-modular system for $\mathcal{O}G$, then we say that $(K, \mathcal{O}, k)$ is a **splitting p-modular system for** G.

Remark 33.2

Let $(K, \mathcal{O}, k)$ be a p-modular system and let G be a finite group with exponent m. If K contains a primitive m-th root of unity then $(K, \mathcal{O}, k)$ is a splitting p-modular system for G.

34 Brauer Reciprocity

We will need the following results for the proof of Brauer Reciprocity.

Exercise 34.1

Let A be a finite dimensional algebra over a commutative ring R. Let V be an A-module and $e \in A$ an idempotent. Prove that

$$\mathrm{Hom}_A(Ae, V) \cong eV$$

as $\mathrm{End}_A(V)$-modules.

For the rest of this section we let G be a finite group and let $(K, \mathcal{O}, k)$ be a splitting p-modular system for G.

Notation 34.2

Recall that Theorem 26.1 (c) showed that for a group algebra over a field there is a bijection between

projective indecomposable modules (up to isomorphism) and simple modules (up to isomorphism). Let S be a simple KG-module or a simple kG-module. As in Exercise 26.6, we let P_S denote a projective indecomposable module corresponding to S via the bijection. Then P_S is called a **projective cover** of S.

Theorem 34.3 (*Brauer Reciprocity*)

Let $V_1, \dots, V_l$ be a complete set of representatives of isomorphism classes of simple KG-modules, and let $S_1, \dots, S_t$ be a complete set of representatives of isomorphism classes of simple kG-modules.

(a) If V is a KG-module and M is an $\mathcal{O}$-form of V, then the number of composition factors of $\overline{M} := M/J(\mathcal{O})M$ isomorphic to S_j for each $1 \leqslant j \leqslant t$ does not depend on the choice of the $\mathcal{O}$-form M.

(b) Let $e_1, \dots, e_t \in \mathcal{O}G$ be idempotents such that $kG\overline{e}_j$ is a projective cover of S_j for each $1 \leqslant j \leqslant t$. Let P_{V_i} be a projective cover of V_i for $1 \leqslant i \leqslant l$. Define d_{ij} to be the number of composition factors of the reduction of an $\mathcal{O}$-form of V_i which are isomorphic to S_j (by part (a), this is well defined). Then

$$KGe_j \cong \bigoplus_{i=1}^{l} d_{ij} P_{V_i}.$$

Proof: (a) Let M be an $\mathcal{O}$-form for V. Let $\overline{M} = M_0 > M_1 > \cdots > M_r = 0$ be a composition series for the quotient module $\overline{M}$. Fix a $j \in \{1, \dots, t\}$ and let P_{S_j} be a projective cover of S_j. By Lemma 30.5 and Proposition 30.3, there exists an idempotent $e_j \in \mathcal{O}G$ such that $P_{S_j} = kG\overline{e}_j$.

For any $1 \leqslant i \leqslant r$, we have an exact sequence of kG-modules $0 \to M_i \to M_{i-1} \to M_{i-1}/M_i \to 0$. It then follows from Proposition-Definition 25.1 (a) that

$$0 \to \mathrm{Hom}_{kG}(P_{S_j}, M_i) \to \mathrm{Hom}_{kG}(P_{S_j}, M_{i-1}) \to \mathrm{Hom}_{kG}(P_{S_j}, M_{i-1}/M_i) \to 0$$

is exact. Hence

$$\begin{aligned}
\dim_k \mathrm{Hom}_{kG}(P_{S_j}, \overline{M}) &= \dim_k \mathrm{Hom}_{kG}(P_{S_j}, M_0) \\
&= \dim_k \mathrm{Hom}_{kG}(P_{S_j}, M_1) + \dim_k \mathrm{Hom}_{kG}(P_{S_j}, M_0/M_1) \\
&= \dim_k \mathrm{Hom}_{kG}(P_{S_j}, M_2) + \dim_k \mathrm{Hom}_{kG}(P_{S_j}, M_1/M_2) \\
&\qquad + \dim_k \mathrm{Hom}_{kG}(P_{S_j}, M_0/M_1) \\
&= \dots \\
&= \sum_{i=1}^{r} \dim_k \mathrm{Hom}_{kG}(P_{S_j}, M_{i-1}/M_i).
\end{aligned}$$

By Exercise 26.6 (a), we know that for each $1 \leqslant i \leqslant r$,

$$\dim_k \mathrm{Hom}_{kG}(P_{S_j}, M_{i-1}/M_i) = \begin{cases} \dim_k \mathrm{End}_{kG}(S_j) & \text{if } M_{i-1}/M_i \cong S_j \\ 0 & \text{otherwise.} \end{cases}$$

Since k is a splitting field for G, $\mathrm{End}_{kG}(S_j) \cong k$ so $\dim_k(\mathrm{End}_{kG}(S_j)) = 1$. Therefore the dimension $\dim_k \mathrm{Hom}_{kG}(P_{S_j}, \overline{M})$ just counts the number of composition factors of $\overline{M}$ isomorphic to S_j.

On the other hand, Exercise 34.1 shows that $\mathrm{Hom}_{kG}(P_{S_j}, \overline{M}) \cong \overline{e}_j\overline{M}$. Since $\mathcal{O}$ is a principal ideal domain and $e_jM \leqslant M$ is a submodule of a free $\mathcal{O}$-module, e_jM is also free over $\mathcal{O}$. Hence $\dim_k(\overline{e}_j\overline{M}) = \dim_k(e_jM/J(\mathcal{O})e_jM) = \mathrm{rank}(e_jM)$. By Proposition 32.2, $\mathrm{rank}(e_jM) = \dim_K(e_jV)$.

Thus, for any $1 \leqslant j \leqslant t$, the number of composition factors of $\overline{M}$ isomorphic to S_j is equal to $\dim_K(e_jV)$, and is therefore independent of the choice of the $\mathcal{O}$-form M.

(b) By Theorem 26.1 (b), $\{P_{V_i}\}_{i=1}^{l}$ is a complete set of representatives of the isomorphism classes of projective indecomposable KG-modules. Since K is a splitting field for G Theorem 13.2 holds for KG (see Remark 13.3) and hence Corollary 26.2 also applies. It follows that the regular module KG° decomposes into a direct sum of P_{V_i}'s, each appearing $\dim_K P_{V_i}/\mathrm{rad}(P_{V_i}) = \dim_K V_i$ times. Hence, for any $1 \leqslant j \leqslant t$, there exist non-negative integers d'_{ij} such that

$$KGe_j = \bigoplus_{i=1}^{l} d'_{ij} P_{V_i},$$

where $d'_{ij} = \dim_K \mathrm{Hom}_{KG}(KGe_j, V_i)$. Fix $i \in \{1, \ldots, l\}$ and $j \in \{1, \ldots, t\}$. It only remains to show that $d'_{ij} = d_{ij}$. Choose an $\mathcal{O}$-form M_i of V_i. We have,

$$\begin{aligned} d'_{ij} &= \dim_K \mathrm{Hom}_{KG}(KGe_j, V_i) \\ &= \dim_K e_jV_i \qquad \text{by Exercise 34.1} \\ &= \mathrm{rank}(e_jM_i) \qquad \text{by Proposition 32.2} \\ &= \dim_k \overline{e}_j\overline{M}_i \\ &= \dim_k \mathrm{Hom}_{kG}(kG\overline{e}_j, \overline{M}_i) \\ &= d_{ij}. \end{aligned}$$

■

Definition 34.4

The **decomposition matrix of** G is the matrix $D := (d_{ij})_{1\leqslant i\leqslant l, 1\leqslant j\leqslant t}$, where the d_{ij} are positive integers defined in the previous theorem.

Remark 34.5

The decomposition matrix D is independent of the choice of splitting p-modular system $(K, \mathcal{O}, k)$ for G.