Modular Representation Theory of Finite Groups

Jun.-Prof. Dr. Caroline Lassueur
TU Kaiserslautern

Skript zur Vorlesung, WS 2020/21
(Vorlesung: 4SWS // Übungen: 2SWS)

Version: 4. Dezember 2021

Contents

Foreword

This text constitutes a faithful transcript of the lecture **Modular Representation Theory** held at the TU Kaiserslautern during the Winter Semester 2020/21 (14 Weeks, 4SWS Lecture + 2SWS Exercises).

Together with the necessary theoretical foundations the main aims of this lecture are to:

- provide students with a modern approach to **finite group theory**;
- learn about the **representation theory of finite-dimensional algebras** and in particular of **the group algebra of a finite group**;
- establish connections between the representation theory of a finite group over a field of **positive** characteristic and that over a field of characteristic **zero**;
- consistently work with **universal properties** and get acquainted with the **language of category theory**.

We assume as pre-requisites bachelor-level algebra courses dealing with *linear algebra* and *elementary group theory*, such as the standard lectures *Grundlagen der Mathematik*, *Algebraische Strukturen*, and *Einführung in die Algebra*. It is also strongly recommended to have attended the lectures *Commutative Algebra* and *Character Theory of Finite Groups* prior to this lecture. Therefore, in order to complement these pre-requisites, but avoid repetitions, the Appendix deals formally with some background material on module theory, but proofs are omitted.
The main results of the lecture *Character Theory of Finite Groups* will be recovered through a different and more general approach, thus it is formally not necessary to have attended this lecture already, but it definitely brings you some intuition.

Acknowledgement: I am grateful to Gunter Malle who provided me with the Skript of his lecture "Darstellungstheorie" hold at the TU Kaiserslautern in the WS 12/13, 13/14, 15/16 and 16/17, which I used as a basis for the development of this lecture. I am also grateful to Niamh Farrell, who shared with me her text from 2019/20 to the second part of the lecture, which I had never taken myself prior to the WS 20/21.
I am also grateful to Kathrin Kaiser, Helena Petri and Bernhard Böhmler who mentioned typos to me in the preliminary version of these notes. Further comments, corrections and suggestions are of course welcome.

Conventions

Unless otherwise stated, throughout these notes we make the following general assumptions:

- all groups considered are **finite**;
- all rings considered are **associative** and **unital** (i.e. possess a neutral element for the multiplication, denoted 1);
- all modules considered are **left** modules;
- if K is a commutative ring and G a finite group, then all KG-modules considered are assumed to be free of finite rank when regarded as K-modules.

Chapter 1. Foundations of Representation Theory

In this chapter we review four important module-theoretic theorems, which lie at the foundations of *representation theory of finite groups*:

1. **Schur's Lemma**: about homomorphisms between simple modules.
2. **The Jordan-Hölder Theorem**: about "uniqueness" properties of composition series.
3. **Nakayama's Lemma**: about an essential property of the Jacobson radical.
4. **The Krull-Schmidt Theorem**: about direct sum decompositions into indecomposable submodules.

Notation: throughout this chapter, unless otherwise specified, we let R denote an arbitrary unital and associative ring.

References:

[Ben98] D. J. Benson. *Representations and cohomology. I.* Vol. 30. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1998.

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons, Inc., New York, 1990.

[Dor72] L. Dornhoff. *Group representation theory. Part B: Modular representation theory.* Marcel Dekker, Inc., New York, 1972.

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

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

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

1 (Ir)Reducibility and (in)decomposability

Submodules and direct sums of modules allow us to introduce the two main notions that will enable us to break modules in *elementary* pieces in order to simplify their study: *simplicity* and *indecomposability*.

Definition 1.1 (*simple/irreducible module* / *indecomposable module* / *semisimple module*)

(a) An R-module M is called **reducible** if it admits an R-submodule U such that $0 \subsetneq U \subsetneq M$. An R-module M is called **simple**, or **irreducible**, if it is non-zero and not reducible.

(b) An R-module M is called **decomposable** if M possesses two non-zero proper submodules M_1, M_2 such that $M = M_1 \oplus M_2$. An R-module M is called **indecomposable** if it is non-zero and not decomposable.

(c) An R-module M is called **completely reducible** or **semisimple** if it admits a direct sum decomposition into simple R-submodules.

Our primary goal in Chapter 1 and Chapter 2 is to investigate each of these three concepts in details.

Remark 1.2

Clearly any simple module is also indecomposable, resp. semisimple. However, the converse does not hold in general.

Exercise 1.3

Prove that if $(R, +, \cdot)$ is a ring, then $R^\circ := R$ itself maybe seen as an R-module via left multiplication in R, i.e. where the external composition law is given by

$$R \times R^\circ \longrightarrow R^\circ, (r, m) \mapsto r \cdot m\,.$$

We call R° the **regular** R-module.

Prove that:

(a) the R-submodules of R° are precisely the left ideals of R;

(b) $I \lhd R$ is a maximal left ideal of $R \Leftrightarrow R^\circ/I$ is a simple R-module, and $I \lhd R$ is a minimal left ideal of $R \Leftrightarrow I$ is simple when regarded as an R-submodule of R°.

2 Schur's Lemma

Schur's Lemma is a basic result, which lets us understand homomorphisms between *simple* modules, and, more importantly, endomorphisms of such modules.

Theorem 2.1 (*Schur's Lemma*)

(a) Let V, W be simple R-modules. Then:

(i) $\mathrm{End}_R(V)$ is a skew-field, and

(ii) if $V \ncong W$, then $\mathrm{Hom}_R(V, W) = 0$.

(b) If K is an algebraically closed field, A is a K-algebra, and V is a simple A-module such that $\dim_K V < \infty$, then

$$\mathrm{End}_A(V) = \{\lambda\,\mathrm{Id}_V \mid \lambda \in K\} \cong K\,.$$

Proof:

(a) First, we claim that every $f \in \mathrm{Hom}_R(V, W)\backslash\{0\}$ admits an inverse in $\mathrm{Hom}_R(W, V)$.
Indeed, $f \neq 0 \implies \ker f \subsetneq V$ is a proper R-submodule of V and $\{0\} \neq \mathrm{Im}\, f$ is a non-zero R-submodule of W. But then, on the one hand, $\ker f = \{0\}$, because V is simple, hence f is injective, and on the other hand, $\mathrm{Im}\, f = W$ because W is simple. It follows that f is also surjective, hence bijective. Therefore, by Example A.4(d), f is invertible with inverse $f^{-1} \in \mathrm{Hom}_R(W, V)$.
Now, (ii) is straightforward from the above. For (i), first recall that $\mathrm{End}_R(V)$ is a ring, which is obviously non-zero as $\mathrm{End}_R(V) \ni \mathrm{Id}_V$ and $\mathrm{Id}_V \neq 0$ because $V \neq 0$ since it is simple. Thus, as any $f \in \mathrm{End}_R(V)\backslash\{0\}$ is invertible, $\mathrm{End}_R(V)$ is a skew-field.

(b) Let $f \in \mathrm{End}_A(V)$. By the assumptions on K, f has an eigenvalue $\lambda \in K$. Let $v \in V\backslash\{0\}$ be an eigenvector of f for λ. Then $(f - \lambda\,\mathrm{Id}_V)(v) = 0$. Therefore, $f - \lambda\,\mathrm{Id}_V$ is not invertible and

$$f - \lambda\,\mathrm{Id}_V \in \mathrm{End}_A(V) \quad \overset{(a)}{\implies} \quad f - \lambda\,\mathrm{Id}_V = 0 \quad \implies \quad f = \lambda\,\mathrm{Id}_V\ .$$

Hence $\mathrm{End}_A(V) \subseteq \{\lambda\,\mathrm{Id}_V \mid \lambda \in K\}$, but the reverse inclusion also obviously holds, so that

$$\mathrm{End}_A(V) = \{\lambda\,\mathrm{Id}_V\} \cong K\,.$$

■

3 Composition series and the Jordan-Hölder Theorem

From Chapter 2 on, we will assume that all modules we work with can be broken into *simple* modules in the sense of the following definition.

Definition 3.1 (*Composition series* / *composition factors* / *composition length*)

Let M be an R-module.

(a) A **series** (or **filtration**) of M is a finite chain of submodules

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n = M \qquad (n \in \mathbb{Z}_{\geqslant 0})\,.$$

(b) A **composition series** of M is a series

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n = M \qquad (n \in \mathbb{Z}_{\geqslant 0})$$

where M_i/M_{i-1} is simple for each $1 \leqslant i \leqslant n$. The quotient modules M_i/M_{i-1} are called the **composition factors** (or the **constituents**) of M and the integer n is called the **composition length** of M.

Notice that, clearly, in a composition series all inclusions are in fact strict because the quotient modules are required to be simple, hence non-zero.

Next we see that the existence of a *composition series* implies that the module is *finitely generated*. However, the converse does not hold in general. This is explained through the fact that the existence of a composition series is equivalent to the fact that the module is both *Noetherian* and *Artinian*.

Definition 3.2 (*Chain conditions / Artinian and Noetherian rings and modules*)

(a) An R-module M is said to satisfy the **descending chain condition** (D.C.C.) on submodules (or to be **Artinian**) if every descending chain $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_r \supseteq \ldots \supseteq \{0\}$ of submodules eventually becomes stationary, i.e. $\exists\ m_0$ such that $M_m = M_{m_0}$ for every $m \geqslant m_0$.

(b) An R-module M is said to satisfy the **ascending chain condition** (A.C.C.) on submodules (or to be **Noetherian**) if every ascending chain $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r \subseteq \ldots \subseteq M$ of submodules eventually becomes stationary, i.e. $\exists\ m_0$ such that $M_m = M_{m_0}$ for every $m \geqslant m_0$.

(c) The ring R is called **left Artinian** (resp. **left Noetherian**) if the regular module R° is Artinian (resp. Noetherian).

Theorem 3.3 (*Jordan-Hölder*)

Any series of R-submodules $0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M$ ($r \in \mathbb{Z}_{\geqslant 0}$) of an R-module M may be refined to a composition series of M. In addition, if

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M \quad (n \in \mathbb{Z}_{\geqslant 0})$$

and

$$0 = M'_0 \subsetneq M'_1 \subsetneq \ldots \subsetneq M'_m = M \quad (m \in \mathbb{Z}_{\geqslant 0})$$

are two composition series of M, then $m = n$ and there exists a permutation $\pi \in \mathfrak{S}_n$ such that $M'_i/M'_{i-1} \cong M_{\pi(i)}/M_{\pi(i)-1}$ for every $1 \leqslant i \leqslant n$. In particular, the composition length is well-defined.

Proof: See *Commutative Algebra*. ■

Corollary 3.4

If M is an R-module, then TFAE:

(a) M has a composition series;

(b) M satisfies D.C.C. and A.C.C. on submodules;

(c) M satisfies D.C.C. on submodules and every submodule of M is finitely generated.

Proof: See *Commutative Algebra*. ■

Theorem 3.5 (*Hopkins' Theorem*)

If M is a module over a left Artinian ring, then TFAE:

(a) M has a composition series;

(b) M satisfies D.C.C. on submodules;

(c) M satisfies A.C.C. on submodules;

(d) M is finitely generated.

Proof: Without proof. ■

4 The Jacobson radical and Nakayama's Lemma

The Jacobson radical is one of the most important two-sided ideals of a ring. As we will see in the next sections and Chapter 2, this ideal carries a lot of information about the structure of a ring and that of its modules.

Proposition-Definition 4.1 (*Annihilator / Jacobson radical*)

(a) Let M be an R-module. Then $\operatorname{ann}_R(M) := \{r \in R \mid rm = 0 \ \ \forall\ m \in M\}$ is a two-sided ideal of R, called **annihilator** of M.

(b) The **Jacobson radical** of R is the two-sided ideal

$$J(R) := \bigcap_{\substack{V \text{ simple} \\ R\text{-module}}} \operatorname{ann}_R(V) = \{x \in R \mid 1 - axb \in R^\times \ \ \forall\ a, b \in R\}\,.$$

(c) If V is a simple R-module, then there exists a maximal left ideal $I \lhd R$ such that $V \cong R^\circ/I$ (as R-modules) and

$$J(R) = \bigcap_{\substack{I \lhd R, \\ I \text{ maximal} \\ \text{left ideal}}} I\,.$$

Proof: See *Commutative Algebra*. ■

Exercise 4.2

(a) Prove that any simple R-module may be seen as a simple $R/J(R)$-module.

(b) Conversely, prove that any simple $R/J(R)$-module may be seen as a simple R-module. [Hint: use a change of the base ring via the canonical morphism $R \longrightarrow R/J(R)$.]

(c) Deduce that R and $R/J(R)$ have the same simple modules.

Theorem 4.3 (*Nakayama's Lemma*)

If M is a finitely generated R-module and $J(R)M = M$, then $M = 0$.

Proof: See *Commutative Algebra*. ■

Remark 4.4

One often needs to apply Nakayama's Lemma to a finitely generated quotient module M/U, where U is an R-submodule of M. In that case the result may be restated as follows:

$$M = U + J(R)M \quad \Longrightarrow \quad U = M$$

5 Indecomposability and the Krull-Schmidt Theorem

We now consider the notion of *indecomposability* in more details. Our first aim is to prove that indecomposability can be recognised at the endomorphism algebra of a module.

Definition 5.1

A ring R is said to be **local** $:\Longleftrightarrow R\backslash R^\times$ is a two-sided ideal of R.

Example 1

(a) Any field K is local because $K\backslash K^\times = \{0\}$ by definition.

(b) Exercise: Let p be a prime number and $R := \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$. Prove that $R\backslash R^\times = \{\frac{a}{b} \in R \mid p|a\}$ and deduce that R is local.

(c) Exercise: Let K be a field and let $R := \left\{A = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & a_1 & \dots & a_{n-1} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & a_1 \end{pmatrix} \in M_n(K)\right\}$. Prove that $R\backslash R^\times = \{A \in R \mid a_1 = 0\}$ and deduce that R is local.

Proposition 5.2

Let R be a ring. Then TFAE:

(a) R is local;

(b) $R\backslash R^\times = J(R)$, i.e. $J(R)$ is the unique maximal left ideal of R;

(c) $R/J(R)$ is a skew-field.

Proof: Set $N := R\backslash R^\times$.

(a)⇒(b): Clear: $I \lhd R$ proper left ideal $\Rightarrow I \subseteq N$. Hence, by Proposition-Definition 4.1(c),

$$J(R) = \bigcap_{\substack{I \lhd R, \\ I \text{ maximal} \\ \text{left ideal}}} I \subseteq N.$$

Now, by (a) N is an ideal of R, hence N must be a maximal left ideal, even the unique one. It follows that $N = J(R)$.

(b)⇒(c): If $J(R)$ is the unique maximal left ideal of R, then in particular $R \neq 0$ and $R/J(R) \neq 0$. So let $r \in R\backslash J(R) \overset{(b)}{=} R^\times$. Then obviously $r + J(R) \in (R/J(R))^\times$. It follows that $R/J(R)$ is a skew-field.

(c)⇒(a): Since $R/J(R)$ is a skew-field by (c), $R/J(R) \neq 0$, so that $R \neq 0$ and there exists $a \in R\backslash J(R)$. Moreover, again by (c), $a + J(R) \in (R/J(R))^\times$, so that $\exists\, b \in R\backslash J(R)$ such that

$$ab + J(R) = 1 + J(R) \in R/J(R)$$

Therefore, $\exists\, c \in J(R)$ such that $ab = 1 - c$, which is invertible in R by Proposition-Definition 4.1(b). Hence $\exists\, d \in R$ such that $abd = (1-c)d = 1 \Rightarrow a \in R^\times$. Therefore $R\backslash J(R) = R^\times$, and it follows that $R\backslash R^\times = J(R)$ which is a two-sided ideal of R. ∎

Proposition 5.3 (*Fitting's Lemma*)

Let M be an R-module which has a composition series and let $\varphi \in \mathrm{End}_R(M)$ be an endomorphism of M. Then there exists $n \in \mathbb{Z}_{>0}$ such that

(i) $\varphi^n(M) = \varphi^{n+i}(M)$ for every $i \geqslant 1$;

(ii) $\ker(\varphi^n) = \ker(\varphi^{n+i})$ for every $i \geqslant 1$; and

(iii) $M = \varphi^n(M) \oplus \ker(\varphi^n)$.

Proof: By Corollary 3.4 the module M satisfies both A.C.C. and D.C.C. on submodules. Hence the two chains of submodules

$$\varphi(M) \supseteq \varphi^2(M) \supseteq \dots,$$
$$\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \dots$$

eventually become stationary. Therefore we can find an index n satisfying both (i) and (ii).

Exercise: Prove that $M = \varphi^n(M) \oplus \ker(\varphi^n)$. ■

Proposition 5.4

Let M be an R-module which has a composition series. Then:

$$M \text{ is indecomposable} \iff \mathrm{End}_R(M) \text{ is a local ring.}$$

Proof: "⇒": Assume that M is indecomposable. Let $\varphi \in \mathrm{End}_R(M)$. Then by Fitting's Lemma there exists $n \in \mathbb{Z}_{>0}$ such that $M = \varphi^n(M) \oplus \ker(\varphi^n)$. As M is indecomposable either $\varphi^n(M) = M$ and $\ker(\varphi^n) = 0$ or $\varphi^n(M) = 0$ and $\ker(\varphi^n) = M$.

- In the first case φ is bijective, hence invertible.
- In the second case φ is nilpotent.

Therefore, $N := \mathrm{End}_R(M) \setminus \mathrm{End}_R(M)^\times = \{\text{nilpotent elements of } \mathrm{End}_R(M)\}$.

Claim: N is a two-sided ideal of $\mathrm{End}_R(M)$.

Let $\varphi \in N$ and $m \in \mathbb{Z}_{>0}$ minimal such that $\varphi^m = 0$. Then

$$\varphi^{m-1}(\varphi\rho) = 0 = (\rho\varphi)\varphi^{m-1} \quad \forall\ \rho \in \mathrm{End}_R(M).$$

As $\varphi^{m-1} \neq 0$, $\varphi\rho$ and $\rho\varphi$ cannot be invertible, hence $\varphi\rho, \rho\varphi \in N$.

Next let $\varphi, \rho \in N$. If $\varphi + \rho =: \psi$ were invertible in $\mathrm{End}_R(M)$, then by the previous argument we would have $\psi^{-1}\rho, \psi^{-1}\varphi \in N$, which would be nilpotent. Hence

$$\psi^{-1}\varphi = \psi^{-1}(\psi - \rho) = \mathrm{Id}_M - \psi^{-1}\rho$$

would be invertible.
(Indeed, $\psi^{-1}\rho$ nilpotent $\Rightarrow (\mathrm{Id}_M - \psi^{-1}\rho)(\mathrm{Id}_M + \psi^{-1}\rho + (\psi^{-1}\rho)^2 + \dots + (\psi^{-1}\rho)^{a-1}) = \mathrm{Id}_M$, where a is minimal such that $(\psi^{-1}\rho)^a = 0$.)
This is a contradiction. Therefore $\varphi + \rho \in N$, which proves that N is an ideal.

Finally, it follows from the Claim and the definition that $\mathrm{End}_R(M)$ is local.

"⇐": Assume M is decomposable and let M_1, M_2 be proper submodules such that $M = M_1 \oplus M_2$. Then consider the two projections

$$\pi_1 : M_1 \oplus M_2 \longrightarrow M_1 \oplus M_2, (m_1, m_2) \mapsto (m_1, 0)$$

onto M_1 along M_2 and

$$\pi_2 : M_1 \oplus M_2 \longrightarrow M_1 \oplus M_2, (m_1, m_2) \mapsto (0, m_2)$$

onto M_2 along M_1. Clearly $\pi_1, \pi_2 \in \mathrm{End}_R(M)$ but $\pi_1, \pi_2 \notin \mathrm{End}_R(M)^\times$ since they are not surjective by construction. Now, as $\pi_2 = \mathrm{Id}_M - \pi_1$ is not invertible it follows from the characterisation of the Jacobson radical of Proposition-Definition 4.1(b) that $\pi_1 \notin J(\mathrm{End}_R(M))$. Therefore

$$\mathrm{End}_R(M) \setminus \mathrm{End}_R(M)^\times \neq J(\mathrm{End}_R(M))$$

and it follows from Proposition 5.2 that $\mathrm{End}_R(M)$ is not a local ring. ■

Next, we want to be able to decompose R-modules into direct sums of indecomposable submodules. The Krull-Schmidt Theorem will then provide us with certain uniqueness properties of such decompositions.

Proposition 5.5

Let M be an R-module. If M satisfies either A.C.C. or D.C.C., then M admits a decomposition into a direct sum of finitely many indecomposable R-submodules.

Proof: Let us assume that M is not expressible as a finite direct sum of indecomposable submodules. Then in particular M is decomposable, so that we may write $M = M_1 \oplus W_1$ as a direct sum of two proper submodules. W.l.o.g. we may assume that the statement is also false for W_1. Then we also have a decomposition $W_1 = M_2 \oplus W_2$, where M_2 and W_2 are proper sumbodules of W_1 with the statement being false for W_2. Iterating this argument yields the following infinite chains of submodules:

$$W_1 \supsetneq W_2 \supsetneq W_3 \supsetneq \cdots,$$

$$M_1 \subsetneq M_1 \oplus M_2 \subsetneq M_1 \oplus M_2 \oplus M_3 \subsetneq \cdots.$$

The first chain contradicts D.C.C. and the second chain contradicts A.C.C.. The claim follows. ■

Theorem 5.6 (*Krull–Schmidt*)

Let M be an R-module which has a composition series. If

$$M = M_1 \oplus \cdots \oplus M_n = M'_1 \oplus \cdots \oplus M'_{n'} \qquad (n, n' \in \mathbb{Z}_{>0})$$

are two decomposition of M into direct sums of finitely many indecomposable R-submodules, then $n = n'$, and there exists a permutation $\pi \in \mathfrak{S}_n$ such that $M_i \cong M'_{\pi(i)}$ for each $1 \leqslant i \leqslant n$ and

$$M = M'_{\pi(1)} \oplus \cdots \oplus M'_{\pi(r)} \oplus \bigoplus_{j=r+1}^{n} M_j \qquad \text{for every } 1 \leqslant r \leqslant n.$$

Proof: For each $1 \leqslant i \leqslant n$ let

$$\pi_i : M = M_1 \oplus \cdots \oplus M_n \to M_i, m_1 + \ldots + m_n \mapsto m_i$$

be the projection on the i-th factor of first decomposition, and for each $1 \leqslant j \leqslant n'$ let

$$\psi_j : M = M'_1 \oplus \cdots \oplus M'_{n'} \to M'_j, m'_1 + \ldots + m'_{n'} \mapsto m'_j$$

be the projection on the j-th factor of second decomposition.

Claim: if $\psi \in \mathrm{End}_R(M)$ is such that $\pi_1 \circ \psi|_{M_1} : M_1 \to M_1$ is an isomorphism, then

$$M = \psi(M_1) \oplus M_2 \oplus \cdots \oplus M_n \text{ and } \psi(M_1) \cong M_1 .$$

Indeed: By the assumption of the claim, both $\psi|_{M_1} : M_1 \to \psi(M_1)$ and $\pi_1|_{\psi(M_1)} : \psi(M_1) \to M_1$ must be isomorphisms. Therefore $\psi(M_1) \cap \ker(\pi_1) = 0$, and for every $m \in M$ there exists $m_1' \in \psi(M_1)$ such that $\pi_1(m) = \pi_1(m_1')$, hence $m - m_1' \in \ker(\pi_1)$. It follows that

$$M = \psi(M_1) + \ker(\pi_1) = \psi(M_1) \oplus \ker(\pi_1) = \psi(M_1) \oplus M_2 \oplus \cdots \oplus M_n .$$

Hence the Claim holds.
Now, we have $\mathrm{Id}_M = \sum_{j=1}^{n'} \psi_j$, and so $\mathrm{Id}_{M_1} = \sum_{j=1}^{n'} \pi_1 \circ \psi_j|_{M_1} \in \mathrm{End}_R(M_1)$. But as M has a composition series, so has M_1, and therefore $\mathrm{End}_R(M_1)$ is local by Proposition 5.4. Thus if all the $\pi_1 \circ \psi_j|_{M_1} \in \mathrm{End}_R(M_1)$ are not invertible, they are all nilpotent and then so is Id_{M_1}, which is in turn not invertible. This is not possible, hence it follows that there exists an index j such that

$$\pi_1 \circ \psi_j|_{M_1} : M_1 \to M_1$$

is an isomorphism and the Claim implies that $M = \psi_j(M_1) \oplus M_2 \oplus \cdots \oplus M_n$ and $\psi_j(M_1) \cong M_1$.
We then set $\pi(1) := j$. By definition $\psi_j(M_1) \subseteq M_j'$ as M_j' is indecomposbale, so that

$$\psi_j(M_1) \cong M_j' = M_{\pi(1)}' .$$

Finally, an induction argument (Exercise!) yields:

$$M = M_{\pi(1)}' \oplus \cdots \oplus M_{\pi(r)}' \oplus \bigoplus_{j=r+1}^{n} M_j,$$

mit $M_{\pi(i)}' \cong M_i$ $(1 \leqslant i \leqslant r)$. In particular, the case $r = n$ implies the equality $n = n'$. ■

Chapter 2. The Structure of Semisimple Algebras

In this chapter we study an important class of rings: the class of rings R which are such that any R-module can be expressed as a direct sum of *simple* R-submodules. We study the structure of such rings through a series of results essentially due to Artin and Wedderburn. At the end of the chapter we will assume that the ring is a finite dimension algebra over a field and start the study of its representation theory.

Notation: throughout this chapter, unless otherwise specified, we let R denote a unital and associative ring.

References:

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons, Inc., New York, 1990.

[Dor72] L. Dornhoff. *Group representation theory. Part B: Modular representation theory.* Marcel Dekker, Inc., New York, 1972.

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

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

6 Semisimplicity of rings and modules

To begin with, we prove three equivalent characterisations for the notion of semisimplicity.

Proposition 6.1

If M is an R-module, then the following assertions are equivalent:

(a) M is semisimple, i.e. $M = \oplus_{i\in I} S_i$ for some family $\{S_i\}_{i\in I}$ of simple R-submodules of M;

(b) $M = \sum_{i\in I} S_i$ for some family $\{S_i\}_{i\in I}$ of simple R-submodules of M;

(c) every R-submodule $M_1 \subseteq M$ admits a complement in M, i.e. $\exists$ an R-submodule $M_2 \subseteq M$ such that $M = M_1 \oplus M_2$.

Proof:

(a)⇒(b): is trivial.

(b)⇒(c): Write $M = \sum_{i\in I} S_i$, where S_i is a simple R-submodule of M for each $i \in I$. Let $M_1 \subseteq M$ be an R-submodule of M. Then consider the family, partially ordered by inclusion, of all subsets $J \subseteq I$ such that

(1) $\sum_{i\in J} S_i$ is a direct sum, and
(2) $M_1 \cap \sum_{i\in J} S_i = 0$.

Clearly this family is non-empty since it contains the empty set. Thus Zorn's Lemma yields the existence of a maximal element J_0. Now, set

$$M' := M_1 + \sum_{i\in J_0} S_i = M_1 \oplus \sum_{i\in J_0} S_i\,,$$

where the second equality holds by (1) and (2). Therefore, it suffices to prove that $M = M'$, i.e. that $S_i \subseteq M'$ for every $i \in I$. But if $j \in I$ is such that $S_j \nsubseteq M'$, the simplicity of S_j implies that $S_j \cap M' = 0$ and it follows that

$$M' + S_j = M_1 \oplus \left(\sum_{i\in J_0} S_i\right) \oplus S_j$$

in contradiction with the maximality of J_0. The claim follows.

(b)⇒(a): follows from the argument above with $M_1 = 0$.

(c)⇒(b): Let M_1 be the sum of all simple R-submodules in M. By (c) there exists a complement $M_2 \subseteq M$ to M_1, i.e. such that $M = M_1 \oplus M_2$. If $M_2 = 0$, we are done. If $M_2 \neq 0$, then M_2 must contain a simple R-submodule (Exercise: prove this fact), say N. But then $N \subseteq M_1$ by definition of M_1, a contradiction. Thus $M_2 = 0$ and so $M = M_1$. ∎

Example 2

(a) The zero module is completely reducible.

(b) If $S_1, \ldots, S_n$ are simple R-modules, then their direct sum $S_1 \oplus \ldots \oplus S_n$ is completely reducible by definition.

(c) The following exercise shows that there exists modules which are not completely reducible.

Exercise (Sheet 1): Let K be a field and let A be the K-algebra $\left\{\left(\begin{smallmatrix} a_1 & a \\ 0 & a_1 \end{smallmatrix}\right) \mid a_1, a \in K\right\}$. Consider the A-module $V := K^2$, where A acts by left matrix multiplication. Prove that:

(1) $\left\{\left(\begin{smallmatrix} x \\ 0 \end{smallmatrix}\right) \mid x \in K\right\}$ is a simple A-submodule of V; but
(2) V is not semisimple.

(d) Exercise (Sheet 1): Prove that any submodule and any quotient of a completely reducible module is again completely reducible.

Theorem-Definition 6.2 (*Semisimple ring*)

A ring R satisfying the following equivalent conditions is called **semisimple**.

(a) All short exact sequences of R-modules split.

(b) All R-modules are semisimple.

(c) All finitely generated R-modules are semisimple.

(d) The regular left R-module R° is semisimple, and is a direct sum of a finite number of minimal left ideals.

Proof: First, (a) and (b) are equivalent as a consequence of Lemma D.4 and the characterisation of semisimple modules given by Proposition 6.1(c). The implication (b) $\Rightarrow$ (c) is trivial, and it is also trivial that (c) implies the first claim of (d), which in turn implies the second claim of (d). Indeed, if $R^\circ = \bigoplus_{i\in I} L_i$ for some family $\{L_i\}_{i\in I}$ of minimal left ideals. Then, by definition of a direct sum, there exists a finite number of indices $i_1, \ldots, i_n \in I$ such that $1_R = x_{i_1} + \ldots + x_{i_n}$ with $x_{i_j} \in L_{i_j}$ for each $1 \leqslant j \leqslant n$. Therefore each $a \in R$ may be expressed in the form

$$a = a \cdot 1_R = ax_{i_1} + \ldots + ax_{i_n}$$

and hence $R^\circ = L_{i_1} + \ldots + L_{i_n}$.
Therefore, it remains to prove that (d) $\Rightarrow$ (b). So, assume that R satisfies (d) and let M be an arbitrary non-zero R-module. Then write $M = \sum_{m\in M} R \cdot m$. Now, each cyclic submodule $R \cdot m$ of M is isomorphic to an R-submodule of R°, which is semisimple by (d). Thus $R \cdot m$ is semisimple as well by Example 2(d). Finally, it follows from Proposition 6.1(b) that M is semisimple. ■

Example 3

Fields are semisimple. Indeed, if V is a finite-dimensional vector space over a field K of dimension n, then choosing a K-basis $\{e_1, \cdots, e_n\}$ of V yields $V = Ke_1 \oplus \ldots \oplus Ke_n$, where $\dim_K(Ke_i) = 1$, hence Ke_i is a simple K-module for each $1 \leqslant i \leqslant n$. Hence, the claim follows from Theorem-Definition 6.2(c).

Corollary 6.3

Let R be a semisimple ring. Then:

(a) R° has a composition series;

(b) R is both left Artinian and left Noetherian.

Proof:

(a) By Theorem-Definition 6.2(d) the regular module R° admits a direct sum decomposition into a finite number of minimal left ideals. Removing one ideal at a time, we obtain a composition series for R°.

(b) Since R° has a composition series, it satisfies both D.C.C. and A.C.C. on submodules by Corollary 3.4. In other words, R is both left Artinian and left Noetherian. ■

Next, we show that semisimplicity is detected by the Jacobson radical. This leads us to introduce a slightly weaker concept: the notion of *J-semisimplicity*.

Definition 6.4 (*J-semimplicity*)

A ring R is said to be **J-semisimple** if $J(R) = 0$.

Exercise 6.5 (*Sheet 1*)

Let $R = \mathbb{Z}$. Prove that $J(\mathbb{Z}) = 0$, but not all $\mathbb{Z}$-modules are semisimple. In other words, $\mathbb{Z}$ is J-semisimple but not semisimple.

Proposition 6.6

Any left Artinian ring R is J-semisimple if and only if it is semisimple.

Proof: "$\Rightarrow$": Assume $R \neq 0$ and R is not semisimple. Pick a minimal left ideal $I_0 \trianglelefteq R$ (e.g. a minimal element of the family of non-zero principal left ideals of R). Then $0 \neq I_0 \neq R$ since I_0 seen as an R-module is simple.

Claim: I_0 is a direct summand of R°.
Indeed: since

$$I_0 \neq 0 = J(R) = \bigcap_{\substack{I \lhd R, \\ I \text{ maximal} \\ \text{left ideal}}} I$$

there exists a maximal left ideal $\mathfrak{m}_0 \lhd R$ which does not contain I_0. Thus $I_0 \cap \mathfrak{m}_0 = \{0\}$ and so we must have $R^\circ = I_0 \oplus \mathfrak{m}_0$, as $R/\mathfrak{m}_0$ is simple. Hence the Claim.

Notice that then $\mathfrak{m}_0 \neq 0$, and pick a minimal left ideal I_1 in $\mathfrak{m}_0$. Then $0 \neq I_1 \neq \mathfrak{m}_0$, else R would be semisimple. The Claim applied to I_1 yields that I_1 is a direct summand of R°, hence also in $\mathfrak{m}_0$. Therefore, there exists a non-zero left ideal $\mathfrak{m}_1$ such that $\mathfrak{m}_0 = I_1 \oplus \mathfrak{m}_1$. Iterating this process, we obtain an infinite descending chain of ideals

$$\mathfrak{m}_0 \supsetneq \mathfrak{m}_1 \supsetneq \mathfrak{m}_2 \supsetneq \cdots$$

contradicting D.C.C.

"$\Leftarrow$": Conversely, if R is semisimple, then $R^\circ \cong R/J(R) \oplus J(R)$ by Theorem-Definition 6.2 and so as R-modules,

$$J(R) = J(R) \cdot (R/J(R) \oplus J(R)) = J(R) \cdot J(R)$$

so that by Nakayama's Lemma $J(R) = 0$.

■

Proposition 6.7

The quotient ring $R/J(R)$ is J-semisimple.

Proof: Since by Exercise 4.2 the rings R and $\overline{R} := R/J(R)$ have the same simple modules (seen as abelian groups), Proposition-Definition 4.1(a) yields:

$$J(\overline{R}) = \bigcap_{\substack{V \text{simple} \\ \overline{R}\text{-module}}} \operatorname{ann}_{\overline{R}}(V) = \bigcap_{\substack{V \text{simple} \\ R\text{-module}}} \operatorname{ann}_R(V) + J(R) = J(R)/J(R) = 0$$

■

7 The Artin-Wedderburn structure theorem

The next step in analysing semisimple rings and modules is to sort simple modules into isomorphism classes. We aim at proving that each isomorphism type of simple modules actually occurs as a direct summand of the regular module. The first key result in this direction is the following proposition:

Proposition 7.1

Let M be a semisimple R-module. Let $\{M_i\}_{i\in I}$ be a set of representatives of the isomorphism classes of simple R-submodules of M and for each $i \in I$ set

$$H_i := \sum_{\substack{V\subseteq M\\ V\cong M_i}} V\,.$$

Then the following statements hold:

(i) $M \cong \bigoplus_{i\in I} H_i$;

(ii) every simple R-submodule of H_i is isomorphic to M_i;

(iii) $\mathrm{Hom}_R(H_i, H_{i'}) = \{0\}$ if $i \neq i'$; and

(iv) if $M = \bigoplus_{j\in J} V_j$ is an arbitrary decomposition of M into a direct sum of simple submodules, then

$$\widetilde{H}_i := \sum_{\substack{j\in J\\ V_j\cong M_i}} V_j = \bigoplus_{\substack{j\in J\\ V_j\cong M_i}} V_j = H_i\,.$$

Proof: We shall prove several statements which, taken together, will establish the theorem.

Claim 1: If $M = \bigoplus_{j\in J} V_j$ as in (iv) and W is an arbitrary simple R-submodule of M, then $\exists\ j \in J$ such that $W \cong V_j$.
Indeed: if $\{\pi_j : M = \bigoplus_{j\in J} V_j \longrightarrow V_j\}_{j\in J}$ denote the canonical projections on the j-th summand, then $\exists\ j \in J$ such that $\pi_j(W) \neq 0$. Hence $\pi_j|_W : W \longrightarrow V_j$ is an R-isomorphism as both W and V_j are simple.

Claim 2: If $M = \bigoplus_{j\in J} V_j$ as in (iv), then $M = \bigoplus_{i\in I} \widetilde{H}_i$ and for each $i \in I$, every simple R-submodule of $\widetilde{H}_i$ is isomorphic to M_i.
Indeed: the 1st statement of the claim is obvious and the 2nd statement follows from Claim 1 applied to $\widetilde{H}_i$.

Claim 3: If W is an arbitrary simple R-submodule of M, then there is a unique $i \in I$ such that $W \subseteq \widetilde{H}_i$.
Indeed: it is clear that there is a unique $i \in I$ such that $W \cong M_i$. Now consider $w \in W\backslash\{0\}$ and write $w = \sum_{j\in J} w_j \in \bigoplus_{j\in J} V_j$ with $w_j \in V_j$. The proof of Claim 1 shows that if any summand $w_j \neq 0$, then $\pi_j(W) \neq 0$, and hence $W \cong V_j$. Therefore $w_j = 0$ unless $V_j \cong M_i$, and hence $w \in \widetilde{H}_i$, so that $W \subseteq \widetilde{H}_i$.

Claim 4: $\mathrm{Hom}_R(\widetilde{H}_i, \widetilde{H}_{i'}) = \{0\}$ if $i \neq i'$.
Indeed: if $0 \neq f \in \mathrm{Hom}_R(\widetilde{H}_i, \widetilde{H}_{i'})$ and $i \neq i'$, then there must exist a simple R-submodule W of $\widetilde{H}_i$ such that $f(W) \neq 0$, hence as W is simple, $f|_W : W \longrightarrow f(W)$ is an R-isomorphism. It follows from Claim 2, that $f(W)$ is a simple R-submodule of $\widetilde{H}_{i'}$ isomorphic to M_i. This contradicts Claim 2 saying that every simple R-submodule of $\widetilde{H}_{i'}$ is isomorphic to $M_{i'} \ncong M_i$.

Now, it is clear that $\widetilde{H}_i \subseteq H_i$ by definition. On the other hand it follows from Claim 3, that $H_i \subseteq \widetilde{H}_i$. Hence $H_i = \widetilde{H}_i$ for each $i \in I$, hence (iv). Then Claim 2 yields (i) and (ii), and Claim 4 yields (iii). ∎

We give a name to the submodules $\{H_i\}_{i\in I}$ defined in Propostion 7.1:

Definition 7.2

(a) If M is a semisimple R-module and S is a simple R-module, then the **S-homogeneous component** of M, denoted $S(M)$, is the sum of all simple R-submodules of M isomorphic to S.

(b) We let $\mathcal{M}(R)$ denote a set of representatives of the isomorphism classes of simple R-modules.

Exercise 7.3 (*Sheet 2*)

Let R be a semisimple ring. Prove the following statements.

(a) Every non-zero left ideal I of R is generated by an **idempotent** of R, in other words $\exists\, e \in R$ such that $e^2 = e$ and $I = Re$. (Hint: choose a complement I' for I, so that $R^\circ = I \oplus I'$ and write $1 = e + e'$ with $e \in I$ and $e' \in I'$. Prove that $I = Re$.)

(b) If I is a non-zero left ideal of R, then every morphism in $\mathrm{Hom}_R(I, R^\circ)$ is given by right multiplication with an element of R.

(c) If $e \in R$ is an idempotent, then $\mathrm{End}_R(Re) \cong (eRe)^{\mathrm{op}}$ (the opposite ring) as rings via the map $f \mapsto ef(e)e$. In particular $\mathrm{End}_R(R^\circ) \cong R^{\mathrm{op}}$ via $f \mapsto f(1)$.

(d) A left ideal Re generated by an idempotent e of R is minimal (i.e. simple as an R-module) if and only if eRe is a division ring. (Hint: Use Schur's Lemma.)

(e) Every simple left R-module is isomorphic to a minimal left ideal in R, i.e. a simple R-submodule of R°.

We recall that:

Definition 7.4 (*Centre*)

The **centre** of a ring $(R, +, \cdot)$ is $Z(R) := \{a \in R \mid a \cdot x = x \cdot a \ \ \forall\, x \in R\}$.

Theorem 7.5 (*Wedderburn*)

If R is a semisimple ring, then the following assertions hold.

(a) If $S \in \mathcal{M}(R)$, then $S(R^\circ) \neq 0$. Furthermore, $|\mathcal{M}(R)| < \infty$.

(b) We have

$$R^\circ = \bigoplus_{S \in \mathcal{M}(R)} S(R^\circ)\,,$$

where each homogenous component $S(R^\circ)$ is a two-sided ideal of R and $S(R^\circ)T(R^\circ) = 0$ if $S \neq T \in \mathcal{M}(R)$.

(c) Each $S(R^\circ)$ is a simple left Artinian ring, the identity element of which is an idempotent element of R lying in $Z(R)$.

Proof:

(a) By Exercise 7.3(e) every simple left R-module is isomorphic to a minimal left ideal of R, i.e. a simple submodule of R°. Hence if $S \in \mathcal{M}(R)$, then $S(R^\circ) \neq 0$. Now, by Theorem-Definition 6.2, the regular module admits a decomposition

$$R^\circ = \bigoplus_{j \in J} V_j$$

into a direct sum of a finite number of minimal left ideals V_j of R, and by Claim 1 in the proof of Proposition 7.1 any simple submodule of R° is isomorphic to V_j for some $j \in J$. Hence $|\mathcal{M}(R)| < \infty$.

(b) Proposition 7.1(iv) also yields $S(R^\circ) = \bigoplus_{V_j \cong S} V_j$ and Proposition 7.1(i) implies that

$$R^\circ = \bigoplus_{S \in \mathcal{M}(R)} S(R^\circ)\,.$$

Next notice that each homogeneous component is a left ideal of R, since it is by definition a sum of left ideals. Now let L be a minimal left ideal contained in $S(R^\circ)$, and let $x \in T(R^\circ)$ for a $T \in \mathcal{M}(R)$ with $S \neq T$. Then $Lx \subseteq T(R^\circ)$ and because $\varphi_x : R^\circ \longrightarrow R^\circ, m \mapsto mx$ is an R-endomorphism of R°, then either $Lx = \varphi_x(L)$ is zero or it is again a minimal left ideal, isomorphic to L. However, as $S \neq T$, we have $Lx = 0$. Therefore $S(R^\circ)T(R^\circ) = 0$, which implies that $S(R^\circ)$ is also a right ideal, hence two-sided.

(c) Part (b) implies that the homogeneous components are rings. Then, using Exercise 7.3(a), we may write $1_R = \sum_{S \in \mathcal{M}(R)} e_S$, where $S(R^\circ) = Re_S$ with e_S idempotent. Since $S(R^\circ)$ is a two-sided ideal, in fact $S(R^\circ) = Re_S = e_S R$. It follows that e_S is an identity element for $S(R^\circ)$.
To see that e_S is in the centre of R, consider an arbitrary element $a \in R$ and write $a = \sum_{T \in \mathcal{M}(R)} a_T$ with $a_T \in T(R^\circ)$. Since $S(R^\circ)T(R^\circ) = 0$ if $S \neq T \in \mathcal{M}(R)$, we have $e_S e_T = \delta_{ST}$. Thus, as e_T is an identity element for the T-homogeneous component, we have

$$\begin{aligned} e_S a &= e_S \sum_{T \in \mathcal{M}(R)} a_T = e_S \sum_{T \in \mathcal{M}(R)} e_T a_T = \sum_{T \in \mathcal{M}(R)} e_S e_T a_T \\ &= e_S a_S \\ &= a_S e_S \\ &= \sum_{T \in \mathcal{M}(R)} a_T e_T e_S = \Big(\sum_{T \in \mathcal{M}(R)} a_T e_T\Big) e_S = \Big(\sum_{T \in \mathcal{M}(R)} a_T\Big) e_S = a e_S\,. \end{aligned}$$

Finally, if $L \neq 0$ is a two-sided ideal in $S(R^\circ)$, then L must contain all the minimal left ideals of R isomorphic to S as a consequence of Exercise 7.3 (check it!). It follows that $L = S(R^\circ)$ and therefore $S(R^\circ)$ is a simple ring. It is left Artinian, because it is semissimple as an R-module. ■

Scholium 7.6

If R is a semisimple ring, then there exists a set of idempotent elements $\{e_S \mid S \in \mathcal{M}(R)\}$ such that

(i) $e_S \in Z(R)$ for each $S \in \mathcal{M}(R)$;

(ii) $e_S e_T = \delta_{ST} e_S$ for all $S, T \in \mathcal{M}(R)$;

(iii) $1_R = \sum_{S \in \mathcal{M}(R)} e_S$;

(iv) $R = \bigoplus_{S \in \mathcal{M}(R)} Re_S$, where each Re_S is a simple ring.

Idempotents satisfying Property (i) are called **central** idempotents, and idempotents satisfying Property (ii) are called **orthogonal**.

Remark 7.7

Remember that if R is a semisimple ring, then the regular module R° admits a composition series. Therefore it follows from the Jordan-Hölder Theorem that

$$R^\circ = \bigoplus_{S \in \mathcal{M}(R)} S(R^\circ) \cong \bigoplus_{S \in \mathcal{M}(R)} \bigoplus_{i=1}^{n_S} S$$

for uniquely determined integers $n_S \in \mathbb{Z}_{>0}$.

Theorem 7.8 (*Artin-Wedderburn*)

If R is a semisimple ring, then, as a ring,

$$R \cong \prod_{S \in \mathcal{M}(R)} M_{n_S}(D_S)\,,$$

where $D_S := \mathrm{End}_R(S)^{\mathrm{op}}$ is a division ring.

Before we proceed with the proof of the theorem, first recall that if we have a direct sum decomposition $U = U_1 \oplus \cdots \oplus U_r$ ($r \in \mathbb{Z}_{>0}$), then $\mathrm{End}_R(U)$ is isomorphic to the ring of $r \times r$-matrices in which the (i,j) entry lies in $\mathrm{Hom}_R(U_j, U_i)$. This is because any R-endomorphism $\phi : U \longrightarrow U$ may be written as a matrix of components $\phi = (\phi_{ij})_{1 \leqslant i,j \leqslant r}$ where $\phi_{ij} : U_j \xrightarrow{inc.} U \xrightarrow{\phi} U \xrightarrow{proj.} U_i$, and when viewed in this way R-endomorphisms compose in the manner of matrix multiplication. (Known from the GDM-lecture if R is a field. The same holds over an arbitrary ring R.)

Proof: By Exercise 7.3(c), we have

$$\mathrm{End}_R(R^\circ) \cong R^{\mathrm{op}}$$

as rings. On the other hand, since $\mathrm{Hom}_R(S(R^\circ), T(R^\circ)) = 0$ for $S \ncong T$ (e.g. by Schur's Lemma, or by Proposition 7.1), the above observation yields

$$\mathrm{End}_R(R^\circ) \cong \prod_{S \in \mathcal{M}(R)} \mathrm{End}_R(S(R^\circ))$$

where $\mathrm{End}_R(S(R^\circ)) \cong M_{n_S}(\mathrm{End}_R(S)) \cong M_{n_S}(\mathrm{End}_R(S)^{\mathrm{op}})^{\mathrm{op}}$. Therefore, setting $D_S := \mathrm{End}_R(S)^{\mathrm{op}}$ yields the result. For by Schur's Lemma $\mathrm{End}_R(S)$ is a division ring, hence so is the opposite ring. ■

8 Semisimple algebras and their simple modules

From now on we leave the theory of modules over arbitrary rings and focus on finite-dimensional algebras over a field K. Algebras are in particular rings, and since K-algebras and their modules are in particular K-vector spaces, we may consider their dimensions to obtain further information. In particular, we immediately see that finite-dimensional K-algebras are necessarily left Artinian rings. Furthermore, the structure theorems of the previous section tell us that if A is a semisimple algebra over a field K, then

$$A^\circ = \bigoplus_{S \in \mathcal{M}(A)} S(A^\circ) \cong \bigoplus_{S \in \mathcal{M}(A)} \bigoplus_{i=1}^{n_S} S$$

where n_S corresponds to the multiplicity of the isomorphism class of the simple module S as a direct summand of A° in any given decomposition of A° into a finite direct sum of simple submodules. We shall

see that over an algebraically closed field the number of simple A-modules is detected by the centre of A and also obtain information about the simple modules of algebras, which are not semisimple.

Exercise 8.1 (*Sheet 2*)

Let A be an arbitrary K-algebra over a commutative ring K.

(a) Prove that $Z(A)$ is a K-subalgebra of A.

(b) Prove that if K is a field and $A \neq 0$, then $K \longrightarrow Z(A), \lambda \mapsto \lambda 1_A$ is an injective K-homomorphism.

(c) Prove that if $A = M_n(K)$, then $Z(A) = K\mathrm{I}_n$, i.e. the K-subalgebra of scalar matrices. (Hint: use the standard basis of $M_n(K)$.)

(d) Assume A is the algebra of 2×2 upper-triangular matrices over K. Prove that

$$Z(A) = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix} \right) \mid a \in K \right\} .$$

We obtain the following Corollary to Wedderburn's and Artin-Wedderburn's Theorems:

Theorem 8.2

Let A be a semisimple finite-dimensional algebra over an algebraically closed field K, and let $S \in \mathcal{M}(A)$ be a simple A-module. Then the following statements hold:

(a) $S(A^\circ) \cong M_{n_S}(K)$ and $\dim_K(S(A^\circ)) = n_S^2$;

(b) $\dim_K(S) = n_S$;

(c) $\dim_K(A) = \sum_{S \in \mathcal{M}(A)} \dim_K(S)^2$;

(d) $|\mathcal{M}(A)| = \dim_K(Z(A))$.

Proof:

(a) Since $K = \overline{K}$, Schur's Lemma implies that $\mathrm{End}_A(S) \cong K$. Hence the division ring D_S in the statement of the Artin-Wedderburn Theorem is $D_S = \mathrm{End}_A(S)^{\mathrm{op}} \cong K^{\mathrm{op}} = K$. Hence Artin-Wedderburn (and its proof) applied to the case $R = S(A^\circ)$ yields $S(A^\circ) \cong M_{n_S}(K)$. Hence $\dim_K(S(A^\circ)) = n_S^2$.

(b) Since $S(A^\circ)$ is a direct sum of n_S copies of S, (a) yields:

$$n_S^2 = n_S \cdot \dim_K(S) \quad \Longrightarrow \quad \dim_K(S) = n_S$$

(c) follows directly from (a) and (b).

(d) Since by Artin-Wedderburn and (a) we have $A \cong \prod_{S \in \mathcal{M}(A)} M_{n_S}(K)$, clearly

$$Z(A) \cong \prod_{S \in \mathcal{M}(A)} Z(M_{n_S}(K)) = \prod_{S \in \mathcal{M}(A)} K\mathrm{I}_{n_S} ,$$

where $\dim_K(K\mathrm{I}_{n_S}) = 1$. The claim follows. ∎

Corollary 8.3

Let A be a finite-dimensional algebra over an algebraically closed field K. Then the number of simple A-modules is equal to $\dim_K(Z(A/J(A)))$.

Proof: We have observed that A and $A/J(A)$ have the same simple modules (see Exercise 4.2), hence $|\mathcal{M}(A)| = |\mathcal{M}(A/J(A))|$. Moreover, the quotient $A/J(A)$ is J-semisimple by Proposition 6.7, hence semisimple by Proposition 6.6 because finite-dimensional algebras are left Artinian rings. Therefore it follows from Theorem 8.2(d) that

$$|\mathcal{M}(A)| = |\mathcal{M}(A/J(A))| = \dim_K \left(Z(A/J(A))\right).$$

■

Corollary 8.4

Let A be a finite-dimensional algebra over an algebraically closed field K. If A is commutative, then any simple A-module has K-dimension 1.

Proof: First assume that A is semisimple. As A is commutative, $A = Z(A)$. Hence parts (d) and (c) of Theorem 8.2 yield

$$|\mathcal{M}(A)| = \dim_K(A) = \sum_{S \in \mathcal{M}(A)} \underbrace{\dim_K(S)^2}_{\geqslant 1},$$

which forces $\dim_K(S) = 1$ for each $S \in \mathcal{M}(A)$.
Now, if A is not semissimple, then again we use the fact that A and $A/J(A)$ have the same simple modules (that is seen as abelian groups). Because $A/J(A)$ is semisimple and also commutative, the argument above tells us that all simple $A/J(A)$-modules have K-dimension 1. The claim follows. ■

Finally, we emphasise that in this section the assumption that the field K is algebraically closed is in general too strong and that it is possible to weaken this hypothesis so that Theorem 8.2, Corollary 8.3 and Corollary 8.4 still hold.

Indeed, if $K = \overline{K}$ is algebraically closed, then Part (b) of Schur's Lemma tells us that $\mathrm{End}_A(S) \cong K$ for any simple A-module S. This is the crux of the proof of Theorem 8.2. The following terminology describes this situation.

Definition 8.5

Let A be a finite-dimensional K-algebra. Then:

(a) A is called **split** if $\mathrm{End}_A(S) \cong K$ for every simple A-module S; and

(b) an extension field K' of K is called a **splitting field for** A if the K'-algebra $K' \otimes_K A$ is split.

Of course if A is split then K itself is a splitting field for A.

Remark 8.6

In fact for a finite-dimensional K-algebra A, the following assertions are equivalent:

(a) A is split;

(b) the product, for S running through $\mathcal{M}(A)$, of the structural homomorphisms $A \longrightarrow \mathrm{End}_K(S)$

(mapping $a \in A$ to the K-linear map $S \longrightarrow S, m \mapsto am$) induces an isomorphism of K-algebras

$$A/J(A) \cong \prod_{S \in \mathcal{M}(A)} \mathrm{End}_K(S)\,.$$

This is a variation of the Artin-Wedderburn Theorem we have seen in the previous section.

Chapter 3. Representation Theory of Finite Groups

Representation theory of finite groups is originally concerned with the ways of writing a finite group G as a group of matrices, that is using group homomorphisms from G to the general linear group $\mathrm{GL}_n(K)$ of invertible $n \times n$-matrices with coefficients in a field K for some positive integer n. Thus, we shall first define representations of groups using this approach. Our aim is then to translate such homomorphisms $G \longrightarrow \mathrm{GL}_n(K)$ into the language of module theory in order to be able to apply the theory we have developed so far. In particular, our first aim is to understand what the general theory of semisimple rings and the Artin-Wedderburn theorem bring to the theory of representations of finite groups.

Notation: throughout this chapter, unless otherwise specified, we let G denote a finite group and K be a commutative ring. Moreover, in order to simplify some arguments, we assume that all KG-modules considered are **free of finite rank** when regarded as K-modules. (This implies, in particular, that they are **finitely generated** as KG-modules.)

References:

[Alp86] J. L. Alperin. *Local representation theory*. Vol. 11. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1986.

[Ben98] D. J. Benson. *Representations and cohomology. I*. Vol. 30. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1998.

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. John Wiley & Sons, Inc., New York, 1990.

[Dor72] L. Dornhoff. *Group representation theory. Part B: Modular representation theory*. Marcel Dekker, Inc., New York, 1972.

[LP10] K. Lux and H. Pahlings. *Representations of groups*. Vol. 124. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2010.

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

9 Linear representations of finite groups

To begin with, we review elementary definitions and examples about representations of finite groups.

Definition 9.1 (*K-representation, matrix representation*)

(a) A **K-representation** of G is a group homomorphism $\rho : G \longrightarrow \mathrm{GL}(V)$, where $V \cong K^n$ ($n \in \mathbb{Z}_{\geqslant 0}$) is a free K-module of finite rank and $\mathrm{GL}(V) := \mathrm{Aut}_K(V)$.

(b) A **matrix representation** of G over K is a group homomorphism $X : G \longrightarrow \mathrm{GL}_n(K)$ ($n \in \mathbb{Z}_{\geqslant 0}$).

In both cases the integer n is called the **degree** of the representation.

(c) If K is a field, then a K-representation (resp. a matrix representation) is called an **ordinary representation** if $\mathrm{char}(K) = 0$ (or more generally if $\mathrm{char}(K) \nmid |G|$), and it is called a **modular representation** if $\mathrm{char}(K) \mid |G|$.

Remark 9.2

Both concepts of a representation and of a matrix representation are closely related. Indeed, recall that every choice of a basis B of V yields a group isomorphism

$$\alpha_B : GL(V) \longrightarrow \mathrm{GL}_n(K), \varphi \mapsto (\varphi)_B$$

(where $(\varphi)_B$ denotes the matrix of φ w.r.t. the basis B). Thus, a K-representation $\rho : G \longrightarrow \mathrm{GL}(V)$ together with the choice of a basis B of V gives rise to a matrix representation of G:

$$G \xrightarrow{\rho} \mathrm{GL}(V) \xrightarrow{\alpha_B} \mathrm{GL}_n(K)$$

Conversely, any matrix representation $X : G \longrightarrow \mathrm{GL}_n(K)$ gives rise to a K-representation

$$\begin{array}{rccl} \rho\colon & G & \longrightarrow & \mathrm{GL}(K^n) \\ & g & \mapsto & \rho(g) : K^n \longrightarrow K^n, v \mapsto X(g)v \ , \end{array}$$

namely we set $V = K^n$, see v as a column vector expressed in the standard basis of K^n and $X(g)v$ denotes the standard matrix multiplication.

Example 4

(a) If G is an arbitrary finite group, then

$$\begin{array}{rccl} \rho\colon & G & \longrightarrow & \mathrm{GL}(K) \cong K^\times \\ & g & \mapsto & \rho(g) := \mathrm{Id}_K \leftrightarrow 1_K \end{array}$$

is a K-representation of G, called **the trivial representation** of G.

(b) If X is a finite G-set, i.e. a finite set endowed with a left action $\cdot : G \times X \longrightarrow X$, and V is a free K-module with basis $\{e_x \mid x \in X\}$, then

$$\begin{array}{rccl} \rho_X\colon & G & \longrightarrow & \mathrm{GL}(V) \\ & g & \mapsto & \rho_X(g) : V \longrightarrow V, e_x \mapsto e_{g\cdot x} \end{array}$$

is a K-representation of G, called the **permutation representation** associated with X.

Two particularly interesting examples are the following:

(1) if $G = S_n$ ($n \geqslant 1$) is the symmetric group on n letters and and $X = \{1, 2, \ldots, n\}$ then ρ_X is called **natural representation** of S_n;

(2) if $X = G$ and the left action $\cdot : G \times X \longrightarrow X$ is just the multiplication in G, then $\rho_X =: \rho_{\text{reg}}$ is called the **regular representation** of G.

Definition 9.3 (*Homomorphism of representations, equivalent representations*)

Let $\rho_1 : G \longrightarrow \mathrm{GL}(V_1)$ and $\rho_2 : G \longrightarrow \mathrm{GL}(V_2)$ be two K-representations of G, where V_1, V_2 are two non-zero free K-modules of finite rank.

(a) A K-homomorphism $\alpha : V_1 \longrightarrow V_2$ such that $\rho_2(g) \circ \alpha = \alpha \circ \rho_1(g)$ for each $g \in G$ is called a **homomorphism of representations** (or a **G-homomorphism**) between ρ_1 and ρ_2.

$$\begin{array}{ccc} V_1 & \xrightarrow{\rho_1(g)} & V_1 \\ {\scriptstyle\alpha}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\alpha} \\ V_2 & \xrightarrow[\rho_2(g)]{} & V_2 \end{array}$$

(b) If, moreover, α is a K-isomorphism, then it is called an **isomorphism of representations** (or a **G-isomorphism**), and the K-representations ρ_1 and ρ_2 are called **equivalent** (or **similar**, or **isomorphic**). In this case we write $\rho_1 \sim \rho_2$.

Remark 9.4

(a) Equivalent representations have the same degree.

(b) Clearly $\sim$ is an equivalence relation.

(c) In consequence, it essentially suffices to study representations up to equivalence (as it essentially suffices to study groups up to isomorphism).

Definition 9.5 (*G-invariant subspace, irreducibility*)

Let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a K-representation of G.

(a) A K-submodule $W \subseteq V$ is called **G-invariant** if

$$\rho(g)\big(W\big) \subseteq W \qquad \forall g \in G\,.$$

(In fact in this case the reverse inclusion holds as well, since for each $w \in W$ we can write $w = \rho(gg^{-1})(w) = \rho(g)\big(\rho(g^{-1})(w)\big) \in \rho(g)\big(W\big)$, hence $\rho(g)\big(W\big) = W$.)

(b) The representation ρ is called **irreducible** if it admits exactly two G-invariant K-submodules, namely 0 and V itself; it is called **reducible** if there exists a proper non-zero G-invariant K-submodule $0 \leqslant W \subseteq V$.

Notice that V itself and the zero K-module 0 are always G-invariant.

Definition 9.6 (*Subrepresentation*)

If $\rho : G \longrightarrow \mathrm{GL}(V)$ is a K-representation and $W \subseteq V$ is a G-invariant K-submodule, then

$$\begin{array}{rccl} \rho_W : & G & \longrightarrow & \mathrm{GL}(W) \\ & g & \mapsto & \rho_W(g) := \rho(g)|_W : W \longrightarrow W \end{array}$$

is called a **subrepresentation** of ρ. (This is clearly again a K-representation of G.)

With this definition, it is clear that a representation $\rho : G \longrightarrow \mathrm{GL}(V)$ is *irreducible* if and only if ρ does not possess any non-trivial proper subrepresentation.

10 The group algebra and its modules

We now want to be able to see K-representations of a group G as *modules*, and more precisely as *modules* over a K-algebra depending on the group G, which is called the *group algebra*:

Lemma-Definition 10.1 (*Group algebra*)

The **group ring** KG is the ring whose elements are the K-linear combinations $\sum_{g\in G} \lambda_g g$ with $\lambda_g \in K\ \forall g \in G$, and addition and multiplication are given by

$$\sum_{g\in G} \lambda_g g + \sum_{g\in G} \mu_g g = \sum_{g\in G} (\lambda_g + \mu_g) g \quad \text{and} \quad \Big(\sum_{g\in G} \lambda_g g\Big) \cdot \Big(\sum_{h\in G} \mu_h h\Big) = \sum_{g,h\in G} (\lambda_g \mu_h) gh$$

respectively. Thus KG is a K-algebra, which as a K-module is free with basis G. Hence we usually call KG the **group algebra of G over K** rather than simply *group ring*.

Proof: By definition KG is a free K-module with basis G, and the multiplication in G is extended by K-bilinearity to the given multiplication $\cdot : KG \times KG \longrightarrow KG$. It is then straightforward that KG bears both the structures of a ring and of a K-module. Finally, axiom (A3) of K-algebras follows directly from the definition of the multiplication and the commutativity of K. ■

Remark 10.2

Clearly:

- $1_{KG} = 1_G$;
- the K-rank of KG is $|G|$;
- KG is commutative if and only if G is an abelian group;
- if K is a field, or more generally (left) Artinian, then KG is a left Artinian ring, so that by Hopkins' Theorem a KG-module is finitely generated if and only if it admits a composition series.

Also notice that since G is a group, the map $KG \longrightarrow KG$ defined by $g \mapsto g^{-1}$ for each $g \in G$ is an anti-automorphism. It follows that any *left* KG-module M may be regarded as a *right* KG-module via the right G-action $m \cdot g := g^{-1} \cdot m$. Thus the sidedness of KG-modules is not usually an issue.

As KG is a K-algebra, we may of course consider modules over KG and we recall that any KG-module is in particular a K-module. Moreover, we adopt the following convention, which is automatically satisfied if K is a field.

Convention: in the sequel all KG-modules considered are assumed to be free of finite rank when regarded as K-modules.

Proposition 10.3

(a) Any K-representation $\rho : G \longrightarrow \mathrm{GL}(V)$ of G gives rise to a KG-module structure on V, where the external composition law is defined by the map

$$\begin{array}{rccc} \cdot : & G \times V & \longrightarrow & V \\ & (g, v) & \mapsto & g \cdot v := \rho(g)(v) \end{array}$$

extended by K-linearity to the whole of KG.

(b) Conversely, every KG-module $(V, +, \cdot)$ defines a K-representation

$$\begin{array}{rccc} \rho_V : & G & \longrightarrow & \mathrm{GL}(V) \\ & g & \mapsto & \rho_V(g) : V \longrightarrow V, v \mapsto \rho_V(g) := g \cdot v \end{array}$$

of the group G.

Proof: (a) Since V is a K-module it is equipped with an internal addition $+$ such that $(V, +)$ is an abelian group. It is then straightforward to check that the given external composition law defined above verifies the KG-module axioms.

(b) A KG-module is in particular a K-module for the scalar multiplication defined for all $\lambda \in K$ and all $v \in V$ by

$$\lambda v := (\underbrace{\lambda 1_G}_{\in KG}) \cdot v \,.$$

Moreover, it follows from the KG-module axioms that $\rho_V(g) \in \mathrm{GL}(V)$ and also that

$$\rho_V(g_1 g_2) = \rho_V(g_1) \circ \rho_V(g_2)$$

for all $g_1, g_2 \in G$, hence ρ_V is a group homomorphism. ■

Example 5

Via Proposition 10.3 the trivial representation (Example 4(a)) corresponds to the so-called **trivial KG-module**, that is the commutative ring K itself seen as a KG-module via the G-action

$$\begin{array}{rcl} \cdot : G \times K & \longrightarrow & K \\ (g, \lambda) & \longmapsto & g \cdot \lambda := \lambda \end{array}$$

extended by K-linearity to the whole of KG.

Exercise 10.4

Prove that the regular representation ρ_{reg} of G defined in Exampale 4(b)(2) corresponds to the regular KG-module KG° via Proposition 10.3.

Convention: In the sequel, when no confusion is to be made, we drop the $\circ$-notation to denote the regular KG-module and simply write KG instead of KG°.

Lemma 10.5

Two representations $\rho_1 : G \longrightarrow \mathrm{GL}(V_1)$ and $\rho_2 : G \longrightarrow \mathrm{GL}(V_2)$ are equivalent if and only if $V_1 \cong V_2$ as KG-modules.

Proof: If $\rho_1 \sim \rho_2$ and $\alpha : V_1 \longrightarrow V_2$ is a K-isomorphism such that $\rho_2(g) = \alpha \circ \rho_1(g) \circ \alpha^{-1}$ for each $g \in G$, then by Proposition 10.3 for every $v \in V_1$ and every $g \in G$ we have

$$g \cdot \alpha(v) = \rho_2(g)(\alpha(v)) = \alpha(\rho_1(g)(v)) = \alpha(g \cdot v)\,,$$

hence α is a KG-isomorphism. Conversely, if $\alpha : V_1 \longrightarrow V_2$ is a KG-isomorphism, then certainly it is a K-homomorphism and for each $g \in G$ and by Proposition 10.3 for each $v \in V_2$ we have

$$\alpha \circ \rho_1(g) \circ \alpha^{-1}(v) = \alpha(\rho_1(g)(\alpha^{-1}(v)) = \alpha(g \cdot \alpha^{-1}(v)) = g \cdot \alpha(\alpha^{-1}(v)) = g \cdot v = \rho_2(g)(v)\,,$$

hence $\rho_2(g) = \alpha \circ \rho_1(g) \circ \alpha^{-1}$ for each $g \in G$. ■

Remark 10.6 (*Dictionary*)

More generally, through Proposition 10.3, we may transport terminology and properties from KG-modules to K-representations and conversely.
This lets us build the following translation **dictionary**:

K-Representations		KG-Modules
K-representation of G	$\longleftrightarrow$	KG-module
degree	$\longleftrightarrow$	K-rank
homomorphism of K-representations	$\longleftrightarrow$	homomorphism of KG-modules
equivalent K-representations	$\longleftrightarrow$	isomorphism of KG-modules
subrepresentation	$\longleftrightarrow$	KG-submodule
direct sum of representations $\rho_{V_1} \oplus \rho_{V_2}$	$\longleftrightarrow$	direct sum of KG-modules $V_1 \oplus V_2$
irreducible representation	$\longleftrightarrow$	simple (= irreducible) KG-module
the trivial representation	$\longleftrightarrow$	the trivial KG-module K
the regular representation of G	$\longleftrightarrow$	the regular KG-module KG
completely reducible K-representation	$\longleftrightarrow$	semisimple KG-module (= completely reducible)
every K-representation of G is completely reducible	$\longleftrightarrow$	KG is semisimple
...		...

Finally we introduce an ideal of KG which encodes a lot of information about KG-modules.

Proposition-Definition 10.7 (*The augmentation ideal*)

The map $\varepsilon : KG \longrightarrow K, \sum_{g\in G} \lambda_g g \mapsto \sum_{g\in G} \lambda_g$ is an algebra homomorphism, called **augmentation homomorphism (or map)**. Its kernel $\ker(\varepsilon) =: I(KG)$ is an ideal and it is called the **augmentation ideal** of KG. The following statements hold:

(a) $I(KG) = \{\sum_{g\in G} \lambda_g g \in KG \mid \sum_{g\in G} \lambda_g = 0\} = \mathrm{ann}_{KG}(K)$ and if K is a field $I(KG) \supseteq J(KG)$;

(b) $KG/I(KG) \cong K$ as K-algebras;

(c) $I(KG)$ is a free K-module of rank $|G|$-1 with K-basis $\{g - 1 \mid g \in G\backslash\{1\}\}$;

Proof: Clearly, the map $\varepsilon : KG \longrightarrow K$ is the unique extension by K-linearity of the trivial representation $G \longrightarrow K^\times \subseteq K, g \mapsto 1_K$ to KG, hence is an algebra homomorphism and its kernel is an ideal of the algebra KG.

(a) $I(KG) = \ker(\varepsilon) = \{\sum_{g\in G} \lambda_g g \in KG \mid \sum_{g\in G} \lambda_g = 0\}$ by definition of ε. The second equality is obvious by definition of $\mathrm{ann}_{KG}(K)$, and the last inclusion follows from the definition of the Jacobson radical.

(b) follows from the 1st isomorphism theorem.

(c) Let $\sum_{g\in G} \lambda_g g \in I(KG)$. Then $\sum_{g\in G} \lambda_g = 0$ and hence

$$\sum_{g\in G} \lambda_g g = \sum_{g\in G} \lambda_g g - 0 = \sum_{g\in G} \lambda_g g - \sum_{g\in G} \lambda_g = \sum_{g\in G} \lambda_g (g-1) = \sum_{g\in G\backslash\{1\}} \lambda_g (g-1)\,,$$

which proves that the set $\{g - 1 \mid g \in G\backslash\{1\}\}$ generates $I(KG)$ as a K-module. The above computations also show that

$$\sum_{g\in G\backslash\{1\}} \lambda_g (g-1) = 0 \quad \Longrightarrow \quad \sum_{g\in G} \lambda_g g = 0$$

Hence $\lambda_g = 0 \; \forall\, g \in G$, which proves that the set $\{g-1 \mid g \in G\backslash\{1\}\}$ is also K-linearly independent, hence a K-basis of $I(KG)$. ■

Lemma 10.8

If K is a field of positive characteristic p and G is p-group, then $I(KG) = J(KG)$.

Exercise 10.9 (*Proof of Lemma 10.8. Proceed as indicated.*)

(a) Recall that an ideal I of a ring R is called a **nil ideal** if each element of I is nilpotent. Accept the following result: if I is a nil left ideal in a left Artinian ring R then I is nilpotent.

(b) Prove that $g - 1$ is a nilpotent element for each $g \in G\backslash\{1\}$ and deduce that $I(KG)$ is a nil ideal of KG.

(c) Deduce from (a) and (b) that $I(KG) \subseteq J(KG)$ using Exercise 3 on Exercise Sheet 2.

(d) Conclude that $I(KG) = J(KG)$ using Proposition-Definition 10.7.

11 Semisimplicity and Maschke's Theorem

Throughout this section, we assume that K is a field.

Our first aim is to prove that the semisimplicity of the group algebra depends on both the characteristic of the field and the order of the group.

Theorem 11.1 (*Maschke*)

If $\mathrm{char}(K) \nmid |G|$, then KG is a semisimple K-algebra.

Proof: By Theorem-Definition 6.2, we need to prove that every s.e.s. $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ of KG-modules splits. However, the field K is clearly semisimple (again by Proposition-Definition 6.2). Hence any such sequence regarded as a s.e.s. of K-vector spaces and K-linear maps splits. So let $\sigma : N \longrightarrow M$ be a K-linear section for ψ and set

$$\widetilde{\sigma} := \tfrac{1}{|G|}\textstyle\sum_{g\in G} g^{-1}\sigma g : \quad \begin{array}{ccc} N & \longrightarrow & M \\ n & \mapsto & \frac{1}{|G|}\sum_{g\in G} g^{-1}\sigma(gn). \end{array}$$

We may divide by $|G|$, since $\mathrm{char}(K) \nmid |G|$ implies that $|G| \in K^\times$. Now, if $h \in G$ and $n \in N$, then

$$\widetilde{\sigma}(hn) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\sigma(ghn) = h\frac{1}{|G|}\sum_{g\in G}(gh)^{-1}\sigma(ghn) = h\widetilde{\sigma}(n)$$

and

$$\psi\widetilde{\sigma}(n) = \frac{1}{|G|}\sum_{g\in G}\psi\left(g^{-1}\sigma(gn)\right) \overset{\psi\ KG\text{-lin}}{=} \frac{1}{|G|}\sum_{g\in G} g^{-1}\psi\sigma(gn) = \frac{1}{|G|}\sum_{g\in G} g^{-1}gn = n\,,$$

where the last-but-one equality holds because $\psi\sigma = \mathrm{Id}_N$. Thus $\widetilde{\sigma}$ is a KG-linear section for ψ. ∎

Example 6

If $K = \mathbb{C}$ is the field of complex numbers, then $\mathbb{C}G$ is a semisimple $\mathbb{C}$-algebra, since $\mathrm{char}(\mathbb{C}) = 0$.

It turns out that the converse to Maschke's theorem also holds, and follows from the properties of the augmentation ideal.

Theorem 11.2 (*Converse of Maschke's Theorem*)

If KG is a semisimple K-algebra, then $\mathrm{char}(K) \nmid |G|$.

Proof: Set $\mathrm{char}(K) =: p$ and let us assume that $p \mid |G|$. In particular p must be a prime number. We have to prove that then KG is not semisimple.

Claim: If $0 \neq V \subset KG$ is a KG-submodule of KG°, then $V \cap I(KG) \neq 0$.

Indeed: Let $v = \sum_{g\in G}\lambda_g g \in V\backslash\{0\}$. If $\varepsilon(v) = 0$ we are done. Else, set $t := \sum_{h\in G} h$. Then

$$\varepsilon(t) = \sum_{h\in G} 1 = |G| = 0$$

as $\mathrm{char}(K) \mid |G|$. Hence $t \in I(KG)$. Now consider the element tv. On the one hand $tv \in V$ since V is a submodule of KG°, and on the other hand $tv \in I(KG)\backslash\{0\}$ since

$$tv = \Big(\sum_{h\in G} h\Big)\Big(\sum_{g\in G}\lambda_g g\Big) = \sum_{h,g\in G}(1_K\cdot\lambda_g)hg = \sum_{x\in G}\Big(\sum_{g\in G}\lambda_g\Big)x = \sum_{x\in G}\varepsilon(v)x \;\Rightarrow\; \varepsilon(tv) = \sum_{x\in G}\varepsilon(v) = |G|\varepsilon(v) = 0\,.$$

The Claim implies that $I(KG)$, which is a KG-submodule by definition, cannot have a complement in KG°. Therefore, by Proposition 6.1, KG° is not semisimple and hence KG is not semisimple by Theorem-Definition 6.2. ■

In the case in which the field K is algebraically closed, or a splitting field for KG, the following exercise offers a second proof of the converse of Maschke's Theorem exploiting the Artin-Wedderburn Theorem (Theorem 8.2).

Exercise 11.3 (*Proof of the Converse of Maschke's Theorem for K splitting field for KG.*)

Assume K is a field of positive characteristic p with $p \mid |G|$ and is a splitting field for KG. Set $T := \langle \sum_{g \in G} g \rangle_K$.

(a) Prove that we have a series of KG-submodules given by $KG^\circ \supsetneq I(KG) \supseteq T \supsetneq 0$.

(b) Deduce that KG° has at least two composition factors isomorphic to the trivial module K.

(c) Deduce that KG is not a semisimple K-algebra using Theorem 8.2.

12 Simple modules over splitting fields

Assumption 12.1

Throughout this section, we assume that K is a splitting field for KG, and we simply say that K **is a splitting field for** G.

As explained at the end of Chapter 2 this assumption, slightly weaker than requiring that $K = \overline{K}$, implies that the conclusions of Theorem 8.2, Corollary 8.3 and Corollary 8.4 still hold.

Corollary 12.2

If K is a splitting field for G, then there are only finitely many isomorphism classes of simple KG-modules.

Proof: The claim follows directly from Assumption 12.1 and Corollary 8.3. ■

Corollary 12.3

If G is an abelian group and K is a splitting field for G, then any simple KG-module is one-dimensional.

Proof: Since KG is commutative the claim follows directly from Assumption 12.1 and Corollary 8.4. ■

Corollary 12.4

Let p be a prime number. If G is a p-group, K is a splitting field for G and $\mathrm{char}(K) = p$, then the trivial module is the unique simple KG-module, up to isomorphism.

Proof: By Lemma 10.8 we have $J(KG) = I(KG)$. Thus $KG/J(KG) \cong K$ as K-algebras by Proposition-Definition 10.7(b). Now, as K is commutative, $Z(K) = K$, and it follows from Assumption 12.1 and Corollary 8.3 that

$$|\mathcal{M}(KG)| = \dim_K Z(KG/J(KG)) = \dim_K K = 1\,.$$

■

Remark 12.5

Another standard proof for Corollary 12.4 consists in using a result of Brauer's stating that $|\mathcal{M}(KG)|$ equals the number of conjugacy classes of G of order not divisible by the characteristic of the field K.

Corollary 12.6

If K is a splitting field for G and $\mathrm{char}(K) \nmid |G|$, then $|G| = \sum_{S \in \mathcal{M}(KG)} \dim_K(S)^2$.

Proof: Since $\mathrm{char}(K) \nmid |G|$, the group algebra KG is semisimple by Maschke's Theorem. Thus it follows from Assumption 12.1 and Theorem 8.2 that

$$\sum_{S \in \mathcal{M}(KG)} \dim_K(S)^2 = \dim_K(KG) = |G|\,.$$

■

Chapter 4. Operations on Groups and Modules

In this chapter we show how to construct new KG-modules from old ones using standard module operations such as tensor products, Hom-functors, duality, or using subgroups or quotients of the initial group. Moreover, we study how these constructions relate to each other.

Notation: throughout this chapter, unless otherwise specified, we let G denote a finite group and K be a commutative ring. All modules over group algebras considered are assumed to be **free of finite rank as K-modules**.

References:

[Alp86] J. L. Alperin. *Local representation theory*. Vol. 11. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1986.

[Ben98] D. J. Benson. *Representations and cohomology. I*. Vol. 30. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1998.

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. John Wiley & Sons, Inc., New York, 1990.

[LP10] K. Lux and H. Pahlings. *Representations of groups*. Vol. 124. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2010.

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

13 Tensors, Hom's and duality

Definition 13.1 (*Tensor product of KG-modules*)

If M and N are two KG-modules, then the tensor product $M \otimes_K N$ of M and N balanced over K becomes a KG-module via the **diagonal action** of G. In other words, the external composition law is defined by the G-action

$$\begin{array}{rccc} \cdot : & G \times (M \otimes_K N) & \longrightarrow & M \otimes_K N \\ & (g, m \otimes n) & \mapsto & g \cdot (m \otimes n) := gm \otimes gn \end{array}$$

extended by K-linearity to the whole of KG.

Definition 13.2 (Homs)

If M and N are two KG-modules, then the abelian group $\mathrm{Hom}_K(M,N)$ becomes a KG-module via the so-called **conjugation action** of G. In other words, the external composition law is defined by the G-action

$$\begin{array}{rccl} \cdot: & G \times \mathrm{Hom}_K(M,N) & \longrightarrow & \mathrm{Hom}_K(M,N) \\ & (g,f) & \mapsto & g \cdot f : M \longrightarrow N, m \mapsto (g\cdot f)(m) := g \cdot f(g^{-1}\cdot m) \end{array}$$

extended by K-linearity to the whole of KG.

Specifying Definition 13.2 to $N = K$ yields a KG-module structure on the K-dual $M^* = \mathrm{Hom}_K(M,K)$.

Definition 13.3 (*Dual of a KG-module*)

(a) If M is a KG-module, then its K-dual M^* becomes a KG-module via the external composition law is defined by the map

$$\begin{array}{rccl} \cdot: & G \times M^* & \longrightarrow & M^* \\ & (g,f) & \mapsto & g \cdot f : M \longrightarrow K, m \mapsto (g\cdot f)(m) := f(g^{-1}\cdot m) \end{array}$$

extended by K-linearity to the whole of KG.

(b) If M, N are KG-modules, then every KG-homomorphism $\rho \in \mathrm{Hom}_{KG}(M,N)$ induces a KG-homomorphism

$$\begin{array}{rccl} \rho^*: & N^* & \longrightarrow & M^* \\ & f & \mapsto & \rho^*(f) : M \longrightarrow K, m \mapsto \rho^*(f)(m) := f \circ \rho(m)\,. \end{array}$$

(See Propotion D.3.)

Lemma 13.4

If M and N are KG-modules, then $\mathrm{Hom}_K(M,N) \cong M^* \otimes_K N$ as KG-modules.

Proof: The map

$$\begin{array}{rccl} \theta := \theta_{M,N}: & M^* \otimes_K N & \longrightarrow & \mathrm{Hom}_K(M,N) \\ & f \otimes n & \mapsto & \theta(f\otimes n) : M \longrightarrow N, m \mapsto \theta(f\otimes n)(m) = f(m)n \end{array}$$

defines a K-isomorphism. (Check it!)
Now, for every $g \in G$, $f \in M^*$, $n \in N$ and $m \in M$, we have on the one hand

$$\begin{aligned} \theta(g\cdot(f\otimes n))(m) = \theta(g\cdot f \otimes g\cdot n))(m) &= (g\cdot f)(m) g\cdot n \\ &= f(g^{-1}\cdot m) g\cdot n \end{aligned}$$

and on the other hand

$$\big(g\cdot\theta(f\otimes n)\big)(m) = g\cdot\big(\theta(f\otimes n)(g^{-1}m)\big) = g\cdot\big(f(g^{-1}m)n\big) = f(g^{-1}\cdot m) g\cdot n\,,$$

hence $\theta(g\cdot(f\otimes n)) = \big(g\cdot\theta(f\otimes n)\big)$ and it follows that θ is in fact a KG-isomorphism. ∎

Remark 13.5

In case $M = N$ the above constructions yield a KG-module structure on $\mathrm{End}_K(M) \cong M^* \otimes_K M$. Moreover, if $\mathrm{rk}_K(M) =: n$, $\{m_1, \dots, m_n\}$ is a K-basis of M and $\{m_1^*, \dots, m_n^*\}$ is the dual K-basis, then $\mathrm{Id}_M \in \mathrm{End}_K(M)$ corresponds to the element $\mathsf{r} := \sum_{i=1}^n m_i^* \otimes m_i \in M^* \otimes_K M$. (Exercise!)
This allows us to define the KG-homomorphism:

$$\begin{array}{rccc} \mathsf{I}\colon & K & \longrightarrow & M^* \otimes_K M \\ & 1 & \mapsto & \mathsf{r} \end{array}$$

Definition 13.6 (*Trace map*)

If M is a KG-module, then the **trace map** associated to M is the KG-homomorphism

$$\begin{array}{rccc} \mathrm{Tr}_M\colon & M^* \otimes_K M & \longrightarrow & K \\ & f \otimes m & \mapsto & f(m)\,. \end{array}$$

Notation 13.7

If M and N are KG-modules, we shall write $M \mid N$ to mean that M is isomorphic to a direct summand of N.

Lemma 13.8

If $\mathrm{rk}_K(M) \in K^\times$, then $K \mid M^* \otimes_K M$.

Proof: By Lemma-Definition D.4(c) it suffices to check that $\frac{1}{\mathrm{rk}_K(M)}\mathsf{I}$ is a KG-section for Tr_M, because then $M^* \otimes_K M \cong \ker(\mathrm{Tr}_M) \oplus K$, hence $K \mid M^* \otimes_K M$. So let $\lambda \in K$. Then

$$\begin{aligned} \left[\mathrm{Tr}_M \circ \frac{1}{\mathrm{rk}_K(M)}\mathsf{I}\right](\lambda) = \frac{1}{\mathrm{rk}_K(M)}\mathrm{Tr}_M(\lambda r) &= \frac{\lambda}{\mathrm{rk}_K(M)}\mathrm{Tr}_M\Big(\sum_{i=1}^n m_i^* \otimes m_i\Big) \\ &= \frac{\lambda}{\mathrm{rk}_K(M)} \sum_{i=1}^n m_i^*(m_i) \\ &= \frac{\lambda}{\mathrm{rk}_K(M)} \sum_{i=1}^n 1 = \lambda\,. \end{aligned}$$

Hence $\mathrm{Tr}_M \circ \frac{1}{\mathrm{rk}_K(M)}\mathsf{I} = \mathrm{Id}_K$. ∎

Exercise 13.9

Assume K is a field (to simplify) and let M,N be KG-modules. Prove the following assertions:

(a) $M \cong (M^*)^*$ as KG-modules (in a natural way);

(b) $M^* \oplus N^* \cong (M \oplus N)^*$ and $M^* \otimes_K N^* \cong (M \otimes_K N)^*$ as KG-modules (in a natural way);

(c) M is simple, resp. indecomposable, resp. semisimple, if and only if M^* is simple, resp. indecomposable, resp. semisimple;

(d) Tr_M is a KG-homomorohism and $\mathrm{Tr}_M \circ \theta_{M,M}^{-1}$ coincides with the ordinary trace of matrices;

(e) $M \mid M \otimes_K M^* \otimes_K M$, and if char(K) $\mid \dim_K(M)$, then $M \oplus M \mid M \otimes_K M^* \otimes_K M$. (This is more challenging!)

Can (a) to (e) be generalised to the case in which K is an arbitrary commutative ring and M and N free of finite rank when seen as K-modules ?

14 Fixed and cofixed points

Fixed and cofixed points explain why in the previous section we considered tensor products and Hom's over K and not over KG.

Definition 14.1 (*G-fixed points and G-cofixed points*)

Let M be a KG-module.

(a) The G-**fixed points** of M are by definition $M^G := \{m \in M \mid g \cdot m = m \ \forall\, g \in G\}$.

(b) The G-**cofixed points** of M are by definition $M_G := M/(I(KG) \cdot M)$.

In other words:

- M^G is the largest KG-submodule of M on which G acts trivially, and
- M_G is the largest quotient of M on which G acts trivially.

Lemma 14.2

If M, N are KG-modules, then $\mathrm{Hom}_K(M,N)^G = \mathrm{Hom}_{KG}(M,N)$ and $(M \otimes_K N)_G \cong M \otimes_{KG} N$.

Proof: A K-linear map $f : M \longrightarrow N$ is a morphism of KG-modules if and only if $f(g \cdot m) = g \cdot f(m)$ for all $g \in G$ and all $m \in M$, that is if and only if $g^{-1} \cdot f(g \cdot m) = f(m)$ for all $g \in G$ and all $m \in M$. This is exactly the condition that f is fixed under the action of G. Hence $\mathrm{Hom}_K(M,N)^G = \mathrm{Hom}_{KG}(M,N)$.
Second claim: similar, Exercise! ∎

Exercise 14.3

Let K be a field and let $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ be a s.e.s. of KG-modules. Prove that if $M \cong L \oplus N$, then the s.e.s. splits.

[Hint: Consider the exact sequence induced by the functor $\mathrm{Hom}_{KG}(N, -)$ (as in Proposition D.3(a)) and use the fact that the modules considered are all finite-dimensional.]

15 Inflation, restriction and induction

In this section we define new module structures from known ones for subgroups, overgroups and quotients, and investigate how these relate to each other.

Remark 15.1

(a) If $H \leqslant G$ is a subgroup, then the inclusion $H \longrightarrow G, h \mapsto h$ can be extended by K-linearity to an injective algebra homomorphism $\iota : KH \longrightarrow KG, \sum_{h \in H} \lambda_h h \mapsto \sum_{h \in H} \lambda_h h$. Hence KH is a K-subalgebra of KG.

(b) Similarly, if $U \trianglelefteq G$ is a normal subgroup, then the quotient homomorphism $G \longrightarrow G/U$, $g \mapsto gU$ can be extended by K-linearity to an algebra homomorphism $\pi : KG \longrightarrow K[G/U]$.

It is clear that we can always perform changes of the base ring using the above homomorphism in order to obtain new module structures. This yields two natural operations on modules over group algebras called *inflation* and *restriction*.

Definition 15.2 (*Restriction*)

Let $H \leqslant G$ be a subgroup. If M is a KG-module, then M may be regarded as a KH-module through a change of the base ring along $\iota : KH \longrightarrow KG$, which we denote by $\mathrm{Res}^G_H(M)$ or simply $M{\downarrow}^G_H$ and call the **restriction** of M from G to H.

Definition 15.3 (*Inflation*)

Let $U \trianglelefteq G$ be a normal subgroup. If M is a $K[G/U]$-module, then M may be regarded as a KG-module through a change of the base ring along $\pi : KG \longrightarrow K[G/U]$, which we denote by $\mathrm{Inf}^G_{G/U}(M)$ and call the **inflation** of M from G/U to G.

Remark 15.4

(a) If $H \leqslant G$ is a subgroup, M is a KG-module and $\rho : G \longrightarrow GL(M)$ is the associated K-representation, then the K-representation associated to $M{\downarrow}^G_H$ is simply the composite morphism

$$H \xrightarrow{\iota} G \xrightarrow{\rho} GL(M)\,.$$

(b) Similarly, if $U \trianglelefteq G$ is a normal subgroup, M is a $K[G/U]$-module and $\rho : G/U \longrightarrow GL(M)$ is the associated K-representation, then the K-representation associated to $\mathrm{Inf}^G_{G/U}(M)$ is simply

$$G \xrightarrow{\pi} G/U \xrightarrow{\rho} GL(M)\,.$$

Lemma 15.5

(a) If $H \leqslant G$ and M_1, M_2 are two KG-modules, then $(M_1 \oplus M_2){\downarrow}^G_H = M_1{\downarrow}^G_H \oplus M_2{\downarrow}^G_H$. If $U \trianglelefteq G$ and M_1, M_2 are two $K[G/U]$-modules, then $\mathrm{Inf}^G_{G/U}(M_1 \oplus M_2) = \mathrm{Inf}^G_{G/U}(M_1) \oplus \mathrm{Inf}^G_{G/U}(M_2)$.

(b) **(Transitivity of restriction)** If $L \leqslant H \leqslant G$ and M is a KG-module, then $M{\downarrow}^G_H{\downarrow}^H_L = M{\downarrow}^G_L$.

(c) If $H \leqslant G$ and M is a KG-module, then $(M^*){\downarrow}^G_H \cong (M{\downarrow}^G_H)^*$. If $U \trianglelefteq G$ and M is a $K[G/U]$-module, then $\mathrm{Inf}^G_{G/U}(M^*) \cong (\mathrm{Inf}^G_{G/U} M)^*$.

Proof:

(a) Straightforward from the fact that the external composition law on a direct sum is defined componentwise.

(b) If $\iota_{L,H} : L \longrightarrow H$ denotes the canonical inclusion of L in H, $\iota_{H,G} : H \longrightarrow G$ the canonical inclusion of H in G and $\iota_{L,G} : L \longrightarrow G$ the canonical inclusion of L in G, then

$$\iota_{H,G} \circ \iota_{L,H} = \iota_{L,G}\,.$$

Thus performing a change of the base ring via $\iota_{L,G}$ is the same as performing two successive changes of the base ring via first $\iota_{H,G}$ and then $\iota_{L,H}$. Hence $M{\downarrow}^G_H{\downarrow}^H_L = M{\downarrow}^G_L$.

(c) Straightforward. ∎

A third natural operation comes from extending scalars from a subgroup to the initial group.

Definition 15.6 (*Induction*)

Let $H \leqslant G$ be a subgroup and let M be a KH-module. Regarding KG as a (KG, KH)-bimodule, we define the **induction** of M from H to G to be the left KG-module

$$\mathrm{Ind}_H^G(M) := KG \otimes_{KH} M\,.$$

We shall also write $M{\uparrow}^G_H$ instead of $\mathrm{Ind}_H^G(M)$.

Example 7

(a) If $H = \{1\}$ and $M = K$, then $K{\uparrow}^G_{\{1\}} = KG \otimes_K K \cong KG$.

(b) **Transitivity of induction**: clearly $L \leqslant H \leqslant G$ and M is a KL-module, then $M{\uparrow}^G_L = (M{\uparrow}^H_L){\uparrow}^G_H$ by the associativity of the tensor product.

First, we analyse the structure of an induced module in terms of the left cosets of H.

Remark 15.7

Recall that $G/H = \{gH \mid g \in G\}$ denotes the set of left cosets of H in G. Moreover, we write $[G/H]$ for a set of representatives of these left cosets. In other words, $[G/H] = \{g_1, \ldots, g_{|G:H|}\}$ (where we assume that $g_1 = 1$) for elements $g_1, \ldots, g_{|G:H|} \in G$ such that $g_iH \neq g_jH$ if $i \neq j$ and G is the disjoint union of the left cosets of H, so that

$$G = \bigsqcup_{g \in [G/H]} gH = g_1H \sqcup \ldots \sqcup g_{|G:H|}H\,.$$

It follows that

$$KG = \bigoplus_{g \in [G/H]} gKH\,,$$

where $gKH = \{g \sum_{h \in H} \lambda_h h \mid \lambda_h \in K \ \forall\, h \in H\}$. Clearly, $gKH \cong KH$ as *right* KH-modules via $gh \mapsto h$ for each $h \in H$. Therefore

$$KG \cong \bigoplus_{g \in [G/H]} KH = (KH)^{|G:H|}$$

and hence is a free *right* KH-module with a KH-basis given by the left coset representatives in $[G/H]$.

In consequence, if M is a given KH-module, then we have

$$KG \otimes_{KH} M = \Big(\bigoplus_{g \in [G/H]} gKH\Big) \otimes_{KH} M = \bigoplus_{g \in [G/H]} (gKH \otimes_{KH} M) = \bigoplus_{g \in [G/H]} (g \otimes M)\,,$$

where we set

$$g \otimes M := \{g \otimes m \mid m \in M\} \subseteq KG \otimes_{KH} M\,.$$

Clearly, each $g \otimes M$ is isomorphic to M as a K-module via the K-isomorphism

$$g \otimes M \longrightarrow M, g \otimes m \mapsto m\,.$$

It follows that

$$\mathrm{rk}_K(\mathrm{Ind}_H^G(M)) = |G : H| \cdot \mathrm{rk}_K(M)\,.$$

Next we see that with its left action on $KG \otimes_{KH} M$, the group G permutes these K-submodules: for if $x \in G$, then $xg_i = g_j h$ for some $h \in H$, and hence

$$x \cdot (g_i \otimes m) = xg_i \otimes m = g_j h \otimes m = g_j \otimes hm\,.$$

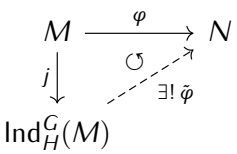
This action is also clearly transitive since for every $1 \leqslant i, j \leqslant |G : H|$ we can write

$$g_j g_i^{-1}(g_i \otimes M) = g_j \otimes M\,.$$

Exercise: Check that the stabiliser of $g_1 \otimes M$ is H (where $g_1 = 1$) and deduce that the stabiliser of $g_i \otimes M$ is $g_i H g_i^{-1}$.

Proposition 15.8 (*Universal property of the induction*)

Let $H \leqslant G$, let M be a KH-module and let $j : M \longrightarrow KG \otimes_{KH} M, m \mapsto 1 \otimes m$ be the canonical map (which in fact a KH-homomorphism). Then, for every KG-module N and for every KH-homomorphism $\varphi : M \longrightarrow \mathrm{Res}_H^G(N)$, there exists a unique KG-homomorphism $\tilde{\varphi} : KG \otimes_{KH} M \longrightarrow N$ such that $\tilde{\varphi} \circ j = \varphi$, or in other words such that the following diagram commutes:



Proof: The universal property of the tensor product yields the existence of a well-defined homomorphism of abelian groups

$$\begin{array}{rccc} \tilde{\varphi}: & KG \otimes_{KH} M & \longrightarrow & N \\ & a \otimes m & \mapsto & a \cdot \varphi(m)\ . \end{array}$$

which is obviously KG-linear. Moreover, for each $m \in M$, we have $\tilde{\varphi} \circ j(m) = \tilde{\varphi}(1 \otimes m) = 1 \cdot \varphi(m) = \varphi(m)$, hence $\tilde{\varphi} \circ j = \varphi$. Finally the uniqueness follows from the fact for each $a \in KG$ and each $m \in M$, we have

$$\tilde{\varphi}(a \otimes m) = \tilde{\varphi}(a \cdot (1 \otimes m)) = a \cdot \tilde{\varphi}(1 \otimes m) = a \cdot (\tilde{\varphi} \circ j(m)) = a \cdot \varphi(m)$$

hence there is a unique possible definition for $\tilde{\varphi}$. ■

Induced modules can be hard to understand from first principles, so we now develop some formalism that will enable us to compute with them more easily.

To begin with, there is, in fact, a further operation that relates the modules over a group G and a subgroup H called *coinduction*. Given a KH-module M, then the **coinduction** of M from H to G is the left KG-module

$$\mathrm{Coind}_H^G(M) := \mathrm{Hom}_{KH}(KG, M)$$

where the left KG-module structure is defined through the natural right KG-module structure of KG, i.e. for $g \in G$:

$$\begin{array}{rccl} \cdot : & KG \times \mathrm{Hom}_{KH}(KG, M) & \longrightarrow & \mathrm{Hom}_{KH}(KG, M) \\ & (g, \theta) & \mapsto & g \cdot \theta : KG \longrightarrow M, x \mapsto (g \cdot \theta)(x) := \theta(x \cdot g) \end{array}$$

Example 8

If $H = \{1\}$ and $M = K$, then $\mathrm{Coind}_{\{1\}}^G(K) \cong (KG)^*$ (i.e. with the KG-module structure on $(KG)^*$ of Definition 13.3).

Exercise: exhibit a KG-isomorphism between the coinduction of K from $\{1\}$ to G and $(KG)^*$.

Now, we see that the operation of coinduction in the context of group algebras is just a disguised version of the induction functor.

Lemma 15.9 (*Induction and coinduction are the same*)

If $H \leqslant G$ is a subgroup and M is a KH-module, then $KG \otimes_{KH} M \cong \mathrm{Hom}_{KH}(KG, M)$ as KG-modules. In particular, $KG \cong (KG)^*$ as KG-modules.

Proof: Mutually inverse KG-isomorphisms are defined by:

$$\begin{array}{rccll} \Phi : & KG \otimes_{KH} M & \longrightarrow & \mathrm{Hom}_{KH}(KG, M) & \\ & g \otimes m & \mapsto & \Phi_{g \otimes m} & (\text{for } g \in G,\ m \in M) \end{array}$$

where $\Phi_{g\otimes m} : KG \longrightarrow M$ is such that for $s \in G$, $\Phi_{g\otimes m}(s) := sgm$ if $sg \in H$ and $\Phi_{g\otimes m}(s) := 0$ if $sg \notin H$; and

$$\begin{array}{rccl} \Psi : & \mathrm{Hom}_{KH}(KG, M) & \longrightarrow & KG \otimes_{KH} M \\ & \theta & \mapsto & \sum_{g \in [G/H]} g \otimes \theta(g^{-1}) \,. \end{array}$$

It follows that in the case in which $H = \{1\}$ and $M = K$,

$$KG \cong KG \otimes_K K \cong \mathrm{Hom}_K(KG, K) \cong (KG)^*$$

as KG-modules. Here we emphasise that the last isomorphism isn't an equality. See the previous example. ∎

Theorem 15.10 (*Adjunction / Frobenius reciprocity / Nakayama relations*)

Let $H \leqslant G$ be a subgroup. Let N be a KG-module and let M be a KH-module. Then, there are K-isomorphisms:

(a) $\mathrm{Hom}_{KH}(M, \mathrm{Hom}_{KG}(KG, N)) \cong \mathrm{Hom}_{KG}(KG \otimes_{KH} M, N)$,
or in other words, $\mathrm{Hom}_{KH}(M, N{\downarrow}_H^G) \cong \mathrm{Hom}_{KG}(M{\uparrow}_H^G, N)$;

(b) $\mathrm{Hom}_{KH}(N{\downarrow}_H^G, M) \cong \mathrm{Hom}_{KG}(N, M{\uparrow}_H^G)$.

Proof:

(a) Since induction and coinduction coincide, we have $\mathrm{Hom}_{KG}(KG, N) \cong KG \otimes_{KG} N \cong N$ as KG-modules. Therefore, $\mathrm{Hom}_{KG}(KG, N) \cong N{\downarrow}^G_H$ as KH-modules, and it suffices to prove the second isomorphism. In fact, this K-isomorphism is given by the map

$$\begin{array}{rccc} \Phi: & \mathrm{Hom}_{KH}(M, N{\downarrow}^G_H) & \longrightarrow & \mathrm{Hom}_{KG}(M{\uparrow}^G_H, N) \\ & \varphi & \mapsto & \tilde{\varphi} \end{array}$$

where $\tilde{\varphi}$ is the KG-homomorphism induced by φ by the universal property of the induction. Since $\tilde{\varphi}$ is the unique KG-homomorphism such that $\tilde{\varphi} \circ j = \varphi$, setting

$$\begin{array}{rccc} \Psi: & \mathrm{Hom}_{KG}(M{\uparrow}^G_H, N) & \longrightarrow & \mathrm{Hom}_{KH}(M, N{\downarrow}^G_H) \\ & \psi & \mapsto & \psi \circ j \end{array}$$

provides us with an inverse map for Φ. Finally, it is straightforward to check that both Φ and Ψ are K-linear.

(b) Exercise: check that the so-called *exterior trace map*

$$\begin{array}{rccc} \widehat{\mathrm{Tr}}^G_H: & \mathrm{Hom}_{KH}(N{\downarrow}^G_H, M) & \longrightarrow & \mathrm{Hom}_{KG}(N, M{\uparrow}^G_H) \\ & \varphi & \mapsto & \widehat{\mathrm{Tr}}^G_H(\varphi): N \longrightarrow M{\uparrow}^G_H, n \mapsto \sum_{g \in [G/H]} g \otimes \varphi(g^{-1}n) \end{array}$$

provides us with the required K-isomorphism. ∎

Proposition 15.11

Let $H \leqslant G$ be a subgroup. Let N be a KG-module and let M be a KH-module. Then, there are KG-isomorphisms:

(a) $(M \otimes_K N{\downarrow}^G_H){\uparrow}^G_H \cong M{\uparrow}^G_H \otimes_K N$; and

(b) $\mathrm{Hom}_K(M, N{\downarrow}^G_H){\uparrow}^G_H \cong \mathrm{Hom}_K(M{\uparrow}^G_H, N)$.

Proof: (a) It follows from the associativity of the tensor product that

$$(M \otimes_K N{\downarrow}^G_H){\uparrow}^G_H = KG \otimes_{KH} (M \otimes_K N{\downarrow}^G_H) \cong (KG \otimes_{KH} M) \otimes_K N = M{\uparrow}^G_H \otimes_K N$$

(b) We push back the proof until we have introduced the concept of an H-free module. (We will then prove that if M is a KH-module, then $(M^*){\uparrow}^G_H \cong (M{\uparrow}^G_H)^*$ and (b) will follow directly from (a) and the KG-isomorphism of Lemma 13.4.) ∎

Exercise 15.12

Let K be a field. Let U, V, W be KG-modules. Prove that there are isomorphisms of KG-modules:

(i) $\mathrm{Hom}_K(U \otimes_K V, W) \cong \mathrm{Hom}_K(U, V^* \otimes_K W)$; and

(ii) $\mathrm{Hom}_{KG}(U \otimes_K V, W) \cong \mathrm{Hom}_{KG}(U, V^* \otimes_K W) \cong \mathrm{Hom}_{KG}(U, \mathrm{Hom}_K(V, W))$.

Chapter 5. The Mackey Formula and Clifford Theory

The results in this chapter go more deeply into the theory. We start with the so-called *Mackey decomposition formula*, which provides us with yet another relationship between induction and restriction. After that we explain Clifford's theorem, which explains what happens when a simple representation is restricted to a normal subgroup. These results are essential and have many consequences throughout representation theory of finite groups.

Notation: throughout this chapter, unless otherwise specified, we let G denote a finite group and K be a commutative ring. All modules over group algebras considered are assumed to be **free of finite rank as K-modules** (hence, in particular, they are **finitely generated** as KG-modules).

References:

[Alp86] J. L. Alperin. *Local representation theory*. Vol. 11. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1986.

[Ben98] D. J. Benson. *Representations and cohomology. I*. Vol. 30. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1998.

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. John Wiley & Sons, Inc., New York, 1990.

[LP10] K. Lux and H. Pahlings. *Representations of groups*. Vol. 124. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2010.

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

16 Double cosets

Definition 16.1 (*Double cosets*)

Given subgroups H and L of G we define for each $g \in G$

$$HgL := \{hgk \in G \mid h \in H, k \in L\}$$

and call this subset of G the (H, L)-**double coset** of g. Moreover, we let $H\backslash G/L$ denote the set of (H, L)-double cosets of G.

First, we want to prove that the (H, L)-double cosets partition the group G.

Lemma 16.2

Let $H, L \leqslant G$.

(a) Each (H, L)-double coset is a disjoint union of right cosets of H and a disjoint union of left cosets of L.

(b) Any two (H, L)-double cosets either coincide or are disjoint. Hence, letting $[H\backslash G/L]$ denote a set of representatives for the (H, L)-double cosets of G, we have

$$G = \bigsqcup_{g \in [H\backslash G/L]} HgL\,.$$

Proof:

(a) If $hgk \in HgL$ and $k_1 \in L$, then $hgk \cdot k_1 = hg(kk_1) \in HgL$. It follows that the entire left coset of L that contains hgk is contained in HgL. This proves that HgL is a union of left cosets of L. A similar argument proves that HgL is a union of right cosets of H.

(b) Let $g_1, g_2 \in G$. If $h_1 g_1 k_1 = h_2 g_2 k_2 \in Hg_1L \cap Hg_2L$, then $g_1 = h_1^{-1} h_2 g_2 k_2 k_1^{-1} \in Hg_2L$ so that $Hg_1L \subseteq Hg_2L$. Similarly $Hg_2L \subseteq Hg_1L$. Thus if two double cosets are not disjoint, they coincide. ∎

If X is a left G-set we use the standard notation $G\backslash X$ for the set of orbits of G on X, and denote a set of representatives for theses orbits by $[G\backslash X]$. Similarly if Y is a right G-set we write Y/G and $[Y/G]$. We shall also repeatedly use the orbit-stabiliser theorem without further mention: in other words, if X is a transitive left G-set and $x \in X$ then $X \cong G/\operatorname{Stab}_G(x)$ (i.e. the set of left cosets of the stabiliser of x in G), and similarly for right G-sets.

Exercise 16.3

(a) Let $H, L \leqslant G$. Prove that the set of (H, L)-double cosets is in bijection with the set of orbits $H\backslash(G/L)$, and also with the set of orbits $(H\backslash G)/L$ under the mappings

$$HgL \mapsto H(gL) \in H\backslash(G/L)$$

$$HgL \mapsto (Hg)L \in (H\backslash G)/L.$$

This justifies the notation $H\backslash G/L$ for the set of (H, L)-double cosets.

(b) Let $G = S_3$. Consider $H = L := S_2 = \{\mathrm{Id}, (1\ 2)\}$ as a subgroup of S_3. Prove that

$$[S_2\backslash S_3/S_2] = \{\mathrm{Id}, (1\ 2\ 3)\}$$

while

$$S_2\backslash S_3/S_2 = \{\,\{\mathrm{Id}, (1\ 2)\}, \{(1\ 2\ 3), (1\ 3\ 2), (1\ 3), (2\ 3)\}\}\,.$$

17 The Mackey formula

If H and L are subgroups of G, we wish to describe what happens if we induce a KL-module from L to G and then restrict it to H.

Remark 17.1

We need to examine KG seen as a (KH, KL)-bimodule (i.e. with left and right external laws by multiplication in G). Since $G = \bigsqcup_{g\in[H\backslash G/L]} HgL$, we have

$$KG = \bigoplus_{g\in[H\backslash G/L]} K\langle HgL\rangle$$

as (KH, KL)-bimodule, where $K\langle HgL\rangle$ denotes the free K-module with K-basis HgL.
Now if M is a KL-module, we will also write ${}^gM$ for $g \otimes M$, which is a left $K({}^gL)$-module with

$$(gkg^{-1}) \cdot (g \otimes m) = g \otimes km$$

for each $k \in L$ and each $m \in M$. With this notation, we have

$$K\langle HgL\rangle \cong KH \otimes_{K(H\cap {}^gL)} (g \otimes KL)\,,$$

where $hgk \in HgL$ corresponds to $h \otimes g \otimes k$.

Theorem 17.2 (*Mackey formula*)

Let $H, L \leqslant G$ and let M be a KL-module. Then, as KH-modules,

$$M\uparrow_L^G\downarrow_H^G \cong \bigoplus_{g\in[H\backslash G/L]} ({}^gM\downarrow_{H\cap {}^gL}^{{}^gL})\uparrow_{H\cap {}^gL}^H .$$

Proof: It follows from Remark 17.1 that as left KH-modules we have

$$\begin{aligned} M\uparrow_L^G\downarrow_H^G \cong (KG \otimes_{KL} M)\downarrow_H^G &\cong \bigoplus_{g\in[H\backslash G/L]} K\langle HgL\rangle \otimes_{KL} M \\ &\cong \bigoplus_{g\in[H\backslash G/L]} KH \otimes_{K(H\cap {}^gL)} (g \otimes KL) \otimes_{KL} M \\ &\cong \bigoplus_{g\in[H\backslash G/L]} KH \otimes_{K(H\cap {}^gL)} (g \otimes M)\downarrow_{H\cap {}^gL}^{{}^gL} \\ &\cong \bigoplus_{g\in[H\backslash G/L]} ({}^gM\downarrow_{H\cap {}^gL}^{{}^gL})\uparrow_{H\cap {}^gL}^H . \end{aligned}$$

■

Remark 17.3

Given an arbitrary finite group Z, write ${}_{KZ}\mathbf{mod}$ for the category of KZ-modules which are free of finite rank as K-modules. Then, expressed in categorical terms, the Mackey formula says that we have the following equality of functors from ${}_{KL}\mathbf{mod}$ to ${}_{KH}\mathbf{mod}$:

$$\mathrm{Res}_H^G \circ \mathrm{Ind}_L^G = \bigoplus_{g\in[H\backslash G/L]} \mathrm{Ind}_{H\cap {}^gL}^H \circ \mathrm{Res}_{H\cap {}^gL}^{{}^gL} \circ \mathrm{Inn}(g)$$

where $\mathrm{Inn}(g)$ is conjugation by $g \in G$.

Exercise 17.4

Let $H, L \leqslant G$, let M be a KL-module and let N be a KH-module. Use the Mackey formula to prove that:

(a) $M\uparrow_L^G \otimes_K N\uparrow_H^G \cong \bigoplus_{g\in[H\backslash G/L]} ({}^gM\downarrow_{H\cap {}^gL}^{{}^gL} \otimes_K N\downarrow_{H\cap {}^gL}^{H})\uparrow_{H\cap {}^gL}^{G}$;

(b) $\mathrm{Hom}_K(M\uparrow_L^G, N\uparrow_H^G) \cong \bigoplus_{g\in[H\backslash G/L]} (\mathrm{Hom}_K({}^gM\downarrow_{H\cap {}^gL}^{{}^gL}, N\downarrow_{H\cap {}^gL}^{H}))\uparrow_{H\cap {}^gL}^{G}$.

18 Clifford theory

We now turn to *Clifford's theorem*, which we present in a weak and a strong form. Clifford theory is a collection of results about induction and restriction of simple modules from/to normal subgroups.

Throughout this section, we assume that K is a field.

First we emphasise again, that this is no loss of generality: indeed if S were a simple KG-module with K an arbitrary commutative ring, then letting I be the annihilator in K of S, we have that I is a maximal ideal of K, so that K/I is a field and S is a $(K/I)G$-module.

Theorem 18.1 (*Clifford's Theorem, weak form*)

If $U \trianglelefteq G$ is a normal subgroup and S is a simple KG-module, then $S\downarrow_U^G$ is semisimple.

Proof: Let V be any simple KU-submodule of $S\downarrow_U^G$. Now, notice that for every $g \in G$, $gV := \{gv \mid v \in V\}$ is also a KU-submodule of $S\downarrow_U^G$, since $U \trianglelefteq G$ for any $u \in U$, we have

$$u \cdot gV = g \cdot \underbrace{(g^{-1}ug)}_{\in U} V = gV$$

Moreover, gV is also simple, since if W were a non-trivial proper KU-submodule of gV then $g^{-1}W$ would also be a non-trivial proper submodule of $g^{-1}gV = V$. Now $\sum_{g\in G} gV$ is non-zero and it is a KG-submodule of S, which is simple, hence $\sum_{g\in G} gV = S$. Restricting to U, we obtain that

$$S\downarrow_U^G = \sum_{g\in G} gV$$

is a sum of simple KU-submodules. Hence $S\downarrow_U^G$ is semisimple. ∎

Remark 18.2

The KU-submodules gV which appear in the proof of Theorem 18.1 are isomorphic to modules we have seen before: more precisely the map

$$\begin{array}{ccc} g \otimes V & \longrightarrow & gV \\ g \otimes v & \mapsto & gv \end{array}$$

is a KU-isomorphism, since $U \trianglelefteq G$ implies that ${}^gU = U$ and hence the action of U on $g \otimes V$ (see Remark 17.1) and gV is prescribed in the same way.

Theorem 18.3 (*Clifford's Theorem, strong form*)

Let $U \trianglelefteq G$ be a normal subgroup and let S be a simple KG-module. Then we may write

$$S\downarrow_U^G = S_1^{a_1} \oplus \cdots \oplus S_r^{a_r}$$

where $r \in \mathbb{Z}_{>0}$ and $S_1, \ldots, S_r$ are pairwise non-isomorphic simple KU-modules, occurring with multiplicities $a_1, \ldots, a_r$ respectively. Moreover, the following statements hold:

(i) the group G permutes the homogeneous components of $S\downarrow_U^G$ transitively;

(ii) $a_1 = a_2 = \cdots = a_r$ and $\dim_K(S_1) = \cdots = \dim_K(S_r)$; and

(iii) $S \cong (S_1^{a_1})\uparrow_{H_1}^G$ as KG-modules, where $H_1 = \mathrm{Stab}_G(S_1^{a_1})$.

Proof: The fact that $S\downarrow_U^G$ is semisimple and hence can be written as a direct sum as claimed follows from Theorem 18.1. Moreover, by the chapter on semisimplicity of rings and modules, we know that for each $1 \leqslant i \leqslant r$ the homogeneous component $S_i^{a_i}$ is characterised by Proposition 7.1: it is the unique largest KU-submodule which is isomorphic to a direct sum of copies of S_i.

Now, if $g \in G$ then $g(S_i^{a_i}) = (gS_i)^{a_i}$, where gS_i is a simple KU-submodule of $S\downarrow_U^G$ (see the proof of the weak form of Clifford's Theorem). Hence there exists an index $1 \leqslant j \leqslant r$ such that $gS_i = S_j$ and $g(S_i^{a_i}) \subseteq S_j^{a_j}$ (alternatively to Proposition 7.1, the theorem of Krull-Schmidt can also be invoked here). Because $\dim_K(S_i) = \dim_K(gS_i)$, we have that $a_i \leqslant a_j$. Similarly, since $S_j = g^{-1}S_i$, we obtain $a_j \leqslant a_j$. Hence $a_i = a_j$ holds. Because

$$S\downarrow_U^G = g(S\downarrow_U^G) = g(S_1^{a_1}) \oplus \cdots \oplus g(S_r^{a_r}),$$

we actually have that G permutes the homogeneous components. Moreover, as $\sum_{g\in G} g(S_1^{a_1})$ is a non-zero KG-submodule of S, which is simple, we have that $\sum_{g\in G} g(S_1^{a_1}) = S$, and so the action on the homogeneous components is transitive. This establishes both (i) and (ii).
For (iii), we define a K-homomorphism via the map

$$\begin{array}{rccc} \Phi: & (S_1^{a_1})\uparrow_{H_1}^G = KG \otimes_{KH_1} S_1^{a_1} = \bigoplus_{g\in[G/H_1]} g \otimes S_1^{a_1} & \longrightarrow & S \\ & g \otimes m & \mapsto & gm \end{array}$$

that is, where $g\otimes m \in g\otimes S_1^{a_1}$. This is in fact a KG-homomorphism. Furthermore, the K-subspaces $g(S_1^{a_1})$ of S are in bijection with the cosets G/H_1, since G permutes them transitively by (i), and the stabiliser of one of them is H_1. Thus both $KG\otimes_{KH_1} S_1^{a_1}$ and S are the direct sum of $|G : H_1|$ K-subspaces $g \otimes S_1^{a_1}$ and $g(S_1^{a_1})$ respectively, each K-isomorphic to $S_1^{a_1}$ (via $g \otimes m \leftrightarrow m$ and $gm \leftrightarrow m$). Thus the restriction of Φ to each summand is an isomorphism, and so Φ itself must be bijective, hence a KG-isomorphism. ■

One application of Clifford's theory is for example the following Corollary:

Corollary 18.4

Assume K is a splitting field for G of arbitrary characteristic. If p is a prime number and G is a p-group, then every simple KG-module has the form $X\uparrow_H^G$, where X is a 1-dimensional KH-module for some subgroup $H \leqslant G$.

Proof: We proceed by induction on $|G|$.

If $|G| = 1$ or $|G|$ is a prime number, then G is abelian and any simple module S is 1-dimensional by Corollary 12.3, so $H = G$, $X = S$ and we are done.

So assume $|G| = p^b$ with $b > 1$, and let S be a simple KG-module and consider the subgroup

$$U := \{g \in G \mid g \cdot x = x \ \ \forall x \in S\}\,.$$

This is obviously a normal subgroup of G since it is the kernel of the K-representation associated to S. Hence $S = \mathrm{Inf}_{G/U}^G(T)$ for a simple $K[G/U]$-module T.
Now, if $U \neq \{1\}$, then $|G/U| < |G|$, so by the induction hypothesis there exists a subgroup $H/U \leqslant G/U$ and a 1-dimensional $K[H/U]$-module Y such that $T = \mathrm{Ind}_{H/U}^{G/U}(Y)$. But then

$$S = \mathrm{Inf}_{G/U}^G(T) = \mathrm{Inf}_{G/U}^G \circ \mathrm{Ind}_{H/U}^{G/U}(Y) = \mathrm{Ind}_H^G \circ \mathrm{Inf}_{H/U}^H(Y)\,,$$

so that setting $X := \mathrm{Inf}_{H/U}^H(Y)$ yields the result. Thus we may assume $U = \{1\}$.
If G is abelian, then all simple modules are 1-dimensional, so we are done. Assume now that G is not abelian. Then G has a normal abelian subgroup A that is not central. Indeed, to construct this subgroup A, let $Z_2(G)$ denote the second centre of G, that is, the preimage in G of $Z(G/Z(G))$ (this centre is non-trivial as $G/Z(G)$ is a non-trivial p-group). If $x \in Z_2(G)\backslash Z(G)$, then $A := \langle Z(G), x\rangle$ is a normal abelian subgroup not contained in $Z(G)$. Now, applying Clifford's Theorem yields:

$$S\downarrow_A^G = S_1^{a_1} \oplus \cdots \oplus S_r^{a_r}$$

where $r \in \mathbb{Z}_{>0}$, $S_1, \ldots, S_r$ are non-isomorphic simple KA-modules and $S = (S_1^{a_1})\uparrow_{H_1}^G$, where $H_1 = \mathrm{Stab}_G(S_1^{a_1})$. We argue that $V := S_1^{a_1}$ must be a simple KH_1-module, since if it had a proper non-trivial submodule W, then $W\uparrow_{H_1}^G$ would be a proper non-trivial submodule of S, which is simple: a contradiction. If $H_1 \neq G$ then by the induction hypothesis $V = X\uparrow_H^{H_1}$, where $H \leqslant H_1$ and X is a 1-dimensional KH-module. Thefore, by transitivity of the induction, we have

$$S = (S_1^{a_1})\uparrow_{H_1}^G = (X\uparrow_H^{H_1})\uparrow_{H_1}^G = X\uparrow_H^G\,,$$

as required.
Finally, the case $H_1 = G$ cannot happen. For if it were to happen then

$$S\downarrow_A^G = S\downarrow_A^{H_1} = S_1^{a_1}\,,$$

is simple by the weak form of Clifford's Theorem, hence of dimension 1 since A is abelian. The elements of A must therefore act via scalar multiplication on S. Since such an action would commute with the action of G, which is faithful on S, we deduce that $A \subseteq Z(G)$, which contradicts the construction of A. ■

Remark 18.5

This result is extremely useful, for example, to construct the complex character table of a p-group. Indeed, it says that we need look no further than induced linear characters. In general, a KG-module of the form $N\uparrow_H^G$ for some subgroup $H \leqslant G$ and some 1-dimensional KH-module is called **monomial**. A group all of whose simple $\mathbb{C}G$-modules are monomial is called an M-**group**. (By the above p-groups are M-groups.)

Chapter 6. Projective Modules over the Group Algebra

We continue developing techniques to describe modules that are not semisimple and in particular indecomposable modules. The indecomposable projective modules are the indecomposable summands of the regular module. Since every module is a homomorphic image of a direct sum of copies of the regular module, by knowing the structure of the projectives we gain some insight into the structure of all modules.

Notation: throughout this chapter, unless otherwise specified, we let G denote a finite group and K be a field. (We will understand in the coming chapters, why it is enough for our purpose to focus on fields, when considering projective module over the group algebra.) All modules over group algebras considered are assumed to be finite-dimensional over K, hence finitely generated as KG-modules. When no confusion is to be made, we denote the regular module simply by KG instead of KG°.

References:

[Alp86] J. L. Alperin. *Local representation theory*. Vol. 11. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1986.

[Ben98] D. J. Benson. *Representations and cohomology. I*. Vol. 30. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1998.

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. John Wiley & Sons, Inc., New York, 1990.

[LP10] K. Lux and H. Pahlings. *Representations of groups*. Vol. 124. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2010.

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

19 Radical, socle, head

Before focusing on projective modules, at this point we examine further the structure of KG-modules which are not semisimple, and try to establish connections with their semisimple submodules, semisimple quotients, and composition factors. This leads us to the definitions of the *radical* and the *socle* of a module.

Definition 19.1

Let M be a KG-module.

(a) The **radical** of M is its submodule $\operatorname{rad}(M) := \bigcap_{V \in \operatorname{Max}(M)} V$ where $\operatorname{Max}(M)$ denotes the set of maximal KG-submodules of M.

(b) The **head** of M is the quotient module $\operatorname{hd}(M) := M/\operatorname{rad}(M)$.

(c) The **socle** of M, denoted $\operatorname{soc}(M)$ is the sum of all simple submodules of M.

Notice that in our setting (i.e. K is a field) KG-modules are always Noetherian, so provided $M \neq 0$ the above intersection is non-empty and hence $\operatorname{rad}(M) \neq M$. Also, informally (talks/spoken mathematics) one also uses the words *top* and *bottom* instead of *head* and *socle*, respectively.

Lemma 19.2

Let M be a KG-module. Then the following KG-submodules of M are equal:

(1) $\operatorname{rad}(M)$;

(2) $J(KG)M$;

(3) the smallest KG-submodule of M with semisimple quotient.

Proof:

"(3)=(1)": Recall that if $V \subset M$ is a maximal submodule, then M/V is simple. Moreover, if $V_1, \ldots, V_r$ ($r \in \mathbb{Z}_{>0}$) are maximal submodules of M, then the map

$$\begin{array}{rccc} \varphi\colon & M & \longrightarrow & M/V_1 \oplus \cdots \oplus M/V_r \\ & m & \mapsto & (m+V_1, \ldots, m+V_r) \end{array}$$

is a KG-homomorphism with kernel $\ker(\varphi) = V_1 \cap \cdots \cap V_r$. Hence $M/(V_1 \cap \cdots \cap V_r) \cong \operatorname{Im}(\varphi)$ is semisimple, since it is a submodule of a semisimple module. Therefore $M/\operatorname{rad}(M)$ is a semisimple quotient. It remains to see that it is the smallest such quotient.

If $X \subseteq M$ is a KG-submodule with M/X semisimple, then by the Correspondence Theorem, there exists KG-submodules $X_1, \ldots, X_r$ of M ($r \in \mathbb{Z}_{>0}$) containing X such that

$$M/X \cong X_1/X \oplus \cdots \oplus X_r/X \qquad \text{and} \qquad X_i/X \text{ is simple } \forall\ 1 \leqslant i \leqslant r\,.$$

For each $1 \leqslant i \leqslant r$, let Y_i be the kernel of the projection homomorphism $M \twoheadrightarrow M/X \twoheadrightarrow X_i/X$, so that Y_i is maximal (as X_i/X is simple) and $X = Y_1 \cap \ldots \cap Y_r$. Thus $X \supseteq \operatorname{rad}(M)$, as required.

"(1)⊆(2)": Observe that the quotient module $M/J(KG)M$ is a $KG/J(KG)$-module as

$$J(KG)\,(M/J(KG)M) = 0\,.$$

Now, as $KG/J(KG)$ is semisimple (by Proposition 6.6 and Proposition 6.7), $M/J(KG)M$ is a semisimple $KG/J(KG)$-module by definition of a semisimple ring, but then it is also semisimple as a KG-module. Since we have already proved that $\operatorname{rad}(M)$ is the smallest KG-submodule of M with semisimple quotient, we must have that $\operatorname{rad}(M) \subseteq J(KG)M$.

"(2)⊆(1)": If $Z \subseteq M$ is any KG-submodule for which M/Z is semisimple, certainly $J(KG) \cdot M/Z = 0$, because $J(KG)$ annihilates all simple KG-modules by definition, and it follows that $J(KG)M \subseteq Z$. Thus, again as we already know that (1)=(3), we obtain that $J(KG)M \subseteq \operatorname{rad}(M)$. ∎

Example 9

If M is a semisimple KG-module, then $\mathrm{soc}(M) = M$ by definition, $\mathrm{rad}(M) = 0$ by the above Lemma, and hence $\mathrm{hd}(M) = M$.

Lemma 19.3

Let M be a KG-module. Prove that the following KG-submodules of M are equal:

(1) $\mathrm{soc}(M)$;

(2) the largest semisimple KG-submodule of M;

(3) $\{m \in M \mid J(KG) \cdot m = 0\}$.

Proof: Exercise. [Hint: $\{m \in M \mid J(KG) \cdot m = 0\}$ is the largest KG-submodule of M annihilated by $J(KG)$, and hence may be seen as a $KG/J(KG)$-module.] ■

Remark 19.4 (*Socle, radical and Loewy layers*)

We can iterate the notions of socle and radical: for each KG-module M and each $n \in \mathbb{Z}_{\geqslant 2}$ we define inductively

$$\mathrm{rad}^n(M) := \mathrm{rad}\left(\mathrm{rad}^{n-1}(M)\right) \qquad \text{and} \qquad \mathrm{soc}^n(M)/\mathrm{soc}^{n-1}(M) := \mathrm{soc}(M/\mathrm{soc}^{n-1}(M))$$

where we understand that $\mathrm{rad}^1(M) = \mathrm{rad}(M)$ and $\mathrm{soc}^1(M) = \mathrm{soc}(M)$.

Exercise. Prove that:

(a) $\mathrm{rad}^n(M) = J(KG)^n \cdot M$ and $\mathrm{soc}^n(M) = \{m \in M \mid J(KG)^n \cdot m = 0\}$;

(b) $\cdots \subseteq \mathrm{rad}^3(M) \subseteq \mathrm{rad}^2(M) \subseteq \mathrm{rad}(M) \subseteq M$ and $0 \subseteq \mathrm{soc}(M) \subseteq \mathrm{soc}^2(M) \subseteq \mathrm{soc}^3(M) \subseteq \cdots$

The chains of submodules in (b) are called respectively, the **radical series** and **socle series** of M. The radical series of M is also known as the **Loewy series** of M. The quotients $\mathrm{rad}^{n-1}(M)/\mathrm{rad}^n(M)$ are called the **radical layers**, or **Loewy layers** of M, and the quotients $\mathrm{soc}^n(M)/\mathrm{soc}^{n-1}(M)$ are called the **socle layers** of M.

Exercise 19.5

Let M and N be KG-modules. Prove the following assertions.

(a) For every $n \in \mathbb{Z}_{\geqslant 1}$, $\mathrm{rad}^n(M \oplus N) \cong \mathrm{rad}^n(M) \oplus \mathrm{rad}^n(N)$ and $\mathrm{soc}^n(M \oplus N) \cong \mathrm{soc}^n(M) \oplus \mathrm{soc}^n(N)$.

(b) The radical series of M is the fastest descending series of KG-submodules of M with semisimple quotients, and the socle series of M is the fastest ascending series of M with semisimple quotients. The two series terminate, and if r and n are the least integers for which $\mathrm{rad}^r(M) = 0$ and $\mathrm{soc}^n(U) = M$ then $r = n$.

Definition 19.6

The common length of the radical series and socle series of a KG-module M is called the **Loewy length** of M. (By the above, we may see it as the least integer n such that $J(KG)^n \cdot M = 0$.)

20 Projective modules

For the sake of clarity, we recall the general definition of a projective module through its most standard equivalent characterisations.

Proposition-Definition 20.1 (*Projective module*)

Let R be an arbitrary ring and let P be an R-module. Then the following are equivalent:

(a) The functor $\mathrm{Hom}_R(P,-)$ is exact. In other words, the image of any s.e.s. of R-modules under $\mathrm{Hom}_R(P,-)$ is again a s.e.s.

(b) If $\psi \in \mathrm{Hom}_R(M,N)$ is a surjective morphism of R-modules, then the morphism of abelian groups $\psi_* : \mathrm{Hom}_R(P,M) \longrightarrow \mathrm{Hom}_R(P,N)$ is surjective. In other words, for every pair of R-morphisms

$$\begin{array}{ccc} & & P \\ & & \downarrow{\scriptstyle \alpha} \\ M & \xrightarrow[\psi]{} & N \end{array}$$

where ψ is surjective, there exists a KG-morphism $\beta : P \longrightarrow M$ such that $\alpha = \psi\beta$.

(c) If $\pi : M \longrightarrow P$ is a surjective R-homomorphism, then π splits, i.e., there exists $\sigma \in \mathrm{Hom}_R(P,M)$ such that $\pi \circ \sigma = \mathrm{Id}_P$.

(d) The module P is isomorphic to a direct summand of a free R-module.

If P satisfies these equivalent conditions, then P is called **projective**. Moreover, a projective indecomposable module is called a **PIM** of R.

Example 10

(a) Any free module is projective.

(b) If e is an idempotent element of the ring R, then $R \cong Re \oplus R(1-e)$ and Re is projective, but not free if $e \neq 0, 1$.

(c) It follows from condition (d) of Proposition-Definition B.5 that a direct sum of modules $\{P_i\}_{i\in I}$ is projective if and only if each P_i is projective.

(d) If R is semisimple, then on the one hand any projective indecomposable module is simple, and conversely, since R° is semisimple. It follows that any R-module is projective.

21 Projective modules for the group algebra

We have seen that over a semisimple ring, all simple modules appear as direct summands of the regular module with multiplicity equal to their dimension. For non-semisimple rings this is not true any more, but replacing simple modules by the *projective* modules, we will obtain a similar characterisation.

To begin with we review a series of properties of projective KG-modules with respect to the operations on groups and modules we have introduced in Chapter 4, i.e. induction/restriction, tensor products, ...

Proposition 21.1

Assume K is an arbitrary commutative ring. Then the following assertions hold.

(a) If P is a projective KG-module and M is an arbitrary KG-module which is free of finite rank as a K-module, then $P \otimes_K M$ is projective.

(b) If P is a projective KG-module and $H \leqslant G$, then $P{\downarrow}^G_H$ is a projective KH-module.

(c) If $H \leqslant G$ and P is a projective KH-module, then $P{\uparrow}^G_H$ is a projective KG-module.

Proof:

(a) Since P is projective, by definition it is a direct summand of a free KG-module, so there exist a KG-module P' and a positive integer n such that $P \oplus P' \cong (KG)^n$. Therefore,

$$(KG)^n \otimes_K M \cong (P \oplus P') \otimes_K M \cong P \otimes_K M \oplus P' \otimes_K M$$

and it suffices to prove that $(KG)^n \otimes_K M$ is free. So observe that Example 7(a), Proposition 15.11(a) and the properties of the tensor product yield

$$\begin{aligned} KG \otimes_K M \cong (K{\uparrow}^G_{\{1\}}) \otimes_K M \cong (K \otimes_K M{\downarrow}^G_{\{1\}}){\uparrow}^G_{\{1\}} &\cong M{\uparrow}^G_{\{1\}} \\ &\cong (K^{\mathrm{rk}_K(M)}){\uparrow}^G_{\{1\}} \cong (K{\uparrow}^G_{\{1\}})^{\mathrm{rk}_K(M)} \cong (KG)^{\mathrm{rk}_K(M)} \end{aligned}$$

since $M{\downarrow}^G_{\{1\}}$ is just M seen as K-module, and, as such, is free of finite rank. It follows immediately that $(KG)^n \otimes_K M \cong (KG)^{n \cdot \mathrm{rk}_K(M)}$ is a free KG-module, as required.

(b) We have already seen that as a KH-module,

$$KG{\downarrow}^G_H \cong KH \oplus \cdots \oplus KH$$

where KH occurs with multiplicity $|G : H|$, so $KG{\downarrow}^G_H$ is a free KH-module. Hence the restriction from G to H of any free KG-module is a free KH-module. Now, by definition $P \mid F$ for some free KG-module F, so that $P{\downarrow}^G_H \mid F{\downarrow}^G_H$ and the claim follows.

(c) Exercise!
[Hint: prove that $KH{\uparrow}^G_H \cong KG$.]

■

We now want to prove that the PIMs of KG are in bijection with the simple KG-modules, and hence that there are a finite number of them, up to isomorphism. We will then be able to deduce from this bijection that each of them occurs in the decomposition of the regular module with multiplicity equal to the dimension of the corresponding simple module.

Theorem 21.2

(a) If P is a projective indecomposable KG-module, then $P/\operatorname{rad}(P)$ is a simple KG-module.

(b) If M is a KG-module and $M/\operatorname{rad}(M) \cong P/\operatorname{rad}(P)$ for a projective indecomposable KG-module P, then there exists a surjective KG-homomorphism $\varphi : P \longrightarrow M$. In particular, if M is also projective indecomposable, then $M/\operatorname{rad}(M) \cong P/\operatorname{rad}(P)$ if and only if $M \cong P$.

(c) There is a bijection

$$\begin{array}{ccc} \left\{\begin{smallmatrix}\text{projective indecomposable}\\ KG\text{-modules}\end{smallmatrix}\right\}/\cong & \xleftrightarrow{\sim} & \left\{\begin{smallmatrix}\text{simple}\\ KG\text{-modules}\end{smallmatrix}\right\}/\cong \\ P & \mapsto & P/\operatorname{rad}(P) \end{array}$$

and hence the number of pairwise non-isomorphic PIMs of KG is finite.

Proof:

(a) By Lemma 19.2, $P/\operatorname{rad}(P)$ is semisimple, hence it suffices to prove that it is indecomposable, or equivalently, by Proposition 5.4 that $\operatorname{End}_{KG}(P/\operatorname{rad}(P))$ is a local ring.
Now, if $\varphi \in \operatorname{End}_{KG}(P)$, then by Lemma 19.2, we have

$$\varphi(\operatorname{rad}(P)) = \varphi(J(KG)P) = J(KG)\varphi(P) \subseteq J(KG)P = \operatorname{rad}(P)\,.$$

Therefore, by the universal property of the quotient, φ induces a unique KG-homomorphism $\overline{\varphi} : P/\operatorname{rad}(P) \longrightarrow P/\operatorname{rad}(P)$ such that the following diagram commutes:

$$\begin{array}{ccc} P & \xrightarrow{\quad\varphi\quad} & P \\ {\scriptstyle\pi_P}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\pi_P} \\ P/\operatorname{rad}(P) & \xrightarrow[\overline{\varphi}]{} & P/\operatorname{rad}(P) \end{array}$$

Then, the map

$$\begin{array}{rccc} \Phi: & \operatorname{End}_{KG}(P) & \longrightarrow & \operatorname{End}_{KG}(P/\operatorname{rad}(P)) \\ & \varphi & \mapsto & \overline{\varphi} \end{array}$$

is clearly a K-algebra homomorphism. Moreover Φ is surjectiv. Indeed, if $\psi \in \operatorname{End}_{KG}(P/\operatorname{rad}(P))$, then by the definition of a projective module there exists a KG-homomorphism $\varphi : P \longrightarrow P$ such that $\psi \circ \pi_P = \pi_P \circ \varphi$. But then ψ satisfies the diagram of the universal property of the quotient and by uniqueness $\psi = \overline{\varphi}$.
Finally, as P is indecomposable $\operatorname{End}_{KG}(P)$ is local, hence any element of $\operatorname{End}_{KG}(P)$ is either nilpotent or invertible, and by surjectivity of Φ the same holds for $\operatorname{End}_{KG}(P/\operatorname{rad}(P))$, which in turn must be local.

(b) Consider the diagram

$$\begin{array}{ccccc} & & & & P \\ & & & & \downarrow{\scriptstyle\pi_P} \\ M & \xrightarrow[\pi_M]{} & M/\operatorname{rad}(M) & \xrightarrow[\psi]{\cong} & P/\operatorname{rad}(P) \end{array}$$

where π_M and π_P are the quotient morphisms. As P is projective, by definition, there exists a KG-homomorphism $\varphi : P \longrightarrow M$ such that $\pi_P = \psi \circ \pi_M \circ \varphi$.
It follows that $M = \varphi(P) + \operatorname{rad}(M) = \varphi(P) + J(KG)M$, so that $\varphi(P) = M$ by Nakayama's Lemma. Finally, if M is a PIM, the surjective homomorphism φ splits by definition of a projective module, and hence $M \mid P$. But as both modules are indecomposable, we have $M \cong P$. Conversely, if $M \cong P$, then clearly $M/\operatorname{rad}(M) \cong P/\operatorname{rad}(P)$.

(c) The given map between the two sets is well-defined by (a) and (b), and it is injective by (b). It remains to prove that it is surjective. So let S be a simple KG-module. As S is finitely generated, there exists a free KG-module F and a surjective KG-homomorphism $\psi : F \longrightarrow S$. But then there is an indecomposable direct summand P of F such that $\psi|_P : P \longrightarrow S$ is non-zero, hence

surjective as S is simple. Clearly $\mathrm{rad}(P) \subseteq \ker(\psi|_P)$ since it is the smallest KG-submodule with semisimple quotient by Lemma 19.2. Then the universal property of the quotient yields a surjective homomorphism $P/\mathrm{rad}(P) \longrightarrow S$ induced by $\psi|_P$. Finally, as $P/\mathrm{rad}(P)$ is simple, $P/\mathrm{rad}(P) \cong S$ by Schur's Lemma. ■

Definition 21.3 (*Projective cover of a simple module*)

If S is a simple KG-module, then we denote by P_S the projective indecomposable KG-module corresponding to S through the bijection of Theorem 21.2(c) and call this module the **projective cover** of S.

Corollary 21.4

Assume K is a splitting field for G. Then, in the decomposition of the regular module KG into a direct sum of indecomposable KG-submodules, each isomorphism type of projective indecomposable KG-module occurs with multiplicity $\dim_K(P/\mathrm{rad}(P))$. In other words, with the notation of Definition 21.3,

$$KG \cong \bigoplus_{S \text{ simple}} (P_S)^{n_s}$$

where more preciely S runs through the set of isomorphism classes of simple KG-modules and $n_S = \dim_K S$.

Proof: Let $KG = P_1 \oplus \cdots \oplus P_r$ ($r \in \mathbb{Z}_{>0}$) be such a decomposition. In particular, $P_1, \ldots P_r$ are PIMs. Then

$$J(KG) = J(KG)KG = J(KG)P_1 \oplus \cdots \oplus J(KG)P_r = \mathrm{rad}(P_1) \oplus \cdots \oplus \mathrm{rad}(P_r)$$

by Lemma 19.2. Therefore,

$$KG/J(KG) \cong P_1/\mathrm{rad}(P_1) \oplus \cdots \oplus P_r/\mathrm{rad}(P_r)$$

where each summand is simple by Theorem 21.2(a). Now as $KG/J(KG)$ is semisimple, by Theorem 8.2, any simple $KG/J(KG)$-module occurs in this decomposition with multiplicity equal to its K-dimension. Thus the claim follows from the bijection of Theorem 21.2(c). ■

The Theorem also leads us to the following important dimensional restriction on projective modules.

Corollary 21.5

Assume K is a splitting field for G of characteristic $p > 0$. If P is a projective KG-module, then

$$|G|_p \,\big|\, \dim_K(P)\,.$$

(Here $|G|_p$ is the p-part of $|G|$, i.e. the exact power of p that divides the order of G.)

Proof: Let $Q \in \mathrm{Syl}_p(G)$ be a Sylow p-subgroup of G. By Lemma 21.1, $P\downarrow_Q^G$ is projective. Moreover, by Corollary 12.4 the trivial KQ-module is the unique simple KQ-module, hence by Theorem 21.2(c) KQ has a unique PIM, namely KQ itself, which has dimension $|Q| = |G|_p$. Hence

$$P\downarrow_Q^G \cong (KQ)^m \qquad \text{for some } m \in \mathbb{Z}_{>0}\,.$$

Therefore,

$$\dim_K(P) = \dim_K(P\downarrow_Q^G) = m \cdot \dim_K KQ = m \cdot |Q| = m \cdot |G|_p$$

and the claim follows. ■

22 The Cartan matrix

Now that we have classified the projective KG-modules we turn to one of their important uses, which is to determine the multiplicity of a simple module S as a composition factor of an arbitrary finitely generated KG-module M (hence with a composition series). We recall that if

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_{n-1} \subset M_n = M$$

is any composition series of M, the number of quotients M_i/M_{i-1} ($1 \leqslant i \leqslant n$) isomorphic to S is determined independently of the choice of composition series, by the Jordan–Hölder theorem. We call this number the multiplicity of S in M as a composition factor.

Proposition 22.1

Let S be a simple KG-module and let P_S be its projective cover.

(a) If T is a simple KG-module then

$$\dim_K \operatorname{Hom}_{KG}(P_S, T) = \begin{cases} \dim_K \operatorname{End}_{KG}(S) & \text{if } S \cong T, \\ 0 & \text{if } S \ncong T. \end{cases}$$

(b) If M is an arbitrary KG-module, then the multiplicity of S as a composition factor of M is

$$\dim_K \operatorname{Hom}_{KG}(P_S, M) / \dim_K \operatorname{End}_{KG}(S)\,.$$

Proof: Exercise, Sheet 4. [Hint: (b) can be proved by induction on the composition length of M.] ■

Definition 22.2

(a) If S and T are simple KG-modules, then the integer

$$c_{ST} := \text{multiplicity of } S \text{ as a composition factor of } P_T$$

is called the **Cartan invariant** associated to the pair (S, T).

(b) The matrix $C := (c_{ST})$ with rows and columns indexed by the isomorphism classes of simple KG-modules is called the **Cartan matrix** of KG.

It follows immediately from Proposition 22.1 that the Cartan invariants can be computed as follows.

Corollary 22.3

If S and T are two simple KG-modules, then

$$c_{ST} = \dim_K \operatorname{Hom}_{KG}(P_S, P_T) / \dim_K \operatorname{End}_{KG}(S)\,.$$

In particular, if the ground field K is a splitting field for G, then

$$c_{ST} = \dim_K \operatorname{Hom}_{KG}(P_S, P_T)\,.$$

We will see later that there is an extremely effective way of computing the Cartan matrix using another matrix associated to the simple KG-modules, called the *decomposition matrix*.

23 Symmetry of the group algebra

We now want to obtain information about projective KG-modules using duality.
Recall that we have already proved in Lemma 15.9 that $(KG)^* \cong KG$ as KG-modules. This allows us to deduce that projectivity is preserved by taking duals.

Proposition 23.1

If P is a KG-module, then P is projective if and only if P^* is.

Proof: As $P^{**} \cong P$ as KG-modules it suffices to prove one implication. Now, if P is a direct summand of $(KG)^n$ ($n \in \mathbb{Z}_{\geqslant 1}$), then P^* is a direct summand of $((KG)^n)^* \cong ((KG)^*)^n \cong (KG)^n$, and so is also projective. ■

Next we want to investigate the relationship between head and socle of projective modules. For this purpose, we recall the following properties of submodules, quotients and duality, seen in the Exercise classes:

$$W \leqslant V \ KG\text{-submodule} \Rightarrow V^* \text{ has a } KG\text{-submodule } M \text{ such that } M \cong (V/W)^* \text{ and } V^*/M \cong W^*$$

Corollary 23.2

Every projective indecomposable KG-module P has a simple socle. More precisely,

$$\operatorname{soc}(P) \cong (P^*/\operatorname{rad}(P^*))^* .$$

Proof: As on the one hand $P^*/\operatorname{rad}(P^*)$ is simple by Theorem 21.2 and on the other hand $\operatorname{rad}(P^*)$ is the smallest KG-submodule of P^* with semisimple quotient by Lemma 19.2, its dual is the largest semisimple KG-submodule of $P^{**} \cong P$, hence isomorphic to $\operatorname{soc}(P)$, which has to be simple, as required.

Alternatively, we could argue that as the socle is by definition the sum of all simple submodules, it suffices to prove that P has a unique simple KG-submodule. Because P^* is projective by Proposition 23.1, if S is any simple KG-module, then by duality the KG-homomorphisms $S \longrightarrow P$ are in bijection with the KG-homomorphisms $P^* \longrightarrow S^*$ and it follows that

$$\dim_K \operatorname{Hom}_{KG}(S, P) = \dim_K \operatorname{Hom}_{KG}(P^*, S^*)$$

Moroever S^* is also simple. Thus it follows from Proposition 22.1(a) that

$$\dim_K \operatorname{Hom}_{KG}(P^*, S^*) = \begin{cases} \dim_K \operatorname{End}_{KG}(S^*) & \text{if } P^* \text{ is the projective cover of } S^*, \\ 0 & \text{else.} \end{cases}$$

Therefore, the claim follows from the fact that $\dim_K \operatorname{End}_{KG}(S^*) = \dim_K \operatorname{End}_{KG}(S)$ (again by duality). ■

Notice that in this proof to see that $\dim_K \mathrm{Hom}_{KG}(S,P) = \dim_K \mathrm{Hom}_{KG}(P^*,S^*)$ and $\dim_K \mathrm{End}_{KG}(S^*) = \dim_K \mathrm{End}_{KG}(S)$ it is also possible to argue using Lemma 13.4 and Lemma 14.2.

In fact, we can obtain a more precise statement and prove that the head and the socle of a PIM are isomorphic. For this purpose, we need the fact that the group algebra is a *symmetric algebra*.

Remark 23.3

The map

$$(\ ,\ ) : G \times G \longrightarrow K,\ (g,h) := \delta_{g,h^{-1}}$$

extended by K-bilinearity to

$$(\ ,\ ) : KG \times KG \to K$$

defines a K-bilinear form, which is symmetric, non-degenerate and associative. (Associative means that $(ab,c) = (a,bc)\ \forall\ a,b,c \in KG$).
More generally, a K-algebra endowed with such a symmetric, non-degenerate and associative K-bilinear form is called a **symmetric algebra**.

Theorem 23.4

If P is a projective indecomposable KG-module, then $P/\mathrm{rad}(P) \cong \mathrm{soc}(P)$.

Proof: Put $S := P/\mathrm{rad}(P)$, which we know is simple as P is a PIM of KG, and assume $S \ncong \mathrm{soc}(P)$. Write $KG = R \oplus Q$, where $Q = P^n$ ($n \in \mathbb{Z}_{>0}$) is the direct sum of all the indecomposable direct summands of KG isomorphic to P and $P \nmid R$. Then

$$\mathrm{soc}(Q) \cong \mathrm{soc}(P)^n$$

and Q does not contain any KG-submodule isomorphic to S. Next, consider the sum of all KG-submodules of KG isomorphic to S and denote it by I, so that clearly $0 \neq I \subset R$ and I is a left ideal of KG. However, as $\psi(I) \subseteq I$ for every $\psi \in \mathrm{End}_{KG}(KG)$, I is an ideal of KG. Now set $J := \{\psi \in \mathrm{End}_{KG}(KG) \mid \mathrm{Im}(\psi) \subset I\}$, so that J is clearly an ideal of $\mathrm{End}_{KG}(KG)$. Let $\pi : KG \to Q$ be the projection onto Q with kernel R. Then:

$$\varphi \in J \Rightarrow \mathrm{rad}(KG) \subseteq \ker(\varphi)$$

as the image of φ is semisimple, because it is a KG-submodule of I, which is itself a KG-submodule. Thus, $\varphi|_R = 0$, as $S \nmid \mathrm{hd}(R)$, and it follows that

$$\varphi \circ \pi = \varphi \text{ und } \pi \circ \varphi = 0$$

(as $\varphi(KG) \subseteq I$) and hence

$$\varphi = \varphi \circ \pi - \pi \circ \varphi \qquad \forall\, \varphi \in J. \qquad (*)$$

Let now $0 \neq \varphi \in J$ (exists since $S = \mathrm{hd}(P) \subseteq \mathrm{hd}(KG)$), and let $\alpha \in \mathrm{End}_{KG}(KG)$, so $\varphi \circ \alpha \in J$ and

$$\varphi\alpha = \varphi\alpha\pi - \pi\varphi\alpha \text{ by } (*).$$

Set then $a := \alpha(1)$, $b := \varphi(1)$, $c := \pi(1)$, so

$$ab = \alpha(1)\varphi(1) = \varphi(\alpha(1)) = \varphi(\alpha(\pi(1))) - \pi(\varphi(\alpha(1))) = cab - abc$$

and it follows from Remark 23.3 that

$$(a,b) = (ab,1) = (cab,1) - (abc,1) = (c,ab) - (ab,c) = 0.$$

This is true for every $\alpha \in \mathrm{End}_{KG}(KG)$, and hence every $a \in KG$. Finally, as $(\ ,\ )$ is non-degenerate, we have $b = 0$ and hence $\varphi = 0$. Contradiction! ∎

Corollary 23.5

Let S be a simple KG-module.

(a) If P is any projective KG-module, then the multiplicity of S in $P/\operatorname{rad}(P)$ equals the multiplicity of S in $\operatorname{soc}(P)$. In particular

$$\dim_K(P^G) = \dim_K(P_G) = \dim_K(P^*)^G = \dim_K(P^*)_G\,.$$

(b) We have $(P_S)^* \cong P_{S^*}$.

Proof:

(a) By Theorem 23.4, the first claim holds for the PIMs of KG, hence this is also true for any finite direct sum of PIMs, because taking socles and radicals commute with the direct sum by Exercise 19.5(a). Next taking $S = K$ yields the equalities $\dim_K(P^G) = \dim_K(P_G) = \dim_K(P^*)^G = \dim_K(P^*)_G$.

(b) We have seen in the proof of Corollary 23.2 that $(P_S)^*$ is the projective cover of the simple module $(\operatorname{soc}(P_S))^*$. Moreover, by Theorem 23.4

$$(\operatorname{soc}(P_S))^* \cong (P_S/\operatorname{rad}(P_S))^* \cong S^*\,.$$

Hence $(P_S)^* \cong P_{S^*}$. ■

Finally, we see that the symmetry of the group algebra also leads us to the symmetry of the Cartan matrix.

Theorem 23.6

If S and T are simple KG-modules, then

$$c_{ST} \cdot \dim_K \operatorname{End}_{KG}(S) = c_{TS} \cdot \dim_K \operatorname{End}_{KG}(T)\,.$$

In particular, if K is a splitting field for G, then the Cartan matrix of KG is symmetric.

Proof: By Corollary 22.3,

$$c_{ST} = \dim_K \operatorname{Hom}_{KG}(P_S, P_T)/\dim_K \operatorname{End}_{KG}(S)$$

and

$$c_{TS} = \dim_K \operatorname{Hom}_{KG}(P_T, P_S)/\dim_K \operatorname{End}_{KG}(T)\,,$$

so it is enough to prove that $\dim_K \operatorname{Hom}_{KG}(P_S, P_T) = \dim_K \operatorname{Hom}_{KG}(P_T, P_S)$.
Now, by Lemma 14.2 and Lemma 13.4 we have

$$\operatorname{Hom}_{KG}(P_S, P_T) = \operatorname{Hom}_K(P_S, P_T)^G \cong ((P_S)^* \otimes_K P_T)^G$$

and

$$\operatorname{Hom}_{KG}(P_T, P_S) = \operatorname{Hom}_K(P_T, P_S)^G \cong ((P_T)^* \otimes_K P_S)^G\,.$$

Moreover, as $(P_S)^* \otimes_K P_T$ is projective by Proposition 21.1(a), it follows from Corollary 23.5(a), that

$$\dim_K(((P_S)^* \otimes_K P_T)^G) = \dim_K(((P_S)^* \otimes_K P_T)^*)^G)\,.$$

But $((P_S)^* \otimes_K P_T)^* \cong P_S \otimes_K (P_T)^* \cong (P_T)^* \otimes_K P_S$, thus we have proved that $\dim_K \operatorname{Hom}_{KG}(P_S, P_T) = \dim_K \operatorname{Hom}_{KG}(P_T, P_S)$.
Finally, if K is a splitting field for G, then by definition $\operatorname{End}_{KG}(S) \cong K \cong \operatorname{End}_{KG}(T)$, so that the dimension of both endomorphism algebras is one and we have $c_{ST} = c_{TS}$ and we conclude that the Cartan matrix is symmetric. ■

24 Representations of cyclic groups in positive characteristic

We now describe the representations of a cyclic group $G := Z_n = \langle g \mid g^n = 1 \rangle$ of order $n \in \mathbb{Z}_{\geqslant 1}$ over a field K of positive characteristic.

Notation: Set $p := \mathrm{char}(K) > 0$ and write $n = p^a m$ with $a \in \mathbb{Z}_{\geqslant 0}$ and $\gcd(p, m) = 1$. Moreover, we assume that K is a splitting field for G, so it follows that K contains a primitive m-th root of unity, which we denote by ζ_m. This enables us to use the theory of Jordan normal forms (Linear Algebra).

Theorem 24.1

There are exactly n isomorphism classes of indecomposable KZ_n-modules. These correspond to the n matrix representations

$$R_{i,r} : G \to \mathrm{GL}_r(K), \quad g \mapsto \begin{bmatrix} \zeta_m^i & 1 & & \\ & \zeta_m^i & \ddots & \\ & & \ddots & 1 \\ & & & \zeta_m^i \end{bmatrix} \qquad (1 \leqslant i \leqslant m,\ 1 \leqslant r \leqslant p^a).$$

Proof: First notice that $R_{i,r}$ $(1 \leqslant i \leqslant m,\ 1 \leqslant r \leqslant p^a)$ defines a matrix representation of $G = Z_n$ since $R_{i,r}(g)^n = I_r$. Furthermore, if $(e_1, \ldots, e_r)$ is the standard K-basis of K^r, then the only Z_n-invariant subspaces are the $\langle e_1, \ldots, e_j \rangle_K$ with $1 \leqslant j \leqslant r$. As they form a chain, $R_{i,r}$ is indecomposable for all $1 \leqslant i \leqslant m$, $1 \leqslant r \leqslant p^a$, because it cannot be written as the direct sum of two non-trivial subrepresentations. It is also clear that the $R_{i,r}$ are pairwise non-equivalent, as they are uniquely determined through K-dimension and eigenvalues at evaluation in g.
It remains to prove that the $R_{i,r}$ $(1 \leqslant i \leqslant m,\ 1 \leqslant r \leqslant p^a)$ account for all the indecomposable KZ_n-modules. We know from the theory of Jordan normal form, that if M is a KG-module with $\dim_K(M) =: r \in \mathbb{Z}_{>0}$, then choosing a suitable K-basis, we may assume that M corresponds to a matrix representation R such that $R(g)$ is a block diagonal matrix where each block is a Jordan block. Assuming now that M is indecomposable, then there can be only one Jordan block. Moreover, as

$$R(g)^n = R(g^n) = R(1_G) = I_r\,,$$

the eigenvalues (i.e. the diagonal entries of the Jordan blocks) can only be n-th roots of unity in K, and hence they are powers ζ_m^i $(1 \leqslant i \leqslant m)$ of ζ_m since $\mathrm{char}(K) = p$. Furthermore,

$$R(g) = su = us$$

with $s = \mathrm{diag}(\zeta_m^i, \ldots, \zeta_m^i)$ and u is the Jordan block with diagonal entries equal to 1, where it holds that

$$(u - I_r)^{p^s} = u^{p^s} - I_r = 0 \quad \forall\ p^s \geqslant r,$$

so u is the p-part of $R(g)$ and it follows that $1 \leqslant r \leqslant p^a$.

■

Corollary 24.2

Up to isomorphism:

- the simple KZ_n-modules correspond precisely to the matrix representations $R_{i,1}$ $(1 \leqslant i \leqslant m)$;
- the PIMs of KZ_n correspond precisely to the matrix representations R_{i,p^a} $(1 \leqslant i \leqslant m)$.

Proof: We can bound the number of modules in both families of modules as follows.

- Firstly, the matrix representations $R_{i,1}$ ($1 \leqslant i \leqslant m$) all have degree 1, hence they must be irreducible and correspond to simple KZ_n-modules. It follows that there are at least m pairwise non-isomorphic simple KZ_n-modules.
- Secondly, by Corollary 21.5, if P is a PIM of KZ_n, then $p^a \mid \dim_K(P)$. Hence, up to equivalence, P corresponds to one of the matrix representations R_{i,p^a} with $1 \leqslant i \leqslant m$. It follows that there are at most m pairwise non-isomorphic PIMs.

However, we know from Theorem 21.2(c) that there is a bijection between the simple KZ_n-modules and the PIMs of KZ_n. The claim follows. ■

Chapter 7. Indecomposable Modules

After simple and projective modules, the goal of this chapter is to understand indecomposable modules in general. Apart for exceptions, the group algebra is of *wild representation type*, which, roughly speaking, means that it is not possible to classify the indecomposable modules over such algebras. However, representation theorists have developed tools which enable us to organise indecomposable modules in packages parametrised by parameters that are useful enough to understand essential properties of these modules. In this respect, first we will generalise the idea of projective modules seen in Chapter 6 by defining what is called **relative projectivity**. This will lead us to introduce the concepts of **vertices** and **sources** of indecomposable modules, which are two typical examples of parameters bringing us useful information about indecomposable modules in general.

Notation: throughout this chapter, unless otherwise specified, we let G denote a finite group and K be a commutative ring. All modules over group algebras considered are assumed to be **free of finite rank as K-modules**.

References:

[Alp86] J. L. Alperin. *Local representation theory*. Vol. 11. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1986.

[Ben98] D. J. Benson. *Representations and cohomology. I*. Vol. 30. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1998.

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. John Wiley & Sons, Inc., New York, 1990.

[LP10] K. Lux and H. Pahlings. *Representations of groups*. Vol. 124. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2010.

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

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

25 Relative projectivity

The relationship between the representations of a group and those of its subgroups are one of the most important tools in representation theory of finite groups. In the context of modular representation theory this relationship shows itself in a refinement of the notion of projectivity, namely relative projectivity.

Definition 25.1

Let $H \leqslant G$.

(a) A KG-module M is called H-**free** if $M \cong V\uparrow_H^G$ for some KH-module V.

(b) A KG-module M is called **relatively** H-**projective**, or simply H-**projective**, if it is isomorphic to a direct summand of an H-free module, i.e. if $M \mid V\uparrow_H^G$ for some KH-module V.

Remark 25.2

It is easy to see that H-freeness is a generalisation of freeness and relative projectivity is a generalisation of projectivity. Indeed,

- freeness is the same as $\{1\}$-freeness: as $KG \cong K\uparrow_{\{1\}}^G$ by Example 7, clearly $(KG)^n \cong (K^n)\uparrow_{\{1\}}^G$;
- projectivity is the same as $\{1\}$-projectivity: a KG-module is projective $\Leftrightarrow$ it is a direct summand of a free KG-module $\Leftrightarrow$ it is a direct summand of a $\{1\}$-free KG-module $\Leftrightarrow$ it is relatively $\{1\}$-projective.

To begin with, we would like to characterise relative projectivity in a similar way we characterised projectivity in Proposition-Definition B.5. To reach this aim, we first take a closer look at the adjunction between induction and restriction, we have seen in Theorem 15.10.

Notation 25.3

Let $H \leqslant G$.

(1) Let $\varphi : U_1 \longrightarrow U_2$ be a KH-homomorphism. Then we denote by $\varphi\uparrow_H^G$ the induced KG-homomorhpism

$$\varphi\uparrow_H^G := \mathrm{Id}_{KG} \otimes \varphi : U_1\uparrow_H^G = KG \otimes_{KH} U_1 \longrightarrow U_2\uparrow_H^G = KG \otimes_{KH} U_2$$
$$x \otimes u \mapsto x \otimes \varphi(u).$$

obtained by tensoring with the identity morphism on KG.

(2) Let U be a KH-module and V be a KG-module. The K-isomorphism

$$\Phi := \Phi_{U,V} : \mathrm{Hom}_{KG}(U\uparrow_H^G, V) \xrightarrow{\cong} \mathrm{Hom}_{KH}(U, V\downarrow_H^G)$$

and

$$\Psi := \Psi_{U,V} : \mathrm{Hom}_{KH}(U, V\downarrow_H^G) \xrightarrow{\cong} \mathrm{Hom}_{KG}(U\uparrow_H^G, V)$$

we obtained in Theorem 15.10 hides the fact that the induction and restriction functors Ind_H^G and Res_H^G form what is called *a pair of adjoint functors* in category theory. More precisely, this isomorphism translates the fact that Ind_H^G is *left adjoint* to Res_H^G.

Explained in more details, there may of course be many such isomorphisms, but there is a choice which is called *natural* in U and V. Spelled out, this means that whenever a morphism $\gamma \in \mathrm{Hom}_{KH}(U_1, U_2)$ is given, the diagram

$$\begin{array}{ccc} \mathrm{Hom}_{KG}(U_1\uparrow_H^G, V) & \xrightarrow[\cong]{\Phi_{U_1,V}} & \mathrm{Hom}_{KH}(U_1, V\downarrow_H^G) \\ {\scriptstyle (\gamma\uparrow_H^G)^*}\uparrow & & \uparrow{\scriptstyle \gamma^*} \\ \mathrm{Hom}_{KG}(U_2\uparrow_H^G, V) & \xrightarrow[\Phi_{U_2,V}]{\cong} & \mathrm{Hom}_{KH}(U_2, V\downarrow_H^G) \end{array}$$

commutes and whenever $\alpha \in \mathrm{Hom}_{KG}(V_1, V_2)$ is given, the diagram

$$\begin{array}{ccc} \mathrm{Hom}_{KH}(U, V_1\downarrow_H^G) & \xrightarrow[\cong]{\Psi_{U,V_1}} & \mathrm{Hom}_{KG}(U\uparrow_H^G, V_1) \\ {\scriptstyle \alpha_*}\downarrow & & \downarrow{\scriptstyle \alpha_*} \\ \mathrm{Hom}_{KH}(U, V_2\downarrow_H^G) & \xrightarrow[\Psi_{U,V_2}]{\cong} & \mathrm{Hom}_{KG}(U\uparrow_H^G, V_2) \end{array}$$

commutes. (For the upper and lower $*$ notation, see again Proposition D.3.)
Furthermore, such natural isomorphisms depend on certain distinguished homomorphisms called the **unit** and the **counit** of the adjunction. In order to understand relative H-projectivity, we need to consider the KH-homomorphism

$$\begin{aligned} \mu : U \longrightarrow U\uparrow_H^G\downarrow_H^G = \bigoplus_{g\in[G/H]} g\otimes U = 1\otimes U \oplus \bigoplus_{g\in[G/H], g\neq 1} g\otimes U \\ u \mapsto 1\otimes u \end{aligned}$$

(i.e. the natural inclusion of U into the summand $1\otimes U$) and the KG-homomorphism

$$\begin{aligned} \varepsilon : V\downarrow_H^G\uparrow_H^G = \bigoplus_{g\in[G/H]} g\otimes (V\downarrow_H^G) \longrightarrow V \\ g\otimes v \mapsto gv \end{aligned}$$

which are, respectively, the *unit* and the *counit* of the adjunction saying that Ind_H^G is *left adjoint* to Res_H^G. Further, we note that for any $u \in U$, we have $\varepsilon\circ\mu(u) = \varepsilon(1\otimes u) = u$, so $\varepsilon\circ\mu = \mathrm{Id}_U$ and thus we deduce that:

- μ is a KH-section for ε;
- μ is injective; and
- ε is surjective.

This allows us to construct mutually inverse natural K-isomorphisms

$$\Phi = \Phi_{U,V} : \mathrm{Hom}_{KG}(U\uparrow_H^G, V) \longrightarrow \mathrm{Hom}_{KH}(U, V\downarrow_H^G), \psi \mapsto \psi\circ\mu\,,$$

$$\Psi = \Psi_{U,V} : \mathrm{Hom}_{KH}(U, V\downarrow_H^G) \longrightarrow \mathrm{Hom}_{KG}(U\uparrow_H^G, V), \beta \mapsto \varepsilon\circ\beta\uparrow_H^G\,.$$

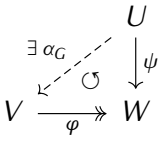
as required.

Proposition 25.4 (*Characterisation of relative projectivity*)

Let $H \leqslant G$. Let U be a KG-module. Then the following are equivalent.

(a) The KG-module U is relatively H-projective.

(b) If $\psi : U \longrightarrow W$ is a KG-homomorphism, $\varphi : V \twoheadrightarrow W$ is a surjective KG-homomorphism and there exists a KH-homomorphism $\alpha_H : U\downarrow_H^G \longrightarrow V\downarrow_H^G$ such that $\varphi \circ \alpha_H = \psi$ on $U\downarrow_H^G$, then there exists a KG-homomorphism $\alpha_G : U \longrightarrow V$ such that $\varphi \circ \alpha_G = \psi$ so that the diagram on the right commutes.



(c) Whenever $\varphi : V \twoheadrightarrow U$ is a surjective KG-homomorphism such that the restriction $\varphi : V\downarrow_H^G \longrightarrow U\downarrow_H^G$ splits as KH-homomorphism, then φ splits as a KG-homomorhpism.

(d) The surjective KG-homomorphism

$$\begin{aligned} U\downarrow_H^G\uparrow_H^G = KG \otimes_{KH} U &\longrightarrow U \\ x \otimes u &\mapsto xu \end{aligned}$$

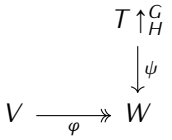
is split.

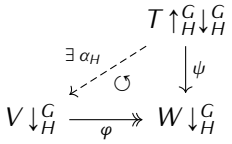
(e) The KG-module U is a direct summand of $U\downarrow_H^G\uparrow_H^G$.

(f) There exists a KG-module N such that $U \mid K\uparrow_H^G \otimes_K N$.

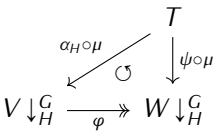
Proof:

(a)⇒(b): First we consider the case where $U = T\uparrow_H^G$ is an induced module. Suppose that we have KG-homomorphisms $\psi : T\uparrow_H^G \longrightarrow W$ and $\varphi : V \twoheadrightarrow W$ as shown in the diagram shown on the left below. Suppose, moreover, that there exists a KH-homomorhpism $\alpha_H : T\uparrow_H^G\downarrow_H^G \longrightarrow V\downarrow_H^G$ such that $\psi = \varphi \circ \alpha_H$, that is, the diagram on the right below commutes:





Let $\mu : T \longrightarrow T\uparrow_H^G\downarrow_H^G$ and $\varepsilon : V\downarrow_H^G\uparrow_H^G \longrightarrow V$ be the unit and the counit of the adjunction of Res_H^G and Ind_H^G as defined in Notation 25.3, so μ is an injective KH-homomorphism and ε is a surjective KG-homomorphism. Then, precomposing with μ, we obtain that the following triangle of KH-modules and KH-homomorphisms commutes:



By the naturality of Φ and Ψ from Notation 25.3, since $\varphi : V \longrightarrow W$ is a KG-homomorphism, we have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{KH}(T, V\downarrow_H^G) & \xrightarrow[\cong]{\Psi_{T,V}} & \mathrm{Hom}_{KG}(T\uparrow_H^G, V) \\ {\scriptstyle \varphi_*}\downarrow & & \downarrow{\scriptstyle \varphi_*} \\ \mathrm{Hom}_{KH}(T, W\downarrow_H^G) & \xrightarrow[\Psi_{T,W}]{\cong} & \mathrm{Hom}_{KG}(T\uparrow_H^G, W) \end{array}$$

In other words,

$$\Psi(\varphi \circ (\alpha_H \circ \mu)) = \varphi \circ (\Psi(\alpha_H \circ \mu)).$$

By the commutativity of the previous triangle, the left hand side of this equation is equal to $\Psi(\psi \circ \mu) = \Psi(\Phi(\psi)) = \psi$ since Ψ and Φ are inverse to one another. Thus

$$\psi = \varphi \circ \varepsilon \circ ((\alpha_H \circ \mu)\uparrow_H^G)$$

and so the triangle of KG-homomorphisms

$$\begin{array}{ccc} & & T\uparrow_H^G \\ & {\scriptstyle \varepsilon\circ((\alpha_H\circ\mu)\uparrow_H^G)}\swarrow \circlearrowleft & \downarrow{\scriptstyle \psi} \\ V & \xrightarrow[\varphi]{} & W \end{array}$$

commutes, proving the implication for $U = T\uparrow_H^G$ an induced module.
Now let U be any direct summand of $T\uparrow_H^G$. Let $U \xrightarrow{\iota} T\uparrow_H^G \xrightarrow{\pi} U$ denote the canonical inclusion and projection. Suppose that there is a KH-homomorphism $\alpha_H : U\downarrow_H^G \longrightarrow V\downarrow_H^G$ such that the diagram

$$\begin{array}{ccc} & & U\downarrow_H^G \\ & {\scriptstyle \exists\,\alpha_H}\swarrow \circlearrowleft & \downarrow{\scriptstyle \psi} \\ V\downarrow_H^G & \xrightarrow[\varphi]{} & W\downarrow_H^G \end{array}$$

commutes, i.e. $\varphi \circ \alpha_H = \psi$ on $U\downarrow_H^G$. Then we consider the following diagrams:

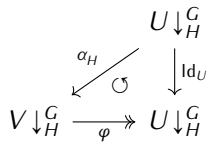
$$\begin{array}{ccc} & & T\uparrow_H^G \\ & & \downarrow{\scriptstyle \psi\circ\pi} \\ V & \xrightarrow[\varphi]{} & W \end{array} \qquad \begin{array}{ccc} & & T\uparrow_H^G\downarrow_H^G \\ & {\scriptstyle \alpha_H\circ\pi}\swarrow \circlearrowleft & \downarrow{\scriptstyle \psi\circ\pi} \\ V\downarrow_H^G & \xrightarrow[\varphi]{} & W\downarrow_H^G \end{array} \qquad \begin{array}{ccc} & & T\uparrow_H^G \\ & {\scriptstyle \alpha_G}\swarrow \circlearrowleft & \downarrow{\scriptstyle \psi\circ\pi} \\ V\downarrow_H^G & \xrightarrow[\varphi]{} & W \end{array}$$

The middle diagram of KH-homomorphisms commutes by definition of α_H, and hence by the first part there is a KG-homomorphism $\alpha_G : T\uparrow_H^G \longrightarrow V$ such that $\varphi \circ \alpha_G = \psi \circ \pi$, so the third diagram of KG-homomorhpisms also commutes.
Now $\varphi \circ \alpha_G \circ \iota = \psi \circ \pi \circ \iota = \psi$, so the triangle

$$\begin{array}{ccc} & & U \\ & {\scriptstyle \alpha_G\circ\iota}\swarrow \circlearrowleft & \downarrow{\scriptstyle \psi} \\ V & \xrightarrow[\varphi]{} & W \end{array}$$

commutes, as required.

(b)⇒(c): Let $\varphi : V \twoheadrightarrow U$ be a surjective KG-homomorphism which is split as a KH-homomorphism, and let α_H be a KH-section for φ. Thus, we have the following commutative diagram of KH-modules:



Then assuming (b) is true, there exists a KG-homomorphism $\alpha_G : U \longrightarrow V$ such that $\varphi \circ \alpha_G = \mathrm{Id}_U$. In particular, α_G is a KG-section for φ.

(c)⇒(d): Since $\mu : U \longrightarrow U\downarrow_H^G\uparrow_H^G$ is a KH-section for $\varepsilon : U\downarrow_H^G\uparrow_H^G \longrightarrow U$ (see Notation 25.3), applying condition (c) yields that ε splits as a KG-homomorhpism, and hence (d) holds.

(d)⇒(e): is immediate.

(e)⇒(f): Recall that by Proposition 15.11 we have $K\uparrow_H^G \otimes_K N \cong (K \otimes_K N\downarrow_H^G)\uparrow_H^G \cong N\downarrow_H^G\uparrow_H^G$. Thus, setting $N := U$ yields the claim.

(f)⇒(a): straightforward from the fact that $K\uparrow_H^G \otimes_K N \cong N\downarrow_H^G\uparrow_H^G$ seen above. ■

Exercise 25.5

Let $H \leqslant J \leqslant G$. Let U be a KG-module and let V be a KJ-module. Prove the following statements.

(a) If U is H-projective then U is J-projective.

(b) If U is a direct summand of $V\uparrow_J^G$ and V is H-projective, then U is H-projective.

(c) For any $g \in G$, U is H-projective if and only if ${}^gU$ is ${}^gH$-projective.

(d) Using part (f) of Proposition 25.4, prove that if U is H-projective and W is any KG-module, then $U \otimes_K W$ is H-projective.

Projectivity relative to a subgroup can be generalised as follows to projectivity relative to a KG-module:

Remark 25.6 (*Projectivity relative to KG-modules*)

(a) Let V be a KG-module. A KG-module M is termed *projective relative to the module* V or *relatively* V*-projective*, or simply V*-projective* if there exists a KG-module N such that M is isomorphic to a direct summand of $V \otimes_K N$, i.e. $M \mid V \otimes_K N$.
We let $\mathrm{Proj}(V)$ denote the class of all V-projective KG-modules.

(b) Proposition 25.4(f) shows that projectivity relative to a subgroup $H \leqslant G$ is in fact projectivity relative to the KG-module $V := K\uparrow_H^G$.

Note that the concept of projectivity relative to a subgroup is proper to the group algebra, but the concept of projectivity relative to a module is not and makes sense in general over algebras/rings.

The following exercise provides us with some elementary properties of projectivity relative to a module, which also hold for projectivity relative to a subgroup, by part (b) of the remark.

Exercise 25.7

Assume K is a field of characteristc $p > 0$ and let A, B, C, U, V be KG-modules. Prove that:

(a) Any direct summand of a V-projective KG-module is V-projective;

(b) If $U \in \mathrm{Proj}(V)$, then $\mathrm{Proj}(U) \subseteq \mathrm{Proj}(V)$;

(c) If $p \nmid \dim_K(V)$ then any KG-module is V-projective;

(d) $\mathrm{Proj}(V) = \mathrm{Proj}(V^*)$;

(e) $\mathrm{Proj}(U \oplus V) = \mathrm{Proj}(U) \oplus \mathrm{Proj}(V)$;

(f) $\mathrm{Proj}(U) \cap \mathrm{Proj}(V) = \mathrm{Proj}(U \otimes_K V)$;

(g) $\mathrm{Proj}(\bigoplus_{j=1}^{n} V) = \mathrm{Proj}(V) = \mathrm{Proj}(\bigotimes_{j=1}^{m} V) \ \ \forall\, m, n \in \mathbb{Z}_{>0}$;

(h) $C \cong A \oplus B$ is V-projective if and only if both A and B are V-projective;

(i) $\mathrm{Proj}(V) = \mathrm{Proj}(V^* \otimes_K V)$.

Hint: you may want to use Lemma 13.8 and Exercise 4(c) on Sheet 3. Proceed in the given order.

After this small parenthesis on projectivity relative to modules, we come back to projectivity relative to subgroups. We investigate further what information this concept brings to the understanding of indecomposable KG-modules in general.

Next we see that any indecomposable KG-module can be seen as a relatively projective module with respect to some subgroup of G.

Theorem 25.8

Let $H \leqslant G$.

(a) If $|G : H|$ is invertible in K, then every KG-module is H-projective.

(b) In particular, if K is a field of characteristic $p > 0$ and H contains a Sylow p-subgroup of G, then every KG-module is H-projective.

Proof: (a) Let V be a KG-module. To prove that V is H-projective, we prove that V satisfies Theorem 25.4(c). So let $\varphi : U \twoheadrightarrow V$ be a surjective KG-homomorphism which splits as a KH-homomorphism. We need to prove that φ splits as a KG-homomorphism.
So let $\sigma : V \longrightarrow U$ be a KH-linear section for φ and set

$$\begin{array}{rccc} \tilde{\sigma}: & V & \longrightarrow & U \\ & v & \mapsto & \frac{1}{|G:H|} \sum_{g \in [G/H]} g^{-1}\sigma(gv). \end{array}$$

We may divide by $|G : H|$ since $|G : H| \in K^\times$ and clearly $\tilde{\sigma}$ is well-defined. Now, if $g' \in G$ and $v \in V$, then

$$\tilde{\sigma}(g'v) = \frac{1}{|G:H|} \sum_{g \in [G/H]} g^{-1}\sigma(gg'v) = g' \frac{1}{|G:H|} \sum_{g \in [G/H]} (gg')^{-1}\sigma(gg'v) = g'\tilde{\sigma}(v)$$

and

$$\varphi\widetilde{\sigma}(v) = \frac{1}{|G:H|}\sum_{g\in G}\varphi\left(g^{-1}\sigma(gv)\right) \overset{\varphi\, KG\text{-lin.}}{=} \frac{1}{|G:H|}\sum_{g\in G} g^{-1}\varphi\sigma(gv) = \frac{1}{|G:H|}\sum_{g\in G} g^{-1}gv = v$$

where the last-but-one equality holds because $\varphi\sigma = \mathrm{Id}_V$. Thus $\widetilde{\sigma}$ is a KG-linear section for φ.

(b) follows immediately from (a). Indeed, if $P \in \mathrm{Syl}_p(G)$ and $H \supseteq P$, then $p \nmid |G:H|$, so $|G:H| \in K^\times$. ■

Considering the case $H = \{1\}$ shows that the previous Theorem is in some sense a generalisation of Maschke's Theorem (Theorem 11.1).

Remark 25.9

Assume that K is a field of characteristic $p > 0$ and $H = \{1\}$ is the trivial subgroup. If H contains a Sylow p-subgroup of G then the Sylow p-subgroups of G are trivial, so $p \nmid |G|$. The theorem then says that all KG-modules are $\{1\}$-projective and hence projective.

We know this already, however! If $p \nmid |G|$ then KG is semisimple by Maschke's Theorem (Theorem 11.1), and so all KG-modules are projective by Example 10(d).

Corollary 25.10

Let $H \leqslant G$ and suppose that $|G:H|$ is invertible in K. Then a KG-module U is projective if and only if $U{\downarrow}^G_H$ is projective.

Again, this holds in particular if K is a field of characteristic $p \geqslant 0$ and H contains a Sylow p-subgroup of G.

Proof: The necessary condition is given by Proposition 21.1(b). To prove the sufficient condition, suppose that $U{\downarrow}^G_H$ is projective. Then, on the one hand,

$$U{\downarrow}^G_H \mid (KH)^n \qquad \text{for some } n \in \mathbb{Z}_{>0}\,.$$

On the other hand, U is H-projective by Theorem 25.8, and it follows from Proposition 25.4(e) that

$$U \mid U{\downarrow}^G_H{\uparrow}^G_H\ .$$

Hence

$$U \mid U{\downarrow}^G_H{\uparrow}^G_H \mid (KH)^n{\uparrow}^G_H \cong (KG)^n\,,$$

so U is projective. ■

26 Vertices and sources

For the remainder of this chapter, we assume that K is a field with $\mathrm{char}(K) =: p > 0$.

As said before, we now want to explain some techniques that are available to understand indecomposable modules better. Vertices and sources are two parameters making this possible.

Theorem 26.1

Let U be an indecomposable KG-module.

(a) There is a unique conjugacy class of subgroups Q of G which are minimal subject to the property that U is Q-projective.

(b) Let Q be a minimal subgroup of G such that U is Q-projective. Then, there exists an indecomposable KQ-module T which is unique, up to conjugacy by elements of $N_G(Q)$, such that U is a direct summand of $T\uparrow_Q^G$. Such a KQ-module T is necessarily a direct summand of $U\downarrow_Q^G$.

Proof:

(a) Suppose that U is both H- and K-projective for subgroups H and K of G. Then, by Proposition 25.4(e),

$$U \mid U\downarrow_H^G\uparrow_H^G \qquad \text{and} \qquad U \mid U\downarrow_K^G\uparrow_K^G \ .$$

Hence U is also a direct summand of $U\downarrow_H^G\uparrow_H^G\downarrow_K^G\uparrow_K^G$. By the Mackey formula and transitivity of induction and restriction, it follows that

$$\begin{aligned} U\downarrow_H^G\uparrow_H^G\downarrow_K^G\uparrow_K^G &= \Big(\big(U\downarrow_H^G\big)\uparrow_H^G\downarrow_K^G \Big)\uparrow_K^G \\ &= \Big(\bigoplus_{g\in[K\backslash G/H]} \big({}^g\big(U\downarrow_H^G\big)\downarrow_{K\cap {}^gH}^{{}^gH}\big)\uparrow_{K\cap {}^gH}^K \Big)\uparrow_K^G \\ &= \bigoplus_{g\in[K\backslash G/H]} \big({}^gU\downarrow_{K\cap {}^gH}^G\big)\uparrow_{K\cap {}^gH}^G . \end{aligned}$$

Therefore, by the Krull-Schmidt Theorem, there exists $g \in G$ such that U is a direct summand of a module induced from $K \cap {}^gH$, and hence U is $K \cap {}^gH$-projective. Now, if both K and H are minimal such that U is projective relative to these subgroups, then $K \cap {}^gH = K$. Thus, $K \subseteq {}^gH$ and $H \subseteq {}^{g^{-1}}K$, hence H and K are G-conjugate.

(b) Let Q be a minimal subgroup relative to which U is projective. Then $U \mid U\downarrow_Q^G\uparrow_Q^G$ by Proposition 25.4(e) so it is a direct summand of $T\uparrow_Q^G$ for some indecomposable direct summand T of $U\downarrow_Q^G$. If T' is another indecomposable KQ-module such that $U \mid T'\uparrow_Q^G$, then $T \mid T'\uparrow_Q^G\downarrow_Q^G$. Mackey's formula says that

$$T'\uparrow_Q^G\downarrow_Q^G = \bigoplus_{g\in[Q\backslash G/Q]} ({}^gT'\downarrow_{Q\cap {}^gQ}^{{}^gQ})\uparrow_{Q\cap {}^gQ}^Q ,$$

hence, again by the Krull-Schmidt Theorem, there exists $g \in G$ such that

$$T \mid ({}^gT'\downarrow_{Q\cap {}^gQ}^{{}^gQ})\uparrow_{Q\cap {}^gQ}^Q$$

and therefore T is $Q \cap {}^gQ$-projective, and hence so is U. Since Q is a minimal subgroup relative to which U is projective, $Q = Q \cap {}^gQ$ and hence $g \in N_G(Q)$. It follows that T is actually a direct summand of ${}^gT'$, for this $g \in G$. Since T and T' are indecomposable, however, this means that $T = {}^gT'$, so T is unique up to conjugacy by elements of $N_G(Q)$.

Now $T = {}^gT'$ is an idecomposable direct summand of $U\downarrow_Q^G$ by definition, so $T' = {}^{g^{-1}}T$ is a direct summand of $({}^{g^{-1}}U)\downarrow_Q^G$. However, $U \cong {}^{g^{-1}}U$ as KG-modules, so this means that T' is also a direct summand of $U\downarrow_Q^G$. ∎

This characterisation leads us to the following definition:

Definition 26.2

Let U be an indecomposable KG-module.

(a) A **vertex** of U is a minimal subgroup Q of G such that U is relatively Q-projective. The set of all vertices of U is denoted by $\mathrm{vtx}(U)$.

(b) Given a vertex Q of U, a KQ-**source**, or simply a **source** of U is a KQ-module T such that $U \mid T\uparrow_Q^G$.

Remark 26.3

(a) Conceptually, the closer the vertices of a module are to the trivial subgroup, the closer this module is to being projective: a KG-module U with trivial vertex is $\{1\}$-projective and hence projective.

(b) A vertex Q of an indecomposable KG-module U is not uniquely defined, in general. However, the vertices of U are unique **up to** G-**conjugacy**, so in particular are all isomorphic. For this reason, in general, one (i.e. you!) should **never** talk about *the* vertex of a module (of course, unless a vertex has been fixed). We either say that Q *is* a *vertex of* U, or talk about *the vertices of* U. (Unfortunately many textbooks/articles by non-experts are very sloppy with this terminology, inducing errors.)

(c) For a fixed vertex Q of U, a source of U is defined up to conjugacy by elements of $N_G(Q)$.

To begin with, we have the following important restriction on the structure of the vertices.

Proposition 26.4

The vertices of an indecomposable KG-module are p-subgroups of G.

Proof: By Theorem 25.8, we know that every KG-module is projective relative to a Sylow p-subgroup of G. Therefore, by minimality, vertices are contained in Sylow p-subgroups, and hence are themselves p-groups. ∎

Warning: vertices and sources are very useful theoretical tools in general, but extremely difficult to compute concretely.

We show here how to compute the vertices and sources of the trivial module.

Example 11

The vertices of the trivial KG-module K are the Sylow p-subgroups of G, i.e. $\mathrm{vtx}(K) = \mathrm{Syl}_p(G)$, and all sources are trivial.

To establish this fact, we need the following indecomposability property:

Claim: If P is a p-group and $H \leqslant P$, then $K\uparrow_H^P$ is an indecomposable KP-module.

Indeed: First recall that as P is a p-group, the only simple KP-module is the trivial module. Hence the socle of $K\uparrow_H^P$ is a direct sum of trivial submodules. This together with Frobenius reciprocity

yields

$$\dim_K \operatorname{soc}(K\uparrow_H^P) = \dim_K \operatorname{Hom}_{KP}(K, K\uparrow_H^P) = \dim_K \operatorname{Hom}_{KH}(K\downarrow_H^P, K) = \dim_K \operatorname{Hom}_{KH}(K,K) = 1\,.$$

If $K\uparrow_H^P$ were decomposable, then so would be its socle: clearly, if $K\uparrow_H^P = U \oplus V$ for some KP-modules $U, V \neq 0$, then

$$\dim_K \operatorname{soc}(K\uparrow_H^P) = \dim_K (\operatorname{soc}(U) \oplus \operatorname{soc}(V)) = \dim_K \operatorname{soc}(U) + \dim_K \operatorname{soc}(V) \geqslant 1+1 = 2\,.$$

A contradiction! Therefore $K\uparrow_H^P$ is indecomposable.

Now, let $Q \in \operatorname{vtx}(K)$ and let $P \in \operatorname{Syl}_p(G)$ such that $P \geqslant Q$. Since K is Q-projective,

$$K \mid K\downarrow_Q^G\uparrow_Q^G = K\uparrow_Q^G$$

so

$$K\downarrow_P^G \mid K\uparrow_Q^G\downarrow_P^G = \bigoplus_{g\in[P\backslash G/Q]} K\uparrow_{P\cap {}^gQ}^P$$

by the Mackey formula, and hence, by the Krull-Schmidt Theorem, is a direct summand of $K\uparrow_{P\cap {}^gQ}^P$ for some $g \in G$, which is indecomposable by the Claim. Thus

$$K = K\downarrow_P^G = K\uparrow_{P\cap {}^gQ}^P$$

and hence $P \cap {}^gQ = P$, so ${}^gQ = P$. Therefore, Q is a Sylow p-subgroup of G and it follows from Theorem 26.1(a), that $\operatorname{vtx}(K) = \operatorname{Syl}_p(G)$. Finally, it is clear that the trivial KQ-module is a KQ-source, and hence all sources are trivial.

27 The Green correspondence

The Green correspondence is a correspondence which relates the indecomposable KG-modules with a fixed vertex with the indecomposable KL-modules with the same vertex for well-chosen subgroups $L \leqslant G$. It is used to reduce questions about indecomposable modules to a situation where a vertex of the given indecomposable module is a normal subgroup. This technique is very useful in many situations. In fact, many properties in modular representation theory are believed to be determined by normalisers of p-subgroups.

Lemma 27.1

Let $Q \leqslant G$ be a p-subgroup and let $L \leqslant G$.

(a) If U is an indecomposable KG-module with vertex Q and $L \geqslant Q$, then there exists an indecomposable direct summand of $U\downarrow_L^G$ with vertex Q.

(b) If $L \geqslant N_G(Q)$, then the following assertions hold.

(i) If V is an indecomposable KL-module with vertex Q and U is a direct summand of $V\uparrow_L^G$ such that $V \mid U\downarrow_L^G$, then Q is also a vertex of U.

(ii) If V is an indecomposable KL-module which is Q-projective and there exists an indecomposable direct summand U of $V\uparrow_L^G$ with vertex Q, then Q is also a vertex of V.

Proof: Exercise, Sheet 5. ∎

Theorem 27.2 (*Green Correspondence*)

Let Q be a p-subgroup of G and let L be a subgroup of G containing $N_G(Q)$.

(a) If U is an indecomposable KG-module with vertex Q, then

$$U\downarrow_L^G = f(U) \oplus X$$

where $f(U)$ is the unique indecomposable direct summand of $U\downarrow_L^G$ with vertex Q and every direct summand of X is $L \cap {}^xQ$-projective for some $x \in G\backslash L$.

(b) If V is an indecomposable KL-module with vertex Q, then

$$V\uparrow_L^G = g(V) \oplus Y$$

where $g(V)$ is unique indecomposable direct summand of $V\uparrow_L^G$ with vertex Q and every direct summand of Y is $Q \cap {}^xQ$-projective for some $x \in G\backslash L$.

(c) With the notation of (a) and (b), we then have $g(f(U)) \cong U$ and $f(g(V)) \cong V$. In other words, f and g define a bijection

$$\begin{Bmatrix}\text{isomorphism classes of indecomposable}\\ KG\text{-modules with vertex } Q\end{Bmatrix} \quad \overset{\sim}{\longleftrightarrow} \quad \begin{Bmatrix}\text{isomorphism classes of indecomposable}\\ KL\text{-modules with vertex } Q\end{Bmatrix}$$

$$U \quad \mapsto \quad f(U)$$

$$g(V) \quad \mapsfrom \quad V \ .$$

Moreover, corresponding modules have a source in common.

Terminology: $f(U)$ is called the KL-**Green correspondent** of U (or simply the **Green correspondent**) and $g(V)$ is called the KG-**Green correspondent of** V (or simply the **Green correspondent** of V).

Warning! In the Green correspondence it is essential that a vertex Q is fixed and not considered up to conjugation, because the G-conjugacy class of Q and the L-conjugacy class of Q do not coincide in general.

Proof: We first note some properties of the subgroups $Q \cap {}^xQ$ and $L \cap {}^xQ$ for $x \in G\backslash L$:

$(*)$ Since $N_G(Q) \leqslant L$, x does not normalise Q and hence $Q \cap {}^xQ$ is a proper subgroup of Q.

$(**)$ $L \cap {}^xQ$ may be of the same order as Q, in which case $L \cap {}^xQ = {}^xQ$.

$(***)$ Suppose that $L \cap {}^xQ$ is conjugate to Q in L, i.e. there exists $z \in L$ such that $L \cap {}^xQ = {}^zQ$. Then ${}^xQ = {}^zQ$ so ${}^{z^{-1}x}Q = Q$ and hence $z^{-1}x \in N_G(Q) \leqslant L$. Therefore $x \in zL = L$. This contradicts $x \in G\backslash L$. Therefore $L \cap {}^xQ$ is never conjugate to Q in L.

(b) Let V be an indecomposable KL-module with vertex Q.

Claim. The KL-module $V\uparrow_L^G\downarrow_L^G$ has a unique direct summand with vertex Q, and all other direct summands are projective relative to subgroups of the form $L \cap {}^xQ$ with $x \in G\backslash L$.

Pf of the Claim: Let T be a KQ-source for V. Then, we may write $T\uparrow_Q^L = V \oplus Z$ for some KL-module Z. Moreover, there exist KL-modules V' and Z' such that $V\uparrow_L^G\downarrow_L^G = V \oplus V'$ and $Z\uparrow_L^G\downarrow_L^G = Z \oplus Z'$. Then, on the one hand we have

$$T\uparrow_Q^G\downarrow_L^G = (V \oplus Z)\uparrow_L^G\downarrow_L^G = V\uparrow_L^G\downarrow_L^G \oplus Z\uparrow_L^G\downarrow_L^G = V \oplus V' \oplus Z \oplus Z' \, .$$

On the other hand, by the Mackey formula we also have

$$\begin{aligned} T\uparrow_Q^G\downarrow_L^G &\cong \bigoplus_{x\in[L\backslash G/Q]} ({}^xT\downarrow_{L\cap {}^xQ}^{{}^xQ})\uparrow_{L\cap {}^xQ}^L \\ &= T\uparrow_Q^L \oplus \bigoplus_{\substack{x\in[L\backslash G/Q]\\ x\notin L}} ({}^xT\downarrow_{L\cap {}^xQ}^{{}^xQ})\uparrow_{L\cap {}^xQ}^L \\ &= V\oplus Z\oplus \bigoplus_{\substack{x\in[L\backslash G/Q]\\ x\notin L}} ({}^xT\downarrow_{L\cap {}^xQ}^{{}^xQ})\uparrow_{L\cap {}^xQ}^L \ . \end{aligned}$$

Therefore, by the Krull-Schmidt Theorem, we have

$$V'\oplus Z' \cong \bigoplus_{\substack{x\in[L\backslash G/Q]\\ x\notin L}} ({}^xT\downarrow_{L\cap {}^xQ}^{{}^xQ})\uparrow_{L\cap {}^xQ}^L$$

where, clearly, all direct summands are $L\cap {}^xQ$-projective for some $x\notin L$. It follows that V is the unique direct summand of $V\uparrow_L^G\downarrow_L^G = V\oplus V'$ with vertex Q, because all the direct summands in V' are projective relative to subgroups of the form $L\cap {}^xQ$ with $x\notin L$ and so are not Q-projective by $(***)$. This proves the Claim.

Now, write $V\uparrow_L^G$ as a direct sum of indecomposable KG-modules and pick a direct summand U such that $V\mid U\downarrow_L^G$. By Lemma 27.1(b), since Q is a vertex of V, Q is also a vertex of U. Therefore $V\uparrow_L^G$ has at least one direct summand with vertex Q. To prove its uniqueness, assume U' is another indecomposable direct summand of $V\uparrow_L^G$. Then

$$V\uparrow_L^G = U\oplus U'\oplus X$$

for some KG-module X, so in the notation of the claim,

$$V\oplus V' = U\downarrow_L^G \oplus U'\downarrow_L^G \oplus X\downarrow_L^G \ .$$

As $V\mid U\downarrow_L^G$, by the Krull-Schmidt-Theorem, $U'\downarrow_L^G\mid V'$ and hence every indecomposable direct summand of $U'\downarrow_L^G$ is $L\cap {}^yQ$-projective for some $y\notin L$ by the proof of the Claim. Now since $V\mid T\uparrow_Q^L$ and $U'\mid V\uparrow_L^G$ it follows that

$$U'\mid T\uparrow_Q^L\uparrow_L^G = T\uparrow_Q^G \ .$$

Thus U' is Q-projective and therefore has a vertex Q' contained in Q.

It remains to prove that $Q'\lneq Q$. So let S be a KQ'-source of U'. Then $S\mid U'\downarrow_{Q'}^G$ by Theorem 26.1(b). Since $Q'\leqslant L$, $U'\downarrow_{Q'}^G = U'\downarrow_L^G\downarrow_{Q'}^L$ and hence S is a direct summand of $Y\downarrow_{Q'}^L$ for some indecomposable direct summand Y of $U'\downarrow_L^G$. It follows from Lemma 27.1 that Q' is also a vertex of Y. But the indecomposable direct summands of $U'\downarrow_L^G$ are all $L\cap {}^yQ$-projective for some $y\notin L$. Therefore one of the subgroups $L\cap {}^yQ$ with $y\notin L$ contains an L-conjugate of Q'. I.e. ${}^zQ'\subseteq L\cap {}^yQ$ for some $z\in L$. Hence $Q'\subseteq {}^{z^{-1}y}Q$ where $z^{-1}y\notin L$ and so there exists $x\in G\backslash L$ such that $Q'\subseteq Q\cap {}^xQ\lneq Q$ by $(*)$. Therefore, we may set $g(V) := U$ and the assertion follows.

(a) Suppose now that U is an indecomposable KG-module with vertex Q and let T be a KQ-source of U. Then U is a direct summand of $T\uparrow_Q^G = T\uparrow_Q^L\uparrow_L^G$, so there is an indecomposable direct summand V of $T\uparrow_Q^L$ such that $U\mid V\uparrow_L^G$. This means that V is Q-projective, and so Q is a vertex of V by Lemma 27.1(b).

Now, by Lemma 27.1(a), there exists an indecomposable direct summand Y of $U\downarrow_L^G$ with vertex Q. But $U\downarrow_L^G\mid V\uparrow_L^G\downarrow_L^G$ and the Claim says that the only direct summand of $V\uparrow_L^G\downarrow_L^G$ with vertex Q is V. Therefore $Y\cong V$ and the remaining direct summands of $U\downarrow_L^G$ are $L\cap {}^xQ$-projective for some $x\in G\backslash L$. This proves part (a).

(c) The claim follows immediately from parts (a) and (b) and the facts that $U\mid U\downarrow_L^G\uparrow_L^G$ and $V\mid V\uparrow_L^G\downarrow_L^G$. ■

Exercise 27.3

(a) Verify that modules corresponding to each other via the Green correspondence have a source in common.

(b) Prove that the Green correspondent of the trivial module is the trivial module.

28 p-permutation modules

Recall from Example 4(b) that any finite G-set X gives rise to a K-representation ρ_X of G. The KG-module corresponding to ρ_X through Proposition 10.3 admits X as K-basis, hence it is standard to denote this module by KX and it is called the **permutation KG-module on X**. Thus, we may pose the following definition.

Definition 28.1 (*Permutation module*)

A KG-module is called a **permutation** KG-module if it admits a K-basis X which is invariant under the action of G. We denote this module by KX.

(Note: it is clear that the basis X is then a finite G-set.)

Permutation KG-modules and, in particular, their indecomposable direct summands have remarkable properties, which we investigate in this section.

Remark 28.2

First, we describe permutation modules and some of their properties more precisely.

If KX is a permutation KG-module on X, then a decomposition of the basis X as a disjoint union of G-orbits, say $X = \bigsqcup_{i=1}^{n} X_i$, yields a direct sum decomposition of KX as a KG-module as

$$KX = \bigoplus_{i=1}^{n} KX_i .$$

Thus, without loss of generality, we can assume that X is a transitive G-set, in which case

$$KX \cong K\uparrow_H^G$$

where $H := \mathrm{Stab}_G(x)$, the stabiliser in G of some $x \in X$. Indeed, clearly we have a direct sum decomposition as a K-vector space

$$KX = \bigoplus_{g \in [G/H]} Kgx$$

and G acts transitively on the summands, so that $KX = K\uparrow_H^G$.

It follows that an arbitrary permutation KG-module is isomorphic to a direct sum of KG-modules of the form $K\uparrow_H^G$ for various $H \leqslant G$.

Notice that, conversely, an induced module of the form $K\uparrow_H^G$ ($H \leqslant G$) is always a permutation KG-module. Indeed, as $K\uparrow_H^G = KG \otimes_{KH} K = \bigoplus_{g \in [G/H]} g \otimes K$ as K-vector space, it has on obvious

G-invariant K-basis given by the set

$$\{g \otimes 1_K \mid g \in [G/H]\}.$$

In fact, more generally if $H \leqslant G$ and KX is a permutation KH-module on X, then $KX\uparrow_H^G$ is a permutation KG-module with G-invariant K-basis $\{g \otimes x \mid g \in [G/H], x \in X\}$. In other words, induction preserves permutation modules.

Exercise 28.3

Prove that direct sums, restriction, inflation and conjugation also preserve permutation modules.

Next, we investigate the indecomposable direct summands of the permutation KG-modules. In order to understand the indecomposable ones, we are going to prove that they all have a trivial source and we will apply the Green correspondence to see that, up to isomorphism, there are only a finite number of them.

Definition 28.4 (*trivial source module*)

A KG-module is called a **trivial source** KG-module if it is a finite direct sum of KG-modules with a trivial source K.

Warning: Some texts (books/articles/...) require that a trivial source module is indecomposable, others do not.

Proposition-Definition 28.5 (*p-permutation module*)

Let M be a KG-module and let $P \in \mathrm{Syl}_p(G)$. Then, the following conditions are equivalent:

(a) $M\downarrow_Q^G$ is a permutation KQ-module for each p-subgroup $Q \leqslant G$;

(b) $M\downarrow_P^G$ is a permutation KP-module;

(c) M has a K-basis which is invariant under the action of P;

(d) M is isomorphic to a direct summand of a permutation KG-module;

(e) M is a trivial source KG-module.

If M fulfils one of these equivalent conditions, then it is called a ***p*-permutation** KG-module.

Note. In fact *p-permutation* KG-modules and *trivial source* KG-modules are two different pieces of terminology for the same concept. French/German speaking authors tend to favour the use of the terminology *p-permutation module* (and reserve the terminology *trivial source module* for an indecomposable module with a trivial source), whereas English speaking authors tend to favour the use of the terminology *trivial source module*.

Proof:

(a)⇔(b): It is obvious that (a) implies (b). For the sufficient condition, notice that for each $g \in G$, we have $M\downarrow_{gP}^G \cong {}^g(M\downarrow_P^G)$. Therefore, as by Exercise 28.3 restriction and conjugation preserve permutation modules, requiring that $M\downarrow_P^G$ is a permutation KP-module implies that $M\downarrow_Q^G$ is a permutation

KQ-module for each p-subgroup $Q \leqslant G$. (Because any p-subgroup Q of G is contained in a Sylow p-subgroup and these are all G-conjugate by the Sylow theorems.)

(b)⇔(c): is obvious by the definition of a permutation KP-module.

(b)⇒(e): **Claim**: If L is a KG-module satisfying (b), then so does any direct summand of L.

Proof of the Claim: By Remark 28.2, if $L{\downarrow}_P^G$ is a permutation KP-module, then there exist $n \in \mathbb{Z}_{n\geqslant 1}$ and subgroups $Q_i \leqslant G$ $(1 \leqslant i \leqslant n)$ such that

$$L{\downarrow}_P^G \cong \bigoplus_{i=1}^{n} K{\uparrow}_{Q_i}^P ,$$

where each $K{\uparrow}_{Q_i}^P$ is indecomposable by the Claim in Example 11. Therefore, by the Krull–Schmidt theorem, if $N \mid L$, then $N{\downarrow}_P^G$ is isomorphic to the direct sum of some of the factors, hence is again a permutation KP-module (by Remark 28.2) and so N satisfies (b) as well, as required.

Now, if M satisfies (b), then by the Claim we can assume w.l.o.g. that M is indecomposable. Let Q be a vertex of M. Then $M \mid M{\downarrow}_Q^G{\uparrow}_Q^G$ by Q-projectivity. Since $M{\downarrow}_Q^G$ is a permutation KQ-module by (a) (⇔ (b)), again by Remark 28.2, there exist $n \in \mathbb{Z}_{\geqslant 0}$ and subgroups $R_i \leqslant Q$ $(1 \leqslant i \leqslant n)$ such that

$$M{\downarrow}_Q^G \cong \bigoplus_{i=1}^{n} K{\uparrow}_{R_i}^Q \ .$$

Inducing this module to G again and using the Krull-Schmidt theorem, we deduce that M, being indecomposable, is isomorphic to a direct summand of $K{\uparrow}_{R_i}^G$ for some $1 \leqslant i \leqslant n$. By minimality of the vertex Q, it follows that $R_i = Q$ and that the trivial KQ-module K must be a source of M, proving that M is a trivial source KG-module.

(e)⇒(d): If L is an indecomposable trivial source module, say with vertex $Q \leqslant G$, then by definition of a source, $L \mid K{\uparrow}_Q^G$. This implies (d) as $K{\uparrow}_Q^G$ is a permutation KG-module by Remark 28.2 and any finite direct sum of permutation KG-module is again permutation.

(d)⇒(b): Assume that $M \mid Z$, where Z is a permutation KG-module. Then $M{\downarrow}_P^G \mid Z{\downarrow}_P^G$, where $Z{\downarrow}_P^G$ is again a permutation KP-module by Exercise 28.3. Thus, it follows from the Claim in (b)⇒(e) (see also the scholium below) that $M{\downarrow}_P^G$ is a permutation KP-module, as required. ■

The Claim in (b)⇒(e) can be formulated as the following result.

Scholium 28.6

If M is a p-permutation KG-module, then any direct summand of M is again a p-permutation KG-module. In particular, if G is a p-group, then any direct summand of a permutation KG-module is a permutation KG-module and so, in this case, any p-permutation module is a permutation module.

Exercise 28.7

Prove that p-permutation modules are preserved by the following operations: direct sums, tensor products, restriction, inflation, conjugation, induction.

Example 12

It is clear that any projective KG-module is a p-permutation KG-module. Also, the PIMs of KG are precisely the KG-modules with vertex $\{1\}$ and trivial source.

Generalising this example, we can characterise the indecomposable p-permutation KG-modules with a given vertex $Q \leqslant G$ as described below.

Example 13

(1) If M is an indecomposable p-permutation KG-module with vertex $Q \leqslant G$, then Q acts trivially on the $KN_G(Q)$-Green correspondent $f(M)$ of M. Thus $f(M)$ can be viewed as a $K[N_G(Q)/Q]$-module. As such, $f(M)$ is indecomposable and projective.

(2) Conversely, if N is a projective indecomposable $K[N_G(Q)/Q]$-module, then $\mathrm{Inf}_{N_G(Q)/Q}^{N_G(Q)}(N)$ is an indecomposable $KN_G(Q)$-module with vertex Q and trivial source. Its KG-Green correspondent is then also an indecomposable KG-module with vertex Q and trivial source, hence is an indecomposable p-permutation KG-module

(3) In this way we obtain a bijection

$$\left\{\begin{array}{c}\text{isomorphism classes of indecomposable}\\ p\text{-permutation } KG\text{-modules with vertex } Q\end{array}\right\} \quad \stackrel{\sim}{\longleftrightarrow} \quad \left\{\begin{array}{c}\text{isomorphism classes of projective}\\ \text{indecomposable } K[N_G(Q)/Q]\text{-modules}\end{array}\right\}.$$

29 Green's indecomposability theorem

To finish our analysis of indecomposable KG-modules we mention without proof an important indecomposability criterion due to J. A. Green (1959). The proof is rather involved and goes beyond the scope of the techniques we have developed so far.

Theorem 29.1 (*Green's indecomposability criterion, 1959*)

Assume that K is an algebraically closed field. Let $H \leqslant G$ be a subnormal subgroup of G of index a power of p and let M be an indecomposable KH-module. Then $M\uparrow_H^G$ is an indecomposable KG-module.

Proof: Without proof in this lecture. See [Thé95, (23.6) Corollary]. ■

Remark 29.2

Green's indecomposability criterion remains true over an arbitrary field of characteristic p, provided we replace *indecomposability* with *absolute indecomposability*. (A KG-module M is called absolutely indecomposable iff its endomorphism algebra $\mathrm{End}_{KG}(M)$ is a *split local algebra*, that is, if $\mathrm{End}_{KG}(M)/J(\mathrm{End}_{KG}(M)) \cong K$.)

Corollary 29.3

Assume that K is an algebraically closed field. If P is a p-group, $Q \leqslant P$ and M is an indecomposable KQ-module, then $M\uparrow_Q^P$ is an indecomposable KP-module.

Proof: By the Sylow theory, since P is a p-group, any subgroup $Q \leqslant P$ can be plugged in a subnormal series where each quotient is cyclic of order p, hence is a subnormal subgroup of P. Therefore, the claim follows immediately from Green's indecomposability criterion. ■

Notice that, in Example 11, we have proved the latter result in the particular case that $M = K$ is the trivial KQ-module using simple arguments.

Exercise 29.4

Assume that K is an algebraically closed field and let M be an indecomposable KG-module.

(a) Let $Q \in \mathrm{vtx}(M)$ and let $P \in \mathrm{Syl}_p(G)$ such that $Q \leqslant P$. Prove that $|P : Q| \,\big|\, \dim_K(M)$.

(b) Prove that if $\dim_K(M)$ is coprime to p, then $\mathrm{vtx}(M) = \mathrm{Syl}_p(G)$.

Chapter 8. p-Modular Systems

R. Brauer started in the late 1920's a systematic investigation of group representations over fields of positive characteristic. In order to relate group representations over fields of positive characteristic to character theory in characteristic zero, Brauer worked with a triple of rings $(F, \mathcal{O}, k)$, called a *p-modular system*, and consisting of a complete discrete valuation ring $\mathcal{O}$ with a residue field $k := \mathcal{O}/J(\mathcal{O})$ of prime characteristic p and fraction field $F := \mathrm{Frac}(\mathcal{O})$ of characteristic zero. The present chapter contains a short introduction to these concepts. We will use p-modular systems and *Brauer 's reciprocity theorem* in the subsequent chapters to gain information about kG and its modules (which is/are extremely complicated) from the group algebra FG, which is semisimple and therefore much better understood, via the group algebra $\mathcal{O}G$. This explains why we considered arbitrary associative rings (resp. fields) K in the previous chapters rather than immediately focusing on fields of positive characteristic.

Notation. Throughout this chapter, unless otherwise specified, we let p be a prime number and G denote a finite group. All modules are assumed to be **finitely generated** and free as ΛG-modules for any $\Lambda \in \{F, \mathcal{O}, k\}$.

References:

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. John Wiley & Sons, Inc., New York, 1990.

[Lin18] M. Linckelmann. *The block theory of finite group algebras. Vol. I*. Vol. 91. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 2018.

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

[Ser68] Jean-Pierre Serre. *Corps locaux*. Deuxième édition, Publications de l'Université de Nancago, No. VIII. Hermann, Paris, 1968.

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

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

30 Complete discrete valuation rings

In this section we review some number-theoretic results without formal proofs. I refer you to your number theory lectures for the details, or to [Ser68; Lin18; Thé95]. Important for the sequel is to keep the definitions and the examples in mind.

To begin with, recall from Chapter 1, §5, that a commutative ring $\mathcal{O}$ is local iff $\mathcal{O}\backslash\mathcal{O}^\times = J(\mathcal{O})$, i.e. $J(\mathcal{O})$ is the unique maximal ideal of $\mathcal{O}$. Moreover, by the commutativity assumption this happens if and only if $\mathcal{O}/J(\mathcal{O})$ is a field. In such a situation, we write $k := \mathcal{O}/J(\mathcal{O})$ and call this field **the residue field of the local ring** $\mathcal{O}$. To ease up notation, we will often write $\mathfrak{p} := J(\mathcal{O})$. This is because our aim is a situation in which the residue field is a field of positive characteristic p.

Definition 30.1 (*Reduction modulo* $\mathfrak{p}$)

Let $\mathcal{O}$ be a local commutative ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$ and residue field $k := \mathcal{O}/\mathfrak{p}$. Let M, N be finitely generated $\mathcal{O}$-modules, and let $f : M \longrightarrow N$ be an $\mathcal{O}$-linear map.

(a) The k-module $\overline{M} := M/\mathfrak{p}M \cong k \otimes_{\mathcal{O}} M$ is called the **reduction modulo** $\mathfrak{p}$ of M.

(b) The induced k-linear map $\overline{f} : \overline{M} \longrightarrow \overline{N}, m+\mathfrak{p}M \mapsto f(m)+\mathfrak{p}N$ is called the **reduction modulo** $\mathfrak{p}$ of f.

Exercise 30.2

Let $\mathcal{O}$ be a local commutative ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$ and residue field $k := \mathcal{O}/J(\mathcal{O})$.

(a) Let M, N be finitely generated free $\mathcal{O}$-modules.

(i) Let $f : M \longrightarrow N$ be an $\mathcal{O}$-linear map and $\overline{f} : \overline{M} \longrightarrow \overline{N}$ its reduction modulo $\mathfrak{p}$. Prove that if $\overline{f}$ is surjective (resp. an isomorphism), then f is surjective (resp. an isomorphism).

(ii) Prove that if elements $x_1, \ldots, x_n \in M$ ($n \in \mathbb{Z}_{\geqslant 1}$) are such that their images $\overline{x}_1, \ldots \overline{x}_2 \in \overline{M}$ form a k-basis of $\overline{M}$, then $\{x_1, \ldots, x_n\}$ is an $\mathcal{O}$-basis of M.
In particular, $\dim_k(\overline{M}) = \mathrm{rk}_{\mathcal{O}}(M)$.

Deduce that any direct summand of a finitely generated free $\mathcal{O}$-module is free.

(b) Prove that if M is a finitely generated $\mathcal{O}$-module, then the following conditions are equivalent:

(i) M is projective;

(ii) M is free.

Moreover, if $\mathcal{O}$ is also a PID, then (i) and (ii) are also equivalent to:

(iii) M is torsion-free.

[Hint: Use Nakayama's Lemma.]

Definition 30.3

A commutative ring $\mathcal{O}$ is called a **discrete valuation ring** if $\mathcal{O}$ is a local principal ideal domain such that $J(\mathcal{O}) \neq 0$.

Example 14

Let p be a prime number. We have already seen in Example 1(b) that the ring $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ is commutative local with unique maximal ideal

$$J(\mathbb{Z}_{(p)}) = \{\frac{a}{b} \in \mathbb{Z}_{(p)} \mid p \mid a\} = p\mathbb{Z}_{(p)}\,.$$

It follows easily that $\mathbb{Z}_{(p)}$ is a PID (every non-zero ideal in $\mathbb{Z}_{(p)}$ is of the form $p^n\mathbb{Z}_{(p)}$ for some integer $n \in \mathbb{Z}_{\geqslant 0}$), hence a *discrete valuation ring*.

In fact this example is a special case of a more general construction principle for discrete valuation rings, which consists in taking $\mathcal{O} := R_{\mathfrak{p}}$, where R is the ring of algebraic integers of an algebraic number field and where $R_{\mathfrak{p}}$ is the localisation of R at a non-zero prime ideal $\mathfrak{p}$ in R.

Remark 30.4

There is in fact a link between Definition 30.3 and the theory of valuations explaining the terminology *discrete valuation ring*, provided by the following result. (Not difficult to prove!)

Theorem 30.5

Let $\mathcal{O}$ be a discrete valuation ring and let $\pi \in \mathcal{O}$ such that $J(\mathcal{O}) = \pi\mathcal{O}$. Then:

(a) For every $a \in \mathcal{O}\backslash\{0\}$ there is a unique maximal (non-negative) integer $v(a)$ such that $a \in \pi^{v(a)}\mathcal{O}$.

(b) For any $a, b \in \mathcal{O}\backslash\{0\}$ we have $v(ab) = v(a) + v(b)$ and $v(a+b) \geqslant \min\{v(a), v(b)\}$.

(c) Every non-zero ideal in $\mathcal{O}$ is of the form $\pi^n\mathcal{O}$ for some unique integer $n \in \mathbb{Z}_{\geqslant 0}$.

The map $v : \mathcal{O}\backslash\{0\} \longrightarrow \mathbb{Z}$ defined in this way is called the **valuation** of the discrete valuation ring $\mathcal{O}$.

One can use valuations to give an alternative definition of *valuation rings*. Suppose that F is a field and that $v : F^\times \longrightarrow \mathbb{Z}$ is a surjective map satisfying

- $v(ab) = v(a) + v(b)$ (so v is a group homomorphism $\Rightarrow v(1) = 0$ and $v(a^{-1}) = -v(a)$), and
- $v(a+b) \geqslant \min\{v(a), v(b)\}$,

for all $a, b \in F$, and we set for notational convenience $v(0) = \infty$. Then, the set

$$\mathcal{O} := \{a \in F \mid v(a) \geqslant 0\}$$

is a discrete valuation ring, and $F = \mathrm{Frac}(\mathcal{O})$ is the fraction field of $\mathcal{O}$. Clearly, the unique maximal ideal in $\mathcal{O}$ is

$$J(\mathcal{O}) = \{a \in F \mid v(a) \geqslant 1\} = \mathcal{O}\backslash\mathcal{O}^\times .$$

Taking for π any element in $\mathcal{O}$ such that $v(\pi) = 1$, one easily checks that $\mathcal{O}$ has the properties stated in the theorem above.

A valuation induces a metric, and hence a topology. For the purpose of representation theory of finite groups, we will need to focus on the situation in which this topology is complete. This can be expressed algebraically as follows.

Definition 30.6 (*Complete discrete valuation ring*)

Let $\mathcal{O}$ be a discrete valuation ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$.

(a) A sequence $(a_m)_{m\geqslant 1}$ of elements of $\mathcal{O}$ is called a **Cauchy sequence** if for every integer $b \geqslant 1$, there exists an integer $N \geqslant 1$ such that $a_m - a_n \in J(\mathcal{O})^b$ for all $m, n \geqslant N$.

(b) $\mathcal{O}$ is called **complete** if for every Cauchy sequence $(a_m)_{m\geqslant 1} \subseteq \mathcal{O}$ there is $a \in \mathcal{O}$ such that for any integer $b \geqslant 1$ there exists an integer $N \geqslant 1$ such that $a - a_m \in J(\mathcal{O})^b$ for all $m \geqslant N$. (In this case, a is a **limit** of the Cauchy sequence $(a_m)_{m\geqslant 1}$.) It is also said that $\mathcal{O}$ is *complete with respect to the* $\mathfrak{p}$*-adic topology*.

Remark 30.7

The previous definition can be generalised to a finitely generated $\mathcal{O}$-algebra A. Moreover, one can prove that A is complete in the $J(A)$-adic topology if $\mathcal{O}$ is complete in the $J(\mathcal{O})$-adic topology.

Example 15

Let p be a prime number. The discrete valuation ring $\mathbb{Z}_{(p)}$ is not complete. However, its completion, the ring of p-adic integers, that is,

$$\hat{\mathbb{Z}}_{(p)} = \mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, \dots, p-1\} \, \forall \, i \geqslant 0 \right\},$$

is a complete discrete valuation ring. Its field of fractions is $\mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Q}_p$, i.e. the field of p-adic integers, $J(\mathbb{Z}_p) = p\mathbb{Z}_p$ and the residue field is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Finally we mention without proof a very useful consequence of Hensel's Lemma.

Corollary 30.8

Let $\mathcal{O}$ be a complete discrete valuation ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$ and residue field $k := \mathcal{O}/\mathfrak{p}$ of prime characteristic p, and let $m \in \mathbb{Z}_{\geqslant 1}$ be coprime to p. Then, for any m-th root of unity $\zeta \in k$, there exists a unique m-th root of unity $\mu \in \mathcal{O}$ such that $\overline{\mu} = \zeta$.

31 Splitting p-modular systems

In order to relate group representations over a field of positive characteristic to character theory in character zero, Brauer chose a *p-modular system*, which is defined as follows:

Definition 31.1 (*p-modular systems*)

Let p be a prime number.

(a) A triple of rings $(F, \mathcal{O}, k)$ is called a **p-modular system** if:

(1) $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero,

(2) $F = \mathrm{Frac}(\mathcal{O})$ is the field of fractions of $\mathcal{O}$ (also of characteristic zero), and

(3) $k = \mathcal{O}/J(\mathcal{O})$ is the residue field of $\mathcal{O}$ and has characteristic p.

(b) If G is a finite group, then a p-modular system $(F, \mathcal{O}, k)$ is a called a **splitting p-modular system for** G, if both F and k are splitting fields for G.

It is often helpful to visualise p-modular systems and the condition on the characteristic of the rings involved through the following commutative diagram of rings and ring homomorphisms:

$$\begin{array}{ccccc} \mathbb{Q} & \hookleftarrow & \mathbb{Z} & \twoheadrightarrow & \mathbb{F}_p \\ \downarrow & & \downarrow & & \downarrow \\ F & \hookleftarrow & \mathcal{O} & \twoheadrightarrow & k \end{array}$$

where the hook arrows are the canonical inclusions and the two-head arrows the quotient morphisms. Clearly, these morphisms also extend naturally to ring homomorphisms

$$FG \hookleftarrow \mathcal{O}G \twoheadrightarrow kG$$

between the corresponding group algebras (each mapping an element $g \in G$ to itself).

Example 16

One usually works with a splitting p-modular system for all subgroups of G, because it allows us avoid problems with field extensions. By a theorem of Brauer on splitting fields such a p-modular system can always be obtained by adjoining a primitive m-th root of unity to $\mathbb{Q}_p$, where m is the exponent of G. (Notice that this extension is unique.) So we may as well assume that our situation is as given in the following commutative diagram:

$$\begin{array}{ccccc} \mathbb{Q}_p & \hookleftarrow & \mathbb{Z}_p & \twoheadrightarrow & \mathbb{F}_p \\ \downarrow & & \downarrow & & \downarrow \\ F & \hookleftarrow & \mathcal{O} & \twoheadrightarrow & k \end{array}$$

More generally, we have the following result, which we mention without proof. The proof can be found in [CR90, §17A].

Theorem 31.2

Let $(F, \mathcal{O}, k)$ be a p-modular system. Let G be a finite group of exponent m. Then the following assertions hold.

(a) The field F contains all m-th roots of unity if and only if F contains the cyclotomic field of m-th roots of unity;

(b) If F contains all m-th roots of unity, then so does k and F and k are splitting fields for G and all its subgroups.

Remark 31.3

If $(F, \mathcal{O}, k)$ is a p-modular system, then it is not possible to have F and k algebraically closed, while assuming $\mathcal{O}$ is complete. (Depending on your knowledge on valuation rings, you can try to prove this as an exercise!)

Let us now investigate changes of the coefficients given in the setting of a p-modular system for group algebras involved.

Definition 31.4

Let $\mathcal{O}$ be a commutative local ring. A finitely generated $\mathcal{O}G$-module L is called an $\mathcal{O}G$-**lattice** if it is free (= projective) as an $\mathcal{O}$-module.

Remark 31.5 (*Changes of the coefficients*)

Let $(F, \mathcal{O}, k)$ be a p-modular system and write $\mathfrak{p} := J(\mathcal{O})$. If L is an $\mathcal{O}G$-module, then:

- setting $L^F := F \otimes_{\mathcal{O}} L$ defines an FG-module, and
- reduction modulo $\mathfrak{p}$ of L, that is $\overline{L} := L/\mathfrak{p}L \cong k \otimes_{\mathcal{O}} L$ defines a kG-module.

We note that, when seen as an $\mathcal{O}$-module, an $\mathcal{O}G$-module L may have torsion, which is lost on passage to F. In order to avoid this issue, we usually only work with $\mathcal{O}G$-lattices. In this way, we obtain functors

$$FG\text{-}\mathbf{mod} \longleftarrow \mathcal{O}G\text{-}\mathbf{lat} \longrightarrow\!\!\!\!\!\rightarrow kG\text{-}\mathbf{mod}$$

between the corresponding categories of finitely generated $\mathcal{O}G$-lattices and finitely generated FG-, kG-modules.

A natural question to ask is: which FG-modules, respectively kG-modules, come from $\mathcal{O}G$-lattices? In the case of FG-modules we have the following answer.

Proposition-Definition 31.6

Let $\mathcal{O}$ be a complete discrete valuation ring and let $F := \mathrm{Frac}(\mathcal{O})$ be the fraction field of $\mathcal{O}$. Then, for any finitely generated FG-module V there exists an $\mathcal{O}G$-lattice L which has an $\mathcal{O}$-basis which is also an F-basis. In this situation $V \cong L^F$ and we call L an $\mathcal{O}$-**form** of V.

Proof: Choose an F-basis $\{v_1, \ldots, v_n\}$ of V and set $L := \mathcal{O}Gv_1 + \cdots + \mathcal{O}Gv_n \subseteq V$.
Exercise: verify that L is as required. ∎

On the other hand, the question has a negative answer for kG-modules.

Definition 31.7 (*liftable kG-module*)

Let $\mathcal{O}$ be a commutative local ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$ and residue field $k := \mathcal{O}/\mathfrak{p}$. A kG-module M is called **liftable** if there exists an $\mathcal{O}G$-lattice $\widehat{M}$ whose reduction modulo $\mathfrak{p}$ of M is isomorphic to M, that is

$$\widehat{M}/\mathfrak{p}\widehat{M} \cong M\,.$$

(Alternatively, it is also said that M is **liftable to an** $\mathcal{O}G$-**lattice**, or **liftable to** $\mathcal{O}$, or **liftable to characteristic zero**.)

Even though every $\mathcal{O}G$-lattice can be reduced modulo $\mathfrak{p}$ to produce a kG-module, not every kG-module is liftable to an $\mathcal{O}G$-lattice.

Being liftable for a kG-module is a rather rare property. However, the next section brings us some answers towards classes of kG-modules which are liftable.

32 Lifting idempotents

Throughout this section, we assume that $\mathcal{O}$ is a complete discrete valuation ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$ and residue field $k := \mathcal{O}/\mathfrak{p}$.

Moreover, we let A denote a finitely generated $\mathcal{O}$-algebra of finite $\mathcal{O}$-rank. Observe that since A is a finitely generated $\mathcal{O}$-module, so is any simple A-module V and it follows from Nakayama's lemma that $\mathfrak{p}V \neq V$, so $\mathfrak{p}V = 0$. If $\mathfrak{m}$ is a maximal left ideal of A, then $A/\mathfrak{m}$ is a simple A-module and therefore $\mathfrak{m} \supseteq \mathfrak{p}A$. This proves that

$$\mathfrak{p}A \subseteq J(A)\,.$$

It follows that $J(A)$ is the inverse image in A under the quotient morphism of the Jacobson radical $J(\overline{A})$ of the finite dimensional k-algebra $\overline{A} := A/\mathfrak{p}A$ (the reduction modulo $\mathfrak{p}$ of A). Consequently,

$$A/J(A) \cong \overline{A}/J(\overline{A})\,.$$

Recall that an idempotent e of a ring R is called primitive if $e \neq 0$ and whenever $e = f + g$ where f and g are orthogonal idempotents, then either $f = 0$ or $g = 0$.

Exercise 32.1

Let A be a ring and let $e \in A$ be an idempotent element. Prove that:

(a) $J(eAe) = eJ(A)e$;

(b) If A is a finite-dimensional k-algebra over a field k, then e is primitive if and only if eAe is a local ring. In that case $eJ(A)e$ is the unique maximal ideal of eAe.

This leads us to the following crucial result for representation theory of finite groups on the lifting of idempotents.

Theorem 32.2 (*Lifting theorem of idempotents (partial version)*)

Let A be a finitely generated $\mathcal{O}$-algebra of finite $\mathcal{O}$-rank. Set $\overline{\overline{A}} := A/J(A)$ and for $a \in A$ write $\overline{\overline{a}} := a + J(A)$. The following assertions hold.

(a) If $\overline{\overline{a}} \in \overline{\overline{A}}^{\times}$, then $a \in A^{\times}$. Thus there is a s.e.s. of groups

$$1 \longrightarrow 1 + J(A) \longrightarrow A^{\times} \longrightarrow \overline{\overline{A}}^{\times} \longrightarrow 1\,.$$

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

(c) Two idempotents $e, f \in A$ are conjugate in A if and only if $\overline{\overline{e}}$ and $\overline{\overline{f}}$ are conjugate in $\overline{\overline{A}}$. More precisely if $\overline{\overline{e}} = \overline{\overline{u}}\,\overline{\overline{f}}\,\overline{\overline{u}}^{-1}$, then $\overline{\overline{u}}$ lifts to an invertible element $u \in A^{\times}$ such that $e = ufu^{-1}$. In particular, if $\overline{\overline{e}} = \overline{\overline{f}}$, then there exists $u \in (1 + J(A)) \subseteq A^{\times}$ such that $e = ufu^{-1}$.

(d) An idempotent $e \in A$ is primitive in A if and only if $\overline{\overline{e}}$ is primitive in $\overline{\overline{A}}$.

(e) The quotient morphism $A \to \overline{\overline{A}}$ induces a bijection between the set $\mathcal{P}(A)$ of conjugacy classes of primitive idempotents of A and the set $\mathcal{P}(\overline{\overline{A}})$ of conjugacy classes of primitive idempotents of $\overline{\overline{A}}$.

Proof: (a) If $a \in A$ is not invertible, then $Aa \neq A$. Then $a \in \mathfrak{m}$ for some maximal left ideal $\mathfrak{m}$ of A by Zorn's lemma. Since $\mathfrak{m} \supseteq J(A)$, its image is a maximal left ideal of $\overline{\overline{A}}$ and we have $\overline{\overline{a}} \in \mathfrak{m}$. Thus $\overline{\overline{a}}$ is not invertible. The claim about the s.e.s. follows immediately.

(b) Let $a_1 \in A$ such that $\overline{\overline{a}}_1 = x$ and let $b_1 := a_1^2 - a_1$. Define by induction two sequences of elements of A:

$$a_n := a_{n-1} + b_{n-1} - 2a_{n-1}b_{n-1} \qquad \text{and} \qquad b_n := a_n^2 - a_n \qquad \forall\, n \geqslant 2.$$

We now prove by induction that $a_n^2 \equiv a_n \pmod{J(A)^n}$, or in other words that $b_n \in J(A)^n$. This is true for $n = 1$, and assuming that this holds for n, we have $b_n^2 \in J(A)^{n+1}$ (because $(J(A)^n)^2 \subseteq J(A)^{n+1}$), and since $a_n^2 = a_n + b_n$ we obtain

$$\begin{aligned} a_{n+1}^2 &\equiv a_n^2 + 2a_nb_n - 4a_n^2b_n \pmod{J(A)^{n+1}} \\ &= a_n + b_n + 2a_nb_n - 4(a_n + b_n)b_n \\ &\equiv a_n + b_n - 2a_nb_n = a_{n+1} \pmod{J(A)^{n+1}}. \end{aligned}$$

It follows that $(b_n)_{n\geqslant 1}$ converges to 0 and that $(a_n)_{n\geqslant 1}$ is a Cauchy sequence in the $J(A)$-adic topology. Since A is complete in the $J(A)$-adic topology (see Remark 30.7), $(a_n)_{n\geqslant 1}$ converges to some element $\tilde{e} \in A$. Clearly, $\tilde{e}^2 - \tilde{e} = \lim_{n\to\infty} b_n = 0$, so $\tilde{e}$ is an idempotent of A. Moreover

$$\overline{\overline{\tilde{e}}} = \overline{\overline{a}}_1 = x\,,$$

as required.

(c) It is clear that $\overline{\overline{e}}$ and $\overline{\overline{f}}$ are conjugate in $\overline{\overline{A}}$ if e and f are conjugate in A ($e = ufu^{-1} \Rightarrow \overline{\overline{e}} = \overline{\overline{u}}\,\overline{\overline{f}}\,\overline{\overline{u}}^{-1}$). Conversely, assume that there exists $\overline{\overline{u}} \in \overline{\overline{A}}^{\times}$ such that $\overline{\overline{e}} = \overline{\overline{u}}\,\overline{\overline{f}}\,\overline{\overline{u}}^{-1}$. Then, by (a), $u \in A^{\times}$ and so, replacing f by ufu^{-1} we can assume $\overline{\overline{e}} = \overline{\overline{f}}$. Now let $v := 1_A - e - f + 2ef$. Then, by (a), $v \in A^{\times}$ because

$$\overline{\overline{v}} = \overline{\overline{1_A - e - f + 2ef}} = \overline{\overline{1}}_A - \overline{\overline{e}} - \overline{\overline{f}} + 2\overline{\overline{e}}\,\overline{\overline{f}} = 1_{\overline{\overline{A}}}\,.$$

Moreover, $ev = ef = vf$ and it follows that $e = evv^{-1} = vfv^{-1}$, as required.

(d) The idempotent e is primitive in A if and only if e and 0 are the only idempotents of eAe. Since by the previous exercise $J(eAe) = eJ(A)e = J(A) \cap eAe$, we have

$$eAe/J(eAe) = \overline{\overline{eAe}} = \overline{\overline{e}}\,\overline{\overline{A}}\,\overline{\overline{e}}\,.$$

Now, if $\overline{\overline{f}}$ is a non-trivial idempotent of $\overline{\overline{e}}\,\overline{\overline{A}}\,\overline{\overline{e}}$, then by (b) applied to the algebra eAe, the idempotent $\overline{\overline{f}}$ lifts to an idempotent $f \in eAe$. This proves that $\overline{\overline{e}}$ is primitive if e is primitive. Conversely if e is not primitive, there exists a non-trivial idempotent $f \in eAe$. Then f is not conjugate (that is, not equal) to 0 nor to the unity element e. Thus, it follows from (c) that $\overline{\overline{f}}$ is a non-trivial idempotent of $\overline{\overline{e}}\,\overline{\overline{A}}\,\overline{\overline{e}}$, as required.

(e) This follows immediately from (b), (c) and (d). ■

A first possible application of Theorem 32.2 is a generalisation of this theorem providing a lifting of idempotents from a quotient $A/\mathfrak{b}$ for an arbitrary ideal $\mathfrak{b} \in A$. (See [Thé95, (3.2) Theorem].) We state here the particular case of interest to us for $\mathfrak{b} = \mathfrak{p}A$.

Theorem 32.3 (*Lifting theorem of idempotents for reduction modulo* $\mathfrak{p}$)

Let A be a finitely generated $\mathcal{O}$-algebra of finite $\mathcal{O}$-rank. Set $\overline{A} := A/\mathfrak{p}A$ and for $a \in A$ write $\overline{a} := a + \mathfrak{p}A$. The following assertions hold.

(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 $e_1 = ue_2u^{-1}$.

(d) The quotient morphism $A \twoheadrightarrow \overline{A}$ induces a bijection between the central idempotents of A and the central idempotents of $\overline{A}$.

Proof: Exercise! (Either use Theorem 32.2 or imitate the proof of Theorem 32.2.) ■

The lifting of idempotents allows us, in particular, to prove that projective indecomposable kG-modules are liftable to projective indecomposable $\mathcal{O}G$-lattices.

Lemma 32.4

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

Proof: Since P is projective, $P \mid (A^\circ)^n$ for some $n \in \mathbb{Z}_{\geqslant 1}$. As P is indecomposable, it follows from the Krull-Schmidt theorem that $P \mid A^\circ$, so $A^\circ = P \oplus Q$ for some A-module Q. Thus, we can write $1_A = e + f$ with $e \in P$ and $f \in Q$. Then

$$fe = (1 - e)e = e - e^2 = ef$$

and this is an element of $Ae \cap Af \subseteq Q \cap P = \{0\}$. Therefore $e^2 = e$ and $ef = fe = 0$. Finally, since

$$A = A \cdot 1_A = A(e + f) = Ae + Af\,,\ Ae \subseteq P \text{ and } Af \subseteq Q\,,$$

it follows that $Ae = P$. ■

Corollary 32.5

Let A be a finitely generated $\mathcal{O}$-algebra of finite $\mathcal{O}$-rank and set $\overline{A} := A/\mathfrak{p}A$. Let P be a projective (indecomposable) $\overline{A}$-module. Then there exists a projective (indecomposable) A-module $\widehat{P}$ such that $P \cong \widehat{P}/\mathfrak{p}\widehat{P}$.

Proof: Let $P = P_1 \oplus \cdots \oplus P_r$ ($r \in \mathbb{Z}_{\geqslant 1}$) be a decomposition of P as a direct sum of indecomposable A-submodules. Then, by Lemma 32.4, there exist idempotents $f_1, \ldots, f_r \in \overline{A}$ such that $P_i \cong Af_i$ for each $1 \leqslant i \leqslant r$, and so

$$P \cong \overline{A}f_1 \oplus \cdots \oplus \overline{A}f_r\,.$$

Now, by Theorem 32.3(a) there exists idempotents $e_1, \ldots, e_r \in A$ such that $\overline{e_i} = f_i$ for each $1 \leqslant i \leqslant r$. Then $\widehat{P} := Ae_1 \oplus \cdots \oplus Ae_r$ is a projective A-module (see Example 10) and $\widehat{P}/\mathfrak{p}\widehat{P} \cong P$.
Moreover, $\widehat{P}$ is indecomposable if P is. Indeed,

$$\widehat{P} = \widehat{P}_1 \oplus \widehat{P}_2 \text{ decomposable } \Rightarrow\ \widehat{P}/\mathfrak{p}\widehat{P} \cong k \otimes_{\mathcal{O}} (\widehat{P}_1 \oplus \widehat{P}_2) \cong (k \otimes_{\mathcal{O}} \widehat{P}_1) \oplus (k \otimes_{\mathcal{O}} \widehat{P}_2) \text{ decomposable}\,.$$

■

Corollary 32.6

Any (projective) indecomposable kG-module is liftable to a (projective) indecomposable $\mathcal{O}G$-lattice.

Proof: This follows immediately from Corollary 32.5 with $A := \mathcal{O}G$ since then

$$\overline{A} = \mathcal{O}G/\mathfrak{p}\mathcal{O}G \cong k \otimes_{\mathcal{O}} \mathcal{O}G \cong (k \otimes_{\mathcal{O}} \mathcal{O})G \cong kG\,.$$

■

Exercise 32.7

Let A be a finitely generated $\mathcal{O}$-algebra of finite $\mathcal{O}$-rank. Let M be an A-module and let $e \in A$ be an idempotent. Prove that, as $\mathrm{End}_A(M)$-modules,

$$\mathrm{Hom}_A(Ae, M) \cong eM\,.$$

33 Brauer Reciprocity

Throughout this section, we let $(F, \mathcal{O}, k)$ be a splitting p-modular system for G and write $\mathfrak{p} := J(\mathcal{O})$.

Reduction modulo $\mathfrak{p} := J(\mathcal{O})$ provides us with a method for going from characteristic zero to characteristic $p > 0$. Moreover, if V is an FG-module, then we can choose an $\mathcal{O}$-form L of V and then consider the reduction modulo $\mathfrak{p}$ of L, i.e. $\overline{L} = L/\mathfrak{p}$. However, the choice of the $\mathcal{O}$-form is not unique. As a consequence, if L_1 and L_2 are two $\mathcal{O}$-forms of V, i.e. $(L_1)^F \cong V \cong (L_2)^F$, then it may happen that $\overline{L_1} \ncong \overline{L_2}$. The following result shows that, however, this does not affect the composition factors, up to isomorphism and multiplicity.

Proposition 33.1

Let $S_1, \ldots, S_t$ ($t \in \mathbb{Z}_{\geqslant 1}$) be a complete set of representatives of the isomorphism classes of simple kG-modules. If V is an FG-module and L is an $\mathcal{O}$-form of V, then for each $1 \leqslant j \leqslant t$ the multiplicity of S_j as a composition factor of $\overline{L} = L/\mathfrak{p}L$ does not depend on the choice of the $\mathcal{O}$-form L.

Proof: Fix $j \in \{1, \ldots, t\}$. Since k is a splitting field for G, $\mathrm{End}_{kG}(S_j) \cong k$. Thus, by Proposition 22.1(b), the multiplicity of S_j as a composition factor of $\overline{L}$ is

$$\dim_k \mathrm{Hom}_{kG}(P_{S_j}, \overline{L}) / \dim_k \mathrm{End}_{kG}(S_j) = \dim_k \mathrm{Hom}_{kG}(P_{S_j}, \overline{L})\,.$$

On the other hand, by Lemma 32.4 and Theorem 32.3, there exists an idempotent $e_j \in \mathcal{O}G$ such that

$$P_{S_j} \cong kG\overline{e}_j\,.$$

Hence, Exercise 32.7 yields

$$\mathrm{Hom}_{kG}(P_{S_j}, \overline{L}) \cong \mathrm{Hom}_{kG}(kG\overline{e}_j, \overline{L}) \cong \overline{e}_j\overline{L} \cong \overline{e_jL}\,.$$

Then, Exercise 30.2(a)(ii) and Proposition-Definition 31.6 yield

$$\dim_k \mathrm{Hom}_{kG}(P_{S_j}, \overline{L}) = \dim_k(\overline{e_jL}) = \mathrm{rk}_{\mathcal{O}}(e_jL) = \dim_F(e_jV)\,.$$

As a consequence, for any $1 \leqslant j \leqslant t$, the number of composition factors of $\overline{L}$ isomorphic to S_j is equal to $\dim_F(e_jV)$, and is therefore independent of the choice of the $\mathcal{O}$-form L. ■

Theorem 33.2 (*Brauer Reciprocity*)

Let $V_1, \dots, V_l$ ($l \in \mathbb{Z}_{\geqslant 1}$) be a complete set of representatives of the isomorphism classes of simple FG-modules, and let $S_1, \dots, S_t$ ($t \in \mathbb{Z}_{\geqslant 1}$) be a complete set of representatives of the isomorphism classes of simple kG-modules. 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 $1 \leqslant j \leqslant t$. For every $1 \leqslant i \leqslant l$ and $1 \leqslant j \leqslant t$ define d_{ij} to be the multiplicity of S_j as a composition factor of the reduction modulo $\mathfrak{p}$ of an $\mathcal{O}$-form of V_i. Then

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

Proof: Since FG is a semisimple F-algebra the set $\{V_i \mid 1 \leqslant i \leqslant l\}$ is a complete set of representatives of the isomorphism classes of the PIMs of FG (by Theorem 21.2(b)). Moreover, as F is a splitting field for G, by Theorem 8.2, each V_i ($1 \leqslant i \leqslant l$) appears precisely $\dim_F V_i$ times in the decomposition of the regular module FG. Hence, for any $1 \leqslant j \leqslant t$, there exist non-negative integers d'_{ij} such that

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

where $d'_{ij} = \dim_F \operatorname{Hom}_{FG}(FGe_j, V_i)$. Thus, it remains to prove that $d'_{ij} = d_{ij}$ for every $1 \leqslant i \leqslant l$ and $1 \leqslant j \leqslant t$. So choose an $\mathcal{O}$-form L_i of V_i ($1 \leqslant i \leqslant$). As in the previous proof, applying Exercise 32.7 and Proposition 31.6 yields

$$d'_{ij} = \dim_F \operatorname{Hom}_{FG}(FGe_j, V_i) = \dim_F(e_j V_i) = \operatorname{rk}_{\mathcal{O}}(e_j L_i) = \dim_k \overline{e}_j \overline{L}_i = \dim_k \operatorname{Hom}_{kG}(kG\overline{e}_j, \overline{L}_i) = d_{ij}.$$

■

Definition 33.3 (*Decomposition matrix*)

The positive integers d_{ij} ($1 \leqslant i \leqslant l, 1 \leqslant j \leqslant t$) defined in Theorem 33.2 are called the p-**decomposition numbers** of G and the matrix

$$\operatorname{Dec}_p(G) := (d_{ij})_{\substack{1 \leqslant i \leqslant l \\ 1 \leqslant j \leqslant t}}$$

is called the p-**decomposition matrix** (or simply the **decomposition matrix**) of G.

Exercise 33.4

Let C be the Cartan matrix of kG and $D := \operatorname{Dec}_p(G)$ be the decomposition matrix of G. Prove that

$$C = D^{tr} D$$

and deduce again that C is symmetric.

Chapter 9. Brauer Characters

Recall that if F is a field of characteristic zero, then FG-modules are isomorphic if and only if their characters are equal. Also, the character of a FG-module provides complete information about its composition factors, including multiplicities, provided that the irreducible characters are known. All this does not hold for fields k of characteristic $p > 0$. For instance, if W is a k-vector space on which G acts trivially and $\dim_k(W) = ap + 1$ for some nonnegative integer a, then the k-character of W is the trivial character. This implies that a k-character can only give information about multiplicities of composition factors modulo p. In view of these issues, the aim of this chapter is to define a slightly different kind of *character theory* for modular representations of finite groups and to establish links with ordinary character theory.

Notation: Throughout, G denotes a finite group and p a prime number. We let $(F, \mathcal{O}, k)$ denote a p-modular system and we assume F contains all $\exp(G)$-th roots of unity, so $(F, \mathcal{O}, k)$ is a splitting p-modular system for G and all its subgroups (see Theorem 31.2). We write $\mathfrak{p} := J(\mathcal{O})$. For $\Lambda \in \{F, \mathcal{O}, k\}$ all ΛG-modules considered are assumed to be free of finite rank over Λ. If $\Lambda \in \{F, k\}$ and U is a ΛG-module, then we write $\rho_U : G \longrightarrow \mathrm{GL}(U)$ for the associated Λ-representation.

For background results in ordinary character theory I refer to my Skript *Character Theory of Finite Groups* from the SS 2020.

References:

[Alp86] J. L. Alperin. *Local representation theory*. Vol. 11. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1986.

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. John Wiley & Sons, Inc., New York, 1990.

[Isa94] I. M. Isaacs. *Character theory of finite groups*. Dover Publications, Inc., New York, 1994.

[Las20] C. Lassueur. *Character theory of finite groups*. Lecture Notes SS 2020, TU Kaiserslautern, 2020.

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

[Nav98] G. Navarro. *Characters and blocks of finite groups*. Cambridge University Press, Cambridge, 1998.

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

Before we start, we recall the following useful terminology from finite group theory.

Definition

Let G be a finite group and p be a prime number.

(a) If $|G| = p^a m$ with $a, m \in \mathbb{Z}_{\geqslant 0}$ and $(p, m) = 1$, then $|G|_p := p^a$ is the p-**part** of the order $|G|$ of G and $|G|_{p'} := m$ is the p'-**part** of the order of G.

(b) An element $g \in G$ is called a p-**regular element** (or a p'-**element**) if $p \nmid o(g)$ and we write

$$G_{p'} := \{g \in G \mid p \nmid o(g)\}$$

for the set of all p-regular elements of G. (Warning: in general this is not a subgroup!)

(c) An element $g \in G$ is called a p-**singular element** if $p \mid o(g)$ and it is called a p-**element** if $o(g)$ is a power of p.

Remark

Let G be a finite group and p be a prime number. Let $g \in G$ and write $o(g) = p^n m$ with $n, m \in \mathbb{Z}_{\geqslant 0}$ such that $(p, m) = 1$. Then, letting $a, b \in \mathbb{Z}$ be such that $1 = ap^n + bm$, we may set

$$g_p := g^{bm} \quad \text{and} \quad g_{p'} := g^{ap^n}$$

It is immediate that

$$(g_p)^{p^n} = 1, \quad (g_{p'})^m = 1, \quad \text{and} \quad g = g_p g_{p'}\,.$$

Thus, g_p is a p-element and is called the p-**part** of g, and $g_{p'}$ is p-regular and is called the p'-**part** of g.

34 Brauer characters

Since we assume that the given p-modular system $(F, \mathcal{O}, k)$ is such that F contains all $\exp(G)$-th roots of unity, both F and k contain a primitive a-th root of unity, where a is the l.c.m. of the orders of the p-regular elements. To start with we examine the relationship between the roots of unity in F and in k. Set

$$\mu_F := \{a\text{-th roots of 1 in } F\}\,;$$

$$\mu_k := \{a\text{-th roots of 1 in } k\}\,.$$

Then $\mu_F \subseteq \mathcal{O}$ and, as both μ_F and μ_k are finite groups, it follows from Corollary 30.8 that the quotient morphism $\mathcal{O} \twoheadrightarrow \mathcal{O}/\mathfrak{p}$ restricted to μ_F induces a group isomorphism

$$\mu_F \xrightarrow{\cong} \mu_k\,.$$

We write the underlying bijection as $\widehat{\xi} \mapsto \xi$, so that if ξ is an a-th root of unity in k then $\widehat{\xi}$ is the unique a-th root of unity in $\mathcal{O}$ which maps onto it.

Lemma 34.1 (*Diagonalisation lemma*)

Let $\rho : G \longrightarrow \mathrm{GL}(U)$ be a k-representation of G. Then, for every p-regular element $g \in G_{p'}$, the k-linear map $\rho(g)$ is diagonalisable and the eigenvalues of $\rho(g)$ are $o(g)$-th roots of unity and lie in μ_k. In other words, there exists an ordered k-basis B of U with respect to which

$$\big(\rho(g)\big)_B = \begin{bmatrix} \xi_1 & 0 & \cdots & \cdots & 0 \\ 0 & \xi_2 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & \xi_n \end{bmatrix},$$

where $n := \dim_k(U)$ and each ξ_i $(1 \leqslant i \leqslant n)$ is an $o(g)$-th root of unity in k.

Proof: Let $g \in G_{p'}$. It is enough to consider the restriction of ρ to the cyclic subgroup $\langle g \rangle$. Since $p \nmid |\langle g \rangle|$, $k\langle g \rangle$ is semisimple by Maschke's Theorem. Moreover, as k is a splitting field for $\langle g \rangle$, it follows from Corollary 12.3 that all irreducible k-representations of $\langle g \rangle$ have degree 1. Hence $\rho|_{\langle g \rangle}$ can be decomposed as the direct sum of degree 1 subrepresentations. As a consequence $\rho(g) = \rho|_{\langle g \rangle}(g)$ is diagonalisable and there exists a k-basis B of U satisfying the statement of the lemma. It follows immediately that the eigenvalues are $o(g)$-th roots of unity because $\rho_U(g^{o(g)}) = \rho_U(1_G) = \mathrm{Id}_U$. They all lie in μ_k, being $o(g)$-th roots of unity, hence a-th roots of unity. ∎

This leads to the following definition.

Definition 34.2 (*Brauer characters*)

Let U be a kG-module of dimension $n \in \mathbb{Z}_{\geqslant 1}$ and let $\rho_U : G \to \mathrm{GL}(U)$ be the associated k-representation. The p-**Brauer character** or simply the **Brauer character** of G afforded by U (resp. of ρ_U) is the F-valued function

$$\begin{aligned} \varphi_U : G_{p'} &\to \mathcal{O} \subseteq F \\ g &\mapsto \widehat{\xi}_1 + \cdots + \widehat{\xi}_n \,, \end{aligned}$$

where $\xi_1, \ldots, \xi_n \in \mu_k$ are the eigenvalues of $\rho_U(g)$. The integer n is also called the **degree** of φ_U. Moreover, φ_U is called **irreducible** if U is simple (resp. if ρ_U is irreducible), and it is called **linear** if $n = 1$. We denote by $\mathrm{IBr}_p(G)$ the set of all irreducible Brauer characters of G and we write $\mathbf{1}_{G_{p'}}$ for the Brauer character of the trivial kG-module.

In the sequel, we want to prove that Brauer characters of kG-modules have properties similar to $\mathbb{C}$-characters.

Remark 34.3

(a) **Warning**: $\varphi(g) \in \mathcal{O} \subseteq F$ even though $\rho_U(g)$ is defined over the field k of characteristic $p > 0$.

(b) Often the values of Brauer characters are considered as complex numbers, i.e. sums of complex roots of unity. Of course, in that case then $\varphi_U(g)$ depends on the choice of embedding of μ_F into $\mathbb{C}$. However, for a fixed embedding, $\varphi_U(g)$ is uniquely determined up to similarity of $\rho_U(g)$.

Immediate properties of Brauer characters are as follows.

Proposition 34.4

Let $U \neq 0$ be a kG-module with Brauer character φ_U. Then:

(a) $\varphi_U(1) = \dim_k(U)$;

(b) φ_U is a class function on $G_{p'}$;

(c) $\varphi_U(g^{-1}) = \varphi_{U^*}(g) \ \forall\ g \in G_{p'}$.

Proof: Let $n := \dim_k(U)$ and let ρ_U be the k-representation associated to U.

(a) Clearly $\rho_U(1_G)$ is the identity map on U and has n eigenvalues all equal to 1_k. Since $\widehat{1_k} = 1_F$ the sum of the lifts is $n = \dim_k(U)$.

(b) If $g, x \in G_{p'}$, then $\rho_U(xgx^{-1}) = \rho_U(x)\rho_U(g)\rho_U(x)^{-1}$, so $\rho_U(g)$ and $\rho_U(xgx^{-1})$ are similar and therefore have the same eigenvalues. Thus, by definition of φ_U we have $\varphi_U(g) = \varphi_U(xgx^{-1})$. [Note that in this proof we could take $x \in G$ and it would not change the result!]

(c) Let $g \in G_{p'}$ and let $\xi_1, \ldots, \xi_n \in \mu_k$ be the eigenvalues of $\rho_U(g)$. As $\rho_U(g)$ is diagonalisable by Lemma 34.1, it follows immediately that the eigenvalues of $\rho_U(g^{-1}) = \rho_U(g)^{-1}$ are $\xi_1^{-1}, \ldots, \xi_n^{-1}$, as are the eigenvalues of $\rho_{U^*}(g) = \rho_U(g^{-1})^{tr}$. Since $\mu_F \longrightarrow \mu_k, \widehat{\xi} \mapsto \xi$ is a group isomorphism, we have $\widehat{\xi_i^{-1}} = \widehat{\xi}_i^{-1}$ for each $1 \leqslant i \leqslant n$, and the claim follows. ∎

Exercise 34.5

Let U, V, W be non-zero kG-modules. Prove the following assertions.

(a) If $0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$ is a s.e.s. of kG-modules, then

$$\varphi_V = \varphi_U + \varphi_W .$$

(b) If the composition factors of U are $S_1, \ldots, S_m$ ($m \in \mathbb{Z}_{\geqslant 1}$) with multiplicities $n_1, \ldots, n_m$ respectively, then

$$\varphi_U = n_1\varphi_{S_1} + \ldots + n_m\varphi_{S_m} .$$

In particular, if two kG-modules have isomorphic composition factors, counting multiplicities, then they have the same Brauer character.

(c) $\varphi_{U\oplus V} = \varphi_U + \varphi_V$ and $\varphi_{U\otimes_k V} = \varphi_U \cdot \varphi_V$.

The link between the Brauer characters and the usual notion of a character, i.e. trace functions, is described below and explains why trace functions are not *good enough*.

Definition 34.6 (*character*)

Let $\Lambda \in \{F, k\}$. Let $U \neq 0$ be a ΛG-module and let $\rho_U : G \longrightarrow \mathrm{GL}(U)$ be the associated Λ-representation, then the trace function

$$\begin{array}{rccc} \mathrm{Tr}(-,U): & G & \longrightarrow & \Lambda \\ & g & \mapsto & \mathrm{Tr}(g,U) := \mathrm{Tr}\left(\rho_U(g)\right) \end{array}$$

is called the Λ-**character** of U.

For $\Lambda = F$, we also write χ_U instead of $\mathrm{Tr}(-, U)$ and we write $\mathrm{Irr}_F(G)$ for the set of all irreducible F-characters of G.

(Recall from *Character Theory of Finite Groups* that an F-character χ_U is called irreducible if U is a simple FG-module.)

Lemma 34.7

Let $U \neq 0$ be a kG-module and let $g \in G$. Then:

(a) $\mathrm{Tr}(g, U) = \mathrm{Tr}(g_{p'}, U)$, and

(b) $\mathrm{Tr}(g, U) = \varphi_U(g_{p'}) + \mathfrak{p}$ in the quotient $k = \mathcal{O}/\mathfrak{p}$.

Proof: Let ρ_U be the k-representation associated to U.

(a) Clearly $\rho_U(g) = \rho_U(g_p)\rho_U(g_{p'}) = \rho_U(g_{p'})\rho_U(g_p)$. Therefore, we know from linear algebra that the eigenvalues of $\rho_U(g)$ are pairwise product of suitably ordered eigenvalues of $\rho_U(g_{p'})$ and $\rho_U(g_p)$. Now, as g_p is a p-element, a p-power of $\rho_U(g_p)$ is the identity and so all the eigenvalues of $\rho_U(g_p)$ are equal to one because $\mathrm{char}(k) = p$. Hence $\rho_U(g)$ and $\rho_U(g_{p'})$ have the same eigenvalues (counted with multiplicities) and the claim follows.

(b) Let $\xi_1, \ldots, \xi_n$ be the eigenvalues of $\rho_U(g_{p'})$. Then, by definition, $\varphi_U(g) = \widehat{\xi}_1 + \cdots + \widehat{\xi}_n$, where, for each $1 \leqslant i \leqslant n$, $\widehat{\xi}_i$ is such that $\widehat{\xi}_i + \mathfrak{p} = \xi_i$ in the quotient $k = \mathcal{O}/\mathfrak{p}$. Therefore, it follows from (a) and the diagonalisation lemma that

$$\mathrm{Tr}(g, U) = \mathrm{Tr}(g_{p'}, U) = \xi_1 + \cdots + \xi_n = (\widehat{\xi}_1 + \mathfrak{p}) + \cdots + (\widehat{\xi}_n + \mathfrak{p}) = (\widehat{\xi}_1 + \ldots + \widehat{\xi}_n) + \mathfrak{p} = \varphi_U(g_{p'}) + \mathfrak{p}\,.$$

■

Notation 34.8

We let $\mathrm{Cl}_F(G) := \{f : G \longrightarrow F \mid f \text{ class function}\}$ denote the F-vector space of F-valued class functions on G and we let $\mathrm{Cl}_F(G_{p'}) := \{f : G_{p'} \longrightarrow F \mid f \text{ class function}\}$ denote the F-vector space of F-valued class functions on $G_{p'}$.

Proposition 34.9

A class function $\varphi \in \mathrm{Cl}(G_{p'})$ is a Brauer character if and only if it is a non-zero non-negative $\mathbb{Z}$-linear combination of elements of $\mathrm{IBr}_p(G)$.

Proof: The necessary condition is clear by Exercise 34.5(b). Conversely, let $n_1, \ldots, n_m \in \mathbb{Z}_{\geqslant 0}$ and let $\varphi_{S_1}, \ldots, \varphi_{S_m} \in \mathrm{IBr}_p(G)$ ($m \in \mathbb{Z}_{\geqslant 1}$) be the Brauer characters afforded by simple kG-modules $S_1, \ldots, S_m$. Then, by Exercise 34.5(c), the class function $\varphi := n_1\varphi_{S_1} + \ldots + n_m\varphi_{S_m}$ is the Brauer character afforded by the kG-module

$$S_1^{n_1} \oplus \ldots \oplus S_m^{n_m}\,.$$

■

Theorem 34.10

The set $\mathrm{IBr}_p(G)$ of irreducible Brauer characters of G is F-linearly independent and hence

$$|\mathrm{IBr}_p(G)| \leqslant \dim_F \mathrm{Cl}_F(G_{p'}) = \text{number of conjugacy classes of } p\text{-regular elements in } G\,.$$

In particular, $\mathrm{IBr}_p(G) = \{1_{G_{p'}}\}$ provided G is a finite p-group.

Without proof.
The second claim is obvious, because the indicator functions on the conjugacy classes of p-regular elements form an F-basis. The third claim is clear since if G is a p-group, then $G_{p'} = \{1_G\}$. Thus $|\mathrm{IBr}_p(G)| = 1$ by the first part, namely $\mathrm{IBr}_p(G) = \{\mathbf{1}_{G_{p'}}\}$.

35 Back to decomposition matrices of finite groups

We now want to investigate the connections between representations of G over F (or $\mathbb{C}$) and representations of G over k through the connections between their F-characters and Brauer characters.

Lemma 35.1

Let V be an FG-module with F-character χ_V. Let L be an $\mathcal{O}$-form of V and let $\overline{L} = L/\mathfrak{p}L$ be the reduction modulo $\mathfrak{p}$ of L. Then,

$$\chi_V|_{G_{p'}} = \varphi_{\overline{L}} ,$$

and is often called the **reduction modulo p of χ_V**.

Proof: Let $g \in G_{p'}$ and write $R_L : G \longrightarrow \mathrm{GL}(\mathcal{O})$ for the $\mathcal{O}$-representation associated to L. Since g is p-regular, the eigenvalues $x_1, \ldots, x_n$ of $R_L(g)$ belong to $\mu_F \subseteq \mathcal{O}$ and $\overline{x_1}, \ldots, \overline{x_n} \in k$ are the eigenvalues of $\rho_{\overline{L}}(g)$. Since by definition $\varphi_{\overline{L}}$ is the sum of the lifts of the latter quantities, we have

$$\varphi_{\overline{L}}(g) = x_1 + \ldots + x_n = \mathrm{Tr}(g, L^F) = \mathrm{Tr}(g, V) = \chi_V(g)$$

since L is an $\mathcal{O}$-form of V. ∎

Proposition 35.2

(a) The set $\mathrm{IBr}_p(G)$ is an F-basis of $\mathrm{Cl}_F(G_{p'})$.

(b) Given an irreducible F-character $\chi \in \mathrm{Irr}_F(G)$, there exist non-negative integers $d_{\chi\varphi}$ such that

$$\chi|_{G_{p'}} = \sum_{\varphi \in \mathrm{IBr}_p(G)} d_{\chi\varphi}\varphi.$$

(c) $|\mathrm{IBr}_p(G)|$ = number of p-regular conjugacy classes of G.

Proof: By Theorem 34.10 it only remains to prove that $\mathrm{IBr}_p(G)$ spans $\mathrm{Cl}_F(G_{p'})$. So let $\mu \in \mathrm{Cl}_F(G_{p'})$ be an arbitrary F-valued class function on $G_{p'}$. Then μ can be extended to $\mu^\# \in \mathrm{Cl}_F(G)$, e.g. by setting $\mu^\#(g) = 0$ for every $g \in G \backslash G_{p'}$. Since $\mathrm{Irr}_F(G)$ is an F-basis for $\mathrm{Cl}_F(G)$, we can write

$$\mu^\# = \sum_{\chi \in \mathrm{Irr}_F(G)} a_\chi \cdot \chi$$

with $a_\chi \in F \ \forall\ \chi \in \mathrm{Irr}_F(G)$. Thus

$$\mu = \mu^\#|_{G_{p'}} = \sum_{\chi \in \mathrm{Irr}_F(G)} a_\chi \cdot \chi|_{G_{p'}}.$$

where by Lemma 35.1 each $\chi|_{G_{p'}}$ is a Brauer character of G, and hence by Proposition 34.9, each $\chi|_{G_{p'}}$ is a non-negative integer linear combination of irreducible Brauer characters. Therefore μ is an F-linear combination of irreducible Brauer characters over F. It follows that $\mathrm{IBr}_p(G)$ is a generating set for $\mathrm{Cl}_F(G_{p'})$. This proves (a). Parts (b) and (c) are immediate consequences of (a) and its proof. ■

Exercise 35.3

Prove that two kG-modules afford the same Brauer character if and only if they have isomorphic composition factors (including multiplicities).

Remark 35.4

If we translate part (b) of Corollary 35.2 from irreducible characters and Brauer characters to FG-modules and kG-modules, we obtain that the integers $d_{\chi\varphi}$ are the same as the p-decomposition numbers of G as defined through Brauer's reciprocity theorem, i.e.

$$D := \mathrm{Dec}_p(G) = (d_{\chi\varphi})_{\substack{\chi\in\mathrm{Irr}_F(G)\\ \varphi\in\mathrm{IBr}_p(G)}}.$$

The Cartan matrix of G is then

$$C = D^{tr}D = (c_{\varphi\mu})_{\varphi,\mu\in\mathrm{IBr}_p(G)}$$

(see Exercise 33.4) and for every $\varphi, \mu \in \mathrm{IBr}_p(G)$ we have

$$c_{\varphi\mu} = \sum_{\chi\in\mathrm{Irr}_F(G)} d_{\chi\varphi}d_{\chi\mu}.$$

Corollary 35.5

(a) The decomposition matrix $\mathrm{Dec}_p(G)$ of G has full rank, namely $|\mathrm{IBr}_p(G)|$.

(b) The Cartan matrix of G is a symmetric positive definite matrix with non-negative integer entries.

Proof: It follows from Proposition 35.2 that $\{\chi|_{G_{p'}} \mid \chi \in \mathrm{Irr}_F(G)\}$ spans $\mathrm{Cl}_F(G_{p'})$ over F. There is therefore a subset $B \subseteq \{\chi|_{G_{p'}} \mid \chi \in \mathrm{Irr}_F(G)\}$ which forms an F-basis for $\mathrm{Cl}_F(G_{p'})$. Now by Proposition 35.2, the columns of the matrix $(d_{\chi\varphi})_{\chi\in B,\varphi\in\mathrm{IBr}_p(G)}$ are F-linearly independent, hence $\mathrm{Dec}_p(G)$ has full rank. This proves (a) and (b) follows immediately. ■

Recall now that projective kG-modules are liftable by Corollary 32.5. This enables us to associate an F-character of G to each PIM of kG.

Definition 35.6

Let $\varphi \in \mathrm{IBr}_p(G)$ be an irreducible Brauer character afforded by a simple kG-module S. Let P_S be the projective cover of S and let $\widehat{P}_S$ denote a lift of P_S to $\mathcal{O}$. Then, the F-character of $(\widehat{P}_S)^F$ is denoted by Φ_φ and is called the **projective indecomposable character** associated to S or φ.

Corollary 35.7

Let $\varphi \in \mathrm{IBr}_p(G)$. Then:

(a) $\Phi_\varphi = \sum_{\chi \in \mathrm{Irr}_F(G)} d_{\chi\varphi}\chi$; and

(b) $\Phi_\varphi|_{G_{p'}} = \sum_{\mu \in \mathrm{IBr}_p(G)} c_{\varphi\mu}\mu$.

Proof: (a) This follows from Brauer reciprocity.

(b) This follows from part (a) because

$$\Phi_\varphi|_{G_{p'}} = \sum_{\chi \in \mathrm{Irr}_F(G)} d_{\chi\varphi}\chi|_{G_{p'}} = \sum_{\chi \in \mathrm{Irr}_F(G)} d_{\chi\varphi} \sum_{\mu \in \mathrm{IBr}_p(G)} d_{\chi\mu}\mu = \sum_{\mu \in \mathrm{IBr}_p(G)} c_{\varphi\mu}\mu\,.$$

■

Theorem 35.8

Assume $p \nmid |G|$, then the following assertions hold:

(a) If V is a simple FG-module and L is an $\mathcal{O}$-form for V, then its reduction modulo $\mathfrak{p}$ is a simple kG-module and the map

$$\begin{array}{ccc} \mathrm{Irr}_F(G) & \longrightarrow & \mathrm{IBr}_p(G) \\ \chi_V & \mapsto & \chi_V|_{G_{p'}} = \chi_V \end{array}$$

is a bijection.

(b) Both the Cartan matrix of G and the decomposition matrix $\mathrm{Dec}_p(G)$ of G are the identity matrix, provided the rows and the columns are ordered in the same way.

Proof: Since $p \nmid |G|$, clearly $G_{p'} = G$. Now, by Maschke's theorem, kG is semisimple, so the simple kG-modules are precisely the PIMs of kG. Thus, if S is a simple kG-module affording the Brauer character φ, then by definition of the Cartan integers (Def. 22.2) and Remark 35.4 we have

$$c_{\varphi\mu} = \delta_{\varphi\mu} \quad \forall\ \mu \in \mathrm{IBr}_p\, G\,.$$

Therefore,

$$1 = c_{\varphi\varphi} = \sum_{\chi \in \mathrm{Irr}_F(G)} d_{\chi\varphi}^2$$

and it follows that there is a unique $\chi_0 \in \mathrm{Irr}_F(G)$ such that $d_{\chi_0\varphi} \neq 0$; in fact we must have $d_{\chi_0\varphi} = 1$. Now, it follows from Corollary 35.7 that

$$\Phi_\varphi = \chi_0 \quad \text{and} \quad \chi_0|_{G_{p'}} = \varphi\,,$$

so the first claim of (a) holds and the given map is well-defined and surjective. It follows immediately that f is bijective since by Proposition 35.2(c) we have

$$|\,\mathrm{IBr}_p(G)| = \#G\text{-conjugacy classes in } G = |\,\mathrm{Irr}_F(G)| < \infty\,.$$

This proves (a) and (b). ■

Finally, we would like to obtain orthogonality relations for Brauer characters, which generalise the row orthogonality relations for ordinary irreducible characters. However, unlike the case of ordinary characters, there are now two significant tables that we can construct: the table of values of Brauer characters of simple modules, and the table of values of Brauer characters of indecomposable projective modules.

Definition 35.9 (*Brauer character table*)

Set $l := |G_{p'}|$ and let $g_1, \dots, g_l$ be a complete set of representatives of the p-regular conjugacy classes of G.

(a) The **Brauer character table** of a finite group G is the matrix $\Big(\varphi(g_j)\Big)_{\substack{\varphi\in \mathrm{IBr}_p(G)\\ 1\leqslant j\leqslant l}} \in M_l(F)$.

(b) The **Brauer projective table** of a finite group G at p is the matrix $\Big(\Phi_\varphi(g_j)\Big)_{\substack{\varphi\in \mathrm{IBr}_p(G)\\ 1\leqslant j\leqslant l}} \in M_l(F)$.

Definition 35.10

Given F-valued class functions f_1, f_2 defined on a subset of G containing $G_{p'}$, define

$$\langle f_1, f_2\rangle_{p'} := \frac{1}{|G|}\sum_{g\in G_{p'}} f_1(g)f_2(g^{-1}).$$

Note. It is straightforward that $\langle\ ,\ \rangle_{p'}$ is F-bilinear on $\mathrm{Cl}_F(G_{p'})$.

With these tools we obtain a replacement for the row orthogonality relations for ordinary irreducible characters. It says that the rows of the Brauer character table and of the p-projective Brauer table are orthogonal to each other.

Theorem 35.11

(a) All projective indecomposable characters Φ_φ ($\varphi \in \mathrm{IBr}_p(G)$) vanish on p-singular elements, and the set $\{\Phi_\varphi \mid \varphi \in \mathrm{IBr}_p(G)\}$ is an F-basis of the subspace

$$\mathrm{Cl}_F^\circ(G) := \{f \in \mathrm{Cl}_F(G) \mid f(g) = 0\ \forall\, g \in G\backslash G_{p'}\}$$

of $\mathrm{Cl}_F(G)$.

(b) For every $\varphi, \psi \in \mathrm{IBr}_p(G)$ we have $\langle \varphi, \Phi_\psi\rangle_{p'} = \delta_{\varphi\psi} = \langle \Phi_\varphi, \psi\rangle_{p'}$.

Proof: Let $g_1, \dots, g_r$ be a complete set of representatives of the conjugacy classes of G such that $g_1, \dots, g_l$ are p-singular and $g_{l+1}, \dots, g_r$ are p-regular. If $l < j \leqslant r$, then by Proposition 35.2(b),

$$\chi(g_j^{-1}) = \chi|_{G_{p'}}(g_j^{-1}) = \sum_{\varphi\in \mathrm{IBr}_p(G)} d_{\chi\varphi}\varphi(g_j^{-1})$$

and for each $1 \leqslant i \leqslant r$ the 2nd Orthogonality Relations for the irreducible F-characters (see [Las20,

Thm. 12.2]) yield

$$(*) \qquad \delta_{ij}|C_G(g_i)| = \sum_{\chi\in \mathrm{Irr}_F(G)} \chi(g_i)\chi(g_j^{-1}) = \sum_{\chi\in \mathrm{Irr}_F(G)} \chi(g_i)\Big(\sum_{\varphi\in \mathrm{IBr}_p(G)} d_{\chi\varphi}\varphi(g_j^{-1})\Big)$$
$$= \sum_{\varphi\in \mathrm{IBr}_p(G)} \Big(\sum_{\chi\in \mathrm{Irr}_F(G)} d_{\chi\varphi}\chi(g_i)\Big)\varphi(g_j^{-1})$$
$$= \sum_{\varphi\in \mathrm{IBr}_p(G)} \Phi_\varphi(g_i)\varphi(g_j^{-1})$$

where the last equality holds by Corollary 35.7(a). Then for each $1 \leqslant i \leqslant l$, we have $\sum_{\varphi\in \mathrm{IBr}_p(G)} \Phi_\varphi(g_i)\varphi = 0$ in $\mathrm{Cl}_F(G_{p'})$ and we obtain that $\Phi_\varphi(g_i) = 0$ for each $\varphi \in \mathrm{IBr}_p(G)$ since $\mathrm{IBr}_p(G)$ is F-linearly independent. Thus the first claim of (a) is established.
Now, (∗) says that the square matrix

$$\left(\frac{\Phi_\varphi(g_i)}{|C_G(g_i)|}\right)^{tr}_{\substack{\varphi\in \mathrm{IBr}_p(G)\\ l+1\leqslant i\leqslant r}}$$

is a left inverse for the square matrix

$$\left(\varphi(g_i^{-1})\right)_{\substack{\varphi\in \mathrm{IBr}_p(G)\\ l+1\leqslant i\leqslant r}}.$$

Therefore, it is also a right inverse, and multiplying both matrices the other way around, we obtain (applying the Orbit-Stabiliser Theorem) that

$$\delta_{\varphi\psi} = \sum_{i=l+1}^{r} \frac{1}{|C_G(g_i)|}\varphi(g_i^{-1})\Phi_\psi(g_i) = \frac{1}{|G|}\sum_{g\in G_{p'}} \varphi(g^{-1})\Phi_\psi(g)$$
$$= \frac{1}{|G|}\sum_{g\in G_{p'}} \varphi(g)\Phi_\psi(g^{-1})$$
$$= \langle \varphi, \Phi_\psi\rangle_{p'}$$

for all $\varphi, \psi \in \mathrm{IBr}_p(G)$. Similarly $\langle \Phi_\varphi, \psi\rangle_{p'} = \delta_{\varphi\psi}$ for all $\varphi, \psi \in \mathrm{IBr}_p(G)$. This means in effect that $\{\Phi_\varphi|_{G_{p'}} \mid \varphi \in \mathrm{IBr}_p(G)\}$ and $\mathrm{IBr}_p(G)$ are dual bases of $\mathrm{Cl}_F(G_{p'})$ with respect to the F-bilinear form $\langle , \rangle_{p'}$. Thus, we have proved (a) and (b). ■

Remark 35.12

The proof of the theorem tells us that writing Φ for the Brauer projective table, Π for the Brauer character table and setting $B := \mathrm{diag}(|C_G(g_{l+1})|, \ldots, |C_G(g_r)|)$, then the orthogonality relations can be written as $\Phi^{tr}B^{-1}\overline{\Pi} = I$.

Exercise 35.13

Let H be a p'-subgroup of a finite group G. Prove that the character Φ_k is a constituent of the trivial F-character of H induced to G.

Exercise 35.14

Let $\varphi, \lambda \in \mathrm{IBr}_p(G)$ and assume that λ is linear. Prove that $\lambda\varphi \in \mathrm{IBr}_p(G)$ and $\lambda\Phi_\varphi = \Phi_{\lambda\varphi}$.

Exercise 35.15

Let G be a finite group and let ρ_{reg} denote the regular F-character of G. Prove that:

$$\rho_{\mathrm{reg}} = \sum_{\varphi\in \mathrm{IBr}_p(G)} \varphi(1)\Phi_\varphi \quad \text{and} \quad (\rho_{\mathrm{reg}})|_{G_{p'}} = \sum_{\varphi\in \mathrm{IBr}_p(G)} \Phi_\varphi(1)\varphi\,.$$

Exercise 35.16

Deduce from Theorem 35.11 that:

(a) the inverse of the Cartan matrix of kG is $C^{-1} = (\langle \varphi, \psi \rangle_{p'})_{\varphi,\psi \in \mathrm{IBr}_p(G)}$; and

(b) $|G|_p \mid \Phi_\varphi(1)$ for every $\varphi \in \mathrm{IBr}_p(G)$.

Exercise 35.17

(a) Let U be a kG-module and let P be a PIM of kG. Prove that

$$\dim_k \mathrm{Hom}_{kG}(P, U) = \frac{1}{|G|} \sum_{g \in G_{p'}} \varphi_P(g^{-1}) \varphi_U(g)$$

(b) Prove that the binary operation $\langle\ ,\ \rangle_{p'}$ is an inner product on $\mathrm{Cl}_F(G_{p'})$.

Exercise 35.18

Let $G := \mathfrak{A}_5$, the alternating group on 5 letters. Calculate the Brauer character table, the Cartan matrix and the decomposition matrix of G for $p = 3$.

[Hints. (1.) Use the ordinary character table of $\mathfrak{A}_5$ and reduction modulo p. (2.) A simple group does not have any irreducible Brauer character of degree 2.]

Exercise 35.19

Deduce from Remark 35.12 that column orthogonality relations for the Brauer characters take the form $\overline{\Pi}^{tr} \Phi = B$, i.e. given $g, h \in G_{p'}$ we have

$$\sum_{\phi \in \mathrm{IBr}_p(G)} \phi(g) \Phi_\varphi(h^{-1}) = \begin{cases} |C_G(g)| & \text{if } g \text{ and } h \text{ are } G\text{-conjugate,} \\ 0 & \text{otherwise.} \end{cases}$$

Chapter 10. Blocks

We can break down the representation theory of finite groups into its smallest parts: the *blocks* of the group algebra. First we will define blocks for arbitrary rings and then specify to the situation of a finite group G and a splitting p-modular system $(F, \mathcal{O}, k)$.

Notation: Throughout, G denotes a finite group, p a prime number. We let $(F, \mathcal{O}, k)$ denote a p-modular system and we assume F contains all $\exp(G)$-th roots of unity, so $(F, \mathcal{O}, k)$ is a splitting p-modular system for G and all its subgroups (see Theorem 31.2). We write $\mathfrak{p} := J(O)$. For $\Lambda \in \{F, \mathcal{O}, k\}$ all ΛG-modules considered are assumed to be free of finite rank over Λ.

References:

[Alp86] J. L. Alperin. *Local representation theory*. Vol. 11. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1986.

[Lin18] M. Linckelmann. *The block theory of finite group algebras. Vol. I*. Vol. 91. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 2018.

[LP10] K. Lux and H. Pahlings. *Representations of groups*. Vol. 124. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2010.

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

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

36 The blocks of a ring

Throughout this section we let A denote an arbitrary associative ring with an identity element (denoted 1_A).

Proposition 36.1

(a) There is a bijection between

(1) the set of decompositions

$$A = A_1 \oplus \cdots \oplus A_r \quad (r \in \mathbb{Z}_{\geqslant 1})$$

of A into a direct sum of (A, A)-subbimodules (or equiv. of two-sided ideals of A), and

(2) the set of decompositions

$$1_A = e_1 + \cdots + e_r$$

of 1_A into a sum of orthogonal idempotents of $Z(A)$,

in such a way that $e_i = 1_{A_i}$ and $A_i = Ae_i$ for every $1 \leqslant i \leqslant r$.

(b) For each $1 \leqslant i \leqslant r$, the direct summand A_i of A is indecomposable as an (A, A)-bimodule if and only if the corresponding central idempotent e_i is primitive.

(c) The decomposition of A into indecomposable (A, A)-subbimodules is uniquely determined.

Proof:

(a) Assume $A = A_1 \oplus \cdots \oplus A_r$ is a decomposition of A into (A, A)-bimodules. Then for each $1 \leqslant i \leqslant r$, there exists $e_i \in A_i$ such that

$$1_A = e_1 + \cdots + e_r\,.$$

Furthermore, for any element $a \in A$,

$$a = 1_A \cdot a = (e_1 + \cdots + e_r)a = e_1a + \cdots + e_ra$$

and

$$a = a \cdot 1_A = a(e_1 + \cdots + e_r) = ae_1 + \cdots + ae_r\,.$$

So for each $1 \leqslant j \leqslant r$, we have $e_ja = ae_j \in A_j$, and it follows in particular that $e_1, \ldots, e_r \in Z(A)$. Also, if $a_i \in A_i$ then $e_ia_i = a_i$ and $e_ja_i = 0$ if $j \neq i$. Hence, $e_i = 1_{A_i}$ and $e_i^2 = e_i$ so $\{e_i\}_{i=1}^r$ is a set of orthogonal idempotents of $Z(A)$, and $A_i = Ae_i$ for $1 \leqslant i \leqslant r$.

Conversely, if $\{e_i\}_{i=1}^r$ is a set of orthogonal idempotents of $Z(A)$ such that $1_A = \sum_{i=1}^r e_i$, then $A_i := Ae_i$ is an (A, A)-subbimodule of A for each $1 \leqslant i \leqslant r$ and $A_1 \oplus \cdots \oplus A_r$ is a direct sum decomposition of A into (A, A)-subbimodules.

(b) "$\Rightarrow$" Consider $A_i = Ae_i$ and suppose there exist orthogonal idempotents $f, h \in Z(A)$ such that $e_i = f + h$. Then $A_i = Af \oplus Ah$, where the sum is direct because if $a \in Af \cap Ah$ then $a = af$ and $a = ah$, hence $a = afh = a \cdot 0 = 0$. Thus, if e_i is not primitive, then A_i is decomposable as an (A, A)-bimodule.

"$\Leftarrow$" Now suppose that $A_i = Ae_i = L_1 \oplus L_2$, where L_1 and L_2 are two non-zero (A, A)-submodules. Then there exist $f \in L_1 \backslash \{0\}$ and $h \in L_2 \backslash \{0\}$ such that $e_i = f + h$. Now, $fh = 0$ since $fh \in L_1 \cap L_2 = \{0\}$. As e_i is the identity in A_i, we get

$$f = e_if = (f + h)f = f^2 + hf = f^2 + 0 = f^2$$

and similarly, $h^2 = h$, hence f and h are orthogonal idempotents, so e_i is not primitive.

(c) Suppose that $A = A_1 \oplus \cdots \oplus A_r$ ($r \in \mathbb{Z}_{r \geqslant 1}$) is a decomposition of A into (A, A)-subbimodules, and suppose that L is an indecomposable direct summand of A from a different such decomposition of A. Every $x \in L$ can be written as

$$x = a_1 + \cdots + a_r \text{ with } a_i \in A_i \text{ for each } 1 \leqslant i \leqslant r,$$

so $L \ni e_ix = a_i$. Hence $L = (L \cap A_1) \oplus \cdots \oplus (L \cap A_r)$ and this is a decomposition of L. Since L is indecomposable there exists $1 \leqslant m \leqslant r$ such that $L = L \cap A_m$. By the indecomposability of A_m, this must be the whole of A_m. Thus the decomposition of A into (A, A)-subbimodules is uniquely determined.

■

Definition 36.2 (*Block, block idempotent, block algebra, belonging to a block*)

(a) The uniquely determined (A,A)-bimodules $A_i = Ae_i$ $(1 \leqslant i \leqslant r)$ given by Theorem 36.1(c) are called the **blocks** of A and the corresponding primitive central idempotents e_i are called the associated **block idempotents**.
(The blocks are sometimes also called **block algebras** when A is an algebra.)

(b) We say that an (indecomposable) A-module M **belongs to (or lies in) the block** $A_i = Ae_i$ if $e_iM = M$ and $e_jM = 0$ for all $j \neq i$.

Exercise 36.3

Let $A = A_1 \oplus \cdots \oplus A_r$ $(r \in \mathbb{Z}_{\geqslant 1})$ be the block decomposition of A and let M be an arbitrary A-module. Prove that M admits a unique direct sum decomposition $M = M_1 \oplus \cdots \oplus M_r$ where for each $1 \leqslant i \leqslant r$ the summand M_i belongs to the block A_i of A. Deduce that every indecomposable A-module lies in a uniquely determined block of A.

Corollary 36.4

Let $A = A_1 \oplus \cdots \oplus A_r$ $(r \in \mathbb{Z}_{\geqslant 1})$ be the block decomposition of A and let $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ be a s.e.s. of A-modules and A-module homomorphisms. Then, for each $1 \leqslant i \leqslant r$:

$$M \text{ lies in the block } A_i \text{ of } A \text{ if and only } L \text{ and } N \text{ lie in } A_i\,.$$

In particular, if an A-module M lies in a block A_i of A, then so do all of its submodules and all of its factor modules.

Proof: Let $e_i \in Z(A)$ be the primitive idempotent corresponding to A_i. Now, by Definition 36.2 an A-module belongs to the block $A_i = Ae_i$ if and only if external multiplication by e_i is an A-isomorphism on that module. Considering the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\ \cong\downarrow & & \downarrow{\scriptstyle e_i\cdot(-)} & & \downarrow{\scriptstyle e_i\cdot(-)} & & \downarrow{\scriptstyle e_i\cdot(-)} & & \downarrow\cong \\ 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

it follows from the five-Lemma that this property holds for M if and only if it holds for L and N. ∎

37 p-Blocks of finite groups

We now return to finite groups and observe the following.

Example 17 (*Blocks of FG*)

Since FG is semisimple, the block decomposition of FG is given by the Artin-Wedderburn Theorem. In particular, the blocks are matrix algebras and can be labelled by the isomorphism classes of simple FG-modules.

Remark 37.1 (*Blocks of $\mathcal{O}G$ and kG*)

The lifting of idempotents obtained in Theorem 32.3 tells us that the quotient morphism $\mathcal{O}G \twoheadrightarrow [\mathcal{O}/\mathfrak{p}]G = kG, x \mapsto \overline{x} := x + \mathfrak{p} \cdot \mathcal{O}G$ induces a bijection

$$\begin{array}{ccc} \{\text{primitive idempotents of } Z(\mathcal{O}G)\} & \overset{\sim}{\longleftrightarrow} & \{\text{primitive idempotents of } Z(kG)\} \\ e & \mapsto & \overline{e} \end{array}$$

Thus a decomposition $1_{\mathcal{O}G} = e_1 + \cdots + e_r$ of the identity element of $\mathcal{O}G$ into a sum of primitive central idempotents corresponds to a decomposition $1_{kG} = \overline{e}_1 + \cdots + \overline{e}_r$ of the identity element of kG into a sum of primitive central idempotents of kG. Therefore, by Proposition 36.1, there is a bijection between the blocks of $\mathcal{O}G$ and the blocks of kG.

Warning: The definition of a block of a finite group may vary from one book (resp. article) to another and different authors use different definitions of *blocks of finite groups* which can, from text to text, be *algebras*, *idempotents*, *sets of modules*, sets of ordinary characters and/or Brauer characters. This may sound confusing at first sight, but in general, the context makes it clear which kind of objects is meant.

Definition 37.2 (*Blocks of finite groups, principal block*)

Let $\Lambda \in \{F, \mathcal{O}, k\}$. Then:

(a) The **blocks** of ΛG are the uniquely determined indecomposable $(\Lambda G, \Lambda G)$-bimodules defined by Theorem 36.1(c).

(b) We define a **p-block** of G to be the specification of a block of $\mathcal{O}G$, understanding also the corresponding block of kG, the corresponding idempotents of $\mathcal{O}G$ or of kG, or the modules which belongs to these blocks. We write $\mathrm{Bl}_p(G)$ for the set of all p-blocks of G, resp. $\mathrm{Bl}_p(kG)$ for the set of all blocks of kG.

Example 18 (*p-block(s) of a p-group*)

If G is a p-group, then G a unique p-block. Indeed, we have already observed that in this case, the trivial module is the unique simple module and hence a unique PIM, namely kG itself. So kG is certainly also indecomposable as a (kG, kG)-bimodule.

Theorem 37.3

Let $K \in \{F, k\}$ and let $S \ncong T$ be simple KG-modules. Then the following assertions are equivalent:

(a) S and T belong to the same block of KG.

(b) There exist simple KG-modules $S = S_1, \ldots, S_m = T$ $(m \in \mathbb{Z}_{\geqslant 2})$ such that S_i and S_{i+1} are both composition factors of the same projective indecomposable KG-module for each $1 \leqslant i \leqslant m-1$.

Proof: It is clear that all (a) and (b) define equivalence relations on the set of simple KG-modules. We have to prove that it is the same relation.

(b)⇒(a): This follows by induction on m because by Corollary 36.4 all the composition factors of a PIM of KG belong to the same block.

(a)⇒(b): Assume S belongs to the block B of KG. Decompose $B = P_1 \oplus \cdots \oplus P_s \oplus Q_1 \oplus \cdots \oplus Q_t$ in PIMs where composition factors of the P_i's are in relation (b) with S but none of the composition factors of the Q_j's are in relation (b) with S. To prove: $t = 0$. Clearly: then all simple modules T

belonging to B are in relation (b) with S by Corollary 36.4 since its projective cover must be one of the P_i's. Now, by construction, no composition factor of the Q_j's can be a composition factor of the P_i's, so $\mathrm{Hom}_B(P_i, Q_j) = 0 = \mathrm{Hom}_B(Q_j, P_i)$ for every $1 \leqslant i \leqslant s$ and every $1 \leqslant j \leqslant r$. Thus both $P_1 \oplus \cdots \oplus P_s$ and $Q_1 \oplus \cdots \oplus Q_t$ are invariant under all B-endomorphisms, in particular under left and right multiplication by elements of B, so they must themselves be blocks of KG. The only possibility is $t = 0$. ■

The effect of this result is that the division of the simple kG-modules into blocks can be achieved in a purely combinatorial fashion, knowing the Cartan matrix of kG. The connection with a block matrix decomposition of the Cartan matrix is probably the origin of the use of the term *block* in representation theory.

Corollary 37.4

On listing the simple kG-modules so that modules in each block occur together, the Cartan matrix of kG has a block diagonal form, with one block matrix for each p-block of the group. Up to permutation of simple modules within p-blocks and permutation of the p-blocks, this is the unique decomposition of the Cartan matrix into block diagonal form with the maximum number of block matrices.

Proof: Given any matrix we may define an equivalence relation on the set of rows and columns of the matrix by requiring that a row be equivalent to a column if and only if the entry in that row and column is non-zero, and extending this by transitivity to an equivalence relation. In the case of the Cartan matrix the row indexed by a simple module S is in the same equivalence class as the column indexed by P_S, because S is a composition factor of P_S. If we order the rows and columns of the Cartan matrix so that the rows and columns in each equivalence class come together, the matrix is in block diagonal form, with square blocks, and this is the unique such expression with the maximal number of blocks (up to permutation of the blocks and permutation of rows and columns within a block). It follows Theorem 37.3 that the matrix blocks biject with the blocks of the group algebra. ■

38 Defect groups

From now on we will only discuss the blocks of kG. (Analogous results hold for the corresponding blocks of $\mathcal{O}G$.) To finish this chapter, for the sake of completeness, in this section and the next section we give an overview of important results concerning p-blocks, mostly with sketches of proofs only.

Remark 38.1

Observe that any (kG, kG)-bimodule B becomes a left $k[G \times G]$-module in a natural way via the $G \times G$-action

$$\begin{aligned}(G \times G) \times B &\to B\\ \big((g,h),b\big) &\mapsto gbh^{-1}\end{aligned}$$

extended by k-bilinearity to the whole of $k[G \times G]$. This action is called the **conjugation action of** G on B. In particular, the group algebra kG itself is a left $k[G \times G]$-module and the blocks of kG can be viewed as indecomposable $k[G \times G]$-modules under this action.

Notation 38.2

Write $\Delta : G \longrightarrow G \times G, g \mapsto (g, g)$ for the diagonal embedding of G in $G \times G$.

Theorem 38.3

If $B \in \mathrm{Bl}_p(kG)$, then every vertex of B, considered as an indecomposable $k[G \times G]$-module, has the form $\Delta(D)$ for some p-subgroup $D \leqslant G$. Moreover, D is uniquely determined up to conjugation in G.

Proof: First, observe that $G \times G$ permutes the k-basis of G consisting of the group elements and

$$\mathrm{Stab}_{G\times G}(1) = \{(g_1, g_2) \in G \times G \mid g_1 \cdot 1 \cdot g_2^{-1} = 1\} = \Delta(G)\,.$$

It follows that

$$kG = k\uparrow_{\Delta(G)}^{G\times G}$$

as a $k[G\times G]$-module, and hence B is relatively $\Delta(G)$-projective since it is by definition a direct summand of kG seen as $k[G \times G]$-module. Therefore, by Definition 26.2, a vertex Q of B (still considered as a $k[G \times G]$-module) lies in $\Delta(G)$. By Proposition 26.4, Q is a p-group, and thus there exists a p-subgroup $D \leqslant G$ such that $Q = \Delta(D)$, proving the first statement.
Moreover, we know that $\Delta(D)$ is determined up to conjugacy in $G \times G$. Now, if $D_1 \leqslant G$ is another p-subgroup such that $\Delta(D_1)$ is a vertex of B, then there exists $(g_1, g_2) \in G \times G$ such that

$$\Delta(D_1) = {}^{(g_1,g_2)}\Delta(D)$$

and so for all $x \in D$, ${}^{(g_1,g_2)}(x, x) = ({}^{g_1}x, {}^{g_2}x) \in \Delta(D_1)$. Hence ${}^{g_1}x \in D_1$ for all $x \in D$. Finally, as $|D| = |D_1|$, it follows that ${}^{g_1}D = D_1$. ∎

Note: As a defect group of a block is uniquely determined up to G-conjugacy, it is clear that in fact all defect groups have the same order.

Definition 38.4 (*Defect group, defect*)

Let $B \in \mathrm{Bl}_p(kG)$.

(a) A **defect group** of B is a p-subgroup D of G such that $\Delta(D)$ is a vertex of B considered as a $k[G \times G]$-module.

(b) If the defect groups of B have order p^d ($d \in \mathbb{Z}_{\geqslant 0}$) then d is called the **defect** of B.

Defect groups are useful and important because in some sense they measure how far a p-block is from being semisimple.

Theorem 38.5

If B is a block of kG with defect group D, then every indecomposable kG-module belonging to B is relatively D-projective, and hence has a vertex contained in D.

Exercise 38.6

Prove Theorem 38.5.

[Hint: Prove that B, considered as kG-module via the conjugation action of G, is relatively D-projective.]

Corollary 38.7

Let B be a block of kG with a trivial defect group. Then B is a simple algebra, and in particular, is semisimple.

Proof: If B has a trivial defect group $D = \{1\}$, then by Theorem 38.5 every indecomposable kG-module belonging to B is $\{1\}$-projective, i.e. projective. So B is semisimple as all its modules are semisimple. But B is an indecomposable algebra by definition. Hence B is simple. ■

Main properties of the defect groups are the following. We mention them without proofs.

Theorem 38.8 (*Green*)

Let B be a block of kG with defect group D. Then:

(a) if P is a Sylow p-subgroup of G containing D, then there exists $g \in C_G(D)$ such that $D = P \cap {}^gP$;

(b) D contains every normal p-subgroup of G;

(c) D is the largest normal p-subgroup of $N_G(D)$, i.e. $D = O_p(N_G(D))$.

Example 19

Let G be a p-group. We already saw that in this case $\mathrm{Bl}_p(kG) = \{kG\}$. Then Theorem 38.8 shows that this block has a unique defect group $D = G$.

39 Brauer's 1st and 2nd Main Theorems

Finally we present two main results due to Brauer.

Definition 39.1

Let $H \leqslant G$, let $b \in \mathrm{Bl}_p(kH)$. Then a block $B \in \mathrm{Bl}_p(kG)$ **corresponds to** b if and only if $b \mid B{\downarrow}^{G\times G}_{H\times H}$, *and* B is the unique block of kG with this property. We then write $B = b^G$. If such a block B exists, then we say that b^G **is defined**.

Proposition 39.2 (*Facts about b^G*)

Let $H \leqslant G$ and let b be a block of kH with defect group D.

(a) If b^G is defined, then D lies in a defect group of b^G.

(b) If $H \leqslant N \leqslant G$, and b^N, $(b^N)^G$ and b^G are defined, then $b^G = (b^N)^G$.

(c) If $C_G(D) \leqslant H$ then b^G is defined.

Theorem 39.3 (*Brauer's First Main Theorem*)

Let $D \leqslant G$ be a p-subgroup and let $H \leqslant G$ containing $N_G(D)$. Then there is a bijection

$$\{\text{Blocks of } kH \text{ with defect group } D\} \xrightarrow{\sim} \{\text{Blocks of } kG \text{ with defect group } D\}$$
$$b \mapsto b^G$$

Moreover, in this case b^G is called the **Brauer correspondent** of b.

Proof (Sketch): This is a particular case of the Green correspondence. ■

Theorem 39.4 (*Brauer's Second Main Theorem*)

Let $H \leqslant G$, let B be a block of kG and let b be a block of kH. Suppose that V is an indecomposable module in B and U is an indecomposable module in b with vertex Q such that $C_G(Q) \leqslant H$. If U is a direct summand of $V{\downarrow}^G_H$, then b^G is defined and $b^G = B$.

Lemma 39.5

Let S be a simple kG-module. Then $O_p(G)$, the largest normal p-subgroup of G, acts trivially on S. In particular, the simple kG-modules are precisely the simple $k[G/O_p(G)]$-modules inflated to kG.

Proof: Since $O_p(G) \trianglelefteq G$, we know from Clifford's Theorem that $S{\downarrow}^G_{O_p(G)}$ is semisimple, hence of the form

$$S{\downarrow}^G_{O_p(G)} = k \oplus \cdots \oplus k$$

since $O_p(G)$ is a p-group and hence has only one simple module up to isomorphism, namely the trivial module. In other words, $O_p(G)$ acts trivially on S. The second claim follows immediately. ■

Corollary 39.6

Let B be a block of kG with defect group D. Then there exists an indecomposable kG-module belonging to B with vertex D.

Proof: Write $N := N_G(D)$. Let $b \in \mathrm{Bl}_p(kN)$ be a p-block with defect group D and let $B \in \mathrm{Bl}_p(kG)$ be the Brauer correspondent of b. As D is a defect group of b, $D = O_p(N)$ by Theorem 38.8(c). Now, let S be a simple kN-module belonging to b. Then, by Lemma 39.5, D acts trivially on S. So S can be viewed as a simple $k[N/D]$-module and we let P_S be the projective cover of S seen as a $k[N/D]$-module. Then, by Corollary 36.4, the inflation $\mathrm{Inf}^N_{N/D}(P_S)$ of P_S to N is an indecomposable kN-module belonging to b.

Claim 1: D is a vertex of $\mathrm{Inf}^N_{N/D}(P_S)$.
Indeed: By definition $P_S \mid k[N/D]$, so

$$\mathrm{Inf}^N_{N/D}(P_S) \mid \mathrm{Inf}^N_{N/D}(k[N/D]) = k{\uparrow}^N_D$$

and is therefore D-projective. Now, since $D \trianglelefteq N$, it follows from Clifford's Theorem that $k{\uparrow}^N_D{\downarrow}^N_D$ is a direct sum of N-conjugates of the trivial kD-module k, which are all again trivial since D is a p-group. So

$$\mathrm{Inf}^N_{N/D}(P_S){\downarrow}^N_D \mid k \oplus \cdots \oplus k\,.$$

Therefore the indecomposable direct summands of $\mathrm{Inf}^N_{N/D}(P_S){\downarrow}^N_D$ all have vertex D. It follows then from Lemma 27.1 that D is a vertex of $\mathrm{Inf}^N_{N/D}(P_S)$, because $\mathrm{Inf}^N_{N/D}(P_S){\downarrow}^N_D$ has at least one indecomposable direct summand with the same vertex as $\mathrm{Inf}^N_{N/D}(P_S)$. This proves Claim 1.

Next we observe that the kG-Green correspondent $f(\mathrm{Inf}_{N/D}^{N}(P_S))$ of $\mathrm{Inf}_{N/D}^{N}(P_S)$ is certainly an indecomposable kG-module with vertex D.

Claim 2: $f(\mathrm{Inf}_{N/D}^{N}(P_S))$ belongs to B.
Indeed, this is clear by definition of the Green correspondent and Brauer's First Main Theorem.

■

The next result shows that the converse of Corollary 38.7 also holds.

Corollary 39.7

A block B of kG is a simple algebra if and only if B has a trivial defect group.

Proof: If $B \in \mathrm{Bl}_p(kG)$ has trivial defect group, then B is a simple algebra by Corollary 38.7. Suppose now that B is a block of kG which is a simple algebra. Then B is semisimple so all B-modules are projective. Hence all indecomposable B-modules have trivial vertices so, by Corollary 39.6, B has a trivial defect group. ■

Definition 39.8 (*Principal block*)

(a) The *principal block* of kG is the block of kG to which the trivial kG-module k belongs. This block is denote by $B_0(kG)$.

(b) A block of kG whose defect groups are the Sylow p-subgroups of G is said to have *full defect*.

Lemma 39.9

(a) Any indecomposable kG-module whose vertices are the Sylow p-subgroups of G belongs to a block of kG of full defect.

(b) The principal block $B_0(kG)$ is a block of full defect.

Proof: (a) is clear by Theorem 38.5.

(b) is clear by (a) since the vertices of the trivial module are the Sylow p-subgroups of G. ■

Appendix 1: Background Material Module Theory

This appendix provides you with a short recap of the notions of the theory of modules, which we will assume as known for this lecture. We quickly review elementary definitions and constructions such as quotients, direct sum, direct products, tensor products and exact sequences, where we emphasise the approach via universal properties.

Notation: throughout this appendix we let R and S denote rings, and unless otherwise specified, all rings are assumed to be *unital* and *associative*.

Most of the results are stated without proof, as they have been studied in the B.Sc. lecture *Commutative Algebra*. As further reference I recommend for example:

References:

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

A Modules, submodules, morphisms

Definition A.1 (*Left R-module, right R-module, (R,S)-bimodule*)

(a) A **left R-module** is an ordered triple $(M,+,\cdot)$, where $(M,+)$ is an abelian group and $\cdot : R \times M \longrightarrow M, (r,m) \mapsto r \cdot m$ is a binary operation such that the map

$$\begin{array}{rccc} \lambda\colon & R & \longrightarrow & \mathrm{End}(M) \\ & r & \mapsto & \lambda(r) := \lambda_r : M \longrightarrow M, m \mapsto r \cdot m \end{array}$$

is a ring homomorphism. The operation $\cdot$ is called a **scalar multiplication** or an **external composition law**.

(b) A **right R-module** is defined analogously using a scalar multiplication $\cdot : M \times R \longrightarrow M$, $(m,r) \mapsto m \cdot r$ on the right-hand side.

(c) An (R,S)**-bimodule** is an abelian group $(M,+)$ which is both a left R-module and a right S-module, and which satisfies the axiom

$$r \cdot (m \cdot s) = (r \cdot m) \cdot s \qquad \forall\, r \in R, \forall\, s \in S, \forall\, m \in M\,.$$

Convention: Unless otherwise stated, in this lecture we always work with left modules. When no confusion is to be made, we will simply write "R-module" to mean "left R-module", denote R-modules by their underlying sets and write rm instead of $r \cdot m$. Definitions for right modules and bimodules are similar to those for left modules, hence in the sequel we omit them.

Definition A.2 (*R-submodule*)

An **R-submodule** of an R-module M is a subgroup $U \leqslant M$ such that $r \cdot u \in U \ \forall \ r \in R, \forall \ u \in U$.

Definition A.3 (*Morphisms*)

A **(homo)morphism** of R-modules (or an **R-linear map**, or an **R-homomorphism**) is a map of R-modules $\varphi : M \longrightarrow N$ such that:

(i) φ is a group homomorphism; and

(ii) $\varphi(r \cdot m) = r \cdot \varphi(m) \ \forall \ r \in R, \forall \ m \in M$.

Furthermore:

- An injective (resp. surjective) morphism of R-modules is sometimes called a **monomorphism** (resp. an **epimorphism**) and we often denote it with a *hook arrow* "$\hookrightarrow$" (resp. a *two-head arrow* "$\twoheadrightarrow$").
- A bijective morphism of R-modules is called an **isomorphism** (or an **R-isomorphism**), and we write $M \cong N$ if there exists an R-isomorphism between M and N.
- A morphism from an R-module to itself is called an **endomorphism** and a bijective endomorphism is called an **automorphism** .

Notation: We let ${}_R\mathbf{Mod}$ denote the category of left R-modules (with R-linear maps as morphisms), we let $\mathbf{Mod}_R$ denote the category of right R-modules (with R-linear maps as morphisms), and we let ${}_R\mathbf{Mod}_S$ denote the category of (R, S)-bimodules (with (R, S)-linear maps as morphisms).

Example A.4

(a) Exercise: Check that Definition A.1(a) is equivalent to requiring that $(M, +, \cdot)$ satisfies the following axioms:

(M1) $(M, +)$ is an abelian group;

(M2) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$ for each $r_1, r_2 \in R$ and each $m \in M$;

(M3) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ for each $r \in R$ and all $m_1, m_2 \in M$;

(M4) $(rs) \cdot m = r \cdot (s \cdot m)$ for each $r, s \in R$ and all $m \in M$.

(M5) $1_R \cdot m = m$ for each $m \in M$.

In other words, modules over rings satisfy the same axioms as vector spaces over fields. Hence: Vector spaces over a field K are K-modules, and conversely.

(b) Abelian groups are $\mathbb{Z}$-modules, and conversely.
Exercise: check it! What is the external composition law?

(c) If the ring R is commutative, then any right module can be made into a left module, and conversely.
Exercise: check it! Where does the commutativity come into play?

(d) If $\varphi : M \longrightarrow N$ is a morphism of R-modules, then the kernel $\ker(\varphi) := \{m \in M \mid \varphi(m) = 0_N\}$ of φ is an R-submodule of M and the image $\mathrm{Im}(\varphi) := \varphi(M) = \{\varphi(m) \mid m \in M\}$ of φ is an R-submodule of N.
If $M = N$ and φ is invertible, then the inverse is the usual set-theoretic *inverse map* φ^{-1} and is also an R-homomorphism.
Exercise: check it!

(e) **Change of the base ring:** if $\varphi : S \longrightarrow R$ is a ring homomorphism, then every R-module M can be endowed with the structure of an S-module with external composition law given by

$$\cdot : S \times M \longrightarrow M, (s, m) \mapsto s \cdot m := \varphi(s) \cdot m\,.$$

Exercise: check it!

Notation A.5

Given R-modules M and N, we set $\mathrm{Hom}_R(M, N) := \{\varphi : M \longrightarrow N \mid \varphi \text{ is an } R\text{-homomorphism}\}$. This is an abelian group for the pointwise addition of maps:

$$\begin{array}{rccc} + : & \mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(M,N) & \longrightarrow & \mathrm{Hom}_R(M,N) \\ & (\varphi, \psi) & \mapsto & \varphi + \psi : M \longrightarrow N, m \mapsto \varphi(m) + \psi(m)\,. \end{array}$$

In case $N = M$, we write $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ for the set of endomorphisms of M and $\mathrm{Aut}_R(M)$ for the set of automorphisms of M, i.e. the set of invertible endomorphisms of M.

Lemma-Definition A.6 (*Quotients of modules*)

Let U be an R-submodule of an R-module M. The quotient group M/U can be endowed with the structure of an R-module in a natural way via the external composition law

$$\begin{aligned} R \times M/U &\longrightarrow M/U \\ \big(r, m + U\big) &\longmapsto r \cdot m + U \end{aligned}$$

The canonical map $\pi : M \longrightarrow M/U, m \mapsto m + U$ is R-linear and we call it the **canonical** (or **natural**) **homomorphism**.

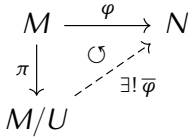
Definition A.7 (*Cokernel, coimage*)

Let $\varphi \in \mathrm{Hom}_R(M, N)$. The **cokernel** of φ is the quotient R-module $\mathrm{coker}(\varphi) := N/\operatorname{Im}\varphi$, and the **coimage** of φ is the quotient R-module $M/\ker\varphi$.

Theorem A.8 (*The universal property of the quotient and the isomorphism theorems*)

(a) **Universal property of the quotient**: Let $\varphi : M \longrightarrow N$ be a homomorphism of R-modules.

If U is an R-submodule of M such that $U \subseteq \ker(\varphi)$, then there exists a unique R-module homomorphism $\overline{\varphi} : M/U \longrightarrow N$ such that $\overline{\varphi} \circ \pi = \varphi$, or in other words such that the following diagram commutes:



Concretely, $\overline{\varphi}(m + U) = \varphi(m) \ \forall \ m + U \in M/U$.

(b) **1st isomorphism theorem**: With the notation of (a), if $U = \ker(\varphi)$, then

$$\overline{\varphi} : M/\ker(\varphi) \longrightarrow \mathrm{Im}(\varphi)$$

is an isomorphism of R-modules.

(c) **2nd isomorphism theorem**: If U_1, U_2 are R-submodules of M, then so are $U_1 \cap U_2$ and $U_1 + U_2$, and there is an isomorphism of R-modules

$$(U_1 + U_2)/U_2 \cong U_1/(U_1 \cap U_2)\,.$$

(d) **3rd isomorphism theorem**: If $U_1 \subseteq U_2$ are R-submodules of M, then there is an isomorphism of R-modules

$$(M/U_1)\,/_{(U_2/U_1)} \cong M/U_2\,.$$

(e) **Correspondence theorem**: If U is an R-submodule of M, then there is a bijection

$$\begin{array}{ccc} \{R\text{-submodules } X \text{ of } M \mid U \subseteq X\} & \longleftrightarrow & \{R\text{-submodules of } M/U\} \\ X & \mapsto & X/U \\ \pi^{-1}(Z) & \hookleftarrow & Z\,. \end{array}$$

B Free modules and projective modules

Free modules

Definition B.1 (*Generating set / R-basis / finitely generated/free R-module*)

Let M be an R-module and let $X \subseteq M$ be a subset. Then:

(a) M is said to be **generated by** X if every element $m \in M$ may be written as an R-linear combination $m = \sum_{x \in X} \lambda_x x$, i.e. where $\lambda_x \in R$ is almost everywhere 0. In this case we write $M = \langle X \rangle_R$ or $M = \sum_{x \in X} Rx$.

(b) M is said to be **finitely generated** if it admits a finite set of generators.

(c) X is an **R-basis** (or simply a **basis**) if X generates M and if every element of M can be written *in a unique way* as an R-linear combination $\sum_{x \in X} \lambda_x X$ (i.e. with $\lambda_x \in R$ almost everywhere 0).

(d) M is called **free** if it admits an R-basis X, and $|X|$ is called the **R-rank** of M.
Notation: In this case we write $M = \bigoplus_{x\in X} Rx \cong \bigoplus_{x\in X} R$.

Remark B.2

(a) **Warning**: If the ring R is not commutative, then it is not true in general that two different bases of a free R-module have the same number of elements.

(b) Let X be a generating set for M. Then, X is a basis of M if and only if S is R-linearly independent.

(c) If R is a field, then every R-module is free. (R-modules are R-vector spaces in this case!)

Proposition B.3 (*Universal property of free modules*)

Let M be a free R-module with R-basis X. If N is an R-module and $f : X \longrightarrow N$ is a map (of sets), then there exists a unique R-homomorphism $\widehat{f} : M \longrightarrow N$ such that the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{f} & N \\ {\scriptstyle \mathrm{inc}}\downarrow & \circlearrowleft & \nearrow {\scriptstyle \exists!\,\widehat{f}} \\ M & & \end{array}$$

We say that $\widehat{f}$ is obtained by **extending f by R-linearity**.

Proof: Given an R-linear combination $\sum_{x\in X} \lambda_x x \in M$, set $\widehat{f}(\sum_{x\in X} \lambda_x x) := \sum_{x\in X} \lambda_x f(x)$. The claim follows. ■

Proposition B.4 (*Properties of free modules*)

(a) Every R-module M is isomorphic to a quotient of a free R-module.

(b) If P is a free R-module, then $\mathrm{Hom}_R(P, -)$ is an exact functor.

Projective modules

Proposition-Definition B.5 (*Projective module*)

Let P be an R-module. Then the following are equivalent:

(a) The functor $\mathrm{Hom}_R(P, -)$ is exact.

(b) If $\psi \in \mathrm{Hom}_R(M, N)$ is a surjective morphism of R-modules, then the morphism of abelian groups $\psi_* : \mathrm{Hom}_R(P, M) \longrightarrow \mathrm{Hom}_R(P, N)$ is surjective.

(c) If $\pi : M \longrightarrow P$ is a surjective R-linear map, then π splits, i.e., there exists $\sigma : P \longrightarrow M$ such that $\pi \circ \sigma = \mathrm{Id}_P$.

(d) P is isomorphic to a direct summand of a free R-module.

If P satisfies these equivalent conditions, then P is called **projective**.

Example B.6

(a) If $R = \mathbb{Z}$, then every submodule of a free $\mathbb{Z}$-module is again free (main theorem on $\mathbb{Z}$-modules).

(b) Let e be an idempotent in R, that is $e^2 = e$. Then, $R \cong Re \oplus R(1-e)$ and Re is projective but not free if $e \neq 0, 1$.

(d) A direct sum of modules $\bigoplus_{i\in I} P_i$ is projective if and only if each P_i is projective.

C Direct products and direct sums

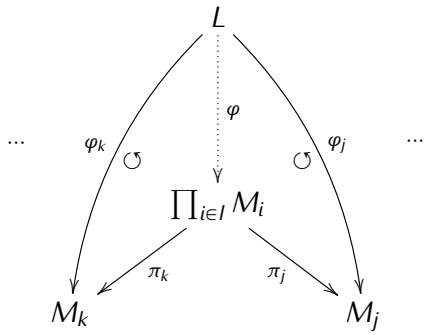
Let $\{M_i\}_{i\in I}$ be a family of R-modules. Then the abelian group $\prod_{i\in I} M_i$, that is the product of $\{M_i\}_{i\in I}$ seen as a family of abelian groups, becomes an R-module via the following external composition law:

$$\begin{aligned} R \times \prod_{i\in I} M_i &\longrightarrow \prod_{i\in I} M_i \\ \left(r, (m_i)_{i\in I}\right) &\longmapsto \left(r \cdot m_i\right)_{i\in I}. \end{aligned}$$

Furthermore, for each $j \in I$, we let $\pi_j : \prod_{i\in I} M_i \longrightarrow M_j, (m_i)_{i\in I} \mapsto m_j$ denotes the j-th projection from the product to the module M_j.

Proposition C.1 (Universal property of the direct product)

If $\{\varphi_i : L \longrightarrow M_i\}_{i\in I}$ is a family of R-homomorphisms, then there exists a unique R-homomorphism $\varphi : L \longrightarrow \prod_{i\in I} M_i$ such that $\pi_j \circ \varphi = \varphi_j$ for every $j \in I$.



Thus,

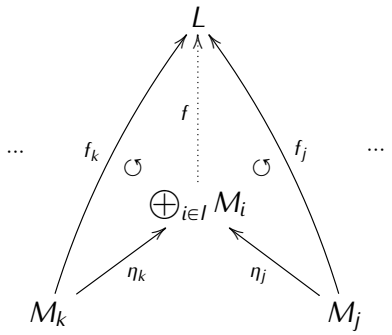
$$\begin{aligned} \mathrm{Hom}_R\left(L, \prod_{i\in I} M_i\right) &\longrightarrow \prod_{i\in I} \mathrm{Hom}_R(L, M_i) \\ f &\longmapsto \left(\pi_i \circ f\right)_{i\in I} \end{aligned}$$

is an isomorphism of abelian groups.

Now let $\bigoplus_{i\in I} M_i$ be the subgroup of $\prod_{i\in I} M_i$ consisting of the elements $(m_i)_{i\in I}$ such that $m_i = 0$ almost everywhere (i.e. $m_i = 0$ exept for a finite subset of indices $i \in I$). This subgroup is called the **direct sum** of the family $\{M_i\}_{i\in I}$ and is in fact an R-submodule of the product. For each $j \in I$, we let $\eta_j : M_j \longrightarrow \bigoplus_{i\in I} M_i, m_j \mapsto$ denote the canonical injection of M_j in the direct sum.

Proposition C.2 (Universal property of the direct sum)

If $\{f_i : M_i \longrightarrow L\}_{i\in I}$ is a family of R-homomorphisms, then there exists a unique R-homomorphism $\varphi : \bigoplus_{i\in I} M_i \longrightarrow L$ such that $f \circ \eta_j = f_j$ for every $j \in I$.



Thus,

$$\begin{aligned} \mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, L\Big) &\longrightarrow \prod_{i\in I} \mathrm{Hom}_R(M_i, L) \\ f &\longmapsto \big(f \circ \eta_i\big)_{i\in I} \end{aligned}$$

is an isomorphism of abelian groups.

Remark C.3

It is clear that if $|I| < \infty$, then $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$.

The direct sum as defined above is often called an *external* direct sum. This relates as follows with the usual notion of *internal* direct sum:

Definition C.4 (*"Internal" direct sums*)

Let M be an R-module and N_1, N_2 be two R-submodules of M. We write $M = N_1 \oplus N_2$ if every $m \in M$ can be written in a unique way as $m = n_1 + n_2$, where $n_1 \in N_1$ and $n_2 \in N_2$.

In fact $M = N_1 \oplus N_2$ (internal direct sum) if and only if $M = N_1 + N_2$ and $N_1 \cap N_2 = \{0\}$.

Proposition C.5

If N_1, N_2 and M are as above and $M = N_1 \oplus N_2$ then the homomorphism of R-modules

$$\begin{array}{rccl} \varphi: & M & \longrightarrow & N_1 \times N_2 = N_1 \oplus N_2 \ \text{ (external direct sum)} \\ & m = n_1 + n_2 & \mapsto & (n_1, n_2)\,, \end{array}$$

is an isomorphism of R-modules.

The above generalises to arbitrary internal direct sums $M = \bigoplus_{i\in I} N_i$.

D Exact sequences

Exact sequences constitute a very useful tool for the study of modules. Often we obtain valuable information about modules by *plugging them* in short exact sequences, where the other terms are known.

Definition D.1 (*Exact sequence*)

A sequence $L \xrightarrow{\varphi} M \xrightarrow{\psi} N$ of R-modules and R-linear maps is called **exact** (**at** M) if $\operatorname{Im}\varphi = \ker\psi$.

Remark D.2 (*Injectivity/surjectivity/short exact sequences*)

(a) $L \xrightarrow{\varphi} M$ is injective $\iff 0 \longrightarrow L \xrightarrow{\varphi} M$ is exact at L.

(b) $M \xrightarrow{\psi} N$ is surjective $\iff M \xrightarrow{\psi} N \longrightarrow 0$ is exact at N.

(c) $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ is exact (i.e. at L, M and N) if and only if φ is injective, ψ is surjective and ψ induces an R-isomorphism $\overline{\psi} : M/\operatorname{Im}\varphi \longrightarrow N, m + \operatorname{Im}\varphi \mapsto \psi(m)$.
Such a sequence is called a **short exact sequence** (**s.e.s.** for short).

(d) If $\varphi \in \operatorname{Hom}_R(L, M)$ is an injective morphism, then there is a s.e.s.

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\pi} \operatorname{coker}(\varphi) \longrightarrow 0$$

where π is the canonical projection.

(e) If $\psi \in \operatorname{Hom}_R(M, N)$ is a surjective morphism, then there is a s.e.s.

$$0 \longrightarrow \ker(\psi) \xrightarrow{i} M \xrightarrow{\psi} N \longrightarrow 0\,,$$

where i is the canonical injection.

Proposition D.3

Let Q be an R-module. Then the following holds:

(a) $\operatorname{Hom}_R(Q, -) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is a *left* exact covariant functor. In other words, if $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ is a s.e.s of R-modules, then the induced sequence

$$0 \longrightarrow \operatorname{Hom}_R(Q, L) \xrightarrow{\varphi_*} \operatorname{Hom}_R(Q, M) \xrightarrow{\psi_*} \operatorname{Hom}_R(Q, N)$$

is an exact sequence of abelian groups. Here $\varphi_* := \operatorname{Hom}_R(Q, \varphi)$, that is $\varphi_*(\alpha) = \varphi \circ \alpha$ for every $\alpha \in \operatorname{Hom}_R(Q, L)$ and similarly for ψ_*.

(b) $\operatorname{Hom}_R(-, Q) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is a *left* exact contravariant functor. In other words, if $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ is a s.e.s of R-modules, then the induced sequence

$$0 \longrightarrow \operatorname{Hom}_R(N, Q) \xrightarrow{\psi^*} \operatorname{Hom}_R(M, Q) \xrightarrow{\varphi^*} \operatorname{Hom}_R(L, Q)$$

is an exact sequence of abelian groups. Here $\varphi^* := \operatorname{Hom}_R(\varphi, Q)$, that is $\varphi^*(\alpha) = \alpha \circ \varphi$ for every $\alpha \in \operatorname{Hom}_R(M, Q)$ and similarly for ψ^*.

Exercise: verify that $\operatorname{Hom}_R(Q, -)$ and $\operatorname{Hom}_R(-, Q)$ are functors.
Notice that $\operatorname{Hom}_R(Q, -)$ and $\operatorname{Hom}_R(-, Q)$ are not *right* exact in general. Exercise: find counter-examples!

Lemma-Definition D.4 (*Split short exact sequence*)

A s.e.s. $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ of R-modules is called **split** if it satisfies one of the following equivalent conditions:

(a) ψ admits an R-linear section, i.e. if $\exists\, \sigma \in \mathrm{Hom}_R(N, M)$ such that $\psi \circ \sigma = \mathrm{Id}_N$;

(b) φ admits an R-linear retraction, i.e. if $\exists\ \rho \in \mathrm{Hom}_R(M, L)$ such that $\rho \circ \varphi = \mathrm{Id}_L$;

(c) $\exists$ an R-isomorphism $\alpha : M \longrightarrow L \oplus N$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}_L} & \circlearrowleft & \downarrow{\scriptstyle \alpha} & \circlearrowleft & \downarrow{\scriptstyle \mathrm{Id}_N} & & \\ 0 & \longrightarrow & L & \xrightarrow{i} & L \oplus N & \xrightarrow{p} & N & \longrightarrow & 0\,, \end{array}$$

where i, resp. p, are the canonical inclusion, resp. projection.

Remark D.5

If the sequence splits and σ is a section, then $M = \varphi(L) \oplus \sigma(N)$. If the sequence splits and ρ is a retraction, then $M = \varphi(L) \oplus \ker(\rho)$.

Example D.6

The s.e.s. of $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

defined by $\varphi([1]) = ([1], [0])$ and where π is the canonical projection onto the cokernel of φ is split but the sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

defined by $\varphi([1]) = ([2])$ and π is the canonical projection onto the cokernel of φ is not split. Exercise: justify this fact using a straightforward argument.

E Tensor products

Definition E.1 (*Tensor product of R-modules*)

Let M be a right R-module and let N be a left R-module. Let F be the free abelian group (= free $\mathbb{Z}$-module) with basis $M \times N$. Let G be the subgroup of F generated by all the elements

$$\begin{aligned} &(m_1 + m_2, n) - (m_1, n) - (m_2, n), \quad \forall m_1, m_2 \in M, \forall n \in N, \\ &(m, n_1 + n_2) - (m, n_1) - (m, n_2), \quad \forall m \in M, \forall n_1, n_2 \in N, \text{ and} \\ &(mr, n) - (m, rn), \quad \forall m \in M, \forall n \in N, \forall r \in R. \end{aligned}$$

The **tensor product of M and N (balanced over R)**, is the abelian group $M \otimes_R N := F/G$. The class of $(m,n) \in F$ in $M \otimes_R N$ is denoted by $m \otimes n$.

Remark E.2

(a) $M \otimes_R N = \langle m \otimes n \mid m \in M, n \in N \rangle_{\mathbb{Z}}$.

(b) In $M \otimes_R N$, we have the relations

$$\begin{aligned} &(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \quad \forall m_1, m_2 \in M, \forall n \in N, \\ &m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \quad \forall m \in M, \forall n_1, n_2 \in N, \text{ and} \\ &mr \otimes n = m \otimes rn, \quad \forall m \in M, \forall n \in N, \forall r \in R. \end{aligned}$$

In particular, $m \otimes 0 = 0 = 0 \otimes n \ \forall\ m \in M, \forall\ n \in N$ and $(-m) \otimes n = -(m \otimes n) = m \otimes (-n)$ $\forall\ m \in M, \forall\ n \in N$.

Definition E.3 (*R-balanced map*)

Let M and N be as above and let A be an abelian group. A map $f : M \times N \longrightarrow A$ is called R-**balanced** if

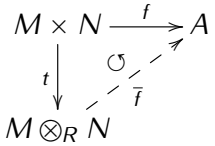
$$\begin{aligned} &f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n), \quad \forall m_1, m_2 \in M, \forall n \in N, \\ &f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2), \quad \forall m \in M, \forall n_1, n_2 \in N, \\ &f(mr, n) = f(m, rn), \quad \forall m \in M, \forall n \in N, \forall r \in R. \end{aligned}$$

Remark E.4

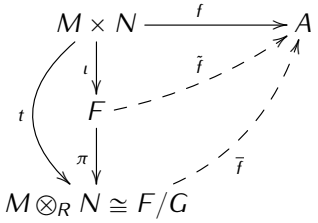
The canonical map $t : M \times N \longrightarrow M \otimes_R N, (m,n) \mapsto m \otimes n$ is R-balanced.

Proposition E.5 (*Universal property of the tensor product*)

Let M be a right R-module and let N be a left R-module. For every abelian group A and every R-balanced map $f : M \times N \longrightarrow A$ there exists a unique $\mathbb{Z}$-linear map $\overline{f} : M \otimes_R N \longrightarrow A$ such that the following diagram commutes:



Proof: Let $\iota : M \times N \longrightarrow F$ denote the canonical inclusion, and let $\pi : F \longrightarrow F/G$ denote the canonical projection. By the universal property of the free $\mathbb{Z}$-module, there exists a unique $\mathbb{Z}$-linear map $\tilde{f} : F \longrightarrow A$ such that $\tilde{f} \circ \iota = f$. Since f is R-balanced, we have that $G \subseteq \ker(\tilde{f})$. Therefore, the universal property of the quotient yields the existence of a unique homomorphism of abelian groups $\overline{f} : F/G \longrightarrow A$ such that $\overline{f} \circ \pi = \tilde{f}$:



Clearly $t = \pi \circ \iota$, and hence $\overline{f} \circ t = \overline{f} \circ \pi \circ \iota = \tilde{f} \circ \iota = f$. ∎

Remark E.6

Let M and N be as in Definition E.1.

(a) Let $\{M_i\}_{i\in I}$ be a collection of right R-modules, M be a right R-module, N be a left R-module and $\{N_j\}_{i\in J}$ be a collection of left R-modules. Then, we have

$$\bigoplus_{i\in I} M_i \otimes_R N \cong \bigoplus_{i\in I}(M_i \otimes_R N)$$
$$M \otimes_R \bigoplus_{j\in J} N_j \cong \bigoplus_{j\in J}(M \otimes_R N_j).$$

(This is easily proved using both the universal property of the direct sum and of the tensor product.)

(b) There are natural isomorphisms of abelian groups given by $R \otimes_R N \cong N$ via $r \otimes n \mapsto rn$, and $M \otimes_R R \cong M$ via $m \otimes r \mapsto mr$.

(c) It follows from (b), that if P is a free left R-module with R-basis X, then $N \otimes_R P \cong \bigoplus_{x\in X} N$, and if P is a free right R-module with R-basis X, then $P \otimes_R M \cong \bigoplus_{x\in X} M$.

(d) Let Q be a third ring. Then we obtain module structures on the tensor product as follows:

(i) If M is a (Q, R)-bimodule and N a left R-module, then $M \otimes_R N$ can be endowed with the structure of a left Q-module via

$$q \cdot (m \otimes n) = q \cdot m \otimes n \quad \forall q \in Q, \forall m \in M, \forall n \in N.$$

(ii) If M is a right R-module and N an (R, S)-bimodule, then $M \otimes_R N$ can be endowed with the structure of a right S-module via

$$(m \otimes n) \cdot s = qm \otimes n \cdot s \quad \forall s \in S, \forall m \in M, \forall n \in N.$$

(iii) If M is a (Q, R)-bimodule and N an (R, S)-bimodule. Then $M \otimes_R N$ can be endowed with the structure of a (Q, S)-bimodule via the external composition laws defined in (i) and (ii).

(e) Assume R is commutative. Then any R-module can be viewed as an (R, R)-bimodule. Then, in particular, $M \otimes_R N$ becomes an R-module (both on the left and on the right).

(f) For instance, it follows from (e) that if K is a field and M and N are K-vector spaces with K-bases $\{x_i\}_{i\in I}$ and $\{y_j\}_{j\in J}$ resp., then $M \otimes_K N$ is a K-vector space with a K-basis given by $\{x_i \otimes y_j\}_{(i,j)\in I\times J}$.

(g) **Tensor product of morphisms:** Let $f : M \longrightarrow M'$ be a morphism of right R-modules and $g : N \longrightarrow N'$ be a morphism of left R-modules. Then, by the universal property of the tensor product, there exists a unique $\mathbb{Z}$-linear map $f \otimes g : M \otimes_R N \longrightarrow M' \otimes_R N'$ such that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

Exercise E.7

(a) Assume R is a commutative ring and I is an ideal of R. Let M be a left R-module. Prove that there is an isomorphism of left R-modules $R/I \otimes_R M \cong M/IM$.

(b) Let m, n be coprime positive integers. Compute $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$, and $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$.

(c) Let K be a field and let U, V be finite-dimensional K-vector spaces. Prove that there is a natural isomorphism of K-vector spaces:

$$\mathrm{Hom}_K(U, V) \cong U^* \otimes_K V\,.$$

Proposition E.8 (*Right exactness of the tensor product*)

(a) Let N be a left R-module. Then $- \otimes_R N : \mathbf{Mod}_R \longrightarrow \mathbf{Ab}$ is a right exact covariant functor.

(b) Let M be a right R-module. Then $M \otimes_R - : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ is a right exact covariant functor.

Remark E.9

The functors $- \otimes_R N$ and $M \otimes_R -$ are not left exact in general.

F Algebras

In this lecture we aim at studying modules over specific rings, which are in particular *algebras*.

Definition F.1 (*Algebra*)

Let R be a commutative ring.

(a) An **R-algebra** is an ordered quadruple $(A, +, \cdot, *)$ such that the following axioms hold:

(A1) $(A, +, \cdot)$ is a ring;
(A2) $(A, +, *)$ is a left R-module; and
(A3) $r * (a \cdot b) = (r * a) \cdot b = a \cdot (r * b)$ $\forall\ a, b \in A$, $\forall\ r \in R$.

(b) A map $f : A \to B$ between two R-algebras is called an **algebra homomorphism** iff:

(i) f is a homomorphism of R-modules;
(ii) f is a ring homomorphism.

Example F.2 (*Algebras*)

(a) The ring R itself is an R-algebra.
[The internal composition law "$\cdot$" and the external composition law "$*$" coincide in this case.]

(b) For each $n \in \mathbb{Z}_{\geqslant 1}$ the set $M_n(R)$ of $n \times n$-matrices with coefficients in R is an R-algebra for its usual R-module and ring structures.

[Note: in particular R-algebras need not be commutative rings in general!]

(c) Let K be a field. Then for each $n \in \mathbb{Z}_{\geqslant 1}$ the polynom ring $K[X_1, \ldots, X_n]$ is a K-algebra for its usual K-vector space and ring structure.

(d) $\mathbb{R}$ and $\mathbb{C}$ are $\mathbb{Q}$-algebras, $\mathbb{C}$ is an $\mathbb{R}$-algebra, ...

(e) Rings are $\mathbb{Z}$-algebras.
Exercise: Check it!

Example F.3 (*Modules over algebras*)

(a) $A = M_n(R) \Rightarrow R^n$ is an A-module for the external composition law given by left matrix multiplication $A \times R^n \longrightarrow R^n, (B, x) \mapsto Bx$.

(b) If K is a field and V a K-vector space, then V becomes an A-algebra for $A := \mathrm{End}_K(V)$ together with the external composition law

$$A \times V \longrightarrow V, (\varphi, v) \mapsto \varphi(v)\,.$$

Exercise: Check it!

(c) An arbitrary A-module M can be seen as an R-module via a change of the base ring since $R \longrightarrow A, r \mapsto r * 1_A$ is a homomorphism of rings by the algebra axioms.

Exercise F.4

Let R be a commutative ring.

(a) Let M, N be R-modules. Prove that:

(1) $\mathrm{End}_R(M)$, endowed with the pointwise addition of maps and the usual composition of maps, is a ring. (Note that the commutativity of R is not necessary!)

(2) The abelian group $\mathrm{Hom}_R(M, N)$ is a left R-module for the external composition law defined by

$$(rf)(m) := f(rm) = rf(m) \qquad \forall\, r \in R,\ \forall f \in \mathrm{Hom}_R(M, N),\ \forall m \in M\,.$$

(b) Let now A be an R-algebra and M be an A-module. Prove that $\mathrm{End}_R(M)$ and $\mathrm{End}_A(M)$ are R-algebras.

Appendix 2: The Language of Category Theory

This appendix gives a short introduction to some of the basic notions of category theory used in this lecture.

References:

[Mac98] S. Mac Lane. *Categories for the working mathematician*. Second. Vol. 5. Springer-Verlag, New York, 1998.

[Wei94] C. A. Weibel. *An introduction to homological algebra*. Vol. 38. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1994.

G Categories

Definition G.1 (*Category*)

A **category** $\mathcal{C}$ consists of:

- a class $\mathrm{Ob}\,\mathcal{C}$ of **objects**,
- a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of **morphisms** for every ordered pair (A, B) of objects, and
- a **composition function**

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) & \longrightarrow & \mathrm{Hom}_{\mathcal{C}}(A,C) \\ (f,g) & \mapsto & g \circ f \end{array}$$

  for each ordered triple (A, B, C) of objects,

satisfying the following axioms:

(C1) **Unit axiom**: for each object $A \in \mathrm{Ob}\,\mathcal{C}$, there exists an **identity morphism** $1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ such that for every $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ for all $B \in \mathrm{Ob}\,\mathcal{C}$,

$$f \circ 1_A = f = 1_B \circ f\,.$$

(C2) **Associativity axiom**: for every $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ and $h \in \mathrm{Hom}_{\mathcal{C}}(C, D)$ with $A, B, C, D \in \mathrm{Ob}\,\mathcal{C}$,

$$h \circ (g \circ f) = (h \circ g) \circ f\,.$$

Let us start with some remarks and examples to enlighten this definition:

Remark G.2

(a) $\mathrm{Ob}\,\mathcal{C}$ need not be a set!

(b) The only requirement on $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is that it be a set, and it is allowed to be empty.

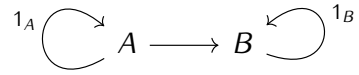
(c) It is common to write $f : A \longrightarrow B$ or $A \xrightarrow{f} B$ instead of $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, and to talk about *arrows* instead of *morphisms*. It is also common to write "$A \in \mathcal{C}$" instead of "$A \in \mathrm{Ob}\,\mathcal{C}$".

(d) The identity morphism $1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ is uniquely determined: indeed, if $f_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ were a second identity morphisms, then we would have $f_A = f_A \circ 1_A = 1_A$.

Example G.3

(a) $\mathcal{C} = \mathbf{1}$: category with one object and one morphism (the identity morphism):

(b) $\mathcal{C} = \mathbf{2}$: category with two objects and three morphism, where two of them are identity morphisms and the third one goes from one object to the other:



(c) A group G can be seen as a category $\mathcal{C}(G)$ with one object: $\mathrm{Ob}\,\mathcal{C}(G) = \{\bullet\}$, $\mathrm{Hom}_{\mathcal{C}(G)}(\bullet, \bullet) = G$ (notice that this is a set) and composition is given by multiplication in the group.

(d) The $n \times m$-matrices with entries in a field k for n, m ranging over the positive integers form a category $\mathbf{Mat}_k$: $\mathrm{Ob}\,\mathbf{Mat}_k = \mathbb{Z}_{>0}$, morphisms $n \longrightarrow m$ from n to m are the $m \times n$-matrices, and compositions are given by the ordinary matrix multiplication.

Example G.4 (*Categories and algebraic structures*)

(a) $\mathcal{C} = \mathbf{Set}$, the *category of sets*: objects are sets, morphisms are maps of sets, and composition is the usual composition of functions.

(b) $\mathcal{C} = \mathbf{Vec}_k$, the *category of vector spaces over the field k*: objects are k-vector spaces, morphisms are k-linear maps, and composition is the usual composition of functions.

(c) $\mathcal{C} = \mathbf{Top}$, the *category of topological spaces*: objects are topological spaces, morphisms are continous maps, and composition is the usual composition of functions.

(d) $\mathcal{C} = \mathbf{Grp}$, the *category of groups*: objects are groups, morphisms are homomorphisms of groups, and composition is the usual composition of functions.

(e) $\mathcal{C} = \mathbf{Ab}$, the *category of abelian groups*: objects are abelian groups, morphisms are homomorphisms of groups, and composition is the usual composition of functions.

(f) $\mathcal{C} = \mathbf{Rng}$, the *category of rings*: objects are rings, morphisms are homomorphisms of rings, and composition is the usual composition of functions.

(g) $\mathcal{C} = {}_R\mathbf{Mod}$, the *category of left R-modules*: objects are *left* modules over the ring R, morphisms are R-homomorphisms, and composition is the usual composition of functions.

(g') $\mathcal{C} = \mathbf{Mod}_R$, the *category of left R-modules*: objects are *right* modules over the ring R, morphisms are R-homomorphisms, and composition is the usual composition of functions.

(g") $\mathcal{C} = {}_R\mathbf{Mod}_S$, the *category of (R,S)-bimodules*: objects are (R,S)-bimodules over the rings R and S, morphisms are (R,S)-homomorphisms, and composition is the usual composition of functions.

(h) Examples of your own ...

Definition G.5 (*Monomorphism/epimorphism*)

Let $\mathcal{C}$ be a category and let $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ be a morphism. Then f is called

(a) a **monomorphism** iff for all morphisms $g_1, g_2 : C \longrightarrow A$,

$$f \circ g_1 = f \circ g_2 \Longrightarrow g_1 = g_2 \,.$$

(b) an **epimorphism** iff for all morphisms $g_1, g_2 : B \longrightarrow C$,

$$g_1 \circ f = g_2 \circ f \Longrightarrow g_1 = g_2 \,.$$

Remark G.6

In categories, where morphisms are set-theoretic maps, then injective morphisms are monomorphisms, and surjective morphisms are epimorphisms.
In module categories (${}_R\mathbf{Mod}$, $\mathbf{Mod}_R$, ${}_R\mathbf{Mod}_S$, ...), the converse holds as well, but:

Warning: It is not true in general, that all monomorphisms must be injective, and all epimorphisms must be surjective.

For example in **Rng**, the canonical injection $\iota : \mathbb{Z} \longrightarrow \mathbb{Q}$ is an epimorphism. Indeed, if C is a ring and $g_1, g_2 \in \mathrm{Hom}_{\mathbf{Rng}}(\mathbb{Q}, C)$

$$\mathbb{Z} \xrightarrow{\iota} \mathbb{Q} \underset{g_1}{\overset{g_2}{\rightrightarrows}} C$$

are such that $g_1 \circ \iota = g_2 \circ \iota$, then we must have $g_1 = g_2$ by the universal property of the field of fractions. However, ι is clearly not surjective.

H Functors

Definition H.1 (*Covariant functor*)

Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A **covariant functor** $F : \mathcal{C} \longrightarrow \mathcal{D}$ is a collection of maps:

- $F : \mathrm{Ob}\,\mathcal{C} \longrightarrow \mathrm{Ob}\,\mathcal{D}, X \mapsto F(X)$, and
- $F_{A,B} : \mathrm{Hom}_{\mathcal{C}}(A, B) \mapsto \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$,

satisfying:

(a) If $A \xrightarrow{f} B \xrightarrow{g} C$ are morphisms in $\mathcal{C}$, then $F(g \circ f) = F(g) \circ F(f)$; and

(b) $F(1_A) = 1_{F(A)}$ for every $A \in \mathrm{Ob}\,\mathcal{C}$.

Definition H.2 (*Contravariant functor*)

Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A **contravariant functor** $F : \mathcal{C} \longrightarrow \mathcal{D}$ is a collection of maps:

- $F : \mathrm{Ob}\,\mathcal{C} \longrightarrow \mathrm{Ob}\,\mathcal{D}, X \mapsto F(X)$, and
- $F_{A,B} : \mathrm{Hom}_{\mathcal{C}}(A, B) \mapsto \mathrm{Hom}_{\mathcal{D}}(F(B), F(A))$,

satisfying:

(a) If $A \xrightarrow{f} B \xrightarrow{g} C$ are morphisms in $\mathcal{C}$, then $F(g \circ f) = F(f) \circ F(g)$; and

(b) $F(1_A) = 1_{F(A)}$ for every $A \in \mathrm{Ob}\,\mathcal{C}$.

Remark H.3

Often in the literature functors are defined only on objects of categories. When no confusion is to be made and the action of functors on the morphism sets are implicitely obvious, we will also adopt this convention.

Example H.4

Let $Q \in \mathrm{Ob}({}_R\mathbf{Mod})$. Then

$$\begin{array}{rccc} \mathrm{Hom}_R(Q,-): & {}_R\mathbf{Mod} & \longrightarrow & \mathbf{Ab} \\ & M & \mapsto & \mathrm{Hom}_R(Q, M)\,, \end{array}$$

is a covariant functor, and

$$\begin{array}{rccc} \mathrm{Hom}_R(-,Q): & {}_R\mathbf{Mod} & \longrightarrow & \mathbf{Ab} \\ & M & \mapsto & \mathrm{Hom}_R(M, Q)\,, \end{array}$$

is a contravariant functor.

Exact Functors.

We are now interested in the relations between functors and exact sequences in categories where it makes sense to define exact sequences, that is categories that behave essentially like module categories

such as ${}_R\mathbf{Mod}$. These are the so-called **abelian categories**. It is not the aim, to go into these details, but roughly speaking abelian categories are categories satisfying the following properties:

- they have a zero object (in ${}_R\mathbf{Mod}$: the zero module)
- they have products and coproducts (in ${}_R\mathbf{Mod}$: products and direct sums)
- they have kernels and cokernels (in ${}_R\mathbf{Mod}$: the usual kernels and cokernels of R-linear maps)
- monomorphisms are kernels and epimorphisms are cokernels (in ${}_R\mathbf{Mod}$: satisfied)

Definition H.5 (*Pre-additive categories/additive functors*)

(a) A category $\mathcal{C}$ in which all sets of morphisms are abelian groups is called **pre-additive**.

(b) A functor $F : \mathcal{C} \longrightarrow \mathcal{D}$ between pre-additive categories is called **additive** iff the maps $F_{A,B}$ are homomorphisms of groups for all $A, B \in \mathrm{Ob}\,\mathcal{C}$.

Definition H.6 (*Left exact/right exact/exact functors*)

Let $F : \mathcal{C} \longrightarrow \mathcal{D}$ be a covariant (resp. contravariant) additive functor between two abelian categories, and let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a s.e.s. of objects and morphisms in $\mathcal{C}$. Then F is called:

(a) **left exact** if $0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$ (resp. $0 \longrightarrow F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A)$)) is an exact sequence.

(b) **right exact** if $F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0$ (resp. $F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A)) \longrightarrow 0$) is an exact sequence.

(c) **exact** if $0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0$ (resp. $0 \longrightarrow F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A)) \longrightarrow 0$) is a short exact sequence.

Example H.7

The functors $\mathrm{Hom}_R(Q, -)$ and $\mathrm{Hom}_R(-, Q)$ of Example H.4 are both left exact functors. Moreover $\mathrm{Hom}_R(Q, -)$ is exact if and only if Q is projective, and $\mathrm{Hom}_R(-, Q)$ is exact if and only if Q is injective.

Index of Notation

General symbols

$\mathbb{C}$	field of complex numbers
$\mathbb{F}_q$	finite field with q elements
Id_M	identity map on the set M
$\mathrm{Im}(f)$	image of the map f
$\ker(\varphi)$	kernel of the morphism φ
$\mathbb{N}$	the natural numbers without 0
$\mathbb{N}_0$	the natural numbers with 0
$\mathcal{O}$	discrete valuation ring
$\mathbb{P}$	the prime numbers in $\mathbb{Z}$
$\mathbb{Q}$	field of rational numbers
$\mathbb{Q}_p$	field of p-adic numbers
$\mathbb{R}$	field of real numbers
$\mathbb{Z}$	ring of integer numbers
$\mathbb{Z}_{\geqslant a}, \mathbb{Z}_{>a}, \mathbb{Z}_{\leqslant a}, \mathbb{Z}_{<a}$	$\{m \in \mathbb{Z} \mid m \geqslant a$ (resp. $m > a, m \geqslant a, m < a)\}$
$\mathbb{Z}_p$	ring of p-adic integers
$\lvert X \rvert$	cardinality of the set X
δ_{ij}	Kronecker's delta
$\bigcup$	union
$\coprod$	disjoint union
$\bigcap$	intersection
$\sum$	summation symbol
$\prod$, $\times$	cartesian/direct product
$\rtimes$	semi-direct product
$\oplus$	direct sum
$\otimes$	tensor product
$\varnothing$	empty set
$\forall$	for all
$\exists$	there exists
$\cong$	isomorphism
$a \mid b$, $a \nmid b$	a divides b, a does not divide b
(a, b)	gcd of a and b
$(F, \mathcal{O}, k)$	p-modular system
$f\lvert_S$	restriction of the map f to the subset S
$\hookrightarrow$	injective map
$\twoheadrightarrow$	surjective map

Group theory

$\mathrm{Aut}(G)$	automorphism group of the group G
$\mathfrak{A}_n$	alternating group on n letters
C_m	cyclic group of order m in multiplicative notation
$C_G(x)$	centraliser of the element x in G
$C_G(H)$	centraliser of the subgroup H in G
D_{2n}	dihedral group of order $2n$
$\delta : G \to G \times G$	diagonal map
$\mathrm{End}(A)$	endomorphism ring of the abelian group A
G/N	quotient group G modulo N
$\mathrm{GL}_n(K)$	general linear group over K
HgL	(H, L)-double coset
$[H\backslash G/L]$	set of (H, L)-double coset representatives
$H \leqslant G$, $H < G$	H is a subgroup of G, resp. a proper subgroup
$N \trianglelefteq G$	N is a normal subgroup G
$N_G(H)$	normaliser of H in G
$N \rtimes_\theta H$	semi-direct product of N in H w.r.t. θ
$\mathfrak{S}_n$	symmetric group on n letters
$\mathrm{SL}_n(K)$	special linear group over K
$\mathbb{Z}/m\mathbb{Z}$	cyclic group of order m in additive notation
${}^x g$	conjugate of g by x, i.e. gxg^{-1}
$\langle g \rangle \subseteq G$	subgroup of G generated by g
$\lvert G : H \rvert$	index of the subgroup H in G
$[G/H]$	set of left coset representatives of H
$\overline{x} \in G/N$	class of $x \in G$ in the quotient group G/N
$\{1\}$, 1	trivial group

Module theory

$\mathrm{Hom}_R(M, N)$	R-homomorphisms from M to N
$\mathrm{End}_R(M)$	R-endomorphism ring of the R-module M
$\mathrm{hd}(M)$	head of the module M
KG	group algebra of the group G over the commutative ring K
$\varepsilon : KG \longrightarrow K$	augmentation map
$I(KG)$	augmentation ideal
$J(R)$	Jacobson radical of the ring R
$M \mid N$	M is a direct summand of N
$M \otimes_R N$	tensor product of M and N balanced over R
M^G	G-fixed points of the module M
M_G	G-cofixed points of the module M
$M{\downarrow}_H^G$, $\mathrm{Res}_H^G(M)$	restriction of M from G to H
$M{\uparrow}_G^H$, $\mathrm{Ind}_H^G(M)$	induction of M from H to G
$\mathrm{Inf}_{G/N}^G(M)$	inflation of M from G/N to G
$R^\times$	units of the ring R
R°	regular left R-module on the ring R
$\mathrm{rad}(M)$	radical of the module M
$\mathrm{soc}(M)$	socle of the module M

$\langle X \rangle_R$	R-module generated by the set X
V^F	extension of scalars $F \otimes_{\mathcal{O}} V$
Z(R)	centre of the ring R

Character and Block Theory

b^G	Brauer correspondent of b
C	Cartan matrix of G
$\mathrm{Cl}_F(G)$, $\mathrm{Cl}_F(G_{p'})$	the class functions on G or $G_{p'}$
$\mathrm{Dec}_p(G)$	decomposition matrix
$G_{p'}$	p-regular elements of G
$\mathrm{Irr}_F(G)$	ordinary irreducible F-characters of G
$\mathrm{IBr}_p(G)$	irreducible p-Brauer characters of G
χ_{reg}	regular character
ρ_{reg}	regular representation
Φ_φ	projective indecomposable character associated to $\varphi \in \mathrm{IBr}(G)$

Category Theory

$\mathrm{Ob}\,\mathcal{C}$	objects of the category $\mathcal{C}$
$\mathrm{Hom}_{\mathcal{C}}(A, B)$	morphisms from A to B
Set	the category of sets
$\mathbf{Vec}_k$	the category of vector spaces over the field k
Top	the category of topological spaces
Grp	the category of groups
Ab	the category of abelian groups
Rng	the category of rings
${}_R\mathbf{Mod}$	the category of left R-modules
$\mathbf{Mod}_R$	the category of left R-modules
${}_R\mathbf{Mod}_S$	the category of (R, S)-bimodules