Modular Representation Theory of Finite Groups

Part I: Caroline Lassueur
Part II: Niamh Farrell
TU Kaiserslautern

Skript zur Vorlesung, WS 2019/20
(Lecture: 4SWS // Exercises: 2SWS)

Version: 8th of April 2020

Contents

Foreword

This text constitutes a faithful transcript of the lecture **Modular Representation Theory** held at the TU Kaiserslautern during the Winter Semester 2019/20 together with **Niamh Farrell** (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*. The lecture is built, so that you don't need to have attended *Commutative Algebra* and *Character Theory of Finite Groups* prior to this lecture. However, both these lectures share common ideas with *Representation Theory*. Therefore, in order to complement these pre-requisites, but avoid repetitions, the first chapter will deal formally with some background material on module theory, but some proofs will be omitted.

Sections marked with a star symbol (*) are presented in this Skript, for the sake of completeness, under a much more detailed version than in the lecture. The two main reasons are the following. Firstly, these notions are dealt with in details in the *Commutative Algebra* lecture, where the the commutativity of rings is most of the time indeed not needed. Secondly these notions are partly well-known from either group theory or linear algebra and easily pass over to modules with the same arguments.
The proofs of the results in these sections are not subject to direct exam questions.

Acknowledgement: We are grateful to Gunter Malle who provided us 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 we used as a basis for the development of this lecture. We are also grateful to the students who mentionned typos in the preliminary versions of these notes. Further comments, corrections and suggestions are of course more than 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.

Part I

Weeks 1-7
written by C. Lassueur

Chapter 0. Background Material: Module Theory

The aim of this preliminary chapter is to introduce (resp. recall) the basics of the theory of modules over finite dimensional algebras, which we will use throughout. We 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.

The **main aim of this lecture** is to study the so-called *representation theory of finite groups*, which amounts to studying modules over a specific ring, called the *group ring* (or *group algebra*), which is built from the group itself as a vector space with a basis given by the group elements. Hence we already get a first feeling that "juggling with algebraic structures" will be one of the recurrent feature of this lecture.

Notation: throughout this chapter we let R and S denote rings, and unless otherwise specified, all rings are assumed to be *unital* and *associative*.

Most results are stated without proof, as they have been / will be studied in the B.Sc. lecture *Commutative Algebra*. As further reference we recommend for example:

References:

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

1 Modules, submodules, morphisms*

Definition 1.1 (*Left R-module, right R-module, (R,S)-bimodule*)

(a) A **left R-module** is an ordered triple $(M,+,\cdot)$, where $(M,+)$ an abelian group and $\cdot : R\times M\longrightarrow M, (r,m)\mapsto r\cdot m$ is a **scalar multiplication** (or **external composition law**) such that the map

$$\begin{array}{rccl}\lambda: & R & \longrightarrow & \mathrm{End}(M)\\ & r & \mapsto & \lambda(r):=\lambda_r : M\longrightarrow M, m\mapsto r\cdot m\,,\end{array}$$

is a ring homomorphism.

(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 1.2 (*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 1.3 (*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) $\varphi(r \cdot m) = r \cdot \varphi(m)\ \forall\ r \in R,\ \forall\ m \in M$.

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). For the language of category theory, see the Appendix.

Example 1

(a) Exercise: Prove that Definition 1.1(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 $\operatorname{Im}(\varphi) := \varphi(M) = \{\varphi(m) \mid m \in M\}$ 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 1.4

Given R-modules M and N, we set $\operatorname{Hom}_R(M, N) := \{\varphi : M \longrightarrow N \mid \varphi \text{ is an } R\text{-homomorphism}\}$.
This is an abelian group for the pointwise addition of maps:

$$\begin{array}{rccl} +: & \operatorname{Hom}_R(M,N) \times \operatorname{Hom}_R(M,N) & \longrightarrow & \operatorname{Hom}_R(M,N) \\ & (\varphi,\psi) & \mapsto & \varphi+\psi : M \longrightarrow N, m \mapsto \varphi(m)+\psi(m)\,. \end{array}$$

In case $N = M$, we write $\operatorname{End}_R(M) := \operatorname{Hom}_R(M, M)$ for the set of endomorphisms of M and $\operatorname{Aut}_R(M)$ for the set of automorphisms of M, i.e. the set of invertible endomorphisms of M.

Lemma-Definition 1.5 (*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**.

Proof: We assume known from the "Algebraische Strukturen" that π is a group homomorphism.
Exercise: check that π preserves the scalar multiplication. ■

Definition 1.6 (*Cokernel, coimage*)

Let $\varphi \in \operatorname{Hom}_R(M, N)$. The **cokernel** of φ is the quotient R-module $\operatorname{coker}(\varphi) := N/\operatorname{Im}\varphi$, and the **coimage** of φ is the quotient R-module $M/\ker\varphi$.

Theorem 1.7 (***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:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & N \\ M/U \arrow[ur, dashed, "\exists!\,\overline{\varphi}"'] & \end{tikzcd}$$

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

$$\overline{\varphi} : M/\ker(\varphi) \longrightarrow \operatorname{Im}(\varphi)$$

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

$$(M/U_1)\big/(U_2/U_1) \cong M/U_2\,.$$

(e) **Correspondence theorem**: If U is an R-submodule of M, then there is a bijection

$$\begin{array}{ccc} \{R\text{-submodules } X \text{ of } M \mid U \subseteq X\} & \longleftrightarrow & \{R\text{-submodules of } M/U\} \\ X & \mapsto & X/U \\ \pi^{-1}(Z) & \leftarrow\!\shortmid & Z\,. \end{array}$$

Proof: We assume it is known (e.g. from the "Einführung in die Algebra") that these results hold for abelian groups and morphisms of abelian groups.
Exercise: check that they carry over to the R-module structure. ■

Definition 1.8 (***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 **R-rank** of M.
Notation: In this case we write $M = \bigoplus_{x\in X} Rx$.

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.

Proposition 1.9 (*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:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\text{inc}"'] \arrow[dr, phantom, "\circlearrowleft"] & N \\ M \arrow[ur, dashed, "\exists!\,\widehat{f}"'] & \end{tikzcd}$$

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. ∎

2 Algebras

In this lecture we aim at studying modules over specific rings, which are in particular *algebras*.

Definition 2.1 (*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 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 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 2.2

(a) Let R be a ring, and 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.

  (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 R be a commutative ring, 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.

3 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 **direct product** of $\{M_i\}_{i \in I}$ seen as a family of abelian groups, becomes an R-module via the following external composition law:

$$\begin{aligned} R \times \prod_{i \in I} M_i &\longrightarrow \prod_{i \in I} M_i \\ \big(r, (m_i)_{i \in I}\big) &\longmapsto \big(r \cdot m_i\big)_{i \in I} \end{aligned}$$

Exercise: check it!

Proposition 3.1 (Universal property of the direct product)

For each $j \in I$, we let $\pi_j : \prod_{i\in I} M_i \longrightarrow M_j$ denotes the j-th projection from the direct product to the module M_j. If $\{\varphi_i : L \longrightarrow M_i\}_{i\in I}$ is a collection of R-linear maps, then there exists a unique morphism of R-modules $\varphi : L \longrightarrow \prod_{i\in I} M_i$ such that $\pi_j \circ \varphi = \varphi_j$ for every $j \in I$.

$$\begin{tikzcd}
 & & M_k \\
L \arrow[urr, bend left, "\varphi_k"] \arrow[r, dashed, "\exists!\,\varphi"] \arrow[drr, bend right, "\varphi_j"'] & \prod_{i\in I} M_i \arrow[ur, "\pi_k"] \arrow[dr, "\pi_j"] \arrow[u, phantom, "\circlearrowleft"] \arrow[d, phantom, "\circlearrowleft"] & \\
 & & M_j
\end{tikzcd}$$

In other words, the map

$$\begin{array}{ccc}
\mathrm{Hom}_R\left(L, \prod_{i\in I} M_i\right) & \longrightarrow & \prod_{i\in I} \mathrm{Hom}_R(L, M_i) \\
\varphi & \longmapsto & \left(\pi_i \circ \varphi\right)_i
\end{array}$$

is an isomorphism of abelian groups.

Proof: Exercise! ■

Let now $\bigoplus_{i\in I} M_i$ 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. $m_i = 0$ except 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. Exercise: check it!

Proposition 3.2 (Universal property of the direct sum)

For each $j \in I$, we let $\eta_j : M_j \longrightarrow \bigoplus_{i\in I} M_i$ denote the canonical injection of M_j in the direct sum. If $\{f_i : M_i \longrightarrow L\}_{i\in I}$ is a collection of R-linear maps, then there exists a unique morphism of R-modules $\varphi : \bigoplus_{i\in I} M_i \longrightarrow L$ such that $f \circ \eta_j = f_j$ for every $j \in I$.

$$\begin{tikzcd}
M_j \arrow[dr, "\eta_j"] \arrow[drr, bend left, "f_j"] & & \\
 & \bigoplus_{i\in I} M_i \arrow[r, dashed, "\exists!\, f"] \arrow[u, phantom, "\circlearrowleft"] \arrow[d, phantom, "\circlearrowleft"] & L \\
M_k \arrow[ur, "\eta_k"] \arrow[urr, bend right, "f_k"'] & &
\end{tikzcd}$$

In other words, the map

$$\begin{array}{ccc}
\mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, L\right) & \longrightarrow & \prod_{i\in I} \mathrm{Hom}_R(M_i, L) \\
f & \longmapsto & \left(f \circ \eta_i\right)_i
\end{array}$$

is an isomorphism of abelian groups.

Proof: Exercise! ■

Remark 3.3

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 3.4 (***"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 3.5

If N_1, N_2 and M are as in Definition 3.4 and $M = N_1 \oplus N_2$ then the map

$$\begin{array}{rccll} \varphi: & M & \longrightarrow & N_1 \times N_2 = N_1 \oplus N_2 & \text{(external direct sum)} \\ & m = n_1 + n_2 & \mapsto & (n_1, n_2) & \end{array}$$

defines an R-isomorphism.
Moreover, the above generalises to arbitrary internal direct sums $M = \bigoplus_{i\in I} N_i$.

Proof: Exercise! ■

4 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 4.1 (***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 4.2 (***Injectivity/surjectivity/short exact sequences***)

(a) $L \xrightarrow{\varphi} M$ is injective $\Longleftrightarrow$ $0 \longrightarrow L \xrightarrow{\varphi} M$ is exact at L.

(b) $M \xrightarrow{\psi} N$ is surjective $\Longleftrightarrow$ $M \xrightarrow{\psi} N \longrightarrow 0$ 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 $\psi \in \mathrm{Hom}_R(M, N)$ 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 4.3

Let Q be an R-module. Then the following holds:

(a) $\mathrm{Hom}_R(Q, -) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ 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

$$0 \longrightarrow \mathrm{Hom}_R(Q, L) \xrightarrow{\varphi_*} \mathrm{Hom}_R(Q, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(Q, N)$$

is an exact sequence of abelian groups. Here $\varphi_* := \mathrm{Hom}_R(Q, \varphi)$, that is $\varphi_*(\alpha) = \varphi \circ \alpha$ for every $\alpha \in \mathrm{Hom}_R(Q, L)$ and similarly for ψ_*.

(b) $\mathrm{Hom}_R(-, Q) : {}_R\mathbf{Mod} \longrightarrow \mathbf{Ab}$ 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

$$0 \longrightarrow \mathrm{Hom}_R(N, Q) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, Q) \xrightarrow{\varphi^*} \mathrm{Hom}_R(L, Q)$$

is an exact sequence of abelian groups. Here $\varphi^* := \mathrm{Hom}_R(\varphi, Q)$, that is $\varphi^*(\alpha) = \alpha \circ \varphi$ for every $\alpha \in \mathrm{Hom}_R(M, Q)$ and similarly for ψ^*.

Notice that $\mathrm{Hom}_R(Q, -)$ and $\mathrm{Hom}_R(-, Q)$ are not *right* exact in general. Exercise: find counter-examples!

Proof: One easily checks that $\mathrm{Hom}_R(Q, -)$ and $\mathrm{Hom}_R(-, Q)$ are functors. Exercise!

(a) · **Exactness at** $\mathrm{Hom}_R(Q, L)$**:** Clear.
· **Exactness at** $\mathrm{Hom}_R(Q, M)$**:** We have

$$\begin{aligned}
\beta \in \ker \psi_* \iff \psi \circ \beta = 0 &\iff \mathrm{Im}\,\beta \subset \ker \psi = \mathrm{Im}\,\varphi \\
&\iff \forall q \in Q, \exists!\ l_q \in L \text{ such that } \beta(q) = \varphi(l_q) \\
&\iff \exists \text{ a map } \lambda : Q \longrightarrow L \text{ which sends } q \text{ to } l_q \text{ and such that } \varphi \circ \lambda = \beta \\
&\overset{\varphi \text{ inj}}{\iff} \exists\, \lambda \in \mathrm{Hom}_R(Q, L) \text{ which send } q \text{ to } l_q \text{ and such that } \varphi \circ \lambda = \beta \\
&\iff \beta \in \mathrm{Im}\,\varphi_*\,.
\end{aligned}$$

(b) Similar. Exercise! ∎

Lemma-Definition 4.4 (*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:

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\varphi"] \arrow[d, "\mathrm{Id}_L"'] \arrow[dr, phantom, "\circlearrowleft"] & M \arrow[r, "\psi"] \arrow[d, "\alpha"] \arrow[dr, phantom, "\circlearrowleft"] & N \arrow[r] \arrow[d, "\mathrm{Id}_N"] & 0 \\ 0 \arrow[r] & L \arrow[r, "i"] & L \oplus N \arrow[r, "p"] & N \arrow[r] & 0\,, \end{tikzcd}$$

where i, resp. p, are the canonical inclusion, resp. projection.

Proof: Exercise! ■

Remark 4.5

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 4

The sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

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.

5 Tensor products*

Definition 5.1 (*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 5.2

(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 5.3 (*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 5.4

The canonical map $t : M \times N \longrightarrow M \otimes_R N, (m, n) \mapsto m \otimes n$ is R-balanced.

Proposition 5.5 (*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:

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "t"'] \arrow[dr, phantom, "\circlearrowleft"] & A \\ M \otimes_R N \arrow[ur, dashed, "\overline{f}"'] & \end{tikzcd}$$

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 $\overline{f} \circ \pi = \tilde{f}$:

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "\iota"] \arrow[dd, bend right=60, "t"'] & A \\ F \arrow[ur, dashed, "\tilde{f}"] \arrow[d, "\pi"] & \\ M \otimes_R N \cong F/G \arrow[uur, dashed, "\overline{f}"'] & \end{tikzcd}$$

Clearly $t = \pi \circ \iota$, and hence $\overline{f} \circ t = \overline{f} \circ \pi \circ \iota = \tilde{f} \circ \iota = f$. ∎

Remark 5.6

Let M and N be as in Definition 5.1.

(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 $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

Proof: Exercise! ∎

Exercise 5.7

(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 5.8 (*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 5.9

The functors $-\otimes_R N$ and $M \otimes_R -$ are not left exact in general.

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.

Again results which intersect the *Commutative Algebra* lecture are stated without proof.

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.

6 (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.

Definition 6.1 (***simple/irreducible module / indecomposable module***)

(a) An R-module M is called **reducible** if it admits an R-submodule U such that $0 \lneq U \lneq M$. 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.

Remark 6.2

Clearly any simple module is also indecomposable. However, the converse does not hold in general. Exercise: find a counter-example!

Exercise 6.3

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 the R-submodules of R° are precisely the left ideals of R. Moreover, $I \lhd R$ 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°.

7 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 7.1 (***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 $f \in \mathrm{Hom}_R(V, W) \setminus \{0\}$ admits an inverse in $\mathrm{Hom}_R(V, W)$. 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 1(d), f is invertible with inverse $f^{-1} \in \mathrm{Hom}_R(V, W)$.

Now, (ii) is straightforward from the above. For (i), by Exercise 2.2, $\mathrm{End}_R(V)$ 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 $f \in \mathrm{End}_R(V) \setminus \{0\}$ 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 $v \in V \setminus \{0\}$ 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

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

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

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

■

8 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 8.1 (*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 8.2 (*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 8.3 (*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 8.4

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 8.5 (*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: See *Commutative Algebra*. (Or Exercise: deduce it from the properties of the Jacobson radical and semisimplicity, which we are going to develop in the next sections.) ■

9 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 9.1 (*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 9.2

(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 9.3 (*Nakayama's Lemma*)

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

Proof: See *Commutative Algebra*. ■

Remark 9.4

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:

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

10 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 10.1

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

Example 5

(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 10.2

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 9.1(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 9.1(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 10.3 (*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) $\ker(\varphi^n) = \ker(\varphi^{n+i})$ or every $i \geqslant 1$; and

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

Proof: By Corollary 8.4 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 10.4

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: "$\Rightarrow$": 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

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

would be invertible.
(Indeed, $\psi^{-1}\rho$ nilpotent $\Rightarrow (\mathrm{Id}_M - \psi^{-1}\rho)(\mathrm{Id}_M + \psi^{-1}\rho + (\psi^{-1}\rho)^2 + \cdots + (\psi^{-1}\rho)^{a-1}) = \mathrm{Id}_M$, 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.

"$\Leftarrow$": 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 9.1(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 10.2 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 10.5

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 10.6 (*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 10.4. 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.

11 Semisimplicity of rings and modules

Proposition-Definition 11.1 (*Completely reducible module / semisimple module*)

An R-module M satisfying the following equivalent conditions is called **completely reducible** or **semisimple**:

(a) $M = \oplus_{i\in I} S_i$ for some family $\{S_i\}_{i\in I}$ of simple submodules of M;

(b) $M = \sum_{i\in I} S_i$ for some family $\{S_i\}_{i\in I}$ of simple 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 $N \subseteq M$ 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) $N \cap \sum_{i\in J} S_i = 0$.

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

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

where the second equality holds by (1) and (2). Therefore, it suffice 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

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

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

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

(c)⇒(b): Let M_1 be the sum of all simple 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 $N \subseteq M_1$, a contradiction. Thus $M_2 = 0$ and so $M = M_1$. ■

Example 6

(a) The zero module is completely reducible, but neither reducible nor irreducible!

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

(1) $\{\left(\begin{smallmatrix} x \\ 0 \end{smallmatrix}\right) \mid x \in K\}$ is a simple A-submodule of V; but

(2) V is not semisimple.

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

Theorem-Definition 11.2 (*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 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 4.4. 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 there exists a finite number of indices $i_1, \dots, i_n \in I$ such that $1_R = x_{i_1} + \dots + x_{i_n}$ 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

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

and hence $R^\circ = L_{i_1} + \dots + L_{i_n}$. 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 a submodule of R°, which is semisimple by (d). Thus $R \cdot m$ is semisimple as well by Example 6(d). Finally, it follows from Proposition-Definition 11.1 that M is semisimple. ■

Example 7

Fields are semisimple. Indeed, if V is a finite-dimensional vector space over a field K of dimension n, then choosing a basis $\{e_1, \cdots, e_n\}$ of V yields $V = Ke_1 \oplus \dots \oplus Ke_n$, 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 11.2(c).

Corollary 11.3

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 11.2(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 8.4. In other words, R is both left Artinian and left Noetherian. ■

Next, we show that semisimplicity is detected by the Jacobson radical.

Definition 11.4

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

Proposition 11.5

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 $\mathfrak{m}_o \neq 0$, and pick a minimal left ideal I_1 of $\mathfrak{m}_o$. 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 11.2 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 $J(R) = 0$.

■

Exercise 11.6

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 11.7

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

Proof: Since by Exercise 9.2 the rings R and $\overline{R} := R/J(R)$ have the same simple modules (seen as abelian groups), Proposition-Definition 9.1(a) yields:

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

■

12 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 occur as direct summand of the regular module. The first key result in this direction is the following proposition:

Proposition 12.1

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 $\pi_j|_W \longrightarrow V_j$ 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 12.1:

Definition 12.2

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

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

Exercise 12.3

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

(a) Every non-zero left ideal I 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 mininmal (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.

We recall that:

Definition 12.4

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 12.5 (*Wedderburn*)

Let R be a semisimple ring. Then the following statements 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 of R lying in the centre of R.

Proof:

(a) By Exercise 12.3(d) 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 11.2, 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 12.1 any simple submodule of R° is isomorphic to V_j for some $j \in J$. Hence $|\mathcal{M}(R)| < \infty$.

(b) Proposition 12.1(d) also yields $S(R^\circ) = \bigoplus_{V_j \cong S} V_j$ and Proposition 12.1(a) 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 12.3(a), we may write $1 = \sum_{S \in \mathcal{M}(R)} e_S$, 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 $a_T \in S(R^\circ)$. 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 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 12.3 (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 12.6

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 12.7

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 12.8 (***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 algebra 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 12.3(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 12.1), 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 . ■

13 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 13.1

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 A-homomorphism.

(c) Prove that if $A = M_n(K)$, then $Z(A) \cong K I_n$, 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 13.2

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 we have $A = \prod_{S \in \mathcal{M}(A)} M_{n_S}(K)$, clearly

$$Z(A) = \prod_{S \in \mathcal{M}(A)} Z(M_{n_S}(K)) = \prod_{S \in \mathcal{M}(A)} = K I_{n_S} ,$$

where $\dim_K(K I_{n_S}) = 1$. The claim follows. ■

Remark 13.3

Notice that in the above Theorem, we require the field K to be algebraically closed, so that we can apply Part (b) of Schur's Lemma. This condition is in general too strong: in fact it would be sufficient that the field K has the property that $\mathrm{End}_A(S) \cong K$ for all simple A-modules. Such a field K is called a **splitting field** for A.

Corollary 13.4

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 9.2), hence $|\mathcal{M}(A)| = |\mathcal{M}(A/J(A))|$. Moreover, the quotient $A/J(A)$ is J-semisimple by Proposition 11.7, hence semisimple by Proposition 11.5 because finite-dimensional algebras are left Noetherian rings. Therefore it follows from Theorem 13.2(d) that

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

■

Corollary 13.5

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 13.2 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. ■

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.

Notation: throughout this chapter, unless otherwise specified, we let G denote a finite group and K be a commutative ring. Moroever, all modules considered are assumed to be **finitely generated**, hence **of finite rank** if they are free.

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.

14 Linear representations of finite groups

Definition 14.1 (*K-representation, matrix representation*)

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

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

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

Often, a representation is called an **ordinary representation** if K is a field of characteristic zero (or more generally of characteristic not dividing $|G|$), and it is called a **modular representation** if K is a field of characteristic p dividing $|G|$.

Remark 14.2

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 in the basis B). Therefore, 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

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

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 8

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

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

is a K-representation of G, called **<u>the</u> trivial representation** of G.

(b) Let $G = S_n$ ($n \geqslant 1$) be the symmetric group on n letters. Let $\{e_1, \dots, e_n\}$ be the standard basis of $V := K^n$. Then

$$\begin{array}{rccl} \rho : & S_n & \longrightarrow & \mathrm{GL}(K^n) \\ & \sigma & \mapsto & \rho(\sigma) : K^n \longrightarrow K^n, e_i \mapsto e_{\sigma(i)} \end{array}$$

is a K-representation, called **natural representation** of S_n.

(c) More generally, 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

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

is a K-representation of G, called **permutation representation** .

Clearly (b) is a special case of (c) with $G = S_n$ and $X = \{1, 2, \dots, n\}$.

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

Definition 14.3 (*Equivalent representations*)

Let $\rho_1 : G \longrightarrow \mathrm{GL}(V_1)$ and $\rho_2 : G \longrightarrow \mathrm{GL}(V_2)$ be two representations of G, where V_1, V_2 are two free K-modules of finite rank. Then ρ_1 and ρ_2 are called **equivalent** (or **similar**, or **isomorphic**) if there exists a K-isomorphism $\alpha : V_1 \longrightarrow V_2$ such that $\rho_2(g) = \alpha \circ \rho_1(g) \circ \alpha^{-1}$ for each $g \in G$.

$$\begin{tikzcd} V_1 \arrow[r, "\rho_1(g)"] \arrow[d, phantom, ""] & V_1 \arrow[d, "\alpha"] \\ V_2 \arrow[u, "\alpha^{-1}"] \arrow[r, "\rho_2(g)"'] \arrow[ur, phantom, "\circlearrowleft"] & V_2 \end{tikzcd}$$

In this case, we write $\rho_1 \sim \rho_2$.

Clearly $\sim$ is an equivalence relation.

15 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 15.1 (*Group algebra*)

The **group ring** KG is the ring whose elements are the linear combinations $\sum_{g\in G} \lambda_g g$ with $\lambda_g \in K$, 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 15.2

Clearly the K-rank of KG is $|G|$ and $G \subseteq (KG)^\times$. Moreover, KG is commutative if and only if G is an abelian group. Also note that if K is a field, then it is clear that KG a left Artinian ring because we may consider K-dimesnions, so that by Hopkin's Theorem a KG-module is finitely generated if and only if it admits a composition series.

Proposition 15.3

(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

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

extended by K-linearity to the whole of KG.

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

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

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 makes $(V,+)$ into a KG-module.

(b) Clearly, it follows from the KG-module axioms that $\rho_V(g) \in \mathrm{GL}(V)$ and also that $\rho_V(g_1 g_2) = \rho_V(g_1)\circ\rho_V(g_2)$ für alle $g_1, g_2 \in G$, hence ρ_V is a group homomorphism. ■

Notice that, since G is a group, the map $KG \longrightarrow KG$ such that $g \mapsto g^{-1}$ 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.

Example 9

The trivial representation of Example 8(b) corresponds to the so-called **trivial** KG**-module**, that is the commutative ring K itself seen as a KG-module via the G-action

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

extended by K-linearity to the whole of KG.

Exercise 15.4

Let G be a finite group and let K be a commutative ring. Prove that the regular representation ρ_{reg} of G defined in Exampale 8(c) corresponds to the regular KG-module KG° via Proposition 15.3.

Remark 15.5

More generally, through Proposition 15.3, we may transport terminology and properties from KG-modules to representations and conversely.

For instance, we say that a representation is *irreducible* (or *simple*) if the corresponding KG-module is irreducible (= simple). (Notice that it is tradition to use the term *simple* for modules, and the term irreducible for *representations*.)

Lemma 15.6

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 15.3 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 ?? 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 $g \in G$. ■

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

Proposition-Definition 15.7 (*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 shows 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 15.8

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

Exercise 15.9 (*Proof of Lemma 15.8. Proceed as indicated.*)

(a) (Facultative: you can accept this result and treat (b), (c) and (d) only.) Recall that an ideal I of a ring R is called a **nil ideal** if each element of I is nilpotent. Prove that 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 10 on Exercise Sheet 2.

(d) Conclude that $I(KG) = J(KG)$ using Proposition-Definition 15.7.

16 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 16.1 (*Maschke*)

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

Proof: By Proposition-Definition 11.2, 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 11.2). 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

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

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 10

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. We obtain it using the properties of the augmentation ideal.

Theorem 16.2 (*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 $v = \sum_{g\in G} \lambda_g g \in V \setminus \{0\}$. 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 $tv \in I(KG)\setminus\{0\}$ 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 inKG°. Therefore, by Proposition-Definition 11.1, KG° is not semisimple and hence KG is not semisimple by Theorem-Definition 11.2. ■

In the case the filed K is algebraically closed, the following Exercise offers a second proof exploiting Artin-Wedderburn.

Exercise 16.3 (*Proof of the Converse of Maschke's Theorem for $K = \overline{K}$*)

Assume $K = \overline{K}$ is an algebraically closed field of characteristic p with $p \mid |G|$. 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 13.2.

17 Simple modules over algebraically closed fields

Throughout this section, we assume that $K = \overline{K}$ is an algebraically closed field.

As mentioned in Chapter 2, §13 this hypothesis may always be replaced by the weaker assumption that the field K is a splitting field for the group algebra KG, which we simply call a *splitting field for G*.

We state here some elementary facts about simple KG-modules, which we obtain as consequences of the Artin-Wedderburn structure theorem.

Corollary 17.1

There are only finitely many isomorphism classes of simple KG-modules, or equivalently, there are only finitely many irreducible K-representations of G, up to similarity.

Proof: Since $K = \overline{K}$, the first claim follows from Corollary 13.4 and the equivalent characterisation from Proposition 15.3. ■

Corollary 17.2

If G is an abelian group, then any simple KG-module is one-dimensional, or equivalently, all irreducible K-representations of G have degree one.

Proof: Since $K = \overline{K}$ and KG is commutative the first claim follows from Corollary 13.5 and the equivalent characterisation from Proposition 15.3. ■

Corollary 17.3

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

Proof: By Lemma 15.8 we have $J(KG) = I(KG)$. Thus $KG/J(KG) \cong K$ as K-algebras by Proposition-Definition 15.7. Now, as K is commutative, $Z(K) = K$, and it follows from Corollary 13.4 that

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

■

Remark 17.4

Another standard proof for Corollary 17.3 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 17.5

If $\mathrm{char}(K) \nmid |G|$, 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 Theorem 13.2 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 has tensor products, Hom-functors, duality, or using subgroups or quotients of the initial group. Moroever, 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 **finitely generated** and **free as K-modules**, hence of **of finite K-rank**.

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.

18 Tensors, Hom's and duality

Definition 18.1 (*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

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

extended by K-linearity to the whole of KG.

Definition 18.2 (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 18.2 to $N = K$ yields a KG-module structure on the K-dual $M^* = \mathrm{Hom}_K(M,K)$.

Definition 18.3 (*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 4.3.)

For the remainder of this section, assume that K is a field.

Properties 18.4

Let M, N be KG-modules. Then the following properties hold:

(a) If $\rho : M \to N$ is an injective (resp. surjective) KG-homomorphism, then $\rho^* : N^* \to M^*$ is surjective (resp. injective).
Conclude that if $X \subseteq N$ is a KG-submodule, there exists a KG-submodule $Y \subseteq N^*$ such that $Y \cong (N/X)^*$ and $N^*/Y \cong X^*$.

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

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

(d) M is simple, resp. indecomposable, if and only if M^* is simple, resp. indecomposable.

Proof: Exercise. ∎

Lemma 18.5

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

Proof: By Exercise 3(c), Sheet 1, there is a K-isomorphism

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

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 18.6

In case $M = N$ the above constructions yield a KG-module structure on $\mathrm{End}_K(M) \cong M^* \otimes_K M$. Moroever, if $\dim_K(M) =: n$, $\{m_1, \dots, m_n\}$ 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 $\mathrm{r} := \sum_{i=1}^n m_i^* \otimes m_i \in M^* \otimes_K M$. (Exercise!)
This allows us to define the KG-homomorphism:

$$\begin{array}{rccc} \mathbf{I}: & K & \longrightarrow & M^* \otimes_K M \\ & 1 & \mapsto & \mathrm{r} \end{array}$$

Definition 18.7 (*Trace map*)

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

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

Notation 18.8

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 18.9

If $\dim_K(M) \in K^\times$, then $K \mid M^* \otimes_K M$.

Proof: By Lemma-Definition 4.4(c) it suffices to check that $\frac{1}{\dim_K(M)}\mathbf{I}$ 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

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

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

Exercise 18.10

Let K be a field and let M be a KG-module. Prove that:

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

(b) $M \mid M \otimes_K M^* \otimes_K M$;

(c) if $p \mid \dim_K(M)$, then $M \oplus M \mid M \otimes_K M^* \otimes_K M$.

19 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 19.1 (***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 19.2

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 $m \in M$, which happens if and only if $g \cdot f(^{-1} \cdot m) = f(m)$ for all $g \in G$ and all $m \in M$. This is exactly the condition that f is fixed under the action of G.
Second claim: similar, Exercise! ∎

Exercise 19.3

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 $\mathrm{Hom}_{KG}(N, -)$ (as in Proposition 4.3(a)) and use the fact that the modules considered are all finite-diemensional.]

20 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 20.1

(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 $U \leqslant G$ 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 20.2 (*Inflation*)

Let $U \leqslant G$ is 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 via π, which we denote by $\mathrm{Inf}_{G/U}^{G}(M)$ and call the **inflation** of M from G/U to G.

Definition 20.3 (*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 via ι, which we denote by $\mathrm{Res}_H^G(M)$ or simply $M{\downarrow}_H^G$ and call the **restriction** of M from G to H.

Remark 20.4

(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 $M{\downarrow}_H^G$ is simply the composite morphism
$$H \xrightarrow{\iota} G \xrightarrow{\rho} GL(M)\,.$$

(b) Similarly, if $U \leqslant G$ 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 $\mathrm{Inf}_{G/U}^{G}(M)$ is simply
$$G \xrightarrow{\pi} G/U \xrightarrow{\rho} GL(M)\,.$$

Lemma 20.5 (*Properties of restriction*)

(a) If $H \leqslant G$ and M_1, M_2 are two KG-modules, then $(M_1 \oplus M_2){\downarrow}_H^G = M_1{\downarrow}_H^G \oplus M_2{\downarrow}_H^G$.

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

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

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

Hence 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 $M{\downarrow}^G_H{\downarrow}^H_L = M{\downarrow}^G_L$. ■

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

Definition 20.6 (*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 sometimes also write $M{\uparrow}_H^G$ instead of $\mathrm{Ind}_H^G(M)$.

Example 11 (*Fundamental example*)

If $H = \{1\}$ and $M = K$, then $K{\uparrow}_{\{1\}}^G = KG \otimes_K K \cong KG$.

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

Remark 20.7

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

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

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: Prove 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 20.8 (*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 is 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:
$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "j"'] \arrow[dr, phantom, "\circlearrowleft"] & N \\ \mathrm{Ind}_H^G(M) \arrow[ur, dashed, "\exists!\,\tilde{\varphi}"'] & \end{tikzcd}$$

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:

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

Example 12

If $H = \{1\}$ and $M = K$, then $\mathrm{Coind}_{\{1\}}^G(K) \cong (KG)^*$ (i.e. with the KG-module structure of $(KG)^*$ of Definition 18.3).

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 20.9 (***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

$$\begin{array}{rccl} \Phi: & KG \otimes_{KH} M & \longrightarrow & \mathrm{Hom}_{KH}(KG, M) \\ & g \otimes m & \mapsto & \Phi(g \otimes m) : KG \longrightarrow M, x \mapsto (xg)m \end{array}$$

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 $N = K$,

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

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

Theorem 20.10 (***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, $\mathrm{Hom}_{KG}(KG, N) \cong N{\downarrow}_H^G$ as KH-modules, and it suffices to prove the second isomorphism. In fact, this K-isomorphism is given by the map

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

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

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

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*

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

provides us with the required K-isomorphism. ■

Proposition 20.11

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) $(M\otimes_K N\downarrow_H^G)\uparrow_H^G \cong M\uparrow_H^G \otimes_K N$; and

(b) $\mathrm{Hom}_K(M, N\downarrow_H^G)\uparrow_H^G \cong \mathrm{Hom}_K(M\uparrow_H^G, N)$.

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

$$(M\otimes_K N\downarrow_H^G)\uparrow_H^G = KG\otimes_{KH}(M\otimes_K N\downarrow_H^G) \cong (KG\otimes_{KH} M)\otimes_K N = M\uparrow_H^G\otimes_K N$$

(b) Exercise! ■

Exercise 20.12

Let $L \leqslant H \leqslant G$. Prove that:

(a) (transitivity of induction) if M is a KL-module, then $M\uparrow_L^G = (M\uparrow_L^H)\uparrow_H^G$;

(b) if M is a KH-module, then $(M^*)\uparrow_H^G \cong (M\uparrow_H^G)^*$; and

(c) if M is a KG-module, then $(M^*)\downarrow_H^G \cong (M\downarrow_H^G)^*$.

Exercise 20.13

Let K be a field.

(a) Let U, V, W be KG-modules. Prove that there isomorphisms of KG-modules:

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

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

(b) Prove Proposition 20.11(b) using Proposition 20.11(a).

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 **finitely generated** and **free as K-modules**, hence **of finite K-rank**.

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.

21 Double cosets

Definition 21.1 (*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 21.2

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 21.3

(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

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

22 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 22.1

We need to examine KG as a (KH, KL)-bimodule, 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 ${}^{g}M$ for $g\otimes M$, which is a left $K({}^{g}L)$-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

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

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

Theorem 22.2 (*Mackey formula*)

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

$$M\uparrow_L^G\downarrow_H^G \cong \bigoplus_{g\in[H\backslash G/L]} ({}^{g}M\downarrow^{{}^{g}L}_{H\cap {}^{g}L})\uparrow^H_{H\cap {}^{g}L}$$

as KH-modules.

Proof: It follows from Remark 22.1 that as left KH-modules we have

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

■

Exercise 22.3

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) $M\uparrow_L^G \otimes_K N\uparrow_H^G \cong \bigoplus_{g\in[H\backslash G/L]}({}^{g}M\downarrow^{{}^{g}L}_{H\cap {}^{g}L} \otimes_K N\downarrow^H_{H\cap {}^{g}L})\uparrow^G_{H\cap {}^{g}L}$;

(b) $\mathrm{Hom}_K(M\uparrow_L^G, N\uparrow_H^G) \cong \bigoplus_{g\in[H\backslash G/L]}(\mathrm{Hom}_K({}^{g}M\downarrow^{{}^{g}L}_{H\cap {}^{g}L}, N\downarrow^H_{H\cap {}^{g}L}))\uparrow^G_{H\cap {}^{g}L}$.

23 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 23.1 (*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

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

Moroever, gV is also simple, since if W were a non-trivial proper KU-submodule of gV then $g^{-1}W$ would also be a 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 23.2

The kU-submodules gV which appear in the proof of Theorem 23.1 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 22.1) and gV is prescribed in the same way.

Theorem 23.3 (*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 23.1. 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 12.1. Now, if $g \in G$ then $g(S_i^{a_i}) = (gS_i)^{a_i}$, where gS_i is simple (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 $g(S_i^{a_i}) \subseteq g(S_j^{a_j})$. 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

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

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 23.4

Assume $K = \overline{K}$ is algebraically closed of arbitrary characteristic and G is a p-group for some prime number p. 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 all simple modules are 1-dimensional, so we are done. So assume $|G|$ is reducible, 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 $K[H/U]$-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 $X := \mathrm{Inf}_H^{H/U}(Y)$ 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 submodule W, then $W\uparrow_{H_1}^G$ would be a proper submodule of S, which is simple. 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

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

is simple, 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. ■

Chapter 6. Projective Modules for the Group Algebra (Part I)

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 is a field. All modules over group algebras considered are assumed to be **finitely generated**, hence **of finite K-dimension**. We recall that then $KG/J(KG)$ is semisimple.

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.

24 Radical, socle, head

Definition 24.1

Let M be a KG-module.

(a) The **radical** of M is its submodule

$$\mathrm{rad}(M) := \bigcap_{\substack{V \subset M, \\ V \text{ maximal} \\ KG\text{-submodule}}} V\,.$$

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

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

Lemma 24.2

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

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

(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

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

is a KG-homomorphism with kernel $\ker(\varphi) = V_1 \cap \cdots \cap V_r$. Hence $M/(V_1 \cap \cdots \cap V_r) \cong \mathrm{Im}(\varphi)$ is semisimple, since it is a submodule of a semisimple module. Therefore $M/\mathrm{rad}(M)$ 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 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 $X \supseteq \mathrm{rad}(M)$, 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 11.5 and Proposition 11.7), $M/J(KG)M$ 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 $\mathrm{rad}(M)$ is the largest KG-submodule of M with semisimple quotient, we must have that $\mathrm{rad}(M) \subseteq J(KG)M$.

"(2)⊆(1)": As $M/J(KG)M$ is semisimple, certainly $J(KG)\,(M/J(KG)M) = 0$, because $J(KG)$ annihilates all simple KG-module by definition. Hence $J(KG)M \subseteq \mathrm{rad}(M)$. ■

Example 13

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

Exercise 24.3

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

25 Projective modules

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

Proposition-Definition 25.1 (*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 morphisms

$$\begin{tikzcd} & P \arrow[d, "\alpha"] \\ M \arrow[r, "\psi"'] & N \end{tikzcd}$$

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-linear map, then π splits, i.e., there exists $\sigma \in \mathrm{Hom}_R(P, M)$ 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**. Moroever, a projective indecomposble module is called a **PIM**.

Proof: See Commutative Algebra. ∎

Example 14

(a) Any free module is projective.

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

(c) A direct sum of modules $\{P_i\}_{i \in I}$ is projective if and only if each P_i is projective.

(c) 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.

26 Projective modules for the group algebra

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.

Theorem 26.1

(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

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

Proof:

(a) By Lemma 24.2, $P/\operatorname{rad}(P)$ is semisimple, hence it suffices to prove that it is indecomposable, or equivalently, by Proposition 10.4 that $\operatorname{End}_{KG}(P/\operatorname{rad}(P))$ is a local ring.
Now, if $\varphi \in \operatorname{End}_{KG}(P)$, then by Lemma 24.2, 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:

$$\begin{tikzcd} P \arrow[r, "\varphi"] \arrow[d, "\pi_P"'] \arrow[dr, phantom, "\circlearrowleft"] & P \arrow[d, "\pi_P"] \\ P/\operatorname{rad}(P) \arrow[r, dashed, "\overline{\varphi}"'] & P/\operatorname{rad}(P) \end{tikzcd}$$

Then, the map

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

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 statisfies 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 belocal.

(b) Consider the diagram

$$\begin{tikzcd} & & P \arrow[d, "\pi_P"] \\ M \arrow[r, "\pi_M"'] & M/\operatorname{rad}(M) \arrow[r, "\cong", "\psi"'] & P/\operatorname{rad}(P) \end{tikzcd}$$

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 $\operatorname{rad}(P) \subseteq \ker(\psi|_P)$ since it is the smallest KG-submodule with semisimple quotient by Lemma 24.2. Then the universal property of the quotient yields a surjective homomorphism $P/\operatorname{rad}(P) \longrightarrow S$ induced by $\psi|_P$. Finally, as $P/\operatorname{rad}(P)$ is simple, $P/\operatorname{rad}(P) \cong S$ by Schur's Lemma. ■

Corollary 26.2

Assume $K = \overline{K}$. Then, in the decomposition of the regular module KG° into a direct sum of indecomposable KG-submodule, each isomorphism type of projective indecomposable KG-module occurs with multiplicity $\dim_K(P/\operatorname{rad}(P))$.

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

$$J(KG) = J(KG)KG^\circ = J(KG)P_1 \oplus \cdots \oplus J(KG)P_r = \operatorname{rad}(P_1) \oplus \cdots \oplus \operatorname{rad}(P_r)$$

by Lemma 24.2. Therefore,

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

where each summand is simple by Theorem 26.1(a). Now as $KG/J(KG)$ is semisimple, by Theorem 13.2, 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 26.1(c). ■

Lemma 26.3

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

Proof: We have already seen that $KG{\downarrow}_H^G \cong KH \oplus \cdots \oplus KH$, where KH occurs with multiplicity $|G : H|$. Hence the restriction from G to H of a free module is again free. Now, by definition $P \mid F$ for some free KG-module F, so that $P{\downarrow}_H^G \mid F{\downarrow}_H^G$ and the claim follows. ■

Corollary 26.4

Let $K = \overline{K}$ be an algebraically closed field of characteristic $p > 0$ and let P be a projective KG-module. If a Sylow p-subgroup Q of G has order p^a with $a \in \mathbb{Z}_{>0}$, then $p^a \mid \dim_K(P)$.

Proof: By Lemma 26.3, $P{\downarrow}_Q^G$ is projective. Moreover, by Corollary 17.3 the trivial KQ-module is the unique simple KQ-module, hence KQ has a unique PIM, namely KQ° itself, which has dimension $|Q| = p^a$. Hence $P{\downarrow}_Q^G$ is a direct sum of copies of KQ° and the claim follows. ■

Exercise 26.5

Prove that:

(a) If P is a projective KG-module, then so is P^*.

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

(c) If P is a projective KG-module and M is an arbitrary KG-module, then $P \otimes_K M$ is projective.

(d) If P is a projective indecomposable KG-module, then $\mathrm{soc}(P)$ is simple. (Hint: consider duals.)

Exercise 26.6

Let S be a simple KG-module and let P_S denote the corresponding PIM (i.e. $P_S/\operatorname{rad}(P_S) \cong S$). Let M be an arbitrary KG-module. Prove that:

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

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

(b) The multiplicity of S as a composition factor of M is

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

Part II

Weeks 8-14
written by N. Farrell

Chapter 7. The Green Correspondence

The goal of this chapter is to prove Green's correspondence. First we will generalise the idea of projective modules seen in Chapter 6 by defining what is called **relative projectivity**. In the second section we will define **vertices** and **sources** of indecomposable modules. Finally, in the third section we will state and prove **Green's correspondence**.

Notation: throughout this chapter, unless otherwise specified, we let G denote a finite group and let K denote a field of characteristic p. All modules over group algebras considered are assumed to be **finitely generated**, hence **of finite K-dimension**.

References:

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

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

27 Relative Projectivity

Relative projectivity is a refinement of the idea of projectivity seen in Chapter 6. A projective module is a summand of a free module. For $H \leqslant G$, we will first define H-free modules. Then a module is relatively H-projective if it is a summand of an H-free module. Relative projectivity enables us to explore the relationship between representations of a group and representations of its subgroups. This is a very important tool for modular representation theory.

Definition 27.1

Let $H \leqslant G$. A KG-module is **H-free** if it is of the form $V{\uparrow}_H^G$ for some KH-module V. A KG-module is **relatively H-projective**, or **H-projective**, if it is isomorphic to a direct summand of an H-free module – that is, if it is isomorphic to a direct summand of a module of the form $V{\uparrow}_H^G$ for some KH-module V.

Remark 27.2

- Free $\iff$ $\{1\}$-free: a free KG-module is of the form $(KG^\circ)^n$ for some $n \in \mathbb{N}$. But $KG^\circ \cong$

$K\uparrow_{\{1\}}^G$ (see Example 11) so $(KG^\circ)^n \cong (K^n)\uparrow_{\{1\}}^G$. Hence being free and $\{1\}$-free is the same. Therefore H-freeness is a generalisation of freeness.

- Projective $\iff$ $\{1\}$-projective: A KG-module is projective $\Leftrightarrow$ it is a summand of a free module $\Leftrightarrow$ it is a summand of a $\{1\}$-free module $\Leftrightarrow$ it is relatively $\{1\}$-projective. Therefore relative projectivity is a generalisation of projectivity.

Exercise 27.3 (*Relative freeness*)

Let $H \leqslant G$. Suppose that V is a relatively H-free KG-module with respect to a KH-submodule X, and suppose that W is a relatively H-free KG-module with respect to a KH-submodule Y. Prove that if $X \cong Y$ as KH-modules, then $V \cong W$ as KG-modules.

Exercise 27.4 (*Relative projectivity*)

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 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.

Notation 27.5 (*Induction and restriction of homomorphisms*)

Let $H \leqslant G$. Let $\varphi : U_1 \to U_2$ be a KH-homomorphism. Then the induced KG-homomorhpism

$$\begin{aligned} \mathrm{Id}_{KG} \otimes \varphi : U_1\uparrow_H^G &\to U_2\uparrow_H^G \\ g \otimes u &\mapsto g \otimes \varphi(u). \end{aligned}$$

is denoted by $\varphi\uparrow_H^G$.

On the other hand, since a KG-homomorhpism $\psi : V_1 \to V_2$ is also a KH-homomorhpism $V_1\downarrow_H^G \to V_2\downarrow_H^G$, we just denote the KH-homomorphism by ψ again, without any arrows.

The following notation will be needed in the proof of the next proposition about characterisations of relative projectivity.

Notation 27.6 (*The μ and ϵ maps*)

Let $H \leqslant G$. Let U be a KH-module and recall that $U\uparrow_H^G = \bigoplus_{g\in[G/H]} g \otimes U$ (see Remark 20.7), and restricting back to H gives a KH-module $U\uparrow_H^G\downarrow_H^G = \bigoplus_{g\in[G/H]} g \otimes U$. We denote the inclusion map from U onto the summand with $g = 1$ by μ:

$$\begin{aligned} \mu : U &\to U\uparrow_H^G\downarrow_H^G \\ u &\mapsto 1 \otimes u. \end{aligned}$$

Let V be a KG-module. Then $V\downarrow_H^G\uparrow_H^G = \bigoplus_{g\in[G/H]} g\otimes(V\downarrow_H^G)$ and we define a KG-module homorphism ϵ as follows.

$$\begin{aligned} \epsilon : V\downarrow_H^G\uparrow_H^G &\to V \\ g \otimes v &\mapsto gv \end{aligned}$$

for $g \in G$ and $v \in V\downarrow_H^G$. Note that for any $u \in U$, $\epsilon \circ \mu(u) = \epsilon(1 \otimes u) = u$, so μ is a KH-section for ϵ.

Now consider the following maps:

$$\begin{aligned} \Phi : \mathrm{Hom}_{KG}(U\uparrow_H^G, V) &\to \mathrm{Hom}_{KH}(U, V\downarrow_H^G) \\ \psi &\mapsto \psi \circ \mu \\ \Psi : \mathrm{Hom}_{KH}(U, V\downarrow_H^G) &\to \mathrm{Hom}_{KG}(U\uparrow_H^G, V) \\ \beta &\mapsto \epsilon \circ \beta\uparrow_H^G \end{aligned}$$

It is possible to show that these are mutually inverse, so $\Psi(\Phi(\psi)) = \psi$ for all $\psi \in \mathrm{Hom}(U\uparrow_H^G, V)$, $\Phi(\Psi(\beta)) = \beta$ for all $\beta \in \mathrm{Hom}_{KH}(U, V\downarrow_H^G)$ and

$$\mathrm{Hom}_{KG}(U\uparrow_H^G, V) \cong \mathrm{Hom}_{KH}(U, V\downarrow_H^G).$$

Moreover, these isomorphisms are *natural* in U and V which means in particular that for any KH-homomorphism $\gamma : U_1 \to U_2$, the following diagram commutes,

$$\begin{tikzcd} \mathrm{Hom}_{KG}(U_1\uparrow_H^G, V) \arrow[r, "\Phi"] & \mathrm{Hom}_{KH}(U_1, V\downarrow_H^G) \\ \mathrm{Hom}_{KG}(U_2\uparrow_H^G, V) \arrow[r, "\Phi"'] \arrow[u, "\_ \circ \gamma\uparrow_H^G"] & \mathrm{Hom}_{KH}(U_2, V\downarrow_H^G) \arrow[u, "\_ \circ \gamma"'] \end{tikzcd}$$

and for any KG-homomorphism $\alpha : V_1 \to V_2$, the following diagram commutes.

$$\begin{tikzcd} \mathrm{Hom}_{KH}(U, V_1\downarrow_H^G) \arrow[r, "\Psi"] \arrow[d, "\alpha \circ \_"'] & \mathrm{Hom}_{KG}(U\uparrow_H^G, V_1) \arrow[d, "\alpha \circ \_"] \\ \mathrm{Hom}_{KH}(U, V_2\downarrow_H^G) \arrow[r, "\Psi"'] & \mathrm{Hom}_{KG}(U\uparrow_H^G, V_2) \end{tikzcd}$$

Proposition 27.7 (*Characteristics 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 $\psi : U \to W$ is a KG-homomorphism, $\varphi : V \twoheadrightarrow W$ is a surjective KG-homomorphism and there exists a KH-homomorphism $\alpha_H : U\downarrow_H^G \to V\downarrow_H^G$ such that $\varphi \circ \alpha_H = \psi$ on $U\downarrow_H^G$, then there exists a KG-homomorphism $\alpha_G : U \to V$ such that $\varphi \circ \alpha_G = \psi$ so that the diagram on the right commutes.

$$\begin{tikzcd} & U \arrow[dl, "\alpha_G"'] \arrow[d, "\psi"] \\ V \arrow[r, two heads, "\varphi"'] & W \end{tikzcd}$$

(c) Whenever $\varphi : V \to U$ is a surjective KG-homomorphism such that the restriction $\varphi : V\downarrow_H^G \to U\downarrow_H^G$ is a split surjective KH-homomorphism, then φ is a split surjective KG-homomorhpism.

(d) The following surjective KG-homomorphism is split.

$$\begin{aligned} U{\downarrow}^G_H{\uparrow}^G_H = KG \otimes_{KH} U &\to U \\ x \otimes u &\mapsto xu \end{aligned}$$

(e) The KG-module U is a direct summand of $U{\downarrow}^G_H{\uparrow}^G_H$.

Proof:

(a)⇒(b): First we consider the case where $U = T{\uparrow}^G_H$ is an induced module. Suppose that we have KG-homomorphisms $\psi : T{\uparrow}^G_H \to W$ and $\varphi : V \twoheadrightarrow W$ as shown in the the diagram on the left. Suppose that there exists a KH-homomorhpism $\alpha_H : T{\uparrow}^G_H{\downarrow}^G_H \to V{\downarrow}^G_H$ such that $\psi = \varphi \circ \alpha_H$ on $T{\uparrow}^G_H{\downarrow}^G_H$, that is, the diagram on the right commutes.

$$\begin{tikzcd} & T{\uparrow}^G_H \arrow[d, "\psi"] \\ V \arrow[r, two heads, "\varphi"'] & W \end{tikzcd} \qquad\qquad \begin{tikzcd} & T{\uparrow}^G_H{\downarrow}^G_H \arrow[dl, "\alpha_H"'] \arrow[d, "\psi"] \\ V{\downarrow}^G_H \arrow[r, two heads, "\varphi"'] & W{\downarrow}^G_H \end{tikzcd}$$

Let $\mu : T \to T{\uparrow}^G_H{\downarrow}^G_H$ and $\epsilon : T{\downarrow}^G_H{\uparrow}^G_H \to T$ be as defined in Notation 27.6, so μ is an injective KH-homomorphism and ϵ is a surjective KG-homomorphism. Then the following triangle of KH-modules and KH-homomorphisms commutes.

$$\begin{tikzcd} & T \arrow[dl, "\alpha_H \circ \mu"'] \arrow[d, "\psi \circ \mu"] \\ V{\downarrow}^G_H \arrow[r, two heads, "\varphi"'] & W{\downarrow}^G_H \end{tikzcd}$$

By the naturality of Φ and Ψ from Notation 27.6, since $\varphi : V \to W$ is a KG-homomorphism, we have the following commutative diagram.

$$\begin{tikzcd} \mathrm{Hom}_{KH}(T, V{\downarrow}^G_H) \arrow[r, "\Psi"] \arrow[d, "\varphi \circ \_"'] & \mathrm{Hom}_{KG}(T{\uparrow}^G_H, V) \arrow[d, "\varphi \circ \_"] \\ \mathrm{Hom}_{KH}(T, W{\downarrow}^G_H) \arrow[r, "\Psi"'] & \mathrm{Hom}_{KG}(T{\uparrow}^G_H, W) \end{tikzcd}$$

Hence the following two KG-homomorphisms $T{\uparrow}^G_H \to W$ are equal.

$$\Psi(\varphi \circ (\alpha_H \circ \mu)) = \varphi \circ (\Psi(\alpha_H \circ \mu))$$

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

$$\psi = \varphi \circ \epsilon \circ ((\alpha_H \circ \mu){\uparrow}^G_H)$$

and so the following triangle of KG-homomorphisms commutes, proving the implication for $U = T{\uparrow}^G_H$ an induced module.

$$\begin{tikzcd} & T{\uparrow}_H^G \arrow[dl, "\epsilon \circ ((\alpha_H \circ \mu){\uparrow}_H^G)"'] \arrow[d, "\psi"] \\ V \arrow[r, two heads, "\varphi"'] & W \end{tikzcd}$$

Now let U be any summand of $T{\uparrow}_H^G$. Let $U \xrightarrow{\iota} T{\uparrow}_H^G \xrightarrow{\pi} U$ denote the inclusion and projection maps. Suppose that there is a KH-homomorphism $\alpha_H : U{\downarrow}_H^G \to V{\downarrow}_H^G$ such that $\varphi \circ \alpha_H = \psi$ on $U{\downarrow}_H^G$.

$$\begin{tikzcd} & U{\downarrow}_H^G \arrow[dl, "\alpha_H"'] \arrow[d, "\psi"] \\ V{\downarrow}_H^G \arrow[r, two heads, "\varphi"'] & W{\downarrow}_H^G \end{tikzcd}$$

Then we have the following diagrams.

$$\begin{tikzcd} & T{\uparrow}_H^G \arrow[d, "\psi \circ \pi"] \\ V \arrow[r, two heads, "\varphi"'] & W \end{tikzcd} \qquad \begin{tikzcd} & T{\uparrow}_H^G{\downarrow}_H^G \arrow[dl, "\alpha_H \circ \pi"'] \arrow[d, "\psi \circ \pi"] \\ V{\downarrow}_H^G \arrow[r, two heads, "\varphi"'] & W{\downarrow}_H^G \end{tikzcd} \qquad \begin{tikzcd} & T{\uparrow}_H^G \arrow[dl, "\alpha_G"'] \arrow[d, "\psi \circ \pi"] \\ V \arrow[r, two heads, "\varphi"'] & W \end{tikzcd}$$

The first is a diagram of KG-homomorphisms. The middle diagram of KH-homomorphisms commutes by definition of α_H, and hence by the first part there is a KG-homomorphism $\alpha_G : T{\uparrow}_H^G \to V$ 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 $\alpha_G \circ \iota : U \to V$ is a KG-module homomorphism such that $\varphi \circ (\alpha_G \circ \iota) = \psi$ and the following triangle commutes, as required.

$$\begin{tikzcd} & U \arrow[dl, "\alpha_G \circ \iota"'] \arrow[d, "\psi"] \\ V \arrow[r, two heads, "\varphi"'] & W \end{tikzcd}$$

(b)⇒(c): Let $\varphi : V \to U$ be a surjective KG-homomorphism which is split as a KH-homomorphism. Suppose that α_H is a KH-section for φ, so we have the following commutative diagram of KH-modules.

$$\begin{tikzcd} & U{\downarrow}_H^G \arrow[dl, "\alpha_H"'] \arrow[d, "\mathrm{Id}_U"] \\ V{\downarrow}_H^G \arrow[r, two heads, "\varphi"'] & U{\downarrow}_H^G \end{tikzcd}$$

Then assuming (b) is true, there exists a KG-homomorphism $\alpha_G : U \to V$ such that $\varphi \circ \alpha_G = \mathrm{Id}_U$. In particular, α_G is a KG-section for φ, so $\varphi : V \to U$ is a split surjective KG-homomorphism.

(c)⇒(d): As mentioned in Notation 27.6, μ is a KH-section for ϵ, so $\epsilon : U{\downarrow}_H^G{\uparrow}_H^G \to U$ is split as a KH-homomorphism. Hence by part (c), $\epsilon : U{\downarrow}_H^G{\uparrow}_H^G \to U$ is split as a KG-homomorhpism, showing part (d).

(d)⇒(e): immediate

(e)⇒(a): immediate ■

Exercise 27.8 (*Relative projectivity*)

Let $H \leqslant G$. Let U be a KG-module. Prove that if U is H-projective and W is a KG-module, then $U \otimes_K W$ is H-projective.

In the next theorem we see a situation where we can always find relatively projective modules.

Theorem 27.9

Let $H \leqslant G$ such that H contains a Sylow p-subgroup of G. Then every KG-module is H-projective.

Before proving this theorem, let us consider its application to the case when $H = 1$.

Example 15

Let $H = 1$. If H contains a Sylow p-subgroup of G then the Sylow p-subgroups of G are trivial, so p does not divide the order of G. The theorem then shows that all KG-modules are $\{1\}$-projective and hence projective. We know this already, however! If p does not divide the order of G then KG is semisimple (Maschke's Theorem 16.1), and so all KG-modules are projective by Example 14 (c).

Proof: Let V be a KG-module and let $H \leqslant G$ such that H contains a Sylow p-subgroup of G. Let $\varphi : U \twoheadrightarrow V$ be a surjective KG-homomorphism which splits as a KH-homomorhpism. We will show that φ splits as a KG-homomorphism, and hence V satisfies Theorem 27.7 (c) so V is H-projective.

Then $U \cong W \oplus V$ as KH-modules, where $W := \ker(\varphi)$. Let $f : U \to W$ be a projection map onto the first factor. Note that since H contains a Sylow p-subgroup of G, $|\, G : H \,|$ is coprime to p. Thus $|\, G : H \,|$ is invertible in K because K is of characteristic p. We can therefore define a map $\tilde{f} : U \to W$ as follows:

$$\tilde{f}(u) := \frac{1}{|\, G : H \,|} \sum_{g \in [G/H]} g^{-1} f(gu) \qquad \text{for } u \in U,$$

where the sum runs over a set of left coset representatives of H in G. Since $gu \in U$ (U is a KG-module), and $f(gu) \in W$ by definition of f, $\tilde{f}(u) \in W$ so the map is well defined. Also, for any $g' \in G$,

$$\begin{aligned}
\tilde{f}(g'u) &= \frac{1}{|\, G : H \,|} \sum_{g \in [G/H]} g^{-1} f(gg'u) \\
&= \frac{1}{|\, G : H \,|} \sum_{g \in [G/H]} g'(gg')^{-1} f(gg'u) \\
&= \frac{1}{|\, G : H \,|} \sum_{g'' \in [G/H]} g'(g'')^{-1} f(g''u) \\
&= g' \frac{1}{|\, G : H \,|} \sum_{g'' \in [G/H]} g''^{-1} f(g''u) \\
&= g' \tilde{f}(u).
\end{aligned}$$

Thus, $\tilde{f} : U \to W$ is in fact a KG-homomorphism.

Now, for any $w \in W$ we have

$$\tilde{f}(w) = \frac{1}{|\, G : H \,|} \sum_{g \in [G/H]} g^{-1} f(gw) = \frac{1}{|\, G : H \,|} \sum_{g \in [G/H]} g^{-1} gw = \frac{1}{|\, G : H \,|} \sum_{g \in [G/H]} w = w,$$

which shows that $\ker(\tilde{f}) \cap W = \{0\}$ and $\tilde{f}^2 = \tilde{f}$.

Finally, for any $u \in U$ we have $u = (u - \tilde{f}(u)) + \tilde{f}(u)$, so

$$\tilde{f}(u) = \tilde{f}(u - \tilde{f}(u)) + \tilde{f}^2(u) = \tilde{f}(u - \tilde{f}(u)) + \tilde{f}(u).$$

In particular, $\tilde{f}(u - \tilde{f}(u)) = 0$ and $u - \tilde{f}(u) \in \ker(\tilde{f})$. Hence every element of U can be expressed as the sum of an element in $\ker(\tilde{f})$ and an element of W, so $U \cong W \oplus \ker \tilde{f}$ as KG-modules. Hence φ splits as a KG-homomorphism, so V is H-projective by Theorem 27.7. ■

Corollary 27.10

Suppose that a subgroup H of G contains a Sylow p-subgroup of G. Then a KG-module U is projective if and only if $U\downarrow^G_H$ is projective.

Proof:

$\Rightarrow$: Lemma 26.3.

$\Leftarrow$: Suppose that $U\downarrow^G_H$ is projective and H contains a Sylow p-subgroup of G. Then $U\downarrow^G_H$ is a summand of a free module $(KH^\circ)^n$, and every KG-module is H-projective. In particular, U is H-projective so U is a summand of $U\downarrow^G_H\uparrow^G_H$ by Theorem 27.7. Hence U is a summand of $U\downarrow^G_H\uparrow^G_H$ which is a summand of $(KH^\circ)^n\uparrow^G_H = (KG^\circ)^n$, so U is projective. ■

28 Vertices and Sources

Theorem 28.1

Let U be an indecomposable KG-module.

(a) There is a unique conjugacy class of subgroups Q of G that 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. There is an indecomposable KQ-module T that is unique up to conjugacy by elements of $N_G(Q)$ such that U is a direct summand of $T\uparrow^G_Q$. Such a T is necessarily a direct summand of $U\downarrow^G_Q$.

Proof:

(a) Suppose that U is both H- and K-projective for subgroups H and K of G. Then U is a direct summand of $U\downarrow^G_H\uparrow^G_H$ and $U\downarrow^G_K\uparrow^G_K$ by Proposition 27.7 (e). Hence U is also a direct summand of $U\downarrow^G_H\uparrow^G_H\downarrow^G_K\uparrow^G_K$. By the Mackey formula and transitivity of induction and restriction, it follows that

$$\begin{aligned} U\downarrow^G_H\uparrow^G_H\downarrow^G_K\uparrow^G_K &= ((U\downarrow^G_H)\uparrow^G_H\downarrow^G_K)\uparrow^G_K \\ &= \left(\bigoplus_{g\in[K\backslash G/H]} \left({}^g(U\downarrow^G_H)\downarrow^{{}^gH}_{K\cap {}^gH}\right)\uparrow^K_{K\cap {}^gH}\right)\uparrow^G_K \\ &= \bigoplus_{g\in[K\backslash G/H]} \left({}^gU\downarrow^G_{K\cap {}^gH}\right)\uparrow^G_{K\cap {}^gH}\,. \end{aligned}$$

Therefore U is a direct summand of some module induced from $K \cap {}^gH$ for some $g \in G$. In other words, U is relatively $K \cap {}^gH$-projective. Suppose that both K and H are minimal such that U is projective with respect to these groups. Then $K \cap {}^gH = K$ so $K \subseteq {}^gH$ 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 is a direct summand of $U{\downarrow}^G_Q{\uparrow}^G_Q$ so it is a direct summand of $T{\uparrow}^G_Q$ for some indecomposable direct summand T of $U{\downarrow}^G_Q$. If T' is another indecomposable KQ-module such that U is a direct summand of $T'{\uparrow}^G_Q$, then T is a direct summand of $T'{\uparrow}^G_Q{\downarrow}^G_Q$. Mackey's formula says that

$$T'{\uparrow}^G_Q{\downarrow}^G_Q = \bigoplus_{g\in[Q\backslash G/Q]} ({}^gT'{\downarrow}^{{}^gQ}_{Q\cap {}^gQ}){\uparrow}^Q_{Q\cap {}^gQ}\,.$$

Hence T is a direct summand of $({}^gT'{\downarrow}^{{}^gQ}_{Q\cap {}^gQ}){\uparrow}^Q_{Q\cap {}^gQ}$, and therefore U is relatively $Q\cap {}^gQ$-projective, for some $g\in G$. 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 $U{\downarrow}^G_Q$ by definition, so $T' = {}^{g^{-1}}T$ is a direct summand of $({}^{g^{-1}}U){\downarrow}^G_Q$. However, $U \cong {}^{g^{-1}}U$ as KG-modules, so this means that T' is also a direct summand of $U{\downarrow}^G_Q$. ■

Definition 28.2

Let U be an indecomposable kG-module. A **vertex** of U is a minimal subgroup Q of G such that U is relatively Q-projective. The vertices of U are unique up to G-conjugacy.
A **KQ-source**, or simply **source** of U is a KQ-module T for which U is a direct summand of $T{\uparrow}^G_Q$, for some vertex Q of U. For a fixed vertex Q, the sources of U are unique up to $N_G(Q)$-conjugacy.

Exercise 28.3

Let $H\leqslant G$ and $J\leqslant G$. Let U be a KG-module. If U is H-projective and W is an indecomposable direct summand of $U{\downarrow}^G_J$ then W is $J\cap {}^gH$-projective for some element $g\in G$, and there is a vertex of W that is contained in this subgroup $J\cap {}^gH$.

The idea is that the closer the vertex of a module is to the trivial group, the closer the module is to being projective: a KG-module U with trivial vertex is $\{1\}$-projective and hence projective.

Proposition 28.4

(a) The vertices of an indecomposable KG-module are p-groups.

(b) If P is a p-group and H is a subgroup of P then $K{\uparrow}^P_H$ is an indecomposable KP-module.

(c) The vertices of the trivial KG-module K are Sylow p-subgroups of G.

Proof:

(a) By Theorem 27.9, we know that every KG-module is projective relative to a Sylow p-subgroup of G. Therefore vertices are contained in Sylow p-subgroups, and hence are themselves p-groups.

(b) Because P is a p-group, the only simple KP-module is the trivial module K (see Cor. 17.3). Moreover,

$$\begin{aligned}\dim \operatorname{soc}(K{\uparrow}^P_H) &= \dim \operatorname{Hom}_{KP}(K, K{\uparrow}^P_H)\\ &= \dim \operatorname{Hom}_{KH}(K{\downarrow}^H_P, K)\end{aligned}$$

by Frobenius reciprocity (Theorem 20.10 (b)). But $\operatorname{Hom}_{KH}(K{\downarrow}^P_H, K) \cong K$ so this, and hence $\operatorname{soc}(K{\uparrow}^P_H)$, has dimension 1. If $K{\downarrow}^H_P$ is decomposable then $K{\downarrow}^H_P = U\oplus V$ for some KP-modules

U and V, and hence $\operatorname{soc}(K{\downarrow}_P^H) = \operatorname{soc}(U) \oplus \operatorname{soc}(V)$. This contradicts the fact that $\operatorname{soc}(K{\uparrow}_H^P)$ has dimension 1, therefore $K{\uparrow}_H^P$ is indecomposable.

(c) Let Q be a vertex of K and let P be a Sylow p-subgroup of G which contains Q. Then $K \mid K{\uparrow}_Q^G$, so $K{\downarrow}_P^G$ is a summand of $K{\uparrow}_Q^G{\downarrow}_P^G = \bigoplus_{g\in[P\backslash G/Q]} K{\uparrow}_{P\cap {}^gQ}^P$ and hence is a summand of $K{\uparrow}_{P\cap {}^gQ}^P$ for some $g \in G$. By part (b), since P is a p-group, $K{\uparrow}_{P\cap {}^gQ}^P$ is indecomposable. Thus $K{\downarrow}_P^G = K{\uparrow}_{P\cap {}^gQ}^P$ and hence $P \cap {}^gQ = P$, so Q is a Sylow p-subgroup of G. ■

29 The Green Correspondence

The Green correspondence is used to reduce questions about indecomposable modules to a situation where the vertex of the module is a normal subgroup. This technique is very useful in many situations, particularly in block theory. Many properties in modular representation theory are believed to be determined by normalisers of p-subgroups.

We will need the following easy properties of vertices and sources in the proof of Green's correspondence.

Exercise 29.1

Prove the following Lemma.

Lemma 29.2

Let Q be a p-subgroup of G and let L be a subgroup of G containing $N_G(Q)$.

(a) Suppose that V is an indecomposable KL-module with vertex Q and let U be a direct summand of $V{\uparrow}_L^G$ such that V is a direct summand of $U{\downarrow}_L^G$. Then Q is also a vertex of U.

(b) Suppose that 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 V also has vertex Q.

Exercise 29.3

Let U be an indecomposable KG-module with vertex Q and let L be a subgroup of G containing Q. Prove that there exists an indecomposable direct summand of $U{\downarrow}_L^G$ with vertex Q.

Theorem 29.4 (*Green Correspondence*)

Let Q be a p-subgroup of G and let L be a subgroup of G containing $N_G(Q)$.

(a) Let U be an indecomposable KG-module with vertex Q. Then in any decomposition of $U{\downarrow}_L^G$ into a direct sum of indecomposable modules, there is a unique indecomposable direct summand with vertex Q which we denote by $f(U)$. Writing $U{\downarrow}_L^G = f(U) \oplus X$, then every direct summand of X is projective relative to a subgroup of the form $L \cap {}^xQ$ for some $x \in G\backslash L$.

(b) Let V be an indecomposable KL-module with vertex Q. Then in any decomposition of $V{\uparrow}_L^G$ into a direct sum of indecomposable modules, there is a unique indecomposable direct summand with vertex Q which we denote by $g(V)$. Writing $V{\uparrow}_L^G = g(V) \oplus Y$, then every direct summand of Y is projective relative to a subgroup of the form $Q \cap {}^xQ$ for some $x \in G\backslash L$.

(c) With this notation, we then have $g(f(U)) \cong U$ and $f(g(V)) \cong V$.

Proof: We first note some properties of the groups $Q \cap {}^xQ$ and $L \cap {}^xQ$ for $x \in G \backslash L$.

- Since $N_G(Q) \leqslant L$, x does not normalize Q and hence $Q \cap {}^xQ$ is a proper subgroup of Q.
- $L \cap {}^xQ$ may be the same size of Q, in which case it is equal to ${}^xQ$.
- Suppose that $L \cap {}^xQ$ is conjugate to Q in L: $L \cap {}^xQ = {}^zQ$ for some $z \in L$. 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 not conjugate to Q in L.

Let V be an indecomposable KL-module with vertex Q.

Claim: Any decomposition of $V\uparrow_L^G\downarrow_L^G$ into a direct sum of indecomposable KL-modules 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 $x \notin L$.

Pf of claim Let T be a KQ-source for V and write $T\uparrow_Q^L = V \oplus Z$ for some KL-module Z. Let V' and Z' denote KL-modules 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

$$\begin{aligned} T\uparrow_Q^G\downarrow_L^G &\cong (V \oplus Z)\uparrow_L^G\downarrow_L^G \\ &= V\uparrow_L^G\downarrow_L^G \oplus Z\uparrow_L^G\downarrow_L^G \\ &= V \oplus V' \oplus Z \oplus Z'. \end{aligned}$$

On the other hand, by Mackey we also have

$$\begin{aligned} T\uparrow_Q^G\downarrow_L^G &= \bigoplus_{x \in [L\backslash G/Q]} ({}^xT\downarrow^{{}^xQ}_{L\cap {}^xQ})\uparrow^L_{L\cap {}^xQ} \\ &\cong T\uparrow_Q^L \oplus \left(\bigoplus_{x \in [L\backslash G/Q],\ x\notin L} ({}^xT\downarrow^{{}^xQ}_{L\cap {}^xQ})\uparrow^L_{L\cap {}^xQ} \right) \\ &= V \oplus Z \oplus \left(\bigoplus_{x \in [L\backslash G/Q],\ x\notin L} ({}^xT\downarrow^{{}^xQ}_{L\cap {}^xQ})\uparrow^L_{L\cap {}^xQ} \right). \end{aligned}$$

Therefore

$$V \oplus V' \oplus Z \oplus Z' \cong V \oplus Z \oplus \left(\bigoplus_{x \in [L\backslash G/Q],\ x\notin L} ({}^xT\downarrow^{{}^xQ}_{L\cap {}^xQ})\uparrow^L_{L\cap {}^xQ} \right).$$

Clearly all direct summands not in $V \oplus Z$ are projective relative to subgroups of the form $L \cap {}^xQ$ for some $x \notin L$. We already saw that $L \cap {}^xQ$ is not conjugate to Q for any $x \notin L$. Hence V is the unique direct summand of $V\uparrow_L^G\downarrow_L^G = V \oplus V'$ with vertex Q, and all other direct summands in V' are projective relative to subgroups of the form $L \cap {}^xQ$ with $x \notin L$.

Pf of (b) We continue with the notation above, with V an indecomposable KL-module with vertex Q. Write $V\uparrow_L^G$ as a direct sum of indecomposable KG-modules and pick a direct summand U such that $U\downarrow_L^G$ has V as a direct summand. By Lemma 29.2 (a), 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.

Let U' be another 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, $V \oplus V' = U\downarrow_L^G \oplus U'\downarrow_L^G \oplus X\downarrow_L^G$. Therefore $U'\downarrow_L^G$ is a direct summand of V' and hence every indecomposable direct summand of $U'\downarrow_L^G$ is projective relative to a subgroup $L \cap {}^yQ$, for some $y \notin L$. Now since V is a direct summand of $T\uparrow_Q^L$ and U' is a direct summand of $V\uparrow_L^G$, it follows that U' is a direct summand of $T\uparrow_Q^G$ and hence U' is projective relative to Q. Hence U' has a vertex Q' which is a subgroup of Q.

Let S be a KQ'-source of U'. Theorem 28.1 (b) shows that S is a direct summand of $U'\downarrow_{Q'}^G$. 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 Exercise 29.3 that Q' is also a vertex of Y. But the indecomposable direct summands of $U'{\downarrow}_L^G$ are projective relative to subgroups of the form $L \cap {}^yQ$ for some $y \notin L$. Therefore one of the subgroups $L \cap {}^yQ$ with $y \notin L$ contains an L-conjugate of Q' – in other words, ${}^zQ' \subseteq L \cap {}^yQ$ for some $z \in L$. Hence $Q' \subseteq {}^{z^{-1}y}Q$ where $z^{-1}y \notin L$. This shows that $Q' \subseteq Q \cap {}^xQ$ for some $x \notin L$, proving part (b) with $g(V) := U$.

Pf of (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 is a direct summand of $V{\uparrow}_L^G$. This means that V is Q-projective (since it is a direct summand of $T{\uparrow}_Q^L$), and so by Lemma 29.2 (b), Q is a vertex of V.

By Exercise 29.3, there exists an indecomposable direct summand Y of $U{\downarrow}_L^G$ with vertex Q. But $U{\downarrow}_L^G$ is a direct summand of $V{\uparrow}_L^G{\downarrow}_L^G$ and the claim shows that the only direct summand of $V{\uparrow}_L^G{\downarrow}_L^G$ with vertex Q is V. Therefore $Y \cong V$ and in any expression of $U{\downarrow}_L^G$ as a direct sum of indecomposables, one direct summand is isomorphic to V and the rest are projective relative to subgroups of the form $L \cap {}^xQ$ for some $x \notin L$. This proves part (a).

Pf of (c) Finally, part (c) follows from parts (a) and (b) and the fact that U is isomorphic to a direct summand of $U{\downarrow}_L^G{\uparrow}_L^G$ and V is isomorphic to a direct summand of $V{\uparrow}_L^G{\downarrow}_L^G$. ■

Chapter 8. Splitting p-modular systems and Brauer Reciprocity

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

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

References:

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

[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.

30 Lifting Idempotents

Definition 30.1

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

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

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

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

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

Example 16 (*Complete discrete valuation ring*)

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

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

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

Proposition 30.2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We will need the following result for the next corollary.

Exercise 30.3

Lemma 30.4

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

Corollary 30.5

(Continue with the notation from before Exercise 30.3.) Let V be a projective $\overline{A}$-module. Then there exists a projective A-module M such that $V \cong M/J(\mathcal{O})M$.

Proof: By Lemma 30.4 there exist idempotents $f_1, \ldots, f_r \in \overline{A}$ such that $V \cong \overline{A}f_1 \oplus \cdots \oplus \overline{A}f_r$. It then follows from Proposition 30.2 (a) that we can choose idempotents $e_1, \ldots, e_r \in A$ such that e_i is a pre-image of f_i in A for each $1 \leqslant i \leqslant r$. Let $M := Ae_1 \oplus \cdots \oplus Ae_r$. Then M is projective (see Example 14) and $M/J(\mathcal{O})M \cong V$. ■

31 Splitting fields

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

Notation 31.1

Let A be an R-algebra and let U be an A-module. Then $A^S := S \otimes_R A$ is an S-algebra with action of S given by $s.(s' \otimes a) = ss' \otimes a$ for all $s, s' \in S$ and $a \in A$; and $U^S := S \otimes_R U$ is an A^S-module with action of A^S given by $(s_1 \otimes a).(s_2 \otimes u) = s_1 s_2 \otimes a.u$ for all $s_1, s_2 \in S, a \in A, u \in U$.

Definition 31.2

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

Definition 31.3 (*Splitting field for an algebra*)

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

Exercise 31.4 (*Splitting fields for an algebra*)

Lemma 31.5

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

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

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

Definition 31.6 (*Splitting field for a group*)

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

Remark 31.7

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

Example 17

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

32 $\mathcal{O}$-forms

Definition 32.1

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

Proposition 32.2

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

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

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

33 Splitting p-modular systems

Definition 33.1 (***p*-modular systems**)

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

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

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

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

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

Remark 33.2

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

34 Brauer Reciprocity

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

Exercise 34.1

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

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

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

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

Notation 34.2

Recall that Theorem 26.1(c) showed that for a group algebra over a field there is a bijection between projective indecomposable modules (up to isomorphism) and simple modules (up to isomorphism). Let S be a simple KG-module or a simple kG-module. As in Exercise 26.6, we let P_S denote a projective indecomposable module corresponding to S via the bijection. Then P_S is called a **projective cover** of S.

Theorem 34.3 (*Brauer Reciprocity*)

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

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

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

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

Proof: (a) Let M be an $\mathcal{O}$-form for V. Let $\overline{M} = M_0 > M_1 > \cdots > M_r = 0$ be a composition series for the quotient module $\overline{M}$. Fix a $j \in \{1, \dots, t\}$ and let P_{S_j} be a projective cover of S_j. By Lemma 30.4 and Proposition 30.2, there exists an idempotent $e_j \in \mathcal{O}G$ such that $P_{S_j} = kG\overline{e}_j$.

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

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

is exact. Hence

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

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

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

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

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

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

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

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

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

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

■

Definition 34.4

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

Remark 34.5

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

Chapter 9. Character Theory and Decomposition Matrices

The goal of this chapter is to define a character theory for modular representations of finite groups and to use character theory to learn more about the decomposition matrices of finite groups.

Notation: Throughout, G denotes a finite group and $(K, \mathcal{O}, k)$ is a splitting p-modular system for G.

References:

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

[Isa94] I. M. Isaacs. *Character theory of finite groups*. Dover Publications, Inc., New York, 1994.

[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.

35 Ordinary Characters

In this section we will briefly review some important definitions and results from ordinary character theory. We work over K, a splitting field for G of characteristic 0. In particular, KG is semisimple. The character theory of G over K is the same as the character theory of G over $\mathbb{C}$, which you have probably seen in an earlier course.

Definition 35.1

Let $\rho : G \to GL(V)$ be a K-representation of G for some $V \cong K^n$, $n \geqslant 1$. Then

$$\begin{aligned} \chi : G &\to K \\ g &\mapsto \operatorname{tr}(\rho(g)) \end{aligned}$$

is the **character of** ρ, or the **character afforded by** ρ. If ρ has degree one then χ is called a **linear** character. If ρ is an irreducible representation then χ is called an **irreducible** character. We denote the set of irreducible characters of G by $\operatorname{Irr}(G)$.

Remark 35.2

- Let $X : G \to \mathrm{GL}_n(K)$ be a matrix representation of G of degree $n \geqslant 1$. Then

$$\begin{aligned} \chi : G &\to K \\ g &\mapsto \mathrm{tr}(X(g)) \end{aligned}$$

is the **character of** X or the **character afforded by** X.

- **Exercise 35.3**

  Show that two similar matrix representations afford the same character.

Exercise 35.4

Lemma 35.5

Let $X : G \to \mathrm{GL}_n(\mathbb{C})$ be a complex representation of G of degree $n \geqslant 1$ and let χ be the character afforded by X.

(a) $\chi(1) = n$.

(b) $\chi(g)$ is a sum of $o(g)$-th roots of unity for all $g \in G$.

(c) $|\chi(g)| \leqslant \chi(1)$ for all $g \in G$.

(d) $\overline{\chi}$ is also a character of G, defined by $\overline{\chi}(g) = \chi(g^{-1})$ for all $g \in G$.

(e) $\chi(g) = \chi(h^{-1}gh)$ for all $g, h \in G$, i.e. characters are class functions.

Notation 35.6

Let $C_1, \dots, C_d$ be the conjugacy classes of G and denote the class sums by

$$\hat{C}_i := \sum_{g \in C_i} g$$

for each $1 \leqslant i \leqslant d$. Let $\mathrm{Cl}(G)$ denote the set of complex valued class functions of G.

Theorem 35.7

The class sums $\hat{C}_i, \dots, \hat{C}_d$ are a basis for $Z(KG)$.

Proof: Let $h \in G$. Then for any $1 \leqslant i \leqslant d$,

$$h\hat{C}_i = \sum_{g \in C_i} hg = \sum_{g \in C_i} hgh^{-1}h = \hat{C}_i h$$

since as g runs over C_i, so does hgh^{-1}. Hence $\hat{C}_i \in Z(KG)$ for any $1 \leqslant i \leqslant d$. Since $\{g \in G\}$ is a basis for KG, the set of class sums $\{\hat{C}_i\}_{1 \leqslant i \leqslant d}$ is linearly independent since they are sums of disjoint sets of elements of G.

Let $h \in G$ and let $z \in Z(KG)$ such that $z = \sum_{g \in G} a_g g$. Then

$$\sum_{g \in G} a_g g = z = h^{-1} z h = \sum_{g \in G} a_g h^{-1} g h = \sum_{g \in G} a_g g^h.$$

Equating coefficients in the sums shows that a_g is constant on conjugacy classes so $z = \sum_{i=1}^{d} a_{g_i} \hat{C}_i$, where $g_i \in C_i$. In particular, $Z(KG) \subseteq \langle \hat{C}_i \rangle$ and hence $\hat{C}_1, \ldots, \hat{C}_r$ is a basis for $Z(KG)$. ■

Remark 35.8

Two irreducible representations with the same character are similar. Thus by the arguments in Chapter 3 we have the following bijections

$$\operatorname{Irr}(G) \leftrightarrow \left\{ \begin{array}{c} \text{Irreducible } K\text{-reps of } G \\ \text{up to equivalence} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Simple } KG\text{-modules} \\ \text{up to isomorphism.} \end{array} \right\}$$

and since KG is semisimple, these sets are of size $\dim_K(Z(KG))$ by Corollary 13.4.

Corollary 35.9

The number of conjugacy classes of G is equal to $|\operatorname{Irr}(G)|$.

Proof: Immediate from Remark 35.8 and Theorem 35.7. ■

Definition 35.10

The **regular character** is the character χ_{reg} afforded by the regular representation ρ_{reg} of G (see Example 8).

Lemma 35.11

For any $g \in G$,

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof: Let $g \in G$. Then $\rho_{\text{reg}}(g) = (a_{hk})_{h,k \in G}$ where

$$a_{hk} = \begin{cases} 1 & \text{if } hg = k \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $\chi_{\text{reg}}(g) = \operatorname{tr}(\rho_{\text{reg}}(g)) = \#\{h \in G \mid hg = h\} = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{otherwise} \end{cases}$ ■

Proposition 35.12

We have $\chi_{\text{reg}} = \sum_{\chi \in \operatorname{Irr}(G)} \chi(1)\chi$.

Proof: By Theorem 13.2, since K is a splitting field for G and KG is semisimple, every irreducible representation X of G appears in the regular representation ρ_{reg} exactly $\dim_K(X)$ times. The result follows. ■

Exercise 35.13

Corollary 35.14 (*Degree forumla*)

Let $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_d\}$. Then $|G| = \sum_{i=1}^{d} \chi_i(1)^2$.

Notation 35.15

Let $\chi \in \mathrm{Irr}(G)$ and let X be an irreducible representation of G affording χ. Let S be the simple module corresponding to X as in Proposition 15.3. Then fix $e_\chi := e_S$, where the latter is the central primitive idempotent associated to S as in Scholium 12.6.

Remark 35.16

We can linearly extend a matrix representation of G to a representation of the group algebra KG,

$$X : KG \to M_n(K).$$

The character of X is defined by $\chi : KG \to K$, $\chi(g) = \mathrm{tr}(X(g))$ for all $g \in G$ and its restriction to G is just a character of G. We can therefore consider characters acting on elements of KG and not just on elements of G.

Proposition 35.17

For any $\chi \in \mathrm{Irr}(G)$, we have

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(1)\chi(g^{-1})g.$$

Proof: Write $e_\chi = \sum_{g \in G} a_g g$. By Lemma 35.11, we have for any $g \in G$,

$$\chi_{\mathrm{reg}}(e_\chi g^{-1}) = \chi_{\mathrm{reg}}\left(\sum_{h \in G} a_h h g^{-1}\right) = \sum_{h \in G} a_h \chi_{\mathrm{reg}}(hg^{-1}) = a_g |G|.$$

On the other hand, Proposition 35.12 shows that

$$\chi_{\mathrm{reg}}(e_\chi g^{-1}) = \sum_{\psi \in \mathrm{Irr}(G)} \psi(1)\psi(e_\chi g^{-1}).$$

Now $e_\chi g^{-1} \in e_\chi KG$, so by the orthogonality of the idempotents, $e_\chi g^{-1}$ is in the kernel of ψ for all $\psi \in \mathrm{Irr}(G)$ such that $\psi \neq \chi$. Therefore $a_g|G| = \chi(1)\chi(e_\chi g^{-1})$. But the idempotent e_χ is the identity in $e_\chi KG$, so $\chi(e_\chi g^{-1}) = \chi(g^{-1})$ for all $g \in G$, $\chi \in \mathrm{Irr}(G)$. Hence

$$e_\chi = \sum_{g \in G} a_g g = \sum_{g \in G} \frac{\chi(1)\chi(e_\chi g^{-1})}{|G|} g = \frac{1}{|G|} \sum_{g \in G} \chi(1)\chi(g^{-1})g,$$

as claimed. ■

Theorem 35.18 (*First Orthogonality Relations*)

For all $h \in G$ and all $\chi, \psi \in \mathrm{Irr}(G)$,

$$\frac{1}{|G|} \sum_{g \in G} \chi(gh)\psi(g^{-1}) = \delta_{\chi\psi} \frac{\chi(h)}{\chi(1)}$$

In particular, for $h = 1$ we have

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\psi(g^{-1}) = \begin{cases} 1 & \text{if } \chi = \psi \\ 0 & \text{otherwise} \end{cases}$$

Proof: Let e_χ and e_ψ be the central primitive idempotents associated to the irreducible characters χ and ψ as in Notation 35.15. Since they are orthogonal idempotents, $e_\chi e_\psi = \delta_{\chi\psi}e_\chi$. Hence from the formula given in Proposition 35.17, we have

$$|G|e_\chi e_\psi = \frac{1}{|G|}\sum_{h\in G}\sum_{g\in G}\chi(1)\psi(1)\chi(h^{-1})\psi(g^{-1})hg = \delta_{\chi\psi}|G|e_\chi = \delta_{\chi\psi}\sum_{k\in G}\chi(1)\chi(k^{-1})k.$$

Comparing coefficients for $k \in G$ and dividing by $\chi(1)$ shows that

$$\frac{1}{|G|}\sum_{g,h\in G, hg=k}\psi(1)\chi(h^{-1})\psi(g^{-1}) = \delta_{\chi\psi}\chi(k^{-1}).$$

Hence with $h = kg^{-1}$,

$$\frac{1}{|G|}\sum_{g\in G}\psi(1)\chi(gk^{-1})\psi(g^{-1}) = \delta_{\chi\psi}\chi(k^{-1}).$$

Now writing h instead of k throughout we get the desired result. ■

Proposition 35.19

The map

$$\begin{aligned} \langle\ ,\ \rangle : \mathrm{Cl}(G)\times\mathrm{Cl}(G) &\to \mathbb{C} \\ (\chi,\psi) &\mapsto \langle\chi,\psi\rangle := \frac{1}{|G|}\sum_{g\in G}\chi(g)\psi(g^{-1}) \end{aligned}$$

is a symmetric $\mathbb{C}$-bilinear form. The irreducible characters $\mathrm{Irr}(G)$ form an orthonormal basis for $\mathrm{Cl}(G)$ with respect to $\langle\ ,\ \rangle$. Further, $\langle\ ,\ \rangle$ is positive definite.

Proof:
- Bilinearity: Exercise
- Symmetry: Exercise
- $\mathbb{C}$-linear independence of $\mathrm{Irr}(G)$: Exercise
- $\mathrm{Irr}(G)$ is an orthonormal basis for $\mathrm{Cl}(G)$: Exercise
- Positive definiteness: Exercise ■

Corollary 35.20

(a) Let f be a class function of G. Then $f = \sum_{\chi\in\mathrm{Irr}(G)}\langle f,\chi\rangle\chi$.

(b) A character χ of G is irreducible if and only if $\langle\chi,\chi\rangle = 1$.

Proof: (a) For $\psi \in \mathrm{Irr}(G)$ we have

$$\left\langle \sum_{\chi\in\mathrm{Irr}(G)}\langle f,\chi\rangle\chi,\psi\right\rangle = \sum_{\chi\in\mathrm{Irr}(G)}\langle f,\chi\rangle\langle\chi,\psi\rangle = \langle f,\psi\rangle$$

by the first orthogonality relations. Hence

$$\left\langle f - \sum_{\chi \in \mathrm{Irr}(G)} \langle f, \chi \rangle, \psi \right\rangle = 0$$

for all $\psi \in \mathrm{Irr}(G)$. Therefore $f - \sum_{\chi \in \mathrm{Irr}(G)} \langle f, \chi \rangle = 0$ by Proposition 35.19, so $f = \sum_{\chi \in \mathrm{Irr}(G)} \langle f, \chi \rangle \chi$.

(b) Since $\mathrm{Irr}(G)$ is a basis for the class functions of G by Proposition 35.19, and characters are class functions by Lemma 35.5 (e), ψ is a character of G if and only if

$$\psi = \sum_{\chi \in \mathrm{Irr}(G)} n_\chi \chi$$

for some $n_\chi \geqslant 0$. Thus,

$$\langle \psi, \psi \rangle = \sum_{\chi, \mu} n_\chi n_\mu \langle \chi, \mu \rangle = \sum_{\chi, \mu} n_\chi n_\mu \delta_{\chi\mu} = \sum_{\chi, \mu} n_\chi^2.$$

Therefore $\langle \psi, \psi \rangle = 1$ if and only if there exists a unique $\chi \in \mathrm{Irr}(G)$ with $n_\chi = 1$ and $n_\varphi = 0$ for all $\varphi \in \mathrm{Irr}(G)$ such that $\varphi \neq \chi$. In other words, $\langle \psi, \psi \rangle = 1$ if and only if $\psi = \chi \in \mathrm{Irr}(G)$. ■

Theorem 35.21 (*Second Orthogonality Relations*)

For all $g, h \in G$, we have

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\chi(h^{-1}) = \begin{cases} |C_G(g)| & \text{if } g \text{ is conjugate to } h \\ 0 & \text{otherwise} \end{cases}$$

Proof: The first orthogonality relations (Theorem 35.18) shows that since characters are class functions, for any $\chi, \psi \in \mathrm{Irr}(G)$ we have

$$\delta_{\chi\psi}|G| = \sum_{g \in G} \chi(g)\psi(g^{-1}) = \sum_{i=1}^{d} \chi(g_i)|C_i|\psi(g_i^{-1}),$$

where $g_1, \ldots, g_d$ is a set of representatives of the conjugacy classes $C_1, \ldots, C_d$ of G. Define the following $d \times d$ matrices:

$$\begin{aligned} I_d &:= \text{ the identity matrix} \\ X &:= (\chi(g_i))_{\chi \in \mathrm{Irr}(G), 1 \leqslant i \leqslant d} \\ \tilde{X} &:= (\chi(g_i^{-1}))_{\chi \in \mathrm{Irr}(G), 1 \leqslant i \leqslant d} \\ D &:= \text{ diag } (|C_1|, \ldots, |C_d|) \end{aligned}$$

Then the equation above can be expressed as

$$|G| I_d = X D \tilde{X}^t,$$

so $\frac{1}{|G|} X$ is a left inverse of $D\overline{X}^t$, and therefore also a right inverse so we have

$$|G| I_d = D \tilde{X}^t X,$$

which gives, for each $1 \leqslant i, j \leqslant d$,

$$|G|\delta_{ij} = \sum_{\chi \in \mathrm{Irr}(G)} |C_i| \chi(g_i^{-1}) \chi(g_j).$$

Hence, since $\frac{|G|}{|C_i|} = |C_G(g_i)|$, we have

$$\delta_{ij}|C_G(g_i)| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(g_i^{-1})\chi(g_j)$$

for all $g_i \in C_i$. ■

Remark 35.22

Let $\rho : G \to \mathrm{GL}(V)$ be a representation of G for some $V \cong K^n$, $n \geqslant 1$, and define a KG-module structure on V as in Proposition 15.3. Since KG is semisimple, $V = \bigoplus_{i=1}^r S_i$ for simple KG-modules S_i. Therefore any matrix representation X associated to ρ is similar to a diagonal representation

$$X = \begin{pmatrix} X_1 & 0 & \dots & 0 \\ 0 & X_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & X_r \end{pmatrix},$$

where X_i are irreducible representations of G called the **irreducible constituents** of X. Let $\chi_i \in \mathrm{Irr}(G)$ denote the character of X_i for each $1 \leqslant i \leqslant r$. Then $\sum_{i=1}^r \chi_i$ is the character of X.

Proposition 35.23

Representations with the same character are similar.

Proof: Let X and X' be representations of G with characters $\sum_{i=1}^r \chi_i$ and $\sum_{j=1}^s \chi_j'$ respectively, where $\chi_i, \chi_j' \in \mathrm{Irr}(G)$ for all $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. Then since the irreducible characters of G are linearly independent, if $\sum_{i=1}^r \chi_i = \sum_{j=1}^s \chi_j'$ then $r = s$ and without loss of generality, $\chi_i = \chi_i'$ for all $1 \leqslant i \leqslant r$. Thus each of the irreducible constituents X_i of X is similar to the corresponding irreducible constituent X_i' of X', so X is similar to X'. ■

36 Brauer Characters

Notation 36.1

We will now fix a particular splitting p-modular system for G.

- Let $X_1, \dots, X_r$ be a complete system of representatives for the isomorphism classes of irreducible representations of G over a splitting field of finite degree over $\mathbb{Q}_p$.
- Let $Y_1, \dots, Y_s$ be a complete system of representatives for the isomorphism classes of irreducible representations of G over a splitting field of finite degree over $\mathbb{F}_p$.
- Let $k_1 \mid \mathbb{F}_p$ be generated by a $|G|_{p'}$- root of unity and the entries in the matrices $Y_i(g)$ for all $g \in G$, $1 \leqslant i \leqslant s$. Then k_1 is a finite extension of $\mathbb{F}_p$, so $k_1 = \mathbb{F}_q$ for some $q = p^f$, $f \geqslant 1$.
- Let $K \mid \mathbb{Q}_p$ be generated by a $(q$-$1)$th root of unity and the entries in the matrices $X_i(g)$ for all $g \in G$, $1 \leqslant i \leqslant r$.
- Let $\mathcal{O}$ be the integral closure of $\mathbb{Z}_p$ in K.

- Define $k := \mathcal{O}/J(\mathcal{O})$.

It is possible to show that the ring $\mathcal{O}$ is a complete discrete valuation ring. Thus $J(\mathcal{O})$ is its unique maximal ideal. The residue class k contains $k_1 = \mathbb{F}_q$, and both K and k are splitting fields for G. Thus $(K, \mathcal{O}, k)$ is a splitting p-modular system for G.

Lemma 36.2

Let X be a k-representation of G. Then the eigenvalues of $X(g)$ are contained in k for all $g \in G$.

Proof: Let $g \in G$ and write $o(g) = p^n m$ for $n \geqslant 0$ and $m \geqslant 1$ such that $(p, m) = 1$. Then $m \mid |G|_{p'}$.

Let ξ be an eigenvalue of $X(g)$. Then $\xi^{o(g)} = 1$, so

$$0 = \xi^{p^n m} - 1 = (\xi^m - 1)p^n,$$

because k has characteristic p. Therefore $\xi^m = 1$. By construction, k contains k_1 which contains the $|G|_{p'}$-th roots of unity. The result follows since $m \mid |G|_{p'}$. ∎

Notation 36.3

Let $\star : \mathcal{O} \to k$ be the natural quotient map and let U denote the set of p'-roots of unity in $K^\times$.

$$U := \{\alpha \in K^\times \mid \alpha^m = 1 \text{ for an } m \in \mathbb{N} \text{ such that } (m, p) = 1\} \subseteq \mathcal{O}.$$

Proposition 36.4

The restriction of $\star$ to U defines an injective homomorphism of multiplicative groups $\star : U \to k^\times$ which is surjective on the $|G|_{p'}$th roots of unity.

Proof: First of all we will show that $J(\mathcal{O}) \cap \mathbb{Z} = p\mathbb{Z}$. It is clear that $p\mathbb{Z} \subseteq J(\mathcal{O}) \cap \mathbb{Z}$. Suppose that $m \in J(\mathcal{O}) \cap \mathbb{Z}$ is not divisible by p. Then there exist integers a and b such that $ap + bm = 1$. Therefore $1 \in J(\mathcal{O})$, which is a contradiction, so every element of $J(\mathcal{O}) \cap \mathbb{Z}$ is divisible by p and hence $J(\mathcal{O}) \cap \mathbb{Z} = p\mathbb{Z}$.

Let $1 \neq \zeta \in U$ be a primitive mth root of unity. Then

$$1 + x + x^2 + \cdots + x^{m-1} = \frac{x^m - 1}{x - 1} = \prod_{i=1}^{m-1} (x - \zeta^i)$$

Setting $x = 1$ we see that m is divisible by $1 - \zeta$. Suppose that $\zeta^\star = 1$. Then $m^\star = 0$ so $m \in J(\mathcal{O})$. But m is p' so this contradicts $J(\mathcal{O}) \cap \mathbb{Z} = p\mathbb{Z}$. Hence the only $\zeta \in U$ such that $\zeta^\star = 1$ is $\zeta = 1$, so the $\star$ map is injective on U.

Now since K contains a $(q-1)$th root of unity and $|G|_{p'}$ divides $q - 1$, it is clear that the map $\star$ is surjective onto the $|G|_{p'}$th roots of unity. ∎

Definition 36.5

Denote the set of **p-regular elements** of G by

$$G^\circ := \{g \in G \mid p \nmid o(g)\}$$

Let $X : G \to \mathrm{GL}_n(k)$ be a matrix representation of G. By the setup of Notation 36.1, for any $g \in G^\circ$, the eigenvalues $\beta_1, \ldots, \beta_n$ of $X(g)$ lie in $k^\times$. Thus Proposition 36.4 shows that there exist uniquely determined roots of unity $\xi_1, \ldots, \xi_n \in U$ such that $\xi_i^\star = \beta_i$ for $1 \leqslant i \leqslant n$. The map

$$\begin{aligned} \varphi : G^\circ &\to \mathcal{O} \\ g &\mapsto \xi_1 + \cdots + \xi_n \end{aligned}$$

is called the **Brauer character** of the representation X of G. The **degree** of φ is n. We note the following.

- $\varphi(g) \in \mathcal{O} \subseteq \overline{\mathbb{Q}}_p$ even though $X(g) \in \mathrm{GL}_n(k)$.
- Often the values of Brauer characters are considered as complex numbers (sums of complex roots of unity). In that case then $\varphi(g)$ depends on the choice of embeddding of U into $\mathbb{C}$. For a fixed embedding, $\varphi(g)$ is uniquely determined up to similarity of X.

Definition 36.6

The Brauer character φ is **irreducible** if X is irreducible. We let $\mathrm{IBr}(G)$ denote the set of all irreducible Brauer characters of G. The Brauer character of the trivial representation $G \to \mathrm{GL}_1(k)$, $g \mapsto 1$ is denoted by 1_{G°. We say that a Brauer character λ is **linear** if $\lambda(1) = 1$.

Notation 36.7

Let $\mathrm{Cl}(G^\circ)$ denote the set of $\mathbb{C}$-valued class functions on G°.

Lemma 36.8

Let $X : G \to \mathrm{GL}_n(k)$ be a representation of G for some $n \geqslant 1$. Then for all $g \in G^\circ$, $X(g)$ is similar to a diagonal matrix $\mathrm{diag}(\xi_1^\star, \ldots, \xi_n^\star)$ for some $\xi_1, \ldots, \xi_n \in U$.

Proof: Let $g \in G^\circ$. Consider the restriction of X to the cyclic group $\langle g \rangle$. Since $\langle g \rangle$ is abelian, it follows from Corollary 17.2 that all irreducible representations of $\langle g \rangle$ have degree 1. Since $(o(g), p) = 1$, the characteristic of k does not divide $|\langle g \rangle|$ and hence by Maschke's Theorem 16.1, $k\langle g \rangle$ is semisimple. Therefore $X(g)$ is similar to a diagonal matrix $\mathrm{diag}(\beta_1, \ldots, \beta_n)$ for some $\beta_1, \ldots, \beta_n \in k^\times$. This yields the result if we let $\xi_i \in U$ be the unique root of unity such that $\xi_i^\star = \beta_i$ for each $1 \leqslant i \leqslant n$. ■

Proposition 36.9

Let φ be a Brauer character of G.

(a) $\varphi \in \mathrm{Cl}(G^\circ)$.

(b) For any $g \in G^\circ$, $\varphi(g^{-1}) = \overline{\varphi(g)}$.

(c) The function $\overline{\varphi} : G^\circ \to \mathbb{C}$, $g \mapsto \varphi(g^{-1})$ is a Brauer character

(d) For $H \leqslant G$, $\varphi_H := \varphi\,|_{H^\circ}$ is a Brauer character of H.

Proof: Let X be a matrix representation affording φ.

(a) For any $g, h \in G^\circ$, $X(g^h) = X(h^{-1})X(g)X(h)$ so the $X(g)$ and $X(g^h)$ are similar and therefore have the same eigenvalues. Thus $\varphi(g) = \varphi(g^h)$ for any $g, h \in G^\circ$.

(b) It follows from Lemma 36.8 that for any $g \in G^\circ$, the matrix $X(g)$ is similar to a diagonal matrix $\mathrm{diag}(\xi_1^\star, \ldots, \xi_n^\star)$ for some $\xi_1, \ldots, \xi_n \in U$. Hence $X(g^{-1}) = X(g)^{-1}$ is similar to

$\operatorname{diag}((\xi_1^{-1})^\star, \dots, (\xi_n^{-1})^\star)$. Now each ξ_i is a root of unity so $\xi_1^{-1} = \overline{\xi}_i$ for $1 \leqslant i \leqslant n$, and hence $\varphi(g^{-1}) = \overline{\varphi(g)}$ for all $g \in G^\circ$.

(c) By (b), the map $Y : G \to \mathrm{GL}_n(k)$, $g \mapsto Y(g) := X(g^{-1})^t$ is a representation with character $\overline{\varphi}$.

(d) The restriction X_H is a representation of H with character φ_H. ■

Remark 36.10

Suppose that $\rho : G \to \mathrm{GL}(V)$ is a representation of G for some $V \cong k^n$, $n \geqslant 1$, and let X be a matrix representation associated to ρ as in Remark 35.22. Since kG is not semisimple in general, we cannot conclude that X is similar to a diagonal representation. We can however, show the following.

Let $0 = V_0 < \cdots < V_r = V$ be a composition series for V for some $r \in \mathbb{N}$. Choose a basis for V_1. Extend this to a basis of V_2, and so on, until you get a basis of V. For this choice of basis, the matrix representation associated to ρ is an upper triangular block matrix of the form

$$\begin{pmatrix} X_1 & * & \dots & * \\ 0 & X_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & X_r \end{pmatrix},$$

where X_i is an irreducible representation corresponding to the simple kG-module V_i/V_{i-1} for $1 \leqslant i \leqslant r$. Hence by abuse of language, we say that X *is similar to a representation in upper block diagonal form*. It follows from Jordan-Hölder that the simple modules V_i/V_{i-1} are determined up to isomorphism by V, and hence the irreducible representations X_i are uniquely determined up to similarity by X. As in the semisimple case, the irreducible representations X_i are called the **irreducible constituents** of X.

Theorem 36.11

A class function $\varphi \in \mathrm{Cl}(G^\circ)$ is a Brauer character if and only if it is a non-negative integer linear combination of elements of $\mathrm{IBr}(G)$.

Proof: By Remark 36.10, if a class function φ is a Brauer character afforded by representation X then X is similar to a representation in upper block diagonal form and φ is just the sum of the irreducible Brauer characters afforded by the irreducible constituents of X. ■

Notation 36.12

For $g \in G$, let $g = g_p g_{p'}$ be the splitting of g into its p-part and its p'-part. Then if $o(g) = p^n m$ with $(p, m) = 1$ and $1 = ap^n + bm$, then $g_p = g^{bm}$ and $g_{p'} = g^{ap^n}$.

Proposition 36.13

Let X be a representation of kG and let ψ be the trace function on X, $\psi : kG \to k$, $\psi(g) = \operatorname{tr} X(g))$ for all $g \in G$. Let φ be the Brauer character afforded by X, and define $\varphi^\star : G \to k^\times$ by $\varphi^\star(g) = \varphi(g_{p'})^\star$ for all $g \in G$. Then,

(a) $\psi(g) = \psi(g_{p'})$ for all $g \in G$,

(b) $\psi(g) = \varphi(g_{p'})^\star$ for all $g \in G$, and

(c) $\{\varphi^\star \mid \varphi \in \mathrm{IBr}(G)\}$ is the set of trace functions of the irreducible kG-representations.

Proof:

(a) Since X is similar to a representation in upper block diagonal form, we can assume that X is irreducible. There is also no loss of generality if we assume that $G = \langle g \rangle$. Then all the irreducible representations of G are one dimensional. Therefore $\psi = X : G \to k^\times$ is a group homomorphism so $\psi(g) = \psi(g_p)\psi(g'_p)$. But g_p has p-power order. Therefore $\psi(g_p) \in k^\times$ also has p-power order. But in a field of characteristic p, the only element with order a power of p is 1. Therefore $\psi(g) = \psi(g_{p'})$, for all $g \in G$.

(b) This holds by definition of φ and part (a).

(c) This holds because $\varphi^\star(g) = \varphi(g_{p'})^\star = \operatorname{tr} X(g) = \psi(g)$ for all $g \in G$. ■

Theorem 36.14

The set of irreducible Brauer characters of G, $\mathrm{IBr}(G)$, is linearly independent over $\mathbb{C}$ and hence

$$|\,\mathrm{IBr}(G)| \leqslant \dim_{\mathbb{C}} \mathrm{Cl}(G^\circ) = \text{ The number of conjugacy classes of } p'\text{-elements in } G$$

Proof: Omitted. ■

37 Decomposition Matrices of Finite Groups

In this section we continue with $(K, \mathcal{O}, k)$ the splitting p-modular system for G defined in Notation 36.1. We now want to look at the connections between representations of G over K (or $\mathbb{C}$), and representations of G over k.

Notation 37.1

For a complex class function $\chi \in \mathrm{Cl}(G)$, we denote the restriction of χ to G° by $\chi^\circ \in \mathrm{Cl}(G^\circ)$. We denote the set of class functions of G which vanish on $G \backslash G^\circ$ – i.e. the $\chi \in \mathrm{Cl}(G)$ for which $\chi(x) = 0$ for all $x \in G\backslash G^\circ$ – by $\mathrm{Cl}^\circ(G)$.

Corollary 37.2

Let χ be an ordinary character of G. Then χ° is a Brauer character of G.

Proof: Let X be an (ordinary) representation of G which affords the character χ. Then X is similar to a representation X' in block diagonal form, with some irreducible representations of G on the diagonal. Thus the entries in $X'(g)$ are contained in K for all $g \in G$ (see the setup in Notation 36.1). Hence by Proposition 32.2, there exists an $\mathcal{O}$-form of the KG-module corresponding to X'. In other words, X is similar to some representation of G with matrix entries in $\mathcal{O}$.

Let $X^\star$ denote the representation of G over k given by $X^\star(g) := X(g)^\star$ for all $g \in G$. Fix an element $g \in G^\circ$ and let $\xi_1, \dots, \xi_n$ be the eigenvalues of $X(g)$, where $n \in \mathbb{N}$ is the degree of X. Since $(p, o(g)) = 1$, the eigenvalues $\xi_1, \dots, \xi_n$ are p'-roots of unity so they lie in U. Then $\xi_1^\star, \dots, \xi_n^\star$ are the roots of the polynomial $\det(xI - X(g))^\star = \det(xI - X^\star(g))$, and hence $\xi_1^\star, \dots, \xi_n^\star$ are the eigenvalues of $X^\star(g)$. Therefore $X^\star$ is a representation of G over k with Brauer character χ°. ■

Corollary 37.3

The set $\mathrm{IBr}(G)$ is a basis of $\mathrm{Cl}(G^\circ)$ over $\mathbb{C}$. In particular, $|\mathrm{IBr}(G)|$ is the number of p'-conjugacy classes of G.

Proof: By Theorem 36.14, $\mathrm{IBr}(G)$ is linearly independent over $\mathbb{C}$. It remains to show that $\mathrm{IBr}(G)$ is a generating set for $\mathrm{Cl}(G^\circ)$. Let $\mu \in \mathrm{Cl}(G^\circ)$ and let $\alpha \in \mathrm{Cl}(G)$ be an extension of μ to a class function of G. Then by Proposition 35.19, since $\mathrm{Irr}(G)$ is a $\mathbb{C}$-basis for $\mathrm{Cl}(G)$,

$$\alpha = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi$$

for some $a_\chi \in \mathbb{C}$, so

$$\mu = \alpha^\circ = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi^\circ.$$

By Corollary 37.2 each χ° is a Brauer character, and hence by Theorem 36.11, each χ° is a non-negative integer linear combination of irreducible Brauer characters. Therefore μ is a linear combination of irreducible Brauer characters over $\mathbb{C}$, so $\mathrm{IBr}(G)$ is a generating set for $\mathrm{Cl}(G^\circ)$. The final claim is then immediate. ■

Remark 37.4

Let $\chi \in \mathrm{Irr}(G)$. Corollary 37.3 says that there exist positive integers $d_{\chi\varphi} \geqslant 0$ such that

$$\chi^\circ = \sum_{\varphi \in \mathrm{IBr}(G)} d_{\chi\varphi}\varphi.$$

Note that if we translate this from characters to modules, we see that the $d_{\chi\varphi}$ are the same as the decomposition numbers from Definition 24.4 and Brauer's Reciprocity, so the decomposition matrix of G with respect to p is

$$D = (d_{\chi\varphi})_{\chi \in \mathrm{Irr}(G), \varphi \in \mathrm{IBr}(G)}.$$

Corollary 37.5

The decomposition matrix D has full rank $|\mathrm{IBr}(G)|$.

Proof: Since $\mathrm{Irr}(G)$ is a basis of $\mathrm{Cl}(G)$, $\{\chi^\circ \mid \chi \in \mathrm{Irr}(G)\}$ spans $\mathrm{Cl}(G^\circ)$. There is therefore a subset $B \subseteq \{\chi^\circ \mid \chi \in \mathrm{Irr}(G)\}$ which forms a basis for $\mathrm{Cl}(G^\circ)$. By Corollary 37.3, the columns of the matrix $(d_{\chi\varphi})_{\chi \in B, \varphi \in \mathrm{IBr}(G)}$ are linearly independent. Hence D has full rank. ■

In particular, D has no zero-columns so every $\varphi \in \mathrm{IBr}(G)$ is a constituent of at least one χ°, for some $\chi \in \mathrm{Irr}(G)$. This gives us a route to $\mathrm{IBr}(G)$, at least in principle.

Definition 37.6

The **Cartan matrix of** G (with respect to p) is defined to be

$$C := D^t D.$$

Since D has maximum rank, $C = (c_{\varphi\mu})_{\varphi,\mu \in \mathrm{IBr}(G)}$ is a positive definite symmetric matrix with non-negative integer entries. Note that for any $\varphi, \mu \in \mathrm{IBr}(G)$,

$$c_{\varphi\mu} = \sum_{\chi \in \mathrm{Irr}(G)} d_{\chi\varphi} d_{\chi\mu}.$$

Definition 37.7

Let $\varphi \in \mathrm{IBr}(G)$ be an irreducible Brauer character afforded by an irreducible k-representation X of G, and let S be a simple kG-module associated to X. Let P_S denote the projective cover of S and let Q_S denote a lift of P_S to $\mathcal{O}G$ as in Corollary 30.6. We say that the character of $KG \otimes_{\mathcal{O}G} Q_S$ is the **projective indecomposable character of** φ, and denote it by Φ_φ.

Corollary 37.8

Let $\varphi \in \mathrm{IBr}(G)$. Then

(a) $\Phi_\varphi = \sum_{\chi \in \mathrm{Irr}(G)} d_{\chi\varphi}\chi$, and

(b) $\Phi_\varphi^\circ = \sum_{\mu \in \mathrm{IBr}(G)} c_{\varphi\mu}\mu$.

Proof: (a) This result follows from Brauer reciprocity.

(b) This follows from part (a) because

$$\Phi_\varphi^\circ = \sum_{\chi \in \mathrm{Irr}(G)} d_{\chi\varphi}\chi^\circ = \sum_{\chi \in \mathrm{Irr}(G)} d_{\chi\varphi} \sum_{\mu \in \mathrm{IBr}(G)} d_{\chi\mu}\mu = \sum_{\mu \in \mathrm{IBr}(G)} c_{\varphi\mu}\mu$$

■

Theorem 37.9

If $p \nmid |G|$, then $\mathrm{IBr}(G) = \mathrm{Irr}(G)$ and the decomposition matrix of G is the identity matrix when the characters are ordered in the same way for the rows and for the columns.

Proof: If $p \nmid |G|$, then by Maschke's theorem, kG is semisimple. By Theorem 13.2 (c), since k is a splitting field for G, $|G| = \dim_k(kG) = \sum_{\varphi \in \mathrm{IBr}(G)} \varphi(1)^2$. We also know that $|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2$ by Exercise 35.14. Now

$$\begin{aligned}|G| &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = \sum_{\chi \in \mathrm{Irr}(G)} \left(\sum_{\varphi \in \mathrm{IBr}(G)} d_{\chi\varphi}\varphi(1) \right)^2 = \sum_{\chi \in \mathrm{Irr}(G)} \sum_{\varphi,\mu \in \mathrm{IBr}(G)} d_{\chi\varphi}d_{\chi\mu}\varphi(1)\mu(1) \\ &\geqslant \sum_{\chi \in \mathrm{Irr}(G)} \sum_{\varphi \in \mathrm{IBr}(G)} (d_{\chi\varphi})^2\varphi(1)^2 = \sum_{\varphi \in \mathrm{IBr}(G)} \left(\sum_{\chi \in \mathrm{Irr}(G)} (d_{\chi\varphi})^2 \right) \varphi(1)^2 \geqslant \sum_{\varphi \in \mathrm{IBr}(G)} \varphi(1)^2 = |G|,\end{aligned}$$

where the last inequality follows from the fact that for every $\varphi \in \mathrm{IBr}(G)$, there is some $\chi \in \mathrm{Irr}(G)$ with $d_{\chi\varphi} \neq 0$. Hence $d_{\chi\varphi}d_{\chi\mu} = 0$ if $\varphi \neq \mu$, and for every $\varphi \in \mathrm{IBr}(G)$ there exists a unique $\chi \in \mathrm{Irr}(G)$ with $d_{\chi\varphi} \neq 0$. In fact $d_{\chi\varphi} = 1$. ■

Definition 37.10

For $\varphi, \psi \in \mathrm{Cl}(G)$ or $\mathrm{Cl}(G^\circ)$, we define

$$\langle \varphi, \psi \rangle^\circ := \frac{1}{|G|} \sum_{g \in G^\circ} \varphi(g)\overline{\psi(g)}.$$

Note that $\langle \varphi, \psi \rangle^\circ = \overline{\langle \psi, \varphi \rangle^\circ}$.

The following theorem is a replacement for the orthogonality relations from ordinary character theory.

Theorem 37.11

The set $\{\Phi_\varphi \mid \varphi \in \mathrm{IBr}(G)\}$ is a basis for $\mathrm{Cl}^\circ(G)$. For every $\varphi, \psi \in \mathrm{IBr}(G)$ we have

$$\langle \varphi, \Phi_\psi \rangle^\circ = \delta_{\varphi\psi} = \langle \Phi_\varphi, \psi \rangle^\circ,$$

and therefore $C^{-1} = (\langle \varphi, \psi \rangle^\circ)_{\varphi,\psi \in \mathrm{IBr}(G)}$.

Proof: Let $x \in G$ and $y \in G^\circ$ and let C_x and C_y be their respective conjugacy classes in G. By the second orthogonality relations (Theorem 35.21), we have

$$\delta_{C_x,C_y}|C_G(x)| = \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(x)}\chi(y).$$

Since $y \in G^\circ$, we know that $\chi(y) = \sum_{\varphi \in \mathrm{IBr}(G)} d_{\chi\varphi}\varphi(y)$. Hence

$$(*) \qquad \delta_{C_x,C_y}|C_G(x)| = \sum_{\varphi \in \mathrm{IBr}(G)} \left(\sum_{\chi \in \mathrm{Irr}(G)} d_{\chi\varphi}\overline{\chi(x)} \right) \varphi(y) = \sum_{\varphi \in \mathrm{IBr}(G)} \overline{\Phi_\varphi(x)}\varphi(y)$$

by Corollary 37.8. Thus for any $x \in G \setminus G^\circ$, we have $\sum_{\varphi \in \mathrm{IBr}(G)} \overline{\Phi_\varphi(x)}\varphi = 0$. But Theorem 36.14 shows that $\mathrm{IBr}(G)$ is a linearly independent set, so $\overline{\Phi_\varphi(x)} = 0$ for all $x \in G \setminus G^\circ$ and therefore $\overline{\Phi_\varphi}$ is a class function which vanishes on $G \setminus G^\circ$, $\overline{\Phi_\varphi} \in \mathrm{Cl}^\circ(G)$.

Let $x_1, \dots, x_r$ be a system of representatives for the conjugacy classes $C_1 \dots, C_r$ in G° ($r \in \mathbb{N}$). Define the following $r \times r$ matrices.

$$\begin{aligned} I_r &:= \text{the identity } r \times r \text{ matrix} \\ \Phi &:= (\Phi_\varphi(x_i))_{\varphi \in \mathrm{IBr}(G), i=1,\dots,r}, \\ Y &:= (\varphi(x_j))_{\varphi \in \mathrm{IBr}(G), j=1,\dots,r} \\ E &:= \mathrm{diag}(|C_G(x_1)|, \dots, |C_G(x_r)|) \end{aligned}$$

Then the equation $(*)$ can be expressed as

$$I_r = \overline{\Phi}^t Y E^{-1}$$

Thus YE^{-1} is a right inverse, and hence a left inverse, for $\overline{\Phi}^t$, so

$$I_r = YE^{-1}\overline{\Phi}^t.$$

It follows that

$$\delta_{\varphi\mu} = \sum_{i=1}^{r} \varphi(x_i) \frac{1}{|C_G(x_i)|} \overline{\Phi_\mu(x_i)}.$$

Now since $\frac{|G|}{|C_i|} = |C_G(x_i)|$,

$$\langle \varphi, \Phi_\mu \rangle^\circ = \frac{1}{|G|} \sum_{g \in G^\circ} \varphi(g)\overline{\Phi_\mu(g)} = \frac{1}{|G|} \sum_{i=1}^{r} \varphi(x_i)|C_i|\overline{\Phi_\mu(x_i)} = \sum_{i=1}^{r} \varphi(x_i) \frac{1}{|C_G(x_i)|} \overline{\Phi_\mu(x_i)} = \delta_{\varphi\mu}.$$

Thus the set of projective indecomposable characters $\{\Phi_\varphi \mid \varphi \in \mathrm{IBr}(G)\}$ is linearly independent. Since $\dim_{\mathbb{C}} \mathrm{Cl}^\circ(G) = \dim_{\mathbb{C}} \mathrm{Cl}(G^\circ) = |\mathrm{IBr}(G)|$ by Corollary 37.2, it follows that $\{\Phi_\varphi \mid \varphi \in \mathrm{IBr}(G)\}$ is a basis for $\mathrm{Cl}^\circ(G)$.

Finally, by Corollary 37.8, for any $\mu \in \mathrm{IBr}(G)$, $\Phi_\mu^\circ = \sum_{\psi \in \mathrm{IBr}(G)} c_{\psi\mu}\psi$. Thus for any $\varphi \in \mathrm{IBr}(G)$,

$$\sum_{\psi \in \mathrm{IBr}(G)} c_{\psi\mu}\langle \varphi, \psi \rangle^\circ = \langle \varphi, \sum_{\psi \in \mathrm{IBr}(G)} c_{\psi\mu}\psi \rangle^\circ = \langle \varphi, \Phi_\mu^\circ \rangle^\circ = \langle \varphi, \Phi_\mu \rangle^\circ = \delta_{\varphi\mu}.$$

Therefore $(\langle \varphi, \psi \rangle^\circ)_{\varphi,\psi \in \mathrm{IBr}(G)}$ is the inverse of the Cartan matrix C. ■

Chapter 10. Blocks and Defect Groups

We can break down the representation theory of finite groups into its smallest parts by studying the *blocks* of group algebras. First we will define blocks for any ring A. For the remainder of the course we will then return to the situation of a finite group G and a splitting p-modular system $(K, \mathcal{O}, k)$. We will briefly talk about the blocks of KG and $\mathcal{O}G$, and then move on to focus on the blocks of kG.

References:

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

[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.

38 Blocks

We first define blocks for any ring A with an identity.

Proposition 38.1

Let A be an arbitrary ring with an identity.

(a) The set of decompositions of A into a direct sum of two-sided ideals

$$A = A_1 \oplus \cdots \oplus A_r$$

(for some $r \in \mathbb{N}$) biject with the set of decompositions of 1_A into a sum of orthogonal central idempotents,

$$1_A = e_1 + \cdots + e_r,$$

where e_i is the identity of A_i and $A_i = Ae_i$ for $1 \leqslant i \leqslant r$.

(b) For each $1 \leqslant i \leqslant r$, the direct summand $A_i = Ae_i$ of A is indecomposable as a ring if and only if the corresponding central idempotent e_i is primitive.

(c) The decomposition of A into indecomposable two-sided ideals is unique.

Proof:

(a) Decompose A into a direct sum of two-sided ideals, $A = A_1 \oplus \cdots \oplus A_r$. Then the identity element of A decomposes into $1_A = e_1 + \cdots + e_r$, where $e_i \in A_i$ for each $1 \leqslant i \leqslant r$. For any element $a \in A$, $a = 1_A a = (e_1 + \cdots + e_r)a = e_1 a + \cdots + e_r a$, with $e_i a \in A_i$. If $a_i \in A_i$ then $e_i a_i = a_i$ and $e_j a_i = 0$ for $j \neq i$. In other words, e_i is the identity of A_i and $e_i^2 = e_i$ so $\{e_i\}_{i=1}^r$ is a set of orthogonal central idempotents of A, and $A_i = Ae_i$ for $1 \leqslant i \leqslant r$.

Conversely, if $\{e_i\}_{i=1}^r$ is a set of central orthogonal idempotents of A such that $1_A = \sum_{i=1}^r e_i$, then $\bigoplus_{i=1}^r Ae_i$ is a direct sum decomposition of A into two-sided ideals.

(b) $\Rightarrow$ Suppose that $A_i = Ae_i$ and $e_i = f + j$ for orthogonal idempotents f, j. Then $A_i = Af \oplus Aj$, where the sum is direct because if $a \in Af \cap Aj$ then $a = af$ and $a = aj$, hence $a = afj = 0$. Thus, if e_i is not primitive, then A_i is not indecomposable.

$\Leftarrow$ Now suppose that $A_i = Ae_i$ and $A_i = L_1 \oplus L_2$ for two two-sided ideals L_1 and L_2 of A. Then $e_i = f + j$ for some $f \in L_1$, $j \in L_2$. Since $L_1 \cap L_2 = \{0\}$ and $fj \in L_1 \cap L_2$, we have $fj = 0$. As e_i is the identity in A_i, we also see that $f = e_i f = (f + j)f = f^2 + jf = f^2$ and similarly, $j^2 = j$, hence f and j are orthogonal idempotents, so e_i is not primitive.

(c) Finally, suppose that $A = A_1 \oplus \cdots \oplus A_r$ for some $r \in \mathbb{N}$, and suppose that L is an indecomposable direct summand of A from a different decomposition of A. Every $x \in L$ has a decomposition $x = a_1 + \cdots + a_r$ with $a_i \in A_i$ for all $1 \leqslant i \leqslant r$. Then $e_i x = a_i$, and this is an element of L because L is a two-sided ideal. Hence $L = (L \cap A_1) + \cdots + (L \cap A_r)$. This is a decomposition of L, which was indecomposable, hence $L = L \cap A_m$ for some $1 \leqslant m \leqslant r$. By the indecomposability of A_m, this must be the whole of A_m. Thus the decomposition of A into indecomposable two-sided ideals is unique. ■

Definition 38.2

Let $A = A_1 \oplus \cdots \oplus A_r$ be the unique decomposition of A into a direct sum of indecomposable two-sided ideals such that $A_i = Ae_i$ for $1 \leqslant i \leqslant r$, as above. Each A_i is a **block** of A and the corresponding primitive central idempotent e_i is called the **block idempotent of** A_i . Note that the blocks of A are direct summands of A, and therefore are projective as A-modules.

Definition 38.3

Let M be an A-module. Then M **lies in the block** $A_i = Ae_i$ if $e_i M = M$ and $e_j M = 0$ for all $j \neq i$.

Proposition 38.4

Let M be an A-module. Then M has a unique direct sum decomposition $M = M_1 \oplus \cdots \oplus M_r$ where M_i lies in the block A_i for $1 \leqslant i \leqslant r$. In particular, every indecomposable A-module lies in a uniquely determined block of A.

Proof: Let $m \in M$. Then $m = 1_A m = e_1 m + \cdots + e_r m$, so $M = e_1 M + \cdots + e_r M$. Denote $e_i M$ by M_i for $1 \leqslant i \leqslant r$. Suppose that $x \in M_i \cap M_j$ for some $i \neq j$. Then $x = e_i x$ and $x = e_j x$ (because the e_n's act as the identity on their respective blocks for $1 \leqslant n \leqslant r$), so $x = e_i(e_j x) = 0$. Thus the sum is direct. Moreover, $e_i M_i = e_i e_i M = e_i M = M_i$ and $e_j M_i = 0$ for all $j \neq i$, so M_i lies in the block A_i for each $1 \leqslant i \leqslant r$.

Suppose that $M = N_1 \oplus \cdots \oplus N_r$ is another direct sum decomposition of M with N_i in block A_i for $1 \leqslant i \leqslant r$. Then $N_i = e_i N_i \subseteq e_i M = M_i$ (because $N_i \subseteq M$) and hence (since N_i and M_i are indecomposable), $N_i = M_i$ for each $1 \leqslant i \leqslant r$.

The final claim follows immediately from the first. ■

Corollary 38.5

Suppose that an A-module M lies in the block A_i. Then every submodule and factor module of M lies in A_i.

Proof: Let $V \subseteq M$ be a submodule of M. Then for $i \neq j$, $e_j V \subseteq e_j M = 0$ so V must lie in A_i. We also have $e_j(M/V) \subseteq e_j M/e_j V = 0$ so M/V also lies in A_i. ■

Definition 38.6

Let X, Y and Z be A-modules. We say that X is **a non-split extension of Y by Z** iff there exists a non-split exact sequence $0 \to Y \to X \to Z \to 0$.

The following theorem characterises when two modules are in the same block for an algebra over a field.

Theorem 38.7

Let A be an algebra over a field. Let S, T be simple A-modules. The following are equivalent.

(a) S and T lie in the same block of A.

(b) There exist simple A-modules $S = S_1, \ldots, S_m = T$ such that S_i, S_{i+1} are composition factors of the same projective indecomposable A-module for $1 \leqslant i \leqslant m-1$.

(c) There exist simple A-modules $S = S_1, \ldots, S_m = T$ such that there exists a non-split extension of S_i by S_{i+1} (or vice versa) for $1 \leqslant i < m$.

Proof: Omitted. ■

We now return to the notation of the previous chapter, with G a finite group and $(K, \mathcal{O}, k)$ the splitting p-modular system for G given in Notation 36.1.

Remark 38.8 (***Blocks of KG***)

Recall that KG is semisimple since K is of characteristic 0. It follows from Scholium 12.6, Proposition 35.17 and Definition 38.2 that

$$KG = \bigoplus_{\chi \in \mathrm{Irr}(G)} KGe_\chi .$$

In other words, the blocks of KG are labelled by the ordinary irreducible characters $\chi \in \mathrm{Irr}(G)$, and e_χ is the block idempotent for the block KGe_χ.

Remark 38.9 (***Blocks of $\mathcal{O}G$ and kG***)

We know from Proposition 30.3 (d) that there is a bijection between the central idempotents of $\mathcal{O}G$ and the central idempotents of kG. Hence a decomposition $1_{\mathcal{O}G} = b_1 + \cdots + b_r$ of the identity element of $\mathcal{O}G$ into a sum of central primitive idempotents of $\mathcal{O}G$ corresponds to a decomposition $1_{kG} = \overline{b}_1 + \cdots + \overline{b}_r$ of the identity element of kG into a sum of central primitive idempotents of kG. In other words, there is a bijection between the blocks of $\mathcal{O}G$ and the blocks of kG. Note that these are the blocks we are interested in! We sometimes refer to the blocks of kG as the *p-blocks of G*.

Remark 38.10

Let S be a simple kG-module. If S is in a block B of kG then the projective cover P_S of S is also in B, by Corollary 38.5.

Example 18

Let G be a p-group. Then kG has exactly one simple module by Corollary 17.3. Hence by Theroem 38.7, all indecomposable modules lie in the same block, so kG has just one block.

39 Defect Groups

We continue with the splitting p-modular system $(K, \mathcal{O}, k)$ for G. From now on we will only discuss the blocks of kG. Analogous results hold for the corresponding blocks of $\mathcal{O}G$. In this section we will study an important block invariant: the defect group.

> **Top Tip:** It will be helpful to recall the definition of the vertex of a module (Defintion 28.2) before going any further!

Remark 39.1

The blocks of kG can be viewed as indecomposable modules of $k[G \times G]$. First of all, notice that kG is a $k[G \times G]$-module with the action of $G \times G$ on kG given by

$$\begin{aligned}(G \times G) \times kG &\to kG \\ ((g_1, g_2), a) &\mapsto g_1 a g_2^{-1},\end{aligned}$$

linearly extended to an action of $k[G \times G]$. A two-sided ideal of kG is, by definition, a submodule of kG which is closed under left and right multiplication by elements of G. In other words, it is a submodule of kG closed under the action of $G \times G$ as defined above – i.e. a $k[G \times G]$-submodule of kG. Thus a block of kG can be viewed as an indecomposable $k[G \times G]$-submodule of kG considered as a $k[G \times G]$-module.

Notation 39.2

Denote the diagonal embedding of G in $G \times G$ by

$$\begin{aligned}\delta : G &\to G \times G \\ g &\mapsto (g, g).\end{aligned}$$

Theorem 39.3

Let B be a block of kG. Every vertex of B, considered as an indecomposable $k[G \times G]$-module, has the form $\delta(D)$ for a p-subgroup $D \leqslant G$. The group D is uniquely determined up to conjugation in G.

Proof: First we show that the $k[G \times G]$-module B is relatively $\delta(G)$-projective. Since B is a direct summand of kG, it is enough to show that kG is $\delta(G)$-projective. But kG contains the subspace $k.1$, which is the trivial $k\delta(G)$-module. Further, when we consider the dimension of these k-vector spaces we see that

$$\dim_k(kG) = |G| \dim_k(k.1) = |G \times G : \delta(G)| \dim_k(k.1).$$

By arguments in Remark 20.7,

$$\dim_k(k.1)\uparrow_{\delta(G)}^{G\times G} = |G\times G:\delta(G)|\ \dim_k(k.1).$$

Consider the homomorphism $\varphi : k.1 \to kG$ sending $k.1$ to $k.1$. By Proposition 20.8 (the universal property of induction) there then exists a $k[G\times G]$-homomorphism

$$\overline{\varphi} : (k.1)\uparrow_{\delta(G)}^{G\times G} \to kG.$$

Since kG is generated by $k.1$, $\overline{\varphi}$ is surjective. Since the two modules have the same dimension, $\overline{\varphi}$ is an isomorphism and hence $kG \cong (k.1)\uparrow_{\delta(G)}^{G\times G}$. It follows that kG, and therefore B, is $\delta(G)$-projective.

By Definition 28.2, then a vertex of B (still considered as a $k[G\times G]$-module) lies in $\delta(G)$. This vertex is a p-group (Proposition 28.4), and thus is the image $\delta(D)$ of some p-subgroup of G, showing the first part.

We know that $\delta(D)$ is uniquely determined up to conjugacy in $G\times G$. We want to show that D this is unique up to conjugation by elements of G. Suppose that D' is another p-subgroup of G such that $\delta(D')$ is a vertex of B. Then $\delta(D') = {}^{(g_1,g_2)}\delta(D)$ for some $(g_1,g_2)\in G\times G$. If $x\in D$, then ${}^{(g_1,g_2)}(x,x) = ({}^{g_1}x, {}^{g_2}x) \in \delta(D')$. Hence ${}^{g_1}x\in D'$ for all $x\in D$. Since D and D' have the same order, it follows that ${}^{g_1}D = D'$. In particular, D is uniquely determined up to conjugation by elements of G. ■

Definition 39.4

Let B be a block of kG. 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. The defect group of a block is uniquely determined up to G-conjugacy. If a defect group D of B has order p^d then d is called the **defect** of B.

Why are defect groups useful and important? We will shortly see that they measure how far a block is from being semisimple.

Lemma 39.5

Let B be a block of kG with defect group D. Then B is relatively D-projective when thought of as a kG-module via conjugation.

Proof: By definition B is a projective kG-module with the usual module structure given by left multiplication. We can also think of B as a kG-module by linearly extending the conjugation action, $g.x = gxg^{-1}$ for all $x\in B$ and all $g\in G$. Then since $G\cong\delta(G)$, we can define a $k[\delta(G)]$-module structure on B via $(g,g).x = gxg^{-1}$ for all $x\in B$, $(g,g)\in\delta(G)$. Notice that this $k[\delta(G)]$-module is just a restriction of the $k[G\times G]$-module, $B\downarrow_{\delta(G)}^{G\times G}$. We will show that B is relatively $\delta(D)$-projective as a $k[\delta(G)]$-module, and hence via the isomorphism above, B is relatively D-projective when thought of as a kG-module via conjugation.

By the definition of defect groups, $\delta(D)$ is a vertex of B as a $k[G\times G]$-module. Thus B is a direct summand of $V\uparrow_{\delta(D)}^{G\times G}$ for some $k[\delta(D)]$-module V. Hence by restricting to $\delta(G)$ and applying the Mackey formula, we have

$$B\downarrow_{\delta(G)}^{G\times G} \ \mid\ V\uparrow_{\delta(D)}^{G\times G}\downarrow_{\delta(G)}^{G\times G} \cong \bigoplus_{(g_1,g_2)\in[\delta(G)\backslash G\times G/\delta(D)]} \left({}^{(g_1,g_2)}V\downarrow^{{}^{(g_1,g_2)}\delta(D)}_{\delta(G)\cap {}^{(g_1,g_2)}\delta(D)}\right)\uparrow^{\delta(G)}_{\delta(G)\cap {}^{(g_1,g_2)}\delta(D)}.$$

Therefore B, considered as a $k[\delta(G)]$-module, is a sum of induced $k[\delta(G)\cap {}^{(g_1,g_2)}\delta(D)]$-modules for some $g_1,g_2\in G$, and hence is relatively $\delta(G)\cap {}^{(g_1,g_2)}\delta(D)$-projective for some $g_1,g_2\in G$. It is now enough to show that these groups are conjugate in $\delta(G)$ to a subgroup of $\delta(D)$ as this would imply that B is then relatively $\delta(D)$-projective, as required.

Let $(g_1, g_2) \in G \times G$. Any element of $\delta(G) \cap {}^{(g_1,g_2)}\delta(D)$ is of the form ${}^{(g_1,g_2)}\delta(d) = {}^{(g_1,g_2)}(d, d)$ for some $d \in D$ such that $g_1 d g_1^{-1} = g_2 d g_2^{-1}$. Therefore ${}^{(g_1,g_2)}\delta(d) = (g_1 d g_1, g_1 d g_1^{-1}) = \delta(g_1)\delta(d)\delta(g_1)^{-1}$ and this is an element of $\delta(g_1)\delta(D)\delta(g_1)^{-1}$. It follows that $\delta(G) \cap {}^{(g_1,g_2)}\delta(D)$ is conjugate in $\delta(G)$ to a subgroup of $\delta(D)$. ■

Theorem 39.6

Let B be a block of kG with defect group D. Then every indecomposable kG-module in B is relatively D-projective, and hence has a vertex in D.

Proof: As in the previous lemma, we consider B as a kG-module via the conjugation action. Let V be a kG-module with the usual action of G via left multiplication. We define a linear map

$$\begin{aligned} \phi : B \otimes V &\to V \\ x \otimes v &\mapsto xv. \end{aligned}$$

Since $g.(x \otimes v) = gxg^{-1} \otimes gv$ and $\phi(g.(x \otimes v)) = gxg^{-1}gv = gxv = g.(xv)$ for all $x \in B$, $v \in V$ and $g \in G$, the map ϕ is a kG-homomorphism.

On the other hand, let b be the block idempotent of B and define another linear map

$$\begin{aligned} \psi : V &\to B \otimes V \\ v &\mapsto b \otimes v. \end{aligned}$$

For any $g \in G$ and $v \in V$, $\psi(g.v) = b \otimes gv$. But b is central in B and we are considering B as a kG-module via conjugation, so $g.b = b$ and therefore $\psi(g.v) = g.(b \otimes v)$ for all $g \in G$ and $v \in V$. Thus ψ is also a kG-homomorphism.

If the module V lies in the block B, then for any $v \in V$,

$$\phi \circ \psi(v) = \phi(b \otimes v) = bv = v,$$

so $\phi \circ \psi$ is the identity map on V. Therefore ϕ is surjective and ψ is injective, and hence $B \otimes V \cong V \oplus \ker(\phi)$.

In Lemma 39.5 we showed that B is relatively D-projective. It then follows from Exercise 27.8 that $B \otimes V$ is also relatively D-projective, and hence, V is D-projective. In particular, every indecomposable kG-module in B has a vertex in D. ■

Corollary 39.7

Let B be a block of kG with trivial defect groups. Then B is a simple algebra, and in particular, is semisimple.

Proof: If B has trivial defect group $D = 1$, then by Theorem 39.6 every indecomposable kG-module in B is 1-projective, and hence projective. Thus every submodule of a B-module is a direct summand of that B-module. Hence B is semisimple as all its modules are semisimple. But B is an indecomposable algebra by definition. Hence B is simple. ■

We will see later that the converse of this Corollary is also true.

Finally we come to the main theorem of this section. It shows that defect groups are far from arbitrary: defect groups contain every normal p-subgroup of G, and a defect group is a radical p-subgroup of G.

Definition 39.8

Let Q be a p-subgroup of G. If Q is the largest normal p-subgroup of $N_G(Q)$ (i.e. $Q = O_p(N_G(Q))$, then Q is a **radical p-subgroup of** G.

Theorem 39.9

Let B be a block of kG with defect group D.

(a) D contains every normal p-subgroup of G.

(b) D is a radical p-subgroup of G.

Proof: Omitted. ■

Example 19

Let G be a p-group. We already saw that kG has only one block. Then Theorem 39.9 shows that this block has defect group $D = G$.

40 Brauer's Main Theorems

Definition 40.1

Let $H \leqslant G$, let b be a block of kH and let B be a block of kG. Then the block B **corresponds to** b if and only if b, as a $k[H \times H]$-module, is a direct summand of the restriction $B{\downarrow}^{G\times G}_{H\times H}$, *and* B is the unique block of kG with this property. We then write $B = b^G$. If such a B exists, then we say the b^G **is defined**.

We will need the following technical result for the proofs that follow.

Remark 40.2

Let $H \leqslant G$,and let $Q \leqslant H$ be a p-subgroup such that $C_G(Q) \leqslant H$. Note that the restriction $kG{\downarrow}^{G\times G}_{H\times H}$ is a disjoint union of the double H-H-cosets,

$$kG{\downarrow}^{G\times G}_{H\times H} = \bigoplus_{t\in[H\backslash G/H]} kHtH \; = kH \oplus \bigoplus_{t\in[H\backslash G/H], t\notin H} kHtH.$$

Fact: if $t \notin H$ then the $k[H \times H]$-submodule $kHtH$ of kG has no direct summands with vertex containing $\delta(Q)$.

In particular, if X is an indecomposable direct summand of $kG{\downarrow}^{G\times G}_{H\times H}$ with vertex containing $\delta(Q)$, then X is a direct summand of kH, so X is a block of kH.

Proposition 40.3 (*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.

Proof: (a) Let $B := b^G$ and let E be a defect group of B. By the definition of defect groups, $\delta(E)$ is a vertex of the $k[G \times G]$-module B, so B is a direct summand of $V\!\uparrow_{\delta(E)}^{G\times G}$ for some $\delta(E)$-module V. Since b is a direct summand of $B\!\downarrow_{H\times H}^{G\times G}$, it follows from the Mackey formula that b is a direct summand of

$$V\!\uparrow_{\delta(E)}^{G\times G}\downarrow_{H\times H}^{G\times G} = \bigoplus_{x\in[H\times H\backslash G\times G/\delta(E)]} \left(\left({}^{x}V\!\downarrow^{{}^{x}\delta(E)}_{(H\times H)\cap\,{}^{x}\delta(E)}\right)\downarrow^{H\times H}_{(H\times H)\cap\,{}^{x}\delta(E)}\right).$$

Hence b is a direct summand of a module induced from $(H \times H) \cap {}^{x}\delta(E)$, for some $x \in G \times G$. In particular, b is a direct summand of a module induced from a conjugate of a subgroup of $\delta(E)$. Since b has defect group D, $\delta(D)$ is a vertex of b so $\delta(D)$ is minimal such that b is relatively $\delta(D)$-projective. It follows that $\delta(D)$ is conjugate to a subgroup of $\delta(E)$.
Suppose that $(g_1, g_2)\delta(D)(g_1, g_2)^{-1} \leqslant \delta(E)$. Then $g_1 D g_1^{-1} \leqslant E$ and hence $D \leqslant g_1^{-1} E g_1$, which is a defect group of B, showing part (a).

(b) Part (b) follows from the definitions. Since b^N is defined, b is a direct summand of $b^N\!\downarrow_{H\times H}^{N\times N}$, and b^N is the unique such block. Since $(b^N)^G$ is defined, b^N is a direct summand of $(b^N)^G\!\downarrow_{N\times N}^{G\times G}$ and $(b^N)^G$ is the unique such block. Therefore b is a direct summand of $b^N\!\downarrow_{H\times H}^{N\times N}$ which is a direct summand of $(b^N)^G\!\downarrow_{N\times N}^{G\times G}\downarrow_{H\times H}^{N\times N} = (b^N)^G\!\downarrow_{H\times H}^{G\times G}$. However, since b^G is defined, b is also a direct summand of $b^G\!\downarrow_{H\times H}^{G\times G}$, and b^G is the unique such block. Therefore $b^G = (b^N)^G$.

(c) Suppose now that $C_G(D) \leqslant H$. To prove part (c), it is enough to show that b occurs precisely once in a decomposition of $kG\!\downarrow_{H\times H}^{G\times G}$ into indecomposable modules, as then there is a unique indecomposable direct summand of kG (i.e. a block of kG) such that b is a direct summand of the restriction of that summand to $H \times H$.
As in Remark 40.2,

$$kG\!\downarrow_{H\times H}^{G\times G} = kH \oplus \bigoplus_{t\in[H\backslash G/H] t\notin H} kHtH.$$

Now kH is, as a $k[H \times H]$-module, a direct sum of blocks of kH, which are not isomorphic to each other. Thus b is a direct summand of kH with multiplicity one. But b has vertex $\delta(D)$. Remark 40.2 shows that if $t \notin H$ then no direct summand of $kHtH$ has a vertex containing $\delta(D)$. Thus b is not a direct summand of any $kHtH$ for $t \notin H$, so b has multiplicity one in $kG\!\downarrow_{H\times H}^{G\times G}$, as required. ■

We now prove a special case of Brauer's first main theorem. The result holds true for any subgroup N of G containing $N_G(D)$, but we will only consider the case where $N = N_G(D)$ as this situation gives rise to the **Brauer correspondence**.

Theorem 40.4 (*Brauer's First Main Theorem*)

Let $D \leqslant G$ be a p-subgroup and let $N := N_G(D)$. Then $b \mapsto b^G$ defines a bijection between the blocks of kN with defect group D, and the blocks of kG with defect group D.

$$\{\text{ Blocks of } kN \text{ with defect group } D\} \to \{\text{ Blocks of } kG \text{ with defect group } D\}$$
$$b \mapsto b^G$$

In this case we call b^G **the Brauer correspondent** of b.

Proof: Let b be a block of kN with defect group D. Then $\delta(D)$ is a vertex of b considered as a $k[N \times N]$-module. The Green correspondence (Theorem 29.4) shows that there exists a unique indecomposable direct summand $g(b)$ of $b\!\downarrow_{N\times N}^{G\times G}$ with vertex $\delta(D)$. Moreover, by the proof of part (b) of the Green Correspondence, b occurs as a direct summand of $g(b)\!\downarrow_{N\times N}^{G\times G}$ with multiplicity one.

By Proposition 40.3 (c), the block b^G is defined, and hence b^G is the unique indecomposable $k[G\times G]$-module such that b occurs in its restriction to $N \times N$. Therefore $b^G \cong g(b)$ so b^G has vertex $\delta(D)$ when considered as a $k[G \times G]$-module. In particular, b^G has defect group D and so $b \mapsto b^G$ is an injective map from blocks of kN with defect group D, to blocks of kG with defect group D.

We now show that this map is surjective. Suppose B is a block of kG with defect group D. Then B is an indecomposable $k[G \times G]$-module with vertex $\delta(D)$ and the Green correspondence shows that $B\downarrow^{G\times G}_{N\times N}$ has a unique direct summand, $f(B)$, with vertex $\delta(D)$. As B is a direct summand of kG, $B\downarrow^{G\times G}_{N\times N}$ and hence $f(B)$, is a direct summand of $kG\downarrow^{G\times G}_{N\times N}$. In Remark 40.2 we saw that any direct summand of $kG\downarrow^{G\times G}_{N\times N}$ with vertex containing $\delta(D)$ is an indecomposable direct summand of kN. Therefore $f(B)$ is a block of kN with vertex $\delta(D)$ when considered as a $k[N \times N]$-module, so $f(B)$ is a block of kN with defect group D. It follows from part (c) of the Green Correspondence that $B \cong g(f(B))$, and $g(f(B)) \cong f(B)^G$ by the first part of the proof, so the map $b \mapsto b^G$ is surjective. ■

Theorem 40.5 (*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 $b^G = B$.

Proof: First we note that Theorem 39.6 shows that there is a defect group D of b which contains the vertex Q of U. Hence $C_G(D) \leqslant C_G(Q)$, which is contained in H by assumption. Thus by Proposition 40.3 (c), b^G is defined.

Suppose that $B \neq b^G$. Let e be the block idempotent of b so $b = kHe = ekH$. For a kH-module X, Proposition 38.4 shows that there is a decomposition $X = eX \oplus (1-e)X$, where eX lies in b and $(1-e)X$ does not. If $X = Y \oplus Z$ then $eX = eY \oplus eZ$ is still a direct sum. Applying this to the decomposition of kG as a $k[H \times H]$-module as in Remark 40.2, if we fix

$$M := \bigoplus_{t\in[H\backslash G/H] t\notin H} kHtH$$

then

$$ekG = ekH \oplus eM = b \oplus eM$$

as kH-modules. But kG, b and M are all $k[H \times H]$-modules, and e commutes with all elements of H, so we also have $ekG = b \oplus eM$ as $k[H \times H]$-modules.

Now since B is a direct summand of kG, eB is a direct summand of $b \oplus eM$ as $k[H \times H]$-modules. But b is an indecomposable $k[H \times H]$-module and is not a direct summand of $B\downarrow^{G\times G}_{H\times H}$ by assumption, so eB is a direct summand of eM, which is a direct summand of M as $k[H \times H]$-modules. Hence by Remark 40.2, no direct summand of the $k[H \times H]$-module eB has a vertex containing $\delta(Q)$.

By the Mackey formula, the direct summands of $eB\downarrow^{H\times H}_{\delta(H)}$ are induced from subgroups of the form $\delta(H) \cap {}^xT$, where T is a vertex of an indecomposable summand of eB and $x \in H \times H$. It follows that no direct summand of the $k[\delta(H)]$-module $eB\downarrow^{H\times H}_{\delta(H)}$ has a vertex containing $\delta(Q)$. By transport of structure via the isomorphism $H \cong \delta(H)$, we see that eB, considered as a kH-module by conjugation (i.e. with the action of H given by $h.ex = hexh^{-1}$, for all $h \in H$, $x \in B$), has no direct summands with vertex containing Q. Hence by Exercise 27.8, $eB \otimes eV$ also has no direct summands with vertex containing Q. Now since U is a module in b, $eU = U$. By assumption, U is a direct summand of $V\downarrow^G_H$ and this implies that $eU = U$ is a direct summand of eV. Recalling that U has vertex Q, it is then enough to show that eV is a summand of $eB \otimes eV$ as this will give us a contradiction.

Define a map

$$\begin{aligned} \varphi : eV &\to eB \otimes eV \\ v &\mapsto ef \otimes v, \end{aligned}$$

where f is the block idempotent of B (so $B = kGf$). Then for any $h \in H$,

$$\varphi(hv) = ef \otimes hv = hefh^{-1} \otimes hv = h(ef \otimes v) = h\varphi(v),$$

so φ is a kH-homomorphism. Define a second map,

$$\begin{aligned} \psi : eB \otimes eV &\to eV \\ a \otimes v &\mapsto av. \end{aligned}$$

This is also a kH-homomorhpism – for all $h \in H$,

$$\psi(h(a \otimes v)) = \psi(hah^{-1} \otimes hv) = hah^{-1}hv = h(av) = h(\psi(a \otimes v)).$$

Now since V is a module in B, for any $v \in eV$ we have

$$\psi(\varphi(v)) = \psi(ef \otimes v) = efv = ev = v.$$

Hence φ is injective and ψ is surjective and therefore eV is a direct summand of $eB \otimes eV$, as required to give a contradiction. ■

Lemma 40.6

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 $k[G/O_p(G)]$-modules made into kG-modules via the quotient homomorphism $G \to G/O_p(G)$.

Proof: Let $P = O_p(G)$ be the largest normal p-subgroup of G and let S be a simple kG-module. Suppose that W is a simple kP-submodule of S. Then W is the trivial kP-module because P is a p-group. Let

$$C_S(P) := \{s \in S \mid ps = s \text{ for all } p \in P\}.$$

We have $W \leqslant C_S(P)$ so $C_S(P) \neq 0$. But P is normal in G, so $C_S(P)$ is a kG-submodule of S, which was simple, and hence $C_S(P) = S$. In other words, P acts trivially on S. The final claim follows immediately. ■

Corollary 40.7

Let B be a block of kG with defect group D. Then there exists an indecomposable kG-module in B with vertex D.

Proof: Let b be a block of $N := N_G(D)$ with defect group D such that B is the Brauer correspondent of b, as defined in Brauer's First Main Theorem 40.4. As D is a defect group of b, $D = O_p(N)$ by Theorem 39.9 (b). Let S be a simple kN-module in b. It follows from Lemma 40.6 that D acts trivially on S and so S can be thought of as a simple $k[N/D]$-module. Let P_S be the projective cover of S (so P is a $k[N/D]$-module). Corollary 38.5 shows that P_S is also in the block b. We will show that P_S has vertex D and that the Green correspondent of P_S is an indecomposable kG-module in B with vertex D.

Denote the trivial kD-module by k. The module P_S is an indecomposable projective $k[N/D]$-module, so it is a direct summand of the free module $k[N/D] \cong k\uparrow_D^N$. Hence P_S is relatively D-projective. Since $D \trianglelefteq N$, it follows from Clifford's Theorem (Theorem 23.2) that $k\uparrow_D^N\downarrow_D^N$ is a direct sum of N-conjugates of k. In other words $P_S\downarrow_D^N$ is a direct summand of $k\uparrow_D^N\downarrow_D^N$, which is a direct sum of copies of the trivial kD-module k. The vertex of the trivial kD-module k is a Sylow p-subgroup of D, by Proposition 28.4 (c), and thus is equal to D. Therefore the direct summands of $P_S\downarrow_D^N$ all have vertex D. By Exercise 29.3, however, $P_S\downarrow_D^N$ has at least one direct summand with the same vertex as P_S. Hence D is a vertex of P_S.

Now consider P_S as an indecomposable $k[N \times N]$-module and let V be the indecomposable $k[G \times G]$-module with vertex D which is the Green correspondent of P_S. Then by Brauer's First Main Theorem 40.4, V lies in B, so B contains an indecomposable kG-module with vertex D. ■

Our final result shows that the opposite direction of Corollary 39.7 also holds.

Corollary 40.8

A block B of kG is a simple algebra if and only if B has trivial defect groups.

Proof: If B is a block of kG with trivial defect groups then B is a simple algebra by Corollary 39.7.

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 40.7, B has trivial defect groups. ∎

Appendix: The Language of Category Theory

This appendix provides 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.

A Categories

Definition A.1 (*Category*)

A **category** $\mathcal{C}$ consists of:

- a class $\operatorname{Ob}\mathcal{C}$ of **objects**,
- a set $\operatorname{Hom}_{\mathcal{C}}(A, B)$ of **morphisms** for every ordered pair (A, B) of objects, and
- a **composition function**

$$\begin{array}{ccc} \operatorname{Hom}_{\mathcal{C}}(A, B) \times \operatorname{Hom}_{\mathcal{C}}(B, C) & \longrightarrow & \operatorname{Hom}_{\mathcal{C}}(A, C) \\ (f, g) & \mapsto & g \circ f \end{array}$$

  for each ordered triple (A, B, C) of objects,

satisfying the following axioms:

(C1) **Unit axiom**: for each object $A \in \operatorname{Ob}\mathcal{C}$, there exists an **identity morphism** $1_A \in \operatorname{Hom}_{\mathcal{C}}(A, A)$ such that for every $f \in \operatorname{Hom}_{\mathcal{C}}(A, B)$ for all $B \in \operatorname{Ob}\mathcal{C}$,

$$f \circ 1_A = f = 1_B \circ f\,.$$

(C2) **Associativity axiom**: for every $f \in \operatorname{Hom}_{\mathcal{C}}(A, B)$, $g \in \operatorname{Hom}_{\mathcal{C}}(B, C)$ and $h \in \operatorname{Hom}_{\mathcal{C}}(C, D)$ with $A, B, C, D \in \operatorname{Ob}\mathcal{C}$,

$$h \circ (g \circ f) = (h \circ g) \circ f\,.$$

Let us start with some remarks and examples to enlighten this definition:

Remark A.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 A.3

(a) $\mathcal{C} = \mathbf{1}$: category with one object and one morphism (the identity morphism):

$$\begin{tikzcd} \bullet \arrow[loop right, "1_\bullet"] \end{tikzcd}$$

(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:

$$\begin{tikzcd} A \arrow[loop left, "1_A"] \arrow[r] & B \arrow[loop right, "1_B"] \end{tikzcd}$$

(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 A.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 A.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 A.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 $g_1, g_2 \in \mathrm{Hom}_{\mathbf{Rng}}(\mathbb{Q}, C)$

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\iota"] & \mathbb{Q} \arrow[r, shift left, "g_2"] \arrow[r, shift right, "g_1"'] & C \end{tikzcd}$$

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.

B Functors

Definition B.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 B.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 B.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 B.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 B.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 $A, B \in \operatorname{Ob}\mathcal{C}$.

Definition B.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 B.7

The functors $\operatorname{Hom}_R(Q, -)$ and $\operatorname{Hom}_R(-, Q)$ of Example B.4 are both left exact functors. Moreover $\operatorname{Hom}_R(Q, -)$ is exact if and only if Q is projective, and $\operatorname{Hom}_R(-, Q)$ 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
$(K, \mathcal{O}, k)$	p-modular system
$f\vert_S$	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
$M \otimes_R N$	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
$M{\downarrow}^G_H$, $\mathrm{Res}^G_H(M)$	restriction of M from G to H
$M{\uparrow}^H_G$, $\mathrm{Ind}^G_H(M)$	induction of M from H to G
$\mathrm{Inf}^G_{G/N}(M)$	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
A^S, M^S	algebra (resp. module) obtained from A (resp. M) by the extension of scalars to S

Character and Block Theory

b^G	the block of G corresponding to b or the Brauer correspondent of b
$C = D^t D$	Cartan matrix
$\hat{C}_i$	the ith class sum
$\mathrm{Cl}(G)$, $\mathrm{Cl}(G^\circ)$	the class functions on G or G°
$D = (d_{\chi\varphi})_{\chi \in \mathrm{Irr}(G), \varphi \in \mathrm{IBr}(G)}$	decomposition matrix
e_χ	primitive central idempotent corresponding to $\chi \in \mathrm{Irr}(G)$
G°	p-regular elements of G
$\mathrm{Irr}(G)$	ordinary irreducible characters of G
$\mathrm{IBr}(G)$	irreducible Brauer characters of G
χ°	restriction of $\chi \in \mathrm{Irr}(G)$ to G°
χ_{reg}	regular character
ρ_{reg}	regular representation
Φ_φ	projective indecomposable character of $\varphi \in \mathrm{IBr}(G)$
$\langle\ ,\ \rangle : \mathrm{Cl}(G) \times \mathrm{Cl}(G) \to \mathbb{C}$	inner product on class functions of 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

Index