Representation Theory of Finite Groups

with a view towards characteristic zero

Prof. Dr. Caroline Lassueur

Skript zur Vorlesung
WS 24/25 @ Leibniz Universität Hannover
(Vorlesung: 4SWS // Übung: 2SWS)

Module:
Spezialisierung Bachelor Algebra, Zahlentheorie,
Diskrete Mathematik und Wahlmodul Bereich
Reine Mathematik im Master Mathematik

Version: 24th of January 2025

Contents

Foreword

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 and character theory of finite groups** and the **representation theory of semisimple algebras**;
- learn about the **applications** of the latter theory **to finite group theory**, such as for example the proof of Burnside's $p^a q^b$-Theorem.

The exercises mentioned in the text are important for the development of the lecture and the general understanding of the topics. Further exercises can be found in the weekly exercise sheets.

Books and lecture notes which were used to prepare these lecture notes are the following.

Textbooks:

[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.

[Dor71] L. Dornhoff. *Group representation theory. Part A: Ordinary representation theory*. Marcel Dekker, Inc., New York, 1971.

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

[Hup98] B. Huppert. *Character theory of finite groups*. Vol. 25. Walter de Gruyter & Co., Berlin, 1998.

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

[JL01] G. James and M. Liebeck. *Representations and characters of groups*. Second. Cambridge University Press, New York, 2001.

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

[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.

[Ser77] J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977.

[Ser78] J.-P. Serre. *Représentations linéaires des groupes finis*. revised. Hermann, Paris, 1978.

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

Lecture Notes:

[Gec14] M. Geck. *Algebra: Gruppen, Ringe, Körper (mit einer Einführung in die Darstellungstheorie endlicher Gruppen)*. Edition Delkhofen, 2014.

[Kül13] B. Külshammer. *Darstellungstheorie*. 2013. URL: `http://www.minet.uni-jena.de/algebra/skripten/dt/dt-2010/dt.pdf`.

[Mal16] G. Malle. *Characters of finite groups*. Lecture Notes SS 2016, TU Kaiserslautern. 2016.

[Thé05] J. Thévenaz. *Représentations linéaires des groupes finis*. Lecture Notes WS 2004/05, EPFL. 2005.

Acknowledgement: I am grateful to Gunter Malle who provided me with the Skript of his lecture "Charaktertheorie" held at the TU Kaiserslautern in the SS 2015, SS 2016 and SS 2018, which was used as a basis for the development of this lecture. I am also grateful to Birte Johansson and Bernhard Böhmler for reading and commenting a preliminary version of these notes, as well as to Annika Bartelt, Cedric Brendel, Hannah Deuring, Florian Elbrandt, Tamara Linke, Kathrin Kaiser, Helena Petri, Adrian Rettich, Marie Roth, Akshay Sant and Martin Wagner. Further comments, corrections and suggestions are welcome.

Kaiserslautern, January 2025
Caroline Lassueur

Conventions

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

- all groups considered are **finite**;
- all vector spaces considered are **finite-dimensional**;
- 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.
Ordinary Representation Theory

Chapter 1. Linear Representations 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 non-negative integer n.

Notation: throughout this chapter, unless otherwise specified, we let:

- G denote a finite group (in multiplicative notation);
- K denote a field of arbitrary characteristic; and
- V denote a K-vector space such that $\dim_K(V) < \infty$ and $\mathrm{GL}(V) := \mathrm{Aut}_K(V)$ its group of K-automorphisms.

In general, unless otherwise stated, all groups considered are assumed to be finite and all K-vector spaces considered are assumed to be **finite-dimensional**.

1 Linear Representations

Definition 1.1 (*K-representation, matrix representation, faithfullness*)

Let $n \in \mathbb{Z}_{\geqslant 0}$ be a non-negative integer.

(a) A **K-representation** of G (or a **(linear) representation of G (over K)**) of **degree** n is a group homomorphism

$$\rho : G \longrightarrow \mathrm{GL}(V)$$

where V is a K-vector space of dimension n.

(b) A **matrix representation** of G over K of **degree** n is a group homomorphism $R : G \longrightarrow \mathrm{GL}_n(K)$.

An injective (matrix) representation of G over K is called **faithful**.

Remark 1.2

We see at once that both concepts of a representation and of a matrix representation are closely connected.
Recall that every choice of an ordered basis B of V yields a group isomorphism

$$\begin{array}{rccc} \alpha_B : & \mathrm{GL}(V) & \longrightarrow & \mathrm{GL}_n(K) \\ & \varphi & \mapsto & (\varphi)_B \end{array}$$

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 an ordered basis B of V gives rise to a matrix representation of G:

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[dr, dashed, "R_B:=\alpha_B\circ\rho"', "\circlearrowleft"] & \mathrm{GL}(V) \arrow[d, "\alpha_B", "\cong"'] \\ & \mathrm{GL}_n(K)\,. \end{tikzcd}$$

Explicitly, R_B sends an element $g \in G$ to the matrix $\big(\rho(g)\big)_B$ of $\rho(g)$ expressed in the basis B.

Another choice of a K-basis of V yields another matrix representation!!

It is also clear from the diagram that, conversely, any matrix representation $R : G \longrightarrow \mathrm{GL}_n(K)$ gives rise to a K-representation $\rho_B := \alpha_B^{-1} \circ R$ of G.

Throughout the lecture, we will favour the approach using representations rather than matrix representations in order to develop theoretical results. However, matrix representations are essential to carry out computations. Being able to pass back and forth from one approach to the other will be an essential feature.

Also note that Remark 1.2 allows us to transfer terminology/results from representations to matrix representations and conversely. Hence, from now on, in general we make new definitions for representations and use them for matrix representations as well.

Example 1

(a) If G is an arbitrary finite group and $V := K$, 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.
Similarly $\rho : G \longrightarrow \mathrm{GL}(V), g \mapsto \mathrm{Id}_V$ with $\dim_K(V) =: n > 1$ is also a K-representation of G and is called **<u>a</u> trivial representation of G of degree n**.

(b) If G is a subgroup of $\mathrm{GL}(V)$, then the canonical inclusion

$$\begin{array}{ccc} G & \hookrightarrow & \mathrm{GL}(V) \\ g & \mapsto & g \end{array}$$

is a faithful representation of G, called the **tautological representation** of G.

(c) Let $G := S_n$ $(n \geqslant 1)$ be the symmetric group on n letters. Let $\{e_1, \ldots, e_n\}$ 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 the **natural representation** of S_n.

(d) 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 K-vector space 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 the **permutation representation** associated with X.

Notice that (c) is a special case of (d) with $G = S_n$ and $X = \{1, 2, \ldots, n\}$.
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.

We shall see later on in the lecture that K-representations are a special case of a certain *algebraic structure* (in the sense of the lecture *Algebraische Strukturen*). Thus, next, we define the notions that shall correspond to a *homomorphism* and an *isomorphism* of this algebraic structure.

Definition 1.3 (*Homomorphism of representations, equivalent representations*)

Let $\rho_1 : G \longrightarrow \mathrm{GL}(V_1)$ and $\rho_2 : G \longrightarrow \mathrm{GL}(V_2)$ be two K-representations of G, where V_1, V_2 are two finite-dimensional K-vector spaces.

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

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

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

(c) Two matrix representations $R_1, R_2 : G \longrightarrow \mathrm{GL}_n(K)$ are called **equivalent** iff $\exists\ T \in \mathrm{GL}_n(K)$ such that

$$R_2(g) = TR_1(g)T^{-1} \qquad \forall\, g \in G\,.$$

In this case we write $R_1 \sim R_2$.

Remark 1.4

(a) Equivalent representations have the same degree.

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

(c) Consequence: it essentially suffices to study representations up to equivalence (as it essentially suffices to study groups up to isomorphism).

Remark 1.5

If $\rho : G \longrightarrow \mathrm{GL}(V)$ is a K-representation of G and $E := (e_1, \dots, e_n)$, $F := (f_1, \dots, f_n)$ are two ordered bases of V, then by Remark 1.2, we have two matrix representations:

$$\begin{array}{rccc} R_E : & G & \longrightarrow & \mathrm{GL}_n(K) \\ & g & \mapsto & \big(\rho(g)\big)_E \end{array} \quad \text{and} \quad \begin{array}{rccc} R_F : & G & \longrightarrow & \mathrm{GL}_n(K) \\ & g & \mapsto & \big(\rho(g)\big)_F \end{array}$$

These matrix representations are equivalent since $R_F(g) = TR_E(g)T^{-1}\ \forall\, g \in G$, where T is the change-of-basis matrix.

2 Subrepresentations and (Ir)reducibility

Subrepresentations allow us to introduce one of the main notions that will enable us to break representations in elementary pieces in order to simplify their study: the notion of (ir)reducibility.

Definition 2.1 (*G-invariant subspace, irreducibility*)

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

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

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

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

(b) The representation ρ is called **reducible** if V admits a non-trivial proper G-invariant K-subspace $\{0\} \subsetneq W \subsetneq V$, whereas ρ is called **irreducible** if it admits exactly two G-invariant subspaces: $\{0\}$ and V itself.

Notice that V itself and the zero subspace $\{0\}$ are always G-invariant K-subspaces. Moreover, ρ is irreducible if it is not reducible and $V \neq \{0\}$.

Definition 2.2 (*Subrepresentation*)

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

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

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

Remark 2.3

Let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a K-representation and $0 \neq W \subseteq V$ be a G-invariant K-subspace of V. Now choose an ordered basis B' of W and complete it to an ordered basis B of V. Then for each

$g \in G$ the corresponding matrix representation evaluated at g is of the form

$$(\rho(g))_B = \begin{array}{c} \left[\begin{array}{c|c} \big(\rho_W(g)\big)_{B'} & * \\ \hline 0 & * \end{array}\right] \\ \begin{array}{cc} B' & \quad B\setminus B' \end{array} \end{array}.$$

Example 2

(a) Any K-representation of degree 1 is irreducible, for dimension reasons!

(b) Let $\rho : S_n \longrightarrow \mathrm{GL}(K^n)$ be the natural representation of S_n $(n \geqslant 1)$ and let $B := (e_1, \dots, e_n)$ be the standard basis of $V = K^n$. Then for each $g \in G$ we have

$$\rho(g)\Big(\sum_{i=1}^{n} e_i\Big) = \sum_{i=1}^{n} \rho(g)(e_i) = \sum_{i=1}^{n} e_i\,,$$

where the last equality holds because $\rho(g) : \{e_1, \dots, e_n\} \longrightarrow \{e_1, \dots, e_n\}, e_i \mapsto e_{g(i)}$ is a bijection. Thus

$$W := \langle \sum_{i=1}^{n} e_i \rangle_K$$

is an S_n-invariant K-subspace of K^n of dimension 1. It follows that ρ is reducible if $n > 1$.

(c) More generally, the trivial representation of a finite group G is a subrepresentation of any permutation representation of G. [Exercise on Sheet 1]

(d) The symmetric group $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle$ admits the following three pairwise non-equivalent irreducible matrix representations over $\mathbb{C}$:

$$\rho_1 : S_3 \longrightarrow \mathbb{C}^\times, \sigma \mapsto 1$$

i.e. the trivial representation,

$$\rho_2 : S_3 \longrightarrow \mathbb{C}^\times, \sigma \mapsto \mathrm{sign}(\sigma)$$

where $\mathrm{sign}(\sigma)$ denotes the sign of the permutation σ, and

$$\begin{array}{cccc} \rho_3 : & S_3 & \longrightarrow & \mathrm{GL}_2(\mathbb{C}) \\ & (1\ 2) & \mapsto & \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \\ & (1\ 2\ 3) & \mapsto & \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right). \end{array}$$

See [Exercise on Sheet 1].
We will prove later in the lecture that these are all the irreducible $\mathbb{C}$-representations of S_3 up to equivalence.

Properties 2.4

Let $\rho_1 : G \longrightarrow \mathrm{GL}(V_1)$ and $\rho_2 : G \longrightarrow \mathrm{GL}(V_2)$ be two K-representations of G and let $\alpha : V_1 \longrightarrow V_2$ be a G-homomorphism.

(a) If $W \subseteq V_1$ is a G-invariant K-subspace of V_1, then $\alpha(W) \subseteq V_2$ is G-invariant.

(b) If $W \subseteq V_2$ is a G-invariant K-subspace of V_2, then $\alpha^{-1}(W) \subseteq V_1$ is G-invariant.

(c) In particular, $\ker(\alpha)$ and $\mathrm{Im}(\alpha)$ are G-invariant K-subspaces of V_1 and V_2 respectively.

Proof: [Exercise on Sheet 1]. ■

3 Maschke's Theorem

We now come to our first major result in the representation theory of finite groups, namely Maschke's Theorem, which provides us with a criterion for representations to decompose into direct sums of irreducible subrepresentations.

Definition 3.1 (*Direct sum of subrepresentations*)

Let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a K-representation. If $W_1, W_2 \subseteq V$ are two G-invariant K-subspaces such that $V = W_1 \oplus W_2$, then we say that ρ is the **direct sum** of the subrepresentations ρ_{W_1} and ρ_{W_2} and we write $\rho = \rho_{W_1} \oplus \rho_{W_2}$.

Remark 3.2

With the notation of Definition 3.1, if we choose an ordered basis B_i of W_i ($i = 1, 2$) and consider the ordered K-basis $B := B_1 \sqcup B_2$ of V, then the corresponding matrix representation is of the form

$$\big(\rho(g)\big)_B = \begin{array}{c} \left[\begin{array}{c|c} \big(\rho_{W_1}(g)\big)_{B_1} & 0 \\ \hline 0 & \big(\rho_{W_2}(g)\big)_{B_2} \end{array}\right] \\ \begin{array}{cc} B_1 & \qquad B_2 \end{array} \end{array} \qquad \forall\, g \in G\,.$$

The following exercise shows that it is not always possible to decompose representations into direct sums of irreducible subrepresentations.

Exercise 3.3

Let p be an odd prime number, let $G := C_p = \langle g \mid g^p = 1 \rangle$, let $K := \mathbb{F}_p$, and let $V := \mathbb{F}_p^2$ with its canonical basis $B = (e_1, e_2)$. Consider the matrix representation

$$\begin{array}{rccc} R : & G & \longrightarrow & \mathrm{GL}_2(K) \\ & g^b & \mapsto & \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \end{array}.$$

(a) Prove that Ke_1 is G-invariant and deduce that R is reducible.

(b) Prove that there is no direct sum decomposition of V into irreducible G-invariant subspaces.

Theorem 3.4 (Maschke)

Let G be a finite group and let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a K-representation of G. If $\mathrm{char}(K) \nmid |G|$, then every G-invariant K-subspace W of V admits a G-invariant complement in V, i.e. a G-invariant K-subspace $U \subseteq V$ such that $V = W \oplus U$.

Proof: To begin with, choose an arbitrary complement U_0 to W in V, i.e. $V = W \oplus U_0$ as K-vector spaces. (Note that, however, U_0 is possibly not G-invariant!) Next, consider the projection onto W along U_0, that is the K-linear map

$$\pi : V = W \oplus U_0 \longrightarrow W$$

which maps an element $v = w + u$ with $w \in W, u \in U_0$ to w, and define a new K-linear map

$$\begin{array}{rccl} \widetilde{\pi}: & V & \longrightarrow & V \\ & v & \mapsto & \frac{1}{|G|}\sum_{g\in G}\rho(g)\pi\rho(g^{-1})(v)\,. \end{array}$$

Notice that it is allowed to divide by $|G|$ because the hypothesis that $\mathrm{char}(K) \nmid |G|$ implies that $|G| \cdot 1_K$ is invertible in the field K.

We prove the following assertions:

(1) $\mathrm{Im}\,\widetilde{\pi} \subseteq W$: indeed, if $v \in V$, then

$$\widetilde{\pi}(v) = \frac{1}{|G|}\sum_{g\in G} \underbrace{\rho(g)\,\underbrace{\pi\rho(g^{-1})(v)}_{\in W}}_{\in W\ (G\text{-invariance})} \quad \in W\,.$$

(2) $\widetilde{\pi}|_W = \mathrm{Id}_W$: indeed, if $w \in W$, then

$$\widetilde{\pi}(w) = \frac{1}{|G|}\sum_{g\in G} \rho(g)\,\underbrace{\pi\ \underbrace{\rho(g^{-1})(w)}_{\substack{\in W \\ \text{(by G-invariance)}}}}_{\substack{=\rho(g^{-1})(w) \\ \text{(by def. of π)}}} = \frac{1}{|G|}\sum_{g\in G} \underbrace{\rho(g)\rho(g^{-1})}_{\substack{=\rho(gg^{-1}) \\ =\rho(1_G) \\ =\mathrm{Id}_V}}(w) = \frac{1}{|G|}\sum_{g\in G} w = w\,.$$

Thus (1)+(2) imply that $\widetilde{\pi}$ is a projection onto W so that as a K-vector space

$$V = W \oplus \ker(\widetilde{\pi})\,.$$

(3) $\ker(\widetilde{\pi})$ is G-invariant: indeed, for each $h \in G$ we have

$$\begin{aligned} \rho(h) \circ \widetilde{\pi} &= \frac{1}{|G|}\sum_{g\in G} \underbrace{\rho(h)\rho(g)}_{=\rho(hg)}\,\pi\rho(g^{-1}) \\ &= \frac{1}{|G|}\sum_{g\in G} \rho(hg)\pi\rho((hg)^{-1}h) \\ &\overset{s:=hg}{=} \frac{1}{|G|}\sum_{s\in G} \rho(s)\pi\rho(s^{-1}h) \\ &= \Big(\frac{1}{|G|}\sum_{s\in G} \rho(s)\pi\rho(s^{-1})\Big)\rho(h) = \widetilde{\pi} \circ \rho(h)\,. \end{aligned}$$

Hence $\widetilde{\pi}$ is a G-homomorphism and it follows from Property 2.4(c) that its kernel is G-invariant. Therefore we may set $U := \ker(\widetilde{\pi})$ and the claim follows. ■

Definition 3.5 (*Completely reducible/semisimple representation / constituent*)

A K-representation which can be decomposed into a direct sum of irreducible subrepresentations is called **completely reducible** or **semisimple**. In this case, an irreducible subrepresentation occuring in such a decomposition is called a **constituent** of the representation.

Corollary 3.6

If G is a finite group and K is a field such that $\mathrm{char}(K) \nmid |G|$, then every K-representation of G is completely reducible.

Proof: Let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a K-representation of G. W.l.o.g. we may assume $V \neq \{0\}$.

- Case 1: ρ is irreducible $\Rightarrow$ nothing to do ✓.
- Case 2: ρ is reducible. Thus $\dim_K(V) \geqslant 2$ and there exists an irreducible G-invariant K-subspace $0 \neq V_1 \lneq V$. Now, by Maschke's Theorem, there exists a G-invariant complement $U \subseteq V$, i.e. such that $V = V_1 \oplus U$. As $\dim_K(V_1) \geqslant 1$, we have $\dim_K(U) < \dim_K(V)$. Therefore, an induction argument yields the existence of a decomposition
$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r \qquad (r \geqslant 2)$$
of V, where $V_1, \ldots, V_r$ are irreducible G-invariant subspaces. ■

Remark 3.7

(a) The hypothesis of Maschke's Theorem requiring that $\mathrm{char}(K) \nmid |G|$ is always verified if K is a field of characteristic zero. E.g. if $K = \mathbb{C}, \mathbb{R}, \mathbb{Q}, \ldots$

(b) The converse of Maschke's Theorem holds as well. It will be proved later on with more appropriate tools.

(c) In the literature, 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 $\mathrm{char}(K) \mid |G|$.

In Part I of these lecture notes we are going to restrict our attention to *ordinary representation theory* and, most of the time, even assume that K is the field $\mathbb{C}$ of complex numbers.

Exercise 3.8 (*Alternative proof of Maschke's Theorem over the field* $\mathbb{C}$)

Assume $K = \mathbb{C}$ and let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation of G.

(a) Prove that there exists a G-invariant scalar product $\langle\ ,\ \rangle : V \times V \longrightarrow \mathbb{C}$, i.e. such that
$$\langle g.u, g.v\rangle = \langle u, v\rangle \quad \forall\, g \in G, \forall\, u, v \in V\,.$$
[Hint: consider an arbitrary scalar product on V, say $(\ ,\ ) : V \times V \longrightarrow \mathbb{C}$, which is not necessarily G-invariant. Use a sum on the elements of G, weighted by the group order $|G|$, in order to produce a new G-invariant scalar product on V.]

(b) Deduce that every G-invariant subspace W of V admits a G-invariant complement.
[Hint: consider the orthogonal complement of W.]

Chapter 2. The Group Algebra and Its Modules

We now introduce the concept of a KG-module, and show that this more modern approach is equivalent to the concept of a K-representation of a given finite group G. Some of the material in the remainder of these notes will be presented in terms of KG-modules. As we will soon see with our second fundamental result, namely Schur's Lemma, there are several advantages to this approach to representation theory.

Notation: throughout this chapter, unless otherwise specified, we let:

- G denote a finite group;
- K denote a field of arbitrary characteristic; and
- V denote a K-vector space such that $\dim_K(V) < \infty$.

In general, unless otherwise stated, all groups considered are assumed to be finite and all K-vector spaces / modules over the group algebra considered are assumed to be finite-dimensional.

4 Modules over the Group Algebra

Lemma-Definition 4.1 (*Group algebra*)

The **group ring** KG is the ring whose elements are the K-linear combinations $\sum_{g\in G}\lambda_g g$ with $\lambda_g \in K$, 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. In fact KG is a K-vector space with basis G, hence a K-algebra. Thus we usually call KG the **group algebra of G over K** rather than simply *group ring*.

Note: In Definition 4.1, the field K can be replaced with a commutative ring R. E.g. if $R = \mathbb{Z}$, then $\mathbb{Z}G$ is called the *integral group ring* of G.

Proof: By definition KG is a K-vector space 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 to check that KG bears both the structures of a ring and of a K-vector space. Finally, axiom (A3) of K-algebras (see Appendix B) follows directly from the definition of the multiplication and the commutativity of K. ∎

Remark 4.2

Clearly $1_{KG} = 1_G$, $\dim_K(KG) = |G|$, and KG is commutative if and only if G is an abelian group.

Proposition 4.3

(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

$$\begin{array}{rccl} \cdot : & KG \times V & \longrightarrow & V \\ & (\sum_{g\in G} \lambda_g g, v) & \mapsto & (\sum_{g\in G} \lambda_g g) \cdot v := \sum_{g\in G} \lambda_g \rho(g)(v) \ . \end{array}$$

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

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

of the group G.

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

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

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

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

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

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

See [Exercise Sheet 2] for the details (Hint: use the remark below!). ■

Remark 4.4

In fact in Proposition 4.3(a) checking the KG-module axioms is equivalent to checking that for all $g, h \in G$, $\lambda \in K$ and $u, v \in V$:

(1) $(gh) \cdot v = g \cdot (h \cdot v)$;

(2) $1_G \cdot v = v$;

(3) $g \cdot (u + v) = g \cdot u + g \cdot v$;

(4) $g \cdot (\lambda v) = \lambda(g \cdot v) = (\lambda g) \cdot v$,

or in other words, that the binary operation

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

is a *K-linear action of the group G on V*. Indeed, the external multiplication of KG on V is just the extension by K-linearity of the latter map. For this reason, sometimes, KG-modules are also called *G-vector spaces*. See [Exercise Sheet 2] for the details.

Lemma 4.5

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

Proof: If $\rho_1 \sim \rho_2$ and $\alpha : V_1 \longrightarrow V_2$ is a K-isomorphism such that $\rho_2(g) = \alpha \circ \rho_1(g) \circ \alpha^{-1}$ for each $g \in G$, then by Proposition 4.3(a) 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 4.3(b) for each $v \in V_2$ and each $g \in G$ we have

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

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

Remark 4.6 (*Dictionary*)

More generally, through Proposition 4.3, we may transport terminology and properties from KG-modules to K-representations of G and conversely.

This lets us build the following **dictionary**:

Representations		Modules
K-representation of G	$\longleftrightarrow$	KG-module
degree	$\longleftrightarrow$	K-dimension
homomorphism of representations	$\longleftrightarrow$	homomorphism of KG-modules
subrepresentation / G-invariant subspace	$\longleftrightarrow$	KG-submodule
direct sum of representations $\rho_{V_1} \oplus \rho_{V_2}$	$\longleftrightarrow$	direct sum of KG-modules $V_1 \oplus V_2$
irreducible representation	$\longleftrightarrow$	simple (= irreducible) KG-module
the trivial representation	$\longleftrightarrow$	the trivial KG-module K
the regular representation of G	$\longleftrightarrow$	the regular KG-module KG
Corollary 3.6 to Maschke's Theorem:	$\longleftrightarrow$	Corollary 3.6 to Maschke's Theorem:
If $\mathrm{char}(K) \nmid \lvert G\rvert$, then every K-representation of G is completely reducible.		If $\mathrm{char}(K) \nmid \lvert G\rvert$, then every KG-module is semisimple.
...		...

Virtually, any result, we have seen in Chapter 1, can be reinterpreted using this translation table. E.g. Property 2.4(c) tells us that the image and the kernel of homomorphisms of KG-modules are KG-submodules, ...

In this lecture, we introduce the equivalence between representations and modules for the sake of completeness. In the sequel we keep on stating results in terms of representations as much as possible. However, we will use modules when we find them more fruitful. In contrast, the M.Sc. Lecture *Representation Theory* will consistently use the module approach to representation theory.

Exercise 4.7 (*The dual representation*)

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

(a) Prove that the dual space $V^* := \mathrm{Hom}_K(V, K)$ is endowed with the structure of a KG-module via the left action

$$\begin{array}{ccc} G \times V^* & \longrightarrow & V^* \\ (g, f) & \mapsto & g.f \end{array}$$

where $(g.f)(v) := f(g^{-1}v)\ \forall\ v \in V$.

(b) Prove the following assertion using module theoretic arguments: if ρ_V decomposes as a direct sum $\rho_{V_1} \oplus \rho_{V_2}$ of two subrepresentations, then $\rho_{V*} = \rho_{V_1^*} \oplus \rho_{V_2^*}$.

5 Schur's Lemma and Schur's Relations

Schur's Lemma is a basic result concerning simple modules, or in other words irreducible representations. Though elementary to state and prove, it is fundamental to representation theory of finite groups.

Theorem 5.1 (Schur's Lemma)

(a) Let V, W be simple KG-modules. Then the following assertions hold.

(i) Any homomorphism of KG-modules $\varphi : V \longrightarrow V$ is either zero or invertible. In other words $\mathrm{End}_{KG}(V)$ is a skew-field.

(ii) If $V \ncong W$, then $\mathrm{Hom}_{KG}(V, W) = 0$.

(b) If K is an algebraically closed field and V is a simple KG-module, then

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

Notice that here we state Schur's Lemma in terms of modules, rather than in terms of representations, because part (a) holds in greater generality for arbitrary unital associative rings and part (b) holds for finite-dimensional algebras over an algebraically closed field.

Proof:

(a) First, we claim that every $\varphi \in \mathrm{Hom}_{KG}(V, W)\backslash\{0\}$ admits an inverse in $\mathrm{Hom}_{KG}(W, V)$.
Indeed, $\varphi \neq 0 \implies \ker\varphi \subsetneq V$ is a proper KG-submodule of V and $\{0\} \neq \mathrm{Im}\,\varphi$ is a non-zero KG-submodule of W. But then, on the one hand, $\ker\varphi = \{0\}$, because V is simple, hence φ is injective, and on the other hand, $\mathrm{Im}\,\varphi = W$ because W is simple. It follows that φ is also surjective, hence bijective. Therefore, by Properties A.7, φ is invertible with inverse $\varphi^{-1} \in \mathrm{Hom}_{KG}(W, V)$.
Now, (ii) is straightforward from the above. For (i), first recall that $\mathrm{End}_{KG}(V)$ is a ring (see Notation A.8), which is obviously non-zero as $\mathrm{End}_{KG}(V) \ni \mathrm{Id}_V$ and $\mathrm{Id}_V \neq 0$ because $V \neq 0$ since it is simple. Thus, as any $\varphi \in \mathrm{End}_{KG}(V)\backslash\{0\}$ is invertible, $\mathrm{End}_{KG}(V)$ is a skew-field.

(b) Let $\varphi \in \mathrm{End}_{KG}(V)$. Since $K = \overline{K}$, φ has an eigenvalue $\lambda \in K$. Let $v \in V\backslash\{0\}$ be an eigenvector of φ for λ. Then $(\varphi - \lambda \mathrm{Id}_V)(v) = 0$. Therefore, $\varphi - \lambda \mathrm{Id}_V$ is not invertible and

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

Hence $\mathrm{End}_{KG}(V) \subseteq \{\lambda \mathrm{Id}_V \mid \lambda \in K\}$, but the reverse inclusion also obviously holds, proving the claim. ■

Exercise 5.2

Prove that in terms of matrix representations the following statement holds:

Lemma 5.3 (*Schur's Lemma for matrix representations*)

Let $R : G \longrightarrow \mathrm{GL}_n(K)$ and $R' : G \longrightarrow \mathrm{GL}_{n'}(K)$ be two irreducible matrix representations. If there exists $A \in M_{n\times n'}(K)\backslash\{0\}$ such that $AR'(g) = R(g)A$ for every $g \in G$, then $n = n'$ and A is invertible (in particular $R \sim R'$).

The next lemma is a general principle, which we have already used in the proof of Maschke's Theorem, and which allows us to transform K-linear maps into KG-linear maps.

Lemma 5.4

Assume $\mathrm{char}(K) \nmid |G|$. Let V, W be two KG-modules and let $\rho_V : G \longrightarrow \mathrm{GL}(V)$, $\rho_W : G \longrightarrow \mathrm{GL}(W)$ be the associated K-representations. If $\psi : V \longrightarrow W$ is K-linear, then the map

$$\widetilde{\psi} := \frac{1}{|G|} \sum_{g\in G} \rho_W(g) \circ \psi \circ \rho_V(g^{-1})$$

from V to W is KG-linear.

Proof: Same argument as in (3) of the proof of Maschke's Theorem: replace π by ψ and apply the fact that a G-homomorphism between representations corresponds to a KG-hmomorphism between the corresponding KG-modules. ■

Proposition 5.5

Assume $\mathrm{char}(K) \nmid |G|$. Let $\rho_V : G \longrightarrow \mathrm{GL}(V)$ and $\rho_W : G \longrightarrow \mathrm{GL}(W)$ be two irreducible K-representations.

(a) If $\rho_V \nsim \rho_W$ and $\psi : V \longrightarrow W$ is a K-linear map, then

$$\widetilde{\psi} := \frac{1}{|G|} \sum_{g\in G} \rho_W(g) \circ \psi \circ \rho_V(g^{-1}) = 0\,.$$

(b) Assume moreover that $K = \overline{K}$ and $\mathrm{char}(K) \nmid n := \dim_K V$. If $\psi : V \longrightarrow V$ is a K-linear map, then

$$\widetilde{\psi} := \frac{1}{|G|} \sum_{g\in G} \rho_V(g) \circ \psi \circ \rho_V(g^{-1}) = \frac{\mathrm{Tr}(\psi)}{n} \cdot \mathrm{Id}_V \,.$$

Proof: Since ρ_V and ρ_W are irreducible, the associated KG-modules are simple. Moreover, by Lemma 5.4, both in (a) and (b) the map $\widetilde{\psi}$ is KG-linear. Therefore Schur's Lemma yields:

(a) $\widetilde{\psi} = 0$ since $V \not\cong W$.

(b) $\widetilde{\psi} = \lambda \cdot \mathrm{Id}_V$ for some scalar $\lambda \in K$. Therefore, on the one hand

$$\mathrm{Tr}(\widetilde{\psi}) = \frac{1}{|G|} \sum_{g\in G} \underbrace{\mathrm{Tr}\left(\rho_V(g) \circ \psi \circ \rho_V(g^{-1})\right)}_{=\mathrm{Tr}(\psi)} = \frac{1}{|G|}|G|\,\mathrm{Tr}(\psi) = \mathrm{Tr}(\psi)$$

and on the other hand

$$\mathrm{Tr}(\widetilde{\psi}) = \mathrm{Tr}(\lambda \cdot \mathrm{Id}_V) = \lambda\,\mathrm{Tr}(\mathrm{Id}_V) = n \cdot \lambda\,,$$

hence $\lambda = \frac{\mathrm{Tr}(\psi)}{n}$. ■

Next, we see that Schur's Lemma implies certain "orthogonality relations" for the entries of matrix representations.

Theorem 5.6 (Schur's Relations)

Assume $\mathrm{char}(K) \nmid |G|$. Let $Q : G \longrightarrow \mathrm{GL}_n(K)$ and $P : G \longrightarrow \mathrm{GL}_m(K)$ be irreducible matrix representations.

(a) If $P \not\sim Q$, then $\frac{1}{|G|}\sum_{g\in G} P(g)_{ri} Q(g^{-1})_{js} = 0$ for all $1 \leqslant r, i \leqslant m$ and all $1 \leqslant j, s \leqslant n$.

(b) If $K = \overline{K}$ and $\mathrm{char}(K) \nmid n$, then $\frac{1}{|G|}\sum_{g\in G} Q(g)_{ri} Q(g^{-1})_{js} = \frac{1}{n}\delta_{ij}\delta_{rs}$ for all $1 \leqslant r, i, j, s \leqslant n$.

Proof: Set $V := K^n$, $W := K^m$ and let $\rho_V : G \longrightarrow \mathrm{GL}(V)$ and $\rho_W : G \longrightarrow \mathrm{GL}(W)$ be the K-representations induced by Q and P, respectively, as defined in Remark 1.2. Furthermore, consider the K-linear map $\psi : V \longrightarrow W$ whose matrix with respect to the standard bases of $V = K^n$ and $W = K^m$ is the elementary matrix

$$\begin{array}{cc} i & \left[\begin{array}{ccc} & \vdots & \\ \cdots & 1 & \cdots \\ & \vdots & \end{array}\right] \\ & j \end{array} =: E_{ij} \in M_{m\times n}(K)$$

(i.e. the unique nonzero entry of E_{ij} is its (i, j)-entry).

(a) By Proposition 5.5(a),

$$\widetilde{\psi} = \frac{1}{|G|} \sum_{g\in G} \rho_W(g) \circ \psi \circ \rho_V(g^{-1}) = 0$$

because $P \not\sim Q$, and hence $\rho_V \not\sim \rho_W$. In particular the (r, s)-entry of the matrix of $\widetilde{\psi}$ with respect to the standard bases of $V = K^n$ and $W = K^m$ is zero. Thus,

$$0 = \frac{1}{|G|} \sum_{g\in G} \left[P(g)E_{ij}Q(g^{-1})\right]_{rs} = \frac{1}{|G|} \sum_{g\in G} P(g)_{ri} \cdot 1 \cdot Q(g^{-1})_{js}$$

because the unique nonzero entry of the matrix E_{ij} is its (i, j)-entry.

(b) Now we assume that $P = Q$, and hence $n = m$, $V = W$, $\rho_V = \rho_W$. Then by Proposition 5.5(b),

$$\widetilde{\psi} := \frac{1}{|G|} \sum_{g\in G} \rho_V(g) \circ \psi \circ \rho_V(g^{-1}) = \frac{\mathrm{Tr}(\psi)}{n} \cdot \mathrm{Id}_V = \begin{cases} \frac{1}{n} \cdot \mathrm{Id}_V & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Therefore the (r,s)-entry of the matrix of $\widetilde{\psi}$ with respect to the standard basis of $V = K^n$ is

$$\frac{1}{|G|}\sum_{g\in G}\big[Q(g)E_{ij}Q(g^{-1})\big]_{rs} = \begin{cases}\left(\frac{1}{n}\cdot \mathrm{Id}_V\right)_{rs} & \text{if } i=j,\\ 0 & \text{if } i\neq j.\end{cases}$$

Again, because the unique nonzero entry of the matrix E_{ij} is its (i,j)-entry, it follows that

$$\frac{1}{|G|}\sum_{g\in G} Q(g)_{ri}Q(g^{-1})_{js} = \frac{1}{n}\delta_{ij}\delta_{rs}\,.$$

■

6 Representations of Finite Abelian Groups

In this section we give an immediate application of Schur's Lemma encoding the representation theory of finite abelian groups over an algebraically closed field K whose characteristic is coprime to the order of the group.

Proposition 6.1

Assume $K = \overline{K}$ and G is a finite abelian group. Then, the K-dimension of any simple KG-module is equal to 1.

Equivalently: any irreducible K-representation of G has degree 1.

Proof: Let V be a simple KG-module, and let $\rho_V : G \longrightarrow \mathrm{GL}(V)$ be the underlying K-representation (i.e. as given by Proposition 4.3).

Claim: any K-subspace of V is in fact a KG-submodule.

Proof: Fix $g\in G$ and consider $\rho_V(g)$. By definition $\rho_V(g)\in \mathrm{GL}(V)$, hence it is a K-linear endomorphism of V. We claim that it is in fact KG-linear. Indeed, as G is abelian, $\forall\, h\in G$, $\forall\, v\in V$ we have

$$\begin{aligned}\rho_V(g)(h\cdot v) = \rho_V(g)\big(\rho_V(h)(v)\big) &= \big[\rho_V(g)\rho_V(h)\big](v)\\ &= \big[\rho_V(gh)\big](v)\\ &= \big[\rho_V(hg)\big](v)\\ &= \big[\rho_V(h)\rho_V(g)\big](v)\\ &= \rho_V(h)\big(\rho_V(g)(v)\big)\\ &= h\cdot\big(\rho_V(g)(v)\big)\end{aligned}$$

and it follows that $\rho_V(g)$ is KG-linear, i.e. $\rho_V(g)\in \mathrm{End}_{KG}(V)$. Now, because K is algebraically closed, by part (b) of Schur's Lemma, there exists $\lambda_g \in K$ (depending on g) such that

$$\rho_V(g) = \lambda_g\cdot \mathrm{Id}_V\,.$$

As this holds for every $g\in G$, it follows that any K-subspace of V is G-invariant, which in terms of KG-modules means that any K-subspace of V is a KG-submodule of V.

To conclude, as V is simple, we deduce from the Claim that the K-dimension of V must be equal to 1. ■

Theorem 6.2 (Diagonalisation Theorem)

Assume $K = \overline{K}$ and $\mathrm{char}(K) \nmid |G|$. Let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a K-representation of an arbitrary finite group G. Fix $g \in G$. Then, there exists an ordered K-basis B of V with respect to which

$$\big(\rho(g)\big)_B = \begin{bmatrix} \varepsilon_1 & 0 & \cdots & 0 \\ 0 & \varepsilon_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \varepsilon_n \end{bmatrix},$$

where $n := \dim_K(V)$ and each ε_i $(1 \leqslant i \leqslant n)$ is an $o(g)$-th root of unity in K.

Proof: Consider the restriction of ρ to the cyclic subgroup generated by g, that is the representation

$$\rho|_{\langle g\rangle} : \langle g\rangle \longrightarrow \mathrm{GL}(V)\,.$$

By Corollary 3.6 to Maschke's Theorem, we can decompose the representation $\rho|_{\langle g\rangle}$ into a direct sum of irreducible K-representations, say

$$\rho|_{\langle g\rangle} = \rho_{V_1} \oplus \cdots \oplus \rho_{V_n}\,,$$

where $V_1, \ldots, V_n \subseteq V$ are $\langle g\rangle$-invariant. Since $\langle g\rangle$ is abelian $\dim_K(V_i) = 1$ for each $1 \leqslant i \leqslant n$ by Proposition 6.1. Now, if for each $1 \leqslant i \leqslant n$ we choose a K-basis $\{x_i\}$ of V_i, then there exist $\varepsilon_i \in K$ $(1 \leqslant i \leqslant n)$ such that $\rho_{V_i}(g) = \varepsilon_i$ and $B := (x_1, \ldots, x_n)$ is an ordered K-basis of V such that

$$\big(\rho(g)\big)_B = \begin{bmatrix} \varepsilon_1 & 0 & \cdots & 0 \\ 0 & \varepsilon_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \varepsilon_n \end{bmatrix}.$$

Finally, as $g^{o(g)} = 1_G$, it follows that for each $1 \leqslant i \leqslant n$,

$$\varepsilon_i^{o(g)} = \rho_{V_i}(g)^{o(g)} = \rho_{V_i}(g^{o(g)}) = \rho_{V_i}(1_G) = 1_K$$

and hence ε_i is an $o(g)$-th root of unity. ■

Scholium 6.3

Assume $K = \overline{K}$, $\mathrm{char}(K) \nmid |G|$ and G is abelian. If $\rho : G \longrightarrow \mathrm{GL}(V)$ is a K-representation of G, then the K-endomorphisms $\rho(g) : V \longrightarrow V$ with g running through G are simultaneously diagonalisable.

Proof: Same argument as in the previous proof, where we may replace "$\langle g\rangle$" with the whole of G. ■

Exercise 6.4 (*On the existence of faithful representations*)

Prove the following assertions.

(a) The regular $\mathbb{C}$-representation of any finite group is faithful.

(b) Every finite simple group G admits a faithful irreducible $\mathbb{C}$-representation.
[Hint: Decompose the regular representation into a direct sum of irreducible subrepresentations and use (a).]

(c) If $G = C_{n_1} \times \cdots \times C_{n_r}$ is a product of finite cyclic groups of order $n_1, \ldots, n_r$ $(r \in \mathbb{Z}_{>0})$, then G admits a faithful $\mathbb{C}$-representation of degree r.

Chapter 3. Characters of Finite Groups

We now introduce the concept of a ***character*** of a finite group. These are functions $G \longrightarrow \mathbb{C}$, obtained from the representations of the group G by post-composing with the trace map. Characters have many remarkable properties, and they are the fundamental tools for performing computations in representation theory. They encode a lot of information about the group itself and about its representations in a compact and efficient manner.

Notation: throughout this chapter, unless otherwise specified, we let:

- G denote a finite group;
- $K := \mathbb{C}$ be the field of complex numbers; and
- V denote a $\mathbb{C}$-vector space such that $\dim_{\mathbb{C}}(V) < \infty$.

Unless otherwise stated, all groups considered are assumed to be finite and all $\mathbb{C}$-vector spaces / modules over the group algebra considered are assumed to be finite-dimensional.

7 Characters

Definition 7.1 (*Character, linear character*)

Let $\rho_V : G \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation. The **character** of ρ_V is the $\mathbb{C}$-valued function

$$\begin{array}{rccl} \chi_V : & G & \longrightarrow & \mathbb{C} \\ & g & \mapsto & \chi_V(g) := \mathrm{Tr}\left(\rho_V(g)\right) \ . \end{array}$$

We also say that ρ_V (or the associated $\mathbb{C}G$-module V) **affords** the character χ_V. The **degree** of χ_V is the degree of ρ_V. If the degree of χ_V is one, then χ_V is called a **linear** character.

Remark 7.2

(a) Recall that in *linear algebra* the trace of a linear endomorphism φ may be concretely computed by taking the trace of the matrix of φ in a chosen basis of the vector space, and this is independent of the choice of the basis.

Thus to compute characters: choose an ordered basis B of V and obtain $\forall\, g \in G$:

$$\chi_V(g) = \mathrm{Tr}\left(\rho_V(g)\right) = \mathrm{Tr}\left(\left(\rho_V(g)\right)_B\right)$$

(b) For a matrix representation $R : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$, the character of R is then

$$\begin{array}{rccl} \chi_R : & G & \longrightarrow & \mathbb{C} \\ & g & \mapsto & \chi_R(g) := \mathrm{Tr}\left(R(g)\right) \ . \end{array}$$

Example 3

The character of the trivial representation of G is the function $\mathbf{1}_G : G \longrightarrow \mathbb{C}, g \mapsto 1$ and is called **the trivial character** of G.

Lemma 7.3

Equivalent $\mathbb{C}$-representations afford the same character.

Proof: If $\rho_V : G \longrightarrow \mathrm{GL}(V)$ and $\rho_W : G \longrightarrow \mathrm{GL}(W)$ are two $\mathbb{C}$-representations, and $\alpha : V \longrightarrow W$ is an isomorphism of representations, then

$$\rho_W(g) = \alpha \circ \rho_V(g) \circ \alpha^{-1} \quad \forall\, g \in G\,.$$

Now, by the properties of the trace for any two $\mathbb{C}$-endomorphisms β, γ of V we have $\mathrm{Tr}(\beta \circ \gamma) = \mathrm{Tr}(\gamma \circ \beta)$, hence for every $g \in G$ we have

$$\chi_W(g) = \mathrm{Tr}\left(\rho_W(g)\right) = \mathrm{Tr}\left(\alpha \circ \rho_V(g) \circ \alpha^{-1}\right) = \mathrm{Tr}\left(\rho_V(g) \circ \underbrace{\alpha^{-1} \circ \alpha}_{=\mathrm{Id}_V}\right) = \mathrm{Tr}\left(\rho_V(g)\right) = \chi_V(g)\,.$$

■

Terminology / Notation 7.4

- Again, we allow ourselves to transport terminology from representations to characters. For example, if ρ_V is irreducible (faithful, ...), then the character χ_V is also called **irreducible** (**faithful**, ...).
- We define $\mathrm{Irr}(G)$ to be the set of all irreducible characters of G, and $\mathrm{Lin}(G)$ to be the set of all linear characters of G. (We will see below that $\mathrm{Irr}(G)$ is a finite set.)

Properties 7.5 (*Elementary properties*)

Let $\rho_V : G \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation and let $g \in G$. Then the following assertions hold:

(a) $\chi_V(1_G) = \dim_{\mathbb{C}} V$;

(b) $\chi_V(g) = \varepsilon_1 + \ldots + \varepsilon_n$, where $\varepsilon_1, \ldots, \varepsilon_n$ are $o(g)$-th roots of unity in $\mathbb{C}$ and $n = \dim_{\mathbb{C}} V$;

(c) $|\chi_V(g)| \leqslant \chi_V(1_G)$;

(d) $\chi_V(g^{-1}) = \overline{\chi_V(g)}$;

(e) if $\rho_V = \rho_{V_1} \oplus \rho_{V_2}$ is the direct sum of two subrepresentations, then $\chi_V = \chi_{V_1} + \chi_{V_2}$.

Proof:

(a) We have $\rho_V(1_G) = \mathrm{Id}_V$ since representations are group homomorphisms, hence $\chi_V(1_G) = \dim_{\mathbb{C}} V$.

(b) This follows directly from the diagonalisation theorem (Theorem 6.2).

(c) By (b) we have $\chi_V(g) = \varepsilon_1 + \ldots + \varepsilon_n$, where $\varepsilon_1, \ldots, \varepsilon_n$ are roots of unity in $\mathbb{C}$. Hence, applying the triangle inequality repeatedly, we obtain that

$$|\chi_V(g)| = |\varepsilon_1 + \ldots + \varepsilon_n| \leqslant \underbrace{|\varepsilon_1|}_{=1} + \ldots + \underbrace{|\varepsilon_n|}_{=1} = \dim_{\mathbb{C}} V \overset{(a)}{=} \chi_V(1_G)\,.$$

(d) Again by the diagonalisation theorem, there exists an ordered $\mathbb{C}$-basis B of V and $o(g)$-th roots of unity $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{C}$ such that

$$(\rho_V(g))_B = \begin{bmatrix} \varepsilon_1 & 0 & \cdots & 0 \\ 0 & \varepsilon_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \varepsilon_n \end{bmatrix}.$$

Therefore

$$(\rho_V(g^{-1}))_B = \begin{bmatrix} \varepsilon_1^{-1} & 0 & \cdots & 0 \\ 0 & \varepsilon_2^{-1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \varepsilon_n^{-1} \end{bmatrix} = \begin{bmatrix} \overline{\varepsilon_1} & 0 & \cdots & 0 \\ 0 & \overline{\varepsilon_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \overline{\varepsilon_n} \end{bmatrix}$$

and it follows that $\chi_V(g^{-1}) = \overline{\varepsilon_1} + \ldots + \overline{\varepsilon_n} = \overline{\varepsilon_1 + \ldots + \varepsilon_n} = \overline{\chi_V(g)}$.

(e) For $i \in \{1, 2\}$ let B_i be an ordered $\mathbb{C}$-basis of V_i and consider the $\mathbb{C}$-basis $B := B_1 \sqcup B_2$ of V. Then, by Remark 3.2 for every $g \in G$ we have

$$(\rho_V(g))_B = \left[\begin{array}{c|c} \big(\rho_{V_1}(g)\big)_{B_1} & 0 \\ \hline 0 & \big(\rho_{V_2}(g)\big)_{B_2} \end{array}\right],$$

hence $\chi_V(g) = \mathrm{Tr}\,(\rho_V(g)) = \mathrm{Tr}\,(\rho_{V_1}(g)) + \mathrm{Tr}\,(\rho_{V_2}(g)) = \chi_{V_1}(g) + \chi_{V_2}(g)\,.$ ■

Corollary 7.6

Any character of G is a sum of irreducible characters of G.

Proof: By Corollary 3.6 to Maschke's theorem, any $\mathbb{C}$-representation can be written as the direct sum of irreducible subrepresentations. Thus the claim follows from Properties 7.5(e). ■

Exercise 7.7 (*Characters of quotient $\mathbb{C}G$-modules*)

Let V be a $\mathbb{C}G$-module and let $W \leqslant V$ be a $\mathbb{C}G$-submodule. Denote by χ_V, χ_W and $\chi_{V/W}$ the characters afforded by V, W and V/W respectively. Prove that $\chi_V = \chi_W + \chi_{V/W}$.

Notation 7.8

Recall from group theory (e.g. *Algebra I,II* or *Einführung in die Algebra*) that a group G *acts on itself by conjugation* via

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \mapsto & gxg^{-1} =: {}^{g}x\,. \end{array}$$

The orbits of this action are the *conjugacy classes* of G, we denote them by $[x] := \{ {}^g x \mid g \in G\}$, and we write $C(G) := \{[x] \mid x \in G\}$ for the set of all conjugacy classes of G.

The stabiliser of $x \in G$ is its *centraliser* $C_G(x) = \{g \in G \mid {}^g x = x\}$ and the orbit-stabiliser theorem yields

$$|C_G(x)| = \frac{|G|}{|[x]|}\,.$$

Moreover, a function $f : G \longrightarrow \mathbb{C}$ which is constant on each conjugacy class of G, i.e. such that $f(gxg^{-1}) = f(x)\ \forall\, g, x \in G$, is called a **class function** (on G).

Lemma 7.9

Characters are class functions.

Proof: Let $\rho_V : G \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation and let χ_V be its character. Again, because by the properties of the trace we have $\mathrm{Tr}(\beta \circ \gamma) = \mathrm{Tr}(\gamma \circ \beta)$ for all $\mathbb{C}$-endomorphisms β, γ of V, it follows that for all $g, x \in G$,

$$\begin{aligned}\chi_V(gxg^{-1}) = \mathrm{Tr}\left(\rho_V(gxg^{-1})\right) &= \mathrm{Tr}\left(\rho_V(g)\rho_V(x)\rho_V(g)^{-1}\right)\\ &= \mathrm{Tr}\left(\rho_V(x)\underbrace{\rho_V(g)^{-1}\rho_V(g)}_{=\mathrm{Id}_V}\right) = \mathrm{Tr}\left(\rho_V(x)\right) = \chi_V(x)\,.\end{aligned}$$

■

Exercise 7.10 (*Real-valued characters*)

Let $\rho_V : G \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation and let χ_V be its character. Prove the following statements.

(a) If $g \in G$ is conjugate to g^{-1}, then $\chi_V(g) \in \mathbb{R}$.

(b) If $g \in G$ is an element of order 2, then $\chi_V(g) \in \mathbb{Z}$ and $\chi_V(g) \equiv \chi_V(1) \pmod 2$.

(c) Prove or disprove the following claims.

(Claim 1) The character values of the symmetric group S_n are real numbers for all $n \in \mathbb{Z}_{>0}$.

(Claim 2) The character values of the alternating group A_n are real numbers for all $n \in \mathbb{Z}_{>0}$.

8 Orthogonality of Characters

We are now going to make use of results from the linear algebra on the $\mathbb{C}$-vector space of $\mathbb{C}$-valued functions on G in order to develop further fundamental properties of characters.

Notation 8.1

(1) Let $\mathcal{F}(G, \mathbb{C}) := \{f : G \longrightarrow \mathbb{C} \mid f \text{ function}\}$ denote the $\mathbb{C}$-vector space of $\mathbb{C}$-valued functions on G. Clearly $\dim_{\mathbb{C}} \mathcal{F}(G, \mathbb{C}) = |G|$ because $\{\delta_g : G \longrightarrow \mathbb{C}, h \mapsto \delta_{gh} \mid g \in G\}$ is a $\mathbb{C}$-basis.

(2) Let $\mathcal{C}l(G) := \{f \in \mathcal{F}(G, \mathbb{C}) \mid f \text{ is a class function}\}$. This is clearly a $\mathbb{C}$-subspace of $\mathcal{F}(G, \mathbb{C})$ and it is called the **space of class functions on** G. We have $\dim_{\mathbb{C}} \mathcal{C}l(G) = |C(G)|$ as a $\mathbb{C}$-basis of this subspace is given by the set $\{\mathbb{1}_C \mid C \in C(G)\}$ of all indicator functions of the conjugacy

classes of G.

Proposition 8.2

The binary operation

$$\begin{array}{cccc} \langle\,,\,\rangle_G : & \mathcal{F}(G,\mathbb{C})\times\mathcal{F}(G,\mathbb{C}) & \longrightarrow & \mathbb{C} \\ & (f_1,f_2) & \mapsto & \langle f_1,f_2\rangle_G := \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f_2(g)} \end{array}$$

is a scalar product on $\mathcal{F}(G,\mathbb{C})$.

Proof: It is straightforward to check that $\langle\,,\,\rangle_G$ is sesquilinear and Hermitian (Exercise!); it is positive definite because for every $f\in\mathcal{F}(G,\mathbb{C})$,

$$\langle f,f\rangle_G = \frac{1}{|G|}\sum_{g\in G} f(g)\overline{f(g)} = \frac{1}{|G|}\sum_{g\in G}\underbrace{|f(g)|^2}_{\in\mathbb{R}_{\geqslant 0}} \geqslant 0$$

and moreover $\langle f,f\rangle_G = 0$ if and only if $f=0$. ■

Remark 8.3

Obviously, the scalar product $\langle\,,\,\rangle_G$ restricts to a scalar product on $\mathcal{C}l(G)$. Moreover, if f_2 is a character of G, then by Property 7.5(d) we can write

$$\langle f_1,f_2\rangle_G = \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f_2(g)} = \frac{1}{|G|}\sum_{g\in G} f_1(g)f_2(g^{-1})\,.$$

The next theorem is the third key result of this lecture. It tells us that the irreducible characters of a finite group form an orthonormal system in $\mathcal{C}l(G)$ with respect to the scalar product $\langle\,,\,\rangle_G$.

Theorem 8.4 (1st Orthogonality Relations)

If $\rho_V : G \longrightarrow \mathrm{GL}(V)$ and $\rho_W : G\longrightarrow \mathrm{GL}(W)$ are two irreducible $\mathbb{C}$-representations affording the characters χ_V and χ_W respectively, then

$$\langle \chi_V,\chi_W\rangle_G = \frac{1}{|G|}\sum_{g\in G}\chi_V(g)\chi_W(g^{-1}) = \begin{cases} 1 & \text{if } \rho_V\sim\rho_W, \\ 0 & \text{if } \rho_V\not\sim\rho_W. \end{cases}$$

Proof: Choose ordered $\mathbb{C}$-bases $E:=(e_1,\dots,e_n)$ and $F:=(f_1,\dots,f_m)$ of V and W respectively. Then for each $g\in G$ write $Q(g):=\big(\rho_V(g)\big)_E$ and $P(g):=\big(\rho_W(g)\big)_F$. If $\rho_V\not\sim\rho_W$ compute

$$\begin{aligned}\langle \chi_V,\chi_W\rangle_G = \frac{1}{|G|}\sum_{g\in G}\chi_V(g)\chi_W(g^{-1}) &= \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}\big(Q(g)\big)\,\mathrm{Tr}\big(P(g^{-1})\big) \\ &= \frac{1}{|G|}\sum_{g\in G}\Big(\sum_{i=1}^{n} Q(g)_{ii}\Big)\Big(\sum_{j=1}^{m} P(g^{-1})_{jj}\Big) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m}\underbrace{\frac{1}{|G|}\sum_{g\in G} Q(g)_{ii}P(g^{-1})_{jj}}_{=0 \text{ by (a) of Schur's Relations}} = 0\end{aligned}$$

and similarly if $\rho_V \sim \rho_W$, then by Lemma 7.3, we may assume w.l.o.g. that $W = V$, so $P = Q$ and we obtain

$$\langle \chi_V, \chi_V \rangle_G = \sum_{i=1}^{n}\sum_{j=1}^{m} \underbrace{\frac{1}{|G|}\sum_{g\in G} Q(g)_{ii}Q(g^{-1})_{jj}}_{=\frac{1}{n}\delta_{ij}\delta_{ij} \text{ by (b) of Schur's Relations}} = \sum_{i=1}^{n}\frac{1}{n} = 1\,.$$

■

9 Consequences of the 1st Orthogonality Relations

In this section we use the 1st Orthogonality Relations in order to deduce a series of fundamental properties of the (irreducible) characters of finite groups.

Corollary 9.1 (***Linear independence***)

The irreducible characters of G are $\mathbb{C}$-linearly independent.

Proof: Assume $\sum_{i=1}^{s} \lambda_i \chi_i = 0$, where $\chi_1, \dots, \chi_s$ are pairwise distinct irreducible characters of G, $\lambda_1, \dots, \lambda_s \in \mathbb{C}$ and $s \in \mathbb{Z}_{>0}$. Then the 1st Orthogonality Relations yield

$$0 = \langle \sum_{i=1}^{s} \lambda_i \chi_i, \chi_j \rangle_G = \sum_{i=1}^{s} \lambda_i \underbrace{\langle \chi_i, \chi_j \rangle_G}_{=\delta_{ij}} = \lambda_j$$

for each $1 \leqslant j \leqslant s$. The claim follows. ■

Corollary 9.2 (***Finiteness***)

There are at most $|C(G)|$ irreducible characters of G. In particular, there are only a finite number of them.

Proof: By Corollary 9.1 the irreducible characters of G are $\mathbb{C}$-linearly independent. By Lemma 7.9 irreducible characters are elements of the $\mathbb{C}$-vector space $Cl(G)$. Therefore there exists at most $\dim_{\mathbb{C}} Cl(G) = |C(G)| < \infty$ of them. ■

Corollary 9.3 (***Multiplicities***)

Let $\rho_V : G \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation and let $\rho_V = \rho_{V_1} \oplus \cdots \oplus \rho_{V_s}$ be a decomposition of ρ_V into irreducible subrepresentations. Then the following assertions hold.

(a) If $\rho_W : G \longrightarrow \mathrm{GL}(W)$ is an irreducible $\mathbb{C}$-representation of G, then the multiplicity of ρ_W in $\rho_{V_1} \oplus \cdots \oplus \rho_{V_s}$ is equal to $\langle \chi_V, \chi_W \rangle_G$.

(b) This multiplicity is independent of the choice of the chosen decomposition of ρ_V into irreducible subrepresentations.

Proof: (a) W.l.o.g., we may assume that we have chosen the labelling such that

$$\rho_V = \rho_{V_1} \oplus \cdots \oplus \rho_{V_l} \oplus \rho_{V_{l+1}} \oplus \cdots \oplus \rho_{V_s}\,,$$

where $\rho_{V_i}\sim\rho_W\ \forall\ 1\leqslant i\leqslant l$ and $\rho_{V_j}\not\sim\rho_W\ \forall\ l+1\leqslant j\leqslant s$. Thus $\chi_{V_i}=\chi_W\ \forall\ 1\leqslant i\leqslant l$ by Lemma 7.3. Therefore the 1st Orthogonality Relations yield

$$\langle\chi_V,\chi_W\rangle_G=\sum_{i=1}^{l}\langle\chi_{V_i},\chi_W\rangle_G+\sum_{j=l+1}^{s}\langle\chi_{V_j},\chi_W\rangle_G=\sum_{i=1}^{l}\underbrace{\langle\chi_W,\chi_W\rangle_G}_{=1}+\sum_{j=l+1}^{s}\underbrace{\langle\chi_{V_j},\chi_W\rangle_G}_{=0}=l\,.$$

(b) Obvious, since $\langle\chi_V,\chi_W\rangle_G$ depends only on V and W, but not on the chosen decomposition. ■

We can now prove that the converse of Lemma 7.3 holds.

Corollary 9.4 (*Equality of characters*)

Let $\rho_V:G\longrightarrow\mathrm{GL}(V)$ and $\rho_W:G\longrightarrow\mathrm{GL}(W)$ be $\mathbb{C}$-representations with characters χ_V and χ_W respectively. Then,

$$\chi_V=\chi_W\quad\Leftrightarrow\quad\rho_V\sim\rho_W\,.$$

Proof: "$\Leftarrow$": The sufficient condition is the statement of Lemma 7.3.

"$\Rightarrow$": To prove the necessary condition decompose ρ_V and ρ_W into direct sums of irreducible subrepresentations

$$\rho_V=\underbrace{\rho_{V_{1,1}}\oplus\cdots\oplus\rho_{V_{1,m_1}}}_{\text{all }\sim\rho_{V_1}}\oplus\cdots\oplus\underbrace{\rho_{V_{s,1}}\oplus\cdots\oplus\rho_{V_{s,m_s}}}_{\text{all }\sim\rho_{V_s}}\,,$$

$$\rho_W=\underbrace{\rho_{W_{1,1}}\oplus\cdots\oplus\rho_{W_{1,p_1}}}_{\text{all }\sim\rho_{V_1}}\oplus\cdots\oplus\underbrace{\rho_{W_{s,1}}\oplus\cdots\oplus\rho_{W_{s,p_s}}}_{\text{all }\sim\rho_{V_s}}\,,$$

where $m_i,p_i\geqslant 0$ for all $1\leqslant i\leqslant s$ and the ρ_{V_i}'s are pairwise non-equivalent irreducible $\mathbb{C}$-representations of G. (Some of the m_i,p_i's may be zero!) Now, as we assume that $\chi_V=\chi_W$, for each $1\leqslant i\leqslant s$ Corollary 9.3 yields

$$m_i=\langle\chi_V,\chi_{V_i}\rangle_G=\langle\chi_W,\chi_{V_i}\rangle_G=p_i\,,$$

hence $\rho_V\sim\rho_W$. ■

Corollary 9.5 (*Irreducibility criterion*)

A $\mathbb{C}$-representation $\rho_V:G\longrightarrow\mathrm{GL}(V)$ is irreducible if and only if $\langle\chi_V,\chi_V\rangle_G=1$.

Proof: "$\Rightarrow$": holds by the 1st Orthogonality Relations.

"$\Leftarrow$": As in the previous proof, write

$$\rho_V=\underbrace{\rho_{V_{1,1}}\oplus\cdots\oplus\rho_{V_{1,m_1}}}_{\text{all }\sim\rho_{V_1}}\oplus\cdots\oplus\underbrace{\rho_{V_{s,1}}\oplus\cdots\oplus\rho_{V_{s,m_s}}}_{\text{all }\sim\rho_{V_s}}\,,$$

where $m_i\geqslant 1$ for all $1\leqslant i\leqslant s$ and the ρ_{V_i}'s are pairwise non-equivalent irreducible $\mathbb{C}$-representations of G. Then, using the assumption, the sesquilinearity of the scalar product and the 1st Orthogonality Relations, we obtain that

$$1=\langle\chi_V,\chi_V\rangle_G=\sum_{i=1}^{s}m_i^2\underbrace{\langle\chi_{V_i},\chi_{V_i}\rangle_G}_{=1}=\sum_{i=1}^{s}m_i^2\,.$$

Hence, w.l.o.g. we may assume that $m_1=1$ and $m_i=0\ \forall\ 2\leqslant i\leqslant s$, so that $\rho_V=\rho_{V_1}$ is irreducible. ■

Theorem 9.6

The set $\mathrm{Irr}(G)$ is an orthonormal $\mathbb{C}$-basis (w.r.t. $\langle\,,\,\rangle_G$) of the $\mathbb{C}$-vector space $\mathcal{Cl}(G)$ of class functions on G.

Proof: We already know that $\mathrm{Irr}(G)$ is a $\mathbb{C}$-linearly independent set and also that it forms an orthonormal system of $\mathcal{Cl}(G)$ w.r.t. $\langle\,,\,\rangle_G$. Hence it remains to prove that $\mathrm{Irr}(G)$ generates $\mathcal{Cl}(G)$ as a $\mathbb{C}$-vector space. So let $X := \langle \mathrm{Irr}(G)\rangle_{\mathbb{C}}$ be the $\mathbb{C}$-subspace of $\mathcal{Cl}(G)$ generated by $\mathrm{Irr}(G)$. It follows that

$$\mathcal{Cl}(G) = X \oplus X^{\perp}$$

where $X^{\perp}$ denotes the orthogonal of X with respect to the scalar product $\langle\,,\,\rangle_G$. Thus it is enough to prove that $X^{\perp} = 0$. So let $f \in X^{\perp}$, set $\check{f} := \sum_{g\in G} \overline{f(g)}g \in \mathbb{C}G$ and we prove the following assertions:

(1) $\check{f} \in Z(\mathbb{C}G)$ (the centre of $\mathbb{C}G$): let $h \in G$ and compute

$$h\check{f}h^{-1} = \sum_{g\in G} \overline{f(g)}hg\cdot h^{-1} \overset{s:=hgh^{-1}}{=} \sum_{s\in G} \overline{\underbrace{f(h^{-1}sh)}_{=f(s)}}s = \sum_{s\in G} \overline{f(s)}s = \check{f}\,.$$

Hence $h\check{f} = \check{f}h$ and this equality extends by $\mathbb{C}$-linearity to the whole of $\mathbb{C}G$, so that $\check{f} \in Z(\mathbb{C}G)$.

(2) If V is a simple $\mathbb{C}G$-module with character χ_V, then the external multiplication by $\check{f}$ on V is scalar multiplication by $\frac{|G|}{\dim_{\mathbb{C}} V}\langle \chi_V, f\rangle_G \in \mathbb{C}$: first notice that the external multiplication by $\check{f}$ on V, i.e. the map

$$\check{f}\cdot - : V \longrightarrow V, v \mapsto \check{f}\cdot v$$

is $\mathbb{C}G$-linear (i.e. an element of $\mathrm{End}_{\mathbb{C}G}(V)$). Indeed, for each $x \in \mathbb{C}G$ and each $v \in V$ we have

$$\check{f}\cdot(x\cdot v) = (\check{f}x)\cdot v = (x\check{f})\cdot v = x\cdot(\check{f}\cdot v)$$

because $\check{f} \in Z(\mathbb{C}G)$. Therefore, by Schur's Lemma, there exists a scalar $\lambda \in \mathbb{C}$ such that $\check{f}\cdot - = \lambda\,\mathrm{Id}_V$. Now, setting $n := \dim_{\mathbb{C}}(V)$, we have

$$\lambda = \frac{1}{n}\mathrm{Tr}(\lambda\,\mathrm{Id}_V) = \frac{1}{n}\mathrm{Tr}(\check{f}\cdot -) = \frac{1}{n}\sum_{g\in G}\overline{f(g)}\,\underbrace{\mathrm{Tr}\left(\text{mult. by } g \text{ on } V\right)}_{=\chi_V(g)} = \frac{1}{n}\sum_{g\in G}\overline{f(g)}\chi_V(g) = \frac{|G|}{n}\langle \chi_V, f\rangle_G\,.$$

(3) If V is a simple $\mathbb{C}G$-module with character χ_V, then the external multiplication by $\check{f}$ on V is zero: indeed, $\langle \chi_V, f\rangle_G = 0$ because $f \in X^{\perp}$ and the claim follows from (2).

(4) $f = 0$: indeed, as the external multiplication by $\check{f}$ is zero on every simple $\mathbb{C}G$-module, it is zero on every $\mathbb{C}G$-module, because any $\mathbb{C}G$-module can be decomposed as the direct sum of simple submodules by the Corollary to Maschke's Theorem. In particular, the external multiplication by $\check{f}$ is zero on $\mathbb{C}G$. Hence

$$0 = \check{f}\cdot 1_{\mathbb{C}G} = \check{f} = \sum_{g\in G}\overline{f(g)}g$$

and we obtain that $\overline{f(g)} = 0$ for each $g \in G$ because G is a $\mathbb{C}$-basis of $\mathbb{C}G$. But then $f(g) = 0$ for each $g \in G$ and it follows that $f = 0$. ■

The theorem now gives us the precise number of distinct irreducible characters.

Corollary 9.7

The number of pairwise distinct irreducible characters of G is equal to the number of conjugacy classes of G. In other words,

$$|\operatorname{Irr}(G)| = |C(G)|\,.$$

Proof: By Theorem 9.6 the set $\operatorname{Irr}(G)$ is a $\mathbb{C}$-basis of the $\mathbb{C}$-vector space $\mathcal{C}l(G)$ of class functions on G. Hence,

$$|\operatorname{Irr}(G)| = \dim_{\mathbb{C}} \mathcal{C}l(G) = |C(G)|$$

where the second equality holds by Notation 8.1. ■

Corollary 9.8

Let $f \in \mathcal{C}l(G)$. Then the following assertions hold:

(a) $f = \sum_{\chi\in\operatorname{Irr}(G)} \langle f, \chi\rangle_G \, \chi$;

(b) $\langle f, f\rangle_G = \sum_{\chi\in\operatorname{Irr}(G)} \langle f, \chi\rangle_G^2$;

(c) f is a character $\iff \langle f, \chi\rangle_G \in \mathbb{Z}_{\geqslant 0} \ \ \forall\, \chi \in \operatorname{Irr}(G)$; and

(d) $f \in \operatorname{Irr}(G) \iff f$ is a character and $\langle f, f\rangle_G = 1$.

Proof: (a)+(b) hold for any orthonormal basis with respect to a given scalar product.

(c) '$\Rightarrow$': If f is a character, then by Corollary 9.3 the complex number $\langle f, \chi\rangle_G$ is the multiplicity of χ as a constituent of f for each $\chi \in \operatorname{Irr}(G)$, hence a non-negative integer.

'$\Leftarrow$': If for each $\chi \in \operatorname{Irr}(G)$, $\langle f, \chi\rangle_G =: m_\chi \in \mathbb{Z}_{\geqslant 0}$, then f is the character of the representation

$$\rho := \bigoplus_{\chi\in\operatorname{Irr}(G)} \bigoplus_{j=1}^{m_\chi} \rho(\chi)$$

where $\rho(\chi)$ is a $\mathbb{C}$-representation affording the character χ.

(d) The necessary condition is given by the 1st Orthogonality Relations. The sufficient condition follows from (b) and (c). ■

Exercise 9.9 (Character of the dual representation)

(a) Let $\rho_V : G \longrightarrow \operatorname{GL}(V)$ be a $\mathbb{C}$-representation with character χ_V. Prove using character-theoretic arguments that:

(i) the character of the dual $\mathbb{C}$-representation ρ_{V^*} is $\chi_{V^*} = \overline{\chi_V}$;

(ii) ρ_V is irreducible if and only if ρ_{V^*} is;

(iii) if ρ_V decomposes as a direct sum $\rho_{V_1} \oplus \rho_{V_2}$ of two $\mathbb{C}$-subrepresentations, then ρ_{V^*} is equivalent to $\rho_{V_1^*} \oplus \rho_{V_2^*}$.

(b) Determine the duals of the 3 irreducible representations of S_3 given in Example 2(d), up to isomorphism.

Exercise 9.10 (*Change of the base group*)

Let $\varphi : G_2 \longrightarrow G_1$ be a homomorphism of groups between two finite groups G_2 and G_1. Let $\rho : G_1 \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation affording the character χ. Prove the following assertions:

(i) $\chi \circ \varphi$ is a character of G_2, afforded by the $\mathbb{C}$-representation $\rho \circ \varphi$;

(ii) if $\chi \in \mathrm{Irr}(G_1)$ and φ is surjective, then $\chi \circ \varphi \in \mathrm{Irr}(G_2)$.

Show by an example, that $\chi \circ \varphi$ is, in general, not irreducible.

Exercise 9.11 (Dimension of the fixed-point space)

Let V be a $\mathbb{C}G$-module affording the character χ_V. Consider the $\mathbb{C}$-subspace of fixed points under the action of G, that is $V^G := \{v \in V \mid g \cdot v = v \;\forall\, g \in G\}$. Prove that

$$\dim_{\mathbb{C}} V^G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)$$

in two different ways:

1. considering the scalar product of χ_V with the trivial character $\mathbf{1}_G$;
2. seeing V^G as the image of the projector $\pi : V \longrightarrow V, v \mapsto \frac{1}{|G|} \sum_{g\in G} g \cdot v$.

10 The Regular Character

Recall from Example 1(d) that a finite left G-set X gives rise a *permutation representation*

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

where V is a $\mathbb{C}$-vector space with basis $\{e_x \mid x \in X\}$ (i.e. indexed by the set X). Given $g \in G$ write $\mathrm{Fix}_X(g) := \{x \in X \mid g \cdot x = x\}$ for the set of fixed points of g on X.

Proposition 10.1 (*Character of a permutation representation*)

Let X be a G-set and let χ_X denote the character afforded by the associated permutation representation ρ_X. Then

$$\chi_X(g) = |\,\mathrm{Fix}_X(g)| \qquad \forall\, g \in G\,.$$

Proof: Let $g \in G$. The diagonal entries of the matrix of $\rho_X(g)$ expressed in the basis $B := \{e_x \mid x \in X\}$ are:

$$\Big(\big(\rho_X(g)\big)_B\Big)_{xx} = \begin{cases} 1 & \text{if } g \cdot x = x \\ 0 & \text{if } g \cdot x \neq x \end{cases} \qquad \forall\, x \in X\,.$$

Hence taking traces, we get $\chi_X(g) = \sum_{x\in X} \Big(\big(\rho_X(g)\big)_B\Big)_{xx} = |\,\mathrm{Fix}_X(g)|$. ■

For the action of G on itself by left multiplication, by Example 1(d), $\rho_X = \rho_{\mathrm{reg}}$ is the regular representation of G. In this case, we obtain the values of the *regular character*.

Corollary 10.2 (*The regular character*)

Let χ_{reg} denote the character of the regular representation ρ_{reg} of G. Then

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

Proof: This follows immediately from Proposition 10.1 since $\mathrm{Fix}_G(1_G) = G$ and $\mathrm{Fix}_G(g) = \varnothing$ for every $g \in G \backslash \{1_G\}$. ■

Theorem 10.3 (*Decomposition of the regular representation*)

The multiplicity of an irreducible $\mathbb{C}$-representation of G as a constituent of ρ_{reg} equals its degree. In other words,

$$\chi_{\mathrm{reg}} = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi\,.$$

Proof: By Corollary 9.3 we have $\chi_{\mathrm{reg}} = \sum_{\chi\in\mathrm{Irr}(G)} \langle \chi_{\mathrm{reg}}, \chi \rangle_G\, \chi$, where for each $\chi \in \mathrm{Irr}(G)$,

$$\langle \chi_{\mathrm{reg}}, \chi \rangle_G = \frac{1}{|G|} \sum_{g\in G} \underbrace{\chi_{\mathrm{reg}}(g)}_{\substack{=\delta_{1g}|G| \\ \text{by Cor. 10.2}}} \overline{\chi(g)} = \frac{|G|}{|G|}\chi(1) = \chi(1)\,.$$

■

Remark 10.4

The theorem tells us that each irreducible $\mathbb{C}$-representation (considered up to equivalence) occurs with multiplicity at least one in a decomposition of the regular representation into irreducible subrepresentations.

Corollary 10.5 (*Degree formula*)

The order of the group G is given in terms of its irreducible character by the formula

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2\,.$$

Proof: Evaluating the regular character at $1 \in G$ yields

$$|G| = \chi_{\mathrm{reg}}(1) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(1) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2\,.$$

■

Exercise 10.6

Use the degree formula to give a second proof of Proposition 6.1 when $K = \mathbb{C}$. In other words, prove that if G is a finite abelian group, then $\mathrm{Irr}(G) = \mathrm{Lin}(G)$.

Chapter 4. The Character Table

In Chapter 3 we have proved that for any finite group G the equality $|\operatorname{Irr}(G)| = |C(G)| =: r$ holds. Thus the values of the irreducible characters of G can be recorded in an $r \times r$-matrix, called the *character table* of G. The entries of this matrix are related to each other in subtle manners, many of which are encapsulated in the 1st Orthogonality Relations and their consequences, as for example the degree formula. Our aim in this chapter is to develop further tools and methods to compute character tables.

Notation: throughout this chapter, unless otherwise specified, we let:

- G denote a finite group;
- $K := \mathbb{C}$ be the field of complex numbers;
- $|\operatorname{Irr}(G)| = |C(G)| =: r$;
- $\operatorname{Irr}(G) = \{\chi_1, \ldots, \chi_r\}$ denote the set of pairwise distinct irreducible characters of G;
- $C_1 = [g_1], \ldots, C_r = [g_r]$ denote the conjugacy classes of G, where $g_1, \ldots, g_r$ is a fixed set of representatives; and
- we use the convention that $\chi_1 = \mathbf{1}_G$ and $g_1 = 1 \in G$.

In general, unless otherwise stated, all groups considered are assumed to be finite and all $\mathbb{C}$-vector spaces / modules over the group algebra considered are assumed to be finite-dimensional.

11 The Character Table of a Finite Group

Definition 11.1 (*Character table*)

The **character table of** G is the matrix $X(G) := \Big(\chi_i(g_j)\Big)_{ij} \in M_r(\mathbb{C})$.

Example 4 (*The character table of a cyclic group*)

Let $G = \langle g \mid g^n = 1 \rangle$ be cyclic of order $n \in \mathbb{Z}_{>0}$. Since G is abelian,

$$\operatorname{Irr}(G) = \{\text{linear characters of } G\}$$

by Proposition 6.1. Moreover, $|\operatorname{Irr}(G)| = |G| = n$ as each conjugacy class is a singleton:

$$\forall\ 1 \leqslant j \leqslant r = n : \quad C_j = \{g_j\} \text{ and we set } g_j := g^{j-1}.$$

Let ζ be a primitive n-th root of unity in $\mathbb{C}$, so that $\{\zeta^i \mid 1 \leqslant i \leqslant n\}$ are all the n-th roots of unity. Now, each $\chi_i : G \to \mathbb{C}^\times$ is a group homomorphism and is determined by $\chi_i(g)$, which has to be an n-th root of $1_\mathbb{C}$. Therefore, we have n possibilities for $\chi_i(g)$. We set

$$\chi_i(g) := \zeta^{i-1} \quad \forall\, 1 \leqslant i \leqslant n \quad \Rightarrow \quad \chi_i(g^j) = \zeta^{(i-1)j} \quad \forall\, 1 \leqslant i \leqslant n, 0 \leqslant j \leqslant n-1$$

Thus the character table of G is

$$X(G) = \Big(\chi_i(g_j)\Big)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}} = \Big(\chi_i(g^{j-1})\Big)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}} = \Big(\zeta^{(i-1)(j-1)}\Big)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}},$$

which we visualise as follows:

	1	g	g^2	$\dots$	g^{n-1}
$\chi_1 = 1_G$	1	1	1	$\dots$	1
χ_2	1	ζ	ζ^2	$\dots$	ζ^{n-1}
χ_3	1	ζ^2	ζ^4	$\dots$	$\zeta^{2(n-1)}$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
χ_n	1	ζ^{n-1}	$\zeta^{2(n-1)}$	$\dots$	$\zeta^{(n-1)^2}$

Example 5 (*The character table of S_3*)

Let now $G := S_3$ be the symmetric group on 3 letters. Recall from Algebra I/II that the conjugacy classes of S_3 are

$$C_1 = \{\mathrm{Id}\},\ C_2 = \{(1\ 2), (1\ 3), (2\ 3)\},\ C_3 = \{(1\ 2\ 3), (1\ 3\ 2)\}$$

$$\Rightarrow \quad r = 3, |C_1| = 1, |C_2| = 3, |C_3| = 2\,.$$

In Example 2(d) we have exhibited three non-equivalent irreducible matrix representations of S_3, which we denoted ρ_1, ρ_2, ρ_3. For each $1 \leqslant i \leqslant 3$ let χ_i be the character of ρ_i and n_i be its degree, so that $n_1 = n_2 = 1$ and $n_3 = 2$. Hence

$$n_1^2 + n_2^2 + n_3^2 = 6 = |G|\,.$$

Therefore, the degree formula tells us that ρ_1, ρ_2, ρ_3 are all the irreducible matrix representations of S_3, up to equivalence. We note that $n_1 = n_2 = 1$, $n_3 = 2$ is in fact the unique solution (up to relabelling) to the equation given by the degree formula! Taking traces of the matrices in Example 2(d) yields the character table of S_3.

	Id	(1 2)	(1 2 3)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

In the next sections we want to develop further techniques to compute character tables of finite groups, before we come back to further examples of such tables for larger groups.

Exercise 11.2

Compute the character table of the Klein-four group $C_2 \times C_2$ and of $C_2 \times C_2 \times C_2$. Compute the character table of an arbitrary finite abelian group.

12 The 2nd Orthogonality Relations

The 1st Orthogonality Relations provide us with orthogonality relations between the rows of the character table. They can be rewritten as follows in terms of matrices.

Exercise 12.1

Let G be a finite group. Set $X := X(G)$ and

$$C := \begin{bmatrix} |C_G(g_1)| & 0 & \cdots & 0 \\ 0 & |C_G(g_2)| & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & |C_G(g_r)| \end{bmatrix} \in M_r(\mathbb{C})\,.$$

Use the Orbit-Stabiliser Theorem in order to prove that the 1st Orthogonality Relations can be rewritten under the form

$$XC^{-1}\overline{X}^{\mathrm{Tr}} = \mathrm{I}_r\,,$$

where $\overline{X}^{\mathrm{Tr}}$ denotes the transpose of the complex-conjugate $\overline{X}$ of the character table X of G. Deduce that the character table is invertible.

There are also some orthogonality relations between the columns of the character table. These can easily be deduced from the 1st Orthogonality Relations given above in terms of matrices.

Theorem 12.2 (*2nd Orthogonality Relations*)

With the notation of Exercise 12.1 we have

$$X^{\mathrm{Tr}}\overline{X} = C\,.$$

In other words,

$$\sum_{\chi\in\mathrm{Irr}(G)} \chi(g_i)\overline{\chi(g_j)} = \delta_{ij}\frac{|G|}{|[g_i]|} = \delta_{ij}|C_G(g_i)| \qquad \forall\, 1 \leqslant i,j \leqslant r\,.$$

Proof: Taking complex conjugation of the formula given by the 1st Orthogonality Relations (Exercise 12.1) yields:

$$XC^{-1}\overline{X}^{\mathrm{Tr}} = \mathrm{I}_r \qquad \Longrightarrow \qquad \overline{X}C^{-1}X^{\mathrm{Tr}} = \mathrm{I}_r$$

Now, since X is invertible, so are all the matrices in the above equations and hence $X^{\mathrm{Tr}} = \left(\overline{X}C^{-1}\right)^{-1}$. It follows that

$$X^{\mathrm{Tr}}\overline{X} = \left(\overline{X}C^{-1}\right)^{-1}\overline{X} = C\overline{X}^{-1}\overline{X} = C\,.$$

The second formula is now obtained by considering the entry (i,j) in the above matrix equation for all $1 \leqslant i,j \leqslant r$. ∎

Exercise 12.3

Prove that the degree formula can be read off from the 2nd Orthogonality Relations.

13 Tensor Products of Representations and Characters

Tensor products of vector spaces and matrices are recalled/introduced in Appendix C. We are now going to use this construction to build *products* of characters.

Proposition 13.1

Let G and H be finite groups, and let $\rho_V : G \longrightarrow \mathrm{GL}(V)$ and $\rho_W : H \longrightarrow \mathrm{GL}(W)$ be $\mathbb{C}$-representations with characters χ_V and χ_W respectively. Then

$$\begin{array}{rccl} \rho_V \otimes \rho_W : & G \times H & \longrightarrow & \mathrm{GL}(V \otimes_{\mathbb{C}} W) \\ & (g,h) & \mapsto & (\rho_V \otimes \rho_W)(g,h) := \rho_V(g) \otimes \rho_W(h) \end{array}$$

(where $\rho_V(g) \otimes \rho_W(h)$ is the tensor product of the $\mathbb{C}$-endomorphisms $\rho_V(g) : V \longrightarrow V$ and $\rho_W(h) : W \longrightarrow W$ as defined in Lemma-Definition C.4) is a $\mathbb{C}$-representation of $G \times H$, called the **tensor product** of ρ_V and ρ_W, and the corresponding character, which we denote by $\chi_{V \otimes_{\mathbb{C}} W}$, is

$$\chi_{V \otimes_{\mathbb{C}} W} = \chi_V \cdot \chi_W ,$$

where $\chi_V \cdot \chi_W(g,h) := \chi_V(g) \cdot \chi_W(h) \ \forall \ (g,h) \in G \times H$.

Proof: First note that $\rho_V \otimes \rho_W$ is well-defined by Lemma-Definition C.4 and it is a group homomorphism because

$$\begin{aligned} (\rho_V \otimes \rho_W)(g_1 g_2, h_1 h_2)[v \otimes w] &= \big(\rho_V(g_1 g_2) \otimes \rho_W(h_1 h_2)\big)[v \otimes w] \\ &= \rho_V(g_1 g_2)[v] \otimes \rho_W(h_1 h_2)[w] \\ &= \rho_V(g_1) \circ \rho_V(g_2)[v] \otimes \rho_W(h_1) \circ \rho_W(h_2)[w] \\ &= \rho_V(g_1) \otimes \rho_W(h_1)\big[\rho_V(g_2)[v] \otimes \rho_W(h_2)[w]\big] \\ &= \big(\rho_V(g_1) \otimes \rho_W(h_1)\big) \circ \big(\rho_V(g_2) \otimes \rho_W(h_2)\big)[v \otimes w] \\ &= \big(\rho_V \otimes \rho_W\big)(g_1, h_1) \circ \big(\rho_V \otimes \rho_W\big)(g_2, h_2)[v \otimes w] \end{aligned}$$

$\forall \ g_1, g_2 \in G$, $h_1, h_2 \in H$, $v \in V$, $w \in W$. Furthermore, for each $g \in G$ and each $h \in H$,

$$\chi_{V \otimes_{\mathbb{C}} W}(g,h) = \mathrm{Tr}\left((\rho_V \otimes \rho_W)(g,h)\right) = \mathrm{Tr}\left(\rho_V(g) \otimes \rho_W(h)\right) = \mathrm{Tr}\left(\rho_V(g)\right) \cdot \mathrm{Tr}\left(\rho_W(h)\right) = \chi_V(g) \cdot \chi_W(h)$$

by Lemma-Definition C.4, hence $\chi_{V \otimes_{\mathbb{C}} W} = \chi_V \cdot \chi_W$. ■

Remark 13.2

The diagonal inclusion $\iota : G \longrightarrow G \times G, g \mapsto (g,g)$ of G in the product $G \times G$ is a group homomorphism with $\iota(G) \cong G$. Therefore, if $G = H$, then

$$G \xrightarrow{\iota} G \times G \xrightarrow{\chi_V \cdot \chi_W} \mathbb{C}, g \mapsto (g,g) \mapsto \chi_V(g) \cdot \chi_W(g)$$

becomes a character of G, which we also denote by $\chi_V \cdot \chi_W$.

Corollary 13.3

If G and H are finite groups, then $\mathrm{Irr}(G \times H) = \{\chi \cdot \psi \mid \chi \in \mathrm{Irr}(G), \psi \in \mathrm{Irr}(H)\}$.

Proof: [Exercise]. Hint: Use Corollary 9.8(d) and the degree formula. ■

Exercise 13.4

(a) If $\lambda, \chi \in \mathrm{Irr}(G)$ and $\lambda(1) = 1$, then $\lambda \cdot \chi \in \mathrm{Irr}(G)$.

(b) The set $\mathrm{Lin}(G) = \{\chi \in \mathrm{Irr}(G) \mid \chi(1) = 1\}$ of linear characters of a finite group G forms a group for the product of characters.

14 Normal Subgroups and Inflation

Whenever a group homomorphism $G \longrightarrow H$ and a representation of H are given, we obtain a representation of G by composition. In particular, we want to apply this principle to normal subgroups $N \trianglelefteq G$ and the corresponding quotient homomorphism, which we always denote by $\pi : G \longrightarrow G/N, g \mapsto gN$.

We will see that by this means, copies of the character tables of quotient groups of G all appear in the character table of G. This observation, although straightforward, will allow us to fill out the character table of a group very rapidly, provided it possesses normal subgroups.

Definition 14.1 (*Inflation*)

Let $N \trianglelefteq G$ and let $\pi : G \longrightarrow G/N, g \mapsto gN$ be the quotient homomorphism. Given a $\mathbb{C}$-representation $\rho : G/N \longrightarrow \mathrm{GL}(V)$, we set

$$\mathrm{Inf}_{G/N}^{G}(\rho) := \rho \circ \pi : G \longrightarrow \mathrm{GL}(V)\,.$$

This is a $\mathbb{C}$-representation of G (see Exercise 9.10), called the **inflation of ρ from G/N to G**.

Note that some texts also call $\mathrm{Inf}_{G/N}^{G}(\rho)$ the *lift* or the *restriction* of ρ along π.

Remark 14.2

(a) If the character afforded by ρ is χ, then by Exercise 9.10(i), the character afforded by $\mathrm{Inf}_{G/N}^{G}(\rho)$ is $\mathrm{Inf}_{G/N}^{G}(\chi) := \chi \circ \pi$. We also call it the **inflation of χ from G/N to G**. Clearly, the values of $\mathrm{Inf}_{G/N}^{G}(\chi)$ are given by the formula

$$\mathrm{Inf}_{G/N}^{G}(\chi)(g) = \chi(gN) \qquad \forall\, g \in G\,.$$

(b) By Exercise 9.10(iii), if ρ (resp. χ) is irreducible, then so is $\mathrm{Inf}_{G/N}^{G}(\rho)$ (resp. $\mathrm{Inf}_{G/N}^{G}(\chi)$).

Exercise 14.3

Let $N \trianglelefteq G$ and let $\rho : G/N \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation of G/N. Compute the kernel of $\mathrm{Inf}_{G/N}^{G}(\rho)$ provided that ρ is faithful.

Definition 14.4 (*Kernel of a character*)

The **kernel of a character** χ of G is $\ker(\chi) := \{g \in G \mid \chi(g) = \chi(1)\}$.

Example 6

(a) $\chi = \mathbf{1}_G$ the trivial character $\Rightarrow \ker(\chi) = G$.

(b) $G = S_3$, $\chi = \chi_2$ the sign character $\Rightarrow \ker(\chi) = C_1 \cup C_3 = \langle (123) \rangle$; whereas $\ker(\chi_3) = \{1\}$. (See Example 5.)

Lemma 14.5

Let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation of G affording the character ψ. Then $\ker(\psi) = \ker(\rho)$, thus it is a normal subgroup of G.

Proof: [Exercise] ■

Theorem 14.6

Let $N \trianglelefteq G$. Then

$$\begin{array}{rccl} \mathrm{Inf}^G_{G/N} : & \{\text{characters of } G/N\} & \longrightarrow & \{\text{characters } \psi \text{ of } G \mid N \leqslant \ker(\psi)\} \\ & \chi & \mapsto & \mathrm{Inf}^G_{G/N}(\chi) \end{array}$$

is a bijection and so is its restriction to the irreducible characters

$$\begin{array}{rccl} \mathrm{Inf}^G_{G/N} : & \mathrm{Irr}(G/N) & \longrightarrow & \{\psi \in \mathrm{Irr}(G) \mid N \leqslant \ker(\psi)\} \\ & \chi & \mapsto & \mathrm{Inf}^G_{G/N}(\chi)\,. \end{array}$$

Proof: First we prove that the first map is well-defined and bijective.

- Let χ be a character of G/N. By Remark 14.2, N is in the kernel of $\mathrm{Inf}^G_{G/N}(\chi)$, hence the first map is well-defined.
- Now let ψ be a character of G with $N \leqslant \ker(\psi)$ and assume ψ is afforded by the $\mathbb{C}$-representation $\rho : G \longrightarrow \mathrm{GL}(V)$.

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[d, two heads, "\pi"'] & \mathrm{GL}(V) \\ G/N \arrow[ur, dashed, "\exists!\,\widetilde{\rho}"'] \arrow[ur, phantom, bend left, "\circlearrowleft"] & \end{tikzcd}$$

By Lemma 14.5 we have $\ker(\psi) = \ker(\rho) \geqslant N$. Therefore, by the universal property of the quotient, ρ induces a unique $\mathbb{C}$-representation $\widetilde{\rho} : G/N \longrightarrow \mathrm{GL}(V)$ with the property that $\widetilde{\rho} \circ \pi = \rho$.

Letting χ be the character afforded by $\widetilde{\rho}$, it follows that $\rho = \mathrm{Inf}^G_{G/N}(\widetilde{\rho})$ and $\psi = \mathrm{Inf}^G_{G/N}(\chi)$. Thus the 1st map is surjective. Its injectivity is clear (e.g. by Remark 14.2).

The second map is well-defined by the above and Exercise 14.3(a). It is injective because it is just the restriction of the 1st map to the $\mathrm{Irr}(G/N)$, whereas it is surjective by the same argument as above as the constructed representation $\widetilde{\rho}$ is clearly irreducible if ρ is, as $\widetilde{\rho} \circ \pi = \rho$. ■

Exercise 14.7

Let G be a finite group. Prove that if $N \trianglelefteq G$, then

$$N = \bigcap_{\substack{\chi \in \mathrm{Irr}(G) \\ N \subseteq \ker(\chi)}} \ker(\chi)\,.$$

It follows immediately from the above exercise that the lattice of normal subgroups of G can be read off from its character table. The theorem also implies that it can be read off from the character table, whether the group is abelian or simple.

Corollary 14.8

(a) Inflation from the abelianization induces a bijection

$$\mathrm{Inf}_{G/G'}^{G} : \mathrm{Irr}(G/G') \xrightarrow{\sim} \mathrm{Lin}(G) \ .$$

In particular, G has precisely $|G : G'|$ linear characters.

(b) The group G is abelian if and only if all its irreducible characters are linear.

Proof:

(a) First, we claim that if $\psi \in \mathrm{Lin}(G)$, then G' is in its kernel. Indeed, if $\psi(1) = 1$, then $\psi : G \longrightarrow \mathbb{C}^\times$ is a group homomorphism. Therefore, as $\mathbb{C}^\times$ is abelian,

$$\psi([g,h]) = \psi(ghg^{-1}h^{-1}) = \psi(g)\psi(h)\psi(g)^{-1}\psi(h)^{-1} = \psi(g)\psi(g)^{-1}\psi(h)\psi(h)^{-1} = 1$$

for all $g, h \in G$, and hence $G' = \langle [g,h] \mid g,h \in G\rangle \leqslant \ker(\chi)$. In addition, any irreducible character of G/G' is linear by Proposition 6.1 because G/G' is abelian. Thus Theorem 14.6 yields a bijection

$$\mathrm{Irr}(G/G') = \mathrm{Lin}(G/G') \xrightarrow[\mathrm{Inf}_{G/G'}^{G}]{\sim} \{\psi \in \mathrm{Irr}(G) \mid G' \leqslant \ker(\psi)\} = \mathrm{Lin}(G),$$

as required.

(b) The group G is abelian if and only if $G/G' = G$, which happens if and only if $\mathrm{Inf}_{G/G'}^{G} = \mathrm{Id}$. Hence, the claim follows from (a). ■

Corollary 14.9

A finite group G is simple $\iff \chi(g) \neq \chi(1)\ \forall\, g \in G\backslash\{1\}$ and $\forall\, \chi \in \mathrm{Irr}(G)\backslash\{\mathbf{1}_G\}$.

Proof: [Exercise] ■

Exercise 14.10

Compute the complex character table of the alternating group A_4 through the following steps:

1. Determine the conjugacy classes of A_4 (there are 4 of them) and the corresponding centraliser orders.
2. Determine the degrees of the 4 irreducible characters of A_4.
3. Determine the linear characters of A_4.
4. Determine the non-linear character of A_4 using the 2nd Orthogonality Relations.

To finish this section we show how to compute the character table of the symmetric group S_4 combining several of the techniques we have developed in this chapter.

Example 7 (***The character table of S_4***)

Again, the conjugacy classes of S_4 are given by the cycle types. We fix

$$C_1 = \{\mathrm{Id}\},\ C_2 = [(1\ 2)],\ C_3 = [(1\ 2\ 3)],\ C_4 = [(1\ 2)(3\ 4)],\ C_5 = [(1234)]$$

$$\Rightarrow \quad r = 5,\ |C_1| = 1,\ |C_2| = 6,\ |C_3| = 8,\ |C_4| = 3,\ |C_5| = 6\,.$$

Hence, $|\operatorname{Irr}(G)| = |C(G)| = 5$ and as always we may assume that $\chi_1 = \mathbf{1}_G$ is the trivial character.

Recall that $V_4 = \{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq S_4$ with $S_4/V_4 \cong S_3$ (seeAlgebra!). Therefore, by Theorem 14.6 we can "inflate" the character table of $S_4/V_4 \cong S_3$ to S_4 (see Example 5 for the character table of S_3). This provides us with three irreducible characters χ_1, χ_2 and χ_3 of S_4:

	Id	(1 2)	(1 2 3)	(1 2)(3 4)	(1 2 3 4)
$\lvert C_G(g_i)\rvert$	24	4	3	8	4
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	−1	2	0
χ_4	·	·	·	·	·
χ_5	·	·	·	·	·

Here we have computed the values of χ_2 and χ_3 using Remark 14.2 as follows:

- Inflation preserves degrees, hence it follows from Example 5 that $\chi_2(\mathrm{Id}) = 1$ and $\chi_3(\mathrm{Id}) = 2$. (Up to relabelling!)
- As $C_4 = [(1\ 2)(3\ 4)] \subseteq V_4$, $(1\ 2)(3\ 4) \in \ker(\chi_i)$ for $i = 2, 3$ and hence $\chi_2((1\ 2)(3\ 4)) = 1$ and $\chi_3((1\ 2)(3\ 4)) = 2$.
- By Remark 14.2 the values of χ_2 and χ_3 at (1 2) and (1 2 3) are given by the corresponding values in the character table of S_3. (Here it is enough to argue that the isomorphism between S_4/V_4 and S_3 must preserve orders of elements, hence also the cycle type in this case.)
- Finally, we compute that $\overline{(1\ 2\ 3\ 4)} = \overline{(1\ 2)} \in S_4/V_4$, hence $\chi_i((1\ 2\ 3\ 4)) = \chi_i((1\ 2))$ for $i = 2, 3$.

Therefore, it remains to compute χ_4 and χ_5. To begin with the degree formula yields

$$\sum_{i=1}^{5} \chi_i(\mathrm{Id})^2 = 24 \quad\Longrightarrow\quad \chi_4(\mathrm{Id})^2 + \chi_5(\mathrm{Id})^2 = 18 \quad\Longrightarrow\quad \chi_4(\mathrm{Id}) = \chi_5(\mathrm{Id}) = 3\,.$$

Next, the 2nd Orthogonality Relations applied to the 3rd column with itself read

$$\sum_{i=1}^{5} \chi_i((1\ 2\ 3))\overline{\chi_i((1\ 2\ 3))} = \sum_{i=1}^{5} \chi_i((1\ 2\ 3))\chi_i((1\ 2\ 3)^{-1}) = |C_G((1\ 2\ 3))| = 3\,,$$

hence $1 + 1 + 1 + \chi_4((1\ 2\ 3))^2 + \chi_5(1\ 2\ 3))^2 = 3$ and it follows that $\chi_4((1\ 2\ 3)) = \chi_5((1\ 2\ 3)) = 0$. Similarly, the 2nd Orthogonality Relations applied to the 2nd column with itself / the 4th column with itself and the 5th column with itself yield that all other entries squared are equal to 1, hence all other entries are ± 1.

The 2nd Orthogonality Relations applied to the 1st and 2nd columns give the 2nd column, i.e. $\chi_4((1\ 2)) = 1$ and $\chi_5((1\ 2)) = -1$ (up to swapping χ_4 and χ_5).
Then the 1st Orthogonality Relations applied to the 3rd and the 4th row yield

$$0 = \sum_{k=1}^{5} \frac{1}{|C_G(g_k)|}\chi_3(g_k)\overline{\chi_4(g_k)} = \frac{6}{24} + \frac{1}{4}\chi_4((1\ 2)(3\ 4)) \;\Rightarrow\; \chi_4((1\ 2)(3\ 4)) = -1\,.$$

Similar with the 3rd row and the 5th row: $\chi_5((1\ 2)(3\ 4)) = -1$. Finally the 1st Orthogonality Relations applied to the 1st and the 4th (resp. 5th) row yield $\chi_4((1\ 2\ 3\ 4)) = -1$ (resp. $\chi_5((1\ 2\ 3\ 4)) = 1$). Thus the character table of S_4 is:

	Id	(1 2)	(1 2 3)	(1 2)(3 4)	(1 2 3 4)
$\|C_G(g_i)\|$	24	4	3	8	4
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	-1	1

Remark 14.11

Two non-isomorphic groups can have the same character table. E.g.: Q_8 and D_8, but $Q_8 \not\cong D_8$. Thus, the character table does not determine:

- the group up to isomorphism;
- the full lattice of subgroups;
- the orders of elements.
- . . .

Exercise 14.12

Compute the character tables of D_8 and Q_8.

[Hint: In each case, determine the commutator subgroup and deduce that there are 4 linear characters.]

Exercise 14.13 (*The determinant of a representation*)

If $\rho : G \longrightarrow \mathrm{GL}(V)$ is a $\mathbb{C}$-representation of G and $\det : \mathrm{GL}(V) \longrightarrow \mathbb{C}^*$ denotes the determinant homomorphism, then we define a linear character of G via

$$\det_\rho := \det \circ \rho : G \longrightarrow \mathbb{C}^*\,,$$

called the **determinant** of ρ. Prove that, although the finite groups D_8 and Q_8 have the same character table, they can be distinguished by considering the determinants of their irreducible $\mathbb{C}$-representations.

Exercise 14.14

Prove the following assertions:

(a) If G is a non-abelian simple group (or more generally if G is perfect, i.e. $G = [G, G]$), then the image $\rho(G)$ of any $\mathbb{C}$-representation $\rho : G \longrightarrow \mathrm{GL}(V)$ is a subgroup of $\mathrm{SL}(V)$.

(b) No simple group G has an irreducible character of degree 2.

Assume that G is simple and $\rho : G \longrightarrow \mathrm{GL}_2(\mathbb{C})$ is an irreducible matrix representation of G with character χ and proceed as follows:

1. Prove that ρ is faithful and G is non-abelian.
3. Determine the determinant $\det_\rho$ of ρ.
4. Prove that $|G|$ is even and G admits an element x of order 2.
5. Prove that $\langle x \rangle \lhd G$ and conclude that assertion (b) holds.

Chapter 8. Central Characters and Class Multiplication Constants

Notation: throughout this chapter, unless otherwise specified, we let:

- G denote a finite group;
- $K := \mathbb{C}$ be the field of complex numbers;
- $\mathrm{Irr}(G)$ denote the set of pairwise distinct irreducible characters of G, which we view as an ordered r-tuple;
- $C(G)$ denotes a set of representatives for the conjugacy classes of G, which we view as an ordered r-tuple.

In general, unless otherwise stated, all groups considered are assumed to be finite and all $\mathbb{C}$-vector spaces / modules over the group algebra considered are assumed to be finite-dimensional.

15 Class Sums and Central Characters

We now extend representations/characters of finite groups to "representations/characters" of the centre of the group algebra $\mathbb{C}G$ in order to obtain further results on character values.

Definition 15.1 (*Class sums*)

The elements $\widehat{C} := \sum_{g\in C} g \in \mathbb{C}G$ where C runs through $C(G)$ are called the **class sums** of G.

Lemma 15.2

The set $\{\widehat{C} \mid C \in C(G)\}$ of all class sums is a $\mathbb{C}$-basis of $Z(\mathbb{C}G)$. In other words, we have $Z(\mathbb{C}G) = \bigoplus_{C\in C(G)} \mathbb{C}\widehat{C}$.

Proof: Notice that the class sums are clearly $\mathbb{C}$-linearly independent in the group algebra $\mathbb{C}G$ because the group elements are. Hence, the sum $\bigoplus_{C\in C(G)} \mathbb{C}\widehat{C}$ is indeed direct in $\mathbb{C}G$ and it is enough to prove that this direct sum is equal to $Z(\mathbb{C}G)$.

'$\supseteq$': First we observe that for each $C \in C(G)$ and each $g \in G$, we have

$$g \cdot \widehat{C} = g(g^{-1}\widehat{C}g) = \widehat{C} \cdot g\,.$$

Extending by $\mathbb{C}$-linearity, we get $a \cdot \widehat{C} = \widehat{C} \cdot a \;\; \forall\; C \in C(G)$ and $\forall\; a \in \mathbb{C}G$, proving that $\bigoplus_{C\in C(G)} \mathbb{C}\widehat{C} \subseteq Z(\mathbb{C}G)$.

'$\subseteq$': Let $a \in Z(\mathbb{C}G)$ and write $a = \sum_{g\in G} \lambda_g g$ with $\{\lambda_g\}_{g\in G} \subseteq \mathbb{C}$. Since a is central, for every $h \in G$, we have

$$\sum_{g\in G} \lambda_g g = a = hah^{-1} = \sum_{g\in G} \lambda_g (hgh^{-1})$$

and comparing coefficients yields $\lambda_g = \lambda_{hgh^{-1}}\ \forall\ g, h \in G$. Namely, the coefficients λ_g are constant on the conjugacy classes of G, say equal to λ_C on the conjugacy class $C \in C(G)$. It follows that

$$a = \sum_{C\in C(G)} \lambda_C \widehat{C} \in \bigoplus_{C\in C(G)} \mathbb{C}\widehat{C}\,.$$

■

Notation 15.3 (*Central characters*)

If $\chi \in \mathrm{Irr}(G)$, then we may consider a $\mathbb{C}$-representation affording χ, say

$$\rho^{\chi} : G \longrightarrow \mathrm{GL}(\mathbb{C}^{n(\chi)}) = \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}^{n(\chi)})$$

with $n(\chi) := \chi(1)$. This group homomorphism extends by $\mathbb{C}$-linearity to a $\mathbb{C}$-algebra homomorphism

$$\begin{array}{rccc} \widetilde{\rho}^{\chi}: & \mathbb{C}G & \longrightarrow & \mathrm{End}_{\mathbb{C}}(\mathbb{C}^{n(\chi)}) \\ & a = \sum_{g\in G} \lambda_g g & \mapsto & \widetilde{\rho}^{\chi}(a) = \sum_{g\in G} \lambda_g \rho^{\chi}(g)\,. \end{array}$$

Now, if $z \in Z(\mathbb{C}G)$, then for each $g \in G$, we have

$$\widetilde{\rho}^{\chi}(z)\widetilde{\rho}^{\chi}(g) = \widetilde{\rho}^{\chi}(zg) = \widetilde{\rho}^{\chi}(gz) = \widetilde{\rho}^{\chi}(g)\widetilde{\rho}^{\chi}(z)\,,$$

so, as we have already seen in Chapter 2 on Schur's Lemma, this means that $\widetilde{\rho}^{\chi}(z)$ is $\mathbb{C}G$-linear. This holds in particular if z is a class sum. Therefore, by Schur's Lemma, for each $C \in C(G)$ there exists a uniquely determined scalar $\omega_{\chi}(\widehat{C}) \in \mathbb{C}$ such that

$$\widetilde{\rho}^{\chi}(\widehat{C}) = \omega_{\chi}(\widehat{C}) \cdot \mathrm{Id}_{\mathbb{C}^{n(\chi)}}\,.$$

The functions defined by

$$\begin{array}{rccc} \omega_{\chi}: & Z(\mathbb{C}G) & \longrightarrow & \mathbb{C} \\ & \widehat{C} & \mapsto & \omega_{\chi}(\widehat{C}) \end{array}$$

(where χ runs through $\mathrm{Irr}(G)$) and extended by $\mathbb{C}$-linearity to the whole of $Z(\mathbb{C}G)$ are homomorphisms of $\mathbb{C}$-vector spaces, called the **central characters** of $\mathbb{C}G$ (or simply of G). In §16 below, we prove they are indeed unital homomorphisms of $\mathbb{C}$-algebras.

Remark 15.4

If $z \in Z(G)$, then $[z] = \{z\}$ and therefore the corresponding class sum is z itself. Therefore, we may see the functions $\omega_{\chi}|_{Z(G)} : Z(G) \longrightarrow \mathbb{C}$ as $\mathbb{C}$-representations of $Z(G)$ of degree 1, or equivalently as linear characters of $Z(G)$.

16 Class Multiplication Constants

We now prove that the central characters are not just $\mathbb{C}$-linear, but indeed unital homomorphisms of $\mathbb{C}$-algebras.

Definition 16.1 (*Class multiplication constant*)

Given three conjugacy classes $C, D, E \in \mathcal{C}(G)$, the **class multiplication constant** associated to the triple (C, D, E) is the non-negative integer

$$m_{CDE} := |\{(c,d) \in C \times D \mid cd = x\}|\,,$$

where x is a fixed element of E.

The next lemma shows that the integer m_{CDE} does not depend on the choice of $x \in E$.

Lemma 16.2

Let $C, D, E \in \mathcal{C}(G)$. Then, the following assertions hold:

(a) $|\{(c,d) \in C \times D \mid cd = x\}| = |\{(c,d) \in C \times D \mid cd = y\}| \qquad \forall\, x, y \in E\,,$

(b) if $E = \{1_G\}$, then $m_{CDE} = \begin{cases} 0 & \text{if } D \neq C^{-1}\,, \\ |C| & \text{if } D = C^{-1}\,. \end{cases}$

Proof:

(a) Since x, y belong to the same conjugacy class of G, there exists $g \in G$ such that $y = gxg^{-1}$. Furthermore, as the conjugation isomorphism

$$\begin{array}{rccc} \gamma_g : & G & \longrightarrow & gGg^{-1} = G \\ & u & \mapsto & xux^{-1} \end{array}$$

restricts to bijections $\gamma_g|_C : C \xrightarrow{\sim} C$ and $\gamma_g|_D : D \xrightarrow{\sim} D$, certainly the map

$$\begin{array}{ccc} \{(c,d) \in C \times D \mid cd = x\} & \longrightarrow & \{(e,f) \in C \times D \mid ef = \gamma_g(x)\} \\ (c,d) & \mapsto & (\gamma_g|_C(c), \gamma_g|_D(d)) \end{array}$$

is a bijection.

(b) If $E = \{1_G\}$, then $m_{CDE} := |\{(c,d) \in C \times D \mid cd = 1_G\}|$. Hence, the latter set can only contain pairs $(c,d) \in C \times D$ such that $d = c^{-1}$ and the formula follows. ■

Lemma 16.3

For any $C, D \in \mathcal{C}(G)$, in the group algebra $\mathbb{C}G$ we have

$$\widehat{C} \cdot \widehat{D} = \sum_{E \in \mathcal{C}(G)} m_{CDE} \widehat{E}\,.$$

Proof: By definition

$$\widehat{C} \cdot \widehat{D} = \Big(\sum_{c \in C} c\Big) \cdot \Big(\sum_{d \in D} d\Big) = \sum_{(c,d) \in C \times D} cd$$

and for each $E \in C(G)$ a fixed element $e \in E$ occurs precisely m_{CDE} times in this sum by Definition 16.1. Moreover, by Lemma 16.2(a), each element of such an E occurs with the same multiplicity. Hence, we get

$$\sum_{(c,d)\in C\times D} cd = \sum_{E\in C(G)} \big(m_{CDE} \sum_{e\in E} e\big) = \sum_{E\in C(G)} m_{CDE}\widehat{E}\,,$$

as required. ■

In practice, the values of the central characters are calculated using the following formulae.

Proposition 16.4 (*Central characters and class multiplication constants*)

Let $\chi \in \mathrm{Irr}(G)$. Let $C, D, E \in C(G)$, let $c \in C$ and let $z_1, z_2 \in Z(\mathbb{C}G)$. Then, the following assertions hold:

(a) $\omega_\chi(\widehat{C}) = \frac{|C|}{\chi(1)}\chi(c)$;

(b) $\omega_\chi(1_{Z(\mathbb{C}G)}) = 1_{\mathbb{C}}$;

(c) $\omega_\chi(\widehat{C}) \cdot \omega_\chi(\widehat{D}) = \sum_{E\in C(G)} m_{CDE} \cdot \omega_\chi(\widehat{E}) = \omega_\chi(\widehat{C} \cdot \widehat{D})$;

(d) $\omega_\chi(z_1 \cdot z_2) = \omega_\chi(z_1) \cdot \omega_\chi(z_2)$.

In particular, the central character $\omega_\chi : Z(\mathbb{C}G) \longrightarrow \mathbb{C}$ associated to χ is a unital homomorphism of $\mathbb{C}$-algebras.

Proof: Let $\rho^\chi : G \longrightarrow \mathrm{GL}(\mathbb{C}^{n(\chi)})$ be a $\mathbb{C}$-representation affording χ.

(a) It follows from Notation 15.3 that

$$\chi(1)\omega_\chi(\widehat{C}) = \mathrm{Tr}\left(\widetilde{\rho}^\chi(\widehat{C})\right) = \mathrm{Tr}\big(\sum_{g\in C} \rho^\chi(g)\big) = \sum_{g\in C} \mathrm{Tr}\left(\rho^\chi(g)\right) = \sum_{g\in C} \chi(g) = |C|\chi(c)\,,$$

where the last equality holds because characters are class functions. The claim follows.

(b) It is clear that $1_{Z(\mathbb{C}G)} = 1_{\mathbb{C}G} = 1_G = \widehat{C_1}$, where we let C_1 denote the conjugacy class of the neutral element of G. Now, it is clear that $\widetilde{\rho}^\chi(\widehat{C_1}) = \widetilde{\rho}^\chi(1_G) = \rho^\chi(1_G) = \mathrm{Id}_{\mathbb{C}^{n(\chi)}}$. Thus, it follows from the definition that

$$\omega_\chi(1_{Z(\mathbb{C}G)}) = \omega_\chi(\widehat{C_1}) = 1_{\mathbb{C}}\,.$$

(c) By Notation 15.3 and Lemma 16.3, we have

$$\begin{aligned}
\big(\omega_\chi(\widehat{C}) \cdot \omega_\chi(\widehat{D})\big) \cdot \mathrm{Id}_{\mathbb{C}^{n(\chi)}} &= \omega_\chi(\widehat{C}) \cdot \mathrm{Id}_{\mathbb{C}^{n(\chi)}} \cdot \omega_\chi(\widehat{D}) \cdot \mathrm{Id}_{\mathbb{C}^{n(\chi)}} \\
&= \widetilde{\rho}^\chi(\widehat{C})\widetilde{\rho}^\chi(\widehat{D}) \\
&= \widetilde{\rho}^\chi(\widehat{C} \cdot \widehat{D}) \\
&= \widetilde{\rho}^\chi\big(\sum_{E\in C(G)} m_{CDE}\widehat{E}\big) \\
&= \sum_{E\in C(G)} m_{CDE}\widetilde{\rho}^\chi(\widehat{E}) \\
&= \sum_{E\in C(G)} m_{CDE}\,\omega_\chi(\widehat{E}) \cdot \mathrm{Id}_{\mathbb{C}^{n(\chi)}} \\
&= \big(\sum_{E\in C(G)} m_{CDE}\,\omega_\chi(\widehat{E})\big) \cdot \mathrm{Id}_{\mathbb{C}^{n(\chi)}}\,,
\end{aligned}$$

proving that $\omega_\chi(\widehat{C})\cdot\omega_\chi(\widehat{D}) = \sum_{E\in C(G)} m_{CDE}\cdot\omega_\chi(\widehat{E})$. Now, as ω_χ is $\mathbb{C}$-linear by definition, we obtain that

$$\Big(\sum_{E\in C(G)} m_{CDE}\,\omega_\chi(\widehat{E})\Big)\cdot \mathrm{Id}_{\mathbb{C}^{n(\chi)}} = \omega_\chi\Big(\sum_{E\in C(G)} m_{CDE}\widehat{E}\Big) = \omega_\chi(\widehat{C}\cdot\widehat{D})\,.$$

(d) Since the set of all class sums of G form a $\mathbb{C}$-basis of $Z(\mathbb{C}G)$ by Lemma 15.2, it suffices to prove that ω_χ is multiplicative on the latter set. Thus, the claim follows from (c).

Finally, we observe that (b) and (d) prove that ω_χ is a unital homomorphism of $\mathbb{C}$-algebras. ■

Exercise 16.5

Prove that the 2nd Orthogonality Relations follow from Proposition 16.4 and Lemma 16.2.
[Hint: For $\chi\in\mathrm{Irr}(G)$ and $g,h\in G$, first express $\chi(g)\overline{\chi(h)}$ in function of the class multiplication constants. Then sum over $\mathrm{Irr}(G)$.]

Proposition 16.6

For any $C,D,E\in C(G)$, we have

$$m_{CDE} = \frac{|C|\cdot|D|}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(c)\chi(d)\chi(e^{-1})}{\chi(1)}$$

where $c\in C$, $d\in D$ and $e\in E$.

Proof: Let $\chi\in\mathrm{Irr}(G)$, let $C,D,E\in C(G)$ and let $c\in C$, $d\in D$ and $e\in E$. Then,

$$\omega_\chi(\widehat{C})\cdot\omega_\chi(\widehat{D}) = \sum_{E\in C(G)} m_{CDE}\cdot\omega_\chi(\widehat{E})$$

by Proposition 16.6(c). Thus, plugging in the formula of Proposition 16.6(a), we obtain

$$\frac{|C|}{\chi(1)}\chi(c)\cdot\frac{|D|}{\chi(1)}\chi(d) = \sum_{F\in C(G)} m_{CDF}\frac{|F|}{\chi(1)}\chi(g_F)$$

where for each $F\in C(G)$, $g_F\in F$ is a fixed element. Multiplying by $\chi(1)\cdot\chi(e^{-1})$ yields

$$\frac{|C|\cdot|D|}{\chi(1)}\chi(c)\cdot\chi(d)\cdot\chi(e^{-1}) = \sum_{F\in C(G)} m_{CDF}|F|\chi(g_F)\cdot\chi(e^{-1})$$

and summing over $\mathrm{Irr}(G)$ and applying the 2nd Orthogonality Relations yields

$$|C|\cdot|D|\cdot\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(c)\chi(d)\chi(e^{-1})}{\chi(1)} = \sum_{F\in C(G)} m_{CDF}|F|\cdot\underbrace{\sum_{\chi\in\mathrm{Irr}(G)}\chi(g_F)\cdot\chi(e^{-1})}_{=\delta_{EF}\frac{|G|}{|F|}}$$
$$= m_{CDE}|G|$$

as only the term for $F=E$ is non-zero. The claim follows. ■

Theorem 16.7

The class multiplication constants of a finite group G are determined by the character table of G, and vice versa, the character table of G is determined by the class multiplication constants of G.

Proof: It follows from Proposition 16.6 that the class multiplication constants can be computed from the character table. Conversely, we need to prove that $X(G)$ can be computed from the class multiplication constants. We describe below **Burnside's Algorithm**. To begin with, given $C \in C(G)$, we set

$$\mathcal{M}_C := \big(m_{CDE}\big)_{\substack{D\in C(G)\\ E\in C(G)}} \in M_r(\mathbb{C})\,.$$

Next, given $\chi \in \mathrm{Irr}(G)$, the vector $e_\chi := (\omega_\chi(\widehat{E}))_{E\in C(G)} \in \mathbb{C}^r$ satisfies

$$\mathcal{M}_C \cdot e_\chi = \Big(\sum_{E\in C(G)} m_{CDE}\,\omega_\chi(\widehat{E})\Big)_{D\in C(G)} = \big(\omega_\chi(\widehat{C})\cdot\omega_\chi(\widehat{D})\big)_{D\in C(G)} = \omega_\chi(\widehat{C})\cdot e_\chi\,,$$

where the second equality holds by Proposition 16.4(c). Thus, it follows that the vector e_χ is an eigenvector of $\mathcal{M}_C$ for the eigenvalue $\omega_\chi(\widehat{C})$. (In fact, e_χ is a common eigenvector of the matrices $\mathcal{M}_C$ for C running through $C(G)$.)

Clearly, $\{e_\chi \in \mathbb{C}^r \mid \chi \in \mathrm{Irr}(G)\}$ is a $\mathbb{C}$-basis of $\mathbb{C}^r$. Thus, each eigenspace of $\mathcal{M}_C$ is generated by some of these vectors. Next, we intersect these eigenspaces with the eigenspaces of $\mathcal{M}_D$ for all $D \neq C$ in $C(G)$. The non-trivial intersections are $\mathbb{C}$-subspaces of the form

$$U_\chi := \{u \in \mathbb{C}^r \mid \mathcal{M}_D \cdot u = \omega_\chi(\widehat{D})\cdot u \ \forall\, D \in C(G)\} \leqslant \mathbb{C}^r$$

for some $\chi \in \mathrm{Irr}(G)$. Observe that for all pairs of irreducible characters $\chi, \psi \in \mathrm{Irr}(G)$ there exists a class sum $\widehat{C}$ such that $\omega_\chi(\widehat{C}) \neq \omega_\psi(\widehat{C})$. Thus, it follows that the sum $\sum_{\chi\in\mathrm{Irr}(G)} U_\chi$ is direct and so for dimension reasons we obtain that $U_\chi = \langle e_\chi\rangle_{\mathbb{C}}$.

Now fix $\chi \in \mathrm{Irr}(G)$. For $C_1 := [1_G]$, we have $\omega_\chi(\widehat{C_1}) = 1$, so the vector e_χ can be computed from U_χ, and hence from the class multiplication constants. By the first Orthogonality Relations there exists a unique vector e_{χ_0}, the coefficients of which are all positive integers. This vector is must be associated to the trivial character and so we obtain the cardinalities of the conjugacy classes as $|C| = \omega_{1_G}(\widehat{C})$ for all $C \in C(G)$, from the class multiplication constants. Furthermore, we have

$$\frac{|G|}{\chi(1)^2} = \frac{|G|}{\chi(1)^2}\langle\chi,\chi\rangle_G = \frac{1}{\chi(1)^2}\sum_{g\in G}|\chi(g)|^2 = \frac{1}{\chi(1)^2}\sum_{C\in C(G)}|C|\cdot\Big|\frac{\omega_\chi(\widehat{C})\chi(1)}{|C|}\Big|^2 = \sum_{C\in C(G)}\frac{|\omega_\chi(\widehat{C})|^2}{|C|}$$

where the second equality holds by definition of the scalar product and the third equality follows from Proposition 16.4(a). This formula yields the degree $\chi(1)$ in terms of the class multiplication constants. The remaining values of χ are then obtained via the formula from Proposition 16.4(a) again, i.e. for $C \in C(G)$ and $c \in C$, we have

$$\chi(c) = \frac{\chi(1)\omega_\chi(\widehat{C})}{|C|}\,.$$

By the above $\chi(1)$, $\omega_\chi(\widehat{C})$ and $|C|$ can all already be computed from the class multiplication constants, as required. ■

Chapter 5. Integrality and Theorems of Burnside's

The main aim of this chapter is to prove *Burnside's p^aq^b theorem*, which provides us with a solubility criterion for finite groups of order p^aq^b with p, q prime numbers, which is extremely hard to prove by purely group theoretic methods. To reach this aim, we need to develop techniques involving the integrality of character values and further results of Burnside's on the vanishing of character values.

Notation: throughout this chapter, unless otherwise specified, we let:

- G denote a finite group;
- $K := \mathbb{C}$ be the field of complex numbers;
- $\mathrm{Irr}(G) := \{\chi_1, \dots, \chi_r\}$ denote the set of pairwise distinct irreducible characters of G;
- $C_1 = [g_1], \dots, C_r = [g_r]$ denote the conjugacy classes of G, where $g_1, \dots, g_r$ is a fixed set of representatives; and
- we use the convention that $\chi_1 = \mathbf{1}_G$ and $g_1 = 1 \in G$.

In general, unless otherwise stated, all groups considered are assumed to be finite and all $\mathbb{C}$-vector spaces / modules over the group algebra considered are assumed to be finite-dimensional.

17 Algebraic Integers and Character Values

First we investigate the algebraic nature of character values.

Recall: (See Appendix D for details.)
An element $b \in \mathbb{C}$ which is integral over $\mathbb{Z}$ is called an *algebraic integer*. In other words, $b \in \mathbb{C}$ is an algebraic integer if b is a root of a monic polynomial $f \in \mathbb{Z}[X]$.
Algebraic integers have the following properties:

- The integers are clearly algebraic integers.
- Roots of unity are algebraic integers, as they are roots of polynomials of the form $X^m - 1 \in \mathbb{Z}[X]$.
- The algebraic integers form a subring of $\mathbb{C}$. In particular, sums and products of algebraic integers are again algebraic integers.
- If $b \in \mathbb{Q}$ is an algebraic integer, then $b \in \mathbb{Z}$. In other words $\{b \in \mathbb{Q} \mid b \text{ algebraic integer}\} = \mathbb{Z}$.

Corollary 17.1

Character values are algebraic integers.

Proof: By the above, roots of unity are algebraic integers. Since the algebraic integers form a ring, so are sums of roots of unity. Hence the claim follows from Property 7.5(b). ■

Next, we want to prove that the values of the central characters are also algebraic integers. Notice that by definition the class sums $\widehat{C}_j$ $(1 \leqslant j \leqslant r)$ are elements of the subring $\mathbb{Z}G$ of $\mathbb{C}G$, hence of the centre of $\mathbb{Z}G$.

Corollary 17.2

(a) The centre $Z(\mathbb{Z}G)$ of the group ring $\mathbb{Z}G$ is finitely generated as a $\mathbb{Z}$-module.

(b) The centre $Z(\mathbb{Z}G)$ of the group ring $\mathbb{Z}G$ is integral over $\mathbb{Z}$; in particular the class sums $\widehat{C}_j$ $(1 \leqslant j \leqslant r)$ are integral over $\mathbb{Z}$.

Proof:

(a) It follows directly from the second part of the proof of Lemma 15.2 that the class sums $\widehat{C}_j$ $(1 \leqslant j \leqslant r)$ span $Z(\mathbb{Z}G)$ as a $\mathbb{Z}$-module.

(b) The centre $Z(\mathbb{Z}G)$ is integral over $\mathbb{Z}$ by Theorem D.2 because it is finitely generated as a $\mathbb{Z}$-module by (a). ■

Theorem 17.3 (*Integrality Theorem*)

The values $\omega_\chi(\widehat{C}_j)$ $(\chi \in \operatorname{Irr}(G),\ 1 \leqslant j \leqslant r)$ of the central characters of G are algebraic integers. Moreover,

$$\omega_\chi(\widehat{C}_j) = \frac{|C_j|}{\chi(1)}\chi(g_j) \qquad \forall\ \chi \in \operatorname{Irr}(G),\ \forall\ 1 \leqslant j \leqslant r\,.$$

Proof: Let $\chi \in \operatorname{Irr}(G)$ and $1 \leqslant j \leqslant r$. By Corollary 17.2 the class sum $\widehat{C}_j$ is integral over $\mathbb{Z}$. Thus there exist integers $n \in \mathbb{Z}_{>0}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that $\widehat{C}_j^n + a_{n-1}\widehat{C}_j^{n-1} + \ldots + a_0 = 0$. Applying ω_χ yields $\omega_\chi(\widehat{C}_j)^n + a_{n-1}\omega_\chi(\widehat{C}_j)^{n-1} + \ldots + a_0 = \omega_\chi(0) = 0$, so that $\omega_\chi(\widehat{C}_j)$ is an algebraic integer.

Now, according to Notation 15.3 we have

$$\chi(1)\omega_\chi(\widehat{C}_j) = \operatorname{Tr}\left(\widetilde{\rho}^\chi(\widehat{C}_j)\right) = \operatorname{Tr}\Big(\sum_{g\in C_j}\rho^\chi(g)\Big) = \sum_{g\in C_j}\operatorname{Tr}\left(\rho^\chi(g)\right) = \sum_{g\in C_j}\chi(g) = |C_j|\chi(g_j)\,,$$

where the last equality holds because characters are class functions. The claim follows. ■

Corollary 17.4

If $\chi \in \operatorname{Irr}(G)$, then $\chi(1)$ divides $|G|$.

Proof: By the 1st Orthogonality Relations we have

$$\frac{|G|}{\chi(1)} = \frac{|G|}{\chi(1)}\langle\chi,\chi\rangle_G = \frac{1}{\chi(1)}\sum_{g\in G}\chi(g)\chi(g^{-1}) = \frac{1}{\chi(1)}\sum_{j=1}^{r}|C_j|\chi(g_j)\chi(g_j^{-1}) = \sum_{j=1}^{r}\underbrace{\frac{|C_j|}{\chi(1)}\chi(g_j)}_{=\omega_\chi(\widehat{C}_j)}\chi(g_j^{-1})\,.$$

Now, for each $1 \leqslant j \leqslant r$, $\omega_\chi(g_j)$ is an algebraic integer by the Integrality Theorem and $\chi(g_j^{-1})$ is an algebraic integer by Corollary 17.1. Hence $|G|/\chi(1)$ is an algebraic integer because these form a subring of $\mathbb{C}$. Moroever, clearly $|G|/\chi(1) \in \mathbb{Q}$. As the algebraic integers in $\mathbb{Q}$ are just the elements of $\mathbb{Z}$, we obtain that $|G|/\chi(1) \in \mathbb{Z}$, as claimed. ■

Example 8 (***The degrees of the irreducible characters of*** $\mathrm{GL}_3(\mathbb{F}_2)$)

The group $G := \mathrm{GL}_3(\mathbb{F}_2)$ is a simple group of order

$$|G| = \#\,\mathbb{F}_2\text{-bases of } \mathbb{F}_2^3 = (2^3-1)(2^3-2)(2^3-2^2) = 168 = 2^3 \cdot 3 \cdot 7\,.$$

For the purpose of this example we accept without proof that G is simple and that it has 6 conjugacy classes.

Question: can we compute the degrees of the irreducible characters of $\mathrm{GL}_3(\mathbb{F}_2)$?

(1) By the above $|\operatorname{Irr}(G)| = |C(G)| = 6$ and the degree formula yields:

$$1 + \sum_{i=2}^{6} \chi_i(1)^2 = |G| = 168\,.$$

(2) Next, as G is simple non-abelian, $G = G'$ and therfeore G has $|G : G'| = 1$ linear characters by Corollary 14.8, namely

$$\chi_i(1) \geqslant 2 \quad \text{for each } 2 \leqslant i \leqslant 6\,.$$

Thus, at this stage, we would have the following possibilities for the degrees of the 6 irreducible characters of G:

$\chi_1(1)$	$\chi_2(1)$	$\chi_3(1)$	$\chi_4(1)$	$\chi_5(1)$	$\chi_6(1)$
1	2	4	5	5	9
1	2	3	3	8	9
1	2	5	5	7	8
1	2	4	7	7	7
1	3	3	6	7	8

(3) By Corollary 17.4 we now know that $\chi_i(1) \mid |G|$ for each $2 \leqslant i \leqslant 6$. Therefore, as $5 \nmid |G|$ and $9 \nmid |G|$, the first three rows can already be discarded:

$\chi_1(1)$	$\chi_2(1)$	$\chi_3(1)$	$\chi_4(1)$	$\chi_5(1)$	$\chi_6(1)$
1	2	4	$\cancel{5}$	$\cancel{5}$	$\cancel{9}$
1	2	3	3	8	$\cancel{9}$
1	2	$\cancel{5}$	$\cancel{5}$	7	8
1	2	4	7	7	7
1	3	3	6	7	8

(4) In order to eliminate the last-but-one possibility, we use Exercise 14.14 telling us that a simple group cannot have an irreducible character of degree 2. Hence

$$\chi_1(1) = 1\,,\ \chi_2(1) = 3\,,\ \chi_3(1) = 3\,,\ \chi_4(1) = 6\,,\ \chi_5(1) = 7\,,\ \chi_6(1) = 8\,.$$

Exercise 17.5

Let G be a finite group of odd order and, as usual, let r denote the number of conjugacy classes of G. Use character theory to prove that

$$r \equiv |G| \pmod{16}\,.$$

[Hint: Label the set $\mathrm{Irr}(G)$ of irreducible characters taking dual characters into account. Use the divisibility property of Corollary 17.4]

18 The Centre of a Character

We now introduced the notion of the centre of a character, which slightly weakens the notion of the kernel of a character. We prove that these centres are closely related to the centre of the group.

Definition 18.1 (*Centre of a character*)

The **centre** of a character χ of G is $Z(\chi) := \{g \in G \mid |\chi(g)| = \chi(1)\}$.

Note: Recall that in contrast, $\chi(g) = \chi(1) \;\Leftrightarrow\; g \in \ker(\chi)$.

Example 9

Recall from Example 5 that the character table of $G = S_3$ is

	Id	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Hence $Z(\chi_1) = Z(\chi_2) = G$ and $Z(\chi_3) = \{\mathrm{Id}\}$.

Lemma 18.2

If $\rho : G \longrightarrow \mathrm{GL}(V)$ is a $\mathbb{C}$-representation affording the character χ and $g \in G$, then:

$$|\chi(g)| = \chi(1) \quad\Longleftrightarrow\quad \rho(g) \in \mathbb{C}^\times \,\mathrm{Id}_V\,.$$

In other words $Z(\chi) = \rho^{-1}\big(\mathbb{C}^\times \,\mathrm{Id}_V\big)$.

Proof: Let $n := \chi(1)$. Recall that we can find a $\mathbb{C}$-basis B of V such that $(\rho(g))_B$ is a diagonal matrix with diagonal entries $\varepsilon_1, \ldots, \varepsilon_n$ which are $o(g)$-th roots of unity. Hence $\varepsilon_1, \ldots, \varepsilon_n$ are the eigenvalues of $\rho(g)$. Applying the Cauchy-Schwarz inequality to the vectors $v := (\varepsilon_1, \ldots, \varepsilon_n)$ and $w := (1, \ldots, 1)$ in $\mathbb{C}^n$ yields

$$|\chi(g)| = |\varepsilon_1 + \ldots + \varepsilon_n| = |\langle v, w\rangle| \leqslant ||v|| \cdot ||w|| = \sqrt{n}\sqrt{n} = n = \chi(1)$$

and equality implies that v and w are $\mathbb{C}$-linearly dependent so that $\varepsilon_1 = \ldots = \varepsilon_n =: \varepsilon$. Therefore $\rho(g) \in \mathbb{C}^\times \,\mathrm{Id}_V$. Conversely, if $\rho(g) \in \mathbb{C}^\times \,\mathrm{Id}_V$, then there exists $\lambda \in \mathbb{C}^\times$ such that $\rho(g) = \lambda \,\mathrm{Id}_V$. Therefore the eigenvalues of $\rho(g)$ are all equal to λ, i.e. $\lambda = \varepsilon_1 = \ldots = \varepsilon_n$ and therefore

$$|\chi(g)| = |n\lambda| = n|\lambda| = n \cdot 1 = n\,.$$

■

Proposition 18.3

Let χ be a character of G. Then:

(a) $Z(\chi) \trianglelefteq G$;

(b) $\ker(\chi) \trianglelefteq Z(\chi)$ and $Z(\chi)/\ker(\chi)$ is a cyclic group;

(c) if χ is irreducible, then $Z(\chi)/\ker(\chi) = Z(G/\ker(\chi))$.

Proof: Let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a $\mathbb{C}$-representation affording χ and set $n := \chi(1)$.

(a) Clearly $\mathbb{C}^\times \mathrm{Id}_V \leqslant Z(\mathrm{GL}(V))$ and hence $\mathbb{C}^\times \mathrm{Id}_V \trianglelefteq \mathrm{GL}(V)$. Therefore, by Lemma 18.2,

$$Z(\chi) = \rho^{-1}(\mathbb{C}^\times \mathrm{Id}_V) \trianglelefteq G$$

as the pre-image under a group homomorphism of a normal subgroup.

(b) By the definitions of the kernel and of the centre of a character, we have $\ker(\chi) \subseteq Z(\chi)$. Therefore $\ker(\chi) \trianglelefteq Z(\chi)$ by (a). By Lemma 18.2 restriction to $Z(\chi)$ yields a group homomorphism

$$\rho|_{Z(\chi)} : Z(\chi) \longrightarrow \mathbb{C}^\times \mathrm{Id}_V$$

with kernel $\ker(\chi)$. Therefore, by the 1st ismomorphism theorem, $Z(\chi)/\ker(\chi)$ is isomorphic to a finite subgroup of $\mathbb{C}^\times \mathrm{Id}_V \cong \mathbb{C}^\times$, hence is cyclic.

(c) By the arguments of (a) and (b) we have

$$Z(\chi)/\ker(\chi) \cong \rho(Z(\chi)) \leqslant Z(\rho(G)) .$$

Applying again the first isomorphism theorem we have $\rho(G) \cong G/\ker(\rho)$, hence

$$Z(\rho(G)) \cong Z(G/\ker(\rho)) = Z(G/\ker(\chi)) .$$

Now let $g\ker(\chi) \in Z(G/\ker(\chi))$, where $g \in G$. As χ is irreducible, by Schur's Lemma, there exists $\lambda \in \mathbb{C}^\times$ such that $\rho(g) = \lambda \mathrm{Id}_V$. Thus $g \in Z(\chi)$ and it follows that

$$Z(G/\ker(\chi)) \leqslant Z(\chi)/\ker(\chi) .$$

■

Exercise 18.4

Prove that if $\chi \in \mathrm{Irr}(G)$, then $Z(G) \leqslant Z(\chi)$. Deduce that $\bigcap_{\chi\in\mathrm{Irr}(G)} Z(\chi) = Z(G)$.

Exercise 18.5

Prove that, if $\chi \in \mathrm{Irr}(G)$, then $\chi(1) \mid |G : Z(\chi)|$. Deduce that $\chi(1) \mid |G : Z(G)|$.

This allows us to prove an important criterion, due to Burnside, for character values to be zero.

Theorem 18.6 (*Burnside*)

Let $\chi \in \mathrm{Irr}(G)$ and let $C = [g]$ be a conjugacy class of G such that $\gcd(\chi(1), |C|) = 1$. Then $\chi(g) = 0$ or $g \in Z(\chi)$.

Proof: As $\gcd(\chi(1), |C|) = 1$, there exist $u, v \in \mathbb{Z}$ such that $u\chi(1) + v|C| = 1$ Set $\alpha := \frac{\chi(g)}{\chi(1)}$. Then

$$\alpha = \frac{\chi(g)}{\chi(1)} \cdot 1 = \frac{\chi(g)}{\chi(1)}\big(u\chi(1) + v|C|\big) = u\chi(g) + v\frac{|C|\chi(g)}{\chi(1)} = u\chi(g) + v\omega_\chi(C)$$

is an algebraic integer because both $\chi(g)$ and $\omega_\chi(C)$ are. Now, set $m := |\langle g\rangle|$ and let $\zeta_m := e^{\frac{2\pi i}{m}}$. As $\chi(g)$ is a sum of m-th roots of unity, certainly $\chi(g) \in \mathbb{Q}(\zeta_m)$. Let $\mathcal{G}$ be the Galois group of the Galois extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_m)$. Then for each field automorphism $\sigma \in \mathcal{G}$, $\sigma(\alpha)$ is also an algebraic integer because α and $\sigma(\alpha)$ are roots of the same monic integral polynomial. Hence $\beta := \prod_{\sigma\in\mathcal{G}} \sigma(\alpha)$ is also an algebaric integer and because $\sigma(\beta) = \beta$ for every $\sigma \in \mathcal{G}$, β is an element of the fixed field of $\mathcal{G}$, namely $\beta \in \mathbb{Q}$ (Galois theory). Therefore $\beta \in \mathbb{Z}$.

If $g \in Z(\chi)$, then there is nothing to do. Thus we may assume that $g \notin Z(\chi)$. Then $|\chi(g)| \neq \chi(1)$, so that by Property 7.5(c) we must have $|\chi(g)| < \chi(1)$ and hence $|\alpha| < 1$. Now, again by Property 7.5(b), $\chi(g) = \varepsilon_1 + \ldots + \varepsilon_n$ with $n = \chi(1)$ and $\varepsilon_1, \ldots, \varepsilon_n$ m-th roots of unity. Therefore, for each $\sigma \in \mathcal{G}\backslash\{\mathrm{Id}\}$, we have $\sigma(\chi(g)) = \sigma(\varepsilon_1) + \ldots + \sigma(\varepsilon_n)$ with $\sigma(\varepsilon_1), \ldots, \sigma(\varepsilon_n)$ m-th roots of unity, because $\varepsilon_1, \ldots, \varepsilon_n$ are. It follows that

$$|\sigma(\chi(g))| = |\sigma(\varepsilon_1) + \ldots + \sigma(\varepsilon_n)| \leqslant |\sigma(\varepsilon_1)| + \ldots + |\sigma(\varepsilon_n)| = n = \chi(1)$$

and hence

$$|\sigma(\alpha)| = \frac{1}{\chi(1)}|\sigma(\chi(g))| \leqslant \frac{\chi(1)}{\chi(1)} = 1\,.$$

Thus

$$|\beta| = |\prod_{\sigma\in\mathcal{G}} \sigma(\alpha)| = \underbrace{|\alpha|}_{<1} \cdot \prod_{\sigma\in\mathcal{G}\backslash\{\mathrm{Id}\}} \underbrace{|\sigma(\alpha)|}_{\leqslant 1} < 1\,.$$

The only way an integer satisfies this inequality is $\beta = 0$. Thus $\alpha = 0$ as well, which implies that $\chi(g) = 0$. ■

Corollary 18.7

Assume now that G is a non-abelian simple group. In the situation of Theorem 18.6 if we assume moreover that $\chi(1) > 1$ and $C \neq \{1\}$, then it is always the case that $\chi(g) = 0$.

Proof: Assume $\chi(g) \neq 0$, then Theorem 18.6 implies that $g \in Z(\chi)$, so $Z(\chi) \neq 1$. As G is simple and $Z(\chi) \trianglelefteq G$ by Proposition 18.3(a), we have $Z(\chi) = G$. Moreover, the fact that G is simple also implies that $\ker(\chi) = 1$, as if it were G, then χ would be reducible. Thus, it follows from Proposition 18.3 that

$$G = Z(\chi)/\ker(\chi) = Z(G/\ker(\chi)) = Z(G) = 1\,,$$

where the last equality holds because G is simple non-abelian. This is contradiction. ■

19 Burnside's $p^a q^b$-Theorem

Character theory has many possible applications to the structure of finite groups. We consider in this section on of the most famous of these: the proof of Burnside's $p^a q^b$-theorem.

Example 10

To begin with we consider two possible minor applications of character theory to finite groups. Both are results of the *Einfürung in die Algebra*, for which you have already seen purely group-theoretic proofs.

(a) G finite group such that $|G| = p^2$ for some prime number $p \implies G$ is abelian.

- **Proof using character theory**. By Corollary 17.4 we have $\chi(1) \mid |G|$ for each $\chi \in \mathrm{Irr}(G)$. Thus
$$\chi(1) \in \{1, p, p^2\}\,.$$
Therefore the degree formula reads
$$p^2 = |G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = \underbrace{\mathbf{1}_G(1)^2}_{=1} + \sum_{\substack{\chi \in \mathrm{Irr}(G)\\ \chi \neq \mathbf{1}_G}} \chi(1)^2\,,$$
which implies that it is not possible that the degree of an irreducible character of G is p or p^2. In other words, all the irreducible characters of G are linear, and thus G is abelian by Corollary 14.8.

(b) G is a non-trivial p-group $\implies G$ is soluble.

[Recall from the *Einfürung in die Algebra* that a finite group G is **soluble** if it admits a chain of subgroups
$$1 = G_0 < G_1 < \ldots < G_s = G$$
such that for $1 \leqslant i \leqslant s$, $G_{i-1} \lhd G_i$ and G_i/G_{i-1} is cyclic of prime order. Moreover, we have the following very useful *solubility criterion*, sometimes coined "the sandwich principle": if $H \trianglelefteq G$ is a normal subgroup, then the group G is soluble if and only if both G and G/H are soluble.]

- **Proof using character theory**. By induction on $|G| =: p^a$ ($a \in \mathbb{Z}_{>0}$). If $|G| = p$ or $|G| = p^2$, then G is abelian (cyclic in the former case). Finite abelian groups are clearly soluble because they are products of cyclic groups of prime power order.
Therefore, we may assume that $|G| \geqslant p^3$. As in (a) Corollary 17.4 implies that
$$\chi(1) \in \{1, p, p^2, \ldots, p^a\} \quad \text{for each } \chi \in \mathrm{Irr}(G)\,.$$
Now, again the degree formula yields
$$p^a = |G| = 1 + \sum_{\substack{\chi \in \mathrm{Irr}(G)\\ \chi \neq \mathbf{1}_G}} \chi(1)^2\,.$$
and for this equality to hold, there must be at least p linear characters of G (including the trivial character). Thus it follows from Corollary 14.8 that $G' \lneq G$. Hence both G' and G/G' are soluble by the induction hypothesis $\Rightarrow G$ is soluble by the *sandwich principle*.

Theorem 19.1 (*Burnside*)

Let G be a finite non-abelian simple group. If C is a conjugacy class of G such that $|C| = p^a$ with p prime and $a \in \mathbb{Z}_{\geqslant 0}$, then $C = \{1\}$.

Proof: Assume ab absurdo that $C \neq \{1\}$ and choose $g \in C$. In particular $g \neq 1$. Since G is non-abelian simple $G = G'$ and it follows from Corollary 14.8 that the unique linear character of G is the trivial character. Hence, for each $\chi \in \mathrm{Irr}(G)\backslash\{\mathbf{1}_G\}$, either $p \mid \chi(1)$ or $1 = \gcd(\chi(1), p) = \gcd(\chi(1), |C|)$, and in the case in which $p \nmid \chi(1)$, then $\chi(g) = 0$ by Corollary 18.7. Therefore, the Second Orthogonality

Relations read

$$0 = 1 + \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi\neq 1_G}} \underbrace{\chi(g)}_{\substack{=0 \text{ if}\\ p\nmid\chi(1)}} \underbrace{\overline{\chi(1)}}_{=\chi(1)} = 1 + \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ p|\chi(1)}} \chi(g)\chi(1)$$

and dividing by p yields

$$\underbrace{\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ p|\chi(1)}} \underbrace{\frac{\chi(1)}{p}}_{\in\mathbb{Z}} \underbrace{\chi(g)}_{\substack{\text{algebraic}\\ \text{integer}}}}_{\text{algebraic integer}} = -\frac{1}{p} \in \mathbb{Q}\backslash\mathbb{Z}\,.$$

This contradicts the fact that rational numbers which are algebraic integers are integers. It follows that $g = 1$ is the only possibility and hence $C = \{1\}$. ■

As a consequence, we obtain Burnside's $p^a q^b$ theorem, which can be found in the literature under two different forms. The first version provides us with a "non-simplicity" criterion and the second version with a solubility criterion, which is extremely hard to prove by purely group theoretic methods.

Theorem 19.2 (*Burnside's $p^a q^b$ Theorem, "simple" version*)

Let p, q be prime numbers and let $a, b \in \mathbb{Z}_{\geqslant 0}$ be integers such that $a + b \geqslant 2$. If G is a finite group of order $p^a q^b$, then G is not simple.

Proof: First assume that $a = 0$ or $b = 0$. Then G is a q-group with $q^2 \mid |G|$, resp. a p-group with $p^2 \mid |G|$. Therefore the centre of G is non-trivial (*Algebra I*), thus of non-trivial prime power order. Therefore, there exists an element $g \in Z(G)$ of order q (resp. p) and $1 \neq \langle g \rangle \lhd G$ is a proper non-trivial normal subgroup. Hence G is not simple.

We may now assume that $a \neq 0 \neq b$. Let $Q \in \mathrm{Syl}_q(G)$ be a Sylow q-subgroup of G (i.e. $|Q| = q^b$). Again, as Q is a q-group, we have $Z(Q) \neq \{1\}$ and we can choose $g \in Z(Q)\backslash\{1\}$. Then

$$Q \leqslant C_G(g)$$

and therefore the Orbit-Stabiliser Theorem yields

$$|[g]| = |G : C_G(g)| = p^r$$

for some non-negative integer $r \leqslant a$. If $r = 0$, then $p^r = 1$ and $G = C_G(g)$, so that $g \in Z(G)$. Hence $Z(G) \neq \{1\}$ and G is not simple by the same argument as above. If $p^r > 1$, then G cannot be simple by Theorem 19.1. ■

Theorem 19.3 (*Burnside's $p^a q^b$ Theorem, "soluble" version*)

Let p, q be prime numbers and $a, b \in \mathbb{Z}_{\geqslant 0}$. Then any finite group of order $p^a q^b$ is soluble.

Proof: Let G be a finite group of order $p^a q^b$. We proceed by induction on $a + b$.

- $a + b \in \{0, 1\} \implies G$ is either trivial or cyclic of prime order, hence clearly soluble.
- $a + b \geqslant 2 \implies G$ is not simple by the "simple" version of Burnside's $p^a q^b$ theorem. Hence there exists a proper non-trivial normal subgroup H in G and both $|H|, |G/H| < p^a q^b$. Therefore both H and G/H are soluble by the induction hypothesis. Thus G is soluble by the sandwich principle. ■

Chapter 6. Induction and Restriction of Characters

In this chapter, we present important methods to construct / relate characters of a group, given characters of subgroups or overgroups. The main idea is that we would like to be able to use the character tables of groups we know already in order to compute the character tables of subgroups or overgroups of these groups.

Notation: throughout this chapter, unless otherwise specified, we let:

- G denote a finite group, $H \leqslant G$ and $N \trianglelefteq G$, $i_H : H \longrightarrow G, h \mapsto h$ is the canonical inclusion of H in G and $\pi_N : G \longrightarrow G/N, g \mapsto gN$ is the quotient morphism;
- $K := \mathbb{C}$ be the field of complex numbers;
- $\mathrm{Irr}(G) := \{\chi_1, \ldots, \chi_r\}$ denote the set of pairwise distinct irreducible characters of G;
- $C_1 = [g_1], \ldots, C_r = [g_r]$ denote the conjugacy classes of G, where $g_1, \ldots, g_r$ is a fixed set of representatives; and
- we use the convention that $\chi_1 = \mathbf{1}_G$ and $g_1 = 1 \in G$.

In general, unless otherwise stated, all groups considered are assumed to be finite and all $\mathbb{C}$-vector spaces / modules over the group algebra considered are assumed to be finite-dimensional.

20 Induction and Restriction

We aim at *inducing* and *restricting* characters from subgroups, resp. overgroups. We start with the operation of induction, which is a subtle operation to construct a class function on G from a given class function on a subgroup $H \leqslant G$. We will focus on characters in a second step.

Definition 20.1 (*Induced class function*)

Let $H \leqslant G$ and $\varphi \in \mathcal{C}l(H)$ be a class function on H. Then the **induction of φ from H to G** is

$$\begin{array}{rccl} \mathrm{Ind}_H^G(\varphi) =: \varphi\!\uparrow_H^G \;: & G & \longrightarrow & \mathbb{C} \\ & g & \mapsto & \varphi\!\uparrow_H^G(g) := \frac{1}{|H|}\sum_{x\in G} \varphi^\circ(xgx^{-1})\,, \end{array}$$

where for $y \in G$, $\varphi^\circ(y) := \begin{cases} \varphi(y) & \text{if } y \in H, \\ 0 & \text{if } y \notin H. \end{cases}$

Remark 20.2

With the notation of Definition 20.1 the following holds:

(a)
$$\varphi\uparrow_H^G(g) = \frac{1}{|H|}\sum_{x\in G}\varphi^\circ(xgx^{-1}) = \frac{1}{|H|}\sum_{\substack{x\in G\\ xgx^{-1}\in H}}\varphi(xgx^{-1})\,;$$

(b) the function $\varphi\uparrow_H^G$ is a class function on G, because for every $g, y \in G$,
$$\varphi\uparrow_H^G(ygy^{-1}) = \frac{1}{|H|}\sum_{x\in G}\varphi^\circ(xygy^{-1}x^{-1}) \overset{s:=yx}{=} \frac{1}{|H|}\sum_{s\in G}\varphi^\circ(sgs^{-1}) = \varphi\uparrow_H^G(g)\,.$$

In contrast, the operation of restriction is based on the more elementary idea that any map can be restricted to a subset of its domain. For class functions / representations / characters we are essentially interested in restricting these (seen as maps) to subgroups.

Definition 20.3 (*Restricted class function*)

Let $H \leqslant G$ and $\psi \in \mathcal{C}l(G)$ be a class function on G. Then the **restriction of ψ from G to H** is
$$\mathrm{Res}_H^G(\psi) := \psi\downarrow_H^G := \psi|_H = \psi\circ i_H\,.$$
This is obviously again a class function on H.

Remark 20.4

If ψ is a character of G afforded by the $\mathbb{C}$-representation $\rho : G \longrightarrow \mathrm{GL}(V)$, then clearly $\psi\downarrow_H^G$ is the character afforded by the $\mathbb{C}$-representation $\mathrm{Res}_H^G(\rho) := \rho\downarrow_H^G := \rho|_H = \rho\circ i_H : H \longrightarrow \mathrm{GL}(V)$. See Exercise 9.10(i).

Exercise 20.5

Let $H \leqslant J \leqslant G$ and let $g \in G$. Prove the following assertions:

(a) $\varphi \in \mathcal{C}l(H) \implies \varphi\uparrow_H^G(g) = \sum_{\substack{Hx\in H\backslash G\\ Hx=Hxg}}\varphi(xgx^{-1})\,;$

(b) $\varphi \in \mathcal{C}l(H) \implies (\varphi\uparrow_H^J)\uparrow_J^G = \varphi\uparrow_H^G$ (transitivity of induction);

(c) $\psi \in \mathcal{C}l(G) \implies (\psi\downarrow_J^G)\downarrow_H^J = \psi\downarrow_H^G$ (transitivity of restriction);

(d) the maps
$$\mathrm{Ind}_H^G : \mathcal{C}l(H) \longrightarrow \mathcal{C}l(G), \varphi \mapsto \varphi\uparrow_H^G \quad\text{and}\quad \mathrm{Res}_H^G : \mathcal{C}l(G) \longrightarrow \mathcal{C}l(H), \psi \mapsto \psi\downarrow_H^G$$
are $\mathbb{C}$-linear;

(e) $\varphi \in \mathcal{C}l(H)$ and $\psi \in \mathcal{C}l(G) \implies \psi\cdot\varphi\uparrow_H^G = (\psi\downarrow_H^G\cdot\varphi)\uparrow_H^G$ (Frobenius formula).

Theorem 20.6 (*Frobenius reciprocity*)

Let $H \leqslant G$, let $\varphi \in \mathcal{C}l(H)$ be a class function on H, and let $\psi \in \mathcal{C}l(G)$ be a class function on G. Then,

$$\langle \varphi\!\uparrow_H^G, \psi\rangle_G = \langle \varphi, \psi\!\downarrow_H^G\rangle_H \qquad \text{and} \qquad \langle \psi, \varphi\!\uparrow_H^G\rangle_G = \langle \psi\!\downarrow_H^G, \varphi\rangle_H\,.$$

Note: If φ and ψ are characters, then clearly all four numbers are equal.

Proof: Since $\langle -,-\rangle_G$ and $\langle -,-\rangle_H$ are hermitian forms, the 1st equality holds if and only if the 2nd equality holds. Hence, it suffices to prove the second one. By the definitions of the scalar products and of the induction, a direct computation yields:

$$\begin{aligned}\langle \psi, \varphi\!\uparrow_H^G\rangle_G = \frac{1}{|G|}\sum_{g\in G}\psi(g)\overline{\varphi\!\uparrow_H^G(g)} &= \frac{1}{|G|}\sum_{g\in G}\psi(g)\frac{1}{|H|}\sum_{x\in G}\overline{\varphi^\circ(xgx^{-1})}\\ &= \frac{1}{|G|\cdot|H|}\sum_{g\in G}\sum_{\substack{x\in G\\ xgx^{-1}\in H}}\psi(xgx^{-1})\overline{\varphi(xgx^{-1})}\\ &= \frac{1}{|H|}\sum_{s\in H}\psi\!\downarrow_H^G(s)\overline{\varphi(s)}\\ &= \langle \psi\!\downarrow_H^G, \varphi\rangle_H\,,\end{aligned}$$

where the third equality comes from the fact that ψ is a class function on G, and for the fourth equality we set $s := xgx^{-1}$. ■

Corollary 20.7

Let $H \leqslant G$ and let χ be a character of H of degree n. Then the induced class function $\chi\!\uparrow_H^G$ is a character of G of degree $n\cdot|G:H|$.

Proof: Given $\psi \in \mathrm{Irr}(G)$ by Frobenius reciprocity we can set

$$m_\psi := \langle \chi\!\uparrow_H^G, \psi\rangle_G = \langle \chi, \psi\!\downarrow_H^G\rangle_H \in \mathbb{Z}_{\geqslant 0}\,,$$

which is an integer because both χ and $\psi\!\downarrow_H^G$ are characters of H. Therefore,

$$\chi\!\uparrow_H^G = \sum_{\psi\in\mathrm{Irr}(G)} m_\psi \psi$$

is a non-negative integral linear combination of irreducible characters of G, hence a character of G. Moreover,

$$\chi\!\uparrow_H^G(1) = \frac{1}{|H|}\sum_{x\in G}\chi^\circ(1) = \frac{1}{|H|}|G|\chi(1) = \chi(1)|G:H|\,.$$

■

Remark 20.8

We conclude from Exercise 20.5(d) and Corollary 9.8, that the induction and the restriction of a virtual character is again a virtual character. In other words, if $H \leqslant G$, then:

(a) $\varphi \in \mathbb{Z}\,\mathrm{Irr}(H) \implies \varphi\!\uparrow_H^G \in \mathbb{Z}\,\mathrm{Irr}(G)$; and

(b) $\psi \in \mathbb{Z}\,\mathrm{Irr}(G) \implies \psi\!\downarrow_H^G \in \mathbb{Z}\,\mathrm{Irr}(H)$.

Example 11

(a) The restriction of the trivial character of G from G to H is obviously the trivial character of H.

(b) If $H = \{1\}$, then $\mathbf{1}_{\{1\}}\uparrow_{\{1\}}^{G} = \chi_{\text{reg}}$. Indeed, if $g \in G$ then, it follows from Corollary 10.2 that

$$\mathbf{1}_{\{1\}}\uparrow_{\{1\}}^{G}(g) = \frac{1}{|\{1\}|}\sum_{x\in G}\underbrace{\mathbf{1}_{\{1\}}^{\circ}(x^{-1}gx)}_{=0 \text{ unless } g=1} = \delta_{1g}|G| = \chi_{\text{reg}}(g)\,.$$

(c) Let $G = S_3$, $H = \langle(1\ 2)\rangle$, and let $\varphi : H \to \mathbb{C}$ with $\varphi(\text{Id}) = 1$, $\varphi((1\ 2)) = -1$ be the sign homomorphism on H. By the remark, it is enough to compute $\varphi\uparrow_H^G$ on representatives of the conjugacy classes of S_3, e.g. Id, $(1\ 2)$ and $(1\ 2\ 3)$:

$$\varphi\uparrow_H^G(\text{Id}) = \frac{1}{2}\sum_{x\in S_3}\varphi^{\circ}(\text{Id}) = \frac{1}{2}\cdot|S_3|\cdot 1 = 3\,,$$

$$\varphi\uparrow_H^G((1\ 2\ 3)) = \frac{1}{2}\sum_{x\in S_3}\varphi^{\circ}(x^{-1}(1\ 2\ 3)x) = \frac{1}{2}\sum_{x\in S_3}0 = 0\,,$$

(as the conjugacy class of a 3-cycle contains only 3-cycles and $\varphi(\text{3-cycle}) = 0$)

$$\varphi\uparrow_H^G((1\ 2)) = \frac{1}{2}\sum_{x\in S_3}\varphi^{\circ}(x^{-1}(1\ 2)x) = \frac{1}{2}\left(2\varphi^{\circ}((1\ 2)) + 2\varphi^{\circ}((1\ 3)) + 2\varphi^{\circ}((2\ 3))\right) = -1\,.$$

Moreover we see from the character table of S_3 (Example 5) that $\varphi\uparrow_H^G = \chi_2 + \chi_3$. But we can also compute with Frobenius reciprocity, that

$$0 = \langle\varphi, \chi_1\downarrow_H^G\rangle_H = \langle\varphi\uparrow_H^G, \chi_1\rangle_G$$

and similarly

$$1 = \langle\varphi, \chi_2\downarrow_H^G\rangle_H = \langle\varphi\uparrow_H^G, \chi_2\rangle_G \quad \text{and} \quad 1 = \langle\varphi, \chi_3\downarrow_H^G\rangle_H = \langle\varphi\uparrow_H^G, \chi_3\rangle_G\,.$$

Example 12 (*The character table of the alternating group A_5*)

The conjugacy classes of $G = A_5$ are

$$C_1 = \{\text{Id}\}\,,\ C_2 = [(1\ 2)(3\ 4)]\,,\ C_3 = [(1\ 2\ 3)]\,,\ C_4 \cup C_5 = \{\text{5-cycles}\}\,,$$

i.e. $g_1 = \text{Id}, g_2 = (1\ 2)(3\ 4), g_3 = (1\ 2\ 3)$ and $g \in C_4 \Rightarrow o(g) = 5$ and $g^{-1} \in C_4$ but $g^2, g^3 \in C_5$ so that we can choose $g_4 := (1\ 2\ 3\ 4\ 5)$ and $g_5 := (1\ 3\ 5\ 2\ 4)$. This yields:

$$|\operatorname{Irr}(A_5)| = 5 \text{ and } |C_1| = 1,\ |C_2| = 15,\ |C_3| = 20,\ |C_4| = |C_5| = 12\,.$$

We obtain the character table of A_5 as follows:

- We know that the trivial character $\mathbf{1}_G = \chi_1$ is one of the irreducible characters, hence we need to determine $\operatorname{Irr}(A_5)\setminus\{\mathbf{1}_G\} = \{\chi_2, \chi_3, \chi_4, \chi_5\}$.
- Now, $H := A_4 \leqslant A_5$ and we have already computed the character table of A_4 in Exercise Sheet 5. Therefore, inducing the trivial character of A_4 from A_4 to A_5 we obtain that

$$\begin{aligned}
\mathbf{1}_H\uparrow_H^G(\mathrm{Id}) &= 1\cdot|G:H| = 5 \quad \text{(see Cor. 20.7)}\\
\mathbf{1}_H\uparrow_H^G\big((1\ 2)(3\ 4)\big) &= \tfrac{1}{12}\cdot 12 = 1\\
\mathbf{1}_H\uparrow_H^G\big((1\ 2\ 3)\big) &= \tfrac{1}{12}\cdot 24 = 2\\
\mathbf{1}_H\uparrow_H^G(\text{5-cycle}) &= \tfrac{1}{12}\cdot 0 = 0
\end{aligned}$$

Now, by Frobenius reciprocity

$$\langle \mathbf{1}_H\uparrow_H^G, \chi_1\rangle_G = \langle \mathbf{1}_H, \underbrace{\chi_1\downarrow_H^G}_{=\mathbf{1}_H}\rangle_H = 1\,.$$

It follows (check it) that $\langle \mathbf{1}_H\uparrow_H^G - \chi_1, \mathbf{1}_H\uparrow_H^G - \chi_1\rangle_G = 1$, so $\mathbf{1}_H\uparrow_H^G - \chi_1$ is an irreducible character, say $\chi_4 := \mathbf{1}_H\uparrow_H^G - \chi_1$. The values of χ_4 are given by $(4, 0, 1, -1, -1)$ on C_1, C_2, C_3, C_4, C_5 respectively.

- Next, as A_5 is a non-abelian simple group, we have $A_5/[A_5, A_5] = 1$, and hence the trivial character is the unique linear character of A_5 and $\chi_2(1), \chi_3(1), \chi_5(1) \geqslant 3$. (You have also proved in Exercise 19, Sheet 6 that simple groups do not have irreducible characters of degree 2.) Then the degree formula yields

$$\chi_2(1)^2 + \chi_3(1)^2 + \chi_5(1)^2 = |A_5| - \chi_1(1)^2 - \chi_4(1)^2 = 60 - 1 - 16 = 43\,.$$

As degrees of characters must divide the group order, it follows from this formula that $\chi_2(1), \chi_3(1), \chi_5(1) \in \{3, 4, 5, 6\}$, but then also that it is not possible to have an irreducible character of degree 6. From this we easily see that only possibility, up to relabelling, is $\chi_2(1) = \chi_3(1) = 3$ and $\chi_5(1) = 5$. Hence at this stage, we already have the following part of the character table:

	C_1	C_2	C_3	C_4	C_5
$\lvert C_k\rvert$	1	15	20	12	12
$\lvert C_G(g_k)\rvert$	60	4	3	5	5
χ_1	1	1	1	1	1
χ_2	3	.	.	.	.
χ_3	3	.	.	.	.
χ_4	4	0	1	-1	-1
χ_5	5	.	.	.	.

- Next, we have that

$$\gcd(\chi_2(1), |C_3|) = \gcd(\chi_3(1), |C_3|) = \gcd(\chi_5(1), |C_4|) = \gcd(\chi_5(1), |C_5|) = 1\,,$$

so that the corresponding character values must all be zero by Corollary 18.7 and we get:

	C_1	C_2	C_3	C_4	C_5
$\lvert C_k\rvert$	1	15	20	12	12
$\lvert C_G(g_k)\rvert$	60	4	3	5	5
χ_1	1	1	1	1	1
χ_2	3	.	0	.	.
χ_3	3	.	0	.	.
χ_4	4	0	1	-1	-1
χ_5	5	.	.	0	0

- Applying the Orthogonality Relations yields:
  1st, 3rd column $\Rightarrow \chi_5(g_3) = -1$ and the scalar product $\langle \chi_1, \chi_5 \rangle_G = 0 \Rightarrow \chi_5(g_2) = 1$.

- Finally, to fill out the remaining gaps, we can induce from the cyclic subgroup $Z_5 := \langle (1\ 2\ 3\ 4\ 5) \rangle \leqslant A_5$. Indeed, choosing the non-trivial irreducible character ψ of Z_5 which was denoted "χ_3" in Example 4 gives

$$\psi\uparrow_{Z_5}^{G} = (12, 0, 0, \zeta^2 + \zeta^3, \zeta + \zeta^4)$$

where $\zeta = \exp(2\pi\mathbf{i}/5)$ is a primitive 5-th root of unity. Then we compute that

$$\langle \psi\uparrow_{Z_5}^{G}, \chi_4 \rangle_G = 1 = \langle \psi\uparrow_{Z_5}^{G}, \chi_5 \rangle_G \quad \Longrightarrow \quad \psi\uparrow_{Z_5}^{G} - \chi_4 - \chi_5 = (3, -1, 0, -\zeta - \zeta^4, -\zeta^2 - \zeta^3)$$

and this character must be irreducible, because it is not the sum of 3 copies of the trivial character. Hence we set $\chi_2 := \psi\uparrow_{Z_5}^{G} - \chi_4 - \chi_5$ and the values of χ_3 then easily follow from the 2nd Othogonality Relations:

	C_1	C_2	C_3	C_4	C_5
$\lvert C_k \rvert$	1	15	20	12	12
$\lvert C_G(g_k) \rvert$	60	4	3	5	5
χ_1	1	1	1	1	1
χ_2	3	-1	0	$-\zeta - \zeta^4$	$-\zeta^2 - \zeta^3$
χ_3	3	-1	0	$-\zeta^2 - \zeta^3$	$-\zeta - \zeta^4$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Remark 20.9 (*Induction of $\mathbb{C}H$-modules*)

At the level of $\mathbb{C}G$-modules induction is just a praticular case of a so-called *extension of scalars* from $\mathbb{C}H$ to $\mathbb{C}G$. More precisely, if M is a $\mathbb{C}H$-module, then the induction of M from H to G is defined to be $\mathbb{C}G \otimes_{\mathbb{C}H} M$. Moreover, if M affords the character χ, then $\mathbb{C}G \otimes_{\mathbb{C}H} M$ affords the character $\chi\uparrow_H^G$.

21 Clifford Theory

Clifford theory is a generic term for a series of results relating the representation / character theory of a given group G to that of a normal subgroup $N \trianglelefteq G$ through induction and restriction.

Notation 21.1

Let $H \leqslant G$ and let $x \in G$.

(1) We let

$$\begin{array}{rccc} c_x : & H & \longrightarrow & xHx^{-1} \\ & h & \mapsto & xhx^{-1} \end{array}$$

denote the conjugation homomorphism by x.

(2) We write $x \in [G/H]$ to mean that $x \in G$ is a representative of the element xH in G/H. In a sum, writing $\sum_{x\in[G/H]}$ means that the sum runs over a full set of representatives for the left cosets in G/H. This is the same as writing $\sum_{xH\in G/H}$.

Definition 21.2 (*Conjugate class function / inertia group*)

Let $H \leqslant G$, let $\varphi \in \mathcal{C}l(H)$, let $g \in G$ and let $c_{g^{-1}} : gHg^{-1} \longrightarrow H$ denote the conjugation homomorphism by g^{-1}. We define:

(a) the **conjugate class function to** φ **by** g to be ${}^g\varphi := \varphi \circ c_{g^{-1}} \in \mathcal{C}l(gHg^{-1})$, i.e. the class function on gHg^{-1} given by

$$ {}^g\varphi : gHg^{-1} \longrightarrow \mathbb{C}, x \mapsto \varphi(g^{-1}xg)\,; $$

and

(b) the **inertia group** of φ in G to be $\mathcal{I}_G(\varphi) := \{g \in G \mid {}^g\varphi = \varphi\}$.

Exercise 21.3

Let $g, h \in G$. With the notation of Definition 21.2, prove that:

(a) ${}^g\varphi$ is indeed a class function on gHg^{-1};

(b) $\mathcal{I}_G(\varphi) \leqslant G$ and $H \leqslant \mathcal{I}_G(\varphi) \leqslant N_G(H)$;

(c) ${}^g\varphi = {}^h\varphi \;\Leftrightarrow\; h^{-1}g \in \mathcal{I}_G(\varphi) \;\Leftrightarrow\; g\mathcal{I}_G(\varphi) = h\mathcal{I}_G(\varphi)$;

(d) if $\rho : H \longrightarrow \mathrm{GL}(V)$ is a $\mathbb{C}$-representation of H with character χ, then

$$ {}^g\rho := \rho \circ c_{g^{-1}} : gHg^{-1} \longrightarrow \mathrm{GL}(V), x \mapsto \rho(g^{-1}xg) $$

is a $\mathbb{C}$-representation of gHg^{-1} with character ${}^g\chi = \chi \circ c_{g^{-1}}$ and ${}^g\chi(1) = \chi(1)$;

(e) if $J \leqslant H$ then ${}^g(\varphi\downarrow_J^H) = ({}^g\varphi)\downarrow_{gJg^{-1}}^{gHg^{-1}}$.

Exercise 21.4 (*Mackey Formula*)

Let $H, L \leqslant G$ and let $\varphi \in \mathcal{C}l(H)$. Prove that

$$ (\varphi\uparrow_H^G)\downarrow_L^G = \sum_{g \in \sqrt{}\text{á}L\backslash G/H]} ({}^g\varphi)\downarrow_{gHg^{-1}\cap L}^{gHg^{-1}}\uparrow_{gHg^{-1}\cap L}^{L}\,. $$

Exercise 21.5

Deduce from the Mackey formula that if $N \trianglelefteq G$, and $\psi \in \mathrm{Irr}(N)$, then

$$ \langle \psi\uparrow_N^G, \psi\uparrow_N^G\rangle_G = \sum_{xN\in G/N} \langle \psi, {}^x\psi\rangle_N\,. $$

Lemma 21.6

(a) If $H \leqslant G$, $\varphi, \psi \in \mathcal{C}l(H)$ and $g \in G$, then $\langle\, {}^g\varphi, {}^g\psi\rangle_{gHg^{-1}} = \langle \varphi, \psi\rangle_H$.

(b) If $N \trianglelefteq G$ and $g \in G$, then we have $\psi \in \mathrm{Irr}(N) \;\Leftrightarrow\; {}^g\psi \in \mathrm{Irr}(N)$.

(c) If $N \trianglelefteq G$ and ψ is a character of N, then $(\psi\uparrow_N^G)\downarrow_N^G = |\mathcal{I}_G(\psi) : N| \cdot \sum_{g\in[G/\mathcal{I}_G(\psi)]} {}^g\psi$.

Proof: (a) Clearly

$$\begin{aligned}\langle\, {}^g\varphi, {}^g\psi\rangle_{gHg^{-1}} &= \frac{1}{|gHg^{-1}|}\sum_{x\in gHg^{-1}} {}^g\varphi(x)\,\overline{{}^g\psi(x)} \\ &= \frac{1}{|H|}\sum_{x\in gHg^{-1}} \varphi(g^{-1}xg)\overline{\psi(g^{-1}xg)} \\ &\overset{y:=g^{-1}xg}{=} \frac{1}{|H|}\sum_{y\in H}\varphi(y)\overline{\psi(y)} = \langle\varphi,\psi\rangle_H\,.\end{aligned}$$

(b) As $N \trianglelefteq G$, $gNg^{-1} = N$. Thus, if $\psi \in \mathrm{Irr}(N)$, then on the one hand ${}^g\psi$ is also a character of N by Exercise 21.3(d), and on the other hand it follows from (a) that $\langle\, {}^g\psi, {}^g\psi\rangle_N = \langle\psi,\psi\rangle_N = 1$. Hence ${}^g\psi$ is an irreducible character of N. Therefore, if ${}^g\psi \in \mathrm{Irr}(N)$, then $\psi = {}^{g^{-1}}({}^g\psi) \in \mathrm{Irr}(N)$, as required.

(c) If $n \in N$ then so does $g^{-1}ng$ $\forall\, g \in G$, hence

$$\psi\uparrow_N^G\downarrow_N^G(n) = \psi\uparrow_N^G(n) = \frac{1}{|N|}\sum_{g\in G}\psi(g^{-1}ng) = \frac{1}{|N|}\sum_{g\in G} {}^g\psi(n) = \frac{|\mathcal{I}_G(\psi)|}{|N|}\sum_{g\in[G/\mathcal{I}_G(\psi)]} {}^g\psi(n).$$

■

Notation 21.7

Given $N \trianglelefteq G$ and $\psi \in \mathrm{Irr}(N)$, we set $\mathrm{Irr}(G \mid \psi) := \{\chi \in \mathrm{Irr}(G) \mid \langle \chi\downarrow_N^G, \psi\rangle_N \neq 0\}$.

Theorem 21.8 (Clifford Theory)

Let $N \trianglelefteq G$. Let $\chi \in \mathrm{Irr}(G)$, $\psi \in \mathrm{Irr}(N)$ and set $\mathcal{I} := \mathcal{I}_G(\psi)$. Then the following assertions hold.

(a) If ψ is a constituent of $\chi\downarrow_N^G$, then

$$\chi\downarrow_N^G = e\left(\sum_{g\in[G/\mathcal{I}]} {}^g\psi\right),$$

where $e = \langle\chi\downarrow_N^G, \psi\rangle_N = \langle\chi, \psi\uparrow_N^G\rangle_G \in \mathbb{Z}_{>0}$ is called the **ramification index** of χ in N (or of ψ in G). In particular, all the constituents of $\chi\downarrow_N^G$ have the same degree.

(b) Induction from $\mathcal{I} = \mathcal{I}_G(\psi)$ to G induces a bijection

$$\begin{array}{rccc}\mathrm{Ind}_{\mathcal{I}}^G: & \mathrm{Irr}(\mathcal{I}\mid\psi) & \longrightarrow & \mathrm{Irr}(G\mid\psi) \\ & \eta & \mapsto & \eta\uparrow_{\mathcal{I}}^G\end{array}$$

preserving ramification indices, i.e. $\langle\eta\downarrow_N^{\mathcal{I}}, \psi\rangle_N = \langle\eta\uparrow_{\mathcal{I}}^G\downarrow_N^{\mathcal{I}}, \psi\rangle_N = e$.

Proof: (a) By Frobenius reciprocity, $\langle\chi,\psi\uparrow_N^G\rangle_G=\langle\chi\downarrow_N^G,\psi\rangle_N\neq 0$. Thus χ is a constituent of $\psi\uparrow_N^G$ and therefore $\chi\downarrow_N^G\mid\psi\uparrow_N^G\downarrow_N^G$.

Now, if $\eta\in\operatorname{Irr}(N)$ is an arbitrary constituent of $\chi\downarrow_N^G$ (i.e. $\langle\chi\downarrow_N^G,\eta\rangle_N\neq 0$) then by the above, we have

$$\langle\psi\uparrow_N^G\downarrow_N^G,\eta\rangle_N\geqslant\langle\chi\downarrow_N^G,\eta\rangle_N>0\,.$$

Moroever, by Lemma 21.6(c) the constituents of $\psi\uparrow_N^G\downarrow_N^G$ are preciely $\{{}^g\psi\mid g\in[G/\mathcal{I}_G(\psi)]\}$. Hence η is G-conjugate to ψ. Furthermore, for every $g\in G$ we have

$$\begin{aligned}\langle\chi\downarrow_N^G,{}^g\psi\rangle_N=\frac{1}{|N|}\sum_{h\in N}\chi(h){}^g\psi(h^{-1}) &\quad=\quad \frac{1}{|N|}\sum_{h\in N}\chi(h)\psi(g^{-1}h^{-1}g)\\ &\overset{\chi\in\mathcal{C}l(G)}{=}\frac{1}{|N|}\sum_{h\in N}\chi(g^{-1}hg)\psi(g^{-1}h^{-1}g)\\ &\overset{s:=g^{-1}hg\in N}{=}\frac{1}{|N|}\sum_{s\in N}\chi(s)\psi(s^{-1})=\langle\chi\downarrow_N^G,\psi\rangle_N=e\,.\end{aligned}$$

Therefore, every G-conjugate ${}^g\psi$ ($g\in[G/\mathcal{I}_G(\psi)]$) of ψ occurs as a constituent of $\chi\downarrow_N^G$ with the same multiplicity e. The claim about the degrees is then clear as ${}^g\psi(1)=\psi(1)\ \forall g\in G$.

(b) **Claim 1:** $\eta\in\operatorname{Irr}(\mathcal{I}\mid\psi)\ \Rightarrow\ \eta\uparrow_{\mathcal{I}}^G\in\operatorname{Irr}(G|\psi)$.

Since $\mathcal{I}=\mathcal{I}_{\mathcal{I}}(\psi)$, (a) implies that $\eta\downarrow_N^{\mathcal{I}}=e'\psi$ with $e'=\langle\eta\downarrow_N^{\mathcal{I}},\psi\rangle_N=\frac{\eta(1)}{\psi(1)}>0$. Now, let $\chi\in\operatorname{Irr}(G)$ be a constituent of $\eta\uparrow_{\mathcal{I}}^G$. By Frobenius Reciprocity we have

$$0\neq\langle\chi,\eta\uparrow_{\mathcal{I}}^G\rangle_G=\langle\chi\downarrow_{\mathcal{I}}^G,\eta\rangle_{\mathcal{I}}\,.$$

It follows that $\eta\downarrow_N^{\mathcal{I}}$ is a constituent of $\chi\downarrow_{\mathcal{I}}^G\downarrow_N^{\mathcal{I}}$ and

$$e:=\langle\chi\downarrow_N^G,\psi\rangle_N=\langle\chi\downarrow_{\mathcal{I}}^G\downarrow_N^{\mathcal{I}},\psi\rangle_N\geqslant\langle\eta\downarrow_N^{\mathcal{I}},\psi\rangle_N=e'>0\,,$$

hence $\chi\in\operatorname{Irr}(G|\psi)$. Moreover, by (a) we have $e=\langle\chi\downarrow_N^G,{}^g\psi\rangle_N\geqslant e'$ for each $g\in G$. Therefore,

$$\chi(1)=e\sum_{g\in[G/\mathcal{I}]}{}^g\psi(1)\overset{(a)}{=}e|G:\mathcal{I}|\psi(1)\geqslant e'|G:\mathcal{I}|\psi(1)=|G:\mathcal{I}|\eta(1)=\eta\uparrow_{\mathcal{I}}^G(1)\geqslant\chi(1)\,.$$

Thus $e=e'$, $\eta\uparrow_{\mathcal{I}}^G=\chi\in\operatorname{Irr}(G)$, and therefore $\eta\uparrow_{\mathcal{I}}^G\in\operatorname{Irr}(G|\psi)$.

Claim 2: $\chi\in\operatorname{Irr}(G\mid\psi)\ \Rightarrow\ \exists!\,\eta\in\operatorname{Irr}(\mathcal{I}\mid\psi)$ such that $\langle\chi\downarrow_{\mathcal{I}}^G,\eta\rangle_{\mathcal{I}}\neq 0$.

Again by (a), as $\chi\in\operatorname{Irr}(G\mid\psi)$, we have $\chi\downarrow_N^G=e\sum_{g\in[G/\mathcal{I}]}{}^g\psi$, where $e=\langle\chi\downarrow_N^G,\psi\rangle_N\in\mathbb{Z}_{>0}$. Therefore, there exists $\eta\in\operatorname{Irr}(\mathcal{I})$ such that

$$\langle\chi\downarrow_{\mathcal{I}}^G,\eta\rangle_{\mathcal{I}}\neq 0\neq\langle\eta\downarrow_N^{\mathcal{I}},\psi\rangle_N$$

because $\chi\downarrow_N^G=\chi\downarrow_{\mathcal{I}}^G\downarrow_N^{\mathcal{I}}$, so in particular $\eta\in\operatorname{Irr}(\mathcal{I}\mid\psi)$. Hence existence holds and it remains to see that uniqueness holds. Again by Frobenius reciprocity we have $0\neq\langle\chi,\eta\uparrow_{\mathcal{I}}^G\rangle_G$. By Claim 1 this forces $\chi=\eta\uparrow_{\mathcal{I}}^G$ and $\eta\downarrow_N^{\mathcal{I}}=e\psi$, so e is also the ramification index of ψ in $\mathcal{I}$.

Now, write $\chi\downarrow_{\mathcal{I}}^G=\sum_{\lambda\in\operatorname{Irr}(\mathcal{I})}a_\lambda\lambda=\sum_{\lambda\neq\eta}a_\lambda\lambda+a_\eta\eta$ with $a_\lambda\geqslant 0$ for each $\lambda\in\operatorname{Irr}(\mathcal{I})$ and $a_\eta>0$. It follows that

$$(a_\eta-1)\eta\downarrow_N^{\mathcal{I}}+\sum_{\lambda\neq\eta}a_\lambda\lambda\downarrow_N^{\mathcal{I}}=\underbrace{\chi\downarrow_N^G}_{=e\sum_{g\in[G/\mathcal{I}]}{}^g\psi}-\underbrace{\eta\downarrow_N^{\mathcal{I}}}_{=e\psi}=e\sum_{g\in[G/\mathcal{I}]\setminus[1]}{}^g\psi.$$

Since ψ does not occur in this sum, but occurs in $\eta\downarrow_N^{\mathcal{I}}$, the only possibility is $a_\eta=1$ and $\lambda\notin\operatorname{Irr}(\mathcal{I}|\psi)$ for $\lambda\neq\eta$. Thus η is uniquely determined as the only constituent of $\chi\downarrow_{\mathcal{I}}^G$ in $\operatorname{Irr}(\mathcal{I}\mid\psi)$.

Finally, Claims 1 and 2 prove that $\operatorname{Ind}_{\mathcal{I}}^G:\operatorname{Irr}(\mathcal{I}\mid\psi)\longrightarrow\operatorname{Irr}(G\mid\psi),\eta\mapsto\eta\uparrow_{\mathcal{I}}^G$ is well-defined and bijective, and the proof of Claim 2 shows that the ramification indices are preserved. ■

Example 13 (*Normal subgroups of index 2*)

Let $N < G$ be a subgroup of index $|G:N| = 2$ ($\Rightarrow N \lhd G$) and let $\chi \in \mathrm{Irr}(G)$, then either

(1) $\chi\downarrow_N^G \in \mathrm{Irr}(N)$, or

(2) $\chi\downarrow_N^G = \psi + {}^g\psi$ for a $\psi \in \mathrm{Irr}(N)$ and a $g \in G\backslash N$.

Indeed, let $\psi \in \mathrm{Irr}(N)$ be a constituent of $\chi\downarrow_N^G$. Since $|G:N| = 2$, we have $\mathcal{I}_G(\psi) \in \{N, G\}$. Theorem 21.8 yields the following:

- If $\mathcal{I}_G(\psi) = N$ then $\mathrm{Irr}(\mathcal{I}_G(\psi) \mid \psi) = \{\psi\}$ and $\psi\uparrow_N^G = \chi$, so that $e = 1$ and we get $\chi\downarrow_N^G = \psi + {}^g\psi$ for any $g \in G\backslash N$.
- If $\mathcal{I}_G(\psi) = G$ then $G/\mathcal{I}_G(\psi) = \{1\}$, so that
$$\chi\downarrow_N^G = e\psi \qquad \text{with } e = \langle \chi\downarrow_N^G, \psi\rangle_N = \langle \chi, \psi\uparrow_N^G\rangle_G\,.$$
Moroever, by Lemma 21.6(c),
$$\psi\uparrow_N^G\downarrow_N^G = |\mathcal{I}_G(\psi):N| \sum_{g\in[G/\mathcal{I}_G(\psi)]} {}^g\psi = 2\psi\,.$$
Hence
$$2\psi(1) = \psi\uparrow_N^G\downarrow_N^G(1) \geqslant \chi\downarrow_N^G(1) = \chi(1) = e\psi(1) \quad \Rightarrow \quad e \leqslant 2\,.$$
Were $e = 2$ then we would have $2\psi(1) = \psi\uparrow_N^G(1)$, hence $\chi = \psi\uparrow_N^G$ and thus
$$1 = \langle \chi, \psi\uparrow_N^G\rangle_G = \langle \chi\downarrow_N^G, \psi\rangle_N = e = 2$$
a contradiction. Whence $e = 1$, which implies that $\chi\downarrow_N^G \in \mathrm{Irr}(N)$. Moreover, $\psi\uparrow_N^G = \chi + \chi'$ for some $\chi' \in \mathrm{Irr}(G)$ such that $\chi' \neq \chi$.

Remember that we have proved that the degree of an irreducible character of a finite group G divides the index of the centre $|G : Z(G)|$. The following consequence of Clifford's theorem due to N. Itô provides us with yet a stronger divisibility criterion.

Theorem 21.9 (Itô)

Let $A \leqslant G$ be an abelian subgroup of G and let $\chi \in \mathrm{Irr}(G)$. Then the following assertions hold:

(a) $\chi(1) \leqslant |G:A|$; and

(b) if $A \trianglelefteq G$, then $\chi(1) \,\big|\, |G:A|$.

Proof: (a) Exercise!

(b) Let $\psi \in \mathrm{Irr}(A)$ be a constituent of $\chi\downarrow_A^G$, so that in other words $\chi \in \mathrm{Irr}(G \mid \psi)$. By Theorem 21.8(b) there exists $\eta \in \mathrm{Irr}(\mathcal{I}_G(\psi) \mid \psi)$ such that $\chi = \eta\uparrow_{\mathcal{I}_G(\psi)}^G$ and $\eta\downarrow_A^{\mathcal{I}_G(\psi)} = e\psi$ (proof of Claim 2). Now, as A is abelian, all the irreducible characters of A have degree 1 and for each $x \in A$, $\psi(x)$ is an $o(x)$-th root of unity. Hence $\forall\, x \in A$ we have
$$|\eta(x)| = |\eta\downarrow_A^{\mathcal{I}_G(\psi)}(x)| = |e\psi(x)| = e|\psi(x)| = e \cdot 1 = e = \eta(1) \quad \Rightarrow \quad A \subseteq Z(\eta)\,.$$

Therefore, by Remark 18.5, we have

$$\eta(1) \,\Big|\, |\mathcal{I}_G(\psi) : Z(\eta)| \,\Big|\, |\mathcal{I}_G(\psi) : A|$$

and since $\chi = \eta\uparrow^G_{\mathcal{I}_G(\psi)}$ it follows that

$$\chi(1) = |G : \mathcal{I}_G(\psi)| \cdot \eta(1) \,\Big|\, |G : \mathcal{I}_G(\psi)| \cdot |\mathcal{I}_G(\psi) : A| = |G : A|\,.$$

■

22 The Theorem of Gallagher

In the context of Clifford theory (Theorem 21.8) we understand that irreducibility of characters is preserved by induction from $\mathcal{I}_G(\psi)$ to G. Thus we need to understand induction of characters from N to $\mathcal{I}_G(\psi)$, in particular what if $G = \mathcal{I}_G(\psi)$. What can be said about $\mathrm{Irr}(G \mid \psi)$?

Lemma 22.1

Let $N \trianglelefteq G$ and let $\psi \in \mathrm{Irr}(N)$ such that $\mathcal{I}_G(\psi) = G$. Then

$$\psi\uparrow^G_N = \sum_{\chi\in\mathrm{Irr}(G)} e_\chi \chi$$

where $e_\chi := \langle \chi\downarrow^G_N, \psi\rangle_N$ is the ramification index of χ in N; in particular

$$\sum_{\chi\in\mathrm{Irr}(G)} e_\chi^2 = |G : N|\,.$$

Proof: Write $\psi\uparrow^G_N = \sum_{\chi\in\mathrm{Irr}(G)} a_\chi \chi$ for suitable $a_\chi \geqslant 0$ (i.e. $a_\chi = \langle \chi, \psi\uparrow^G_N\rangle_G$). By Frobenius reciprocity, $a_\chi \neq 0$ if and only if $\chi \in \mathrm{Irr}(G \mid \psi)$. But by Theorem 21.8: if $\chi \in \mathrm{Irr}(G|\psi)$, then $\chi\downarrow^G_N = e_\chi\psi$, so

$$e_\chi = \langle \chi\downarrow^G_N, \psi\rangle_N = \langle \chi, \psi\uparrow^G_N\rangle_G = a_\chi \qquad \text{and also } \chi(1) = e_\chi \cdot \psi(1)\,.$$

Therefore,

$$|G : N| \cdot \psi(1) = \psi\uparrow^G_N (1) = \sum_{\chi\in\mathrm{Irr}(G)} a_\chi \chi(1) = \sum_{\chi\in\mathrm{Irr}(G)} e_\chi \chi(1) = \sum_{\chi\in\mathrm{Irr}(G)} e_\chi^2 \psi(1) = \psi(1) \cdot \sum_{\chi\in\mathrm{Irr}(G)} e_\chi^2$$

and it follows that $|G : N| = \sum_{\chi\in\mathrm{Irr}(G)} e_\chi^2$. ■

Therefore the multiplicities $\{e_\chi\}_{\chi\in\mathrm{Irr}(G)}$ behave like the irreducible character degrees of the factor group G/N. This is not a coincidence in many cases.

Definition 22.2 (*Extension of a character*)

Let $N \trianglelefteq G$ and $\chi \in \mathrm{Irr}(G)$ such that $\psi := \chi\downarrow^G_N$ is irreducible. Then we say that ψ **extends to** G, and χ is an **extension of** ψ.

Exercise 22.3

Let $N \trianglelefteq G$ and $\chi \in \mathrm{Irr}(G)$. Prove that

$$\chi\downarrow^G_N\uparrow^G_N = \mathrm{Inf}^G_{G/N}(\chi_{\mathrm{reg}}) \cdot \chi\,,$$

where χ_{reg} is the regular character of G/N.

Theorem 22.4 (Gallagher)

Let $N \trianglelefteq G$ and let $\chi \in \mathrm{Irr}(G)$ such that $\psi := \chi\downarrow^G_N \in \mathrm{Irr}(N)$. Then

$$\psi\uparrow^G_N = \sum_{\lambda \in \mathrm{Irr}(G/N)} \lambda(1)\ \mathrm{Inf}^G_{G/N}(\lambda) \cdot \chi,$$

where the elements of the set $\{\mathrm{Inf}^G_{G/N}(\lambda) \cdot \chi \mid \lambda \in \mathrm{Irr}(G/N)\}$ are are pairwise distinct irreducible characters of G.

Proof: By Exercise 22.3 we have $\psi\uparrow^G_N = \mathrm{Inf}^G_{G/N}(\chi_{\mathrm{reg}}) \cdot \chi$, where χ_{reg} denotes the regular character of G/N. Recall that by Theorem 10.3, $\chi_{\mathrm{reg}} = \sum_{\lambda \in \mathrm{Irr}(G/N)} \lambda(1)\,\lambda$, so that we have

$$\psi\uparrow^G_N = \sum_{\lambda \in \mathrm{Irr}(G/N)} \lambda(1)\,\mathrm{Inf}^G_{G/N}(\lambda) \cdot \chi\,.$$

Now, by Lemma 22.1, we have

$$\begin{aligned}|G:N| = \sum_{\tilde{\chi} \in \mathrm{Irr}(G)} e^2_{\tilde{\chi}} = \langle \psi\uparrow^G_N, \psi\uparrow^G_N\rangle_G &= \sum_{\lambda,\mu \in \mathrm{Irr}(G/N)} \lambda(1)\mu(1)\langle \mathrm{Inf}^G_{G/N}(\lambda)\cdot\chi, \mathrm{Inf}^G_{G/N}(\mu)\cdot\chi\rangle_G \\ &\geqslant \sum_{\lambda \in \mathrm{Irr}(G/N)} \lambda(1)^2 = |G:N|\,.\end{aligned}$$

Hence equality holds throughout. This proves that

$$\langle \mathrm{Inf}^G_{G/N}(\lambda)\cdot\chi, \mathrm{Inf}^G_{G/N}(\mu)\cdot\chi\rangle = \delta_{\lambda\mu}.$$

By Erercise 13.4, $\mathrm{Inf}^G_{G/N}(\lambda)\cdot\chi$ are characters of G and hence the characters $\{\mathrm{Inf}^G_{G/N}(\lambda)\cdot\chi \mid \lambda \in \mathrm{Irr}(G/N)\}$ are irreducible and pairwise distinct, as claimed. ∎

Therefore, given $\psi \in \mathrm{Irr}(N)$ which extends to $\chi \in \mathrm{Irr}(G)$, we get $\mathrm{Inf}^G_{G/N}(\lambda) \cdot \chi$ ($\lambda \in \mathrm{Irr}(G/N)$) as further irreducible characters.

Example 14

Let $N < G$ with $|G:N| = 2$ ($\Rightarrow N \trianglelefteq G$) and let $\psi \in \mathrm{Irr}(N)$. We saw:

- if $\mathcal{I}_G(\psi) = N$ then $\psi\uparrow^G_N \in \mathrm{Irr}(G)$;
- if $\mathcal{I}_G(\psi) = G$ then ψ extends to some $\chi \in \mathrm{Irr}(G)$ and $\psi\uparrow^G_N = \chi + \chi'$ with $\chi' \in \mathrm{Irr}(G)\backslash\{\chi\}$. It follows that $\chi' = \chi \cdot \mathrm{sign}$, where sign is the inflation of the sign character of $G/N \cong S_2$ to G.

Chapter 7. Frobenius Groups

In this chapter we show how to understand the irreducible characters of an important class of finite groups: the *Frobenius groups*. After Burnside's $p^a q^b$-Theorem this provides us with a second fundamental application of character theory to the structure theory of finite groups.

Notation: throughout this chapter, unless otherwise specified, we let:

- G denote a finite group in multiplicative notation with neutral element $1 := 1_G$;
- $K := \mathbb{C}$ be the field of complex numbers.

In general, unless otherwise stated, all groups considered are assumed to be finite and all $\mathbb{C}$-vector spaces / modules over the group algebra considered are assumed to be finite-dimensional.

23 Frobenius Group / Frobenius Complement / Frobenius Kernel

Definition 23.1 (*Frobenius group / Frobenius complement*)

A finite group G admitting a non-trivial proper subgroup H such that

$$H \cap {}^gH = \{1\} \qquad \forall\, g \in G \backslash H$$

is called a **Frobenius group** with **Frobenius complement** H or a **Frobenius group with respect to** H.

Note: The definition implies immediately that $N_G(H) = H$. Also, a Frobenius complement need not be unique.

Example 15

Assume $P \in \mathrm{Syl}_p(G)$ is such that $|P| = p$ and $N_G(P) = P < G$. (In words: P is cyclic of order p and self-normalising!) Then, clearly, $P \cap {}^gP = \{1\}$ for any $g \in G \backslash P = G \backslash N_G(P)$, and so G is a Frobenius group with Frobenius complement P.

This yields immediately that the following well-known groups are Frobenius groups:

(1) the symmetric group $\mathfrak{S}_3$ is a Frobenius group with Frobenius complement $\langle(1\ 2)\rangle$;

(2) the dihedral group
$$D_{2(2m+1)} = \langle a, b \mid a^{2m+1} = b^2 = (ab)^2 = 1\rangle$$
of order $2(2m+1)$ with $m \in \mathbb{Z}_{\geqslant 1}$ is a Frobenius group with Frobenius complement $\langle b\rangle$;

(3) the alternating group $\mathfrak{A}_4$ is a Frobenius group with Frobenius complement $\langle(1\ 2\ 3)\rangle$;

(4) non-abelian groups of order $p \cdot q$ with $3 \leqslant p < q$ are Frobenius groups with Frobenius complement given by a Sylow p-subgroup of G.

Theorem 23.2 (Frobenius)

If G is a Frobenius group with Frobenius complement H, then there exists a normal subgroup $N \trianglelefteq G$ such that $G = HN$ and $H \cap N = \{1\}$. Moreover, such an N is uniquely determined, and it is called the **Frobenius kernel**.

We see below that the normal subgroup N is easily defined as a set and proved to be unique with the required properties; the crux of the difficulty lies in proving that it is a subgroup of G. This requires character theoretical arguments!

Proof: Define $N := \big(G \setminus \bigcup_{g\in G} {}^gH\big) \cup \{1\}$.

Claim 1: $H \cap N = \{1\}$ and $|N| = |G : H|$.

Indeed, from the definition of N we have $H \cap N = \{1\}$ and from the definition of Frobenius complement, $H = N_G(H)$, so there are exactly $|G : N_G(H)| = |G : H|$ distinct conjugates ${}^gH$ of H because if $g, x \in G$ then we have:
$${}^gH = {}^xH \Leftrightarrow x^{-1}g \in N_G(H) = H \Leftrightarrow gH = xH\,.$$
Moreover, these have only the identity element in common, because if $g, x \in G$ are such that ${}^gH \neq {}^xH$, then $x^{-1}g \notin N_G(H) = H$, so by the definition of the Frobenius complement,
$$\{1\} = {}^{x^{-1}g}H \cap H = {}^{x^{-1}}({}^gH \cap {}^xH)\,,$$
proving that ${}^gH \cap {}^xH = \{1\}$. It now follows that
$$\Big|\bigcup_{g\in G} {}^gH\Big| = |G : H| \cdot (|H| - 1) + 1 = |G| - |G : H| + 1\,.$$
It follows that
$$|N| = |G| - \Big|\bigcup_{g\in G} {}^gH\Big| + 1 = |G| - |G| + |G : H| - 1 + 1 = |G : H|\,.$$

Claim 2: if G contains a normal subgroup $\widetilde{N}$ such that $\widetilde{N}H = G$ and $\widetilde{N} \cap H = \{1_G\}$, then $\widetilde{N} = N$.
(*Be careful! At this stage, this does not mean that such an $\widetilde{N}$ exists!*)

Indeed, since $\widetilde{N} \cap H = \{1_G\}$ and $\widetilde{N} \trianglelefteq G$, certainly
$$\widetilde{N} \cap {}^gH = {}^g\widetilde{N} \cap {}^gH = {}^g(\widetilde{N} \cap H) = {}^g\{1\} = \{1\}$$
for any $g \in G$, whence $\widetilde{N} \subseteq N$ by the definition of N. Moreover, the 2nd Isomorphism Theorem implies that $|\widetilde{N}| = |G : H| = |N|$, where the 2nd equality holds by Claim 1, proving that $\widetilde{N} = N$.

Claim 3: if $\theta \in \mathcal{C}l(H)$ is such that $\theta(1_H) = 0$, then $\theta\uparrow_H^G\downarrow_H^G = \theta$.
To begin with, the values of the two class functions $\theta\uparrow_H^G\downarrow_H^G$ and θ at 1 coincide since by Corollary 20.7 we have $\theta\uparrow_H^G\downarrow_H^G(1) = |G : H| \cdot \theta(1) = 0$. Now, let $h \in H\backslash\{1\}$. Then, given $x \in G$, $\theta^\circ(xhx^{-1}) \neq 0$ only if ${}^xh \neq 1$ and ${}^xh \in H \cap {}^xH$, so $x \in H$. Moreover, as θ is a class function, we get

$$\theta\uparrow_H^G(h) = \frac{1}{|H|}\sum_{x\in G}\theta^\circ(xhx^{-1}) = \frac{1}{|H|}\sum_{x\in H}\theta(h) = \theta(h)\,,$$

as required.

Claim 4: $\mathrm{Ind}_H^G : \{\theta \in \mathcal{C}l(H) \mid \theta(1) = 0\} \longrightarrow \mathcal{C}l(G), \theta \mapsto \theta\uparrow_H^G$ is an isometry with respect to the scalar products $\langle -, -\rangle_H$ and $\langle -, -\rangle_G$.
Indeed, let $\theta, \eta \in \mathcal{C}l(H)$ be such that $\theta(1_H) = 0 = \eta(1)$. Then Frobenius Reciprocity and Claim 3 yield

$$\langle \theta\uparrow_H^G, \eta\uparrow_H^G\rangle_G = \langle \theta\uparrow_H^G\downarrow_H^G, \eta\rangle_H = \langle \theta, \eta\rangle_H\,,$$

as desired.

Claim 5: If $\eta \in \mathrm{Irr}(H)\}$ and $\theta := \eta - \eta(1)\mathbf{1}_H$, then $\eta^* := \theta\uparrow_H^G + \eta(1)\mathbf{1}_G$ is an irreducible character of G.
Clearly, $\theta \in \mathbb{Z}\mathrm{Irr}(H) \subseteq \mathcal{C}l(H)$, $\theta(1) = 0$, and $\eta^* \in \mathbb{Z}\mathrm{Irr}(G) \subseteq \mathcal{C}l(G)$ (see Remark 20.8). Now, on the one hand by Claim 4, we have

$$\langle \theta\uparrow_H^G, \theta\uparrow_H^G\rangle_G = \langle \theta, \theta\rangle_H = \langle \eta, \eta\rangle_H + \eta(1)^2\,.$$

On the other hand, by Frobenius reciprocity, $\langle \theta\uparrow_H^G, \mathbf{1}_G\rangle_G = \langle \theta, \mathbf{1}_H\rangle_H = -\eta(1)$, hence the above together with the fact that $\theta\uparrow_H^G$ is a virtual character (by Remark 20.8) implies that

$$\begin{aligned}\langle \eta^*, \eta^*\rangle_G &= \langle \theta\uparrow_H^G + \eta(1)\mathbf{1}_G, \theta\uparrow_H^G + \eta(1)\mathbf{1}_G\rangle_G\\ &= \langle \theta\uparrow_H^G, \theta\uparrow_H^G\rangle_G + 2\eta(1)\langle \theta\uparrow_H^G, \mathbf{1}_G\rangle_G + \eta(1)^2\langle \mathbf{1}_G, \mathbf{1}_G\rangle_G\\ &= \langle \eta, \eta\rangle_H + \eta(1)^2 + 2\eta(1)\cdot(-\eta(1)) + \eta(1)^2\\ &= \langle \eta, \eta\rangle_H = 1\end{aligned}$$

As η^* is a virtual character, it now follows that $\pm\eta^* \in \mathrm{Irr}(G)$. However,

$$\eta^*(1) = \theta\uparrow_H^G(1) + \eta(1)\mathbf{1}_G(1) = 0 + \eta(1)\cdot 1 = \eta(1) > 1\,,$$

whence $\eta^* \in \mathrm{Irr}(G)$.

The next claim eventually proves that N is a normal subgroup of G.

Claim 6: $N = \bigcap_{\eta\in\mathrm{Irr}(H)} \ker(\eta^*)$.
By Claim 5 ,

$$M := \bigcap_{\eta\in\mathrm{Irr}(H)} \ker(\eta^*)$$

defines a normal subgroup of G. First we claim that $M \leqslant N$. Observe that Claim 3 implies that for any $\eta \in \mathrm{Irr}(H)$,

$$\eta^*\downarrow_H^G = \theta\uparrow_H^G\downarrow_H^G + \eta(1)\mathbf{1}_G\downarrow_H^G = \theta + \eta(1)\mathbf{1}_H = \eta\,.$$

Thus, if $h \in M \cap H$, then for all $\eta \in \mathrm{Irr}(H)$, we have

$$\eta^*(1) = \eta^*(h) = \eta(h).$$

It follows that $\eta(h) = \eta(1)$ for all $\eta \in \mathrm{Irr}(H)$, and so

$$M \cap H \leqslant \bigcap_{\eta\in\mathrm{Irr}(H)} \ker(\eta) = \{1\}$$

where the last equality holds by Exercise 14.7. This proves that $M \cap H = \{1\}$, whence also $M \cap {}^xH = \{1\}$ for each $x \in G$ since $M \trianglelefteq H$. Therefore $M \leqslant N$, and it remains to prove that $N \leqslant M$. So, let $g \in N \setminus \{1\}$. Then, by the definition of N, for every $x \in G$, we have $g \notin {}^xH$. Hence, by definition of induced characters, $\theta\!\uparrow_H^G(g) = 0$ for each θ as defined in Claim 5, and so $\eta^*(g) = \eta^*(1)$ for each $\eta \in \mathrm{Irr}(H) \setminus \{\mathbf{1}_H\}$. It follows that $g \in \ker(\eta^*)$ for each $\eta \in \mathrm{Irr}(H)$, proving that $g \in M$. This proves Claim 6.

The statement of the theorem now follows from Claim 6, Claim 1 and Claim 2. ■

Remark 23.3

(a) To use standard group theory terminology, the theorem says that the Frobenius kernel is a *normal complement of H in G* and that G is an *internal semi-direct product of N by H*.

(b) There is no known proof of Frobenius' theorem which does not make use of character theory.

(c) Thompson proved that the Frobenius kernel N of a Frobenius group is always a nilpotent group (i.e. N is the direct product of its Sylow subgroups).

Exercise 23.4

(a) Find two non-isomorphic finite groups which are Frobenius groups and not isomorphic to any of the Frobenius groups given in Example 15.

(b) Find two infinite families of non-abelian finite groups which are not Frobenius groups.

Justify your answers with proofs.

24 Characters of Frobenius Groups

We now construct the whole character table of an arbitrary Frobenius group.

Theorem 24.1 (*Brauer's Permutation Lemma*)

Let A, B be finite groups, and assume that A acts on both $\mathrm{Irr}(B)$ and $C(B)$ via left actions

$$\begin{aligned} A \times \mathrm{Irr}(B) &\to \mathrm{Irr}(B), \quad (a, \chi) \mapsto a.\chi, \\ A \times C(B) &\to C(B), \quad (a, C) \mapsto a.C, \end{aligned}$$

such that $(a.\chi)(a.c) = \chi(c)$ for each $a \in A$, each $c \in C$ and each $C \in C(B)$. Then

$$|\,\mathrm{Fix}_{\mathrm{Irr}(B)}(a)| = |\{\chi \in \mathrm{Irr}(B) \mid a.\chi = \chi\}| = |\{C \in C(B) \mid a.C = C\}| = |\,\mathrm{Fix}_{C(B)}(a)|$$

for every $a \in A$. (In other words, the permutation representations induced by the two actions afford the same character.) Moreover, the number of A-orbits on $\mathrm{Irr}(B)$ and on $C(B)$ coincide.

Proof: Set $h := |\,\mathrm{Irr}(B)| = |C(B)|$ and write $\mathrm{Irr}(B) = \{\chi_1, \ldots, \chi_h\} =: X_1$ and $C(B) = \{C_1, \ldots, C_h\} =: X_2$. By Example 1(d), the A-actions on $\mathrm{Irr}(B) =: X_1$ and $C(B) =: X_2$ define permutation representations

$$\rho_{X_1} : A \to \mathrm{GL}(\mathbb{C}^h) \cong \mathrm{GL}_h(\mathbb{C}) \text{ and } \rho_{X_2} : A \to \mathrm{GL}(\mathbb{C}^h) \cong \mathrm{GL}_h(\mathbb{C})$$

respectively, which we see as matrix representations w.r.t. to the ordered $\mathbb{C}$-basis $(\chi_1, \ldots, \chi_h)$ and $(C_1, \ldots, C_h)$, respectively. Moreover, we denote by χ_{X_1} and χ_{X_2}, respectively, the characters afforded by these representations. Now, by Proposition 10.1, for each $a \in A$ we have

$$\chi_{X_1}(a) = |\mathrm{Fix}_{X_1}(a)| \qquad \text{and} \qquad \chi_{X_2}(a) = |\mathrm{Fix}_{X_2}(a)|\,.$$

Hence, in order to complete the proof of the first claim, it is enough to prove that $\chi_{X_1} = \chi_{X_2}$. Fix $a \in A$ and observe that the action of a on X_1 and X_2 permutes the rows and the columns of $X(B)$, sending the row indexed by χ_i to the row indexed by $a.\chi_i$, and the column indexed by C_j to the column indexed by $a^{-1}.C_j$. (The reason for this choice will become clear in the next lines.) Then, the permutation of the rows is given by left multiplication with $\rho_{X_1}(a)$, i.e. $\rho_{X_1}(a)X(B)$, and the permutation of the columns is given by right multiplication with $\rho_{X_2}(a)$, i.e. $X(B)\rho_{X_2}(a)$. Moreover, the hypothesis of the theorem implies that

$$(a.\chi)(c) = \chi(a^{-1}.c) \qquad \forall\, a \in A,\ \forall\, c \in C,\ \forall\, C \in C(B)\,.$$

It follows that

$$\rho_{X_1}(a)X(B) = X(B)\rho_{X_2}(a)$$

and hence, since $X(B)$ is an invertible matrix, we get

$$\rho_{X_1}(a) = X(B)\rho_{X_2}(a)X(B)^{-1}\,,$$

proving that $\rho_{X_1} \sim \rho_{X_2}$ and the claim follows.
For the last claim, remember that the number of A-orbits on $\mathrm{Irr}(B)$ is given by $\langle \chi_{X_1}, \mathbf{1}_A \rangle_A$ and the number of A-orbits on $C(B)$ is given by $\langle \chi_{X_2}, \mathbf{1}_A \rangle_A$. Now, both numbers are equal by the first claim. ■

We want to apply Brauer's Permutation Lemma in order to obtain information on the character table of Frobenius groups.

Remark 24.2

If $N \trianglelefteq G$, then G acts by conjugation on the sets $\mathrm{Irr}(N)$ and $C(N)$. In other words, there are left G-actions

$$\begin{array}{ccc} G \times \mathrm{Irr}(N) & \longrightarrow & \mathrm{Irr}(N) \\ (g, \chi) & \mapsto & g.\chi := {}^g\chi \end{array}$$

and

$$\begin{array}{ccc} G \times C(N) & \longrightarrow & C(N) \\ (g, C) & \mapsto & g.C := {}^gC = \{gcg^{-1} \mid c \in C\}\,. \end{array}$$

Moreover, it follows from the definition of a conjugate character that these actions satisfy the condition

$$(g.\chi)(g.c) = \chi(c) \qquad \forall\ c \in C \text{ and any } C \in C(N)\,.$$

It follows that we may apply Brauer's Permutation Lemma to this setting.

Theorem 24.3

Let G be an arbitrary finite group. Assume that $N \trianglelefteq G$ and assume that $C_G(n) \leqslant N$ for all $n \in N \backslash \{1\}$. Then, the following assertions hold:

(a) if $\psi \in \mathrm{Irr}(N) \backslash \{\mathbf{1}_N\}$, then $\psi\uparrow_N^G \in \mathrm{Irr}(G)$;

(b) if $\chi \in \mathrm{Irr}(G)$ is such that $N \nleqslant \ker(\chi)$, then there exists $\psi \in \mathrm{Irr}(N)$ such that $\chi = \psi\uparrow_N^G$.

Proof:

(a) First, it follows from the Mackey formula that $\langle \psi\uparrow_N^G, \psi\uparrow_N^G\rangle_G = \sum_{xN\in G/N}\langle {}^x\psi, \psi\rangle_N$. (See Exercise 21.5.) Thus, to prove that $\psi\uparrow_N^G$ is irreducible, it suffices to prove that $\psi \neq {}^x\psi$ for each $x \notin N$, since then the latter sum is equal to 1. Now, by Brauer's Permutation Lemma and Remark 24.2, it is enough to prove that for each conjugacy class $[1] \neq C \in C(N)$ and each $x \in G$ that the equality $xCx^{-1} = C$ implies that $x \in N$. So, let $n \in C$. Then, $xCx^{-1} = C$ implies that $xnx^{-1} = yny^{-1}$ for some $y \in N$ and hence $y^{-1}x \in C_G(n) \leqslant N$ by the hypothesis, proving that $x \in N$, as required.

(b) Since $N \nleqslant \ker(\chi)$, certainly $\chi\downarrow_N^G$ has at least one non-trivial constituent, say $\psi \in \mathrm{Irr}(N)\backslash\{\mathbf{1}_N\}$. Moreover, Frobenius reciprocity yields

$$\langle \chi, \psi\uparrow_N^G\rangle_G = \langle \chi\downarrow_N^G, \psi\rangle_H \neq 0\,.$$

Thus χ is a constituent of $\psi\uparrow_N^G$, but then this $\chi = \psi\uparrow_N^G$ since $\psi\uparrow_N^G \in \mathrm{Irr}(G)$ by (a). ■

This leads to the following characterisation of the irreducible characters of Frobenius groups.

Theorem 24.4

Let G be a Frobenius group with Frobenius complement H and Frobenius kernel N. Then,

$$\mathrm{Irr}(G) = \mathrm{Inf}_{G/N}^G\left(\mathrm{Irr}(G/N)\right) \sqcup \left\{\psi\uparrow_N^G \mid \psi \in \mathrm{Irr}(N)\backslash\{\mathbf{1}_N\}\right\}.$$

Note. Notice that the Frobenius complement H does not occur in the description of $\mathrm{Irr}(G)$. Thus, choosing a different Frobenius complement would not change the result. Also notice that the second set $\{\psi\uparrow_N^G \mid \psi \in \mathrm{Irr}(N)\backslash\{\mathbf{1}_N\}\}$ may contain repetitions! In order to describe all characters of G which do not have N in their kernel, it suffices to consider a set of representatives of the G-orbits for the conjugation action of G on $\mathrm{Irr}(N)\backslash\{\mathbf{1}_N\}$ instead of $\mathrm{Irr}(N)\backslash\{\mathbf{1}_N\}$.

Proof: It follows from Theorem 24.3 that it suffices to prove that $C_G(n) \leqslant N$ for all $n \in N\backslash\{1\}$. So, let $n \in N\backslash\{1\}$ and suppose that $C_G(n) \nleqslant N$. Then, by the definition of N, there exists $x \in G$ such that $C_G(n) \cap {}^xH \neq \{1\}$. Now, conjugating by x^{-1} and replacing n with $x^{-1}nx$, we may assume that $C_G(n) \cap H \neq \{1\}$. Thus, given $1 \neq h \in C_G(n) \cap H$, we have $h \in H \cap {}^nH$, which contradicts the fact that H is a Frobenius complement. ■

Exercise 24.5

Compute the character table of the dihedral group $D_{2(2m+1)}$ for all $m \in \mathbb{Z}_{\geqslant 1}$.

Exercise 24.6

Let $p \neq q$ be two prime numbers. Let G be a non-abelian finite group such that $|G| = pq$. Compute $|\mathrm{Irr}(G)|$ and $\chi(1_G)$ for each $\chi \in \mathrm{Irr}(G)$.

Exercise 24.7

Use Brauer's Permutation Lemma to prove that:

(a) the character table $X(S_n)$ is an integral matrix for all $n \geqslant 1$;

(b) if G is a finite group of odd order, then the map $\mathrm{Irr}(G) \longrightarrow \mathrm{Irr}(G), \chi \mapsto \overline{\chi}$ admits a unique fixed point, namely the trivial character $\mathbf{1}_G$.

Part II.
Semisimple Algebras and Their Modules

Chapter 8. Modules over arbitrary rings

In this chapter, we review important module-theoretic concepts and main results, which lie at the foundations of *module theory over arbitrary rings*:

1. **Simplicity and indecomposability** of modules.
2. **Schur's Lemma**: about homomorphisms between simple modules.
2. **Nakayama's Lemma**: about an essential property of the Jacobson radical.
3. **The Krull-Schmidt Theorem**: about direct sum decompositions into indecomposable submodules.

Notation: throughout this chapter, unless otherwise specified, we let $(R, +, \cdot)$ denote an arbitrary associative ring, which we assume to be unital. We denote the neutral element for the multiplication by 1_R or simply 1. Modules are assumed to be left modules.

25 (Ir)Reducibility and (In)decomposability

As already mentioned in Appendix A (see in particular Definition A.11) submodules and direct sums of modules allow us to introduce the two main notions which enable us to break modules in *elementary* pieces in order to simplify their study: *simplicity* and *indecomposability*.

Definition 25.1 (***simple/irreducible module / indecomposable module / semisimple module***)

(a) An R-module M is called **reducible** if it admits an R-submodule U such that $0 \subsetneq U \subsetneq M$. An R-module M is called **simple**, or **irreducible**, if it is non-zero and not reducible.
We let $\text{Irr}(R)$ denote a set of representatives of the isomorphism classes of simple R-modules.

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

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

Our goal for the forthcoming chapters is to investigate each of these concepts in more details.

Remark 25.2

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

Notice that Schur's Lemma (see 5.1) is true over an arbitrary ring. It reads as follows.

Theorem 25.3 (Schur's Lemma)

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

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

  (ii) if $V \not\cong W$, 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: Replacing KG by R (resp. A), copy, word for word, the proof of Theorem 5.1. ■

26 The Regular Module

The ring R itself maybe seen as an R-module via left multiplication in R. Similarly to Part I, where we used the regular representation in order to understand essential properties of the irreducible representations, we will be able to use this module to understand essential properties of the simple R-modules.

Definition 26.1 (*The regular module*)

The **regular** R-module, denoted R°, is the abelian group $(R, +)$ endowed with the external composition law
$$R \times R^\circ \longrightarrow R^\circ, (r, m) \mapsto r \cdot m\,.$$

Exercise 26.2

Prove that:

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

(b) $I \lhd R$ is a maximal left ideal of $R \Leftrightarrow R^\circ/I$ is a simple R-module; and

(c) $I \lhd R$ is a minimal left ideal of $R \Leftrightarrow I$ is simple when regarded as an R-submodule of R°.

27 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 chapters, this ideal carries a lot of information about the structure of a ring and that of its modules.

Proposition-Definition 27.1 (*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 the **annihilator** of M.

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

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

(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 Algebra II / Exercise! ■

Exercise 27.2

(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 (i.e. when regarded as additive abelian groups).

Theorem 27.3 (Nakayama's Lemma)

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

Proof: If $M = 0$, then the claim is trivial. So, assume $M \neq 0$ and let $\{m_1, \ldots, m_n\}$ ($n \in \mathbb{Z}_{>0}$) be a set of generators for M which is minimal in the sense that none of its proper subsets generates M. Since $J(R)M = M$, there exist elements $r_i \in J(R)$ for $i = 1, \ldots, n$ such that $m_1 = \sum_{i=1}^n r_i m_i$ and hence

$$(1 - r_1)m_1 = \sum_{i=2}^n r_i m_i$$

Now, Proposition-Definition 27.1(b) implies that $1 - r_1 \in R^\times$. Thus, letting $u := (1 - r_1)^{-1}$, we have

$$m_1 = 1_R \cdot m_1 = u(1 - r_1)m_1 = \sum_{i=2}^n u r_i m_i\,,$$

which is a contradiction to the minimality of $\{m_1, \ldots, m_n\}$. ■

Remark 27.4

(a) 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 interpreted as follows:

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

(b) The hypothesis that the module M be finitely generated is necessary. See Exercise 28.2(a)(ii) below.

28 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 28.1

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

Example 16

Any field K is local because $K\setminus K^\times = \{0\}$ by definition. The zero ring is not local.

Exercise 28.2

(a) Let p be a prime number and $R := \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$.

(i) Prove that $R\setminus R^\times = \{\frac{a}{b} \in R \mid p|a\}$ and deduce that R is local.

(ii) Assume $p = 2$ and consider the R-module $M := \mathbb{Q}$. Prove that $J(R)M = M$.

(b) Let K be a field and let $R := \left\{A \in M_n(K) \mid A = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & a_1 & \dots & a_{n-1} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & a_1 \end{pmatrix}\right\}$.

Prove that $R\setminus R^\times = \{A \in R \mid a_1 = 0\}$ and deduce that R is local.

Proposition 28.3

Let R be a ring. Then TFAE:

(a) R is local;

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

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

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

(a)⇒(b): Clear: $I \lhd R$ proper left ideal ⇒ $I \subseteq N$. Hence, by Proposition-Definition 27.1(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 27.1(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 28.4 (Fitting's Lemma)

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

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

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

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

Proof: By Corollary E.4 the module M satisfies both A.C.C. and D.C.C. on submodules. Hence the two chains of submodules

$$\varphi(M) \supseteq \varphi^2(M) \supseteq \ldots,$$

$$\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \ldots$$

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 28.5

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

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

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

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

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

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

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

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

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

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

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

would be invertible.
(Indeed, $\psi^{-1}\rho$ nilpotent $\Rightarrow$ $(\mathrm{Id}_M - \psi^{-1}\rho)(\mathrm{Id}_M + \psi^{-1}\rho + (\psi^{-1}\rho)^2 + \cdots + (\psi^{-1}\rho)^{a-1}) = \mathrm{Id}_M$, 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 27.1(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 28.3 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 28.6

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 28.7 (*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 the 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 the 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 28.5. 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 9. 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 dimensional algebra over a field and start the study of its representation theory.

Notation: throughout this chapter, unless otherwise specified, we let $(R, +, \cdot)$ denote a unital associative ring, and we recall that $\mathrm{Irr}(R)$ denotes a set of representatives for the simple R-modules and R° is the regular module.

29 Semisimplicity of Rings and Modules

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

Proposition 29.1

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

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

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

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

Before we prove of this result, it is useful to note the following property of semisimple modules.

Remark 29.2

Notice that if an R-module M satisfies Condition (c), then so does any R-submodule of M. (Take a complement in M and intersect with the submodule considered.) In other words, any submodule of a semisimple module is again semisimple.

Proof:
(a)$\Rightarrow$(b): is trivial.

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

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

Clearly this family is non-empty since it contains the empty set. Thus Zorn's Lemma yields the existence of a maximal element J_0. (Upper bounds are given by unions.) Now, set

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

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

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

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

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

(c)⇒(b): Let M_1 be the sum of all simple R-submodules in M. By (c) there exists a complement $M_2 \subseteq M$ to M_1, i.e. such that $M = M_1 \oplus M_2$.

- Case 1: $M_2 = 0$. We are done by definition of M_1.
- Case 2: $M_2 \neq 0$. We prove that this case cannot happen. In fact, it is enough to prove that M_2 contains a simple R-submodule, say L, since then $L \subseteq M_1$ by definition of M_1, which is a contradiction.
  So let $m \in M_2, m \neq 0$. By Remark 29.2 enough to treat the case $M_2 = Rm$. By Zorn's Lemma, there exists an R-submodule N of M_2, maximal w.r.t. the property that $m \notin N$. Take a (necessarily non-zero) R-submodule N' such that $M_2 = N \oplus N'$. Then N' is simple. Indeed, if N'' is a non-zero submodule of N', then $N \oplus N''$ must contain m by the maximality of N and so $N \oplus N'' = M_2$, which implies that $N'' = N'$, as required.

It follows that $M_2 = 0$, proving that $M = M_1$, as required. ■

Example 17

(a) The zero module is semisimple.

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

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

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

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

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

Theorem-Definition 29.3 (*Semisimple ring*)

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

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

(b) All R-modules are semisimple.

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

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

Proof: First, (a) and (b) are equivalent as a consequence of Lemma A.14 and the characterisation of semisimple modules given by Proposition 29.1(c). The implication (b) $\Rightarrow$ (c) is trivial, and it is also trivial that (c) implies the first claim of (d), which in turn implies the second claim of (d). Indeed, if $R^\circ = \bigoplus_{i\in I} L_i$ for some family $\{L_i\}_{i\in I}$ of minimal left ideals. Then, by definition of a direct sum, there exists a finite number of indices $i_1, \ldots, i_n \in I$ such that $1_R = x_{i_1} + \ldots + x_{i_n}$ with $x_{i_j} \in L_{i_j}$ for each $1 \leqslant j \leqslant n$. Therefore each $a \in R$ may be expressed in the form

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

and hence $R^\circ = L_{i_1} + \ldots + L_{i_n}$.
Therefore, it remains to prove that (d) $\Rightarrow$ (b). So, assume that R satisfies (d) and let M be an arbitrary non-zero R-module. Then write $M = \sum_{m\in M} R \cdot m$. Now, each cyclic submodule $R \cdot m$ of M is isomorphic to an R-submodule of R°, which is semisimple by (d). Thus $R \cdot m$ is semisimple as well by Example 17(d). Finally, it follows from Proposition 29.1(b) that M is semisimple. ■

Example 18

Fields are semisimple. Indeed, if V is a finite-dimensional vector space over a field K of dimension n, then choosing a K-basis $\{e_1, \cdots, e_n\}$ of V yields $V = Ke_1 \oplus \ldots \oplus Ke_n$, where $\dim_K(Ke_i) = 1$, hence Ke_i is a simple K-module for each $1 \leqslant i \leqslant n$. Hence, the claim follows from Theorem-Definition 29.3(c).

Corollary 29.4

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 29.3(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 E.4. In other words, R is both left Artinian and left Noetherian. ■

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

Definition 29.5 (*J-semisimplicity*)

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

Exercise 29.6

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 29.7

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

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

Claim: I_0 is a direct summand of R°.

Indeed: since

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

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

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

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

contradicting D.C.C. and proving the claim.

"⇐": Conversely, if R is semisimple, then $R^\circ \cong R/J(R) \oplus J(R)$ by Theorem-Definition 29.3 and so as R-modules,

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

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

■

Proposition 29.8

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

Proof: Since by Exercise 27.2 the rings R and $\overline{R} := R/J(R)$ have the same simple modules (seen as abelian groups), Proposition-Definition 27.1(a) yields

$$J(\overline{R}) = \bigcap_{V \in \mathrm{Irr}(\overline{R})} \mathrm{ann}_{\overline{R}}(V) = \bigcap_{V \in \mathrm{Irr}(R)} \mathrm{ann}_R(V) + J(R) = J(R)/J(R) = 0\,.$$

■

30 The Artin-Wedderburn Structure Theorem

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

Proposition 30.1

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

(iv) if $M = \bigoplus_{j\in J} V_j$ is an arbitrary decomposition of M into a direct sum of simple submodules, then
$$\widetilde{H}_i := \sum_{\substack{j\in J\\ V_j\cong M_i}} V_j = \bigoplus_{\substack{j\in J\\ V_j\cong M_i}} V_j = H_i \,.$$

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

Claim 1: If $M = \bigoplus_{j\in J} V_j$ as in (iv) and W is an arbitrary simple R-submodule of M, then $\exists\ j \in J$ such that $W \cong V_j$.

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

Claim 2: If $M = \bigoplus_{j\in J} V_j$ as in (iv), then $M = \bigoplus_{i\in I} \widetilde{H}_i$ and for each $i \in I$, every simple R-submodule of $\widetilde{H}_i$ is isomorphic to M_i.

Indeed: the 1st statement of the claim is obvious and the 2nd statement follows from Claim 1 applied to $\widetilde{H}_i$.

Claim 3: If W is an arbitrary simple R-submodule of M, then there is a unique $i \in I$ such that $W \subseteq \widetilde{H}_i$.

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

Claim 4: $\operatorname{Hom}_R(\widetilde{H}_i, \widetilde{H}_{i'}) = \{0\}$ if $i \neq i'$.

Indeed: if $0 \neq f \in \operatorname{Hom}_R(\widetilde{H}_i, \widetilde{H}_{i'})$ 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 30.1:

Definition 30.2

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

Exercise 30.3

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

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

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

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

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

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

Theorem 30.4 (*Wedderburn*)

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

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

(b) We have

$$R^\circ = \bigoplus_{S \in \mathrm{Irr}(R)} S(R^\circ)\,,$$

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

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

Proof:

(a) By Exercise 30.3(e) every simple left R-module is isomorphic to a minimal left ideal of R, i.e. a simple submodule of R°. Hence if $S \in \mathrm{Irr}(R)$, then $S(R^\circ) \neq 0$. Now, by Theorem-Definition 29.3, 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 30.1 any simple submodule of R° is isomorphic to V_j for some $j \in J$. Hence, we have $|\mathrm{Irr}(R)| \leqslant |J| < \infty$.

(b) Proposition 30.1(iv) also yields $S(R^\circ) = \bigoplus_{V_j \cong S} V_j$ and Proposition 30.1(i) implies that

$$R^\circ = \bigoplus_{S \in \mathrm{Irr}(R)} S(R^\circ)\,.$$

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 $T \in \mathrm{Irr}(R)$ 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 30.3(a), we may write

$$1_R = \sum_{S \in \mathrm{Irr}(R)} e_S\,,$$

where $S(R^\circ) = Re_S$ with e_S idempotent. Since $S(R^\circ)$ is a two-sided ideal, in fact we have $S(R^\circ) = Re_S = e_S R$. 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 $a = \sum_{T \in \mathrm{Irr}(R)} a_T$ with $a_T \in T(R^\circ)$. Since $S(R^\circ)T(R^\circ) = 0$ if $S \neq T \in \mathrm{Irr}(R)$, we have $e_S e_T = \delta_{ST} e_S$. Thus, as e_T is an identity element for the T-homogeneous component, we have

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

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 30.3 (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 30.5

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

(i) $e_S \in Z(R)$ for each $S \in \mathrm{Irr}(R)$;

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

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

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

Idempotents satisfying Property (i) are called **central** idempotents, and idempotents satisfying Property (ii) are called **orthogonal**. So, we say that $\{e_S \in R \mid S \in \mathrm{Irr}(R)\}$ is a set of pairwise distinct central idempotents of R.

Remark 30.6

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

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

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

Theorem 30.7 (*Artin-Wedderburn*)

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

$$R \cong \prod_{S\in\mathrm{Irr}(R)} M_{n_S}(D_S)\,,$$

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

Proof: By Exercise 30.3(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 30.1), Wedderburn's Theorem and the above observation yield

$$\mathrm{End}_R(R^\circ) = \mathrm{End}_R\Big(\bigoplus_{S\in\mathrm{Irr}(R)} S(R^\circ)\Big) \cong \prod_{S\in\mathrm{Irr}(R)} \mathrm{End}_R(S(R^\circ))$$

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. ■

31 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

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

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 31.1

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 K-homomorphism.

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

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

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

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

Theorem 31.2

Let A be a semisimple finite-dimensional algebra over an algebraically closed field K, and let $S \in \mathrm{Irr}(A)$ 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) $\dim_K(A) = \sum_{S \in \mathrm{Irr}(A)} \dim_K(S)^2$;

(d) $|\,\mathrm{Irr}(A)| = \dim_K(Z(A))$.

Proof:

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

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

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

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

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

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

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

Corollary 31.3

Let A be a finite-dimensional algebra over an algebraically closed field K. Then,

$$|\operatorname{Irr}(A)| = \dim_K(Z(A/J(A)))\,.$$

Proof: We have observed that A and $A/J(A)$ have the same simple modules (see Exercise 27.2), hence $|\operatorname{Irr}(A)| = |\operatorname{Irr}(A/J(A))|$. Moreover, the quotient $A/J(A)$ is J-semisimple by Proposition 29.8, hence semisimple by Proposition 29.7 because finite-dimensional algebras are left Artinian rings. Therefore it follows from Theorem 31.2(d) that

$$|\operatorname{Irr}(A)| = |\operatorname{Irr}(A/J(A))| = \dim_K\big(Z(A/J(A))\big)\,.$$

■

Corollary 31.4

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

Proof: First assume that A is semisimple. As A is commutative, $A = Z(A)$. Hence parts (d) and (c) of Theorem 31.2 yield

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

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

Finally, we emphasise that in this section the assumption that the field K is algebraically closed is in general too strong and that it is possible to weaken this hypothesis so that Theorem 31.2, Corollary 31.3 and Corollary 31.4 still hold.

Indeed, if $K = \overline{K}$ is algebraically closed, then Part (b) of Schur's Lemma tells us that $\operatorname{End}_A(S) \cong K$ for any simple A-module S. This is the crux of the proof of Theorem 31.2. The following terminology describes this situation.

Definition 31.5

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

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

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

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

Remark 31.6

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

(a) A is split;

(b) the product, for S running through $\mathrm{Irr}(A)$, of the structural homomorphisms $A \longrightarrow \mathrm{End}_K(S)$ (mapping $a \in A$ to the K-linear map $S \longrightarrow S, m \mapsto am$) induces an isomorphism of K-algebras

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

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

Exercise 31.7

Let K be a field and let $A \neq 0$ be a finite-dimensional K-algebra. The aim of this exercise is to prove that $J(A)$ is the unique maximal nilpotent left ideal of A and $J(Z(A)) = J(A) \cap Z(A)$.

Proceed as follows:

(a) Prove that there exists $n \in \mathbb{Z}_{>0}$ such that $J(A)^n = J(A)^{n+1}$.
[Hint: consider dimensions.]

(b) Apply Nakayama's Lemma to deduce that $J(A)^n = 0$ and conclude that $J(A)$ is nilpotent.

(c) Prove that if I is an arbitrary nilpotent left ideal of A, then $I \subseteq J(A)$.
[Hint: here you should see $J(A)$ as the intersection of the annihilators of the simple A-modules.]

(d) Use the nilpotency of the Jacobson radical to prove that $J(Z(A)) = J(A) \cap Z(A)\,.$

Chapter 10. Back to the Group Algebra

Our aim in this chapter is to understand what the general theory of semisimple rings and the Artin-Wedderburn theorem bring to the theory of representations of finite groups.

Notation. Throughout this chapter, unless otherwise specified, we let $(G, \cdot)$ denote a finite group and K be a field. All KG-modules considered are assumed to be finite-dimensional over K. This implies, in particular, that they are **finitely generated** as KG-modules.

32 The Augmentation Ideal

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

Proposition-Definition 32.1 (*The augmentation ideal*)

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

(a) $I(KG) = \{\sum_{g\in G} \lambda_g g \in KG \mid \sum_{g\in G} \lambda_g = 0\} = \operatorname{ann}_{KG}(K)$ 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 K-vector space of dimension $|G|$-1 with K-basis $\{g - 1 \mid g \in G \setminus \{1\}\}$.

Proof: First, observe that 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 KG. Moreover, each $x \in KG$ acts on K as multiplication by $\varepsilon(x)$, and so acts as 0 precisely when $\varepsilon(x) = 0$.

(a) We have $I(KG) = \ker(\varepsilon) = \{\sum_{g\in G} \lambda_g g \in KG \mid \sum_{g\in G} \lambda_g = 0\}$ by definition of ε. The second equality follows from the observation above as $\operatorname{ann}_{KG}(K) = \{x \in KG \mid x \cdot K = 0\}$. If K is a field, then the trivial KG-module K is simple, hence

$$\operatorname{ann}_{KG}(K) \supseteq \bigcap_{V\in \operatorname{Irr}(KG)} \operatorname{ann}_{KG}(V) = J(KG)\,.$$

(b) Since ε is clearly surjective, the claim is immediate 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

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

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

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

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

Lemma 32.2

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

Exercise 32.3 (*Proof of Lemma 32.2. Proceed as indicated.*)

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

(b) Prove that $g-1$ is a nilpotent element for each $g\in G\setminus\{1\}$ 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 31.7

(d) Conclude that $I(KG) = J(KG)$ using Proposition-Definition 32.1.

33 Semisimplicity and Maschke's Theorem

Our first aim is to reformulate the proof of Maschke's Theorem in module-theoretic terms.

Theorem 33.1 (*Maschke*)

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

Proof: By Theorem-Definition 29.3, 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 29.3). 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

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

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

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

and
$$\psi\tilde{\sigma}(n) = \frac{1}{|G|}\sum_{g\in G}\psi\left(g^{-1}\sigma(gn)\right) \overset{\psi\ KG\text{-lin}}{=} \frac{1}{|G|}\sum_{g\in G} g^{-1}\psi\sigma(gn) = \frac{1}{|G|}\sum_{g\in G} g^{-1}gn = n\,,$$
where the last-but-one equality holds because $\psi\sigma = \mathrm{Id}_N$. Thus $\tilde{\sigma}$ is a KG-linear section for ψ. ■

Example 19

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

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

Theorem 33.2 (*Converse of Maschke's Theorem*)

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

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

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

Indeed: Let $v = \sum_{g\in G}\lambda_g g \in V\backslash\{0\}$. If $\varepsilon(v) = 0$ we are done. Else, set $t := \sum_{h\in G} h$. Then
$$\varepsilon(t) = \sum_{h\in G} 1 = |G| = 0$$
as $\mathrm{char}(K) \mid |G|$. Hence $t \in I(KG)$. Now consider the element tv. On the one hand $tv \in V$ since V is a submodule of KG°, and on the other hand $tv \in I(KG)\backslash\{0\}$ since
$$tv = \Big(\sum_{h\in G} h\Big)\Big(\sum_{g\in G}\lambda_g g\Big) = \sum_{h,g\in G}(1_K\cdot\lambda_g)hg = \sum_{x\in G}\Big(\sum_{g\in G}\lambda_g\Big)x = \sum_{x\in G}\varepsilon(v)x \Rightarrow \varepsilon(tv) = \sum_{x\in G}\varepsilon(v) = |G|\varepsilon(v) = 0\,.$$

The Claim implies that $I(KG)$, which is a KG-submodule by definition, cannot have a complement in KG°. Therefore, by Proposition 29.1, KG° is not semisimple and hence KG is not semisimple by Theorem-Definition 29.3. ■

In the case in which the field K is algebraically closed, or a splitting field for KG, the following exercise offers a second proof of the converse of Maschke's Theorem exploiting the Artin-Wedderburn Theorem (Theorem 31.2).

Exercise 33.3 (*Proof of the Converse of Maschke's Theorem for K splitting field for KG.*)

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

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

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

(c) Deduce that KG is not a semisimple K-algebra using Theorem 31.2.

34 Simple Modules over Splitting Fields

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

As explained at the end of the previous chapter this assumption, slightly weaker than requiring that $K = \overline{K}$, implies that the conclusions of Theorem 31.2, Corollary 31.3 and Corollary 31.4 still hold.

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

Corollary 34.1

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

Proof: The claim follows directly from Assumption 34 and Corollary 31.3. ■

Corollary 34.2

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

Proof: Since KG is commutative the claim follows directly from Assumption 34 and Corollary 31.4. ■

Corollary 34.3

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

Proof: By Lemma 32.2 we have $J(KG) = I(KG)$. Thus $KG/J(KG) \cong K$ as K-algebras by Proposition-Definition 32.1(b). Now, as K is commutative, $Z(K) = K$, and it follows from Assumption 34 and Corollary 31.3 that

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

■

Remark 34.4

Another standard proof for Corollary 34.3 consists in using a result of Brauer's stating that $|\operatorname{Irr}(KG)|$ equals the number of conjugacy classes of G of elements of order not divisible by the characteristic of the field K.

Corollary 34.5

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

Proof: Since $\mathrm{char}(K) \nmid |G|$, the group algebra KG is semisimple by Maschke's Theorem. Thus it follows from Assumption 34 and Theorem 31.2 that

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

■

35 Outlook: Further Directions and Connected Topics

The topics treated in the last week of the semester do not appear in these notes. They are not officially part of this series of lectures and are not exam matters.

Appendix I: Complements on Algebraic Structures

This appendix provides a short recap / introduction to some of the basic notions of module theory used in this lecture.

Reference:

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

A Modules

Notation: Throughout this section we let $R = (R, +, \cdot)$ denote a unital associative ring.

Definition A.1 (*Left R-module*)

A **left** R**-module** is an ordered triple $(M, +, \cdot)$, where M is a set endowed with an **internal composition law**

$$\begin{array}{cccc} +: & M \times M & \longrightarrow & M \\ & (m_1, m_2) & \mapsto & m_1 + m_2 \end{array}$$

and an **external composition law** (or **scalar multiplication**)

$$\begin{array}{cccc} \cdot: & R \times M & \longrightarrow & M \\ & (r, m) & \mapsto & r \cdot m \end{array}$$

satisfying 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 every $r_1, r_2 \in R$ and every $m \in M$;

(M3) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ for every $r \in R$ and every $m_1, m_2 \in M$;

(M4) $(rs) \cdot m = r \cdot (s \cdot m)$ for every $r, s \in R$ and every $m \in M$.

(M5) $1_R \cdot m = m$ for every $m \in M$.

Remark A.2

(a) Note that in this definition both the addition in the ring R and in the module M are denoted with the same symbol. Similarly both the internal multiplication in the ring R and the external multiplication in the module M are denoted with the same symbol. This is standard practice and should not lead to confusion.

(b) **Right R-modules** can be defined analogously using a *right* external composition law $\cdot : M \times R \longrightarrow R, (m, r) \mapsto m \cdot r$.

(c) Unless otherwise stated, in this lecture we always work with left modules. Hence we simply write "R-module" to mean "left R-module", and as usual with algebraic structures, we simply denote R-modules by their underlying sets.

(d) We often write rm instead of $r \cdot m$.

Example A.3

(a) 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.
(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 by setting $r \cdot m := m \cdot r \; \forall\, r \in R, \forall\, m \in M$, and conversely.
(Check it! Where does the commutativity come into play?)

Definition A.4 (*R-submodule*)

An R-**submodule** of an R-module M is a subgroup $U \leqslant M$ such that $r \cdot u \in U \; \forall\, r \in R, \; \forall\, u \in U$.

Properties A.5 (*Direct sum of R-submodules*)

If U_1, U_2 are R-submodules of an R-module M, then so is $U_1 + U_2 := \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$. Such a sum $U_1 + U_2$ is called a **direct sum** if $U_1 \cap U_2 = \{0\}$ and in this case we write $U_1 \oplus U_2$.

Definition A.6 (*Morphisms*)

Let M, N be R-modules. A **(homo)morphism** of R-modules (or an R-**linear map**, or an R-**homomorphism**) is a map $\varphi : M \longrightarrow N$ such that:

(i) $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2) \; \forall\, m_1, m_2 \in M$; and

(ii) $\varphi(r \cdot m) = r \cdot \varphi(m) \; \forall\, r \in R, \; \forall\, m \in M$.

A bijective morphism of R-modules is called an R-**isomorphism** (or simply an **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**.

Properties A.7

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.

Notation A.8

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. This is a ring for the pointwise addition of maps and the usual composition of maps.

Lemma-Definition A.9 (*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** or the **quotient homomorphism**.

Proof: Similar proof as for groups/rings/vector spaces/... ■

Theorem A.10 (*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

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

(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: Similar proof as for groups/rings/vector spaces/... ■

Definition A.11 (***Irreducible/reducible/completely reducible module***)

An R-module M is called:

(a) **simple** (or **irreducible**) if it has exactly two submodules, namely the zero submodule 0 and itself;

(b) **reducible** if it admits a non-zero proper submodule $0 \subsetneq U \subsetneq M$;

(c) **semisimple** (or **completely reducible**) if it admits a direct sum decomposition into simple submodules.

Notice that the zero R-module 0 is neither reducible, nor irreducible, but it is completely reducible.

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 A.12 (***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 A.13 (***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 $\psi \in \operatorname{Hom}_R(M, N)$ is a surjective morphism, then there is a s.e.s.

$$0 \longrightarrow \ker(\psi) \xrightarrow{i} M \xrightarrow{\psi} N \longrightarrow 0\,,$$

where i is the canonical injection.

Lemma-Definition A.14 (*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 $\exists\, \sigma \in \operatorname{Hom}_R(N, M)$ such that $\psi \circ \sigma = \operatorname{Id}_N$;

(b) φ admits an R-linear retraction, i.e. if $\exists\, \rho \in \operatorname{Hom}_R(M, L)$ such that $\rho \circ \varphi = \operatorname{Id}_L$;

(c) $\exists$ an R-isomorphism $\alpha : M \longrightarrow L \oplus N$ such that the following diagram commutes:

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

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

Remark A.15

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 $M = \varphi(L) \oplus \ker(\rho)$.

B Algebras

In this lecture we aim at studying modules over *the group algebra*, which are specific rings.

Definition B.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; and

(ii) f is a ring homomorphism.

Example 20

(a) A commutative 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 a commutative ring 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) If K is a field and V a finite-dimensional K-vector space, then $\mathrm{End}_K(V)$ is a K-algebra.

(e) $\mathbb{R}$ and $\mathbb{C}$ are $\mathbb{Q}$-algebras, $\mathbb{C}$ is an $\mathbb{R}$-algebra, ...

(f) Rings are $\mathbb{Z}$-algebras.

Definition B.2 (*Centre*)

The **centre** of an R-algebra $(A, +, \cdot, *)$ is $Z(A) := \{a \in A \mid a \cdot b = b \cdot a \ \ \forall\, b \in A\}$.

C Tensor Products of Vector Spaces

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

Definition C.1 (*Tensor product of vector spaces*)

Let V, W be two finite-dimensional K-vector spaces with bases $B_V = \{v_1, \dots, v_n\}$ and $B_W = \{w_1, \dots, w_m\}$ ($m, n \in \mathbb{Z}_{\geqslant 0}$) respectively. The **tensor product of V and W (balanced) over K** is by definition the $(n \cdot m)$-dimensional K-vector space

$$V \otimes_K W$$

with basis $B_{V\otimes_K W} = \{v_i \otimes w_j \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$.

In this definition, you should understand the symbol "$v_i \otimes w_j$" as an element that depends on both v_i and w_j. The symbol "$\otimes$" itself does not have any hidden meaning, it is simply a piece of notation: we may as well write something like $x(v_i, w_j)$ instead of "$v_i \otimes w_j$", but we have chosen to write "$v_i \otimes w_j$".

Properties C.2

(a) An arbitrary element of $V \otimes_K W$ has the form

$$\sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_{ij}(v_i \otimes w_j) \quad \text{with } \{\lambda_{ij}\}_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} \subseteq K\,.$$

(b) The binary operation

$$\begin{array}{ccc} B_V \times B_W & \longrightarrow & B_{V\otimes_K W} \\ (v_i, w_j) & \mapsto & v_i \otimes w_j \end{array}$$

can be extended by K-linearity to

$$\begin{array}{rccc} -\otimes -: & V \times W & \longrightarrow & V \otimes_K W \\ & \left(v = \sum_{i=1}^{n} \lambda_i v_i, w = \sum_{i=1}^{n} \mu_j w_j\right) & \mapsto & v \otimes w = \sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_i \mu_j (v_i \otimes w_j)\,. \end{array}$$

It follows that $\forall\ v \in V, w \in W, \lambda \in K$,

$$v \otimes (\lambda w) = (\lambda v) \otimes w = \lambda(v \otimes w)\,,$$

and $\forall\ x_1, \dots, x_r \in V, y_1, \dots y_s \in W$,

$$\Big(\sum_{i=1}^{r} x_i\Big) \otimes \Big(\sum_{j=1}^{s} y_j\Big) = \sum_{i=1}^{r}\sum_{j=1}^{s} x_i \otimes y_j\,.$$

Thus any element of $V \otimes_K W$ may also be written as a K-linear combination of elements of the form $v \otimes w$ with $v \in V, w \in W$. In other words, $\{v \otimes w \mid v \in V, w \in W\}$ generates $V \otimes_K W$ (although it is not a K-basis).

(c) Up to isomorphism $V \otimes_K W$ is independent of the choice of the K-bases of V and W.

Definition C.3 (*Kronecker product*)

If $A = \left(A_{ij}\right)_{ij} \in M_n(K)$ and $B = \left(B_{rs}\right)_{rs} \in M_m(K)$ are two square matrices, then their **Kronecker product** (or **tensor product**) is the matrix

$$A \otimes B = \begin{bmatrix} A_{11}B \cdots\cdots A_{1n}B \\ \vdots \qquad\qquad \vdots \\ A_{n1}B \cdots\cdots A_{nn}B \end{bmatrix} \in M_{n \cdot m}(K)\,.$$

Notice that it is clear from the above definition that $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\,\mathrm{Tr}(B)$.

Example 21

E.g. the tensor product of two 2×2-matrices is of the form

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \otimes \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{bmatrix} \in M_4(K)\,.$$

Lemma-Definition C.4 (*Tensor product of K-endomorphisms*)

If $f_1 : V \longrightarrow V$ and $f_2 : W \longrightarrow W$ are two endomorphisms of finite-dimensional K-vector spaces V and W, then the **tensor product** of f_1 and f_2 is the K-endomorphism $f_1 \otimes f_2$ of $V \otimes_K W$ defined by

$$\begin{aligned} f_1 \otimes f_2 : \quad V \otimes_K W &\longrightarrow V \otimes_K W \\ v \otimes w &\mapsto (f_1 \otimes f_2)(v \otimes w) := f_1(v) \otimes f_2(w)\,. \end{aligned}$$

Furthermore, $\mathrm{Tr}(f_1 \otimes f_2) = \mathrm{Tr}(f_1)\,\mathrm{Tr}(f_2)$.

Proof: It is straightforward to check that $f_1 \otimes f_2$ is K-linear. Then, choosing ordered bases $B_V = (v_1, \dots, v_n)$ and $B_W = (w_1, \dots, w_m)$ of V and W respectively, it is straightforward from the definitions to check that the matrix of $f_1 \otimes f_2$ w.r.t. the basis $B_{V \otimes_K W}$, ordered w.r.t. the lexicographical order, is the Kronecker product of the matrices of f_1 w.r.t. B_V and of f_2 w.r.t. to B_W. The trace formula follows. ■

D Integrality and Algebraic Integers

We introduce here the concept of integrality for elements of a commutative ring. We are, however, essentially interested in the field of complex numbers and its subring $\mathbb{Z}$.

Definition D.1 (*integral element, algebraic integer*)

Let A be a subring of a commutative ring B.

(a) An element $b \in B$ is said to be **integral** over A if b is a root of monic polynomial $f \in A[X]$ (i.e. f is a polynomial of the form $X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ with $a_{n-1}, \ldots, a_0 \in A$ and $f(b) = 0$). If all the elements of B are integral over A, then we say that B is **integral** over A.

(b) If $A = \mathbb{Z}$ and $B = \mathbb{C}$, an element $b \in \mathbb{C}$ which is integral over $\mathbb{Z}$ is called an **algebraic integer**.

Theorem D.2

Let B be a commutative ring, let $A \subseteq B$ be a subring and let $b \in B$. Then, the following assertions are equivalent:

(a) b is integral over A;

(b) the ring $A[b]$ is finitely generated as an A-module;

(c) there exists a subring S of B containing A and b which is finitely generated as an A-module.

Recall that $A[b]$ denotes the subring of B generated by A and b.

Proof:

(a)⇒(b): Let $a_0, \ldots, a_{n-1} \in A$ such that $b^n + a_{n-1}b^{n-1} + \ldots + a_1b + a_0 = 0$ $(*)$. We prove that $A[b]$ is generated as an A-module by $1, b, \ldots, b^{n-1}$, i.e. $A[b] = A + Ab + \ldots + Ab^{n-1}$. Therefore, it suffices to prove that $b^k \in A + Ab + \ldots + Ab^{n-1} =: C$ for every $k \geqslant n$. We proceed by induction on k:

- If $k = n$, then $(*)$ yields $b^n = -a_{n-1}b^{n-1} - \ldots - a_1b - a_0 \in C$.
- If $k > n$, then we may assume that $b^n, \ldots, b^{k-1} \in C$ by the induction hypothesis. Hence multiplying $(*)$ by b^{k-n} yields

$$b^k = -a_{n-1}b^{k-1} - \ldots - a_1b^{k-n+1} - a_0b^{k-n} \in C$$

because $a_{n-1}, \ldots, a_0, b^{k-1}, \ldots, b^{k-n} \in C$.

(b)⇒(c): Set $S := A[b]$.

(c)⇒(a): By the assumption, $A[b] \subseteq S = Ax_1 + \ldots + Ax_n$, with $x_1, \ldots, x_n \in B$, $n \in \mathbb{Z}_{>0}$. Thus, for each $1 \leqslant i \leqslant n$ we have $bx_i = \sum_{j=1}^{n} a_{ij}x_j$ for certain $a_{ij} \in A$. Set $x := (x_1, \ldots, x_n)^{\mathrm{Tr}}$ and consider the $n \times n$-matrix $M := bI_n - (a_{ij})_{ij} \in M_n(S)$. Hence,

$$Mx = 0 \qquad \Rightarrow \quad \mathrm{adj}(M)Mx = 0\,,$$

where $\mathrm{adj}(M)$ is the adjugate matrix of M (i.e. the transpose of its cofactor matrix). By the properties of the determinant (Linear Algebra), we have

$$\mathrm{adj}(M)M = \det(M)I_n\,.$$

Hence, $\det(M)x_i = 0$ for each $1 \leqslant i \leqslant n$, and so we have $\det(M)s = 0$ for every $s \in S$. As $1 \in S$, this implies that $\det(M) = 0$. It now follows from the definition of M that b is a root of the monic polynomial $\det(X \cdot I_n - (a_{ij})_{ij}) \in A[X]$, thus integral over A.

■

Corollary D.3

Let B be a commutative ring and let $A \subseteq B$ be a subring. Then $\{b \in B \mid b \text{ integral over } A\}$ is a subring of B.

Proof: We need to prove that if $b, c \in B$ are integral over A, then so are $b + c$ and $b \cdot c$. By Theorem D.2(b) and its proof both $A[b]$ and $A[c]$ are finitely generated as an A-modules. More precisely, there exist $n, m \in \mathbb{Z}_{>0}$ such that $A[b] = A + Ab + \ldots + Ab^{n-1}$ and $A[c] = A + Ac + \ldots + Ac^{m-1}$. Thus, $S := A[b, c]$ is generated as an A-module by the set $\{b^i c^j \mid 0 \leqslant i < n, 0 \leqslant j < m\}$, i.e. finitely generated. Theorem D.2(c) now yields that $b + c$ and $b \cdot c$ are integral over A because they belong to S. ■

Example 22

All the elements of the ring $\mathbb{Z}[i]$ of Gaussian integers are integral over $\mathbb{Z}$, hence algebraic integers, since i is a root of $X^2 + 1 \in \mathbb{Z}[X]$.

Lemma D.4

If $b \in \mathbb{Q}$ is integral over $\mathbb{Z}$, then $b \in \mathbb{Z}$.

Proof: We may write $b = \frac{c}{d}$, where c and d are coprime integers and $d \geqslant 1$. By the hypothesis, there exist $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that

$$\frac{c^n}{d^n} + a_{n-1}\frac{c^{n-1}}{d^{n-1}} + \ldots + a_1\frac{c}{d} + a_0 = 0\,,$$

hence

$$c^n + \underbrace{da_{n-1}c^{n-1} + \ldots + d^{n-1}a_1 + d^n a_0}_{\text{divisible by } d} = 0\,.$$

Thus $d \mid c^n$. As $\gcd(c, d) = 1$ and $d \geqslant 1$ this is only possible if $d = 1$, and we deduce that $b \in \mathbb{Z}$. ■

Clearly, the aforementioned lemma can be generalised to integral domains and their field of fractions.

E Chain Conditions and the Jordan-Hölder Theorem

Definition E.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.

The zero module is understood to have a composition series $0 = M_0 = M$ (i.e. with $n = 0$) and composition length equal to 0. Moreover, clearly, in a composition series of a non-zero module all inclusions are in fact strict because the quotient modules are required to be simple, hence non-zero.

Definition E.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).

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*.

Theorem E.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 $M \neq 0$ which has a composition series 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 *Algebra II.* ■

Corollary E.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 *Algebra II.* ■

Theorem E.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 *Algebra II.* ■

Index of Notation

General symbols

$\mathbb{C}$	field of complex numbers
$\mathbb{F}_q$	finite field with q elements
i	primitive square root of one in $\mathbb{C}$
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
$\mathbb{P}$	the prime numbers in $\mathbb{Z}$
$\mathbb{Q}$	field of rational 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. $m > a, m \geqslant a, m < a$)$\}$
$\lvert X\rvert$	cardinality of the set X
δ_{ij}	Kronecker's delta
$\bigcup$	union
$\coprod$	disjoint union
$\bigcap$	intersection
$\sum$	summation symbol
$\prod$, $\times$	cartesian product
$\oplus$	direct sum
$\otimes$	tensor product
$\varnothing$	empty set
$\forall$	for all
$\exists$	there exists
$\cong$	isomorphism
$\overline{a}$	complex conjugate of $a \in \mathbb{C}$
$a \mid b$, $a \nmid b$	a divides b, a does not divide b
$f\vert_S$	restriction of the map f to the subset S

Group theory

A_n	alternating group on n letters
C_m	cyclic group of order m in multiplicative notation
$C_G(x)$	centraliser of x in G
$C(G)$	set of conjugacy classes of G
D_{2n}	dihedral group of order $2n$
$\mathrm{Fix}_X(g)$	set of fixed points of g on X

$[G,G]$ or G'	commutator subgroup of G
G/N	quotient group G modulo N
$\mathrm{GL}_n(K)$	general linear group over K
$H \leqslant G$, $H < G$	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
$\mathrm{PGL}_n(K)$	projective linear group over K
Q_8	quaternion group of order 8
S_n	symmetric group on n letters
$\mathrm{SL}_n(K)$	special linear group over K
$\mathrm{Syl}_p(G)$	set of Sylow p-subgroups of the group G
$Z(G)$	centre of the group G
$\mathbb{Z}/m\mathbb{Z}$	cyclic group of order m in additive notation
$\lvert G\rvert$	order of the group G
$\lvert G:H\rvert$	index of H in G
$[x]$	conjugacy class of x
$[g,h]$	commutator of g and h
$\langle g\rangle$	cyclic group generated by g
$\langle g \mid g^m = 1\rangle$	cyclic group of order m generated by g

Linear algebra

det	determinant of a matrix/linear transformation
$\dim_K$	K-dimension
$\mathrm{End}_K(V)$	endomorphism ring of the K-vector space V
$\mathrm{GL}(V)$	set of invertible linear transformations of the vector space V
$\langle x_1, \cdots, x_n\rangle_K$	K-linear span of the set $\{x_1, \cdots, x_n\}$
$M_{n\times m}(K)$	ring of $n \times m$-matrices with coefficients in K
$M_n(K)$	ring of $n \times n$-matrices with coefficients in K
$\overline{K}$	algebraic closure of the field K
Tr	trace of a matrix/linear transformation
$W \leqslant V$	W is a K-subspace of V
$\{e_1, \cdots, e_n\}$	a basis of K^n
$(e_1, \cdots, e_n)$	an ordered basis of K^n

Representations and characters

$C_1, \dots, C_r$	the conjugacy classes of G
$\widehat{C_1}, \dots, \widehat{C_r}$	the class sums of G
$\mathcal{C}l(G)$	$\mathbb{C}$-vector space of class functions on G
$\mathcal{I}_G(\psi)$	inertia group of ψ in G
$\mathrm{Inf}_{G/N}^G$	inflation from G/N to G
$\mathrm{Ind}_H^G, \uparrow_H^G$	induction from H to G
$\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$	set of irreducible characters of G
$\mathrm{Irr}(G\mid\psi)$	set of irreducible characters of G above ψ
$\ker(\chi)$	kernel of the characters of χ
$\mathcal{F}(G,K)$	space of K-valued functions of G

KG	group algebra of G over the field K
$\mathrm{Res}^G_H, \downarrow^G_H$	restriction from G to H
$Z(KG)$	centre of KG
$Z(\chi)$	centre of the character χ
$\rho \sim \rho'$	ρ is equivalent to ρ'
ρ_{reg}	the regular representation of G
ρ_V	representation associated to the G-vector space V
χ_{reg}	regular character of G
χ_V	character of the G-vector space V
$\omega_1, \ldots, \omega_r$	the central characters of G
$\langle -, - \rangle_G$	scalar product on $\mathcal{C}l(G)$
$\mathbf{1}_G$	the trivial character of G

Ring and 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
KG	group algebra of the group G over the field K
$\varepsilon : KG \longrightarrow K$	augmentation map
$I(KG)$	augmentation ideal
$\mathrm{Irr}(R)$	set of representatives of the isomorphism classes of simple R-modules
$J(R)$	Jacobson radical of the ring R
$M \mid N$	M is a direct summand of N
$M \otimes_R N$	tensor product of M and N balanced over R
R°	regular left R-module on the ring R

Greek Alphabet

lower-case letter	upper-case letter	name
α	A	alpha
β	B	beta
γ	Γ	gamma
δ	Δ	delta
ε, ϵ	E	epsilon
ζ	Z	zeta
η	H	eta
θ	Θ	theta
ι	I	iota
κ	K	kappa
λ	Λ	lambda
μ	M	mu
ν	N	nu
ξ	Ξ	xi
o	O	omicron
π, ϖ	Π	pi
ρ, ϱ	P	rho
σ, ς	Σ	sigma
τ	T	tau
υ	Υ	upsilon
ϕ, φ	Φ	phi
χ	X	chi
ψ	Ψ	psi
ω	Ω	omega