Character Theory of Finite Groups

Jun.-Prof. Dr. Caroline Lassueur
RPTU Kaiserslautern–Landau

Skript zur Vorlesung, SS 2022 + SS 2023
(Vorlesung: 2SWS // Übung: 1SWS)

Version: 30th of June 2023

Now contains:
small updates/typo corrections and

a Chapter 7 on Frobenius groups

Contents

This text constitutes a faithful transcript of the lecture **Character Theory of Finite Groups** held at the TU Kaiserslautern during the Summer Semester 2022 and the Summer Semester 2023 (14 Weeks, 2SWS Lecture + 1SWS Exercises).

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

- provide students with a modern approach to **finite group theory**;

- learn about the **ordinary character theory of finite groups**;

- 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.

We assume as pre-requisites bachelor-level algebra courses dealing with *linear algebra* and *elementary group theory*, such as the standard lectures *Grundlagen der Mathematik*, *Algebraische Strukturen*, and *Einführung in die Algebra*.

The 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 fortnightly exercise sheets.

The content of the appendix is important for the lecture. Some of you may have encountered (or will encounter) this material in other algebra lectures. For this reason, no direct question on the appendix will be asked in the oral exam.

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

Textbooks:

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

[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.

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.

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 $GL_n(K)$ 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 $GL(V) := \text{Aut}_K(V)$ 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
$$\rho : G \longrightarrow GL(V)$$
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 $R : G \longrightarrow GL_n(K)$.

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

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

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

$$
\begin{array}{ccc}
G & \xrightarrow{\quad \rho \quad} & \mathrm{GL}(V) \\
& \raisebox{1ex}{$\circlearrowleft$} & \cong \Big\downarrow \alpha_B \\
R_B := \alpha_B \circ \rho \searrow & & \\
& & \mathrm{GL}_n(K) \,.
\end{array}
$$

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

$$\rho: \quad G \quad \longrightarrow \quad \mathrm{GL}(K) \cong K^{\times}$$
$$g \quad \mapsto \quad \rho(g) := \mathrm{Id}_K \leftrightarrow 1_K$$

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

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

$$G \quad \hookrightarrow \quad \mathrm{GL}(V)$$
$$g \quad \mapsto \quad g$$

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

$$\rho: \quad S_n \quad \longrightarrow \quad \mathrm{GL}(K^n)$$
$$\sigma \quad \mapsto \quad \rho(\sigma) : K^n \longrightarrow K^n, e_i \mapsto e_{\sigma(i)}$$

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

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

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.

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

(b) If, moreover, α is a K-isomorphism, then it is called an **isomorphism of representations** (or a G-**isomorphism**), and the K-representations ρ_1 and ρ_2 are called **equivalent** (or **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
$$R_2(g) = T R_1(g) T^{-1} \qquad \forall \, g \in G \, .$$
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 $E := (e_1, \ldots, e_n)$, $F := (f_1, \ldots, f_n)$ are two ordered bases of V, then by Remark 1.2, we have two matrix representations:

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

These matrix representations are equivalent since $R_F(g) = T R_E(g) T^{-1} \ \forall \, g \in G$, 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

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

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

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

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 $B := (e_1, \ldots, e_n)$ be the standard basis of $V = K^n$. Then for each $g \in G$ we have

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

where the last equality holds because $\rho(g) : \{e_1, \ldots, e_n\} \longrightarrow \{e_1, \ldots, e_n\}, e_i \mapsto e_{g(i)}$ 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

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

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 $\rho_1 : G \longrightarrow GL(V_1)$ and $\rho_2 : G \longrightarrow GL(V_2)$ 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 $\rho : G \longrightarrow GL(V)$ 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

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

$$\quad\;\; B_1 \qquad\quad B_2$$

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

$$\begin{array}{rccc} R: & G & \longrightarrow & GL_2(K) \\ & g^b & \mapsto & \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right). \end{array}$$

(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

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

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

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

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

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

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) $\underline{\ker(\widetilde{\pi}) \text{ is } G\text{-invariant}}$: 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 $\operatorname{char}(K) \nmid |G|$, then every K-representation of G is completely reducible.

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

· <u>Case 1:</u> ρ is irreducible $\Rightarrow$ nothing to do $\checkmark$.

· <u>Case 2:</u> ρ is reducible. Thus $\dim_K(V) \geqslant 2$ and there exists an irreducible G-invariant K-subspace $0 \neq V_1 \lneqq V$. 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. $\blacksquare$

Remark 3.7

(a) The hypothesis of Maschke's Theorem requiring that $\operatorname{char}(K) \nmid |G|$ 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 $\operatorname{char}(K) \mid |G|$.

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 $\rho : G \longrightarrow \operatorname{GL}(V)$ 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.]

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. $\blacksquare$

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

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

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

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

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

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

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 $\mathrm{char}(K) \nmid |G|$, then every K-representation of G is completely reducible.		If $\mathrm{char}(K) \nmid |G|$, 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 $V \not\cong W$, 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 $\varphi \in \mathrm{Hom}_{KG}(V, W) \setminus \{0\}$ 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 $\varphi \in \mathrm{End}_{KG}(V) \setminus \{0\}$ is invertible, $\mathrm{End}_{KG}(V)$ is a skew-field.

(b) Let $\varphi \in \operatorname{End}_{KG}(V)$. 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 $(\varphi - \lambda\operatorname{Id}_V)(v) = 0$. Therefore, $\varphi - \lambda\operatorname{Id}_V$ is not invertible and

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

Hence $\operatorname{End}_{KG}(V) \subseteq \{\lambda\operatorname{Id}_V \mid \lambda \in K\}$, 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 $R : G \longrightarrow \operatorname{GL}_n(K)$ and $R' : G \longrightarrow \operatorname{GL}_{n'}(K)$ 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 $\operatorname{char}(K) \nmid |G|$. Let V, W be two KG-modules and let $\rho_V : G \longrightarrow \operatorname{GL}(V)$, $\rho_W : G \longrightarrow \operatorname{GL}(W)$ 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 $\operatorname{char}(K) \nmid |G|$. Let $\rho_V : G \longrightarrow \operatorname{GL}(V)$ and $\rho_W : G \longrightarrow \operatorname{GL}(W)$ be two irreducible K-representations.

(a) If $\rho_V \not\sim \rho_W$ 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 $\operatorname{char}(K) \nmid n := \dim_K V$. If $\psi : V \longrightarrow V$ is a K-linear map, then

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

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

$$i\begin{bmatrix} & & \vdots & & \\ \ldots & \ldots & 1 & \ldots & \ldots \\ & & \vdots & & \\ & & \vdots & & \\ & & j & & \end{bmatrix} =: E_{ij} \in M_{m \times n}(K)$$

(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

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

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

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

$\blacksquare$

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 G is a finite <u>abelian</u> group and $K = \overline{K}$. 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).

<u>Claim</u>: any K-subspace of V is in fact a KG-submodule.

<u>Proof:</u> 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. $\blacksquare$

Theorem 6.2 (DIAGONALISATION THEOREM)

Assume $K = \overline{K}$ and $\operatorname{char}(K) \nmid |G|$. Let $\rho : G \longrightarrow \operatorname{GL}(V)$ 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

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

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

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

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

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

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 $K = \overline{K}$, $\operatorname{char}(K) \nmid |G|$ and G is abelian. If $\rho : G \longrightarrow \operatorname{GL}(V)$ 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.

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

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

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

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

Therefore

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

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

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

hence $\chi_V(g) = \operatorname{Tr}\left(\rho_V(g)\right) = \operatorname{Tr}\left(\rho_{V_1}(g)\right) + \operatorname{Tr}\left(\rho_{V_2}(g)\right) = \chi_{V_1}(g) + \chi_{V_2}(g)$. ∎

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

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

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 $g, x \in G$,

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

∎

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 $\mathcal{Cl}(G) := \{f \in \mathcal{F}(G, \mathbb{C}) \mid f \text{ is a class function}\}$. 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 $\dim_{\mathbb{C}} \mathcal{Cl}(G) = |C(G)|$ 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

$$\langle\,,\,\rangle_G: \quad \begin{aligned} \mathcal{F}(G,\mathbb{C}) \times \mathcal{F}(G,\mathbb{C}) &\longrightarrow \mathbb{C} \\ (f_1, f_2) &\longmapsto \langle f_1, f_2\rangle_G := \tfrac{1}{|G|} \sum_{g\in G} f_1(g)\overline{f_2(g)} \end{aligned}$$

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

$$\langle \chi_V, \chi_W\rangle_G = \frac{1}{|G|} \sum_{g\in G} \chi_V(g)\chi_W(g^{-1}) = \begin{cases} 1 & \text{if } \rho_V \sim \rho_W, \\ 0 & \text{if } \rho_V \nsim \rho_W. \end{cases}$$

Proof: Choose ordered $\mathbb{C}$-bases $E := (e_1, \ldots, e_n)$ and $F := (f_1, \ldots, f_m)$ 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 $\rho_V \nsim \rho_W$ compute

$$\langle \chi_V, \chi_W\rangle_G = \frac{1}{|G|} \sum_{g\in G} \chi_V(g)\chi_W(g^{-1}) = \frac{1}{|G|} \sum_{g\in G} \mathrm{Tr}\,\big(Q(g)\big)\,\mathrm{Tr}\,\big(P(g^{-1})\big)$$

$$= \frac{1}{|G|} \sum_{g\in G} \Big(\sum_{i=1}^{n} Q(g)_{ii}\Big)\Big(\sum_{j=1}^{m} P(g^{-1})_{jj}\Big)$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{m} \underbrace{\frac{1}{|G|} \sum_{g\in G} Q(g)_{ii} P(g^{-1})_{jj}}_{=0 \text{ by (a) of Schur's Relations}} = 0$$

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

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

$\blacksquare$

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 $\chi_1, \ldots, \chi_s$ are pairwise distinct irreducible characters of G, $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ 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. $\blacksquare$

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. $\blacksquare$

Corollary 9.3 (*Multiplicities*)

> Let $\rho_V : G \longrightarrow GL(V)$ 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 $\rho_W : G \longrightarrow GL(W)$ 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 $Cl(G)$ 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 $Cl(G)$ w.r.t. $\langle\,,\,\rangle_G$. Hence it remains to prove that $\mathrm{Irr}(G)$ generates $Cl(G)$ as a $\mathbb{C}$-vector space. So let $X := \langle \mathrm{Irr}(G)\rangle_{\mathbb{C}}$ be the $\mathbb{C}$-subspace of $Cl(G)$ generated by $\mathrm{Irr}(G)$. It follows that

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

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

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

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 $Cl(G)$ of class functions on G. Hence,
$$|\operatorname{Irr}(G)| = \dim_{\mathbb{C}} Cl(G) = |C(G)|$$

where the second equality holds by Notation 8.1. ∎

Corollary 9.8

Let $f \in Cl(G)$. 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 $\Longleftrightarrow \langle f, \chi \rangle_G \in \mathbb{Z}_{\geq 0} \ \forall \, \chi \in \operatorname{Irr}(G)$; and

(d) $f \in \operatorname{Irr}(G) \Longleftrightarrow f$ 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 $\chi \in \operatorname{Irr}(G)$, $\langle f, \chi \rangle_G =: m_\chi \in \mathbb{Z}_{\geq 0}$, 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 $\rho_V : G \longrightarrow GL(V)$ 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 $\rho : G_1 \longrightarrow GL(V)$ 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 $\chi \in Irr(G_1)$ and φ is surjective, then $\chi \circ \varphi \in Irr(G_2)$.

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 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*

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

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 $Fix_X(g) := \{x \in X \mid g \cdot x = x\}$ 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

$$\chi_X(g) = |Fix_X(g)| \qquad \forall \, g \in G \, .$$

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:

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

Hence taking traces, we get $\chi_X(g) = \sum_{x \in X} \left((\rho_X(g))_B \right)_{xx} = |Fix_X(g)|$. ∎

For the action of G on itself by left multiplication, by Example 1(d), $\rho_X = \rho_{\text{reg}}$ 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 $\mathrm{Irr}(G) = \mathrm{Lin}(G)$.

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 $X(G) := \left(\chi_i(g_j)\right)_{ij} \in M_r(\mathbb{C})$.

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 $\{\zeta^i \mid 1 \leq i \leq n\}$ 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

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

Thus the character table of G is

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

which we visualise as follows:

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

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

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

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

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 $1 \leq i \leq 3$ 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

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

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

$$
X C^{-1} \overline{X}^{\mathrm{Tr}} = I_r,
$$

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:

$$
X C^{-1} \overline{X}^{\mathrm{Tr}} = I_r \qquad \Longrightarrow \qquad \overline{X} C^{-1} X^{\mathrm{Tr}} = I_r
$$

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

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

(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

$$(\rho_V \otimes \rho_W)(g_1 g_2, h_1 h_2)[v \otimes w] = (\rho_V(g_1 g_2) \otimes \rho_W(h_1 h_2))[v \otimes w]$$
$$= \rho_V(g_1 g_2)[v] \otimes \rho_W(h_1 h_2)[w]$$
$$= \rho_V(g_1) \circ \rho_V(g_2)[v] \otimes \rho_W(h_1) \circ \rho_W(h_2)[w]$$
$$= \rho_V(g_1) \otimes \rho_W(h_1)[\rho_V(g_2)[v] \otimes \rho_W(h_2)[w]]$$
$$= (\rho_V(g_1) \otimes \rho_W(h_1)) \circ (\rho_V(g_2) \otimes \rho_W(h_2))[v \otimes w]$$
$$= (\rho_V \otimes \rho_W)(g_1, h_1) \circ (\rho_V \otimes \rho_W)(g_2, h_2)[v \otimes w]$$

$\forall \ g_1, g_2 \in G, h_1, h_2 \in H, v \in V, w \in W$. 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. ∎

(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. $\mathrm{Inf}_{G/N}^{G}(\chi)$).

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

$$\mathrm{Inf}_{G/N}^G : \quad \{\text{characters of } G/N\} \quad \longrightarrow \quad \{\text{characters } \psi \text{ of } G \mid N \leqslant \ker(\psi)\}$$
$$\chi \quad \mapsto \quad \mathrm{Inf}_{G/N}^G(\chi)$$

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

$$\mathrm{Inf}_{G/N}^G : \quad \mathrm{Irr}(G/N) \quad \longrightarrow \quad \{\psi \in \mathrm{Irr}(G) \mid N \leqslant \ker(\psi)\}$$
$$\chi \quad \mapsto \quad \mathrm{Inf}_{G/N}^G(\chi) .$$

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

$$\begin{array}{ccc} G & \xrightarrow{\rho} & \mathrm{GL}(V) \\ \pi \downarrow & \circlearrowleft \nearrow & \\ G/N & {}_{\exists ! \widetilde{\rho}} & \end{array}$$
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 $\rho = \mathrm{Inf}_{G/N}^G(\widetilde{\rho})$ and $\psi = \mathrm{Inf}_{G/N}^G(\chi)$. 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 $\Longleftrightarrow$ $\chi(g) \neq \chi(1) \ \forall \, g \in G\backslash\{1\}$ 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

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

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

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

Recall that $V_4 = \{\text{Id}, (1\; 2)(3\; 4), (1\; 3)(2\; 4), (1\; 4)(2\; 3)\} \trianglelefteq S_4$ 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)
$|C_G(g_i)|$	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	.	.	.	.	.
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 $\chi_2(\text{Id}) = 1$ and $\chi_3(\text{Id}) = 2$. (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

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

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 follwing 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.

The main aim of this chapter is to prove *Burnside's $p^a q^b$ theorem*, which provides us with a solubility criterion for finite groups of order $p^a q^b$ 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;

· $\mathrm{Irr}(G) := \{\chi_1, \ldots, \chi_r\}$ 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.

15 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 15.1

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). ∎

16 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 16.1 (*Class sums*)

The elements $\widehat{C}_j := \sum_{g \in C_j} g \in \mathbb{C}G$ ($1 \leqslant j \leqslant r$) are called the **class sums** of G.

Lemma 16.2

The set of all class sums $\{\widehat{C}_j \mid 1 \leqslant j \leqslant r\}$ is a $\mathbb{C}$-basis of $Z(\mathbb{C}G)$. In other words, $Z(\mathbb{C}G) = \bigoplus_{j=1}^{r} \mathbb{C}\widehat{C}_j$.

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, we do have a direct sum $\bigoplus_{j=1}^{r} \mathbb{C}\widehat{C}_j$ in $\mathbb{C}G$ and it is enough to prove that this direct sum is equal to $Z(\mathbb{C}G)$.

'$\supseteq$': $\forall\, 1 \leqslant j \leqslant r$ and $\forall\, g \in G$, we have

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

and extending by $\mathbb{C}$-linearity, we get $a \cdot \widehat{C}_j = \widehat{C}_j \cdot a \; \forall\, 1 \leqslant j \leqslant r$ and $\forall\, a \in \mathbb{C}G$, proving that $\bigoplus_{j=1}^{r} \mathbb{C}\widehat{C}_j \subseteq Z(\mathbb{C}G)$.

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

Comparing coefficients yield $\lambda_g = \lambda_{hgh^{-1}} \; \forall\, g, h \in G$. Namely, the coefficients λ_g are constant on the conjugacy classes of G, and hence

$$a = \sum_{j=1}^{r} \lambda_{g_j} \widehat{C}_j \in \bigoplus_{j=1}^{r} \mathbb{C}\widehat{C}_j.$$

∎

Now, 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 16.3

(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 16.2 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).

∎

Notation 16.4 (*Central characters*)

If $\chi \in \text{Irr}(G)$, then we may consider a $\mathbb{C}$-representation affording χ, say $\rho^\chi : G \longrightarrow \text{GL}(\mathbb{C}^{n(\chi)}) = \text{Aut}_\mathbb{C}(\mathbb{C}^{n(\chi)})$ with $n(\chi) := \chi(1)$. This group homomorphism extends by $\mathbb{C}$-linearity to a $\mathbb{C}$-algebra homomorphism

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

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

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

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 $1 \leqslant j \leqslant r$ there exists a scalar $\omega_\chi(\widehat{C}_j) \in \mathbb{C}$ such that

$$\widetilde{\rho}^\chi(\widehat{C}_j) = \omega_\chi(\widehat{C}_j) \cdot I_{n(\chi)} .$$

The functions defined by

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

(where χ runs through $\text{Irr}(G)$) and extended by $\mathbb{C}$-linearity to the whole of $Z(\mathbb{C}G)$ are homomorphisms of $\mathbb{C}$-algebras; they are called the **central characters** of $\mathbb{C}G$ (or simply of G).

Remark 16.5

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 $Z(G)$.

Theorem 16.6 (*Integrality Theorem*)

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

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

Proof: Let $\chi \in \text{Irr}(G)$ and $1 \leqslant j \leqslant r$. By Corollary 16.3 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 16.4 we have

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

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

Corollary 16.7

If $\chi \in \mathrm{Irr}(G)$, 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 15.1. 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 oder

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

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 $|\mathrm{Irr}(G)| = |C(G)| = 6$ 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

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

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 16.7 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	~~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

(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 16.8

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 16.7]

17 The Centre of a Character

Definition 17.1 (*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, $\chi(g) = \chi(1) \iff g \in \ker(\chi)$.

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 17.2

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 $\rho(g) \in \mathbb{C}^\times \operatorname{Id}_V$. Conversely, if $\rho(g) \in \mathbb{C}^\times \operatorname{Id}_V$, then there exists $\lambda \in \mathbb{C}^\times$ such that $\rho(g) = \lambda \operatorname{Id}_V$. 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 17.3

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

(a) Clearly $\mathbb{C}^\times \operatorname{Id}_V \leqslant Z(\operatorname{GL}(V))$ and hence $\mathbb{C}^\times \operatorname{Id}_V \trianglelefteq \operatorname{GL}(V)$. Therefore, by Lemma 17.2,

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

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 17.2 restriction to $Z(\chi)$ yields a group homomorphism

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

with kernel $\ker(\chi)$. Therefore, by the 1st ismomorphism theorem, $Z(\chi)/\ker(\chi)$ is isomorphic to a finite subgroup of $\mathbb{C}^\times \operatorname{Id}_V \cong \mathbb{C}^\times$, 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 $\rho(g) = \lambda \operatorname{Id}_V$. Thus $g \in Z(\chi)$ and it follows that

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

∎

Exercise 17.4

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

Exercise 17.5

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 17.6 (*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 17.7

Assume now that G is a non–abelian simple group. In the situation of Theorem 17.6 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 17.6 implies that $g \in Z(\chi)$, so $Z(\chi) \neq 1$. As G is simple and $Z(\chi) \trianglelefteq G$ by Proposition 17.3(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 17.3 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. ∎

18   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 16.7 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 16.7 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 $G' \lneqq G$. Hence both G' and G/G' are soluble by the induction hypothesis $\Rightarrow G$ is soluble by the *sandwich principle*.

Theorem 18.1 (*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 17.7. Therefore, the Second Orthogonality Relations read

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

and dividing by p yields

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

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 18.2 (*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 (*Einfürung in die Algebra*), 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 18.1. ∎

Theorem 18.3 (*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. ∎

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.

19 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 19.1 (*Induced class function*)

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

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

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 19.2

With the notation of Definition 19.1 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 19.3 (*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 19.4

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 19.5

Let $H \leqslant J \leqslant G$ and let $g \leqslant G$. 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 19.6 (*Frobenius reciprocity*)

Let $H \leqslant G$, let $\varphi \in Cl(H)$ be a class function on H, and let $\psi \in Cl(G)$ 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 19.7

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 19.8

We conclude from Exercise 19.5(d) and Frobenius Reciprocity 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 $\mathbf{1}_{\{1\}}\uparrow^{G}_{\{1\}} = \chi_{\mathrm{reg}}$. Indeed, if $g \in G$ then, it follows from Corollary 10.2 that

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

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

$$\varphi\uparrow^{G}_{H}(\mathrm{Id}) = \frac{1}{2}\sum_{x\in S_3}\varphi^{\circ}(\mathrm{Id}) = \frac{1}{2}\cdot|S_3|\cdot 1 = 3\,,$$

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

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

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

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

$$0 = \langle\varphi, \chi_1\downarrow^{G}_{H}\rangle_H = \langle\varphi\uparrow^{G}_{H}, \chi_1\rangle_G$$

and similarly

$$1 = \langle\varphi, \chi_2\downarrow^{G}_{H}\rangle_H = \langle\varphi\uparrow^{G}_{H}, \chi_2\rangle_G \quad\text{and}\quad 1 = \langle\varphi, \chi_3\downarrow^{G}_{H}\rangle_H = \langle\varphi\uparrow^{G}_{H}, \chi_3\rangle_G\,.$$

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

The conjugacy classes of $G = A_5$ are

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

i.e. $g_1 = \mathrm{Id}, g_2 = (1\ 2)(3\ 4), g_3 = (1\ 2\ 3)$ 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:

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

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 $\mathrm{Irr}(A_5)\backslash\{\mathbf{1}_G\} = \{\chi_2, \chi_3, \chi_4, \chi_5\}$.

· 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

$$\mathbf{1}_H{\uparrow}_H^G\,(\mathrm{Id}) = 1 \cdot |G : H| = 5 \quad (\text{see Cor. 19.7})$$
$$\mathbf{1}_H{\uparrow}_H^G\,\big((1\ 2)(3\ 4)\big) = \tfrac{1}{12} \cdot 12 = 1$$
$$\mathbf{1}_H{\uparrow}_H^G\,\big((1\ 2\ 3)\big) = \tfrac{1}{12} \cdot 24 = 2$$
$$\mathbf{1}_H{\uparrow}_H^G\,(5\text{-cycle}) = \tfrac{1}{12} \cdot 0 = 0$$

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
$|C_k|$	1	15	20	12	12
$|C_G(g_k)|$	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 17.7 and we get:

	C_1	C_2	C_3	C_4	C_5
$|C_k|$	1	15	20	12	12
$|C_G(g_k)|$	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
$|C_k|$	1	15	20	12	12
$|C_G(g_k)|$	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 19.9 (*Induction of $\mathbb{C}H$-modules*)

If you have attended the lecture *Commutative Algebra* you have studied the *tensor product of modules*. In the M.Sc. lecture *Representation Theory* you will see that induction of modules is defined through a tensor product, extending the 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 $\chi \uparrow_H^G$.

20 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 20.1

Let $H, L \leqslant G$ and let $x \in G$.

(1) The conjugation homomorphism by x on H is denoted by

$$c_x: \quad H \quad \longrightarrow \quad xHx^{-1}$$
$$h \quad \mapsto \quad xhx^{-1}.$$

(2) Assume 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 $\sum_{xH \in G/H}$. Similarly, we write $x \in [L \backslash G/H]$ to mean that $x \in G$ is a representative of the double coset LxH and writing $\sum_{x \in [L \backslash G/H]}$ means that the sum runs over a full set of representatives for the (L, H)–double cosets of in G.

Definition 20.2 (*Conjugate class function / inertia group*)

Let $H \leqslant G$, let $\varphi \in Cl(H)$, 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 ${}^g\varphi := \varphi \circ c_{g^{-1}} \in Cl(gHg^{-1})$, 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 20.3

Let $g, h \in G$. With the notation of Definition 20.2, 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) ${}^g\varphi = {}^h\varphi \iff h^{-1}g \in \mathcal{I}_G(\varphi) \iff g\mathcal{I}_G(\varphi) = h\mathcal{I}_G(\varphi)$;

(d) if $\rho : H \longrightarrow GL(V)$ is a $\mathbb{C}$-representation of H with character χ, then

$$ {}^g\rho := \rho \circ c_{g^{-1}} : gHg^{-1} \longrightarrow GL(V), x \mapsto \rho(g^{-1}xg) $$

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 ${}^g(\varphi\downarrow^H_J) = ({}^g\varphi)\downarrow^{gHg^{-1}}_{gJg^{-1}}$.

Exercise 20.4 (*Mackey Formula*)

Let $H, L \leqslant G$ and let $\varphi \in Cl(H)$. Prove that

$$ (\varphi\uparrow^G_H)\downarrow^G_L = \sum_{g \in [L \backslash G/H]} ({}^g\varphi)\downarrow^{gHg^{-1}}_{gHg^{-1} \cap L}\uparrow^L_{gHg^{-1} \cap L} . $$

Exercise 20.5

Deduce from the Mackey formula that if $N \trianglelefteq G$, and $\psi \in \mathrm{Irr}(N)$, then

$$ \langle \psi\uparrow^G_N, \psi\uparrow^G_N \rangle_G = \sum_{xN \in G/N} \langle \psi, {}^x\psi \rangle_N . $$

Lemma 20.6

(a) If $H \leqslant G$, $\varphi, \psi \in Cl(H)$ 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

$$\langle {}^g\varphi, {}^g\psi \rangle_{gHg^{-1}} = \frac{1}{|gHg^{-1}|} \sum_{x \in gHg^{-1}} {}^g\varphi(x)\overline{{}^g\psi(x)}$$

$$= \frac{1}{|H|} \sum_{x \in gHg^{-1}} \varphi(g^{-1}xg)\overline{\psi(g^{-1}xg)}$$

$$\underset{y := g^{-1}xg}{=} \frac{1}{|H|} \sum_{y \in H} \varphi(y)\overline{\psi(y)} = \langle \varphi, \psi \rangle_H .$$

(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 20.3(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

$$\psi\uparrow_N^G\downarrow_N^G (n) = \psi\uparrow_N^G (n) = \frac{1}{|N|}\sum_{g \in G}\psi(g^{-1}ng) = \frac{1}{|N|}\sum_{g \in G}{}^g\psi(n) = \frac{|\mathcal{I}_G(\psi)|}{|N|}\sum_{g \in [G/\mathcal{I}_G(\psi)]}{}^g\psi(n). \qquad\blacksquare$$

Notation 20.7

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 20.8 (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

$$\mathrm{Ind}_{\mathcal{I}}^G : \quad \mathrm{Irr}(\mathcal{I} \mid \psi) \quad \longrightarrow \quad \mathrm{Irr}(G \mid \psi)$$
$$\eta \quad \mapsto \quad \eta\uparrow_{\mathcal{I}}^G$$

preserving ramification indices, i.e. $\langle \eta\downarrow_N^{\mathcal{I}}, \psi \rangle_N = \langle \eta\uparrow_{\mathcal{I}}^G\downarrow_N^G, \psi \rangle_N = e$.

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 $\eta \in \mathrm{Irr}(N)$ 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 20.6(c) the constituents of $\psi\uparrow_N^G\downarrow_N^G$ are precialy $\{ {}^g\psi \mid g \in [G/\mathcal{I}_G(\psi)] \}$. Hence η is G-conjugate to ψ. Furthermore, for every $g \in G$ we have

$$\langle \chi\downarrow_N^G, {}^g\psi \rangle_N = \frac{1}{|N|}\sum_{h\in N}\chi(h){}^g\psi(h^{-1}) \quad = \quad \frac{1}{|N|}\sum_{h\in N}\chi(h)\psi(g^{-1}h^{-1}g)$$

$$\overset{\chi\in\mathcal{C}l(G)}{=} \quad \frac{1}{|N|}\sum_{h\in N}\chi(g^{-1}hg)\psi(g^{-1}h^{-1}g)$$

$$\overset{s:=g^{-1}hg\in N}{=} \quad \frac{1}{|N|}\sum_{s\in N}\chi(s)\psi(s^{-1}) = \langle \chi\downarrow_N^G, \psi \rangle_N = e \,.$$

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:** $\eta \in \mathrm{Irr}(\mathcal{I} \mid \psi) \;\Rightarrow\; \eta\uparrow_{\mathcal{I}}^G \in \mathrm{Irr}(G|\psi)$.

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 $\chi \in \mathrm{Irr}(G)$ 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 $\chi \in \mathrm{Irr}(G|\psi)$. 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 $e = e'$, $\eta\uparrow_{\mathcal{I}}^G = \chi \in \mathrm{Irr}(G)$, and therefore $\eta\uparrow_{\mathcal{I}}^G \in \mathrm{Irr}(G|\psi)$.

Claim 2: $\chi \in \mathrm{Irr}(G \mid \psi) \;\Rightarrow\; \exists! \; \eta \in \mathrm{Irr}(\mathcal{I} \mid \psi)$ such that $\langle \chi\downarrow_{\mathcal{I}}^G, \eta \rangle_{\mathcal{I}} \neq 0$.

Again by (a), as $\chi \in \mathrm{Irr}(G \mid \psi)$, 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 $\eta \in \mathrm{Irr}(\mathcal{I})$ 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 $\eta \in \mathrm{Irr}(\mathcal{I} \mid \psi)$. 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 $\chi\downarrow_{\mathcal{I}}^G = \sum_{\lambda\in\mathrm{Irr}(\mathcal{I})} a_\lambda \lambda = \sum_{\lambda\neq\eta} a_\lambda\lambda + a_\eta\eta$ with $a_\lambda \geqslant 0$ for each $\lambda \in \mathrm{Irr}(\mathcal{I})$ 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 $\lambda \notin \mathrm{Irr}(\mathcal{I}|\psi)$ for $\lambda \neq \eta$. Thus η is uniquely determined as the only constituent of $\chi\downarrow_{\mathcal{I}}^G$ in $\mathrm{Irr}(\mathcal{I} \mid \psi)$.

Finally, Claims 1 and 2 prove that $\mathrm{Ind}_{\mathcal{I}}^G : \mathrm{Irr}(\mathcal{I} \mid \psi) \longrightarrow \mathrm{Irr}(G \mid \psi), \eta \mapsto \eta\uparrow_{\mathcal{I}}^G$ 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 20.8 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 20.6(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 20.9 (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 $A \unlhd G$, 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 20.8(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 17.5, we have

$$\eta(1) \,\Big|\, |\mathcal{I}_G(\psi) : Z(\eta)| \,\Big|\, |\mathcal{I}_G(\psi) : A|$$

and since $\chi = \eta\uparrow_{\mathcal{I}_G(\psi)}^{G}$ it follows that

$$\chi(1) = |G : \mathcal{I}_G(\psi)| \cdot \eta(1) \,\Big|\, |G : \mathcal{I}_G(\psi)| \cdot |\mathcal{I}_G(\psi) : A| = |G : A| \,.$$

∎

21 The Theorem of Gallagher

In the context of Clifford theory (Theorem 20.8) 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 21.1

Let $N \trianglelefteq G$ and let $\psi \in \mathrm{Irr}(N)$ such that $\mathcal{I}_G(\psi) = G$. Then

$$\psi\uparrow_N^G = \sum_{\chi \in \mathrm{Irr}(G)} e_\chi\, \chi$$

where $e_\chi := \langle \chi\downarrow_N^G, \psi \rangle_N$ is the ramification index of χ in N; in particular

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

Proof: Write $\psi\uparrow_N^G = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi\, \chi$ for suitable $a_\chi \geq 0$ (i.e. $a_\chi = \langle \chi, \psi\uparrow_N^G \rangle_G$). By Frobenius reciprocity, $a_\chi \neq 0$ if and only if $\chi \in \mathrm{Irr}(G \mid \psi)$. But by Theorem 20.8: if $\chi \in \mathrm{Irr}(G|\psi)$, then $\chi\downarrow_N^G = e_\chi \psi$, so

$$e_\chi = \langle \chi\downarrow_N^G, \psi \rangle_N = \langle \chi, \psi\uparrow_N^G \rangle_G = a_\chi \qquad \text{and also } \chi(1) = e_\chi \cdot \psi(1) \,.$$

Therefore,

$$|G : N| \cdot \psi(1) = \psi\uparrow_N^G(1) = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi(1) = \sum_{\chi \in \mathrm{Irr}(G)} e_\chi \chi(1) = \sum_{\chi \in \mathrm{Irr}(G)} e_\chi^2 \psi(1) = \psi(1) \cdot \sum_{\chi \in \mathrm{Irr}(G)} e_\chi^2$$

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 21.2 (*Extension of a character*)

Let $N \trianglelefteq G$ and $\chi \in \mathrm{Irr}(G)$ such that $\psi := \chi\downarrow_N^G$ is irreducible. Then we say that ψ **extends to** G, and χ is an **extension of** ψ.

Exercise 21.3

Let $N \trianglelefteq G$ and $\chi \in \mathrm{Irr}(G)$. Prove that

$$\chi\downarrow_N^G\uparrow_N^G = \mathrm{Inf}_{G/N}^G(\chi_{\mathrm{reg}}) \cdot \chi,$$

where χ_{reg} is the regular character of G/N.

Theorem 21.4 (Gallagher)

Let $N \trianglelefteq G$ and let $\chi \in \mathrm{Irr}(G)$ such that $\psi := \chi\downarrow_N^G \in \mathrm{Irr}(N)$. Then

$$\psi\uparrow_N^G = \sum_{\lambda \in \mathrm{Irr}(G/N)} \lambda(1)\,\mathrm{Inf}_{G/N}^G(\lambda) \cdot \chi,$$

where the elements of the set $\{\mathrm{Inf}_{G/N}^G(\lambda) \cdot \chi \mid \lambda \in \mathrm{Irr}(G/N)\}$ are are pairwise distinct irreducible characters of G.

Proof: By Exercise 21.3 we have $\psi\uparrow_N^G = \mathrm{Inf}_{G/N}^G(\chi_{\mathrm{reg}}) \cdot \chi$, 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

$$\psi\uparrow_N^G = \sum_{\lambda \in \mathrm{Irr}(G/N)} \lambda(1)\,\mathrm{Inf}_{G/N}^G(\lambda) \cdot \chi.$$

Now, by Lemma 21.1, we have

$$|G : N| = \sum_{\tilde\chi \in \mathrm{Irr}(G)} e_{\tilde\chi}^2 = \langle \psi\uparrow_N^G, \psi\uparrow_N^G\rangle_G = \sum_{\lambda,\mu \in \mathrm{Irr}(G/N)} \lambda(1)\mu(1)\langle \mathrm{Inf}_{G/N}^G(\lambda)\cdot\chi, \mathrm{Inf}_{G/N}^G(\mu)\cdot\chi\rangle_G$$
$$\geqslant \sum_{\lambda \in \mathrm{Irr}(G/N)} \lambda(1)^2 = |G : N|.$$

Hence equality holds throughout. This proves that

$$\langle \mathrm{Inf}_{G/N}^G(\lambda)\cdot\chi, \mathrm{Inf}_{G/N}^G(\mu)\cdot\chi\rangle = \delta_{\lambda\mu}.$$

By Erercise 13.4, $\mathrm{Inf}_{G/N}^G(\lambda)\cdot\chi$ are characters of G and hence the characters $\{\mathrm{Inf}_{G/N}^G(\lambda)\cdot\chi \mid \lambda \in \mathrm{Irr}(G/N)\}$ are irreducible and pairwise distinct, as claimed. ∎

Therefore, given $\psi \in \mathrm{Irr}(N)$ which extends to $\chi \in \mathrm{Irr}(G)$, we get $\mathrm{Inf}_{G/N}^G(\lambda) \cdot \chi$ $(\lambda \in \mathrm{Irr}(G/N))$ 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 $\psi\uparrow_N^G \in \mathrm{Irr}(G)$;

- if $\mathcal{I}_G(\psi) = G$ then ψ extends to some $\chi \in \mathrm{Irr}(G)$ and $\psi\uparrow_N^G = \chi + \chi'$ with $\chi' \in \mathrm{Irr}(G)\setminus\{\chi\}$. 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.

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.

22   Frobenius Group / Frobenius Complement / Frobenius Kernel

Definition 22.1 (*Frobenius group / Frobenius complement*)

A finite group G admitting a non-trivial proper subgroup H such that

$$H \cap {}^g H = \{1\} \qquad \forall\, g \in G \backslash H$$

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, $P \cap {}^g P = \{1\}$ 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 22.2 (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 $N := \left(G \setminus \bigcup_{g \in G} {}^g H \right) \cup \{1\}$.

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 ${}^g H$ of H because if $g, x \in G$ then we have:
$${}^g H = {}^x H \Leftrightarrow x^{-1}g \in N_G(H) = H \Leftrightarrow gH = xH.$$

Moreover, these have only the identity element in common, because if $g, x \in G$ are such that ${}^g H \neq {}^x H$, then $x^{-1}g \notin N_G(H) = H$, so by the definition of the Frobenius complement,
$$\{1\} = {}^{x^{-1}g}H \cap H = {}^{x^{-1}}({}^g H \cap {}^x H),$$
proving that ${}^g H \cap {}^x H = \{1\}$. It now follows that
$$\left| \bigcup_{g \in G} {}^g H \right| = |G : H| \cdot (|H| - 1) + 1 = |G| - |G : H| + 1.$$

It follows that
$$|N| = |G| - \left| \bigcup_{g \in G} {}^g H \right| + 1 = |G| - |G| + |G : H| - 1 + 1 = |G : H|.$$

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
$$\widetilde{N} \cap {}^g H = {}^g \widetilde{N} \cap {}^g H = {}^g(\widetilde{N} \cap H) = {}^g\{1\} = \{1\}$$

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 $\theta \in Cl(H)$ 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 19.7 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: $\mathrm{Ind}_H^G : \{\theta \in Cl(H) \mid \theta(1) = 0\} \longrightarrow Cl(G), \theta \mapsto \theta\uparrow_H^G$ is an isometry with respect to the scalar products $\langle -, - \rangle_H$ and $\langle -, - \rangle_G$.

Indeed, let $\theta, \eta \in Cl(H)$ 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 $\theta := \eta - \eta(1)1_H$, then $\eta^* := \theta\uparrow_H^G + \eta(1)1_G$ is an irreducible character of G.

Clearly, $\theta \in \mathbb{Z}\mathrm{Irr}(H) \subseteq Cl(H)$, $\theta(1) = 0$, and $\eta^* \in \mathbb{Z}\mathrm{Irr}(G) \subseteq Cl(G)$ (see Remark 19.8). 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, $\langle\theta\uparrow_H^G, 1_G\rangle_G = \langle\theta, 1_H\rangle_H = -\eta(1)$, hence the above together with the fact that $\theta\uparrow_H^G$ is a virtual character (by Remark 19.8) implies that

$$\begin{aligned}
\langle\eta^*, \eta^*\rangle_G &= \langle\theta\uparrow_H^G + \eta(1)1_G, \theta\uparrow_H^G + \eta(1)1_G\rangle_G \\
&= \langle\theta\uparrow_H^G, \theta\uparrow_H^G\rangle_G + 2\eta(1)\langle\theta\uparrow_H^G, 1_G\rangle_G + \eta(1)^2\langle 1_G, 1_G\rangle_G \\
&= \langle\eta, \eta\rangle_H + \eta(1)^2 + 2\eta(1)\cdot(-\eta(1)) + \eta(1)^2 \\
&= \langle\eta, \eta\rangle_H = 1
\end{aligned}$$

As η^* is a virtual character, it now follows that $\pm\eta^* \in \mathrm{Irr}(G)$. However,

$$\eta^*(1) = \theta\uparrow_H^G(1) + \eta(1)1_G(1) = 0 + \eta(1)\cdot 1 = \eta(1) > 1\,,$$

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 $\eta \in \mathrm{Irr}(H)$,

$$\eta^*\downarrow_H^G = \theta\uparrow_H^G\downarrow_H^G + \eta(1)1_G\downarrow_H^G = \theta + \eta(1)1_H = \eta\,.$$

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 $M \cap {}^x H = \{1\}$ for each $x \in G$ since $M \trianglelefteq H$. Therefore $M \leqslant N$, and it remains to prove that $N \leqslant M$. So, let $g \in N\backslash\{1\}$. Then, by the definition of N, for every $x \in G$, we have $g \notin {}^x H$. 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 $\eta \in \mathrm{Irr}(H)\backslash\{\mathbf{1}_H\}$. 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 22.3

(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 22.4

(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.

23 Characters of Frobenius groups

We now construct the whole character table of an arbitrary Frobenius group.

Theorem 23.1 (*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

$$A \times \mathrm{Irr}(B) \to \mathrm{Irr}(B), \quad (a, \chi) \mapsto a.\chi,$$
$$A \times C(B) \to C(B), \quad (a, C) \mapsto a.C,$$

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 23.2

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 23.3

Let G be an arbitrary finite group. Assume that $N \trianglelefteq G$ and assume that $C_G(n) \leqslant N$ for all $n \in N \setminus \{1\}$. Then, the following assertions hold:

(a) if $\psi \in \mathrm{Irr}(N) \setminus \{\mathbf{1}_N\}$, 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 20.5.) 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 23.2, 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 23.4

Let G be a Frobenius group with Frobenius complement H and Frobenius kernel N. Then,

$$\mathrm{Irr}(G) = \mathrm{Inf}_{G/N}^G \big(\mathrm{Irr}(G/N) \big) \sqcup \big\{ \psi \uparrow_N^G \mid \psi \in \mathrm{Irr}(N) \backslash \{\mathbf{1}_N\} \big\} \,.$$

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 23.3 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 23.5

Compute the character table of the dihedral group $D_{2(2m+1)}$ for all $m \in \mathbb{Z}_{\geqslant 1}$.

Exercise 23.6

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 23.7

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 $\mathbf{1}_G$.

This appendix provides a short recap / introduction to some of the basic notions of module theory used in this lecture. Tensor products of vector spaces and algebraic integers are also recapped.

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**

$$
\begin{array}{rccc}
+ : & M \times M & \longrightarrow & M \\
& (m_1, m_2) & \mapsto & m_1 + m_2
\end{array}
$$

and an **external composition law** (or **scalar multiplication**)

$$
\begin{array}{rccc}
\cdot : & R \times M & \longrightarrow & M \\
& (r, m) & \mapsto & r \cdot m
\end{array}
$$

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

$$\mathrm{Im}(\varphi) := \varphi(M) = \{\varphi(m) \mid m \in M\}$$

of φ is an R-submodule of N. If $M = N$ and φ is invertible, then the inverse is the usual set-theoretic *inverse map* φ^{-1} and is also an R-homomorphism.

Notation A.8

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

$$\begin{aligned} +: \quad \mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(M, N) &\longrightarrow \quad \mathrm{Hom}_R(M, N) \\ (\varphi, \psi) &\longmapsto \quad \varphi + \psi : M \longrightarrow N, m \mapsto \varphi(m) + \psi(m) \,. \end{aligned}$$

In case $N = M$, we write $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ 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

$$\begin{aligned} R \times M/U &\longrightarrow M/U \\ (r, m + U) &\longmapsto r \cdot m + U \,. \end{aligned}$$

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:

$$\begin{array}{ccc} M & \xrightarrow{\ \varphi\ } & N \\ {\scriptstyle \pi}\downarrow & \circlearrowleft \ \nearrow & \\ M/U & {\scriptstyle \exists! \,\overline{\varphi}} & \end{array}$$

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

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

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.

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 16

(a) A commutative ring R itself is an R-algebra.
[The internal composition law "·" 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 $B_V = \{v_1, \ldots, v_n\}$ and $B_W = \{w_1, \ldots, w_m\}$ ($m, n \in \mathbb{Z}_{\geqslant 0}$) 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 symbole "$v_i \otimes w_j$" as an element that depends on both v_i and w_j. The symbole "$\otimes$" 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

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{ij}(v_i \otimes w_j) \quad \text{with } \{\lambda_{ij}\}_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \subseteq K.$$

(b) The binary operation

$$\begin{aligned} B_V \times B_W &\longrightarrow B_{V \otimes_K W} \\ (v_i, w_j) &\longmapsto v_i \otimes w_j \end{aligned}$$

can be extended by $\mathbb{C}$-linearity to

$$\begin{aligned} -\otimes-: \qquad V \times W &\longrightarrow V \otimes_K W \\ \left(v = \sum_{i=1}^{n} \lambda_i v_i, w = \sum_{i=1}^{n} \mu_j w_j\right) &\longmapsto v \otimes w = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_i \mu_j (v_i \otimes w_j). \end{aligned}$$

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 $\forall\, x_1, \ldots, x_r \in V, y_1, \ldots y_s \in W$,

$$\left(\sum_{i=1}^{r} x_i\right) \otimes \left(\sum_{j=1}^{s} y_j\right) = \sum_{i=1}^{r} \sum_{j=1}^{s} x_i \otimes y_j.$$

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 $A = (A_{ij})_{ij} \in M_n(K)$ and $B = (B_{rs})_{rs} \in M_m(K)$ 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 $\operatorname{Tr}(A \otimes B) = \operatorname{Tr}(A)\operatorname{Tr}(B)$.

Example 17

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

$$\begin{aligned} f_1 \otimes f_2 : \quad V \otimes_K W &\longrightarrow \quad V \otimes_K W \\ v \otimes w &\longmapsto \quad (f_1 \otimes f_2)(v \otimes w) := f_1(v) \otimes f_2(w) \, . \end{aligned}$$

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 $B_V = (v_1, \ldots, v_n)$ and $B_W = (w_1, \ldots, w_m)$ 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 recall/introduce here some notions of the *Commutative Algebra* lecture on integrality of ring elements. However, we are 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 $f \in A[X]$, that is $f(b) = 0$ and f is a polynomial of the form $X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ with $a_{n-1}, \ldots, a_0 \in A$. 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 $b \in \mathbb{C}$ integral over $\mathbb{Z}$ is called an **algebraic integer**.

Theorem D.2

Let $A \subseteq B$ be a subring of a commutative ring and let $b \in B$. TFAE:

(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 $b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0$ (∗). 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 $b^n = -a_{n-1}b^{n-1} - \ldots - a_1 b - a_0 \in C$.
- 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

$$b^k = -a_{n-1}b^{k-1} - \ldots - a_1 b^{k-n+1} - a_0 b^{k-n} \in C$$

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 assumption $A[b] \subseteq S = Ax_1 + \ldots + Ax_n$, where $x_1, \ldots, x_n \in B$, $n \in \mathbb{Z}_{>0}$. 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 $x := (x_1, \ldots, x_n)^{\mathsf{Tr}}$ and consider the $n \times n$-matrix $M := bI_n - (a_{ij})_{ij} \in M_n(S)$. Hence

$$Mx = 0 \qquad \Rightarrow \qquad \mathrm{adj}(M)Mx = 0\,,$$

where $\mathrm{adj}(M)$ is the adjugate matrix of M (i.e. the transpose of its cofactor matrix). By the properties of the determinant (GDM), 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 $\det(M)s = 0$ for every $s \in S$. As $1 \in S$ this gives us $\det(M) = 0$. 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 $A \subseteq B$ be a subring of a commutative ring. 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 $A[b] = A + Ab + \ldots + Ab^{n-1}$ and $A[c] = A + Ac + \ldots + Ac^{m-1}$ for some $n, m \in \mathbb{Z}_{>0}$. Thus $S := A[b, c]$ is finitely generated as an A-module by $\{b^i c^j \mid 0 \leqslant i \leqslant n, 0 \leqslant j \leqslant m\}$. Theorem D.2(c) now yields that $b + c$ and $b \cdot c$ are integral over A because they belong to S. ∎

Example 18

All the elements of the ring $\mathbb{Z}[i]$ of Gaussian intergers 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

$$c^n + \underbrace{d a_{n-1}c^{n-1} + \ldots + d^{n-1}a_1 + d^n a_0}_{\text{divisible by } d} = 0\,.$$

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 aforementionnend lemma can be generalised to integral domains and their field of fractions.

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
$f\rvert_S$	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
$\|G\|$	order of the group G
$\|G : H\|$	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

Rings and linear algebra

$R[X]$	ring of polynomials in an indeterminate X over the ring R
$R^\times$	group of units of the ring R
$\mathrm{char}(K)$	characteristic of the field K
$\det$	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

$C_1, \ldots, C_r$	the conjugacy classes of G
$\widehat{C_1}, \ldots, \widehat{C_r}$	the class sums of G
$Cl(G)$	$\mathbb{C}$-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
$\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_r\}$	set of irreducible characters of G
$\mathrm{Irr}(G\|\psi)$	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
$\mathrm{Res}_H^G, \downarrow_H^G$	restriction from G to H
$Z(KG)$	center of KG
$Z(\chi)$	center 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

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