# Representation Theory of Finite Groups, VT2024

Benjamin Andersson
Victor Groth

Last updated february 2026

# Contents

## 0.1 Typos/Mistakes

Please send any mistakes or typos you find to benjamin35813@gmail(dot)com.

# Chapter 1

# Lecture 1

Other textbooks: Serre, linear representations of finite groups [6].

## 1.1 Introduction

- A group $G$.
- a field $\mathbb{F}$.
- An $\mathbb{F}$ vectorspace $V$.

This course focuses on $G$ **finite**, $\mathbb{F} = \mathbb{C}$ or $\mathbb{F}$ **algebraically closed** of $\mathrm{char}(\mathbb{F}) = 0$.

- $\mathbb{F}$ algebraically closed versus not.
- $\mathrm{char}(\mathbb{F}) = 0$ versus $\mathrm{char}(\mathbb{F}) = p$ for prime $p$.

**Definition 1.1.1.** Given $G, \mathbb{F}$ and $V$ as above, a **representation** of $G$ is an *action* of $G$ on $V$ that is $\mathbb{F}$-linear, $G \times V \to V$, where, for fixed $g$, we get $g : V \to V$ defined by $V \ni v \mapsto gv \in V$.

Equivalently, a representation is a **group homomorphism**

$$\begin{aligned} \varphi : G \to \mathrm{Aut}(V) &= \mathrm{Aut}_{\mathbb{F}}(V) \\ &= \{T : V \to V \mid T \text{ linear} + \ T \text{ invertible}\}. \end{aligned}$$

**Definition 1.1.2.** A **finite dimensional representation** of $G$ over $\mathbb{F}$ is a group homomorphism $G \to \mathrm{GL}(n, \mathbb{F})$ for some $n \geq 1$.

A representation is finite-dimensional if $V$ is finite-dimensional. We find that for $V$ finite, definition 1.1.1 and 1.1.2 are equivalent. Let

$$\varphi : G \to \mathrm{GL}(n, \mathbb{F}).$$

Take $V = \mathbb{F}^n$. If $\varphi : G \to \mathrm{Aut}(V)$ and $\dim(V) = n$, then if $b_1, \ldots, b_n$ basis for $V$, $V \cong \mathbb{F}^n$ is an isomorphism, explicitly by $b_i \mapsto e_i$. We have an isomorphism

$$\mathrm{Aut}(V) \cong \mathrm{GL}(n, \mathbb{F}).$$

If $V$ is finite-dimensional, we write $\mathrm{Aut}(V) = \mathrm{GL}(V)$.

### 1.1.1 Motivation

- We want to understand groups.
- Look at some classes of groups with rich extra structure, e.g. $S_n$ or $\mathrm{GL}(n, \mathbb{F})$.
- Reduce math to linear algebra, i.e. "linearize". In our case, math = group theory.
- Want to study linear algebra in groups/families, i.e. a collection of linear transformations that forms a group.

Theme: Representational objects in their own right. Have groups, rings, fields, representations.

Representations of $\mathbb{Z}$:

$$\varphi : \mathbb{Z} \longrightarrow \mathrm{GL}(n, \mathbb{F}) \quad \text{homomorphism} \quad \Leftrightarrow \quad \text{Invertible matrix } A \in \mathrm{GL}(n, \mathbb{F}).$$

We have $\varphi(1) = A \rightsquigarrow \varphi(\mathbb{Z}) = \{A^n \mid n \in \mathbb{Z}\}$.

$\varphi \mapsto \varphi(1)$, $A \mapsto \varphi$ such that $\varphi(1) = A$. Questions about $A$, e-values, trace, $A^t A = 1$?, and determinant. We have that $A^n = 1$ for some $n$ or $A$ has infinite order. $A$ diagonalizable.

**Definition 1.1.3.** Let $\varphi : G \to \mathrm{GL}(V) \cong \mathrm{GL}(n, \mathbb{F})$ be a representation. A **subrepresentation**, **invariant subspace** or **G-stable subspace** is a vector subspace $W \subset V$ such that $\varphi(g)(W) \subset W, \forall g \in G$.

**Definition 1.1.4.** A representation is **irreducible** if *the only subrepresentations are* the zero subspace, and $V$.

*Question* 1.1.5. Given $G, \mathbb{F}$; classify all irreducible representations of $G$ over $\mathbb{F}$.

**Definition 1.1.6.** A representation is **semisimple** (also known as **completely reducible**) if $V$ is a direct sum of irreducible representations. That is, $V = \bigoplus_i W_i$ where $W_i$ is irreducible, for all $i$, and $W_i, W_j \subset V$ where $i \neq j$, $W_i + W_j \cong W_i \oplus W_j \Leftrightarrow W_i \cap W_j = \{0\}$.

If $\varphi_1 : G \to \mathrm{GL}(W_1)$ and $\varphi_2 : G \to \mathrm{GL}(W_2)$ are representations, then we have a representation

$$\varphi_1 \oplus \varphi_2 : G \to \mathrm{GL}(W_1 \oplus W_2)$$

explicitly defined by

$$(\varphi_1 \oplus \varphi_2) g = \varphi_1(g) \oplus \varphi_2(g).$$

$\dim(W_1) = m_1, \dim(W_2) = m_2$.

If $W_1, W_2$ are subrepresentations of $V$ then $W_1 + W_2$ is a subrepresentation of $V$, where $g(w_1 + w_2) = gw_1 + gw_2 \quad (w_1 + w_2 \in W_1 + W_2, g \in G)$.

Going back to the semisimple definition, i.e. if $V = W_1 \oplus \ldots \oplus W_n$ for some irreducible representations $W_1, \ldots, W_n$, then **semisimple** $\Leftrightarrow$ **diagonalizable**.

$W \subset V$ is *stable* under $\mathbb{Z}$, i.e. $\varphi(\mathbb{Z}) \Leftrightarrow \varphi(1) = A$

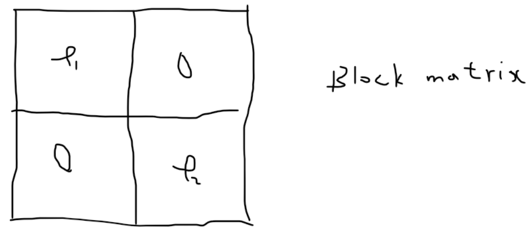


Figure 1.1: Block matrix

$$\mathbb{Z} \xrightarrow{\varphi_\lambda} \mathrm{GL}(1, \mathbb{F}) = \mathbb{F}^\times$$

$$1 \longmapsto \lambda$$

$b_1, \ldots, b_n$ basis of $A_\lambda$, where $A_\lambda = \bigoplus_{i=1}^r b_i \mathbb{F}_i$.

We have $A_\lambda = (\varphi_\lambda)^r$ as representations of $\mathbb{Z}$.

E.g.

$$A = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{bmatrix} = \varphi_3 \oplus \varphi_5 \oplus \varphi_5.$$

$\mathrm{Char}(\mathbb{F}) \neq 3, 5$ (otherwise, **not invertible**! Hence not in $\mathrm{GL}(3, \mathbb{F})$). Note that $\varphi_3 \oplus \varphi_5 \oplus \varphi_5 = \text{span } e_1 \oplus \text{span } e_2 \oplus \text{span } e_3$ and $\text{span}\{e_2, e_3\} = A_5$.

**Definition 1.1.7.** A morphism of representations

$$r_1 : G \to \mathrm{GL}(V_1)$$
$$r_2 : G \to \mathrm{GL}(V_2)$$

and a linear representation $\varphi : V_1 \to V_2$ which is $G$-**equivariant**.

$$\begin{tikzcd} V_1 \arrow[r, "\varphi"] \arrow[d, "r_1(g)"'] \arrow[dr, phantom, "\circlearrowleft"] & V_2 \arrow[d, "r_2(g)"] \\ V_1 \arrow[r, "\varphi"'] & V_2 \end{tikzcd} \qquad \text{commutes } \forall g \in G$$

$\varphi$ is an isomorphism of representations *if* it is *invertible*.

$\varphi(1) = A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ where span $e_1$ is the subrepresentation $Ae_1 = e_1$, but there is no $W$ such that $\mathbb{F}^2 = \text{span } e_1 \oplus W$ <u>and</u> $W$ is $\mathbb{Z}$-stable.

$\varphi : G \to \mathrm{GL}(V)$ representation; $W \subset V \rightsquigarrow$ subrepresentation $V/W := \{v + W \mid v \in V\}$.

$g \cdot (v + W) = g \cdot v + W$. So if $W$ is a subrepresentation of $V \implies V/W$ is a representation called the **quotient**. So here before we have $\mathbb{F}^2/\text{span } e_1 \cong \varphi_1$.

$\mathbb{Z}/p\mathbb{Z}, \varphi(1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\mathbb{F} = \mathbb{Z}/p = \mathbb{F}_p$, $G = \mathbb{Z}/p\mathbb{Z}$

# Chapter 2

# Lecture 2

Recap: $\{\text{representations of } \mathbb{Z}\} \Leftrightarrow \{\text{invertible matrices}\}$

explicitly by $\rho \mapsto \rho(1)$.

- $\exists$ representations of $\mathbb{Z}$ over $\mathbb{C}$ that are not semisimple.

  $\rho$ semi-simple $\Leftrightarrow \rho(1) = A$ diagonalizable. So if $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ where $a \neq 0$.

**Definition 2.0.1.** A representation is **indecomposable** if $\rho$ is *not* a direct sum.

**Example 2.0.2.** $\exists$ representations of of $\mathbb{Z}/p$ over $\overline{\mathbb{F}}_p$ that are not semisimple.

Fact: The only irreducible representation of $\mathbb{Z}/p$ in char $= p$ is 1 (the "trivial representation").

If $\text{char}(\mathbb{F}) = 0$, then every representation of $\mathbb{Z}/p$ over $\mathbb{F}$ is semisimple $\Leftrightarrow$ every matrix of finite order is diagonalizable over an algebraically closed field of char 0. Special case of "Maschke's theorem".

**Theorem 2.0.3.** *(Maschke's theorem) Assume $G$ finite and char$(\mathbb{F}) \nmid |G| \implies$ every representation of $G$ over $\mathbb{F}$ is semisimple. Let $S_n$ symmetric group acting on $\{1, \ldots, n\}$, where $\rho : G \to GL(n, \mathbb{F})$ for all fields $\mathbb{F}$ is defined explicitly by $\sigma \mapsto A_\sigma$, where $\mathbb{F}\sigma e_i = e_{\sigma(i)}$ and $A_\sigma = \left( e_{\sigma(1)} \middle| e_{\sigma(2)} \middle| \ldots \middle| e_{\sigma(n)} \right)$.*

Recall: Cayles theorem, where, if $|G| = n$ then

$$G \hookrightarrow S_n \hookrightarrow \text{GL}(n, \mathbb{F}).$$

That is, $G$ is isomorphic to a subgroup of $S_n$ by cayley's theorem.

**Definition 2.0.4.** A representation is **faithful** if it is injective.

The one above is the **regular** representation of $G$. We find that

$$\begin{aligned} \mathbb{F}[G] &= \mathbb{F}^G \\ &= \bigoplus_{g \in G} \mathbb{F} e_g. \end{aligned}$$

$G$ acts on $\mathbb{F}^G$ as a group action, explicitly by by

$$h \cdot e_g = e_{hg}$$

$$\rightsquigarrow G \to \mathrm{GL}(\mathbb{F}^G) \cong \mathrm{GL}(n, \mathbb{F})$$

where $n = |G|$.

### 2.0.1 Schur's lemma

**Theorem 2.0.5.** *(Schur's lemma) Let $\mathbb{F}$ be an algebraically closed field, where $(V_1, \rho_1), (V_2, \rho_2)$ are irreducible representations of some group $G$ and $V_1, V_2$ are vector spaces over $\mathbb{F}$ (of finite dimension, atleast for $(b)$). Then*

*(a)* $\dim \mathrm{Hom}_G(V_1, V_2) = \begin{cases} 0, & \text{if } V_1 \ncong V_2 \\ 1, & \text{if } V_1 \cong V_2 \end{cases}$

*(b) If $V_1 = V_2 = V$ then $\mathrm{End}_G(V) = \{\lambda I \mid \lambda \in \mathbb{F}\}$.*

*(c) Recall: 1.1.7. If $\varphi : V_1 \to V_2$ is $G$-equivariant, then $\varphi = 0$ or is an isomorphism of representations.*

*Proof.* $a)$ exercise: If $\varphi : (V_1, \rho_1) \to (V_2, \rho_2)$ is $G$-equivariant then $\ker \varphi$ and $\mathrm{im}\, \varphi$ are $G$-stable subspaces of $V_1$ and $V_2$ respectively. $V_1$ irreducible $\Leftrightarrow \ker \varphi = (0)$ or $V_1$. If $\ker \varphi = V_1 \Leftrightarrow \mathrm{im}\, \varphi = (0) \Leftrightarrow \varphi = 0$.

$V_2$ irreducible $\Leftrightarrow \mathrm{im}\, \varphi = (0)$ or $V_2$, if $\varphi \neq 0$ then $\ker \varphi = (0)$ and $\mathrm{im}\, \varphi = V_2 \implies \varphi$ is an isomorphism.

$b)$ If $(V_1, \rho_1) \ncong (V_2, \rho_2)$ then $\mathrm{Hom}_G(V_1, V_2) = (0)$ by $a)$. Assume $V_1 \cong V_2$. We may assume $V_1 = V_2$.

$$G \xrightarrow{\ \rho_1\ } \mathrm{GL}(V_1) \xrightarrow{\ \mathrm{GL}(\varphi)\ } \mathrm{GL}(V_2)$$

$$A \longmapsto \varphi \circ A \circ \varphi^{-1}$$

$V_1 \xrightarrow{\mathfrak{S}} V_2$ induces $\mathrm{End}_G(V_1) \simeq \mathrm{End}_G(V_2)$. Look at $\mathrm{End}_G(V)$ and note that $\lambda I \in \mathrm{End}_G(V)$ (scalars commute with everything), so

$$\lambda I \in Z(\mathrm{End}(V)).$$

We have $\mathrm{End}_G(V) \subset \mathrm{End}(V)$. Let $\varphi \in \mathrm{End}_G(V)$. Since $\mathbb{F}$ is algebraically closed and $\dim V < \infty$, then $\varphi$ admits an eigenvalue $\lambda$ (follows from the fact that the characteristic polynomial $p(x) \in \mathbb{F}[x]$ has a root in $\mathbb{F}$) $\implies$ that there exists *non-zero* $v \in V$ so that $\varphi v = \lambda v$. Therefore,

$$(\varphi - I\lambda)v = 0 \implies v \in \ker(\varphi - I\lambda) \implies V = \ker(\varphi - I\lambda) \implies \varphi = I\lambda.$$

□

*Remark* 2.0.6. Note that we used the fact that we had $v \neq 0 \in \ker(\varphi - \lambda I)$ together with the fact of the irreduciblity of $V_1 = V_2 = V$, as well as the fact that $\varphi - I\lambda \in \mathrm{End}_G(V)$ to say that $V = \ker(\varphi - I\lambda)$, since if $V \neq \ker(\varphi - I\lambda)$ then $\ker(\varphi - I\lambda)$ would be a non-trivial, proper $G$-stable subspace, which is a contradiction to the assumption that $V = V_1 = V_2$ is an irreducible representation.

Caution: Schur's lemma can fail if $\mathbb{F}$ is **not** algebraically closed.

*Remark* 2.0.7. Note that what we mean when we say that $\varphi : (V_1, \rho_1) \to (V_2, \rho_2)$ is $G$-equivariant, is that

$$\rho_2(g)(\varphi(v_1)) = \varphi(\rho_1(g)v_1).$$

See 1.1.7.

**Example 2.0.8.** $\mathbb{F} = \mathbb{R}$.

$$\rho : \mathbb{Z}/n \longrightarrow \mathrm{GL}(2, \mathbb{R})$$

$$1 \longmapsto \begin{bmatrix} \cos(v) & -\sin(v) \\ \sin(v) & \cos(v) \end{bmatrix}$$

where $v = \dfrac{2\pi}{n}$. If $n \geq 3 \implies$ not diagonalizable over $\mathbb{R}$ since the eigenvalues over $\mathbb{C}$ are

$$e^{\frac{2\pi i}{n}}$$

and

$$e^{\frac{-2\pi i}{n}}.$$

Consider $\mathrm{Hom}_G(\mathbb{R}^2, \mathbb{R}^2)$. For all $g \in \mathrm{SO}(2, \mathbb{R})$ is a $G$-equivariant map.

$$\left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{R} \right\} \simeq \mathbb{R}^2$$

$$\begin{tikzcd} \rho : \mathbb{Z}/n \arrow[r] \arrow[dr] & \mathrm{GL}(2, \mathbb{R}) \\ \rho_{\mathbb{C}} : \mathbb{Z}/n \arrow[r] & \mathrm{GL}(2, \mathbb{C}) \end{tikzcd}$$

but

$$\rho_{\mathbb{C}} = \rho_{e^{\frac{2\pi i}{n}}} \oplus \rho_{e^{\frac{-2\pi i}{n}}}.$$

### 2.0.2 Application

**Definition 2.0.9.** (Character) A 1-dimensional representation is a **character**.

**Definition 2.0.10.** (Character of a representation) The **character of a representation** $\rho : G \to \mathrm{GL}(V)$ over $\mathbb{F}$ is the function $\chi : G \to \mathbb{F}$ defined explicitly by $\chi(g) = \mathrm{tr}(\rho(g))$.

Definition 2.0.9 and definition 2.0.10 agree **only** when $\dim \rho = 1$. I.e. $\chi = \mathrm{tr}(\rho)$ is usually not a homomorphism.

Recall that the center of a group $G$, $Z(G)$, is defined as

$$Z(G) := \{g \in G \mid gx = xg, \forall x \in G\}.$$

**Theorem 2.0.11.** *Assume $\rho : G \to GL(V)$ is an irreducible representation. Then there exists a character*

$$\chi : Z(G) \to \mathbb{F}$$

*such that*

$$\rho(z) = \chi(z)I \qquad (\forall z \in Z(G)).$$

**Definition 2.0.12.** $\chi$ in 2.0.11 is called the **central character** of $\rho$.

*Proof.* For all $z \in Z(G)$, we have that $\rho(z)$ is $G$-equivariant. Therefore, $\rho(z) \in \mathrm{Hom}_G(V, V)$. By 2.0.5, one has

$$\mathrm{Hom}_G(V, V) = \{\lambda I \mid \lambda \in \mathbb{F}\}.$$

It follows that $\rho(z) = \lambda I$. Set $\chi(z) = \lambda I$, so that

$$\chi(z_1 z_2) = \chi(z_1)\chi(z_2)$$

and

$$\rho(z_1 z_2) = \rho(z_1)\rho(z_2).$$

We get

$$\begin{aligned} \rho(z_1)\rho(z_2)v &= \rho(z_1)\chi(z_2)v \\ &= \rho(z_1)v\chi(z_2) \\ &= \chi(z_2)v\chi(z_2) \\ &= \chi(z_2)\chi(z_1)v. \end{aligned}$$

$\square$

**Corollary 2.0.13.** *Let $G$ be an abelian group. Then every irreducible representation is one dimensional.*

*Proof.* $G = Z(G)$ acts by central character (2.0.11, 2.0.12). If $\rho$ is irreducible then

$$\rho := \chi : G \to \mathbb{F}^{\times}.$$

$\square$

# Chapter 3

# Lecture 3

Recall 2.0.5. Let $V, W$ be irreducible representations and let $\mathbb{F}$ be an algebraically closed field.

$\mathrm{Hom}_G(V, W) = (0)$ if $V \ncong W$ and $\mathrm{End}_G(V) = \{\lambda I \mid \lambda \in \mathbb{F}\}$.

$\mathrm{id} : \mathrm{GL}(V) \to \mathrm{GL}(V)$ explicitly defined by $A \longmapsto A$, also known as "standard representation"(?).

*Question* 3.0.1. Is it irreducible?

*Question* 3.0.2. Given $0 \subsetneqq W \subsetneqq V$, does there exist $A \in \mathrm{GL}(V)$ mapping $W$ not into $W$.

In general, if $r : G \to \mathrm{GL}(V)$, if $G$ acts transitively on $V \setminus \{0\}$ then $r$ is irreducible.

$\mathrm{GL}(V)$ acts transitively on $V \setminus \{0\}$

**Corollary 3.0.3.** $Z(GL(n, \mathbb{F})) = \{\lambda I \mid \lambda \in \mathbb{F}^\times\}$.

*Proof.* Let $z \in Z(\mathrm{GL}(n, \mathbb{F}))$, and note that $\mathrm{GL}(n, \mathbb{F}) \subset M_n(\mathbb{F})$ and that $M_n(\mathbb{F}) \cong \mathrm{End}(\mathbb{F}^n)$. $G$-equivariant with $G = \mathrm{GL}(n, \mathbb{F})$, so by Schur, $z$ is a scalar multiplication. □

*Remark*: Corollary 3.0.3 is true even if $\mathbb{F}$ is not algebraically closed.

**Definition 3.0.4.** (Group ring/ Group Algebra) Let $R$ be a commutative ring and let $G$ be a group. The **group ring/group algebra** of $G$ over $R$ is $R[G] = \{\sum_{\text{finite}} a_g g \mid a_g \in R, g \in G\}$.

One could also write $R[G] = \{\sum_{g \in G} a_g \mid a_g \in R\}$.

This course focuses on $R = \mathbb{F}$ where $\mathbb{F}$ field. Then $\mathbb{F}[G]$ is an $\mathbb{F}$-vector space of dim $|G|$ with basis $G$. $R[G]$ has a left-and-right module structure. $R[G]$ is also a ring: use multiplication of $G$ and extend by linearity/distribution.

$$\left(\sum a_g g\right)\left(\sum b_h h\right) = \sum a_g b_h gh.$$

The coefficient of $s \in G$ is

$$\sum_{\substack{g,h \\ gh = s}} a_g a_h.$$

We have $G$ abelian $\Leftrightarrow R[G]$ commutative and $R[\mathbb{Z}] \cong R[x, x^{-1}] \cong R[x, y]/(xy - 1)$.

- $R[G]$ is an $R$-algebra.
- $M_n(\mathbb{F})$ and $\mathrm{End}(V)$ are isomorphic as $\mathbb{F}$-algebras.
- $\mathbb{F}[G]$ is a regular representation of $G$.

**Theorem 3.0.5.** *Let $\mathbb{F}$ be an algebraically closed field of char$(\mathbb{F}) = 0 \implies \mathbb{F}[G] \cong M_{n_1}(\mathbb{F}) \times \ldots \times M_{n_r}(\mathbb{F})$ where $= \#$ of representations of $G$ over $\mathbb{F}$ up to isomorphism $= \#$ of conjugacy classes of $G$, and where $n_1, \ldots, n_r$ are the dimensions of the irreducible representations.*

If $A$ is an $R$-algebra, an $A$-module (left) is a module for $A$ as a ring.

$\{$Module for $\mathbb{F}[G]\} \Leftrightarrow \{$representations of $G$ over $\mathbb{F}\}$.

For the "if-direction"; $r : G \to \mathrm{GL}(V)$ then extend $r$ by linearity to $\mathbb{F}[G]$.

### 3.0.1 Algebras, Modules and Maschke's theorem

- $\mathbb{Z}/n\mathbb{Z}$ ring and also $\mathbb{Z}$-algebra (note that ring $R \Leftrightarrow \mathbb{Z}$-algebra) where $\varphi : R \to Z(A)$ not injective. We have the canonical projection $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ as the $\mathbb{Z}$-algebra, i.e. $(\mathbb{Z}/n\mathbb{Z}, \pi)$ is our $\mathbb{Z}$-algebra.
- But if $R = \mathbb{F}$ is a field, then $\varphi$ is injective. We identify $\mathbb{F}$ with a subring of $R$, i.e. $\mathbb{F} \cong \varphi(\mathbb{F}) \subset Z(A)$.
- In key case $R = \mathbb{F}$ and $A$ is an $\mathbb{F}$-algebra then an $A$-module is the same as an algebra-homomorphism $A \to \mathrm{End}(V)$.

If $s : \mathbb{F}[G] \to \mathrm{End}(V)$, then restricting to $G$, $s|_G : G \to \mathrm{GL}(V) \subset \mathrm{End}(V)$ since all $g \in G$ are invertible.

A representation of $G$ is irreducible $\Leftrightarrow$ corresponding representation of $\mathbb{F}[G]$ is irreducible.

$$\{G\text{-stable } W \subset V\} \Leftrightarrow \{\mathbb{F}[G] \text{ stable } W \subset V\}.$$

**Theorem 3.0.6.** *(Maschke's theorem) Let $G$ be a finite group, and assume* $\mathrm{char}\,\mathbb{F} \nmid |G|$. *Then for all representations $r$*

$$r : G \longrightarrow GL(V)$$

$$r : \mathbb{F}[G] \longrightarrow \mathrm{End}(V)$$

*and every $G$-stable subspace $W$ there exists a $G$-stable complement $W'$ such that $V = W \oplus W'$.*

**Definition 3.0.7.** A **projector** (or **projection, idempotent**) in $\mathrm{End}(V)$ is $A \in \mathrm{End}(V)$ such that $A^2 = A$.

Exercise: $A$ projector $\implies$

(a) $\ker A \cap \operatorname{im} A = (0)$.

(b) $V = \ker A \oplus \operatorname{im} A$

(c) There exists basis of $V$ such that $A$ is diagonal with entries $\{0,1\}$, i.e. $A = \operatorname{diag}(\varepsilon_1, \dots, \varepsilon_r)$ with $\varepsilon_i \in \{0,1\}$.

$A$ is the projection onto $\operatorname{im}(A)$, i.e. $V \to \operatorname{im}(A) \subset V$.

We now prove Maschke's theorem (3.0.6):

*Proof.* $W$ admits a complement $W'$ as vector spaces (but might not be $G$-stable). We have $V = W \oplus W'$ by extending basis, and we get a projection $\varphi : V \to W$ defined by

$$V = W \oplus W' \ni (w, w') \overset{\varphi}{\longmapsto} w \in W.$$

$\varphi$ is $G$-equivariant $\Leftrightarrow$ $W$ is $G$-stable.

$$\varphi^{av} := \underbrace{\frac{1}{|G|}}_{\text{Need } \operatorname{char}(\mathbb{F}) \nmid |G|} \sum_{g \in G} g \varphi g^{-1}.$$

Here we note that $g$ is an abbreviation for $\rho_W(g)$ where $\rho : G \to \mathrm{GL}(W)$ is a representation, and $g^{-1}$ is an abbreviation for $\rho_V(g^{-1})$ where $\rho_V : G \to \mathrm{GL}(V)$ is a representation.

<u>Claim</u> 1: $\varphi^{av}$ is $G$-equivariant.

*Proof.*

$$\begin{aligned} h\varphi^{av}h^{-1} &= h\left(\frac{1}{|G|}\sum_{g\in G} g\varphi g^{-1}\right)h^{-1} \\ &= \frac{1}{|G|}\sum_{g\in G} hg\varphi g^{-1}h^{-1} \\ &= \frac{1}{|G|}\sum_{s\in G} s\varphi s^{-1} \\ &= \varphi^{av} \end{aligned}$$

where $s = hg$. □

<u>Claim</u> 2: $\varphi^{av}$ is a projector, i.e. $(\varphi^{av})^2 = \varphi^{av}$.

*Proof.*

$$\varphi^{av}(\varphi^{av} v) = \varphi^{av}\left(\frac{1}{|G|}\sum_{g\in G} g\varphi g^{-1}\right) v.$$

We note that $\varphi(g^{-1}(v)) \in W$ and hence $g(\varphi(g^{-1}(w)) \in W$, since $\rho_V(g)$ act's stably on $\varphi(\rho_W(g))v \in W$

$\rightsquigarrow$

$$
\begin{aligned}
\varphi^{av}(\varphi^{av}v) = \\
&\vdots \\
&= \varphi^{av}w \\
&= \frac{1}{|G|}\sum_{g\in G} g\varphi g^{-1}w \\
&= \frac{1}{|G|}\sum_{g\in G} g\varphi \underbrace{\rho_V(g^{-1})w}_{\in W,\ \text{W } G\text{-stable}} \\
&= \frac{1}{|G|}\sum_{g\in G} \rho_W(g)(\rho_V(g^{-1}))w \\
&= \frac{1}{|G|}\sum_{g\in G} w = w.
\end{aligned}
$$

Here we have used the fact that $\rho_W$ is the restriction of $\rho_V$ to $W$, i.e. $\rho_W = \rho_V|_W$, hence they cancel each other out on $w \in W$, and that $\varphi(w) = w$ for $w \in W$.

Or in "relaxed" notation, disregarding the sum and the fact that $g := \rho(g)$, we have

$$
\begin{aligned}
g\varphi g^{-1}w &= g\varphi(g^{-1}w) \\
&= gg^{-1}w \\
&= w.
\end{aligned}
$$

So $\varphi^{av}(\ldots) = (\ldots)$. $\square$

$\square$

**Theorem 3.0.8.** *Let $V$ be an $A$-module where $A$ is an $\mathbb{F}$-algebra. Then the following are equivalent:*

*(a) $V$ is a direct sum of irreducible $A$-modules.*

*(b) $V$ is a sum of irreducible $A$-modules.*

*(c) For all $G$-stable subspaces $W \subset V$, there is $G$-stable complement $W'$.*

*Proof.* $b) \implies a)$ Let $W$ be a maximal $G$-stable subspace that is a direct sum of irreducible representations. Assume $\underbrace{W \subsetneq V}_{\implies \exists i, \text{ such that } V_i \not\subset W}$, by $b)$ we get $V = \sum_{i=1}^{n} V_i$ where $V_i$ is an irreducible representation.

<u>Exercise</u>: Let $V_i$ be an irreducible representation and let $W$ be a subrepresentation (i.e. "$G$-stable"). Then either $V_i \subset W$ or $V_i \cap W = (0)$.

Following up from before <u>*Exercise*</u>, we have that since $\exists i$ such that $V_i \not\subset W \implies V_i \cap W = (0) \implies$ we can form $V_i \oplus W$, which contradicts maximality of $W$. $\square$

# Chapter 4

# Lecture 4

Recap:

**Theorem 4.0.1.** *Let $A$ be a finite-dimensional $\mathbb{F}$-algebra (so finite dimensional as an $\mathbb{F}$ vector space) and let $V$ be a finite-dimensional $A$-module.*

*Then the following are equivalent*

*(a) $V$ is a direct sum of irreducible $A$-modules.*

*(b) For all submodules $W \subset V$ there is a ($A$-submodule) complement $W'$ such that $V = W \oplus W'$, where $W'$ is $A$-stable.*

*(c) $V$ is a sum of irreducible $A$-modules.*

*Proof.* $c) \implies b)$: Let $W \subset V$ be a submodule. Let $U \subset V$ be the maximal submodule such that $U \cap W = 0$.

$W \oplus U \subseteq V$, know from $a)$ that $V = \bigoplus_i V_i$, where $V_i$ is irreducible. Assume that

$$W \oplus U \subsetneq V$$

which implies that there exists an $i$ such that $V_i \not\subseteq W \oplus U$. This in turn implies that

$$V_i \cap (W \oplus U) = 0 \implies (V_i \oplus U) \cap W = 0$$

which contradicts the maximality of $U$, hence there can not exist an $V_i$ which is not in $W \oplus U$. Therefore

$$V = \bigoplus_i V_i \subseteq W \oplus U \implies W \oplus U = V.$$

□

*Remark* 4.0.2. In the proof $(c) \implies b)$, we used the fact that if $V_i \cap (W \oplus U) = 0$ then since $U \hookrightarrow W \oplus U$ we have $V_i \cap U = 0$. One can show that $V_i \oplus U$ is a submodule of $V$. Hence $V_i \oplus U$ is a submodule of $V$ strictly greater than $U$.

*Proof.* $c) \implies a)$: Let $V'$ be a maximal direct sum of irreducible $A$-modules in $V$. Assume $V' \subsetneq V$ (for contradiction). $c) \implies b) \implies \exists W'$ such that $V = V' \oplus W'$. Let $W_0 \subseteq W'$ be irreducible (f.d.), then $V' \oplus W_0$ contradicts maximality of $V'$. □

**Definition 4.0.3.** Let $V$ be an $A$-module and let $M$ be an irreducible $A$-module. Then the $M$-**isotypic** component of $V$ is

$$V_M = \sum_{\substack{W \subset V \\ W \cong M}} W.$$

(The "$M^{\text{th}}$ homogenous component" $M(V)$ in [2], def. 1.12).

*Analogy:* If $B \in M_n(\mathbb{F})$ then $B_\lambda =$ **eigenspace** of $B = \underbrace{\lambda \oplus \ldots \oplus \lambda}_{\dim(B_\lambda)\ \text{times}}$.

If $B$ is invertible $\rightsquigarrow \lambda : \mathbb{Z} \to \mathrm{GL}(1, \mathbb{F}) = \mathbb{F}^\times \subset M(1, \mathbb{F})$, where $\lambda$ is defined explicitly by $1 \longmapsto \lambda$.

- In general, $\mathbb{F}$-algebra, then

$$\begin{array}{ccc} \lambda : \mathbb{F}[x] & \longrightarrow & \mathbb{F} \\ x & \longmapsto & \lambda \\ \mathbb{F} & = & \mathbb{F} \end{array}$$

$B \rightsquigarrow$ an $\mathbb{F}$-algebra homomorphism

$$\begin{array}{ccc} \mathbb{F}[x] & \longrightarrow & M_n(\mathbb{F}) \\ x & \longmapsto & B \\ \mathbb{F} & = & \mathbb{F} \end{array}$$

*Comment* 4.0.4. In the *representation* $\rho_B$, the $\lambda$-isotypic component is the $\lambda$-eigenspace.

**Lemma 4.0.5.**

$$V_M = \sum_{\substack{W \subset V \\ W \cong M}} W$$

*is an* $\mathrm{End}_A(V)$*-submodule of* $V$*.*

*Proof.* Let $\rho \in \mathrm{End}_A(V)$. We want to show that $\rho(V_M) \subset V_M$, which is equivalent to showing that $\rho(W) \subset V_M$ for all $W$ in the sum $V_M$. $W$ irreducible $\implies \rho(W) = 0 \subset V_M$ or $\rho(W) \cong W \cong M \implies \rho(W) \subset V_M$. □

$$\begin{tikzcd} V \text{ is an A-module} \arrow[d, dash] & \\ \rho : A \arrow[r, "\rho"] & \mathrm{End}(V) \\ & \cup \\ & \mathrm{End}_A(V) \end{tikzcd}$$

A-equivariant maps

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[d, "a"'] & V \arrow[d, "a"] \\ V \arrow[r, "\varphi"'] & V \end{tikzcd}$$

We have that $\varphi \in \mathrm{End}_A(V) \Leftrightarrow$ square commutes.

**Lemma 4.0.6.** *Assume that* $V = \bigoplus_i W_i$ *where* $W_i$ *is irreducible, for all* $i$. *Then*

*(a)* $V_M \cong \bigoplus_{W_j \cong M} W_j$.

*(b)* $|\{j \mid W_j \cong M\}|$ *is invariant of the direct sum decomposition of* $V$ *(*$n_M(V)$ *in [2], lemma* 1.13.(*c*)*).*

*Comment* 4.0.7. By lemma 1.11 in [2], WLOG, if $V_M = \sum_{\substack{W \subset V \\ W \cong M}} W$ then $V_M = \bigoplus_{W \in \mathcal{M}} W$ where

$$\mathcal{M} \subset \{W \subset V, W \text{ irreducible} \mid W \cong M\}.$$

*Proof.* $V_M' = \bigoplus_{W_i \cong M} W_i$ which is equivalent to showing that $V_M' \cong V_M$. We have $V_M' \subset V_M$ by definition. We want to show that $V_M \subset V_M'$. This is equivalent to showing that $W \subset V_M'$ for all $W \subset V$ such that $W \cong M$.

Let $\pi_i : V \twoheadrightarrow W_i$ be the projection map from $V$ onto $W_i$. By irreducibility of $W_i$, we get $\pi_i(W) = 0$ or $\pi_i(W) = W_i$. If the latter, then $W \subset \bigoplus_{\pi_i(W) \neq 0} W_i \subset V_M$. □

*Proof.* $b$) By $a$) we have that

$$\dim(V_M) = |\{j \mid W_j \cong M\}| \dim M \Leftrightarrow \frac{\dim(V_M)}{\dim M} = |\{j \mid W_j \cong M\}|.$$

Note that the LHS is independent of which direct sum decomposition we choose for $V$ (since the dimension of both $M$ and $V_M$ must be independent of direct sum decomposition, I believe), hence RHS is independent of the direct sum decomposition of $V$. □

<u>Note</u>: $\mathbb{F}^{\neg} = \mathbb{F}e_1 \oplus \mathbb{F}e_2 \oplus \mathbb{F}e_3$. For $\mathbb{F}(e_1+e_2)$ we have $\pi_1 \neq 0$, $\pi_2 \neq 0$ and $\pi_3 = 0$ then $\mathbb{F}(e_1+e_2) \subset \pi_1(\mathbb{F}(e_1+e_2)) + \pi_2 F(e_1+e_2)$.

**Corollary 4.0.8.**

$$V = \bigoplus_{M \text{ irreducible}} V_M$$

*decomposition of $X$ into* ***isotypic*** *components.*

<u>Recall</u>: $G$ group, then $\mathbb{F}[G]$ **regular** representation of $G$ (note that the regular representation of $G$ is the *linear* representation of $G$ on itself afforded by *translation*).

Similarly, $A$ as an $A$-module is the regular representation (module of $A$). Note; in [2],we denote $A^\circ$ as the **right** $A$-module structure on $A$.

$$A \longrightarrow \mathrm{End}_{\mathbb{F}}(A)$$

$$M_n(\mathbb{F}) \longrightarrow M_{n^2}(\mathbb{F})$$

**Proposition 4.0.9.** *Every irreducible $A$-module is a* ***quotient*** *of $A$.*

*Proof.* Let $V$ be irreducible and let $0 \neq v \in V$. Define $\varphi : A \to V$ explicitly by

$$A \ni a \overset{\varphi}{\longmapsto} av \in V.$$

Note that $\varphi$ is $A$-equivariant

$$\begin{tikzcd}
b \arrow[d, phantom, "\in" rotate=-90] \arrow[drr, bend left] \arrow[drr, bend right] & & \\
A \arrow[rr, "\varphi"] \arrow[d, "a"'] & & V \arrow[d, "a"] \\
A \arrow[rr, "\varphi"'] & & V
\end{tikzcd}$$

$$\begin{array}{ccc}
a\varphi(b) & = & a(bv) \\
 & & \| \\
\varphi(ab) & = & (ab)v
\end{array}$$

where we have used the module axioms.

Since $V$ is irreducible and $\varphi(1_A) = v \neq 0 \in V$, we have that $\varphi$ is surjective, so that

$$A/\ker\varphi \cong V.$$

$\square$

- Group analogy: Let $G \curvearrowright X$[1] **transitively**.
- Orbit-stabilizer:
$$G/\mathrm{Stab}(y) \xrightarrow{\sim} \mathrm{orb}(y) = X$$
as $G$-sets. Every **transitive** $G$-set is a quotient of $(\underbrace{G/\text{left-multiplication}}_{\text{regular G-set}})$

Let $V$ be an $A$-module.

**Definition 4.0.10.** Let $A$ be a finite-dimensional algebra over $\mathbb{F}$. Then $A$ is **semisimple** if $A$ is semisimple as an $A$-module.

**Corollary 4.0.11.** *If $A$ is semisimple, then every irreducible $A$-module is isomorphic to a submodule of the regular $A$-module. That is, for arbitrary irreducible $A$-module $M$, we have that $M \cong N \subset A^\circ$ for some submodule $N$ of $A^\circ$.*

*Remark* 4.0.12. Again, note that $A^\circ$ is $A$ with the canonical $A$-module structure.

Exercise: If $\pi : W \to W$ is surjective, and $W_0$ is the complement to $\ker \pi$, then
$$\pi|_{W_0} : W_0 \xrightarrow{\sim} W.$$

**Corollary 4.0.13** (Of Maschke's)**.** *If $|G| \nmid \mathrm{char}(\mathbb{F})$, then $\mathbb{F}[G]$ is semisimple.*

Henceforth, by "ideal" we mean "two-sided ideal".

**Definition 4.0.14** (Minimal ideal)**.** Let $R$ be a ring and let $I \subset R$ be an ideal of $R$. We call $I$ **minimal** if $J \subset I$ ideal of $R$ then $J = 0$ or $J = I$.

## 4.1 Wedderburns theorem

**Theorem 4.1.1.** *Assume that $A$ is an semisimple $\mathbb{F}$-algebra. Then*

*a)*
$$\left\{\textit{Minimal ideals of } A\right\} = \left\{A_M \colon M \textit{ irreducible } A\textit{-module}\right\}$$

*b) For all irreducible $A$-modules $W$, we have that $A_M \cdot W = 0$, if $W \ncong M$.*

*c) For all irreducible $A$-modules $M$, we have that the restriction of*

$$\begin{tikzcd} A \arrow[r, "\rho"] & \mathrm{End}(M) \\ A_M \arrow[u, hook, "\iota"] \arrow[ur, "\rho|_{A_M}"'] & \end{tikzcd}$$

*to $A_M$ is an isomorphism onto* $\mathrm{im}(\rho) \subset \mathrm{End}(M)$.

[1] $G \curvearrowright X$ denotes the group action $G \times X \to X$.

*d) $A$ has* finitely *many isomorphism classes of irreducible modules (when $A = \mathbb{C}[G] \implies$ this number $=$ # conjugacy classes of $G$).*

**Corollary 4.1.2.**

$$A = \prod_{M irreducible} A_M$$

*is a direct product of simple rings $A_M$, which is in fact $\mathbb{F}$-algebraic.*

*Proof.* Follows from 4.2.1.$c$). ☐

**Definition 4.1.3.** A ring $R$ is simple if $R$ has no non-trivial 2-sided ideals.

We'll see that $\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times \ldots \times M_{n_r}(\mathbb{C})$ where the irreducible representations of $G$ have dimension $n_1, \ldots, n_r$.

**Lemma 4.1.4.** *$A_M$ is an ideal of $A$.*

*Proof.* $A_M \subset A$ is a left-submodule of $A$, by definition[2]. We want to show that it is also a right submodule of $A$. By lemma 4.0.2, $A_M$ is an $\mathrm{End}_A(A)$ submodule of $A$. $\forall b \in A$, set $R_b : A \to A$, explicitly defined by $a \longmapsto ab$. The claim is that $R_b$ is $A$-equivariant, so in $\mathrm{End}(A)$ (apparently, check!). Furthermore, it is claimed that $R_b(A_M) = (A_M)b \subset A_M$, so that $A_M$ is a right module. ☐

We prove $b$) of theorem 4.1.1:

*Proof.* If $W \ncong M$ then

$$A_W \cap A_M = 0$$

(Note that $A_W \cong W(A)$ and $A_M \cong M(A)$).

<u>Recall</u>: For ideals $I, J$ in $R$, we have that the product-ideal

$$IJ \subset I \cap J$$

so that

$$A_W A_M \subset A_W \cap A_M = 0.$$

$W$ irreducible + $A$ semisimple $\implies \exists W_0 \subset A$ so that $W_0 \cong W$ (lemma 1.14 in [2]). It follows[3] that $W_0 \subset A_M \implies A_M \cdot W_0 \subset A_M \cdot A_W = 0$. ☐

[2] I believe this follows from the fact that $A_M$ is isomorphic to $M(A)$, as formulated in [2], where $M(A)$ is the $M^{\text{th}}$ isotypic component of $A$, i.e. the sum of all submodules of $A$ isomorphic to the irreducible $A$-module $M$. $M(A)$ is a submodule of $A$, so under the identification $A_M \cong M(A)$ we get that $A_M$ is a submodule of $A$, even though formally $A_M \subseteq \mathrm{End}(M)$.

[3] Again, under the identification $A_W \cong M(W)$, I believe.

# Chapter 5

# Lecture 5

## 5.1 Double Centralizer theorem

**Theorem 5.1.1.** *Let $A$ be a semsimple $\mathbb{F}$-algebra, and let $\rho : A \to \mathrm{End}(M)$ where $M$ is an irreducible $A$-module. Then* $\mathrm{End}_{\mathrm{End}_A(M)}(M) = \mathrm{im}\,\rho$.

*Comment* 5.1.2. Note that $\mathrm{im}\,\rho = A_M$ in [2].

*Proof.* If the theorem is true for $M$ and $M \cong M'$ then the theorem also holds for $M'$.

$A$ semisimple $\implies$ every irreducible $A$-module is isomorphic to a submodule of $A$ (lemma 1.14 in [2]). We may assume that $M$ is a submodule of $A$.

Unravel definitions: $\mathrm{im}(\rho) \subset \mathrm{End}_{\mathrm{End}_A(M)}(M)$. Here $\rho(a)$ commutes with things that commute with $\rho(a)$, for all $a \in A$. Let $s \in \mathrm{End}_A(M)$, so that we get the following diagram

$$\begin{tikzcd} M \arrow[r, "s"] \arrow[d, "\rho(a)"'] & M \arrow[d, "\rho(a)"] \\ M \arrow[r, "s"] & M \end{tikzcd}$$

where

$$\mathrm{End}_A(M) = \{s \in \mathrm{End}_{\mathbb{F}}(M) \mid s \text{ commutes with } \mathrm{im}\,\rho\}$$

and

$$\mathrm{End}_{\mathrm{End}_A(M)}(M) = \{s \in \mathrm{End}_{\mathbb{F}}(M) \mid s \text{ commutes with} \,\mathrm{End}_A(M)\}.$$

□

We want to show that $\mathrm{End}_{\mathrm{End}_A(M)}(M) \subset \mathrm{im}\,\rho$. Let $\theta \in \mathrm{End}_{\mathrm{End}_A(M)}(M)$. Then, can we show that

$$\theta(m) = um$$

for some $u \in A$? For all $m \in M$, set

$$R_m : M \longrightarrow A$$

explicitly defined by

$$x \longmapsto xm.$$

$M$ is a a submodule of $A$, hence $M$ is an ideal of $A$ if we give $A$ the *canonical* $A$-module structure. We have that $xm \in M$, so in fact, $R_m : M \to M$. Furthermore, since every element in $M$ commutes with elements of $\mathbb{F}$ (since $M \subset A$, and $A$ is an $\mathbb{F}$-algebra), then we have $R_m \in \mathrm{End}_{\mathbb{F}}(M)$.

$$\begin{tikzcd} M \arrow[r, "R_m"] \arrow[dr] & A \\ & M \arrow[u, hook] \end{tikzcd}$$

For all $a \in A$ and $m \in M$, we have

$$\begin{aligned} R_m(ax) &= axm \\ &= aR_m(x) \\ &\implies R_m \in \mathrm{End}_A(M). \end{aligned}$$

$$\begin{aligned} \theta(mn) &= \theta(R_n(m)) \\ &= R_n(\theta(m)) \\ &= \theta(m)n. \end{aligned}$$

Recall: $A_M = M$-isotypic subalgebra. $1 \in A_M$ unit. Let $n \in M, n \neq 0$. Then

$$M \subset A_M \implies AnA \subset A_M.$$

*Remark* 5.1.3. Note that theorem 1.15.*c* in [2] gives $M(A) \cong A_M$ and since $\exists W_0 \subset M(A)$ so that $W_0 \cong M$, we can identify $W_0$ with $M$, so that $M \subset M(A) \cong A_M$. Again, identifying $M(A)$ with $A_M$, we get $M \subset A_M$.

Exc:

**Lemma 5.1.4.** *Let $R$ be a ring and let $s \in R$. Then $RsR$ is an ideal of $R$.*

Recall that $n \in M$ and $M \subset A$ so that $n \in A$. Therefore, by 5.1.4 $AnA$ is an ideal of $A$. Furthermore, since $M$ is a submodule of $A$, $M$ is an *ideal* of $A$ (with the $A$-module structure). It follows that $AnA \subset M \subset M(A) = A_M$. Here

**Definition 5.1.5.**

$$RsR = \left\{ \sum_{\text{finite}} r_i n r_i' \;\middle|\; r_i, r_i' \in A \right\}.$$

If $n \neq 0$, then since $A$ is a ring, it has a 1, so that $1n1 = n \in AnA$. By minimality of $A_M$, we have that

$$\begin{aligned} AnA &= A_M \\ &= \operatorname{im} \rho. \end{aligned}$$

Then we get that

$$1 = \sum a_i n b_i \qquad (a_i, b_i \in A).$$

We have (5.1.5)

$$AnA := \left\{ \sum_{\text{finite}} r_i n r_i' \text{ for } r_i, r_i' \in A \right\}.$$

It follows that

$$\begin{aligned} m &= 1 \cdot m \\ &= \left( \sum a_i n b_i \right) \cdot m \\ &= \sum (a_i n)(b_i m) \end{aligned}$$

where $a_i, n, b_i$ and $m$ are all in $M$.

Recall: $\theta(mn) = \theta(m)n$ for $\theta \in \operatorname{End}_{\operatorname{End}_A(M)}(M)$. Hence

$$\begin{aligned} \theta(m) &= \theta\left( \sum (a_i n)(b_i m) \right) \\ &= \sum \theta(a_i n)(b_i m) \\ &= \left( \sum \theta(a_i n) b_i \right) m \end{aligned}$$

Hence $\theta$ acts on $M$ by $\sum \theta(a_i n) b_i \in M$.

So $R_{\sum \theta(a_i n) b_i} : M \to M$ is such that

$$\theta = R_{\sum \theta(a_i n) b_i} \in A_M = \operatorname{im} \rho.$$

Therefore, $\operatorname{End}_{\operatorname{End}_A(M)}(M) \subset \operatorname{im} \rho \implies \operatorname{End}_{\operatorname{End}_A(M)}(M) = \operatorname{im} \rho$.

## 5.2 Analogy: Galois theory

Let $\mathbb{K}/\mathbb{F}$ be a finite extension of fields. Then $\operatorname{Aut}(\mathbb{K}/\mathbb{F}) := \{\sigma \in \operatorname{Aut}(\mathbb{K}) \mid \sigma(\lambda) = \lambda, \forall \lambda \in \mathbb{F}\}$.

If $|\operatorname{Aut}(\mathbb{K}/\mathbb{F})| = \dim_{\mathbb{K}} \mathbb{F}$ then $\mathbb{K}^{\operatorname{Aut}(\mathbb{K}/\mathbb{F})} = \mathbb{F}$, where $\mathbb{K}^G := \{\alpha \in \mathbb{K} \mid \sigma\alpha = \alpha, \forall \sigma \in G\}$ (for $G \subset \operatorname{Aut}(\mathbb{K})$). Then $\mathbb{F} \subset \mathbb{K}^{\operatorname{Aut}(\mathbb{K}/\mathbb{F})}$ holds by definition, even if $|\operatorname{Aut}(\mathbb{K}/\mathbb{F})| < \dim_{\mathbb{K}} \mathbb{F}$; "$\mathbb{F}$ fixed by automorphisms of $\mathbb{K}$ fixing $\mathbb{F}$". On the other hand, the inclusion $\mathbb{K}^{\operatorname{Aut}(\mathbb{K}/\mathbb{F})} \subset \mathbb{F}$ is one of the main theorems of galois theory.

## 5.3 Smallest and largest

We claim that $\mathbb{F} \subset \mathrm{End}_A(M)$: Given an $\mathbb{F}$-algebra $(A, \alpha)$ where $\alpha : \mathbb{F} \to A$ is a unital ring-homomorphism such that $\alpha(\mathbb{F}) \subseteq Z(A)$, we define

$$f(m) = \alpha(f) \cdot m$$

for $f \in \mathbb{F}$ and $m \in M$. Then we can give an irreducible $A$-module $M$ an $\mathbb{F}$-module structure by

$$f \cdot m = \alpha(f)m \in M.$$

Let $\varphi \in \mathrm{End}_A(M)$. Then we find that

$$\begin{aligned} \varphi(f \circ m) &= \varphi(\alpha(f) \cdot m) \\ &= \alpha(f) \cdot \varphi(m) \\ &= f \circ \varphi(m) \end{aligned}$$

Hence $\mathbb{F} \subset \mathrm{End}_A(M)$. It is claimed that $\mathbb{F}$ is the "smallest" set with some structure such that $\mathrm{End}_A(M) = \mathbb{F}$. Then we find that

$$\mathrm{End}_{\mathrm{End}_A(M)}(M) = \mathrm{End}_{\mathbb{F}}(M).$$

On the other hand, since we have that $\mathrm{End}_A(M) \subset \mathrm{End}_{\mathbb{F}}(M)$ and $\mathrm{End}_{\mathbb{F}}(M)$ is supremum to $\mathrm{End}_A(M)$ (or maximum), one finds that the "largest" $\mathrm{End}_A(M) := \mathrm{End}_{\mathbb{F}}(M)$. Assume that $\mathrm{End}_A(M) = \mathrm{End}_{\mathbb{F}}(M)$. Then

$$\begin{aligned} \mathrm{End}_{\mathrm{End}_A(M)}(M) &= \mathrm{End}_{\mathrm{End}_{\mathbb{F}}(M)}(M) \\ &= Z(\mathrm{End}_{\mathbb{F}}(M)) \\ &\cong Z(M_n(\mathbb{F})) \\ &\cong \mathbb{F}. \end{aligned}$$

<u>Claim</u>: $\mathrm{End}_{\mathrm{End}_{\mathbb{F}}(M)}(M) = Z(\mathrm{End}_{\mathbb{F}}(M))$.

*Proof.* If

$$g \in \mathrm{End}_{\mathrm{End}_{\mathbb{F}}(M)}(M)$$

then for $\theta \in \mathrm{End}_{\mathbb{F}}(M)$ we have that

$$g(\theta(m)) = \theta g(m)$$

so that $g\theta = \theta g$. Therefore, $g \in Z(\mathrm{End}_{\mathbb{F}}(M))$. On the other hand, if $g \in Z(\mathrm{End}_{\mathbb{F}}(M))$, then for $\theta \in \mathrm{End}_{\mathbb{F}}(M)$, we have that

$$g(\theta(m)) = \theta g(m),$$

so that $g \in \mathrm{End}_{\mathrm{End}_{\mathbb{F}}(M)}(M)$. □

Since $M$ is an $A$-module and $A$ an $\mathbb{F}$-algebra, we can give $M$ an $\mathbb{F}$-module structure, by

$$fm := \alpha(f)m$$

hence $M$ is an $\mathbb{F}$-vector space. Assuming $\dim_{\mathbb{F}} M < \infty$, we find that $M$ has a basis. It follows that $Z(\mathrm{End}_{\mathbb{F}}(M)) \cong Z(M_n(\mathbb{F}))$. Furthermore,

$$\begin{aligned} Z(M_n(\mathbb{F})) &= \{aI \mid a \in \mathbb{F}\} \\ &\cong \mathbb{F}. \end{aligned}$$

$\mathrm{End}_A(M) = A$-equivariant maps $= A$-linear maps.

**Corollary 5.3.1.** *Assume that $\mathbb{F}$ is algebraically closed, that $A$ is a semisimple $\mathbb{F}$-algebra and that $M$ is an irreducible $A$-module. Let $\rho : A \longrightarrow \operatorname{End}(M)$. Then*

*a)*

$$\operatorname{im} \rho = \operatorname{End}_{\mathbb{F}}(M) \qquad (\textit{Burnsides theorem}).$$

*b)*

$$\begin{aligned} \dim \operatorname{im} \rho &= \dim A_M \\ &= (\dim_{\mathbb{F}} M)^2 \end{aligned}$$

*c)*

$$\dim n_M(A) = \dim_{\mathbb{F}}(M).$$

*Proof.* $a$): By 2.0.5, we have

$$\operatorname{End}_A(M) = \mathbb{F}.$$

By 5.1.1, we have

$$\begin{aligned} \operatorname{im} \rho &= \operatorname{End}_{\operatorname{End}_A(M)}(M) \\ &= \operatorname{End}_{\mathbb{F}}(M). \end{aligned}$$

$b$)

$$\begin{aligned} \dim \operatorname{im} \rho &= \dim \operatorname{End}_{\mathbb{F}}(M) \\ &= \dim(M_n(\mathbb{F})) \\ &\cong n^2 \end{aligned}$$

$c$)

$$\begin{aligned} n_M(A) &= \frac{\dim A_M}{\dim M} \\ &= \frac{(\dim M)^2}{\dim M} \\ &= \dim M. \end{aligned}$$

□

## 5.4 $\operatorname{End}_A(M)$

3 points of view:

- $\operatorname{End}_A(M) = A$-linear endomorphisms $M \longrightarrow M$.
- $\operatorname{End}_A(M) = A$-equivariant endomorphisms.
- $\operatorname{End}_A(M) =$ Centralizer of $\operatorname{im} \rho$, i.e. $\mathbf{C}_{\operatorname{End}(M)}(\operatorname{im} \rho)$, where $\rho : A \longrightarrow \operatorname{End}(M)$.

Let $\varphi \in \mathrm{End}_A(M)$, then

$$
\begin{tikzcd}
m \in M \arrow[rrr, mapsto] \arrow[ddd, mapsto] & & & \varphi(m) \arrow[ddd, mapsto] \\
& M \arrow[r, "\varphi"] \arrow[d, "a"'] & M \arrow[d, "a"] & \\
& M \arrow[r, "\varphi"'] & M & \\
am \in M \arrow[rrr, mapsto] & & & \varphi(am) = a\varphi(m)
\end{tikzcd}
$$

$$\mathrm{End}_A(M) = \{\varphi \in \mathrm{End}(M) \mid \varphi(am) = a\varphi(m)\}.$$

We can write $\rho$ or not

$$= \{\varphi \in \mathrm{End}_A(M) \mid \varphi(\rho(a)m) = \rho(a)\varphi(m)\}.$$

$\mathrm{End}(M) = \mathrm{End}_{\mathbb{F}}(M)$.

# Chapter 6

# Lecture 6

Recall:

**Corollary 6.0.1.** *Assume*

- $\mathbb{F}$ *algebraically closed*
- $A$ *semisimple* $\mathbb{F}$*-algebra*
- *That* $M$ *is an irreducible* $A$*-module,* $\rho : A \to \mathrm{End}(M)(\cong M_n(\mathbb{F}))$

*Then*

*a)* $\mathrm{im}\,\rho = \mathrm{End}(M)$

*b)* $\dim \rho = \dim A_M = \dim(M)^2$

*c)* $n_M(A) = \dim M$

**Corollary 6.0.2.** *Let* $\mathcal{M}(A)$ *be the set of isomorphism classes of irreducible* $A$*-modules. Then*

$$\dim A = \sum_{M \in \mathcal{M}(A)} (\dim M)^2$$

*Proof.*

$$A = \prod_{M \in \mathcal{M}(A)} A_M$$

is a direct product of $A$-algebras = the **isotypic** components. □

Special case: $A = \mathbb{F}[G]$, where $\mathrm{char}(\mathbb{F}) \nmid |G|$ (consider 2.0.3, for semisimple $A$).

Then we have that

$$\begin{aligned} |G| &= \dim \mathbb{F}[G] \\ &= \sum_{M \in \mathcal{M}(\mathbb{F}[G])} (\dim M)^2. \end{aligned}$$

**Example 6.0.3.** Let

$$\begin{aligned} G &= D_6 \\ &\cong S_3 \end{aligned}$$

of order

$$6 = 1^2 + 1^2 + 2^2.$$

For all $n$ there are two 1-dimensional subrepresentations. One can see that

$$S_n \twoheadrightarrow S_n/A_n \simeq Z_2$$

where $A_n$ is the <u>commutator subgroup</u> of $S_n$ for $n > 1$.

Let $G \xrightarrow{\pi} G/N \xrightarrow{r} \mathrm{GL}(V)$ by the composition of the projection map $\pi$ onto a normal subgroup $N$, with a representation $r$ of $G/N$.

If $r$ is a representation of $G/N$, then $r \circ \pi$ is a representation of $G$. We get the following (commutative) diagram

$$\begin{tikzcd} G \arrow[rr, "r"] \arrow[dr, two heads, "\pi"'] & & \mathrm{GL}(V) \\ & G/\ker r \arrow[ur] & \end{tikzcd}$$

<u>Recall</u>: If $G$ is abelian $\implies$ every irreducible representation is 1-dimensional (2.0.13).

**Corollary 6.0.4.** *Let $G$ be a (finite) abelian group. Then $G$ has $|G|$ isomorphism classes of irreducible representations, all of dimension 1, that is*

$$\begin{aligned} |G| &= 1^2 + \ldots + 1^2 \\ &= \text{\# of isomorphism classes.} \end{aligned}$$

*Proof.* Use the fact that

$$G \text{ abelian} \Leftrightarrow G' = \{1\}$$

together with the fact that $|G/G'| = |G|$ gives the number of irreducible one dimensional representations. Since

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 \tag{6.1}$$

we find that all of $G$:s representations are one dimensional. □

*Remark* 6.0.5. We will see that the converse of the statement also holds.

**Corollary 6.0.6.** *The dimension of the center of the $\mathbb{F}$-algebra $A$, $Z(A)$, equals # isomorphism classes of irreducible $A$-modules:*

$$\dim Z(A) = \text{\# isomorphism classes of irreducible } A\text{-modules.}$$

**Lemma 6.0.7.** *Let $R$ be a unital ring. If*

$$R = R_1 \times R_2$$

*then*

$$Z(R) = Z(R_1) \times Z(R_2).$$

*Proof.* Consider

$$Z(R_1) = \{a \in R_1 \mid ar_1 = r_1 a, \forall r_1 \in R_1\}$$

and

$$Z(R_2) = \{b \in R_2 \mid br_2 = r_2 b, \forall r_2 \in R_2\}$$

as well as

$$Z(R) = Z(R_1 \times R_2) = \{(a,b) \in R = R_1 \times R_2 \mid (a,b) \cdot (c,d) = (c,d) \cdot (a,b), \forall (c,d) \in R\}.$$

If $(a,b) \in Z(R_1) \times Z(R_2)$, then for arbitrary $(c,d) \in R$ one finds that

$$\begin{aligned}(a,b) \cdot (c,d) &= (ac, bd) = (ca, db) \\ &= (c,d) \cdot (a,b)\end{aligned}$$

so that

$$(a,b) \in Z(R) \implies Z(R_1) \times Z(R_2) \subset Z(R).$$

We want to show that $Z(R) \subset Z(R_1) \times Z(R_2)$. Let

$$z = (z_1, z_2) \in Z(R).$$

Then we want to show that $z_i \in Z(R_i)$. Note that

$$\begin{aligned}(z_1 a, 0) &= (z_1, z_2) \cdot (a, 0) \\ &= (a,0) \cdot (z_1, z_2) \\ &= (a z_1, 0) \\ &\implies z_1 \in Z(R_1).\end{aligned}$$

Similarly, we find that $z_2 \in Z(R_2)$, so that

$$(z_1, z_2) \in Z(R_1) \times Z(R_2) \implies Z(R) \subset Z(R_1) \times Z(R_2)$$

$$\implies Z(R) = Z(R_1) \times Z(R_2).$$

□

Now, we prove corollary 6.0.6.

*proof of corollary* 6.0.6. Recall:

$$A = \prod_{M \in \mathcal{M}(A)} A_M.$$

6.0.7 gives us that

$$Z(A) = \prod_{M \in \mathcal{M}(A)} Z(A_M).$$

We want to show that $\dim Z(A_M) = 1$. By burnsides theorem (5.3.1) we know that $\operatorname{im}\rho = \operatorname{End}_{\mathbb{F}}(M)$ and that $\dim \operatorname{im}\rho = \dim A_M$. Therefore,

$$\begin{aligned}\dim \operatorname{im}\rho &= \dim \operatorname{End}_{\mathbb{F}}(M)\\ &= \dim A_M\end{aligned}$$

Therefore,

$$\begin{aligned}\dim Z(A_M) &= \dim Z(\operatorname{End}_{\mathbb{F}}(M))\\ &= \dim_{\mathbb{F}}(\mathbb{F})\\ &= 1.\end{aligned}$$

□

*Remark* 6.0.8. Note that, in the proof above, we used that $\operatorname{End}(M) \cong M_n(\mathbb{F})$ so that

$$\begin{aligned}Z(\operatorname{End}(M)) &\cong Z(M_n(\mathbb{F}))\\ &= \{fI_n \mid f \in \mathbb{F}\}\\ &\cong \mathbb{F}.\end{aligned}$$

If we go back to the special case $\mathbb{F}[G]$, where $\operatorname{char}(\mathbb{F}) \nmid |G|$, we don't need $\mathbb{F}$ algebraically closed. Let $G \curvearrowright G$ be the group-action of $G$ acting on itself by conjugation, i.e.

$$(g, x) \longmapsto gxg^{-1}.$$

We have

$$G = \coprod_{i=1}^{s} \mathscr{K}_i$$

where $\mathscr{K}_i$ for $1 \leq i \leq s$ are the conjugacy-classes of $G$. Put

$$\begin{aligned}K_i &:= \sum_{g \in \mathscr{K}_i} g\\ &= \sum_{g \in \mathscr{K}_i} 1_{\mathbb{F}} \cdot g \in \mathbb{F}[G]\end{aligned}$$

.

<u>Observe</u>: $K_i \in Z(\mathbb{F}[G])$ and $hK_ih^{-1} = K_i$ for all $h \in G$ (6.0.7).

**Lemma 6.0.9.** *$(K_i)_{i=1}^s$ is a basis of $Z(\mathbb{F}[G])$.*

*Proof.* $K_i$ is linearly independent from $K_j$, where $i \neq j$, since $\mathscr{K}_i \cap \mathscr{K}_j = \varnothing$ for all $i \neq j$. We know that $G$ is a basis of $\mathbb{F}[G]$.

Let $\alpha \in Z(\mathbb{F}[G])$, so that

$$\alpha = \sum a_g g.$$

Then $\alpha$ is in the span of $(K_i)_{i=1}^s$. We note that

$$\alpha \in Z(\mathbb{F}[G]) \Leftrightarrow h\alpha h^{-1} = \alpha, \forall h \in G.$$

We consider that

$$\begin{aligned} h\alpha h^{-1} &= h\Big(\sum_{g\in g} a_g g\Big)h^{-1} \\ &= \sum_{g\in G} a_g hgh^{-1} \\ &= \sum_{g\in G} a_g g \\ &= \alpha. \end{aligned}$$

Then we find that we can rewrite

$$\begin{aligned} \sum_{g\in G} a_g g &= \sum_{hgh^{-1}\in G} a_{hgh^{-1}} hgh^{-1} \\ \rightsquigarrow \sum_{g\in G} a_g hgh^{-1} &= \sum_{hgh^{-1}\in G} a_{hgh^{-1}} hgh^{-1}. \end{aligned}$$

By the linear independence of the basis elements $hgh^{-1} \in G$, one finds that

$$a_g = a_{hgh^{-1}} \tag{6.2}$$

By definition, if $x, y \in \mathrm{Cl}(x) = \{hxh^{-1} \mid h \in G\}$, then there exists $h \in G$ so that $hxh^{-1} = y$. But then we find that $a_{hxh^{-1}} = a_y$. Then 6.2 shows that for an arbitrary element

$$\alpha = \sum_{g\in G} a_g g \in Z(\mathbb{F}[G])$$

the coefficients $a_g, a_h$ for elements $h, g$ in the same conjugacy class, must be the same. We conclude that we can write arbitrary $\alpha \in Z(\mathbb{F}[G])$ as $\alpha = \sum_{i=1}^{s} a_i K_i$ for $a_i \in \mathbb{F}$. □

*Remark* 6.0.10. Remember that $hgh^{-1} = hg'h^{-1} \Leftrightarrow g = g'$, hence $hGh^{-1} = G$, so WLOG one can rewrite $G$ as $hGh^{-1}$ in the index of the sum in the proof (of lemma 6.0.9)

Proof of claim in proof of lemma 6.0.9: We want to prove the direction: If $h\alpha h^{-1} = \alpha$ for arbitrary $\alpha \in \mathbb{F}[G]$ and for all $h \in G$, then $\alpha \in Z(\mathbb{F}[G])$.

*Proof.* Note that one finds that $h\alpha = \alpha h \Leftrightarrow \sum_{g\in G} a_g hg = \sum_{g\in G} a_g gh$. Rewriting the RHS as

$$\sum_{hgh^{-1}\in G} a_{hgh^{-1}}(hgh^{-1})h = \sum_{hgh^{-1}\in G} a_{hgh^{-1}} hg$$

we have

$$\sum_{g\in G} a_g hg = \sum_{hgh^{-1}\in G} a_{hgh^{-1}} hg.$$

It follows that $a_g = a_{hgh^{-1}}$ for arbitrary $h \in G$. This shows that (as in the proof of lemma 6.0.9) the coefficients $a_g$ is the same for all elements $g$ in the same conjugacy class.

Now, take arbitrary

$$\beta = \sum_{h\in G} b_h h.$$

We find that

$$\begin{aligned}\beta\alpha &= \left(\sum_{h\in G} b_h h\right)\left(\sum_{g\in G} a_g g\right)\\ &= \sum_{(h,g)\in G\times G} b_h a_g hg.\end{aligned}$$

On the other hand, we have

$$\begin{aligned}\alpha\beta &= \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right)\\ &= \sum_{(g,h)\in G\times G} a_g b_h gh.\end{aligned}$$

We rewrite $\alpha\beta$ as

$$\begin{aligned}\alpha\beta &= \sum_{\substack{(hgh^{-1},h)\in G\times G\\ h\in G}} a_{hgh^{-1}} b_h (hgh^{-1})h\\ &= \sum_{\substack{(hgh^{-1},h)\in G\times G\\ h\in G}} a_g b_h hg.\end{aligned}$$

We see that $(hgh^{-1}, h) \in G \times G$, as we let $h$ and $g$ vary over all elements in $G$, covers every element $(g, h) \in G \times G$ ($\mathrm{int}(h)(g) = hgh^{-1}$ is an automorphism of $G$). We have

$$a_g b_h = b_h a_g \quad (a_g, b_h \in \mathbb{F}).$$

Furthermore, all $hg \in G$ are basis elements of $\mathbb{F}[G]$ so that $\alpha\beta = \beta\alpha \implies \alpha \in Z(\mathbb{F}[G])$. □

From lemma 6.0.9 one finds that

**Corollary 6.0.11.** $\dim Z(\mathbb{F}[G]) = \#$ *of conjugacy classes.*

**Corollary 6.0.12.** $\mathbb{F}$ *algebraically closed* $\implies$ $\#$ *of conjugacy classes of* $G = \#$ *of isomorphism classes of irreducible representations.*

## 6.1 Application of burnside's theorem

**Definition 6.1.1.** A linear transformation $T : V \to V$ is **unipotent** if $\lambda = 1$ is its only eigenvalue (over an algebraic closure $\overline{\mathbb{F}} \supset \mathbb{F}$, given that $V$ is a vector space over $\mathbb{F}$). Equivalently, $T$ is unipotent $\Leftrightarrow T - I$ is nilpotent $\Leftrightarrow \exists x \in \mathrm{GL}(V)$ so that

$$xTx^{-1} = \begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

(see “Jordan Canonical Form” (JCF)).

JCF $\implies$ $A$ nilpotent in $\mathrm{End}(V) \Leftrightarrow A^n = 0 \Leftrightarrow \exists x \in \mathrm{GL}(V)$ such that

$$xAx^{-1} = \begin{pmatrix} 0 & * & * & \dots & * \\ 0 & 0 & * & \dots & * \\ 0 & 0 & 0 & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

**Theorem 6.1.2.** *If $A \in M_n(\mathbb{F})$ is a nilpotent matrix, then all eigenvalues of $A$ are zero.*

*Proof.* Assume there exists an eigenvalue $\lambda$ of $A$ such that $\lambda \neq 0$. Then $Av = \lambda v$ for the associated eigenvector $v \in \mathbb{F}^n$. Then $A^2v = A(Av) = A(\lambda v) = \lambda A(v) = \lambda^2 v \rightsquigarrow A^n v = \lambda^n v$, but $A^n = \mathbf{0}_{n\times n}$, and the zero matrix has only 0 as an eigenvalue, since $\mathbf{0}_{n\times n}v = \mathbf{0}_n$, contradicting our assumption. Hence all eigenvalues of $A$ are zero. □

**Definition 6.1.3.** A subgroup $G \subset \mathrm{GL}(V)$ is **unipotent** if $g$ is unipotent, $\forall g \in G$.

**Theorem 6.1.4.** *Assume that $\mathbb{F}$ is an algebraically closed field, and that $char(\mathbb{F}) \nmid |G|$, for a finite group $G$. Then we have that if $G$ is unipotent $\implies \exists x \in GL(V)$ such that*

$$xGx^{-1} \subset \mathbb{U}_n = \left\{ \begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \right\}$$

*so that there exists a basis $\{e_1, \dots, e_n\}$ in which matrices of $g \in G$ are unipotent. Furthermore, we have that*

1. *$\rho : G \to GL(V)$ is reducible $\Leftrightarrow$ exists a basis $\{e_1, \dots, e_n\}$ so that $\rho$ is a* block upper triangular *matrice*

$$\begin{pmatrix} r \times r & r \times n - r \\ \mathbf{0} & n - r \times n - r \end{pmatrix}$$

2. *$\rho = \rho_1 \oplus \rho_2$ where $\rho_i : G \to GL(V_i) \implies \exists$ basis $\{e_1, \dots, e_n\}$ so that we get a block-matrix on the form*

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

.

*Remark* 6.1.5.

$$\mathbb{U}_n = \left\{ \begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \right\}$$

in 6.1.4 is the **group** of quadratic unipotent matrices of dimension $n \times n$. It follows from the group axioms that each matrix $u \in \mathbb{U}_n$ is invertible.

*Proof.* To prove 1., in the direction $\Longleftarrow$: We have that the span of $\{e_1, \dots, e_r\}$ is $G$-stable.

To prove 1., in the direction $\Longrightarrow$: If $\{e_1, \dots, e_r\}$ basis for $W$ and extending. □

<u>Proof of the statement</u> that if $\mathbb{F}$ is algebraically closed, and $\operatorname{char} \mathbb{F} \nmid |G|$ for finite group $G$, then if $G$ is *unipotent* $\implies \exists x \in \mathrm{GL}(V)$ such that $xGx^{-1}$ is a subset of $\mathbb{U}_n$:

*Proof.* Assume $\exists 0 \subsetneqq W \subsetneqq V$ where $W$ is a *G-stable subspace*. Then $G \to \mathrm{GL}(W)$ and $G \to \mathrm{GL}(V/W)$ have *unipotent image*. By induction, there exists bases $w_1, \dots, w_r$ of $W$ and $v_1 + W, \dots, v_s + W$ of $V/W$ such that the matrices are on unipotent form for all $g \in G$. □

Here is (I believe) the same proof, but with a bit more detail:

*Proof.* Let $\mathrm{id} : G \hookrightarrow \mathbb{U}_n \hookrightarrow \mathrm{GL}(V)$ be the identity representation of $G$. id is not an irreducible representation, since $\mathrm{span}(e_1)$ is $\mathbb{U}_n$-stable, hence gives a non-trivial subrepresentation of id.

We divide the proof in two cases.

Assume first that $(V, \mathrm{id})$ is *reducible*. We now perform induction (with respect to unipotent action) on the dimension of $W$; that is, we show the action of id acting unipotently in the base case $k = 1$, and in the inductive step, we assume it holds for $n - 1$, and shows that it must hold for $n$, where $\dim V = n$.

Assume first that we have $0 \subsetneqq W \subsetneqq V$ that is 1-dimensional and $G$-stable. Then $V = \mathrm{span}(e_1)$. But then $\mathrm{id}(g) = 1, \forall g \in G$, which is a unipotent action (note that $\mathbb{U}_1 := \{1\}$). Then we get the induced representation $V/\mathrm{span}(e_1)$ of dimension $n-1$. By induction, we find that id act's unipotently (through $U_{n-1}$) on $V/\mathrm{span}(e_1)$. It follows that

$$V \cong \mathrm{span}(e_1) \oplus V/\mathrm{span}(e_1)$$

with associated homomorphisms

$$\rho_{\mathrm{span}(e_1)} \oplus \rho_{V/\mathrm{span}(e_1)}$$

can be represented in a basis as

$$\begin{pmatrix} 1 & * \\ 0 & A \end{pmatrix}$$

where $A \subset \mathbb{U}_{n-1}$. This shows that $G$:s action on $V$ can be represented as acting through $\mathbb{U}_n$.

Assume that $(V, \mathrm{id})$ is *irreducible*. We apply burnsides theorem on matrix rings (see [3]). Then we have that the $\mathbb{F}$-span of $G$ is $M_n(\mathbb{F}) \cong \mathrm{End}(V)$.

Since $G$ acts unipotently on $V$, we have that $\mathrm{tr}(g) = n, \forall g \in G$. Since $\mathrm{tr}(A + B) = \mathrm{tr}(A) + \mathrm{tr}(B)$ for $A, B \in M_n(\mathbb{F})$, we have that $\mathrm{tr}(g - I) = 0$.

<u>Claim</u>: $\mathrm{tr}(gA - A) = 0$, for all $A \in \mathrm{End}(V)$ and for all $g \in G$.

*Proof.* Using the fact that $\mathrm{Span}_{\mathbb{F}}(G) = M_n(\mathbb{F}) \cong \mathrm{End}(V)$, we have that for all $A \in \mathrm{End}(V)$

$$A = \sum_{h \in G} \lambda_h h.$$

Then for each $g \in G$, we find that

$$\begin{aligned}
\operatorname{tr}(gA - A) &= \operatorname{tr}\left(g\sum_{h\in G}\lambda_h h - \sum_{h\in G}\lambda_h h\right)\\
&= \operatorname{tr}\left(\sum_{h\in G}\lambda_h hg - \sum_{h\in G}\lambda_h h\right)\\
&= \sum_{h\in G}\left(\lambda_h \operatorname{tr}(gh) - \lambda_h \operatorname{tr}(h)\right)\\
&= 0.
\end{aligned}$$

Here we used that $\operatorname{tr}(cA) = c\operatorname{tr}(A)$ for $c \in \mathbb{F}$ and $A \in M_n(\mathbb{F})$, as well as the fact that for each term $\operatorname{tr}(gh)$ there there exists a $s \in G$ so that $\operatorname{tr}(s) = \operatorname{tr}(gh)$, and the other way around, which explains why the sum equals 0. $\square$

It follows that

$$\operatorname{tr}(gA - A) = \operatorname{tr}((g - I)A) = 0$$

for all $A \in \operatorname{End}(V)$.

Fact: One can show that the trace **form** (codomain $\mathbb{F}$)

$$\operatorname{tr} : M_n(\mathbb{F}) \times M_n(\mathbb{F}) \to \mathbb{F}$$

defined explicitly by

$$(A, B) \mapsto \operatorname{tr}(AB)$$

is **non-degenerate**.

Recall: A non-degenerate form in finite dimensions (with respect to $V$) $f : V \times V \to \mathbb{F}$ is such that if $f(x, y) = 0$ for all $y \in V$, then $x = 0$.

One finds that

$$(g - I, A) \longmapsto \operatorname{tr}((g - I)A) = 0$$

for all $A \in \operatorname{End}(V) \cong M_n(\mathbb{F}) \implies g - I = 0 \Leftrightarrow g = I$, for all $g \in G$. It follows that $G = 1$ is the trivial group, and that $G$ acts unipotently on $V$. $\square$

# Chapter 7

# Lecture 7

Let $G$ be a finite *group*, and let $\mathbb{F}$ be a field of characteristic not dividing the order of $G$. Then the group-ring $\mathbb{F}[G]$ is *semisimple* and we have $\mathbb{F}[G] = \underbrace{A_{M_1} \times \ldots \times A_{M_s}}_{\text{isotypic components}}$, where all $A_{M_i}$ are $\mathbb{F}$-algebras (set $A = \mathbb{F}[G]$).

When $\mathbb{F}$ is *algebraically closed*, we have $A_{M_i} \cong M_{n_i}(\mathbb{F})$, where $n_i$ is the dimension of the irreducible representation $M_i$ (that is, $\chi_{M_i}(1)$ of the induced character $\chi_{M_i}$ from the representation $\rho_{M_i}$ on $M_i$).

The above applies if $A$ is semisimple, i.e. even if $A$ is not $\mathbb{F}[G]$.

Note: If $M_i$ is an $\mathbb{F}[G]$-module, then $M_i$ is an $\mathbb{F}$-module (induced by restricting the module-action of $\mathbb{F}[G]$ on $M_i$ to $\mathbb{F}$), hence an $\mathbb{F}$ vector space, so that a basis exists (Zorns lemma).

*Comment* 7.0.1. We will implicitly assume that any $\mathbb{F}$-algebra is finite-dimensional, unless otherwise specified.

**Definition 7.0.2.** A *unital* ring $R$ is a **division-ring** if $R^\times = R \setminus \{0\}$ and $R \neq 0$, i.e. $0 \neq 1$. That is, for all $a \in R, a \neq 0$, there is a $b \in R$ such that

$$\begin{aligned} ab &= ba \\ &= 1 \end{aligned} \tag{7.1}$$

*Remark* 7.0.3. By definition of a multiplicative inverse, we need $b$ to be a two-sided inverse to $a$, which explains 7.1, without assuming that $R$ is commutative.

**Definition 7.0.4.** A **division $\mathbb{F}$-algebra** is an $\mathbb{F}$-algebra which is also a division-ring.

**Definition 7.0.5.** A simple $\mathbb{F}$-algebra $R$ is a **central simple $\mathbb{F}$-algebra** if $Z(R) = \mathbb{F}$.

**Example 7.0.6.** The matrix ring $M_n(\mathbb{C})$ is a central simple $\mathbb{C}$-algebra. $M_n(\mathbb{C})$ is also a *simple* $\mathbb{R}$-algebra, but not a central $\mathbb{R}$-algebra over $\mathbb{R}$, since $Z(M_n(\mathbb{C})) \cong \mathbb{C} \ncong \mathbb{R}$.

*Comment* 7.0.7. Recall that for a matrix ring $M_n(\mathbb{F})$ over a field $\mathbb{F}$, we have that

$$Z(M_n(\mathbb{F})) = \{\lambda \cdot I \mid \lambda \in \mathbb{F}\} \cong \mathbb{F}.$$

We find that the ring-homomorphism $r : \mathbb{F} \to M_n(\mathbb{F})$ defined by $\mathbb{F} \ni f \longmapsto f \cdot I \in M_n(\mathbb{F})$ gives us a well-defined unital $\mathbb{F}$-algebra-homomorphism.

**Theorem 7.0.8.** *(Wedderburn)*

a) *Let $R$ be a simple $\mathbb{F}$-algebra $\implies$ $R = M_n(D)$ for some positive integer $n \geq 1$ and some division $\mathbb{F}$-algebra $D$ (recall 7.0.4).*

b) *Let $R$ be a* central *simple $\mathbb{F}$-algebra $\implies$ $R = M_n(D)$ with $D$ a division $\mathbb{F}$-algebra such that $Z(D) = \mathbb{F}$.*

*Conversely, for all $n \geq 1$, where $n$ is a positive integer, and for all division $\mathbb{F}$-algebras, we have that $M_n(\mathbb{F})$ is a simple $\mathbb{F}$-algebra and if $Z(D) = \mathbb{F}$ then $Z(M_n(D)) = \mathbb{F}$.*

*Remark* 7.0.9. If $D$ is a division-ring, then $Z(D)$ is a field (recall: a field is a *commutative division ring* with $0 \neq 1$).

From the theorem, we see that if $R$ is a semisimple $\mathbb{F}$-algebra, then

$$Z(R) = Z(M_n(D)) = Z(D)$$

is a field.

Exercise: Show that $Z(M_n(D)) = Z(D)$.

Sketch: For any matrix-ring, the center $Z(M_n(D)) = \{\lambda \cdot I \mid \lambda \in Z(D)\}$ (we are not assuming that $D$ is commutative).

We get a natural unital ring-homomorphism $f : Z(M_n(D)) \to Z(D)$ defined by $\lambda \cdot I \longmapsto \lambda$.

This unital ring-homomorphism is clearly bijective.

Another (related) way that division-rings arise in representation-theory: Let $A$ be a *finitely* generated $\mathbb{F}$-algebra (not assuming semisimple) and let $M$ be an irreducible $A$-module. Part of Schur's lemma that holds even if is not $\mathbb{F}$ algebraically closed:

$$\mathrm{End}_A(M) = \mathrm{Hom}_A(M, M)$$

is a division-ring.

Claim: When $\mathbb{F}$ is algebraically closed, a finite-dimensional division $\mathbb{F}$-algebra $\cong \mathbb{F}$.

*Proof.* Let $D$ be a finite-dimensional division $\mathbb{F}$-algebra and let $\alpha \in D \setminus \{0\}$. The idea is to construct a *minimal polynomial* of $\alpha/\mathbb{F}$.

Recall: A *field extension* of $\mathbb{F}$ is a field $\mathbb{L} \supset \mathbb{F}$. $\mathbb{L}$ is a *finite field extension* if $\dim_{\mathbb{F}} \mathbb{L}$ is finite-dimensional, i.e. if $\mathbb{L}$ seen as an $\mathbb{F}$ vector space, is finite-dimensional. If $\mathbb{L}/\mathbb{F}$ is a field-extension $\implies$ $\mathbb{L}$ is an $\mathbb{F}$-algebra.

We consider the evaluation-homomorphism $\mathrm{ev}_\alpha : \mathbb{F}[x] \to D$ defined explicitly by

$$\mathbb{F}[x] \ni f(x) = a_n x^n + \ldots + a_1 x + a_0 \longmapsto a_n \alpha^n + \ldots + a_1 \alpha + a_0 \in D$$

for $a_i \in \mathbb{F}$ (note that since $D$ is an $\mathbb{F}$-algebra, it is an $\mathbb{F}$-vector space, so that addition and multiplication of $\alpha$ by $a_i$ is well-defined).

$$\begin{array}{ccc} \mathbb{F}[x] & \longrightarrow & D \\ 1 & \longmapsto & 1 \\ x & \longmapsto & \alpha \end{array}$$

We consider the kernel of the evaluation-homomorphism,

$$\ker(\mathrm{ev}_\alpha) = \{f(x) \in \mathbb{F}[x] \mid f(\alpha) = 0\}.$$

Note that since $\mathbb{F}[x]$ is an infinite-dimensional $\mathbb{F}$-vector space with a basis $\{1, x, x^2, \ldots, \}$, we can not have an injection into $D$, since we then see that $\{1, \alpha, \alpha^2, \ldots\}$ would be an infinite-dimensional $\mathbb{F}$-vector space basis for $D$. Hence $\ker(\mathrm{ev}_\alpha) \neq 0$.

Recall: If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a prinicipal ideal domain (P.I.D.). Since $\ker(\mathrm{ev}_\alpha) \lhd \mathbb{F}[x]$ then $(m_\alpha(x)) = \ker(\mathrm{ev}_\alpha)$.[1]

Indeed, there is a unique monic generator $m(x)$ for every ideal $I = (m(x)) \lhd \mathbb{F}[x]$. We denote this unique monic generator of $\ker(\mathrm{ev}_\alpha))$ as $m_\alpha(x)$.

We find that $\mathbb{F}[x]/\ker(\mathrm{ev}_\alpha) \cong \mathrm{im}(\mathrm{ev}_\alpha) \subset D$. We claim that the image $\mathrm{im}(\mathrm{ev}_\alpha)$ is an integral domain (I.D.).

*Proof.* First, recall that the image of a ring-homomorphism is a subring of the codomain, here $D$. Note that

$$f(r(x)s(x)) = f(r(x))f(s(x))$$

and

$$f(s(x)r(x)) = f(s(x))f(r(x))$$

while

$$f((r(x)s(x)) = f(s(x)r(x))$$

for all $r(x), s(x) \in \mathbb{F}[x]$, so that all elements in the image under the evaluation-homorphism $\mathrm{ev}_\alpha$ commutes. Furthermore, if $a, b \in D$ so that

$$ab = 0 \Leftrightarrow a^{-1}ab = 0 \implies b = 0$$

(where we have used that $D$ is a division-ring). $\square$

$\mathrm{im}(\mathrm{ev}_\alpha)$ is an integral domain $\Leftrightarrow \ker(\mathrm{ev}_\alpha)$ is a *prime*-ideal. Since $\mathbb{F}[x]$ is an P.I.D., the prime ideals are also maximal ideals.

Therefore, $\ker(\mathrm{ev}_\alpha)$ is maximal $\Leftrightarrow \mathbb{F}[x]/\ker(\mathrm{ev}_\alpha) \cong \mathrm{im}(\mathrm{ev}_\alpha)$ is a *field*.

We note that if $a \in \mathrm{im}(\mathrm{ev}_\alpha)$ then for $f \in F$, we have that $f \cdot a \in \mathrm{im}(\mathrm{ev}_\alpha)$. Thus, $\mathrm{im}(\mathrm{ev}_\alpha)$ is closed under multiplication by elements from $\mathbb{F}$. Since $D$ is already an $\mathbb{F}$-algebra, we see that then $\mathrm{im}(\mathrm{ev}_\alpha)$ is an $\mathbb{F}$-vectorspace, and actually a subspace of the finite-dimensional $\mathbb{F}$-vectorspace $D$, hence finite-dimensional.

[1] If $R$ is a ring, then we let $I \lhd R$ denote that $I$ is an ideal of $R$.

Any ring-homomorphism $f : \mathbb{F} \to D$ where $\mathbb{F}$ is a field is injective (recall that $\ker(f)$ is an ideal), we find that $D$ contains an isomorphic copy of $\mathbb{F}, \operatorname{im}(f)$, so that $\mathbb{F} \subset D$. Now, $\mathbb{F} \subset \operatorname{im}(\mathrm{ev}_\alpha)$ is a finite field extension, but since $\mathbb{F}$ is algebraically closed, $\operatorname{im}(\mathrm{ev}_\alpha) = \mathbb{F}$, so that $\alpha \in \mathbb{F}$.

To summarize, we have shown that if $\alpha \in D \setminus \{0\}$ then $\alpha \in \mathbb{F}$, so that $D \subset \mathbb{F}$, and $\mathbb{F} \subset D$ by the previous paragraph $\implies D = \mathbb{F}$. □

*Remark* 7.0.10. If $\mathbb{L} \supset \mathbb{F}$ is a finite-field extension of an algebraically closed field $\mathbb{F}$, then $\mathbb{L} = \mathbb{F}$. All finite field extensions are algebraic, so that every element $\alpha \in \mathbb{L}$ have an associated minimal polynomial $m_{\alpha,\mathbb{F}} \in \mathbb{F}[x]$. But since $m_{\alpha,\mathbb{F}}$ splits into linear factors, we have that $\alpha \in \mathbb{F}$.

**Example 7.0.11.** If $\mathbb{F}$ is a finite field then every finite-dimensional $\mathbb{F}$-division algebra is a field. Equivalently, every finite-dimensional division ring is a field (proof on HW).

**Example 7.0.12.** (Hamilton quaternions) Let $\mathbb{F} = \mathbb{R}$ and let $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, so that $\mathbb{H}$ is a 4-dimensional $\mathbb{R}$-vector space.

Note that if $\mathbb{L}/\mathbb{R}$ is a finite-dimensional field extension, then $\mathbb{L} = \mathbb{R}$ or $\mathbb{L} = \mathbb{C}$.

Any $q \in \mathbb{H}$ is on the form $q = a + bi + cj + dk$ for $a, b, c, d \in \mathbb{R}$ where $ij = k$ and $ji = -k$.

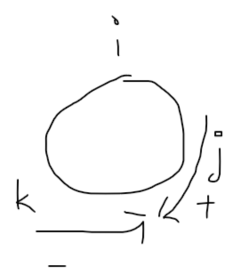


Figure 7.1: Multiplication in $\mathbb{H}$

Multiplication works as illustrated in the figure above, e.g. $kj = -i$ and $jk = i$.

Multiplication in $\mathbb{H}$ makes $\mathbb{H}$ into an $\mathbb{R}$-algebra. Furthermore, if $\mathbb{H} \ni q = a + bi + cj + dk$ then we define $\overline{q} := a - bi - cj - dk$ and $N(q) = q\overline{q} = a^2 + b^2 + c^2 + d^2$. We have $q^{-1} = \dfrac{1}{N(q)} \cdot \overline{q} \implies \mathbb{H}$ is a division-algebra.

Recall: A finite subgroup of the multiplicative group $\mathbb{F}^\times$ of a field $\mathbb{F}$ is cyclic (by HW1, question 2). This is *not true for division-rings.*

We have $Q_8$, the quaternion group of order 8, where $Q_8 \subset \mathbb{H}^\times$.

**Theorem 7.0.13.** *Let $D/\mathbb{R}$ be a finite-dimensional division-algebra. Then $D \cong \mathbb{R}$, $D \cong \mathbb{C}$ or $D \cong \mathbb{H}$.*

- If $D$ is a division $\mathbb{F}$-algebra, with center $\mathbb{F}$, and where $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F} \rightsquigarrow D \otimes_{\mathbb{F}} \overline{\mathbb{F}}$ is a simple $\overline{\mathbb{F}}$-algebra $\implies D \otimes_{\mathbb{F}} \overline{\mathbb{F}} \cong M_n(\overline{\mathbb{F}})$, where $\dim_{\overline{\mathbb{F}}} M_n(\overline{\mathbb{F}}) = n^2$.
- Let $A$ be a *central simple* $\mathbb{F}$-algebra and let $\mathbb{L}/\mathbb{F}$ be a *finite* field extension $\implies A \otimes_{\mathbb{F}} \mathbb{L}$ which we call "extension of scalars" is a $\mathbb{L}$-algebra, where $\dim_{\mathbb{F}} A = \dim_{\mathbb{L}} A \otimes_{\mathbb{F}} \mathbb{L}$

Therefore, every division-algebra $D$ with center $\mathbb{F}$ has square dim $/\mathbb{F}$.

**Example 7.0.14.** $\mathbb{C}/\mathbb{R}$ not central simple over $\mathbb{R}$.

**Example 7.0.15.** $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$ not simple.

**Example 7.0.16.** $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$.

There are a lot of division algebras $/\mathbb{Q}$.

**Example 7.0.17.** $\mathbb{R}$ is the *completion* of $\mathbb{Q}$ relative to the usual absolute value. There exists other absolute values on $\mathbb{Q}$.

For example, for all $p \in \mathbb{Z}^+, p$ prime, we have $|-|_p$ as the $p$-adic absolute value. If $n \in \mathbb{Z}$ and $n = p^m a$ where $p \nmid a$ we set $|n| = p^{-m}$.

Note: Any $n \in \mathbb{Z}$ can be written on the form $n = p^m a$ where $p \nmid a$.

We have $\left|\frac{a}{b}\right|_p = \frac{|a|_p}{|b|_p}$ and $|a+b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$.

If we complete $\mathbb{Q}$ relative to $|-|_p$ using cauchy-sequences (in the classical sense), we get a field $\mathbb{Q}_p$ of $p$-adic numbers and division-algebras over $\mathbb{Q}_p$ with center $\mathbb{Q}_p$ of dimension $n^2$.

There exists $n-1$ non-isomorphic division-algebras over $\mathbb{Q}_p$, with center $\mathbb{Q}_p$, of dimension $n^2$.

**Example 7.0.18.** If $\mathbb{F}$ is a field then $\mathrm{Br}(\mathbb{F}) = \{[A] \mid A$ is a finite dimensional central simple $\mathbb{F}$-algebra$/ \sim \}$ where $A \sim B$ if there is a division $\mathbb{F}$-algebra $D$ with center $\mathbb{F}$ such that $A \cong M_n(D) \cong B$.

Hence $\mathrm{Br}(\mathbb{F}) = \{$div. alg.$/\mathbb{F}$ with center $\mathbb{F}\}$.

More precisely, $\mathrm{Br}(\mathbb{F})$ is a group under $\otimes$. We have $D_1 \otimes_{\mathbb{F}} D_2 \cong M_n(D)$ and $D_1 \cdot D_2 = D$.

**Example 7.0.19.** $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2$.

**Theorem 7.0.20.** *If $\mathbb{F}$ is algebraically closed, or finite, then* $\mathrm{Br}(\mathbb{F}) = 1$.

**Example 7.0.21.** $\mathrm{Br}(\mathbb{Q}_p) = \mathbb{Q}/\mathbb{Z}$.

**Lemma 7.0.22.** *Let $R$ be a simple $\mathbb{F}$-algebra, where $R$ is unital, and let $\mathcal{L}$ be a minimal left-ideal of $R$, then $R \cong \mathcal{L}^n$ as left $R$-modules.*

*Remark* 7.0.23. Think about $M_n(\mathbb{C})$ as a $\mathbb{C}$-algebra, which is not simple as left $M_n(\mathbb{C})$-module.

*Proof.* $\mathcal{L}R := \{\sum \ell_i r_i \mid \ell_i \in \mathcal{L}, r_i \in R\}$, which we claim is a two-sided ideal of $R$. Since $1 \in R$ we have that $0 \neq \mathcal{L} \subset \mathcal{L}R \implies \mathcal{L}R = R \implies 1 = \sum_{i=1}^{n} \ell_i r_i$ with $n$ minimal # of $\ell_i$ so that $\sum \ell_i r_i = 1$.

Claim:

$$\mathcal{L}^n \xrightarrow{\varphi} R$$

with

$$(a_1, \ldots, a_n) \longmapsto \sum a_i r_i$$

is an $R$-module isomorphism, where $r_i \in R$ fixed so that

$$\sum \ell_i r_i = 1.$$

*Proof.* $\varphi$ surjective: $\exists(\ell_1, \dots, \ell_n) \in \mathcal{L}^n$ so that $(\ell_1, \dots, \ell_n) \longmapsto \sum \ell_i r_i = 1$.

Recall that $\mathcal{L}$ is an left ideal of $R \rightsquigarrow \mathcal{L}^n$ left ideal of $R$.

We see that

$$\begin{aligned}
\varphi(r \cdot (\ell_1, \dots, \ell_n)) &= \varphi((r\ell_1, \dots, r\ell_n)) \\
&= \sum r\ell_i r_i = r \sum \ell_i r_i \\
&= r\varphi((\ell_1, \dots, \ell_n)) \\
&= r.
\end{aligned}$$

$\varphi$ injective: Let $K = \ker \varphi$. We want to show that $K = 0$. Assume that $K \neq 0$. Then there is an $i$ so that the projection $\pi_i : K \to \mathcal{L}$ is such that we have $(a_1, \dots, a_n) \in K \subset \mathcal{L}^n$ where

$$\pi_i(a_1, \dots, a_i, \dots, a_n) = a_i$$

where $a_i \neq 0$. Since $\pi_i$ is an $R$-module homomorphism, the image $\operatorname{im}(\pi_i) \subset \mathcal{L}$ is an $R$-submodule of $\mathcal{L}$.

Since any non-trivial left $R$-submodule of $B$ is also a non-trivial left ideal of $R$ properly contained in $B$, we need $\pi_i(K) = \mathcal{L} \implies \exists(a_1, \dots, a_i, \dots, a_n) \in K$ so that $a_i = \ell_i$.

$$\begin{aligned}
\rightsquigarrow 1 &= \varphi((\ell_1, \dots, \ell_n)) \\
&= \varphi((\ell_1, \dots, \ell_n) - (a_1, \dots, a_n)) \\
&= \varphi((\ell_1, \dots, \ell_n)) - \varphi((a_1, \dots, a_n)) \\
&= \sum_{j \neq i} \underbrace{(\ell_j - a_j) r_j}_{\leq n-1 \text{ terms}}
\end{aligned}$$

But this contradicts the assumed minimality of $n$ coefficients $\ell_i$ to express $1 \implies K = 0$. □

□

**Lemma 7.0.24.** *Let $R$ be an $\mathbb{F}$-algebra and let $\mathcal{L}$ be a left $R$-module. If $D = \operatorname{End}_R(\mathcal{L})$ then $\operatorname{End}_R(\mathcal{L}^n) \cong M_n(D)$.*

*Proof.* $\varphi$ injective: Let $\varphi : M_n(D) \to \operatorname{End}_R(\mathcal{L}^n)$, then, for $A \in M_n(D)$, we have

$$\varphi(A)(\ell_1, \dots, \ell_n) = A \begin{pmatrix} \ell_1 \\ \vdots \\ \ell_n \end{pmatrix}.$$

If $\varphi(A) = 0 \implies$

$$A(\ell e_i) = \mathbf{0}$$

$$= \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix} \cdot \ell$$
$$= \begin{pmatrix} a_{1i} \cdot \ell \\ \vdots \\ a_{ni} \cdot \ell \end{pmatrix}$$

$\implies a_{1i} \cdot \ell = \ldots = a_{ni} \cdot \ell = 0.$ for all $\ell \in \mathcal{L}$ and all $i$.

Note: $D = \mathrm{End}_R(\mathcal{L}) \implies a_{ij} \in \mathrm{End}_R(\mathcal{L})$. It follows that if $a_{ij}(\ell) = 0$ for all $i, j \in \{1, \ldots, n\}$ and all $\ell \in \mathcal{L}$ then $a_{ij} = 0$ for all $i, j \in \{1, \ldots, n\} \implies A = 0$.

(I believe).

$\varphi$ surjective:

Let $T \in \mathrm{End}_R(\mathcal{L}^n)$ and $\ell \in \mathcal{L}$. Assume $T(\ell e_j) = (\ell_{1j}, \ldots, \ell_{nj})$. Define $a_{ij} \in \mathrm{End}_R(\mathcal{L})$ so that $a_{ij}(\ell) = \ell_{ij}$.

Now, if we piece together the matrix $A = (a_{ij})$ we find that

$$A(\ell e_j) = \begin{pmatrix} a_{1j}(\ell) \\ \vdots \\ a_{nj}(\ell) \end{pmatrix}$$
$$= \begin{pmatrix} \ell_{1j} \\ \vdots \\ \ell_{nj} \end{pmatrix}.$$

We can write an arbitrary $\ell = (\ell_1, \ldots, \ell_n) \in \mathcal{L}^n$ on the form $(\ell_1, \ldots, \ell_n) = (\ell e_1 + \ldots + \ell e_n)$. Since both $T$ and $A$ act linearly on $\mathcal{L}^n$, we see that $\varphi(A) = T$. □

*Remark* 7.0.25. To see that $A$ acts linearly, note that the elements $a_{ij} \in \mathrm{Hom}_R(\mathcal{L}, \mathcal{L})$ for all $i, j \in \{1, \ldots, n\}$.

*Remark* 7.0.26. Consider that what we mean by $\ell e_j$ is

$$\ell e_j = (0, 0, \ldots, 0, \underbrace{\ell}_{j^{\text{th}} \text{ index}}, 0, \ldots 0, 0)$$

since we can't assume that $\mathcal{L}$ contains a 1.

**Corollary 7.0.27.** *Assume that $\mathcal{L}$ is simple. Then $\mathrm{End}_R(\mathcal{L}^n) \cong M_n(D)$, where $D$ is a division-ring.*

*Proof.* By lemma 7.0.24 we have $\mathrm{End}_R(\mathcal{L}^n) \cong M_n(D)$, where $D = \mathrm{End}_R(\mathcal{L})$. By schur's lemma, the endomorphism ring of a simple module is a division ring. Since $\mathcal{L}$ is simple, we have that $\mathrm{End}_R(\mathcal{L})$ is a division ring. □

We have that

$$\begin{aligned} R^{\mathrm{opp}} &\cong \mathrm{End}_R(R) \\ &\cong \mathrm{End}_R(\mathcal{L}^n) \\ &\cong M_n(D) \end{aligned}$$

and that

$$R \cong M_n(D^{\mathrm{opp}}).$$

*Comment* 7.0.28. We have an isomorphism

$$\varphi : (M_n(D))^{\mathrm{opp}} \to M_n(D^{\mathrm{opp}})$$

given by

$$(M_n(D))^{\mathrm{opp}} \ni A^{\mathrm{opp}} \longmapsto (A^{\mathrm{opp}})^t \in M_n(D^{\mathrm{opp}}).$$

# Chapter 8

# Lecture 8

- Recalll $A$ semisimple $\implies A = A_1 \times \ldots \times A_s$ where $A_i$ are the **isotypic components** and $A_1 \times \ldots \times A_s$ is the **isotypic decomposition**.
- Recall that $A_{M_i}$ annihilates $A_{M_j}$ for $i \neq j$.

  We have
  $$1 = e_1 + \ldots + e_s \tag{8.1}$$
  where $e_i$ is the identity of $A_{M_i}$. By this we mean that $e_i \cdot a_{M_i} = e_i \cdot a_{M_i} = a_{M_i}$ for all $a_{M_i} \in A_{M_i}$.

  We have that $\dim A_{M_i} = (\dim M_i)^2$ (see 1.17.b in [2]) $\rightsquigarrow \dim A = \sum \dim M_i^2$

Let $G$ be a finite group., and let $\rho : G \to \mathrm{GL}(V)$ be a representation, over an algebraically closed field $\mathbb{F}$, where $\mathrm{char}(\mathbb{F}) \nmid |G|$. We have $\chi_\rho = \mathrm{tr}\rho$, and $|G| = \sum (\dim M_i)^2$.

Let $\rho_i : G \to \mathrm{GL}(M_i)$ be the representation corresponding to one of the representative irreducible modules $M_i$ taken from the isomorphism class $\mathcal{M}(\mathbb{F}[G])$[1]

Then we see that $\chi_\rho(1) = \dim \rho$ and $\chi_i = \chi_{\rho_i}$ so that
$$|G| = \sum_{i=1}^{s} \chi_i(1)^2.$$

### 8.0.1 Class functions

**Definition 8.0.1.** A class function on $G$ is a function $f : G \to \mathbb{F}$ constant on conjugacy classes of $G$, i.e. $f(gxg^{-1}) = f(x)$ for all $x, g \in G$.

We denote $\mathbf{Class}(G, \mathbb{F}) :=$ vector space of class functions, where we have $\dim \mathbf{Class}(G, \mathbb{F}) = \#$ conjugacy classes.

Furthermore, let $\mathrm{Irr}(G)$ denote the set of irreducible characters.

**Theorem 8.0.2.**

*a)* $\mathrm{Irr}(G)$ *is a basis of* $\mathbf{Class}(G, \mathbb{F})$.

[1] I believe that we are talking about irreducible $\mathbb{F}[G]$-modules here.

*b)* $f \in \mathbf{Class}(G, \mathbb{F})$ *is a character* $\Leftrightarrow f = \sum\limits_{\chi \in \mathrm{Irr}(G)} a_\chi \chi$ *where* $a_\chi \in \mathbb{Z}_{\geq 0}$ *and* $f \neq 0$*.*

**Theorem 8.0.3.** *Let* $W, V$ *be representations of* $G$*. Then* $\chi_V = \chi_W \Leftrightarrow V \cong W$ *as* $G$*-representations.*

Assume $A = \mathbb{F}[G]$). Then the center of the group ring/group algebra $\mathbb{F}[G]$, which we denote $Z(\mathbb{F}[G])$, has two natural bases.

1. $(e_i)_1^s$ (recall 8.1).

2. $(K)_{i=1}^s$ (recall equation 6.1).

We remind ourselves that $K_i = \sum\limits_{g \in \mathscr{K}_i} g$ where $(\mathscr{K}_i)_{i=1}^s$ are the conjugacy classes of $G$.

- One has $\mathbf{Class}(G, \mathbb{F}) = Z(\mathbb{F}[G])$ where $f_\alpha(g) = a_i \longleftarrow\!\!\!\mid \alpha = \sum a_i K_i$, if $g \in \mathscr{K}_i$.

- Furthermore, we have $\mathbf{Funct}(G, \mathbb{F}) = \mathbb{F}[G]$ with $f_\beta(g) = a_g \longleftarrow\!\!\!\mid \beta = \sum a_g g$.

**Lemma 8.0.4.** *Let* $\mathbb{F} = \mathbb{C}$*, and assume we have a finite group* $G$*, so that*

$$\mathbb{C}[G] = \bigoplus_{i=1}^{k} M_i(\mathbb{C}[G]) \qquad (M_i \in \mathcal{M}(\mathbb{C}[G])).$$

*We get a set of associated characters* $\{\chi_1, \ldots, \chi_k\}$*. Then if* $i \neq j$*, we have* $\chi_i \neq \chi_j$*.*

*Proof.* Let $\rho_i : G \to \mathrm{GL}(M_i)$ be irreducible representations of $G$ over $\mathbb{C}$.

We extend $\rho_i$ to $\rho_i' : \mathbb{C}[G] \to \mathrm{GL}(M_i)$ by linearity. We have $1 = e_1 + \ldots + e_s$, where $e_i$ is the identity of $M_i(\mathbb{C}[G])$. Furthermore, we see that $\rho_i'(e_j) = 0$ if $i \neq j$ since $A_{M_i}$ annihilates $A_{M_j} \ni e_j$. It follows that $\rho_i'(1) = \rho_i'(e_i) = I$.

To see that $\rho_i'(e_j) = 0$, note that

$$\begin{aligned} \rho_i'(e_i e_j) &= \rho_i'(0) \\ &= 0 \\ &= \rho_i'(e_j) \cdot \rho_i'(e_i) \\ &= \rho_i'(e_j) \cdot I. \end{aligned}$$

It follows that

$$\rho_i'(e_j) = 0.$$

Note that the extension is no longer only a group-homomorphism, but a ring-homomorphism $\rho_i' : \mathbb{C}[G] \to \mathrm{End}(M_i)$, defined explicitly by

$$\rho_i'\left(\sum a_g g\right) := \sum a_g \rho_i(g).$$

It follows that $\chi_i'$ as functions on $\mathbb{C}[G]$ are distinct for distinct extended representations $\rho_i'$.

We want to show that it follows that the unextended $\chi_i$ are distinct for distinct $i$.

Since

$$\begin{aligned} \langle G \rangle &:= \left\{ \sum a_g g \mid a_g \in \mathbb{C} \right\} \\ &= \mathbb{C}[G] \end{aligned}$$

we see that if

$$\begin{aligned}\chi_i'|_G &= \chi_i \\ &= \chi_j \\ &= \chi_j'|_G\end{aligned}$$

then since $G$ is a basis for $\mathbb{C}[G]$, we would have $\chi_i' = \chi_j'$, contradicting our earlier results, hence we find that if $i \neq j$, then $\chi_i \neq \chi_j$. $\square$

Fact: $\chi_i$ irreducible $\implies \chi_i(1) \mid |G|$.

$$\mathbb{Z} \longrightarrow \mathbb{F}$$

$$1 \longmapsto 1$$

**Proposition 8.0.5.** Irr$(G)$ *is a basis of* **Class**$(G, \mathbb{F})$.

We already know that $|\operatorname{Irr}(G)| = \dim \mathbf{Class}(G, \mathbb{F})$, so it is enough to show that $\operatorname{Irr}(G)$ is linearly independent.

Assume that $\sum_{i=1}^{s} a_i \chi_i = 0$, then evaluation at $e_j$ for all $j \in \{1, \ldots, s\}$ gives us $a_j \chi_j(e_j) = a_j \underbrace{\operatorname{tr}(I)}_{\neq 0} = 0 \implies a_1 = \ldots = a_s = 0$. Linear independence follows.

**Theorem 8.0.6.** *Assume that* $f \in \mathbf{Class}(G, \mathbb{F})$. *Then we have that* $f$ *is a character and*

$$f = \sum_{\chi \in \operatorname{Irr}(G)} a_\chi \chi$$

$$\Leftrightarrow f \neq 0 \text{ and } a_\chi \in \mathbb{Z}_{\geq 0}.$$

*Proof.* $\Longleftarrow$

Assume $f = 0$ and $a_\chi \in \mathbb{Z}_{\geq 0}$. Let $\operatorname{Irr}(G) = \{\chi_1, \ldots, \chi_s\}$.

Then since we already know that $\operatorname{Irr}(G)$ is a basis of $\mathbf{Class}(G, \mathbb{F})$, we know that we can write

$$f = \sum a_i \chi_i.$$

Since $f$ corresponds precisely to the character of a representation

$$M_1^{\oplus a_1} \oplus \ldots \oplus M_s^{\oplus a_s}$$

and since $\operatorname{Irr}(G)$ is a basis $\implies$ exists unique expression for every class function, and in particular every character $\implies f$ is a character. $\square$

**Theorem 8.0.7.** *Given representations* $r_1, r_2$, *one has* $\chi_{r_1 + r_2} = \chi_{r_1} + \chi_{r_2}$.

*Proof.*

$$\mathrm{tr}(A \oplus B) = \mathrm{tr}\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \mathrm{tr}A + \mathrm{tr}B.$$

□

We now want to prove the other direction of theorem 8.0.6.

*Proof.* $\implies$ direction:

Assume that

$$f = \sum_{i=1}^{s} a_i \chi_i$$

is a character. Then $\exists$ representation $(V, \rho)$ s.t. $f = \chi_\rho$.

By Maschke's theorem we have $V = M_1^{\oplus b_1} \oplus \ldots \oplus M_s^{\oplus b_s}$ where $M_i$ are irreducible $\mathbb{F}[G]$-modules $\rightsquigarrow$

$$\begin{aligned} f &= \chi_V \\ &= b_1\chi_1 + \ldots + b_s\chi_s \\ &= \chi_\rho. \end{aligned}$$

It follows that $b_i \in \mathbb{Z}_{\geq 0}$ and not all can be zero, since

$$\begin{aligned} f(1) &= \chi_\rho(1) \\ &= \dim \rho \\ &\neq 0. \end{aligned}$$

Since $\mathrm{Irr}(G)$ is a basis $\implies$ $b_i = a_i$, for all $i$. □

**Theorem 8.0.8.** $\chi_V = \chi_W \Leftrightarrow V \cong W$

*Proof.* $\impliedby$ :

We recall that if $(V, \rho_1), (W, \rho_2)$ are representations such that $V \cong W$, then there

If $V \cong W$ then $\chi_V = \chi_W$ since $\mathrm{tr}(gxg^{-1}) = \mathrm{tr}(x)$ .

$\implies$ : If $\chi_V = \chi_W$ then $V = M_1^{\oplus a_1} \oplus \ldots \oplus M_s^{\oplus a_s}$ and $W = M_1^{\oplus b_1} \oplus \ldots \oplus M_s^{\oplus b_s}$ $\rightsquigarrow$

$$\begin{aligned} \chi_V &= \sum a_i\chi_i \\ &= \sum b_i\chi_i \\ &= \chi_W \end{aligned}$$

$$\Leftrightarrow$$

$$\begin{aligned} \chi_V - \chi_W &= \sum (a_i - b_i)\chi_i \\ &= 0 \end{aligned}$$

which implies that $a_i = b_i$ (linear independence of $\mathrm{Irr}(G)$ as basis). It follows that $V \cong W$. □

**Example 8.0.9.** Let $\rho_1, \rho_2 : \mathbb{Z} \rightrightarrows \mathrm{GL}(2, \mathbb{F})$, explicitly defined by

$$1 \xmapsto{\rho_1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$1 \xmapsto{\rho_2} \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}.$$

where $\rho_1, \rho_2$ are *semisimple* representations of $\mathbb{Z}$.

We have

$$\begin{aligned} \chi_1(1) &= \chi_2(1) \\ &= 2 \end{aligned}$$

and since

$$2 \xmapsto{\rho_1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$2 \xmapsto{\rho_2} \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix}$$

we find that $\chi_1(2) = 2$ and

$$\begin{aligned} \chi_2(2) &= 9 + 1 \\ &= 10. \end{aligned}$$

**Example 8.0.10.** Let $\rho_1, \rho_2 : \mathbb{Z} \rightrightarrows \mathrm{GL}(V)$, explicitly defined by

$$1 \xmapsto{\rho_1} A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

and

$$1 \xmapsto{\rho_2} B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

where $a \neq b$. We find that $\mathrm{tr} A = 2$ and that

$$A^n = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na \\ 0 & 1 \end{pmatrix}$$

so that $\chi_{\rho_1} \equiv 2$.

**Example 8.0.11.** Let

$$A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2. \end{pmatrix}$$

We note that

$$\mathrm{tr} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \lambda_1 + \lambda_2$$

and that

$$\begin{aligned} \mathrm{tr} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}^2 &= \mathrm{tr} \begin{pmatrix} \lambda_1^2 & 0 \\ 0 & \lambda_2^2 \end{pmatrix} \\ &= \lambda_1^2 + \lambda_2^2. \end{aligned}$$

If the matrix is *diagonalizable*, it is enough to know the **characteristic polynomial**

$$(x-\lambda_1)(x-\lambda_2) = x^2 - \mathrm{tr}A(x) + \det(A)$$

if $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) \neq 2$.

We note that

$$\begin{aligned}\frac{(\mathrm{tr}(A))^2 - \mathrm{tr}(A^2)}{2} &= \frac{(\lambda_1+\lambda_2)^2 - (\lambda_1^2+\lambda_2^2)}{2} \\ &= \frac{2\lambda_1\lambda_2}{2} \\ &= \lambda_1\lambda_2 \\ &= \det(A).\end{aligned}$$

*Remark* 8.0.12. Compare 8.0.11 with $\Lambda^2\chi(g) = \dfrac{\chi(g)^2 - \chi(g^2)}{2}$.

## 8.1 Regular representations, and its associated characters

Let $A = \mathbb{F}[G] = A_{M_1} \times \ldots A_{M_s}$.

For a group $G$, the regular action is $G$ acting on itself bý left-multiplication.

- For the group-ring $\mathbb{C}[G]$, if we give $\mathbb{C}[G]$ the canonical $\mathbb{C}[G]$-module structure ($\mathbb{C}[G]^\circ$ in [2]), then the regular representation is just this canonical structure of a module on itself, decomposed into irreducible subrepresentations of $\mathbb{C}[G]$, i.e. $A_{M_1} \times \ldots \times A_{M_s}$.
- Let $\chi_{\mathrm{reg}}$ denote the regular representations character, called the **regular character** ($\chi_\rho$ in [2]).
- We then have $\chi_{\mathrm{reg}} = \chi_{A_{M_1}} + \ldots + \chi_{A_{M_s}}$.
- Note that $A_{M_i} = M_i^{\oplus \dim M_i}$.
- $$\begin{aligned}\chi_{A_{M_i}} &= (\dim M_i)\chi_i \\ &= \chi_i(1)\chi_i.\end{aligned}$$
- $$\begin{aligned}\chi_{\mathrm{reg}} &= \sum_{i=1}^{s} \chi_i(1)\chi_i \\ &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi.\end{aligned}$$

## 8.2 Permutation character

Let $G \curvearrowright X$ be a group action $\rightsquigarrow$ there is a permutation-representation

$$G \to S_X \hookrightarrow \mathrm{GL}(\mathbb{F}^X)$$

with base $\{e_x\}_{x\in X}$ for $\mathrm{GL}(\mathbb{F}^X)$.

- $ge_x := e_{gx}$ and then extend by linearity (?)

**Example 8.2.1.** $X = \{1, \ldots, n\}$ with

$$\rho : G \to S_n \hookrightarrow \mathrm{GL}(n, \mathbb{F})$$

and

$$\rho_{\mathrm{reg}} : G \to S_G \hookrightarrow \mathrm{GL}(\mathbb{F}[G])$$

which is the regular representation of $G$, with $G$ acting by left-multiplication.

- We call $\chi_\rho$ the **permutation character**.
- $$\begin{aligned}\chi_\rho(g) &= |\mathrm{Fix}(g)| \\ &= |\{x \in X \mid g \cdot x = x\}|\,.\end{aligned}$$
- $\dim \chi_\rho = |X|$.
- $\chi_\rho = \chi_{\mathrm{reg}}$.

We have that

$$\begin{aligned}\chi_{\mathrm{reg}}(g) &= |\mathrm{Fix}(g)| \\ &= \begin{cases} |G|, & \text{if } g = \mathrm{id} \\ 0, & \text{if } g \neq \mathrm{id} \end{cases}\end{aligned}$$

## 8.3 Class functions

**Definition 8.3.1.** Let

$$(-,-) : \mathbf{Class}(G, \mathbb{F}) \times \mathbf{Class}(G, \mathbb{F}) \to \mathbb{F}$$

be defined by

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

Note that $(-,-)$ is bilinear, which means that

1) $(\chi_1 + \chi_2, \psi) = (\chi_1, \psi) + (\chi_2, \psi) \qquad (\forall \chi_1, \chi_2, \psi \in \mathbf{Class}(G, \mathbb{F}))$.

2) $(\chi, \psi_1 + \psi_2) = (\chi, \psi_1) + (\chi, \psi_2) \qquad (\forall \chi, \psi_1, \psi_2 \in \mathbf{Class}(G, \mathbb{F}))$.

3) $(a\chi, \psi) = (\chi, a\psi) = a(\chi, \psi) \qquad (\forall \chi, \psi \in \mathbf{Class}(G, \mathbb{F}), \forall a \in \mathbb{F})$.

- When $\mathbb{F} = \mathbb{C}$ we also have
$$\langle \chi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)}.$$
- If $G$ is finite and $\psi$ is a character, then $\psi(g^{-1}) = \overline{\psi(g)} \implies (\chi, \psi) = \langle \chi, \psi \rangle$.

**Lemma 8.3.2.** *Let $\chi$ be a character. Then $\chi$ is irreducible* $\Leftrightarrow (\chi, \chi) = 1$.

*Proof.* Let $\chi = \sum a_i \chi_i$ with $\chi_i \in \{\chi_1, \dots, \chi_s\}$ induced from the isomorphism-class $\mathcal{M}(A) = \{M_1, \dots, M_s\}$. We note that

$$(\chi, \chi) = \sum a_i a_j (\chi_i, \chi_j).$$

Then we see that $(\chi_i, \chi_j) = 0$ if $i \neq j$

$$\rightsquigarrow (\chi, \chi) = \sum a_i^2 (\chi_i, \chi_i).$$

By the first orthogonality relation 9.0.1 this is equal to $a_1^2 + \dots + a_s^2$. Since $a_i \in \mathbb{Z}_{\geq 0}$ one finds that if $(\chi, \chi) = 1$ then $\exists ! a_i = 1$ and $a_j = 0$ for all $j \neq i$. Again, by 9.0.1 one finds that if $\chi$ is irreducible then $(\chi, \chi) = 1$.

$\square$

# Chapter 9

# Lecture 9

Today: Orthogonality relations. Recall that $(-,-) : \mathbf{Class}(G,\mathbb{F}) \times \mathbf{Class}(G,\mathbb{F}) \to \mathbb{F}$ is defined by $(\chi,\psi) = \frac{1}{|G|}\sum_{g\in G}\chi(g)\psi(g^{-1})$, where we assumed that $\mathrm{char}(\mathbb{F}) \nmid |G|$.

Let $\mathbb{F} = \mathbb{C}$. Then we also have $\langle -,- \rangle : \mathbf{Class}(G,\mathbb{F}) \times \mathbf{Class}(G,\mathbb{F}) \to \mathbb{F}$ (denoted as $[-,-]$ in [2]), defined explicitly by $\langle \chi,\psi \rangle = \dfrac{1}{|G|}\displaystyle\sum_{g\in G}\chi(g)\overline{\psi(g)}$.

We have seen (8) that if $\mathbb{F} = \mathbb{C}$ then $(-,-) = \langle -,- \rangle$, given that $\psi$ is a character.

<u>Fact</u>: $\mathrm{Irr}(G)$ is a basis for $\mathbf{Class}(G,\mathbb{F})$ when $\mathbb{F}$ is algebraically closed and $\mathrm{char}(\mathbb{F}) \nmid |G|$.

One has that $\psi(g^{-1}) = \overline{\psi(g)}$ when $\psi$ is a character. However, $(\chi,\psi) \neq \langle \chi,\psi \rangle$ more generally.

### 9.0.1 First orthogonality relation

If $\chi_1,\ldots,\chi_n$ are irreducible characters of $G$, then

$$(\chi_i,\chi_j) = \delta_{ij}$$

$$= \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

### 9.0.2 Second orthogonality relation

The second orthogonality statement:

$$\sum_{\chi\in\mathrm{Irr}(G)} \chi(g)\chi(h) = \begin{cases} |\mathbf{C}_G(g)|, & \text{if } g \sim h \\ 0, & \text{if } g \not\sim h \end{cases}$$

where $g \sim h$ means that $g$ and $h$ are *conjugate*, i.e. $\exists g' \in G$ so that $g'gg'^{-1} = h$.

Recall that the centralizer of $g$ in $G$ is

$$\mathbf{C}_G(g) := \{h \in G \mid hg = gh\}.$$

Furthermore, recall that $(e_i)_{i=1}^s$ is a basis for $Z(\mathbb{F}[G])$ and that $(K_i)_{i=1}^n$ is another basis, where $K_i = \sum_{g\in\mathscr{K}_i} g$, where $\mathscr{K}_i$ is a conjugacy-class.

We note that $K_i \in Z(\mathbb{F}[G])$ for all $i \in \{1,\dots,n\}$, since for an arbitrary element $h \in G$, we have that

$$h\left(\sum_{g\in\mathscr{K}_i} g\right)h^{-1} = \sum_{g\in\mathscr{K}_i} hgh^{-1}$$

where we see that if $g, g' \in \mathscr{K}_i$ with $g \neq g'$, then we have that if $hgh^{-1} = hg'h^{-1} \implies g = g'$, a contradiction, but by definition, we have that $hgh^{-1} \in \mathscr{K}_i$, for all $g \in \mathscr{K}_i$. Hence we find that

$$\begin{aligned} hKh^{-1} &= h\left(\sum_{g\in\mathscr{K}_i} g\right)h^{-1} \\ &= K_i. \end{aligned}$$

**Theorem 9.0.1.**

$$\begin{aligned} e_i &= \frac{1}{|G|}\sum_{g\in G}\chi_i(1)\chi_i(g^{-1})g \\ &= \frac{1}{|G|}\sum_{j=1}^{s}\chi_i(1)\chi_i(\mathscr{K}_j^{-1})K_j. \end{aligned}$$

*Proof.* Note that $\mathbb{F}[G] = \mathbb{F}[G]_{M_1} \times \ldots \times \mathbb{F}[G]_{M_s}$ where $M_1,\dots,M_s$ are irreducible representations of $G$ from distinct isomorphism classes, and $\chi_1,\dots,\chi_s$ are their associated characters. Furthermore, we have that $e_i \in \mathbb{F}[G]_{M_i}$ act as the identity in $\mathbb{F}[G]_{M_i}$.

Recall that $\chi_{\text{reg}}(g) = \begin{cases} |G|, & \text{if } g = \text{id} \\ 0, & \text{if } g \neq \text{id} \end{cases}$

We use lemma 2.11 in [2] to see that

$$\chi_{\text{reg}} = \sum_{i=1}^{s}\chi(1)\chi_i \tag{9.1}$$

We also write

$$e_i = \sum_{g\in G} a_g g \tag{9.2}$$

using the fact that $G$ is a basis for $\mathbb{F}[G] \ni e_i$. We want to show that $a_g = \frac{1}{|G|}\chi_i(1)\chi_i(g^{-1})$.

We get

$$\begin{aligned} \chi_{\text{reg}}(e_i g^{-1}) &= \chi_{\text{reg}}\left(\sum_{h\in G} a_h hg^{-1}\right) \\ &= \sum_{h\in G} a_h\chi_{\text{reg}}(hg^{-1}) \\ &= a_g|G|. \end{aligned}$$

The next to last equality follows from how we originally extended $\chi_{\text{reg}}$ from $G$ to $\mathbb{F}[G]$ by linearity.

The last equality follows from the definition of $\chi_{\text{reg}}$, since only when $h = g$ is the associated term in the sum non-zero.

$\rightsquigarrow \chi_{\text{reg}}(e_i g^{-1}) = \sum_{j=1}^{s} \chi_j(1)\chi_j(e_i g^{-1})$ (RHS follows from (9.1)) $\Leftrightarrow a_g|G| = \sum_{j=1}^{s} \chi_j(1)\chi_j(e_i g^{-1})$.

Let $\rho_j : G \to \mathrm{GL}(M_j)$ be the representation associated with the character $\chi_j$. Recall that

$$\rho_j(e_i) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \implies \chi_j(e_i) = \delta_{ij} \underbrace{\chi_j(1)}_{\dim \text{of } \rho_j}$$

.

Since $\rho_j$ is $\mathbb{C}[G]$-algebra homomorphism, we have that

$$\rho_j(e_i g^{-1}) = \rho_j(e_i)\rho_j(g^{-1})$$

$$= \begin{cases} \rho_j(g^{-1}), & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

Then we see that $\chi_j(e_i g^{-1}) = \begin{cases} \chi_j(g^{-1}), & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$

<u>Note</u>: $\chi_j(g^{-1}) := \mathrm{tr}(\rho_j(g^{-1}))$.

It follows that $a_g|G| = \chi_i(1)\chi_i(g^{-1}) \Leftrightarrow a_g = \frac{1}{|G|}\chi_i(1)\chi_i(g^{-1})$.

Hence

$$\begin{aligned} e_i &= \sum_{g \in G} a_g g \\ &= \sum_{g \in G} \frac{\chi_i(1)\chi_i(g^{-1})g}{|G|} \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g. \end{aligned}$$

We see that since a character $\chi_i$ is constant on conjugacy-classes $\mathscr{K}_j$, one has that

$$\begin{aligned} \frac{1}{|G|} \sum_{j=1}^{s} \chi_i(1)\chi_i\left(\mathscr{K}_j^{-1}\right) K_j &= \frac{\chi_i(1)}{|G|} \sum_{j=1}^{s} \chi_i\left(\mathscr{K}_j^{-1}\right) \left( \sum_{g \in \mathscr{K}_j} g \right) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g. \end{aligned}$$

$\square$

*Remark* 9.0.2. Aside from the fact that characters are constant on conjugacy-classes, in the equalities of equations 9.3, 9.4, we have used that $(\mathscr{K}_i)_{i=1}^{s}$ partitions $G$ into disjoint sets. Furthermore, if $\mathscr{K}_j$ is a conjugacy class, and $a, b \in \mathscr{K}_j$, then $\exists g \in G$ so that

$$gag^{-1} = b \Leftrightarrow (gag^{-1})^{-1} = b^{-1} \Leftrightarrow ga^{-1}g^{-1} = b^{-1}$$

so that if $a, b \in \mathscr{K}_j$ then $\mathscr{K}_j^{-1}$ is precisely the set of inverses of the elements in $\mathscr{K}_j$, and they form their own conjugacy-class.

### 9.0.3 Generalized orthogonality relation

**Theorem 9.0.3.** *For all $h \in G$, and for all $\chi_i, \chi_j \in \mathrm{Irr}(G)$, one has that*

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(gh)\chi_j(g^{-1}) = \delta_{ij} \frac{\chi_i(h)}{\chi_i(1)} \tag{9.3}$$

*Proof.* We note that $e_i \in \mathbb{F}[G]_{M_i}$ and that

$$\mathbb{F}[G]_{M_i} \cap \mathbb{F}[G]_{M_j} = (0), \quad (\text{for } i \neq j).$$

Hence, one has that

$$e_i e_j = 0$$

where $e_i \in Z(\mathbb{F}[G])$ is called a **central idempotent/projector**. Furthermore, recall that

$$\begin{aligned} 1 &= e_1 + \ldots + e_s \\ \rightsquigarrow e_i &= e_1 e_i + \ldots + e_s e_i \\ &= e_i^2. \end{aligned}$$

That is, one has

$$e_i e_j = \delta_{ij} e_i.$$

From theorem 9.0.1 we have

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

We see that the coefficient of $h$ in

$$\delta_{ij} e_i = \frac{\delta_{ij}}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g \tag{9.4}$$

is

$$\frac{\delta_{ij}}{|G|} \chi_i(1)\chi_i(h^{-1}).$$

On the other hand, the coefficient of $h$ in

$$e_i e_j = \left( \frac{1}{|G|} \sum_{g_1 \in G} \chi_i(1)\chi_i(g_1^{-1})g_1 \right) \left( \frac{1}{|G|} \sum_{g_2 \in G} \chi_j(1)\chi_j(g_2^{-1})g_2 \right)$$

are pairs $g_1 g_2 = h \Leftrightarrow g_1 = hg_2^{-1} = (g_2 h^{-1})^{-1}$. Let's denote $g_2 = g$. Then we find that the cofficient of $h$ is

$$\frac{1}{|G|^2} \sum_{g \in G} \chi_i(1)\chi_i(((gh^{-1})^{-1})^{-1})\chi_j(1)\chi_j(g^{-1}) = \frac{1}{|G|^2} \sum_{g \in G} \chi_i(1)\chi_i(gh^{-1})\chi_j(1)\chi_j(g^{-1}) \tag{9.5}$$

If we assume that $\mathbb{F} \ni \chi_i(1) \neq 0$, then since $\delta_{ij} e_i = e_i e_j$, and $G$ is a basis for $\mathbf{Class}(G, \mathbb{F})$, we find that

$$\frac{\delta_{ij}}{|G|}\chi_i(1)\chi_i(h^{-1}) = \frac{1}{|G|^2}\sum_{g\in G}\chi_i(1)\chi_i(gh^{-1})\chi_j(1)\chi_j(g^{-1})$$

$$\Leftrightarrow \delta_{ij}\chi_i(h^{-1}) = \frac{1}{|G|}\sum_{g\in G}\chi_i(gh^{-1})\chi_j(1)\chi_j(g^{-1})$$

$$\Leftrightarrow \frac{\delta_{ij}\chi_i(h^{-1})}{\chi_j(1)} = \frac{1}{|G|}\sum_{g\in G}\chi_i(gh^{-1})\chi_j(g^{-1})$$

We replace $h$ with $h^{-1}$

$$\rightsquigarrow \underbrace{\frac{\delta_{ij}\chi_i(h)}{\chi_j(1)}}_{=0 \text{ if } i\neq j} = \frac{1}{|G|}\sum_{g\in G}\chi_i(gh)\chi_j(g^{-1})$$

$$\Leftrightarrow \frac{\delta_{ij}\chi_i(h)}{\chi_i(1)} = \frac{1}{|G|}\sum_{g\in G}\chi_i(gh^{-1})\chi_j(g^{-1})$$

□

**Corollary 9.0.4.** *A character $\chi$ is* irreducible $\Leftrightarrow (\chi, \chi) = 1$*.*

*Proof.* $\Longrightarrow$ follows from the *first orthogonality relation.*

For $\Longleftarrow$: Let $\chi = \sum m_i\chi_i$ where $\chi$ is a character $\Leftrightarrow m_i \in \mathbb{Z}_{\geq 0}$, where *not all* $m_i$ are 0. We see that

$$\begin{aligned}(\chi, \chi) &= \sum_{i,j} m_i m_j (\chi_i, \chi_j)\\ &= \sum m_i^2.\end{aligned}$$

It follows that only one $m_i$ is *non-zero*, from the fact that $(\chi, \chi) = 1$ together with the fact that $m_i \in \mathbb{Z}_{\geq 0}$. From, this, we also see that the only non-zero $m_i$ must be equal to 1. Hence $\chi = 1 \cdot \chi_i$ for some irreducible $\chi_i$. It follows that $\chi$ is irreducible. □

A corollary of this + HW is the following:

**Corollary 9.0.5.** *If $G \curvearrowright X$ is a* doubly transitive group action*, and $\rho$ is its permutation-representation, with character $\chi_\rho$, where $\chi_\rho(g) = \#$ fixed points, then $\chi_\rho - \mathbf{1}$ is an irreducible character.*

*Proof.* We showed in the HW that $\langle \chi_\rho, \chi_\rho \rangle = 2$ and that $\langle \chi_\rho, \mathbf{1} \rangle = 1$. We then see that

$$\begin{aligned}
\langle \chi_\rho - \mathbf{1}, \chi_\rho - \mathbf{1} \rangle &= \langle \chi_\rho, \chi_\rho \rangle - \langle \chi_\rho, \mathbf{1} \rangle - \langle \mathbf{1}, \chi_\rho \rangle + \langle \mathbf{1}, \mathbf{1} \rangle \\
&= 2 - 1 - \overline{1} + \langle \mathbf{1}, \mathbf{1} \rangle \\
&= \langle \mathbf{1}, \mathbf{1} \rangle \\
&= \frac{1}{|G|} \sum_{g \in G} \mathbf{1}(g) \overline{\mathbf{1}(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} 1^2 \\
&= \frac{|G|}{|G|} \\
&= 1.
\end{aligned}$$

Since $\mathbf{1}$ is a character, one has

$$\begin{aligned}
\langle \mathbf{1}, \mathbf{1} \rangle &= (\mathbf{1}, \mathbf{1}) \\
&= 1.
\end{aligned}$$

By 9.0.4, we see that $\chi_\rho - \mathbf{1}$ is irreducible. $\square$

**Example 9.0.6.** $S_n \curvearrowright \{1, \ldots, n\} \rightsquigarrow \chi_{\text{stnd}} :=$ fixed points $-1$ then $\chi_{\text{stnd}}$ is irreducible $\forall n \geq 2$.

Let $r : G \to \mathrm{GL}(V)$ be a representation over an *algebraically closed field* $\mathbb{F}$, where $\mathrm{char}(\mathbb{F}) \nmid |G|$. We want to prove that $r(g)$ is *diagonalizable* for all $g \in G$.

Note that $\langle g \rangle$ is cyclic $\implies$ abelian.

We have $r|_{\langle g \rangle} \cong \psi_1 \oplus \ldots \oplus \psi_{\dim r|_{\langle g \rangle}}$. We know that every irreducible representation of an abelian group is 1-dimensional (2.0.13).

It follows that $\psi_i : \langle g \rangle \to \mathbb{F}^\times$ and that $r(g) \sim \begin{pmatrix} \psi_1(g) & 0 & 0 & \ldots & 0 \\ 0 & \psi_2(g) & 0 & \ldots & 0 \\ 0 & 0 & \psi_3(g) & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \psi_{\dim r|_{\langle g \rangle}} \end{pmatrix}$

**Lemma 9.0.7.** *Let $\mathbb{F} = \mathbb{C}$, and recall that $\chi(g^{-1}) = \overline{\chi(g)}$ for all* characters $\chi$. *Then $|\chi(g)| \leq \chi(1)$.*

*Proof.* Let $r$ be a representation with $\chi_r = \chi$. One has

$$r(g) \sim \begin{pmatrix} \lambda_1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2 & 0 & \ldots & 0 \\ 0 & 0 & \lambda_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_n \end{pmatrix} = D$$

where

$$\begin{aligned}
n &= \dim r \\
&= \chi(1).
\end{aligned}$$

Then

$$\begin{aligned}\chi(g) &= \mathrm{tr}(r(g))\\ &= \mathrm{tr}(BDB^{-1})\\ &= \mathrm{tr}(B(DB^{-1}))\\ &= \mathrm{tr}((DB^{-1})B)\\ &= \mathrm{tr}(D(B^{-1}B))\\ &= \mathrm{tr}(D)\\ &= \lambda_1 + \ldots + \lambda_n.\end{aligned}$$

□

where we have used that the matrix-group $\mathrm{GL}(V) \cong \mathrm{GL}(n, F)$ is associative with respect to multiplication, that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, and that if $r(g)$ is similar to $D$ then there exists an invertible matrix $B$ so that $B^{-1}r(g)B = D$.

Furthermore, note that

$$\begin{aligned}r(g^n) &= r(g)^n\\ &= I_n.\end{aligned}$$

It follows that

$$\begin{aligned}(BDB^{-1})^n &= \underbrace{(BDB^{-1})(BDB^{-1})\cdots(BDB^{-1})}_{n \text{ times}}\\ &= BD^nB^{-1}\\ &= I_n\\ &\Leftrightarrow\\ D^n &= B^{-1}I_nB\\ &= I_n\end{aligned}$$

$\implies \lambda_i^n = 1 \Leftrightarrow \lambda_i^n - 1 = 0$ for all $i \in \{1, \ldots, n\}$. This shows that $\lambda_i$ is an $n$:th root of unity. Assuming $\mathbb{F} = \mathbb{C}$, with absolute value $|z|$. Then we note that

$$\begin{aligned}|\lambda_i^n| &= |\lambda_i|^n\\ &= 1\end{aligned}$$

$\implies |\lambda_i| = 1$; see footnote.[1]

Therefore

$$|\chi(g)| = |\lambda_1 + \ldots + \lambda_n| \leq |\lambda_1| + \ldots + |\lambda_n| = n.$$

*Remark* 9.0.8. Recall that if a representation $V$ is a *direct sum* of irreducible representations $W_1, \ldots, W_n$, so that $V = W_1 \oplus \ldots \oplus W_n$, then semisimple $\Leftrightarrow$ diagonalizable.

[1] We have used that $\overline{z^n} = (\overline{z})^n$. We prove this by induction: For $k = 1$, we see that $\overline{z^1} = \overline{z}^1$. Assume that it holds for $k = n$. We want to show that it holds for $n + 1 \rightsquigarrow \overline{z^{n+1}} = \overline{z^n} \cdot \overline{z^1} = \overline{z}^n \cdot \overline{z} = (\overline{z})^{n+1}$

## 9.1 Hermitian Inner product

**Definition 9.1.1.** Let $\mathbb{F} = \mathbb{C}$. Then we call $\langle -, - \rangle$, defined earlier in the text, the **hermitian inner product**.

The hermitian inner product $\langle -, - \rangle$ possesses the following properties:

a) $\langle \chi_1 + \chi_2, \psi \rangle = \langle \chi_1, \psi \rangle + \langle \chi_2, \psi \rangle$.

b) $\langle \chi, \psi_1 + \psi_2 \rangle = \langle \chi, \psi_1 \rangle + \langle \chi, \psi_2 \rangle$.

c) $\langle c\chi, \psi \rangle = c\langle \chi, \psi \rangle \qquad (\forall c \in \mathbb{C})$.

d)

$$\begin{aligned} \langle \chi, c\psi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{c\psi(g)} \\ &= \frac{\overline{c}}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} \\ &= \overline{c}\langle \chi, \psi \rangle \qquad (\forall c \in \mathbb{C}). \end{aligned}$$

e) $\langle \chi, \chi \rangle > 0$ and $\langle 0, 0 \rangle = 0$.

Let $\chi \in \mathbf{Class}(G, \mathbb{C}) \rightsquigarrow \chi = \sum a_i \chi_i$ where $a_i \in \mathbb{C}$. Then

$$\begin{aligned} \langle \chi, \chi \rangle &= \sum_{g \in G} a_i \overline{a_j} \langle \chi_i, \chi_j \rangle \\ &= \sum_{g \in G} a_i \overline{a}_j \delta_{ij} \\ &= \sum_i a_i \overline{a}_i \\ &= \sum_i |a_i| \geq 0. \end{aligned}$$

f) $\mathrm{Irr}(G)$ forms an *orthonormal* basis for $\mathbf{Class}(G, \mathbb{C})$.

g) Let $\chi = \sum a_i \chi_i$. Then $\langle \chi, \chi_i \rangle = \sum a_j \langle \chi_j, \chi_i \rangle = a_i$. If $\chi$ is a character, then $\langle \chi, \chi_i \rangle$ is the number of times $\chi_i$ appears in $\chi$. $\chi_i$ is irreducible, and $\chi - \langle \chi, \chi_i \rangle \chi_i$ is a character.

# Chapter 10

# Lecture 10

Recall the orthogonality relations. The first orthogonality relation is proved. We want to prove the second. These relations hold for $G$ finite, $\mathbb{F}$ algebraically closed and $\mathrm{char}(\mathbb{F}) \nmid |G|$.

Fact: $\chi(g) \mid |G|, \forall \chi \in \mathrm{Irr}(G)$. *But we have not proved this.*

Question: What information about $G$ is stored in its **character table**? We know that the isomorphism class of $G$ is not stored there, since $D_8$ and $Q_8$ have the same character table, but are not isomorphic.

*Remark* 10.0.1. Note that for

$$Q_8 = \{e, -e, i, -i, j, -j, k, -k\}$$

we have 1 of order 1, $-1$ of order 2, and $i, -i, j, -j, k, -k$ of order 4, while in

$$D_8 = \{e, s, s^2, r, r^2, r^3, sr, sr^2, sr^3\}$$

one has that $s, r^2, sr, sr^3$ all have order 2.

For example, we have that

$$\begin{aligned}(sr)^2 &= (sr)(sr)\\ &= (sr)(r^{-1}s)\\ &= s^2\\ &= e.\end{aligned}$$

To see this, recall a presentation of $D_8$ as

$$D_8 := \langle r, s \mid r^4 = s^2 = e, srs^{-1} = r^{-1}\rangle.$$

Noting that

$$\begin{aligned}
sr^3 &= (sr)(r^2) \\
&= (r^{-1}s)(r^2) \\
&= ((r^{-1}(sr)r) \\
&= ((r^{-1})(r^{-1}sr)) \\
&= ((r^{-2})(sr)) \\
&= ((r^{-2})(r^{-1}s)) \\
&= r^{-3}s.
\end{aligned}$$

One finds that

$$\begin{aligned}
(sr^3)^2 &= (sr^3)(sr^3) \\
&= (sr^3)(r^{-3}s) \\
&= s^2 \\
&= e.
\end{aligned}$$

For any group-isomorphism $f : D_8 \to Q_8$ and element $x \in D_8$ of order $n$, we need $f(x)$ to be of order $n$, since

$$\begin{aligned}
f(e) &= f(x^n) \\
&= f(x)^n \\
&= e.
\end{aligned}$$

Clearly this does not work, since # of elements of order 2 are not equal in the domain and codomain, and we need an isomorphism.

We now prove the *second orthogonality relation.*

**Theorem 10.0.2.** *Let $g, h \in G$. If $g$ and $h$ are* not *in the same conjugacy-class, then*

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = 0.$$

*Otherwise, the sum is equal to $|\mathbf{C}_G(g)|$.*

*Proof.* Let $\mathscr{K}_1, \ldots, \mathscr{K}_s$ be representative elements of the conjugacy-classes of $G$. Let $X$ be the matrix who:s $(i, j)$ entry is $\chi_i(\mathscr{K}_j)$, that is,

$$X = \begin{pmatrix} \chi_1(\mathscr{K}_1) & \ldots & \chi_1(\mathscr{K}_s) \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \chi_s(\mathscr{K}_1) & \ldots & \chi_s(\mathscr{K}_s) \end{pmatrix}$$

where $\{\chi_1, \ldots, \chi_s\} = \mathrm{Irr}(G)$.

Let $D$ be the diagonal matrix with entries $(i,j)$ on the form $\delta_{ij}|\mathscr{K}_i|$. That is,

$$D = \operatorname{diag}(|\mathscr{K}_1|, \dots, |\mathscr{K}_s|) = \begin{pmatrix} |\mathscr{K}_1| & 0 & 0 & \dots & 0 \\ 0 & |\mathscr{K}_2| & 0 & \dots & 0 \\ 0 & 0 & |\mathscr{K}_3| & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & |\mathscr{K}_s| \end{pmatrix}.$$

Let $X'$ be the matrix with entries $(i,j)$ as $\chi_j(\mathscr{K}_i^{-1})$

Note: When $\mathbb{F} = \mathbb{C}$, we can take $X' := {}^t\overline{X}$, i.e. the *hermitian transpose/conjugate transpose* of $X$. To see this, note that $\overline{\chi(g)} = \chi(g^{-1})$, if we assume that $\chi$ is a character (recall: with $\mathbb{F} = \mathbb{C}$).

Claim: $(XDX')_{ij} = \sum_{\nu=1}^{s} \chi_i(\mathscr{K}_\nu)|\mathscr{K}_\nu|\chi_j(\mathscr{K}_\nu^{-1})$.

*Proof.* We have

$$XDX' = \begin{pmatrix} \chi_1(\mathscr{K}_1) & \dots & \chi_1(\mathscr{K}_s) \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \chi_s(\mathscr{K}_1) & \dots & \chi_s(\mathscr{K}_s) \end{pmatrix} \begin{pmatrix} |\mathscr{K}_1| & 0 & 0 & \dots & 0 \\ 0 & |\mathscr{K}_2| & 0 & \dots & 0 \\ 0 & 0 & |\mathscr{K}_3| & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & |\mathscr{K}_s| \end{pmatrix} \begin{pmatrix} \chi_1(\mathscr{K}_1^{-1}) & \dots & \chi_s(\mathscr{K}_1^{-1}) \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \chi_1(\mathscr{K}_s^{-1}) & \dots & \chi_s(\mathscr{K}_s^{-1}) \end{pmatrix}.$$

We see that $(XD)_{ij} = \chi_i(\mathscr{K}_j)|\mathscr{K}_j| \rightsquigarrow (XDX')_{ij} = \sum_{\nu=1}^{s} \chi_i(\mathscr{K}_\nu)|\mathscr{K}_\nu|\chi_j(\mathscr{K}_\nu^{-1})$ □

Recall: The first orthogonality-relation asserts that

$$\delta_{ij} = (\chi_i, \chi_j) = \frac{1}{|G|}\sum_{g\in G} \chi_i(g)\chi_j(g^{-1}) \Leftrightarrow |G|\delta_{ij} = \sum_{g\in G} \chi_i(g)\chi_j(g^{-1}).$$

Recall further that both $\chi_i$ and $\chi_j$ are characters, hence constant on conjugacy classes, and that the conjugacy-classes partition $G$ into disjoint sets

$$\rightsquigarrow |G|\delta_{ij} = \sum_{\nu=1}^{s} |\mathscr{K}_\nu|\chi_i(\mathscr{K}_\nu)\chi_j(\mathscr{K}_\nu^{-1})$$

It follows that

$$\begin{aligned} (XDX')_{ij} &= |G|\delta_{ij} \\ \implies XDX' &= |G|I_s \\ \Leftrightarrow X\left(\frac{DX'}{|G|}\right) &= I_s. \end{aligned}$$

Note: $\mathrm{char}(\mathbb{F}) \nmid |G|$ means that dividing by $|G|$ is well-defined.

We have

$$\begin{aligned}
1 &= \det(I_s) \\
&= \det\left(X\frac{DX'}{|G|}\right) \\
&= \det(X)\det\left(\frac{D'X}{|G|}\right) \\
&\implies \det(X) \neq 0 \\
&\implies X \text{ is invertible.}
\end{aligned}$$

It follows that

$$\begin{aligned}
XDX' &= |G|I_s \\
\Leftrightarrow DX' &= X^{-1}|G|I_s \\
&= |G|I_sX^{-1} \\
\Leftrightarrow DX'X &= |G|I_s
\end{aligned}$$

(using that $\lambda I_s \in Z(M_s(\mathbb{F}))$, for $\lambda \in \mathbb{F}$).

Note that $(X'X)_{ij} = \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_i^{-1})\chi_\nu(\mathscr{K}_j)$.

Hence

$$D(XX') = \begin{pmatrix} |\mathscr{K}_1| & 0 & 0 & \dots & 0 \\ 0 & |\mathscr{K}_2| & 0 & \dots & 0 \\ 0 & 0 & |\mathscr{K}_3| & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & |\mathscr{K}_s| \end{pmatrix} \begin{pmatrix} \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_1^{-1})\chi_1(\mathscr{K}_1) & \dots & \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_1^{-1})\chi_\nu(\mathscr{K}_s) \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_s^{-1})\chi_{\nu=1}^{s}(\mathscr{K}_1) & \dots & \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_s^{-1})\chi_\nu(\mathscr{K}_s) \end{pmatrix}$$

$$= \begin{pmatrix} |\mathscr{K}_1| \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_1^{-1})\chi_1(\mathscr{K}_1) & \dots & |\mathscr{K}_1| \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_1^{-1})\chi_\nu(\mathscr{K}_s) \\ \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots \\ |\mathscr{K}_s| \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_s^{-1})\chi_{\nu=1}^{s}(\mathscr{K}_1) & \dots & |\mathscr{K}_s| \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_s^{-1})\chi_\nu(\mathscr{K}_s) \end{pmatrix}$$

We see that

$$\begin{aligned}
|G|\delta_{ij} &= (DX'X)_{ij} \\
&= |\mathscr{K}_i| \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_i^{-1})\chi_\nu(\mathscr{K}_j).
\end{aligned}$$

Recall the orbit-stabilizer theorem:

**Lemma 10.0.3.** *Let $G$ be a group which acts on a finite set $X$. Let $x \in X$. Let* $\mathrm{Orb}(x) := \{gx \mid g \in G\}$ *be the* orbit *of $x$ with respect to $G \curvearrowright X$. Furthermore, let* $\mathrm{Stab}(x) := \{g \in G \mid gx = x\}$*, and let* $[G : \mathrm{Stab}(x)]$ *denote the index of the stabilizer of $x$ in $G$. Then*

$$\begin{aligned}\mathrm{Orb}(x) &= [G : \mathrm{Stab}(x)] \\ &= \frac{|G|}{|\mathrm{Stab}(x)|}.\end{aligned}$$

If we let $G \curvearrowright G$ by conjugation, then, for $h \in G$, we have that

$$\begin{aligned}\mathrm{Stab}(h) &= \{g \in G \mid g \cdot h = h \Leftrightarrow ghg^{-1} = h \Leftrightarrow gh = hg\} \\ &= \mathbf{C}_G(h)\end{aligned}$$

and that

$$\begin{aligned}\mathrm{Orb}(h) &= \{g \cdot h := ghg^{-1} \mid g \in G\} \\ &= \mathrm{Cl}(h)\end{aligned}$$

where $\mathrm{Cl}(h)$ is the conjugacy-class of $h$.

Specializing lemma 10.0.3 to this context gives us that

$$|\mathrm{Cl}(h)| = \frac{|G|}{|\mathbf{C}_G(h)|}$$

Or, as before, letting $\mathscr{K}_i$ be a representative element of a conjugacy-class, we find that

$$\begin{gathered}|\mathscr{K}_i| = \frac{|G|}{|\mathbf{C}_G(\mathscr{K}_i)|} \\ \Leftrightarrow \\ |\mathbf{C}_G(\mathscr{K}_i)| = \frac{|G|}{|\mathscr{K}_i|}.\end{gathered}$$

$$\begin{gathered}\rightsquigarrow |G|\delta_{ij} = |\mathscr{K}_i| \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_i^{-1})\chi_\nu(\mathscr{K}_j) \\ \Leftrightarrow \\ \frac{|G|\delta_{ij}}{|\mathscr{K}_i|} = \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_i^{-1})\chi_\nu(\mathscr{K}_j) \\ \Leftrightarrow \\ |\mathbf{C}_G(\mathscr{K}_i)|\delta_{ij} = \sum_{\nu=1}^{s} \chi_\nu(\mathscr{K}_i^{-1})\chi_\nu(\mathscr{K}_j).\end{gathered}$$

Again, we recall that we took $\mathscr{K}_i$ to be a representative element from a conjugacy class.

Let

$$\begin{aligned}[x, y]_{\mathrm{Irr}(G)} &:= \sum_{\chi \in \mathrm{Irr}(g)} \chi(x)\chi(y^{-1}) \qquad (\forall x, y \in G) \\ \rightsquigarrow [x, y]_{\mathrm{Irr}(G)} &= \begin{cases} |\mathbf{C}_G(h)|, & \text{if } x \sim y \\ 0, & \text{if } x \not\sim y \end{cases}\end{aligned}$$

where $\sim$ is the equivalence relation of being in the same conjugacy-class, i.e. $x \sim y \Leftrightarrow x$ and $y$ are *conjugate.* □

We have that

$$[-,-] : \mathbb{F}[G] \times \mathbb{F}[G] \to \mathbb{F}$$

is a biadditive form (hermitian when $\mathbb{F} = \mathbb{C}$).

Recall: Form when $V \times V \to \mathbb{F}$ for a vector space $V$ over $\mathbb{F}$. Also note that $\mathbb{F}[G]$ is a vector space over $\mathbb{F}$.

**Theorem 10.0.4.** $[-,-]$ *restricts to a positive-definite form on* $Z(\mathbb{C}[G])$*, i.e.*

$$[-,-] : Z(\mathbb{C}[G]) \times Z(\mathbb{C}[G]) \to \mathbb{C}$$

*is positive-definite;*

$$[x,x] > 0$$

*if* $x \neq 0, x \in Z(\mathbb{C}[G])$ *and*

$$[0,0] = 0.$$

*Proof.* Let $\chi = \sum a_i K_i$ (recall lemma 6.0.8), where $K_i = \sum_{g \in \mathscr{K}_i} g$ for conjugacy class $\mathscr{K}_i$. □

$\vdots$

**Proposition 10.0.5.** *For all* $x, y \in G$*, we have that* $x \sim y \Leftrightarrow \chi(x) = \chi(y), \forall \chi \in \mathrm{Irr}(G)$.

*Proof.* We will construct two proofs.

Proof 1: For $\implies$: We know that if $x \sim y$,then since class-functions (and in particular, characters) are constant over conjugacy-classes, we see that $\chi(x) = \chi(y)$ for all $\chi \in \mathrm{Irr}(G)$ (even true for $\mathbf{Class}(G, \mathbb{F})$).

For $\impliedby$: Assume that $\chi(x) = \chi(y)$ for all $\chi \in \mathrm{Irr}(G)$. For $\mathbb{F} = \mathbb{C}$, we have that (from Gorensteins book)

$$\begin{aligned}
[x,y]_{\mathrm{Irr}(G)} &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(x)\chi(y^{-1}) \\
&= \sum_{\chi \in \mathrm{Irr}(G)} \chi(x)\overline{\chi(y)} \\
&= \sum_{\chi \in \mathrm{Irr}(G)} |\chi(x)|^2.
\end{aligned}$$

Recall that the trivial representation $\mathbf{1}_G(g) = 1 \in \mathrm{GL}(1, \mathbb{C}) \cong \mathbb{C}^\times$ has an associated irreducible character (since every 1-dimensional representation is irreducible), and that the trace of this representation is 1, for every element $x \in G$. It follows that

$$[x,y]_{\chi \in \mathrm{Irr}(G)} = \sum_{\chi \in \mathrm{Irr}(G)} |\chi(x)|^2 \geq |\chi_{\mathbf{1}}(x)| = 1 > 0.$$

By the contrapositive of the second orthogonality relation, we see that if $[x,y]_{\mathrm{Irr}(G)} \neq 0 \implies x \sim y$, hence $x$ and $y$ are conjugate.

Proof 2: Assume that $\mathrm{char}(\mathbb{F}) \nmid \chi(1)$, for all $\chi \in \mathrm{Irr}(G)$. Recall that both $(e_i)_{i=1}^s$ (where $e_i \in A_{M_i}$ acts as the identity, "locally") and $(K_i)_{i=1}^s$ are bases for $Z(\mathbb{F}[G])$.

We can then write $K_i$ in the basis $(e_i)_{i=1}^s$, that is, $K_i = \sum_{j=1}^s a_{ij} e_j$. This gives us a change-of-basis matrix $A = (a_{ij})$.

Recall: $\chi_i(e_j) = \chi_i(1)\delta_{ij}$.

Assume that e.g. $x \in K_1$ and $y \in K_2$. For $r = 1, 2$, one has

$$\begin{aligned}\chi(K_r) &= \chi\left(\sum_{j=1}^s a_{rj} e_j\right) \\ &= \sum_{j=1}^s a_{ij}\chi_i(e_j) \\ &= \sum_{j=1}^s a_{rj}\chi_i(1)\delta_{ij} \\ &= a_{ri}\chi_i(1).\end{aligned}$$

As we have done before, let $\mathscr{K}_i$ denote a representative element from the "$i^{\text{th}}$" conjugacy-class.

We see that $\chi_i(\mathscr{K}_1) = \chi_i(\mathscr{K}_2) \Leftrightarrow \chi(K_1) = \chi_i(K_2) \Leftrightarrow a_{1i} = a_{2i} \quad (\forall i \in \{1, \ldots, s\}) \Leftrightarrow K_1 = K_2 \Leftrightarrow \mathscr{K}_1 = \mathscr{K}_2 \Leftrightarrow x \sim y$. □

*Remark* 10.0.6. The step $\chi_i(\mathscr{K}_1) = \chi_i(\mathscr{K}_2)$ is non-trivial, and uses the following lemma

**Lemma 10.0.7.** *If $\chi(x) = \chi(y)$ for all $\chi \in \mathrm{Irr}(G) \implies |\mathbf{C}_G(x)| = |\mathbf{C}_G(y)|$*

*Proof.* □

### 10.0.1 Burnside $(p^a q^b)$ theorem

To introduce the next theorem, we need some definitions.

**Definition 10.0.8.** A group $G$ is **solvable** if it has *subnormal series*

$$e = G_0 \lhd G_1 \lhd \ldots \lhd G_k = G$$

such that its *factor groups* $G_j/G_{j-1}$ are all *abelian.* There is no requirement that $G_{j-1}$ is normal in $G$, only that $G_{j-1}$ is normal in $G_j$[1].

**Theorem 10.0.9** (Burnside $p^a q^b$ theorem)**.** *If $|G| = p^a q^b$ for primes $p, q \in \mathbb{Z}_{>0}$, then $G$ is* solvable.

The proof of theorem 10.0.9 uses characters.

**Proposition 10.0.10.** *If $N \lhd G$, then $|\mathbf{C}_{G/N}(gN)| \leq |\mathbf{C}_G(g)| \quad (\forall g \in G)$.*

[1]We use $H \lhd G$ for a group $G$ and a subgroup $H$ to denote that $H$ **is normal in** $G$.

Proposition 10.0.10 is possible to prove without characters, but trickier. One can use ideas of *pullback* of representations

$$\begin{tikzcd} G_1 \arrow[r, "\varphi"] \arrow[drr, bend right, "\varphi^* r := r \circ \varphi"'] & G_2 \arrow[dr, "r"] & \\ & & \mathrm{GL}(V) \end{tikzcd}$$

(in the diagram, we "pullback" $r$ along $\varphi$).

$$\begin{tikzcd} \mathrm{Rep}(G_1) & \mathrm{Rep}(G_2) \arrow[l, "\varphi^*"'] \\ \varphi^*(r) = r\varphi & r \arrow[l, mapsto] \end{tikzcd}$$

*Remark* 10.0.11. $\varphi^*$ is a *functor*, $\mathrm{Rep}(G)$ is a *category.* For $G$ finite, one has that $\mathrm{Rep}(G)$ with $\oplus, \otimes$ is an example of a *Tannakian category.* One then finds that $\mathrm{Rep}(G)$ characterizes $G$ up to isomorphism (see e.g. [4]).

### 10.0.2 2 special cases

- $G_1 \subset G_2$ with $\varphi : G_1 \hookrightarrow G_2$ inclusion $\rightsquigarrow \varphi^* r = \mathrm{Res}^{G_2}_{G_1} r$ the restriction.
- $\varphi : G_1 \to G_2$ surjective. If $r$ is irreducible $\implies \varphi^* r = r \circ \varphi$ irreducible. We have that
$$G \overset{\pi}{\to} G/N$$
is surjective. If $G_1 \overset{\varphi}{\to} G_2$ then $G_1 \cong G_2/\ker\varphi$. Hence an irreducible representation of $G/N$ *pulls back* to an irreducible representation of $G$.
- An irreducible representation $\rho$ of $G$ *factors through* $G/N \Leftrightarrow N \subset \ker\rho$.

$\rho : G_1 \to \mathrm{GL}(V)$ factors through $G_i \Leftrightarrow \ker\varphi \subset \ker\rho$.

**Proposition 10.0.12.** *Let* $\mathbb{F} = \mathbb{C}$. *Then* $|\mathbf{C}_{G/N}(g)| \leq |\mathbf{C}_G(g)|$.

*Proof.* By the second orthogonality relation, we have that
$$[gN, gN] = |\mathbf{C}_{G/N}(g)|$$
and
$$[g, g] = |\mathbf{C}_G(g)|.$$

We also have

$$\begin{aligned}
|\mathbf{C}_{G/N)}(g)| &= [gN, gN] \\
&= \sum_{\chi \in \mathrm{Irr}(G/N)} \chi(gN)\overline{\chi(gN)} \\
&= \sum_{\chi \in \mathrm{Irr}(G/N)} |\chi(gN)|^2 \\
&= \sum_{\chi \in \mathrm{Irr}(G) \mid N \subseteq \ker \chi} |\chi(g)|^2 \\
&\leq \sum_{\chi \in \mathrm{Irr}(G)} |\chi(g)|^2 \\
&= [g, g] \\
&= |\mathbf{C}_G(g)|
\end{aligned}$$

□

*Remark* 10.0.13. In the proof, we applied the second orthogonality relation to the trivial fact that $g$ is conjugate to itself.

# Chapter 11

# Leture 11

**Recall**: Every *irreducible* representation of an abelian group over an *algebraically closed field* $\mathbb{F}$, is 1-dimensional.

**Lemma 11.0.1.** *For $G$ finite over $\mathbb{F}$ algebraically closed of $\mathrm{char} = 0$, we have*

$$|\{\chi \in \mathrm{Irr}(G) \mid \chi(1) = 1\}| = |G/G'|$$

*where $G' = [G, G]$ is the commutator subgroup.*

*Proof.* We have the following (commutative) diagram

$$\begin{tikzcd} G \arrow[rr, "\chi"] \arrow[dr, two heads, "\pi"'] & & \mathbb{F}^{\times} \\ & G/G' \arrow[ur, "\hat{\chi}"'] & \end{tikzcd}$$

so that $\chi = \hat{\chi} \circ \pi$. The image of $\chi$ is *abelian*, and $\chi$ is a homomorphism. Hence we have that for every element in $G'$, all on the form $xyx^{-1}y^{-1}$ are such that

$$\begin{aligned} \chi(xyx^{-1}y^{-1}) &= \chi(x)\chi(x^{-1})\chi(y)\chi(y^{-1}) \\ &= 1. \end{aligned}$$

We know from [2], lemma 2.7 that

$$\begin{aligned} |\,\mathrm{Irr}(G/G')| &= \#\text{ of conjugacy classes of } G/G' \\ &= |G/G'|. \end{aligned}$$

So there can be at most $|G/G'|$ distinct 1-dimensional characters $\chi : G \to \mathbb{F}^{\times}$.

On the other hand, if we are given $\psi : G \to \mathbb{F}^{\times}$, then we have the following diagram

$$\begin{tikzcd}
& G/G' \arrow[dr, dotted, "\exists!\phi"] & \\
G \arrow[ur, two heads, "\pi"] \arrow[rr, "\psi"] \arrow[dr, two heads] & & \mathbb{F}^{\times} \\
& G/\ker\psi \arrow[ur, hook] &
\end{tikzcd}$$

By the first isomorphism theorem, we have that $G/\ker\psi \cong \operatorname{im}\psi$, which is abelian. Furthermore, we have that $G' \subset \ker\psi \rightsquigarrow$ by the **universal property of the quotient**, there is a unique homomorphism $\phi : G/G' \to \mathbb{F}^{\times}$ so that $\psi = \phi \circ \pi$.

This shows that every 1-dimensional representation is on the form $\psi = \phi \circ \pi$, so there are atleast as many distinct 1-dimensional representations as there are homomorphisms $\phi : G/G' \to \mathbb{F}^{\times}$. It follows that $\phi : G/G' \to \mathbb{F}^{\times} \leftrightsquigarrow \psi : G \to \mathbb{F}^{\times}$ are in bijective correspondence. We already know that there are $|G/G'|$ distinct $\phi$, hence there are exactly $|G/G'|$ distinct $\psi$. $\square$

### 11.0.1 Tensor products $\rightsquigarrow$ 2 key operations on representations/characters

- **Tensor products** of representations / products of characters.
- **Induction** of representations/of characters (e.g. Frobenious Groups).

Let $V, W$ be representations of $G$. Then $V \otimes W$ is a representation of $G$, by $G$-action defined as

$$g(v \otimes w) := gv \otimes gw$$

which we then extend linearly.

### 11.0.2 Restriction to subgroup

Let $H \subset G$ be a subgroup. We can then restrict the representation of $G$ to a representation $\operatorname{Res}_H^G \rho : H \to \mathrm{GL}(V)$ of $H$

$$\begin{tikzcd}
G \arrow[r, "\rho"] & \mathrm{GL}(V) \\
H \arrow[u, hook, "i"] \arrow[ur, "\operatorname{Res}_H^G \rho"'] &
\end{tikzcd}$$

### 11.0.3 Induction to group from subgroup

We can also go the other way. Let $H \subset G$ be a subgroup, and let $r : H \to \mathrm{GL}(W)$ be a representation of $H$.

We then get $\operatorname{Ind}_H^G r : G \to \mathrm{GL}(?)$.

Formally, we have

$$\operatorname{Ind}_H^G r := \mathbb{F}[G] \otimes_{\mathbb{F}[H]} W.$$

or

$$\mathrm{Ind}_{\mathbb{F}[H]}^{\mathbb{F}[G]} r := \mathbb{F}[G] \otimes_{\mathbb{F}[H]} W. \tag{11.1}$$

which becomes an $\mathbb{F}[G]$-module. It follows that it has an $\mathbb{F}$-module structure, hence is an $\mathbb{F}$-vector space.

*Remark* 11.0.2. I suppose that in (11.1), one first wants to extend $r : H \to \mathrm{GL}(W)$ to

$$r' : \mathbb{F}[H] \to \mathrm{End}(W).$$

*Comment* 11.0.3. " We discussed that since $\mathbb{F}[H]$ is not a commutative ring, we need some special structure"). This comment seemed to have been regarding (11.1).

**Lemma 11.0.4.** *Let $V, W$ be representations of $G$, $G$ finite and $\mathbb{F}$ algebraically closed of characteristic $0$, then*

1. $\chi_{V\otimes W} = \chi_V \chi_W$ *is a* character.
2. $\chi_{V\otimes W}(g) := \chi_V(g)\chi_W(g)$.

*Proof.* Let $g \curvearrowright V$, $g \curvearrowright W$ be computed in a basis such that actions are diagonal, i.e. we choose a basis $(e_i), (f_j)$ of $V, W$ respectively, so that $G$:s action is diagonal, and $(e_i), (f_j)$ are eigenvectors. Hence we get $ge_i = \lambda_i e_i$ and $gf_i = \mu_j f_j$.

We have that $\{e_i \otimes f_j \ \mid 1 \leq i \leq |V|, 1 \leq j \leq |W|\}$ is a basis for $V \otimes W$.

We get

$$\begin{aligned} g(e_i \otimes f_j) &:= ge_i \otimes gf_j \\ &= \lambda_i e_i \otimes \mu_j f_j \\ &= \lambda_i \mu_j (e_i \otimes f_j). \end{aligned}$$

One has $\chi_V(g) = \sum_{i=1}^{|V|} \lambda_i$ and $\chi_W(g) = \sum_{j=1}^{|W|} \mu_j$

$$\begin{aligned} \rightsquigarrow \chi_{V\otimes W}(g) &= \sum_{i,j} \lambda_i \mu_j \\ &= \left(\sum_i \lambda_i\right)\left(\sum_j \mu_j\right) \\ &= \chi_V(g)\chi_W(g). \end{aligned}$$

$\square$

More generally, let $V$ be a representation of $G_1$ and $W$ be a representation of $G_2$. Then

$$V \otimes W$$

is a representation of $G_1 \times G_2$.

If $G_1 = G_2$ then $V \otimes W$ is a representation of $G \times G$. We can make a restriction to $G$ and get a representation $\mathrm{Res}_G^{G\times G} V \otimes W$

$$\begin{aligned} G &\xhookrightarrow{\quad\Delta\quad} G \times G \\ g &\longmapsto (g,g) \end{aligned}$$

<u>Facts</u>:

- $\chi_V \chi_W$ is **not** irreducible as representations of $G$ if $\dim V, \dim W > 1$.
- $\chi_V \chi_W = \chi_{V\otimes W}$ is a representation of $G_1 \times G_2$.

If $\chi_V, \chi_W$ are irreducible then $\chi_V \otimes \chi_W$ is an irreducible character of $G_1 \times G_2$.

**Lemma 11.0.5.** *Assume that* $\mathbb{F} = \mathbb{C}$. *Then we have*

$$\mathrm{Irr}(G_1 \times G_2) = \{\chi_1\chi_2 \mid \chi_1 \in \mathrm{Irr}(G_1), \chi_2 \in \mathrm{Irr}(G_2)\}.$$

*Proof.*

$$\begin{aligned} [\chi_1\chi_2, \chi_1\chi_2] &= \frac{1}{|G_1 \times G_2|} \sum_{(g_1,g_2)\in G_1\times G_2} \chi_1(g)\chi_2(g)\overline{\chi_1(g)\chi_2(g)} \\ &= \left(\frac{1}{|G_1} \sum_{g_1\in G_1} \chi_1(g_1)\overline{\chi_1(g_1)}\right)\left(\frac{1}{|G_2|} \sum_{g_2\in G_2} \chi_2(g_2)\overline{\chi_2(g)_2)}\right) \\ &= [\chi_1,\chi_1]_{G_1}[\chi_2,\chi_2]_{G_2}. \end{aligned}$$

Since $\chi_1\chi_2 = \chi_{V_1\otimes V_2}$, we know that (I believe) $\chi_1\chi_2$ is a character. Recall that if $\chi_i$ is a character, then irreducible $\Leftrightarrow [\chi_i, \chi_i] = 1$. Since $\chi_1 \in \mathrm{Irr}(G_1)$ and $\chi_2 \in \mathrm{Irr}(G_2)$, one has

$$[\chi_1,\chi_1]_{G_1}[\chi_2,\chi_2]_{G_2} = 1$$

so that $\chi_1\chi_2$ is irreducible. This shows that

$$\{\chi_1, \chi_2 \mid \chi_1 \in \mathrm{Irr}(G_1), \chi_2 \in \mathrm{Irr}(G_2)\} \subseteq \mathrm{Irr}(G_1 \times G_2).$$

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

Let $\mathrm{Irr}(G_1) = \{\chi_1, \ldots, \chi_r\}$ and $\mathrm{Irr}(G_2) = \{\psi_1, \ldots, \psi_s\}$. It follows that

$$\sum_{i=1}^r \chi_i(1)^2 = |G_1|$$

and

$$\sum_{j=1}^s \psi_j(1)^2 = |G_2|$$

so that

$$\begin{aligned} \sum_{i,j} \chi_i(1)^2\psi_j(1)^2 &= \left(\sum_{i=1}^r \chi_i(1)^2\right)\left(\sum_{j=1}^s \psi_j(1)^2\right) \\ &= |G_1| \cdot |G_2| \\ &= |G_1 \times G_2|. \end{aligned}$$

By considering the size of $\mathrm{Irr}(G_1 \times G_2)$ and $\{\chi_1\chi_2 \mid \chi_1 \in \mathrm{Irr}(G_1), \chi_2 \in \mathrm{Irr}(G_2)\}$ we see that there can not be any other element in $\mathrm{Irr}(G_1 \times G_2)$, since we would then have

$$\sum_{\chi \in \mathrm{Irr}(G_1 \times G_2)} \chi(1)^2 = \sum_{\chi \neq \chi_1\chi_2} \chi(1)^2 + \sum_{i,j} \chi_i(1)^2\psi_j(1)^2 > \sum_{i,j} \chi_i(1)^2\psi_j(1)^2 = |G_1 \times G_2|.$$

But this would contradict earlier results! Hence we have

$\mathrm{Irr}(G_1 \times G_2) \subseteq \{\chi_1\chi_2 \mid \chi_1 \in \mathrm{Irr}(G_1), \chi_2 \in \mathrm{Irr}(G_2)\} \implies \mathrm{Irr}(G_1 \times G_2) = \{\chi_1\chi_2 \mid \chi_1 \in \mathrm{Irr}(G_1), \chi_2 \in \mathrm{Irr}(G_2)\}.$

□

### 11.0.4 Symmetric and exterior powers

**Definition 11.0.6.** Let $V^{\otimes n} := \underbrace{V \otimes \cdots \otimes V}_{n \text{ times}}$.

**Definition 11.0.7.** Let

$$\mathrm{Sym}^n V := V^{\otimes n} / \langle v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)} \mid v_i \in V, \forall \sigma \in S_n \rangle.$$

We call this the $\mathbf{n}^{th}$ **symmetric power** of $V$.

Let $v_1 \cdots v_n$ be the image of $v_1 \otimes \cdots \otimes v_n$ in $\mathrm{Sym}^n V$.

One can see this as follows: Let $\pi : V^{\otimes n} \twoheadrightarrow \mathrm{Sym}^n V$.

Let $\mathfrak{S} = \langle v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)} \mid v_i \in V, \forall \sigma \in S_n \rangle$. Then we see that

$$\pi((v_1 \otimes \cdots v_n) - (v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)})) = 0\mathfrak{S} \Leftrightarrow (v_1 \otimes \cdots \otimes v_n)\mathfrak{S} = (v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)})\mathfrak{S}$$

But $(v_1 \otimes \cdots \otimes v_n)\mathfrak{S} := v_1 \cdots v_n$ and $(v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)})\mathfrak{S} := v_{\sigma(1)} \cdots v_{\sigma(n)}$. The conclusion follows.

If $e_1, \ldots, e_m$ is a basis for $V$, then

$$\{e_{i_1} \otimes \cdots \otimes e_{i_n} \mid 1 \leq i_j \leq m\}$$

is a basis for $V^{\otimes n}$, and

$$\{e_{i_1} \cdots e_{i_n} \mid 1 \leq i_1 \leq \ldots \leq i_n \leq m\}$$

is a basis for $\mathrm{Sym}^n V$.

We have that

$$\begin{aligned} \dim \mathrm{Sym}^n V &= \binom{m+n-1}{n} \\ &= \binom{m+n-1}{m-1}. \end{aligned}$$

*Remark* 11.0.8. See `https://en.wikipedia.org/wiki/Stars_and_bars_(combinatorics)#` for how to think about dimensionality.

**Example 11.0.9.** Let $V$ be 3-dimensional with basis $e_1, e_2, e_3$. Then we have that

$$\begin{aligned}\dim \operatorname{Sym}^2 V^3 &= \binom{2+3-1}{2} \\ &= \binom{4}{2} \\ &= \frac{4!}{2!2!} \\ &= 6.\end{aligned}$$

**Definition 11.0.10.**

$$\chi_{\operatorname{Sym}^2 V} = \sum_{i \le j} \lambda_i \lambda_j$$

Note that $\chi_V(g) = \sum \lambda_i$ and $\chi_V(g)^2 = \left(\sum \lambda_i\right)^2$ and if $g \sim \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ then $g^2 \sim \operatorname{diag}(\lambda_1^2, \ldots, \lambda_n^2)$.

We have

$$\begin{aligned}\frac{\chi_V(g)^2 + \chi_V(g^2)}{2} &= \frac{\left(\sum \lambda_i\right)^2 + \left(\sum \lambda_j^2\right)}{2} \\ &= \sum_{i \le j} \lambda_i \lambda_j \\ &= \chi_{\operatorname{Sym}^2 V}.\end{aligned}$$

**Definition 11.0.11.**

$$\chi_{\operatorname{Sym}^3 V} = \sum_{i \le j \le k} \lambda_i \lambda_j \lambda_k.$$

Using character table of $D_8$, one calculates $\operatorname{Sym}^2 \chi_2$

| $D_8$ | 1 | $r^2$ | $s$ | $r$ | $sr$ |
|---|---|---|---|---|---|
| **1** | 1 | 1 | 1 | 1 | 1 |
| $\psi_r$ | 1 | 1 | 1 | 1 | 1 |
| $\psi_s$ | 1 | 1 | 1 | $-1$ | $-1$ |
| $\psi_{sr}$ | 1 | 1 | $-1$ | $-1$ | 1 |
| $\chi_2$ | 2 | $-2$ | 0 | 0 | 0 |
| $\operatorname{Sym}^2 \chi_2$ | 3 | 3 | 1 | $-1$ | 1 |

We have

$$\begin{aligned}\langle \operatorname{Sym}^2 \chi_2, \operatorname{Sym}^2 \chi_2 \rangle &= \frac{1}{8}\left( (\operatorname{Sym}^2 \chi_2(1))^2 + (\operatorname{Sym}^2 \chi_2(r^2))^2 + 2(\operatorname{Sym}^2 \chi_2(s))^2 + 2(\operatorname{Sym}^2 \chi_2(r))^2 + 2(\operatorname{Sym}^2 \chi_2(sr))^2 \right) \\ &= \frac{3^2 + 3^2 + (2+2+2)}{8} = \frac{24}{8} = 3\end{aligned}$$

and

$$\begin{aligned}\langle \operatorname{Sym}^2 \chi_2, \mathbf{1}\rangle &= \frac{1}{8}\left(\operatorname{Sym}^2 \chi_2(1)\overline{\mathbf{1}(1)} + \operatorname{Sym}^2 \chi_2(r^2)\overline{\mathbf{1}(r^2)} + 2\operatorname{Sym}^2 \chi_2(s)\overline{\mathbf{1}(s)} + 2\operatorname{Sym}^2 \chi_2(r)\overline{\mathbf{1}(r)} + 2\operatorname{Sym}^2 \chi_2(sr)\overline{\mathbf{1}(sr)}\right)\\ &= \frac{3+3+2-2+2}{2}\\ &= \frac{8}{8}\\ &= 1.\end{aligned}$$

One can show that

$$\operatorname{Sym}^2 \chi_2 = 1 + \psi_s + \psi_{sr}$$

because of the pairing of $\operatorname{Sym}^2 \chi_2$ with itself is $3 = 1^2 + 1^2 + 1^2$, and clearly $\chi_2$ can not be one of them (since $\chi_2(1)^2 = 4 > 3$), so that it must be a sum of *three* irreducible characters.

Recall the character table for $Q_8$

| $Q_8$ | $1$ | $-1$ | $i$ | $j$ | $k$ |
|---|---|---|---|---|---|
| $\mathbf{1}$ | 1 | 1 | 1 | 1 | 1 |
| $\psi_j$ | 1 | 1 | $-1$ | 1 | $-1$ |
| $\psi_i$ | 1 | 1 | 1 | $-1$ | $-1$ |
| $\psi_k$ | 1 | 1 | $-1$ | $-1$ | 1 |
| $\chi_2^{Q_8}$ | 2 | $-2$ | 0 | 0 | 0 |
| $\operatorname{Sym}^2 \chi_2^{Q_8}$ | 3 | 3 | $-1$ | $-1$ | $-1$ |

Where we have added the row $\operatorname{Sym}^2 \chi_2^{Q_8}$, and used that

$$\begin{aligned}\chi_2^{Q_8}(i^2) &= \chi_2^{Q_8}(j^2)\\ &= \chi_2^{Q_8}(k^2)\\ &= \chi_2^{Q_8}(-1)\\ &= -2\end{aligned}$$

to get the last three columns in the row $\operatorname{Sym}^2 \chi_2^{Q_8}$.

We find that

$$\begin{aligned}\langle \operatorname{Sym}^2 \chi_2^{Q_8}, \mathbf{1}\rangle &= \frac{3+3+(-2-2-2)}{8}\\ &= 0.\end{aligned}$$

This shows that we can use $\operatorname{Sym}^2 \chi_2$ and $\operatorname{Sym}^2 \chi_2^{Q_8}$ to *distinguish* between $D_8$ and $Q_8$.

# Chapter 12

# Lecture 12

### 12.0.1 More on tensor products

Fore more on tensors; see chapter 10.4 in [1].

Let $H \subset G$ be a subgroup.

Recall

$$\operatorname{Ind}_H^G M = \mathbb{F}[G] \otimes_{\mathbb{F}[H]} M.$$

If $M$ is a representation of $H \Leftrightarrow$ M is a representation of $\mathbb{F}[H]$ (extend by linearity) $\Leftrightarrow M$ left $\mathbb{F}[H]$-module.

- ring $R$ with $1 \Leftrightarrow \mathbb{F}[H]$.
- $N$ right $R$-module $\Leftrightarrow \mathbb{F}[G]$.
- $M$ left $R$-module $\Leftrightarrow M$.

$N \otimes_R M$ abelian group and $(nr, m) = (n, rm)$.

If in addition, $N$ is a left $S$-module for some ring $S \supset R$ and

$$(sn)r = s(nr) \qquad (\forall s \in S, n \in N, r \in R)$$

then

$$s \cdot (n \otimes m) = sn \otimes m$$

makes $N \otimes_R M$ into a left $S$-module (Again, for $R = \mathbb{F}[H]$, $S = \mathbb{F}[G] = N$, $M$ representation of $\mathbb{F}[H]/\mathbb{F}[H]$-module).

- Ring theory background, see chapter 1 of [2].
- Basics of character theory: see chapter 2 of [2].

$$\sum_{\chi \in \operatorname{Irr}(G)} \chi(1)^2 = |G| \qquad\qquad \operatorname{Irr}(G) = \#\text{of conjugacy classes}$$

$\downarrow$ Induced characters — $\downarrow$ Product of characters + Symmetric and exterior powers, tensor operations

Induced characters $\to$ Brauers theorem

Induced characters $\to$ Frobenius groups (chapter 7 of Isaac)

(12.1)

### 12.0.2 Chapter 5 of [2], induced characters.

Let $\chi$ be a character of $H$.

$$\operatorname{Ind}_H^G \chi = \chi_{\operatorname{Ind}_H^G M}$$

given that $M$ is a representation of $G$ affording us with the character $\chi$, i.e. $\chi_M = \chi$.

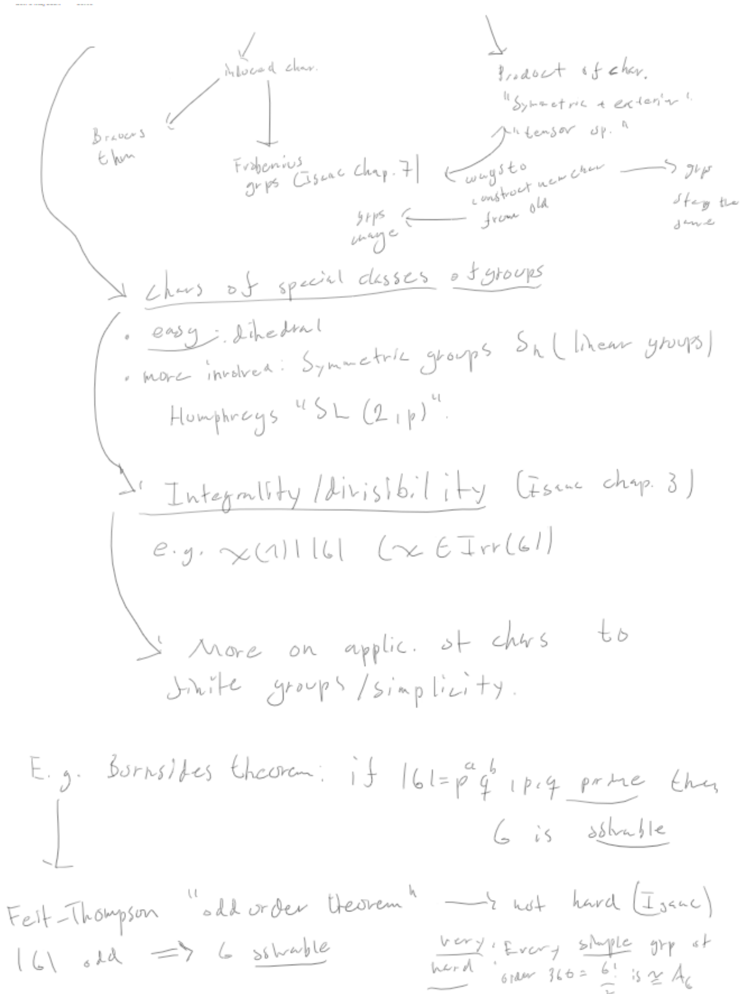


Figure 12.1: Continuation of 12.1

**Definition 12.0.1.** A character $\chi$ of $G$ is **monomial** if $\exists H \leq G$ ($H$ subgroup) and $\psi$ character of $H$ of degree 1 ($\psi \in X^*(H)$) so that

$$\chi = \operatorname{Ind}_H^G \psi.$$

**Definition 12.0.2.** If all the characters of complex representations of $G$ are monomial, then we say that $G$ is an "**Monomial group/$M$-group**."

*Remark* 12.0.3. Clarification here: For $\chi \in \operatorname{Irr}(G)$ in 12.0.2 the $H$ in 12.0.1 can be distinct for distinct $\chi$. The important thing is that for all irreducible (complex-valued) $\chi$ for $G$, there exists some $H$ and $\psi \in X^*(H)$ so that induction to $G$ of $\psi$ gives $\chi$.

**Theorem 12.0.4** (Artin)**.** *If $G$ is nilpotent then $G$ is an $M$-group.*

*Remark* 12.0.5. $G$ is finite and nilpotent $\Leftrightarrow$ $G$ is a direct product of its sylow $p$-subgroups. In particular, $p$-groups are $M$-groups.

Note that $\mathrm{SL}(2, \mathbb{F}_3)$ is solvable, and *not* an $M$-group.

**Theorem 12.0.6** (Brauers theorem)**.** *For all finite groups $G$, every $\chi \in \operatorname{Irr}(G)$ is a $\mathbb{Z}$-linear combination of monomial characters.*

**Definition 12.0.7.** A **directed poset** $(I, \leq)$ is a set $I$ with a partial order $\leq$ on $I$, such that for all pairs $x, y \in I$ there exists a $z$ in $I$, so that $x \leq z$ and $y \leq z$.

**Definition 12.0.8.** Let $(I, \leq)$ be a directed poset and let $(A_i)_{i \in I}$ be a family of groups, and suppose we have group homomorphisms $f_{ij} : A_j \to A_i$ whenever $i \leq j$, with the following properties:

- $f_{ii} = \mathrm{id}_{A_i}$.
- $f_{ij} \circ f_{jk} = f_{ik}$ for all $i \leq j \leq k$.

Then we call the pair $((A_i)_{i \in I}, (f_{ij})_{i \leq j \in (I, \leq)})$ an **inverse system** of groups and morphisms over $I$, and the $f_{ij}$ are called the *transition* morphisms of the system.

**Definition 12.0.9.** The **inverse limit** of a system

$$((A_i)_{i \in I}, (f_{ij})_{i \leq j \in (I, \leq)})$$

as in 12.0.8, is a particular subgroup $A$, defined as

$$A = \varprojlim_{i \in I} A_i := \left\{ a \in \prod_{i \in I} A_i \;\middle|\; a_i = f_{ij}(a_j), \forall i \leq j \in (I, \leq) \right\}.$$

<u>Links to number theory:</u>

For every irreducible polynomial $f \in \mathbb{Q}[x]$ there exists a group $\operatorname{Gal}(f)$ that is a subgroup of $S_n$, where $n = \deg f$. There is a way to put all $\operatorname{Gal}(f)$ together in a big group

$$\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim \operatorname{Gal}(f)$$

where the RHS is the **inverse limit** (12.0.9).

**Definition 12.0.10.** $\rho$ in (12.2) is called the **Artin representation**

$$\begin{tikzcd} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{GL}(n,\mathbb{C}) \\ & \mathrm{Gal}(f) \arrow[ur] \arrow[ul, bend left] & \end{tikzcd} \tag{12.2}$$

**Definition 12.0.11.** Artins $\mathcal{L}(\rho, s)$ generalizes the riemann zeta function $\zeta$, so that

$$\zeta(s) = \mathcal{L}(\mathbf{1}, s).$$

Artins conjecture: $\mathcal{L}(\rho, s)$ admits an *analytic continuation* to all of $\mathbb{C}$, if $\rho$ is irreducible, $\rho \neq \mathbf{1}$ and satisfies a functional equation.

If $\rho$ is monomial, then Artins conjecture holds.

Brauers theorem implies that $\mathcal{L}(\rho, s)$ satisfies functional equation, with $\mathcal{L}(\rho_1, s_1)$, $\mathcal{L}(\rho_2, s_2)$ *entire* (i.e. holomorphic on all of $\mathbb{C}$), then

$$\mathcal{L}(\rho, s) = \frac{\mathcal{L}(\rho_1, s_1)}{\mathcal{L}(\rho_2, s_2)}.$$

### 12.0.3 Exterior powers

Recall that

$$V^{\otimes n} = \underbrace{V \otimes \cdots \otimes V}_{n \text{ times}}.$$

We have

$$f : V^{\otimes n} \twoheadrightarrow \mathrm{Sym}^n V := V^{\otimes n}/\mathfrak{S}$$

where

$$\mathfrak{S} = \langle v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)} \mid v_i \in V, \forall \sigma \in S_n \rangle.$$

**Definition 12.0.12.** We define the $\mathbf{n}^{\text{th}}$ **exterior power** $\Lambda^n V$ of a vector space $V$ as

$$\Lambda^n V = V^{\otimes n}/\langle v_1 \otimes \cdots \otimes v_n \mid v_i = v_j \text{ for } i \neq j \rangle.$$

Let

$$g : V^{\otimes n} \twoheadrightarrow \Lambda^n V.$$

Then the image of $v_1 \otimes \cdots \otimes v_n$ under $g$ is denoted as $v_1 \wedge \cdots \wedge v_n$

We have

$$v_1 \wedge v_2 \wedge v_3 = -v_1 \wedge v_3 \wedge v_2 = v_3 \wedge v_1 \wedge v_2.$$

The general rule, which holds for any vector space of $\dim V = n \in \mathbb{Z}_{>0}$ is that $v_{\sigma(1)} \wedge \ldots \wedge v_{\sigma(n)} = \mathrm{sgn}(\sigma) v_1 \wedge \ldots \wedge v_n$. If $M$ is an $R$-module over the commutative ring $R$, then for each $n$-bilinear alternating map

$$f : M^n \to N$$

there is a *unique* $R$-module homomorphism $\bar{f} : \Lambda^n(M) \to N$ so that

$$f = \bar{f} \circ \iota$$

where $\iota : M^n \twoheadrightarrow \Lambda^n(M)$ is the canonical projection defined by $i(m_1, \ldots, m_n) := m_1 \wedge \cdots \wedge m_n$.

We have that

$$\dim \Lambda^n V = \binom{d}{n}$$

where $\dim V = d$. If $e_1, \ldots, e_d$ is a basis for $V$, then $\{e_i \wedge e_j \mid 1 \leq i < j \leq d\}$ is a basis for $\Lambda^2 V$ of dimension $\binom{d}{2}$.

Similarly, we have $\{e_i \wedge e_j \wedge e_k \mid 1 \leq i < j < k \leq d\}$ as a basis for $\Lambda^3 V$ of dimension $\binom{d}{3}$.

$\vdots$

$\{e_1 \wedge \cdots e_d\}$ basis for $\Lambda^d V$ of dimension $\binom{d}{d} = 1$, and so that we have $\Lambda^n V = 0$ for $n > d$.

### 12.0.4 Linear maps and tensor operations

Let $T : V \to W$ be a linear maps between vector spaces $V, W$. We get a map $T \otimes T : V \otimes V \to W \otimes W$ defined by sending $v_1 \otimes v_2$ to $T(v_1) \otimes T(v_2)$.

Similary, given $T$, we get

- $T^{\otimes n} : V^{\otimes n} \to W^{\otimes n}$.
- $\operatorname{Sym}^n T : \operatorname{Sym}^n V \to \operatorname{Sym}^n W$.
- $\Lambda^n T : \Lambda^n V \to \Lambda^n W$.
- $\det T : \Lambda^d V \to \Lambda^d W$, if $\dim V = \dim W = d$.
- $T : V \to V \rightsquigarrow \Lambda^d T : \Lambda^d V \to \Lambda^d V$. We have $\Lambda^d(T)(\alpha) = c\alpha$ for some scalar $c = \det T$. *Basis independent* definition of determinant of $T$.

**Example 12.0.13.** $\dim(\operatorname{Sym}^n \mathbb{F}^2) = n + 1$, $\dim(\operatorname{Sym}^2 \mathbb{F}^n) = \binom{n+1}{2}$

Again, note that $\operatorname{Sym}^n V$ and $\Lambda^n V$ are *quotients*. We also have symmetric and exterior tensors which gives subspaces.

We have an action

$$S_n \curvearrowright V^{\otimes n}$$

given explicitly by

$$\sigma(v_1 \otimes \cdots \otimes v_n) := v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)}.$$

**Definition 12.0.14.** $\alpha \in V^{\otimes n}$ is **symmetric** if $\sigma(\alpha) = \alpha$ for all $\sigma \in S_n$, so that

$$\alpha \in (V^{\otimes n})^{S_n}$$

where
$$(V^{\otimes n})^{S_n} := \{v \in V^{\otimes n} \mid \sigma v = v, \forall \sigma \in S_n\}$$
i.e. the fixed points of the group action $S_n \times V^{\otimes n} \to V^{\otimes n}$.

**Definition 12.0.15.** $\alpha \in V^{\otimes n}$ is **alternating** if $\sigma\alpha = \operatorname{sgn}(\sigma)\alpha$ for all $\sigma \in S_n$ (under $S_n \curvearrowright V^{\otimes n}$).

If $\operatorname{char}\mathbb{F} \nmid n!$ then $f : V^{\otimes n} \to \Lambda^n V$ have sections
$$v_1 \wedge \cdots \wedge v_n \overset{s}{\longmapsto} \frac{1}{n!} \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}.$$

In the case of $f' : V^{\otimes n} \to \operatorname{Sym}^n V$ and $\operatorname{char}\mathbb{F} \nmid n!$ then we have sections
$$v_1 \cdots v_n \overset{s'}{\longmapsto} \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}.$$

In $\operatorname{char}\mathbb{F} = 0$ we have $\operatorname{Sym}^n V \cong$ symmetric $n$-tensors and $\Lambda^n V \cong$ alternating tensors.

Recall that
$$\chi_{\operatorname{Sym}^2}(g) = \frac{\chi_V(g)^2 + \chi_V(g^2)}{2}.$$
Let $\dim V = d$ so that $\lambda_1, \ldots, \lambda_n$ are the eigenvalues associated with $g \sim \operatorname{diag}(\lambda_1, \ldots, \lambda_d)$. We have
$$(\lambda_1 \ldots \lambda_n)^2 = \sum \lambda_i^2 + 2\sum_{i<j} \lambda_i \lambda_j$$

Again, recall that if $g \sim \operatorname{diag}(\lambda_1, \ldots, \lambda_d)$ then $g \sim \operatorname{diag}(\lambda_1^2, \ldots, \lambda_d^2) \rightsquigarrow \chi_V(g^2) = \lambda_1^2 + \ldots + \lambda_d^2$.

We define
$$\begin{aligned}
\chi_{\Lambda^2 V}(g) &:= \frac{\chi_V(g)^2 - \chi_V(g^2)}{2} \\
&= \frac{(\sum \lambda_i)^2 - (\sum \lambda_i^2)}{2} \\
&= \frac{2\sum\limits_{i<j} \lambda_i \lambda_j}{2} \\
&= \sum_{i<j} \lambda_i \lambda_j.
\end{aligned}$$

*Remark* 12.0.16. $\chi_{\operatorname{Sym}^3/\Lambda^3 V}(g)$ uses $\chi_V(g^3)$.

Dihedral group

$$\begin{tikzcd}
1 & r^2 \arrow[l, bend right] & r \arrow[l, bend right] & s \arrow[lll, bend right] & sr \arrow[llll, bend right]
\end{tikzcd} \tag{12.3}$$

12.3 shows where the square of the elements goes (even the conjugacy class, of which we have choosen representatives; everyone besides $sr^3$ is trivial, quick calculation using group-presentation for $D_8$ shows that it holds).

If $\operatorname{char}\mathbb{F} \neq 2$ then $\operatorname{Sym}^2 V, \Lambda^2 V \hookrightarrow V^{\otimes 2}$.

$$\begin{aligned}\binom{d+1}{2} + \binom{d}{2} &= \frac{(d+1)!}{2!(d-1)!} + \frac{d!}{2!(d-2)!}\\ &= \frac{(d+1)(d)}{2} + \frac{(d)(d-1)}{2}\\ &= \frac{d}{2}\left(d+1+(d-1)\right)\\ &= \frac{d}{2}(2d)\\ &= d^2.\end{aligned}$$

This is precisely the dimension of $V^{\otimes 2}$ given that $\dim V = d$.

One has

$$V^{\otimes 2} = \operatorname{Sym}^2 V \oplus \Lambda^2 V$$

If $\operatorname{char}\mathbb{F} \neq 3! = 6$ then $V^{\otimes 3} = \operatorname{Sym}^3 V \oplus \Lambda^3 V \oplus S_{2,1} V$ where $S_{2,1}V$ is an extra part needed (compare dimensions, i.e. $\dim \operatorname{Sym}^3 V + \dim \Lambda^3 V = \frac{d^3}{3} - \frac{d^2}{2} + \frac{d}{6}$ but $V^{\otimes 3}$ has dimension $d^3$).

In general, assume $\operatorname{char}\mathbb{F} = 0$. For all partitions $\lambda$ of $n$, there exists **Schur functor** $S_\lambda$ such that

$$V^{\otimes n} = \bigoplus_{\substack{\text{partitions } \lambda \\ \text{of } n}} S_\lambda V$$

<u>$n = 2$</u>:

$$\begin{aligned}2 &= 2 \qquad (\operatorname{Sym}^2)\\ 2 &= 1+1 \qquad (\Lambda^2)\end{aligned}$$

<u>$n = 3$</u>:

$$\begin{aligned}3 &= 1+1+1 \qquad (\Lambda^3)\\ 3 &= 2+1 \qquad (S_{2,1})\\ 3 &= 3 \qquad (\operatorname{Sym}^3)\end{aligned}$$

$\vdots$

<u>For arbitrary $n$</u>:

$$\begin{aligned}n &= n \qquad (\operatorname{Sym}^n)\\ n &= \underbrace{1+1+\ldots+1}_{n \text{ times}} \qquad (\Lambda^n).\end{aligned}$$

Partitions of $d$ also parametrizes irreducible representations/characters of symmetric group $S_d$.

# Chapter 13

# Lecture 13

### 13.0.1 Induced representation

Let $G$ be a group with subgroup $H \leq G$.

- If $(\rho, V)$ is a representation of $G$ then $\operatorname{Res}_H^G \rho$ is a representation of $H$, defined by
$$\operatorname{Res}_H^G \rho(h) := \rho(h).$$
- If $(\lambda, W)$ is a representation of $H$, we want to define $\operatorname{Ind}_H^G \lambda$ as a representation of $G$.

**Definition 13.0.1** (definition 1)**.** The representation $(\lambda, W)$ of $H$ corresponds to a $\mathbb{F}[H]$-module $W$, such that
$$\operatorname{Ind}_H^G W = \mathbb{F}[G] \otimes_{\mathbb{F}[H]} W.$$

**Definition 13.0.2** (definition 2)**.** Let
$$G/H = \{g_i H \mid g_i \in G\}$$
and define
$$V = \bigoplus_{g_i H \in G/H} W_{g_i}.$$
If $g \in G$ then $gg_i = g_{f(i)} h_i$. Let $v \in V$, then
$$v = \sum_{i=1}^{k} v_i \qquad (v_i \in W_{g_i}).$$

$$(\operatorname{Ind}_H^G \lambda)(g)(v) = \sum_{i=1}^{k} \lambda(h_i) v_{f(i)}.$$

**Lemma 13.0.3.** $\dim(\operatorname{Ind}_H^G \lambda) = [G : H] \dim \lambda$.

**Definition 13.0.4** (definition 3)**.** Let $f : H \to \mathbb{F}$ be a class function.

$$\begin{aligned}\operatorname{Ind}_H^G f(x) &= \frac{1}{|H|}\sum_{g\in G} f^0(gxg^{-1}) \\ &= \sum_{g_iH\in G/H} f^0(gxg^{-1})\end{aligned}$$

where

$$f^0(g) = \begin{cases} f(g), \text{ if } g \in H \\ 0, \text{ if } g \notin H \end{cases}.$$

If $\chi \in \operatorname{Irr}(H)$ then $\operatorname{Ind}_H^G \chi$ is a character of $G$. We prove 13.0.3

*Proof.*

$$\begin{aligned}\operatorname{Ind}_H^G(\chi)(1) &= \frac{1}{|H|}\sum_{g\in G}\chi^0(g1g^{-1}) \\ &= \frac{1}{|H|}\sum_{g\in G}\chi(1) \\ &= \frac{1}{|H|}\cdot(|G|\chi(1)) \\ &= \frac{|G|}{|H|}\cdot\chi(1) \\ &= [G:H]\chi(1)\end{aligned}$$

$\square$

**Theorem 13.0.5** (Frobenius reciprocity)**.** *Let* $\chi : G \to \mathbb{F}$ *and* $\lambda : H \to \mathbb{F}$ *be* class functions*; then*

$$[\operatorname{Res}_H^G \chi, \lambda]_H = [\chi, \operatorname{Ind}_H^G \lambda]_G.$$

*Proof.*

$$\begin{aligned}
[\chi, \operatorname{Ind}_H^G \lambda]_G &= \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\operatorname{Ind}_H^G \lambda(g)} \\
&= \frac{1}{|G|}\sum_{g\in G} \chi(g)\operatorname{Ind}_H^G \lambda(g^{-1}) \\
&= \left(\frac{1}{|G|}\sum_{g\in G} \chi(g)\right)\left(\frac{1}{|H|}\sum_{h\in G} \lambda^0(hg^{-1}h^{-1})\right) \\
&= \frac{1}{|G||H|}\left(\sum_{g\in G}\sum_{h\in G} \chi(g)\lambda^0(\underbrace{hg^{-1}h^{-1}}_{=y})\right) \\
&= \frac{1}{|G||H|}\left(\sum_{h\in G}\sum_{y\in G} \chi(h^{-1}y^{-1}h)\lambda^0(y)\right) \\
&= \frac{1}{|G||H|}\left(\sum_{h\in G}\sum_{y\in G} \chi(y^{-1})\lambda^0(y)\right) \\
&= \frac{1}{|G||H|}|G|\left(\sum_{y\in G} \chi(y^{-1})\lambda^0(y)\right) \\
&= \frac{1}{|H|}\left(\sum_{y\in H} \chi(y^{-1})\lambda(y)\right) \\
&= [\operatorname{Res}_H^G \chi, \lambda]_H
\end{aligned}$$

□

*Remark* 13.0.6. In the last step, we used that $[-,-]$ is *symmetric* on (not neccessarily irreducible) characters (see corollary 2.17 in [2]).

**Corollary 13.0.7.** *If $\lambda$ is a character of $H$, then $\operatorname{Ind}_H^G \lambda$ is a character of $G$.*

*Proof.* Let $\operatorname{Irr}(G) = \{\chi_1, \dots, \chi_r\}$.

$$\operatorname{Ind}_H^G \lambda = \sum a_i\chi_i \qquad (a_i \in \mathbb{F}).$$

Another formulation of 13.0.5 gives

$$[\operatorname{Ind}_H^G \chi, \lambda]_G = [\lambda, \operatorname{Res}_H^G \chi]_H.$$

Applying this gives us that (together with ortogonality relations)

$$a_i = [\operatorname{Ind}_H^G \lambda, \chi_i] = [\lambda, \operatorname{Res}_H^G \chi_i]. \tag{13.1}$$

By the introduction of this lecture, we assumed that $\operatorname{Res}_H^G \chi_i$ was a character. By corollary 2.17 in [2], we know that 13.1 is a non-negative integer. By 13.0.3 we have that $\operatorname{Ind}_H^G \lambda \neq 0$ so that $\exists a_i \neq 0$. It follows that $\operatorname{Ind}_H^G \lambda$ is indeed a character. □

$$[\chi, \lambda] = \frac{1}{|G|} \sum_{g \in G} \chi(g)\lambda(g^{-1}) \qquad \text{(symmetric on characters)}$$

$$\langle \chi, \lambda \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\lambda(g)} \qquad \text{(hermitian and equal to } [-,-] \text{ on } \mathbb{C}).$$

**Definition 13.0.8.** Let $G$ be a group. A non-identity proper subgroup $H \subsetneqq G$ is called a **frobenius complement** if

$$H \cap gHg^{-1} = \{1_G\}$$

for all $g \in G \setminus H$. We call $G$ a **frobenius group** if such a subgroup $H$ exists.

**Theorem 13.0.9.** *Let $G$ be a group and let $H \subset G$ be a frobenius-complement. Then there exists a normal subgroup $N$ in $G$ such that*

$$H \cap N = \{1_G\}.$$

*and*

$$HN = G \qquad (\textit{Semidirect product}).$$

**Lemma 13.0.10.** *Let*

$$N = \left( G \setminus \bigcup_{x \in G} xHx^{-1} \cup \{1_G\} \right).$$

*Then*

$$|N| = [G : H]$$

*and if $M \trianglelefteq G$ and $M \cap H = \{1_G\}$ then $M \subseteq N$.*

*Proof.* The number of conjugates of $H$ in $G$ is

$$[G : N_G(H)] \qquad \text{(Orbit-stabilizer theorem)}$$

where we used the orbit-stabilizer theorem applied to the action

$$G \times \mathcal{P}(G) \to \mathcal{P}(G)$$

with $H \in \mathcal{P}(G)$, and $\mathcal{P}(G)$ the *power set* of $G$.

We have the obvious inclusion $H \subseteq N_G(H)$. Recall that

$$H \cap gHg^{-1} = \{1_G\} \qquad (\forall g \in G \setminus H). \tag{13.2}$$

Assume that $g \in N_G(H)$ so that $gHg^{-1} = H$. Then by (13.2) we see that $g \in H$ so that $N_G(H) \subseteq H$, hence $H = N_G(H)$, so that

$$[G : N_G(H)] = \frac{|G|}{|N_G(H)|} = \frac{|G|}{|H|} = [G : H].$$

From this we see that

$$\begin{aligned} \Big| \bigcup_{x \in G} xHx^{-1} \Big| &= 1 + [G : N_G(H)](|H| - 1) \\ &= 1 + [G : H](|H| - 1) \\ &= 1 + \frac{|G|}{|H|}(|H| - 1). \end{aligned}$$

Here we count the identity element once, and then we have $[G : N_G(H)]$ distinct orbits with $|H|-1$ *non-identity* elements in each. We claim that if $g \in xHx^{-1}$ then $g \notin yHy^{-1}$ for $g \neq 1$ and $xHx^{-1} \neq yHy^{-1}$

*Proof.* Assume that $g \in xHx^{-1} \cap yHy^{-1}$ and $g \neq 1$. Then $\exists h, h' \in H$ such that

$$g = xhx^{-1}$$
$$g = yh'y^{-1}$$

so that

$$xhx^{-1} = yh'y^{-1} \Leftrightarrow y^{-1}xhx^{-1}y = h'.$$

By assumption ($g \neq 1$) we have that $h' \neq 1_G$, so that

$$1_G \neq h' \in H \cap (y^{-1}x)H(y^{-1}x)^{-1}$$

which by the *frobenius property* of $H$ shows us that $y^{-1}x \in H$.

But then we have that $(y^{-1}x)H(y^{-1}x)^{-1} = (y^{-1}x)H(x^{-1}y) = H \Leftrightarrow xHx^{-1} = yHy^{-1}$ (contradiction!). □

It follows that

$$\begin{aligned} |N| &= |G| - \left(1 + \frac{|G|}{|H|}(|H|-1)\right) + 1 \\ &= \frac{|G|}{|H|} \\ &= [G : H]. \end{aligned}$$

**Lemma 13.0.11.** *Let $M$ be as in 13.0.10, and $H$ a frobenius complement of $G$. Then for $x \in G$, we have*

$$xMx^{-1} \cap xHx^{-1} = M \cap xHx^{-1} = \{1_G\}$$

*Proof.* The first equality follows from the normality of $M$.

Assume that there there exists some *non-identity* element $m \in M \cap xHx^{-1}$. Then it follows that $xhx^{-1} = m$, but then we have that $x^{-1}mx = h$. But $M \cap H = \{1_G\}$ and $M$ is normal, so that $x^{-1}mx = h \in M$. If $h = 1_G$ then $x1_Gx^{-1} = 1_G = m$, contradicting the assumption that $m$ is a *non-identity* element. □

Let $M$ be as in the lemma. If $x \in G$ then

$$xMx^{-1} \cap xHx^{-1} = M \cap xHx^{-1} = \{1_G\}.$$

Since $x$ was arbitrary (and obviously $M \subseteq G$), we see that $M \subseteq G \setminus \bigcup_{x \in G} xHx^{-1} \cup \{1_G\} = N$. □

**Lemma 13.0.12.** *Let $\theta$ be a* class function *of $H$, where $H$ is a frobenius complement of a group $G$, such that $\theta(1) = 0$. Then*

$$\operatorname{Res}^G_H \operatorname{Ind}^G_H \theta = \theta.$$

*Proof.* Let $h \in H, h \neq 1$. Recall 13.0.4 and 13.0.8.

We know that

$$gHg^{-1} = \begin{cases} H, \text{if } g \in H \\ \{1_G\}, \text{if } g \notin H \end{cases}$$

We have

$$\begin{aligned} \operatorname{Ind}_H^G \theta(h) &= \frac{1}{|H|} \sum_{g \in G} \theta^0(ghg^{-1}) \\ &= \frac{1}{|H|} \sum_{g \in H} \theta(ghg^{-1}) \\ &= \frac{1}{|H|} \sum_{h \in H} \theta(h) \\ &= \frac{1}{|H|} |H| \theta(h) \\ &= \theta(h). \end{aligned}$$

*Remark* 13.0.13. To avoid confusion, note that $\theta$ is a **class function**, so constant on conjugacy classes. This explains the third equality above.

For $h = 1_G$ we have

$$\begin{aligned} \operatorname{Ind}_H^G \theta(1) &= \frac{1}{|H|} \sum_{g \in G} \theta^0(g 1_G g^{-1}) \\ &= \frac{1}{|H|} \sum_{g \in G} \theta^0(1_G) \\ &= [G : H] \theta(1_G) \\ &= 0 \end{aligned}$$

where we used that $1_G \in H$ so that $\theta^0(1_G) = \theta(1_G) = 0$ for all $g \in G$.

Finally, pay attention to the fact that $\operatorname{Res}_H^G(\operatorname{Ind}_H^G \theta)(h) := \operatorname{Ind}_H^G \theta(h)$, which explains why we did not say much about the $\operatorname{Res}_H^G$-part. □

**Theorem 13.0.14.** *Let $G$ be a group and let $H$ be a frobenius complement (frobenius pair $(G, H)$). Let $\chi \in \operatorname{Irr}(H)$ be a non-trivial irreducible character. Then*

$$\chi^* := \operatorname{Ind}_H^G \chi + \chi(1)(\mathbf{1}_G - \operatorname{Ind}_H^G \mathbf{1}_H)$$

*is an irredicible character of $G$, extending $\chi$.*

*Proof.* Let $\theta = \chi - \chi(1)\,\mathbf{1}_H$ and $\theta(1) = 0$

$$\rightsquigarrow \left[\operatorname{Ind}_H^G \theta, \operatorname{Ind}_H^G \theta\right]_G = \left[\theta, \operatorname{Res}_H^G \operatorname{Ind}_H^G \theta\right]_H = [\theta, \theta]_H$$

where we have used 13.0.12 and 13.0.5. Continuing, we expand, using 8.3.1 and corollary 2.17 of [2] (specifically that $[-,-]$ is symmetric on characters), together with orthogonality relations, and we get

$$\begin{aligned}
[\theta,\theta]_H &= [\chi - \chi(1)\,\mathbf{1}_H, \chi - \chi(1)\,\mathbf{1}_H]_H \\
&= [\chi,\chi]_H - 2\chi(1)\,[\mathbf{1}_H,\mathbf{1}_H]_H + [\mathbf{1}_H,\mathbf{1}_H]_H \\
&= [\chi,\chi]_H - 2\chi(1)\,[\chi,\mathbf{1}_H]_H + \chi(1)^2\,[\mathbf{1}_H,\mathbf{1}_H]_H \\
&= 1 - 0 + \chi(1)^2 \\
&= 1 + \chi(1)^2.
\end{aligned}$$

Furthermore, one has

$$\begin{aligned}
\left[\operatorname{Ind}_H^G \theta, \mathbf{1}_G\right]_G &= \left[\theta, \operatorname{Res}_H^G \mathbf{1}_G\right]_H \\
&= [\theta, \mathbf{1}_H]_H \\
&= [\chi - \chi(1)\,\mathbf{1}_H, \mathbf{1}_H]_H \\
&= [\chi, \mathbf{1}_H]_H - [\chi(1)\,\mathbf{1}_H, \mathbf{1}_H]_H \\
&= -\chi(1)
\end{aligned}$$

**Lemma 13.0.15.** $\operatorname{Ind}_H^G(-)$ *is $\mathbb{F}$-linear.*

*Proof.* Let $\varphi_1, \varphi_2$ be characters, and let $f \in \mathbb{F}$. Set $\psi = f\varphi_1 + \varphi_2$. Then

$$\operatorname{Ind}_H^G \psi(s) = \frac{1}{|H|} \sum_{g \in G} (f\varphi_1 + \varphi_2)^0 (gsg^{-1})$$

where

$$(f\varphi_1 + \varphi_2)^0(gsg^{-1}) := \begin{cases} (f\varphi_1 + \varphi_2)(s), \text{if } gsg^{-1} \in H \\ 0, \text{if } gsg^{-1} \notin H \end{cases}$$

$$\begin{aligned}
\rightsquigarrow \operatorname{Ind}_H^G \psi(s) &= \frac{1}{|H|} \left( \sum_{gsg^{-1} \in H} f\varphi_1(gsg^{-1}) + \varphi_2(gsg^{-1}) \right) \\
&= \frac{f}{|H|} \sum_{gsg^{-1} \in H} \varphi_1(gsg^{-1}) + \frac{1}{|H|} \sum_{gsg^{-1} \in H} \varphi_2(gsg^{-1}) \\
&= f \operatorname{Ind}_H^G \varphi_1 + \operatorname{Ind}_H^G \varphi_2.
\end{aligned}$$

□

From the statement of the theorem, we have

$$\chi^* = \operatorname{Ind}_H^G \chi - \chi(1) \operatorname{Ind}_H^G \mathbf{1}_H + \chi(1)\,\mathbf{1}_G$$

Using 13.0.15, we can rearrange this as

$$\begin{aligned}
\chi^* &= \operatorname{Ind}_H^G (\chi - \chi(1)\,\mathbf{1}_H) + \chi(1)\,\mathbf{1}_G \\
&= \operatorname{Ind}_H^G \theta + \chi(1)\,\mathbf{1}_G
\end{aligned}$$

Putting together our earlier computations, we find that

$$\begin{aligned}
[\chi^*, \chi^*]_G &= \left[\operatorname{Ind}_H^G \theta + \chi(1)\, \mathbf{1}_G, \operatorname{Ind}_H^G \theta + \chi(1)\, \mathbf{1}_G\right]_G \\
&= \left[\operatorname{Ind}_H^G \theta, \operatorname{Ind}_H^G \theta\right]_G + 2\chi(1)\left[\operatorname{Ind}_H^G \theta, \mathbf{1}_G\right]_G + \chi(1)^2\,[\mathbf{1}_G, \mathbf{1}_G]_G \\
&= (1 + \chi(1)^2) - 2\chi(1)^2 + \chi(1)^2 \\
&= 1.
\end{aligned}$$

Let $\operatorname{Irr}(G) = \{\chi_1, \ldots, \chi_r\}$. Since $\chi^*$ is a class-function (it is a sum of class functions on $G$), we have that

$$\chi^* = a_1\chi_1 + \ldots + a_r\chi_r$$

so that

$$[\chi^*, \chi^*] = a_1^2 + \ldots + a_r^2 = 1 \implies \exists! a_i \neq 0$$

while if $j \neq i$ then $a_j = 0$.

Hence

$$\chi^* = a_i\chi_i.$$

we have $\chi^*(1_G) = \chi(1_G) + \operatorname{Ind}_H^G \theta(1_G) = \chi(1_G) + \theta(1_G) = \chi(1_G) > 0$ and $\chi^*(1_G) = \chi(1_G) = a_i\chi_i(1)$ where $\chi_i(1) > 0$ so that $a_i > 0$. Hence $\chi^*$ is irreducible. □

Hence $\chi^*$ extends $\chi$ to $G$. Let

$$\operatorname{Irr}(H) = \{\chi_1, \ldots, \chi_r\}$$

and define

$$M = \bigcap_{i=1}^{r} \ker \chi_i$$

$M$ is normal since it is the intersection of normals.

If $x \in M \cap H$ then $\chi_i^*(x) = \chi_i(x) = 1$ so that $x \in \bigcap_{i=1}^{r} \chi_i = \{1\}$.

In particular, $M \cap H = \{1\} \implies M \subseteq N$ by lemma .

Let $g \in N$ so that $g$ is no conjugate of $H$.

Then

$$\begin{aligned}
\chi_i^*(g) - \chi_i(1)\, \mathbf{1}_G(g) &= \operatorname{Ind}_H^G \theta_i(g) \\
&= \frac{1}{|H|} \sum_{h \in G} \theta_i^0(hgh^{-1}) \\
&= 0.
\end{aligned}$$

Hence

$$\begin{aligned}\chi_i^*(g) &= \chi_i(1)\,\mathbf{1}_G(g)\\ &= \chi_i(1)\end{aligned}$$

Therefore $g \in M$, so that $N \subseteq M$ which implies that $M = N$.

So $N \cap H = M \cap H = \{1\}$.

We have

$$\begin{aligned}|NH| &= \frac{|N||H|}{|N \cap H|}\\ &= |N||H|\\ &= [G : H]|H|\\ &= \frac{|G|}{|H|}|H|\\ &= |G|.\end{aligned}$$

We conclude that $N \cap H = \{1\}$ and $NH = G$.

# Chapter 14

# **Lecture** 14

$$\begin{tikzcd}
\text{Tensor products} \arrow[d] & \text{Induced characters} \arrow[d] & \text{Integrality properties (Isaac, ch. 3)} \\
\text{Brauer-Burnside} & \text{Frobenius groups} &
\end{tikzcd}$$

Recall that $\chi_{\text{reg}} = \sum_{i=1}^{r} \chi_i(1)\chi_i$ for $\chi_i \in \operatorname{Irr}(G)$

$$\begin{aligned} \rightsquigarrow |G| &= \chi_{\text{reg}}(1) \\ &\sum_{i=1}^{r} \chi_i(1)^2. \end{aligned}$$

**Theorem 14.0.1.** *Let $S$ be a commutative ring and let $R \subset S$ be a* subring*, so that $\alpha \in R$. Then the following are equivalent:*

*a) $\exists f(x) \in R[x]$, $f(x)$ monic and non-zero polynomial, so that $f(\alpha) = 0$.*

*b) $R[\alpha]$ is finitely generated as an $R$-module.*

*c) There exists a subring $S_0$ of $S$ such that $R \subset R[\alpha] \subset S_0 \subset S$, and so that $S_0$ is finitely generated as an $R$-module (not needed for the course; see [5]).*

**Definition 14.0.2.** If *a*)-*c*) in 14.0.1 hold, $\alpha$ is **integral over** $R$**.**

**Example 14.0.3.** $\frac{1}{2}$ is *not* integral over $\mathbb{Z}$. $m_{\frac{1}{2},\mathbb{Q}}(x) = x - \frac{1}{2}$, where $2x - 1$ is *not monic.* We have

$$\mathbb{Z}\left[\frac{1}{2}\right] = \mathbb{Z} + \mathbb{Z}\frac{1}{2} + \mathbb{Z}\frac{1}{4} + \ldots + \mathbb{Z}\frac{1}{2^n} + \ldots$$

is not finitely generated, as a $\mathbb{Z}$-module.

**Example 14.0.4.** $\sqrt{2}$ *is integral over* $\mathbb{Z}$. We have $x^2 - 2 \in \mathbb{Z}[x]$ monic, and $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ as a $\mathbb{Z}$-module.

**Definition 14.0.5.** Let $S$ and $R$ be as in 14.0.1. Then the **integral closure** of $R$ in $S$ is the subset

$$\{\alpha \in S \mid \alpha \text{ integral in } R\}.$$

**Theorem 14.0.6.** *The integral closure in 14.0.5 is a* subring *of $S$.*

If $R$ is a *domain* $\implies \exists$ Frac($R$) ("fraction field of $R$").

$$\mathrm{Frac}(R) := \left\{ \frac{a}{b} \,\middle|\, a, b \in R, b \neq 0 \right\}$$

with equivalence relation $\sim$ given by $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$.

**Example 14.0.7.** $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

**Definition 14.0.8.** Assume $R$ is a *domain.* Then $R$ is **integrally closed** if $R$ is *its own integral closure* in Frac($R$) (in algebraic geometry, one has integrally closed $\Leftrightarrow$ normal).

**Lemma 14.0.9.** *$\mathbb{Z}$ is integrally closed.*

The proof strategy uses the "rational root test".

*Proof.* Let $f(x) \in \mathbb{Z}[x]$ so that $f(x) = a_n x^n + \ldots + a_1 x + a_0$ where $a_i \in \mathbb{Z}$. Let $\frac{a}{b} \in \mathbb{Q}$ and $(a, b) = 1$. Assume that $f\left(\frac{a}{b}\right) = 0$. Then (by the "rational root test") one has $b \mid a_n$ and $a \mid a_0$. We will show that $a \mid a_0$.

So

$$0 = f\left(\frac{a}{b}\right) = a_n \left(\frac{a}{b}\right)^n + \ldots + a_1 \frac{a}{b} + a_0$$

We multiply both sides by $b^n$ and get

$$a_n a^n + a_{n-1} a^{n-1} b + \ldots + a_1 a b^{n-1} + a_0 b^n = 0. \tag{14.1}$$

Moving $a_0 b^n$ to the right side, we get

$$a_n a^n + a_{n-1} a^{n-1} b + \ldots + a_1 a b^{n-1} = -a_0 b^n$$

Factoring out $a$, we get

$$a(a_n a^{n-1} + a_{n-1} a^{n-2} b + \ldots + a_1 b^{n-1}) = -a_0 b^n.$$

$\mathbb{Z}$ is a *bezout domain*, so bezout's identity holds for $a, b$, i.e. $\exists x, y \in \mathbb{Z}$ so that $ax + by = 1$. Multiplying both sides by $a_0$, we get $a_0 a x + a_0 b y = a_0$. Since we know that $a \mid -a_0 b$ (so $a \mid a_0 b$), there is a $k \in \mathbb{Z}$ so that $ak = a_0 b$.

Then we see that $a_0 a x + a k y = a_0 \Leftrightarrow a(a_0 x + k y) = a_0$. Hence $a$ divides $a_0$.

In the same fashion, one can move $a_n a^n$ over to the RHS in (14.1) and see that $b \mid a_n$ (using that if $(a, b) = 1$ then $(a^n, b) = 1$). $\square$

**Definition 14.0.10.** $\overline{\mathbb{Z}} =$ **integral closure of** $\mathbb{Z}$ in $\mathbb{C}$.

$$\overline{\mathbb{Z}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q} \text{ and } m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]\}.$$

We call $\overline{\mathbb{Z}}$ the **ring of algebraic integers**.

**Lemma 14.0.11.** $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

**Proposition 14.0.12.** *Let* $u = \sum_{g \in G} u_g g \in Z(\overline{\mathbb{Z}}[G])$, *that is,* $u_g \in \overline{\mathbb{Z}}$, *where* $u_g = u_h$ *if* $g$ *is conjugate to* $h$.

*Then* $u$ *is* integral *over* $\mathbb{Z}$, *that is, so that* $u \in \overline{\mathbb{Z}}$.

In the proof below, we are implicitly using that $\overline{\mathbb{Z}}$ is a domain (I don't think we can be sure about linear independence otherwise) when we say that $(K_i)_{i=1}^s$ is a basis for $\overline{\mathbb{Z}}[G]$.

*Proof.* $u = \sum_{i=1}^{s} u_g K_i$ where $g_i \in \mathscr{K}_i$, and $\mathscr{K}_1, \ldots, \mathscr{K}_s$ are the conjugacy classes when $G$ acts on itself by conjugation.

We know that $K_i \in Z(\mathbb{Z}[G]) \subset Z(\overline{\mathbb{Z}}[G])$. It is enough to show that $K_i$ is integral over $\mathbb{Z}$. Consider that $K_i K_j = \sum a_{ij\ell} K_\ell$ where $a_{ij\ell} \in \mathbb{Z}_{\geq 0}$. The coefficient $a_{ij\ell}$ is the coefficient of $g \in \mathscr{K}_\ell$ $(\{h_i h_j \mid h_i h_j = g\}$ where $h_i \in \mathscr{K}_i, h_j \in \mathscr{K}_j)$.

The ring $\mathbb{Z}[K_1, \ldots, K_s]$ is a subring of $Z(\overline{\mathbb{Z}}[G])$ that is finitely generated as a $\mathbb{Z}$-module. Using $b) \implies a)$ in 14.0.1 the $K_i$ are integral over $\mathbb{Z}$. □

**Proposition 14.0.13.** *if* $\rho : G \to GL(V)$ *is irreducible, with* $u$ *as before, then*

$$\frac{1}{\chi(1)} \sum_{g \in G} u_g \chi(g) \in \overline{\mathbb{Z}}.$$

*Proof.* 2.0.5 gives us that if $\rho$ is irreducible then $Z(\mathbb{C}[G])$ acts by <u>central character</u> $\omega$, so that $\rho(\alpha) := \omega(\alpha) I$ for all $\alpha \in Z(\mathbb{C}[G])$. One has that $\omega : Z(\mathbb{C}[G]) \to \mathbb{C}$ is a $\mathbb{Z}$-algebra homomorphism, so that $\omega(\alpha\beta) = \omega(\alpha)\omega(\beta)$.

$$\begin{array}{ccc} Z(\mathbb{C}[G]) & \xrightarrow{\quad\omega\quad} & \mathbb{C} \\ \cap & & \cup \\ Z(\overline{\mathbb{Z}}[G]) & \xrightarrow{\qquad} & \overline{\mathbb{Z}} \end{array}$$

Let $f(x) = x^n + \ldots + a_1 x + a_0$ so that $f(\alpha) = 0$. Then

$$\begin{aligned}0 &= \omega(0)\\ &= \omega(\alpha^n + \ldots + a\alpha + a_0)\\ &= \omega(\alpha^n) + \ldots + \omega(a_1\alpha) + \omega(a_0)\\ &= \omega(\alpha)^n + \ldots + a_1\omega(\alpha) + \omega(a_0).\end{aligned}$$

If $a_i \in \mathbb{Z}$ then $\omega(a_i) = a_i$, so $\omega(f) = f$. This means that if $\alpha$ is integrable then $\omega(\alpha)$ is. We have that $\rho(u) = \omega(u)I$ and

$$\chi(u) = \omega(u)\chi(1) \tag{14.2}$$

$$\begin{aligned}\chi(u) &= \chi\left(\sum_{g\in G} u_g g\right)\\ &= \sum_{g\in G} u_g \chi(g).\end{aligned}$$

So, by (14.2) we have

$$\begin{aligned}\omega(u) &= \frac{\chi(u)}{\chi(1)}\\ &= \frac{1}{\chi(1)}\sum_{g\in G} u_g\chi(g).\end{aligned}$$

□

**Corollary 14.0.14.** $\chi(1) \mid |G|$.

*Proof.* Let $u = \sum_{g\in G}\chi(g^{-1})g$. If $\rho : G \to \mathrm{GL}(V)$ where $G$ is finite, then $V$ is a vector space over $\mathbb{C}$. A corollary of 14.0.12 is that $\chi(g) \in \overline{\mathbb{Z}}, \forall g \in G$. This is because $\chi(g)$ is a sum of $\dim V = r$ many roots of unity $\zeta_1, \ldots, \zeta_r$. And $\zeta_i \in \overline{\mathbb{Z}}$, and $\overline{\mathbb{Z}}$ is a ring, so closed under addition, hence $\chi(g) = \zeta_1 + \ldots + \zeta_r \in \overline{\mathbb{Z}}$.

Let $\mu_n$ be the *group* of $n^{\text{th}}$ roots of unity. Then $\chi(g) \in \mathbb{Z}[\mu_n] = \mathbb{Z}[\zeta]$ where $\zeta$ is a *primitive* $n^{\text{th}}$ root of unity.

We note in passing (not needed here) that $\mathbb{Z}[\zeta]$ is the *integral closure* of $\mathbb{Z}$ in $\mathbb{Q}(\zeta) := \mathbb{Q}(\mu_n)$.

<u>Warning</u>: The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{3})$´is $\mathbb{Z}[\zeta_3] \supsetneqq \mathbb{Z}[\sqrt{3}]$.

Returning to the proof; by 14.0.12 we see that $\frac{1}{\chi(1)}\sum_{g\in G}\chi(g^{-1})\chi(g) \in \overline{\mathbb{Z}}$.

By 9.0.1 we have

$$\frac{|G|}{\chi(1)}(\chi,\chi) = \frac{|G|}{\chi(1)}. \tag{14.3}$$

We just saw that the LHS in (14.3) is in $\overline{\mathbb{Z}}$. But we also know that $\frac{|G|}{\chi(1)} \in \mathbb{Q}$ since $|G| \in \mathbb{Z}$ and $\chi(1) = \dim V \in \mathbb{Z}$. By 14.0.11 we have that $\frac{|G|}{\chi(1)} \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. So $\chi(1) \mid |G|$. □

**Corollary 14.0.15.** $\omega(K_i) = \dfrac{\chi(g)|\mathscr{K}_i|}{\chi(1)} \in \overline{\mathbb{Z}}$.

*Proof.* Set $u = K_i$. By the proof of 14.0.13, we have

$$\begin{aligned}
\omega(u) &= \omega(K_i) \\
&= \frac{\chi(u)}{\chi(1)} \\
&= \frac{\chi\left(\sum\limits_{g \in \mathscr{K}_i} g\right)}{\chi(1)} \\
&= \frac{\sum\limits_{g \in \mathscr{K}_i} \chi(g)}{\chi(1)} \\
&= \frac{\chi(g)|\mathscr{K}_i|}{\chi(1)}
\end{aligned}$$

since $\chi$ is *constant* on conjugacy classes. By 14.0.13 we see that $\dfrac{\chi(g)|\mathscr{K}_i|}{\chi(1)} \in \overline{\mathbb{Z}}$. ☐

**Theorem 14.0.16** (Burnside)**.** *Let $\chi \in \mathrm{Irr}(G)$, let $\mathscr{K}$ be a conjugacy class (of the action of $G$ on itself by conjugation), and let $g \in \mathscr{K}$. Then*

$$(\chi(1), |\mathscr{K}|) = 1 \implies g \in Z(\chi) \text{ or } \chi(g) = 0.$$

**Definition 14.0.17.** $Z(\chi)$ in 14.0.16 is defined as

$$Z(\chi) := \{g \in G \mid |\chi(g)| = \chi(1)\}.$$

**Lemma 14.0.18.** *If $G$ is non-abelian, simple, finite group, and $\chi$ is a non-trivial irreducible complex character, then*

$$\begin{aligned}
Z(\chi) &= Z(G) \\
&= \{1\}.
\end{aligned}$$

**Theorem 14.0.19.** *Let $G$ be a non-abelian simple group. Then $\{1\}$ is the only conjugacy class of prime power size.*

*Proof.* Let $g \in G, g \neq 1$ so that $|\mathscr{K}| = p^\alpha$, where $g \in \mathscr{K}$. Let $\chi \in \mathrm{Irr}(G), \chi \neq \mathbf{1}_G$. By 14.0.18 one has $Z(\chi) = \{1\} \implies g \notin Z(\chi)$. By 14.0.16 this implies that $\chi(g) = 0$, if $p \nmid \chi(1)$. This is because if $p \nmid \chi(1)$ then $(\chi(1), p) = 1$ so that

$$\begin{aligned}
(\chi(1), p^\alpha) &= (\chi(1), |\mathscr{K}|) \\
&= 1.
\end{aligned}$$

Recall that $\chi_{\mathrm{reg}} = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$. Since $g \neq 1$, we have

$$\begin{aligned} 0 &= \chi_{\mathrm{reg}}(g) \\ &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) \\ &= 1 + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ p \,\mid\, \chi(1)}} \chi(1)\chi(g). \end{aligned} \tag{14.4}$$

Set $\alpha := \sum_{p \,\mid\, \chi(1)} \frac{\chi(1)}{p}\chi(g) \in \overline{\mathbb{Z}}$. Rearranging (14.4) we get

$$\begin{aligned} -1 &= \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ p \,\mid\, \chi(1)}} \chi(1)\chi(g) \\ &\Leftrightarrow -\frac{1}{p} = \alpha \in \overline{\mathbb{Z}}. \end{aligned}$$

The RHS is an algebraic integer, but the LHS is not in $\overline{\mathbb{Z}}$ by 14.0.11 unless $p = 1$. $\square$

*Remark* 14.0.20. $\alpha$ is an algebraic integer, since $\frac{\chi(1)}{p} \in \mathbb{Z} \subset \overline{\mathbb{Z}}$ and we saw in the proof of 14.0.14 that $\chi(g) \in \overline{\mathbb{Z}}$ for all $g \in G$. Since $\overline{\mathbb{Z}}$ is a ring (14.0.10), we find that $\alpha \in \overline{\mathbb{Z}}$ (closure under multiplication).

# Chapter 15

# Lecture 15

**Theorem 15.0.1** (Burnside-Brauer). *Let $G$ be a finite group, and work over $\mathbb{C}$. Let $\chi$ be a* faithful *character of $G$. If $\chi$ takes precisely $m$ distinct values, then for all $\psi$ in $\mathrm{Irr}(G)$, $\psi$ is a constituent of $\chi^j$ for some $0 \leq j \leq m-1$ ($\chi^0 = \mathbf{1}_G$ is the trivial character). Equivalently, by 9.0.1, one has that $\langle \chi^j, \psi \rangle \neq 0$ for some $0 \leq j \leq m-1$.*

Recall: $\chi$ faithful $\Leftrightarrow \ker \chi = \{1\}$, and $\langle \eta, \lambda \rangle = \dfrac{1}{|G|} \sum_{g \in G} \eta(g)\overline{\lambda(g)}$.

*Proof.* Let $\chi(G) = \{a_1, \dots, a_m\}$, ordered such that $\chi(a_1) = \chi(1)$. Set $b_i = \sum_{\substack{g \in G \\ \chi(g) = a_i}} \overline{\psi(g)}$. Then

$$\begin{aligned} \langle \chi^j, \psi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi^j(g)\overline{\psi(g)} \\ &= \frac{1}{|G|} \sum_{i=1}^{m} a_i^j b_i \end{aligned} \tag{15.1}$$

We introduce the **Vandermonde matrix**: Let $a_1, \dots, a_m \in \mathbb{F}$ for a field $\mathbb{F}$ (here $\mathbb{F} = \mathbb{C}$). Then the Vandermonde matrix $\underline{V(a_1, \dots, a_m)}$ is defined as

$$\underline{V(a_1, \dots, a_m)} := \begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{m-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_m & a_m^2 & \dots & a_m^{m-1} \end{pmatrix}.$$

This is a matrix of dimension $m \times m$.

**Lemma 15.0.2.**

$$
\begin{aligned}
V(a_1,\ldots,a_m) &:= \det \underline{V(a_1,\ldots,a_m)} \\
&= \prod_{j<i}(a_i - a_j) \\
&= \prod_{i<j}(-1)^{\frac{m(m-1)}{2}}(a_i - a_j)
\end{aligned}
$$

One has that $V(a_1,\ldots,a_n) = 0 \Leftrightarrow a_i = a_j$ for some $i \neq j$. For example, let $x^2+ax+b = (x-\alpha)(x-\beta)$. Then the **discriminant** is defined (in this case) as

$$
\begin{aligned}
V(\alpha,\beta)^2 &= \begin{vmatrix} 1 & \alpha \\ 1 & \beta \end{vmatrix}\begin{vmatrix} 1 & \alpha \\ 1 & \beta \end{vmatrix} \\
&= (\beta - \alpha)^2 \\
&= (-(\alpha - \beta))^2 \\
&= (-1)^2(\alpha - \beta)^2 \\
&= (\alpha - \beta)^2.
\end{aligned}
$$

Consider that

$$
\begin{aligned}
(x-\alpha)(x-\beta) &= x^2 - x(\alpha+\beta) + \alpha\beta \\
&= x^2 + ax + b.
\end{aligned}
$$

By comparing coefficients, we see that

$$a = -(\alpha + \beta) \tag{15.2}$$

and

$$b = \alpha\beta. \tag{15.3}$$

One has

$$(\alpha - \beta)^2 = \alpha^2 - 2\alpha\beta + \beta^2.$$

Using (15.2) we see that

$$
\begin{aligned}
a^2 &= (-(\alpha+\beta))^2 \\
&= (-1)^2(\alpha+\beta)^2 \\
&= \alpha^2 + 2\alpha\beta + \beta^2
\end{aligned}
$$

and by (15.3) we have

$$-4b = -4\alpha\beta$$

so that

$$
\begin{aligned}
a^2 - 4b &= \alpha^2 + 2\alpha\beta + \beta^2 - 4\alpha\beta \\
&= \alpha^2 - 2\alpha\beta + \beta^2 \\
&= (\alpha - \beta)^2.
\end{aligned}
$$

In the general case, one has, for a polynomial

$$\begin{aligned} f(x) &= a_n x^n + \ldots + a_1 x + a_0 \\ &= \prod_{i=1}^{n} (x - \alpha_i) \end{aligned}$$

that $\mathrm{Disc}(f) = V(\alpha_1, \ldots, \alpha_n)^2$. As a side note, we see that $\mathrm{Disc}(f) = 0 \Leftrightarrow f$ has a multiple root.

Back to the proof. In our case, we had that $a_1, \ldots, a_m$ are *distinct*, so $V(a_1, \ldots, a_m) \neq 0$. Since $\chi$ was faithful, we have that $\ker \chi = \{1\}$. So

$$\begin{aligned} b_1 &= \overline{\psi(1)} \\ &= \psi(1) \\ &\neq 0. \end{aligned}$$

*Remark* 15.0.3. In this case, $\psi(1) \neq 0$ is obvious, since $\psi$ is an irreducible character over $\mathbb{C}$. For a general character $\lambda$ of a finite group $G$ over $\mathbb{C}$, one has $\lambda = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi$ so that $\lambda(1) = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi(1)$. Since $a_\chi \in \mathbb{Z}_{\geq 0}$ and $\chi(1) \geq 1$ for all $\chi \in \mathrm{Irr}(G)$, we find that $\lambda \geq 0$, and zero if and only if $a_\chi = 0$ for all $\chi \in \mathrm{Irr}(G)$. But this can not happen (8.0.6)!

Continuing with the proof. Assume that $\langle \chi^j, \psi \rangle$ vanishes for all $0 \leq j \leq m-1$. Since $a_1, \ldots, a_m$ are all distinct, by 15.0.2 $V(a_1, \ldots, a_m)$ is non-zero, so (by linear algebra) $\underline{V(a_1, \ldots, a_m)}$ is invertible.

Pay attention the the fact that $\underline{V(a_1, \ldots, a_m)}_{ij} = a_i^j$ (with $0 \leq i, j \leq m-1$), so in the transpose of the vandermonde matrix, ${}^t\underline{V(a_1, \ldots, a_m)}$, one has ${}^t\underline{V(a_1, \ldots, a_m)}_{ij} = a_j^i$. So, for example, column 1 (with zero-numbering) will all be of the form $a_2^i$ with $i$ determined by the row. Therefore, we have

$${}^t\underline{V(a_1, \ldots, a_m)} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ a_1 & a_2 & a_3 & \ldots & a_{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{m-1} & a_2^{m-1} & a_3^{m-1} & \ldots & a_m^{m-1} \end{pmatrix}.$$

Then we see that

$${}^t\underline{V(a_1, \ldots, a_m)} \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = 0_{m \times 1}. \tag{15.4}$$

*Remark* 15.0.4. (15.4) follows immediately from (15.1).

The following lemma might be well known by the reader, but we remind ourselves.

**Lemma 15.0.5.** *If a matrix $A$ of dimension $m \times m$ is invertible, then ${}^tA$ is invertible with inverse ${}^t(A^{-1})$.*

*Proof.* Recall that ${}^t(AB) = {}^tB\,{}^tA$. Then we see that

$$\begin{aligned} {}^tA\,{}^t(A^{-1}) &= {}^t(A^{-1}A) \\ &= {}^t(I_m) \\ &= I_m. \end{aligned}$$

and

$$\begin{aligned} {}^t(A^{-1})\,{}^tA &= {}^t(AA^{-1}) \\ &= {}^t(I_m) \\ &= I_m \end{aligned}$$

□

It follows from 15.0.5 that $\underline{{}^tV(a_1,\dots,a_m)}$ is invertible

$$\implies \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = 0_{m\times 1}.$$

But we saw that $b_1 \neq 0$ (contradiction)! □

*Remark* 15.0.6. $\mathrm{GL}(n,\mathbb{C}) = G$ is an infinite group.

$$G \xrightarrow[\mathrm{id}]{} \mathrm{GL}(n,\mathbb{C})$$

$$G \xrightarrow{\mathrm{id}^\vee} \mathrm{GL}(n,\mathbb{C})$$

$$A \longmapsto {}^tA^{-1}$$

For all $n \geq 1$, one has that $\mathrm{id}^\vee$ is *not a constituent* of $\mathrm{id}^{\otimes n}$.

Recall Burnsides "$p^aq^b$ theorem" (10.0.9). Here is an outline of how to prove it:

Step 1: Use 14.0.15.

Step 2: 14.0.16.

Step 3: 14.0.19

(My understanding is that the proof is by contradiction). Then we come to Step 4, which proves 10.0.9:

*Proof.* If $N \triangleleft G$, then $G$ *solvable* $\Leftrightarrow$ $N$, $G/N$ are solvable.. Let $P \in \mathrm{Syl}_p(G)$. Then $Z(P) \neq 1$ (use the class-equation to see this). Let $z$ be a *non-trivial* element in $Z(P)$. Then we know that $P$ is included in the centralizer of $z$ in $G$, i.e. $\mathbf{C}_G(z) \supset P$, so $|\mathbf{C}_G(z)| = p^aq^{b_0}$ for $b_0 \leq b$.

Consider that $b_0 = b \Leftrightarrow z \in Z(G)$. But if $b_0 = b$, then $G$ would have a non-trivial proper normal subgroup, so this can not happen (we assumed that $G$ was simple). If $b_0 \neq b$, then by orbit-stabilizer (10.0.3), we have that

$$\begin{aligned}|\mathrm{Orb}(z)| &= \frac{|G|}{|\mathbf{C}_G(z)|}\\ &= \frac{p^a q^b}{p^a q^{b_0}}\\ &= q^{b-b_0} > 1.\end{aligned}$$

Then the conjugacy class of $z$ has prime-power order. Since we assumed that $G$ was simple, by the contrapositive of 14.0.19, $G$ is not simple (If $G$ was abelian, then $G$ would be solvable; $\{1\} \triangleleft G$ is a subnormal series).

We aim to prove step 2, i.e. 14.0.16. Assume that $g \notin Z(\chi)$, and show that $\chi(g) = 0$. Since we know (corollary 2.15 in [2]) that $|\chi(g)| \leq 1$, if $g \notin Z(\chi)$ then $|\chi(g)| < \chi(1) \Leftrightarrow \dfrac{|\chi(g)|}{\chi(1)} < 1$. Set $\alpha := \dfrac{\chi(g)}{\chi(1)}$. Recall that in $\mathbb{Z}$, if $a \mid bc$ and $(a, b) = 1$ then $a \mid c$ (cf. proof of 14.0.9).

Recall from 14.0.15 that $\chi(1) \mid \chi(\mathscr{K}_i)|\mathscr{K}_i| \in \overline{\mathbb{Z}}$, where $\mathscr{K}_i$ in $\chi(\mathscr{K}_i)$ denotes a *representative* element of the conjugacy-class $\mathscr{K}_i$. We know that $\chi(1) \in \mathbb{Z}$ and $|\mathscr{K}_i|$ in $\mathbb{Z}$. By the antecedent of 14.0.16, $(\chi(1), |\mathscr{K}_i) = 1$, so there exists $u, v \in \mathbb{Z}$ (recall that $\mathbb{Z}$ is bezout domain) such that

$$u\chi(1) + v|\mathscr{K}_i| = 1$$

so that

$$\chi(\mathscr{K}_i)u\chi(1) + \chi(\mathscr{K}_i)v|\mathscr{K}_i| = \chi(\mathscr{K}_i).$$

Since $\chi(1) \mid \chi(\mathscr{K}_i)|\mathscr{K}_i|$ we find that $\chi(1)$ divides the LHS, hence RHS, so $\chi(1)$ divides $\chi(\mathscr{K}_i)$.

<u>Want</u>: If $\beta \in \overline{\mathbb{Q}}$ and $m_{\beta,\mathbb{Q}}(x) = m_{\alpha,\mathbb{Q}}(x)$ then $|\beta| \leq 1$, where, for us, $\alpha = \dfrac{\chi(g)}{\chi(1)}$.

<u>Caution</u>: This is not true in general; related to **Lehmer's polynomial**: $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$.

But we prove it in our case. Let $n = |G|$. Recall that

$$\begin{aligned}\mu_n &= \text{group of } n^{\text{th}} \text{ roots of unity}\\ &= \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}\\ &= \left\{ e^{\frac{2\pi m i}{n}} \,\middle|\, 0 \leq m \leq n-1 \right\}\\ &= \left\langle e^{\frac{2\pi i}{n}} \right\rangle.\end{aligned}$$

Let $\zeta$ be a *primitive* $n^{\text{th}}$ root of unity, e.g. $\zeta = e^{\frac{2\pi i}{n}}$. Then

$$\begin{aligned}\mathbb{Q}(\mu_n) &= \mathbb{Q}(\zeta)\\ &\cong \mathbb{Q}[x]/(m_{\zeta,\mathbb{Q}}(x)).\end{aligned}$$

We note in passing that $m_{\zeta,\mathbb{Q}}(x) = \Phi_n(x)$. We know that $\chi(g) = \zeta_1 + \ldots + \zeta_{\chi(1)}$, where $\zeta_i \in \mu_n$.

<u>Need</u>:

1. If $m_{\alpha,\mathbb{Q}}(x) = m_{\beta,\mathbb{Q}}(x)$ then there exists an isomorphism $\varphi : \mathbb{Q}(\alpha) \overset{\cong}{\to} \mathbb{Q}(\beta)$ such that $\varphi(\alpha) = \beta$

$$\begin{tikzcd}
\mathbb{Q}(\alpha) \arrow[rr, "\cong", "\varphi"'] \arrow[dr, "\cong", "\mathrm{ev}_\alpha"'] & & \mathbb{Q}(\beta) \arrow[dl, "\cong"', "\mathrm{ev}_\beta"] \\
& \mathbb{Q}[x]/(m_{\alpha,\mathbb{Q}}(x)) &
\end{tikzcd}$$

2. $$\begin{tikzcd}
\mathbb{Q}(\zeta) \arrow[r, "\cong", "\sigma"'] \arrow[d, dash] & \mathbb{Q}(\zeta) \arrow[d, dash] \\
\mathbb{Q}(\alpha) \arrow[r, "\cong", "\varphi"'] \arrow[d, dash] & \mathbb{Q}(\beta) \arrow[d, dash] \\
\mathbb{Q} & \mathbb{Q}
\end{tikzcd}$$

If $\alpha \in \mathbb{Q}(\zeta)$, $\beta \in \overline{\mathbb{Q}} \subset \mathbb{C}$ and $m_{\alpha,\mathbb{Q}}(x) = m_{\beta,\mathbb{Q}}(x)$ then $\beta \in \mathbb{Q}(\zeta)$ (not hard to see; it follows almost by definition).

### 15.0.1 Interlude on extending embeddings of fields

Assume $\mathbb{K}_1/\mathbb{F}_1$ finite field extension (so algebraic; transcendental extensions are of infinite degree).

$$\begin{tikzcd}
\mathbb{K}_1 \arrow[d, dash] & \\
\mathbb{F}_1 \arrow[r, "\varphi", "\sim"'] & \mathbb{F}_2
\end{tikzcd}$$

Let $\mathbb{L}$ be an algebraically closed field containing $\mathbb{F}_2$. Claim: There exists a field embedding $\mathbb{K}_1 \hookrightarrow \mathbb{L}$.

*Proof.* Let $\alpha_1, \ldots, \alpha_n$ be a basis of $\mathbb{K}_1/\mathbb{F}_1$ (recall that $\mathbb{K}_1/\mathbb{F}_1$ is an $\mathbb{F}_1$ vector space of dimension $n$). Then $\mathbb{K}_1 = \mathbb{F}_1(\alpha_1 \ldots, \alpha_n)$. By induction, reduce to $\mathbb{K}_1 = \mathbb{F}_1(\alpha_1)$. Let $f_1(x) = m_{\alpha_1,\mathbb{F}_1}(x) \in \mathbb{F}_1[x]$. Set $f_2(x) := \varphi(f_1(x))$. Let $f_1(x) = \sum a_j x^j$. Then $f_2(x) = \sum \varphi(a_j)x^j$

*Remark* 15.0.7. Implicitly, we extend $\mathbb{F}_1, \mathbb{F}_2$ by linearity to $\mathbb{F}_1[x], \mathbb{F}_2[x]$ through $\varphi(a_n x^n + \ldots + a_1 x + a_0) := \varphi(a_n)x^n + \ldots + \varphi(a_1)x + \varphi(a_0)$, that is, $\varphi$ "leaves" $x^j$ invariant.

From $\mathbb{F}_1 \xrightarrow{\sim} \mathbb{F}_2$ by $\varphi$, we get an induced isomorphism $\mathbb{F}_1[x] \to \mathbb{F}_2[x]$ (check; should not be hard to see). Then we get the following diagram

$$\begin{tikzcd}
 & \mathbb{F}_2[x] \arrow[rr, two heads] & & \mathbb{F}_2[x]/(f_2(x)) \\
\mathbb{F}_1[x] \arrow[ur, "\sim"] \arrow[rr, two heads] & & \mathbb{F}_1[x]/(f_1(x)) \arrow[ur, "\sim", "\tilde{\varphi}"'] &
\end{tikzcd}$$

Since $\mathbb{L}$ is algebraically closed, $f_2$ contains a root $\beta_1$ in $\mathbb{L}$.

$$\begin{tikzcd}
\mathbb{F}_1[x] \arrow[r, "\mathrm{ev}_1"] \arrow[dr] & \mathbb{F}_1(\alpha_1) \\
 & \mathbb{F}_1[x]/(f_1(x)) \arrow[u, dotted, "\cong"', "\tilde{\mathrm{ev}}_1"]
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{F}_2[x] \arrow[r, "\mathrm{ev}_2"] \arrow[dr] & \mathbb{F}_2(\beta_1) \\
 & \mathbb{F}_2[x]/(f_2(x)) \arrow[u, dotted, "\tilde{\mathrm{ev}}_2"', "\cong"]
\end{tikzcd}$$

So, $\tilde{\mathrm{ev}}_2 \circ \tilde{\varphi} \circ \tilde{ev}_1^{-1} : \mathbb{F}_1(\alpha_1) \cong \mathbb{F}_2(\beta_1)$, extending $\varphi$. By repeated application of this, we get an isomorphism $\tilde{\varphi} : \mathbb{K}_1 = \mathbb{F}_1(\beta_1, \ldots, \beta_n) \to \mathbb{F}_2(\alpha_1, \ldots, \alpha_n) \subset \mathbb{L}$. $\square$

*Remark* 15.0.8. That $\mathbb{F}_2(\beta_1, \ldots, \beta_n) \subset \mathbb{L}$ is clear from the fact that we in each step in the proof (we just show the first step in the proof above), choose $\beta_i \in \mathbb{L}$.

*Remark* 15.0.9. It is not entirely clear from what we have written that $\tilde{\varphi} : \mathbb{F}_1(\alpha_1, \ldots, \alpha_n) \to \mathbb{F}_2(\beta_1, \ldots, \beta_n)$ is such that $\tilde{\varphi}|_{\mathbb{F}_1} = \varphi$ (check!).

**Definition 15.0.10.** Assume that $\mathbb{K}/\mathbb{F}$ is a finite field extension, and that $\mathbb{L}$ is an algebraically closed field containing $\mathbb{K}$. Then $\mathbb{K}/\mathbb{F}$ is **normal** if for all embeddings $\mathbb{K} \overset{\varphi}{\hookrightarrow} \mathbb{L}$ *fixing* $\mathbb{F}$, we have that $\varphi(\mathbb{K}) \subset \mathbb{K}$.

$$\begin{tikzcd}
\mathbb{K} \arrow[r] \arrow[dr, "\varphi"'] & \mathbb{K} \arrow[d] \\
 & \mathbb{L}
\end{tikzcd}$$

*Remark* 15.0.11. If $\operatorname{char} \mathbb{F} = 0$ then normal extension $\Leftrightarrow$ galois extension.

Below, let $\mu_n$ denote the group of $n^{\text{th}}$ roots of unity with multiplication as binary operator.

**Lemma 15.0.12.** $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta)$ *($\zeta \in \mu_n$ primitve $n^{th}$ root of unity) is* <u>*normal*</u>.

*Proof.* Let $\varphi : \mathbb{Q}(\zeta) \hookrightarrow \mathbb{C}$. Then $\varphi$ is determined by $\varphi(\zeta)$ (follows from the definition of $\mathbb{Q}(\zeta)$ together with the fact that $\varphi$ is a homomorphism). We have $\zeta^n = 1$ so that $\varphi(\zeta)^n = 1$, so $\varphi(\zeta) = \zeta^j$ for some $j$ (recall that $\zeta$ *generates* $\mu_n$). So, we see that $\varphi(\mathbb{Q}(\zeta)) \subset \mathbb{Q}(\zeta)$. $\square$

*Remark* 15.0.13. In fact, $\varphi$ exists $\Leftrightarrow (j, n) = 1$. To see one direction, assume that $(j, n) = k \neq 1$. Then $\varphi(\zeta)^{\frac{n}{k}} = 1$. But that would mean that $\varphi(\zeta^{\frac{n}{k}}) = 1$. We know that $\zeta^{\frac{n}{k}} \neq 1$. But this is impossible, since $\varphi$ must be injective.

**Corollary 15.0.14.** *Assume that $\mathbb{F}_1, \mathbb{F}_2 \subset \mathbb{K}$ and $\mathbb{K}/\mathbb{F}$ normal. Then there exists an automorphism $\tilde{\varphi} \in Aut(\mathbb{K}/\mathbb{F})$ such that $\tilde{\varphi}|_{\mathbb{F}_1} = \varphi$.*

$$\begin{tikzcd}
\mathbb{F}_1 \arrow[r, "\varphi", "\sim"'] \arrow[d, dash] & \mathbb{F}_2 \arrow[d, dash] \\
\mathbb{F} \arrow[r, equal] & \mathbb{F}
\end{tikzcd}$$

*Proof.* Let $\mathbb{K} \subset \mathbb{L}$ where $\mathbb{L}$ is an algebraically closed field. By 15.0.1 there exists $\tilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{L}$ such that $\tilde{\varphi}|_{\mathbb{F}_1} = \varphi$. Since $\mathbb{K}/\mathbb{F}$ is normal (if assuming $\operatorname{char} \mathbb{F} = 0$ then actually galois), one has $\tilde{\varphi}(\mathbb{K}) \subset \mathbb{K}$. $\square$

*Remark* 15.0.15. We can apply similar reasoning as in 15.0.1 to get $\varphi : \mathbb{F}_1 \to \mathbb{F}_2$ from some automorphism $\sigma$ of $\mathbb{F}$, I believe. This would explain why $\tilde{\varphi}$ from 15.0.1 fixes $\mathbb{F}$, so that $\tilde{\varphi}$ actually is an automorphism in $\operatorname{Aut}(\mathbb{K}/\mathbb{F})$.

**Proposition 15.0.16.** *Let $\alpha, \beta \in \mathbb{Q}(\zeta)$ with $m_{\alpha,\mathbb{Q}}(x) = m_{\beta,\mathbb{Q}}(x)$. Then there exists an automorphism $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ so that $\sigma(\alpha) = \beta$.*

*Proof.* Since $m_{\alpha,\mathbb{Q}}(x) = m_{\beta,\mathbb{Q}}(x)$, there exists an isomorphism $\varphi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$. By 15.0.14, since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a normal extension (we do not show this here), and $\mathbb{Q}(\alpha), \mathbb{Q}(\beta) \subset \mathbb{Q}(\zeta)$, there exists an automorphism $\sigma \in \operatorname{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $\sigma|_{\mathbb{Q}(\alpha)} = \varphi$. $\square$

Back to the proof. Recall that

$$\alpha = \frac{\chi(g)}{\chi(1)} \tag{15.5}$$

where $\chi(g) = \zeta_1 + \ldots + \zeta_{\chi(1)}$. We want to show that $|\beta| \leq 1$.

**Corollary 15.0.17.** $|\beta| \leq 1$ *for all $\beta$ such that $m_{\alpha,\mathbb{Q}}(x) = m_{\beta,\mathbb{Q}}(x)$, with $\alpha$ as in 15.5.*

*Proof.* By 15.0.16 there exists $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ such that $\sigma(\alpha) = \beta$. So

$$\begin{aligned}
\sigma(\alpha) &= \beta \\
&= \frac{\sigma(\zeta_1) + \ldots + \sigma(\zeta_{\chi(1)})}{\chi(1)}
\end{aligned}$$

So

$$
\begin{aligned}
|\beta| &= \left|\frac{\sigma(\zeta_1)+\ldots+\sigma(\zeta_{\chi(1)})}{\chi(1)}\right| \\
&\leq \sum_{i=1}^{\chi(1)} \frac{|\sigma\chi(\zeta_i)|}{\chi(1)} \\
&= \frac{\chi(1)}{\chi(1)} \\
&= 1.
\end{aligned} \tag{15.6}
$$

Since $\sigma(\zeta_i)$ is also an $n^{\text{th}}$ root of unity, hence has absolute value 1. □

*Remark* 15.0.18. Note that in the proof of 15.0.17, we used that $\sigma\left(\frac{1}{\chi(1)}\right) = \frac{1}{\chi(1)}$ and that $\sigma$ is a field homomorphism, for the equalities in 15.6.

Set

$$\gamma = \prod_{\{\beta \mid m_{\beta,\mathbb{Q}}(x)=m_{\alpha,\mathbb{Q}}(x)\}} . \tag{15.7}$$

Let $m_{\alpha,\mathbb{Q}}(x) = x^n + \ldots + a_1x + a_0$. By vietas formulas, we know that

$$\prod_{\{\beta \mid m_{\beta,\mathbb{Q}}(x)=m_{\alpha,\mathbb{Q}}(x)\}} \beta$$

is equal to $\frac{(-1)^{\deg m_{\alpha,\mathbb{Q}}(x)}}{a_n = 1}$. So the LHS in (15.7) equals $(-1)^{\deg m_{\alpha,\mathbb{Q}}(x)}a_0$. So $\gamma \in \mathbb{Q}$.

Note that $|\alpha| < 1$ by assumption, and $\alpha \in \overline{\mathbb{Z}}$. Since $\alpha$ is one such $\beta$ so that $m_{\beta,\mathbb{Q}}(x) = m_{\alpha,\mathbb{Q}}(x)$, we have $|\gamma| < 1$. Recall that since $\alpha$ is an algebraic integer, then $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$ (14.0.10). Then we see that for any $\beta$ so that $m_{\alpha,\mathbb{Q}}(x) = m_{\beta,\mathbb{Q}}(x)$, we have $\beta \in \overline{\mathbb{Z}}$. But then we know that $\gamma \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ and $|\gamma| < 1$ so that $\gamma = 0$. So there must be atleast one $\beta = 0$.

But then, by 15.0.16 we have that there is an automorphism $\sigma$ such that $\sigma(\alpha) = 0$. It follows that $\alpha = 0$ ($\sigma$ injective). □

### 15.0.2 SL$(2, \mathbb{F}_p)$ and GL$(2, \mathbb{F}_p)$

One has $|\operatorname{SL}(2,\mathbb{F}_p)| = p(p^2-1)$ and $|\operatorname{GL}(2,\mathbb{F}_p)| = (p^2-1)(p^2-p)$.

$$1 \hookrightarrow \operatorname{SL}(2,\mathbb{F}_p) \xhookrightarrow{\psi} \operatorname{GL}(2,\mathbb{F}_p) \xrightarrow{\det} \mathbb{F}_p^\times \longrightarrow 1$$

is a short exact sequence of groups; the kernel of det is $\operatorname{SL}(2,\mathbb{F}_p) = \operatorname{im}\psi$, and $\psi$ is an injective group homomorphism, while det is a surjective group homomorphism, where $1 = I_2$, $-1 = -I$.

Set $S_1 = \begin{pmatrix} s & 0 \\ 0 & s^{-1} \end{pmatrix}$ where $\langle s \rangle = \mathbb{F}_p^\times$ (recall that a finite subgroup of $\mathbb{F}^\times$ is cyclic; so in particular, when $\mathbb{F}$ is finite, then $\mathbb{F}^\times$ is cyclic, by HW1).

**Definition 15.0.19.** Let $\mathbb{F}_p$ be a finite field, and $\mathbb{F}_p^\times$ be the multiplicative group of invertible elements in $\mathbb{F}_p$ (so $\mathbb{F}_p \setminus \{0\}$). Then

$$\mathbb{F}_p^{\times^2} := \{q \in \mathbb{F}_p^\times \mid \exists x \in \mathbb{F}_p \text{ such that } x^2 = q\}$$

denotes the **quadratic residues** of $\mathbb{F}_p^\times$.

We also set $S_2 = \begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$ where $\delta \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times^2}$ and such that $\det S_2 = 1$. Set $U_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $U_2 = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$. One sees (check!) that $U_1$ and $U_2$ are conjugate by $\begin{pmatrix} \sqrt{s} & 0 \\ 0 & \sqrt{s} \end{pmatrix}$ over $\mathbb{F}_{p^2}$.

We have the following conjugacy classes, where the subscript indicates the *size* of the conjugacy class:

$$\begin{aligned}
&(1)_1 \\
&(-1)_1 \\
&(S_1^r)_{p(p+1)} \text{ where } 1 \leq r \leq \frac{p-3}{2} \\
&S_2^r)_{p(p-1)} \text{ where } 1 \leq r \leq \frac{p-1}{2} \\
&(U_1)_{\frac{p^2-1}{2}} \\
&(U_2)_{\frac{p^2-1}{2}} \\
&(-U_1)_{\frac{p^2-1}{2}} \\
&(-U_2)_{\frac{p^2-1}{2}}
\end{aligned}$$

Together, we then have $\underbrace{1 + 1 + \frac{p-3}{2} + \frac{p-1}{2}}_{=p} + 4 = p + 4$ conjugacy classes of $\mathrm{SL}(2, \mathbb{F}_p)$.

We also see that

$$\begin{aligned}
1 + 1 + \frac{p-3}{2}(p(p+1)) + \frac{p-1}{2}(p(p-1)) + 4 \cdot \frac{p^2-1}{2} &= p^3 - p \\
&= p(p^2 - 1) \\
&= |\,\mathrm{SL}(2, \mathbb{F}_p)|.
\end{aligned}$$

<u>Check this</u>: Let $\chi \in \mathrm{Irr}(G)$.

| dim | # |
|---|---|
| $p+1$ | $\frac{p-3}{2}$ |
| $p$ | 1 |
| 1 | 1 |
| $p-1$ | $\frac{p-1}{2}$ |
| $\frac{p+1}{2}$ | 2 |
| $\frac{p-1}{2}$ | 2 |

Table 15.1: Dimension of irreducible character, and how many

Let $B = \left\{ A = \begin{pmatrix} a & * \\ 0 & a^{-1} \end{pmatrix} \;\middle|\; A \in \mathrm{SL}(2, \mathbb{F}_p) \right\}$ where we have $p-1$ choices for $a$ and $p$ choices for $*$, so $|B| = p(p-1)$. Then

$$\begin{aligned} [G : B] &= \frac{|G|}{|B|} \\ &= \frac{p(p^2-1)}{p(p-1)} \\ &= p+1. \end{aligned}$$

Set $U = \left\{ u = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \;\middle|\; u \in \mathrm{SL}(2, \mathbb{F}_p) \right\}$ and $D = \left\{ d = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \;\middle|\; d \in \mathrm{SL}(2, \mathbb{F}_p) \right\}$ so that $B = DU$.

One has $B \longrightarrow B/U \xrightarrow{\cong} D \xrightarrow{\lambda_i} \mathbb{F}_p$.

Then $\mathrm{Ind}_B^{\mathrm{SL}(2,\mathbb{F}_3)} \lambda_i$ is irreducible for $1 \leq i \leq \frac{p-3}{2}$ where $D \ni \zeta \xmapsto{\lambda_i} \zeta^i \in \mathbb{F}_p^\times$.

# Bibliography


[1] David Steven Dummit and Richard M. Foote. *Abstract algebra*. 3rd. Wiley; Sons, 2004.

[2] I. Martin Isaacs. *Character theory of finite groups*. eng. American Mathematical Society, 2006. ISBN: 9780821842294.

[3] T. Y. Lam. "A Theorem of Burnside on Matrix Rings". In: *The American Mathematical Monthly* 105.7 (1998), pp. 651–653. ISSN: 00029890, 19300972. URL: `http://www.jstor.org/stable/2589248` (visited on 03/10/2024).

[4] James Milne and Pierre Deligne. *Tannakian Categories*. 2018. URL: `https://www.jmilne.org/math/xnotes/tc2018.pdf`.

[5] P. Samuel. *Algebraic Theory of Numbers*. Hermann, 1970. ISBN: 9780901665065. URL: `https://books.google.se/books?id=uQzvAAAAMAAJ`.

[6] Jean-Pierre Serre. *Linear representations of finite groups*. Springer, 1977.