

# Higher Algebra 2

MATH 571

Nicholas Hayek

*Taught by Prof. Eyal Goren*

## CONTENTS

<b>I</b>	<b>Review</b>	<b>3</b>
	Commutator Subgroups . . . . .	3
	Tensor Products of Modules . . . . .	4
	<i>Construction</i>	
	Representations of Finite Groups . . . . .	5
	<i>Examples</i>	
	<i>Irreducible Representations</i>	
	<i>Class Functions</i>	
	<i>Character Tables</i>	
	<i>Induced Representations</i>	
	<i>Supersolvable Groups</i>	
	<i>Fourier Transforms</i>	
	<i>Random Walks on Cyclic Groups</i>	
<b>II</b>	<b>Homological Algebra</b>	<b>27</b>
	Exact Sequences . . . . .	27

# I Review

The first third of this course will be review from **MATH 457**. In particular, we will cover representation theory, with an emphasis on Fourier analysis and induced representations. The remainder of the course will be an introduction to homological algebra.

We require a cursory understanding of tensor products, categories, and functors. The official prerequisite for this course is MATH 570 (which includes category theory, commutative algebra, Noetherian rings), but these notes will be written from the point of view of someone (me) who has not studied these topics.

## COMMUTATOR SUBGROUPS

**DEF 1.1** Let  $G$  be a group. The **commutator** of  $a, b \in G$ , denoted by  $[a, b]$ , is the element  $aba^{-1}b^{-1}$ . Clearly,  $[a, b] = 1 \iff a$  and  $b$  commute. Let  $G' \subseteq G$  be generated by all finite multiplications of commutators, i.e.

$$G' = \langle [a, b] : a, b \in G \rangle$$

**DEF 1.2**  $G'$  is called the **commutator subgroup** of  $G$ .

**PROP 1.1** The commutator subgroup of  $G$  is normal.

**PROOF.**

Note that  $g[a, b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = [gag^{-1}, gbg^{-1}]$ . Then,

$$g[a_1, b_1] \cdots [a_N, b_N]g^{-1} = g[a_1, b_1]g^{-1} \cdot g[a_2, b_2]g^{-1} \cdots g[a_N, b_N]g^{-1} \in G' \quad \square$$

**PROP 1.2** If  $H \triangleleft G$ , then  $G/H$  is abelian  $\iff G' \subseteq H$ .

**PROOF.**

Suppose  $G/H$  is abelian. Consider  $aba^{-1}b^{-1} = [a, b] \in G'$ . Then

$$aba^{-1}b^{-1}H = aH \cdot bH \cdot a^{-1}H \cdot b^{-1}H = aa^{-1}H \cdot bb^{-1}H = H$$

Hence,  $[a, b] \in H$ , so  $G' \subseteq H$ . Conversely, suppose  $G' \subseteq H$ . Then

$$a^{-1}b^{-1}abH = H \implies abH = baH$$

so  $G/H$  is abelian.  $\square$

**PROP 1.3**  $G/G'$  is the largest abelian subgroup of the form  $G/H$  for  $H \triangleleft G$ . In other words,  $G'$  is the smallest normal subgroup of  $G$  such that  $G/G'$  is abelian.

**PROOF.**

Suppose  $G/H$  is abelian. Then  $G' \subseteq H$  by **Prop 1.2**. Thus,  $|G/G'| \geq |G/H|$ .  $\square$

**DEF 1.3**  $G^{ab} := G/G'$  is called the **abelianization** of  $G$ .

### Theorem 1.1 Unique Factoring Over Abelianizations

Let  $\varphi : G \rightarrow A$  be a homomorphism into an abelian group. Then  $\varphi$  factors uniquely into  $\varphi = \psi \circ \pi$ , where  $\pi : G \twoheadrightarrow G^{ab}$  is the natural quotient and  $\psi : G^{ab} \rightarrow A$ .

Recall the homomorphism theorem, of which the isomorphism theorem is a special case. Let  $\varphi : G \rightarrow H$ . Let  $N \subseteq \ker(\varphi)$  be a normal subgroup of  $G$ . Then  $\varphi = \psi \circ \pi$ , where  $\pi : G \twoheadrightarrow G/N$  is the natural quotient and  $\psi : G/N \rightarrow H$  is a homomorphism (surjective into  $\text{Im}(\varphi)$ ). Moreover, this decomposition is unique.

We apply this directly to the theorem above. Since  $A$  is abelian, so is  $\text{Im}(\varphi)$ . But  $\text{Im}(\varphi) \cong G/\ker(\varphi)$ . By [Prop 1.2](#), it follows that  $G' \subseteq \ker(\varphi)$ . Since  $G'$  is normal, the homomorphism theorem applies.  $\square$

PROOF.

## TENSOR PRODUCTS OF MODULES

Let  $\mathbf{Mod}_R$  and  ${}_R\mathbf{Mod}$  denote the categories of left and right modules over a ring  $R$ , respectively. Recall that, for an  $R$ -module  $M$ ,  $r \in R$ , and  $m \in M$ , left modules act by  $(r, m) \mapsto rm$  and right modules act by  $(r, m) \mapsto mr$ .

1/7/26

If a module is both a left and right module, and obeys all respective module axioms, we call it a *bimodule*, and write  ${}_S\mathbf{Mod}_R$  for the category of bimodules.

DEF 1.4

If  $A \in \mathbf{Mod}_R$  and  $B \in {}_R\mathbf{Mod}$ , an  *$R$ -biadditive* map is a function

DEF 1.5

$$f : A \times B \rightarrow G$$

where  $H$  is a abelian. Additionally, we require that

- $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$
- $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$
- $f(ar, b) = f(a, rb)$

As  $H$  is a group, we do not impose any scaling qualities for  $f$  with respect to  $R$ .

We would like to construct an abelian group  $G$  and associated  $R$ -biadditive function  $\varphi$  such that, for any  $R$ -biadditive function  $f$ , there is a unique group homomorphism  $g$  with

$$\begin{array}{ccc} A \times B & \xrightarrow{\varphi} & G =: A \otimes_R B \\ & \searrow f & \downarrow g \\ & & H \end{array}$$

commuting. If such a pair  $(G, \varphi)$  exists, we say it satisfies the *universal property*.

DEF 1.6

### Construction

We will construct a group  $G$  which satisfies the universal property, as above

Consider  $H = \mathbb{Z} \cdot (A \times B)$ , the  $\mathbb{Z}$ -module, and hence free abelian group. In other words,

$$H \ni h = \oplus_{(a,b) \in A \times B} k_{(a,b)} \cdot (a, b) \quad \text{where} \quad k_{(a,b)} \in \mathbb{Z}$$

Furthermore, consider the subgroup  $N < H$  by

$$N = \{(a_1 + a_2, b) - (a_1, b) - (a_2, b)\} \cup \{(a, b_1 + b_2) - (a, b_1) - (a, b_2)\} \cup \{(ar, b) - (a, rb)\}$$

under  $a, a_i \in A$ ,  $b, b_i \in B$ , and  $r \in R$ .

One shows manually that this is a group

DEF 1.7 Define  $A \otimes_R B := H/N$ , and call this the *tensor product* of  $A$  and  $B$  over  $R$ .

Let  $\varphi : A \times B \rightarrow A \otimes_R B$  be the natural map formed by viewing  $(a, b)$  as an element of the  $\mathbb{Z}$ -module  $H$ , and modding out by  $N$  as above.

Immediately, we see that the subgroup  $N$  ensures that  $\varphi$  is biadditive.

DEF 1.8 We denote the image of  $(a, b)$  under  $\varphi$  by  $a \otimes b$ , and call the result a *tensor*.

PROP 1.4  $(\varphi, A \otimes_R B)$  has the universal property.

DEF 1.9  $V^* = \text{Hom}_k(V, k)$  is called the *dual vector space*. Recall that  $\dim_k(V^*) = \dim_k(V)$ .

#### Theorem 1.2 Properties of the Tensor Product

1.  $\text{Hom}_k(V, W) \cong V^* \otimes_k W$ ,  $V, W$  are finite dimensional vector spaces over  $k$ .
2.  $\dim(V \otimes_k W) = \dim_k(V) \cdot \dim_k(W)$
3. If  $f \in \text{Hom}_R(A, A')$ ,  $g \in \text{Hom}_R(B, B')$ , then

$$f \otimes g : A \otimes_R B \rightarrow A' \otimes_R B' \text{ given by } (a \otimes b) \mapsto f(a) \otimes g(b)$$

is a homomorphism.

4. If  $A \cong A'$  and  $B \cong B'$ , then  $A \otimes_R B \cong A' \otimes_R B'$
5.  $A \otimes_R R = A$  and  $R \otimes_R B = B$
6.  $(\oplus_{i \in I} A_i) \otimes_R B \cong \oplus_{i \in I} (A_i \otimes_R B)$  and  $A \otimes (\oplus_{i \in I} B_i) = \oplus_{i \in I} A \otimes B_i$
7. If  $R$  is commutative, then  $A \otimes_R B = B \otimes_R A$ .
8. If  $R$  is commutative, then  $A \otimes_R (B \otimes_R C) \cong (A \otimes_R B) \otimes_R C$ .

## REPRESENTATIONS OF FINITE GROUPS

DEF 1.10 A *linear representation* of a finite group  $G$  is a vector space  $V$  over a field  $\mathbb{F}$  equipped with a group action

$$G \times V \rightarrow V$$

that respects the vector space, i.e.  $m_g : V \rightarrow V$  with  $m_g(v) = gv$  is a linear transformation. We make the following assumptions unless otherwise stated:

1.  $G$  is finite.
2.  $V$  is finite dimensional.
3.  $\mathbb{F}$  is algebraically closed and of characteristic 0. We write  $\mathbb{F} = \mathbb{C}$ .

Since  $V$  is a  $G$ -set,  $\rho : G \rightarrow \text{Aut}_{\mathbb{C}}(V)$  which sends  $g \mapsto m_g$  is a homomorphism.

Relatedly, if  $\dim(V) < \infty$ , then  $\rho : G \mapsto \text{Aut}_{\mathbb{C}}(V) = \text{GL}_n(\mathbb{C})$ .

The **group ring**  $\mathbb{C}[G]$  is a (typically) non-commutative ring consisting of all finite linear combinations  $\{\sum_{g \in G} \lambda_g g : \lambda_g \in \mathbb{C}\}$ , with  $1 \cdot \mathbb{1}_G = \mathbb{1}_{\mathbb{C}[G]}$ . It's endowed with the multiplication rule

DEF 1.11

$$\left( \sum_{g \in G} \alpha_g g \right) \left( \sum_{h \in G} \beta_h h \right) = \sum_{(g,h) \in G \times G} \alpha_g \beta_h (gh)$$

We can view representations as a module over the group ring  $\mathbb{C}[G]$ .

PROP 1.5

Let  $V$  be a  $\mathbb{C}[G]$ -module. Consider  $g \in G \subseteq \mathbb{C}[G]$ ,  $\lambda \mathbb{1}_G \in \mathbb{C}[G]$ , and  $v_1, v_2 \in V$ . Since  $V$  is a  $\mathbb{C}[G]$ -module,

PROOF.

$$g(v_1 + v_2) = gv_1 + gv_2 \quad (gh)v_1 = g(hv_1)$$

Then:  $(g\lambda \mathbb{1}_G)v_1 = (\lambda(g\mathbb{1}_G))v_1 = (\lambda g)v_1$ . But also,  $(g\lambda \mathbb{1}_G)v_1 = g(\lambda \mathbb{1}_G v_1) = g(\lambda v_1)$ . Hence, the map  $v \mapsto gv$  is a linear transformation on  $V$  over  $\mathbb{C}$ .  $\square$

We will frequently return to this view when module theory is more convenient.

**Eg. 1.1** Consider  $\rho : G \rightarrow \{1\}$ , the **trivial representation**, which maps  $\rho(g)(v) = v$ . We will denote the trivial representation simply by  $\mathbb{1}$ , subject to context.

DEF 1.12

**Eg. 1.2** We call  $\rho^{\text{reg}} : h \mapsto \left[ \sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g hg \right]$  the **regular representation**, with  $G \curvearrowright \mathbb{C}[G]$  by left multiplication.

DEF 1.13

Over  $\mathbb{C}$ ,  $\mathbb{C}[G]$  has basis  $\{g_1, \dots, g_n\}$ , where  $n = |G|$ . Then  $\chi(h) = |\{g_i \in G : hg_i = g_i\}|$ . If  $h = 1$ , then  $\chi(h) = |G|$ . Otherwise, it is impossible for  $hg_i = g_i$ .

We conclude that

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & g = 1 \\ 0 & \text{o.w.} \end{cases}$$

Generally, recall that the trace counts the number of basis vectors which are fixed by a transformation

## Examples

### RESTRICTED AND INDUCED REPRESENTATIONS

Let  $H < G$  be a subgroup. Then we consider a functor between the categories of representations of  $G$  and  $H$ ,

$$\text{Res}_H^G : \mathbf{Rep}(G) \rightarrow \mathbf{Rep}(H) : \rho \mapsto \rho|_H = \text{Res}_H^G(\rho)$$

DEF 1.14 called the *restricted representation* of  $G$  to  $H$ . Analogously, this sends a  $\mathbb{C}[G]$ -module  $V$  to the submodule  $W$  defined over  $\mathbb{C}[H]$ .

Similarly, we consider a functor

$$\text{Ind}_H^G : \mathbf{Rep}(H) \rightarrow \mathbf{Rep}(G) : V \mapsto \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$$

DEF 1.15 called the *induced representation* of  $H$  to  $G$ , where we view  $V$  as a  $\mathbb{C}[G]$ -module. Observe that  $\dim_{\mathbb{C}[H]}(\mathbb{C}[G]) = [G : H]$ , so  $\dim(\text{Ind}_H^G) = [G : H] \dim(V)$ .

**Eg. 1.3** Consider  $H = \{1\}$  with the trivial representation on  $V = \mathbb{C}$ . Then  $\text{Ind}_H^G(\mathbb{C}) = \mathbb{C}[G] \otimes_{\mathbb{C}} \mathbb{C} = \mathbb{C}[G]$ , i.e. the regular representation.

### DUAL REPRESENTATIONS

Let  $\rho, V$  be a representation of  $G$ . Recall the dual,  $V^* = \text{Hom}_{\mathbb{C}}(V, \mathbb{C})$ , the set of linear transformations from  $V \rightarrow \mathbb{C}$ . Given an endomorphism  $T : V \rightarrow V$ , we call

$$T^t : V^* \rightarrow V^* : (T^t \varphi)(v) := \varphi(Tv)$$

DEF 1.16 the *transpose*. If  $\beta = \{v_1, \dots, v_n\}$  is a basis for  $V$ , then we construct the *dual basis*  $\beta^* = \{\varphi_1, \dots, \varphi_n\}$  for  $V^*$ , where  $\varphi_i(v_j) = \delta_{ij}$ . In the dual basis, we have

DEF 1.17

PROP 1.6

$$[T^t]_{\beta^*} = [T]_{\beta}^t \implies \text{tr}(T) = \text{tr}(T^t)$$

PROOF.

See **MATH 251** notes. □

When  $T = \rho(g) : V \rightarrow V$ , we also observe

$$(\rho(gh)^t \varphi)(v) = (\rho(h)^t \rho(g)^t \varphi)(v) \implies \rho(gh)^t = \rho(h)^t \rho(g)^t$$

DEF 1.18

Given a representation  $\rho, \rho^* : G \rightarrow \text{GL}(V^*)$  by  $g \mapsto \rho(g^{-1})^t$  is called the *dual representation*.

PROP 1.7

$$\chi_{\rho^*} = \overline{\chi_{\rho}}$$

PROOF.

If  $g \in G$  has order  $n$ , then  $\rho(g)$  has order  $m|n$ , since  $\rho(g)^n = \rho(g^n) = \rho(1) = I$ . Hence, in a certain basis,

$$\rho(g) = \begin{pmatrix} \xi_1 & & & \\ & \xi_2 & & \\ & & \ddots & \\ & & & \xi_n \end{pmatrix} \quad \text{where} \quad \xi_i^m = 1$$

If  $\xi$  is a root of unity,  
 $\xi \bar{\xi} = 1$  (try viewing  
 this geometrically)

It follows that

$$\rho(g^{-1}) = \begin{pmatrix} \xi_1^{-1} & & \\ & \ddots & \\ & & \xi_n^{-1} \end{pmatrix} = \begin{pmatrix} \bar{\xi}_1 & & \\ & \ddots & \\ & & \bar{\xi}_n \end{pmatrix}$$

Thus,  $\text{tr}(\rho^*(g)) = \text{tr}(\rho(g^{-1})^t) = \text{tr}(\rho(g^{-1})) = \overline{\text{tr}(\rho(g))}$ , using [Prop 1.2](#).  $\square$

## 1-DIM REPRESENTATIONS

A **1-dim representation**  $(\rho, V)$  is a representation with  $\dim(V) = 1$ . In this case, as  $V$  is a  $\mathbb{C}$ -vector space and  $\rho(g) \in \text{GL}(V)$ , we write  $V = \mathbb{C}^\times$ . Also observe that  $\chi_\rho = \rho$ .

DEF 1.19

$G^* = \text{Hom}(G, \mathbb{C}^\times)$ , as groups, is called the **group of multiplicative characters**.

DEF 1.20

If  $G$  is a finite, abelian group, then every irreducible representation has dimension 1.

PROP 1.8

See MATH 457.  $\square$

PROOF.

$$(G^{ab})^* \cong G^*$$

PROP 1.9

If  $f \in (G^{ab})^*$  is a homomorphism  $f : G^{ab} \rightarrow \mathbb{C}^\times$ , then  $f \circ \pi : G \twoheadrightarrow G/N \rightarrow \mathbb{C}^\times$  is also a homomorphism. Conversely, any  $F : G \rightarrow \mathbb{C}^\times$  must factor uniquely into  $f \circ \pi$  by [Thm 1.1](#), where  $f : G^{ab} \rightarrow \mathbb{C}^\times$ . See the following diagram:

PROOF.

$$\begin{array}{ccc} G & \xrightarrow{F} & \mathbb{C}^\times \\ & \searrow \pi \quad \nearrow f & \\ & G^{ab} & \end{array}$$

## TENSOR REPRESENTATIONS

If  $\rho$  is a finite representation of  $G$  and  $\tau$  is a 1-dim representation, we can generate a new representation

$$\rho \otimes \tau : G \rightarrow \text{GL}(V \otimes_{\mathbb{C}} \mathbb{C}) \cong \text{GL}(V) : g \mapsto \tau(g) \otimes \rho(g)$$

Note that  $\tau(g) \in \mathbb{C}^\times$ , so  $\chi_{\rho \otimes \tau} = \tau \chi_\rho$ .

In generality, given two representations  $\rho_1, \rho_2$ , we generate the tensor product representation  $\rho_1 \otimes \rho_2$  over  $V_1 \otimes_{\mathbb{C}} V_2$ , with dimension  $\dim(V_1) \dim(V_2)$  and trace  $\chi_{\rho_1} \chi_{\rho_2}$ .

## Irreducible Representations

Let  $(\rho, V)$  be a representation. It is called an **irreducible representation** if there are no  $G$ -stable, nontrivial subspaces of  $V$  (i.e. no nontrivial subrepresentations). In the language of modules, irreducible representations are simple  $\mathbb{C}[G]$ -modules.

DEF 1.21



### Theorem 1.3 Semi-Simplicity of Representations

Every finite dimensional, non-zero representation of  $G$  is a direct sum of irreducible representations.

This is "Maschke's Theorem" without uniqueness

PROOF.

Pick any Hermitian inner product  $\langle \cdot, \cdot \rangle$  on  $V$ . Define

$$\langle u, v \rangle^* = \frac{1}{|G|} \sum_{g \in G} \langle gu, gv \rangle$$

It can be easily verified that  $\langle \cdot, \cdot \rangle^*$  is an inner product which is  $G$ -equivariant. If  $W \subseteq V$  is a subrepresentation, then set  $W^\perp = \{u : \langle u, v \rangle = 0 \ \forall v \in W\}$ , i.e. the orthogonal complement of  $W$  with respect to  $\langle \cdot, \cdot \rangle^*$ . It follows that  $V = W \oplus W^\perp$ , with  $W^\perp$  being  $G$ -stable by the  $G$ -equivariance of the inner product.

We then argue by induction to yield a direct sum of irreducible representations. See **MATH 457** for more details on semi-simplicity.  $\square$

Based on this proof, we see that  $\rho(g)$  is unitary. One necessary and sufficient condition for a transformation to be unitary is the existence of an inner product  $\langle \cdot, \cdot \rangle^*$  with  $\langle Tv, Tw \rangle^* = \langle v, w \rangle^*$ . Unitary matrices are interesting for the following reasons:

- $\overline{\rho(g)}^t = \rho(g)^{-1} = \rho(g^{-1})$
- $\rho(g)$  is diagonalizable. With  $g^n = 1$ , we must be able to write  $\rho(g)$  with roots of unity on the diagonal and zeros otherwise. In particular, the  $i$ -th diagonal element is  $\xi_i$ , where  $\xi_i^{m_i} = 1, m_i | n$ .

### SCHUR'S LEMMA

In this section, we will build up the intuition necessary for proving Schur's Lemma.

1/9/26

DEF 1.22

Let  $(\rho, V)$  be a representation. Let  $V^G = \{v : \rho(g)(v) = v : \forall g \in G\}$  be the space of **invariant vectors**. Notice that  $V^G$  is a subrepresentation of  $V$  equivalent to  $\underbrace{1 \oplus \dots \oplus 1}_{\dim(V^G) \text{ times}}$ .

Recall that  $1$  denotes the trivial representation.

PROP 1.10

$$\dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)$$

PROOF.

Let  $\pi : v \mapsto \frac{1}{|G|} \sum_{g \in G} \rho(g)(v)$ . Writing  $\rho(h)\pi = \frac{1}{|G|} \sum_{g \in G} \rho(hg) = \frac{1}{|G|} \sum_{g \in G} \rho(g)$  verifies that  $\text{Im}(\pi) \subseteq V^G$ . It is also easy to verify that  $\pi|_{V^G} = \text{Id}_{V^G}$ . Hence, we may write  $V = \ker(\pi) \oplus V^G$ . It follows that, in some basis,

$$\pi = \begin{pmatrix} 0 & 0 \\ 0 & I_{\dim(V^G)} \end{pmatrix}$$

$$\text{and thus } \text{tr}(\pi) = \dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g). \quad \square$$

Let  $(\rho_1, V_1), (\rho_2, V_2)$  be two representations. Consider

$$\text{Hom}_{\mathbb{C}}(V_1, V_2) = \{T : V_1 \rightarrow V_2 \text{ with } T \text{ } \mathbb{C}\text{-linear}\}$$

This is a  $\mathbb{C}$ -vector space of dimension  $\dim(V_1)\dim(V_2)$ . Similarly, we consider

$$\text{Hom}_G(V_1, V_2) = \{T : V_1 \rightarrow V_2 \text{ with } T\rho_1(g) = \rho_2(g)T\}$$

DEF 1.23

It is often more natural to think of  $\text{Hom}_G(V_1, V_2)$  as transformations which satisfy  $T(gv) = gT(v) \forall v \in V_1$ , noting the distinct actions of  $g$  on  $V_1$  and  $V_2$ , respectively.

Over the vector space  $\text{Hom}_{\mathbb{C}}(V_1, V_2)$ ,  $\rho : g \mapsto [T \mapsto \rho_2(g^{-1})T\rho_1(g)]$  is a  $G$ -representation.

PROP 1.11

Clearly  $\rho_2(g^{-1})T\rho_1(g) \in \text{Hom}_{\mathbb{C}}(V_1, V_2)$ . Also note

$$\rho_2((gh)^{-1})T\rho_1(gh) = \rho_2(h^{-1})\rho_2(g^{-1})T\rho_1(g)\rho_2(h)$$

so  $\rho(gh) = \rho(g)\rho(h)$ . □

PROOF.

$$\text{Hom}_G(V_1, V_2) = (\text{Hom}_{\mathbb{C}}(V_1, V_2))^G$$

PROP 1.12

Let  $T \in (\text{Hom}_{\mathbb{C}}(V_1, V_2))^G$ . Let  $g \in G$ . Then

$$gT = T \implies \rho_2(g^{-1})T\rho_1(g) = T \implies T\rho_1(g) = \rho_2(g)T \quad \square$$

PROOF.

$\text{Hom}_{\mathbb{C}}(V_1, V_2) \cong V_1^* \otimes V_2$  as vector spaces and as  $G$ -representations.

PROP 1.13

$$\dim(\text{Hom}_G(V_1, V_2)) = \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)}$$

PROP 1.14

$$\begin{aligned} \dim(\text{Hom}_G(V_1, V_2)) &= \dim(\text{Hom}_{\mathbb{C}}(V_1, V_2)^G) = \dim((V_1^* \otimes V_2)^G) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{\rho_1^* \otimes \rho_2}(g) = \frac{1}{|G|} \sum_{g \in G} \chi_{\rho_1^*}(g) \chi_{\rho_2}(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_{\rho_1}(g)} \chi_{\rho_2}(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{\rho_1}(g) \overline{\chi_{\rho_2}(g)} \end{aligned}$$

PROOF.

In the last step, we use the fact that the dimension is always real, so  $\overline{\dim} = \dim$ . □

**Eg. 1.4** Let  $G = S_n$ ,  $V = \mathbb{C}^n$ , and let  $\rho$  be the standard representation (i.e. permuting indices). Then  $V^G = \{\langle x, \dots, x \rangle : x \in \mathbb{C}\}$ . This implies that

$$1 = \dim(V^G) = \frac{1}{|G|} \sum_{\sigma \in S_n} \chi_{\rho}(\sigma) \quad \text{Prop 1.10}$$

But the trace of  $\rho(\sigma)$  is exactly the number of fixed points of  $\sigma$ . To see this,

note that  $\sigma$  permutes  $i \rightarrow j$  if the  $i^{\text{th}}$  row is equal to  $e_j$ . Hence

$$1 = \frac{1}{n!} \sum_{\sigma \in S_n} \# \text{FP of } \sigma$$

On average, then, a random permutation has 1 fixed point.

#### Theorem 1.4 Schur's Lemma

Let  $(\rho, V), (\tau, W)$  be irreducible representations of  $G$ . Then

$$\text{Hom}_G(V, W) \cong \begin{cases} \mathbb{C} & \rho \cong \tau \\ 0 & \rho \not\cong \tau \end{cases}$$

PROOF.

We claim that any nonzero  $T \in \text{Hom}_G(V, W)$  is an isomorphism.

$\ker(T)$  and  $\text{Im}(T)$  are subrepresentations of  $\rho$  and  $\tau$ , respectively. Since both  $\rho$  and  $\tau$  are irreducible, it follows that  $\ker(T) = V \vee 0$ , and  $\text{Im}(T) = W \vee 0$ .

$\ker(T) = 0$ , since  $T$  is nonzero.  $\text{Im}(T) \neq 0$  for the same reason, so  $\text{Im}(T) = W$ . It follows that  $T$  is an isomorphism. Immediately,  $\text{Hom}_G(V, W) = 0$  when  $\rho \neq \tau$ .

Suppose  $\rho \cong \tau$ . We can write  $\text{Hom}_G(V, W) = \text{End}_G(V)$ . Let  $T \in \text{End}_G(V)$  be nonzero. Let  $\lambda$  be some eigenvalue of  $T$  with corresponding eigenspace  $U_\lambda \subseteq V$ . Then

$$T(gu) = g(Tu) = g(\lambda u) = \lambda gu \quad \forall u \in U, g \in G$$

It follows that  $gu \in U_\lambda$ . Hence,  $U_\lambda$  is a  $G$ -stable subspace, and hence a subrepresentation. By irreducibility,  $U_\lambda = V$ , so  $T = \lambda$ .

By this argument, we can map  $T \mapsto \lambda_T = \text{tr}(T)/\dim(V) \in \mathbb{C}$ . The converse map  $\lambda \mapsto \lambda I$  completes the proof. The well-structuredness of this map derives from the fact that

$$\frac{\text{tr}(T + G)}{\dim(V)} = \frac{\text{tr}(T)}{\dim(V)} + \frac{\text{tr}(G)}{\dim(V)}$$

□

Equivalently, the kernel and image of a homomorphism of modules are submodules

#### Class Functions

DEF 1.24 A function  $f : G \rightarrow \mathbb{C}$  is called a **class function** if  $f(hgh^{-1}) = f(g)$ . In other words,  $f$  is constant on each conjugacy class of  $G$ .

We will denote by  $h(G)$  the number of conjugacy classes of  $G$ . Similarly,

DEF 1.25  $\text{Class}(G) = \{f : f \text{ is a class function on } G\}$

Note that  $\text{Class}(G)$  is a  $\mathbb{C}$ -vector space with dimension  $h(G)$ .

Its basis consists of functions that are the identity on each class, and zero elsewhere

**Eg. 1.5** If  $G$  is abelian, then  $h(G) = |G|$ .

**Eg. 1.6**  $h(S_n)$  is the number of permutations of  $n$ .

We can endow  $\text{Class}(G)$  with the inner product

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

Note also that  $\chi_\rho$  is a class function. For the following theorems and propositions, we will denote by  $(p_1, V_1), \dots, (p_n, V_n)$  the irreducible representations of  $G$ , along with their dimensions  $d_i$  and characters  $\lambda_i$  for  $i \in [n]$ .

**Theorem 1.5 Irreducible Characters Form Orthonormal Basis of  $\text{Class}(G)$**

Up to isomorphism, the irreducible characters of  $G$  form an orthonormal basis for  $\text{Class}(G)$ . We conclude that  $\#h(G) = \#\text{irreducible representations of } G$ .

Let  $\sigma, \tau$  be irreducible representations. We do not distinguish between  $\sigma, \tau$  and their associated vector spaces. Then, by Schur's Lemma ([Thm 1.4](#)) and [Prop 1.14](#),

PROOF.

$$\delta_{\sigma, \tau} = \dim(\text{Hom}_{\mathbb{C}}(\sigma, \tau)^G) = \frac{1}{|G|} \sum_{g \in G} \chi_\sigma(g) \overline{\chi_\tau(g)} = \langle \chi_\sigma, \chi_\tau \rangle$$

From this, we conclude that the irreducible characters are orthonormal in  $\text{Class}(G)$ . It remains to show that they are a basis. From linear algebra (see [MATH 251](#)), we recall the criterion

$$\langle \chi_i, \beta \rangle = 0 \quad \forall i \in [n] \implies \beta \in \text{Class}(G)^\perp \equiv 0$$

This ensures that Fourier coefficients always exist using the irreducible characters provided, which establishes spanning-ness. Let  $\alpha \in \text{Class}(G) : G \rightarrow \mathbb{C}$ . Consider

$$A_\rho = \sum_{g \in G} \alpha(g) \rho(g) \in \text{End}_{\mathbb{C}}(V)$$

We claim that  $A_\rho \in \text{End}_G(V)$ . Write

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

We claim that, if  $\alpha = \overline{\beta}$ , with  $\rho$  irreducible, then  $A_\rho = 0$ . Schur's Lemma gives the map

$$\text{End}_G(V) \rightarrow \mathbb{C} : T \mapsto \frac{\text{tr}(T)}{\dim(\rho)}$$

Which we apply to  $A_\rho$

$$A_\rho \mapsto \frac{\text{tr}(\sum_{g \in G} \alpha(g) \rho(g))}{\dim(\rho)} = \frac{|G|}{\dim(\rho)} \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \beta(g) = \frac{|G|}{\dim(\rho)} \langle \chi_\rho, \beta \rangle = 0$$

This holds for any irreducible representation, so, in particular,  $A_{\rho_i} \forall i \in [n]$ . It must also hold for the regular representation. Hence,  $A_{\rho^{\text{reg}}} = 0$  on  $\text{End}_G(\mathbb{C}[G])$ . Consider  $\mathbb{1}_G$ . Then we must have

$$\sum_{g \in G} \alpha(g) \rho^{\text{reg}}(g)(\mathbb{1}_G) = \sum_{g \in G} \alpha(g)[g] = 0$$

Since  $[g] : g \in G$  is a basis for  $\mathbb{C}[G]$ , it must be that  $\alpha(g) = 0 \forall g \in G$ . As  $\alpha = \bar{\beta}$ , the result follows.  $\square$

### Theorem 1.6 Mascke's Theorem

If  $(\rho, V)$  is a representation of  $G$ , then it has a unique decomposition

$$\rho \cong \rho_1^{a_1} \oplus \cdots \oplus \rho_n^{a_n} V \psi$$

where  $a_i = \langle \lambda_\rho, \lambda_i \rangle$ .

PROOF.

Letting  $a_i$  be as in [Thm 1.3](#), we know  $\chi_\rho = \sum_{i=1}^n a_i \lambda_i$ . It remains to show that  $a_i$  are unique. But we can compute

$$\langle \chi_\rho, \chi_i \rangle = \sum_{j=1}^n a_j \underbrace{\langle \chi_j, \chi_i \rangle}_{\delta_{ij} \text{ by } \text{Thm 1.5}} = a_i$$

**PROP 1.15**  $\rho \cong \tau \iff \chi_\rho = \chi_\tau$

PROOF.

We only need to consider the  $(\Leftarrow)$  direction. In this case, we write

$$\langle \chi_\rho, \chi_i \rangle = \langle \chi_\tau, \chi_i \rangle \forall i$$

But these are the multiplicities of the irreducible characters in  $\rho$  and  $\tau$ , so  $\rho \cong \tau$ .  $\square$

**PROP 1.16** Let  $\rho^{\text{reg}}$  be the regular representation of  $G$  on  $\mathbb{C}[G]$ . We have

$$\rho^{\text{reg}} \cong \rho_1^{d_1} \oplus \cdots \oplus \rho_n^{d_n}$$

Consequently,  $|G| = \sum_{i=1}^n d_i^2$ .

PROOF.

$$\langle \chi^{\text{reg}}, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi^{\text{reg}}(g) \overline{\chi_i(g)} = \frac{1}{|G|} |G| \chi_i(1) = d_i$$

□

$\rho$  is irreducible  $\iff \|\chi_\rho\|^2 = 1$ . Similarly,  $\rho$  is the direct sum of two irreducible representations  $\iff \|\chi_\rho\|^2 = 2$ .

PROP 1.17

We know  $\|\chi_\rho\|^2 = \sum_{i=1}^h a_i^2$ , where  $a_i$  is the multiplicity of the  $i$ -th irreducible representation in  $\rho$ 's decomposition. Recall

PROOF.

$$\begin{aligned} \|\chi_\rho\|^2 &= \langle \chi_\rho, \chi_\rho \rangle = \langle a_1 \chi_1 + \dots + a_h \chi_h, a_1 \chi_1 + \dots + a_h \chi_h \rangle \\ &= \sum_{i=1}^h \langle a_i \chi_i, a_1 \chi_1 + \dots + a_h \chi_h \rangle \\ &= \sum_{i=1}^h a_i^2 \langle \chi_i, \chi_i \rangle = \sum_{i=1}^h a_i^2 \end{aligned}$$

It follows that  $\|\chi_\rho\|^2 = 1$  if and only if exactly one of  $a_i^2 = 1$ , i.e.  $\chi_\rho$  is irreducible. If  $\|\chi_\rho\|^2 = 2$ , we must have some  $i \neq j$  with  $a_i^2 = a_j^2 = 1$ , and so  $\rho = \rho_i \otimes \rho_j$ , where  $\rho_i, \rho_j$  are irreducible. □

**Eg. 1.7** Consider  $S_n : n \geq 2$ . We consider  $\rho^{\text{std}}$ , the natural action of  $S_n$  on a set of  $n$  elements (e.g. permuting the indices of  $v \in \mathbb{C}^n$ ). Recall [Example 1.4](#), where we derived

$$1 = \frac{1}{n!} \sum_{\sigma \in S_n} \chi^{\text{std}}(\sigma) = \frac{1}{n!} \sum_{\sigma \in S_n} \# \text{FP of } \sigma$$

But also

$$\|\chi^{\text{std}}\|^2 = \frac{1}{n!} \sum_{\sigma \in S_n} (\chi^{\text{std}}(\sigma))^2 = \frac{1}{n!} \sum_{\sigma \in S_n} (\# \text{FP of } \sigma)^2$$

To analyze this equation, we define an action of  $S_n$  on  $[n]^2$ , which sends  $\sigma(i, j) = (\sigma(i), \sigma(j))$ . We observe exactly 2 orbits under this action:  $\{(i, i) : i \in [n]\}$  and  $\{(i, j) : i \neq j \in [n]\}$ . By Burnside's Lemma,

$$2 = \frac{1}{n!} \sum_{\sigma \in S_n} (\# \text{FP of } \sigma \text{ on } [n]^2)$$

Observe that,  $\sigma$  has a fixed point  $(k, \ell) \in F$  on  $[n]^2$  if and only if it is fixed on each coordinate of each fixed point. In this way, we have a  $n - to - n^2$  mapping, and conclude that  $\|\chi^{\text{std}}\|^2 = 2$ .

Note that the trivial representation is a  $G$ -stable subrepresentation of  $\rho^{\text{std}}$ . By "subtracting"  $\mathbb{1}$  from  $\rho^{\text{std}}$  we can recover the other irreducible representation implied by the computation above, which we denote by  $\rho^{\text{std},0}$ . In particular

$$\rho^{\text{std}} = \mathbb{1} \oplus \rho^{\text{std},0}$$

**PROP 1.18** Every irreducible representation of an abelian group is one dimensional.

PROOF.

As  $G$  is abelian,  $h = |G|$ . Then,  $|G| = \sum_{i=1}^{|G|} d_i^2$ , from which we conclude  $d_i = 1 \ \forall i$ .  $\square$

### Character Tables

We'll fire off a few propositions that follow immediately from the work we've done on class functions.  $\sum_{i=1}^n d_i \chi_i = \chi_{\text{reg}}$  (recall [Def 1.13](#))

**PROP 1.19**

PROOF.

Follows immediately from [Prop 1.19](#).  $\square$

**PROP 1.20**

Let  $\chi$  be irreducible. Let  $C_1, \dots, C_n$  be conjugacy classes. Then  $\sum_{i=1}^n \chi(C_i)|C_i| = \begin{cases} 0 & \chi \neq \mathbb{1} \\ |G| & \chi = \mathbb{1} \end{cases}$ .  
By  $\chi(C_i)$ , we mean the representation evaluated on any element in  $C_i$ .

Recall that the number of conjugacy classes and irreducible representations are the same, i.e.  $n$

PROOF.

Note that  $\chi_{\mathbb{1}}(g) = 1 \ \forall g \in G$ . Hence,

$$\sum_{i=1}^n \chi(C_i)|C_i| = \sum_{g \in G} \chi(g) \overline{\chi_{\mathbb{1}}(g)} = |G| \langle \chi, \chi_{\mathbb{1}} \rangle$$

$\square$

**PROP 1.21**

The number of 1-dim irreducible representations is equal to  $|G^{ab}|$ .

PROOF.

Observe that  $G^* = \text{Hom}(G, C^\times) \cong \text{Hom}(G^{ab}, C^\times)$  by [Thm 1.1](#). But, in homework, we proved  $\text{Hom}(G^{ab}, C^\times) \cong G^{ab}$  (in particular, for any finite, abelian group).  $\square$

**PROP 1.22**

The inner product of character table rows, weighted by class size, is 0, unless the rows are equal, in which case it is  $|G|$ . Similarly, the inner product of character table columns is 0, unless the rows are equal, in which case it is  $\frac{|G|}{|C_i|}$ .

PROOF.

For rows:  $\sum_{i=1}^n \chi_i(C_k) \overline{\chi_j(C_k)} |C_k| = \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = |G| \langle \chi_i, \chi_j \rangle$ .

For columns, see MATH 457.  $\square$

**PROP 1.23**

DEF 1.26

If  $\dim(\chi_i) = 1$ , then  $\forall j \in [n]$ ,  $\chi_i \chi_j$  is also an irreducible character. We call this *twisting*.

$\chi_i \chi_j$  refers to the character  $\chi_{\rho_i \otimes \rho_j}$ . We use the criterion outlined in [Prop 1.20](#).

PROOF.

$$\|\chi_i \chi_j\|^2 = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_i(g)} \chi_j(g) \overline{\chi_j(g)} = \|\chi_j\|^2 = 1$$

Observing that  $\chi_i(g) \in \mathbb{C}^\times$  is a root of unity, and therefore  $\overline{\chi_i(g)} = \chi_i(g)^{-1} = \chi_i(g^{-1})$ . We conclude that  $\chi_i \chi_j$  is irreducible.  $\square$

We define  $\ker(\chi) = \{g : \chi(g) = \chi(1)\}$ . Recall  $\chi(1) = \dim(V)$ .

$\ker(\chi_\rho) = \ker(\rho)$ , where  $\rho$  is not necessarily irreducible.

PROP 1.24

With  $g^n = 1$ , recall that we can write

PROOF.

$$\rho(g) = \begin{pmatrix} \xi_1 & & \\ & \ddots & \\ & & \xi_d \end{pmatrix} \quad \xi_i^n = 1$$

Then,  $\chi(g) = d \iff \rho(g) = I_d \iff g \in \ker(\rho)$ .  $\square$

Let  $\rho$  be a representation with a decomposition into irreducible characters  $\chi_\rho = \sum_{i \in I} a_i \chi_i$ ,  $a_i > 0$ . Then  $\ker(\chi_\rho) = \bigcap_{i \in I} \ker(\chi_i)$ .

PROP 1.25

$g \in \ker(\chi) \iff \rho(g) = I_{\dim(\rho)} \forall i \in I \iff \rho_i(g) = I_{d_i} \iff g \in \ker(\chi_i) \forall i \in I$ . For the middle if-and-only-if, note that, as a direct sum of irreducible representations, we may write  $\rho(g)$ 's matrix as  $a_i$  diagonally-adjacent block matrices of  $\rho_i(g)$ , for each  $i \in I$ .  $\square$

PROOF.

For any  $N \triangleleft G$ , we have  $N = \ker(\chi)$  for some representation  $\chi$ .

PROP 1.26

Let  $\sigma$  be the composition of maps

PROOF.

$$G \xrightarrow{\pi} G/N \xrightarrow{\rho_{\text{reg}}} \text{GL}(\mathbb{C}[G/N])$$

Then  $\sigma$  is a representation, and  $\ker(\pi) = N$ . But  $\rho_{\text{reg}}(g)$  is faithful, i.e only the identity when  $g = 1$ . We conclude that  $\ker(\sigma) = N$ , so  $\ker(\chi_\sigma) = N$ .  $\square$

### Theorem 1.7 Normal Subgroups and Characters

Let  $N_i = \ker(\chi_i) : i \in [n]$ . Then, for any  $I \subseteq [n]$ , we have

$$N_I := \bigcap_{i \in I} N_i$$

is a normal subgroup of  $G$ . Furthermore, for any  $N \triangleleft G$ , there is some index set  $I \subseteq [n]$  for which  $N = N_I$ .



PROOF.

Since  $N_i = \ker(\rho_i)$ , we know that  $N_i \triangleleft G$ . Thus,  $N_I = \cap_{i \in I} N_i$  is also normal. Finally, if  $N \triangleleft G$ , then by [Prop 1.29](#),  $N = \ker(\chi)$  for some representation  $\chi$ . By [Prop 1.28](#), we can write  $N = \cap_{i \in I} \ker(\chi_i)$ , where  $\rho = \oplus_{i \in I} \rho^{a_i}$ .  $\square$

Recall that  $\rho_i : G \rightarrow \text{GL}(V_i)$  is a homomorphism

### Induced Representations

Let  $H < G$ , and let  $(\rho, \chi, V)$  be a representation of  $H$ . Recall the induced representation, [Def 1.15](#),  $\text{Ind}_H^G(\rho) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ . We wish to study its character, denoted by  $\text{Ind}_H^G(\chi)$ .

Let  $g_1, \dots, g_d$  be the coset representations for  $H$ , where  $d = [G : H]$ . In particular, we can write  $G = \sqcup_{i \in [d]} g_i H$ , and thus  $\mathbb{C}[G] = \oplus_{i \in [d]} [g_i] \mathbb{C}[H]$ . Then

$$\text{Ind}_H^G(\rho) = \left( \oplus_{i \in [d]} [g_i] \mathbb{C}[H] \right) \otimes_{\mathbb{C}[H]} V = \oplus_{i \in [d]} \left( [g_i] \mathbb{C}[H] \otimes_{\mathbb{C}[H]} V \right) = \oplus_{i \in [d]} ([g_i] \otimes_{\mathbb{C}[H]} V)$$

Given  $g \in G$ , how does  $\text{Ind}_H^G(\rho)$  act? We first write  $gg_i = g_j h$  for some unique coset representative  $g_j$  and  $h \in H$ . Then,  $\forall v \in V$ ,

$$g([g_i] \otimes v) = (g \otimes 1)([g_i] \otimes v) = [gg_i] \otimes v = [g_j h] \otimes v$$

From here on out, we will drop the  $[\cdot]$  notation. Now, viewing  $\rho$  as a  $\mathbb{C}[H]$ -module, and using the balancing property of tensor products,  $g_j h \otimes v = g_j \otimes hv$ , where  $hv = \rho(h)(v)$ :

$$g(g_i \otimes v) = g_j \otimes \rho(h)(v)$$

At this point, we let  $\hbar(g, i)$  be element  $h \in H$  that satisfies  $gg_i = g_j h = g_j \hbar(g, i)$ . Similarly, we let  $\delta(g, i)$  be  $g_j \in G$  such that  $gg_i = \delta(g, i) \hbar(g, i)$ .

In  $\text{Ind}_H^G(\rho)$ , we have

$$g(g_1 \otimes v_{i_1}, \dots, g_d \otimes v_{i_d}) = (\delta(g, 1) \otimes \rho(\hbar(g, 1))(v_1), \dots, \delta(g, d) \otimes \rho(\hbar(g, d))(v_d))$$

$\delta(g, i) : i \in [d]$  permutes the basis vectors  $g_1, \dots, g_d$ . Hence,  $\text{Ind}_H^G(\rho)(g)$ , in some suitable basis, can be thought of as a set of block matrices  $\{\rho(\hbar(g, i)) : i \in [d]\}$ , positioned accordingly in columns  $i \in [d]$ . However, to account for the permutation  $\delta(g, i)$ , the block matrix  $\rho(\hbar(g, i))$  is placed in the  $\delta(g, i)$ -th row, or rather the  $k$ -th column, where  $g_k = \delta(g, i)$ .

This block contributes to the trace if and only if  $\delta(g, i)$  corresponds to the  $i$ -th basis vector, i.e.  $\iff gg_i = g_i \hbar(g, i) \iff g_i^{-1} gg_i \in H$ . In this case, the trace contributed is equal to  $\chi(\hbar(g, i)) = \chi(g_i^{-1} gg_i)$ . In short, then, we have the following result:

#### Theorem 1.8 Character of the Induced Representation

$$\text{Ind}_H^G(\chi)(g) = \sum_{g_i: g_i^{-1} gg_i \in H} \chi(g_i^{-1} gg_i)$$

See above discussion. □

PROOF.

This lends itself to some simplifications. We adopt the notation  $\dot{\chi}(g) = \begin{cases} \chi(g) & g \in H \\ 0 & \text{o.w.} \end{cases}$ .

$$\text{Ind}_H^G(\chi)(g) = \frac{1}{|H|} \sum_{b \in G} \dot{\chi}(b^{-1}gb)$$

PROP 1.27

$\text{Ind}_H^G(\chi)(g) = \sum_{i \in [d]} \dot{\chi}(g_i^{-1}gg_i)$ . Let  $h \in H$ . Then  $(g_i h)^{-1}g(g_i h) = h^{-1}(g_i^{-1}gg_i)h$ . But  $\chi$  is a class function, so  $\chi(h^{-1}(g_i^{-1}gg_i)h) = \chi(g_i^{-1}gg_i)$ . As  $g_i$  are coset representatives,

PROOF.

$$\frac{1}{|H|} \sum_{b \in g_i H} \dot{\chi}(b^{-1}gb) = \dot{\chi}(g_i^{-1}gg_i)$$

Then, summing over cosets gives the result. □

When  $H \triangleleft G$ ,

PROP 1.28

$$\text{Ind}_H^G(\chi)(g) = \begin{cases} \frac{1}{|H|} \sum_{b \in G} \chi(b^{-1}gb) & g \in H \\ 0 & g \notin H \end{cases}$$

Since  $H$  is normal,  $b^{-1}gb \in H \iff g \in H$ . It follows that  $\dot{\chi}(b^{-1}gb) = \chi(b^{-1}gb)$  when  $g \in H$ . On the other hand, we have  $g \notin H \iff b^{-1}gb \notin H$ , so  $\dot{\chi}(b^{-1}gb) = 0$  when  $g \notin H$ . □

PROOF.

### Theorem 1.9 Frobenius Reciprocity

Let  $H < G$ . Denote by  $\langle \cdot, \cdot \rangle_H$  and  $\langle \cdot, \cdot \rangle_G$  the usual inner products on  $\text{Class}(H)$  and  $\text{Class}(G)$ , respectively. Let  $\eta$  and  $\gamma$  be representations of  $H$  and  $G$ , respectively. Then

$$\langle \text{Ind}_H^G(\eta), \gamma \rangle_G = \langle \eta, \text{Res}_H^G(\gamma) \rangle_H$$

PROOF.

$$\begin{aligned}
\langle \text{Ind}_H^G(\eta), \gamma \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \text{Ind}(\eta)(g) \overline{\gamma(g)} = \frac{1}{|G|} \sum_{g \in G} \sum_{b \in G} \frac{1}{|H|} \eta(b^{-1}gb) \overline{\gamma(g)} \\
&= \frac{1}{|G| \cdot |H|} \sum_{g, b: b^{-1}gb = t \in H} \eta(t) \overline{\gamma(bt b^{-1})} \\
&= \frac{1}{|G| \cdot |H|} \sum_{t \in H} \sum_{b \in G} \eta(t) \overline{\gamma(bt b^{-1})} = \frac{1}{|G|} \sum_{t \in H} \eta(t) \overline{\gamma(t)} \\
&= \langle \eta, \text{Res}_H^G(\gamma) \rangle_H \quad \square
\end{aligned}$$

**Eg. 1.8** Let  $H = \{1\}$  and  $\eta = \chi_{\text{triv}}$ . Then  $\text{Ind}_H^G(\eta) = \chi_{\text{reg}}$ . Let  $\chi$  be irreducible on  $G$ . By the theorem above,

$$\langle \chi_{\text{reg}}, \chi \rangle_G = \langle \chi_{\text{triv}}, \sigma \rangle_H = \dim(\chi)$$

where  $\sigma$  is a  $\dim(\chi)$ -identity matrix on  $H = \{1\}$ . At the same time, we know that  $\langle \chi_{\text{reg}}, \chi \rangle_G$  is the multiplicity of  $\chi$  in  $\chi_{\text{reg}}$ . But this is exactly consistent with what we found.

## Supersolvable Groups

DEF 1.27 We say that  $G$  is *solvable* if there exists a chain

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_N = \{1\}$$

with  $G_{i+1} \triangleleft G_i$  and  $G_i/G_{i+1}$  abelian. We may assume that  $G_i/G_{i+1}$  is cyclic of prime order.

PROOF.

Refine the chain until no normal subgroups can be inserted. In other words, if there exists  $H : G_{i+1} \triangleleft H \triangleleft G_i$ , insert this into the chain. Once this is complete, it must be that  $G_i/G_{i+1}$  is simple. Suppose not, and let  $H \triangleleft G_i/G_{i+1}$ . Consider the following:



The preimage under a homomorphism of a normal subgroup is also normal. This contradicts the refinement of the chain. It is well-known that the only simple abelian

groups are prime and cyclic. Hence,  $G_i/G_{i+1}$  are assumed to be so.  $\square$

We say that  $G$  is *supersolvable* if there exists a chain

DEF 1.28

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_N = \{1\}$$

with  $G_i \triangleleft G$  and  $G_i/G_{i+1}$  cyclic. As before, we may assume that  $G_i/G_{i+1}$  has prime order.

The following are properties of supersolvable groups:

PROP 1.29

1. If  $G$  is supersolvable, then so is  $H < G$
2. If  $G$  is supersolvable, and  $G \twoheadrightarrow H$  is surjective, then so is  $H$
3. If  $G$  is a  $p$ -group, then it is supersolvable
4. If  $G_1, G_2$  are both supersolvable, then so is  $G_1 \oplus G_2$ .

### Theorem 1.10 Blichfeldt's Lemma

Let  $G$  be a finite, non-abelian supersolvable group. Then there exists  $N \triangleleft G$ , with  $N$  abelian but  $N \not\subseteq Z(G)$ .

Since  $G$  is non-abelian, we know  $G_0 = G \not\subseteq Z(G)$ . But it is true that  $G_N = \{1\} \subseteq Z(G)$ . Hence, there must be some  $G_i$  with  $G_i \not\subseteq Z(G)$  but  $G_{i-1} \subseteq Z(G)$ . It only remains to show that  $N = G_i$  is abelian.

PROOF.

Since  $G_i/G_{i+1}$  is cyclic, we can generate it with  $\langle x \rangle$  for some  $x \in N$ . Then, any element in  $G_i$  can be written as  $x^a y$  for some integer  $a$  and  $y \in G_{i+1}$ .

$$x^{a_1} y_1 x^{a_2} y_2 \stackrel{G_{i-1} \subseteq Z(G)}{=} x^{a_1} x^{a_2} y_1 y_2 = x^{a_2} y_2 x^{a_1} y_1$$

as desired.  $\square$

### Theorem 1.11 Blichfeldt's Theorem

Let  $G$  be a finite, supersolvable group. Let  $(\rho, V)$  be some irreducible representation of  $G$ . Then  $\rho \cong \text{Ind}_H^G(\psi)$  for some subgroup  $H < G$  and 1-dim representation  $\psi$  of  $H$ .

If  $G$  is abelian, we have no work to do.  $\text{Ind}_G^G(\rho) = \rho$  clearly, and for all representations of  $G$ ,  $\rho \in G^*$  is 1-dim. Hence, assume  $G$  is non-abelian. We also assume that  $\rho$  is faithful, i.e. has a trivial kernel, as quotients of supersolvable groups are supersolvable. In particular,  $\rho$  is faithful on  $G/\ker(\rho)$ .

PROOF.

We proceed by induction on  $|G|$ . Let  $N$  be as in [Thm 1.10](#). Then  $V$  can be viewed as a representation of  $N$  via  $\text{Res}_N^G(\rho)$ . As  $N$  is abelian, its irreducible characters are 1-dim. Hence,  $V \cong \bigoplus_{\psi \in N^*} V_\psi$ , where  $V_\psi = \{v \in V : \rho(n)(v) = \psi(v) \ \forall n \in N\}$ .

For any  $\psi \in N^*$  and  $g \in G$ , we define  $\psi^g : N \rightarrow \mathbb{C}^\times : \psi^g(n) = \psi(g^{-1}ng)$ . We claim that

$\rho(g)$  is a map  $V_\psi \rightarrow V_{\psi^g}$ . Let  $v \in V_\psi$ . Then

$$\rho(n)(\rho(g)(v)) = \rho(ng)(v) = \rho(g)(\rho(g^{-1}ng)(v)) = \dots$$

But  $\rho(g^{-1}ng)(v) = \psi(g^{-1}ng)(v) = \psi^g(n)(v)$ , by assumption. As this is a scalar, we can pull it out:

$$\dots = \psi^g(n)\rho(g)(v)$$

Hence,  $\rho(g)(v) \in V_{\psi^g}$ , as claimed. Since we have easy access to the inverse  $\rho(g^{-1})$ , it follows that  $V_\psi \cong V_{\psi^g}$ . Pick any  $\psi \in N^*$  such that  $V^\psi \neq \{0\}$ . Let  $S = \{\psi^g : g \in G\} \subseteq N^*$ .

$$\bigoplus_{\chi \in S} V^\chi \subseteq V \implies \bigoplus_{\chi \in S} V^\chi = V$$

by irreducibility. Then,  $\dim(V) = \#S \dim(V^\psi)$ . In particular, if  $H = \{g \in G : \psi^g = \psi\}$ , then  $\#S = [G : H]$ . We claim that  $\text{Ind}_H^G(V^\psi) \cong \rho$ .

BLAH! □

### Fourier Transforms

Let  $G$  be a finite group. Let  $C(G, \mathbb{C})$  denote the space of functions (with no particular structure)  $f : G \rightarrow \mathbb{C}$ . We can view this as a  $\mathbb{C}$ -vector space equipped with addition and scalar multiplication:

$$(f + g)(s) = f(s) + g(s) \quad f(\alpha s) = \alpha f(s)$$

Under this view,  $C(G, \mathbb{C})$  has a basis  $\{\delta_s : s \in G\}$ , where  $\delta_s(g) = \begin{cases} 1 & g = s \\ 0 & \text{o.w.} \end{cases}$ .

We can also view  $C(G, \mathbb{C})$  through the group ring  $\mathbb{C}[G]$ . In particular, by defining the **convolution** as follows

$$(f * g)(s) = \sum_{t \in G} f(st^{-1})g(t)$$

we see that  $C(G, \mathbb{C}) \cong \mathbb{C}[G]$  by associating

$$\sum_{s \in G} a_s[s] \mapsto f : f(s) = a_s \quad f \mapsto \sum_{s \in G} f(s)[s]$$

We note the addition maps in the usual way:

$$\sum_{s \in G} a_s[s] + \sum_{s \in G} b_s[s] \mapsto f + g : f(s) = a_s, g(s) = b_s$$

And multiplication maps via convolutions:

$$\left( \sum_{s \in G} a_s[s] \right) \left( \sum_{s \in G} b_s[s] \right) = \sum_{s, t \in G \times G} a_s b_t[st] = \sum_{s, t \in G \times G} a_{st^{-1}} b_t[s] \mapsto h : h(s) = \sum_{t \in G} a_{st^{-1}} b_t = (f * g)(s)$$

where  $f \leftrightarrow \sum_{s \in G} a_s[s]$  and  $g \leftrightarrow \sum_{s \in G} b_s[s]$ .

**Theorem 1.12 Properties of Group Convolutions**

1.  $(f * g) * h = f * (g * h)$
2.  $f * (g_1 + g_2) = f * g_1 + f * g_2$
3.  $(g_1 + g_2) * f = g_1 * f + g_2 * f$
4.  $\delta_g * \delta_h = \delta_{gh}$
5. The representation  $\rho$  of  $G$  on  $C(G, \mathbb{C})$  given by  $(bf)(x) = f(b^{-1}x)$  is equivalent to the regular representation  $\rho_{\text{reg}}$  on  $\mathbb{C}[G]$ .

Each of these is established via inheritance from the  $\mathbb{C}[G]$  view (in particular, points 1, 2, and 3 are immediate).

PROOF.

For 4, see that  $\delta_g \mapsto [g]$  in  $\mathbb{C}[G]$ , so we conclude that  $\delta_g * \delta_h \mapsto [gh] \leftarrow \delta_{gh}$ .

For 5,

$$bf \leftrightarrow \sum_{s \in G} (bf)(s)[s] = \sum_{s \in G} f(b^{-1}s)[s] = \sum_{s \in G} f(s)[bs] = [b] \sum_{s \in G} f(s)[s]$$

which is exactly  $\rho(b)(\sum_{s \in G} f(s)[s])$ . □

For  $f \in C(G, \mathbb{C})$ , we define the *Fourier transform*, denoted  $\hat{f}$ , to be a function from representations  $(\rho, V)$  to their endomorphism group  $\text{End}(V)$ , with

DEF 1.30

$$\hat{f}(\rho) = \sum_{s \in G} f(s)\rho(s) \in \text{End}(V)$$

**Theorem 1.13 Properties of Fourier Transforms**

Let  $f, g \in C(G, \mathbb{C})$ . Let  $(\rho, V)$  be a representation. Then

1.  $\widehat{\hat{f} + \hat{g}} = \widehat{\hat{f}} + \widehat{\hat{g}}$  and  $\widehat{\alpha \hat{f}} = \alpha \hat{f}$ .
2.  $\widehat{\delta_s}(\rho) = \rho(s)$
3.  $\widehat{f * g} = \widehat{\hat{f}} \circ \widehat{\hat{g}}$
4. Let  $U \in C(G, \mathbb{C})$  be the uniform probability distribution on  $G$ . Then  $\hat{U}(\rho)$  is a projection from  $V \rightarrow V^G$ . We conclude that  $\hat{U}(\rho_{\text{triv}}) = 1 \in \mathbb{C}^\times$ , and  $\hat{U}(p_i) = 0$  for any irreducible  $\rho_i$ .

1, 2 can be left as an exercise.

PROOF.

For 3, write

$$\begin{aligned}
 \widehat{f * g}(\rho) &= \sum_{s \in G} \left( \sum_{t \in G} f(st^{-1})g(t) \right) \rho(s) \\
 &= \sum_{s \in G} \sum_{t \in G} f(st^{-1})g(t)\rho(s) = \sum_{s \in G} \sum_{t \in G} f(s)g(t)\rho(st) \\
 &= \sum_{s \in G} \sum_{t \in G} f(s)\rho(s)g(t)\rho(t) = \left( \sum_{s \in G} f(s)\rho(s) \right) \left( \sum_{t \in G} g(t)\rho(t) \right) \\
 &= (\hat{f} \circ \hat{g})(\rho)
 \end{aligned}$$

For 4, we see that

$$g\hat{U}(\rho)(v) = g \sum_{s \in G} U(s)\rho(s)(v) = U(1) \sum_{s \in G} \rho(gs)(v) = U(1) \sum_{s \in G} \rho(s)(v) = \hat{U}(\rho)(v)$$

Noting that  $U(g)$  is constant over all  $g \in G$ . Thus,  $\text{Im}(\hat{U}(\rho)) \subseteq V^G$ . Showing  $\hat{U}(\rho)(\hat{U}(\rho)(v)) = \hat{U}(\rho)(v)$  is left as an exercise.

Observe that  $V^G$  under  $\rho_{\text{triv}} = V$ , and thus  $\hat{U}(\rho_{\text{triv}})$  acts as the identity. However,  $\text{Im}(\hat{U}(\rho_i))$ , for any irreducible  $\rho_i$ , forms a non-trivial  $G$ -stable subspace  $V^G$ . Thus,  $\hat{U}(\rho_i)$  must be 0.  $\square$

Note that, if  $f$  is a probability distribution on  $G$ , we can view  $\hat{f}(\rho) = \mathbb{E}[\rho]$ , viewing  $\rho$  as a random variable which takes on values  $\rho(g) : g \in G$ .

### Theorem 1.14 Fourier Inversion and Plancherel

#### Fourier Inversion Formula

$$f(s) = \frac{1}{|G|} \sum_{i=1}^n d_i \text{tr}(\rho_i(s^{-1})\hat{f}(\rho_i))$$

#### Plancherel's Formula

$$\sum_{s \in G} f_1(s^{-1})f_2(s) = \frac{1}{|G|} \sum_{i=1}^n d_i \text{tr}(\hat{f}_1(\rho_i)\hat{f}_2(\rho_i))$$

PROOF.

Note that both sides of the Fourier inversion are linear in  $f$ . Similarly, both sides of Plancherel's formula are bi-linear in  $(f_1, f_2)$ . Thus, it is enough to prove Fourier inversion on  $f = \delta_g$ , and similarly on  $f = \delta_g, g = \delta_h$  for Plancherel. Thus:

Fourier Inversion Formula Recalling that  $\widehat{\delta_g}(\rho) = \rho(g)$ ,

$$\begin{aligned} \frac{1}{|G|} \sum_{i=1}^n d_i \operatorname{tr}(\rho_i(s^{-1}) \widehat{\delta_g}(\rho_i)) &= \frac{1}{|G|} \sum_{i=1}^n d_i \operatorname{tr}(\rho_i(s^{-1}) \rho_i(g)) \\ &= \frac{1}{|G|} \sum_{i=1}^n d_i \chi_i(s^{-1}g) = \frac{1}{|G|} \chi_{\operatorname{reg}}(s^{-1}g) \\ &= \begin{cases} 1 & s = g \\ 0 & \text{o.w.} \end{cases} = \delta_g \end{aligned}$$

Plancherel's Formula

$$\begin{aligned} \frac{1}{|G|} \sum_{i=1}^n d_i \operatorname{tr}(\rho_i(g) \rho_i(h)) &= \frac{1}{|G|} \chi_{\operatorname{reg}}(gh) = \begin{cases} 1 & g = h^{-1} \\ 0 & \text{o.w.} \end{cases} \\ &= \sum_{s \in G} \delta_g(s^{-1}) \delta_h(s) \end{aligned}$$

□

PROP 1.30

$$\langle f_1, f_2 \rangle = \frac{1}{|G|^2} \sum_{i=1}^n d_i \operatorname{tr}(\hat{f}_1(\rho_i) \overline{\hat{f}_2(\rho_i)}^t)$$

To help with notation, we write  $k(s) = \overline{f_2(s^{-1})}$ . We have

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

Applying Plancherel gives

$$\frac{1}{|G|^2} \sum_{i=1}^n d_i \operatorname{tr}(\hat{f}_1(\rho_i) \hat{k}(\rho_i))$$

It thus remains to show that  $\hat{k}(\rho_i) = \overline{\hat{f}_2(\rho_i)}^t = \hat{f}_2(\rho_i)^* \forall i \in [n]$ . Let  $\rho$  be arbitrary. In some basis, we know that a  $\rho(s)$  is unitary, i.e.  $\rho(s)\rho(s)^* = \operatorname{Id} \implies \rho(s)^* = \rho(s^{-1})$ . With this in mind,

$$\begin{aligned} \hat{k}(\rho) &= \sum_{s \in G} k(s) \rho(s) = \sum_{s \in G} \overline{f_2(s^{-1})} \rho(s) = \sum_{s \in G} \overline{f_2(s)} \rho(s^{-1}) \\ &= \sum_{s \in G} \overline{f_2(s)} \rho(s)^* = \overline{\sum_{s \in G} f_2(s) \rho(s)}^t = \hat{f}_2(\rho)^* \end{aligned}$$

where we note that  $f_2(s)^t = f_2(s)$ , as it is a scalar.

□



We make some final miscellaneous remarks about the Fourier transform:

When  $G$  is abelian, we only have abstract isomorphisms  $G \cong G^*$ . However, a canonical isomorphism can be formed from  $G \cong G^{**}$  by  $g \mapsto (\chi \mapsto \chi(g))$ . We denote by  $[g] : G^* \rightarrow \mathbb{C}^\times$  the function  $\chi \mapsto \chi(g)$ , i.e.  $G \cong G^{**}$  by  $g \mapsto [g]$ .

When  $G$  is abelian,  $C(G, \mathbb{C}) = \text{Class}(G)$ , which we know to be an inner product space with the usual inner product. As discussed earlier,  $f = \sum_{g \in G} f(g) \delta_g$ . Let  $N = |G|$ . Rewriting this in terms of the inner product gives

$$\langle f, \sqrt{N} \delta_g \rangle = \sqrt{N} f(g) \implies f = \sum_{g \in G} \langle f, \sqrt{N} \delta_g \rangle \sqrt{N} \delta_g$$

It follows that  $\{\sqrt{N} \delta_g : g \in G\}$  is an orthonormal basis for  $C(G, \mathbb{C}) = \text{Class}(G)$ .

**PROP 1.31** When  $G = \mathbb{Z}/N\mathbb{Z}$ , with  $f \in C(G, \mathbb{C})$ , we have

$$f(b) = \frac{1}{N} \sum_{a=0}^{n-1} \hat{f}(a) \xi_N^{-ab} \quad \|f\|^2 = \frac{1}{N} \|\hat{f}\|^2$$

where  $\xi_N = e^{\frac{2\pi i}{N}}$ .

**PROOF.**

By Fourier inversion, we get

$$f(b) = \frac{1}{N} \sum_{a=0}^{n-1} \text{tr}(\hat{f}(\chi_a) \chi_a(b^{-1})) = \frac{1}{N} \sum_{a=0}^{n-1} \hat{f}(\chi_a) \chi_a(b^{-1})$$

where we remove trace due to  $G$ -representations being 1-dim. In particular, we parameterize  $G$ 's representations by  $\chi_a : a \in G$ , where

$$\chi_a(b) = e^{\frac{2ab\pi i}{N}} = \xi_N^{ab}$$

Using this parameterization, we view  $\hat{f} : G \rightarrow \mathbb{C}^\times$ . Furthermore, in  $\mathbb{Z}/N\mathbb{Z}$ , we have  $\chi_a(b^{-1}) = \chi_a(-b) = \overline{\chi_a(b)}$ . The first result follows. By [Prop 1.33](#),

$$\langle f, f \rangle = \frac{1}{N^2} \sum_{a=0}^{n-1} \hat{f}(\chi_a) \overline{\hat{f}(\chi_a)} = \frac{1}{N^2} \sum_{a=0}^{n-1} \hat{f}(a) \overline{\hat{f}(a)} = \frac{1}{N} \langle \hat{f}, \hat{f} \rangle$$

From which the second result follows. □

## Random Walks on Cyclic Groups

We can use the theory of finite representations to analyze random walks on  $\mathbb{Z}/N\mathbb{Z}$ , as Markov processes. Much of this work was pioneered by Diaconis and Shahshahani, who picked much of the "low hanging fruit," i.e. processes on the finite groups whose representations are well-understood (supersolvable, abelian, symmetric, dihedral). Further study has been limited.

Let  $G$  be a finite group, with irreducible representations  $\rho_1, \dots, \rho_n$  of dimensions  $d_1, \dots, d_n$ . Define probability distributions  $P$  and  $Q$  on  $G$ . We define the *total variation norm* on probability measures to be

DEF 1.31

$$\|P - Q\|_{\max} = \frac{1}{2} \sum_{s \in G} |P(s) - Q(s)|$$

Apply Kolmogorov's axioms yields  $\|P - Q\|_{\max} = \max_{A \subseteq G} |P(A) - Q(A)|$ . This norm provides a worst-case measure for the convergence of  $P$  to a distribution  $Q$ .

### Theorem 1.15 Diaconis-Shahshahani Lemma

Let  $U \sim U(G)$  be the uniform distribution on  $G$ . Let  $P$  be an arbitrary probability distribution on  $G$ . Then

$$\|P - U\|_{\max}^2 \leq \frac{1}{4} \sum_{i=2}^n d_i \operatorname{tr}(\hat{P}(\rho_i) \hat{P}(\rho_i)^*)$$

Utilizing  $(\sum a_i b_i)^2 \leq (\sum a_i^2)(\sum b_i^2)$ , with  $b_i = 1$ ,

PROOF.

$$4\|P - U\|^2 = \left( \sum_{s \in G} |P(s) - U(s)| \right)^2 \leq \#G \sum_{s \in G} (P(s) - U(s))^2$$

As  $P(s) - U(s) \in \mathbb{R}$ , we have  $4\|P - U\|^2 \leq \#G^2 \cdot \langle P - U, P - U \rangle$ . Applying Plancherel and [Prop 1.33](#) gives

$$4\|P - U\|^2 \leq \sum_{i=1}^n d_i \operatorname{tr}(\widehat{P - U}(\rho_i) \widehat{P - U}(\rho_i)^*)$$

We've noted in [Thm 1.13](#) that  $\hat{U}(\rho_i) = 0$  except on the trivial representation. Also note that  $\hat{P}(\rho_{\text{triv}}) = 1$  (this disappears  $\rho_{\text{triv}} = \rho_1$  in the sum). Since the Fourier transform is linear on  $C(G, \mathbb{C})$ , we conclude that

$$4\|P - U\|^2 \leq \sum_{i=2}^n d_i \operatorname{tr}(\widehat{P}(\rho_i) \widehat{P}(\rho_i)^*)$$

as desired. □

Using the Diaconis-Shahshahani lemma, we will consider a worked example on  $G = \mathbb{Z}/N\mathbb{Z}$ . To maintain consistent multiplicative notions, we take on the view

$$G = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in G \right\} = \mathbb{Z}/N\mathbb{Z}$$

Suppose  $X \sim P$  and  $Y \sim Q$ . We ask  $\mathbb{P}(XY = s)$ . This is exactly

$$\sum_{t \in G} P(st^{-1})Q(t) = (P * Q)(s)$$

Inductively, if  $X_1, \dots, X_n \stackrel{\text{iid}}{\sim} P$ , we conclude that  $\mathbb{P}(\prod_{i=1}^n X_i = s) = P^{*n}(s)$ . We use these notions to model the process  $Y_i = Y_{i-1} + b_i : b_i \in \mathbb{Z}/N\mathbb{Z}$ , with  $Y_0 = 0$ .

Using  $G$ , this is

$$Y_0 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad Y_i = \begin{pmatrix} 1 & b_i \\ 0 & 1 \end{pmatrix} Y_{i-1} : b_i \in \mathbb{Z}/N\mathbb{Z}$$

Our primary question is the following:

Given some distribution  $P$  on  $[n]$ , do random walks on  $\mathbb{Z}/N\mathbb{Z}$  via  $P$  converge to the uniform distribution  $U$  on  $G$ . In other words,  $\lim_{n \rightarrow \infty} Y_n = \lim_{n \rightarrow \infty} P^{*n} \sim U$ ?

**Fig. 1.9** Let  $P \sim \text{Ber}(\frac{1}{2})$  on  $\{-1, 1\}$ , with  $G = \mathbb{Z}/N\mathbb{Z}$ . Then the random walk on  $\mathbb{Z}/N\mathbb{Z}$  is approximately uniform for  $n$  large enough.

We can write  $P = \frac{1}{2}(\delta_1 + \delta_{-1})$ . Then

$$\hat{P}(j) = \frac{1}{2}(\chi_1(j) + \chi_{-1}(j)) = \frac{1}{2} \left( e^{\frac{2\pi i j}{N}} + e^{-\frac{2\pi i j}{N}} \right) = \cos\left(\frac{2\pi j}{N}\right)$$

where  $\chi$  are the irreducible 1-dim representations parameterized by  $-1, 1$ . As convolutions on  $C(G, \mathbb{C})$  acts as composition on  $\mathbb{C}[G]$  (see [Thm 1.13](#)), we have

$$\widehat{P^{*n}}(j) = \cos^n\left(\frac{2\pi j}{N}\right)$$

Applying the Diaconis-Shahshahani lemma gives

$$\|P^{*n} - U\|_{\max}^2 \leq \frac{1}{4} \sum_{j=2}^n \widehat{P^{*n}}(j) = \frac{1}{4} \sum_{j=2}^n \cos^{2n}\left(\frac{2\pi j}{N}\right) \stackrel{(!)}{\leq} e^{\frac{-\pi^2 n}{2N^2}}$$

for  $n \geq N^2$  and  $N \geq 7$  is odd. The (!) bound is shown by Shahshahani in a brute-force way. Note, for an even cyclic group  $\mathbb{Z}/N\mathbb{Z}$ , this process cannot converge: when we take  $n$  even steps, we will land on an even number mod  $N$ , and when we take  $n$  odd steps, we will land on an odd number mod  $N$ .

After  $N^2$  steps we are close to the uniform distribution:

$$\|P^{*n} - U\|^2 \leq e^{\frac{-\pi^2}{2}} \approx 0.007$$

When  $P$  is uniform on  $\{-1, 0, 1\}$ , one can show that  $P^{*n} \approx U$  after  $N^2$  steps as well. Funnily, if we consider distribution above, with  $X_n = 3X_{n-1} + b_n$ , Diaconis-Shahshahani showed that we converge to  $U$  in only  $\log(N)$  steps!

## II Homological Algebra

### EXACT SEQUENCES

This is as good as you can do, as we require  $\log(N)$  steps to simply observe all  $N$  integers via a branching process.