REPRESENTATION THEORY OF FINITE GROUPS

SAM RASKIN

“If you liked it then you should have put a ring on it.” -Beyoncé Knowles

Contents

1. Basic definitions 1
2. Maschke’s theorem 4
3. Schur’s lemma 9
4. The center of the group algebra 11
5. The character table 14
6. Some examples 20
7. Arithmetic 23
8. Burnside’s theorem 27
9. Induced representations 30

1. Basic definitions

1.1. Let G be a finite group. We write the multiplication in G using either concatenation or $\cdot$ (so $gg' = g \cdot g'$) and we will denote the unit in G by 1.

Throughout these notes, $\mathbb{C}$ denotes any algebraically closed field of characteristic 0. Of course, it’s fine to have the complex numbers in mind, but there’s no problem with using $\overline{\mathbb{Q}}$ or anything else. In particular, the use of analytic properties of the complex numbers is forbidden.

(Actually, in this section, it’s enough for $\mathbb{C}$ to be *any* field).

1.2. Let us begin by defining what a representation is. For a vector space V, let GL(V) (alias, $\mathrm{Aut}(V)$) denote the group of invertible linear endomorphisms of V.

Definition 1.1. A *(complex)* representation of G (or G-representation) is a pair (V, ρ) consisting of a $\mathbb{C}$-vector space V and a homomorphism $\rho : G \longrightarrow \mathrm{GL}(V)$. By a *finite-dimensional G-representation* we understand a representation which is finite-dimensional as a mere vector space.

> *Remark* 1.2. Often, if there is no possible ambiguity, for V a G-representation, $g \in G$ and $v \in V$, we will write gv or $g \cdot v$ for $(\rho_V(g))(v)$. In this notation, the condition of being a G-representation is just that for all $g \in G$ the map $g \cdot - : V \longrightarrow V$ is linear and for all $g, g' \in G$ and all $v \in V$, $g \cdot (g' \cdot v) = (g \cdot g') \cdot v$. Similarly, we will sometimes omit ρ from the notation.

Example 1.3. If V is the one-dimensional vector space $\mathbb{C}$, then such a representation is the same thing as a homomorphism $G \longrightarrow \mathbb{C}^{\times}$. Since G is finite, any such homomorphism lands in the roots of unity.

Date: Summer, 2011.

1.3. Let us give an equivalent perspective on what a representation is.

Let $\mathbb{C}[G]$ be the (finite-dimensional) vector space of $\mathbb{C}$-valued functions on G. This vector space has a canonical algebra structure called "convolution." Explicitly, this is given as follows:

$$(f_1 \cdot f_2)(g) = \sum_{x \in G} f_1(gx^{-1}) f_2(x).$$

The unit for the algebra is δ_1 (which we also denote by 1 when convenient).

This algebra structure is characterized as follows. For $g \in G$, let $\delta_g \in \mathbb{C}[G]$ be the "delta function at g" whose value at $g' \in G$ is 0 if $g' \neq g$ and is 1 if $g' = g$. Note that $\{\delta_g\}_{g \in G}$ forms a basis for $\mathbb{C}[G]$. I.e., every element of $\mathbb{C}[G]$ can be written in the form:

$$\sum_{g \in G} a_g \cdot \delta_g$$

for $a_g \in \mathbb{C}$ (note that a_g is the value of the corresponding function at g). Then convolution is characterized by the requirements that it be $\mathbb{C}$-linear and satisfies:

$$\delta_g \cdot \delta_{g'} = \delta_{gg'}.$$

Remark 1.4. Let X be any set and let $\text{Fun}(X)$ be the vector space of $\mathbb{C}$-valued functions on X. Then $\text{Fun}(X)$ has a canonical algebra structure of pointwise multiplication. In the case $X = G$, this is very different from the algebra structure we constructed above. E.g., convolution is non-commutative if G is, and $\text{Fun}(X)$ is always commutative. We will always use $\mathbb{C}[G]$ to denote functions considered with the convolution algebra structure structure above and $\text{Fun}(G)$ to denote functions considered with this algebra structure of pointwise multiplication.

1.4. We claim that the datum of a left $\mathbb{C}[G]$-module is canonically equivalent to the datum of a G-representation.

First, note that there is a canonical algebra map $\mathbb{C} \longrightarrow \mathbb{C}[G]$ sending λ to $\lambda \cdot \delta_1$. In particular, any $\mathbb{C}[G]$-module admits a canonical vector space structure.

Then for a $\mathbb{C}[G]$-module V, we let $\rho_V(g)$ be the operator of action by δ_g. This obviously satisfies the condition to be a representation.

To go the other way, let V be a representation of G. Then we define a $\mathbb{C}[G]$-module structure on V by having $\sum_{g \in G} a_g \cdot \delta_g$ act by $\sum_{g \in G} a_g \cdot \rho_V(g)$.

Remark 1.5. For this reason, we sometimes call G-representations "G-modules."

Remark 1.6. Another way of phrasing this is the following: a representation of G, which by definition is a group homomorphism $\rho : G \longrightarrow GL(V)$, is equivalent to a $\mathbb{C}$-algebra homomorphism $\rho' : \mathbb{C}[G] \longrightarrow \text{End}(V)$. In this language, to pass from a ring homomorphism $\rho' : \mathbb{C}[G] \longrightarrow \text{End}(V)$ to a group homomorphism $\rho : G \longrightarrow GL(V)$, one just restricts ρ' to elements of the form δ_g.

1.5. Now let us give some examples of representations.

Examples 1.7.

(1) For any vector space V, we have the canonical "trivial" action of G on V defined by letting $\rho_V(g)$ be the identity operator. I.e., it is defined by restriction of scalars of the algebra map $\varepsilon : \mathbb{C}[G] \longrightarrow \mathbb{C}$ mapping:

$$\sum_{g \in G} a_g \cdot \delta_g \mapsto a_1.$$

(2) Let G act on a set X. Then $\text{Fun}(X)$ has the canonical structure of G-representation, where we define $\rho(g)(f)$ to be the function:

$$x \mapsto f(g^{-1} \cdot x)$$

i.e., G acts by translating functions under the action of G on the set. This satisfies the condition to be a representation since:

$$(g' \cdot (g \cdot f))(x) = (g \cdot f)(g'^{-1}x) = f(g^{-1}(g')^{-1}x) = f((g'g)^{-1}x) = ((g'g) \cdot f)(x).$$

Representations that arise in this way are called *permutation representations.*

(3) Recall that $G \times G$ acts on the set G by $(g,h) \cdot x := gxh^{-1}$. Therefore, $\mathrm{Fun}(G)$ has the canonical structure of $G \times G$ representation. Explicitly, it is given by:

$$\rho_{reg}(g,h)(f)(x) := f(g^{-1}xh).$$

This representation is called the "regular representation." Note that it induces two structures of G-representation on $\mathrm{Fun}(G)$ coming from the two homomorphisms $G \longrightarrow G \times G$ given by $g \mapsto (g,1)$ and $g \mapsto (1,g)$. The first is called the "left regular representation" and the second is called the "right regular representation."

The map $G \longrightarrow G$ sending $x \mapsto x^{-1}$ intertwines the two G-module structures, so they really aren't so different. When there's possible ambiguity, we regard $\mathrm{Fun}(G)$ as a G-module through the left regular representation.

1.6. For two representations V, W of G, we let $\mathrm{Hom}_G(V,W)$ denote the vector subspace of $\mathrm{Hom}(V,W)$ of linear transformations consisting of those linear transformations which commute with the action of G, i.e., those $T \in \mathrm{Hom}(V,W)$ such that $T \circ \rho_V(g) = \rho_V(g) \circ T$. These are called *$G$-equivariant maps* or *maps of G-representations*, or *G-linear map*, etc.

1.7. Let us study the regular representation a little more carefully. We have the canonical map $ev_1 : \mathrm{Fun}(G) \longrightarrow \mathbb{C}$ given by evaluation at the point 1. Note that this is *not* a G-linear map (for either G-module structure on $\mathrm{Fun}(G)$).

Lemma 1.8. *For any representation V, the map:*

$$\mathrm{Hom}_G(V, \mathrm{Fun}(G)) \longrightarrow \mathrm{Hom}(V, \mathbb{C}) =: V^*$$

given by:

$$T \mapsto ev_1 \circ T$$

is an isomorphism.

Remark 1.9. In other words, this says: to give a map of G-representations from V to $\mathrm{Fun}(G)$ is the same as giving an element of V^* the dual vector space to V. So the moral is: it's very easy to map a representation into the regular representation.

Proof. We have to see that this map is injective and surjective.

This map is manifestly linear, so to show injectivity it suffices to show that the kernel is 0. For a G-equivariant map $T : V \longrightarrow \mathrm{Fun}(G)$ to lie in the kernel translates to saying that:

$$T(v)(1) = 0$$

for all $v \in V$ (note that $T(v)$ is a function on G, so it makes sense to evaluate it on an element of G; so $T(v)(1)$ could also be denoted $(T(v))(1)$). To see that T is itself zero, we need to show that $T(v)(g) = 0$ for all $g \in G$ and $v \in V$. But by G-equivariance:

$$T(v)(g) = \big(g^{-1} \cdot (T(v)\big)(1) = T(g^{-1}(v))(1) = 0.$$

Let us explain these manipulations a little more clearly. Here, $g^{-1} \cdot (T(v)) \in \mathrm{Fun}(G)$ is the function defined by acting on $T(v)$ via the left regular representation, so the fact that $T(v)(g) = \big(g^{-1} \cdot (T(v)\big)(1)$ follows from the definition of the action in the left regular representation. But since the assignment $v \mapsto T(v)$ is G-equivariant, $g^{-1} \cdot T(v) = T(g^{-1}v)$. But since $T(w)(1)$ is equal to 0 for all $w \in V$, setting $w = g^{-1}v$ we get the desired result.

The above proof of injectivity shows us how to prove surjectivity as well. Namely, suppose we have a linear functional $\lambda : V \longrightarrow \mathbb{C}$. Then we define $T_\lambda(v)$ to be the function:

$$T_\lambda(v)(g) := \lambda(g^{-1}v).$$

The map $T_\lambda : V \longrightarrow \mathrm{Fun}(G)$ given by $v \mapsto T_\lambda(v)$ is G-equivariant since for $x \in G$ we have:

$$T_\lambda(xv)(g) = \lambda(g^{-1}xv) = (T_\lambda(v))(x^{-1}g) = (x \cdot T_\lambda(v))(g).$$

That is to say: $T_\lambda(xv) = x \cdot T_\lambda(v)$, as desired.

□

Remark 1.10. This remark can safely be ignored. The above constructions give another reason to distinguish notationally between $\mathrm{Fun}(G)$ and $\mathbb{C}[G]$: morally, they play very different roles in the theory. Namely, if G were an infinite group, then the "correct" analogue of $\mathbb{C}[G]$ would be functions which are allowed to be non-zero only on a finite subset of G, while $\mathrm{Fun}(G)$ would continue to be all functions. These are "correct" in the following sense: the construction of Section 1.4 requires that the sum $\sum_{g\in G} a_g \cdot \delta_g$ be a *finite* sum, since we don't know how to act by an infinite sum. However, Lemma 1.8 goes through even in the case when G is infinite. (The following can especially be ignored for us: if G were not a discrete group but, say, a Lie group or a p-adic group, then it would be even smarter to define $\mathbb{C}[G]$ as *measures* on G).

2. MASCHKE'S THEOREM

2.1. In this section, it's only important that $\mathbb{C}$ have characteristic 0.

2.2. For a G-representation V, we denote by V^G the subspace of G-invariant vectors, i.e.:

$$V^G := \{v \in V \mid g \cdot v = v \text{ for all } g \in G\}.$$

Of course, a G-equivariant map $T : V \longrightarrow W$ induces a map on invariants: $V^G \longrightarrow W^G$.

Our goal for this section is to prove the following result and discuss some corollaries:

Theorem 2.1. *Let $T : V \longrightarrow W$ be a G-equivariant surjection. Then the induced map on invariants $V^G \longrightarrow W^G$ is surjective.*

Remark 2.2. This property is particular to both finite groups and to characteristic 0 fields (actually, the careful reader will observe that the proof goes through if we merely assume that the characteristic of the ground field does not divide the order of the group). Here are two counterexamples, which may safely be skipped by the reader.

(1) Let $G = \mathbb{Z}$. Then a $\mathbb{Z}$-representation is the same thing as a vector space V equipped with an automorphism φ. A $\mathbb{Z}$-equivariant map between two vector spaces (V_i, φ_i) equipped with automorphisms is the same thing as a linear transformation intertwining the automorphisms, i.e., $T : V_1 \longrightarrow V_2$ such that $T \circ \varphi_1 = \varphi_2 \circ T$. Let $V_1 = \mathbb{C}^2$ and let φ_1 be defined by the matrix:

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

Let V_2 be the trivial, one-dimensional representation of $\mathbb{Z}$ on $\mathbb{C}$. There is a $\mathbb{Z}$-equivariant map $V_1 \longrightarrow V_2$ sending $\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix}$ to λ_2. However, $V_1^{\mathbb{Z}} = \mathbb{C} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, so the induced map on invariants is 0.

(2) For a prime number p, let $G = \mathbb{Z}/p\mathbb{Z}$ and let K be a field of characteristic p. In this case, the above construction of a 2-dimensional representation of $\mathbb{Z}$ works verbatim. However, in this case the representation of $\mathbb{Z}$ on $K^{\oplus 2}$ factors through $\mathbb{Z}/p\mathbb{Z}$ since:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Therefore, the same map $V_1 = K^{\oplus 2} \longrightarrow V_2 = K$ defines a G-equivariant map which is not surjective on invariants for the same reason: however, now the group is finite.

2.3. Here is a general construction. Let $T : V \longrightarrow W$ be a G-equivariant map and let $x = \sum_{g \in G} a_g \cdot \delta_g \in \mathbb{C}[G]$. Then we have operators on each of V and W defined by x, and T intertwines these operators.

Remark 2.3. This is really the point of introducing the group algebra. Namely, we define a representation as a vector space V which has some particular symmetries (labelled by elements of the group G) which satisfy some relations. However, the group algebra keeps track of the additional symmetries that the representation carries by mere virtue of being a representation. This is a part of a general philosophy in representation theory: where possible, it's best to relate representations to modules over an associative algebra since (in a precise sense) the algebra encodes the complete set of symmetries carried by the representations.

2.4. For a finite set X, let $|X|$ denote the order of X.

2.5. Define $\mathrm{Av}_G \in \mathbb{C}[G]$ as $\frac{1}{|G|} \sum_{g \in G} \delta_g$. Note that the definition of Av_G could not be given if G were infinite or the characteristic of the ground field divided the order of the group!

Proposition 2.4. Av_G *satisfies the following properties:*

1. *For any $g \in G$, $\delta_g \cdot \mathrm{Av}_G = \mathrm{Av}_G$ and $\mathrm{Av}_G \cdot \delta_g = \mathrm{Av}_G$.*
2. *Av_G is an idempotent in $\mathbb{C}[G]$, i.e., $\mathrm{Av}_G \cdot \mathrm{Av}_G = \mathrm{Av}_G$.*
3. *For V a G-representation and $v \in V$, $\mathrm{Av}_G \cdot v \in V^G$.*
4. *For V a G-representation and $v \in V^G$, $\mathrm{Av}_G \cdot v = v$.*

Proof. Let us begin with (1). For any $g \in G$, we have:

$$g \cdot \mathrm{Av}_G = \frac{1}{|G|} \sum_{g' \in G} (\delta_g \cdot \delta_{g'}) = \frac{1}{|G|} \sum_{g' \in G} \delta_{gg'} = \frac{1}{|G|} \sum_{g' \in G} \delta_{g'} = \mathrm{Av}_G .$$

Similarly, we see that $\mathrm{Av}_G \cdot \delta_g = \mathrm{Av}_G$. The first of these identities immediately implies (3).

Next, let us show (4). We compute:

$$\mathrm{Av}_G \cdot v = \frac{1}{|G|} \sum_{g \in G} (\delta_g \cdot v) = \frac{1}{|G|} \sum_{g \in G} v = v.$$

Finally, let us deduce (2). Indeed, $\mathrm{Av}_G \in \mathbb{C}[G]^G$ is the subspace of invariants with respect to the left (or right) G-action on $\mathbb{C}[G]$ by (1). Therefore, by (4) we have $\mathrm{Av}_G \cdot \mathrm{Av}_G = \mathrm{Av}_G$ as desired. ☐

Remark 2.5. Let Av_G^{naive} be $\sum_{g \in G} \delta_g (= |G| \cdot \mathrm{Av}_G)$. Note that the definition of Av_G^{naive} does not require division by $|G|$ and therefore can be defined over a field of any characteristic. Then conclusions (1) and (3) continue to hold for Av_G^{naive}, but (2) and (4) do not.

2.6. Now we can prove the theorem.

Proof of Theorem 2.1. Let $T : V \twoheadrightarrow W$ be as in the statement of the proposition and let $w \in W^G$. We need to find $v \in V^G$ such that $T(v) = w$.

Because T is surjective, there exists $v_0 \in V$ such that $T(v_0) = w$. Since T is G-equivariant, we have $T \circ \mathrm{Av}_G = \mathrm{Av}_G \circ T$. Therefore, we have:

$$T(\mathrm{Av}_G \cdot v_0) = \mathrm{Av}_G \cdot T(v_0) = \mathrm{Av}_G \cdot w = w.$$

Here the last equality follows from Proposition 2.4. Applying the proposition again, we see that $v := \mathrm{Av}_G \cdot v_0 \in V^G$. This completes the proof.

□

Remark 2.6. Here's another way to understand this proof. Note that for a representation V, the subspace $V^G \subset V = \mathrm{Hom}(\mathbb{C}, V)$ of invariants coincides with $\mathrm{Hom}_G(\mathbb{C}, V)$. Therefore, we want to show that $\mathbb{C}$ is *projective* as a $\mathbb{C}[G]$-module. It suffices to show that it is a direct summand of $\mathbb{C}[G]$. We have the canonical map $\mathbb{C} \longrightarrow \mathbb{C}[G]$ sending 1 to δ_e, and we have the G-equivariant splitting $\mathbb{C}[G] \longrightarrow \mathbb{C}$ defined by:

$$\sum_{g \in G} a_g \cdot \delta_g \mapsto \frac{1}{|G|} \sum_{g \in G} a_g \in \mathbb{C}.$$

2.7. Before proceeding, we will need to give some ways of constructing new representations starting from old ones. Namely, given two G-representations V and W, we will explain how to make each of $V \otimes W$ and $\mathrm{Hom}(V, W)$ into a G-representation in a convenient way. This digression will occupy Sections 2.8-2.10.

2.8. Suppose first that V and W are representations of groups G and H respectively. Then $V \otimes W$ inherits a natural structure of $G \times H$-representation.

Indeed, the construction goes as follows: for $(g, h) \in G \times H$ and $\sum_{i=1}^n v_i \otimes w_i \in V \otimes W$, we define:

$$(g, h) \cdot \sum_{i=1}^n v_i \otimes w_i = \sum_{i=1}^n (g \cdot v_i) \otimes (h \cdot w_i).$$

One immediately checks that this is well-defined and defines the desired structure of $G \times H$-representation.

Remark 2.7. In terms of group algebras, this construction can be phrased as follows. Suppose M and N are modules for $\mathbb{C}$-algebras A and B respectively. Then $M \otimes N$ has a canonical structure of $A \otimes B$-module. Applying this to group algebras and noting the canonical isomorphism $\mathbb{C}[G] \otimes \mathbb{C}[H] \xrightarrow{\simeq} \mathbb{C}[G \times H]$ (defined by $\delta_g \otimes \delta_h \mapsto \delta_{(g,h)}$) gives the above construction.

2.9. Now suppose that V and W are representations of the same group G. We claim that the construction from Section 2.8 defines a canonical structure of representation on $V \otimes W$.

Indeed, we have the canonical "diagonal" homomorphism $\Delta : G \longrightarrow G \times G$ given by $g \mapsto (g, g)$. Since $V \otimes W$ has the structure of $G \times G$-representation, we can restrict this structure along Δ to give a G-module structure.

In terms of formulae, this action is defined by:

$$g \cdot \sum_{i=1}^n v_i \otimes w_i = \sum_{i=1}^n (g \cdot v_i) \otimes (g \cdot w_i).$$

2.10. Now let us define the structure of G-representation on $\mathrm{Hom}(V,W)$.

Proposition-Construction 2.8. *There is a unique structure of G-representation on $\mathrm{Hom}(V,W)$ such that the "evaluation" map:*

$$\mathrm{ev} : \mathrm{Hom}(V,W) \otimes V \longrightarrow W$$

(sending $T \otimes v$ to $T(v)$) is G-equivariant with respect to the induced G-module structure on the tensor product defined above.

With respect to this G-module structure, the invariants $\mathrm{Hom}(V,W)^G$ coincide with the subspace of G-equivariant maps $\mathrm{Hom}_G(V,W)$.

Remark 2.9. For $T \in \mathrm{Hom}(V,W)$, we will denote by ${}^gT$ the element of $\mathrm{Hom}(V,W)$ given by acting on T by g under the G-module structure on $\mathrm{Hom}(V,W)$ from the construction. The reason for this notation is to avoid ambiguity: if we used $g \cdot T$ then $g \cdot T(v)$ could reasonably mean $g \cdot (T(v))$ or $(g \cdot T)(v)$ (the latter being what we are denoting ${}^gT(v)$), and these two vectors are in general different.

Proof. For $T \in \mathrm{Hom}(V,W)$ and $v \in V$, the fact G-equivariance of ev implies that:

$${}^gT(g \cdot v) = \mathrm{ev}(g \cdot (T \otimes v)) = g \cdot \mathrm{ev}(T \otimes v) = g \cdot T(v).$$

Replacing v by $g^{-1}v$, we see that ${}^gT(v) = g \cdot T(g^{-1}v)$, so ${}^gT = \rho_W(g) \circ T\rho_V(g^{-1})$. It's immediate to see that this is actually a G-module structure.

With respect to this structure of representation, a map $T \in \mathrm{Hom}(V,W)$ lies in the invariants $\mathrm{Hom}(V,W)^G$ if and only if it lies in the subspace of G-equivariant maps $\mathrm{Hom}_G(V,W)$. Indeed, we have ${}^gT = T$ for all $g \in G$ if and only if for all $v \in V$ we have $g \cdot T(g^{-1} \cdot v) = T(v)$. Replacing v by $g \cdot v$ (since this is supposed to hold for all $v \in V$), this equation becomes $g \cdot T(v) = T(g \cdot v)$ as desired.

□

Remark 2.10. For example, if V is the trivial representation, then $\mathrm{Hom}(V,W) = \mathrm{Hom}(\mathbb{C},W)$ is just W as a vector space, and we deduce from the uniqueness that this identifies them as representations as well.

Remark 2.11. Let us note a similar compatibility. Recall that Lemma 1.8 said that in the case $W = \mathrm{Fun}(G)$ the (left) regular representation, we have $\mathrm{Hom}_G(V, \mathrm{Fun}(G)) \xrightarrow{\simeq} V^*$ (where the map to V^* is given by evaluation at $1 \in G$). Actually, this isomorphism defines the structure of G-representation on V^* using the *right* action of G on $\mathrm{Fun}(G)$. We also have the structure of G-representation on V^* by realizing V^* as $\mathrm{Hom}(V,\mathbb{C})$ (where $\mathbb{C}$ is given the trivial G-module structure).

Again, by the uniqueness statement we deduce that these two structures of G-representation on V^* are the same. Explicitly, for $\lambda \in V^*$ and $g \in G$ we have:

$$(g \cdot \lambda)(v) = \lambda(g^{-1} \cdot v)$$

with respect to this structure.

2.11. With this construction in hand, we can prove the following result:

Corollary 2.12. *Given a G-equivariant surjection $T : V \longrightarrow W$ of G-representations, there exists a G-equivariant splitting, i.e. a map $S : W \longrightarrow V$ such that $T \circ S = \mathrm{Id}_W$.*

Proof. Consider the induced map:

$$\mathrm{Hom}(W,V) \longrightarrow \mathrm{Hom}(W,W)$$

which sends a linear transformation $S : W \longrightarrow V$ to the composition $T \circ S$. One immediately sees that the G-equivariance of T implies that this is a G-equivariant map with respect to the G-module structures defined on $\mathrm{Hom}(W, V)$ and $\mathrm{Hom}(W, W)$ defined in Proposition-Construction 2.8. Moreover, it is obviously surjective. E.g., since T is surjective, there is (possibly not G-equivariant) linear transformation $\sigma : W \longrightarrow V$ such that $T \circ \sigma = \mathrm{Id}$ which immediately implies the surjectivity (since any $\varphi \in \mathrm{Hom}(W, W)$ is $T \circ (\sigma \circ \varphi)$).

Note that Id_W is a G-equivariant map and therefore lies in the invariants of $\mathrm{Hom}(W, W)$. Therefore, by Theorem 2.1 there exists $S \in \mathrm{Hom}_G(W, V)$ such that S maps to Id_W under this map, i.e., $T \circ S = \mathrm{Id}_W$ as desired.

□

Remark 2.13. Here's a more explicit way of combining the proofs of Corollary 2.12 and Theorem 2.1 to obtain a proof of Corollary 2.12. Let $\sigma : W \longrightarrow V$ be as in the proof of Corollary 2.12, namely, a (possibly not G-equivariant) splitting of T and define S to be

$$^{\mathrm{Av}_G}\sigma = \frac{1}{|G|} \sum_{g \in G} \rho_V(g) \circ \sigma \circ \rho_V(g^{-1}).$$

2.12. The following definition will be fundamental to our future studies:

Definition 2.14. A non-zero G-representation V is *irreducible* if the only subspaces V which are preserved by the G-action are 0 and V. A representation V is said to be reducible if it is not irreducible.

Examples 2.15.
(1) Any 1-dimensional representation is irreducible.
(2) A representation V is irreducible if and only if its dual V^* is, since if $W \subset V$ is stable under the G-action, then $W^\perp := \{\lambda \in V^* \mid \lambda(w) = 0 \text{ for all } w \in W\} \subset V^*$ is also stable under the G-action.

Remark 2.16. Here is a more computationally-minded perspective on an irreducible representation: a representation is irreducible if and only if for *every* non-zero vector $0 \neq v \in V$, the vectors $\{g \cdot v\}_{g \in G}$ span V. Indeed, if the span of these vectors is visibly a G-submodule W of V, so if V is irreducible, $0 \neq v \in W$ implies $W = V$ by irreducibility. Conversely, if we have $0 \underset{\neq}{\subset} W \underset{\neq}{\subset} V$ then for v any non-zero vector in W we see that the span of $\{g \cdot v\}_{g \in G}$ is contained in W, and therefore if V is not irreducible then there exists a vector $0 \neq v$ such that $\{g \cdot v\}_{g \in G}$ does not span V.

It's very important here that one check this conidition for every non-zero v. It's easy to find counter-examples where there exists some non-zero v such that $\{g \cdot v\}_{g \in G}$ spans V but such that V is not itself irreducible.

2.13. Corollary 2.12 then admits the following immediate corollary due to Maschke:

Corollary 2.17 (Maschke's theorem)**.** *Any finite-dimensional G-representation V admits a direct sum decomposition $V \xrightarrow{\simeq} \oplus_{i=1}^n V_i$ where each V_i is irreducible.*

Proof. We prove this by induction on $\dim(V)$. For $\dim(V) = 0$, this is clear: take the empty direct sum. Otherwise, there are two possibilities: either V is irreducible, in which case we are done, or else it is not irreducible, in which case there exists:

$$0 \underset{\neq}{\subset} W \underset{\neq}{\subset} V$$

where W is a subrepresentation. Since W is a subrepresentation, the quotient V/W admits (uniquely) the structure of G-representation such that $T : V \longrightarrow V/W$ is G-equivariant. By Corollary 2.12, there exists a splitting $S : V/W \longrightarrow T$ of T. This expresses V as the direct sum of

W and V/W as a G-representation, and since $\dim W < \dim V$ and $\dim V/W < \dim V$, we deduce the desired result by induction.

□

Remarks 2.18.

1. A similar proof goes through for infinite-dimensional representations (if one allows infinite direct sums), but requires Zorn's lemma. E.g., when G is the trivial group, this theorem already says that every vector space admits a basis.
2. Irreducible representations of a group are of fundamental importance in the study of representation theory. Indeed, by Maschke's theorem, all other representations are built out of them via direct sums. However, for a given finite group G, it is non-trivial to compute all of its irreducible representations. We will develop some general tools over the next several sections to help.

3. SCHUR'S LEMMA

3.1. The following result exemplifies the rigidity of irreducible representations.

Proposition 3.1. *Let V be an irreducible representation of G and let W be any representation of G.*

(1) Any G-equivariant map $T : V \longrightarrow W$ is either the zero map or else injective.
(2) Any G-equivariant map $T : W \longrightarrow V$ is either the zero map or else surjective.
(3) If W is also irreducible, then any G-equivariant map $T : V \longrightarrow W$ is either 0 or else an isomorphism.

Proof. For any G-equivariant map $T : V \longrightarrow W$ one immediately sees that the kernel is a subrepresentation of V. Therefore, it is either 0 or V. If the kernel is 0, then T is injective, and if the kernel is V then T is 0.

Similarly, for any G-equivariant map $T : W \longrightarrow V$, one immediately sees that the image is a subrepresentation of V and therefore either 0 or V. If the image is 0, then $T = 0$, and if the image is V then T is surjective.

We observe that (3) follows immediately from (1) and (2).

□

In particular, we deduce the following numerological result, which will be vastly improved upon later:

Corollary 3.2. *For V any irreducible representation of G,* $\dim(V) \leq |G|$.

Proof. Recall that Lemma 1.8 says that $\mathrm{Hom}_G(V, \mathrm{Fun}(G)) \xrightarrow{\simeq} V^*$. Therefore, choosing an non-zero $\lambda \in V^*$ defines a non-zero G-equivariant map $V \longrightarrow \mathrm{Fun}(G)$. This map, being non-zero, is injective by Proposition 3.1. Therefore, we deduce that:

$$\dim(V) \leq \dim(\mathrm{Fun}(G)) = |G|.$$

□

Remark 3.3. Here is another proof of the corollary. If V is irreducible, then by Remark 2.16, for any non-zero v the set $\{g \cdot v\}_{g \in G}$ spans V. However, the perspective used in the proof of the corollary will give stronger results later (see e.g. Corollary 3.8) so we emphasize this technique now.

3.2. From now on, we will really use that $\mathbb{C}$ is algebraically closed of characteristic 0 (okay, fine: Schur's lemma only needs algebraically closed, but we'll combine it with Maschke's theorem soon enough).

Lemma 3.4 (Schur's lemma)**.** *For V an irreducible representation of G,* $\mathrm{End}_G(V)$ *is* 1*-dimensional with generator the identity.*

Proof. Suppose that $T \in \mathrm{End}_G(V)$ is G-equivariant endomorphism of V. We need to show that T is a scalar multiple of the identity.

Since V is finite-dimensional (by Corollary 3.2) and since $\mathbb{C}$ is algebraically closed, T has an eigenvalue λ. Recall that λ being an eigenvalue means that $T - \lambda \cdot \mathrm{Id}_V$ has non-zero kernel. But by Proposition 3.1, this means that the G-equivariant map:

$$T - \lambda \cdot \mathrm{Id}_V : V \longrightarrow V$$

must be zero, i.e., $T = \lambda \cdot \mathrm{Id}_V$ as desired.

□

3.3. Let $\mathrm{Irrep}(G)$ denote the set of isomorphism classes of irreducible G-representations. We will sometimes say $V \in \mathrm{Irrep}(G)$ to mean that V is an irreducible representation, i.e., a representative of an isomorphism class. Note that such a choice is non-canonical (by Schur's lemma, if V and W are isomorphic and irreducible then the set $\mathrm{Isom}_G(V, W)$ is a simply-transitive $\mathbb{C}^\times$-set under the action of $\mathbb{C}^\times$ by homotheties).

Here is a nice way of combining the content of Schur's lemma and Maschke's theorem into one result:

Proposition 3.5. *For any finite-dimensional representation V, the canonical map:*

$$\oplus_{V_i \in \mathrm{Irrep}(G)} \mathrm{Hom}_G(V_i, V) \otimes V_i \longrightarrow V$$

is an isomorphism of G-representations.

Remarks 3.6.
(1) The statement of the proposition implicitly chooses representatives for each isomorphism class of irreducible representation.
(2) Of course, statement goes through verbatim when V is infinite-dimensional if one allows the infinite-dimensional form of Maschke's theorem.

Proof. Both the left and right hand sides of the map:

$$\oplus_{V_i \in \mathrm{Irrep}(G)} \mathrm{Hom}_G(V_i, V) \otimes V_i \longrightarrow V$$

commute with direct sums in the V-variable. Therefore, since Maschke's theorem tells us that V is a direct sum of irreducible representations, it suffices to check the statement of the proposition when V is irreducible. By Proposition 3.1 (3), for $V_i \in \mathrm{Irrep}(G)$ we have $\mathrm{Hom}(V_i, V) = 0$ unless $V_i \xrightarrow{\simeq} V$. Therefore, the left hand side is just $\mathrm{Hom}_G(V, V) \otimes V$. Therefore, by Schur's lemma our map is just $(\mathbb{C} \cdot \mathrm{Id}_V) \otimes V \longrightarrow V$, which is clearly an isomorphism.

□

Exercise 3.7. Conversely, deduce Maschke's theorem and Schur's lemma from Proposition 3.5.

3.4. As a corollary, we give the following (somewhat striking) improvement of the numerology from Corollary 3.2.

Corollary 3.8. *We have the equality:*

$$\sum_{V_i \in \mathrm{Irrep}(G)} \dim(V_i)^2 = |G|.$$

Proof. Applying Proposition 3.5 to $V = \mathrm{Fun}(G)$ the (left) regular representation and applying Lemma 1.8, we deduce:

$$\oplus_{V_i \in \mathrm{Irrep}(G)} \mathrm{Hom}_G(V_i, \mathrm{Fun}(G)) \otimes V_i \xrightarrow{\simeq} \oplus_{V_i \in \mathrm{Irrep}(G)} V_i^* \otimes V_i \xrightarrow{\simeq} \mathrm{Fun}(G).$$

Taking the dimensions of the middle and right terms, we immediately deduce the result.

□

Remark 3.9. In particular, there are at most $|G|$ many irreducible representations of G. In the next section, we'll give a precise calculation of the number of irreducible representations (in terms of the pure group theory of the group G).

3.5. Here is another result in the spirit of Corollary 3.8.

Corollary 3.10. *For any finite-dimensional representation V of G, we have the equality:*

$$\dim(\mathrm{End}_G(V)) = \sum_{V_i \in \mathrm{Irrep}(G)} \dim(\mathrm{Hom}_G(V_i, V))^2$$

In particular, V is irreducible if and only if $\dim(\mathrm{End}_G(V)) = 1$.

Proof. Applying $\mathrm{Hom}_G(-, V)$ to the isomorphism from Proposition 3.5, we deduce an isomorphism:

$$\mathrm{Hom}_G(\oplus_{V_i \in \mathrm{Irrep}(G)} \mathrm{Hom}_G(V_i, V) \otimes V_i, V) \xrightarrow{\simeq} \mathrm{End}_G(V)$$

The left hand side is isomorphic to the space:

$$\oplus_{V_i \in \mathrm{Irrep}(G)} \mathrm{Hom}_G(\mathrm{Hom}_G(V_i, V) \otimes V_i, V) \xrightarrow{\simeq} \oplus_{V_i \in \mathrm{Irrep}(G)} \mathrm{End}(\mathrm{Hom}_G(V_i, V))$$

But this dimension of this term is given by $\dim(\mathrm{Hom}_G(V_i, V))^2$. ☐

3.6. Here is another corollary of Schur's lemma:

Corollary 3.11. *Let A be a finite abelian group and let V be an irreducible representation of A. Then* $\dim(V) = 1$.

Proof. Observe ρ_V maps A to $\mathrm{Aut}_A(V)$. Indeed, this immediate from the commutativity of A. But since V is irreducible, we have seen that $\mathrm{Aut}_A(V)$ consists of invertible scalar multiples of the identity operator of V. Since such scalars preserve *every* subspace of V, we deduce the result. ☐

Example 3.12. Now we will give a counterexample to Schur's lemma when the field is not algebraically closed. Suppose $G = \mathbb{Z}/3\mathbb{Z}$. We define a 2-dimensional representation V which sends the generator of $\mathbb{Z}/3\mathbb{Z}$ to the matrix:

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

It's easy to see that this does not stabilize any $\mathbb{Q}$-lines because its eigenvalues are the non-trivial third roots of unity, and in particular they are not defined over $\mathbb{Q}$.

Note that in this case the argument used to prove Schur's lemma shows that $\mathrm{End}_G(V)$ is a (non-commutative) division algebra over $\mathbb{Q}$.

4. THE CENTER OF THE GROUP ALGEBRA

4.1. Schur's lemma tells us that every time we have an irreducible representation V and a G-equivariant endomorphism of it, this endomorphism must be a scalar multiple of the identity. Our goal for this section is to give a large supply of G-equivariant endomorphisms of representations. The natural approach to this is through the *center* of the group algebra $\mathbb{C}[G]$.

4.2. Recall that if A is an algebra, then the *center* $Z(A)$ of A is the subalgebra consisting of elements $z \in A$ such that $za = az$ for every $a \in A$. E.g., if A is commutative, then $Z(A) = A$.

The action of $Z(A)$ on a left A-module commutes with the action of A, i.e., there is an action of $Z(A)$ on every A-module by A-module endomorphisms. Note that this is *not* true for elements which are not in the center! By considering the case when the module is A itself, one sees that the center is the best thing which acts on every A-module by A-module endomorphisms.

4.3. We denote by $Z(G)$ the center of the group algebra $\mathbb{C}[G]$. Suppose that V is any representation of G. Then since any element of $\mathbb{C}[G]$ acts on V, in particular the element z defines a G-equivariant endomorphism of V (note that this is *not* true for elements which are not in the center!). Thus, as indicated above, we see that the center of the group algebra gives a convenient way of producing G-equivariant endomorphisms of representations.

4.4. We will construct a canonical basis of $Z(G)$ labelled by conjugacy classes of G. First, let us recall the basic definitions about conjugacy classes and establish some notation.

Recall that G acts on itself in three natural ways: by left translation, right translation, and by the adjoint action (alias: conjugation), i.e., $g \overset{ad}{\cdot} x := g^{-1}xg$. Recall that a *conjugacy class* in G is an orbit for the conjugation action. We will denote the set of conjugacy classes by $G \overset{ad}{/} G$. For $g \in G$, we let $[g] \in G \overset{ad}{/} G$ denote the conjugacy class containing g.

4.5. Now let us construct the basis. Let $C \in G \overset{ad}{/} G$ be a conjugacy class. We define:

$$b_C = \frac{1}{|C|} \sum_{\{g \in G | [g] = C\}} \delta_g \in Z(G).$$

Remark 4.1. The scalar $\frac{1}{|C|}$ is not important for defining a basis, but rather is used to adhere to standard normalizations. We will also see it appear naturally in the proof of Proposition 4.3.

Proposition 4.2. *The set:*

$$\{b_C\}_{C \in G \overset{ad}{/} G}$$

is a basis of $Z(G)$. *In particular,* $\dim(Z(G)) = |G \overset{ad}{/} G|$, *the number of conjugacy classes of* G.

This proposition will be proved in Section 4.7.

4.6. We will deduce Proposition 4.2 from the following more general proposition:

Proposition 4.3. *Let X be a finite set equipped with a G-action and let* $\mathrm{Fun}(X)$ *be the associated permutation representation. For each orbit $O \subset X$, let* $b_O \in \mathrm{Fun}(X)$ *be the function which take the value* $\frac{1}{|O|}$ *on O and is* 0 *otherwise. Then the set* $\{b_O\}_{O \text{ an orbit}}$ *forms a basis for the invariants* $\mathrm{Fun}(X)^G$.

Proof. The set $\{\delta_x\}_{x \in X}$ is a basis for $\mathrm{Fun}(X)$ (here δ_x takes the value 1 at x and 0 away from x). Therefore, by Proposition 2.4, the elements $\mathrm{Av}_G \cdot \delta_x$ span $\mathrm{Fun}(X)^G$. An immediate computation shows that $\mathrm{Av}_G \cdot \delta_x = b_O$ where O is the orbit containing x. Therefore, the elements b_O span the invariants, and it's immediate to see that they are linearly independent as well.

□

4.7. Now let us give the proof of Proposition 4.2.

Proof of Proposition 4.2. Consider the action of G on the set G given by conjugation. By Proposition 4.3, it suffices to show that under the natural identification $\mathbb{C}[G] \xrightarrow{\simeq} \mathrm{Fun}(G)$ the center of the algebra identifies with the invariants of the conjugation action.

This space of invariants consists of elements $x \in \mathbb{C}[G]$ such that $\delta_{g^{-1}} \cdot x \cdot \delta_g = x$ for all $g \in G$, i.e., elements x such that $x \cdot \delta_g = \delta_g \cdot x$. Since the δ_g form a basis of $\mathbb{C}[G]$, this is exactly the center of the algebra.

□

4.8. For a commutative algebra A finite-dimensional over $\mathbb{C}$, define the *spectrum* $\mathrm{Spec}(A)$ of A to be the set of all $\mathbb{C}$-linear ring homomorphisms $\chi : A \longrightarrow \mathbb{C}$.

Examples 4.4.

1. If $A = \mathbb{C}$, then $\mathrm{Spec}(A)$ is just the singleton set consisting of the identity. (Indeed, any ring homomorphism preserves units, so $\mathbb{C}$-linearity ensures that any such homomorphism is the identity).
2. More generally, if X is a finite set then $\mathrm{Spec}(\mathrm{Fun}(X))$ is canonically identified with the set X, where the map $X \longrightarrow \mathrm{Spec}(\mathrm{Fun}(X))$ assigns to a point $x \in X$ the homomorphism $ev_x : \mathrm{Fun}(X) \longrightarrow \mathbb{C}$ sending f to $f(x)$.
3. For any A finite-dimensional over $\mathbb{C}$, there is a canonical homomorphism $A \longrightarrow \mathrm{Fun}(\mathrm{Spec}(A))$ which sends an element $a \in A$ to the function $\mathrm{ev}_a : \mathrm{Spec}(A) \longrightarrow \mathbb{C}$ sending $\chi : A \longrightarrow \mathbb{C}$ to $\chi(a)$. When $A = \mathrm{Fun}(X)$ for a finite set X, then this map is an isomorphism. For more general A, this is not the case: e.g., if $A = \mathbb{C}[x]/x^n$, then $\mathrm{Spec}(A)$ is a singleton set, while $\dim(\mathrm{Fun}(A)) = n$. (However, one can show that as long as there are no non-zero nilpotents in A, then this map *is* an isomorphism, but we won't need this result.)

4.9. There is a canonical map:

$$\mathfrak{F} : \mathrm{Irrep}(G) \longrightarrow \mathrm{Spec}(Z(G))$$

defined as follows.

Let V be a representation of G. The structure of representation defines an algebra homomorphism $\mathbb{C}[G] \longrightarrow \mathrm{End}(V)$. Since $Z(G)$ acts on V by G-equivariant endomorphisms, we have a diagram of ring homomorphisms:

$$\begin{tikzcd}
Z(G) \arrow[r, "\mathfrak{F}(V)"] \arrow[d, hook] & \mathrm{End}_G(V) \arrow[d, hook] \\
\mathbb{C}[G] \arrow[r] & \mathrm{End}(V).
\end{tikzcd}$$

If $V \in \mathrm{Irrep}(G)$, then by Schur's lemma $\mathrm{End}_G(V) = \mathbb{C}\cdot\mathrm{Id}_V$, i.e., $\mathrm{End}_G(V)$ is canonically isomorphic to $\mathbb{C}$ as an algebra. Therefore, the map $\mathfrak{F}(V) : Z(G) \longrightarrow \mathrm{End}_G(V) = \mathbb{C}$ is an element of $\mathrm{Spec}(Z(G))$.

Our map $\mathfrak{F}$ then sends V to $\mathfrak{F}(V)$.

Remark 4.5. The letter $\mathfrak{F}$ stands for "Fourier." The reason is that this map is a generalization of the (finite) Fourier transform. Indeed, when A is a finite abelian group, we have $Z(A) = \mathbb{C}[A] = \mathrm{Fun}(A)$ (but the algebra structure is the convolution algebra structure) and $\mathrm{Irrep}(A) = \widehat{A}$ the Pontryagin dual group. Then the induced map on functions $\mathfrak{F}^* : \mathrm{Fun}(A) \longrightarrow \mathrm{Fun}(\widehat{A})$ (see below) is given by the Fourier transform.

4.10. We have a map $\mathfrak{F}^* : Z(G) \longrightarrow \mathrm{Fun}(\mathrm{Irrep}(G))$ coming from $\mathfrak{F}$. Indeed, by Example 4.4 we have canonical maps:

$$Z(G) \longrightarrow \mathrm{Fun}(\mathrm{Spec}(Z(G)) \longrightarrow \mathrm{Fun}(\mathrm{Irrep}(G))$$

The following result is our present concern:

Theorem 4.6. *The induced homomorphism:*

$$\mathfrak{F}^* : Z(G) \longrightarrow \mathrm{Fun}(\mathrm{Irrep}(G))$$

is an isomorphism. In particular, by Example 4.4, the map $\mathfrak{F} : \mathrm{Irrep}(G) \longrightarrow \mathrm{Spec}(Z(G))$ *is a bijection.*

Exercise 4.7. As in Proposition 2.4, $\mathrm{Av}_G \in Z(G)$. Show that the corresponding function $\mathfrak{F}^*(\mathrm{Av}_G)$ takes the value 1 on the trivial representation and 0 on every non-trivial irreducible representation.

Corollary 4.8. $|\operatorname{Irrep}(G)| = |G \overset{ad}{/} G|$.

Proof of Corollary 4.8 assuming Theorem 4.6. We compute the dimension of both sides of the isomorphism from Theorem 4.6. By Proposition 4.2, the dimension of $Z(G)$ is $|G \overset{ad}{/} G|$, while obviously the dimension of $\operatorname{Fun}(\operatorname{Irrep}(G))$ is $|\operatorname{Irrep}(G)|$.

$\square$

This gives the following strengthening of Corollary 3.11.

Corollary 4.9. *A group G is abelian if and only if every irreducible representation of G is of dimension* 1*.*

Proof. Indeed, since $\sum_{V \in \operatorname{Irrep}(G)} \dim(V)^2 = |G|$ by Corollary 3.8, Corollary 4.8 implies that $|G \overset{ad}{/} G| = |G|$, so every conjugacy class C has order 1. But this means every element of the group is central, i.e., G is abelian.

$\square$

4.11. We will deduce Theorem 4.6 from the following:

Proposition 4.10. *The canonical map $\mathbb{C}[G] \longrightarrow \prod_{V \in \operatorname{Irrep}(G)} \operatorname{End}(V)$ is an isomorphism of algebras.*

Proof. This map is clearly an algebra homomorphism. Moreover, by Corollary 3.8, the dimension of both sides is (finite and) equal. Therefore, to see that this map is an isomorphism it suffices to show that it is injective.

Suppose $x \in \mathbb{C}[G]$ is in the kernel of the homomorphism. This means that x acts by 0 on each irreducible representation of G. By Maschke's theorem, this implies that x acts trivially on *every* finite-dimensional representation of G. In particular, x acts trivially by 0 on the left regular representation of G, i.e., for every $y \in \mathbb{C}[G]$ we have $xy = 0$. But this clearly implies that $x = 0$: indeed, for $y = 1$ we deduce that $x = x \cdot 1 = 0$.

$\square$

We now immediately deduce Theorem 4.6 from Proposition 4.10 by computing the center of $\prod_{V \in \operatorname{Irrep}(G)} \operatorname{End}(V)$ using the following elementary lemma from linear algebra:

Lemma 4.11. *For a finite-dimensional vector space V, the center of the algebra* $\operatorname{End}(V)$ *consists of scalar matrices.*

Remark 4.12. There are various easy (and elementary) ways of proving this lemma. One approach consistent with our methods is to note that V is irreducible as an $\operatorname{End}(V)$-module (in the sense that it has no proper submodules, which is true because every non-zero vector obviously generates this module under the action of $\operatorname{End}(V)$) and then use the same argument we used to prove Schur's lemma.

5. The character table

5.1. An obvious problem in the representation theory of finite groups is to "compute" all representations of a given finite group G. I.e., one would want to write down models for each of the isomorphism classes of G-representation. By Maschke's theorem, it essentially suffices to compute all irreducible representations.

However, this problem is generally difficult, and more difficult than is necessary for the applications of the theory. For many applications, it is enough to compute the "character table" of G, which will be defined below. This turns out to be more computable in practice in part because the product is of a simpler nature: it is not a sequence of vector spaces with some particular automorphisms, but merely a matrix (with as many rows and columns as G has conjugacy classes).

5.2. First, let us establish some notation.

For V a finite-dimensional representation of G, we have the function $\delta_V \in \mathrm{Fun}(\mathrm{Irrep}(G))$ defined by:

$$V_i \mapsto \dim(\mathrm{Hom}_G(V_i, V)).$$

Recall that we have defined an isomorphism $\mathfrak{F}^* : Z(G) \xrightarrow{\simeq} \mathrm{Fun}(\mathrm{Irrep}(G))$. For V as above, let $\chi_V \in Z(G)$ denote $(\mathfrak{F}^*)^{-1}(\frac{1}{\dim(V)} \cdot \delta_V)$, i.e., the element of $Z(G)$ corresponding to $\frac{1}{\dim(V)} \cdot \delta_V$ under the isomorphism $\mathfrak{F}^*$.

Remark 5.1. The scalar $\frac{1}{\dim(V)}$ appears so that we adhere to standard normalizations. It is convenient for Proposition 5.4.

5.3. Recall from the previous section that we have two bases for $Z(G)$. The first was the basis $\{b_C\}_{C \in G \overset{ad}{/} G}$ where $b_C = \frac{1}{|C|} \sum_{g \in C} \delta_g$. The second came from the isomorphism $Z(G) \xrightarrow{\simeq} \mathrm{Fun}(\mathrm{Irrep}(G))$ and the basis $\{\dim(V_i) \cdot \mathfrak{F}(V_i)\}_{V_i \in \mathrm{Irrep}(G)}$ of $\mathrm{Fun}(\mathrm{Irrep}(G))$.

Definition 5.2. The *character table* of G is the change of basis matrix for these two bases.

I.e., the character table is a matrix with rows labelled by conjugacy classes of G and columns labelled by irreducible representations of G. The entry of the matrix corresponding to $(C, V) \in G \overset{ad}{/} G \times \mathrm{Irrep}(G)$ is the χ_V-coordinate of $b_C \in Z(G)$.

Remark 5.3. Let V be an irreducible representation. The element $\chi_V \in Z(G)$ defines a function $G \longrightarrow \mathbb{C}$ as follows. For $g \in G$, recall that $[g] \in G \overset{ad}{/} G$ is associated conjugacy class. The value of our function at $g \in G$ is the $b_{[g]}$-coordinate of χ_V. By abuse of notation, we will denote the associated function $G \longrightarrow \mathbb{C}$ by χ_V.

5.4. Here is a more explicit way to describe an entry of the character table.

Proposition 5.4. *Let $\gamma \in G$ and let (V, ρ_V) be an irreducible representation of G. Then $\chi_V(g)$ is the trace $\mathrm{Tr}(\rho_V(\gamma))$ of $\rho_V(\gamma)$.*

Remark 5.5. In particular, $\rho_V(1) = \dim(V)$.

Proof. This is a matter of chasing the constructions we've given so far.

We have:

$$\mathfrak{F}^*(b_C) = \sum_{V \in \mathrm{Irrep}(G)} \mathfrak{F}(V)(b_C) \cdot \delta_V = \sum_{V \in \mathrm{Irrep}(G)} \dim(V) \cdot \mathfrak{F}(V)(b_C) \cdot \frac{1}{\dim(V)} \cdot \delta_V$$

where $\mathfrak{F} : \mathrm{Irrep}(G) \xrightarrow{\simeq} \mathrm{Spec}(Z(G))$ is as in the previous section, and by $\mathfrak{F}(V)(b_C)$ we understand the homomorphism $\mathfrak{F}(V) : Z(G) \longrightarrow \mathbb{C}$ evaluated at b_C.

Therefore, we need to compute $\dim(V) \cdot \mathfrak{F}(V)(b_C)$. By definition of $\mathfrak{F}$, this is computed as follows: by Schur's lemma, $Z(G)$ acts by scalars on V, and $\mathfrak{F}(V)(b_C)$ is the scalar by which $b_C \in Z(G)$ acts.

The trace of the operator $\rho_V(b_C)$ is therefore $\dim(V) \cdot \mathfrak{F}(V)(b_C)$. For each g such that $g \in C$, the endomorphisms $\rho_V(g)$ are conjugate (indeed, $\rho_V(x^{-1}gx) = \rho_V(x)^{-1}\rho_V(g)\rho_V(x)$). Therefore, the traces of these endomorphisms are constant. Thus, we have:

$$\mathrm{Tr}(\rho_V(b_C)) = \frac{1}{|C|} \sum_{g \in C} \mathrm{Tr}(\rho_V(g)) = \frac{1}{|C|} \sum_{g \in C} \mathrm{Tr}(\rho_V(\gamma)) = \mathrm{Tr}(\rho_V(\gamma))$$

as desired.

□

Remark 5.6. Proposition 5.4 gives a definition of the function $\chi_V : G \longrightarrow \mathbb{C}$ (factoring through $G\overset{ad}{/}G$) of any finite-dimensional representation of G.

A sour piece of terminology is that the function $\chi_V : G \longrightarrow \mathbb{C}$ is called the *character* of the representation V. Therefore, the phrase "characters of G" may refer either to characters of representations (or even just characters of irreducible representations) or to homomorphisms $\chi : G \longrightarrow \mathbb{C}^\times$. Note that the character $G \longrightarrow \mathbb{C}$ of such a homomorphism $\chi : G \longrightarrow \mathbb{C}^\times$ (regarded as a 1-dimensional representation) is just the composition $G \longrightarrow \mathbb{C}^\times \hookrightarrow \mathbb{C}$. Therefore, we will sometimes call homomorphisms $G \longrightarrow \mathbb{C}^\times$ "1-dimensional characters."

5.5. Let us give a computation of the character table in the easiest case. Let $G = \mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{Z}^{>0}$. Let σ denote the generator of $\mathbb{Z}/n\mathbb{Z}$.

By Corollary 3.11, all irreducible representations of $\mathbb{Z}/n\mathbb{Z}$ are 1-dimensional. It's easy to compute these: they are characters $\chi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^\times$, which are in clear bijection with μ_n the set of nth roots of unity by considering where the generator of $\mathbb{Z}/n\mathbb{Z}$ goes. Therefore, the columns of our matrix are labelled by μ_n.

Let ζ denote a primitive nth root of unity, so $\mu_n = \{1 = \zeta^0, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$. The character table is then given by the following matrix:

$$\mathbb{Z}/n\mathbb{Z}\left\{\overbrace{\begin{array}{cc} & \begin{array}{ccccc} 1 & \zeta & \zeta^2 & \cdots & \zeta^{n-1} \end{array} \\ \begin{array}{c} 1 \\ \sigma \\ \sigma^2 \\ \vdots \\ \sigma^{n-1} \end{array} & \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2\cdot(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{n-1} & \zeta^{2\cdot(n-1)} & \cdots & \zeta^{(n-1)\cdot(n-1)} \end{pmatrix} \end{array}}^{\mu_n=\mathrm{Irrep}(\mathbb{Z}/n\mathbb{Z})}\right. .$$

Exercise 5.7. Compute the character table of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5.6. The following describes the compatibility of characters with direct sums and tensor products:

Proposition 5.8. *Let V and W be two finite-dimensional representations of G. Then we have:*

$$\chi_{V\oplus W} = \chi_V + \chi_W$$

and:

$$\chi_{V\otimes W} = \chi_V \cdot \chi_W$$

(i.e., for $g \in G$, $\chi_{V\oplus W} = \chi_V(g) + \chi_W(g)$ and $\chi_{V\otimes W}(g) = \chi_V(g) \cdot \chi_W(g)$).

Proof. This follows from general facts about linear operators: given two finite dimensional vector spaces V and W with endomorphisms $T \in \mathrm{End}(V)$ and $S \in \mathrm{End}(W)$, the trace $\mathrm{Tr}(T \oplus S)$ (resp. $\mathrm{Tr}(T \otimes S)$) of the operator $T \oplus S \in \mathrm{End}(V \oplus W)$ (resp. $T \otimes S \in \mathrm{End}(V \otimes W)$) is the sum $\mathrm{Tr}(V) + \mathrm{Tr}(W)$ (resp. product $\mathrm{Tr}(T) \cdot \mathrm{Tr}(S)$). Applying this to the definition of the structure of representation on $V \oplus W$ and $V \otimes W$ and using Proposition 5.4, we deduce the result.

□

5.7. Now we compute the character of a permutation representation.

Proposition 5.9. *Suppose G acts on a finite set X. Then for $g \in G$, we have:*

$$\chi_{\mathrm{Fun}(X)}(g) = |\{x \in X \mid g \cdot x = x\}|.$$

Proof. This is a direct computation: we have the basis $\{\delta_x\}_{x \in X}$ of $\mathrm{Fun}(X)$ (here $\delta_x(x') = 0$ if $x \neq x'$ and $\delta_x(x) = 1$). Then $g \cdot \delta_x = \delta_{g \cdot x}$, i.e., it permutes the basis vectors. Considering the corresponding matrix immediately gives the result. ☐

Corollary 5.10. *Suppose G acts on a finite set X. Then the average number of points fixed by an element of G is* $\dim(\mathrm{Fun}(X)^G)$.

Proof. The operator $\rho_{\mathrm{Fun}(X)}(\mathrm{Av}_G)$ is a projection onto $\mathrm{Fun}(X)^G$. As with any projection operator, its trace is equal to the dimension of its image. But by Proposition 5.9, we have:

$$\chi_{\mathrm{Fun}(X)}(\mathrm{Av}_G) = \frac{1}{|G|} \sum_{g \in G} |\{x \in X \mid g \cdot x = x\}|$$

where the right hand side is exactly the average number of fixed points. ☐

Exercise 5.11. Combining this corollary with Proposition 4.3, we see that the average number of fixed points in X of an element of G is exactly the number of orbits of the action of G on X. Give a proof of this without representation theory.

5.8. Now let us proceed to discuss the numerology of the character table. These will be presented as Propositions 5.12 and 5.14. (These two relations are usually called the "orthogonality relations for characters").

Proposition 5.12. *Suppose V and W are irreducible representations of G. Let V^* be the dual representation. If $W \not\simeq V^*$, then there is an equality:*

$$\frac{1}{|G|} \sum_{g \in G} \chi_V(g) \cdot \chi_W(g) = 0.$$

For $W = V^*$, we have:

$$\frac{1}{|G|} \sum_{g \in G} \chi_V(g) \cdot \chi_{V^*}(g) = 1.$$

Proof. Consider $V \otimes W$ as a representation. By Proposition 2.4, $\mathrm{Av}_G \in Z(G)$ defines a projection operator $\rho_{V \otimes W}(\mathrm{Av}_G)$ onto the space of invariants $(V \otimes W)^G$. As for any projection operator, $\mathrm{Tr}(\rho_{V \otimes W})(\mathrm{Av}_G))$ is the dimension of its image. Since trace is additive, we therefore have:

$$\dim(V \otimes W)^G = \mathrm{Tr}(\rho_{V \otimes W}(\mathrm{Av}_G)) = \mathrm{Tr}(\frac{1}{|G|} \sum_{g \in G} \rho_{V \otimes W}) = \frac{1}{|G|} \sum_{g \in G} \chi_{V \otimes W}(g)$$

By Proposition 5.8, we have $\chi_{V \otimes W}(g) = \chi_V(g) \otimes \chi_W(g)$.

Therefore, all that needs to be proved is that for V and W irreducible, $(V \otimes W)^G$ is zero-dimensional if $W \not\simeq V^*$ and one-dimensional if $W \simeq V^*$. But since $\mathrm{Hom}(V^*, W) \xrightarrow{\simeq} V \otimes W$ as representations, we see that $\mathrm{Hom}_G(V^*, W) \xrightarrow{\simeq} (V \otimes W)^G$ and the result now follows from Schur's lemma. ☐

Corollary 5.13. *Two finite-dimensional representations are isomorphic if and only if they have the same character.*

Proof. Suppose V is a finite-dimensional representation of G. By Maschke's theorem, $V \xrightarrow{\simeq} \oplus_{V_i \in \mathrm{Irrep}(G)} V_i^{\oplus d_i}$ for some non-negative integers d_i. The set of integers d_i clearly determines the isomorphism class of V.

But by Proposition 5.12, the character of V alone determines the integers d_i since we have:

$$d_i = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \cdot \chi_{V_i^*}(g).$$

□

5.9. Now we prove the second orthogonality relation.

Proposition 5.14. *Let $g, h \in G$ be two elements of the group. If $[g] \neq [h] \in G \overset{ad}{/} G$ (i.e., if g and h are not conjugate), then we have:*

$$\sum_{V \in \mathrm{Irrep}(G)} \chi_V(g) \cdot \chi_{V^*}(h) = 0.$$

For $[g] = [h] = C$, we have:

$$\sum_{V \in \mathrm{Irrep}(G)} \chi_V(g) \cdot \chi_{V^*}(h) = \frac{|G|}{|C|}.$$

Remark 5.15. For $g = h = 1$, we have $\chi_V(1) = \dim(V)$. Therefore, the second result is a generalization of Corollary 3.8.

Proof. As in the proof of Corollary 3.8, we have:

$$\mathrm{Fun}(G) \xrightarrow{\simeq} \oplus_{V \in \mathrm{Irrep}(G)} V^* \otimes V$$

as $G \times G$-representations (note that the right hand side is a $G \times G$-representation by the initial construction from Section 2.8). We compute the trace $\chi_{\mathrm{Fun}(G)}(h, g)$ of the action of (h, g) on this space in two different ways.

By Proposition 5.9, $\chi_{\mathrm{Fun}(G)}((g, h))$ equals the number of $x \in G$ such that $hxg^{-1}(= (h, g) \cdot x) = x$, i.e., the number of x such that $x^{-1}hx = g$. This is obviously 0 if g is not conjugate to h and is equal to the order of $|G|$ divided by the order of the conjugacy class otherwise (by orbit-stabilizer).

But by the isomorphism above, we have $\chi_{\mathrm{Fun}(G)}(h, g) = \sum_{V \in \mathrm{Irrep}(G)} \chi_{V^* \otimes V}(h, g)$. However, by Proposition 5.8 (or rather, its slight generalization which has the same proof), we have:

$$\chi_{V^* \otimes V}(h, g) = \chi_{V^*}(h) \cdot \chi_V(g)$$

as desired.

□

5.10. Here is a corollary that follows trivially from the orthogonality relations.

Corollary 5.16. *(1) For V a* non-trivial *irreducible representation of G, we have:*

$$\sum_{g \in G} \chi_V(g) = 0$$

(2) For $g \neq 1$ in G, we have:

$$\sum_{V \in \mathrm{Irrep}(G)} \chi_V(g) \cdot \dim(V) = 0$$

Indeed, the first relation follows from Proposition 5.12 with W being the trivial representation and the second relation follows from Proposition 5.14 with $h = 1$.

5.11. As an application, let us compute the character table of the symmetric group S_3. First, let us recall some generalities regarding symmetric groups.

Recall that for $n \in \mathbb{Z}^{>0}$, the symmetric group S_n is defined as $\mathrm{Aut}(\{1, 2, \dots, n\})$. We write elements of S_n using their cycle decomposition.

Exercise 5.17. Two elements of S_n are conjugate if and only if the number of cycles each has of a given length are the same. In particular, the conjugacy classes of S_n are labelled by the partitions of the integer n.

Now recall that for $n \geq 2$, S_n has exactly two 1-dimensional characters $S_n \longrightarrow \mathbb{C}^\times$: the trivial character and the "sign character" ε given as a composition:

$$S_n \longrightarrow \mathbb{Z}/2\mathbb{Z} = \{\pm 1\} = \mu_2 \hookrightarrow \mathbb{C}^\times.$$

(E.g., ε can be defined by taking the determinant of the standard dimension n permutation representation of S_n.)

5.12. Now let us compute the character table of S_3.

By the above, S_3 has exactly 3 conjugacy classes, labelled by the partitions $1+1+1$, $2+1$ and 3. Note that the partition $1+1+1$ corresponds to the conjugacy class of 1, $1+2$ corresponds to the conjugacy class of (12) and 3 corresponds to the conjugacy class of (123).

We have found two irreducible representations already: the trivial representation and ε. We know that there are three (since S_3 has exactly three distinct conjugacy classes). We denote the third, as yet mysterious, representation's character by χ. Then, the character table looks as follows:

$$S_3 \overset{ad}{/} S_3 \left\{ \overbrace{\begin{array}{l} \\ 1+1+1 \\ 2+1 \\ 3 \end{array} \begin{array}{ccc} \text{triv} & \varepsilon & \chi \\ \left(\begin{array}{c} 1 \\ 1 \\ 1 \end{array}\right. & \begin{array}{c} 1 \\ -1 \\ 1 \end{array} & \left.\begin{array}{c} ? \\ ? \\ ? \end{array}\right) \end{array}}^{\text{Irrep}(S_3)} \right. .$$

However, it's easy to compute the values of χ using the orthogonality relations. First, by Corollary 3.8 we have:

$$\chi_{\text{triv}}(1)^2 + \varepsilon(1)^2 + \chi(1)^2 = 1 + 1 + \chi(1)^2 = |S_3| = 6.$$

Since $\chi(1) > 0$ (being the dimension of the associated representation) we have $\chi(1) = 2$.

Now applying Corollary 5.16, we see:

$$\chi_{\text{triv}}((12)) + \varepsilon((12)) + \chi(1) \cdot \chi((12)) = 1 - 1 + 2 \cdot \chi((12)) = 0$$
$$\chi_{\text{triv}}((123)) + \varepsilon((123)) + \chi(1) \cdot \chi((123)) = 1 + 1 + 2 \cdot \chi((123)) = 0$$

Therefore, the character table completes to give:

$$S_3 \overset{ad}{/} S_3 \left\{ \overbrace{\begin{array}{l} \\ 1+1+1 \\ 2+1 \\ 3 \end{array} \begin{array}{ccc} \text{triv} & \varepsilon & \chi \\ \left(\begin{array}{c} 1 \\ 1 \\ 1 \end{array}\right. & \begin{array}{c} 1 \\ -1 \\ 1 \end{array} & \left.\begin{array}{c} 2 \\ 0 \\ -1 \end{array}\right) \end{array}}^{\text{Irrep}(S_3)} \right. .$$

Exercise 5.18. Note that we used Corollary 5.16 (1) to compute the values of χ. Verify explicitly that the character table above satisfies the relations from Corollary 5.16 (2).

Remark 5.19. In the next section, we will explain how to construct the irreducible two-dimensional representation of S_3 whose character χ we just computed.

6. SOME EXAMPLES

6.1. Let G be a finite group and let X be a finite G-set (i.e., a finite set equipped with an action of G). As in Example 1.7 (2), we have the associated permuation representation $\mathrm{Fun}(X)$ of G.

Define $N_2(X)$ to be the number of orbits of the diagonal action of G on $X \times X$ (we note that, despite the notation, $N_2(X)$ depends not only on X, but also on the action of G).

Proposition 6.1. *We have the equality:*

$$\sum_{V_i \in \mathrm{Irrep}(G)} \dim(\mathrm{Hom}_G(V_i, \mathrm{Fun}(X))^2 = N_2(X).$$

We will prove this proposition in Section 6.3 after some preliminary remarks.

6.2. Here are some examples:

Examples 6.2. (1) Let $X = G$ equipped with the action by left translation. Then it is direct to see that $N_2(X) = |G|$. Indeed, the orbits of the action of G on $G \times G$ are labeled by elements of the group, where $(g, h) \in G \times G$ lies in the orbit for $x \in G$ if and only if $g^{-1}h = x$.

In this case, Proposition 6.1 gives the same result as Corollary 3.8.

(2) Let $G = S_n$ the symmetric group with $n \geq 2$. There is a tautological permutation representation of S_n on the set $X = \{1, \dots, n\}$. We claim that there are two orbits of S_n on $X \times X$, one which is the diagonal $X \subset X \times X$ and the other which is its complement. Indeed, clearly the diagonal is an orbit since S_n acts transitively on X. To see that the complement is, note that for $x_1 \neq x_2$ and $x'_1 \neq x'_2$ there is always an automorphism $\sigma \in S_n$ of X taking x_i to x'_i for $i = 1, 2$.[1]

Therefore, by Proposition 6.1, for $n \geq 2$ the tautological permuatation representation of S_n on $\mathbb{C}^{\oplus n}$ splits up into a direct sum of two irreducible representations. It's easy to find them: one of them is $\{v = (\lambda_1, \dots, \lambda_n) \mid \lambda_i = \lambda_j \text{ for all } i, j\}$ and the other is $\{v = (\lambda_1, \dots, \lambda_n) \mid \sum_i \lambda_i = 0\}$. In particular, we have found an irreducible representation of S_n of dimension $n - 1$.

The corresponding 2-dimensional representation of S_3 is perhaps the simplest example of an irreducible higher-dimensional representation of a finite group. Explicitly, this representation is defined by permuting coordinates on $\{(x_1, x_2, x_3) \in \mathbb{C}^{\oplus 3} \mid x_1 + x_2 + x_3 = 0\}$.

Exercise 6.3. Verify explicitly that the character S_3 corresponding to the 2-dimensional irreducible representation constructed above is given by the third column of the character table computed in Section 5.12.

6.3. Now let's give the proof of Proposition 6.1.

Proof of Proposition 6.1. By Corollary 3.10, the left hand side of the equality of the proposition is given by $\dim(\mathrm{End}_G(\mathrm{Fun}(X)))$. Therefore, it suffices to show that $\dim(\mathrm{End}_G(\mathrm{Fun}(X))) = N_2(X)$.

Note that $\mathrm{Fun}(X)^* \xrightarrow{\simeq} \mathrm{Fun}(X)$ as a representation. Indeed, there is a canonical such isomorphism of vector spaces (since $\mathrm{Fun}(X)$ has the preferred basis labelled by elements of the set X), and one immediately checks that this is actually an isomorphism of representations.

Therefore, we have:

$$\mathrm{End}_G(\mathrm{Fun}(X)) = \mathrm{Hom}_G(\mathrm{Fun}(X), \mathrm{Fun}(X)) = \mathrm{Hom}_G(\mathrm{Fun}(X)^*, \mathrm{Fun}(X)) =$$

$$= \mathrm{Hom}(\mathbb{C}, \mathrm{Fun}(X) \otimes \mathrm{Fun}(X)) = (\mathrm{Fun}(X) \otimes \mathrm{Fun}(X))^G.$$

---

[1] E.g., σ can be constructed as follows: the set $X \backslash \{x_1, x_2\}$ and $X \backslash \{x'_1, x'_2\}$ have the same order $(n - 2)$ and therefore there exists a bijection between them; define $\sigma(x_i) = x'_i$ for $i = 1, 2$ and to be some such bijection otherwise.

One immediately sees that $\mathrm{Fun}(X) \otimes \mathrm{Fun}(X)$ is isomorphic as a representation to $\mathrm{Fun}(X \times X)$, where the latter term is the permutation representation associated to the diagonal action of G on $X \times X$ (e.g., one can check this using the basis above). By Proposition 4.3, we deduce the desired result.

$\square$

6.4. Let us give an application of Example 6.2 (2). Let $G = S_n$ and let X be the set $\{1, \dots, n\}$ equipped with its tautological action of S_n.

By the example, $\dim(\mathrm{Fun}(X)^G)$ has dimension 1. Therefore, by Corollary 5.10, the average number of fixed points of an element of the symmetric group is 1.

6.5. Similarly, we can compute the standard deviation of the number of fixed points of an element of the symmetric group (acting on X as above) using this permutation representation. We assume $n \geq 2$.

We have seen that $\mathrm{Fun}(X)$ splits as a direct sum of a trivial representation $\mathbb{C}$ and an irreducible representation V. Therefore, we have $\chi_V = \chi_{\mathrm{Fun}(X)} - \chi_{triv}$. Since V is irreducible and self-dual (as in the proof of Proposition 6.1), by Proposition 5.12 we have:

$$1 = \frac{1}{|S_n|} \sum_{g \in S_n} \chi_V(g)^2 = \frac{1}{|S_n|} \sum_{g \in S_n} (\chi_{\mathrm{Fun}(X)}(g) - \chi_{triv}(g))^2$$

But $\chi_{triv}(g) = 1$ for all g, and 1 is the average number of fixed points of an element of the symmetric group. Since $\chi_{\mathrm{Fun}(X)}(g)$ is exactly the number of fixed points, we see that the square of this standard deviation is 1, so the standard deviation itself is also 1.

Remark 6.4. This analysis goes through in the general setting of a group acting 2-transitively on a set X, i.e., with precisely two orbits on $X \times X$.

Exercise 6.5. Conversely, show that if G acts on X with average number of fixed points 1 and standard deviation 1, then G acts 2-transitively on X.

Exercise 6.6. For a positive integer n, we say that G acts n-transitively on X if $|X| \geq n$ and G acts transitively on the set:

$$X^n \backslash \{(x_i)_{i=1}^n \mid x_i = x_j \text{ for some } i \neq j\}$$

of n-tuples of distinct elements of X.

1. Show that S_n acts n-transitively on $\{1, \dots, n\}$.
2. Formulate and prove an analogue of the previous exercise describing n-transitive group actions in terms of the statistics of the action.

6.6. We'll conclude this section by sketching the computation of the character table of the symmetric group S_4 using the above construction.

As in Section 5.11, the conjugacy classes of S_n are labelled by permutations of 4. There are exactly 5 of them: $1+1+1+1$, $2+1+1$, $2+2$, $3+1$ and 4. We have already found 3 irreducible representations of S_4: the trivial representation, the sign representation ε, and the 3-dimensional representation constructed in Example 6.2 (2). We easily find a fourth one by tensoring the one-dimensional character ε with our three-dimensional representation.

Computing these representations explicitly, we find that the character table of S_4 begins:

$$S_4 \overset{ad}{/} S_4 \left\{ \overbrace{\begin{array}{l c} & \begin{array}{ccccc} \text{triv} & \varepsilon & \chi_1 & \chi_2 & \chi_3 \end{array} \\ \begin{array}{l} 1+1+1+1 \\ 2+1+1 \\ 2+2 \\ 3+1 \\ 4 \end{array} & \begin{pmatrix} 1 & 1 & 3 & 3 & ? \\ 1 & -1 & 1 & -1 & ? \\ 1 & 1 & -1 & -1 & ? \\ 1 & 1 & 0 & 0 & ? \\ 1 & -1 & -1 & 1 & ? \end{pmatrix} \end{array}}^{\mathrm{Irrep}(S_4)} \right. .$$

Finally, as in the case of S_3, we use Corollary 5.16 (1) to find the last column of the character table, giving the result:

$$S_4 \overset{ad}{/} S_4 \left\{ \overbrace{\begin{array}{l c} & \begin{array}{ccccc} \text{triv} & \varepsilon & \chi_1 & \chi_2 & \chi_3 \end{array} \\ \begin{array}{l} 1+1+1+1 \\ 2+1+1 \\ 2+2 \\ 3+1 \\ 4 \end{array} & \begin{pmatrix} 1 & 1 & 3 & 3 & 2 \\ 1 & -1 & 1 & -1 & 0 \\ 1 & 1 & -1 & -1 & 2 \\ 1 & 1 & 0 & 0 & -1 \\ 1 & -1 & -1 & 1 & 0 \end{pmatrix} \end{array}}^{\mathrm{Irrep}(S_4)} \right. .$$

Exercise 6.7. Verify all this.

6.7. Let us construct explicitly this last irreducible representation of S_4. Recall that there is a surjective homomorphism $\varphi : S_4 \longrightarrow S_3$ realizing S_3 as a quotient of S_4. This is a "special" map in that no analogue of it exists for other symmetric groups (one can show that for $n \neq 4$ any proper, normal subgroup of S_n is the alternating group). Its construction is therefore of a somewhat special nature, appealing in particular to classical Euclidean geometry.

Then, to obtain the irreducible representation of S_4 corresponding to the last column of the character table, simply restrict the irreducible 2-dimensional representation of S_3 along the map φ.

6.8. Let us construct the homomorphism φ. Recall that S_4 is the group $\mathrm{Aut}(\Box_3)$ of rigid automorphisms of the cube in $\mathbb{R}^3$ (i.e., the group of orientation-preserving isometries of $\mathbb{R}^3$ preserving the cube with vertices at $(\pm 1, \pm 1, \pm 1)$). Indeed, let V be the set of vertices of the cube: this is a set of order 8 with a free action of $\mathbb{Z}/2\mathbb{Z}$ sending a vertex v to $-v$. The action of $\mathrm{Aut}(\Box_3)$ on V induces an action of $\mathrm{Aut}(\Box_3)$ on $V/(\mathbb{Z}/2\mathbb{Z})$. Since $|V/(\mathbb{Z}/2\mathbb{Z})| = 4$, this gives a map $\mathrm{Aut}(\Box_3) \longrightarrow S_4$. In words: the map is defined by acting on opposite pairs of vertices.

Exercise 6.8. Show that the map $\mathrm{Aut}(\Box_3) \longrightarrow S_4$ which we constructed is an isomorphism. Hint: first, show it is injective, then show that it contains all transpositions in S_4.

Therefore, it suffices to give an action of $\mathrm{Aut}(\Box_3)$ on a set with three elements to define a map $S_4 \longrightarrow S_3$. The pairs of opposite faces on the cube provide just such a set. One immediately verifies that this is actually a surjective map.

Exercise 6.9. Compute explicitly that the induced two-dimensional irreducible representation of S_4 (pulled-back from S_3 via φ) has character given by the fifth column of the character table above. Also prove this without computing anything.

7. ARITHMETIC

7.1. The principal goal for this section is to prove the following theorem:

Theorem 7.1. *For a finite group G, the dimension* $\dim(V)$ *of any irreducible representation V divides $|G|$.*

This result is of a number-theoretic flavor, so will need to develop some techniques from algebraic number theory to prove it. Therefore, we will need to give a digression on algebraic integers before returning to representation theory.

7.2. Let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of the rational numbers $\mathbb{Q}$. By a *lattice*, we understand a finite rank free $\mathbb{Z}$-module.

Lemma-Definition 7.2. *For $x \in \overline{\mathbb{Q}}$, the following are equivalent:*

(1) There exist integers $a_1, \ldots a_n \in \mathbb{Z}$ such that $x^n + a_1 \cdot x^{n-1} + \ldots + a_n = 0$.

(2) There exists a lattice Λ with an endomorphism T such that x is an eigenvalue of $T \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$.

When these conditions are satisfied, we say that x is an algebraic integer.

Remarks 7.3. (1) We will denote the set of algebraic integers by $\mathcal{O} \subset \overline{\mathbb{Q}}$.

(2) Note that the first condition says that x is the root to a *monic* polynomial with coefficients in $\mathbb{Z}$. It's clear that every element of $\overline{\mathbb{Q}}$ is a root of a polynomial with coefficient in $\mathbb{Z}$ (just clear denominators), so the condition that this polynomial is monic is essential.

(3) For any algebraically closed field $\mathbb{C}$ of characteristic zero, we will slightly abuse notation by defining $\mathcal{O} \subset \mathbb{C}$ as the subset of $\mathbb{C}$ consisting of elements satisfying (1) from the Lemma-Definition. After an identification of $\overline{\mathbb{Q}}$ with the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, this subset of $\mathbb{C}$ is identified with the subset of $\overline{\mathbb{Q}}$ of algebraic integers.

(4) One feature distinguishing $\mathcal{O}$ from $\overline{\mathbb{Q}}$ is that $\mathcal{O}$ is not a field: this follows from Proposition 7.5 below. E.g., for p a prime number, one can show that $\mathcal{O}/p \cdot \mathcal{O}$ is an algebraic closure of the finite field $\mathbb{F}_p$ of order p.

(5) One can show that $\mathcal{O}$ is non-Noetherian.

Proof. First, let us show that (2)⇒(1). Choosing a basis for Λ, we see that T is given by a matrix with coefficient in $\mathbb{Z}$. Therefore, its characteristic polynomial is a monic polynomial with coefficients in $\mathbb{Z}$ so any root satisfies 1.

For the converse, note that if $x^n + a_1 \cdot x^{n-1} + \ldots + a_n = 0$, then x is an eigenvalue of the matrix:

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_n \\ 1 & 0 & \ldots & 0 & -a_{n-1} \\ 0 & 1 & \ldots & 0 & -a_{n-2} \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \ldots & 1 & -a_0 \end{pmatrix}$$

Indeed, the characteristic polynomial of this matrix is the polynomial $p(\lambda) = \lambda^n + a_1 \cdot \lambda^{n-1} + \ldots + a_n$. Therefore, setting $\Lambda = \mathbb{Z}^{n+1}$ and T to be the operator defined by this matrix gives the result. □

7.3. Let us give some examples of algebraic integers:

Examples 7.4. (1) The integers $\mathbb{Z} \subset \mathbb{Q}$ are contained in $\mathcal{O}$, since every $n \in \mathbb{Z}$ is a root of the monic polynomial $x - n$.

(2) If ζ is a root of unity, then ζ is an algebraic integer since ζ is a root of $x^n - 1$ for some appropriate n.

(3) Let A be a commutative ring which is finitely generated as an abelian group (under addition), i.e., a finite $\mathbb{Z}$-algebra. Let $\chi : A \longrightarrow \overline{\mathbb{Q}}$ be any homomorphism. Then for every $a \in A$, we claim that $\chi(a) \in \mathcal{O}$.

Indeed, let Λ be the image $\chi(A) \subset \overline{\mathbb{Q}}$. This is a finitely generated abelian group (because A is) and is torsion-free (because $\overline{\mathbb{Q}}$ is) and therefore a finite rank free $\mathbb{Z}$-module (by the classification theory of finitely generated $\mathbb{Z}$-modules), i.e., Λ is a lattice. Then $a \in A$ defines an endomorphism of Λ given by multiplication by $\chi(a)$. One of the eigenvalues of this operator is $\chi(a)$ (it is assocaited to the eigenvector $\chi(1) = 1$). Therefore, $\chi(a)$ fits the paradigm of Lemma-Definition 7.2 (2).

(4) We will not need the following example (which may be regarded as an exercise for the reader): if d is a square-free integer, then for $a, b \in \mathbb{Q}$, $a + b\sqrt{d}$ is an algebraic integer if and only if:
   (a) $a, b \in \mathbb{Z}$, or:
   (b) $d = 1 \mod 4$, $a, b \in \frac{1}{2} \cdot \mathbb{Z}$ and $a - b \in \mathbb{Z}$.

E.g., the "golden ratio" $\frac{1+\sqrt{5}}{2}$ satisfies (4b) and is an algebraic integer since it is a root of the quadratic polynomial $x^2 - x - 1$.

7.4. The following is a fundamental result about $\mathcal{O}$.

Proposition 7.5. *The set $\mathcal{O}$ of algebraic integers is a subring of $\overline{\mathbb{Q}}$. The intersection of $\mathcal{O}$ with $\mathbb{Q}$ is exactly $\mathbb{Z}$.*

Proof. We need to show that $\mathcal{O}$ is closed under addition and multiplication in $\overline{\mathbb{Q}}$. We will do this using characterization (2) of algebraic integers. If x, y are eigenvalues of (Λ, T) and (Λ', S) (where these are pairs of a lattice and an endomorphism), then $x \cdot y$ is an eigenvalue of:

$$(\Lambda \otimes \Lambda', T \otimes S)$$

and $x + y$ is an eigenvalue of

$$(\Lambda \otimes \Lambda', T \otimes \mathrm{Id}_{\Lambda'} + \mathrm{Id}_{\Lambda} \otimes S).$$

That $\mathcal{O} \bigcap \mathbb{Q} = \mathbb{Z}$ is immediate from characterization (1) of algebraic integers and Gauss' lemma. ☐

Remark 7.6. With this proposition, we can explain the use of $\mathcal{O}$ in proving Theorem 7.1. Namely, we will show that $\frac{|G|}{\dim(V)} \in \mathcal{O}$ for any irreducible representation V. Since this number is rational, by the proposition it must be integral.

7.5. The connection between algebraic integers and representation theory of finite groups is given by the following:

Proposition 7.7. *For every finite-dimensional representation V of a finite group G and for every $g \in G$, $\chi_V(g) \in \mathcal{O}$.*

We will deduce Proposition 7.7 from the following more precise statement:

Proposition 7.8. *For every finite-dimensional representation V of a finite group G and for every $g \in G$, $\rho_V(g)$ is a diagonalizable matrix with each eigenvalue a $|G|$-th root of unity.*

Remarks 7.9. (1) Of course, the matrices $\{\rho_V(g)\}_{g \in G}$ are not simultaneously diagonalizable unless ρ_V factors through the abelianization of G.

(2) A more precise statement holds (and follows immediately from the proof): if g has order n, then $\rho_V(g)$ has nth roots of unity as eigenvalues.

Proof that Proposition 7.8 ⇒ Proposition 7.7. We have seen in Example 7.4 (2) that roots of unity are algebraic integers. Since the trace is the sum of the eigenvalues and since algebraic integers form a ring by Proposition 7.5, we immediately deduce the result.

$\square$

Proof of Proposition 7.8. Let $n := |G|$. For every $g \in G$, we have $g^n = 1$, and therefore $(\rho_V(g))^n = \mathrm{Id}_V \in \mathrm{End}(V)$. We deduce that the minimal polynomial of $\rho_V(g)$ divides the polynomial $x^n - 1$. Since $x^n - 1$ is a separable polynomial (i.e., it has distinct roots), this means that the minimal polynomial of $\rho_V(g)$ is also separable. But any matrix with separable minimal polynomial is clearly diagonalizable. Since the minimal polynomial divides $x^n - 1$, we see that all the eigenvalues of $\rho_V(g)$ are nth roots of unity.

$\square$

Exercise 7.10. Using the counterexample from Remark 2.2 (2), show that the diagonalizability of $\rho_V(g)$ fails if the characteristic of the ground field is non-zero. Where does the proof of Proposition 7.8 fail in this case?

7.6. We will also need the following variant of Proposition 7.7.

Proposition 7.11. *Let V be an irreducible representation of G. Then for every $g \in G$ with associated conjugacy class $C \in G \overset{ad}{/} G$, we have:*

$$\frac{|C|}{\dim(V)} \cdot \chi_V(g) \in \mathcal{O}.$$

Proof. Let $\mathbb{Z}[G] \subset \mathbb{C}[G]$ be the subalgebra:

$$\{\sum_{g \in G} a_g \cdot \delta_g \mid a_g \in \mathbb{Z} \text{ for all } g \in G\}.$$

Let $Z_{int}(G) \subset Z(G)$ be the subalgebra $Z(G) \cap \mathbb{Z}[G]$. Note that $Z_{int}(G)$ has the $\mathbb{Z}$-basis $\{b_C^{naive}\}_{C \in G \overset{ad}{/} G}$ where $b_C^{naive} := |C| \cdot b_C = \sum_{g \in C} \delta_g$. In particular, $Z_{int}(G)$ is finitely generated as an abelian group.

Let $\mathfrak{F}(V) \in \mathrm{Spec}(Z(G))$ be the character of $Z(G)$ associated to V by $\mathfrak{F}$. By Example 7.4 (3), $\mathfrak{F}(V)(z) \in \mathcal{O}$ for all $z \in Z_{int}(G)$. In particular, applying this to b_C^{naive}, we see that $\mathfrak{F}(V)(b_C^{naive}) \in \mathcal{O}$.

For $g \in C$, we have:

$$\chi_V(g) = \dim(V) \cdot \mathfrak{F}(V)(b_C) = \frac{\dim(V)}{|C|} \cdot \mathfrak{F}(V)(b_C^{naive}).$$

Since $\mathfrak{F}(V)(b_C^{naive}) \in \mathcal{O}$ by the above, we see that:

$$\frac{|C|}{\dim(V)} \cdot \chi_V(g) \in \mathcal{O}$$

as desired.

$\square$

Remark 7.12. Propositions 7.7 and 7.11 tell us that for an irreducible[2] representation V and $g \in G$, $\chi_V(g)$ and $\frac{|C|}{\dim(V)} \cdot \chi_V(g)$ are both algebraic integers. Although these two numbers are rational multiples of each other, neither of these statements is strictly stronger than the other. (In fact, the interaction of these two statements will ultimately be responsible for the results of this section and the next).

Indeed, if $\dim(V) = 1$, then $\chi_V(g) \in \mathcal{O}$ clearly implies $|C| \cdot \chi_V(g) \in \mathcal{O}$. But if $|C| = 1$ (i.e., the unique element in C is central in G), then $\frac{1}{\dim(V)} \cdot \chi_V(g) \in \mathcal{O}$ clearly implies that $\chi_V(g) \in \mathcal{O}$.

---

[2] Note that Proposition 7.7 does not need this hypothesis.

7.7. Finally, we are prepared to prove Theorem 7.1.

Proof of Theorem 7.1. We may assume V is a non-trivial irreducible representation.

By Proposition 5.12, we have:

$$|G| = \sum_{g \in G} \chi_V(g) \cdot \chi_{V^*}(g) = \sum_{C \in G \overset{ad}{/} G} |C| \cdot \chi_V(b_C).$$

Therefore, we have:

$$\frac{|G|}{\dim(V)} = \sum_{g \in G} \left(\frac{|C|}{\dim(V)} \cdot \chi_V(g) \right) \cdot \chi_{V^*}(g).$$

By Propositions 7.7 and 7.11, the right hand side of the above equation is in $\mathcal{O}$. Therefore, we deduce that $\frac{|G|}{\dim(V)} \in \mathcal{O}$. Clearly $\frac{|G|}{\dim(V)} \in \mathbb{Q}$, so we deduce that $\frac{|G|}{\dim(V)} \in \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$.

☐

7.8. We conclude this section with a result of a different flavor, but which is of an arithmetic nature similar to what we have discussed in this section.

Proposition 7.13. *For every n, the character table of the symmetric group S_n has integer entries.*

We will give the proof of Proposition 7.13 in the remainder of this section.

Remark 7.14. Our earlier computations corroborate this proposition when $n \leq 4$.

7.9. We immediately deduce Proposition 7.13 from the following two lemmas.

Lemma 7.15. *Let G be a finite group with the following property:*

(*): *For every $g \in G$ of order n and for every $m \in \mathbb{Z}^{>0}$ relatively prime to n, g^m is conjugate to g.*

Then for every $g \in G$ and every representation V of G, $\chi_V(g) \in \mathbb{Z}$. I.e., the character table of G is an integral matrix.

Lemma 7.16. *The symmetric group S_n satisfies the property $(*)$ from Lemma 7.15.*

Proof of Lemma 7.16. This is immediate from the description of conjugacy classes in S_n from Section 5.11.

Indeed, if $g \in S_n$ has cycles of lengths $\ell_1, \ldots, \ell_r$ (so $\sum_{i=1}^r \ell_i = S_n$), then the order of g is the least common multiple of the set $\{\ell_i\}_{i=1}^r$. This means $m \in \mathbb{Z}^{>0}$ is relatively prime to the order of g if and only if it is relatively prime to each ℓ_i. But iterating a cycle of length ℓ_i to a power prime to ℓ_i gives another cycle of length ℓ_i.

☐

Proof of Lemma 7.15. Suppose $g \in G$ of order n and V is a finite-dimensional representation of G.

Let $K \subset \overline{\mathbb{Q}}$ be the subfield of $\mathbb{Q}$ spanned by the nth roots of unity. By the irreducibility of the cyclotomic polynomial, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is $(\mathbb{Z}/n \cdot \mathbb{Z})^\times$, where $\sigma \in (\mathbb{Z}/n \cdot \mathbb{Z})^\times$ acts on a root of unity ζ by sending ζ to ζ^σ. We will denote the action of $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/n \cdot \mathbb{Z})^\times$ by $\cdot$, so e.g. $\sigma \cdot \zeta = \zeta^\sigma$.

We have seen in Proposition 7.7 that $\chi_V(g) \in \mathcal{O}$. Therefore, to see that $\chi_V(g) \in \mathbb{Z}$, it suffices to show that $\chi_V(g) \in \mathbb{Q}$ since $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$. By Galois theory, $\chi_V(g) \in \mathbb{Q}$ if and only if it is invariant under the action of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, i.e., if and only if $\sigma \cdot \chi_V(g) = \chi_V(g)$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Since $\rho_V(g)$ is diagonal with nth roots of unity as eigenvalues (c.f. Remark 7.9 (2)), the description of the action of the Galois group above shows that for $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/r \cdot \mathbb{Z})^\times$, we have:

$$\mathrm{Tr}((\rho_V(g)^\sigma) = \sigma \cdot \chi_V(g).$$

Since $\rho_V(g)^\sigma = \rho_V(g^\sigma)$ and since we have g^σ conjugate to g by assumption, this implies:

$$\mathrm{Tr}(\rho_V(g^\sigma)) = \mathrm{Tr}(\rho_V(g))$$

and comparing this to the above gives $\sigma \cdot \chi_V(g) = \chi_V(g)$ as desired.

□

8. Burnside's theorem

8.1. Throughout this section, we fix p, q two distinct primes. The goal for this section is to prove the following theorem:

Theorem 8.1 (Burnside)**.** *Every group G of order $|G| = p^a q^b$ for $a, b \in \mathbb{Z}^{\geq 0}$ is solvable.*

Remark 8.2. Recall that a group G is *solvable* if it has a filtration $\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ such that G_{i+1}/G_i is abelian for all $0 \leq i < n$. (To clarify the notation: we mean that G_i is normal in G_{i+1}, but do not require that it is normal in all of G).

Remark 8.3. To prove Burnside's theorem, it is enough to show that every group of order $p^a q^b$ with $a + b > 1$ has a proper normal subgroup. Indeed, then the result follows by induction on $a + b$, noting that every group of order p (or q) is abelian.

Corollary 8.4. *Every non-abelian simple group has order with at least three prime factors.*

Remark 8.5. The Feit-Thompson theorem, a deep result in finite group theory, says that every group of odd order is solvable. This gives a much more precise version of Corollary 8.4: every non-abelian simple group has order divisible by 2 and at least two odd primes.

This result is in some sense optimal. Indeed, the alternating group $A_5 (:= \mathrm{Ker}(\varepsilon : S_5 \longrightarrow \{\pm 1\})$ is known to be simple, and its order is $\frac{5!}{2} = 60 = 2^2 \cdot 3 \cdot 5$.

8.2. We will deduce Theorem 8.1 from the following result, also due to Burnside.

Theorem 8.6. *Suppose G is a group with a conjugacy class C of order $|C| = p^k$ where p is a prime, $C \neq \{1\}$. Then either G is cyclic of prime order or else G admits a proper normal subgroup.*

Remark 8.7. This theorem immediately implies that every conjugacy class $C \neq \{1\}$ in a non-abelian simple group has order divisible by at least two primes.

Proof that Theorem 8.6 ⇒ Theorem 8.1. Let G be a group of order $p^a \cdot q^b$ with $a + b > 1$. By Remark 8.3, it suffices to show that G has a proper normal subgroup. Since $a + b > 1$, we see that G is not a cyclic group of prime order. Therefore, by Theorem 8.6, it suffices to show that G has a conjugacy class $C \neq \{1\}$ of order a prime power.

Suppose otherwise. Then every conjugacy class $C \neq \{1\}$ has order divisible by $p \cdot q$. We have:

$$|G| = \sum_{C \in G \overset{ad}{/} G} |C| = 1 + \sum_{C \in (G \overset{ad}{/} G \setminus \{1\})} |C|.$$

Reducing modulo p (or q), we arrive at a contradiction.

□

Therefore, for the remainder of the section we will be concerned with proving Theorem 8.6.

8.3. We will use the following lemma:

Lemma 8.8. *Let $\zeta_1, \ldots, \zeta_n$ be roots of unity such that:*

$$\frac{\sum_{i=1}^n \zeta_i}{n} \in \mathcal{O}.$$

Then, either:

(1) $\zeta_i = \zeta_j$ for all i, j, or:
(2) $\sum_{i=1}^n \zeta_i = 0$.

Proof. Let us denote by ξ the sum:

$$\xi := \frac{\sum_{i=1}^n \zeta_i}{n} \in \mathcal{O}.$$

Let $| \cdot |$ denote the complex absolute value. Let us assume $\zeta_i \neq \zeta_j$ for some i, j. By the triangle inequality, if $\zeta_i \neq \zeta_j$ for some i, j then we have $|\xi| < 1$. We need to show that this implies that $\xi = 0$.

Suppose that all the ζ_i are rth roots of unity, and let $K \subset \overline{\mathbb{Q}}$ be the field spanned by the rth roots of unity (so $\zeta_i \in K$ for all i). As in the proof of Lemma 7.15, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is $(\mathbb{Z}/r\mathbb{Z})^\times$, where $\sigma \in (\mathbb{Z}/r\mathbb{Z})^\times$ acts by sending ζ to ζ^σ.

For any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, observe that $\sigma \cdot \xi$ is also an algebraic integer (indeed: $\sigma \cdot \xi$ is clearly a root of any polynomial with rational coefficients having ξ as a root, and in particular any monic one). Moreover, by the above description of the Galois group, we see that $\sigma \cdot \xi$ also has the same form: $n \cdot (\sigma \cdot \xi)$ is a sum of n roots of unity, so $|\sigma \cdot \xi| < 1$ as well.

Therefore, we see that:

$$|\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma \cdot \xi| = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} |\sigma \cdot \xi| < 1.$$

Note that:

$$\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma \cdot \xi \in \mathcal{O}$$

since this term is a product of elements of $\mathcal{O}$. We also observe that

$$\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma \cdot \xi \in \mathbb{Q}$$

because K is Galois over $\mathbb{Q}$ and $\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma \cdot \xi$ is obviously invariant under the Galois group. Therefore, we have:

$$\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma \cdot \xi \in \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}.$$

Thus, this product is an integer of absolute value strictly less than 1 and therefore zero. This implies that $\sigma \cdot \xi = 0$ for some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, which immediately gives that $\xi = 0$ as desired.

□

8.4. We will also need the following (easy) lemma about algebraic integers:

Lemma 8.9. *Suppose $m, n \in \mathbb{Z}$ are relatively prime and $x \in \mathcal{O}$ such that $\frac{m}{n} \cdot x \in \mathcal{O}$. Then $\frac{1}{n} \cdot x \in \mathcal{O}$.*

Proof. Since m, n are relatively prime, there exists $r, s \in \mathbb{Z}$ such that $rm + sn = 1$. Then:

$$\frac{1}{n} \cdot x = \frac{rm + sn}{n} \cdot x = r \cdot (\frac{m}{n} \cdot x) + s \cdot x.$$

Since $\frac{m}{n} \cdot x$ and x are algebraic integers, the result follows.

□

8.5. Our principal application of Lemma 8.8 is the following:

Proposition 8.10. *Let C be a conjugacy class of a finite group G of order p^k for p a prime and $k \geq 1$. Suppose V is an irreducible representation of G of dimension prime to p such that $\chi_V(b_C) \neq 0$. Then every $g \in C$ acts on V by a scalar matrix.*

Proof. Let $g \in C$. By Proposition 7.11, we have:

$$\frac{|C|}{\dim(V)} \cdot \chi_V(g) \in \mathcal{O}.$$

Since $|C|$ and $\dim(V)$ are relatively prime, Lemma 8.9 implies $\frac{1}{\dim(V)} \cdot \chi_V(g) \in \mathcal{O}$.

However, by Proposition 7.8, $\chi_V(g)$ is a sum of $\dim(V)$-many roots of unity. Therefore, by Lemma 8.8 (and since we assume $\chi_V(g) \neq 0$) all of these eigenvalues must be equal, i.e., the corresponding operator is a scalar operator.

□

8.6. Now we are ready to prove Theorem 8.6 (and thereby Theorem 8.1). The proof will occupy Sections 8.7-8.10.

8.7. Let G be a group with a conjugacy class $C \neq \{1\}$ of order p^k. If $k = 0$, then G has a nontrivial central element (the sole occupant of C) and a non-zero center, so in this case the result is clear. Therefore, it suffices to prove the result when $k \geq 1$.

8.8. Next, we reduce to the case where every non-trivial representation V of G has dimension greater than 1.

Otherwise, G admits a non-trivial homomorphism to $\mathbb{C}^\times$, and since G is non-cyclic the kernel of this homomorphism is a proper normal subgroup (since the image is a finite subgroup of $\mathbb{C}^\times$ and therefore cyclic).

8.9. We claim that there exists a non-trivial irreducible representation V of order prime to p such that $\chi_V(g) \neq 0$ for $g \in C$.

Indeed, suppose otherwise. By Corollary 5.16 (2), we have:

$$|C| = \sum_{V \in \mathrm{Irrep}(G)} \chi_V(g) \cdot \dim(V).$$

Since each $\chi_V(g)$ is in $\mathcal{O}$, we can reduce the left hand side modulo $p \in \mathbb{Z} \subset \mathcal{O}$ to obtain:

$$0 = |C| = \sum_{V \in \mathrm{Irrep}(G)} \chi_V(g) \cdot \dim(V) = \sum_{\substack{V \in \mathrm{Irrep}(G) \\ p \nmid \dim(V)}} \chi_V(g) \cdot \dim(V) = 1 + \sum_{\substack{V \in \mathrm{Irrep}(G) \\ p \nmid \dim(V) \\ V \text{ non-trivial}}} \chi_V(g) \mod p.$$

(Here $\mod p$ means "in the ring $\mathcal{O}/p\mathcal{O}$"). Since the ring $\mathcal{O}/p\mathcal{O} \neq 0$ (by virtue of containing, e.g., $\mathbb{Z}/p\mathbb{Z}$), this means that:

$$0 \neq \sum_{\substack{V \in \mathrm{Irrep}(G) \\ p \nmid \dim(V) \\ V \text{ non-trivial}}} \chi_V(g) \mod p.$$

In particular, there must exist some representation V of the described type such that $\chi_V(g) \neq 0$, since this holds $\mod p$.

8.10. Let V be an irreducible representation as described above: non-trivial of dimension prime to p.

Define $N \lhd G$ as $\rho_V^{-1}(\mathbb{C}^\times \cdot \mathrm{Id}_V)$ (i.e., $\mathrm{Ker}(G \longrightarrow GL(V)/\mathbb{C}^\times \cdot \mathrm{Id}_V)$). Since $\dim(V) > 1$, $N \neq G$. By Proposition 8.10, $C \subset N$, so in particular $N \neq \{1\}$. Thus, we have found a non-trivial normal subgroup of G, as desired.

9. INDUCED REPRESENTATIONS

9.1. This section is devoted to another technique of producing new representations from old. More precisely, "induction" takes representations of a subgroup and produces representations of the group.

9.2. Let $H \subset G$ be a subgroup and let W be an H-representation. We will define two G-representations $\mathrm{ind}_H^G(W)$ and $\mathrm{Ind}_H^G(W)$ characterized by isomorphisms for every G-representation V (functorial in both variables):

$$\mathrm{Hom}_G(\mathrm{ind}_H^G(W), V) \xrightarrow{\simeq} \mathrm{Hom}_H(W, V) \qquad \mathrm{Hom}_G(V, \mathrm{Ind}_H^G(W)) \xrightarrow{\simeq} \mathrm{Hom}_H(V, W)$$

Here we regard V as an H-representation by restriction.

Examples 9.1. Suppose $H = \{1\}$.

1. For any H-module W, i.e., vector space W, we have $\mathrm{ind}_H^G(W) = \mathbb{C}[G] \otimes_{\mathbb{C}} W$.
2. Similarly, for such W, by Lemma 1.8 we have $\mathrm{Ind}_H^G(W) = \mathrm{Fun}(G) \otimes W$.

9.3. Let us first construct $\mathrm{ind}_H^G(W)$.

There is a more general setup for this construction. Let A and B be two algebras with a map $f : A \longrightarrow B$. Then for any A-module M, the tensor product $B \otimes_A M$ admits an obvious B-module structure (from the left B-module structure on B) and satisfies:

$$\mathrm{Hom}_{B\text{-mod}}(B \underset{A}{\otimes} M, N) \xrightarrow{\simeq} \mathrm{Hom}_{A\text{-mod}}(M, N).$$

(The isomorphism is induced by restriction along the map $M = A \otimes_A M \overset{f \otimes \mathrm{Id}_M}{\longrightarrow} B \otimes_A M$.)

Applying this in the case of group algebras, we see that defining $\mathrm{ind}_H^G(W)$ as $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$, we obtain the desired properties.

9.4. Next, let us construct $\mathrm{Ind}_H^G(W)$. We will imitate the construction from Example 9.1 (2).

Consider $\mathrm{Fun}(G) \otimes W$. More explicitly, this is the vector space of functions $\{f : G \longrightarrow W\}$. Considering this space as a G-module via the (permutation) G-representation structure coming from the *right*[3] action of G on itself (and forgetting the action of H on W), we see that this satisfies the property that for any G-representation V we have:

$$\mathrm{Hom}_G(V, \mathrm{Fun}(G) \otimes W) \xrightarrow{\simeq} \mathrm{Hom}(V, W).$$

Note that $W \otimes \mathrm{Fun}(G)$ also has a commuting structure of H-module, where this structure comes from the action of H (by way of G) on $\mathrm{Fun}(G)$ corresponding to the *left* action of H on G combined with the H-module structure on W. Under the isomorphism above, this corresponds to the H-module structure on $\mathrm{Hom}(V, W)$ coming from realizing both V and W as H-representations.

Therefore, we can form $(\mathrm{Fun}(G) \otimes W)^H$ (the H-module structure as above) and we retain a G-action on this space. Moreover, we see that:

$$\mathrm{Hom}_G(V, (\mathrm{Fun}(G) \otimes W)^H) \xrightarrow{\simeq} \mathrm{Hom}(V, W)^H = \mathrm{Hom}_H(V, W).$$

Therefore, we define $\mathrm{Ind}_H^G(W)$ as $(\mathrm{Fun}(G) \otimes W)^H$.

---

[3] Unsurprisingly, this normalization doesn't matter, but we have to choose something to work with consistently.

9.5. Let us take a moment to write more explicit formulae for Ind_H^G.

One realizes $\mathrm{Ind}_H^G(W)$ as the following subspace of W-valued functions on G:

$$\{f : G \longrightarrow W \mid f(h \cdot g) = h \cdot f(g) \text{ for all } g \in G, h \in H\}.$$

The action of G on this space of functions is given by:

$$(g \cdot f)(x) = f(x \cdot g).$$

Given an H-equivariant map $T : V \longrightarrow W$ (with V a G-representation), the induced map $V \longrightarrow \mathrm{Ind}_H^G(W)$ sends v to the function $f_v : G \longrightarrow W$:

$$f_v : g \mapsto T(g \cdot v).$$

This lands in the desired space of functions since for $h \in H$ we have:

$$f_v(h \cdot g) := T(h \cdot g \cdot v) = h \cdot T(g \cdot v) = h \cdot f_v(g)$$

by H-equivariance of T.

Remark 9.2. In the tensorial language, the map $V \longrightarrow (\mathrm{Fun}(G) \otimes W)^H$ is the map:

$$v \mapsto \sum_{g \in G} T(g \cdot v) \otimes \delta_g.$$

Exercise 9.3. Suppose that H acts on a finite set X. Define the set $G \overset{H}{\times} X$ to be the set $(G \times X)/H$ where H acts diagonally via its right action on G. Note that G acts on $G \overset{H}{\times} X$ via its left action on G.

Considering $\mathrm{Fun}(X)$ as a permutation representation of H, show that:

$$\mathrm{Ind}_H^G(\mathrm{Fun}(X)) \xrightarrow{\simeq} \mathrm{Fun}(G \overset{H}{\times} X)$$

as G-representations.

In particular, $\mathrm{Ind}_H^G(\mathbb{C})$ is the permutation representation $\mathrm{Fun}(G/H)$.

9.6. Let us give an example in the case of cyclic groups.

Suppose n and m are integers with n dividing m, so we have $\mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}/m\mathbb{Z}$ (sending the generator to the residue class of $\frac{m}{n}$, which we also denote by $\frac{m}{n}$). Suppose $\chi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^\times$ send the generator to a root of unity ζ.

Let us compute $\mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{\mathbb{Z}/m\mathbb{Z}} \chi$. This is the space of functions $f : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{C}$ which satisfies the equivariance property:

$$f(x + \frac{m}{n}) = \zeta \cdot f(x).$$

Therefore, such functions form a $\frac{m}{n}$-dimensional space with basis $\{\delta_i\}_{i=0}^{\frac{m}{n}-1}$. The matrix of the generator of $\mathbb{Z}/m\mathbb{Z}$ with respect to this basis is:

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ \zeta & 0 & 0 & \dots & 0 \end{pmatrix}$$

Remark 9.4. In particular, we see that as long as $n \neq m$, the character of the induced representation of χ has value zero on the generator of $\mathbb{Z}/m\mathbb{Z}$. Since every representation of V decomposes as a direct sum of characters and because induction commutes with direct sums, we see that this is true for every representation of $\mathbb{Z}/m\mathbb{Z}$ induced from a representation of a proper cyclic subgroup.

9.7. We will prove the following result:

Theorem 9.5 (Frobenius' reciprocity theorem)**.** *There is a natural isomorphism of G-representations $\varphi : \mathrm{ind}_H^G(W) \xrightarrow{\simeq} \mathrm{Ind}_H^G(W)$.*

Remarks 9.6.
1. Although the above constructions of ind and Ind carry through in the case of infinite groups, Frobenius reciprocity requires that the groups be finite.
2. Frobenius reciprocity is useful in part because (as we will see) Ind_H^G is easier to compute with for many purposes, so this allows us to deduce results about ind_H^G as well. E.g., we will use this later in this section (see Section 9.16) to compute the character of an induced representation.
3. Some texts refer to the mere (defining) identities:

$$\mathrm{Hom}_G(\mathrm{ind}_H^G(W), V) \xrightarrow{\simeq} \mathrm{Hom}_H(W, V) \qquad \mathrm{Hom}_G(V, \mathrm{Ind}_H^G(W)) \xrightarrow{\simeq} \mathrm{Hom}_H(V, W)$$

   as "Frobenius reciprocity."

We will prove Theorem 9.5 in Section 9.10.

9.8. To put the proof of Frobenius reciprocity on better conceptual foundations, it is useful to introduce the notion of "coinvariants."

Definition 9.7. For a G-representation V, the coinvariant space V_G is the maximal quotient $V \twoheadrightarrow V_G$ of V for which the quotient map is G-equivariant for the trivial action of G on V_G.

Remarks 9.8.
1. It's easy to construct the coinvariants more explicitly. Namely, it is the quotient $V/\operatorname{Span}(\{g \cdot v - v\}_{g \in G, v \in V})$. Equivalently, it is the tensor product:

$$V_G = V \underset{\mathbb{C}[G]}{\otimes} \mathbb{C}.$$

2. The coinvariants satisfy the universal property that for a vector space W considered as a G-module via the trivial action, we have:

$$\mathrm{Hom}(V_G, W) \xrightarrow{\simeq} \mathrm{Hom}_G(V, W).$$

   This is dual to the universal property for the invariants V^G, which is that for such W we have:

$$\mathrm{Hom}(W, V^G) \xrightarrow{\simeq} \mathrm{Hom}_G(W, V).$$

Lemma 9.9. *For G finite, the composition:*

$$V^G \longrightarrow V \longrightarrow V_G$$

is an isomorphism $V^G \xrightarrow{\simeq} V_G$.

Indeed, this follows immediately from Maschke's theorem.

Exercise 9.10. Using Av_G, construct an explicit inverse to the map $V^G \longrightarrow V_G$. Deduce Maschke's theorem (say, in the form of Theorem 2.1) from Lemma 9.9.

9.9. The reason for introducing coinvariants is the following interpretation of ind_H^G.

Let W be an H-representation and consider $\mathbb{C}[G]\otimes W$. This is a $G\times G\times H$-module, corresponding to the left and right G-module structures of $\mathbb{C}[G]$ and the H-module structure on W. We will prefer to consider it as a $G\times H$-module, where the G-module structure comes from the left G-module structure, and the H-module structure comes from the right H-module structure of $\mathbb{C}[G]$ and the H-module structure of W. (Note the similarity to the construction from Section 9.4.

Then the tensor product:

$$\mathbb{C}[G] \underset{\mathbb{C}[H]}{\otimes} W$$

coincides as a G-module with the H-coinvariants of $\mathbb{C}[G]\otimes W$ (under the structures constructed above).

9.10. Now let us prove the Frobenius reciprocity theorem.

The (tautological) isomorphism $\mathbb{C}[G]\longrightarrow \mathrm{Fun}(G)$ induces a map $\mathbb{C}[G]\otimes W\longrightarrow \mathrm{Fun}(G)\otimes W$. It's easy to see that this map is $G\times G\times H$-equivariant, and therefore $G\times H$-equivariant (for structures as above).

Therefore, we have the following diagram:

$$\begin{tikzcd}
 & (\mathbb{C}[G]\otimes W)^H \arrow[r] \arrow[d] & (\mathrm{Fun}(G)\otimes W)^H \arrow[r, equal] \arrow[d] & \mathrm{Ind}_H^G(W) \\
 & \mathbb{C}[G]\otimes W \arrow[r] \arrow[d] & \mathrm{Fun}(G)\otimes W \arrow[d] & \\
\mathrm{ind}_H^G(W) \arrow[r, equal] & (\mathbb{C}[G]\otimes W)_H \arrow[r] & (\mathrm{Fun}(G)\otimes W)_H &
\end{tikzcd}$$

Clearly each of the horizontal arrows is an isomorphism. Moreover, both of the compositions of vertical arrows are isomorphisms by Lemma 9.9. Tracing the "outer rectangle" in this diagram gives the desired isomorphism.

9.11. Suppose $H'\subset G$ is a second subgroup of G. Our next goal is to "compute" $\mathrm{Ind}_H^G(W)$ as an H'-representation.

Examples 9.11.
1. When $H'=G$, this computation will tell us nothing new.
2. When $H'=\{1\}$, the computation essentially amounts to giving the dimension of $\mathrm{Ind}_H^G(W)$. By construction of $\mathrm{Ind}_H^G(W)$, it's clear that a function $f:G\longrightarrow W$ in $\mathrm{Ind}_H^G(W)$ is determined by its values at H-coset representatives and without other constraints, so this dimension is $|G/H|\cdot\dim(W)$.
3. The most interesting case is when $H'=H$.

The computation will be given in Sections 9.12-9.15 and will be stated as Proposition 9.13.

9.12. We will need the following construction.

For $g\in G$ and W an H-representation, define ${}^gW$ to be the representation of the subgroup $g\cdot H\cdot g^{-1}$ which is "W with action twisted by the adjoint action of g on G," i.e., the underlying vector space is W and for $x\in g\cdot H\cdot g^{-1}$ the operator $\rho_{{}^gW}(x)$ is defined as:

$$\rho_{{}^gW}(x)=\rho_W(g^{-1}xg).$$

Exercise 9.12. Let $H=G$. Show that ${}^gV$ is isomorphic to V as G-representations (note that the "identity" map between V and ${}^gV$ is not usually G-equivariant!).

9.13. Let W be an H-representation.

For $g \in G$, we will define a canonical G-equivariant isomorphism:

$$T_g : \mathrm{Ind}_H^G(W) \longrightarrow \mathrm{Ind}_{g\cdot H\cdot g^{-1}}^G({}^gW).$$

This map T_g sends a function $f : G \longrightarrow W$ (satisfying the appropriate equivariance property) the corresponding function translated $G \longrightarrow W$ translated by g^{-1}, i.e.:

$$T_g(f) : G \longrightarrow W \qquad T_g(f) : x \mapsto f(g^{-1}\cdot x).$$

Let us check that $T_g(f)$ satisfies the appropriate equivariance property to lie in $\mathrm{Ind}_{g\cdot H\cdot g^{-1}}^G({}^gW)$.

Suppose $h \in g\cdot H\cdot g^{-1}$. Then we want to show that for every $x \in G$ we have an equality:

$$f(g^{-1}\cdot h\cdot x) = T_g(f)(h\cdot x) = \rho_{{}^gW}(h)(T_g(f)(x)) = g^{-1}\cdot h\cdot g\cdot (f(g^{-1}x)).$$

(For a vector $w \in W$ and $h \in H$, we will use $h\cdot w$ to denote the initial action of H on W and not the one twisted by the adjoint action of g). By assumption on h, $g^{-1}hg \in H$. Therefore, since $f \in \mathrm{Ind}_H^G(W)$, we have:

$$g^{-1}\cdot h\cdot g\cdot f(g^{-1}x) = f((g^{-1}\cdot h\cdot g)\cdot(g^{-1}x)) = f(g^{-1}\cdot h\cdot x)$$

as desired.

9.14. We have tautological maps:

$$\mathrm{Ind}_{g\cdot H\cdot g^{-1}}^G({}^gW) \hookrightarrow \mathrm{Ind}_{H'\cap g\cdot H\cdot g^{-1}}^G({}^gW) \twoheadrightarrow \mathrm{Ind}_{H'\cap g\cdot H\cdot g^{-1}}^H({}^gW).$$

Composing this with T_g from above, we obtain a map we will also denote by $T_g(f)$ which is:

$$T_g(f) : \mathrm{Ind}_H^G(W) \longrightarrow \mathrm{Ind}_{H'\cap g\cdot H\cdot g^{-1}}^{H'}({}^gW).$$

Explicitly, this again sends a function $f : G \longrightarrow W$ to the function $H' \longrightarrow W$ given by translating by g^{-1}. This map $T_g(f) : \mathrm{Ind}_H^G(W) \longrightarrow \mathrm{Ind}_{H'\cap g\cdot H\cdot g^{-1}}^{H'}({}^gW)$ is by construction H'-equivariant.

9.15. To formulate Proposition 9.13, we will need a choice of representatives of double cosets, i.e., a splitting

$$\sigma : H'\backslash G/H \longrightarrow G$$

of the surjection $G \longrightarrow H'\backslash G/H$ sending an element of the group to its corresponding double coset.

Proposition 9.13. *The H'-equivariant map:*

$$\mathrm{Ind}_H^G(W) \longrightarrow \bigoplus_{x\in H'\backslash G/H} \mathrm{Ind}_{H'\cap\sigma(x)\cdot H\cdot\sigma(x)^{-1}}^{H'}({}^{\sigma(x)}W)$$

given as:

$$\oplus_{x\in H'\backslash G/H} T_{\sigma(x)}$$

is an isomorphism.

Proof. First, let us show that the map $\oplus_{x\in H'\backslash G/H} T_{\sigma(x)}$ is injective.

Indeed, suppose $f : G \longrightarrow W$ is an element of $\mathrm{Ind}_H^G(W)$ which lies in the kernel of this map. Let $g^{-1} \in G$ have image $x \in H'\backslash G/H$, so that there exists $h' \in H'$ and $h \in H$ such that $g^{-1} = h'\cdot\sigma(x)\cdot h$. Since $T_{\sigma(x)}(f) : H' \longrightarrow W$ is 0, we have:

$$0 = T_{\sigma(x)}(f)(h'^{-1}) = f(\sigma(x)\cdot h'^{-1}).$$

Since f is in $\mathrm{Ind}_H^G(W)$, we have:

$$0 = h^{-1}\cdot 0 = h^{-1}\cdot f(\sigma(x)\cdot h'^{-1}) = f(h^{-1}\cdot\sigma(x)\cdot h'^{-1}) = f(g).$$

As this holds for all $g \in G$, this implies that $f = 0$.

Therefore, to see that $\oplus_{x\in H'\backslash G/H} T_{\sigma(x)}$ is an isomorphism, it suffices to show that both the domain and the target have the same dimension. By Example 9.11 (2), we have:

$$\dim(\mathrm{Ind}_H^G(W)) = |G/H| \cdot \dim(W)$$

and:

$$\dim\Big(\underset{x\in H'\backslash G/H}{\oplus} \mathrm{Ind}_{H'\cap\sigma(x)\cdot H\cdot\sigma(x)^{-1}}^{H'}({}^{\sigma(x)}W)\Big) = \sum_{x\in H'\backslash G/H} \dim(\mathrm{Ind}_{H'\cap\sigma(x)\cdot H\cdot\sigma(x)^{-1}}^{H'}({}^{\sigma(x)}W)) =$$

$$= \sum_{x\in H'\backslash G/H} |H'/(H'\cap\sigma(x)\cdot H\cdot\sigma(x)^{-1})| \cdot \dim(W)$$

and we have:

$$\sum_{x\in H'\backslash G/H} |H'/(H'\cap\sigma(x)\cdot H\cdot\sigma(x)^{-1})| = |G/H|$$

since the stabilizer of $\overline{\sigma(x)} \in G/H$ (the image of $\sigma(x)$) for the action of H' on G/H is the subgroup:

$$H'/(H'\cap\sigma(x)\cdot H\cdot\sigma(x)^{-1}).$$

□

9.16. Next, let us compute the character of an induced representation.

Proposition 9.14. *Let W be a finite-dimensional representation of $H \subset G$. For $x \in G$, let $\overline{x}$ denote the image of x in G/H. Then we have:*

$$\chi_{\mathrm{Ind}_H^G(W)}(g) = \frac{1}{|H|} \sum_{\substack{x\in G \\ g\in \mathrm{Stab}_G(\overline{x})}} \chi_{{}^xW}(g).$$

Remark 9.15. More concretely, $g \in \mathrm{Stab}_G(\overline{x})$ if and only if $g \in x\cdot H\cdot x^{-1}$.

Remark 9.16. For $g \in G$, let $(G/H)^{(g)}$ denote the fixed point set:

$$\{y \in G/H \mid g\cdot y = y\}.$$

Let us choose H-coset representatives, i.e., a splitting $\sigma : G/H \longrightarrow G$ of $G \longrightarrow G/H$. Then by Exercise 9.12, Proposition 9.14 can be reformulated as saying:

$$\chi_{\mathrm{Ind}_H^G(W)}(g) = \sum_{y\in(G/H)^{(g)}} \chi_{{}^{\sigma(y)}W)}(g).$$

Proof of Proposition 9.14. Let $H' = (g)$ be the cyclic subgroup of G generated by g. We choose a splitting

$$\sigma : (g)\backslash G/H \longrightarrow G.$$

By Proposition 9.13, we have an isomorphism:

$$\mathrm{Ind}_H^G(W) \xrightarrow{\simeq} \underset{y\in(g)\backslash G/H}{\oplus} \mathrm{Ind}_{(g)\cap\sigma(y)\cdot H\cdot\sigma(y)^{-1}}^{(g)}({}^{\sigma(y)}W)$$

which is compatible with the obvious operators induced by g on both sides.

As in Remark 9.4, for $y \in (g)\backslash G/H$ such that $(g)\cap\sigma(y)\cdot H\cdot\sigma(y)^{-1} \neq (g)$, the trace of g on the corresponding summand is zero, i.e.:

$$\chi_{\mathrm{Ind}_{(g)\cap\sigma(y)\cdot H\cdot\sigma(y)^{-1}}^{(g)}({}^{\sigma(y)}W)}(g) = 0.$$

Therefore, $\chi_{\mathrm{Ind}_H^G(W)}(g)$ is the trace of g acting on the space:

$$\bigoplus_{\substack{y\in(g)\backslash G/H\\ g\in\sigma(y)\cdot H\cdot\sigma(y)^{-1}}} {}^{\sigma(y)}W.$$

Note that the map:

$$\{y\in G/H \mid g\cdot y=y\}\longrightarrow\{y\in(g)\backslash G/H \mid g\in\sigma(y)\cdot H\cdot\sigma(y)^{-1}\}$$

is a bijection since the corresponding orbits of (g) in G/H have size one (the (g)-stabilizer of some $y\in G/H$ being $(g)\cap\mathrm{Stab}_G(y)$). Therefore, $\chi_{\mathrm{Ind}_H^G(W)}(g)$ is the trace of g acting on the space:

$$\bigoplus_{\substack{y\in G/H\\ g\in\mathrm{Stab}_G(y)}} {}^{\sigma(y)}W$$

giving the desired result in the form stated in Remark 9.16.

□

Exercise 9.17. Give a more direct computation proving Proposition 9.14, i.e., one which does not rely on the special case of cyclic groups.

The formula from Proposition 9.14 takes the following simpler form when H is normal in G.

Corollary 9.18. *Let W be a finite-dimensional representation of H a normal subgroup of G. Then if $g\notin H$ we have:*

$$\chi_{\mathrm{Ind}_H^G(W)}(g)=0.$$

For $g\in H$, we have:

$$\chi_{\mathrm{Ind}_H^G(W)}(g)=\frac{1}{|H|}\sum_{x\in G}\chi_{{}^xW}(g)=\frac{1}{|H|}\sum_{x\in G}\chi_W(x^{-1}\cdot g\cdot x).$$

Remark 9.19. We already observed the phenomenon from Corollary 9.18 in a special case. Indeed, in Remark 9.4, we saw that for cyclic groups, characters induced from proper (necessarily normal) subgroups vanish on the generator of the group.

9.17. Next, let us give Mackey's criterion describing when $\mathrm{Ind}_H^G(W)$ is irreducible.

Theorem 9.20 (Mackey's irreducibility criterion)**.** *Let W be an irreducible representation of $H\subset G$. Then $\mathrm{Ind}_H^G(W)$ is irreducible if and only if for every $g\in G\setminus H$ (i.e., $g\notin H$) the representations W and ${}^gW$ of $H\cap g\cdot H\cdot g^{-1}$ have no isomorphic irreducible summands.*

Proof. By Corollary 3.10, it suffices to show that $\dim(\mathrm{End}_G(\mathrm{Ind}_H^G(W)))=1$. Applying Frobenius reciprocity, we have:

$$\mathrm{End}_G(\mathrm{Ind}_H^G(W))=\mathrm{Hom}_G(\mathrm{Ind}_H^G(W),\mathrm{Ind}_H^G(W))=\mathrm{Hom}_G(\mathrm{ind}_H^G(W),\mathrm{Ind}_H^G(W))=\mathrm{Hom}_H(W,\mathrm{Ind}_H^G(W)).$$

By Proposition 9.13, we have:

$$\mathrm{Ind}_H^G(W)\xrightarrow{\simeq}\bigoplus_{x\in H\backslash G/H}\mathrm{Ind}^H_{H\cap\sigma(x)\cdot H\cdot\sigma(x)^{-1}}({}^{\sigma(x)}W)$$

as an H-representation (with σ as in *loc. cit.*). For the identity coset $1\in H\backslash G/H$ the identity coset, the corresponding summand is merely W. Therefore, the failure of $\mathrm{End}_G(\mathrm{Ind}_H^G(W))$ to be one-dimensional occurs only in the presence of $x\in H\backslash G/H$ a non-identity coset and a non-zero H-equivariant map:

$$W\longrightarrow\mathrm{Ind}^H_{H\cap\sigma(x)\cdot H\cdot\sigma(x)^{-1}}({}^{\sigma(x)}W)$$

or what is the same, a non-zero $H \cap \sigma(x) \cdot H \cdot \sigma(x)^{-1}$-equivariant map:

$$W \longrightarrow^{\sigma(x)} W.$$

But this can only occure if W and ${}^{\sigma(X)}W$ share an irreducible summand as $H \cap \sigma(x) \cdot H \cdot \sigma(x)^{-1}$-representations. It's immediate to see that this condition is independent of the choice of σ, and therefore it is equivalent that it holds for all $g \in G$.

□

9.18. Mackey's criterion takes a simpler form when $\dim(W) = 1$:

Corollary 9.21. *Let $\chi : H \longrightarrow \mathbb{C}^\times$ be a 1-dimensional character of H a subgroup of G. Then $\mathrm{Ind}_H^G(W)$ is irreducible if and only if for every $g \in G \setminus H$ we have $\chi|_{H \cap g \cdot H \cdot g^{-1}} \neq^g \chi|_{H \cap g \cdot H \cdot g^{-1}}$ (where ${}^g\chi$ is χ composed with the map $G \longrightarrow G$ given by conjugation by g).*

Similarly, we have the following simpler form when H is normal:

Corollary 9.22. *Let W be an irreducible representation of H a* normal *subgroup of G. Then $\mathrm{Ind}_H^G(W)$ is irreducible if and only if for every $g \in G \setminus H$ (i.e., $g \notin H$) the representations W and ${}^gW$ of H are not isomorphic.*

9.19. Let us apply the techniques developed above to compute the character table of the dihedral group D_n of order $2n$. This computation will occupy the remainder of the section.

9.20. Recall that the dihedral group has generators and relations:

$$< \sigma, \tau \mid \sigma^2 = \tau^n = 1, \quad \sigma \cdot \tau \cdot \sigma^{-1} = \tau^{-1} > .$$

The dihedral group acts by linear symmetries on $\mathbb{R}^2$ preserving a regular n-gon with center at the origin, where σ is a reflection across a line through some fixed vertex and τ is a rotation by $\frac{2\pi}{n}$.

9.21. Let us compute the conjugacy classes of D_n.

We have the relations:

$$\sigma \cdot \tau^r \cdot \sigma^{-1} = \tau^{-r} \qquad \tau \cdot (\sigma \cdot \tau^r) \cdot \tau^{-1} = \sigma \cdot \tau^{r-2} \qquad \sigma \cdot (\sigma \cdot \tau^r) \cdot \sigma^{-1} = \sigma \cdot \tau^{-r}$$

Therefore, if n is odd we have the conjugacy classes:

$$\{1\}, \{\tau, \tau^{-1}\}, \ldots, \{\tau^{\frac{n-1}{2}}, \tau^{\frac{n+1}{2}}\}, \{\sigma, \sigma \cdot \tau, \ldots \sigma \cdot \tau^{n-1}\}.$$

Similarly, if n is even we have the conjugacy classes:

$$\{1\}, \{\tau, \tau^{-1}\}, \ldots, \{\tau^{\frac{n}{2}-1}, \tau^{\frac{n}{2}+1}\}, \{\tau^{\frac{n}{2}}\}, \{\sigma, \sigma \cdot \tau^2, \ldots \sigma \cdot \tau^{n-2}\}, \{\sigma \cdot \tau, \sigma \cdot \tau^3, \ldots \sigma \cdot \tau^{n-1}\}.$$

In particular, we see that if n is odd then there are $1 + \frac{n-1}{2} + 1 = \frac{n+3}{2}$ conjugacy classes and if n is even then there are $1 + \frac{n-2}{2} + 1 + 2 = \frac{n+6}{2}$ conjugacy classes.

9.22. The subgroup generated by τ is a cyclic group of order n in D_n. For each nth root of unity ζ, let $\chi_\zeta : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^\times$ be the character sending the generator to ζ. Then for each such ζ, we have the representation $\mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{D_n}(\chi_\zeta)$.

Proposition 9.23. *The representation $\mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{D_n}(\chi_\zeta)$ is irreducible if and only if $\zeta \neq \pm 1$.*

Proof. Note that $\mathbb{Z}/n\mathbb{Z} = \{\tau^r\}_{r=0}^{n-1}$ is normal is D_n. Therefore, we will apply Mackey's criterion in the form of Corollary 9.22.

Every $g \in G \setminus H$ has the form $\sigma \cdot \tau^r$ for some r. Then we have:

$$(\sigma \cdot \tau^r) \cdot \tau \cdot (\sigma \cdot \tau^r)^{-1} = \sigma \cdot \tau \cdot \sigma^{-1} = \tau^{-1}.$$

Therefore, Mackey's criterion says that the representation is irreducible if and only if:

$$\zeta = \chi_\zeta(\tau) \neq \chi_\zeta(\tau^{-1}) = \zeta^{-1}$$

which amounts to the condition in the proposition.

□

9.23. Next, let us compute the character of $\mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{D_n}(\chi_\zeta)$.

Proposition 9.24. *We have:*

$$\chi_{\mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{D_n}(\chi_\zeta)}(\tau^r) = \zeta^r + \zeta^{-r}$$
$$\chi_{\mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{D_n}(\chi_\zeta)}(\sigma \cdot \tau^r) = 0.$$

Proof. We compute the character using Corollary 9.18. By *loc. cit.*, the character of $\mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{D_n}(\chi_\zeta)$ is zero off of $\mathbb{Z}/n\mathbb{Z} = \{\tau^r\}_{r=0}^{n-1}$ and we have:

$$\chi_{\mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{D_n}(\chi_\zeta)}(\tau^r) = \frac{1}{n}\Big(\sum_{i=1}^{n} \chi_\zeta(\tau^r) + \sum_{i=1}^{n} \chi_\zeta(\sigma \cdot \tau^r \cdot \sigma^{-1})\Big) = \chi_\zeta(\tau^r) + \chi_\zeta(\tau^{-r}) = \zeta^r + \zeta^{-r}.$$

□

9.24. Now let ζ denote a fixed *primitive* nth root of unity.

By Proposition 9.24, we see that $\{\mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{D_n}(\chi_{\zeta^i})\}_{i=1}^{\lfloor \frac{n-1}{2} \rfloor}$ consists of pairwise non-isomorphic irreducible representations (of dimension 2). We also have two obvious 1-dimensional representations of D_n: the trivial representation and the "sign" character (i.e., the character obtained from the non-trivial character of $\mathbb{Z}/2\mathbb{Z} = D_n/(\mathbb{Z}/n\mathbb{Z})$).

When n is odd, this gives:

$$1 + 1 + \frac{n-1}{2} = \frac{n+3}{2}$$

representations, and by Section 9.21, this gives all of the irreducible representations of D_n.

Example 9.25. Recall that we have $D_3 \xrightarrow{\simeq} S_3$. The irreducible 2-dimensional representation of D_3 constructed above is therefore the same as the unique irreducible 2-dimensional representation of S_3. In particular, this representation of S_3 is induced from a non-trivial character of $\mathbb{Z}/3\mathbb{Z} \subset S_3$.

9.25. When n is even, we have found:

$$1 + 1 + \frac{n-2}{2} = \frac{n+2}{2}$$

representations, so by Section 9.21 we are still 2 short.

Note that (for n even) D_n has the normal subgroup $\{1, \tau^2, \ldots, \tau^{n-2}\}$, and the quotient by this subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This quotient gives rise to three non-trivial 1-dimensional characters of D_n, one which we have already found (the sign character) and two more. Thus, we have computed all of the irreducible representations of D_n in this case as well.