Representation Theory

This is a course in representation theory, which essentially is the study of abstract algebra through (the language of) linear algebra. The ideas and methods from representation theory permeate many disparate areas of mathematics. For example, it is one of the (many) key components in the proof of Wiles Theorem[1].

No prior knowledge of group theory is needed for this course, though it will certainly be useful. However, a good basis in linear algebra and (abstract) vector spaces will be essential.

Material for these notes is derived from these primary sources: (1) *Representation Theory of Finite Groups* by Martin Barrow, (2) *Algebra* by Michael Artin, (3) *The Symmetric Group* by Bruce Sagan, and (4) lecture notes on algebra by Allen Bell[2]. I should also throw in a shoutout to the Unapologetic Mathematician[3].

1. A short (re)introduction to group theory

Definition. A group is a pair $(G, \cdot)$ with G a set and $\cdot$ a binary operation[4] on G satisfying

(1) Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$.
(2) Identity: there exists $e \in G$ such that $a \cdot e = e \cdot a$ for all $a \in G$.
(3) Inverses: for all $a \in G$ there exists an element $a' \in G$ such that $a \cdot a' = a' \cdot a = e$.

If in addition, $a \cdot b = b \cdot a$ for all $a, b \in G$ (commutativity) the group is said to be abelian. The number $|G|$ is called order of the group G (this may be infinite).

There are two "generic" group operations: addition and multiplication. Almost universally, the addition operation is reserved for abelian groups. Thus, multiplication is a more generic operation because it can be used for both abelian and nonabelian groups.

Example 1.1. The following are examples of groups.

- $(\mathbb{Z}, +)$ is a group. One can also replace $\mathbb{Z}$ by $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ (but not $\mathbb{N}$).

---

[1] Also known to some as Fermat's Last Theorem.

[2] Allen Bell was my PhD advisor. The complete notes can be found at https://pantherfile.uwm.edu/adbell/www/Teaching/731/2008/book.pdf

[3] https://unapologetic.wordpress.com/

[4] A binary operation is just a function $f : G \times G \to G$.

- $(\mathbb{Q}^\times, \cdot)$ is a group where $\mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$. One can also replace $\mathbb{Q}^\times$ by $\mathbb{R}^\times$ or $\mathbb{C}^\times$ (but not $\mathbb{Z}^\times$).
- Let $M_n(\mathbb{C})$ denote the set of $n \times n$ matrices with entries in $\mathbb{C}$. Then $(M_n(\mathbb{C}), +)$ is a group, where $+$ is the operation of matrix addition.
- Let $\mathrm{GL}_n(\mathbb{C}) \subset M_n(\mathbb{C})$ denote the set of $n \times n$ *invertible* matrices. Then $(\mathrm{GL}_n(\mathbb{C}), \cdot)$ is a group where $\cdot$ is the operation of matrix multiplication[5].

Exercise 1.2. Show that the set of even integers forms a group under addition but that the set of odd integers does not.

All of the examples presented above are abelian groups, except for $\mathrm{GL}_n(\mathbb{C})$. As we learn in linear algebra, matrix multiplication is not commutative.

In addition to the groups above, with which you are most certainly already familiar, we will be concerned primarily with two groups: the cyclic groups and the symmetric groups. The rest of this lecture is dedicated to defining and exploring these groups.

Proposition 1.3. Let G be a group.

(1) The identity element of G is unique.
(2) For all $g \in G$, the inverse element $g^{-1} \in G$ is unique.
(3) For $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

Proof. (1) Let $e, e' \in G$ be identity elements. Because e is an identity element, then $e = ee'$. Because e' is an identity element, $ee' = e$. Thus, $e = ee' = e'$.

(2) Fix $g \in G$ and let $g', g'' \in G$ be inverses of G. Then

$$e = gg' \Rightarrow g''e = g''gg' \Rightarrow g'' = eg' \Rightarrow g'' = g'.$$

(3) By (2), it suffices to show that $h^{-1}g^{-1}$ is *an* inverse of gh. We verify this below,

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e.$$

One verifies similarly that $(h^{-1}g^{-1})(gh) = e$. □

Exercise 1.4. Let G be a group and $g \in G$. If $g' \in G$ satisfies $gg' = e$ or $g'g = e$, then $g' = g^{-1}$. (A left/right inverse element in a group is a two-sided inverse).

Exercise 1.5. Show that left and right cancellation hold in any group. That is, if $a, b, c \in G$ satisfy $ab = ac$ or $ba = ca$, then $b = c$.

[5]This follows from the fact that $\det(A)\det(B) = \det(AB)$ for all $n \times n$ matrices A, B

Definition. A subgroup H of a group G is a subset such that H is a group with respect to the operation associated to G.

Example 1.6. (1) Let G be a group. Then G is a subgroup of itself. If $e \in G$ is the identity element, then $\{e\}$ is a subgroup called the trivial subgroup. A subgroup of G that is not G and not the trivial subgroup is called proper.

(2) $2\mathbb{Z}$, the set of even numbers, is a subgroup of $\mathbb{Z}$ (under addition). The set of odd numbers is not a subgroup.

(3) $\mathbb{R}^\times$ is a group under multiplication and $\mathbb{Q}^\times$ is a subgroup.

(4) $\mathrm{SL}_n(\mathbb{C})$ is a subgroup of $\mathrm{GL}_n(\mathbb{C})$ under matrix multiplication.

(5) $\mathrm{GL}_n(\mathbb{C})$ is a subset of $M_n(\mathbb{C})$ but not a subgroup because $M_n(\mathbb{C})$ is a group under matrix addition and $\mathrm{GL}_n(\mathbb{C})$ a group under matrix multiplication.

Definition. Let G be a group (not necessarily cyclic) and let $a \in G$. Then the set

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is a subgroup of G called the cyclic subgroup of G generated by a. The order of the element a, denoted $|a|$, is the order of the group $|\langle a \rangle|$.

It is implied by the definition that if $|a| = n$, then $a^n = e$ and that n is the least positive integer such that this is true.

Exercise 1.7. Verify that for an element a in a group G, the set $\langle a \rangle$ is indeed a subgroup of G.

Next we move on to defining cyclic groups.

Definition. A group G is cyclic if there exists $a \in G$ such that $\langle a \rangle = G$. In this case, the element a is called a generator.

Example 1.8. The group $\mathbb{Z}_3 = \{e, a, a^2\}$ is a cyclic group of order 3. Both a and a^2 are generators. We can make a *Cayley table* to work out all multiplications in the group.

	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a^2	e	a

In fact, it turns out that $\mathbb{Z}_3$ is *the* cyclic group of order 3. To make this precise, one needs to develop the concept of group isomorphisms and we do not do that here. However, we will frequently refer to $\mathbb{Z}_n$ as the cyclic group of order n.

Exercise 1.9. Construct the Cayley Table for $\mathbb{Z}_5$.

Exercise 1.10. The Klein-4 group K is an abelian group with four element $\{e, a, b, c\}$ with the properties that $a^2 = b^2 = c^2 = e$ and the product of any two of a, b, or c is the other (e.g., $ab = c$). Construct the Cayley table for K.

Theorem 1.11. Every cyclic group is abelian.

Proof. Let $G = \langle a \rangle$ be a cyclic group and let $g, h \in G$. Then $g = a^k$ and $h = a^\ell$ for some $k, \ell \in \mathbb{Z}$. By properties of exponents, $gh = a^k a^\ell = a^{k+\ell} = a^{\ell+k} = a^\ell a^k = hg$. Thus, G is abelian. □

The converse of Theorem 1.11 is not true. There are lots of abelian groups that are not cyclic (see, e.g. Example 1.10), but in some sense cyclic groups form the building blocks for all *finite* abelian groups. Also, cyclic groups need not be finite, the group of integers is an infinite cyclic group. We now turn our attention to the symmetric group.

Definition. A permutation is a bijective function on the set X (from X to itself). The set of permutations on X is denoted $\mathcal{S}_X$. If X is finite we write $X = \{1, \ldots, n\}$ and denote $\mathcal{S}_X$ by $\mathcal{S}_n$ and call it the symmetric group on n letters.

Theorem 1.12. S_n is a group of order $n!$ under composition.

Proof. The composition of two bijective functions is again a bijective function. Moreover, the operation of composition is associative (check!). The identity function is given by $\mathrm{id}(x) = x$ for all $x \in X$ and this is clearly bijective. Finally, every bijective function has an inverse that is again a bijective function.

The last part of the theorem is left as an exercise. □

There are two standard types of notation to represent elements of $\mathcal{S}_n$: two-line and cycle. Two-line is in some ways easier to use at first but much clumsier. We will learn both but as we go on we will use cycle notation exclusively.

In two-line notation we write the elements of $\mathcal{S}_n$ as $2 \times n$ matrices. For a given element $\sigma \in \mathcal{S}_n$ we write in the first row $1, \ldots, n$ and in the second the image of each value under σ:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Note that the elements of S_n are functions and therefore we compose right-to-left.

Example 1.13. Consider the following elements of $\mathcal{S}_4$:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

These elements form a subgroup of $\mathcal{S}_4$ with Cayley table:

	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	τ	μ	id
τ	τ	μ	id	σ
μ	μ	id	σ	τ

Is this group cyclic? Why or why not?

In general, the elements of $\mathcal{S}_n$ do not commute. Consider the following elements of S_3:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{and} \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

A more compact way of representing elements of $\mathcal{S}_n$ is with *cycles*.

Definition. A permutation $\sigma \in \mathcal{S}_n$ is a cycle of length k if there exists $a_1, \ldots, a_k \in \{1, \ldots, n\}$ such that

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \quad \ldots \quad \sigma(a_k) = a_1$$

and $\sigma(i) = i$ for $i \notin \{a_1, \ldots, a_k\}$. We denote the cycle by $(a_1 \ a_2 \ \cdots \ a_k)$.

To compose cycles, one *could* translate back to two-line notation but I strongly advise against that. Instead, we compose (from right-to-left) by tracking the image of each element through successive cycles, remembering to close cycles when we get back to where we started.

Example 1.14. In the previous example, the elements would be written in cycle notation by

$$\mathrm{id} = (1), \quad \sigma = (1\ 4\ 3\ 2), \quad \tau = (1\ 3)(2\ 4), \quad \mu = (1\ 2\ 3\ 4).$$

Then

$$\sigma\tau = (1\ 4\ 3\ 2)(1\ 3)(2\ 4) = (2\ 3\ 4\ 1) = (1\ 2\ 3\ 4) = \mu.$$

Definition. Two cycles $\sigma = (a_1 \ a_2 \ \cdots \ a_k)$ and $\tau = (b_1 \ b_2 \ \cdots \ b_\ell)$ are said to be disjoint if $a_i \neq b_j$ for all i, j.

Example 1.15. $(1\ 3\ 5)(2\ 7)$ are disjoint but $(1\ 3\ 5)(3\ 4\ 7)$ are not. Note that $(1\ 3\ 5)(3\ 4\ 7) = (3\ 4\ 7\ 5\ 1)$.

Exercise 1.16. Prove that disjoint cycles in $\mathcal{S}_n$ commute and that every element in $\mathcal{S}_n$ can be written as the product of disjoint cycles.

Example 1.17. As an additional example, we will compute the Cayley table for $\mathcal{S}_3$ using cycle notation. As a set (in cycle notation), $\mathcal{S}_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. The Cayley Table is

	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	(1)	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	(1)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	(1)	(1 2 3)

One helpful observation to make regarding the previous example is that any two of the *transpositions* $(1\ 2)$, $(1\ 3)$, and $(2\ 3)$ generate the group. That is, we can get any element in $\mathcal{S}_3$ by taking (possibly repeated) products of any two of these elements.

2. Group representations

Here is an example that will motivate much of what we try to do today. Consider the vector space $V = \mathbb{C}^3$ with standard basis $\{e_1, e_2, e_3\}$. Let T be the linear transformation defined by

$$T(e_1) = e_2, \quad T(e_2) = e_1, \quad T(e_3) = e_3.$$

Recall that, to define a linear transformation, it is sufficient to denote its action on basis elements. Similarly, let S be the linear transformation defined by

$$S(e_1) = e_3, \quad S(e_2) = e_e, \quad S(e_3) = e_1.$$

Recall that by elementary linear algebra, a linear transformation on a finite-dimensional vector space can be *represented* by a matrix. That is, there are matrices M_T and M_S such that $T(\mathbf{v}) = M_T\mathbf{v}$ and $S(\mathbf{v}) = M_S\mathbf{v}$ for all $\mathbf{v} \in V$.

We observe that T acts on the basis elements of V in the same way that the permutation $(1\ 2)$ acts on the set $\{1, 2, 3\}$. Similarly, S corresponds to the permutation $(1\ 3)$. In fact, we could bypass T and S completely and write down a map $\mathcal{S}_3 \to \mathrm{GL}_3(\mathbb{C})$.

Notice that, for example, $(1\ 2)(1\ 3) = (1\ 3\ 2)$. In the matrix representation,

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

A naive, but correct, way of viewing the correspondence is that a nonzero element in $M_{i,j}$ indicates that the corresponding bijection sends $j \mapsto i$.

Here's another way that is more aligned with what we will do. Consider the set of standard basis vectors (of $\mathbb{C}^3$). If $\sigma \in \mathcal{S}_3$, then the corresponding matrix M_σ maps (by left multiplication) e_i to $e_{\sigma(i)}$.

What we have found is formally called a (matrix) representation of the group $\mathcal{S}_3$. This lecture will be devoted to defining representations and the concept of irreducibility. First, we need some further background on group homomorphisms.

Definition. A (group) homomorphism is a function $\phi : G \to H$ between groups such that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. If ϕ is bijective, then it is said to be an isomorphism. The set $\operatorname{im}\phi = \{h \in H : \phi(g) = h \text{ for some } g \in G\}$ is called the image of ϕ.

Example 2.1. (1) $\phi : \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ given by $\phi(M) = \det(M)$ is a homomorphism. Note that in this case ϕ is surjective but not injective.

(2) $\phi : M_n(\mathbb{C}) \to \mathbb{C}$ given by $\phi(M) = \det(M)$ is *not* a homomorphism because, in general, $\det(M+N) \neq \det(M) + \det(N)$.
(3) Let $\mathbb{Z}_2 = \langle g \rangle$ (so $g^2 = e$) and $\mathbb{Z}_4 = \langle h \rangle$ (so $h^4 = e$). Define $\phi : \mathbb{Z}_2 \mapsto \mathbb{Z}_4$ by $\phi(e) = e$ and $\phi(g) = h^2$. Then ϕ is an injective homomorphism that is not surjective. On the other hand, the map $\psi : \mathbb{Z}_4 \to \mathbb{Z}_2$ given by $\psi(h) = \psi(h^2) = g$ and $\psi(e) = \psi(h^2) = e$ is a surjective homomorphism that is not injective.
(4) Choose $g \in G$, G a group, and define $\phi : \mathbb{Z} \to G$ by $\phi(n) = g^n$. Then ϕ is a homomorphism and $\operatorname{im}\phi = \langle g \rangle$.

Exercise 2.2. Let $\sigma \in \mathcal{S}_n$ be a permutation. Show that σ can be written as a product of transpositions (cycles of length 2). This decomposition is not unique, but if σ can be written as a product of an even number of transpositions, then it can only be written as a product of an even number of transpositions (this is difficult to prove, you may assume this part of the exercise). We say such a permutations is even. Otherwise we say it is odd

Now define $\phi : \mathcal{S}_n \to \mathbb{C}^\times$ by $\sigma(\sigma) = \operatorname{sgn}\sigma$ where $\operatorname{sgn}\sigma = 1$ if σ is even and -1 is σ is odd. (We say $\operatorname{sgn}\sigma$ is the sign of σ). Show that ϕ is a group homomorphism.

Proposition 2.3. Let $\phi : G \to H$ be a homomorphism of groups.

(1) $\phi(e_G) = e_H$.
(2) For any $g \in G$, $\phi(g^{-1}) = g^{-1}$.
(3) If K is a subgroup of G, then $\phi(K)$ is a subgroup of H.
(4) If L is a subgroup of H, then $\phi^{-1}(L) = \{g \in G : \phi(g) \in L\}$ is a subgroup of G.

Proof. Let $g \in G$, then $\phi(g)e_H = \phi(g) = \phi(ge_G) = \phi(g)\phi(e_G)$. By left cancellation, $e_H = \phi(e_G)$. This proves (1). Now $e_H = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$. By uniqueness of the inverse, $\phi(g^{-1}) = \phi(g)^{-1}$, proving (2).

Parts (3) and (4) are left as an exercise.

□

Definition. The kernel of a homomorphism $\phi : G \to H$ is the set

$$\ker\phi = \{g \in G : \phi(g) = e\}.$$

Theorem 2.4. Let $\phi : G \to H$ be a group homomorphism. Then $\ker\phi$ is a subgroup of G.

Proof. It is clear that $\ker\phi$ is a subset of G. Also, by the previous proposition, $e_G \in \ker\phi$. Let $g_1, g_2 \in \ker\phi$. Then $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = ee = e$, so $\ker\phi$ is closed under the operation.

Finally, since $g_1 \in \ker\phi$, then by the previous proposition, $\phi(g_1^{-1}) = \phi(g_1)^{-1} = e^{-1} = e$, so $\ker\phi$ is closed under inverses and is thus a subgroup. $\square$

Example 2.5. (1) $\phi : \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ given by $\phi(M) = \det(M)$. Then $\ker\phi = \mathrm{SL}_2(\mathbb{C})$.

(2) Let $\psi : \mathbb{Z}_4 \mapsto \mathbb{Z}_2$ be the homomorphism above given by $\phi(h) = g$. We can check directly that $\ker\psi = \{e, h^2\}$.

(3) Choose $g \in G$, G a group, and define $\phi : \mathbb{Z} \to G$ by $\phi(n) = g^n$. If $|g| = \infty$ then $\ker\phi = \{0\}$. If $|g| = k$, then $\ker\phi = k\mathbb{Z}$.

(4) Let $\phi : \mathcal{S}_n \to \mathbb{C}^\times$ by $\sigma(\sigma) = \operatorname{sgn}\sigma$. Thus, the kernel of ϕ is the subgroup consisting of all even permutations of $\mathcal{S}_n$. We call this subgroup the alternating group on n letters, denoted A_n.

Definition. Let G be a group and V a vector space over a field F. A representation of G on V is a homomorphism $\rho : G \to \mathrm{GL}(V)$. If V is of dimension $n < \infty$, then by fixing a basis we obtain a homomorphism $\rho' : G \to \mathrm{GL}_n(F)$.

We will only deal with finite-dimensional representations and so the vector space itself will be largely inconsequential. In addition, we will focus on *complex* representations over $\mathbb{C}$. We will see that this provides greater flexibility in finding representations. Finally, note that $\mathrm{GL}_1(\mathbb{C})$ is essentially just the complex numbers themselves (under multiplication), denoted $\mathbb{C}^\times$. We will frequently use this fact without comment.

We have already seen one example of a group representation at the beginning of this section. Here is another.

Example 2.6. Let ρ be a 1-dimensional representation of the group $\mathbb{Z}_2 = \langle g\rangle$. Thus, $\rho : \mathbb{Z}_2 \mapsto \mathbb{C}^\times$, so $\rho(g) = a$ for some nonzero complex number a. As ρ is a group homomorphism,

$$e = \rho(e) = \rho(g^2) = \rho(g)\rho(g) = a^2.$$

Thus, $a = \pm 1$. It follows that there are two 1-dimensional representation of $\mathbb{Z}_2$. The first, ρ_1, maps $g \mapsto 1$. We call this the trivial representation. The second, ρ_2, maps $g \mapsto -1$.

Exercise 2.7. Show that there are exactly n distinct 1-dimensional representations of $\mathbb{Z}_n$.

Example 2.8. For $\mathcal{S}_3$, there are two 1-dimensional representations. One is the trivial representations, ρ_1, that maps every element to 1. The second is the sign representation, ρ_2, defined by the sgn map.

There is a two-dimensional representation of $\mathcal{S}_3$, $\rho_3 : \mathcal{S}_3 \to \mathrm{GL}_2(\mathbb{C})$, defined by

$$\rho_3((1\ 2)) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho_3((1\ 3)) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

This last example may seem to have come out of thin air, and it is not clear presently how to construct representations beyond simple 1-dimensional examples. We will see that these examples are in fact quite natural.

There are lots of important and interesting questions in representation theory. Representations can give important information about a group itself. Or, given a group, one may want to know what all of the representations are (sometimes this is an intractable problem). In the case of finite abelian groups this is always possible.

Definition. Let G be a group. Let $\rho_1 : G \to \mathrm{GL}_n(\mathbb{C})$ and $\rho_2 : G \to \mathrm{GL}_m(\mathbb{C})$ be two representations of G. The direct sum of the representations ρ_1 and ρ_2 is the map $\rho_1 \oplus \rho_2 : G \to \mathrm{GL}_{n+m}(\mathbb{C})$ defined by,

$$(\rho_1 \oplus \rho_2)(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix},$$

for all $g \in G$.

If ρ is a representation of G, then ρ is decomposable if it can be written as the direct sum of two representations and indecomposable otherwise.

Example 2.9. There is a representation ρ of $\mathcal{S}_3$ given by

$$\rho((1\ 2)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \rho((1\ 3)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}.$$

But of course, $\rho = \rho_1 \oplus \rho_3$ from Example 2.8.

Definition. Two representations $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathbb{C})$ of a group G are said to be equivalent (or isomorphic) if there exists a matrix $T \in \mathrm{GL}_n(\mathbb{C})$ such that $\rho_2(g) = T\rho_1(g)T^{-1}$ for all $g \in G$.

Example 2.10. Let ρ be the representation of $\mathcal{S}_3$ given at the beginning of this section, so

$$\rho((1\ 2)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho((1\ 3)) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Let

$$T = \begin{pmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ 1 & 1 & -2 \end{pmatrix}.$$

Then

$$T\rho((1\ 2))T^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } T\rho((2\ 3))T^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Thus, ρ is equivalent to $\rho_1 \oplus \rho_3$.

Our goal, then, is to find all indecomposable representations of a given group. It will be useful to study a weaker notion, known as reducibility.

Definition. Let ρ be a representation of a group G. Suppose there exists representations ρ_1 and ρ_2 of G such that

$$\rho(g) = \begin{pmatrix} \rho_1(g) & 0 \\ M(g) & \rho_2(g) \end{pmatrix},$$

for every $g \in G$ (here $M(g)$ is some matrix depending on g). In this case, we say ρ, or any representation equivalent to it, is reducible. Otherwise, ρ is said to be irreducible.

Exercise 2.11. Show that the two-dimensional representation of $\mathcal{S}_3$ given in Example 2.8 is irreducible.

Theorem 2.12. Every irreducible representation of a finite abelian group is one-dimensional.

The proof of this theorem will follows once we have developed the theory of *characters*. Theorem 2.12 is *not* true for arbitrary groups.

Here is one more way to form new representations from old ones. Recall that the Kronecker product of two matrices $A = (a_{ij})$ and B is defined as the block matrix $(A \otimes B)_{ij} = a_{ij}B$.

Definition. Let $\rho_1 : G \to \mathrm{GL}_m(\mathbb{C})$ and $\rho_2 : G \to \mathrm{GL}_n(\mathbb{C})$ be two representations of a group G. The tensor product of the representations ρ_1 and ρ_2, denoted $\rho_1 \otimes \rho_2$, is defined by $(\rho_1 \otimes \rho_2)(g) = \rho_1(g) \otimes \rho_2(g)$ for all $g \in G$, where the symbol on the right denotes the Kronecker product of the matrices $\rho_1(g)$ and $\rho_2(g)$.

Observe that the tensor product of two representations is again a representation. In the notation of the definition, $\rho_1 \otimes \rho_2 : G \to \mathrm{GL}_{mn}(\mathbb{C})$. Thus, the tensor product of two one-dimensional representations is again a one-dimensional representation.

Exercise 2.13. Let G be a group and ρ_e its trivial representation. Show that if ρ is any representation, then $\rho_e \otimes \rho$ is equivalent to ρ.

Exercise 2.14. Let ρ_1, ρ_2, and ρ_3 be the irreducible representations of $\mathcal{S}_3$. Construct the matrices corresponding to $\rho_3 \otimes \rho_3$. Show that this representation is equivalent to $\rho_1 \oplus \rho_2 \oplus \rho_3$.

3. Characters

Our goal is to prove that finite-dimensional irreducible representations of abelian groups are 1-dimensional. To do this, we need to develop the theory of *characters*. A character is an invariant of the representation in that two representations (of the same group) with the same character are isomorphic.

Definition. Let G be a group and ρ a representation of G. The character χ of ρ is the map $\chi : G \to \mathbb{C}$ given by $\chi(g) = \text{trace}(\rho(g))$. The dimension of $\chi(g)$ is the dimension of the representation $\rho(g)$. A character is irreducible if ρ is irreducible.

As a consequence of the definition, $\chi(g)$ is invariant under conjugation (since $\text{trace}(AB) = \text{trace}(BA)$). Thus, if R_g is the matrix representation obtained by choosing a basis for V, then $\chi(g) = \text{trace}(R_g) =$ where the λ_i are the eigenvalues of $\rho(g)$.

Theorem 3.1. Let G be a group with representations ρ and ρ'. Let χ and χ' be the characters of ρ and ρ', respectively.

(1) $\chi(e)$ is the dimension of ρ.
(2) $\chi(g) = \chi(hgh^{-1})$ for all $g, h \in G$.
(3) $\chi(g^{-1}) = \overline{\chi(g)}$.
(4) The character of $\rho \oplus \rho'$ is $\chi + \chi'$.

Proof. (1) $\chi(e) = \text{trace}(I) = \dim V = \dim \chi$.

(2) Since the map ρ is a homomorphism, then

$$\begin{aligned}\chi(hgh^{-1}) &= \text{trace}(\rho(hgh^{-1})) = \text{trace}(\rho(h)\rho(g)\rho(h^{-1})) \\ &= \text{trace}(\rho(h)\rho(g)\rho(h)^{-1}) = \text{trace}(\rho(g)) = \chi(g).\end{aligned}$$

(3) This follows from linear algebra. If the eigenvalues of $\rho(g)$ are $\lambda_1, \ldots, \lambda_n$[6], then $\chi(g) = \text{trace}(\rho(g)) = \lambda_1 + \ldots + \lambda_n$. Moreover, the eigenvalues of $\rho(g^{-1}) = \rho(g)^{-1}$ are $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$. Since G is a finite group, then every element has finite order (by Lagrange's Theorem). If

[6]There are lots of proofs of this and some are simpler depending on your background. The simplest is to observe that by simple row reduction (adding a multiple of one row to another) you can put any matrix into upper (or lower) triangular form. Then the eigenvalues are just the diagonal entries. Alternatively, recall that the characteristic polynomial of $\rho(g)$ factors as $(t-\lambda_1)(t-\lambda_2)\cdots(t-\lambda_n)$. For any matrix A, the coefficient of t^{n-1} in the characteristic polynomial $|A - tI|$ is $-\text{trace}(A)$, then by expanding the characteristic polynomial of $\rho(g)$ we get that the coefficient of t^{n-1} is $-(\lambda_1 + \lambda_2 + \cdots + \lambda_n)$.

$g^r = 1$, then $\rho(g)$ is a matrix of order r and so its eigenvalues are roots of unity (exercise!). Hence, $|\lambda_i| = 1$ so $\lambda_i^{-1} = \overline{\lambda_i}$. It follows then that

$$\chi(g^{-1}) = \lambda_1^{-1} + \cdots + \lambda_n^{-1} = \overline{\lambda_1} + \cdots + \overline{\lambda_n}.$$

(4) Exercise. $\square$

Property (2) in the previous theorem says that characters are constant on each conjugacy class. Given an element x in a group G, the conjugacy class of x is the set

$$C(x) = \{gxg^{-1} : g \in G\}.$$

A function $\phi : G \to \mathbb{C}$ that is constant on conjugacy classes is called a class function. It follows that characters are class functions.

Exercise 3.2. (Easy) Show that if G is abelian, then every conjugacy class has only one element.

(Easy) Show that in $\mathcal{S}_3$, conjugacy classes are determined by cycle type.

(Medium) Show that in $\mathcal{S}_4$, conjugacy classes are determined by cycle type.

(Hard) Show that in $\mathcal{S}_n$, conjugacy classes are determined by cycle type.

Example 3.3. There are three conjugacy classes of $\mathcal{S}_3$,

$$C_1 = \{e\}, C_2 = \{(12)\}, C_3 = \{(123)\}.$$

Let $\rho : \mathcal{S}_3 \to \mathrm{GL}_3(\mathbb{C})$ be the usual representation sending $\sigma \in \mathcal{S}_3$ to its corresponding permutation matrix. Let χ be the character of ρ. Then

$$\chi(g) = \begin{cases} 3 & \text{if } g \in C_1 \\ 1 & \text{if } g \in C_2 \\ 0 & \text{if } g \in C_3. \end{cases}$$

To exploit the full power of characters we need to explore more of the structure behind them.

Definition. Let V be a vector space over $\mathbb{C}$. A map $\langle , \rangle : V \times V \to \mathbb{C}$ is called an inner product if it satisfies the following conditions for $u, v, w \in V$ and $\alpha \in \mathbb{C}$:

(1) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$;
(2) $\langle \alpha u, w \rangle = \alpha \langle u, w \rangle$;
(3) $\langle v, w \rangle = \overline{\langle w, v \rangle}$ (conjugate symmetry);
(4) $\langle v, v \rangle \geq 0$ and $\langle v, v \rangle = 0$ if and only if $v = 0$ (positive definite).

There is a standard inner product on characters (the dot product):

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi'(g).$$

Theorem 3.4. Let G be a group of order N, let $\rho_1, \rho_2, \ldots$ denote the distinct isomorphism classes of irreducible representations of G, χ_i the character of ρ_i, and d_i the dimension of ρ_i.

(1) Orthogonality relations: The characters χ_i are orthonormal. That is,

$$\langle \chi_i, \chi_j \rangle = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j. \end{cases}$$

(2) There are finitely many isomorphism classes of irreducible representations (up to equivalence), the same number as the number of conjugacy classes in the group.

(3) Each d_i divides N and $N = d_1^2 + \ldots + d_r^2$ where r is the number of conjugacy classes of the group.

We will defer the proof of this theorem. Instead we will look at some of the consequences.

Example 3.5. There are three conjugacy classes of $\mathcal{S}_3$ and the only way to write 6 as a sum of three squares is $1^2+1^2+2^2$. Hence, $\mathcal{S}_3$ has two (irreducible) one-dimensional representations and one irreducible two-dimensional representation, which we saw in Example 2.8.

Exercise 3.6. Let G be a group of order 8. Show that G has either eight distinct one-dimensional representations, or it has four distinct one-dimensional representations and one irreducible two-dimensional representations.

Theorem 3.7. Every irreducible representation of a finite group is 1-dimensional if and only if the group is abelian.[7]

Proof. Let G be a finite abelian group with $N = |G|$. If G is abelian, the number of conjugacy classes is N and so there are N irreducible representations. Thus, $|G| = d_1^2 + \cdots + d_N^2$ and so $d_i = 1$ for all $i = 1, \ldots, N$. Conversely, if every irreducible representation is 1-dimensional, then there are N conjugacy classes and so every conjugacy class is a singleton. It follows that G is abelian. $\square$

Exercise 3.8. Show that the set of class functions form a complex vector space, denoted $\mathcal{C}$.

[7]Admittedly, this theorem might be a little bit of a let down because we completely skipped the proof behind literally everything, but that's coming, I promise.

Corollary 3.9. The irreducible characters form an orthonormal basis of the class functions. Consequently, we may decompose any character into a linear combination of irreducible characters.

Proof. The characters are linearly independent because they are orthogonal and they span because the dimension of $\mathcal{C}$ is the number of conjugacy classes. $\square$

Corollary 3.10. Let $\chi_1, \ldots, \chi_r$ be the irreducible characters of a finite group and let χ be any character. Then $\chi = n_1\chi_1 + \ldots + n_r\chi_r$ where $n_i = \langle \chi, \chi_i \rangle$.

Proof. Since the irreducible characters form a basis for the space of class functions and χ is a class function, then $\chi = n_1\chi_1 + \ldots + n_r\chi_r$ for *some* n_i. By linearity of the inner product and orthogonality,

$$\langle \chi, \chi_i \rangle = \langle n_1\chi_1 + \ldots + n_r\chi_r, \chi_i \rangle = n_1\langle \chi_1, \chi_i \rangle + \cdots + n_i\langle \chi_i, \chi_i \rangle + \cdots + n_r\langle \chi_r, \chi_i \rangle = n_i. \quad \square$$

Corollary 3.11. If two representations have the same character, then they are isomorphic.

Proof. Let ρ, ρ' be two representations and χ, χ' their respective characters. Decompose ρ, ρ' into (unique) sums of irreducible representations,

$$\rho = n_1\rho_1 + \cdots + n_r\rho_r$$
$$\rho' = m_1\rho_1 + \cdots + m_r\rho_r.$$

The corresponding characters are

$$\chi = n_1\chi_1 + \cdots + n_r\chi_r$$
$$\chi' = m_1\chi_1 + \cdots + m_r\chi_r.$$

Since the χ_i are linearly independent, then $\chi = \chi'$ if and only if $n_i = m_i$ for each i. $\square$

Corollary 3.12. A character has the property $\langle \chi, \chi \rangle = 1$ if and only if it is irreducible.

Proof. By orthogonality, $\langle \chi, \chi \rangle = n_1^2 + \cdots + n_r^2$ and this is 1 if and only if one of the n_i is 1 and the rest are 0. $\square$

Example 3.13. Recall from Example 3.5 that $\mathcal{S}_3$ has 3 irreducible representations. These are listed in Example 2.8. Namely, they are the trivial representation ρ_1, the sign representation ρ_2, and the two-dimensional representation ρ_3.

We will arrange this information in a *character table*. If we list the irreducible characters χ_1, χ_2, χ_3 and the conjugacy classes C_1, C_2, C_3 (see Example 3.5), then the character table is a matrix whose (i,j) entry is the value of χ_i on C_j. Thus, for $\mathcal{S}_3$ the character table is

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

Only χ_3 needs to be explicitly checked. Recall that $\rho_3 : \mathcal{S}_3 \to \mathrm{GL}_2(\mathbb{C})$ is given by

$$\rho_3((1\ 2)) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho_3((1\ 3)) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

Since ρ_3 is 2-dimensional, then $\chi_3((1)) = 2$. Clearly $\chi_3((1\ 2)) = 0$ and

$$\rho_3((1\ 2\ 3)) = \rho_3((1\ 3)(1\ 2)) = \rho_3((1\ 3))\rho_3((1\ 2)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

so $\chi_3((1\ 2\ 3)) = -1$.

Why is χ_3 irreducible? $\mathcal{S}_3$ only has two 1-dimensional irreducible representations (characters). Hence, if χ_3 were reducible, then it would be a linear combination of χ_1 and χ_2. But the determinant of the character table is nonzero, so this is impossible.

Here's how we can do it using the inner product on characters.

$$\begin{aligned}
\langle \chi_3, \chi_3 \rangle &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_3(g)} \chi_3(g) \\
&= \frac{1}{6} \left[1 \cdot (\overline{\chi_3((1))} \chi_3((1)) + 3 \cdot (\overline{\chi_3((12))} \chi_3((12)) + 2 \cdot (\overline{\chi_3((123))} \chi_3((123)) \right] \\
&= \frac{1}{6} [1 \cdot 2 + 3 \cdot 0 + 2 \cdot 1] = 1.
\end{aligned}$$

Example 3.14. Let $G = \mathbb{Z}_3 = \langle a \rangle$. Since G is abelian there are three irreducible representations. It suffices to say how each representation acts on the generator a. Let ξ be a 3rd root of unity. Then $\rho_1(a) = 1$, $\rho_2(a) = \xi$, and $\rho_3(a) = \xi^2$. The character table is then

	e	a	a^2
χ_1	1	1	1
χ_2	1	ξ	ξ^2
χ_3	1	ξ^2	ξ

One can then use the orthogonality conditions to check that these representations are distinct.

Exercise 3.15. Construct the character table the Klein-4 group K from Exercise 1.10.

Exercise 3.16. Let ρ and ρ' be two representations of a group G and χ, χ' their respective characters. Show that the character of $\rho \otimes \rho'$ is $\chi \cdot \chi'$, where the multiplication is pointwise. Show further that the characters of G form a group under this operation.

4. Proof of the Orthogonality Relations

We now set out to prove the orthogonality relations from Theorem 3.4. Along the way we'll prove an fundamental result in algebra called *Schur's Lemma*.

To do these proofs purely using matrix representations requires a fair amount of algebraic acrobatics that can be avoided by introducing the language of G-modules. Thus, we redefine several of the concepts we have already seen.

Let V be a finite-dimensional vector space. Recall that V is a representation of a group G if there is a group homomorphism $\rho : G \to \mathrm{GL}(V)$. That is, for every $g \in G$, $\rho(g)$ is a linear transformation on V and so we may regard $\rho(g)$ as a matrix acting on V by left multiplication. Instead of writing $\rho(g)v$ for this action ($g \in G$ and $v \in V$), we simply write $g.v$. This action satisfies a number of axioms coming from the properties of groups and the properties of vector spaces:

- $e.v = v$ for every $v \in V$;
- $(gh).v = g.(h.v)$ for every $g, h \in G$ and $v \in V$;
- $g.(v + v') = g.v + g.v'$ for every $g \in G$ and $v, v' \in V$;
- $g.(cv) = c(g.v)$ for every $g \in G$, $v \in V$, and $c \in F$.

The dimension of the representation is the vector-space dimension of V.

Definition. A homomorphism $T : V \to V'$ of G-representations is a G-invariant linear map. That is, $T(g.v) = g.T(v)$ for all $g \in G$ and $v \in V$. Stated in terms of the corresponding homomorphisms ρ, ρ' this says $T \circ \rho = \rho' \circ T$.

If we fix bases for V, V' and let R_g, R'_g, A be the matrices corresponding to $\rho(g), \rho'(g)$, and T, respectively, then this statement becomes $R_g A = A R'_g$. This implies that if $\rho = \rho'$, then a V-endomorphism is one that commutes with $\rho(g)$ for every g.

Definition. Let ρ be a representation of G on a vector space V. A subspace W of V is G-invariant if $g.w \in W$ for all $w \in W$ and $g \in G$. The representation ρ is irreducible if V contains no non-trivial G-invariant subspace, otherwise it is reducible.

Lemma 4.1. Let $T : V \to V'$ be a homomorphism of G-representations. Then $\ker T$ and $\operatorname{im} T$ are G-invariant subspaces of V and V', respectively.

Proof. That $\ker T$ and $\operatorname{im} T$ are subspaces follows from standard linear algebra. We will prove that they are G-invariant.

Let $v \in \ker T$. Because T is a homomorphism of G-representations, then $T(g.v) = g.T(v) = 0$, so $g.v \in \ker T$ and $\ker T$ is G-invariant.

Similarly, if $w \in \operatorname{im} T$, then there exists $u \in V$ such that $T(u) = w$. Thus, $g.w = g.T(u) = T(g.u)$. Because V is a G-representation then $g.u \in V$ so $T(g.u) \in \operatorname{im} T$. Thus, $\operatorname{im} T$ is G-invariant. □

Theorem 4.2 (Schur's Lemma)**.** Let $T : V \to V'$ be a homomorphism of irreducible G-representations.

(1) Either T is an isomorphism, or else $T = 0$.
(2) If $V = V'$, then T is multiplication by a scalar.

Proof. (1) Since V is irreducible and $\ker T$ is a G-invariant subspace, then $\ker T = V$ or $\ker T = 0$. In the first case, $T = 0$. In the second, $V \cong \operatorname{im} T$. Since $\operatorname{im} T \neq 0$ is a G-invariant subspace of V' and V' is irreducbile, then $\operatorname{im} T = V'$ so T is an isomorphism.

(2) Suppose $V = V'$, so T is a linear operator on V. Choose an eigenvalue λ of T. Then $(T - \lambda I) = T_1$ is also G-invariant. Its kernel is nonzero because it contains an eigenvector. Since ρ is irreducible, $\ker T_1 = V$, so $T_1 = 0$. Thus, $T = \lambda I$. □

Let V be a representation and W a subspace of V. A projection map is a linear transformation $\pi : V \to W$ such that $\pi(w) = w$ for all $w \in W$. One way to do this is to take a basis for W and extend it to a basis for V. Then π fixes the basis vectors for W and sends the others to 0.

Lemma 4.3. Let W be an invariant subspace of the representation V. Let $\pi : V \to W$ be a projection. Then $V = W \oplus \ker \pi$.

Proof. Suppose $x \in W \cap \ker \pi$. Because π is a projection, $\pi(x) = x$, but because $x \in \ker \pi$ we have $x = \pi(x) = 0$, so $x = 0$.

Choose $v \in V$ and let $w = \pi(v)$. If $w = 0$ (or $w = v$) then we are done. Otherwise, write $v = w + (v - w)$. Then $w \in W$ and $v - w \in \ker \pi$. □

The next theorem is important in its own right and will lead to an important corollary regarding reducible representations. However, the trick involved in this theorem is important to understand for our original goal.

Theorem 4.4 (Maschke's Theorem)**.** Let G be a finite group and suppose $\operatorname{char} F \nmid G$. If V is a representation of G and W is an invariant subspace of V, then there is an invariant subspace W' of V such that $V = W \oplus W'$.

Proof. Let $\pi : V \to W$ be the projection map onto W (so $\pi(w) = w$). Define a new map $\pi' : V \to V$ by

$$\pi'(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1}.\pi(g.v).$$

The hypothesis on $\operatorname{char} F$ ensures that $|G|$ is invertible in F. We claim that π' is a G-equivariant linear map.

Linearity is clear. Since W is an invariant subspace of V, then for all $w \in W$,

$$\pi'(w) = \frac{1}{|G|} \sum_{g \in G} g^{-1}.\pi(g.w) = \frac{1}{|G|} \sum_{g \in G} g^{-1}.\pi(w') = \frac{1}{|G|} \sum_{g \in G} g^{-1}.w' = \frac{1}{|G|} \sum_{g \in G} w = w.$$

If $v \in V$, then $\pi(g.v) \in W$, so $g^{-1}.(\pi(g.v)) \in W$. It follows that $\pi'(v) \in W$, so $\pi' : V \to W$ is a projection.

Let $h \in G$, then

$$\begin{aligned} \pi'(h.v) &= \frac{1}{|G|} \sum_{g \in G} g^{-1}.\pi(g.(h.v)) = \frac{1}{|G|} \sum_{g \in G} (h.h^{-1}).(g^{-1}.\pi((gh).v)) \\ &= \frac{1}{|G|} \sum_{g \in G} h.((gh)^{-1}.\pi((gh).v))) = h.\frac{1}{|G|} \sum_{g \in G} (gh)^{-1}.\pi((gh).v)) = h.\pi'(v). \end{aligned}$$

This last claim follows by reindexing over the group. Thus, π' is G-equivariant.

Set $W' = \ker \pi'$. Then $V = W \oplus W'$ by the lemma. If $w' \in W'$ and $g \in G$, then $\pi'(g.w') = g.\pi'(w') = 0$, so $g.w' \in W'$. Thus W' is invariant. $\square$

Corollary 4.5. If G is a finite group and $\operatorname{char} F \mid |G|$, then every finite-dimensional representation of G is completely reducible.

Proof. This follows from Maschke's Theorem and induction. $\square$

It turns out that this result is true also in the infinite-dimensional case but more technology is needed.

Here is the moral of Maschke's Theorem. Given an arbitrary linear transformation $T : V \to V'$ of G-representations, we would not necessarily expect it to be G-invariant. However, we can always *create* a G-invariant linear transformation by averaging.

Exercise 4.6. Let $T : V \to V'$ be a linear transformation of G-representations. Prove that the map $\widehat{T} : V \to V'$ given by

$$\widehat{T}(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1}(T(gv)) \tag{1}$$

is a homomorphism of G-representations.

Observe that if ρ, ρ' are irreducible G-representations and T a linear transformation, then $\widehat{T}$ as defined above will be zero. If $\rho = \rho'$, the we will get that $\operatorname{trace} \widehat{T} = \operatorname{trace} T$.

Let χ', χ be two nonisomorphic irreducible characters for a group G corresponding to representations ρ, ρ' on vector spaces V, V'. We claim

$$\langle \chi', \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi'(g)} \chi(g) = \frac{1}{|G|} \sum_{g \in G} \chi'(g^{-1}) \chi(g) = 0.$$

Suppose $T : V \to W$ is *any* linear transformation. Averaging as in (1) gives a homomorphism $\widehat{T}$ which must be 0 by Schur's Lemma. Let's restate this in terms of matrices. Fix bases for V, W. Then for a matrix A of appropriate size,

$$\sum_{g \in G} \rho'(g^{-1}) A \rho(g) = 0. \tag{2}$$

Before continuing to the general case, suppose $\dim \rho = \dim \rho' = 1$. Then $\rho'(g^{-1})$ and $\rho(g)$ are 1×1 matrices and, moreover, $\rho(g) = \chi(g)$, $\rho'(g^{-1}) = \chi'(g^{-1})$ and we are done.

In general, $\chi(g) = \operatorname{trace} \rho(g) = \sum_j (\rho(g))_{jj}$ and $\chi'(g^{-1}) = \operatorname{trace} \rho'(g^{-1}) = \sum_i (\rho'(g^{-1}))_{ii}$. Thus,

$$\langle \chi', \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j} (\rho'(g^{-1}))_{ii} (\rho(g))_{jj}$$

Exercise 4.7. Let M, N be matrices and let $P = M e_{\alpha\beta} N$, where $e_{\alpha\beta}$ is a matrix unit of suitable size. The entries of P are $(P)_{ij} = (M)_{i\alpha} (N)_{\beta j}$.

Taking $A = e_{ij}$ in (2) we get for every $g \in G$,

$$0 = (0)_{ij} = \sum_g (\rho'(g^{-1}) e_{ij} \rho(g))_{ij} = \sum_g (\rho'(g^{-1}))_{ii} (\rho(g))_{jj}.$$

Hence, $\langle \chi', \chi \rangle = 0$.

Now we need to prove the second part of the orthogonality relations. Take $\chi = \chi'$ (so $\rho'(g^{-1}) = \rho(g^{-1})$). We claim $\langle \chi, \chi \rangle = 1$.

Note that in this case, averaging A gives (by Schur's Lemma),

$$\frac{1}{|G|}\sum_{g\in G}\rho(g^{-1})A\rho(g) = aI \tag{3}$$

for some scalar a. Now $\mathrm{trace}(A) = \mathrm{trace}(aI) = da$ where $d = \dim\rho$ so $a = \mathrm{trace}(A)/d$.

Set $A = e_{ij}$, then as before,

$$(aI) = \frac{1}{|G|}\sum_{g\in G}\sum_{i,j}(\rho(g^{-1})e_{ij}\rho(g))_{ij} = \frac{1}{|G|}\sum_{g\in G}\sum_{i,j}(\rho(g^{-1}))_{ii}(\rho(g))_{jj}$$

where $a = \mathrm{trace}(e_{ij})/d$. If $i \neq j$ then the left-hand side vanishes and otherwise it is equal to $1/d$. Thus,

$$\langle\chi,\chi\rangle = \frac{1}{|G|}\sum_{g}\sum_{j}(\rho(g^{-1}))_{ii}(\rho(g))_{ii} = \sum_{i}\left(\frac{1}{|G|}\sum_{g\in G}(\rho(g^{-1}))_{ii}(\rho(g))_{ii}\right) = \sum_{i}\frac{1}{d} = 1.$$

For the other character properties, the reader is directed to Artin's *Algebra* upon which most of the notes in this section are based.

5. Permutation representations

Where do we find these representations? We know that every group has a trivial representation and the symmetric groups have a sign representation, but beyond that representations can be hard to construct. There are a few other canonical representations that, while not irreducible, can be used to get information on the irreducibles.

Restricting the definition of a representation, we say a group G acts on a set S if there is a function $G \times S \to S$. As with representations, we typically write $g.s$ for the image of this map. Given any such set, we can turn it into a representation using the following definition.

Definition. Let S be a set on which G acts and let $\mathbb{C}(S)$ be the vector space of formal sums of elements of S. That is, $\mathbb{C}(S) = \left\{\sum_{s\in S} a_s s \mid a_s \in \mathbb{C}\right\}$. Then $\mathbb{C}(S)$ is a representation, called the permutation representation of G on S where the action is extended linearly from the action on S. Formally,

$$g.\left(\sum_{s\in S} a_s s\right) = \sum_{s\in S} a_s (g.s).$$

Suppose now that S is finite and fix an ordering on the elements, $s_1, \dots, s_n$. Then $\{s_1, \dots, s_n\}$ is a basis for $\mathbb{C}(S)$. Let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be the corresponding homomorphism. Since G acts on S it permutes the elements of S and hence $\rho(g)$ is a permutation matrix (see the discussion at the beginning of Section 2). If $n > 1$, then the permutation representation is never irreducible because the element $w = s_1 + \cdots + s_n$ is G-invariant. This corresponds to the trivial representation.

Proposition 5.1. Let G be a finite group acting on a finite set S, ρ the (associated) permutation representation, and χ it character. For all $g \in G$, $\chi(g)$ is the number of elements of S fixed by g.

Proof. For every index fixed by the permutation matrix $\rho(g)$, there is a 1 on the diagonal and otherwise there is a 0. □

Example 5.2. Recall our action of $\mathcal{S}_3$ on $V = \mathbb{C}^3$ with ($\sigma.e_i = e_{\sigma(i)}$). This *is* the permutation represention ρ on the set $S = \{e_1, e_2, e_3\}$.

We have seen this representation before. Recall that the image of ρ is

$$\rho((1)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho((1\,2)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho((1\,2\,3)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

By observation or using the previous proposition, the character χ of the representation ρ is

	(1)	(12)	(123)
χ	3	1	0

Recall that the character table for $\mathcal{S}_3$ is

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

Here, χ_1 is the character of the trivial representation, χ_2 is the character of the sign representation, and χ_3 is the irreducible two-dimensional representation.

Since χ_1 is a summand of χ, it follows that from the character table that $\chi = \chi_1 + \chi_3$. Hence, $\rho \cong \rho_1 \oplus \rho_3$. Therefore, to find ρ_3 to suffices to find the complement of the trivial representation. This representation is known as the *standard representation.* We can find it using Maschke's Theorem (it is $\ker \pi'$).

We will ignore the tedious calculations and cut to the chase (it's an easy verification once you know the answer). Let V be the permutation representation and write $V = W \oplus W^\perp$ where W is the trivial representation with basis $\{e_1 + e_2 + e_3\}$. Then

$$W^\perp = \mathrm{Span}\{(x_1, x_2, x_3) \mid x_1 + x_2 + x_3 = 0\}.$$

A basis for $W^\perp$ is $\{(1, -1, 0), (0, 1, -1)\} = \{e_1 - e_2, e_2 - e_3\}$. Call these elements $\{b_1, b_2\}$.

Applying (1 2) and (1 3) to this basis gives

$$\begin{aligned}
(1\ 2) :&\{e_2 - e_1, e_1 - e_3\} = \{-b_1, b_1 + b_2\}, \\
(1\ 3) :&\{e_3 - e_2, e_2 - e_1\} = \{-b_2, -b_1\}.
\end{aligned}$$

This corresponds to $\rho_3 : \mathcal{S}_3 \to \mathrm{GL}_2(\mathbb{C})$ given by

$$\rho_3((1\ 2)) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho_3((1\ 3)) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

Definition. The standard representation of $\mathcal{S}_n$ is the complement of the trivial representation. When $\mathcal{S}_n$ acts on $V = \mathbb{C}^n$ via $\sigma.e_i = e_{\sigma(i)}$, the standard representation is

$$\left\{ (x_1, \ldots, x_n) \mid \sum_{i=1}^n x_i = 0 \right\}.$$

Exercise 5.3. Verify that the standard representation is indeed a representation of $\mathcal{S}_n$, that it is the complement of the trivial representation, and find a basis.

Let's use what we have so far to construct the character table for $\mathcal{S}_4$. The group $\mathcal{S}_4$ has order 24 and four conjugacy classes with representatives: $(1), (1\ 2), (1\ 2\ 3), (1\ 2\ 3\ 4), (1\ 2)(3\ 4)$. Thus, there are five irreducible representations.

The trivial and sign representations are 1-dimensional, while the permutation representation is 4-dimensional. Their characters are below.

	(1)	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_{triv}	1	1	1	1	1
χ_{sgn}	1	-1	1	-1	1
χ_{perm}	4	2	1	0	0

The standard representation is the complement of the trivial representation in the permutation representation. Thus, $\chi_{std} = \chi_{perm} - \chi_{triv}$.

	(1)	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_{std}	3	1	0	-1	-1

This is irreducible since $\langle \chi_{std}, \chi_{std} \rangle = \frac{1}{24}\left(1 \cdot 3^2 + 6 \cdot 1^2 + 8 \cdot 0^2 + 6 \cdot (-1)^2 + 3 \cdot (-1)^2\right) = 1$.

One of the other two is obtained by taking the tensor product of χ_{sgn} and χ_{std}.

	(1)	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
$\chi_{sgn} \otimes \chi_{std}$	3	-1	0	1	-1

This is also irreducible and not a scalar multiple of χ_{std}. The last representation is the hardest to locate. We start by taking the tensor product of two copies of χ_{std}.

	(1)	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
$\chi_{std} \otimes \chi_{std}$	9	1	0	1	1

Set $\chi_5 = \chi_{std} \otimes \chi_{std} - (\chi_{std} + \chi_{sgn} \otimes \chi_{std} + \chi_{triv})$.

	(1)	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_5	2	0	-1	0	2

Again, one can check that this character is irreducible. The full table is listed below.

	(1)	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_{triv}	1	1	1	1	1
χ_{sgn}	1	-1	1	-1	1
χ_{std}	3	1	0	-1	-1
$\chi_{sgn} \otimes \chi_{std}$	3	-1	0	1	-1
χ_5	2	0	-1	0	2

Exercise 5.4. Find matrix representations for the irreducible representations of $\mathcal{S}_4$.

Another important representation derives from the action of a group G on itself.

Definition. Let G be a group and S the underlying set of G. Then G acts on S via left multiplication. The regular representation of G is the permutation representation associated to this action.

Let ρ_{reg} be the regular representation of a finite group G and χ_{reg} its character. Remember that $\chi_{reg}(g)$ is the number of fixed points of g. Since $gh = h \Rightarrow g = e$, Then $\chi_{reg}(e) = |G|$ and $\chi_{reg}(g) = 0$ if $g \neq 0$.

Proposition 5.5. Let G be a finite group with irreducible representations $\rho_1, \ldots, \rho_r$, ρ_{reg} the regular representation of G and χ_{reg} its character. Setting $d_i = \dim \rho_i$ we have

$$\chi_{reg} = d_1\chi_1 + \cdots + d_r\chi_r \text{ and } \rho_{reg} = d_1\rho_1 \oplus \cdots \oplus d_r\rho_r.$$

Proof. Let χ be any character of G. Then

$$\langle \chi_{reg}, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_{reg}(g)}\chi(g) = \frac{1}{|G|}\overline{\chi_{reg}(e)}\chi(e) = \frac{1}{|G|} \cdot |G| \cdot \dim \rho = \dim \rho.$$ □

Example 5.6. In $\mathcal{S}_3$, the character of the regular representation is

	(1)	(12)	(123)
χ_{reg}	6	0	0

It follows from the character table of $\mathcal{S}_3$ that $\chi_{reg} = \chi_1 + \chi_2 + 2\chi_3$.

A final representation we will introduce needs a little setup.

Definition. Let H be a subgroup of a group G and $g \in G$. The left coset of H in G with representative g is the set

$$gH = \{gh : h \in H\}.$$

Note that the left coset gH is a set and has no additional structure.

Proposition 5.7. Let H be a subgroup of a group G. The relation $\sim$ defined on G by $x \sim y$ if $x \in yH$ is an equivalence relation.

Proof. Let $x, y, z \in G$.

Since H is a subgroup, then $e \in H$ so $x = xe \in xH$. Thus, the relation is reflexive.

Suppose $x \sim y$, so $x \in yH$. Then $x = yh$ for some $h \in H$. Thus, $y = xh^{-1} \in xH$, so $y \sim x$ and $\sim$ is symmetric.

Finally, suppose $x \sim y$ and $y \sim z$, then $x \in yH$ and $y \in zH$. Thus, $x = yh_1$ and $y = zh_2$, so $x = (zh_2)h_1 = z(h_2h_1) \in zH$, so $x \in zH$ and $\sim$ is transitive. $\square$

It now follows that the left cosets of H in G *partition* G. That is, given two cosets g_1H and g_2H, they are either equal or disjoint ($g_1H \cap g_2H = \emptyset$). Moreover, $\bigcup_{g\in G} gH = G$. If G is finite, there are only finitely many left cosets of H in G. We say $\{g_1, \ldots, g_k\}$ a complete set of left coset representatives if $g_iH \neq g_jH$ for $i \neq j$ and $\bigcup_{i=1}^{k} g_iH = G$.

Definition. Let H be a subgroup of a group G and $\{g_1, \ldots, g_k\}$ a complete set of left coset representatives. Set $\mathcal{H} = \{g_1H, \ldots, g_kH\}$, then G acts on $\mathcal{H}$ via $g(g_iH) = (gg_i)H$. The left coset representation of G with respect to H is the permutation representation of G on $\mathcal{H}$.

Exercise 5.8. Let G be a group and H a subgroup. If $H = G$ then the left coset representation is the trivial representation. If $H = \{e\}$ then the left coset representation is the regular representation.

Example 5.9. Let $G = \mathcal{S}_3$ and $H = \langle(23)\rangle$. Then $\{(1), (12), (13)\}$ is a complete set of left coset representatives and so we take $\mathcal{H} = \{H, (12)H, (13)H\}$. Then

$$\mathbb{C}H = \{c_1H + c_2(12)H + c_3(13)H \mid c_i \in \mathbb{C}\}.$$

Let ρ be the left coset representation of G with respect to H. A computation shows that

$$\rho((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

As an exercise, you can compute $\rho((13))$ to find that this is the permutation representation of $\mathcal{S}_3$.

6. Restricted and induced representations

We'll end this unit by discussing how the representations of a subgroup H of G give representations of G and vice versa.

Definition. Let G be a group, H a subgroup of G and $\rho : G \to \mathrm{GL}(V)$ a representation of G. The restriction of ρ to H, denoted $\mathrm{Res}_H\, \rho$, is given by

$$\mathrm{Res}_H^G\, \rho(h) = \rho(h) \text{ for all } h \in H.$$

If χ is the character of ρ, then we denote the character of $\mathrm{Res}_H^G\, \rho$ by $\chi\downarrow_H^G$.

Exercise 6.1. (Easy) Verify that $\mathrm{Res}_H\, \rho$ is a representation of H.

Note that $\mathrm{Res}_H\, \rho$ may be reducible even if ρ is irreducible.

Definition. Let G be a group with subgroup H and $\{t_1, \ldots, t_m\}$ a complete set of (left) coset representatives. If $\pi : G \to \mathrm{GL}_d(\mathbb{C})$ is a (matrix) representation of H (of dimension d), then the corresponding induced representation, denoted is a map

$$\begin{aligned} \mathrm{Ind}_H\, \pi^G : G &\to \mathrm{GL}_{md}(\mathbb{C}) \\ g &\mapsto M_{ij} \end{aligned}$$

where

$$M_{ij} = \begin{cases} \pi(t_i^{-1} g t_j) & \text{if } t_i^{-1} g t_j \in H \\ 0 & \text{otherwise.} \end{cases}$$

If ψ is the character of π, we denote the character of $\mathrm{Ind}_H^G\, \pi$ by $\psi\uparrow_H^G$.

It is nontrivial that $\mathrm{Ind}_H\, \pi$ is a representation of G. The remainder of this section will be devoted to proving this fact, along with *Frobenius Reciprocity*, which relates induced and restricted characters via the inner product.

Example 6.2. Let $G = \mathcal{S}_3$ and $H = \langle (23) \rangle$. Then $\{(1), (12), (13)\}$ is a complete set of coset representatives. Let π be the trivial representation of H. We will compute $\mathrm{Ind}_H^G\, \pi$.

$$\begin{aligned} \pi((1)^{-1}(12)(1)) &= \pi((12)) = 0 && \text{since } (12) \notin H \\ \pi((1)^{-1}(12)(12)) &= \pi((1)) = 1 && \text{since } e \in H \\ \pi((1)^{-1}(12)(13)) &= \pi((123)) = 0 && \text{since } (123) \notin H. \end{aligned}$$

This gives us the first column for the matrix corresponding to $\operatorname{Ind}_H^G \pi((12))$. Continuing in this way we get

$$\operatorname{Ind}_H^G \pi((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that this is the same matrix we got for the coset representation of H.

Proposition 6.3. Let G be a group with subgroup H and let 1 be the trivial representation of H. Then $\operatorname{Ind}_H^G 1$ is isomorphic to the left coset representation of G with respect to H.

Proof. $\{t_1, \ldots, t_k\}$ a complete set of (left) coset representatives. Set $\mathcal{H} = \{t_1 H, \ldots, t_k H\}$ and let ρ be the left coset represntation.

Fix $g \in G$. Let $M = (M_{ij})$ be the matrix for $\operatorname{Ind}_H^G 1(g)$ and $N = (N_{ij})$ the matrix for $\rho(g)$. Note that both are matrices with entries 0 and 1 (why?). Then,

$$M_{ij} = 1 \Leftrightarrow t_i^{-1} g t_j \in H \Leftrightarrow g t_j \in t_i H \Leftrightarrow N_{ij} = 1. \qquad \square$$

Theorem 6.4. Let H be a subgroup of a group G and $\{t_1, \ldots, t_k\}$ a complete set of (left) coset representatives. If π is a representation of H, then $\operatorname{Ind}_H^G \pi$ is a representation of G.

Proof. Let $\rho = \operatorname{Ind}_H^G \pi$. For $g \in G$, we claim $\rho(g)$ is a block permutation matrix. That is, each row and column contains exactly one nonzero block: $(\pi(t_i^{-1} g t_j))$. Consider the first column. Then $g t_1 \in t_i H$ for exactly one t_i in our complete set of coset representatives. Hence, $t_i^{-1} g t_1 \in H$ and so $\pi(t_i^{-1} g t_1)$ is the desired block.

It is clear from the definition of induction that $\rho(e)$ is the identity matrix. It is only left to prove that π is a group homomorphism, that is,

$$\rho(g)\pi(h) = \rho(gh) \text{ for all } g, h \in G.$$

Consider the (i, j) block on both sides of the equation. It suffices to prove

$$\sum_k \pi(t_i^{-1} g t_k)\pi(t_k^{-1} h t_j) = \pi(t_i^{-1} g t_k).$$

Let $a_k = t_i^{-1} g t_k$, $b_k = t_k^{-1} h t_j$ and $c = \pi(t_i^{-1} g t_k)$, so our claim can be written more simply as

$$\sum_k \pi(a_k)\pi(b_k) = \pi(c).$$

If $\pi(c) = 0$, then $c \notin H$. Since $a_k b_k = c$ for all k, this implies $a_k \notin H$ or $b_k \notin H$ for all k. Thus, $\pi(a_k)$ or $\pi(b_k)$ is zero for each k, which forces the sum to be zero.

If $\pi(c) \neq 0$, then $c \in H$. Let m be the unique index such that $a_m \in H$. Thus, $b_m = a_m^{-1}c$ and so

$$\sum_k \pi(a_k)\pi(b_k) = \pi(a_m)\pi(b_m) = \pi(a_m b_m) = \pi(c). \qquad \square$$

The next proposition shows that the induced representation does not depend on the choice of representatives, that is, the map is well-defined.

Proposition 6.5. Suppose H is a subgroup of a group G and π is a representation of H. If $\{t_1, \dots, t_k\}$ and $\{s_1, \dots, s_k\}$ are two complete sets of (left) coset representatives inducing representation ρ and ρ' of G, then ρ and ρ' are equivalent.

Proof. Let χ, ψ, and ϕ be the respective character of ρ, π, and ρ'. We claim $\chi = \phi$ (equal characters implies isomorphic representations). Since the trace of a block matrix is the sum of the traces of the blocks on the diagonal, we have

$$\chi(g) = \sum_i \operatorname{trace} \pi(t_i^{-1}gt_i) = \sum_i \psi(t_i^{-1}gt_i),$$

where $\psi(g) = 0$ if $g \notin H$. Similarly,

$$\phi(g) = \sum_i \psi(s_i^{-1}gs_i).$$

The ordering of a set of representatives is irrelevant, so we can permute subscripts so that $t_iH = s_iH$ for all i. Thus, for each i, there exists $h_i \in H$ such that $t_i = s_ih_i$ and so $t_i^{-1}gt_i = h_i^{-1}s_i^{-1}gs_ih_i$. Thus, $t_i^{-1}gt_i \in H$ if and only if $s_i^{-1}gs_i \in H$, and if they both lie in H they are in the same conjugacy class, whence $\pi(t_i^{-1}gt_i) = \pi(s_i^{-1}gs_i)$ because characters are constant on conjugacy classes. $\square$

It follows from this proposition and the formulas therein that

$$\psi \uparrow^G (g) = \frac{1}{|H|}\sum_i \sum_{h \in H} \psi(h^{-1}t_i^{-1}gt_ih) = \frac{1}{|H|}\sum_{x \in G} \psi(x^{-1}gx). \tag{4}$$

Note that we have the following equivalent formulation of our inner product on characters:

$$\langle \chi, \chi' \rangle = \frac{1}{|G|}\sum_{g \in G} \overline{\chi(g)}\chi'(g) = \frac{1}{|G|}\sum_{g \in G} \overline{\chi(g^{-1})}\chi'(g^{-1}) = \frac{1}{|G|}\sum_{g \in G} \chi(g)\chi'(g^{-1}).$$

Theorem 6.6 (Frobenius Reciprocity)**.** Let H be a subgroup of a group G and suppose that ψ and χ are characters of H and G respectively. Then

$$\langle \psi \uparrow^G, \chi \rangle = \langle \psi, \chi \downarrow_H \rangle$$

where the left inner product is calculated in G and the right in H.

Proof. This follows from the inner product and the following inequalities:

$$\begin{aligned}
\langle \psi \uparrow^G, \chi \rangle &= \frac{1}{|G|} \sum_{g \in G} \psi \uparrow^G (g) \chi(g^{-1}) \\
&= \frac{1}{|G||H|} \sum_{x \in G} \sum_{g \in G} \psi(x^{-1}gx) \chi(g^{-1}) \qquad \text{by (4)} \\
&= \frac{1}{|G||H|} \sum_{x \in G} \sum_{y \in G} \psi(y) \chi(xy^{-1}x^{-1}) \qquad \text{let } y = x^{-1}gx \\
&= \frac{1}{|G||H|} \sum_{x \in G} \sum_{g \in G} \psi(y) \chi(y^{-1}) \qquad \chi \text{ is constant on } G\text{'s conjugacy classes} \\
&= \frac{1}{|H|} \sum_{g \in G} \psi(y) \chi(y^{-1}) \\
&= \frac{1}{|H|} \sum_{h \in H} \psi(y) \chi(y^{-1}) \qquad \psi(y) = 0 \text{ if } y \notin H \\
&= \langle \psi, \chi \downarrow_H \rangle.
\end{aligned}$$

□