MATH-314: Representation Theory of Finite Groups

Sidharth Hariharan

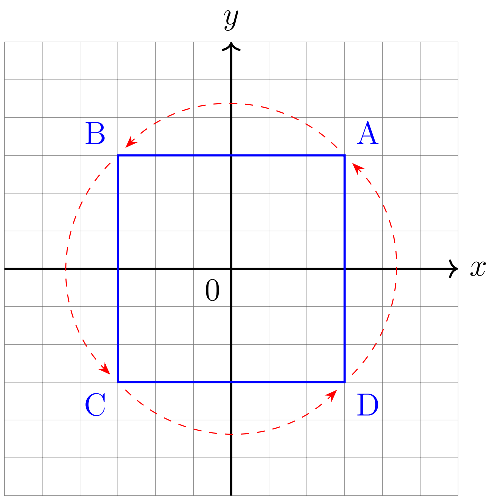
École Polytechnique Fédérale de Lausanne - Spring 2024

Contents

Chapter 1

An Introduction to the Theory of Representations of Groups

As I understand it, the fundamental idea behind Representation Theory is to study the actions of groups on vector spaces. While arbitrary vector spaces over arbitrary fields might not have naturally visualisable geometric properties, representations of groups in the ones that do can greatly illustrate the nature of these groups, especially to individuals like myself who delight in (somewhat literally) *seeing* mathematics come alive.



A key motivating example in the study of representation theory would be the representations of Dihedral groups over $\mathbb{R}^2$. It is very natural to (at least informally) view the Dihedral group D_n of order $2n$ as the group of symmetries of the regular n-gon; in other words, elements of D_n have natural actions on a regular n-gon that preserve its structure. For instance, D_4 contains an element that rotates a square clockwise by $90°$, an action under which the square is, of course, invariant.

If one were to now plot this square in $\mathbb{R}^2$, then action of the same element on the square can be extended to an orthogonal transformation of $\mathbb{R}^2$ that maps the x-axis to the y-axis and vice-versa, but in a manner preserving orientation (ie, that *rotates the plane clockwise by* $90°$). In a similar fashion, one can extend the actions of all dihedral groups D_n to actions on the entirety of $\mathbb{R}^2$. More precisely, to every element of a dihedral group, one can ascribe a specific *matrix* that transforms $\mathbb{R}^2$ in a manner preserving the regular n-gon.

This motivates the formal definition of a representation.

1.1 Important Definitions

1.1.1 What is a Representation?

It turns out that representations can be defined quite broadly, sidestepping the geometric niceties (or are they constraints?) of Euclidean spaces.

Definition 1.1.1 (Group Representation)**.** Let G be a group. A representation of G is a pair (V, ρ) of a vector space V and a group homomorphism $\rho : G \to \mathrm{GL}(V)$.

Here, $\mathrm{GL}(V)$ refers to the **G**eneral **L**inear group over V, consisting of all vector space automorphisms of V equipped with the binary operation of composition.

Definition 1.1.2 (Degree of a Representation)**.** Let G be a group and let (V, ρ) be a representation of G. We define the degree of V to be the dimension of V over its base field.

There exist innumerable examples of representations throughout mathematics. Below, we give some important ones.

Example 1.1.3 (Important Classes of Representations)**.**

1. The trivial representation. Let G be a group and V be any vector space. The map $\rho : G \to \mathrm{GL}(V) : g \mapsto \mathrm{id}_V$ is a representation.
2. The zero representation. Let G be a group and let $V = \{0\}$ be the zero vector space over an arbitrary field K. The trivial representation over V is known as the zero representation.

3. The sign representation. Let $G = S_n$, the symmetric group on n elements, and let $V = K$, a field. Then, $\mathrm{GL}(V) = K^\times$, the multiplicative group of K. Denoting by ξ the canonical map from $\mathbb{Z}$ to K, the map

$$\rho : G \to \mathrm{GL}(V) : \sigma \mapsto \xi(\mathrm{sgn}(\sigma))$$

is a representation, where $\mathrm{sgn} : G \to \{-1, 1\}$ denotes the sign homomorphism.

4. Permutation representations. Let G be a group acting on a finite set X, and let $V = K[X]$, the free vector space (over some field K) generated by X. Consider a K-basis $\{e_x \in V : x \in X\}$ of V. Then, the map $\rho : G \to \mathrm{GL}(V)$ given by

$$\rho(g)(e_x) = e_{g(x)}$$

is a representation.

5. The regular representation. Let G be a *finite* group. The permutation representation corresponding to the canonical action of G on itself by left-multiplication gives a representation of G over $K[G]$, the free vector space generated by G (as a set) over any field K.

Non-Example 1.1.4. Let G be a group and let V be a nonzero vector space over an arbitrary field. The map $g \mapsto 0 : G \to (V \to V)$ is not a representation because the zero map $0 : V \to V$ is not invertible.

Definition 1.1.5 (Faithfulness)**.** Let G be a group and let (V, ρ) be a representation of G. We say (V, ρ) is faithful if $\ker(\rho)$ is trivial.

As it turns out, we also have a notion of morphisms of representations.

1.1.2 Morphisms of Representations

Definition 1.1.6 (Homomorphism of Representations)**.** Let G be a group and let (V, ρ) and (V', ρ') be two representations of G. A homomorphism of representations $T : V \to V$ is a linear map $T : V \to V'$ such that $\forall g \in G$,

$$T \circ \rho(g) = \rho'(g) \circ T$$

or equivalently, the following diagram commutes:

$$\begin{tikzcd} V \arrow[r, "\rho(g)"] \arrow[d, "T"'] & V \arrow[d, "T"] \\ V' \arrow[r, "\rho'(g)"'] & V' \end{tikzcd} \tag{1.1.1}$$

Such a map T is said to be G-*linear*.

Remark. The term G-linear comes from the fact that a homomorphism of representations satisfies the property that $T(g(v)) = g(T(v))$, where the notation $g(\cdot)$ represents the action of some $g \in G$, encoded by a representation. In this sense, T is somehow "linear over G".

A natural way to define two representations to be equal, or 'isomorphic,' is as follows.

Definition 1.1.7 (Equivalence of Representations)**.** Let G be a group and let (V, ρ) and (V', ρ') be two representations of G. We say that (V, ρ) and (V', ρ') are equivalent, denoted $(V, \rho) \sim (V', \rho')$, if there exists a homomorphism $T : (V, \rho) \to (V', \rho')$ that is invertible as a linear map—ie, that gives a linear isomorphism between V and V'.

Representations of the same group over the same vector space need not be equivalent.

Example 1.1.8 (Non-Equivalent Representations of the Klein 4-Group)**.** Let $G = C_2 \times C_2$ be the Klein 4-group (where $C_2 = \langle x \rangle$ is the cyclic group of order 2). Let $\alpha = (x, 1)$ and $\beta = (1, x)$. Together, they generate G.

Now, let K be a field. Consider a degree 1 representation $\rho : G \to K^\times$. We know that $\rho(G)$ must be a subgroup of $K^\times$ such that $|\rho(G)| \in \{1, 2, 4\}$. If $\mathrm{char}(K) = 2$, then ρ

must be the trivial representation, since $2 \nmid |K^\times|$. Else, all four maps ρ satisfying

$$(\rho(\alpha)\,, \rho(\beta)) = (\pm 1, \pm 1)$$

give *non-equivalent* representations of G in $K^\times$. In particular, we see the non-equivalence because $K^\times$ is commutative.

The point of morphisms of representations is to be able to move from one vector space to another without losing the structural information captured by the representation. This is precisely illustrated in (1.1.1).

Example 1.1.9 (Representations of Cyclic Groups over $\mathbb{R}^2$ and $\mathbb{R}^3$)**.** Consider the cyclic group $C_n = \langle g \rangle$ of order n. Let $V = \mathbb{R}^2, V' = \mathbb{R}^3$. Together with the respective maps

$$\rho : G \to \mathrm{GL}\big(\mathbb{R}^2\big) : g^m \mapsto \begin{bmatrix} \cos(2\pi/m) & -\sin(2\pi/m) \\ \sin(2\pi/m) & \cos(2\pi/m) \end{bmatrix}$$

$$\rho' : G \to \mathrm{GL}\big(\mathbb{R}^3\big) : g^m \mapsto \begin{bmatrix} \cos(2\pi/m) & -\sin(2\pi/m) & 0 \\ \sin(2\pi/m) & \cos(2\pi/m) & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

they give representations of C_n. Consider now the inclusion $T : \mathbb{R}^2 \to \mathbb{R}^3$ whose matrix with respect to the standard bases of $\mathbb{R}^2$ and $\mathbb{R}^3$ is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$. One can see that T gives a map from (V, ρ) to (V', ρ'). Indeed, the corestriction of T to its image is a linear isomorphism, which gives an equivalence between (V, ρ) and $(T(V), \rho)$, where we restrict the domains of each $\rho(g^m)$ to $T(V)$.

The above example leads to an interesting question. Can we think of one representation as being "contained" in another?

It turns out that we can.

1.1.3 Subrepresentations

We have the objects; we have the morphisms. It is only natural to think about what the subobjects would be in the context of group representations. And if Example 1.1.9 is any indication, they involve something more than just an inclusion. There is some structural property of a sub-vector space of a representation that makes it *compatible* with the representation structure. In the case of Example 1.1.9, for instance, this is the fact that the representation ρ' acted only "horizontally"–ie, "parallel" to the subspace $T(V)$.

More generally, it turns out that the property we really require a subspace to have in order to be 'compatible' with the representation structure is the following.

Definition 1.1.10 (G-Invariance)**.** Let G be a group and let (V, ρ) be a representation of G. We say that a sub-vector space $W \leq V$ is G-invariant if for all $w \in W$ and $g \in G$,

$$\rho(g)(w) \in W$$

In other words, W is G-invariant if W is $\rho(g)$-invariant for every $g \in G$.

One can make the following observation. Let G be a group, (V, ρ) a representation of G, and $W \leq V$ a G-invariant subspace. Then, $\forall g \in G$, $\rho(g) \in \mathrm{GL}(W)$. That is, $\rho(g)$ is a linear automorphism of W whose inverse, $\rho(g^{-1})$, is *also* a linear automorphism of W. This then leads to the following definition of a subrepresentation.

Definition 1.1.11 (Subrepresentation)**.** Let G be a group and let (V, ρ) be a representation of G. A subrepresentation of V is a pair $(W, \rho|_W)$ consisting of a G-invariant subspace $W \leq V$ and the map

$$\rho|_W : G \to \mathrm{GL}(W) : g \mapsto \rho(g)|_W$$

It is very important to note that the map $\rho|_W$ is *not actually a restriction of ρ to a specific domain.* Rather, it is a map that restricts the domain of $\rho(g)$ for every $g \in G$.

One can also observe easily that a subrepresentation is given uniquely by a G-invariant subspace. Hence, we will often abuse notation and not distinguish between the pair $(W, \rho|_W)$

(which is actually a representation) and simply W (which is merely a subspace).

Example 1.1.12. Let G be a finite group and K a field. Consider the regular representation $\rho : G \to K[G]$. Let $\{e_g : g \in G\}$ denote a basis of $K[G]$. Then, the subspace $W := \operatorname{Span}\left(\sum_{g\in G} e_g\right)$ is G-invariant.

It turns out that morphisms of representations also give us subrepresentations.

Proposition 1.1.13. *Let G be a group and let (V,ρ) be a representation of G. Let $T : (V,\rho) \to (V,\rho)$ be a homomorphism of representations. Then, the subspaces* $\ker(T)$ *and* $\operatorname{im}(T)$ *of V are G-invariant.*

Proof. Fix $g \in G$ and $v \in \ker(T)$. We know $T(\rho(g)(v)) = \rho(g)(T(v))$. Since $T(v) = 0$, $T(\rho(g)(v)) = 0$. Hence, $\rho(g)(v) \in \ker(T)$, proving that $\ker(T)$ is G-invariant.

Now, fix $w \in \operatorname{im}(T)$. Then, $w = T(u)$ for some $u \in V$. Clearly, $\rho(g)(w) = \rho(g)(T(u)) = T(\rho(g)(u)) \in \operatorname{im}(T)$, proving that $\operatorname{im}(T)$ is G-invariant as well. □

1.1.4 Irreducibility

Having discussed the subobjects of representations (namely, subrepresentation), it is only natural to wish to describe whether a representation ever contains a nontrivial subrepresentation. I say "nontrivial" because any representation naturally admits two (uninteresting) subrepresentations: the trivial representation and itself.

Akin to the definition of simple groups, where we answer a similar question, we have the following definition that captures this idea.

Definition 1.1.14 (Irreducibility)**.** Let G be a group and (V,ρ) a nonzero representation of G. We say (V,ρ) is irreducible if V contains no proper, nonzero G-invariant subspaces.

In similar fashion, we say a nonzero representation is reducible if it is not irreducible.

Given that MATH-314 focuses on *finite* groups, the following result is quite useful.

Proposition 1.1.15. *Let G be a group and let (V, ρ) be a representation of G. If G is finite and (V, ρ) is irreducible, then V is finite-dimensional.*

Proof. Since (V, ρ) is irreducible, in particular, $V \supsetneq \{0\}$—ie, $\exists v \in V$ such that $v \neq 0$. Let $W := \mathrm{Span}(\{\rho(g)(v) : g \in G\})$. Since $0 \neq v \in W$, W is a nonzero subspace of V. Furthermore, since G is finite, W is finite-dimensional. We show that W is, in fact, G-invariant. Then, since V is irreducible, W could not possibly be a proper subspace of V, meaning that $W = V$, making V finite-dimensional as well.

Fix $h \in G$, and consider an arbitrary element $w = \sum_{g \in G} \lambda_g \rho(g)(v) \in W$. Then,

$$\begin{aligned}
\rho(h)(w) &= \sum_{g \in G} \lambda_g \rho(h)(\rho(g)(v)) \\
&= \sum_{g \in G} \lambda_g \left(\rho(h) \circ \rho(g)\right)(v) \\
&= \sum_{g \in G} \lambda_g \rho(hg)(v) \in W
\end{aligned}$$

proving that W is $\rho(h)$-invariant for every $h \in G$, making it a G-invariant subspace of V. Therefore, as argued above, $W = V$, proving that V is finite-dimensional. □

Example 1.1.16 (Simple Examples of Irreducible Representations)**.**

1. Any representation of degree 1 is irreducible.
2. Let K be a field. The trivial embedding $\mathrm{SL}(n, K) \hookrightarrow \mathrm{GL}(n, K)$ gives an irreducible representation of $\mathrm{SL}(n, K)$ over K^n.

   Proof. Assume $n > 1$ (else, the result follows from the previous point). For the sake of contradiction, suppose there exists a nonzero, $\mathrm{SL}(n, K)$-invariant subspace W of K^n having dimension $m < n$. Let $\mathcal{B} = \{e_1, \ldots, e_m\}$ be a basis of W, extending to a basis $\bar{\mathcal{B}} = \{e_1, \ldots, e_m, e_{m+1}, \ldots, e_n\}$ of V. Consider the linear map

$T \in \mathrm{SL}(n, K)$ having matrix

$$[T]_{\bar{\mathcal{B}}} = \begin{bmatrix} & & & (-1)^{n+1} \\ & & \cdot^{\cdot^{\cdot}} & \\ & -1 & & \\ 1 & & & \end{bmatrix}$$

with respect to $\bar{B}$. Clearly, $T(e_1) = e_n$, even though $e_1 \in W$ and $e_n \notin W$, contradicting the $\mathrm{SL}(n, K)$-invariance of W. $\square$

Non-Example 1.1.17. Let G be a finite group and K a field. Consider the regular representation $(K[G], \rho)$. In the notation of Example 1.1.12, we know that $W := \mathrm{Span}\left(\sum_{g \in G} e_g\right)$ is G-invariant. If $|G| > 1$, then W is a proper subspace of $K[G]$, as it has dimension 1 (whereas $K[G]$ has dimension $|G|$). Furthermore, W is nonzero. Hence, $(K[G], \rho)$ is not irreducible (unless $|G| = 1$, in which case it follows from the first point of Example 1.1.16 that $(K[G], \rho)$ is irreducible).

We also have the following interesting criterion for irreducibility of representations of finite groups over $\mathbb{C}$.

Lemma 1.1.18. *Let G be a finite group and let $(\mathbb{C}^2, \rho)$ be a representation of G over $\mathbb{C}$. If there exist $g, h \in G$ such that g and h do not commute, then $(\mathbb{C}^2, \rho)$ is irreducible.*

Proof. `sorry` $\square$

1.2 Invariant Constructions

In this section, we briefly examine how ordinary linear algebraic constructions can interact with representations. We are particularly interested in the notion of *invariance*, wherein a construction respects the structure of the representation(s) involved.

1.2.1 Direct Sums of Representations

The most elementary operation we can think about when we have two objects is *putting them together*. One of the most meaningful ways of doing so in the context of linear algebra is the direct sum of two vector spaces. It turns out that this extends rather naturally to representations.

Definition 1.2.1 (The Direct Sum of Two Representations)**.** Let G be a group and let (V, ρ) and (V', ρ') be representations of G. We define the direct sum of (V, ρ) and (V', ρ') to be the pair $(V \oplus V', \rho \oplus \rho')$, where $V \oplus V'$ is the direct sum of V and V' as vector spaces and $\rho \oplus \rho' : G \to \mathrm{GL}(V \oplus V')$ maps every $g \in G$ to the map

$$(\rho \oplus \rho')(g)(v \oplus v') = \rho(g)(v) \oplus \rho'(g)(v') \in \mathrm{GL}(V)$$

Proposition 1.2.2. *Let G be a group and let (V, ρ) and (V', ρ') be representations of G.*

1. *The direct sum $(V \oplus V', \rho \oplus \rho')$ of (V, ρ) and (V', ρ') is, indeed, a representation of G.*
2. *V and V' are G-invariant subspaces*[1] *of $V \oplus V'$.*

Proof.

1. Fix $g, h \in G$. For all $v \oplus v' \in V \oplus V'$,

$$\begin{aligned}(\rho \oplus \rho')(gh)(v \oplus v') &= \rho(gh)(v) \oplus \rho'(gh)(v') \\ &= \rho(g)(\rho(h)(v)) \oplus \rho'(g)(\rho'(h)(v')) \\ &= (\rho \oplus \rho')(g)((\rho \oplus \rho')(h)(v \oplus v'))\end{aligned}$$

   proving that $\rho \oplus \rho'$ is multiplicative. Then, for any $g \in G$, $(\rho \oplus \rho')(g)$ has inverse $(\rho \oplus \rho')(g^{-1})$. Hence, $\rho \oplus \rho'$ is a homomorphism from G to $\mathrm{GL}(V \oplus V')$.
2. Fix $g \in G$ and $v \in V$. Clearly, $(\rho \oplus \rho')(g)(v) = \rho(g)(v)$. Since $\rho(g) \in \mathrm{GL}(V)$, it follows that $\rho(g)(v) \in V$. The proof that V' is G-invariant is identical.

$\square$

[1] Technically, isomorphic to the subspaces $V \oplus \{0\}$ and $\{0\} \oplus V'$, but we overlook such distinctions.

The above proposition gives us another reason to consider the direct sum to be an "invariant" construction: while it enriches both the vector space structure and the representation structure of a summand by adding another representation into the mix, it does not take anything away from the constructions that already exist.

With direct sums, we also have similar notions to reducibility.

Definition 1.2.3 (Indecomposability)**.** A nonzero representation is said to be indecomposable if it is inexpressible as a direct sum of two proper, nonzero subrepresentations.

Nonzero representations that are not indecomposable are said to be decomposable.

We have a natural relationship between irreducibility and indecomposability.

Proposition 1.2.4. *Let G be a group and let (V, ρ) be a representation of G. If (V, ρ) is irreducible, then it is indecomposable.*

Proof. If $V = \{0\}$, then the result is vacuously true. If $V \neq \{0\}$, then if it is decomposable, it contains a proper, nonzero, G-invariant subspace, making it reducible. □

Example 1.2.5. Let $C_2 = \langle a \rangle$ be the cyclic group of order 2, and let (V, ρ) be the regular representation of C_2 over a field K.

1. Let $K = \mathbb{C}$. Then, let $W_1 := \operatorname{Span}(e_1 + e_a)$ and $W_2 := \operatorname{Span}(e_1 - e_a)$. It is obvious that $W_1 \oplus W_2 = V$. Furthermore, W_1 and W_2 are both C_2-invariant. Hence, the regular representation of C_2 over $\mathbb{C}$ is decomposable.
2. Let $K = \mathbb{F}_2$. Then, $V = \{0, e_1, e_a, e_1 + e_a\}$. If (V, ρ) were reducible, it would need to be expressible as the direct sum of two subrepresentations of degree 1. But, the only G-invariant subspace of V of dimension 1 is $\{0, e_1 + e_a\}$. Hence, (V, ρ) cannot be indecomposable.

The $K = \mathbb{F}_2$ case in the above example demonstrates an important fact: *the converse of Proposition 1.2.4 is not true.* The regular representation of C_2 over $\mathbb{F}_2$ is clearly reducible—the subspace $\{0, e_1 + e_a\}$ is clearly C_2-invariant—but it is still indecomposable. That said, it turns out that under certain conditions, we *do* have a converse.

Proposition 1.2.6. *Let G be a finite group and let K be a field. All indecomposable representations of G are irreducible if and only if* $\mathrm{char}(K)$ *does not divide* $|G|$*.*

Proof. `sorry` □

Finally, just like everywhere else in mathematics where we encounter the word "irreducible," in the context of representation theory, too, we have a notion of decomposition into irreducibles.

Definition 1.2.7 (Complete Reducibility)**.** A representation is said to be completely reducible if it is expressible as a direct sum of irreducible representations.

1.2.2 Complementary Subrepresentations

It is a well-known fact from Linear Algebra that for any finite-dimensional vector space V, for any subspace $W \leq V$, there exists a *complementary* subspace $W' \leq V$ such that $W \oplus W' = V$. Over Euclidean spaces, for example, we have the very important notion of *orthogonal* complements.

We can define a similar notion for representations, too.

Definition 1.2.8 (Complementary Subrepresentation)**.** Let G be a group and let (V, ρ) be a representation of G. Let $(W, \rho|_W)$ be a subrepresentation of (V, ρ). A complementary subrepresentation of $(W, \rho|_W)$ is a subrepresentation $(U, \rho|_U)$ such that $V = U \oplus W$.

This notion of complementarity is, indeed, compatible with the notion of direct sums of representations.

Proposition 1.2.9. *Let G be a group and let (V, ρ) be a representation of G. Let $(W, \rho|_W)$ and $(U, \rho|_U)$ be complementary subrepresentations. Then, their direct sum $(V, \rho|_W \oplus \rho|_U)$ is equivalent to (V, ρ) as a representation of G.*

Proof. It suffices to show that $\rho = \rho|_W \oplus \rho|_U$. Then, the identity map would give an equivalence of representations. Indeed, every $v \in V$ is expressible uniquely as a direct sum $w \oplus u$ for some $w \in W$ and $u \in U$. So, for all $g \in G$,

$$\begin{aligned}\rho(g)(v) &= \rho(g)(w \oplus u)\\ &= \rho(g)(w) \oplus \rho(g)(u)\\ &= \rho|_W(g)(w) \oplus \rho|_U(g)(u)\\ &= (\rho|_W \oplus \rho|_U)(g)(w \oplus u)\end{aligned}$$

where the sum in the second equality is direct because W and U are $\rho(g)$-invariant. □

We now recall an important result from Linear Algebra.

Definition 1.2.10 (Projection)**.** Let V be a vector space and let $T : V \to V$ be linear. Observe that we have the following equivalence:

$$T^2 = T \iff \forall w \in \mathrm{im}(T)\,,\ T(w) = w \tag{1.2.1}$$

If T satisfies either one of the above conditions, T is said to be a projection.

We do not prove (1.2.1), but we do prove the following lemma, which will prove to be useful.

Lemma 1.2.11. *Let V be a vector space. For all projections $T : V \to V$, $V = \ker(T) \oplus \mathrm{im}(T)$.*

Proof. Let $T : V \to V$ be a projection. We then have the following.

$\underline{\mathrm{im}(T) \cap \ker(T) = \{0\}}$: Fix $w \in \mathrm{im}(T) \cap \ker(T)$. Since $w \in \mathrm{im}(T)$, $\exists v \in V$ such that $w = T(v)$. Furthermore, since $w \in \ker(T)$, $T(w) = 0$. Since $w = T(v)$, this is equivalent to saying that $T(T(v)) = 0$. But, by (1.2.1), $T(T(v)) = T(v)$. Hence, $T(v) = 0$. Then, since $T(v) = w$, it follows that $w = 0$.

$\underline{V = \ker(T) + \mathrm{im}(T)}$: Fix $v \in V$. We write $v = T(v) + (v - T(v))$. Clearly, $T(v) \in \mathrm{im}(T)$. Further, $T(v - T(v)) = T(v) - T(v) = 0$. Hence, $v - T(v) \in \ker(T)$.

Therefore, we do, indeed, have $V = \ker(T) \oplus \mathrm{im}(T)$. □

It turns out that this gives us an important criterion for decomposability.

Corollary 1.2.12. *Let G be a group and let (V, ρ) be a representation of G. If $T : (V, \rho) \to (V, \rho)$ is a G-linear projection, then $V = \ker(T) \oplus \operatorname{im}(T)$ is a direct sum of subrepresentations.*

Proof. The result follows immediately from Lemma 1.2.11 and Proposition 1.1.13. □

One also has a converse criterion for G-linearity.

Proposition 1.2.13. *Let G be a group and let (V, ρ) be a representation of G, and let $T : V \to V$ be a projection. If $\ker(T)$ and $\operatorname{im}(T)$ are both G-invariant, then T is G-linear.*

Proof. Since T is a projection, we know that $V = \ker(T) \oplus \operatorname{im}(T)$. Now, fix $g \in G$ and $v \in V$. We know v can uniquely be expressed as $u + w$, where $u \in \ker(T)$ and $w \in \operatorname{im}(T)$. Then,

$$\begin{aligned} T(\rho(g)(v)) &= T\left(\underbrace{\rho(g)(u)}_{\in \ker(T)} + \underbrace{\rho(g)(w)}_{\in \operatorname{im}(T)}\right) \\ &= \rho(g)(w) \\ &= \rho(g)(T(v)) \end{aligned}$$

proving that T is, indeed, G-linear. □

Example 1.2.14. Consider the situation in Example 1.1.9. As we discussed briefly at the beginning of Subsection 1.1.3, we can view (V, ρ) as a subrepresentation of (V', ρ'). Now, consider the linear map $S : V' \to V' : (x, y, z) \mapsto (x, y, 0)$, where (x, y, z) are coordinates with respect to the standard basis. This is clearly a projection operator with image V, the (x, y) plane, and kernel the z-axis. These are both clearly G-invariant, making S a G-linear projection.

1.2.3 Maschke's Theorem

Given the theme of this section—namely, understanding the compatibility of ordinary linear-algebraic constructions with representation structures—one might wonder under what conditions (if any) we have the existence of a complementary subrepresentations. The answer lies in Maschke's Theorem, which is the first major result of the course.

Theorem 1.2.15 (Maschke's Theorem)**.** *Let G be a finite group, K a field such that $\mathrm{char}(K) \nmid |G|$, and (V, ρ) a representation of G over K. Then, any subrepresentation of V admits a complementary subrepresentation.*

Proof. Let $W \leq V$ be G-invariant. The idea is to construct a G-linear map from V to V with image W. Then, by Corollary 1.2.12, its kernel would give a complementary subrepresentation.

From Linear Algebra, we know that W admits a complementary (but not necessarily G-invariant) subspace $U \leq V$. Then, every $v \in V$ can uniquely be expressed as a sum $u + w$, where $u \in U$ and $w \in W$. Define $T : V \to V : u + w \mapsto w$. Clearly, T is a projection operator with image W and kernel U.

If T were G-linear, we would be done with the proof; unfortunately, T does not have to be G-linear. We therefore "convert" T into a G-linear projection $S : V \to V$ by *averaging over* G. Specifically, define

$$S := \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ T \circ \rho(g)^{-1} \tag{1.2.2}$$

which is well-defined because $|G| \neq 0$ in K. We then show the following.

<u>S is a projection with image W.</u> Fix $v \in V$ and express it as $u + w$ for a unique $u \in U$ and $w \in W$. Then, for all $g \in G$,

- $T(\rho(g)^{-1}(v)) \in W$ because T is a projection with image W.
- $\rho(g)(T(\rho(g)^{-1}(v))) \in W$ because $T(\rho(g)^{-1}(v)) \in W$ and W is G-invariant.

Combined with the fact that W is closed under addition, this proves that $\mathrm{im}(S) \subseteq W$. Conversely, for all $w \in W$ and $g \in G$,

- $(\rho(g)^{-1})(w) = \rho(g^{-1})(w) \in W$ because W is G-invariant.
- $T(\rho(g^{-1})(w)) \in W$ because $\rho(g^{-1})(w) \in W$ and W is T-invariant.
- $\rho(g)(T(\rho(g^{-1})(w))) \in W$ because W is G-invariant.

Combined, again, with the fact that W is closed under addition, this proves that $W \subseteq$

im(S). Therefore, we have that $W = \text{im}(S)$.

Finally, since $T|_W = \text{id}_W$, we have that $\forall w \in \text{im}(S) = W$,

$$\begin{aligned} S(w) &= \frac{1}{|G|} \sum_{g \in G} \rho(g) \left(T \left(\underbrace{\rho(g)^{-1}(w)}_{\in W} \right) \right) \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\rho(g) \circ \rho(g)^{-1} \right)(w) \\ &= \frac{1}{|G|} \sum_{g \in G} w = w \end{aligned}$$

proving that S is, indeed, a projection.

<u>S is G-linear.</u> Fix $v \in V$ and $h \in G$. We have

$$\begin{aligned} S(\rho(h)(v)) &= \frac{1}{|G|} \sum_{g \in G} \left(\rho(g) \circ T \circ \rho(g)^{-1} \right)(\rho(h)(v)) \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\rho(g) \circ T \circ \rho\left(g^{-1}h\right) \right)(v) \end{aligned}$$

We now perform a change of variables. Observe that the map $g \mapsto h^{-1}g : G \to G$ is an automorphism. Hence, writing $g' = h^{-1}g$, we have

$$\begin{aligned} S(\rho(h)(v)) &= \frac{1}{|G|} \sum_{g' \in G} \left(\rho(hg') \circ T \circ \rho\left((g')^{-1} \right) \right)(v) \\ &= \rho(h) \left(\frac{1}{|G|} \sum_{g' \in G} \left(\rho(g') \circ T \circ \rho(g')^{-1} \right) \right)(v) \\ &= \rho(h)(S(v)) \end{aligned}$$

proving that S is, indeed, G-linear.

Therefore, by Corollary 1.2.12, $\ker(S)$ is a complementary subrepresentation of W. □

We also have the following important corollary.

Corollary 1.2.16. *Let G be a finite group, K a field such that $\text{char}(K) \nmid |G|$. Then, every representation of G over K is completely reducible.*

Proof. Let (V, ρ) be a representation of G over K. If (V, ρ) is irreducible, we are done;

else, it admits a nonzero, proper subrepresentation, which, by Maschke's Theorem, admits a complementary subrepresentation that is also proper and nonzero. If both of these are irreducible, then we are done; else, repeat this process. □

Remark. Nowhere in Definition 1.2.7 do we specify that the decomposition must be finite.

We note that both hypotheses of Maschke's Theorem—namely, that G is a finite group and that $\mathrm{char}(K) \nmid |G|$—are essential for Theorem 1.2.15 (and hence Corollary 1.2.16) to hold.

Non-Example 1.2.17 (Failure of Maschke's Theorem when $\mathrm{char}(K) \mid |G|$)**.** Let $G = \langle a \rangle$ be a cyclic group of prime order p. Let $V = \mathbb{F}_p^2$, and define $\rho : G \to \mathrm{GL}(2, \mathbb{F}_p)$ by

$$\rho(a^r) = \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \quad \text{for } 0 \leq r \leq p-1.$$

1. (V, ρ) is a representation of G over $\mathbb{F}_p$.
2. (V, ρ) is not irreducible.
3. (V, ρ) is not completely reducible.

It turns out that Maschke's Theorem also has a *converse.*

Theorem 1.2.18 (Converse of Maschke's Theorem)**.** *Let G be a finite group such that every finite-dimensional representation of G over some field K is completely reducible. Then,* $\mathrm{char}(K) \nmid |G|$.

Proof. Consider the regular representation $(K[G], \rho)$ of G over K, with basis $\mathcal{B} = \{e_g : g \in G\}$. The idea is to take advantage of the G-invariant properties of $\mathcal{B}$.

Consider the subspace

$$W := \left\{ \sum_{g \in G} \alpha_g e_g : \sum_{g \in G} \alpha_g = 0 \right\}$$

of dimension $\dim(V) - 1$. It turns out that W is G-invariant: for all $\sum_{g \in G} \alpha_g e_g \in W$ and

$h \in G$, we have

$$\rho(h)\left(\sum_{g\in G} \alpha_g e_g\right) = \sum_{g\in G} \alpha_g e_{hg} \in W$$

(where the sum of the coefficients α_g is still zero). Then, by assumption, $\exists U \leq V$ that is both G-invariant and complementary to W. This means that U must be of dimension 1, and is hence the span of a single vector $u \in U$.

We study the action of G on U. Fix $h \in G$, and write $u = \sum_{g\in G} \beta_g e_g$ for $\beta_g \in K$. Then,

$$\rho(h)(u) - u = \sum_{g\in G} \underbrace{\beta_g e_{hg} - \beta_g e_g}_{\in W}$$

meaning that $\rho(h)(u) - u \in W$. But, $\rho(h)(u) - u \in U$ as well. Since $U \cap W = \{0\}$, this means that $\rho(h)(u) = u$ for all $h \in G$. Hence, the action of G on U is *trivial.* Therefore, for all $x \in G$,

$$\sum_{g\in G} \beta_g e_{hg} = \sum_{g\in G} \beta_g e_g$$

Comparing coefficients, we conclude that $\beta_{h^{-1}g} = \beta_g$ for all $h, g \in G$. Letting $h = g$, we get, in particular, that $\forall g \in G$, $\beta_g = \beta_1$. Therefore, $u = \beta_1 \sum_{g\in G} e_g$. This, in particular, implies that $u' := \sum_{g\in G} e_g \notin W$, because otherwise, $u = \beta_1 u'$ would also lie in W, which it does not. Therefore, the sum of the coordinates of u' with respect to $\mathcal{B}$ cannot be zero. But, this sum is nothing but the cardinality of G (or rather, its image in the canonical map $\mathbb{Z} \to K$). Since this is nonzero, it must be that $\mathrm{char}(K) \nmid |G|$, as required. □

Combining Theorems 1.2.15 and 1.2.18, we conclude that $\mathrm{char}(K) \mid |G|$ if and only if every subrepresentation of G over K admits a complementary subrepresentation.

1.2.4 The G-Invariant Inner-Product

It turns out that we also have a notion of inner-products being compatible with representation strutures.

Definition 1.2.19 (G-Invariant Inner-Product)**.** Let G be a group and let (V, ρ) be a representation of G over $\mathbb{C}$ such that V admits an inner-product $\langle \cdot, \cdot \rangle$.We say that $\langle \cdot, \cdot \rangle$ is G-invariant if $\forall g \in G$ and $\forall x, y \in V$,

$$\langle x, y \rangle = \langle \rho(g)(x), \rho(g)(y) \rangle$$

Equivalently, $\langle \cdot, \cdot \rangle$ is G-invariant if $\mathrm{im}(\rho) \subseteq \mathrm{U}(V)$, ie, if, for every $g \in G$, $\rho(g)$ is a *unitary* $\mathbb{C}$-linear map from V to V.

Intrinsic to the notion of an inner-product is that of orthogonality. In the following proposition, we understand the significance of G-invariance in the context of subrepresentations.

Proposition 1.2.20. *Let G be a group and let (V, ρ) be a representation of G over $\mathbb{C}$ of finite dimension. Let $\langle \cdot, \cdot \rangle$ be a G-invariant inner-product on V. Then, the orthogonal complement of any G-invariant subspace of V is also G-invariant.*

Proof. Let $W \leq V$ be G-invariant, and denote by $W^{\perp}$ its orthogonal complement. Fix $g \in G$ and $w \in W^{\perp}$. To show that $\rho(g)(w) \in W^{\perp}$, we show it is orthogonal to every $v \in W$ with respect to $\langle \cdot, \cdot \rangle$.

Fix $v \in W$. Then, since $\langle \cdot, \cdot \rangle$ is G-invariant,

$$\begin{aligned} \langle v, \rho(g)(w) \rangle &= \left\langle \rho\left(g^{-1}\right)(v)\,, \rho\left(g^{-1}g\right)(w) \right\rangle \\ &= \left\langle \rho\left(g^{-1}\right)(v)\,, w \right\rangle \end{aligned}$$

Since W is G-invariant, $\rho(g^{-1})(v) \in W$, making it orthogonal to w, which lies in the orthogonal complement of W. Therefore, $\langle v, \rho(g)(w) \rangle = 0$, proving that $\rho(g)(w) \in W^{\perp}$ as required. $\square$

Corollary 1.2.21. *Let G be a group and let (V, ρ) be a representation of G over $\mathbb{C}$. If V is finite dimensional and admits a G-invariant inner-product, then V is completely reducible.*

Proof. If V is finite dimensional and admits a G-invariant inner-product, then by Proposition 1.2.20, for any $W \leq V$ G-invariant, $W^{\perp}$ is G-invariant as well. Since $W \oplus W^{\perp} = V$ and both W and $W^{\perp}$ are finite-dimensional, we can prove the result using similar reasoning to what we used to prove Corollary 1.2.16. □

1.3 Group Algebras and Modules

In this section, we study an important class of field algebras, namely, group algebras, and an important class of modules over said algebras, namely, group modules.

1.3.1 A Few Definitions

Definition 1.3.1 (Group Algebra)**.** Let G be a finite group and let K be a field. The group algebra KG is the K-algebra obtained by endowing the free vector space $K[G]$ generated by G (as a set) with the multiplication

$$\left(\sum_{g \in G} \alpha_g e_g\right) \cdot \left(\sum_{g \in G} \beta_g e_g\right) := \sum_{g \in G} \sum_{h \in G} \alpha_g \beta_h e_{gh}$$

Remark.

1. For ease of notation, we often denote elements e_g of the basis as simply g.
2. It is easy to verify that KG is, indeed, a K-algebra, with the multiplicative identity given by e_1 (where $1 \in G$ is the identity).
3. The map $g \mapsto e_g : G \to KG$ gives a trivial embedding of G in KG.

We have a similar notion of group modules.

Definition 1.3.2 (Group Module)**.** Let G be a group and let V be a vector space over a field K. We say that V is a KG-module if we can define a multiplication $g \cdot v$ for some $g \in G$ and $v \in V$ that satisfies the following conditions for all $u, v \in V$, $g, h \in G$ and $\lambda \in K$:

1. $g \cdot v \in V$
2. $(gh) \cdot v = g \cdot (h \cdot v)$
3. $1 \cdot v = v$
4. $g \cdot (\lambda v) = \lambda (g \cdot v)$

5. $g \cdot (u + v) = g \cdot u + g \cdot v$

Note that a KG-module is, indeed, a module over KG.

Proposition 1.3.3. *Let G be a group and let V be a vector space over a field K. If V is a KG-module with multiplication $\cdot$ (as per Definition 1.3.2), then for $v \in V$, the multiplication*

$$\left(\sum_{g \in G} \lambda_g e_g\right) \cdot v := \sum_{g \in G} \lambda_g (g \cdot v)$$

endows V with a module structure over $K[G]$.

Furthermore, it turns out that we can move from modules to representations and vice-versa quite easily.

Proposition 1.3.4. *Let G be a group and let V be a vector space over a field K.*

1. *If $\rho : G \to \mathrm{GL}(V)$ gives a representation of G, then V is a KG-module with multiplication given by $g \cdot v = \rho(g)(v)$ for all $g \in G$ and $v \in V$.*

2. *If V is a KG-module with multiplication $\cdot$, the map $\rho : G \to \mathrm{GL}(V)$ given by $\rho(g)(v) := g \cdot v$ is a representation.*

The proofs of the above propositions are trivial and merely involve manually checking several basic conditions. Hence, we omit them.

We now give a basic 'dictionary' of sorts to go back and forth between the language of group modules and that of representations:

KG-**Modules**	**Representations**
Simple	Irreducible
Semi-Simple	Completely Irreducible
Submodule	Subrepresentation
Viewing KG as a KG-Module	The Regular Representation
Isomorphism	Equivalence of Representations
Dimension (as a K-vector space)	Degree

We illustrate the above equivalence by stating Maschke's Theorem in the language of KG-Modules.

Lemma 1.3.5 (Maschke's Theorem, Module Version)**.** *Let G be a finite group, K a field whose characteristic does not divide the order of G. Then, any KG-Module V is semi-simple.*

1.3.2 Schur's Lemmas

In this subsection, we explore several versions of an important result by Schur.

Theorem 1.3.6 (Schur's Lemmas for Rings)**.** *Let A be a ring and let S, T be simple A-modules.*

1. *If S and T are non-isomorphic, then* $\mathrm{Hom}_A(S, T) = \{0\}$.
2. *If S and T are isomorphic, then* $\mathrm{Hom}_A(S, T)$ *is a division ring.*

Proof. We rely on the fact that for all $\phi \in \mathrm{Hom}_A(S, T)$, $\ker(\phi) \leq S$ and $\mathrm{im}(\phi) \leq T$.

1. Let S and T be non-isomorphic. Fix $\phi \in \mathrm{Hom}_A(S, T)$. Since S is simple, we must have that $\ker(\phi) \in \{\{0\}, S\}$. If $\ker(\phi) = \{0\}$, then $\mathrm{im}(\phi) = T$, meaning $S \cong T$, a contradiction.

2. Let $\phi \in \mathrm{Hom}_A(S, T) \setminus \{0\}$. Then, $\ker(\phi) \neq S$, meaning that $\ker(\phi) = \{0\}$. Then, $\mathrm{im}(\phi) = T$, making ϕ an isomorphism. In particular, this means that ϕ admits an inverse, making $\mathrm{Hom}_A(S, T)$ a division ring.

□

Theorem 1.3.7 (Schur's Lemmas for Algebras)**.** *Let K be an algebraically closed field and A a K-algebra. Let S and T be simple A-modules.*

1. *If $S \ncong T$, then* $\mathrm{Hom}_A(S, T) = \{0\}$.
2. *If $S \cong T$, then $K \cong \mathrm{Hom}_A(S, T)$ via the map $\alpha \mapsto \alpha \cdot \mathrm{id}$.*

Proof.

1. As before.

2. We do not distinguish S and T in this proof.

Fix $\phi \in \mathrm{Hom}_A(S, S)$. Then, ϕ can be viewed as an element of $\mathbf{M}_n(K)$, where $n = \dim(S)$. Since K is algebraically closed, ϕ admits an eigenvalue $\lambda \in K$. Now, consider the map $\phi - \lambda\,\mathrm{id} \in \mathrm{Hom}_A(S, S)$. Clearly, $\ker(\phi - \lambda\,\mathrm{id}) \neq \{0\}$, since it contains all eigenvectors with eigenvalue λ. Since S is simple, it must be that $\ker(\phi - \lambda\,\mathrm{id}) = S$, meaning $\phi - \lambda\,\mathrm{id} = 0$. In other words, $\phi = \lambda\,\mathrm{id}$.

$\square$

Theorem 1.3.8 (Schur's Lemmas for Finite Groups, over $\mathbb{C}$)**.** *Let G be a finite group and let S and T be simple $\mathbb{C}G$ modules that are finite-dimensional (as vector spaces) over K, with associated representations $\rho_S : G \to \mathrm{GL}(S)$ and $\rho_T : G \to \mathrm{GL}(T)$.*

1. *If $S \ncong T$, then for all $\mathbb{C}$-linear maps $f : S \to T$, the map*
$$\hat{f} := \frac{1}{|G|} \sum_{g \in G} \rho_T(g) \circ f \circ \rho_S\left(g^{-1}\right)$$
is identically zero.
2. *If $S \cong T$, then for all $\mathbb{C}$-linear maps $f : S \to T$, we have*
$$\begin{aligned} \hat{f} &:= \frac{1}{|G|} \sum_{g \in G} \rho_T(g) \circ f \circ \rho_S\left(g^{-1}\right) \\ &= \frac{1}{\dim(S)} \mathrm{Tr}(f) \cdot \mathrm{id}_S \end{aligned}$$

Proof. Let $f : S \to T$ be $\mathbb{C}$-linear. We show that $\hat{f} \in \mathrm{Hom}_{\mathbb{C}G}(S, T)$: for all $h \in G$,

$$\begin{aligned} \rho_T(h) \circ \hat{f} &= \rho_T(h) \left(\frac{1}{|G|} \sum_{g \in G} \rho_T(g) \circ f \circ \rho_S\left(g^{-1}\right) \right) \\ &= \frac{1}{|G|} \sum_{g \in G} \rho_T(hg) \circ f \circ \rho_S\left(g^{-1}\right) \circ \rho_S\left(h^{-1}\right) \circ \rho_S(h) \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\rho_T(hg) \circ f \circ \rho_S\left(g^{-1}h^{-1}\right)\right) \circ \circ \rho_S(h) \\ &= \hat{f} \circ \rho_S(h) \end{aligned}$$

proving that $\hat{f}$ is, indeed, a homomorphism of $\mathbb{C}G$-modules.

$\square$