1   Representations

1.1   Introduction

The lecturer is Roman Bezrukavnikov. These notes are taken by **Sanjana Das** and **Jakin Ng**, and the note-taking is supervised by Ashay Athalye. Here is some basic information about the class:

- The text used in this class will be the 2nd edition of **Algebra**, by Artin.

- The course website is found on **Canvas**, and the problem sets will be submitted on **Gradescope**.

- The problem sets will be due Wednesday at 11:59PM.

During this class, we will cover three main topics.

1. Representation theory: In 18.701, we studied group actions, which let us think of groups as a set of symmetries of the set being acted on. Here we'll study how groups can act by symmetry on a *vector space* — this combines the fundamental concepts of of symmetry and linearity.

2. Ring theory: We'll learn to add *and* multiply in abstract settings.

3. Galois theory: We'll study the symmetries of solutions to polynomial equations. For example, a quadratic equation $ax^2 + bx + c = 0$ has two solutions,

$$x_\pm = \frac{-b \pm \sqrt{b^2 - 4ac}}{2}.$$

There's an ambiguity in the sign of the square root, and this gives a symmetry between the two roots (by swapping the sign). For higher-degree polynomial equations, we'll see that symmetries (such as changing $+$ to $-$ in the above formula) control the existence of formulas such as the quadratic formula, and the shape of such formulas when they do exist.

1.2   What is a Representation?

In representation theory, we think of a group as the symmetries of a *vector space* — this perspective lets us study the group using tools from linear algebra.

> **Guiding Question**
> How can we represent elements of groups as symmetries or linear operations on vector spaces?

The following definition formalizes this idea, by representing elements of groups as *matrices*:

> **Definition 1.1**
> Let G be a group. A **complex, n-dimensional matrix representation** of G is a homomorphism
> $$R : G \to \mathrm{GL}_n(\mathbb{C})^a.$$
> ─────────────
> [a]Recall that $\mathrm{GL}_n(\mathbb{C})$ denotes the group of invertible $n \times n$ matrices with entries in $\mathbb{C}$.

Similarly, a real representation is a homomorphism

$$R : G \to \mathrm{GL}_n(\mathbb{R}).$$

Representations can be defined over any field (for instance, we could even define representations over the finite field $\mathbb{F}_p$), but in this class, we will mostly work with only *complex* representations of *finite* groups.

Earlier, we mentioned that in representation theory, we want to think of elements of a group as symmetries of a vector space. To see why the above definition achieves this, note that invertible matrices play a special role for the vector space $\mathbb{C}^n$: they act on the column vectors. More explicitly, any matrix $A \in \mathrm{Mat}_{n \times n}(\mathbb{C})$ defines a linear transformation from $\mathbb{C}^n$ to itself, by taking $v \mapsto Av$. Moreover, $\mathrm{GL}_n(\mathbb{C})$ consists of invertible $n \times n$ matrices, which are exactly the matrices for which $v \mapsto Av$ is a *bijective* linear transformation. So $\mathrm{GL}_n(\mathbb{C})$ equivalent to a group of linear automorphisms[*] on $\mathbb{C}^n$, which can be thought of as the symmetries of the vector space.

─────────────
[*]Isomorphisms from $\mathbb{C}^n$ to itself

This means that writing down a homomorphism $R : G \to \mathrm{GL}_n(\mathbb{C})$ is equivalent to writing down a *linear group action* of G on $\mathbb{C}^n$, where each $g \in G$ acts by taking $v \mapsto R_g(v)$. More explicitly, to write down a representation R by thinking in terms of group actions, for each $g \in G$ we need to define an operator R_g on $\mathbb{C}^n$ such that it is:

- **Group Action.** The map

$$G \times V \to V$$
$$(g, v) \mapsto R_g(v)$$

satisfies the axioms of a group action of G on V:

1. Since R is a homomorphism, $R_{gh} = R_g R_h$, so $R_{gh}(v) = R_g(R_h(v))$ for all $g, h \in G$ and $v \in V$.

2. Again, because R is a homomorphism, $R_{1_G} = \mathrm{Id}$, and so $R_{1_G}(v) = v$ for all $v \in V$.

- **Linear.** For each $g \in G$, the map $v \mapsto R_g(v)$ is linear. We have

$$R_g(v + w) = R_g(v) + R_g(w)$$

and

$$R_g(\lambda v) = \lambda R_g(v)$$

for all $v, w \in V$ and $\lambda \in \mathbb{C}$. From definition 1.1, these properties correspond to the fact that elements of $\mathrm{GL}_n(\mathbb{C})$ are linear operators on $\mathbb{C}^n$.

> **Note 1.2**
> It is a notational convention to write R_g instead of $R(g)$. Using the notation of group actions, $R_g(v)$ can also be written as gv for a vector $v \in \mathbb{C}^n$.

1.3 Examples of Representations

The simplest example of a representation is the *trivial representation*.

> **Example 1.3** (Trivial Representation)
> The **trivial representation** of any group G is the one-dimensional representation where $R_g = 1$ for all g. That is, every element of the group maps to the 1×1 identity matrix $\begin{bmatrix} 1 \end{bmatrix} \in \mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$.

The trivial representation is clearly a homomorphism[†], and therefore a valid representation. Every group has a trivial representation, and it will turn out to be a "building block" for more complicated representations.

The symmetric group S_n has another one-dimensional representation:

> **Example 1.4** (Sign Representation)
> A symmetric group S_n has a one-dimensional representation, called the **sign representation**, where
>
> $$R_\sigma = \mathrm{sgn}(\sigma)^a = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$
>
> Again, the target space is $\mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$.
>
> ---
> [a]Recall that every $\sigma \in S_n$ can be written as a product of transpositions $\tau_1 \tau_2 \cdots \tau_k$; the parity of σ is the parity of k, and $\mathrm{sgn}(\sigma) = (-1)^k$.

As an example of a representation that is not one-dimensional, S_n also has another representation with dimension n, the permutation representation.

[†]Try writing a short proof of this!

Example 1.5 (Permutation Representation)

The group S_n has a n-dimensional representation, called the **permutation representation**, which takes each element $\sigma \in S_n$ to its corresponding permutation matrix — the $n \times n$ matrix which sends the ith basis vector $\vec{e}_i$ to the $\sigma(i)$th basis vector $\vec{e}_{\sigma(i)}$, meaning that its ith column is $\vec{e}_{\sigma(i)}$. As an example, when $n = 3$,

$$R_{(123)} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

A representation is called **faithful** if it is injective, in which case G is isomorphic to its image under the representation. The permutation representation is faithful, while the trivial and sign representations are not faithful (except for very small $n^{\ddagger}$).

A familiar example of a representation is $\mathbb{Z}/m\mathbb{Z}^{\S}$ acting as a group of rotational symmetries.

Example 1.6

The group $\mathbb{Z}/m\mathbb{Z}$ corresponds to the rotational symmetries of a regular m-gon. By placing the polygon in the two-dimensional plane and using the standard basis for the plane, we get a two-dimensional representation of $\mathbb{Z}/m\mathbb{Z}$ where every element $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ is mapped to the corresponding rotation matrix: more explicitly, the representation is

$$\bar{a} \mapsto \begin{bmatrix} \cos 2\pi a/m & -\sin 2\pi a/m \\ \sin 2\pi a/m & \cos 2\pi a/m \end{bmatrix}.$$

This can be thought of either as a real representation, where the target space is $GL_2(\mathbb{R})$ or a complex one, where the codomain is $GL_2(\mathbb{C})$.

When describing a representation of a given group G, it may be somewhat time-consuming to list the images of *all* elements of G. But it's possible to describe a representation much more efficiently — if G is given by generators and relations, then to define a matrix representation R, it's enough to specify the images of the generators and check that they satisfy the relations. More explicitly, suppose

$$G = \langle x_1, \dots, x_k \mid r_1, \dots, r_m \rangle,$$

where the x_i are the generators, and the r_i are the relations. It is enough to specify

$$R_{x_1}, R_{x_2}, \cdots R_{x_k}$$

in order to define a unique representation. It's clear that $R_{x_1}, \dots, R_{x_k}$ must satisfy the same relations as $x_1, \dots, x_k$. Conversely, given any n matrices $\gamma_1, \dots, \gamma_k$ in $\mathrm{GL}_n(\mathbb{C})$ which satisfy these relations, we can set $R_{x_i} = \gamma_i$ for all i; then this determines the entire representation, since we can obtain R_g for *any* $g \in G$ simply by multiplying the γ_i in the same way that we would multiply the x_i to obtain g (since R is a homomorphism). The γ_i may also satisfy additional relations other than the $r_{j=1,\cdots m}$; if they do not, the representation will be faithful.

Example 1.7

The group $\mathbb{Z}/m\mathbb{Z}$ can be written as $\langle x \mid x^m = 1 \rangle$ (this denotes that it's generated by one element x, with the relation $x^m = 1$). So to define the above two-dimensional representation in Example 1.6, it's enough to specify that

$$\bar{1} \mapsto A = \begin{bmatrix} \cos 2\pi/m & -\sin 2\pi/m \\ \sin 2\pi/m & \cos 2\pi/m \end{bmatrix},$$

and to verify that $A^m = 1$.

Another familiar example is the following representation of the dihedral group, which is the group of *all* symmetries of a regular m-gon (meaning rotations and reflections).

---

‡For $n = 1$, the trivial representation is faithful, since there is only one element, and for $n = 1, 2$, the sign representation is faithful

§The group of integers mod m; we'll use $\bar{a}$ to denote the residue of a mod m

> **Example 1.8**
> We can write the dihedral group as $D_m = \langle r, s \mid r^m = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$. Then D_m has a two-dimensional representation given by
> $$r \mapsto \begin{bmatrix} \cos 2\pi/m & -\sin 2\pi/m \\ \sin 2\pi/m & \cos 2\pi/m \end{bmatrix},$$
> $$s \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$
> since it can be verified that the images of r and s satisfy the same relations. Intuitively, this construction is quite similar to the representation of $\mathbb{Z}/m\mathbb{Z}$ in Example 1.6 — we can think of r as a rotation by $2\pi/m$ and s as a reflection, since these are the symmetries of the m-gon. Then to obtain this representation, we simply place the m-gon on the plane, and take the matrices corresponding to these transformations of the plane.

1.4 Linear Representations

Unfortunately, the current formulation of a representation requires a basis, as it is not possible to write down a matrix without choosing a basis. We are interested in the *story* of a journey, and not the particular *coordinates* of the journey.

> **Guiding Question**
> How can we think about representations in a coordinate-free way, without specifying a basis?

Given a matrix representation, a new **conjugate representation** can be obtained by choosing a different basis of $\mathbb{C}^n$ and rewriting the original matrices in the new basis.
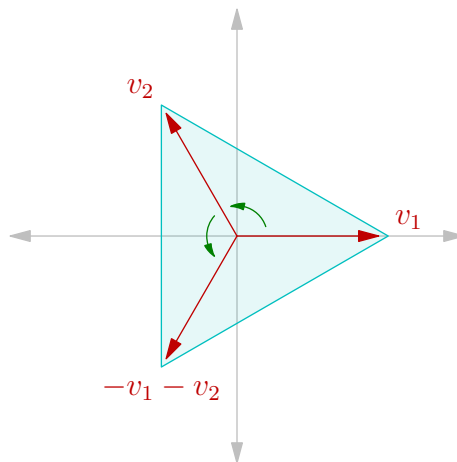
> **Example 1.9**
> The representation of $\mathbb{Z}/3\mathbb{Z}$ described in Example 1.6 (as the rotations of a triangle) can be written in the standard basis as
> $$\bar{1} \mapsto \begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{bmatrix}.$$
> But if we instead take the basis consisting of $v_1 = (1,0)^t$ and $v_2 = (-1/2, \sqrt{3}/2)^t$, then this representation can be written as
> $$\bar{1} \mapsto \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

Clearly, the new representation is in fact technically a different matrix representation, but conceptually, it can be interpreted in the same way — it still describes the rotations of a triangle.

In general, suppose we have two bases of $\mathrm{GL}_n(\mathbb{C})$ with change of basis matrix P — in Example 1.9, the change

of basis matrix was

$$P = \begin{bmatrix} 1 & -1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix}.$$

Then if we have a representation R with matrices written in the first basis, the conjugate representation obtained by writing R in the new basis is given by

$$R'_g = P^{-1} R_g P,$$

by simply applying the change of basis formula to each matrix.

Conjugate representations are essentially the same story, just presented in different coordinates, so we generally consider conjugate matrix representations as the same — we want to study the conjugacy classes of matrix representations, rather than the basis-dependent matrix representations themselves. In fact, we can eliminate the need for matrices altogether by using the concept of a *linear representation*, which does not require specifying a basis.

Definition 1.10

For a vector space V, let $\mathrm{GL}(V)$ be the group of linear automorphisms of V. A **linear representation** of V is a homomorphism

$$\rho : G \to \mathrm{GL}(V).$$

Note that a linear representation doesn't depend on coordinates or column vectors! In a matrix representation, we thought of group elements as acting on a vector space (specifically $\mathbb{C}^n$) by linear automorphisms, and we wrote down these automorphisms in a given basis by using matrices. But here instead of writing down the matrices corresponding to the linear automorphisms, we work with the automorphisms themselves.

We *can* turn a linear representation into a matrix representation — if we fix a basis of V, then we get an isomorphism between $\mathrm{GL}_n(\mathbb{C})$ and $\mathrm{GL}(V)$ (where $n = \dim V$), and for each linear automorphism ρ_g, we can write down the matrix corresponding to ρ_g in that basis. Choosing a different basis of V would give us a conjugate representation; thus specifying a linear representation provides a conjugacy class of matrix representations. Choosing a suitable basis and working with matrix representations can be helpful in computations, but we generally want to work with properties that are basis-independent and thus well-defined for linear representations.

As in our definition of conjugate *matrix* representations, we still need a way of describing when two *linear* representations are essentially the same:

Definition 1.11

Two linear representations $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(W)$ are **isomorphic** if there exists a linear isomorphism $I : V \to W$ such that $I(\rho_g(v)) = \rho'_g(I(v))$ for all $g \in G$ and $v \in V$ — in other words, an isomorphism between vector spaces that is also compatible with the action of G.

Note that given two finite-dimensional vector spaces V and W, there exists an isomorphism between V and W if and only if they have the same dimension. However, we can't just pick *any* isomorphism — our isomorphism should also be compatible with the action of G. (Definition 1.11 essentially states that we should be able to relabel the elements of W as elements of V without changing the vector space structure or the way G acts on the space.) Linear representations up to isomorphism correspond precisely to matrix representations up to conjugacy.

As mentioned earlier, we want to study properties of a representation which don't depend on the basis. For a matrix, operations such as the trace or the determinant are invariant under conjugation, and thus are basis-independent. This motivates the following definition.

Definition 1.12 (Character)

The **character** of a representation R is the function χ_R on G defined as $\chi_R(g) = \mathrm{Tr}(R_g)$.

It might be surprising that we use the trace in this definition, rather than the determinant or some other basis-independent property. However, the trace will turn out to be the right choice, as it is extremely useful. In particular, by the end of next week, it will be shown that for a finite group G, the character completely determines the isomorphism class of the representation!

MIT OpenCourseWare
https://ocw.mit.edu

Resource: Algebra II Student Notes
Spring 2022
Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng

For information about citing these materials or our Terms of Use, visit: https://ocw.mit.edu/terms.