(Representation Theory) Notes on Groups & Linear Algebra

George McNinch

2024-01-17

In the first lecture, we discussed some examples of groups and some basics of linear algebra.

Groups

- the elements of the *cylic group* $\mathbb{Z}/n\mathbb{Z}$ are the equivalence classes of integers under the relation "$\equiv \pmod{n}$"

  this group is *additive*

- we observed that the mapping $\phi : \mathbb{R} \to \mathbf{S}^1$ given by $\phi(t) = e^{2\pi it}$ is a *group homomorphism* since $\phi(t+s) = \phi(t)\phi(s)$ for all $t, s \in \mathbb{R}$.

  we observed that ker $\phi = \mathbb{Z}$, and that - by the **First Isomorphism Theorem** - ϕ induces an isomorphism
  $$\overline{\phi} : \mathbb{R}/\mathbb{Z} \to \mathbf{S}^1.$$

- for a non-zero natural number the symmetric group S_n is the collection of all bijections $I_n \to I_n$ where $I_n = \{1, 2, \cdots, n\}$.

  We may sometimes use *cycle notation* for elements of S_n.

  The subgroup
  $$H = \langle (1234), (14)(23) \rangle$$
  has order 8 and is sometimes called the *dihedral group* D_4 or D_8 – it has order 8.

- Let F be a field.

  Recall that typically examples are: $F = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z}$ for a prime number p.

  The set
  $$\mathrm{GL}_n(F) = \{\text{all invertible } n \times n \text{ matrices with entries in } F\}$$
  forms a group under matrix multiplication.

  The determinant function yields a group homomorphism
  $$\det : \mathrm{GL}_n(F) \to F^\times$$
  (here $F^\times$ means $F \quad \{0\}$, which is a commutative group under multiplication in the field F).

Linear Algebra

Let F be a field. An F-vector space V is an additive abelian group together with an operation of *scalar multiplication* – this amounts to a function
$$F \times V \to V$$
– satisfying certain axioms.

If V, W are F-vector spaces, a linear mapping $T : V \to W$ is a function which satisfies
$$T(\alpha v + w) = \alpha T(v) + T(w).$$

Let's suppose that V is *finite dimensional* and that $\phi : V \to V$.

We write $\phi^2 = \phi \circ \phi$ and more generally $\phi^n = \phi \circ \phi^{n-1}$.

trace, det, char poly

The *trace* of a matrix $M = [M_{ij}]$ is the sum of the diagonal entries:

$$\text{tr}(M) = \sum_{i=1}^{n} M_{ii}.$$

I'm assuming you recall the definition of the *determinant* det M.

The characteristic polynomial $\text{cp}_M(X) \in F[X]$ of M is defined to be

$$\text{cp}_M(X) = \det(M - X \cdot \mathbf{I}_n).$$

For a linear transformation ϕ we define

- $\text{tr}(\phi) = \text{tr}([\phi]_{\mathcal{B}})$
- $\det(\phi) = \det([\phi]_{\mathcal{B}})$
- $\text{cp}_\phi(X) = \text{cp}_{[\phi]_{\mathcal{B}}}(X)$

Proposition $\text{tr}(\phi)$, $\det(\phi)$, and $\text{p}_\phi(X)$ are independent of the choice $\mathcal{B}$ of basis for V.

The main point here is that if $\mathcal{B}$ and $\mathcal{B}'$ are two basis for V, there is an invertible matrix ("change of basis matrix") P for which

$$[\phi]_{\mathcal{B}} = P[\phi]_{\mathcal{B}'}P^{-1}.$$

Evaluation of polynomials at linear transformations

Suppose that $f = f(X) \in F[X]$ is a polynomial; thus

$$f = \sum_{i=0}^{N} a_i X^i$$

for some coefficients $a_i \in F$.

We may *evaluate* the polynomial f at the linear endmorphism ϕ:

$$f(\phi) = \sum_{i=0}^{N} a_i \phi^i.$$

Proposition Let $\phi : V \to V$ be a linear transformation, and let

$$I = \{f \in F[X] \mid f(\phi) = 0\}.$$

Then I is an *ideal* in the polynomial ring $F[X]$. In particular, there is a unique monic polynomial $m_\phi(X) \in F[x]$ for which $I = m_\phi(X)F[X]$.

In particular, if $f \in F[X]$ and $f(\phi) = 0$, then $m_\phi | f$.

Theorem (Cayley-Hamilton) Let $\phi : V \to V$ be a linear transformation, and let $\text{cp}(X) = \text{cp}_\phi(X) \in F[X]$ be the characteristic polynomial.

Then $\text{cp}(\phi) = 0$.

Recall that the *eigenvalues* of ϕ are precisely the roots of the characteristic polynomial. The Cayley-Hamilton Theorem implies that any root of the minimal polynomial is an eigenvalue. In fact, we have the converse as well:

Proposition: If $\lambda \in F$ is an eigenvalue of ϕ – i.e. a root of the characteristic polynomial – then λ is a root of the minimal polynomial.

Theorem: ϕ is *diagonalizable* – i.e. V has a basis of eigenvectors for ϕ – if and only the minimal polynomial has no multiple roots.

Remark: This theorem should be proved in Math215-216 here at Tufts using the *Fundamental Theorem for modules over a PID*. We don't need the full force of this result in our class.

Example

Suppose that $\phi : V \to V$ satisfies $\phi^N = \mathrm{id}_V$ for some positive natural number N.

We suppose that F is *algebraically closed* and of *characteristic zero*.

Notice that the polynomial $f(X) = X^N - 1 \in F[X]$ has distinct roots.

(If $F = \mathbb{C}$, these roots are exactly

$$\{\exp(2\pi k i/n) \mid 0 \leq k < N\}.$$

)

Since the minimal polynomial of ϕ divides f, we see that the minimal polynomial has distinct roots and hence ϕ is diagonalizable by the **Theorem** quoted above.

Bibliography