MATH 301 · FALL 2026

Problem Set 5: Linear Representations

DUE Friday, October 2nd by 11:59pm

The geometrician teaches me how to work out the size of my estates—rather than how to work out how much a man needs in order to have enough. What use is it to me to be able to divide a piece of land into equal areas if I'm unable to divide it with a brother? The geometrician teaches me how I may avoid losing any fraction of my estates, but what I really want to learn is how to lose the lot and still keep smiling.

From *Letters from a Stoic* by Seneca

Solutions must be typeset in LaTeX and written in complete, grammatical sentences. **You must list all your collaborators explicitly**. Feel free to DM on Discord if you have any questions. Problems marked (Challenge) are optional but encouraged.

Up to this point we have studied permutation representations of a group G. A simple summary is that we have studied and classified all the homomorphisms from a (finite) group G into symmetric groups. Next we begin studying *linear representations*, which may be similarly summarized as the study of homomorphisms from G into general linear groups $\mathrm{GL}_n(K)$ for some field K. First we need to review some linear algebra.

5.1 · Modules

Linear algebra is fundamentally the theory of systems of linear equations. It is likely that your first exposure to linear algebra was fairly concrete and practical, before you learned how to write proofs or to think about abstract structures. Now that you're all grown up, we can revisit linear algebra through the lens of modern algebra. From this perspective, linear algebra is the study of *vector spaces* and the *linear maps* between them.

PROBLEM 5.1

Let V be an additive abelian group. An **endomorphism** of V is a homomorphism $f : V \to V$. Let $\mathrm{End}(V)$ be the set of all endomorphisms of V.

1. If $f, g \in \mathrm{End}(V)$, prove that $f + g$ defined by $(f + g)(v) := f(v) + g(v)$ also belongs to $\mathrm{End}(V)$.
2. If $f, g \in \mathrm{End}(V)$ we write fg as a shorthand for the composition $f \circ g$. We also tend to write fv as a shorthand for $f(v)$ when $v \in V$. Since the composition of homomorphisms is a homomorphism, $fg \in \mathrm{End}(V)$. Note that generally $fg \neq gf$ since function composition is typically not commutative. Prove that if $f, g, h \in \mathrm{End}(V)$, then $f(g + h) = fg + fh$.

In fact, $\mathrm{End}(V)$ is a non-commutative ring with the addition operation as defined above and multiplication given by composition. The additive identity 0 is the constant zero function $0v = 0$ for all v. The multiplicative identity 1 is given by the identity function $1v = v$ for all $v \in V$. We call $\mathrm{End}(V)$ the **endomorphism ring** of V.

DEFINITION 5.1
Let R be a (possibly noncommutative) ring. An R**-module** is an additive abelian group V together with a homomorphism $\varphi : R \to \mathrm{End}(V)$.

Now suppose that (V, φ) is an R-module. If $a \in R$, then we write $\varphi_a \in \mathrm{End}(V)$ for the endomorphism of V associated to a. This succinct definition packs a lot of information. For example, if $a, b \in R$ and $v \in V$ we have

$$\varphi_{a+b}v = (\varphi_a + \varphi_b)v = \varphi_a v + \varphi_b v. \tag{5.1.1}$$

The first equality follows from the additivity of φ, the second equality is the definition of addition in $\mathrm{End}(V)$. Notice that this is sort of like saying v distributes over the sum $a + b$ on the right.

On the other hand, if $a \in R$ and $v, w \in V$, then we also have a distributive-like property

$$\varphi_a(v + w) = \varphi_a v + \varphi_a w, \tag{5.1.2}$$

but here this just follows from φ_a being an endomorphism of V.

We can think of an R-module as a **representation** of a ring R: it is an abelian group on which R acts. The extra operations in a ring mean that the simplest kinds of objects on which it makes sense for them to act on/be represented by are abelian groups.

Just like with group actions, the homomorphism $\varphi : R \to \mathrm{End}(V)$ is often understood in context and suppressed. This leads to the following elegant notation. Given $a \in R$ and $v \in V$ we write

$$av := \varphi_a v.$$

That is, we think of the elements of V as vectors and elements of R as scalars; the action of the endomorphism φ_a on v is then simply scalar multiplication of v by a. For example, in this notation (5.1.1) becomes simply

$$(a + b)v = av + bv,$$

and (5.1.2) becomes

$$a(v + w) = av + aw.$$

Another example is the calculation

$$\varphi_{ab}v = (\varphi_a \varphi_b)v = \varphi_a(\varphi_b v),$$

which uses the multiplicativity of φ for the first identity and the definition of multiplication in $\mathrm{End}(V)$ as composition of functions for the second identity. This becomes simply an associative-like identity,

$$(ab)v = a(bv).$$

Hence the way we usually think about R-modules is that they are abelian groups V which have a notion of scalar multiplication by the ring R.

Just as we can learn a lot about a group G by studying its representations, we can learn a lot about a ring R by studying its R-modules. **Commutative algebra** is essentially the branch of mathematics devoted to the study of R-modules when R is a commutative ring.

You have already studied some important classes of R-modules, though probably not expressed in that language. For example, if V is any additive abelian group and $n \in \mathbb{Z}$, then there is already a default way to interpret nv for any vector $v \in V$: if n is positive, then nv is the same as adding v to itself n-times; if n is negative, nv is the sum of the inverse $-v$ to itself $|n|$ times. In other words, any abelian group may be viewed as a $\mathbb{Z}$-module in exactly one way. [1] Thus *abelian groups are the same thing as $\mathbb{Z}$-modules*.

Here is the other essential example:

DEFINITION 5.2
Let K be a field. Then a **K-vector space** is a K-module V.

Indeed, a K-vector space is an additive abelian group V for which we can scale the vectors $v \in V$ by elements of K. When you took linear algebra, you may have only studied vector spaces over $\mathbb{R}$ or maybe over $\mathbb{C}$, but the definition and the basic theory works verbatim if we replace those with any arbitrary field K.

Vector spaces tend to feel more familiar than modules, and so it is common to think of modules as *vector spaces which allow scaling by a ring instead of a field*. However, vector spaces are the simplest kind of module; modules over rings that are not fields can be much more complicated than the kinds of vector spaces you may be familiar with.

PROBLEM 5.2

Let R be a ring and suppose that V and W are R-modules. Let $\varphi : R \to \mathrm{End}(V)$ and $\psi : R \to \mathrm{End}(W)$ be the explicit scalar multiplication maps. The "right kind of maps" between R-modules are called **R-linear maps**. How should we define R-linear maps? How should we define isomorphism of R-modules? Use your experience from linear algebra and our study of G-sets to guide you.

Later in the course we will return to study more kinds of modules–including for a special class of noncommutative rings–but for now we turn our focus to vector spaces.

5.2 · Vector spaces

Let's recall some important definitions.

[1] Another way to say this is that for any ring R there is a unique homomorphism $\varphi : \mathbb{Z} \to R$. Hence in particular this holds for $R = \mathrm{End}(V)$. This is called the **initial property** of $\mathbb{Z}$.

DEFINITION 5.3

Let K be a field and let V be a K-vector space.

- We say vectors $v_1, v_2, \ldots, v_n \in V$ are **linearly dependent** if there are $c_1, c_2, \ldots, c_n \in K$, not all zero, such that
$$c_1 v_1 + c_2 v_2 + \ldots + c_n v_n = 0.$$
Otherwise we say the v_i are **linearly independent**.
- We say $v_1, v_2, \ldots, v_n$ **span** V if every vector $v \in V$ may be expressed as
$$v = c_1 v_1 + c_2 v_2 + \ldots + c_n v_n$$
for some $c_i \in K$.
- We say V is **finitely generated** if it is spanned by finitely many vectors.
- We say $v_1, v_2, \ldots, v_n$ a **basis** if the vectors v_i are linearly independent and span V.

The following could be called the Fundamental Theorem of Linear Algebra.

THEOREM 5.4

Every finitely generated K-vector space V has a basis and any two bases contain the same number of vectors. The **dimension** of V is the number of vectors in a basis of V.

So, up to K-linear isomorphism, there is only one vector space of each dimension. A simple model for the K-vector space of dimension n is K^n, n-tuples of elements of K. Other examples of K-vector spaces show up in nature, but they will all be isomorphic to some K^n.

PROBLEM 5.3

This problem is optional practice with bases and dimension; skip it if you feel comfortable with these ideas. Let $n \geq 1$ and let $P_n(K)$ be the set of all polynomials in $K[x]$ with degree at most $n-1$.

1. Observe that $P_n(K)$ forms a K-vector space with respect to addition of polynomials and the natural scaling action of K (think it through!) Prove that $P_n(K)$ has dimension n and find a K-linear isomorphism $P_n(K) \cong K^n$.
2. The vector space $P_n(K)$ has a fairly natural basis (which I will guess you found in the previous part). However there are other convenient bases for this space. Suppose $a := \{a_1, a_2, \ldots, a_n\} \subseteq K$ is a set of n distinct elements. Show that for each i there is a unique polynomial $f_i(x) \in P_n(K)$ such that
$$f_i(a_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$
3. Prove that for any $(b_1, b_2, \ldots, b_n) \in K^n$, there exists a unique $f(x) \in P_n(K)$ such that $f(a_i) = b_i$. This result is known as **Lagrange's Interpolation Theorem**.

5.3 · Matrices

Linear maps $\varphi : K^n \to K^m$ may be succinctly expressed as a matrix. Recall the **standard basis** of K^n consisting of the vectors $e_1, e_2, \ldots, e_n$ where every entry of e_i is 0 except the ith entry which is 1. A linear map $\varphi : K^n \to K^m$ is completely determined by where it sends a basis, hence by the values

$$v_j := \varphi e_j = \sum_{i=1}^{m} a_{ij} e_i.$$

We may neatly package all this data into a matrix $[\varphi] := (a_{ij})$ where $a_{ij} \in K$, $1 \le i \le m$, and $1 \le j \le n$. Composition of linear maps is given by the operation of matrix multiplication: If $\psi : K^r \to K^n$ has matrix $[\psi] = (b_{jk})$, then $\varphi\psi : K^r \to K^m$ is K-linear and $[\varphi\psi] = [\varphi][\psi] = (c_{ik})$ where

$$c_{ik} := \sum_{j=1}^{n} a_{ij} b_{jk}.$$

These formulas can be difficult to remember, especially the order of the indices. Here is the key thing to keep in mind: The columns of the matrix $[\varphi]$ record the values of φe_j.

An automorphism of a vector space V is a K-linear isomorphism $\varphi : V \to V$. We write $\mathrm{Aut}(V)$ to denote the group of all such automorphisms of V. In the case $V = K^n$ this group has a special name, the n**th general linear group**

$$\mathrm{GL}_n(K) := \mathrm{Aut}(K^n).$$

We can view the elements of $\mathrm{GL}_n(K)$ as invertible $n \times n$ matrices with entries in K. Recall that the simple way to check if a square matrix is invertible is to calculate its *determinant*.

The **determinant** is a homomorphism $\det : \mathrm{GL}_n(K) \to K^\times$ which may be calculated recursively using the cofactor expansion formula: If $A = (a_{ij})$, then for any $1 \le i \le n$ the i**th row cofactor expansion** of $\det(A)$ is

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}),$$

and for any $1 \le j \le n$ the j**th column cofactor expansion** of $\det(A)$ is

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}).$$

In both cases A_{ij} refers to the matrix we get by removing the ith row and jth column from A. Since we have been talking about symmetric groups, let me also share another formula for the complete expansion of the determinant using permutations,

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}.$$

This one is sometimes useful for proving things but not very useful in practice (too many terms in the sum!) Determinants are challenging to calculate and to analyze—there are entire books filled with nothing but identities for various kinds of special determinants. The main thing to keep in mind for now is that a square matrix A is invertible if and only if $\det(A) \neq 0$.

Now we get to the point. Let G be a group. A permutation representation of G is an action of G on a set X, or equivalently a homomorphism $\rho : G \to S_X = \mathrm{Aut}(X)$.

DEFINITION 5.5
A **linear representation** of G is a linear action of G on a vector space V, or equivalently a homomorphism $\rho : G \to \mathrm{Aut}(V)$.

When ρ is understood, we follow the same convention as with G-sets and write $gv := \rho_g(v)$. What makes these actions linear is how they interact with the vector space operations. If $u, v \in V$ and $c \in K$, then for all $g \in G$ we have

$$g(u + v) = gu + gv$$

and

$$g(cv) = c(gv).$$

Note that if $V \cong K^n$ as K-vector spaces, then $\mathrm{Aut}(V) \cong \mathrm{GL}_n(K)$ as groups. Hence a linear representation of G is equivalent to a way of representing the elements of G as matrices.

Up to this point we have let K be an arbitrary field. While representations are interesting over all fields, they are simplest over the complex numbers. We will now switch from K to $\mathbb{C}$. The two features of $\mathbb{C}$ which make it the simplest venue are

1. $\mathbb{C}$ is algebraically closed, and
2. $\mathbb{C}$ has characteristic zero.

Any field with these two properties will be just as good.

The simplest example of a linear representation is the **trivial representation** on a vector space V, where every element of G acts as the identity: $gv = v$ for all $g \in G$ and $v \in V$. In other words, $\rho : G \to \mathrm{Aut}(V)$ is the trivial homomorphism $\rho(g) = 1$. When we refer to *the* trivial representation without specifying V, we mean the trivial representation on the 1-dimensional space $\mathbb{C}$.

PROBLEM 5.4

Note that a 1×1 invertible matrix is essentially just a unit, which is to say that $\mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$. Hence homomorphisms $\rho : G \to \mathbb{C}^\times$ are the same thing as 1-dimensional representations. These are sometimes also called **characters**[2] and in that context often denoted by $\chi : G \to \mathbb{C}^\times$ instead of ρ.

1. Let G be a finite group and suppose that $\rho : G \to \mathbb{C}^\times$ is a 1-dimensional representation. Prove that $\rho(g)$ is a root of unity[3] for all $g \in G$.
2. Let $C_4 := \langle g : g^4 = 1 \rangle$ be the 4th cyclic group. Find all of the 1-dimensional representations $\rho : C_4 \to \mathbb{C}^\times$.

[2] Though they are a special case of a more general concept of character we will discuss later.
[3] A complex solution of $x^n = 1$ for some n.

3. A representation $\rho : G \to \mathrm{Aut}(V)$ is **faithful** if ρ is injective. How many faithful 1-dimensional representations does C_n have?

4. Determine all of the 1-dimensional representations of S_3.

Every permutation representation can be turned into a linear representation, giving us an immediate and ample supply of examples. Let X be a finite set. For each $x \in X$ we create a formal vector e_x (just a symbolic expression) and then let $\mathbb{C}X$ be the $\mathbb{C}$-vector space of all formal $\mathbb{C}$-linear combinations of the vectors e_x,

$$\mathbb{C}X := \left\{ \sum_{x \in X} c_x e_x : c_x \in \mathbb{C} \right\}.$$

We call $\mathbb{C}X$ the **free $\mathbb{C}$-vector space generated by** X. The vectors $\{e_x : x \in X\}$ form a basis for $\mathbb{C}X$ by fiat. Hence we have $\sum_{x \in X} c_x e_x = \sum_{x \in X} d_x e_x$ if and only if $c_x = d_x$ for all $x \in X$.

For example, if $X = \{1, 2, 3\}$, then

$$\mathbb{C}X = \{c_1 e_1 + c_2 e_2 + c_3 e_3 : c_i \in \mathbb{C}\} \cong \mathbb{C}^3.$$

More generally the dimension of $\mathbb{C}X$ is $|X|$, hence

$$\mathbb{C}X \cong \mathbb{C}^{|X|}.$$

If a group G acts on a set X by permutations, then we can extend this to a linear action of G on $\mathbb{C}X$ by defining

$$g \sum_{x \in X} c_x e_x := \sum_{x \in X} c_x e_{gx}.$$

(Check that this really is a linear action of G on $\mathbb{C}X$!) The most important instance of this construction is when $X = G$ acting on itself by left multiplication. The resulting linear representation $\mathbb{C}G$ is called the **regular representation** of G. It has dimension $|G|$, and $g \in G$ acts on the basis vectors by $g e_h = e_{gh}$. We will see later that the regular representation contains a copy of every representation of G we could ever want.

PROBLEM 5.5

Let's explore this construction with $G = S_3$ and $X = \{1, 2, 3\}$ with its standard action. In this case $\mathbb{C}X \cong \mathbb{C}^3$. Let $\rho : S_3 \to \mathrm{GL}_3(\mathbb{C})$ be the natural linear representation of S_3.

1. Write down the matrices $\rho(\sigma)$ with respect to the standard basis for each $\sigma \in S_3$.

2. Note that if $\rho : G \to \mathrm{Aut}(V)$ is any linear representation, composing ρ with the determinant $\det : \mathrm{Aut}(V) \to \mathbb{C}^\times$ gives us a 1-dimensional representation $\det(\rho) : G \to \mathbb{C}^\times$. Which 1-dimensional representation of S_3 do we get from taking the determinant of ρ?

3. If V is a representation of G, we call a subspace $U \subseteq V$ a **G-invariant subspace** if $gU \subseteq U$ for all $g \in G$. Classify all the S_3-invariant subspaces of $\mathbb{C}^3$.

4. Try plotting the real points in these invariant spaces; what do you notice about the geometric relationship between the invariant subspaces?