Lecture 30: Vector spaces and determinants.

1. Some preliminaries and the free module on 0 generators

Exercise 30.1. Let M be a left R-module. Show that

$$r0_M = 0_M, \qquad \text{and} \qquad r(-x) = -rx.$$

PROOF. By homework, an R-action on M is the same thing as a ring homomorphism $R \to \mathrm{End}(M)$. In particular, every $r \in R$ determines an abelian group homomorphism. Hence scaling by r preserves the additive identity of M, and additive inverses.

If you prefer a more computational proof, you can observe:

$$r0_M + r0_M = r(0_M + 0_M) = r0_M.$$

So by cancellation for abelian groups, we can subtract $r0_M$ from both sides to obtain

$$r0_M = 0_M.$$

So

$$r(-x) + rx = r(-x + x) = r0_M = 0_M$$

which shows that $r(-x)$ is the additive inverse to rx. □

Remark 30.2. We know what $R^{\oplus n}$ is for $n \geq 1$. But what about $n = 0$?

Well, the proposition from last time tells us that we should look for an R-module $R^{\oplus 0}$ such that there is a bijection

$$\mathrm{Hom}_R(R^{\oplus 0}, M) \cong \mathrm{Map}_{\mathsf{Sets}}(\emptyset, M).$$

But there is one and only one function from the empty set to any set; so we must look for a module $R^{\oplus 0}$ which has one and only one module homomorphism to any M. The only such module is the zero module—i.e., the trivial abelian group with the module action $r0 = 0$.

2. Review of last time; dimension

Last time we studied finitely generated modules over a field F. We proved

Theorem 30.3. Let V be a vector space over F—i.e., a module over F. If $y_1, \dots, y_m$ is a linearly independent set, and $x_1, \dots, x_n$ is a spanning set, then $m \leq n$.

We stated two corollaries:

Corollary 30.4. Any two bases of a finitely generated F have the same number of elements in them.

Definition 30.5. Let V be a finitely generated F-module—i.e,. a finitely generated vector space. We call such a V a *finite-dimensional* vector space, and define the dimension of V

$$\dim_F V$$

to be the number of elements in any basis for V.

Example 30.6. The 0-dimensional vector space is the module given by the trivial abelian group, $M = \{0\}$.

The second corollary was:

Corollary 30.7. If M is a finitely generated vector space, any linearly independent collection $w_1, \dots, w_m$ can be completed to a basis—that is, we can find $w_{m+1}, \dots, w_n$ so that the resulting collection $w_1, \dots, w_n$ is both linearly independent and spanning.

Chit-chat 30.8. What are we going to do? Well, you have studied matrices whose entries are real numbers before. You did a lot with them—multiply them, add them, and also figure out when they're invertible. I claim that almost everything you could do with real matrices, you can pretty much do with matrices with coefficients in any field.

3. More corollaries

Corollary 30.9. Any finitely generated module over a field F is isomorphic to F^n for some n.

Proof. Begin with the linearly independent set 0 and complete to a basis. A basis defines an isomorphism from F^n to your module. □

Remark 30.10. This is definitely not true for R-modules if R is not a field—as we saw last time, $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module but doesn't even admit a linearly independent, non-empty collection of elements (let alone a basis).

Corollary 30.11. If $V' \subset V$ is a subspace,

$$\dim V' = \dim V \iff V = V'.$$

PROOF. One implication is obvious. For the other direction, let $y_1, \ldots, y_n$ be a basis for V'. Since these vectors are linearly independent, they can be completed to a basis in V by one of the corollaries above. But this basis must have exactly n elements in it by the definition of dimension—in other words, the y_i are already a basis. $\square$

Corollary 30.12. Let $V' \subset V$ be a subspace. Then $\dim V' + \dim V/V' = \dim V$.

PROOF. Let $v_1, \ldots, v_{\dim V'}$ be a basis for V'. Let $\overline{u_1}, \ldots, \overline{u_{\dim V/V'}}$ be a bsis for V/V'. Then choosing representatives u_i for $\overline{u_i}$, the set

$$v_1, \ldots, v_{\dim V'}, u_1, \ldots, u_{\dim V/V'}$$

is a basis for V. It obviously spans since for each $a \in V$, $\overline{a}$ is a linear combination of $\overline{u_i}$, hence a is in the V'-orbit of some linear combination of the u_i. It is linearly independent because if we have that

$$0 = a_1 v_1 + \ldots a_{\dim V'} v_{\dim V'} + b_1 u_1 + \ldots + b_{\dim V/V'} u_{\dim V/V'}$$

then

$$\overline{0} = a_1 \overline{v}_1 + \ldots a_{\dim V'} \overline{v_{\dim V'}} + b_1 \overline{u_1} + \ldots b_{\dim V/V'} \overline{u_{\dim V/V'}}.$$

The a_i terms go to zero since $\overline{v}_i = 0$, hence we get an equation saying a linear combination of the $\overline{u}_i$ is zero. This means each b_i must be zero by linear independence of the $\overline{u}_i$. The original equation then says that $0 = \sum a_i v_i$, so by linear independence of the v_i, the a_i must be zero. $\square$

Corollary 30.13 (Rank-nullity theorem)**.** Let $f : V \to W$ be a map of F-modules and assume V is finitely generated. Then $\dim \ker f + \dim \operatorname{im} f = \dim V$.

PROOF. By the first isomorphism theorem, we know there is a group isomorphism $V/\ker f \cong \operatorname{im} f$. But this homomorphism is also an F-module map, as you can check by hand. Thus $\operatorname{im} f \cong V/\ker f$. $\square$

Corollary 30.14 (Criterion for isomorphisms)**.** Let $f : V \to W$ be a linear map between finite-dimensional vector spaces. Then f is an isomorphism if and only if f is injective and $\dim V = \dim W$.

Proof. By the rank-nullity theorem, the image of f has dimension V since f is injective. □

4. The take-away

The take-away from all the above is how powerful the notion of dimension is. Whether your field be something familiar like $\mathbb{R}$, or something foreign (for now) like $\mathbb{Z}/p\mathbb{Z}$; whether the linear map be something as familiar as a matrix, or something that you didn't realize was linear like evaluating polynomial functions (see homework), we have a powerful way of studying linear maps.

5. Determinants

The other powerful tool we have from linear algebra is the notion of determinant. Well, the determinant only required a notion of multiplying by -1 (taking additive inverses), multiplying entries of a matrix, and adding things together. So we should be able to define a determinant for any matrix with coefficients in a ring R.

As it turns out, some formulas may not hold true if the ring R isn't commutative—the order of multiplication is important—so we'll restrict ourselves to commutative rings.

Definition 30.15. Let R be a commutative ring. A $k \times k$ matrix in R is a collection of elements

$$A_{ij} \in R$$

where $i \in 1, \dots, k$ and $j \in 1, \dots, k$. We'll represent a matrix by the symbol

$$A = (A_{ij}).$$

Example 30.16. A 3×3 matrix in R can be drawn in the usual way:

$$\begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}.$$

Definition 30.17. The *ring* of $k \times k$ matrices in R, denoted $M_{k\times k}(R)$, has addition given by

$$(A_{ij}) + (B_{ij}) = (A_{ij} + B_{ij}) \qquad (A_{ij})(B_{ij}) = (\sum_{l=1}^{k} A_{il}B_{lj}).$$

That is, addition is the usual entry-by-entry addition. In the product, the i, jth entry is given by taking the jth column of B and pairing it with the ith row of A.

Definition 30.18 (Cofactor matrix)**.** Let A be a $k \times k$ matrix. The $(i.j)$th *cofactor matrix* of A is the matrix obtained by deleting the ith row and jth column of A. When A is implicit, we will write

$$C_{i,j}$$

for the $(k-1) \times (k-1)$ matrix given by the (i, j)th cofactor matrix of A.

Definition 30.19. The determinant of a 1×1 matrix in R is the unique element A_{11} of the matrix.

Inductively: Let A be a $k \times k$ matrix. Then the determinant of A is defined to be the sum

$$\det A = A_{11} \det C_{1,1} - A_{21} \det C_{2,1} + \ldots + (-1)^{1+k} A_{k1} \det C_{k,1}.$$

Using summation notation,

$$\det A := \sum_{i=1}^{k} (-1)^{i+1} A_{i1} \det C_{i,1}.$$

This defines a function

$$\det : M_{k\times k}(R) \to R.$$

Example 30.20. If A is a 2×2 matrix,

$$\det(A) = A_{11}A_{22} - A_{12}A_{21}.$$

We won't prove the following theorems, but the same proofs you did for real numbers carries through:

Theorem 30.21. Let A and B be $k \times k$ matrices. Then

$$\det(A) \det(B) = \det(AB)$$

and

$$\det(A^T) = \det(A).$$

Theorem 30.22. Let adj(A) be the $k \times k$ matrix whose (i,j)th entry is given by

$$(-1)^{i+j} \det C_{j,i}.$$

Then

$$A \cdot (\text{adj}\, A) = (\text{adj}\, A) \cdot A = \det A \cdot I$$

where $\det A \cdot I$ is the diagonal matrix with entries given by the element $\det A \in R$.

Remark 30.23. In case you haven't seen this last statement before, let me give a small idea of how the proof goes. The (i,j)th entry of the first multiplication is given by

$$\sum_{l=1}^{k} A_{il} (\text{adj}\, A)_{lj} = \sum_{l=1}^{k} A_{il} (-1)^{j+l} \det C_{j,l}.$$

So for instance, the $(1,1)$ entry is precisely the definition of the determinant of A. By using properties about swapping rows only changing the determinant by a sign, you can prove that every diagonal entry is the determinant of A.

For the off-diagonal entry, you observe that the summation above becomes the determinant for a matrix with two equivalent rows; hence equals zero.

Corollary 30.24. Let $A \in M_{k \times k}(R)$. Then A is an invertible matrix if and only if $\det A \in R$ has a multiplicative inverse.

Proof. Let $B = \det A^{-1} \,\text{adj}\, A$. Then

$$BA = \det A^{-1} \,\text{adj}\, A \cdot A = \det A^{-1} \det A \cdot I = I.$$

Likewise for BA. □

Example 30.25. If A is a matrix with only integer entries, then there exists an inverse matrix with integer entries if and only if $\det A = \pm 1$.

Example 30.26. Let A be a matrix with entries in $\mathbb{Z}/n\mathbb{Z}$. It is invertible if and only if its determinant is relatively prime to n.