10. Vector spaces

Vector Spaces

Quick reminder about fields

Fields we know about:

- $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Q}(x)$, ... these are fields of characteristic zero
- $\mathbb{Z}/p\mathbb{Z}$ where p is prime, these are finite fields of characteristic p.
- $\mathbb{Z}/p\mathbb{Z}(x)$, rational functions with coefficients in $\mathbb{Z}/p\mathbb{Z}$, this is an infinite field of characteristic p.
- $\mathbb{Z}/p\mathbb{Z}[x]/(f(x))$ where $f(x)$ is an irreducible polynomial of degree d over $\mathbb{Z}/p\mathbb{Z}$, this is a finite field with p^d elements. For example

$$\mathbb{Z}/2\mathbb{Z}[x]/(x^x + x + 1)$$

and

$$\mathbb{Z}/3\mathbb{Z}[x]/(x^2 + 1).$$

Next semester we will prove the following.

Theorem: If F is a finite field of characteristic p, then F has p^d elements for some $d \geq 1$ and all finite fields of the same order are isomorphic.

Key definitions

In the following, F is a field.

Definition: A vector space V over F is an abelian group together with a map $F \times V \to V$, called scalar multiplication, which satisfies, for all $a, b \in F$ and $v, w \in V$: - $a \cdot (b \cdot v) = (ab) \cdot v$ - $(a+b) \cdot v = a \cdot v + b \cdot v$ - $a \cdot (v + w) = a \cdot v + a \cdot w$ - $1 \cdot v = v$

Remark: If, in the above definition, we replace F by a ring R with 1, then the same axioms characterize an object called a *left R-module*. So a module is like a vector space but you only have scalar multiplication by elements of a ring instead of a field.

Definition: Let V be a vector space over F. - A subspace is a subgroup of V closed under scalar multiplication. - A *linear map* $f : V \to W$ is a group homomorphism that satisfies $f(av) = af(v)$ for all $a \in F$. - A (possibly infinite) set S of vectors in V is called *linearly independent* if, for any finite set $v_1, \ldots, v_k$ of elements of S, if $\sum_{i=1}^{k} a_i v_i = 0$ then all $a_i = 0$. - A set of vectors S is said to *span* V if it generates V as a vector space, meaning the smallest subspace of V containing S is all of V. - A linearly ordered set of vectors S is a *basis* of V if it is linearly independent and spans V.

Basis and dimension

If a vector space V has a finite basis with n elements, then every basis of V has n elements and n is called the dimension of V.

Every vector space of dimension n over F is isomorphic to each other and to F^n.

The group of bijective linear maps from V to V is called $\mathrm{Aut}(V)$ or $\mathrm{GL}(V)$.

Counting

If F is a finite field with $q = p^d$ elements, and W is a vector space of dimension k, then:

1. The number of distinct bases of W is $(q^k - 1)(q^k - q)(q^k - q^2) \cdots (q^k - q^{k-1})$.
2. The number of subspaces of dimension k is

$$\frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - (q^{k-1})}$$

3. The group $\mathrm{Aut}(V)$ has the same order as in part 1. (To see this, fix a basis of V. Given another basis, there is a bijective linear map from the fixed basis to this new basis. So the number of linear maps is the same as the number of different bases of V)

Subspaces and quotients

The kernel of a linear map $f : V \to K$ is a subspace of V.

If $W \subset V$ is a subspace, the quotient group V/W is a vector space. It satisfies the "isomorphism theorem" that any linear map $g : V \to K$ such that $W \subset \ker(g)$ factors through the quotient W/V:

$$\begin{tikzcd}
V \arrow[d, "\pi"] \arrow[dr, "f"] & \\
V/W \arrow[r, "\overline{f}"'] & K
\end{tikzcd}$$

Proposition: If V is finite dimensional, then $\dim(V) = \dim(W) + \dim(V/W)$. (In the infinite dimensional case, both sides are infinite).

Proposition: If $f : V \to W$ is a linear map between vector spaces, then the image $f(V)$ is a subspace of W and $\dim(V) = \dim\ker(f) + \dim f(V)$. This follows from the isomorphism theorem and the preceeding result.

A little Zorn

Theorem: Every vector space has a basis.

Proof: Let V be a vector space and consider the collection of linearly independent subsets of V ordered by inclusion. This is a nonempty set, and if $A_1 \subset A_2 \subset \ldots$ is a chain, then the union of the A_i is an independent set containing all of the A_i. So every ascending chain has an upper bound. By Zorn's Lemma, the set of linearly independent subsets has a maximal element B. Let $x \in W$. The set $B \cap \{x\}$ must be linearly dependent, since B is maximal, so x is a linear combination of elements of B. Thus B is a basis of V.

Matrices

Let V and W be finite dimensional vector spaces with basis A and B respectively. Let f be a linear map from V to W. Then we have equations

$$f(a_j) = \sum e_{ij} b_i$$

for each j between 1 and $n = \dim(V)$ and i between 1 and $m = \dim(W)$ respectively. **TAKE NOTE OF HOW THE INDICES ARE ORGANIZED**

Define

$$M_A^B(f) = \begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1n} \\ \vdots & \vdots & \ldots & \vdots \\ e_{m1} & e_{m2} & \cdots & e_{mn} \end{bmatrix}$$

Thus we associate to a linear map $f : V \to W$ an $m \times n$ matrix where $n = \dim(V)$ and $m = \dim(W)$. This **depends on the choice of bases** A and B.

This correspondence has the property that, if $v \in V$ satisfies $v = \sum_{j=1}^{n} x_j a_j$ then $f(v) = \sum_{j=1}^{m} y_j b_j$ where

$$M_A^B(f) \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix}$$

Proposition: The map sending $f : V \to W$ to $M_A^B(f) \in M_{m\times n}(F)$ is an isomorphism of vector spaces between $\mathrm{Hom}(V, W)$ and $M_{m\times n}(F)$.. If $V = W$ and $A = B$, it is a ring isomorphism from $\mathrm{Hom}(V, V)$ to $M_n(F)$.