Day 19

Vector Spaces

Notes on fields

A closer look at the fields

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

and

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

with 4 and 9 elements respectively.

Vector spaces

If V is an abelian group, then let

$$\text{End}(V) = \{f : V \to V \text{ where } f \text{ is a homomorphism}\}$$

Proposition: $\text{End}(V)$ is a ring with unity, where: - addition is addition of maps $(f+g)(v) = f(v)+g(v)$. - multiplication is composition of maps $(fg)(v) = f(g(v))$. - The identity map is the identity element for multiplication. - The zero map is the identity element for addition.

Let F be a field. A non-trivial ring homomorphism (sending 1 to 1) $F \to \text{End}(V)$ makes V an F vector space; and an F-vector space structure on an abelian group V is equivalent to a non-trivial homomorphism $F \to \text{End}(V)$.

Notice that $\mathbb{Z}/3\mathbb{Z}$ maps into $\text{End}(\mathbb{Z}/6\mathbb{Z}) = \mathbb{Z}/6\mathbb{Z}$, but this map doesn't send 1 to 1. So $\mathbb{Z}/6\mathbb{Z}$ is not a vector space over $\mathbb{Z}/3\mathbb{Z}$.

A linear map $f : V \to W$ is a group homomorphism such that $f(av) = af(v)$ for all $a \in F$. The space $\text{Hom}(V, W)$ of linear maps from V to W is a vector space over F. The space $\text{Hom}(V, V)$ of linear maps from V to V is a ring.

Lemma: If $f : V \to V$ is linear and bijective, then its inverse is also linear.

Proof: Let $g = f^{-1}$. Then $g(f(ax))) = ax$ so $g(af(x)) = ax$. Write $f(x) = y$ and $x = g(y)$, and we have $g(ay) = ag(y)$.

An isomorphism of vector spaces is a bijective linear map $V \to W$. The units in the ring $\mathrm{Hom}(V, V)$ are the automorphisms of V – that is, the invertible linear maps from V to V.

A subspace is a subgroup W such that $aW = W$ for all $a \in F$.

Basis and Dimension

Definition: A basis of V is a subset that both spans V and is linearly independent.

Proposition: A basis is a minimal spanning set. In other words, if B is a set of vectors that spans V, but no proper subset of B spans V, then B is a basis.

Proof: Suppose that B is not a basis. Then it is linearly dependent, so there is a finite set of vectors $v_1, \ldots, v_n$ such that $\sum a_i v_i = 0$ with not all $a_i = 0$. Therefore we can "solve" for one of the v_i in terms of the others, and conclude that there is a proper subset of B that spans V.

The ring $F[x]/(f(x))$, where $f(x)$ is a monic polynomial of degree d, is a vector space over F with basis $1, x, \ldots, x^{d-1}$.

Corollary: A finite spanning set of V contains a basis.

Proof: Choose a minimal spanning subset.

Proposition: If $A = \{a_1, \ldots, a_n\}$ is a basis for V and $B = \{b_1, \ldots, b_k\}$ is a linearly independent set, then one can reorder the elements of A so that $A' = \{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\}$ is a basis of V. In particular, A has at least as many elements as B.

Proof: DF give an inductive argument. Axler describes a process for reducing a spanning set to a linearly independent set.
His argument is: put A and B together, with B first:

$$b_1, \ldots, b_k, a_1, \ldots, a_n$$

This is a spanning set. The list $b_k, a_1, \ldots, a_n$ must be linearly dependent since b_k is in the span of the a_i. This means there's a linear relation expressing b_k as a sum of a_i's – let's say a_n, renumbering if necessary – so $b_k, a_1, \ldots, a_{n-1}$ is again a basis. Now consider $b_{k-1}, b_k, a_1, \ldots, a_{n-1}$. Again b_{k-1} is a linear combination of $b_k, a_1, \ldots$; and this linear combination must involve at least one of the a_i since the b's are linearly independent. So again we can eliminate one of the a's, say a_{n-1} after renumbering, and continue.

Corollary: Suppose V has a basis with n elements. Then any spanning set has at leas n elements, and any independent set has at most n elements.

Corollary: If V has a finite basis, then any two bases have the same number of elements. This number is called the *dimension* of V. If V does not have a finite basis, it is *infinite dimensional*.

Corollary: Any linearly independent set in a finite dimensional space can be extended to a basis.

Proof: Choose any basis and apply the construction in the proposition above with your given independent set and basis.

Corollary: If W is a subspace of V and V is finite dimensional, then the dimension of W is less than or equal to the dimension of V, with equality only when $V = W$.

Proof: Inductively construct a linearly independent set in W. The process terminates since it can have at most $\dim(V)$ elements.

Proposition: Any two vector spaces over F of finite dimension n are isomorphic. In particular, any such V is isomorphic to F^n.