MATH 433

Applied Algebra

Lecture 25:
Vector spaces over a field.
Algebras over a field.

Vector spaces over a field

Definition. Given a field F, a **vector space** V over F is an additive Abelian group endowed with an action of F called **scalar multiplication** or **scaling**.

An **action** of F on V is an operation that takes elements $\lambda \in F$ and $v \in V$ and gives an element, denoted λv, of V.

The scalar multiplication is to satisfy the following axioms:

(V1) for all $v \in V$ and $\lambda \in F$, λv is an element of V;
(V2) $\lambda(\mu v) = (\lambda\mu)v$ for all $v \in V$ and $\lambda, \mu \in F$;
(V3) $1v = v$ for all $v \in V$;
(V4) $(\lambda + \mu)v = \lambda v + \mu v$ for all $v \in V$ and $\lambda, \mu \in F$;
(V5) $\lambda(v + w) = \lambda v + \lambda w$ for all $v, w \in V$ and $\lambda \in F$.

(Almost) all linear algebra developed for vector spaces over $\mathbb{R}$ can be generalized to vector spaces over an arbitrary field F. This includes: linear independence, span, basis, dimension, determinants, matrices, eigenvalues and eigenvectors.

Examples of vector spaces over a field F:

- The space F^n of n-dimensional coordinate vectors $(x_1, x_2, \ldots, x_n)$ with coordinates in F.
- The space $\mathcal{M}_{n,m}(F)$ of $n \times m$ matrices with entries in F.
- The space $F[X]$ of polynomials $p(x) = a_0 + a_1 X + \cdots + a_n X^n$ with coefficients in F.
- Any field F' that is an extension of F (i.e., $F \subset F'$ and the operations on F are restrictions of the corresponding operations on F'). In particular, $\mathbb{C}$ is a vector space over $\mathbb{R}$ and over $\mathbb{Q}$, $\mathbb{R}$ is a vector space over $\mathbb{Q}$.

Counterexample. • Consider the Abelian group $V = \mathbb{R}^n$ with a nonstandard scalar multiplication over $\mathbb{R}$ ("lazy scaling"):

$$\boxed{r \odot \mathbf{v} = \mathbf{v}} \quad \text{for any } \mathbf{v} \in \mathbb{R}^n \text{ and } r \in \mathbb{R}.$$

Let us verify the axioms.

V1. $r \odot \mathbf{v} = \mathbf{v} \in V$

V2. $(rs) \odot \mathbf{v} = r \odot (s \odot \mathbf{v}) \iff \mathbf{v} = \mathbf{v}$

V3. $1 \odot \mathbf{v} = \mathbf{v} \iff \mathbf{v} = \mathbf{v}$

V4. $(r + s) \odot \mathbf{v} = r \odot \mathbf{v} + s \odot \mathbf{v} \iff \mathbf{v} = \mathbf{v} + \mathbf{v}$

V5. $r \odot (\mathbf{v}+\mathbf{w}) = r \odot \mathbf{v} + r \odot \mathbf{w} \iff \mathbf{v}+\mathbf{w} = \mathbf{v}+\mathbf{w}$

The only axiom that fails is V4.

Finite fields

Theorem 1 Any finite field F has nonzero characteristic.

Proof: Consider a sequence $1, 1+1, 1+1+1, \dots$ Since F is finite, there are repetitions in this sequence. Clearly, the difference of any two elements is another element of the sequence. Hence the sequence contains 0 so that the characteristic of F is nonzero.

Theorem 2 The number of elements in a finite field F is p^k, where p is a prime number.

Proof: Let p be the characteristic of F. By the above, $p > 0$. As we know from the previous lecture, p is prime. Let F' be the set of all elements $1, 1+1, 1+1+1, \dots$ Clearly, F' consists of p elements. One can show that F' is a subfield (canonically identified with $\mathbb{Z}_p$). It follows that F has p^k elements, where $k = \dim F$ as a vector space over F'.

Algebra over a field

Definition. An **algebra** A over a field F (or F-**algebra**) is a vector space with a multiplication which is a bilinear operation on A. That is, the product xy is both a linear function of x and a linear function of y.

To be precise, the following axioms are to be satisfied:

(A1) for all $x, y \in A$, the product xy is an element of A;
(A2) $x(y+z) = xy+xz$ and $(y+z)x = yx+zx$ for $x, y, z \in A$;
(A3) $(\lambda x)y = \lambda(xy) = x(\lambda y)$ for all $x, y \in A$ and $\lambda \in F$.

An F-algebra is **associative** if the multiplication is associative. An associative algebra is both a vector space and a ring.

An F-algebra A is a **Lie algebra** if the multiplication (usually denoted $[x, y]$ and called **Lie bracket** in this case) satisfies:

(Antisymmetry): $[x, y] = -[y, x]$ for all $x, y \in A$;
(Jacobi's identity): $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in A$.

Examples of associative algebras:

- The space $\mathcal{M}_n(F)$ of $n \times n$ matrices with entries in F.
- The space $F[X]$ of polynomials $p(x) = a_0 + a_1 X + \cdots + a_n X^n$ with coefficients in F.
- The space of all functions $f : S \to F$ on a set S taking values in a field F.
- Any field F' that is an extension of a field F is an associative algebra over F.

Examples of Lie algebras:

- $\mathbb{R}^3$ with the cross product is a Lie algebra over $\mathbb{R}$.
- Any associative algebra A with a Lie bracket (called the **commutator**) defined by $[x, y] = xy - yx$.