AMAT 584 Lec 16 2/26/20

Today: Prime Fields, Continued
Abstract Vector Spaces
Dimension of a Vector Space

Review:

Definition: A field is a set F, together with functions
$+: F \times F \to F$ (addition)
$\cdot: F \times F \to F$ (multiplication)

Note: $+(a,b)$ is written as $a+b$
$\cdot(a,b)$ is written as $a \cdot b$.

satisfing all the familiar properties of arithmetic over the rational numbers $\mathbb{Q}$ or real numbers $\mathbb{R}$.

We gave these properties explicitly in the last lecture.

Most important properties to remember:
- $\exists$ an additive and multiplicative identities $0, 1 \in F$
- $\forall$ $a \in F$, $a \neq 0$, $\exists$ a multiplicative inverse $a^{-1} \in F$ (also writen $\frac{1}{a}$). This meas $a \cdot \frac{1}{a} = 1$.
- $\forall a \in F$, $\exists$ an additive inverse $-a \in F$, i.e. $a + {-a} = 0$.

Example: Prime fields
Let p be a prime number, e.g. $p = 2, 3, 5,$ or 7.

Let $\mathbb{F}_p = \{0, 1, \dots, p-1\}$.
Define $+ : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ by taking $a+b$ to be the remainder of the usual integer sum after dividing by p.

e.g. in $\mathbb{F}_5$, $4+4=3$.

Similarly, define $\cdot : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ by taking $a \cdot b$ to be the remainder of the usual integer product after dividing by p.

e.g. in $\mathbb{F}_5$, $4 \cdot 4 = 1$.

With these choices of addition and multiplication, $\mathbb{F}_p$ is a field.

<u>Example</u> $\mathbb{F}_3 = \{0, 1, 2\}$

Addition and Multiplication in $\mathbb{F}_3$ are given by the following tables:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Note: If q is not prime, e.g. $q=4$, $\mathbb{F}_q$ can still be defined in the same way. It still satisfies all the properties of a field except the existence of mutiplicative inverses.

($\mathbb{F}_q$ is a ring. But we won't worry about rings in this class.)

Abstract Vector Spaces

Definition: A vector space over a field F is a set V together with functions

$+ : V \times V \to V$ (addition)
$\cdot : F \times V \to V$ (scalar multiplication)

Note: $+(a,b)$ is written as $a+b$
$\cdot(a,b)$ is written as $a \cdot b$ or ab.

Satisfying all the usual properties of addition and scalar multiplication of vectors in $\mathbb{R}^n$ or $\mathbb{C}^n$, namely:

All the properties satisfied by addition in a field:
- associativity
- commutativity
- existence of additive identity $\vec{0}$ and additive inverses

Other properties:

- $\forall \vec{w} \in V$, $1\vec{w} = \vec{w}$ (1 denotes the multiplicative identity of F)

- An associativity-like property for field mult. + scalar mult.:
  $\forall a, b \in F$ and $\vec{w} \in V$, $(ab)\vec{w} = a(b\vec{w})$.

- Distributivity version 1:
  $\forall a \in F$ and $\vec{v}, \vec{w} \in V$, $a(\vec{v} + \vec{w}) = a\vec{v} + a\vec{w}$

- Distributivity version 2:
  $\forall a, b \in F$ and $\vec{w} \in V$, $(a+b)\vec{w} = a\vec{w} + b\vec{w}$.

To be clear, all properties listed are part of the definition of an abstract vector space.

(that is, these properties are axioms)

There are other properties satisfied by an abstract vector space that are consequences of the axioms, e.g. $\forall a \in F$, $a\vec{0} = \vec{0}$.

Notation / Terminology: If V is an abstract vector space, we call elements of V vectors and write them using the arrow notation, as above, e.g. $\vec{w} \in V$.

Examples:

1) $\mathbb{R}^n$, with its usual addition and scalar multiplication, is a vector space over $\mathbb{R}$.

2) Similarly, $\mathbb{C}^n$ is a vector space over $\mathbb{C}$.

3) For any set S, the set of all functions $f: S \to \mathbb{R}$ with addition

$$(f+g)(x) = f(x) + g(x)$$

and scalar multiplication

$$(c \cdot f)(x) = c \cdot f(x)$$

is a vector space over $\mathbb{R}$, denoted $\mathrm{Fun}(S, \mathbb{R})$

For example, take $S = \mathbb{R}$ or $S = [0,1]$.

4) More generally, for any field F, the set of all functions $f: S \to F$ is a vector space over F, denoted $\mathrm{Fun}(S, F)$.

5) The set of all polynomial functions $f: \mathbb{R} \to \mathbb{R}$ with the same addition and scalar multiplication rules as above is a vector space over $\mathbb{R}$.

<u>Def</u>: A <u>subspace</u> of a vector space V over F is a subset $W \subset V$ such that

$$\vec{w}_1 + \vec{w}_2 \in W \quad \forall\ \vec{w}_1, \vec{w}_2 \in W$$
$$a\vec{w} \in W \quad \forall\ a \in F,\ \vec{w} \in W.$$

If W is a subspace of V, we write $W < V$.

<u>Fact</u>: For W a subspace of V,
$+ : V \times V$ to $W \times W$ and
$\cdot : F \times V$ to $F \times W$
give W the structure of a vector space.

<u>Examples</u>:
1) For any $c \in \mathbb{R}$, the line $\{(x,y) \mid y = cx\}$ is a subspace of $\mathbb{R}^2$.
2) The set of all continuous (or differentiable, or polynomial) functions is a subspace of $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$.