ECE 269- Thursday Jan 9th

- Field
- Vector space

Anoancements:

- HW1 is posted

- Do the Fin Aid assignment on Canvas

Field: $(\mathbb{F}, +, \cdot)$ such that

- $(\mathbb{F}, +)$ is an Abelian group:

(0) - $x+y = y+x \quad \forall x, y \in \mathbb{F}$

(1) - $\exists! z \; ; \quad x+z = z+x = x \quad \forall x \in \mathbb{F}$ (identity element $+$)

(2) - $\forall x \in \mathbb{F} \; ; \; \exists y : \quad x+y = z$ (existence of inverse wrt $+$)

(3) - $\forall x, y, z \in \mathbb{F}; \quad x+(y+z) = (x+y)+z$

- $(\mathbb{F}^*, \cdot)$ is an Abelian group:

$\downarrow$

$\mathbb{F} - \{z\}$,

let u be the identity element of $(\cdot)$

- $+$ and $\cdot$ should satisfy: $x \cdot (y+z) = x \cdot y + x \cdot z$

$\forall x, y, z \in \mathbb{F}$.

Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with the usual $+$ and $\cdot$.

Q: How about $\mathbb{Z}$?

- $(\mathbb{Z}, +)$ is an Abelian

- $(\mathbb{Z}^*, \cdot)$ is not an Abelian group: as 2 does not have multiplicative inverse.

Why fields? We can solve

$$a \cdot x + b = c$$

(if $a e = u$)

$$a \cdot x = a \cdot x + (b+d) = (c+d) \equiv \underbrace{e \cdot a}_{u} \cdot x = e \cdot (c+d)$$

$$\Rightarrow x = e \cdot (c+d)$$

$2x+1=2$ for $x \in \mathbb{Z}$?

$p \geq 2$

Define: $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, $+$ and $\cdot$ to be corresponding operations over $\mathbb{Z}$ mod p.

$(\mathbb{Z}_3, +, \cdot)$: is a finite field

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

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Notations:

- Denote the additive identity element by 0
- " " multiplicative " " by 1
- Denote the additive inverse of $a \in \mathbb{F}$ by $-a$
- " " multiplicativ inverse of $a \in \mathbb{F}$ by a^{-1} or $\frac{1}{a}$ or

- The solution to $ax+b=c$ is $x = a^{-1}(c-b)$

Q: What $(4)^{-1}$ in $\mathbb{Z}_5$? $(4)^{-1} = 4$!

Q: In $\mathbb{Z}_4$ what is $(2)^{-1}$?

Fact: $\mathbb{Z}_p$ is a field iff p is prime!

Q: For any $n \geq 2$ does there exists a finite field with n elements?

A: Finite field of order $n \geq 2$ exists iff $n = p^k$ for some prime number p power $k \geq 1$! (and it is essentially unique)

These finite fields are called Galois fields and are denoted by $GF(p^k)$.

For most part of the course $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$

Vector Space: A <u>vector space</u> over a field $(\mathbb{F}, +_F, \cdot_F)$ is $(V, +_V, \cdot_V)$ satisfying:

a set (non-empty)

- $(V, +_V)$ should be an Abelian group.
- $\cdot_V : \mathbb{F} \times V \to V$ satisfying:
  - $(a +_F b) \cdot_V v = a \cdot_V v +_V b \cdot_V v \quad \forall a, b \in F, \ \forall v \in V$
  - $a \cdot_V (v + u) = a \cdot v + a \cdot u \quad \forall a \in F, \ \forall u, v \in V$
  - $a \cdot (b \cdot v) = (a \cdot_F b) \cdot v \quad \forall a, b \in F, \ \forall v \in V$
  - $1 \cdot v = v \quad \forall v \in V$

Examples: $(\mathbb{R}^2, +_V, \cdot)$ over $\mathbb{R}$ is a vector space

- $(a,b) + (c,d) \equiv (a+c, b+d)$

- $\alpha \cdot (a,b) \equiv (\alpha a, \alpha b)$

Here $(0,0)$ is the identity element of $+_V$.

In general $(\mathbb{R}^n, +, \cdot)$ over $\mathbb{R}$ is vector space with the standard summation over $\mathbb{R}^n$ and scalar multiplication.

In fact for any field $(\mathbb{F}, +, \cdot)$ and any $k \geq 1$, $(\mathbb{F}^k, +_V, \cdot_V)$ defined by

$$(a_1, \ldots, a_k) +_V (b_1, \ldots, b_k) := (a_1 +_F b_1, \ldots, a_k +_F b_k)$$

$$\alpha \cdot_V (a_1, \ldots, a_k) := (\alpha \cdot_F a_1, \ldots, \alpha \cdot_F a_k)$$

We refer to elements of a vector space as <u>vectors</u>.

Notation: For sets S, T: $S \times T \overset{\text{define}}{:=} \{(x, y) \mid x \in S, y \in T\}$

$S^k = \overbrace{S \times S \times \cdots \times S}^{k \text{ times}}$

Example: Let V be the set of functions $f: I \to \mathbb{R}$ for an interval $I \subseteq \mathbb{R}$. $(V, +_V, \cdot_V)$ is a vector space over $\mathbb{R}$.

- $(f +_V g)(x) := f(x) + g(x)$
- $(\alpha \cdot f)(x) := \alpha \cdot f(x)$

Note that $0_I(x) := 0$ for all $x \in I$ is the identity element of $+_V$.