Math 117

Overview / Admin Stuff

- Look at syllabus for grades / hw details
  - HW
    - Small HW due usually tuesday/th } think of these as "discussions"
    - Larger HW due usually tue (monday)
  - Glossary

- Final Problem Set

Email

darubins@ucsc.edu

OH :

M : 3:45 - 4:45

Th : 11:45 - 12:45

Overview of Course

- More general vector spaces and fields

  $\rightsquigarrow \mathbb{R}, \mathbb{C}, \mathbb{F}_p$

- More advanced topics / in depth

  $\sim$ quotient spaces, tensor products, wedge/exterior products, spectral theorem

- Prove things!!!!!

Yiddish of the day

"Er halt az er iz der pupik fun der velt" = „ער האַלט אַז ער איז דער פּופּיק פֿון דער וועלט"

"He thinks he is the belly-button of the world" =

Vector Spaces

- **Math 21**

Study the set $\mathbb{R}^n$: $\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in \mathbb{R} \right\}$

- In this set we could

1) Add "vectors" ex) $\begin{pmatrix} 2 \\ 3 \end{pmatrix} + \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 5 \\ 7 \end{pmatrix}$

2) Scale "vectors" ex) $-2 \begin{pmatrix} 4 \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} -8 \\ -6 \\ -2 \end{pmatrix}$

in some <u>coherent</u> way

ex) $(a+b)\vec{x} = a\vec{x} + b\vec{x}$

$a(\vec{x}+\vec{y}) = a\vec{x} + a\vec{y}$

$(ab)\vec{x} = a(b\vec{x})$

$0(\vec{x}) = \vec{0}$

$1\vec{x} = \vec{x}$

Such a structure can be axiomitized

Q) What are the "essential notions" needed in describing the structure of $\mathbb{R}^n$ above?

First focus on these "Scalars" (or "numbers")

- how to generalize $\mathbb{R}$? What can we do in $\mathbb{R}$?

  1) We can add/subtract

  2) We can multiply/divide

Def: A field is a set $\mathbb{F}$ with 2 "operations"

$$\mathbb{F} \times \mathbb{F} \xrightarrow{+} \mathbb{F} \qquad \mathbb{F} \times \mathbb{F} \xrightarrow{\cdot} \mathbb{F}$$

$$(a, b) \longmapsto a+b \qquad (a, b) \longmapsto a \cdot b$$

<u>Such that</u>

(A1) Associativity of $\underline{+}$: For $a, b, c \in \mathbb{F}$ have

$$(a+b)+c = a+(b+c)$$

(A2) Commutativity of $\underline{+}$: For $a, b \in \mathbb{F}$ have

$$a+b = b+a$$

(A3) $\exists!$ element $\underline{0_{\mathbb{F}}}$ such that, $\forall a \in \mathbb{F}$

$$a + 0 = a$$

(A4) For $a \in \mathbb{F}$, $\exists!\ (-a)$ such that

$a + (-a) = 0$

(M1) Associativity of $\cdot$: For $a, b, c \in \mathbb{F}$

$(ab)c = a(bc)$

(M2) Commutativity of $\cdot$: For $a, b \in \mathbb{F}$

$ab = ba$

(M3) $\exists!$ element $1_{\mathbb{F}}$ called the identity such that $\forall a \in \mathbb{F}\ \ a \cdot 1 = a$

(M4) $\forall\ a \neq 0 \in \mathbb{F}$ $\exists!$ a^{-1} called the (mult) inverse

such that $a \cdot a^{-1} = 1$

(D) Distributive law: For all $a, b, c \in \mathbb{F}$

$(a+b)c = ac + bc$

ex) 1) $\mathbb{R}$

2) $\mathbb{Q}$ } check these satisfy the axioms above.

3) $\mathbb{C}$ = complex #'s $\mathbb{C} = \{a+bi \mid a, b \in \mathbb{R}\}$

new one! → 4) $\mathbb{Z}/p = \mathbb{F}_p$ = integers "mod p"

$= \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$

$\bar{a} = \{b \mid a \equiv b \bmod p\}$

$\bar{0} = \{b \mid b \equiv 0 \bmod p\}$

ex) $\underline{p=5}$: $\bar{7} = \bar{2}$ $7 \equiv \underline{2} \bmod 5$

$\bar{8} = \bar{3}$

Pf) Define addition by $\bar{a} + \bar{b} = \overline{a+b}$

ex) $\bar{7} + \bar{8} = \overline{15} = \bar{0} \bmod 5$

$\overline{2}+\overline{3} = \overline{5} = \overline{0} \mod 5$

Turns out this addition rule does not depend on choice of coset.

Ie if $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$

then $\overline{a+b} = \overline{a'+b'}$

If $\overline{a} = \overline{a'}$ then $p \mid a-a'$ and $p \mid b-b'$

Then $pl_1 = a-a_1$ and $pl_2 = b-b_1$

Then $a+b-(a'+b') = a-a'+b-b'$

$= p(l_1+l_2)$

ie $p \mid (a+b)-(a'+b')$

The 0 in $\mathbb{F}_p$ is $\bar{0}$

Given $\bar{a} \in \mathbb{F}_p$ $\exists$ element such that $\bar{a} + \bar{b} = \bar{0}$

ex) $\underline{p=5}$: $-\bar{a} = ?$ for $\bar{a} = \bar{2}$

$-\bar{a} = \bar{3}$

Define multiplication by $\bar{a} \cdot \bar{b} = \overline{ab}$ (Check this is well-defined)

Lemma: Let $a, b \in \mathbb{Z}$ and let $d = \gcd(a, b)$
There exist integers n_1, n_2 such that
$n_1 a_1 + n_2 b = d$

Note: If p is prime then $a \neq 0$ $(1 \leq a < p)$ $\gcd(a, p) = 1$

$\Rightarrow \exists n_1, n_2$ such that

$$n_1 a + n_2 p = 1$$

reduce mod p

$\Rightarrow$ in $\mathbb{F}_p$ $\quad \overline{n_1}\,\overline{a_1} + \overline{0} = \overline{1} \Rightarrow \overline{n_1}\,\overline{a_1} = \overline{1}$

This n_1 is the multiplicative inverse.

ex) $p=5$ $\quad a^{-1} = ?$ for $a=2$ $\quad a^{-1} = 3$

Non-examples:

1) $\mathbb{Z}_n$ for n not prime

2) $\mathbb{N}$ or $\mathbb{Z}$

Def: Something "different" about $\mathbb{R}$ vs $\mathbb{F}_p$

- Note that $1_{\mathbb{R}} + 1_{\mathbb{R}} + \cdots + 1_{\mathbb{R}} \neq 0_{\mathbb{R}}$

• However! $\underbrace{1_{\mathbb{F}_p} + \cdots + 1_p}_{p\text{-times}} = 0$

$\Rightarrow$ True in general: Only 1 of two things happen

1) Either $\exists n$ st $n \cdot 1_{\mathbb{F}} = 0$

2) $n \cdot 1_{\mathbb{F}} \neq 0$

Case 1: The smallest n st $\overbrace{1 + \cdots + 1}^{n\text{-times}}$ is called the characteristic

Case 2: $\mathbb{F}$ said to be of characteristic 0 ex) i) $\mathbb{F} = \mathbb{C} \longrightarrow$ char 0

ii) $\mathbb{F} = \mathbb{F}_{17} \longrightarrow$ char 17

Lemma: For any field $\mathbb{F}$, $0_{\mathbb{F}}\, a = 0_{\mathbb{F}}$ $\forall a$

Pf) $0_{\mathbb{F}} a = (0_{\mathbb{F}} + 0_{\mathbb{F}}) a = 0_{\mathbb{F}} a + 0_{\mathbb{F}} a$

Subtract by $(-0_{\mathbb{F}} a)$ to both sides

$$-0_{\mathbb{F}}a + 0_{\mathbb{F}}a = -0_{\mathbb{F}}a + 0_{\mathbb{F}}a + 0_{\mathbb{F}}a$$

$$\Rightarrow 0_{\mathbb{F}} = -0_{\mathbb{F}} + 0_{\mathbb{F}}a$$

$$= 0_{\mathbb{F}}a$$

HW Q: For $a, b \in \mathbb{F}$, if $ab = 0_{\mathbb{F}}$ then $a = 0$ or $b = 0$

(show that if n not prime $\mathbb{Z}/n$ is not a field)

Quik Vector on polynomials

- we will see, many questions in this class really boil down to the existance of a root for some polynomial p.

- Certain Fields are "better behaved" in this respect

<u>Def</u>: $\mathbb{F}$ a field, say $\mathbb{F}$ is <u>algebraically closed</u> if for any (monic) <u>polynomial</u>

$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{F}$

$\exists\, \alpha \in \mathbb{F}$ called a <u>root</u> of p

such that $p(\alpha) = 0_{\mathbb{F}}$ $x^2 - 1$

ex) $\mathbb{Q}$? x^2+1 no roots

$\mathbb{R}$? x^2+1 x^2-2 has a root in $\mathbb{R}$, not $\mathbb{Q}$

$\mathbb{C}$ = :) yes alg closed

$\mathbb{F}_p$? turns out not alg closed.

2nd Generalization

• Now we can ask for a generalization of the "vectors"

Def: Let $\mathbb{F}$ be field. Then a Vector Space over $\mathbb{F}$ is a set V with 2 operations

$$V \times V \xrightarrow{+_V} V \qquad \mathbb{F} \times V \xrightarrow{\cdot} V$$

$$(v, w) \longmapsto v + w \qquad (\alpha, v) \longmapsto \alpha v$$

such that

(A1) For $u, v, w \in V$

$$u +_V (v +_V w_V) = (u +_V v) +_V w$$

(A2) For $u, v \in V$

$$u +_V v = v +_V u$$

(A3) $\exists$ element $\underline{0_V}$ such that, $\forall v \in V$

$$v + 0_V = v$$

(A4) $\forall v$, $\exists$ $\underline{(-a)}$ such that

$$a + (-a) = 0$$

(S1) $\forall v \in V$, $1_{\mathbb{F}} v = v$

(S2) $\forall a, b \in \mathbb{F}$, $v \in V$

$$(a +_{\mathbb{F}} b) v = av +_V bv$$

(S3) $\forall a \in \mathbb{F}$, $v, w \in V$

$$a(v +_V w) = av +_V aw$$

Lemma: A Vector-Space has a unique 0_V

Pf) Assume $\exists \tilde{0}$ another 0-vector in V

$$0_V = \tilde{0} + 0_V = \tilde{0}_V$$

So $0_V = \tilde{0}_V$

HW) 1) Additive inverses are unique

2) $0_{\mathbb{F}} \cdot v = 0_V \quad \forall v \in V$

3) $a 0_V = 0_V \quad \forall a \in \mathbb{F}$

examples

1) Let $\mathbb{F}$ be any field, then the set

$$\underline{\mathbb{F}^n} = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_i \in \mathbb{F} \right\}$$

math 21

is a vector space over $\mathbb{F}$ with

a) $$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{pmatrix}$$

b) $$c \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ca_1 \\ \vdots \\ ca_n \end{pmatrix} \quad c \in \mathbb{F}$$

2) Again, let $\mathbb{F}$ be field, then

$$M_{m\times n}(\mathbb{F}) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} : a_{ij} \in \mathbb{F} \right\}$$

is a vector space over $\mathbb{F}$ with

a) $m_1 = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$, $m_2 = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ & & \\ b_{m1} & \cdots & b_{mn} \end{pmatrix}$

$m_1 + m_2 = (a_{ij} + b_{ij})$

b)

$c m_1 = (c a_{ij})$ componentwise

3) Let $n \in \mathbb{N}$. The set

$$\mathbb{F}[t]_{\leq n} = \left\{ a_n t^n + \cdots + a_1 t + a_0 \;\middle|\; a_i \in \mathbb{F} \right\}$$

is a vector space over $\mathbb{F}$

4) Let S be any set and $\mathbb{F}$ a field. The set

$$\mathrm{Fct}(S, \mathbb{F}) = \left\{ f: S \to \mathbb{F} \;\middle|\; f \text{ function} \right\}$$

is a vector space over $\mathbb{F}$ with

a) $f_1 : S \to \mathbb{F}$ and $f_2 : S \to \mathbb{F}$

$$(f_1 + f_2)(s) := f_1(s) +_{\mathbb{F}} f_2(s)$$

Q: What is the 0 vector? A: $0 : S \to \mathbb{F}$

$0(s) = 0_{\mathbb{F}}$

b) Given $c \in \mathbb{F}$ and $f : S \to \mathbb{F}$

$$(cf)(s) := c f(s)$$

5) Variations on (4). Let $X \subseteq \mathbb{F}^n$, consider $\mathrm{Fct}(X, \mathbb{F})$.

- cts functions : $CTS(X, \mathbb{F}) = C^0(X, \mathbb{F})$
- diff functions $Diff(X, \mathbb{F}) = C^1(X, \mathbb{F})$

- smooth functions $\mathrm{Sm}(X, \mathbb{F}) = \mathcal{C}^{\infty}(X, \mathbb{F})$

$\rightsquigarrow$ these are all subsets...

$$\mathrm{Sm}(X, \mathbb{F}) \subseteq \mathrm{Diff}(X, \mathbb{F}) \subseteq \mathrm{Cts}(X, \mathbb{F}) \subseteq \mathrm{Fct}(X, \mathbb{F})$$

$\rightsquigarrow$ Leads to notion of Subspaces

Next time!