Math 117 Section

Email: darubins@ucsc.edu

Topics thus far

- Def of field
    - examples of fields ($\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Q}$)

      $\mathbb{F}_p = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}$
    - basic properties of fields

ex) Char of field $= \begin{cases} 0 & \text{if } n \cdot 1 \neq 0 \text{ for all } n \\ p & \text{if } p \cdot 1 = 0 \end{cases}$

- If $ab = 0$ in $\mathbb{F}$ then either a or b are zero.

- Alg closed fields

  ex) $\mathbb{C}$ (fundamental thm of algebra)

  non-example) $\mathbb{Q}$, $\mathbb{R}$ and in HW show $\mathbb{F}_p$

  $f(x) = x^2 + 1$

- Def of vector space

  - examples: $\mathbb{R}^n$

    - $\mathbb{F}^n$ for $\mathbb{F}$ field.

  Q: Is $\mathbb{Z}^n$ a real? rational vector space?

  ex) $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ and $\bar{5} = \bar{2}$

  No! Only a module.

- $M_{m\times n}(\mathbb{F})$ = the set of all $m\times n$ matrices with entries in $\mathbb{F}$.
- $\mathbb{F}_n[x]$ = the set of all polynomials up to degree n (w/ coefficients in $\mathbb{F}$)
- $\mathbb{F}[x]$ = the set of all polynomials

- **Linear transf**

Let V, W be vector spaces.

Def: Then a linear transformation $T: V \to W$ is a function st

1) $T(v+w) = T(v) + T(w)$
2) $T(cv) = cT(v)$

Exc: Show T linear then $T(0_v) = 0_w$

ex) $V = \mathbb{C}^3$ and $W = \mathbb{C}_2[x]$

$T: V \to W$ defined by

$$T\left(\begin{pmatrix} a \\ b \\ c \end{pmatrix}\right) = a + bx + cx^2$$

Check: Show $T\left(\begin{pmatrix}1\\1\\1\end{pmatrix} + \begin{pmatrix}2\\2\\2\end{pmatrix}\right) \neq T\begin{pmatrix}3\\3\\3\end{pmatrix}$

Check: T is a linear transformation.

$$T\left(\begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} + \begin{pmatrix} a_2 \\ b_2 \\ c_2 \end{pmatrix}\right) = T\left(\begin{pmatrix} a_1+a_2 \\ b_1+b_2 \\ c_1+c_2 \end{pmatrix}\right)$$

$$= (a_1+a_2) + (b_1+b_2)x + (c_1+c_2)x^2$$

$$= a_1 + b_1x + c_1x^2 + a_2 + b_2x + c_2x^2 = T\begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} + T\begin{pmatrix} a_2 \\ b_2 \\ c_2 \end{pmatrix}$$

Non ex: $V = \mathbb{C}^3$ $W = \mathbb{C}_2[x]$

$$T\left(\begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix}\right) = 2 + (a_1+b_1)x + c_1x^2$$

- Subspace

Q: Is $\{f : \mathbb{R} \to \mathbb{R} \text{ differentiable} \mid f(1) = 1\}$ $= S$

a subspace of Diff($\mathbb{R}, \mathbb{R}$)?

Check: Let $f, g \in S$. Q: Is $(f+g) \in S$?

$$(f+g)(x) \stackrel{\text{def}}{=} f(x) + g(x)$$

Then $(f+g)(1) = f(1) + g(1) = 2 \neq 1 \notin S$.

- **Span**: Let $v_1 \ldots v_n$ in V. The set of all linear combinations of $v_1 \ldots v_n$ is the span of $v_1 \ldots v_n$: $\underline{\text{span}(v_1 \ldots v_n)}$
  - If $\text{span}(v_1 \ldots v_n) = V$ we say the vectors span V
- **LI**: Let $v_1 \ldots v_n$ be vectors V. We say they are Linearly independent if the only solution to

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0$$

is

$$a_1 = a_2 = \ldots = a_n = 0.$$

ex) $V = \mathbb{R}^2$ $\quad v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\quad v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\quad v_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

are NOT LI in $\mathbb{R}^2$

$1v_1 + 1v_2 - v_3 = 0_V$

$\begin{pmatrix} 2 \\ 3 \end{pmatrix} \in \text{Span}(v_1, v_2, v_3)$: $\begin{pmatrix} 2 \\ 3 \end{pmatrix} = 2v_1 + 3v_2$

$\begin{pmatrix} 2 \\ 3 \end{pmatrix} = 2v_3 + v_2$

- Dimension: size of a basis.

Q: Is there a vector space without a basis?

No - try to prove this. (uses the axiom of choice)

- Gauss-Jordan but in $\mathbb{F}_p$

Q: Why must we have p prime in $\mathbb{F}_p$?

If n not prime then can $\mathbb{F}_n$ be field?

If not prime it! (hint, think about properties of fields we mentioned today)

(hint 2: work it out in concrete examples if you are stuck)

Pigeonhole Principle

" Suppose that $n > m$. If there are n-pigeons and m holes, then there will be at least 1 hole with 2 pigeons "

i.e., 2 things (at least) will "be equal"

ex) How many nonzero elements in $\mathbb{F}_5$? $= 4$

Consider $\bar{2}$ in $\mathbb{F}_5$.

Consider $\bar{2}^0 \quad \bar{2}^1 \quad \bar{2}^2 \quad \bar{2}^3 \quad \bar{2}^4$

Q1) Are any of these $= \bar{0}$? No!

Q2) Explain why $\overline{2}^i = \overline{2}^j$ for some i, j

Above is list of 5 numbers.

Q3) Explain how this shows $\exists\, n \le p-1$ st

$2^n = 1 \mod 5$

Assume $i > j$ $\quad \overline{2}^{i-j} = \overline{1}$

$$\|$$

$2^{i-j} \equiv 1 \mod 5$ $\quad \square$