LECTURE 10

(Fri. JAN. 31, 2020)

Recall: $A \sim B$ means A, B represent the same lin. transformation $T: \mathbb{R}^n \to \mathbb{R}^n$ w.r.t. different bases.

(numbers)

"invariant": $\det(B) = \det(CAC^{-1}) = \det(C)\det(A)\det(C^{-1}) = \det(A)$.

i.e.,

$$A \sim B \Rightarrow \det(A) = \det(B)$$

(same for trace) — can use to show not similar:

$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $B = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$ are not similar

($\det A = -2$, $\det B = 5$)

EX $A \in M_2(\mathbb{R})$ with two eigenvalues $\alpha \neq \beta$.

Then A is similar to $D = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ "diagonalization".

– remember, eigenvectors: $u, v \in \mathbb{R}^2$ sat.

$$Au = \alpha u \quad \text{and} \quad Av = \beta v.$$

Letting $C = (u \ v)$ this says $AC = CD$.

I.e., $A = CDC^{-1}$.

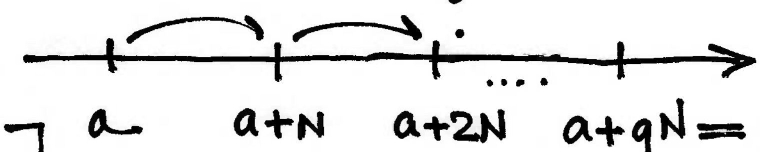
(C invertible? otherwise u, v proportional, but $\alpha \neq \beta$)

<u>EX</u> (congruences) Fix an $N \in \mathbb{N}$. Use it to define a relation on $\mathbb{Z}$ by: For $a, b \in \mathbb{Z}$,

$a \equiv b \pmod N$ <u>means</u> $N \mid (a-b)$

– i.e., can write $b = a + qN$ for some $q \in \mathbb{Z}$.

"go from a to b with steps of length N".



– Claim it's an <u>equivalence relation</u>:

- <u>reflexive</u>:

  $a \equiv a \pmod N$

  [indeed N divides $0 = a - a$]

- <u>symmetric</u>: $a \equiv b \pmod N \Longrightarrow b \equiv a \pmod N$.

  [we're assuming $b = a + qN$. Then $a = b + \underbrace{(-q)}_{\in \mathbb{Z}} N$.]

- <u>transitive</u>:

  $a \equiv b \pmod N \wedge b \equiv c \pmod N \Longrightarrow a \equiv c \pmod N$

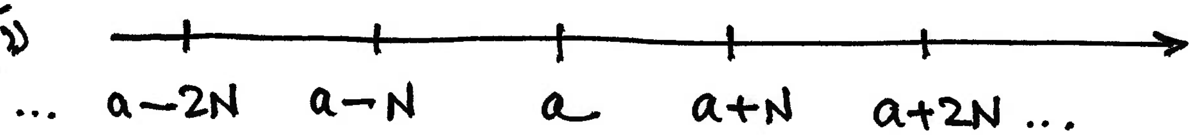
  [here $b = a + qN$ and $c = b + pN$, some $p, q \in \mathbb{Z}$. implies $c = (a + qN) + pN = a + \underbrace{(p+q)}_{\in \mathbb{Z}} N$.]

In this ex. equiv. classes are called "<u>residue</u> <u>classes</u>": $a \in \mathbb{Z}$,

$$[a] = \{ b \in \mathbb{Z} : b \equiv a \pmod N \}$$

$$[a] = \{b \in \mathbb{Z} : \ b = a + qN \text{ for some } q \in \mathbb{Z}\}$$
$$= \{a + qN : \ q \in \mathbb{Z}\}$$
$$= \{a, a \pm N, a \pm 2N, a \pm 3N, \dots\}.$$

"arithmetic progression"



These "boxes of numbers" form a partition of $\mathbb{Z}$.

- $N = 2$: $\mathbb{Z} = [0] \cup [1]$.

  even — odd.

- $N = 3$: $\mathbb{Z} = [0] \cup [1] \cup [2]$ — cf. previous lectures. ($A \cup B \cup C$)

  $3q$ — $3q+1$ — $3q+2$

(in general we'll have N boxes).

Rk. From the general theory, $a, b \in \mathbb{Z}$ def. the same class precisely when they're congruent.

I.e., $$[a] = [b] \iff a \equiv b \pmod{N}.$$