Let $\mu(n)$ be the sum of the <u>primitive</u> n^{th} roots of unity. (\mu)

$\boxed{\text{HW}}$ (1) evaluate $\mu(1), \mu(2), \ldots, \mu(6), \mu(p)$ with p prime.

(2) Prove: $(\forall n)(\mu(n) \in \mathbb{Z})$

$\boxed{\text{CH}}$ Prove: $(\forall n)(\mu(n) \in \{0, \pm 1\})$

Hint for HW from yesterday!

def (circulant)

$$C(a_0, a_1, \ldots, a_{n-1}) = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \\ & \ddots & \ddots & \ddots \\ & & \ddots & a_1 \\ a_1 & a_2 \cdots & a_{n-1} & a_0 \end{pmatrix}$$

$$= \Pi(\text{linear forms in the } a_i)$$

$$\overset{\wedge}{\alpha_0 a_0 + \cdots + \alpha_{n-1} a_{n-1}} \quad \alpha_i \in \mathbb{C}.$$

$n=2$ $$\begin{vmatrix} a_0 & a_1 \\ a_1 & a_0 \end{vmatrix} = a_0^2 - a_1^2 = (a_0 + a_1)(a_0 - a_1).$$

Wednesday, July 12, 2017 9:37 AM

Hint. $C(a_0, a_1, \dots, a_n)$ is a polynomial of the cyclic shift matrix.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\begin{tikzcd} e_0 \arrow[r, mapsto] & e_1 \arrow[r, mapsto] & \cdots \arrow[r, mapsto] & e_{n-1} \arrow[lll, bend left, mapsto] \end{tikzcd}$$

$\varphi: V \to V$ dim $= n$

all n eigenvalues are distinct

$\boxed{\text{HW}}$ What is the # of φ-invariant subspaces? (Prove your answer - should be very simple function of n.)

$A \in M_n(\mathbb{R}) \overset{?}{\Longrightarrow} A \sim$ ◥ $\in M_n(\mathbb{R})$.

T/F - If $A \in M_n(\mathbb{R})$

No. If $A \sim$ ◥ $\in M_n(\mathbb{R})$, then eigenvalues must be real (along diagonal), so any matrix that has a non-real eigenvalue will not work (e.g. the rotation matrix.)

Wednesday, July 12, 2017 9:45 AM

DO $A \in M_n(\mathbb{R})$ and all eigenvalues are real $\Rightarrow$

$A \sim ◥ \in M_n(\mathbb{R})$

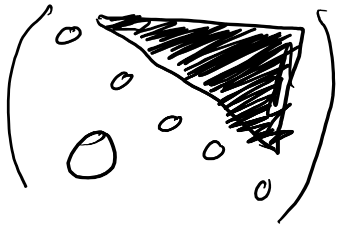
This holds for any number field $\mathbb{F}$:

If $A \in M_n(\mathbb{F})$ and all eigenvalues $\in \mathbb{F} \Rightarrow$

$A \sim ◥ \in M_n(\mathbb{F})$.

Def. $N \in M_n(\mathbb{F})$ is *nilpotent* if $(\exists k)(N^k = 0)$.

DO Every strictly upper triangular matrix is nilpotent.



HW N is nilpotent $\iff$ $f_N(t) = t^n$.

HW N is nilpotent $\iff$ $N \sim$ strictly upper triangular matrix.

(do not use 2nd for 1st)

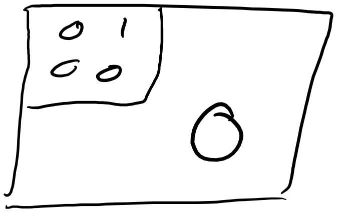
HW If N is nilpotent, then $I + N$ is nonsingular.

Wednesday, July 12, 2017 9:51 AM

$\boxed{\text{HW}}$ Find a nilpotent 2x2 matrix N and nonsingular diagonal matrix D s.t. D+N is singular.

(A diagonal matrix is nonsingular is all the diagonal elements are nonzero)

DO If N is nilpotent, $N^n = 0$.



$N^2 = 0$.

Thm. If $A \in M_n(\mathbb{C})$ then $A \sim \text{diag}(B_1, \dots, B_k)$.

proto-Jordan normal form

↓

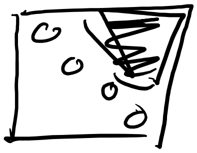
block-diagonal matrix - diagonal blocks are square and of the form

B_1	0	0	0
0	B_2	0	0
0	0	B_3	0
0	0	0	B_4

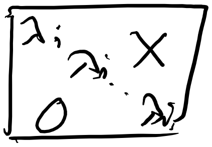
$B_i = \lambda_i I + N_i$

where N_i is strictly upper triangular $\lambda_i \neq 0$.

N_i :



B_i :



Wednesday, July 12, 2017 9:59 AM

<u>Def.</u> (direct sum of subspaces)

$V = U_1 \oplus U_2 \qquad U_i \leq V \quad i = 1, 2$

if $(\forall v \in V)(\exists u_1, u_2)(u_i \in U_i \text{ and } v = u_1 + u_2)$

in particular $V = U_1 + U_2$.

<u>e.g.</u> G_3 : xy-plane and z-axis.

DO $V = U_1 \oplus U_2 \iff V = U_1 + U_2$ and $U_1 \cap U_2 = \{0\}$.

DO If $U_1 \oplus U_2 = V$ then
$\dim V = \dim U_1 + \dim U_2$

<u>Proof.</u> Pick bases of U_1, U_2 and show these combined form a basis of V.

<u>Def.</u> $V = U_1 \oplus \cdots \oplus U_k \qquad U_i \leq V \quad \forall i \in [k]$

if $(\forall v \in V)(\exists!\, u_1, \ldots, u_k)(u_i \in U_i \text{ and } v = \sum_{i \in [k]} u_i)$.

DO If $V = \bigoplus_{i=1}^{k} U_i$ then $\dim V = \sum_{i=1}^{k} \dim U_i$.

Wednesday, July 12, 2017 10:05 AM

DO

$V = U_1 \oplus \cdots \oplus U_k \iff$

(1) $V = U_1 + U_2 + \cdots + U_k$

(2) ?

Intersection 0 ? xy, yz, xz planes intersect only at 0.. but only need 2 distinct planes to create space

Pairwise intersection 0 ? 3 different lines have pairwise intersection 0.. but only need 2 lines on $\mathbb{R}^2$

$$(2) \quad (\forall i)\Big(U_i \cap \sum_{\substack{j \\ j\neq i}} U_j = \{0\}\Big)$$

HW $\varphi: V \to V$ $U_\lambda = \{x \in V \mid \varphi(x) = \lambda x\}$

eigensubspace to λ

Then $\sum_\lambda U_\lambda = \bigoplus_\lambda U_\lambda$.

(verify second condition from above.)

Wednesday, July 12, 2017 10:16 AM

$\boxed{\text{DO}}$ $A \in M_n(\mathbb{F})$ is diagonalizable $\iff \sum U_\lambda = \mathbb{F}^n$.

<u>Lemma</u> If $f = g \cdot h$ with $\gcd(g, h) = 1$, $\boxed{\text{HW}}$

$\varphi : V \to V$ and $f(\varphi) = 0$, (for Monday.)

then $V = \ker(g(\varphi)) \oplus \ker(h(\varphi))$

(Ask for a hint on Friday.)

(Pre-hint: uses a fact about gcd.)

Predicate over a set Ω:

$f : \Omega \to \{0, 1\}$

1	Yes	True
0	No	False

A <u>relation</u> over Ω is a predicate over $\Omega \times \Omega$:

<u>Examples</u>: $\Omega = \mathbb{R}$ $\quad f(x, y) = \begin{cases} 1 & \text{if } x < y \\ 0 & \text{o/w} \end{cases}$ $\downarrow$

$<(x, y) = 1$

similar $\downarrow$

Ω = geometric shapes $\quad f(x, y) = \begin{cases} 1 & \text{if } x \sim y \\ 0 & \text{o/w} \end{cases}$ $\downarrow$

$\sim(x, y) = 1$.

$\Omega = \{\text{humans}\}$ "x is a parent of y"

Properties of some relations $R \to xRy$

Reflexive: $(\forall x)(xRx)$

ex: $\leq$, $\sim$, ~~parent~~

Symmetric: $(\forall x, y)(xRy \Rightarrow yRx)$

ex: $\cancel{\leq}$, $\sim$, ~~parent~~

Transitive: $(\forall x, y, z)(xRy \text{ and } yRz \Rightarrow xRz)$.

ex: $\leq$, $\sim$, ~~parent~~ (ancestor ✓)

irreflexive, $(\forall x)(x \not R x)$

irreflexive, symmetric $\}$ graph (adjacency relation)

Def R is an equivalence relation if R is reflexive, symmetric, and transitive.

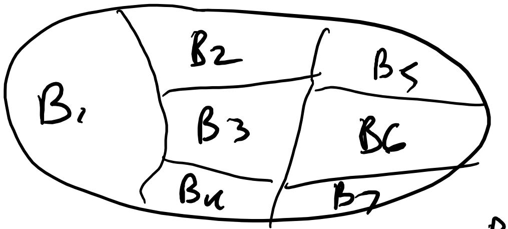
ex: similarity ($\sim$), having the same parents "sibling or equal", residing in the same state.

Wednesday, July 12, 2017 10:34 AM

Partition of a set Ω:

$\Omega = B_1 \,\dot\cup\, \cdots \,\dot\cup\, B_k$ into disjoint blocks:

$B_i \cap B_j = \emptyset \quad \forall i, j,\ i \neq j$ and $B_i \neq \emptyset.\ \forall i$



$$\underset{\substack{\uparrow \\ \text{partition}}}{\Pi} = \{\underbrace{B_1, \ldots, B_k}_{\text{blocks of partition}}\}$$

"Partition of Poland" - Russia, Germany, Austria

Π : partition of Ω

→ defines an equivalence relation $\sim_\pi$

Suppose $\pi = \{B_1, \ldots, B_k\}$

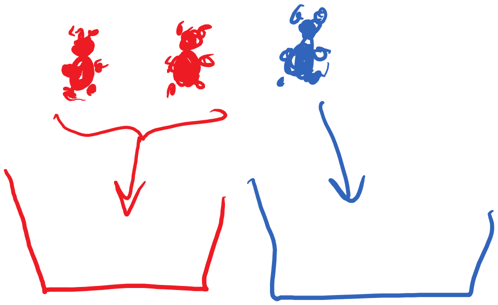
Def $x \sim_\pi y$ $(x, y \in \Omega)$ if $(\exists i)(x, y \in B_i)$.

Thm (Fundamental Theorem of Equivalence Relations ...

$\forall$ eq. relation R over Ω, $\exists!$ partition π of Ω s.t. $R = \sim_\pi$.

and of human concept forming.)

Wednesday, July 12, 2017 10:34 AM



Every equivalence relation creates a new concept

3 : {3 cows, 3 trees, --- }

mother: {my mother, your mother, his mother --- }

Rational number: $\frac{3}{5}$ $\frac{6}{10}$

$(3,5)$ $(6,10)$

$\frac{a}{b} \sim \frac{c}{d}$ if $ad = bc$.

DO Prove this is an equivalence relation on pairs (a,b) s.t $b \neq 0$.

Equivalence classes of pairs are the rationals.

↳ Blocks of the partition that correspond to this eq. relation.

Def $\mathbb{Z}$ $a \underset{\uparrow \text{ congruent / congruence}}{\equiv} b \mod m$ (a \equiv b \pmod{m})

if $m \mid a-b$.

(DO) Fix m. Then mod m congruence is an equivalence relation on $\mathbb{Z}$.

Residue classes mod m: equivalence classes.

mod 2 residue classes: $\mathbb{Z} = \underbrace{2\mathbb{Z}}_{\text{evens}} \dot{\cup} \underbrace{2\mathbb{Z}+1}_{\text{odds}}$

mod 3 residue classes: $\mathbb{Z} = 3\mathbb{Z} \dot{\cup} 3\mathbb{Z}+1 \dot{\cup} 3\mathbb{Z}+2$

-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
	$\vdots$	

residue classes <u>mod m</u> is $|m|$.

(Note: $x \equiv y \mod 0 \Leftrightarrow x = y$, so each # forms its own class — the definition above works if we think of 0 as infinity.)

$\boxed{\text{DO}}$ $(x+y)^p \equiv x^p + y^p \mod p$ (p prime.)

Back to proof of Thm

<u>Thm</u> (proto - Jordan normal form)

$$A \in M_n(\mathbb{C}) \Rightarrow A \sim \begin{pmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_k \end{pmatrix}$$

where B_i is $n_i \times n_i$

and $B_i = \lambda_i I_{n_i} + N_i$

$\uparrow$ strictly upper triangular

<u>Proof.</u> $\dim_{\mathbb{C}} V = n$ and $[\varphi]_{\underline{e}} = A$.

$V = U_1 \oplus U_2$

$$\begin{array}{c|c|c|} \hline U_1 \{ & \varphi|_{U_1} & 0 \\ \hline U_2 \{ & 0 & \varphi|_{U_2} \\ \hline & U_1 & U_2 \end{array}$$

$\varphi : V \to V$

U_1 and U_2 φ-invariant

$\varphi = \varphi_1 \oplus \varphi_2$

where $\varphi_i = \varphi|_{U_i}$.

$\varphi(u_1 + u_2) = \varphi_1(u_1) + \varphi_2(u_2)$

Wednesday, July 12, 2017 11:14 AM

$f_\varphi := f_{[\varphi]_g}$ where g is any basis (does not depends on basis b/c similar matrices have same char. poly.)

$= \prod (t-\lambda_i)^{n_i}$ ↑ algebraic multiplicities

$$= \underbrace{(t-\lambda_1)^{n_1}}_{g} \cdot \underbrace{\prod_{j\neq 1} (t-\lambda_j)^{n_j}}_{h}$$

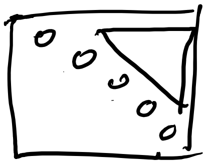
g, h rel prime - no common roots

$f_\varphi(\varphi) = 0$ ✓

$U_1 = \ker(g(\varphi))$

$\varphi|_{U_1} = \varphi_1 \rightarrow (\varphi_1 - \lambda_1 I)^{n_1} = 0 \Rightarrow$ on U_1 : $\varphi_1 - \lambda I$ is nilpotent

def of kernel :

$[\varphi_1 - \lambda_1 I]_{f_1} =$ 

new basis of U_1

$[\varphi]_{\underline{f}} = \lambda_1 I + N_1 = B_1$

By induction on # of distinct eigenvalues, we are done □

$\boxed{\text{HW}}$ (for Mon):

$A \in M_n(\mathbb{C})$ w/ eigenvalues $\lambda_1, \ldots, \lambda_n$.

Prove: if $(\forall i)(|\lambda_i| < 1)$ then

$$\lim_{k \to \infty} A^k = 0.$$

Ring: set R with $+$, $\cdot$, normal properties (associativity, distributivity, ...)

$(R, +)$ abelian group

$(R, +, \cdot)$ $\cdot$ assoc. distributes over addition

$\mathbb{Z}$ is a ring.

Commutative ring: $(\forall a, b)$ $a \cdot b = b \cdot a$

$M_n(\mathbb{F})$ is a non-commutative ring.

Ring with identity:

$\exists 1$ s.t. $(\forall a \in R)(1 \cdot a = a \cdot 1 = a)$

$2\mathbb{Z}$ is a ring without identity.

DO $0 \cdot a = a \cdot 0 = 0$.

An integral domain is a commutative ring s.t. $(\forall a, b)(ab = 0 \iff a = 0$ or $b = 0)$.

$\mathbb{Z}$ mod 6 is not an integral domain.

$2 \cdot 3 = 0$.

$M_n(\mathbb{F})$ not either: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

A field $\mathbb{F}$ is a commutative ring with identity $1 \neq 0$

s.t. $(\forall a \in \mathbb{F})(a \neq 0 \Rightarrow \exists \underset{\Uparrow}{\frac{1}{a}})$

a^{-1}: multiplicative inverse

Cor $\mathbb{F}^{\times} = \mathbb{F} \setminus \{0\}$

$(\mathbb{F}^{\times}, \underset{\uparrow}{\times})$ is an abelian group.

multiplication

Ex. number fields, integers mod p (p prime)

$\boxed{\text{HW}}$ (for Mon.) If R is a finite integral domain with $|R| \geq 2$, then R is a field

<u>Notation:</u> If π is a partition of Ω then Ω/π is a set of blocks (eq. classes),
If R is an equivalence relation on Ω then Ω/R is a set of blocks (eq classes)

$\mathbb{Z}/m\mathbb{Z}$ set of mod m residue classes.
(eq. relation: congruence mod m) for $m \geq 1$:

$$|\mathbb{Z}/m\mathbb{Z}| = m.$$

$\forall x \in \Omega$, $[x]$ is the equivalence class of x.

Define $\underbrace{+, \cdot}_{\downarrow}$ on $\mathbb{Z}/m\mathbb{Z} \rightarrow$ commutative ring w/identity

by representatives

$a \in \mathbb{Z} \rightarrow [a] = a + m\mathbb{Z}$ (residue class of a; a is a representative)

Wednesday, July 12, 2017 11:39 AM

Mod 7

-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

$(2+7\mathbb{Z}) = (9+7\mathbb{Z})$

$(-3+7\mathbb{Z}) = (11+7\mathbb{Z})$

$$\begin{array}{rcl} & 2+7\mathbb{Z} = 9+7\mathbb{Z} & ☆ \\ \oplus & -3+7\mathbb{Z} = 11+7\mathbb{Z} & ☆ \\ \hline & -1+7\mathbb{Z} = 20+7\mathbb{Z} & ☆ \end{array}$$

If $a \equiv b \mod m$ and $u \equiv v \mod m$,

then:

- $a+u \equiv b+v \mod m$
- $a \cdot u = b \cdot v \mod m$

This defines arithmetic on residue classes.

DO $\mathbb{Z}/m\mathbb{Z}$ forms a commutative ring with identity.

Wednesday, July 12, 2017 11:44 AM

$\boxed{\text{DO}}$ $\mathbb{F}$ field $\Rightarrow$ $\mathbb{F}$ integral domain.

NTS: $ab=0 \Rightarrow a=0$ or $b=0$.

Suppose $a \neq 0$. NTS $b=0$.

multiply by a^{-1}:

$$a^{-1}ab = a^{-1}\cdot 0$$

$$b = a^{-1}(ab) = a^{-1}\cdot 0 = 0$$ □

When is $\mathbb{Z}/m\mathbb{Z}$ an integral domain?

iff m is prime.

Ex. $\mathbb{Z}/6\mathbb{Z}$: $2\cdot 3 = 0$.

$\mathbb{Z}/p\mathbb{Z}$ is integral domain?

$a \in \mathbb{Z}$

$\underline{a}$: residue class $a + p\mathbb{Z}$.

Suppose $\underline{a}\cdot\underline{b} = \underline{0}$

NTS: $\underline{a} = \underline{0}$ or $\underline{b} = \underline{0}$.

$e, a \in \mathbb{Z}$, $\underline{a} = a + m\mathbb{Z}$

$e \in \underline{a} \Leftrightarrow$

$e \equiv a \mod m$

$e \in \underline{0} \Leftrightarrow$

$e \equiv 0 \mod m$

$\Leftrightarrow m \mid e$

Note $\boxed{\underline{a}\cdot\underline{b} = \underline{a\cdot b}}$ (definition of multiplication of residue classes)

So $\underline{a}\cdot\underline{b} = \underline{0} \iff ab \in \underline{0} \iff m \mid ab$

NTS: for $m=p$, $\underline{a}\cdot\underline{b} = \underline{0}$ then $\underline{a}$ or $\underline{b} = \underline{0}$.

<u>i.e.</u> $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

(True - prime #s have the prime property.)

So then $a \in \underline{0}$ or $b \in \underline{0}$.

□

Thus $\underline{a} = \underline{0}$ or $\underline{b} = \underline{0}$.

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ finite field of order p. → # of elements

<u>Thm</u> If $\mathbb{L}$ is a finite field, then $|\mathbb{L}|$ is a prime power

Let R be an <u>integral domain</u>. $|R| \geq 2$.

For $a \in R$ let $n_a = \gcd(k \mid \underbrace{ka}_{\underbrace{a+a+\cdots+a}_{k \text{ times}}} = 0)$

$\mathrm{Ann}(a) = \{k \in \mathbb{Z} \mid ka = 0\} \leq \mathbb{Z}$

↑ annihilator of $\underline{a}$

↑ subgroup.

$\mathrm{Ann}(a) = n_a \mathbb{Z}$

DO For $a \neq 0$, n_a does not depend on a.

DO n_a is $\underline{\text{prime}}$ or $\underline{0}$.

↓ $\underline{\text{characteristic}}$ of R.

$\underline{\text{Ex}}$. $\mathrm{char}(\mathbb{Z}) = 0$

$\mathrm{char}(\mathbb{R}) = 0$

$\mathrm{char}(\mathbb{F}) = 0$

$\mathrm{char}(\mathbb{F}_p) = p$ (p prime)

HW If $\mathrm{char}\,\mathbb{F} = p$, then $(a+b)^p = a^p + b^p$.

($\mathbb{F}$ integral domain.)

DO If $\mathrm{char}\,\mathbb{F} = p$, then $\mathbb{F} \geq \mathbb{F}_p$

↑ int domain, $|\mathbb{F}| \geq 2$

↑ subdomain

<u>Proof</u> ($\mathbb{L}$ finite field $\Rightarrow$ $|\mathbb{L}|$ is prime power)

char $\mathbb{L} \neq 0$ if $\mathbb{L}$ is finite $\boxed{\text{DO}}$,

so char $\mathbb{L} = p$.

$\Rightarrow \mathbb{L} \supset \mathbb{F}_p$ subfield.

$\therefore$ $\mathbb{L}$ is a vector space over $\mathbb{F}_p$.

$\dim_{\mathbb{F}_p} \mathbb{L} =: d$

$$\begin{bmatrix} a_1 \\ \vdots \\ a_d \end{bmatrix}$$

$\mathbb{L}$ as a $\mathbb{F}_p$ - space $\cong \mathbb{F}_p^{\,d}$

$|\mathbb{L}| = |\mathbb{F}_p^{\,d}| = p$. □

<u>Thm.</u> (Galois)

$\forall$ prime power q $\exists!$ field $\mathbb{F}_q$ of order q.

$p^2 = q$ $\quad \mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$

q not prime, so $\mathbb{Z}/q\mathbb{Z}$ is not an integral domain and thus not a field

Wednesday, July 12, 2017 12:11 PM

$$\mathbb{F}_p[\underbrace{\sqrt{-1}}_{i}] = \{a+bi \mid a,b \in \mathbb{F}_p,\ i^2=-1\}$$

commutative ring with identity of order p^2

For what primes is this a field?

$$\left.\begin{array}{l}\text{① experiment}\\ \text{② discover pattern}\\ \text{③ make conjecture}\end{array}\right\}\ \boxed{\text{HW}}\ \text{(for Mon).}$$

④ prove it. $\boxed{\text{CH}}$