Problem Session

Prove $rk(A^TA) = rk(A)$

Elementary row/col operations preserve rank.

Let $rk(A) = m$.

Use elementary row operations to transform A:

$$E_1 \cdots E_t A = \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix} \quad k \times \ell$$

$I_m = m \times m$ identity.

$$A^T E_t^T \cdots E_1^T = \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix} \quad \ell \times k$$

$$\underbrace{(E_1 \cdots E_t)}_{\text{rank preserving}} A A^T \underbrace{(E_t^T \cdots E_1^T)}_{\text{rank preserving}}$$

* col ops ... can't recover AA^T ?

→ switch columns.

so $rk(\quad) = rk(AA^T)$

$$= rk\left(\begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix}\right) = rk\begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix} = m.$$

a_i = row vector of A

$$A \cdot A^T = \begin{pmatrix} a_1 \cdot a_1 & a_1 \cdot a_2 & \cdots & a_1 \cdot a_k \\ a_2 \cdot a_1 & a_2 \cdot a_2 & \cdots & a_2 \cdot a_k \\ \vdots & \vdots & \ddots & \vdots \\ a_k \cdot a_1 & a_k a_2 & \cdots & a_k \cdot a_k \end{pmatrix}$$

$k \times l$ $l \times k$

Suppose $a_{i_1}, \ldots, a_{i_m}$ are lin. indep.

Now suppose column is lin. dep. in AA^T

$\exists\, i \quad \forall j \; (1, k) \quad a_j \cdot a_i = \sum_{k=2}^{m} a_j \cdot (a_k \beta_k)$

$$a_j \cdot \left(a_i - \sum_{k=2}^{n} a_k \beta_k\right) = 0$$

↙ bilinearity of dot product

Suppose $rk(A) = m$.

i^{th} column in $A^T A$ = $(a_1 \cdot a_i, \ldots, a_n \cdot a_i)$

Show n cols. in $A^T A$ are lin. indep.

$$\sum_{i=1}^{m} c_i (a_1 \cdot a_i, \ldots, a_n \cdot a_i) = 0$$

$$\hookrightarrow \sum_{i=1}^{m} c_i a_i \cdot a_j = 0 \quad \Rightarrow \sum_{i=1}^{n} c_i \|a_i\|^2 = 0$$

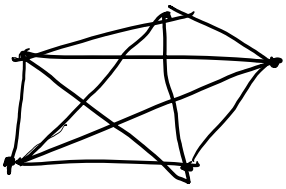
$\Rightarrow c_i = 0 \;\; \forall i$

So then $rk(A^TA) \geq rk(A) = m$

and we proved earlier that $rk(A) \geq rk(A^TA)$

so $rk(A^TA) = rk(A)$. □

Chromatic polynomial



complete graph

$t(t-1)\cdots(t-n+1)$ possible colorings.

But some edges might not be there.

Remove one edge at a time ... you can "merge" the two unconnected pts. to make a smaller graph.

Inducting on the number of edges - assume all smaller #s of edges are polynomial.

Summing polynomials gives a polynomial.

Induct on m - # of edges.

Consider graph G

$G - e$ (remove an edge) - remove edge e connecting v, w

$$f_{G-e}(t) = f_G(t) + f_{G|e}(t)$$

- $f_{G-e}(t)$: ↓ polynomial by inductive hyp. (fewer edges)
- $f_G(t)$: ↓ inherit colorings from bigger graph - still valid.
- $f_{G|e}(t)$: contract v/w - extra colorings ↓ polynomial by inductive hyp. (fewer edges) w/o connection.

$$f_G(t) = \underbrace{f_{G-e}(t) - f_{G|e}(t)}_{\text{difference of polynomials.}} \qquad \square$$

Another approach:

Colorings partition your set into independent sets.

(t) (t-1)

P_k = # of partitions into k independent sets.

# of colorings w/2 : $P_2\, t(t-1)$

$$\sum_{k=1}^{n} p_k\, t(t-1)\cdots(t-k+1) = f_G(t)$$

↑

Summing polynomials is a polynomial. □

---

similar matrices have the same characteristic polynomial.

(i.e. if $A \sim B$ then $f_A = f_B$).

$A \sim B \Rightarrow \exists\, S, S^{-1}$ s.t. $B = S^{-1}AS$

$\in M_n(\mathbb{R})$

$$f_B = \det(\lambda I - B) = \det(\lambda I - S^{-1}AS)$$

$$* \quad \lambda I = S^{-1}\lambda I S$$

$$= \det(S^{-1}\lambda I S - S^{-1}AS)$$

$$= \det(S^{-1}(\lambda I S - AS))$$

$$= \det(S^{-1})\det(\lambda I S - AS)$$

$$= \det(S^{-1})\det((\lambda I - A)S)$$

$$= \det(S^{-1})\det(\lambda I - A)\det(S) = \det(\lambda I - A) = f_A. \quad \square$$

but $\det(S^{-1})\det(S) = \det(S^{-1}S) = \det(I) = 1$, so

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

Not similar ... but same characteristic polynomial.

Find A and B diagonalizable where λ is an eigenvalue of A iff λ is an eigenvalue of B but $f_A \neq f_B$.

$$\begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix} \qquad \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$$

$\lambda_1 \neq \lambda_2$

$(x-\lambda_1)(x-\lambda_2)^2$ $\qquad$ $(x-\lambda_1)^2(x-\lambda_2)$

Different multiplicities produce different characteristic polynomials.

A is diagonalizable if $A \sim B$ and B is a diagonal matrix.

$A \sim B$ if $\exists\ S, S^{-1}$ s.t. $B = S^{-1}AS$.

Let $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

$$f_A = (x-1)(x) - 1 = x^2 - x - 1$$

$$x = \frac{1 \pm \sqrt{1 - 4(1)(-1)}}{2} = \frac{1 \pm \sqrt{5}}{2}$$ (Golden Ratio?)

Distinct eigenvalues $\Rightarrow$ has an eigenbasis

$\Downarrow$

diagonalizable

$$A = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}$$

$$S^{-1}AS = I$$

$$A = S^{-1}IS = I$$

but $A \neq I$. □

Lecture.

$a, b \in \mathbb{Z}$

d is a greatest common divisor of a, b if

(1) d is a common divisor:

$d \mid a$ and $d \mid b$

(2) d is a common multiple of the common divisors:

if $e \mid a$ and $e \mid b$, then $e \mid d$.

Let $S \subseteq \mathbb{Z}$.

How to define greatest common divisor of S?

Def. (a) $(\forall a \in S)(d \mid a)$

(b) if $(\forall a \in S)(e \mid a)$, then $e \mid d$.

e is a common divisor

Thm $\forall S \subseteq \mathbb{Z}$ $\exists$ greatest common divisor d and

$(\exists x_s\ (s \in S))\left(d = \sum_{s \in S} x_s \cdot s\right)$. ← all but a finite # of coefficients are 0.

(e.g. $\gcd(a,b,c) = xa + yb + zc$)

$\gcd(\emptyset) = ?$

$Div(\emptyset) = \mathbb{Z}$. (all integers divide every element of the empty set.)

$\gcd(\emptyset) = 0$ $(\forall z \in \mathbb{Z},\ z \mid 0.)$

HW Find $\gcd(p^2+1 \mid p$ odd prime$)$.

Least Common Multiple

Def. m is a least common multiple of $S \subseteq \mathbb{Z}$ if

(1) m is a common multiple: $(\forall a \in S)(a \mid m)$

(2) m divides all common multiples:

$(\forall f \in \mathbb{Z})$(if $(\forall a \in S)(a \mid f)$ then $m \mid f$)

f is a common multiple

(DO) If lcm exists, it is unique up to sign (±)

Convention: take ≥ 0 value for lcm(S),

so lcm(a, a) = |a|.

$\exists$? lcm(a, b)

$12\mathbb{Z} \cap 15\mathbb{Z}$ ↙ subgroup

Lemma $a\mathbb{Z} \cap b\mathbb{Z} \leq \mathbb{Z}$. ↳ numbers in this set are in the set of common multiples of 12 and 15.

(Shown on HW.)

$\therefore (\exists k)(a\mathbb{Z} \cap b\mathbb{Z} = k\mathbb{Z})$

$\stackrel{?}{=} 60\mathbb{Z}$

Claim: k is a lcm of a, b. (DO)

(DO) Same for lcm(S) where $S \subseteq \mathbb{Z}$.

Let's take an easier approach.

lcm is (1) common multiple
(2) common divisor of common multiples,

m := gcd(all common multiples)

(DO) This satisfies def. of lcm.

Arithmetic - synonym for theory of numbers (esp. whole #s / integers)

Greeks established math — before — empirical tool. → proofs.

Descartes - unification of arithmetic / + geometry, algebra

(continues happening on higher and higher levels)

Fundamental Theorem of Arithmetic. ∃

If n is a positive integer then n can be written as a product of primes uniquely up to order.

Def. $p \geq 1$ is a prime number if $p \neq 1$ and the only positive divisors of p are 1 and p.

(i.e $|Div(p)| = 4$: $Div(p) = \{\pm 1, \pm p\}$)

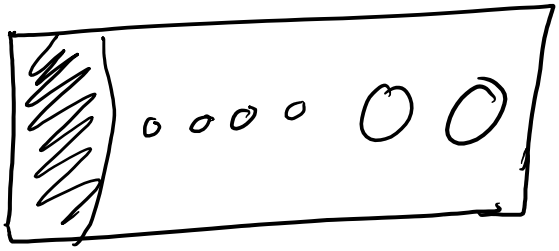
Lemma. If $n \geq 1$ then $\exists$ prime factorization of n.

(DO) Prove by induction

$n = 1$ has a prime factorization : product of empty set of primes

send a picture as a string ... how?

Product of $p \cdot q$ (two primes) length.



only 2 ways to orient picture.

$(p \cdot q \quad q \cdot p)$

Def $q \in \mathbb{Z}$ has the prime property if $q \neq \pm 1$ and $(\forall a, b)$ (if $q \mid ab$ then $q \mid a$ or $q \mid b$).

which integers do not have the prime property?

± 1 (by def), 6 (counterexample) — $6 \mid 3 \cdot 4$ but $6 \nmid 3$ and $6 \nmid 4$.

we can show all composite numbers do not have this property

composite number : $n = ab$ where $|a|, |b| < |n|$.

$6 = 3 \cdot 2$

$6 \mid 3 \cdot 2$ but $6 \nmid 3$ and $6 \nmid 2$.

All that's left are $\pm$ primes and 0.

(DO) 0 has the prime property.

Thm. All $+$ primes have the prime property, (Then $-p$ does too.)

(essence of Fun Theorem of Arithmetic)

Cor. uniqueness of prime factorization.

Proof. by induction: True for $n = 1$

Assume $n \geq 2$ and uniqueness holds $\forall n' < n$. (Induction Hyp)

Suppose $n = p_1 \cdots p_k = q_1 \cdots q_\ell$ are two prime factorizations. $(k, \ell \geq 1)$

$p_1 \mid q_1 \cdots q_\ell \Rightarrow (\exists i)(p_1 \mid q_i)$ (Prime Property of p_1)

but $\mathrm{Div}(q_i) = \{\pm 1, \pm q_i\}$ and $p_1 \neq 1$, so $(\exists i)(p_1 = q_i)$.

$$n' := \frac{n}{p_1} = \frac{n}{q_i} = \underbrace{p_2 \cdots p_k}_{k-1} \overset{?}{=} \underbrace{q_1 \cdots \hat{q}_i \cdots q_\ell}_{\ell-1}$$

By inductive hyp. , . □

Proof (of prime property of prime #s)

Lemma. $\gcd(ac, bc) = \underbrace{\gcd(a,b)}_{d} \cdot |c|$

NTS: LHS | RHS
RHS | LHS — easy by ↓

Observation: $k \mid \gcd(r,s) \iff k \mid r$ and $k \mid s$. (DO)

RHS | LHS: NTS $\leftarrow$ $d|ac$, $dc \mid bc$ $\Leftarrow$ $b|c$, $d|a$, $d|b$.

LHS | RHS ?

Use: $(\exists x, y)(d = ax + by)$.

NTS: $\underbrace{\gcal(ac, bc)}_{e} \mid dc = (ax+by)c = \underbrace{(ac)x + (bc)y}_{\text{lin comb.}}$ ✓

$e|ac$

$e|bc$

Thm Primes have the prime property.

Proof Suppose $p \mid ab$ but $p \nmid a$. NTS: $p \mid b$.

$\gcd(p, a) = 1$.

b/c $Div(p) = \{\pm 1, \pm p\}$ so only pos divisors of p are $\begin{cases} p & \leftarrow \text{cannot be } \gcd(p,a) \text{ b/c } p \nmid a. \\ 1 & \checkmark \end{cases}$

By lemma, $\gcd(pb, ab) = |b|$.

we know $p \mid pb$ and $p \mid ab$ by assumption,

so $p \mid \gcd(pb, ab)$ and $p \mid |b|$. □

Euclid: Elements (first appearance of "axiom")

Algorithm: Al-Khwarizmi (Persian) - living in Baghdad and wrote in Arabic.

Al-Jabr - formed algebra

Al-Biruni - measured circumference of Earth, chronicled India, natural scientist, cartographer ✡ postulated existence of Americas

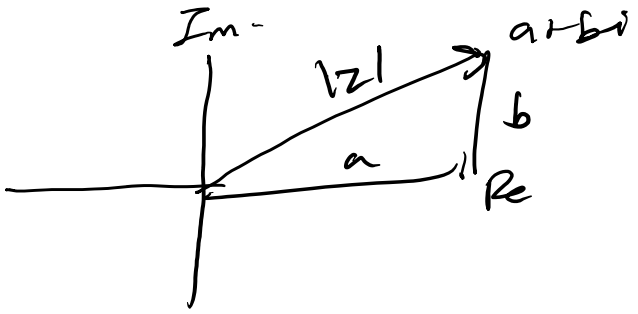
DO! Review complex numbers

$z = a + bi$

$\bar{z} = a - bi$ (conjugate)

$i^2 = -1$

$|z|^2 = a^2 + b^2 = z \cdot \bar{z}$



$Re(z) = a$ (real part)

$Im(z) = b$ (imaginary part)

$r = r + 0i$.

$\mathbb{R}$ $\mathbb{C}$ $\mathbb{C}$

$\overline{z \cdot w} = \bar{z} \cdot \bar{w}$

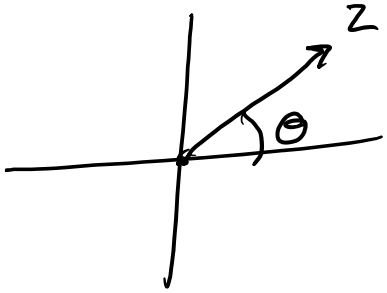
$\overline{z+w} = \bar{z} + \bar{w}$

(conjugate is isomorphism.)

1 consequence $|z \cdot w| = |z| \cdot |w|$

$\arg(zw) = \arg(z) + \arg(w)$ mod 2π

$\theta = \arg(z)$ unique mod 2π



$|z| = r$, $\arg(z) = \theta$ $\Rightarrow$ $z = re^{i\theta}$ where

$$e^{i\theta} = \cos\theta + i\sin\theta$$

$w = se^{i\psi}$ then $zw = (rs)e^{i(\theta+\psi)}$

$$\arg(z^n) = n\theta$$

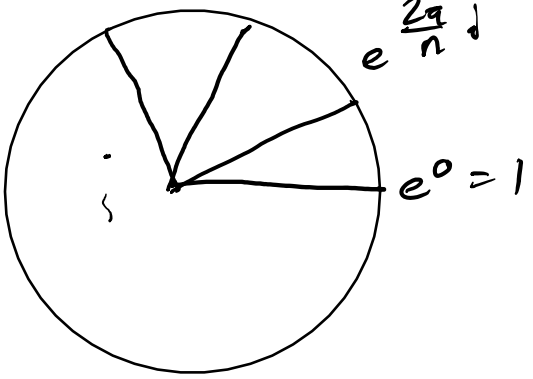
$$z^n = r^n e^{in\theta}$$

ω is an n^{th} root of unity if $\omega^n = 1$.

$\therefore$ $|\omega| = 1$ $\quad n\theta \equiv 0 \mod 2\pi$

i.e. $n\theta = 2k\pi$

$e^{\frac{6\pi}{n}i}$ $e^{\frac{4\pi}{n}i}$ $e^{\frac{2\pi}{n}i}$ $\quad \theta = \frac{2k}{n}\pi \qquad k = 0, \ldots, n-1$



HW Prove: for $n \geq 2$ sum of n^{th} roots of unity $= 0$.

Order of $z \in \mathbb{C}$ is smallest positive n s.t

$z^n = 1$.

If no such n exists : $\text{ord}(z) = -\infty$

If $\exists$ such an n : z is a root of unity.

Def z is a primitive n^{th} root of unity if

$\text{ord}(z) = n$.

HW List all primitive n^{th} roots of unity in canonical form ($a+bi$ form) for

$n = 1, 2, 3, 4, 6$.

DO Prove : $x^n - 1 = \prod_{\omega : n^{\text{th}} \text{ roots of unity}} (x - \omega)$.

Def $\Phi_n(x) = \prod_{\omega : \text{primitive } n^{\text{th}} \text{ root of unity}} (x - \omega)$

HW List $\Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_6, \Phi_p$ if p prime

HW (for Monday): Prove $\Phi_n \in \mathbb{Z}[x]$.

q

all coeff are $\in \mathbb{Z}$.

Fundamental Theorem of Algebra

$\forall f \in \mathbb{C}[x]$, $\deg f \geq 1 \Rightarrow (\exists \alpha \in \mathbb{C})(f(\alpha) = 0)$

Cor. (DO)

If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ where $a_i \in \mathbb{C}$

and $a_n \neq 0$, then

$\exists \alpha_1, \ldots, \alpha_n \in \mathbb{C}$ s.t. $f(x) = \pi(x - \alpha_i)$.

Def α is a multiple root of f if

$(x-\alpha)^2 \mid f$.

HW Prove: $f \in \mathbb{C}[x]$ has a multiple root $\Leftrightarrow$

$\gcd(f, f') \neq 1$.

HW Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Find A^n.

HW Let $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Find B^n.

Def $(a_0, a_1, a_2 \dots)$ is a Fibonacci-type sequence if $\forall n \geq 2 \quad a_n = a_{n-1} + a_{n-2}$.

$Fib := \{\text{Fibonacci-type sequences}\}$

HW (a) Fib is an invariant subspace under S: left shift operator (i.e. Show $S(Fib) \subseteq Fib$ and find dim of Fib.)

(b) Let $\bar{S} : Fib \to Fib$ be the restriction of S to Fib. Find the eigenvalues and an eigenbasis of $\bar{S}$.