Tuesday, July 11, 2017 9:32 AM

Euclid's Algorithm efficiency:

Prove the # of iterations of Euclid's algorithm for #s $a, b \mid 1 \le b \le a$ is $\le 1 + 2\log_2 b$.

$a = bq + r$

① $r \le \frac{b}{2} \rightarrow \gcd(b, r) \rightarrow r \le \frac{b}{2}$.

② $r > \frac{b}{2} \rightarrow \gcd(b, r) \rightarrow b = qr + r_1 \rightarrow \gcd(r, r_1)$

Claim: $r_1 = b - r$

$r_1 = b - r < \frac{b}{2}$ Since $r > \frac{b}{2}$, $q = 1$.

For any 2 steps of Euclid's algorithm, b (the second argument) is halved.

$\underbrace{2\log_2 b}_{\text{\# of times b can be halved} \cdot \text{2 steps per halving}} + 1$

halving process ends at 1, but need 0

$\dim_{\mathbb{Q}} \mathbb{R} = \infty$.

Each # in $\mathbb{R}$ can be written as a sequence of digits.

$\forall r \in \mathbb{R}$,

$$r = a_0 + a_1\left(\frac{1}{10}\right)^1 + a_2\left(\frac{1}{100}\right)^2 + \cdots$$

$a_0, a_1, a_2, \ldots \in \mathbb{Z}$. $\frac{1}{10}, \frac{1}{100}$ not lin indep. X

Suppose $\exists$ finite basis of $\mathbb{R}$:

$b_1, b_2, \ldots, b_n$.

$\forall r \in \mathbb{R}$, $r = q_1 b_1 + q_2 b_2 + \cdots + q_n b_n$.

Each q_i has $|\mathbb{Q}|$ possibilities...

Can we make an argument w/o cardinality?

Suppose $\dim_{\mathbb{Q}} \mathbb{R} = n < \infty$.

Then $n+1$ elements are linearly dependent.

<u>WTS:</u> $(1, \pi, \pi^2, \ldots, \pi^n)$ is lin. indep.

$$q_0 + q_1\pi + q_2\pi^2 + \cdots + q_n\pi^n = 0$$

All elements distinct b/c π transcendental:

$$q_k\pi^k = q_\ell\pi^\ell$$

$$\pi^{k-\ell} - \frac{q_\ell}{q_k} = 0$$

a rational polynomial w/ π as a root, bad.

In addition, $q_0, q_1, \ldots, q_n$ cannot be nontrivial for the same reason.

$\square$

$\therefore (1, \pi, \pi^2, \ldots, \pi^n)$ lin indep.

DO $\{\log p\}_{p \text{ is prime}}$ is lin. indep. over $\mathbb{Q}$.

DO $f, g \in \mathbb{Z}[x]$ (monic), $g \mid f$ in $\mathbb{Q}[x]$ ($gh = f$ for some $h \in \mathbb{Q}[x]$)

Then $g \mid f$ in $\mathbb{Z}[x]$ ($gh = f$ for some $h \in \mathbb{Z}[x]$)

Tuesday, July 11, 2017 9:58 AM

$(\forall \lambda)(\text{geom. mult}_A(\lambda) \leq \text{alg. mult}_\lambda(A))$

geom. mult : $\dim U_\lambda(A)$

alg. mult : # of times appearing in char. poly.

Let geom mult = m.

$$S = \begin{pmatrix} | & & | & & | \\ x_1 & \cdots & x_m & \cdots & x_n \\ | & & | & & | \end{pmatrix} \to n \text{ lin indep cols} : S \text{ invertible}$$

$\underbrace{x_1 \cdots x_m}_{\text{eigenvectors}}$ $\underbrace{\cdots x_n}_{\text{extend to basis}}$

B =

$$S^{-1}AS = \begin{array}{cc} & m \\ m & \left[\begin{array}{c|c} \begin{matrix} \lambda & & 0 \\ & \lambda & \\ 0 & & \lambda \end{matrix} & * \\ \hline 0 & * \end{array}\right] \end{array}$$

corresponds to basis of eigenspace - eigenvectors stay w/in first m vectors

no additional vectors needed here $\to$ 0

$$A = \begin{pmatrix} \text{---} & a_1 & \text{---} \\ \text{---} & a_2 & \text{---} \\ & \vdots & \\ \text{---} & a_n & \text{---} \end{pmatrix}$$

$\to (t-\lambda)^{m} \det(tI - A)$

alg. mult at least m.

$AS = a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$

Char poly. is multiple of char polys of diagonal blocks in a block triangular matrix.

($\Leftarrow$) Assume $\forall \lambda$ alg. $\text{mult}_A(\lambda) = \text{geom. mult}_A(\lambda)$.

$\forall \lambda$ suppose $\text{Geom}_A(\lambda) = a_\lambda$.

$\Rightarrow \exists\, a_\lambda$ lin. independent eigenvectors associated w/ λ.

$\sum_\lambda \text{alg}_A(\lambda) = \sum_\lambda a_\lambda = n$

$\deg f_A = n \Rightarrow n$ lin. independent eigenvectors

(eigenvectors to distinct eigenvalues are lin. indep.)

These form an eigenbasis.

$$\underbrace{\sum_i a_{1,i} e_{1,i}}_{\substack{(\lambda_1)}} + \underbrace{\sum a_{2,i} e_{2,i}}_{\substack{(\lambda_2) \\ u_2}} + \dots + \underbrace{\sum a_{n,i} e_{n,i}}_{\substack{(\lambda_n) \\ u_n}} = 0$$

this is also an eigenvector for λ_1, v_1 (or 0.)

$$\underbrace{v_1 + v_2 + \dots + v_n}_{} = 0$$

eigenvectors to distinct eigenvalues are lin. independent.

A diagonalizable : $A \sim D$, D diagonal

$f_A = f_D \Rightarrow$ λ is eigenvalue of $A \Leftrightarrow$ λ is eigen value of D

and alg mult$_A(\lambda)$ = alg mult$_D(\lambda)$

$\text{geom}_D(\lambda) = n - rk(\lambda I - D) = \text{alg}_D(\lambda)$

$$\begin{bmatrix} \lambda-\lambda_1 & & & 0 \\ & \lambda-\lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda-\lambda_n \end{bmatrix}$$

Find eigenvalues + eigenbasis for $\begin{pmatrix} 1 & & 0 & 1 \\ & \ddots & & \\ 0 & & \ddots & 1 \end{pmatrix}$

$$\det(\lambda I - A) = \begin{vmatrix} \lambda & & & & -1 \\ -1 & \lambda & & 0 & \\ & -1 & \ddots & & \\ & & \ddots & \lambda & \\ 0 & & & -1 & \lambda \end{vmatrix}$$

$$\lambda \begin{vmatrix} \lambda & & & \\ -1 & \lambda & & \\ & -1 & \ddots & \\ & & \ddots & \lambda \\ & & & -1 \end{vmatrix} + (-1)^{n+1}(-1) \begin{vmatrix} -1 & \lambda & & 0 \\ & -1 & & \\ & & \ddots & \lambda \\ 0 & & & -1 \end{vmatrix}$$

$$\lambda(\lambda^{n-1}) + (-1)^{n+2}(-1)^{n-1} \quad 1 = \lambda^n - 1 = 0$$

$\rightarrow$ nth roots of unity.

Tuesday, July 11, 2017 10:30 AM

$$\omega = e^{\frac{2\pi}{n}i}$$

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}$$

$$A\vec{x} = \omega\vec{x}$$

$$\begin{bmatrix} \omega^{n-1} \\ \omega^{n-2} \\ \vdots \\ 1 \end{bmatrix} \quad \omega^n = 1$$

Works for any of the n^{th} roots of unity.

$\lambda^n = 1$

λ

λ^2

$\vdots$

λ^{n-1}

matrix: $$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)^2} \end{pmatrix}$$

discrete Fourier transform matrix

$V(1, \omega, \ldots, \omega^{n-1})$

Vandermonde matrix

Lecture

Circulant matrix

$$C(a_0, a_1, a_2, \ldots, a_{n-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

(for Thurs.)

$\boxed{\text{HW}}$ ✓ Find $\det(C(a_0, a_1, \ldots, a_{n-1}))$

factored into linear forms of the a_i:

$$\prod_{j=0}^{n-1} (\alpha_{0,j} a_0 + \cdots + \alpha_{n-1,j} a_{n-1}), \quad \alpha_{ij} \in \mathbb{C}.$$

Do not calculate.

(Ask for a hint tomorrow.)

$\operatorname{rk}(A+B) \le \operatorname{rk}(A) + \operatorname{rk}(B)$

DO $\operatorname{rk}(A) \le r \iff A$ is the sum of r matrices of $\operatorname{rk} = 1$.

$\Leftarrow$ ✓ (obvious)

$\Rightarrow$?

$rk(AB) \leq \min\{rk(A), rk(B)\}$

DO $C \in \mathbb{F}^{k \times l}$ has rank $\leq r \iff$

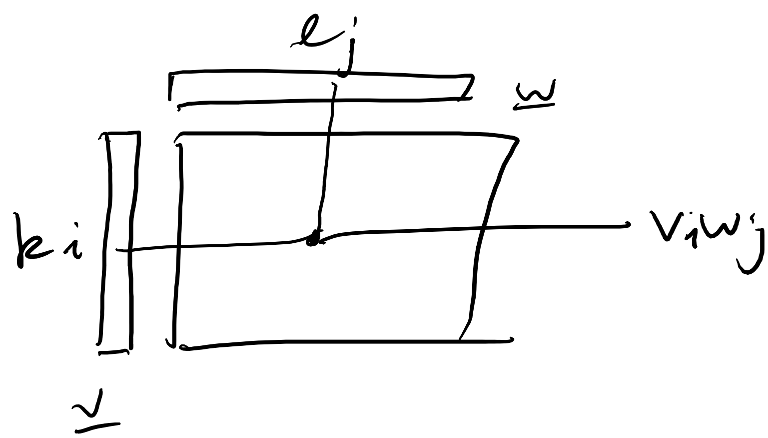
$(\exists A \in \mathbb{F}^{k \times r}, B \in \mathbb{F}^{r \times l})(AB = C)$

DO $A \in \mathbb{F}^{k \times l}$

$rk(A) \leq 1 \iff \exists\, v \in \mathbb{F}^k, w \in \mathbb{F}^l$ s.t.

$A = vw^T$.

(If v or w is 0 then $rk(A) = 0$.)



$A \in M_n(\mathbb{F})$

$I, A, A^2, \ldots, A^{n^2}$ are lin dep.

<u>Claim.</u> $M_n(\mathbb{F})$ vector space $\cong \mathbb{F}^{n^2}$

$\therefore \dim M_n(\mathbb{F}) = n^2$

so n^2+1 matrices are lin. dep. $\square$.

<u>i.e.</u> $\exists f \in \mathbb{F}[t]$ s.t. $f \neq 0$ and $f(A) = 0$,

with $\deg f \leq n^2$.

$$\operatorname{diag}(\lambda_1, \ldots, \lambda_n) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = A$$

$\operatorname{diag}(\mu_1, \ldots, \mu_n) = B$ <u>μ $\backslash$mu</u>

$A + B = \operatorname{diag}(\lambda_1 + \mu_1, \lambda_2 + \mu_2, \ldots, \lambda_n + \mu_n)$

$AB = \operatorname{diag}(\lambda_1\mu_1, \lambda_2\mu_2, \ldots, \lambda_n\mu_n)$ DO

$$\therefore f(A) = \begin{pmatrix} f(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & f(\lambda_n) \end{pmatrix} = \operatorname{diag}(f(\lambda_1), \ldots, f(\lambda_n))$$

polynomial

$cA = \mathrm{diag}(c\lambda_1, \dots, c\lambda_n)$

Cor. For a diagonal matrix A,

$f(A) = 0 \iff$ all λ_i are roots of f.

Cor $f_A(A) = 0$.

Cayley - Hamilton Theorem

$(\forall A \in M_n(\mathbb{F}))(f_A(A) = \underline{\underline{0}})$

Silly proof:

$f_A(t) = \det(tI - A)$

$f_A(A) = \det(AI - A) = \det \underline{\underline{0}} = 0$ ...?

this is a scalar... not a matrix.

Prove Cayley - Hamilton for diagonalizable matrices.

proof. $A \sim D = \mathrm{diag}$

$f_A = f_D$

$f_A(A) \sim$

$f_A(D) =$

$f_D(D) = \underline{\underline{0}}$

DO Lemma: If $A \sim B$ and g is poly, $g(A) \sim g(B)$.

For any $A \in M_n(\mathbb{C})$, use density of diagonalizable matrices in $\mathbb{C}$.

we know $\mathbb{F} \subseteq \mathbb{C}$, so this should hold for any number field

C-H mod p also follows.

DO C-H (general fields)

<u>Thm</u> $\forall A \in M_n(\mathbb{C})$ is similar to 

This is equivalent to saying (<u>Thm</u>*)

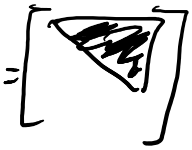
if V is a vector space over $\mathbb{C}$ and $\varphi: V \to V$, then $\exists$ maximal chain of φ-invariant subspaces.

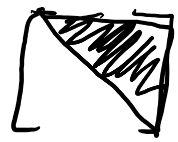
$0 = U_0 < U_1 < \dots < U_n = V$ where

$\dim U_i = i$.

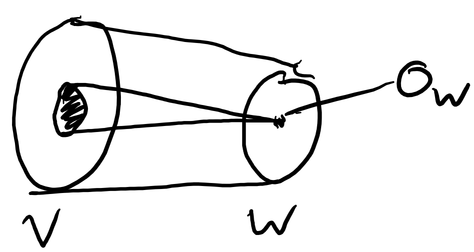
How do we know $\underline{Thm}^* \Rightarrow \underline{Thm}$?

Let $[\varphi]_{\underline{e}} = A$.

Need to find other basis s.t. $[\varphi]_f =$ 

<u>Lemma</u> $[\varphi] =$  $\Leftrightarrow$

$$\left.\begin{matrix} \operatorname{span}(f_1) \\ \operatorname{span}(f_1, f_2) \\ \operatorname{span}(f_1, f_2, f_3) \\ \vdots \end{matrix}\right\} \text{ are } \varphi\text{-invariant subspaces.}$$



$\psi : V \xrightarrow[\text{onto}]{} W$

$n \qquad n-k$

Let $K := \ker \psi = \psi^{-1}(0_W) = \{ v \in V \mid \psi(v) = 0 \}$

$\dim K = n - \dim \underbrace{\operatorname{im}(\psi)}_{W} = n - (n-k) = k$

(by rank-nullity theorem)

DO There is a one-to-one correspondence between subspaces of W and subspaces of V that contain K.

(If $R \leq W$, R corresponds w/ $\psi^{-1}(R)$.)

preimage.

This correspondence preserves inclusion:

$R_1 \leq R_2 \Rightarrow \psi^{-1}(R_1) \leq \psi^{-1}(R_2)$

<u>Def</u> <u>Codimension</u>

If $W \leq V$, then $\text{codim}_V(W) =$ max. # of vectors in V that are lin independent <u>modulo W</u>.

<u>Def</u>. $v_1, \dots, v_k$ are linearly independent modulo W if

$(\forall \alpha_i)(\text{if } \sum \alpha_i v_i \in W \text{ then } \alpha_1 = \dots = \alpha_k = 0)$.

Consider a line in G_3 as W.
On a perpendicular plane passing through
origin, pick 2 lin. indep. vectors.
s.t. lin. comb $\in W$.
However, then must be 0, so coefficients
are 0 b/c lin. indep.

DO $v_1, \ldots, v_k$ are lin. indep. mod W
$\iff$ $v_1, \ldots, v_k$ are lin. indep. and
$\operatorname{Span}(v_1, \ldots, v_k) \cap W = \{0\}$.

<u>Cor.</u> If $\dim V = n$
$\dim W = k$

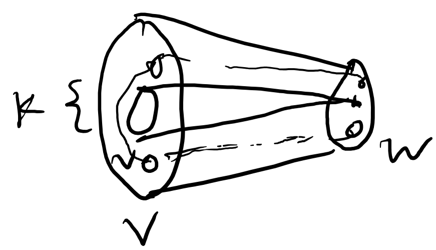
Then $\operatorname{codim}_V(W) = n-k$.
If $R_1 \le R_2$, then $\psi^{-1}(R_1) \le \psi^{-1}(R_2)$ and
$\operatorname{codim}_{R_2} R_1 = \operatorname{codim}_{\psi^{-1}(R_2)} \psi^{-1}(R_1)$.

In particular, if $0 = W_0 < W_1 < \dots < W_{n-k} = W$

s.t. $\dim W_i = i$,

then $K = \psi^{-1}(W_0) < \psi^{-1}(W_1) < \dots < \psi^{-1}(W_{n-k}) = V$

codim = 1

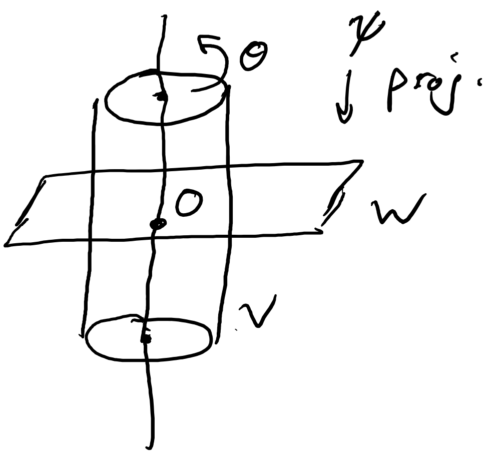


$\varphi : V \to V$.

If K is φ-invariant,

then we can define

φ-action on W.



K = axis of rotation.

action: rotation of plane.

φ-action on W: $\bar{\varphi} : W \to W$ s.t.

$\bar{\varphi}(w) := \psi(\varphi(v)))$ where $v \in \psi^{-1}(w)$.

find $v \in \psi^{-1}(w)$, take $\varphi(v)$, and look at image back into W: ψ.

NTS: If $v' \in \psi^{-1}(w)$, then $\psi(\varphi(v')) = \psi(\varphi(v))$.

$\boxed{\text{HW}}$ Show this b/c K is φ-invariant

<u>Proof of Thm.</u>

Base case: $n=0$. ✓

By induction on $\dim V = n$. Assume $n \geq 1$.

we have already seen $\exists$ 1-dim φ-invariant subspace

I.H true for dim $= n-1$

$\underline{e}$ ← b/c $\exists$ eigenvector

$K := \text{span}(\underline{e})$

(char poly has a root → b/c $\mathbb{C}$)

→ Take span of eigenvector

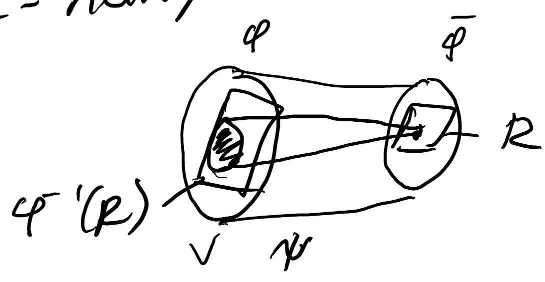
DO Find $\psi : V \twoheadrightarrow W$ s.t. $\ker \psi = K$

(true for any $K \leq V$)

$\dim K = 1$

(by rank-nullity)

$\therefore \dim W = n-1$



φ acts on V

$\bar{\varphi}$ acts on W

$\bar{\varphi}$ has max. chain of $\bar{\varphi}$-inv. subspaces.

$0 < W_0 < W_1 < \dots < W_{n-1} = W$

Tuesday, July 11, 2017 11:47 AM

$U_0 = \{0_V\}$

$U_i = \varphi^{-1}(W_{i-1})$

|

dim i

all these U_i are φ-invariant b/c W_{i-1} is $\bar{\varphi}$-invariant.

dim $W_i = i$

dim $\varphi^{-1}(W_i) = i+1$

φ increases dimension by dim. of kernel $\to 1$.

DO

$\square$

lin transformation - k-dim space $\to$ acts on K

φ-invariant $\leftarrow K$

$K = \text{span}(e_1, \ldots, e_k)$

$$\begin{array}{cc} k & n-k \\ \left(\begin{array}{c|c} \boxed{\varphi|_K} & \\ \hline 0 & \begin{matrix} \bar{\varphi} \\ \text{on } W \end{matrix} \end{array}\right) & n-k \end{array}$$

what is the trans? φ restricted to K:

$\varphi|_K : K \to K$

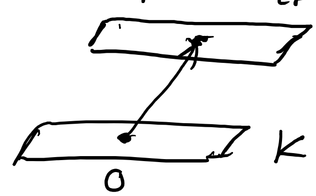
restriction.

<u>Notation:</u>

$W = V/K$ <u>quotient space</u>.

<u>Def</u> If $K \subseteq V$, translation of K by $v \in V$: $K + v$. $K+v = \{k+v \mid k \in K\}$

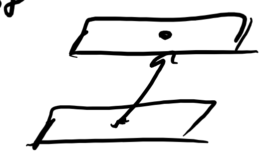
$k+v$: called a <u>coset</u> of k in V.



DO $K = K + v \iff v \in K$.

$\boxed{\text{HW}}$ $K + v = K + v' \iff v - v' \in K$.

<u>Def</u> V/K is the set of cosets of K in V.



How many parameters are necessary in G_3 plane example?

1 - two don't matter (remain in plane).

<u>Claim</u> V/K is a vector space under the operations of

$(K + v) + (K + u) := K + (v + u)$

$\lambda \cdot (K + v) := K + \lambda v$.

(operation defined by representatives -- should not change between representatives.)

Definition is sound.

$\boxed{\text{HW}}$ Prove this definition is sound.

(Replacing v, u with other members of the same translate will not change the translate.)

$v \longmapsto K + v$

This map is a linear map $V \twoheadrightarrow V/K$ with kernel K. (Anything in K amounts to not a translation.)