$\mathbb{F}$ - field (e.g. $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_p$)

DO $\mathbb{F}[x]$ polynomials: integral domain

$\mathbb{F}^n$ $\quad \underline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \underline{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{F}^n$

$$\underline{x} \cdot \underline{y} = \underline{x}^T \underline{y} = \sum_i x_i y_i$$

$\underline{x} \perp \underline{y}$ if $\underline{x} \cdot \underline{y} = 0$;

perpendicular

If $S \subseteq V$, $\underline{x} \perp S$ if $(\forall \underline{s} \in S)(\underline{x} \perp \underline{s})$

If $S, T \subseteq V$, $S \perp T$ if $(\forall \underline{s} \in S)(\forall \underline{t} \in T)(\underline{s} \perp \underline{t})$

If $S \subseteq V$, we let $S^\perp$ be the "perp" of S:

$$S^\perp = \{\underline{x} \in V \mid \underline{x} \perp S\}$$

DO $S^\perp \leq V$

subspace

DO $S \subseteq T \Rightarrow S^{\perp} \supseteq T^{\perp}$

DO $S \subseteq (S^{\perp})^{\perp}$

$\boxed{\text{HW}}$ If $\mathcal{U} \leq V = \mathbb{F}^n$, then

$\dim \mathcal{U} + \dim \mathcal{U}^{\perp} = n$.

<u>Cor</u> If $\mathcal{U} \leq V$, then $\mathcal{U}^{\perp\perp} = \mathcal{U}$.

<u>Proof</u> we know $\mathcal{U} \leq \mathcal{U}^{\perp\perp}$

$\therefore$ NTS: $\dim \mathcal{U} = \dim \mathcal{U}^{\perp\perp}$.

But by HW $\dim \mathcal{U} = \dim \mathcal{U}^{\perp\perp} = n - \dim \mathcal{U}^{\perp}$. ▫

<u>Def</u> $\underline{v} \in V$ is <u>isotropic</u> if $\underline{v} \neq \underline{0}$ but

$\underline{v} \cdot \underline{v} = 0$.

$\mathbb{F}^2$ - find isotropic vectors

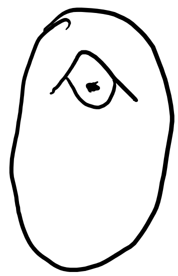
Case $\mathbb{F} = \mathbb{R}$ $\quad \underline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \underline{x} \cdot \underline{x} = \sum x_i^2$

In $\mathbb{R}$, must all be 0.

Friday, July 14, 2017 9:42 AM

<u>Case</u> $\mathbb{F} = \mathbb{C}$

Find $x, y \in \mathbb{C}$, not both 0 s.t. $x^2 + y^2 = 0$.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ i \end{bmatrix} \longrightarrow$$  cyclops

<u>Case</u> $\mathbb{F} = \mathbb{F}_5 \longrightarrow \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ i \end{bmatrix}$

$2^2 = -1$

$\boxed{\text{HW}}$ For what primes p does $\mathbb{F}_p^{\,2}$ have an isotropic vector?

(a) Show: $\mathbb{F}_p^{\,2}$ has an isotropic vector $\Longleftrightarrow$

$$(\exists x \in \mathbb{F}_p)(x^2 = -1)$$

(b) Experiment, find pattern, make conjecture

$\boxed{\text{CH}}$ Prove conjecture.

DO $V = \mathbb{F}^n \Rightarrow V^\perp = \{0\}$

$\{0\}^\perp = V$

$\emptyset^\perp = V$

$S, T \subseteq V \Rightarrow (S \cup T)^\perp = S^\perp \cap T^\perp$

$S \subseteq V \Rightarrow S^\perp = \text{Span}(S)^\perp$.

<u>Defn</u> $S \subseteq \mathbb{F}^n$

S is <u>totally isotropic</u> if $S \perp S$.

<u>Cor.</u> S is totally isotropic $\Leftrightarrow$ Span (S) is totally isotropic

DO $\forall S, T \subseteq V$, if $S \perp T$, then Span $(S) \perp$ Span (T)

<u>Thm</u> Let $U \leq V = \mathbb{F}^n$ be totally isotropic.

Then $\dim U \leq \lfloor \frac{n}{2} \rfloor$

DO For $S \subseteq V$, S is totally isotropic $\Leftrightarrow$ $S \subseteq S^\perp$.

Proof of Thm.

we know from lemma that $U \leq U^\perp$

$k := \dim U$ $\quad$ $k \leq n-k$

$n-k = \dim U^\perp$ $\quad$ $k \leq \frac{n}{2}$

$k \leq \lfloor \frac{n}{2} \rfloor$ $\quad$ $\square$

$\boxed{\text{HW}}$ For all even n, find an $\frac{n}{2}$-dim. totally-isotropic subspace in $\mathbb{C}^n$, $\mathbb{F}_5{}^n$, $\mathbb{F}_2{}^n$.

Project: for what pairs (p, n) is there a totally-isotropic $\frac{n}{2}$-dim. subspace in $\mathbb{F}_p{}^n$? (n is even.)

$\boxed{\text{CH}}$ Prove: every maximal (cannot increase.) totally-isotropic subspace of $\mathbb{F}_2{}^n$ is maximum, and in fact, has $\dim = \lfloor \frac{n}{2} \rfloor$.

Oddtown rules: $X = \{\text{citizens}\}$, $|X| = n$

$$c_1, \dots, c_m \subseteq X$$

(1) $(\forall i)(|c_i|$ is odd$)$

(2) $(\forall i, j)(|c_i \cap c_j|$ is even$)$

$\boxed{\text{HW}}$ $(\forall n)($Find maximal Oddtown system with very few clubs.$)$

If $\mathbb{F} = \mathbb{F}_q$ (field of order q),

V vector space of $\dim = d$ over $\mathbb{F}_q$,

then $|V| = q^d$ b/c $V \cong \mathbb{F}_q^{\,d}$.

Eventown Rules

(0) $(\forall i, j)(i \neq j \Rightarrow c_i \neq c_j)$

(1) $(\forall i)(|c_i|$ is even$)$

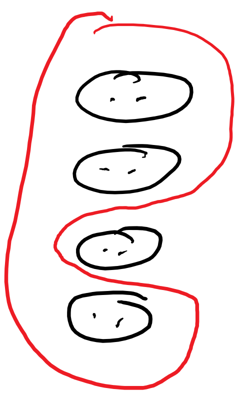
(2) $(\forall i, j)(i \neq j \Rightarrow |c_i \cap c_j|$ is even$)$

$\Big\}$ (12) $(\forall i, j)(|c_i \cap c_j|$ is even$)$

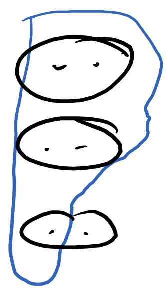
We found such a system with $m = 2^{\lfloor \frac{n}{2} \rfloor}$ clubs.

("married couples" solution)

Why is this maximal?



Clubs = subsets of the couples.



Why can't we add this club?

Each married couple forms a club ...

so this would have an odd intersection.

$\boxed{\text{CH}}$ For $n \geq 7$ find solution with $m = 2^{\lfloor \frac{n}{2} \rfloor}$ which is not a "married-couples" solution.

$\boxed{\text{HW}}$ (for Tues.)

Prove : $m \leq 2^{\lfloor \frac{n}{2} \rfloor}$

Hint : this class so far (3-4 lines).

(Hint: not aware we were talking about Eventown)

Oddtown / Eventown

Elwyn Berlekamp - coding theory.

DO Every maximal Eventown system is maximum.

(Allowed to use things stated but not proved.)

Vector space V over $\mathbb{F}$.

bilinear form

$f : V \times V \to \mathbb{F}$

linear in each variable

$$\begin{cases} f(\underline{u}+\underline{v}, \underline{w}) = f(\underline{u}, \underline{w}) + f(\underline{v}, \underline{w}) \\ f(\lambda \underline{u}, \underline{w}) = \lambda f(\underline{u}, \underline{w}) \end{cases}$$

linear in 1^{st} var.

$$\left\{\begin{array}{l} f(\underline{u}, \underline{w}+\underline{z}) = f(\underline{u}, \underline{w}) + f(\underline{u}, \underline{z}) \\ f(\underline{u}, \lambda \underline{w}) = \lambda f(\underline{u}, \underline{w}) \\ \text{linear in 2nd variable} \end{array}\right.$$

<u>Ex.</u> $V = \mathbb{F}^n \qquad A \in M_n(\mathbb{F})$

$$f(\underline{x}, \underline{y}) = \underline{x}^T A \underline{y}.$$

DO If $f : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$, then

$$(\exists!\ A \in M_n(\mathbb{F}))(f(\underline{x}, \underline{y}) = \underline{x}^T A \underline{y}.)$$

<u>Def</u> f is <u>symmetric</u> if $f(\underline{x}, \underline{y}) = f(\underline{y}, \underline{x})$.

DO $f(\underline{x}, \underline{y}) = \underline{x}^T A \underline{y}$ is symmetric

$\iff A = A^T$ (A is symmetric.)

<u>Def.</u> f is <u>alternating</u> if $(\forall \underline{x})(f(\underline{x}, \underline{x}) = 0)$.

$\boxed{\text{HW}}$ (a) If f is alternating, then
$$f(\underline{x}, \underline{y}) = -f(\underline{y}, \underline{x}).$$

(b) $f(\underline{x}, \underline{y}) = -f(\underline{y}, \underline{x}) \Rightarrow f(\underline{x}, \underline{x}) = 0$ if char $\mathbb{F} \neq 2$.

(c) $f(\underline{x},\underline{y}) = -f(\underline{y},\underline{x}) \not\Rightarrow f(\underline{x},\underline{x}) = 0$ over $\mathbb{F}_2$.

Def. $f: \underbrace{V \times \cdots \times V}_{k \text{ times}} \to \mathbb{F}$

f is k-linear if linear in each variable.

Def f is k-linear alternating if

(1) k-linear

(2) in every pair of vars, f is alternating.

$\boxed{\text{CH}}$ If $f: \underbrace{\mathbb{F}^n \times \cdots \times \mathbb{F}^n}_{n \text{ times}} \to \mathbb{F}$ is an alternating n-linear form, then $(\exists \alpha \in \mathbb{F})(f = \alpha \cdot \det)$

$f: \mathbb{F}^n \to \mathbb{F}$ linear form $\Rightarrow$

$(\exists a \in \mathbb{F}^n)(\forall \underline{x},\ f(\underline{x}) = \underline{a} \cdot \underline{x})$

$= a_1x_1 + \cdots + a_nx_n$.

$f: \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$ bilinear form $\Rightarrow$

$f(\underline{x},\underline{y}) = \underline{x}^T A \underline{y}$ for some $A \in M_n(\mathbb{F})$,

$A = (a_{ij})$

$f(\underline{x}, \underline{y}) = \underline{x}^T A \underline{y}$

$= \sum_i \sum_j a_{ij} x_i y_j$

Def A quadratic form associated with the bilinear form f is

$q(\underline{x}) = f(\underline{x}, \underline{x})$

(If f is alternating : $q(\underline{x}) = 0$.)

Thm
$\forall$ quadratic form q $\exists$ symmetric bilinear form g

s.t. $q(\underline{x}) = g(\underline{x}, \underline{x})$...

unless $\mathbb{F}$...

$q_f(\underline{x}) = f(\underline{x}, \underline{x})$ f bilinear form

$\|$ $f^*(\underline{x}, \underline{y}) := f(\underline{y}, \underline{x})$

$q_{f^*}(\underline{x})$

$q(\underline{x}) = \dfrac{f(x, x) + f^*(x, x)}{2}$

Friday, July 14, 2017 10:52 AM

$$\tilde{f}(x,y) = \frac{f(x,y) + f(y,x)}{2}$$ – symmetric

$$q_{\tilde{f}}(x) = \frac{f(x,x) + f^*(x,x)}{2}$$

unless char $\mathbb{F} = 2$. (cannot divide by 0)

Thus,

Thm

$\forall$ quadratic form q $\exists$ symm bilinear form g

s.t $q(\underline{x}) = g(\underline{x}, \underline{x})$

unless char $\mathbb{F} = 2$. symmetric

$$q(\underline{x}) = \underline{x}^T A \underline{x} \overset{\text{WTS}}{=} \underline{x}^T \tilde{A} \underline{x}$$

$$\tilde{A} = \frac{A + A^T}{2}$$

$$f(\underline{x},\underline{y}) = a_{11} x_1 y_1 + a_{12} x_1 y_2 + a_{21} x_2 y_1 + a_{22} x_2 y_2$$

$$q(\underline{x}) = f(\underline{x}, \underline{x}) = a_{11} x_1^2 + (a_{12} + a_{21}) x_1 x_2 + a_{22} x_2^2$$

$q(\underline{x}) = 1$

equation

$q(x, y) = ax^2 + bxy + cy^2$

$x, y \in \mathbb{R}$

$$q(\underline{x}, \underline{y}) = [x, y] \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

split mixed coefficients

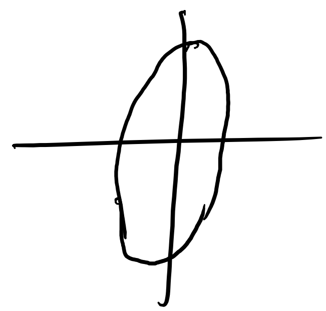
$x \leftarrow x_1$

$y \leftarrow x_2$

ellipses:

$x^2 + y^2 = 1$

$5x^2 + y^2 = 1$



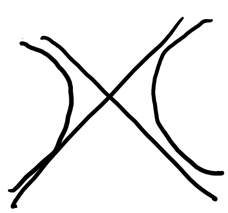
$\begin{pmatrix} -x \\ -y \end{pmatrix} \leftarrow \begin{pmatrix} x \\ y \end{pmatrix}$

$5x^2 + xy + y^2 = 1$ (rotated)

(origin symmetry)

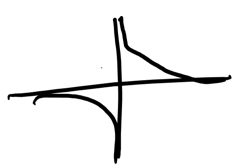
hyperbolas:

$x^2 - y^2 = 1$



$2x^2 - y^2 = 1$

$xy = 1$



empty set

- b, c neg. and a 0.

$x^2 = 1$

- all 0.

$x = \pm 1$

$x = -1$ $\quad x = 1$

Friday, July 14, 2017 11:07 AM

$$q(x,y,z) = ax^2 + by^2 + cz^2 + dxy + exz + fyz$$

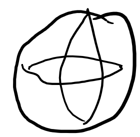
$q(x,y,z) =$

$[x, y, z] \, A \begin{bmatrix} x \\ y \\ z \end{bmatrix}$

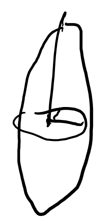
$$A = \begin{bmatrix} a & d/2 & e/2 \\ d/2 & b & f/2 \\ e/2 & f/2 & c \end{bmatrix}$$

$q(x,y,z) = 1$

$x^2 + y^2 + z^2 = 1$ — sphere



$3x^2 + 5y^2 + z^2 = 1$ - ellipsoid



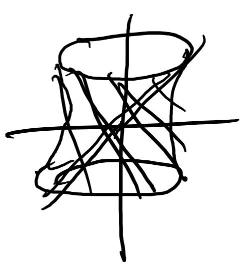
(all 3 traces are ellipses)

$\frac{1}{\sqrt{3}} \quad \frac{1}{\sqrt{3}} \quad 1$

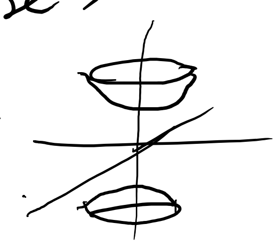
semi-axis lengths.

$3x^2 - 5y^2 + z^2 = 1$ hyperboloid of 1 sheet

(2 hyperbolas, 1 ellipse)



formed of straight lines. 2 sheets:



St Mary's Church - San Francisco roof formed this way.

St Gregory's Church - Gandhi and Paul Erdös.

<u>Thm</u> If $A \in M_n(\mathbb{R})$ is a symmetric real matrix, then A has an <u>orthonormal</u> eigenbasis.

$\perp$ $\|\cdot\| = 1$

(Spectral Theorem)

$e_1, e_2, \ldots, e_n$ s.t. $Ae_i = \lambda_i e_i$, $\lambda_i \in \mathbb{R}$

and $\underline{e_i} \cdot \underline{e_j} = \delta_{ij} = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$

$I = (\delta_{ij})$ Kronecker delta

$\underline{e_i} \cdot \underline{e_i} = 1 \Rightarrow \|e_i\| = 1$

If $\underline{x} \in \mathbb{R}^n$, $\|\underline{x}\| = \sqrt{\underline{x} \cdot \underline{x}} = \sqrt{\sum x_i^2}$.

norm

$A = A^T$

$q(\underline{x}) = \underline{x}^T A \underline{x}$

$\{e_i\}$ ON eigenbasis

$\underline{x} = \sum \alpha_i \underline{e_i}$

$A\underline{e_i} = \lambda \underline{e_i}$

$A\underline{x} = \sum \alpha_i A\underline{e_i}$

$= \sum \alpha_i \lambda_i \underline{e_i}$

$x^T\left(\sum \lambda_i \alpha_i \underline{e_i}\right) = \sum \lambda_i \alpha_i \underbrace{(\underline{x}^T \underline{e_i})}_{\underline{x} \cdot \underline{e_i}}$

$x = \sum_j \alpha_j \underline{e_j}$

$\underline{x} \cdot \underline{e_i} =$

$\sum_j \alpha_j \underbrace{\underline{e_j} \cdot \underline{e_i}}_{0 \text{ unless } i=j}$

so $\underline{x}\cdot\underline{e}_i = \sum_j \alpha_j \underline{e}_j\cdot\underline{e}_i = \alpha_i \underbrace{\underline{e}_i\cdot\underline{e}_i}_{\text{normality}} = \alpha_i$

and $\sum \lambda_i \alpha_i (x^T e_i) = \sum \lambda_i \alpha_i (\underline{x}\cdot\underline{e}_i)$

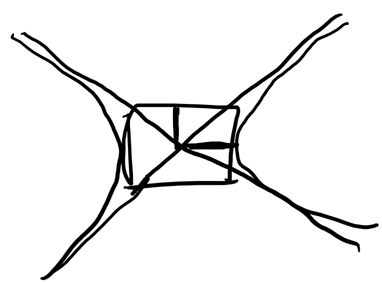
$= \sum \lambda_i \alpha_i^2 = q(\underline{x})$.

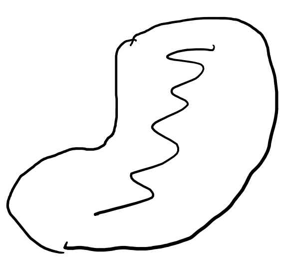
So equation $q(\underline{x}) = 1$ is equivalent

to $\sum \lambda_i \alpha_i^2 = 1$.

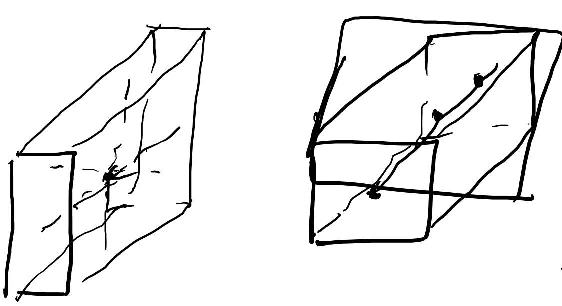
This is an ellipsoid $\Leftrightarrow \forall \lambda_i > 0$.

half axes: $\frac{1}{\sqrt{|\lambda_i|}}$





potato in outer space.



any line in $\perp$ plane - inertial axis of rotation

inertial tensor $\rightarrow$

symmetric real matrix $\Rightarrow$

by Spectral Thm. has an orthonormal eigenbasis.

Thus, every object sim to ellipsoid - 3

$\perp$ axes of rotation.

Rayleigh's Principle.

$A = A^T \in M_n(\mathbb{F})$

$q(\underline{x}) = \underline{x}^T A \underline{x}$

$$\boxed{R_A(\underline{x}) = \frac{q(\underline{x})}{\|\underline{x}\|^2}}$$ Rayleigh quotient.

$(\forall \mu \neq 0)(R_A(\mu \underline{x}) = R_A(\underline{x}))$

DO $(\exists \underline{x_0})(R_A(\underline{x_0}) = \max_{\underline{x} \neq \underline{0}} R_A(\underline{x}))$

$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \quad \lambda_n = \min_{\underline{x} \neq \underline{0}} R_A(x).$

Rayleigh's Principle: $\lambda_1 = \max_{\underline{x} \neq \underline{0}} R_A(\underline{x}).$ $\Bigg\}$ $\boxed{HW}$

(Hint: $q(\underline{x}) = 1$ can be expressed as $\sum \lambda_i \alpha_i^2 = 1$)

orthonormal basis of $\mathbb{R}^n$: basis $\underline{e_1}, \ldots, \underline{e_n}$

Def Orthonormal basis of $\mathbb{R}^n$: basis $\underline{e_1}, \ldots, \underline{e_n}$

s.t. $\underline{e_i} \cdot \underline{e_j} = \delta_{ij}$. (ex. standard basis.)

Suppose $e_1, \dots, e_n$ is ONB of $\mathbb{R}^n$.

$$[\underline{x}]_{\underline{e}} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \underline{\alpha} \qquad \underline{x} = \sum \alpha_i \underline{e_i}$$

$$\underline{y} = \sum \beta_i \underline{e_i}$$

$$[\underline{y}]_{\underline{e}} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \underline{\beta}$$

$$\underline{x} \cdot \underline{y} = \left(\sum_i \alpha_i \underline{e_i}\right)\left(\sum_j \beta_j e_j\right)$$

$$= \sum_i \sum_j \alpha_i \beta_j \underbrace{\underline{e_i} \cdot \underline{e_j}}_{0 \text{ unless } i=j} = \sum_i \alpha_i \beta_i \underline{e_i \cdot e_i}$$

$$= \sum_i \alpha_i \beta_i = \underline{\alpha} \cdot \underline{\beta}.$$

<u>Thm</u> $\underline{x} \cdot \underline{y} = \underline{\alpha} \cdot \underline{\beta}$ if $[\underline{x}]_{\underline{e}} = \underline{\alpha}$ and $[\underline{y}]_{\underline{e}} = \underline{\beta}$ in ONB $\underline{e}$.

$$\|x\|^2 = \underline{x} \cdot \underline{x} = \underline{\alpha} \cdot \underline{\alpha} = \|\alpha\|^2 = \sum \alpha_i^2$$

$$\underline{x} \perp \underline{y} \Leftrightarrow \underline{\alpha} \perp \underline{\beta}.$$

In ONB $q(\underline{x}) = \sum \lambda_i \alpha_i^2$ and $\|x\|^2 = \sum \alpha_i^2$.

Friday, July 14, 2017 11:53 AM

$\boxed{\text{Fischer - Courant Thm}}$

$$\boxed{\lambda_i = \max_{\substack{U \leq \mathbb{R}^n \\ \dim = i}} \min_{\substack{\underline{x} \in U \\ \underline{x} \neq \underline{0}}} R_A(\underline{x})}$$

$\boxed{\text{HW}}$ (for Tues.)

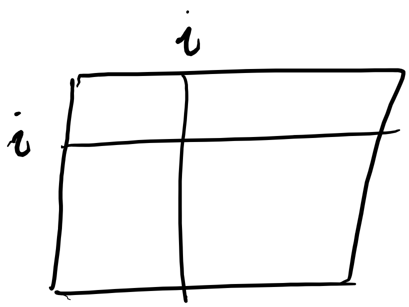
$U = \operatorname{span}(e_1, e_2)$

$$\min_{\substack{x \in U \\ x \neq 0}} R_A(x) = \lambda_2$$

by Rayleigh Principle

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

cut out i^{th} row and i^{th} column.



$B \in M_{n-1}(\mathbb{R})$ symm $\qquad B = \hat{i} A \hat{i}$ (removal.)

$A: \lambda_1 \geq \cdots \geq \lambda_n$

$B: \mu_1 \geq \cdots \geq \mu_{n-1}$

Eigenvalues interlace ... (follows from Fischer - Courant)

<u>Thm.</u> (Interlacing Theorem for eigenvalues of real matrices.)

$\boxed{HW}$ A is adjacency matrix of a graph $G = (V, E)$, with $|V| = n$.

Eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$.

Remember: $\lambda_1 \leq$ max degree.

Show: $\lambda_1 \geq$ avg. degree $= \dfrac{\sum_{a \in V} \deg(a)}{n} = \dfrac{2m}{n}$

(1 line based on Rayleigh's Principle).

Hint for Lemma assigned <u>Wed</u>:

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

f is polynomial s.t. $f(A) = \underline{\underline{0}}$

Suppose $f = g \cdot h$ s.t. $\gcd(g, h) = 1$.

Then $\mathbb{F}^n = \operatorname{Ker}(g(A)) \oplus \operatorname{Ker}(h(A))$.

Hint: gcd is a linear combination, with polynomials as coefficients.

* Reminder! $\boxed{HW}$ from Wed/Thurs. lectures due Mon.