Every ideal in $\mathbb{R}[x]$ is principal. (~~principle~~)

($\mathbb{R}[x]$: polynomials)

$I \trianglelefteq \mathbb{R}[x]$ means: $I \subseteq \mathbb{R}[x]$, $0 \in I$, closed under addition, $(\forall f \in I)(\forall g \in \mathbb{R}[x])(f \cdot g \in I)$

($\trianglelefteq$: ideal)

NTS: If $I \trianglelefteq \mathbb{R}[x]$ then $(\exists f)(I = f \cdot \mathbb{R}[x])$

Proof: Case 1: $I = \{0\}$ then $f := 0$ ✓

case 2: $I \neq 0$ $\therefore$ $\exists$ polynomials of degree ≥ 0 in I.

Let $f \in I$ be of lowest degree, $f \neq 0$. (suspect)

Obs. $f \in I \Rightarrow f \cdot \mathbb{R}[x] \subseteq I$

Claim. $f \cdot \mathbb{R}[x] = I$.

NTS: $f \cdot \mathbb{R}[x] \supseteq I$, i.e. $(\forall h \in I)(h \in f \cdot \mathbb{R}[x])$

($h \in f \cdot \mathbb{R}[x]$: i.e. $f \mid h$.)

Use Division Theorem: $\exists q, r$

$h = f \cdot q + r, \quad \deg r < \deg f$

$f \in I \Rightarrow f \cdot q \in I$
$h \in I$
$\Big\} \; r = h - f \cdot g \in I$

$\therefore \deg r < 0$ i.e. $\boxed{r = 0}$ $\therefore f \mid h.$ □

$\mathbb{Z}$

Alternate proof of existence of gcd

algorithmic proof, paraphrasing Euclid's proof.

$Div(a) = \{d \in \mathbb{Z} \mid d \mid a\} = \{$all divisors of $a\}$

$Div(a,b) = Div(a) \cap Div(b) = \{$common divisors of a and $b\}$

Thm. $(\forall a, b)(\exists d)(Div(a,b) = Div(d))$

↑ i.e. d is a greatest common divisor of a and b.

DO (Euclid's Lemma.)

$Div(a,b) = Div(a-b, b)$

(based on distributivity.)

DO $(\forall q)(Div(a,b) = Div(a-qb, b)$

Proof: Induction on q for $q \geq 0$ (and figure out what to do with the negatives.)

Note: $Div(a,b) = Div(b,a)$

$Div(a,0) = Div(a)$

$Div(a) = Div(|a|)$

$Div(a,b) = Div(|a|, |b|)$.

WLOG we may assume $a, b \geq 0$ ... in fact, (without loss of generality) $a, b > 0$.

Proof. By induction on $a+b$.

Base case: $a+b \leq 1 \rightarrow$ Done (at least one is 0)

Suppose $a, b \geq 1$, $a \geq b$ WLOG, so

$a \geq b \geq 1$. $\exists d$

$Div(a,b) = Div(a-b, b) = Div(d)$

$(a-b)+b = a < a+b$ — By inductive hypothesis.

□

Euclid's Algorithm (made efficient)

Input: (a, b) where $a \geq b \geq 1$

WHILE $a, b \geq 1$:

IF $b > a$ THEN $a \leftrightarrow b$ (swap a, b)

$a = bq + r$ by Div. Theorem

$(a, b) \leftarrow (b, r)$

END WHILE

RETURN a

Ex. $(72, 13)$

$72 = \underline{13} \cdot 5 + \underline{7}$

$\rightarrow (13, 7)$

$13 = \underline{7} \cdot 1 + \underline{6}$

$\rightarrow (7, 6)$

$7 = \underline{6} \cdot 1 + \underline{1}$

$\rightarrow (6, 1)$

$6 = \underline{1} \cdot 6 + \underline{0}$

$\rightarrow (1, 0)$ end return $\boxed{1}$.

Ex. $(76, 14)$ $\quad 76 = \underline{14} \cdot 5 + \underline{6}$

$\rightarrow (14, 6)$ $\quad 14 = \underline{6} \cdot 2 + \underline{2}$

$\rightarrow (6, 2)$ $\quad 6 = \underline{2} \cdot 3 + \underline{0}$

$\rightarrow (2, 0)$ end return $\boxed{2}$.

How do we know that Euclid's Algorithm stops?

$b = r_0 \quad a = r_{-1}$

(a, b)

(b, r_1)

(r_1, r_2)

By Div. Theorem, r is decreasing, so

$r_{-1} \geq r_0 > r_1 > r_2 > \cdots$

$\therefore$ Algorithm terminates in finite time:

$\leq b$ steps.

This is not very efficient for large #s ... but the algorithm moves faster than this.

HW Prove: # iterations in "efficient" Euclid's algorithm is $\leq 1 + 2\log_2 b$.

(Proof should be no more than 3 lines.)

DO Euclid's algorithm for polynomials.

(You can find a version of Euclid's algorithm for anything with a Division Theorem.)

Def. $\mathbb{F} \subseteq \mathbb{C}$ is a <u>number field</u> if

$0, 1 \in \mathbb{F}$ and $\mathbb{F}$ is closed under $+, -, \times, \div$ (other than by 0)

Ex. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ (rational #s)

Is $\{0, 1\}$ a number field?

no: $1+1=2$: not closed under addition

$\{a+bi \mid a, b \in \mathbb{Q}\}$ $\quad a_0 + a_1 i + a_2 i^2 + a_3 i^3 + \cdots$

$= \mathbb{Q}[i]$

If $\mathbb{F}$ is a <u>number field</u> and $\alpha \in \mathbb{C}$ then

$\mathbb{F}[\alpha] = \{f(\alpha) \mid f \in \mathbb{F}[x]\}$.

↖ polynomials over $\mathbb{F}$

(ie. if $f \in \mathbb{F}[x]$ and $f = a_0 + a_1 x + \cdots + a_n x^n$ then $a_i \in \mathbb{F}$ $(\forall i \in [n])$)

DO $\mathbb{Q}[i]$ is a number field. ($\mathbb{Q}[i]$ are called the "Gaussian rationals")

(NTS: $\frac{1}{a+bi}$ has same form.)

DO $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

This is a number field.

(Note: $(\sqrt{2})^3 = 2\sqrt{2}$, $(\sqrt{2})^4 = 4$, etc.)

DO* $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$

is a number field.

HW $\mathbb{Q}[\pi]$ is not a number field.

Hint: $\frac{1}{\pi} \notin \mathbb{Q}[\pi]$ and use the fact that

π is transcendental (not algebraic)

Def. $\alpha \in \mathbb{C}$ is an algebraic number if

$(\exists f \in \mathbb{Q}[t])(f \neq 0$ and $f(\alpha) = 0)$

Ex. i: $f = t^2 + 1$ $\sqrt[3]{2}$: $f = t^3 - 2$

$\sqrt{2}$: $f = t^2 - 2$

Thm. (Hard!) π is transcendental.

Note: $\mathbb{Z}$ not closed under division.

(DO) If $\mathbb{F}$ is a number field, then $\mathbb{Q} \subseteq \mathbb{F}$.

we can do linear algebra over $\mathbb{F}$ - number fields.

"scalars"

HW over $\mathbb{C}$, $rk(A^TA) = rk(A)$ is not always true.

(Find a counterexample - as simple as possible.)

Suppose $\mathbb{F}, \mathbb{G}$ are number fields s.t. $\mathbb{F} \subseteq \mathbb{G}$.

Then $\mathbb{G}$ is an extension field of $\mathbb{F}$.

Ex. $\mathbb{C}$ is an extension field of every number field.

$\mathbb{G}$ can be viewed as a vector space over $\mathbb{F}$.

HW $1, \sqrt{2}, \sqrt{3}$ are lin. indep. over $\mathbb{Q}$.

CH $\{\sqrt{p} \mid p \text{ prime}\}$ is lin. indep. over $\mathbb{Q}$.

HW $\dim_{\mathbb{Q}}(\mathbb{R}) = \infty$

(Proof: 2-3 lines.)

Estados Unidos = EEUU

$\dim_{\mathbb{R}}(\mathbb{C}) = 2$

$\dim_{\mathbb{F}}(\mathbb{F}) = 1$

CCHH If $\dim_{\mathbb{F}}(\mathbb{C})$ is finite, then $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

DO $\dim_{\mathbb{Q}}(\mathbb{Q}[i]) = 2$

$\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) = 2$

$\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}]) = 3$

DO* $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{ f(\sqrt{2}, \sqrt{3}) \mid f(x,y) \in \mathbb{Q}[x,y] \}$

Prove: number field and find dim over $\mathbb{Q}$.

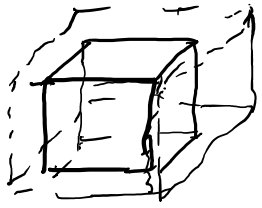
polynomials in 2 vars.

DO If $\mathbb{F} \subset \mathbb{G} \subset \mathbb{H}$ then

number fields

$\dim_{\mathbb{F}} \mathbb{H} = (\dim_{\mathbb{F}} \mathbb{G})(\dim_{\mathbb{G}} \mathbb{H})$.

Consequence: Cube cannot be doubled.



(Ancient Greek problem - given a cube, construct a cube using straightedge and compass with double the volume.)

Can you construct $\sqrt[3]{2}$ from 1?

we can construct numbers from a chain of field extensions

$$\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_k$$

$$\dim_{\mathbb{F}_i} \mathbb{F}_{i+1} = 2, \quad \therefore \dim_{\mathbb{Q}} \mathbb{F}_k = 2^k$$

Claim $\sqrt[3]{2} \notin \mathbb{F}_k$.

Suppose $\sqrt[3]{2} \in \mathbb{F}_k$. Then $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{F}_k$.

$\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{2}] = 3$ and $\dim_{\mathbb{Q}[\sqrt[3]{2}]} \mathbb{F}_k = s$, so

$2^k = 3 \cdot s \rightarrow$ a contradiction. □

$\begin{bmatrix} 1 & 2 & 3 \\ 6 & 9 & 17 \\ -1 & 0 & 55 \end{bmatrix}$ What is the rank of this matrix?

- over what field?

It doesn't matter -- $rk_{\mathbb{F}} A$ is the same for all number fields.

HW Let $\mathbb{F} \subset \mathbb{G}$ be number fields. $A \in \mathbb{F}^{k \times l}$. Prove: $rk_{\mathbb{F}}(A) = rk_{\mathbb{G}}(A)$

OR Example (solve for full credit :) Let $A \in \mathbb{Q}^{k \times l}$. Prove: $rk_{\mathbb{Q}}(A) = rk_{\mathbb{R}}(A)$.

HW $\gcd(2^k - 1, 2^l - 1) = 2^d - 1$ where $d = \gcd(k, l)$.

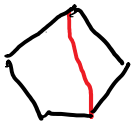
Def Fibonacci numbers:

$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}$

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89 ...

DO $\lim_{n \to \infty} \frac{F_{n+1}}{F_n}$ = golden ratio = $\frac{1+\sqrt{5}}{2}$

Béla Bartók - Concerto — 89 beats - 55 in reverse, 34 clear.
(based on Fibonacci #s)

Golden Ratio:  ratio of — to — is the Golden Ratio

HW $\gcd(F_{n+1}, F_n) = 1$

CH (a) $k \mid \ell \Rightarrow F_k \mid F_\ell$

(b) $(\forall k, \ell)\ (\gcd(F_k, F_\ell) = F_d$ where $d = \gcd(k, \ell))$

(Hint: for elegant solution, look at powers of $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.)

Euler's φ function ("totient function")

$\varphi(n) = |\{ i \mid 1 \le i \le n,\ \underbrace{\gcd(i,n) = 1}_{\text{relatively prime}} \}|$

$\varphi(1) = 1$ (just 1)
$\varphi(2) = 1$ (just 1)
$\varphi(3) = 2$ (1, 2)
$\varphi(4) = 2$ (1, 3)
$\varphi(5) = 4$ (1, 2, 3, 4)
$\varphi(6) = 2$ (1, 5)

$\varphi(p) = p - 1 = p\left(1 - \frac{1}{p}\right)$ ← (1, 2, ..., p-1)

$\varphi(p^2) = p^2 - p = p^2\left(1 - \frac{1}{p}\right)$

$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$

DO The φ function is multiplicative: if $\gcd(a,b) = 1$ then $\varphi(a,b) = \varphi(a)\varphi(b)$.

∴ If $n = p_1^{k_1} \cdots p_s^{k_s}$ where p_i are distinct primes,

then $\varphi(n) = n \prod \left(1 - \frac{1}{p_i}\right)$.

CH $A = (\gcd(i,j))_{n \times n}$

Prove: $\det A = \varphi(1)\varphi(2)\cdots\varphi(n)$.

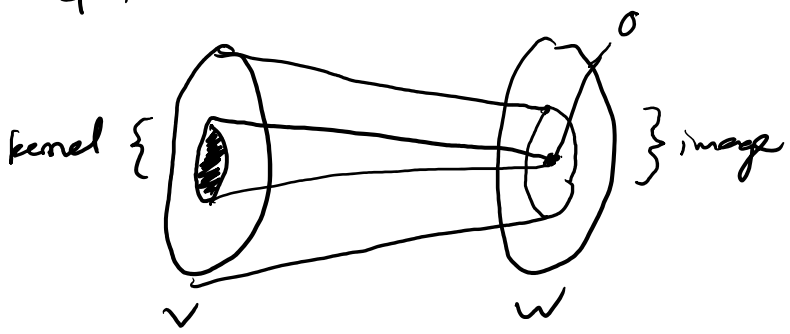
Al Biruni – born in the Persian province of Kwarizm

Linear map: $\varphi: V \to W$ (over both $\mathbb{F}$)

Thm If $\dim_{\mathbb{F}} V = k$, then $V \cong \mathbb{F}^k$.

Kernel of φ: $\ker \varphi = \varphi^{-1}(0) = \{v \in V \mid \varphi(v) = 0\}$

Image of φ: $\operatorname{im} \varphi = \{\varphi(v) \mid v \in V\}$.



(DO) Prove: $\ker(\varphi) \leq V$ (subspaces)
$\operatorname{im}(\varphi) \leq W$

Thm. (Rank-Nullity Thm.)

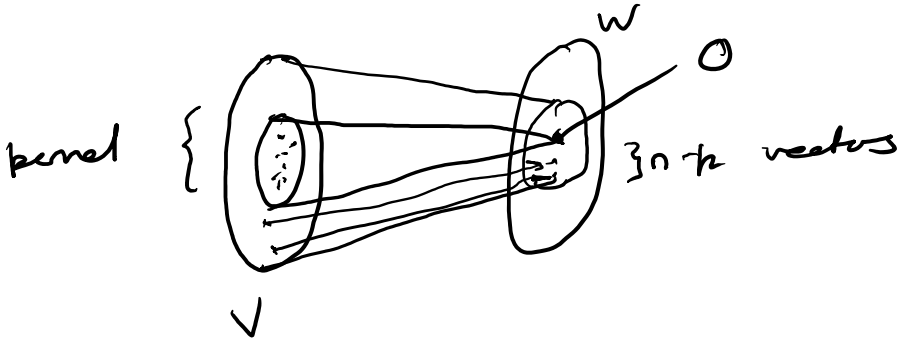
$\dim(\ker \varphi) + \dim(\operatorname{im} \varphi) = \dim V.$

Def $\operatorname{rk}(\varphi) := \dim(\operatorname{im} \varphi)$

$\operatorname{nullity}(\varphi) := \dim(\ker \varphi)$

(DO) $\operatorname{rk}(\varphi) = \operatorname{rk}([\varphi]_{\underline{e},\underline{f}})$ where $\underline{e}$ = basis in V
$\underline{f}$: basis in W.

Proof. (of rank-nullity thm.)



Let $\dim(\ker \varphi) = k$ and $\dim V = n$. Pick
$e_1, e_2, \ldots, e_k$: basis of $\ker \varphi$. Extend this
to a basis $e_1, e_2, \ldots, e_n$ of V.

$f_j = \varphi(e_{k+j})$ (note $\varphi(e_i) = 0$ if $i \leq k$.)

Claim: $f_1, \ldots, f_{n-k}$ is a basis of $\operatorname{im}(\varphi)$.

(DO) Verify $\operatorname{span}(f_1, \ldots, f_{n-k}) = \operatorname{im} \varphi$.

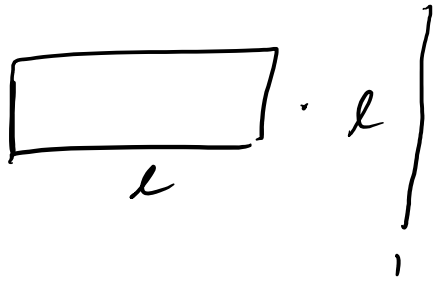
(DO) Prove: $f_1, \ldots, f_{n-k}$ are lin indep

□

Conclusion: $\dim(\operatorname{im} \varphi) = n - k$.

$\{x \in \mathbb{F}^\ell \mid Ax = 0\}$ $\quad A \in \mathbb{F}^{k \times \ell}$

$= \ker A$



eqns: k

unknowns: ℓ

View A as a linear map $\mathbb{F}^\ell \to \mathbb{F}^k$:

$x \longmapsto Ax$

φ

$\dim(\ker A) = \ell - \operatorname{rk}(A)$

set of solutions of homogeneous lin. system of equations.

$\operatorname{im} A = \{Ax \mid x \in \mathbb{F}^\ell\}$ ← maps to

(DO) Prove $\operatorname{rk} A = \dim \operatorname{im} A$.

$$\begin{bmatrix} x_1 \\ \vdots \\ x_\ell \end{bmatrix} \qquad \begin{aligned} a_{11}x_1 + \cdots + a_{1\ell}x_\ell &= 0 \\ a_{21}x_1 + \cdots + a_{2\ell}x_\ell &= 0 \\ a_{31}x_1 + \cdots + a_{3\ell}x_\ell &= 0 \\ &\vdots \end{aligned}$$

reduce a degree of freedom with each new equation (unless lin. dep.)

$$\dim(\text{space of sol's}) = \ell - k$$

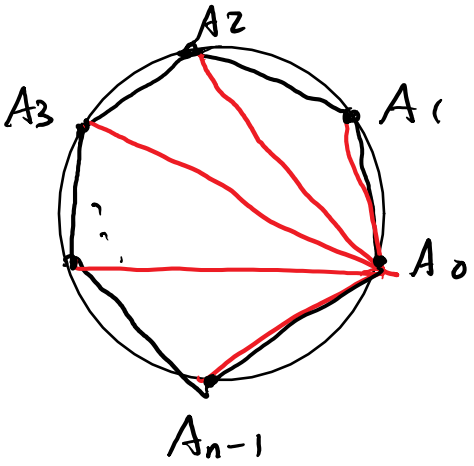
(if eqn's lin. indep

John von Neumann
(formalized quantum mechanics; driver of computer + nuclear projects)

DO (Modular identity)
If $U, W \subseteq V$, then $\dim(U \cap W) + \dim(U + W) = \dim(U) + \dim(W)$.

DO $U + W = \text{span}(U, W)$.
(Note $U + W := \{u + w \mid u \in U, w \in W\}$.)

DO Cor. Let $n = \dim V$. If $\dim U + \dim V > n$, then $U \cap W \neq \{0\}$.



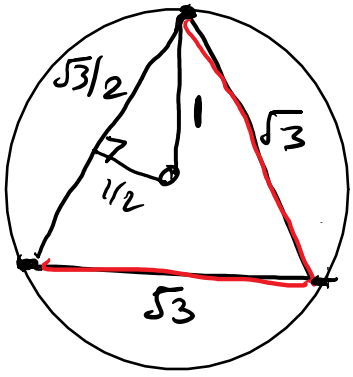
unit circle

CH $\prod_{i=1}^{n-1} \overline{A_0 A_i} = n$

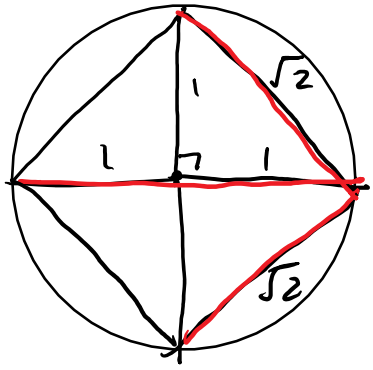
length

(Proof: 5 lines)

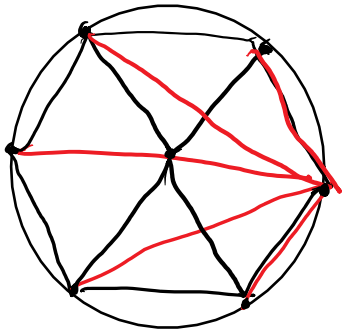
$n = 3$



$n = 3$ $\quad \sqrt{3} \cdot \sqrt{3} = 3$



$n = 4$ $\quad \sqrt{2} \cdot 2 \cdot \sqrt{2} = 4$



$n = 6$ $\quad 1 \cdot \sqrt{3} \cdot 2 \cdot \sqrt{3} \cdot 1 = 6$

Monic polynomials over $\mathbb{C}$

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n \qquad a_n = 1$$

$$= (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n)$$

$\alpha_i \in \mathbb{C}$ roots

(not necessarily distinct)

Coefficients vs. roots

$$a_0 = (-1)^n \prod \alpha_i \quad = f(0)$$

$$a_{n-1} = -\sum \alpha_i$$

$$a_{n-2} = \alpha_1\alpha_2 + \alpha_1\alpha_2 + \cdots = \sum_{i<j} \alpha_i\alpha_j$$

$$a_{n-3} = -\sum_{i<j<k} \alpha_i\alpha_j\alpha_k$$

$$\vdots$$

$$\sigma_1(x_1, \ldots, x_n) = x_1 + \cdots + x_n$$

$$\sigma_2(x_1, \ldots, x_n) = \sum_{i<j} x_i x_j \qquad \sigma_n = \prod_{i\in[n]} x_i.$$

$$\sigma_3(x_1, \ldots, x_n) = \sum_{i<j<k} x_i x_j x_k$$

# of terms in σ_i : $\binom{n}{i}$

Thm $a_{n-i} = (-1)^i \sigma_i(\alpha_1, \ldots, \alpha_n)$ (DO)

HW Pirate's treasure.

$f \in \mathbb{R}[x]$

$f(x) = x^{100} + 5x^{99} + 13x^{98} + \cdots$

Prove: not all roots are real. (2 lines).