ALGEBRA lineare 17/05/2017.

- Dato un endomorfismo, questo è diagonalizzabile se e solo se esiste una base di V formata da autovettori $\{v_1, \dots, v_n\}$

- Se $[f]^{standard}_{standard} \Rightarrow [f]^{\mathcal{B}}_{\mathcal{B}} = D = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$

Non sempre esiste la base formata da autovettori.

A = matrice di f secondo una base $\mathcal{E}$ di partenza

$$A = [f]^{\mathcal{E}}_{\mathcal{E}}$$

Calcolo il polinomio caratteristico

$$P_f(x) = P_A(x) = \det(A - xI) \Rightarrow \text{polinomio di grado } n$$

dove $n = \dim V$.

cerco gli autovalori $\Rightarrow$ Radici del polinomio

$\lambda_1, \dots, \lambda_k$ k può non essere uguale a n. $k \leq n$

$p(x)$ può essere espresso come

$$p(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_k)$$

$(x-\lambda_1) \mid p(x)$

$(x-\lambda_2) \mid p(x)$ $\Rightarrow (x-\lambda_1)(x-\lambda_2) \mid p(x)$

e così via solo perché son irriducibili

TUTTO QUELLO CHE VALE PER I NUMERI VALE ANCHE PER I POLINOMI

se i fattori sono n $(\lambda_n, n=k)$ allora tutto regolare, altrimenti può essere del tipo $p(x) = (x-\lambda_1)^{a_1}(x-\lambda_2)\cdots q(x)$.

La molteplicità algebrica dell'autovalore λ_i è il massimo esponente a_i t.c.

$$(x-\lambda_i)^{a_i} \mid p(x)$$

es: $p(x) = (x-3)^2(x-5)^3$

radice 3 con molteplicità 2.

5 " " 3.

molteplicità geometrica:

riferita all'autovalore λ è la dimensione dell'autospazio ⇒ quanti autovettori indipendenti ci sono con quel λ.

$$mg(\lambda) = \dim(V_\lambda)$$

$$V_\lambda = \{v \in V \mid f(v) = \lambda v\} = \ker(A - \lambda I)$$

TEOREMA:

1) $mg(\lambda) \leq ma(\lambda)$ λ è un autovalore

2) f è diagonalizzabile se e solo se $mg(\lambda) = ma(\lambda) \quad \forall \lambda$.

3) se f ha n autovalori diversi ⇒ è diagonalizzabile.

es: $f: \mathbb{R}^3 \to \mathbb{R}^3$ $\quad [f]^{std.}_{std} = \begin{pmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{pmatrix} = A$

$$p_f(x) = \det \begin{pmatrix} -x & 2 & 2 \\ 2 & -x & 2 \\ 2 & 2 & -x \end{pmatrix} = x^3 - 12x - 16.$$

es: $t: \mathbb{R}^3 \to \mathbb{R}^3$

$$[T]^{std}_{std} = \begin{pmatrix} 0 & 0 & -3 \\ -5 & 5 & 1 \\ 2 & -2 & -1 \end{pmatrix}$$

$P_t(x)$ = "sottraggo x dalla diagonale" =

$$= -\det \begin{pmatrix} -x & 0 & -3 \\ -5 & 5-x & 1 \\ 2 & -2 & -1-x \end{pmatrix} = -x\left(x^2-4x+3\right)$$

$x=0$ 1ª radice

$$x^2-4x+3=0 \qquad x = 2 \pm \sqrt{4-3} = 2 \pm 1$$

$p(x) = -x(x-3)(x-1)$ gli autovalori sono $\to 0, 3, 1$

(diversi tra loro $\Rightarrow$ t è diagonalizzabile).

$$D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

troveremo 3 autovettori

$v_0 : f(v_0) = 0$

$v_3 : f(v_3) = 3v_3$

$v_1 : f(v_1) = 1v_1$

gli autovettori con autovalori distinti sono autovettori indipendenti e formano una base (se #autovettori $= n$ (dim V)).

dimostrazione del punto 3)

V_1, V_2 sottospazi di V

$V_1, \dots, V_k$ sono in somma diretta se

$\forall v_1 \in V_1 \setminus \{0\}, v_2 \in V_2 \setminus \{0\}, \dots, v_k \in V_k \setminus \{0\}$

$\Rightarrow v_1, \dots, v_k$ sono indipendenti.

quindi $V_1, \dots, V_k$ indipendenti $\Leftrightarrow$

$V_1 \cap (V_2 + \dots + V_k) = \{\bar{0}\}$

$V_2 \cap (V_1 + \dots + V_k) = \{\bar{0}\}$

$\vdots$ per tutti i V_i.

Teorema

Se $\lambda_1, \dots, \lambda_k$ sono autovalori distinti di f

$v_1 \in V_{\lambda_1} \setminus \{0\} \quad \dots \quad v_k \in V_{\lambda_k} \setminus \{0\}$

$\Rightarrow v_1, \dots, v_k$ sono indipendenti quindi $V_{\lambda_1}, \dots, V_{\lambda_k}$ sono in somma diretta

dimostrazione *

per $k=2$

$\lambda_1 \neq \lambda_2 \Rightarrow V_{\lambda_1} \oplus V_{\lambda_2}$ (da dimostrare)

$\Rightarrow V_{\lambda_1} \cap V_{\lambda_2} = \{\bar{0}\}$

supponga

$v \in V_{\lambda_1} \cap V_{\lambda_2}$

$\Rightarrow f(v) = \lambda_1 v = \lambda_2 v$

$\Downarrow$

$(\lambda_1 - \lambda_2) v = 0$ ma $\lambda_1 - \lambda_2 \neq 0$

$\Rightarrow v = 0 \Rightarrow V_{\lambda_1} \cap V_{\lambda_2} = \{\bar{0}\}$

es: $V_1 = \text{span}\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix}\right)$

$V_2 = \text{span}\left(\begin{pmatrix}1\\1\\0\end{pmatrix}\right)$

$\Big\rangle$ non sono in somma diretta $\Rightarrow$ non formano una base

$V_1 = \text{span}\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix}\right)$

$V_2 = \text{span}\left(\begin{pmatrix}0\\0\\3\end{pmatrix}\right)$

$\Big\rangle$ sono in somma diretta $\Rightarrow$ i 3 vettori formano una base.

* $k > 2$ induzione su k

$a_1 v_1 + a_2 v_2 + \dots + a_k v_k = 0$

$\downarrow$ applico la f

$a_1 f(v_1) = a_1 \lambda_1 v_1$ (e così per tutti)

$\Rightarrow a_1 \lambda_1 v_1 + a_2 \lambda_2 v_2 + \dots + a_k \lambda_k v_k = \bar{0}$ (II)

moltiplico la prima equazione $\cdot \lambda_1$

$$a_1\lambda_1 v_1 + a_2\lambda_1 v_2 + \dots + a_k\lambda_1 v_k = 0 \quad (III)$$

sottraggo (II) − (III)

$$\Rightarrow a_2(\lambda_2-\lambda_1)v_2 + \dots + a_k(\lambda_k-\lambda_1)v_k = 0 \quad (IV)$$

$v_2 \dots v_k$ sono $k-1$ autovettori con autovalori distinti.

per ipotesi induttiva sono indipendenti

$\Rightarrow$ i coefficienti di (IV) sono $= 0$

$$a_2\underbrace{(\lambda_2-\lambda_1)}_{\neq 0}, \dots, a_k\underbrace{(\lambda_k-\lambda_1)}_{\neq 0}$$

$$\Downarrow$$

$$a_2 = \dots = a_k = 0.$$

quindi rimane

$$a_1 v_1 = 0 \Rightarrow a_1 = 0 \Rightarrow v_1, \dots, v_k \text{ sono indipendenti}$$

es: Tipico d'esame

$$L_k : \mathbb{R}^4 \to \mathbb{R}^4 \quad \text{lineare}$$

$$\left[L_k\right]^{std}_{std} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -k^2 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & k^2+1 & 0 \end{pmatrix}$$

Per quali k è diagonalizzabile?

1) Calcolo polinomio caratteristico

$$p(\lambda) = \det(\lambda I - A) =$$

$$= \det\begin{pmatrix} \lambda & -1 & 0 & 0 \\ 0 & \lambda & k^2 & 0 \\ 0 & 0 & \lambda & -1 \\ -1 & 0 & -k^2-1 & \lambda \end{pmatrix}$$

· sviluppo secondo la prima riga:

$$\lambda \det\begin{pmatrix} \lambda & k^2 & 0 \\ 0 & \lambda & -1 \\ 0 & -k^2-1 & \lambda \end{pmatrix} + \det\begin{pmatrix} 0 & k^2 & 0 \\ 0 & \lambda & -1 \\ -1 & -(k^2+1) & \lambda \end{pmatrix}$$

sviluppo secondo la 1ª colonna

$$= \lambda\lambda \det\begin{pmatrix} \lambda & -1 \\ -(k^2+1) & \lambda \end{pmatrix} + (-1)\det\begin{pmatrix} k^2 & 0 \\ \lambda & -1 \end{pmatrix} =$$

sviluppo secondo la 1ª colonna

$$\lambda^2(\lambda^2 - k^2 - 1) + k^2 =$$

$p(x) = \lambda^4 - (k^2+1)\lambda^2 + k^2 = 0$ → con trovo le radici

$\lambda^2 = x$ $\qquad x^2 - (k^2+1)x + k^2 = 0$

$$x = \frac{k^2+1 \pm \sqrt{(k^2+1)^2 - 4k^2}}{2}$$

$$(k^2+1)^2 - 4k^2 = k^4 + 1 + 2k^2 - 4k^2 =$$
$$= k^4 - 2k^2 + 1 =$$
$$= (k^2-1)^2$$

$$x = \frac{k^2+1 \pm (k^2-1)}{2} \quad \begin{cases} \frac{k^2+1+k^2-1}{2} = k^2 \\ \frac{k^2+1-k^2+1}{2} = 1 \end{cases}$$

$\lambda^2 = k^2 \Rightarrow \lambda = \pm k$

$\lambda^2 = 1 \Rightarrow \lambda = \pm 1$

è diagonalizzabile se $k \neq \pm 1$

autovalori

$p(x) = (x-1)(x+1)(x-k)(x+k)$

$k \neq \pm 1$ $\qquad D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & k & 0 \\ 0 & 0 & 0 & -k \end{pmatrix}$ → l'ordine degli autovalori è dato dall'ordine degli autovettori che ho nella base B.

studio i casi in cui $k=1$, $k=-1$

$p(x) = (x-1)(x+1)(x-1)(x+1) =$
$= (x-1)^2(x+1)^2$ $\qquad 1, -1$ hanno ma $= 2$.

se $k=1$

$$A=\begin{pmatrix}0&1&0&0\\0&0&-1&0\\0&0&0&1\\1&0&2&0\end{pmatrix}=L_1$$

ora guardo che $mg=2$.

- Calcolo gli autospazi

$$V_1=\ker(L_1-1\,I)=\ker(1\,I-L_1)=$$

$$=\ker\begin{pmatrix}-1&1&0&0\\0&-1&-1&0\\0&0&-1&1\\1&0&2&-1\end{pmatrix}$$

righe e colonne indipendenti.

↑ minore con $\det\neq 0$

↓ rango $=3$

$\dim(\ker)=1$

$\dim(V_1)=1 \Rightarrow$ non è diagonalizzabile.

Dimostriamo che se f è diagonalizzabile

$\Rightarrow ma(\lambda)=mg(\lambda)\quad\forall\lambda_i$

nell'esempio:

V_1 V_{-1} per $k=1$

↓

salo in somma diretta $V_1\oplus V_2$

con $\dim(V_1)\leq ma(1)=2$

$\dim(V_{-1})\leq ma(-1)=2$ → esponenti

ma in V_1 ne abbiamo 1 solo di vettori indipendenti

RICEVIMENTO COLLETTIVO 18/05/2017

Es: combinatoria.

- 22 persone. Quanti modi di dividere in 2 squadre da 11?

domanda ambigua.

① se le squadre sono distinguibili (es A, B) allora due persone in A ≠ dalle stesse persone in B.

② squadre indistinguibili.

① $\binom{22}{11}$ modi di formare la squadra A

1 modo per formare l'altra

$$\frac{\binom{22}{11}}{}$$

② $a_1 \dots a_{11}$ in A $\quad = \quad a_1 \dots a_{11}$ in B
$b_1 \dots b_{11}$ in B $\quad\quad b_1 \dots b_{11}$ in A.

per ogni ripartizione delle squadre distinguibili ce ne è una dell'ecando problema

$$\binom{22}{11} \cdot \frac{1}{2}$$

Es: combinatoria

- 30 alunni da distribuire in 3 aule A, B, C.

1) nessun vincolo

2) tutte le classi uguali

3) tutte le classi non vuote.

1) 3^{30} ⇒ per ogni persona ho 3 scelte.

2) $\binom{30}{10}$ in A.

$\binom{20}{10}$ in B

1 in C

$\Rightarrow \binom{30}{10} \cdot \binom{20}{10}$

3) Tutte le classi - ≠ car abbiano 1 vuota.

3^{30} ↑ conto le $\{$funzioni $: [30] \to [3]\}$ X

↑ di anequazione (ogni studente in una classe o nessuna).

$X_A \subseteq X = \{f \mid f : [30] \to \{B, C\}\}$

X_B e X_C

$\#X_A = 2^{30}$ $\#X_B = 2^{30}$ $\#X_C = 2^{30}$

almeno una classe vuota ⇒ unione ⇒ $X_A \cup X_B \cup X_C$.

$$\#(X_A \cup X_B \cup X_C) = \#X_A + \#X_B + \#X_C - \#(X_A \cap X_B) + - \#(X_B \cap X_C) - \#(X_A \cap X_C) + + \#(X_A \cap X_B \cap X_C) =$$

$$= 2^{30} + 2^{30} + 2^{30} - 1 - 1 - 1 + 0 = 3 \cdot 2^{30} - 3$$

Soluzione $3^{30} - (3 \cdot 2^{30} - 3)$.

Es: $\sum_{i=0}^{5} \binom{5}{i} 2^i = ? = (1+2)^5 = 3^5$

↑ dal binomio di Newton.

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

$x = 1$ $y = 2$

1) Targhe di 13 caratteri $\{0, 1, \dots, 9, A\}$

totale delle targhe?

1) ogni targa è una stringa di 13

1ª posizione 2ª posizione

11 modi 11 modi $\dots \Rightarrow 11^{13}$

2) dove metto le A? 3 A in targa

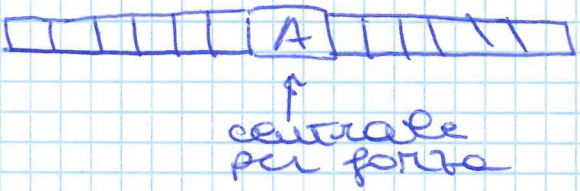
$\binom{13}{3} \cdot 10^{10}$ → modi di riempire le altre caselle.

3) esattamente 3 A calcolate?

11 modi → calcolo a mano.

$11 \cdot 10^{10}$

4) esattamente 3 A e palindrome.



· dove metto la A → 6 posti

per i restanti 5 posti $\Rightarrow 10^5$ possibilità.

$6 \cdot 10^5 \cdot (1)$

unico modo per riempire l'altra parte

5) Con <u>almeno</u> 3 A.

usiamo il complemento

tutte le targhe − # 0 A − # 1 A − # 2 A

11^{13} 10^{13} $13 \cdot 10^{12}$ $\binom{13}{2}(10^{11})$

$$11^{13} - 10^{13} - 13 \cdot 10^{12} - \binom{13}{2} \cdot 10^{11}$$

es: complessi.

$\sqrt[20]{1} \Rightarrow z^{20} = 1$ cerco le radici

$z = 1, -1, i, -i$

$z = \rho e^{i\theta}$ $\quad z^{20} = (e^{i\theta})^{20} = e^{i20\theta} = 1$

$\rho = 1$

$e^{i\gamma} = 1$ se $\gamma = 2\pi k$

$\theta = 2\pi\gamma \Rightarrow z^{20} = (e^{i2\pi\gamma})^{20} = e^{i2\pi\gamma \cdot 20} = 1$

$2\pi\gamma 20 = 2\pi k$

$\gamma = \frac{k}{20}$

le radici: $z = e^{i2\pi\left(\frac{k}{20}\right)} \quad 0 \le k < 20$

$z^{20} = e^{i2\pi\frac{k}{20}\cdot 20} = e^{i2\pi k} = 1$

Matematica discreta 18/05/2017

es:

$x^3 \equiv 1 \ (31)$ Trovare tutte le soluzioni

- una soluzione ovvia $\Rightarrow x \equiv 1 \ (31)$

$x^3 - 1 \equiv 0 \ (31)$

si parla del polinomio $x^3 - 1 = p(x)$ mo modulo 31. $\Downarrow$ $x^3 - 1 = 0$ in $\mathbb{Z}/(31)$

importante che sia un campo.

$p(1) = 0 \Rightarrow 1$ è radice.

$\Downarrow (x-1) \mid p(x) \Rightarrow p(x) = (x-1)q(x)$

$x^3 - 1 \ \big| \ x - 1$

$x^3 - x^2 \ \big| \ x^2 + x + 1$

$x^2 - 1$

$x^2 - x$

$x - 1$

$x - 1$

$(x^2 + x + 1)(x - 1) = p(x)$.

$$x^3-1 \equiv 0 \ (31)$$

$$\Downarrow$$

$$(x-1)(x^2+x+1) \equiv 0 \ (31)$$

$\vee$ prodotto di 2 numeri che fa 0 $\Rightarrow$ uno dei due è ϕ. (POSSIBILE perché siamo in un campo)

$$\begin{cases} \vee & x-1 \equiv 0 \ (31) \\ & x^2+x+1 \equiv 0 \ (31) \end{cases}$$

$\downarrow$ polinomio di II° grado

$\downarrow$ cerco le radici mod (31)

si provano a mano

$x = 5$ è soluzione.

$x = 5 + 31\ell$.

Visto che 5 è soluzione di x^2+x+1 posso dividere il polinomio per $(x-5)$

$$\begin{array}{r|l} x^2+x+1 & x-5 \\ \hline x^2-5x & x+6 \\ \hline / \quad 6x+1 & \\ \quad 6x+31 \rightarrow -30 \text{ mod } (31) & \\ \hline \quad // & \end{array}$$

$$x^2+x+1 = (x-5)(x+6) \text{ mod } (31)$$

$$(x-5)(x+6) \equiv 0 \ (31)$$

$$\Downarrow$$

$$\begin{cases} \vee & x \equiv 5 \ (31) \\ & x \equiv +6 \ (31) \end{cases}$$

$$x^3-1 \equiv (x-1)(x-5)(x+6) \ (31)$$

$$(x-1)(x-5)(x+6) \equiv 0 \ (31)$$

in $\mathbb{C}[x]$ tutti i polinomi possono essere fattorizzati con polinomi di primo grado (cosa che in $\mathbb{R}[x]$ non è sempre possibile).

$$p(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)a$$

fattori irriducibili

λ_i sono radici.

in $\mathbb{R}[x]$ i fattori irriducibili possono essere anche di grado II.

in $\mathbb{Q}[x]$ molto più difficile ma abbiamo un vantaggio: possiamo vedere "subito" se ci sono o no delle radici.

Lemma di Gauss:

Sia un polinomio a coefficienti interi irriducibile in $\mathbb{Q}[x]$ se e solo se è irriducibile in $\mathbb{Z}[x]$.

Cercare le radici razionali di un polinomio a coefficienti interi è facile:

1) $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$.

ho una radice razionale $\frac{r}{s}$ $r, s \in \mathbb{Z}$ $(r,s)=1$?

per capire se $\frac{r}{s}$ è radice sostituisco e deve fare $\emptyset$.

$$\cdot s^n \left(a_0 + a_1\frac{r}{s} + a_2\frac{r^2}{s^2} + \ldots + a_n\frac{r^n}{s^n} = 0 \right.$$

$$\underbrace{s^n a_0 + a_1 r s^{n-1} + \ldots}_{\text{sono multipli di } s} + \underbrace{a_n r^n}_{\text{anche questo deve essere un multiplo di } s.} = 0$$

$s \mid a_n r^n$ ma $(s,r)=1 \Rightarrow s \mid a_n$.

così ho limitato la scelta del denominatore.

lo stesso ragionamento vale per limitare la scelta di s:

tutti i termini, escluso il primo $a_0 s^n$ sono multipli di $r \Rightarrow$ anche $a_0 s^n$ è multiplo di r

$$r \mid a_0 s^n \quad \text{ma} \quad (r, s) = 1 \Rightarrow r \mid a_0.$$

es:

$f(x) = x^3 - x^2 - 8x + 12$ in $\mathbb{Q}[x]$

1) è riducibile?

2) ha radici in $\mathbb{Q}[x]$?

2) $\Rightarrow$ 1)

1) $\Rightarrow$ 2) in generale no!

ma siccome ha grado 3 allora sì

ha sicuramente un polinomio di grado 1 e un altro di grado 2 $\Rightarrow$ quello di grado 1 ha sicuro una radice cioè è a sua volta radice di $f(x)$.

$\frac{r}{s} \in \mathbb{Q}$ $\quad r \mid 12$ e $s \mid 1$

$r = 1, 2, 3, 4, 6, 12$

$-1, -2, -3, -4, -6, -12$

$f(2) = 8 - 4 - 16 + 12 = 0$ ✓ la base

$f(2) = 0 \Rightarrow$ 2 è una radice.

È Riducibile.

3) trovare tutte le radici? (in $\mathbb{Q}$)

4) fattorizzarlo in irriducibili

faccio la divisione con $x - 2$

$$
\begin{array}{r|l}
x^3 - x^2 - 8x + 12 & x - 2 \\
\cline{2-2}
x^3 - 2x^2 & x^2 + x - 6 \\
\cline{1-1}
\quad x^2 - 8x + 12 & \\
\quad x^2 - 2x & \\
\cline{1-1}
\quad -6x + 12 & \\
\quad -6x + 12 & \\
\cline{1-1}
\quad 0 &
\end{array}
$$

$$x^3 - x^2 - 8x + 12 = (x-2)(x^2+x-6)$$

$$x^2 + x - 6 = 0 \qquad x = \frac{-1 \pm \sqrt{1+24}}{2} = \frac{-1 \pm 5}{2} \begin{cases} -3 \\ 2 \end{cases}$$

$$x^3 - x^2 - 8x + 12 = (x-2)^2(x+3)$$

la radice $= 2$ ha molteplicità 2.
" $= 3$ " " 1.

abbiamo trovato "3" radici $\Rightarrow$ non ci sono più radici reali (o $\mathbb{C}$).

Se K è un campo ($\mathbb{R}, \mathbb{Q}, \mathbb{C}, \not{\mathbb{Z}}$) quasi tutto quello che vale in $\mathbb{Z}$ vale in $K[x]$

es. Bezout
numeri primi
Euclide.

↳ $\mathrm{mcd}(x^2+5x+6, x^2+6x+8)$

↓ intendiamo M $\Rightarrow$ grado più alto.

possiamo ottenere da uno i multipli degli altri.

$(x^2-5x+6, x+2)$

↓ $-x(x+2)$

$(3x+6, x+2) = (x+2, x+2) = x+2$ mcd.

$\Rightarrow 2$ è una radice di entrambi i polinomi

possiamo scrivere sempre combinazione lineare.

$x+2 = \square\,(x^2+5x+6) + \square\,(x^2+6x+8)$

non dei polinomi (ma già interi)

$x^2+5x+6 = 1\,(x^2+5x+6) + 0\,(x^2+6x+8)$

$x^2+6x+8 = 0\,(x^2+5x+6) + 1\,(x^2+6x+8)$

$x+2 = -1\,(x^2+5x+6) + 1\,(x^2+6x+8)$

$R_2 - xR_3 \Rightarrow \quad 3x+6 = x\,(x^2+5x+6) + (1-x)(x^2+6+8)$

Anello A

$a \in A$ irriducibile se non posso scriverlo come $a=bc$ con b, c non invertibile

$a \in A$ è primo se $a \mid bc \Rightarrow a \mid b \quad a \mid c$.

$\Rightarrow$ irriducibile $\neq$ primo. (in generale)

in $\mathbb{Z}$ irriducibile = primo.

Un caso in cui irriducibile $\neq$ primo

$$A = \mathbb{Z}/(30)[x]$$

↑ ma è un campo.

$$p(x) = x^2 1 = (x-1)(x-29) \mod(30).$$

$$= (x-19)(x-11)$$

$(x-1)$ è irriducibile

$(x-1) \mid (x-19)(x-11)$ ma non divide nessuno dei due fattori

$\Rightarrow$ $(x-1)$ non è primo.

in un campo tutto sarebbe andato bene.

irriducibile $\Rightarrow$ primo in un campo

$a \mid bc \quad (a,b) = 1 \Rightarrow a \mid c$

(in $\mathbb{Z}$ ma funziona anche in $\mathbb{R}[x]$)

lo dimostriamo con Bezout

$1 = \alpha a + \beta b$ (con che vale anche con i polinomi $\alpha, \beta \in \mathbb{R}[x]$)

$\cdot c$ ⇓

$c = \underbrace{\alpha ac}_{\text{multiplo di } a} + \underbrace{\beta bc}_{\text{multiplo di } a}$

⇓

$a \mid c.$

a irriducibile $a \mid bc$. (irr $\Rightarrow$ primo) dim

calcolo $\mathrm{mcd}(a,b) = 1 \Rightarrow a \mid c$

$\mathrm{mcd}(a,b) \neq 1 \Rightarrow$ l'unico divisore comune deve essere a visto che è irriducibile

⇓

$a \mid b$

(Finito il programma di matematica discreta)

es: $x^2 + 5x + 3 \equiv 0 \ (31)$ → o in un campo

posso usare la formula $x = \frac{-5 \pm \sqrt{5^2 - 4ac}}{2a}$

e funziona in un campo

$x = \frac{-5 \pm \sqrt{13}}{2}$

$\sqrt{13} \bmod (31)$? → se ∃ lo calcolo → se ∄ lo calcolo

$\frac{1}{2} \bmod (31) \Rightarrow 16$

$n^2 \equiv 13 \ (31)$

: si prova con i numeri.