1 proprietà

commutativa (c) $\implies f(a,b) = f(b,a)$
associativa (a) $\implies f(f(a,b),c) = f(a,f(b,c)) = f(a,b,c)$

2 insiemi

$s \in S$ appartenenza
$s \notin S$ non appartenenza
$\emptyset$ insieme vuoto
$B \subseteq A$ sottoinsieme
$\forall A \quad \emptyset \subseteq A$
$A = B \implies A \subseteq B \wedge B \subseteq A$
$B \subsetneq A \implies B \subseteq A \wedge B \neq A$
$A \cap B = \{x | x \in A \wedge x \in B\}$
$\cap = c, a$
$\forall A \quad A \cap \emptyset = \emptyset$
$A_1 \cap A_2 ... \cap A_{100} = \bigcap_{i=1}^{100} A_i$
$A \cup B = \{x | x \in A \vee x \in B\}$
$\cup = c, a$
$A \cup A = A$
$A \cup \emptyset = A$
$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$U = universo$
complemento di A $A^c = \{x \in U | x \notin A\}$
$(A \cap B)^C = A^C \cup B^C$
$(A \cup B)^C = A^C \cap B^C$
$B \backslash A = \{x \in B | x \notin A\}$
$P(A) = \{B | B \subseteq A\}$
$A \mathrm{x} B = \{(a,b) | a \in A, b \in B\}$
$A_1 \mathrm{x} A_2 \mathrm{x} ... \mathrm{x} A_n = \{(a_1, a_2, ..., a_n) | a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n\}$
$\mathbb{N}\mathrm{x}\mathbb{N}\mathrm{x}\mathbb{N} = \mathbb{N}^3$
$\mathrm{x} = a$

$\emptyset \mathrm{x} A = \emptyset$
$(A_1 \cap A_2) \mathrm{x} B = (A_1 \mathrm{x} B) \cap (A_2 \mathrm{x} B)$
$(A_1 \cup A_2) \mathrm{x} B = (A_1 \mathrm{x} B) \cup (A_2 \mathrm{x} B)$

3 relazioni

$A\mathrm{p}B \subseteq A\mathrm{x}B$
$a\mathrm{p}b = (a,b) \subseteq \mathrm{p}$
$B = A \implies$ relazione definita su A
p è una relazione di equivalenza se definita su A e
1)$\forall a \in A \quad a\mathrm{p}a$
2)$a\mathrm{p}b \implies b\mathrm{p}a$
3)$a\mathrm{p}b \wedge b\mathrm{p}c \implies a\mathrm{p}c$
se p è una relazione di equivalenza $a\mathrm{p}b$ si dice a è equivalente a b
sia p una relazione di equivalenza su A,
la classe di equivalenza modulo p di un $a \in A$ è l'insieme $[a] = \{b \in A | b\mathrm{p}a\}$
$[a] = [b] \iff a\mathrm{p}b$
$[a] \neq [b] \implies [a] \cap [b] = \emptyset$
p è una relazione di ordine(parziale) su A se
1)$\forall a \in A \quad a\mathrm{p}a$
2)$a\mathrm{p}b \wedge b\mathrm{p}a \implies a = b$
3)$a\mathrm{p}b \wedge b\mathrm{p}c \implies a\mathrm{p}c$
parziale significa che non tutti gli elementi sono confrontabili,
se ogni 2 elementi sono confrontabili allora è di ordine totale

4 massimo,minimo,massimale,minimale

in generale una relazione di ordine si indica con $\leq$
sia $\leq$ una relazione di ordine su un insieme A. un elemento $a \in A$ è detto

1. massimo: se è confrontabile con ogni elemento di A e risulta che $y \leq a \quad \forall y \in A$
2. massimo: se è confrontabile con ogni elemento di A e risulta che $a \leq y \quad \forall y \in A$
3. massimale: $\forall y \in A \wedge y \neq a \nexists a \leq y$
4. minimale: $\forall y \in A \wedge y \neq a \nexists y \leq a$

5 funzioni

la relazione p è detta funzione e si indica di solito con f se $\forall x \in A, \exists! y \in B, (x,y) \in f$
$f(x) = y, x \in A, y \in B, f : A \to B$ A è dominio B è codominio
immagine di f: $Im(f) = \{y \in B | \exists x \in A, f(x) = y\}$
controimmagine di f: $f^{-1}(y) = \{x \in A | f(x) = y\}$
una funzione $f : A \to B$ è detta iniettiva se $\forall x_1, x_2 \in A, x_1 \neq x_2, f(x_1) \neq f(x_2)$
una funzione $f : A \to B$ è detta suriettiva se $\forall y \in B, \exists x \in A, f(x) = y$
biettiva = iniettiva $\wedge$ suriettiva
quando $f : A \to B$ è biettiva si può costruire la funzione inversa $g : B \to A$

$$(g \circ f)(x) = x \quad \forall x \in A$$
$$(f \circ g)(y) = y \quad \forall y \in B$$

siano $f : A \to B$ e $g : B \to C$ definiamo la funzione composizione $(g \circ f) : A \to C$
come $(g \circ f)(x) = g(f(x))$
composizione = not c, a
insieme ordinato = esiste una relazione di ordine totale
campo = ha due operazioni dove ogno elemento ha un opposto e ogni elemento non nullo è invertibile rispetto alla moltiplicazione

6 equazioni

di primo grado = lineare

fratte = la x è in qualche frazione, si risolvono con mcm

disequazioni = soluzioni poi parabola

disequazioni fratte = il prodotto/quoziente è positivo se e solo se entrambi sono positivi o negativi (risolvi N e D e poi tabella li strana)

7 sistemi

$$\begin{cases} equazione_1 \\ equazione_2 \\ \vdots \\ \vdots \end{cases} \tag{1}$$

verificato quando tutte vere, roba con rigette

8 radice quadrata

$\forall x \in \mathbb{R}, x \geq 0 . y \geq 0, \exists! y, y^2 = x$

$$\begin{aligned} &\sqrt{f(x)} = g(x) \\ &\updownarrow \\ &\begin{cases} f(x) \geq 0 \\ g(x) \geq 0 \\ f(x) = g^2(x) \end{cases} \end{aligned}$$

(campo di esistenza)

$$\begin{aligned} &\sqrt[3]{f(x)} = g(x) \\ &\updownarrow \\ &f(x) = g^3(x) \end{aligned}$$

$$\begin{aligned} &\sqrt{f(x)} \geq g(x) \\ &\updownarrow \\ &\begin{cases} f(x) \geq 0 \\ g(x) \geq 0 \\ f(x) \geq g^2(x) \end{cases} \bigcup \begin{cases} f(x) \geq 0 \\ g(x) < 0 \end{cases} \end{aligned}$$

(campo di esistenza)

$$\begin{aligned} &\sqrt{f(x)} > g(x) \\ &\updownarrow \\ &\begin{cases} f(x) \geq 0 \\ g(x) \geq 0 \\ f(x) > g^2(x) \end{cases} \bigcup \begin{cases} f(x) \geq 0 \\ g(x) < 0 \end{cases} \end{aligned}$$

(campo di esistenza)

$$\sqrt{f(x)} \leq g(x)$$
$$\updownarrow$$
$$\begin{cases} f(x) \geq 0 \\ g(x) \geq 0 \\ f(x) \leq g^2(x) \end{cases}$$
(campo di esistenza)

$$\sqrt{f(x)} < g(x)$$
$$\updownarrow$$
$$\begin{cases} f(x) \geq 0 \\ g(x) \geq 0 \\ f(x) < g^2(x) \end{cases}$$
(campo di esistenza)

$$\sqrt[3]{f(x)} \geq g(x)$$
$$\updownarrow$$
$$f(x) \geq g^3(x)$$

$$\sqrt[3]{f(x)} \leq g(x)$$
$$\updownarrow$$
$$f(x) \leq g^3(x)$$

$$\sqrt[3]{f(x)} > g(x)$$
$$\updownarrow$$
$$f(x) > g^3(x)$$

$$\sqrt[3]{f(x)} < g(x)$$
$$\updownarrow$$
$$f(x) < g^3(x)$$

9 logaritmo

$\forall a, a > 0, a \neq 1, y > 0, \exists! x, a^x = y \quad x = \log_a y$

e = numero di nepero, reale ma non razionale, $\log_e = \ln$

$a^{\log_a x} = x, x > 0$
$log_a a^x = x, \forall x \in \mathbb{R}$

1. $\log_a(xy) = \log_a(x) + \log_a(y)$
2. $\log_a(\frac{x}{y}) = \log_a(x) - \log_a(y)$
3. $\log_a(x^b) = b \log_a(x), b \in \mathbb{R}$
4. $\log_b(x) = \frac{\log_a(x)}{\log_a(b)}$

$|f(x)| = |g(x)| \leftrightarrow f(x) = g(x) \vee f(x) = -g(x)$

$$|f(x)| = g(x)$$
$$\updownarrow$$
$$\begin{cases} f(x) \geq 0 \\ f(x) = g(x) \end{cases} \bigcup \begin{cases} f(x) \geq 0 \\ -f(x) = g(x) \end{cases}$$
(campo di esistenza)

notazione: $a|b \Leftrightarrow \exists c, b = c \cdot a$
$a, b \in \mathbb{Z}, a, b \neq 0, \exists MCD(a,b) = d, d = ax + by \leftarrow$ identità di bezout
teorema fondamentale dell'aritmetica:

$$\begin{cases} \forall n \in \mathbb{N}, n \neq 0,1 \exists P = \{(p_0, m_0), (p_1, m_1) ... (p_n, m_n)\}, \prod_{(p,m) \in P} p^m = n \\ \forall z \in \mathbb{Z}, z \neq -1, 0, 1 \exists P = \{(p_0, m_0), (p_1, m_1) ... (p_n, m_n)\}, \prod_{(p,m) \in P} p^m = z \end{cases} \implies$$
$$\implies D = \{x^n | \}$$

(usando la definizione delle coppie di Kuratowski)

$$p = (x,y) = \{\{x\}, \{x,y\}\} \implies \begin{cases} \bigcap p = \bigcap \{\{x\}, \{x,y\}\} = \{x\} \cap \{x,y\} = \{x\} \\ \bigcup p = \bigcup \{\{x\}, \{x,y\}\} = \{x\} \cup \{x,y\} = \{x,y\} \end{cases} \implies$$
$$\implies \begin{cases} \pi_1(p) = \bigcup \bigcap p = \bigcup \{x\} = x \\ \pi_2(p) = \bigcup \{a \in \bigcup p \mid \bigcup p \neq \bigcap p \rightarrow a \notin \bigcap p\} = \\ \qquad = \bigcup \{a \in \{x,y\} \mid \{x,y\} \neq \{x\} \rightarrow a \notin \{x\}\} = \bigcup \{y\} = y \end{cases}$$

$$\begin{cases} MCD(a,b) = \prod \{x^n | x = \pi_1(P_1) \wedge x = \pi_1(P_2), n = \min\{\pi_2(P_1), \pi_2(P_2)\}, P_1 \subseteq P_a, P_2 \subseteq P_b\} \\ MCM(a,b) = \prod \{x^n | x = \pi_1(P_1) \vee x = \pi_1(P_2), \\ \qquad n = \max\{\pi_2(m) | m \subseteq \{P | P = P_1, x = \pi_1(P_1)\} \cup \\ \qquad\qquad \{P | P = P_2, x = \pi_1(P_1)\}\}, P_1 \subseteq P_a, P_2 \subseteq P_b\} \end{cases}$$
$$MCD(a,b) \cdot MCM(a,b) = a \cdot b$$

```
mcd :: Int -> Int -> Int
mcd a b
  | r1 == 0 = b
  | otherwise = mcd b r1
    where r1 = a `mod` b
```

se MCD(a,b) = 1 si dice che a, b sono coprimi tra loro

equazione diofantee $5x + 3y = 16$, determinare tutte le soluzioni (x, y) intere dell'equazione

basta risolvere $5u+3v = 1$, infatti dopo multiplico per 16, 5(16u) + 3(16v) = 16 $\left(\begin{cases} x = 16U \\ y = 16V \end{cases} \right)$

5u+3v è un'identità di bezout, si può realizzare? si, perché (5, 3) = 1

$$5 = 3 \cdot 1 + 2, r_1 = 2$$
$$3 = 2 \cdot 1 + 1, r_2 = 1$$
$$2 = 1 \cdot 2 + 0, \text{stop}$$

$MCD(5,3) = r_2 = 1$

bezout:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (5 - 3 \cdot 1) \cdot 1 \\ &= 3 - 5 \cdot 1 + 3 \cdot 1 \\ &= 3 \cdot 2 - 5 \cdot 1 \end{aligned}$$

$u = -1$
$v = 2$

una soluzione di 5x+3y=16 è $\begin{cases} x = 16u = -16 \\ y = 16v = 32 \end{cases}$

tutte le soluzioni sono $(x - 3h, y + 5h)$, in quanto $5(x-3h) + 3(y+5h) = 5x - 15 + 3y + 15 = 5x + 3y = 16$
quindi le soluzioni sono $(x,y) = (-16 - 3h, 32 + 5h) \forall h \in \mathbb{Z}$

ax+by=c ha solozioni intere $\iff (a,b)|c$

su $\mathbb{Z}$ definiamo una relazione $a \mathrm{p}_n b \iff a \cong b \mod n$
le classi di equivalenza sono $[a]_n = \{b \in \mathbb{Z} | a \mathrm{p}_n n\}$ l'insieme quoziente è l'insieme delle classi di equivalenza, lo si indica con $\mathbb{Z}_n = \{[m]_n | \forall m \in \mathbb{N}, \mathtt{0} \leq m < n\}$

congruente in $\mathbb{Z}$ a è congruente a b modulo n se $n \in \mathbb{N}, n \geq \mathtt{1}, a, b \in \mathbb{Z}, a \mod n = b \mod n \implies b - a = kn, n|(a-b)$
la relazione di congruenza mod n è una relazione di equivalenza qualsiasi sia $n \in \mathbb{N}_{\mathtt{0}}$

riflessiva : $\forall a \in \mathbb{Z}, a \cong a \mod n (n|(a-a) = n|\mathtt{0})$
simmetrica : $\forall a, b \in \mathbb{Z}, a \cong b \mod n \implies b \cong a \mod n (n|(b-a) = n|-(a-b))$
transitiva : $\begin{array}{l} \forall a, b, c \in \mathbb{Z}, a \cong b \mod n \wedge b \cong c \mod n \implies a \cong c \mod n \\ (n|(b-a) \wedge n(c-b) \implies n|(b-a+c-b) = n|(c-a) \end{array}$

classi di equivalenza quante sono? quante n
$[\mathtt{0}]_n, [\mathtt{1}]_n, [\mathtt{2}]_n, ..., [n-\mathtt{1}]_n$
$[\mathtt{0}]_n = \{a \in \mathbb{Z} | a \cong \mathtt{0} \mod n\}$
$\forall a, b \in \mathbb{Z}, [a]_n + [b]_n = [a+b]_n$
$\forall a, b \in \mathbb{Z}, [a]_n \cdot [b]_n = [a \cdot b]_n$
$[a]$ invertibile in $\mathbb{Z}_n \iff \exists [x], [a] \cdot [x] = [\mathtt{1}] \iff [a \cdot x] = [\mathtt{1}] \iff ax \cong \mathtt{1} \mod n \iff n|(ax - \mathtt{1}) \iff ax - \mathtt{1} = kn, k \in \mathbb{Z} \iff ax - kn = \mathtt{1}, k \in \mathbb{Z} \iff MCD(a,n) = \mathtt{1}$
$\mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}} = \{[m]_n | m \in \mathbb{N}, \mathtt{0} \leq m < n\}$
$ax \cong b \mod n, d = (a.n)$ ammette una soluzione $\iff d|b$, in caso $x_{\mathtt{0}}$ è una soluzione, tutte le altre sono $x = x_{\mathtt{0}} + \frac{n}{d}k, k \in \mathbb{Z}$
siano $n_{\mathtt{1}}, ..., n_r \in \mathbb{N} > \mathtt{0}$
siano $b_{\mathtt{1}}, ..., b_r \in \mathbb{Z}$
allora

1. il sistema $\begin{cases} x \cong b_{\mathtt{1}} \mod n_{\mathtt{1}} \\ \vdots \\ x \cong b_r \mod n_r \end{cases}$
2. tutte le soluzioni sono della forma $c + kn_{\mathtt{1}} \cdot n_{\mathtt{2}} \cdot ... \cdot n_r$, cioè la soluzione $[c]_{n_{\mathtt{1}} \cdot ... \cdot n_r}$

algoritmo: risolvo indipendetemente le congruenze, per i=1,...,r

1. $N_i y_i = \mathtt{1} \mod n_i, N_i = \prod_{j=\mathtt{1}, j \neq i}^{r} n_j$
   esempio:
   $\begin{cases} x \cong \mathtt{3} \mathrm{mod} \mathtt{8}, b_{\mathtt{1}} = \mathtt{3}, n_{\mathtt{1}} = \mathtt{8}, N_{\mathtt{1}} y_{\mathtt{1}} = \mathtt{1} \mathrm{mod} n_{\mathtt{1}} \Rightarrow \mathtt{5} \cdot \mathtt{21} y_{\mathtt{1}} \cong \mathtt{1} \mathrm{mod} \mathtt{8} \Rightarrow y_{\mathtt{1}} \cong \mathrm{tot}_{\mathtt{1}} \mathrm{mod} \mathtt{8} \\ x \cong -\mathtt{1} \mathrm{mod} \mathtt{5}, b_{\mathtt{2}} = -\mathtt{1}, n_{\mathtt{2}} = \mathtt{5}, N_{\mathtt{2}} y_{\mathtt{2}} = \mathtt{1} \mathrm{mod} n_{\mathtt{2}} \Rightarrow \mathtt{8} \cdot \mathtt{21} y_{\mathtt{2}} \cong \mathtt{1} \mathrm{mod} \mathtt{5} \Rightarrow y_{\mathtt{2}} \cong \mathrm{tot}_{\mathtt{2}} \mathrm{mod} \mathtt{5} \\ x \cong \mathtt{27} \mathrm{mod} \mathtt{21}, b_{\mathtt{3}} = \mathtt{27}, n_{\mathtt{3}} = \mathtt{21}, N_{\mathtt{3}} y_{\mathtt{3}} = \mathtt{1} \mathrm{mod} n_{\mathtt{3}} \Rightarrow \mathtt{8} \cdot \mathtt{5} y_{\mathtt{3}} \cong \mathtt{1} \mathrm{mod} \mathtt{21} \Rightarrow y_{\mathtt{3}} \cong \mathrm{tot}_{\mathtt{3}} \mathrm{mod} \mathtt{21} \end{cases}$
2. pongo $c = \sum_{i=\mathtt{1}}^{r} b_i y_i N_i$

teorema cinese del resto generalizzato il sistema $\begin{cases} x = b_{\mathtt{1}} \mod n_{\mathtt{1}} \\ \vdots \\ x = b_r \mod n_r \end{cases}$ ha soluzione $\iff$ $\forall i, j \leq r, MCD(n_{\mathtt{1}}, n_j) | (b_{\mathtt{1}} - b_j)$, una soluzione c e le altre nella forma $c + kMCM(n_{\mathtt{1}}, ..., n_r)$

funzione di eulero se A è un insieme finito, il simbolo $\#A$ indica il numeri di elementi di A
$\forall n \in \mathbb{N}, n \geq \mathtt{1}, \phi(n) = \#\{a \in \mathbb{Z} | \mathtt{0} < a < n, (a,n) = \mathtt{1}\} = \#\{\text{classi invertibili di } \mathbb{Z}_n\}$
$\forall n \in \mathbb{N}, n \geq \mathtt{1}, n \text{ primo}, (a,n) = \mathtt{1} \implies a^{\phi(n)} \cong \mathtt{1} \mod n$

```
eulero:: Int -> Int
eulero n
  | isPrimo n = n-1
  | isPrimo (h `sqrt` p) = (p `pow` h) - (p `pow` (h-1))
  | otherwise = map eulero $ toFattoriPrimi n
  where h >= 1
```

piccolo teorema di fermat
$a \in \mathbb{Z}, p > 0, p$ primo $\implies a^p \cong a \mod p$
$(a,p) = 1 \implies a^{p-1} \cong 1 \mod p$

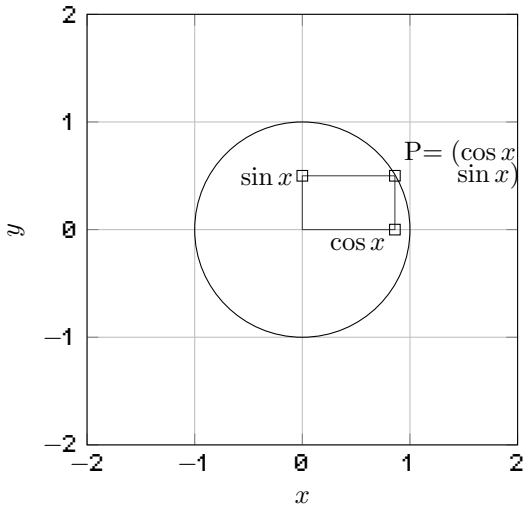
10 basi

$\forall n \geq 2, \forall a \in \mathbb{N}, a \geq 0, \exists! A_n = \{B \in \mathbb{R}^2 | \#B < \infty, \prod_{r=\pi_1(p), n=\pi_2(p), p \subseteq B} rn^h = a\}$

```
basechange :: Int -> Int -> [Int]
basechange a n = _basechange a n n
_basechange :: Int -> Int -> Int -> [Int]
_basechange a n e
  | e == 0 = [a `mod` n]
  | otherwise = a `mod` n : _basechange (a `div` n) n (e - 1)
```

11 trigonometria

circonferenza raggio 1



$\cos^2 x + \sin^2 x = 1$ periodiche in periodo 2π

$$\sin(x + 2\pi) = \sin x$$
$$\cos(x + 2\pi) = \cos x$$

$\sin -x = -\sin x$
$\cos -x = \cos x$

$$\sin(\pi - x) = \sin x$$
$$\cos(\pi - x) = -\cos x$$
$$\sin(\pi + x) = -\sin x$$
$$\cos(\pi + x) = -\cos x$$
$$\sin(2x) = 2\sin x \cos x$$
$$\cos(2x) = \cos^2 x - \sin^2 x$$
$$\sin\left(\frac{x}{2}\right) = \pm\sqrt{\frac{1 - \cos x}{2}}$$
$$\cos\left(\frac{x}{2}\right) = \pm\sqrt{\frac{1 + \cos x}{2}}$$

$\tan x = \frac{\sin x}{\cos x}$
$\tan \frac{\pi}{4} = 1, \tan \frac{\pi}{6} = \frac{\sqrt{3}}{3}, \tan \frac{\pi}{3} = \sqrt{3}$
periodica di periodo π

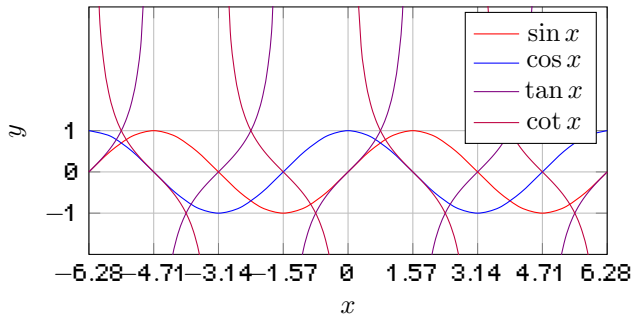
$$\tan(x + \pi) = \tan x$$

$\cot = \text{cotan} = \frac{\cos x}{\sin x}$
$180^\circ = \pi$

$$\sin 0 = 0, \cos 0 = 1, \tan 0 = 0$$
$$\sin \frac{\pi}{2} = 1, \cos \frac{\pi}{2} = 0, \tan \frac{\pi}{2} = \emptyset$$
$$\sin \pi = 0, \cos \pi = -1, \tan \pi = 0$$
$$\sin \frac{3\pi}{2} = -1, \cos \frac{3\pi}{2} = 0, \tan \frac{3\pi}{2} = \emptyset$$

$$\cos(x+y) = \cos x \cos y - \sin x \sin y$$
$$\cos(x-y) = \cos x \cos y + \sin x \sin y$$
$$\sin(x+y) = \sin x \cos y + \cos x \sin y$$
$$\sin(x-y) = \sin x \cos y - \cos x \sin y$$

funzioni trigonometriche

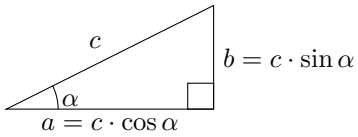


DISEQUAZIONI:

$$\cos x > \frac{\sqrt{2}}{2}$$
$$2k\pi - \frac{\pi}{4} < x < \frac{\pi}{4} + 2k\pi$$

12 triangoli rettangoli

triangolo retangolo



13 immaginari

Re(x) = parte reale Im(y) = parte immaginaria

se $z = x + iy$ il coniugato è $\overline{z} = x - iy$

due complessi sono uguali se hanno stesso modulo e stesso argomento a meno di multipli di 2π

$$\begin{cases} x_1 = x_2 \\ y_1 = y_2 + 2k\pi \end{cases}$$

operazioni sui complessi:

somma $(x+iy) + (x'+iy') = x + x' + i(y+y')$

prodotto $(x+iy) \cdot (x'+iy') = xx' + ixy' + iyx' + i^2yy' = xx' - yy' + i(xy' + yx')$

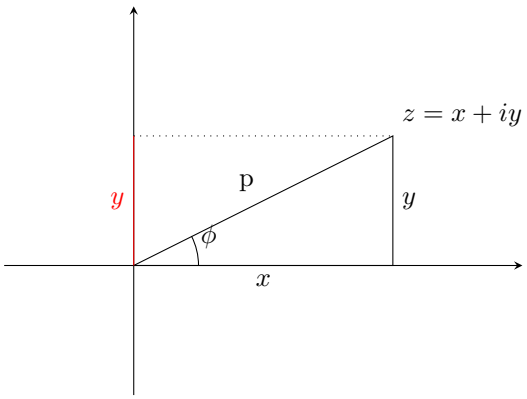
modulo di $z = x + iy$ è $|z| = \sqrt{x^2 + y^2}$

$|z|^2 = z\overline{z}$

$$\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$$
$$\overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2$$
$$\overline{\left(\frac{1}{z}\right)} = \frac{1}{\overline{z}}$$
$$\overline{\overline{z}} = z$$

$$|z| \geq 0$$
$$z = 0 \iff |z| = 0$$
$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|$$
$$|z| = |\overline{z}|$$
$$|z_1 + z_2| \leq |z_1| + |z_2|$$

forma trigonometrica



p $= |z|$
ϕ = angolo formato dal segmento e asse x
$\begin{cases} \cos\phi = \frac{x}{\mathrm{p}} \\ \sin\phi = \frac{y}{\mathrm{p}} \end{cases}$
$z = x + iy = \mathrm{p}\cos\phi + i(\mathrm{p}\sin\phi) = \mathrm{p}(\cos\phi + i\sin\phi)$
p = modulo di z
ϕ = argomento di z
altra formula per ϕ

$$\phi = \begin{cases} \arctan\frac{y}{x} & \text{se } x > 0 \text{ e } y \text{ qualsiasi} \\ \arctan\frac{y}{x} + \pi & \text{se } x < 0 \text{ e } y \geq 0 \\ \arctan\frac{y}{x} + \pi & \text{se } x < 0 \text{ e } y < 0 \\ \frac{\pi}{2} & \text{se } x = 0 \text{ e } y > 0 \\ -\frac{\pi}{2} & \text{se } x = 0 \text{ e } y < 0 \end{cases} \quad , \phi \in (-\pi, \pi]$$

DE MOIVRE

$$z_1 = \mathrm{p}_1(\cos\phi_1 + i\sin\phi_1)$$
$$z_2 = \mathrm{p}_2(\cos\phi_2 + i\sin\phi_2)$$
$$z_1 \cdot z_2 = \mathrm{p}_1\mathrm{p}_2(\cos\phi_1 i\sin\phi_1)(\cos\phi_2 i\sin\phi_2) =$$
$$= \mathrm{p}_1\mathrm{p}_2(\cos\phi_1\cos\phi_2 + i\cos\phi_1\sin\phi_2 + i\sin\phi_1\cos\phi_2 + i^2\sin\phi_1\sin\phi_2)$$
$$= \mathrm{p}_1\mathrm{p}_2(\cos\phi_1\cos\phi_2 - \sin\phi_1\sin\phi_2 + i(\cos\phi_1\sin\phi_2 + \sin\phi_1\cos\phi_2))$$
$$= \mathrm{p}_1\mathrm{p}_2(\cos(\phi_1 + \phi_2) + i\sin(\phi_1 + \phi_2))$$

generalizzando

$$z_1 \cdot z_2 \cdot \ldots \cdot z_n = \mathrm{p}_1\mathrm{p}_2..\mathrm{p}_n(\cos(\phi_1 + \phi_2 + \ldots + \phi_n) + i\sin(\phi_1 + \phi_2 + \ldots + \phi_n))$$
$$z^n = \mathrm{p}^n(\cos(n\cdot\phi) + i\sin(n\cdot\phi))$$

DE MOIVRE per i quozienti

$$z_1 = \mathrm{p}_1(\cos\phi_1 + i\sin\phi_1)$$
$$z_2 = \mathrm{p}_2(\cos\phi_2 + i\sin\phi_2)$$
$$\frac{z_1}{z_2} = \frac{\mathrm{p}_1}{\mathrm{p}_2}(\cos(\phi_1 - \phi_2) + i\sin(\phi_1 - \phi_2))$$

radici n-esime
$\sqrt[n]{w} = z, z^n = w$
sia $w = r(\cos\phi + i\sin\phi) \neq 0$
w ammette esattamente n radici n-esime

queste sono

$$k = \{x | x \geq 0 \wedge x < n/x \in \mathbb{N}\}$$
$$z_k = r^{\frac{1}{n}}(\cos\phi_k + i\sin\phi_k)$$
$$\phi_k = \frac{\phi + 2k\pi}{n}$$

$\mathbb{C}$ è algebricamente chiuso, ogni equazione polinomiale in $\mathbb{C}$: $a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0 = 0$ $a_0, a_1, ..., a_n \in \mathbb{C}$
ha esattamente n radici (=soluzioni) contate con molteplicità
$\mathbb{R}$ non è algebricamente chuso, infatti $x^2 + 1 = 0$ non ha soluzioni in $\mathbb{R}$
MOLTIPLICAZIONE PER i
$z = \mathrm{p}(\cos\phi + i\sin\phi)$
vogliamo capire modulo e argomento di iz
$|iz| = |i| \cdot |z| = 1 \cdot \mathrm{p} = \mathrm{p}$
argomenti di iz

$$\begin{aligned} iz &= \mathrm{p}i(\cos\phi + i\sin\phi) = \\ &= \mathrm{p}(i\cos\phi + i^2\sin\phi) = \\ &= \mathrm{p}(-\sin\phi + i\cos\phi) = \\ &= \mathrm{p}\left(\cos\left(\phi + \frac{\pi}{2}\right) + i\sin\left(\phi + \frac{\pi}{2}\right)\right) \end{aligned}$$

$$\begin{aligned} (\text{dato che } \cos\left(\phi\frac{\pi}{2}\right) &= -\sin\phi \\ \sin\left(\phi\frac{\pi}{2}\right) &= \cos\phi) \end{aligned}$$

l'argomento di iz è $\phi + \frac{\pi}{2}$

14 relazione di equivalenza

relazioni binarie

$$x = \{a, b, c, d\}$$
$$x = \mathbb{N}$$
$$x = \mathbb{C}$$
$$R \in x^2 = \{(x, y) | x, y \in X\}$$
$$R = \{(a, a)\} | \{(b, c), (a, c)\}...$$

relazione di eguaglianza

1.riflessive $\quad \forall x \in X, (x, x) \in R | R(x, x) | xRx$
2.simmetriche $\quad \forall x, y \in X, (x, y) \in R \implies (y, x) \in R$
3.transitiva $\quad \forall x, y, z \in X, (x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R$

principio di induzione (I^a forma) $n_0 \in \mathbb{N}, P(n_0) \implies \forall n \geq n_0, n \in \mathbb{N}, P(n+1)$
principio di induzione (II^a forma) $n_0, n, k \in \mathbb{N}, P(n_0) \wedge \forall k, n > k > n_0 \implies P(n+1) \implies \forall n \geq n_0, P(n)$

15 gruppi

un gruppo $(G, *)$ è un insieme G dotato di una operazione binaria

$$\begin{aligned} * : & G\mathrm{x}G \to G \\ & (a, b) \to a * b \end{aligned}$$

che verifica le seguenti proprietà

(*a*) * è associativa $\forall a, b, c \in G, (a * b) * c = a * (b * c)$

(*b*) $\exists e \in G$ detto elemento neutro rispetto all'operazione *: $\forall a \in G, e * a = a = a * e = a$

(*c*) $\forall a \in G, \exists a^{-1} \in G$ detto elemento inverso tale che $a * a^{-1} = e = a^{-1} * a$

se inoltre vale che $\forall a, b \in G, a * b = b * a$, si diche che (G,*) è un gruppo abeliano
$\exists! e \in (G, *), \forall a \in G, a * e = a = e * a$
$\exists! a^{-1} \in (G, *), \forall a \in G, a * a^{-1} = e = a^{-1} * a$
$\forall a, b \in (G, *), (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
$\forall a \in G, \left(a^{-1}\right)^{-1} = a$

$$\forall g \in (G, *), \forall i \in \mathbb{Z}$$
$$g^i = \begin{cases} g * g * g * ... * g & i > 0 \\ e & i = 0 \\ g^{-1} * g^{-1} * ... * g^{-1} & i < 0 \end{cases}$$

l'ordine r di $g \in G$ è il più piccolo intero positivo r tale che $g^r = e$. È indicato con $o(g)$. Se $\nexists r$ si dice che g ha ordine infinito
un gruppo è detto finito di ordine R se G ha un numero finito di elementi uguale a R
si indica con $|G|$ il numero di elementi di G (che è anche il suo ordine se è finito)

Lagrange $\forall g \in G, |G| < \infty \implies o(g) || G|$
un gruppo G è detto ciclico se $\exists g \in G, \forall a \in G, \exists i \in \mathbb{Z}, a^i = g, g^0 = e \implies G =< g >$

1. $|G| = 1 \implies G = \{e\}$
2. $|G| = 2, G = \{a, a^2 = e\} =< a >$, è un gruppo ciclico

*	e	a
e	e	a
a	a	e

3. $|G| = 3, G = \{g, g^2, g^3 = e\} =< g >$, ciclico

*	e	g	g^2
e	e	g	g^2
g	g	g^2	e
g^2	g^2	e	g

4. $|G| = 4$, due strutture distinte di gruppo:
   (a) il gruppo ciclico: $G = \{g, g^2, g^3, e = g^4\} =< g >$

*	e	g	g^2	g^3
e	e	g	g^2	g^3
g	g	g^2	g^3	e
g^2	g^2	g^3	e	g
g^3	g^3	e	g	g^2

   (b) il gruppo di klein: $G = \{e, a, b, c = a * b = b * a\}$

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	e

5. $|G| = 5, G = \{g, g^2, g^3, g^4, e = g^5\} =< g >$, ciclico
6. $|G| = 6$ molte strutture

se $|G| = p$ primo allora G è ciclico
se $|G| \leq 5$ allora G è abeliano. ci sono gruppi non abeliani a partire da ordine 6
ogni gruppo ciclico è abeliano

gruppi di permutazione /gruppo simmetrico S_n
$\{1, 2, 3, 4, ..., n\} = x \to \{1, 2, 3, 4, ..., n\}$
funzioni bigettive
$S_n = \{$funzioni bigettive da $\{1, ..., n\} \to \{1, ..., n\}\}$
$|S_n| = n!$
operazione: composizione fog
$x \xrightarrow{g} x \xrightarrow{f} x$
$x - g(x) - f(g(x)) := fog(x)$
neutro: $idog(x) = g(x)$
inverso: $fof^{-1} = f^{-1}of = id$ $(f(x) = y, f^{-1}(y) = x)$

Permutazioni "facili": scambi: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$: (1 2): stiamo scambando solo 1 con 2

Cicli: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$: (1 2 3)(4)(5) = (2 3 1)(5)(4) = (4)(5)(3 1 2)

$(a\ b)^2 = (a\ b)\mathrm{o}(a\ b) = id$

$\sigma : (a_1 ... a_n)$

anelli strutture algebriche con 2 operazioni

un anello $(R, +, \cdot)$ è un insieme R dotato di due operazioni binarie:

$$+ : R\mathrm{x}R \to R$$
$$\cdot : R\mathrm{x}R \to R$$

tali che

1. (a) $+$ è associativa: $(a+b)+c = a+(b+c)$
   (b) esiste l'elemento neutro $0 \in R$ rispetto alla $+$: $\forall a \in R, a+0 = a = 0+a$
   (c) $\forall a \in R, \exists -a \in R$ detto elemento opposto tale che: $a+(-a) = 0 = (-a)+a$
   (d) $+$ è commutativa: $\forall a, b \in R, a+b = b+a$
2. $\cdot$ è associativa: $\forall a, b, c \in R, a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. valgono le leggi distributive:

$$a \cdot (b+c) = a \cdot b + a \cdot c$$
$$(a+b) \cdot c = a \cdot c + b \cdot c$$

(R, +) è un gruppo abeliano

se vale che $\cdot$ è commutativo si dice che $(R, +, \cdot)$ è commutativo

se vale che esiste l'elemento neutro $1 \in R$ rispetto al prodotto, si dice che l'anello è unitario

un campo è un anello commutativo unitario in cui ogni elemento diverso da 0 è invertibile

anello dei polinomi a coefficienti in A : $A[x]$

sia $A = (A, +, \cdot)$ un anello

$\{0\} \cup \{\sum_{i=0}^{n} a_i x^i | n \in \mathbb{N}, a_i \in A\}$

grado di un polinomio:

$$\text{grado}(0) = -1$$
$$\text{grado}(\sum_{i=0}^{n} a_1 x^i = \max\{i | a_1 \neq 0\}$$

monomio: $a_i x^i$

operazioni: $+$: è la classica somma termine a termine $\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$

prodotti: stesso discorso $\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i \cdot b_i) x^i$

teorema ruffini: se $P(x) \in A[x]$, A campo, $a \in A, P(a) = 0$ (a è radice di P(x)) $\iff (x-a) | P(x)$

matrice fissiamo A anello, una matrice di tipo (m, n), con $m, n \in \mathbb{N}, m \geq 1 \leq n$ è una tabella M di mxn elementi di A

$$\begin{pmatrix} r_1 \\ r_1 \\ \vdots \\ r_m \end{pmatrix} = (c_1 | ... | c_n) = \begin{pmatrix} a_{11}\ a_{12}\ ...\ a_{1n} \\ \vdots\ \vdots\ a_{i,j} \\ a_{m1}\ a_{m2}\ ...\ a_{mn} \end{pmatrix}, a_{ij}, i = \text{riga}, j = \text{colonna}$$

$M = (a_{i,j})_{i \leq m, j \leq n}$

$a_{i,j}$ sono i coefficienti/entrate di M

(m, n) è la dimensione della matrice, se M è quadrata (cioè $m = n$) si dice anche che è quadrata di dim. n

$M_{mxn}(A) = M_{m,n}(A)$:=l'insieme delle matrici di dimensione (m,n) a coefficienti in A

somma: $m_1 \neq m_2 \vee n_1 \neq n_2$ non si somma

$$m_1 == m_2 \wedge n_1 == n_2, \begin{pmatrix} a_{11}\ ...\ a_{1n} \\ \vdots\ \ddots\ \vdots \\ a_{m1}\ ...\ a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11}\ ...\ b_{1n} \\ \vdots\ \ddots\ \vdots \\ b_{m1}\ ...\ b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11}\ ...\ a_{1n}+b_{1n} \\ \vdots\ \ddots\ \vdots \\ a_{m1}+b_{m1}\ ...\ a_{mn}+b_{mn} \end{pmatrix}$$

1. $A + B = B + A$

2. $A + (B + C) = (A + B) + C$

3. elemento neutro $\mathbb{0} = \begin{pmatrix} \mathbb{0} & \dots & \mathbb{0} \\ \vdots & \ddots & \vdots \\ \mathbb{0} & \dots & \mathbb{0} \end{pmatrix}$

4. opposto di A è $-A = \begin{pmatrix} -a_{11} & \dots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{m1} & \dots & -a_{mn} \end{pmatrix}$

operazione di trasposta: "rifletti" $A = (a_{ij}), A^T = (at_{ji}), a = at$
$\left(A^T\right)^T = A$
l'operazione di transposizione è idempotente
$A \in M_{2x3}(\mathbb{K}), A^T \in M_{3x2}(\mathbb{K})$
$A \in M_{nxm}(\mathbb{K}), A^T \in M_{mxn}(\mathbb{K})$
A è simmetrica se $A^T = A$
prodotto esterno: $\forall k \in \mathbb{K}, \forall A \in M_{nxm}(\mathbb{K}), A = (a_{i,j}), k \cdot A = (ka_{i,j})$
prodotto interno: $v = (a_1 ... a_n), w = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$, il prodotto vettore $v \cdot w = \sum_{i=1}^{n} a_i b_i \in \mathbb{K}$
prodotto tra matrici: $A \in M_{mxn}(\mathbb{K}), A \in M_{nxh}(\mathbb{K}), C \in M_{mxh}, c_{i,j} = \sum_{r=1}^{n} a_{ir} b_{rj}$

1. $(A + B) \cdot C = AC + BC$
   $A \cdot (C + D) = AC + AD$
2. $\forall k \in \mathbb{K} A(kB) = (kA)B = kAB$
3. $(AB)C = A(BC) := ABC$
4. elemento neutro nel caso quadrato: $I_n = \begin{pmatrix} 1 & \mathbb{0} & \dots & \mathbb{0} \\ \mathbb{0} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \mathbb{0} & \dots & \dots & 1 \end{pmatrix}$
5. $(AB)^T = B^T A^T$
6. $(A + B)^T = A^T + B^T$

matrici invertibili $M(\mathbb{R}, n) = \{\text{matrici quadrate } n\text{x}n \text{ a coefficienti in } \mathbb{R}\}$
$(M(\mathbb{R}, n), +, \cdot)$ anello non commutativo, è unitario, esiste l'elemento neutro rispetto al prodotto che è la matrice identità $I = \begin{pmatrix} 1 & & \mathbb{0} \\ & \ddots & \\ \mathbb{0} & & 1 \end{pmatrix} \in M(\mathbb{R}, n), \forall A \in M(\mathbb{R}), A \cdot I = A = I \cdot A$

una matrice quadrata NxN è invertibile se esiste una matrice A^{-1} quadrata NxN tale che $A \cdot A^{-1} = I$ e $A^{-1} \cdot A = I$
non tutte le matrici non nulle sono invertibili
matrici non quadrate non sono invertibili
data A voglio trovare B tale che $A \cdot B = I$.
$B = (b_1 | b_2 | ... | b_n)$

$$A \cdot B = I \iff A \cdot b_1 = \begin{pmatrix} 1 \\ \mathbb{0} \\ \vdots \\ \mathbb{0} \end{pmatrix}, A \cdot b_2 = \begin{pmatrix} \mathbb{0} \\ 1 \\ \vdots \\ \mathbb{0} \end{pmatrix}, ..., A \cdot b_n = \begin{pmatrix} \mathbb{0} \\ \mathbb{0} \\ \vdots \\ 1 \end{pmatrix}$$

$$\iff (A \vdots I) \xrightarrow[\text{gauss-jordan}]{\text{dall'alto e dal basso}} (I \vdots B)$$

con $B = A^{-1}$ matrice inversa
A di tipo NxN invertibile $\iff rk(A) = N$ (ossia è massimale)

1. $(AB)^{-1} = B^{-1} A^{-1}$
2. $(A^{-1})^{-1} = A$
3. $(A^T)^{-1} = (A^{-1})^T$

determinanti $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$

il determinante di A è lo scalare $det(A) = |A| = \sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} i\sigma(i)$

$sgn(x) = \begin{cases} +1 & \text{se } x \text{ è pari} \\ -1 & \text{se } x \text{ è dispari} \end{cases}$

il determinante per 3x3 (regola di sarrus) $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & c \end{pmatrix}, det(A) = aei+dhc+bfg-ceg-hfa-dbi$

1. se B si ottiene da A scambiando due righe o colonne, allora $det(B) = -det(A)$
2. se A ha due righe o colonne uguali, il determinante è zero
3. se A ha una riga o colonna di zeri, il determinante è zero
4. se B si ottiene da A moltiplicando una riga per $k \in \mathbb{R}$ allora $det(B) = k \cdot det(A)$
5. se B si ottiene da A sommano ad una riga di A un multiplo di un'altra riga, allora $det(B) = det(A)$
6. matrice triangolare superiori $(\forall i < n, \forall j > i, a_{ji} = 0)$ $det(A) = a_{11}a_{22}...a_{nn}$

A nxn è invertibile $\iff rk(A) = n \iff det(A) \neq 0$

regola di laplace $A = M(\mathbb{R}, N)$

indichiamo con $A_{i,j}$ la sottomatrice di A ottenuta cancellando la i-esima riga e la j-esima colonna, allora fissato $i \in \{1, ..., N\}$ si ha $det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} det(A_{i,j})$

binet

1. $det(A \cdot B) = det(A) \cdot det(B)$
2. $det(A^k) = [det(A)]^k$
3. $det(A^{-1}) = \frac{1}{det(A)}$

autovettore e autovalore $A \in M(\mathbb{K}, N\text{x}N), v \in \mathbb{K}^N, v \neq 0, \lambda \in \mathbb{K}, A \cdot v = \lambda v \implies \lambda$ è un autovalore di A e v è un autovettore relativo all'autovalore λ

polinomio caratteristico $p_A(t) = det(A - tI) \in \mathbb{K}[t]$

gli zeri di $p_A(t)$ in $\mathbb{K}$ sono gli autovalori di A, e viceversa

la moleplicità algebrica di un autovalore è la molteplicità dello zero come soluzione del polinomio $M_A(\lambda) = \max m(x-a)^m | P(x)$

dato λ un autovalore di A definiamo l'autospazio relativo all'autovalore λ:

$$V_\lambda = \left\{ v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{K}^N | Av = \lambda v \right\} = \left\{ v \in \mathbb{K}^N | Av - \lambda v = 0 \right\} = \left\{ v \in \mathbb{K}^N | (A - \lambda I)v = 0 \right\}$$

la molteplicità geometrica dell'autovalore λ è la dimensione di V_λ. si indica con $M_G(\lambda) = \dim(V_\lambda)$, $\dim(V_\lambda) \geq 1$ $\forall \lambda$ autovalore

$1 \leq m_g(a) \leq m_a(a)$

n = ordine matrice, $\sum_{a \text{ autovalori}} m_a(a) \neq n \implies$ matrice non diagonalizzabile

diagonalizzazione le matrici + semplici sono quelle diagonali $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$

non tutte le matrici sono diagonali, però in realtà la magior parte sono diagonalizzabili, cioè ammettono una forma diagonale

due matrici $A, B \in M(\mathbb{K}, N\text{x}N)$ sono simili se esiste C matrice invertibile tale che $B = C^{-1} \cdot A \cdot C$

una matrice è diagonalizzabile se è simile ad una matrice diagonale

se A è diagonalizzabile la sua forma diagonale è composta dagli autovalori di A e inoltre la matrice diagonalizzante C è composta da una base di autovettori

$M_A(\lambda) = 1 \implies M_A(\lambda) = M_G(\lambda)$

A diagonalizzabile $\iff \forall\lambda$ autovalore, $M_A(\lambda) = M_G(\lambda)$

16 sistemi di equazioni lienari

con grado max 1

equazioni lineare omogenea: $\begin{bmatrix} a_1x_1 + ... + a_nx_n = 0 \\ 3x_1 - x_2 + 5x_3 = 0 \end{bmatrix}$

equazione lineare non omogenea: $\begin{matrix} a_1x_1 + ... + a_nx_n = b_1 \\ 3x_1 - x_2 + 5x_3 = 7 \end{matrix}\Bigg)$

sistema di equazioni lineari
$$\begin{matrix} a_{11}x_1 + ... + a_{1n}x_n = b_1 \\ a_{21}x_1 + ... + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n = b_m \end{matrix}$$

sistema di m equazioni in n incognite, gli $a_{i,j}$ sono coefficienti, $(b_1...b_m)$ vettore dei termini noti. se $b_1 = ... = b_m = 0$ il sistema è omogeneo

una soluzione del sistema è una qualche $(x_1, ..., x_n)$ che risolve tutte le equazioni

cosa centrano le matrici?
$$\begin{matrix} a_{11}x_1 + ... + a_{1n}x_n = b_1 \\ a_{21}x_1 + ... + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n = b_m \end{matrix} \quad , \quad \begin{matrix} (a_{11}, ..., a_{1n}) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \\ (a_{21}, ..., a_{2n}) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \\ \vdots \\ (a_{m1}, ..., a_{mn}) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \end{matrix} ,$$

$$\begin{pmatrix} a_{11}...a_{1n} \\ \vdots \ddots \vdots \\ a_{m1}...a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + ... + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \leftarrow \text{(vettore dei termini noti)}$$

$\uparrow$

vettore indeterminate

$[A|b] \leftarrow$ queste sono quelle da manipolare

processo do gauss-jordan: ridurre il sistema ad un sistema a gradini equivalente
$$\begin{cases} a'_{11}x_1 + a'_{12}x_2 + ... + a'_{1n}x_n = b'_1 \\ a'_{22}x_2 + ... + a'_{2n}x_n = b'_2 \\ \ddots \quad \vdots \\ a'_{mm}x_m + ... + a'_{mn}x_n = b'_m \end{cases}$$

sono sistemi equivalenti, cioè hanno le stesse soluzioni. il sistema a gradini è facile da risolvere, perché si risolve per sostituzione a partire dall'ultima equazione.

si ottengono sistemi equivalenti se opero con le seguenti operazioni, dette elementari:

1. scambiare di posto due equazioni
2. moltiplicare una equazione per uno scalare non nullo
3. sostituire una equazione con la soma di se stessa e un multipo scalare di un'alatra equazione

il rango di una matrica A è il numero di pivot nella sua forma a gradini, si indica con $rg(A)$ oppure con $rk(A)$

un sistema lineare è compatibile $\iff rg(A\vdots b) = rg(A)$, in tal caso, il sistema possiede ∞^{n-r} soluzioni dove n è il numero di incognite, $r = rg(A)$

17 algebra lineare

spazio vettoriale (ancora un'altra struttura algebrica)

uno spazio vettoriale V su un campo $\mathbb{K}$ è un insieme V con due operazioni:

$$+ : V\text{x}V \to V \ (v, w) \to v + w$$
$$\cdot : \mathbb{K}\text{x}V \to V \ (c, v) \to c \cdot V$$

1. (V,+) è un gruppo abeliano, in pratica: esiste un elemento neutro, si indica con 0 e detto vettore nullo e esiste anche elemento inverso di W detto -W: $W + (-W) = \mathbb{0}$
2. $\forall c \in \mathbb{K}, \forall W, U \in V, c(W + U) = cW + cU$
3. $\forall c_1, c_2 \in \mathbb{K}, \forall W \in V, (c_1 + c_2)W = c_1 W + c_2 W$
4. $\forall c_1, c_2 \in \mathbb{K}, \forall W \in V, (c_1 c_2)W = c_1 (c_2 W)$
5. $\forall W \in V, \mathbb{1} \cdot W = W$
6. il vettore nullo 0 è unico
7. $\forall W \in V, \mathbb{0} \cdot W = \mathbb{0}$
8. $\forall k \in \mathbb{K}, k \cdot \mathbb{0} = \mathbb{0}$

un sottoinsieme non vuoto W di uno spazio vettoriale V sul campo $\mathbb{K}$ è detto sottospazio vettoriale di V se:

1. W è chiuso rispetto alla somma: $\forall w_1, w_2 \in W \implies w_1 + w_2 \in W$
2. W è chiuso rispetto alla moltiplicazione per uno scalare: $\forall c \in \mathbb{K}, w \in W \implies c \cdot w \in W$

un vettore $v \in V$ è una combinazione lineare dei vettori $v_1, v_2, ..., v_m \in V$ se $c_1 v_1 + c_2 v_2 + ... + c_m v_m = v$ dove $c_1 ... c_m$ sono scalari

diciamo che i vettori $v_1 ... v_m \in V$ generano V se ogni vettore $v \in V$ è una combinazione lineare di $v_1 ... v_m$, si scrive $V =< v_1 ... v_m >$

dipendenza lineare, $v_1 ... v_m \in V$ sono vettori linearmente dipendenti se esistono scalari $c_1 ... c_m \in \mathbb{R}$ non tutti nulli tali che $c_1 v_1 ... c_m v_m = \mathbb{0}$. altrimenti si dicono linermente indipendenti

un vettore singolo $v \in V$ è linearmente indipendente $\iff v \neq \mathbb{0}$

una base di V è un insieme di vettori $\{v_1 ... v_n\}$ che genera V e sono linearmente indipendenti

equicardinalità delle basi le basi di uno spazio vettoriale hanno lo stesso numero di elementi. questo numero è detto dimensione di V, si indica con $\dim(V)$

se $\dim(V) = N$

1. N vettori che generano V sono anche linearmente indipendenti
2. N vettori lin. indip. di V allora generano V

N vettori $v_1 ... v_n \in R^N$ formano una base $\iff rk(v_1, v_2 ... v_n) = N \iff det(v_1, v_2 ... v_n) \neq \mathbb{0}$

estrazione di una base dati vettori di V che generano esiste un loro sottoinsieme formante una base di V (basta rimuovere i vettori dipendenti)

complemento ad una base dati vettori di V linearmente indipendenti, possiamo aggiungere altri vettori in modo da ottenere una basei di V

sottospazi un sottoinsieme non vuoto W di uno spazio vettorieale V è detto sottospazio se:

1. W è chiuso rispetto alla somma ($\forall w_1, w_2 \in W \implies w_1 + w_2 \in W$)
2. W è chiuso rispetto alla moltiplicazione per uno scalare ($\forall w \in W, \forall c \in \mathbb{R} \implies c \cdot w \in W$)

se $W \subseteq V$ sottospazio, allora $\dim(W) \leq \dim(V)$, inoltre se $\dim(W) = \dim(V)$ allora $W = V$

sottospazi generati da vettori dati $v_1, v_2, ..., v_m \in V$ lo spazio generato da questi vettori è definito come $< v_1, v_2 ... v_m >= \{c_1 v_1 + c_2 v_2 + ... + c_m b_m, c_1 ... c_m$ variano in $\mathbb{R}\}$

$< v_1, v_2, ..., v_m > \subseteq V$ è un sottospazio (la somma di combinazioni lineari è di nuovo una combinazione lineare)

sottospazio somma e intersezione

somma di sottospazio

siano $S \subseteq V$ e $T \subseteq V$ due sottospazi di V. $\dim(S) = M, \dim(T) = N$, definiamo $S + T = \{v+w | v \in S, w \in T\} \subseteq V$ in realtà è un sotospazio. come si trova una base di S+T? si parte da $B_S = \{v_1, ..., v_m\}$ base di S e $B_T = \{w_1, ..., w_n\}$ base di T allora S+T è generato da $v_1, ..., v_m, w_1, ..., w_n$ dai quali estraggo una base.

$\dim(S + T) \leq \dim(S) + \dim(T)$

intersezione

S, T sottospazi di V, $S \cap T = \{v \in V | v \in S, v \in T\} \subseteq V$ è un sottospazio

formula di grassman

$\dim(S) + \dim(T) = \dim(S + T) + \dim(S \cap T) \implies \dim(S) + \dim(T) + \dim(S + T) = \dim(S \cap T)$

$S, T \subseteq V$ sottospazi, se $S + T = V$ e $S \cap T = \{\mathbb{0}\}$ si dice che $V = S \oplus T$ è somma diretta di S e T. ogni $v \in V$ si scrive in modo unico come $v = v_1 + v_2$) con $v_1 \in S$ e $v_2 \in T$

applicazioni lineare /omomorfismi tra spazi vettoriali

siano V, W due spazi vettoriali in $\mathbb{K}$, un'applicazione lineare tra V e W è $f : V \to W, \forall v \in V, \forall k \in \mathbb{K}, f(\sum_{i=1}^{n} k_i v_i) = \sum_{i=1}^{n} k_i f(v_i)$

$\ker(f) = \{v \in V | f(v) = \mathbb{0}\} \subseteq V$

$\ker(f)$ è un sottospazio vettoriale di V

ker = kernel

$Im(f) = \{w \in W | \exists v \in V f(v) = w\} \subseteq W$

$Im(f)$ è un sottospazio vettoriale di W

sia $f : V \to W$ applicazione lineare, sia $\dim(V) = n$ allora $n = \dim(V) = \dim(\ker(f)) + \dim(Im(f))$

un'applicazione lineare si dice

1. iniettiva quando la funzione è iniettiva
2. surgettiva quando la funzione è surgettiva
3. isomorfismo, quando è entrambe

siano V, W spazi vettoriali su $\mathbb{K}$, sia $B = \{v_1, ..., v_n\}$ base di V, siano $w_1, ..., w_n$ vettori qualsiasi di W, allora $\exists! f : V \to W$ applicazione lineare $\begin{cases} f(v_1) = w_1 \\ \vdots \\ f(v_n) = w_n \end{cases}$

coordinate V spazio vettoriale su $\mathbb{R}$ (in generale su un campo qualsiasi $\mathbb{K}$), fissiamo una base $B = \{v_1, ..., v_n\}$ do V quindi $dim(V) = N$

ogni vettore $v \in V$ si può scrivere come combinazione lineare dei vettori della base in modo unico, $v = x_1 v_1 + ... + x_n v_n$ con $x_1, ..., x_n \in \mathbb{R}$ univocamene

il vettore $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ è detto vettore delle coordinate. si indica con $[v]_B$ oppure con $\underline{x}$

applicazione delle coordinate V con vase $B, dim(V) = n$ definiamo l'applicazione delle coordinate (rispetto a B) $\phi_B : \begin{matrix} V \to \mathbb{R}^N \\ v \to [v]_B \end{matrix}$

ϕ_B è lineare ed un isomorfismo, quindi lavorare in V è come lavorare in $\mathbb{R}^N$, che è piú semplice

ogni spazio vettoriale V di dimensione N è isomorfo a $\mathbb{R}^N$ (due spazi vettoriali V e W della stessa dimensione, diciamo N, sono isomorfi, perché entrambi isomorfi a R^N)

matrice del cambiamento di coordinate V fissiamo due basi: B e e, $B = \{v_1, v_2, ..., v_n\}$, $e = \{w_1, ..., w_n\}$

in particolare $dim(V) = n$, ogni vettore $v \in V$ ammette ue vettori di coordinate: $[v]_B$ e $[v]_e$

matrice del cambiamento di coordinate dalla base B alla base e ${}_eM_B = \begin{pmatrix} | & | & | \\ [v_1]_e & [v_2]_e ... & [v_n]_e \\ | & | & | \end{pmatrix}$

$\forall v \in V, [v]_e = {}_eM_B \cdot [v]_B$

matrice rappresentative $f : V \to W$ applicazione lineare, $B = \{v_1, ..., v_n\}$ base di V, $e = \{w_1, ..., w_m\}$ base di W

la matrice di rappresentazione di f rispetto alle basi B e in dominio e e in codominio

$${}_eM_B(f) = \begin{pmatrix} | & | & | \\ [f(v_1)]_e & [f(v_2)]_e & ... [f(v_n)]_e \\ | & | & | \end{pmatrix}$$

${}_eM_B(f)$ = transforma le B-coordinate di v nelle e-coordinate di $f(v)$

$\forall v \in V, [f(v)]_e = {}_eM_B(f) \cdot [v]_B$

endomorfismo se $W = V$, $f : V \to V$ è detto endomorfismo su V

siano B e e due basi di V abbiamo due matrici di rappresentazione di f: ${}_BM_B(f)$ e ${}_eM_e(f)$, ${}_eM_e(f) = {}_eM_B \cdot {}_BM_B(f) \cdot {}_BM_e$

${}_eM_B = {}_BM_e^{-1}$

${}_eM_e(f) = {}_BM_e^{-1} \cdot {}_BM_B(f) \cdot {}_BM_e$ (formula di cambiamento delle matrici rappresentanti degli endomorfismi)

le matrici rappresentanti di un endomorfismo rispetto a basi diverse sono simili

diciamo che un endomorfismo $f : V \to V$ è diagonalizzabile se siste una base B di V tale che la matrice rappresentante ${}_BM_B(f)$ è diagonale

$f : V \to V$ endomorfismo e sia A una matrice rappresentante di $f \implies det(A) \neq 0 \iff f$ suriettivo $\iff f$ iniettivo

rango il rango di una matrice A è anche uguale al massimo ordine di un minore non nullo, un minore di ordine k è il determinante di una sottomatrice formata da k righe e k colonne

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 2 \end{pmatrix}$, $\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \neq 0$, $\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 2 \end{vmatrix} = 0$, max ordine minore non nullo è 2