

(utili x esercizi, non approfondite o dimostrate)


---

---

---

---

---



## GENERALI

### anello

$$a+b = b+a \quad \text{comm. +}$$

$$(a+b)c = a+(b+c) \quad \text{ass. +}$$

$$a+0_A = 0_A+a = a \quad \text{el. neutro +}$$

$$a+(-a) = 0_A \quad \text{opposto}$$

$$a \cdot b = b \cdot a \quad \text{comm.} \quad \text{anello commutativo}$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{ass.}$$

$$a \cdot 1_A = 1_A \cdot a = a \quad \text{el. neutro} \quad \text{anello unitario}$$

$$a(b+c) = a \cdot b + a \cdot c \quad \text{distr.}$$

### N. PRIMO

$$a \in A \setminus A^\times, a \neq 0$$

$$\forall b, c \in A, a|bc \Rightarrow a|b \vee a|c$$

### CAMPO

A anello comm. un.

$$\text{t.c. } \forall a \in A \setminus \{0\}$$

$$a \in A^\times$$

$$\text{Nota: } \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \text{ campo}$$

$$(e, \text{ in } \mathbb{F}_p, ([a] + [b])^p = [a]^p + [b]^p)$$

### Cancellazione in un anello A

$$\text{Se } a \text{ non divisore di } 0_A, ab=ac \Rightarrow b=c$$

$$(\text{in } \mathbb{Z}, \text{ se } a \neq 0)$$

$$\text{INVERTIBILI } ab=ba=1_A$$

$$\text{prop. inversi: } (ab)^{-1} = a^{-1}b^{-1}$$

il prodotto di due invertibili è invertibile

### EL. IRREDUCIBILI

$$a \in A \setminus A^\times \quad \forall b, c \in A,$$

$$a=bc \Rightarrow b \cdot c \in A^\times$$

$$\text{primo} \Leftrightarrow \text{irriducibile}$$

### DOMINIO

A anello  $\neq \{0\}$  in cui

l'unico divisore di zero è  $0_A$

campo

### ALGEBRICAMENTE CHIUSO

K campo, se:  $\forall f \in K[X] \setminus K$

$\exists x \in K$  t.c. x radice di f

(se ha almeno una radice in K)

• è alg. chiuso se e solo se i soli

polinomi irr. monici sono di 1° grado

## MONDO DELLA DIVISIBILITÀ

$$(\text{div. euclidea}) \quad a, n \in \mathbb{Z}, n \neq 0 \quad \exists! q \in \mathbb{Z}, r \in \{0, \dots, |n|-1\}$$

t.c.  $a = qn + r$  t.c.  $r < n$

$$\text{è una rel. di c.: } a|b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$$

### DIVISIBILITÀ E CONGRUENZA MOD N

$$a|b \Leftrightarrow b = a \cdot c$$

b resto a/b

$$a \equiv_n b \Leftrightarrow n | a-b$$

$$\text{è una rel. di equivalenza} \rightarrow \text{utile!} \quad a \equiv_n b \Leftrightarrow b \equiv_n a$$

simm.

$$(n | a-b \Leftrightarrow n | b-a)$$

nota:

$$a \equiv_n a', b \equiv_n b' \Rightarrow a+b \equiv_n a'+b'$$

$$ab \equiv_n a'b'$$

utili!!

$$1. \text{ Gauss: se } \text{MCD}(a, b) = 1$$

$$\text{allora } a|bc \Rightarrow a|c$$

$$(a, b \in \mathbb{Z}^*, c \in \mathbb{Z})$$

$$\text{lemma: se } \text{MCD}(a, b, c) = 1$$

$$\text{e } a, b | c \text{ allora } abc | c$$

### TEOREMA FONDAMENTALE ARITMETICA

$$\forall a \in \mathbb{Z}^*, \quad ① \text{ l'insieme } I_a = \{p \text{ primo: } p|a\} \text{ è finito}$$

$$② \quad a = \pm 1 \cdot \prod_p p^{v_p(a)}$$

uniche  $\in \mathbb{N}$

(ogni numero è una combinazione di primi elevati a qualcosa)

$$a \cdot b = \prod_p p^{v_p(a) + v_p(b)}$$

$$= p^{v_p(a)} \cdot p^{v_p(b)} = p^{v_p(a) + v_p(b)}$$

### FERMAT

$$n^p \equiv_p n \quad (p \text{ primo})$$

$$\text{quindi } n^{p-1} \equiv 1$$

$$\text{conseguenza: } [n]_p^{-1} = [n]_p^{p-2}$$

### MCD

$$\delta = \text{MCD}(a, b) \quad \text{se}$$

$$① \delta | a, \delta | b$$

$$② \text{ dato } d' \in \mathbb{N} \text{ t.c. } d'|a \text{ e } d'|b$$

allora  $d' | \delta$

$$\bullet \delta \mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$$

$$\text{id. Bézout } \delta = u \cdot a + v \cdot b \quad \exists u, v \in \mathbb{Z}$$

$$\text{Fibo e MCD: } \text{MCD}(F_m, F_{m+1}) = 1$$

### conseguenze

$$a|b \Leftrightarrow \forall p, v_p(a) \leq v_p(b)$$

$$\text{MCD}(a, b) = \prod_p p^{\min(v_p(a), v_p(b))}$$

## POLINOMI (sono domini)

### def polinomio

$$P = \sum_{i \geq 0} a_i X^i$$

### operazioni

$$P+Q := \sum_{i \geq 0} (a_i + b_i) X^i$$

$$P \cdot Q := \sum_{k \geq 0} c_k X^k \quad \text{Cauchy}$$

$$c_k = \sum_{i+j=k} a_i b_j$$

### grado di un polinomio

$$\deg(0) = -\infty \quad (\deg(a) = -\infty \iff a = 0)$$

$$\deg(P) = \max \{i \in \mathbb{N}, a_i \neq 0\}$$

$$\deg: K[X] \longrightarrow \mathbb{N} \cup \{-\infty\}$$

$$\deg(a+b) \leq \max(\deg(a), \deg(b))$$

$$(\deg(a+b) = \max(\deg(a), \deg(b)) \text{ se } \deg(a) \neq \deg(b))$$

$$\deg(ab) = \deg(a) + \deg(b)$$

### POLINOMI MONICI

$$P = a_0 + a_1 X + \dots + a_n X^n$$

$$\text{con } a_n = 1 \quad (\text{coeff. deg massima})$$

$$\text{prodotto di monici \u00e8 monico}$$

### FATTORIZZAZIONE

i polinomi irriducibili sono:

$$\bullet \text{ in } \mathbb{C}[X]: \deg(P) = 1 \quad (\text{forma } X - \alpha \quad \alpha \in \mathbb{C})$$

$$\bullet \text{ in } \mathbb{R}[X] \quad \textcircled{1} \deg(P) = 1$$

$$\textcircled{2} \deg(P) = 2 \quad \text{e} \quad \Delta = a^2 - 4b < 0$$

polinomi noti:

$$n \geq 1 \quad X^n - 1 = \prod_{i=0}^{n-1} (X - x^i) \quad \text{con } x = e^{\frac{2\pi i}{n}}$$

### C- VALORE ASSOLUTO

$$|P|_c := c^{\deg(P)} \quad c > 1$$

$$|0| := 0 = c^{-\infty}$$

$$\bullet |a|_c = 0 \iff a = 0$$

$$\bullet |ab|_c = |a|_c \cdot |b|_c$$

$$\bullet |a+b|_c \leq \max(|a|_c, |b|_c) \\ \leq |a|_c + |b|_c$$

$$(\text{div. euclideo}) \quad a, b \in A = K[X] \quad (a, b) \neq (0, 0)$$

$$\exists! (q, r) \in A \text{ t.c. } a = qb + r \quad \text{con } \deg(r) < \deg(b) \\ \text{ovvero } |r|_c < |b|_c$$

inversi

$$A^\times = K^\times$$

(sono le "costanti" inverse del campo)

$$(\text{anche qui vale } a|b, b|a \iff \exists \lambda \in A^\times \text{ t.c. } b = \lambda a)$$

$$(A/HA = \{a + Ha : a \in A \text{ t.c. } \deg(a) < \deg(H)\} \text{ \u00e8 anello cu.})$$

(anche qui MCD)

### FATTORIZZAZIONE UNICA

$$\forall H \in A \setminus \{0\}$$

$$H = \lambda \cdot \prod_{\substack{p \text{ irr.} \\ p \in A^+}} p^{v_p(H)}$$

$$\text{con } (v_p(H) \in \mathbb{N} \text{ e } \{p: v_p(H) \neq 0\} \text{ finito})$$

### VALUTAZIONE

$$F \in K[X] = F_0 + F_1 X + \dots + F_n X^n$$

$$\text{ev}_x(F) = F_0 + F_1 x + \dots + F_n x^n$$

$$\text{ev}: K[X] \longrightarrow K$$

$$\bullet \text{ev}_x^{-1}(\{0\}) = (X - x)A$$

(pol. che si annullano in x)

campo

### ALGEBRICAMENTE CHIUSO

$$K \text{ campo, se: } \forall F \in K[X] \setminus K$$

$$\exists x \in K \text{ t.c. } x \text{ radice di } F$$

(se ho almeno una radice in K)

\u2022 \u00e8 alg. chiuso se e solo se i soli

polinomi irr monici sono di 1o grado



MOLTEPLICITÀ

K algebricamente chiuso

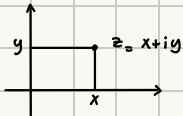
# NUMERI COMPLESSI

$\mathbb{R} \subset \mathbb{C}$   $\mathbb{C}$  è un Campo


$$\mathbb{C} = \{x+iy : x, y \in \mathbb{R}\} \quad i: \sqrt{-1} \text{ caratterizzata come } i^2 = -1$$

$= \mathbb{R} + i\mathbb{R}$

numero complesso:  $z = \overbrace{x+iy}^{\text{parte reale}} + \underbrace{iy}_{\text{parte immaginaria}}$



## RAPPRESENTAZIONE POLARE



$z = \rho e^{i\theta} \quad \rho = \sqrt{x^2 + y^2} = |z|$

Oss: cerchio delle unità

$z \in \mathbb{C}$  è della forma  $z = e^{i\theta}$

$\iff |z| = 1$  quindi giace sul cerchio delle unità

e  $\exists \theta$  t.c.  $z = \cos(\theta) + i\sin(\theta)$

operazioni:  $-z = -x + i(-y)$  opposto

$$z + z' = (x+x') + i(y+y')$$

$$zz' = xx' - yy' + i(x'y + xy')$$

## CONIUGAZIONE COMPLESSA

$$\bar{z} = x - iy$$

formule fondamentali

$$z\bar{z} = x^2 + y^2$$

realtà:  $z \in \mathbb{R} \iff z = \bar{z}$

$$\overline{z+z'} = \bar{z} + \bar{z}'$$

$$\overline{zz'} = \bar{z} \bar{z}'$$

$$\overline{-z} = -\bar{z}$$

$$\bar{\bar{z}} = z \text{ biettiva } h^{-1} = h$$

VAL. ASS. COMPLESSO

$$|z| = \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$$

$$|z| = 0 \iff z = 0$$

$$|zz'| = |z| \cdot |z'|$$

$$|z+z'| \leq |z| + |z'|$$

esponenziale di Eulero

$$e^{i\theta} = \cos(\theta) + i\sin(\theta)$$

$$(e^{i\theta})^n = e^{i\theta n} \quad [\cos(\theta) + i\sin(\theta)]^n = \cos(n\theta) + i\sin(n\theta)$$

proprietà:  $\forall \theta \in \mathbb{R}$

$$|e^{i\theta}| = 1$$

$$(e^{i\theta})^{-1} = \overline{e^{i\theta}} = e^{-i\theta}$$

inverso

$$z \cdot \bar{z} (x^2 + y^2)^{-1} = 1$$

