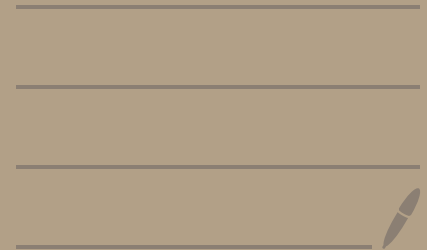


*(utili x esercizi, non approfondite o dimostrate)*

---

# FORMULE ALGEBRA



## GENERALI

anello  $(A, +, \cdot, 0_A, 1_A)$

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

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

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

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

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

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

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

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

Cancellazione in un anello A

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

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

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

prop. inversi:  $(ab)^{-1} = a^{-1}b^{-1}$   
il prodotto di due invertibili è invertibile

EL. IRREDUCIBILI

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

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

primo  $\Leftrightarrow$  irriducibile

N. PRIMO

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

$$\forall b, c \in A, \quad a|bc \Rightarrow a|b \text{ o } a|c$$

CAMPO

A anello comm. un.

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

$$a \in A^\times$$

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

ogni campo  
è un dominio

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

GRUPPO  $(G, *, e)$

$$(a*b)*c = a*(b*c) \quad \text{assoc.}$$

$$a*e = e*a = a \quad \text{el. neutro}$$

$$a*a' = a'*a = e \quad \text{inverso}$$

$$\text{abeliano: } a*b = b*a \quad \text{commutativo}$$

not. additive  $(G, +, 0)$  moltiplicativa  $(G, \cdot, 1)$

## MONDO DELLA DIVISIBILITÀ

(div. euclidea)  $a, n \in \mathbb{Z}, n \neq 0 \quad \exists! q \in \mathbb{Z}, r \in \{0, \dots, |n|-1\}$   
t.c.  $a = qn + r$   $\hookrightarrow$  utile!  $r < n$

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

DIVISIBILITÀ E CONGRUENZA MOD N

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

b resto a/b

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

è una rel. di equivalenza  $\rightarrow$  utile!  $a \equiv_n b \Leftrightarrow b \equiv_n a$   
simmetria  
( $n | a-b \Leftrightarrow n | b-a$ )

nota:

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

utili!!

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

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

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

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

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

TEOREMA FONDAMENTALE ARITMETICA

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

$$\text{② } a = \pm 1 \cdot \prod_p p^{v_p(a)} \quad \text{unici } e \in \mathbb{N}$$

(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

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

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

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

$$\text{in } \mathbb{Z}/p\mathbb{Z}: ([a]+[b])^p = [a]^p + [b]^p$$

MCD

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

$$\text{① } \delta | a, \delta | b$$

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

allora  $d' | \delta$

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

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

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

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

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

con  $a_n = 1$  (coeff. deg massima)

• prodotto di monici è 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:

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

•  $P \in \mathbb{R}[X]$  di grado dispari ammette almeno una radice reale

(es.  $\mathbb{Q}[X]$ )

in  $K[X]$ : •  $\deg(Q) = 1$  irriducibile

$$\bullet \deg(Q) = 2 \quad \text{irriducibile} \quad Q = P_1 P_2 \quad \text{irr. deg 1}$$

$$\bullet \deg(Q) = 3 \quad \text{irriducibile} \quad Q = P_1 P_2 \quad \deg(P_1) = 1, P_2 \text{ irr. deg 2}$$

$$\bullet \deg(Q) = 4 \quad \text{irriducibile} \quad Q = P_1 P_2 \quad \deg(P_1) = 1 \deg(P_2) = 3$$

### C- VALORE ASSOLUTO

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

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

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

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

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

(div. euclidea)  $a, b \in A = K[X] \quad (a, b) \neq (0, 0)$

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

inversi:

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

(sono le "costanti" inverse del campo)

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

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

(anche qui MCD)

### VALUTAZIONE

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

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

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

### polinomio convergente

$$\text{data } F = F_0 + F_1 X + \dots + F_n X^n,$$

$$\bar{F} = \bar{F}_0 + \bar{F}_1 X + \dots + \bar{F}_n X^n$$

insieme radici

$$\mathcal{R} = \mathcal{R}_{\mathbb{R}} \sqcup \mathcal{R}_{\mathbb{C} \setminus \mathbb{R}}^+ \sqcup \mathcal{R}_{\mathbb{C} \setminus \mathbb{R}}^-$$

### FATTORIZZAZIONE UNICA

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

$$H = \lambda \cdot \prod_{P \text{ irr.}} P^{v_P(H)}$$

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

campo

### ALGEBRICAMENTE CHIUSO

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

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

(se ho almeno una radice in  $K$ )

• è alg. chiuso se e solo se i soli

polinomi irr. monici sono di 1° grado

### MOLTEPLICITÀ

$K$  algebricamente chiuso  $\implies \forall F \in K[X] \setminus \{0\}$

si scrive in modo unico come:

$$F = \lambda \prod_{x \in K} (X - x)^{v_x(F)}$$

$v_x(F) \rightarrow$  è la molteplicità di  $F$  in  $x$

$$\text{fatt. in } \mathbb{R}[X] \quad \forall F \in \mathbb{R}[X], F = \lambda \prod_{\substack{x \in \mathbb{R} \\ x \in \mathbb{R}}} (X - x)^{v_x(F)} \prod_{\substack{z \in \mathbb{C} \\ z \in \mathbb{C} \setminus \mathbb{R}}} [(X - z)(X - \bar{z})]^{v_z(F)}$$

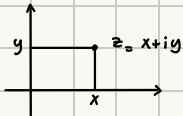
# NUMERI COMPLESSI

$\mathbb{R} \subset \mathbb{C}$   $\mathbb{C}$  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:  $z = \overbrace{x}^{\text{parte reale}} + i \overbrace{y}^{\text{parte immaginaria}}$



## 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

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

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

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

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

$\bar{\bar{z}}$  biettiva  $h^{-1} = h$   
ed è un isomorf. di anelli

## formule fondamentali

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

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

## 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

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

$\mathbb{C}$  è algebricamente chiuso  
(teorema fond. algebra)

# GRUPPI

## GRUPPO $(G, *, e)$

- $(a * b) * c = a * (b * c)$  *associativo*
- $a * e = e * a = a$  *el neutro*
- $a * a' = a' * a = e$  *inverso*
- abeliano*:  $a * b = b * a$  *commutativo*

not. additive  $(G, +, 0)$  *multiplicativa*  $(G, \cdot, 1)$

## OMOMORFISMO DI GRUPPI

$f: G_1 \rightarrow G_2$  t.c.  
 $f(a \cdot b) = f(a) \cdot f(b)$

(quindi, ①  $f(1_{G_1}) = 1_{G_2}$   
②  $f(a^{-1}) = f(a)^{-1}$ )

isomorfismo: omom. biiettivo

## PERMUTAZIONI

$E$  finito,  $S(E) = \{f: E \rightarrow E: f \text{ bi} \}$   
 $(S(E), \circ, Id_E)$  è un gruppo (di perm.)  
•  $f, g \in S(E) \rightarrow g \circ f \in S(E)$

permutazione  $f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$

$n$ -ciclo:  $\begin{pmatrix} a_1 & a_2 & \dots & a_{s-1} & a_s & a_{s+1} \\ a_2 & a_3 & \dots & a_s & a_{s+1} & a_1 \end{pmatrix}$

fissa gli el.  $\notin \{a_1, \dots, a_s\}$ , manda gli altri:  
 $a_i \rightarrow a_{i+1}$ , tranne  $a_s \rightarrow a_1$

notazione  $(a_1 a_2 a_3 \dots a_s)$

noto:  $(a_1 a_2 a_3) = (a_3 a_1 a_2)$   
 $\neq (a_2 a_1 a_3)$

trasposizione: 2-ciclo

## SOTTOGRUPPO

$H \leq G$  t.c.  $\forall a, b \in H$   
 $a * b^{-1} \in H$   
 $1_G = 1_H \in H, ab \in H$

## SG. NORMALE $H \triangleleft G$

- $xH = Hx \quad \forall x \in G$
- $gh = h'g \quad \forall g \in G, \forall h \in H, \exists h' \in H$
- $H^g = H \quad \forall g \in G$

•  $G$  abeliano e  $H \leq G \Rightarrow H \triangleleft G$

• se  $f: G_1 \rightarrow G_2$  omom.,  $\text{Ker}(f) \triangleleft G_1$   
inoltre, se  $H \triangleleft G$ , allora  $H = \text{Ker}(\pi_H)$

## KERNEL

$f: G_1 \rightarrow G_2$  omom.  
 $H = \{g \in G_1: f(g) = 1_{G_2}\}$   
 $= f^{-1}(\{1_{G_2}\})$  *el.  $G_1$  che passano a  $1_{G_2}$*

•  $\text{Ker}(f) = \{1_{G_1}\} \iff f$  iniettivo

## IMMAGINE

$f: G_1 \rightarrow G_2$  omom.  
 $f(G_1) \leq G_2$   
 $= \{y \in G_2: \exists x \in G_1 \text{ con } f(x) = y\}$

## SOTTOGRUPPI CONIUGATI

dato  $H \leq G, g \in G$   
 $H^g := \{g' \in G: \exists h \in H \text{ t.c. } g' = g^{-1} h g\}$   
• se  $G$  abeliano,  $H^g = H$  ( $g^{-1} \cdot g = 1_G$ )

## SOTTOGR. GENERATO da $I \leq G$

$\langle I \rangle := \bigcap_{\substack{H \leq G: \\ I \leq H}} H$

$\langle g \rangle = \bigcap_{\substack{H \leq G: \\ g \in H}} H = g^{\mathbb{Z}}$  se  $G$  finito,  $\exists n \in \mathbb{N}^*$

$\langle g \rangle = g^{\mathbb{Z}} \cong \mathbb{Z}/\text{ord}(g)\mathbb{Z}$

## ORDINE DI UN EL

$G$  finito e  $g \in G$ ,  
 $\text{ord}(g) = \min \{d \in \mathbb{N}^* \text{ t.c. } g^d = 1_G\}$

•  $\sigma$   $n$ -ciclo,  $\text{ord}(\sigma) = n$   
quindi  $\sigma^n = 1_S$

## ORD( $\sigma$ )

$\text{ord}(\sigma) = \text{mcm}(\text{ord}(c_1), \dots, \text{ord}(c_n))$   
cicli a supp. disgiunti

## SEGNO DI UNA PERM

$S$  numero di trasposizioni in cui si decompone  $\sigma$   
 $\varepsilon_\sigma = (-1)^S \in \mathbb{Z}^x$  (+1 pari, -1 disp)

•  $\sigma$   $n$ -ciclo  $\Rightarrow \varepsilon(\sigma) = (-1)^{n-1}$

•  $S_n \xrightarrow{\varepsilon} \mathbb{Z}^x$  omom. gruppi

## PRODOTTO DIRETTO CART. GRUPPI (è gruppo)

$G_1 \times G_2 = \{(g_1, g_2): g_1 \in G_1, g_2 \in G_2\}$

op:  $(g_1, g_2) + (g_3, g_4) = (g_1 + g_3, g_2 + g_4)$   
neutro:  $(0_{G_1}, 0_{G_2})$

• è abeliano se  $G_1, G_2$  lo sono

## relazione $\sim$

$H \leq G, x, x' \in G \quad x \sim x' \iff x(x')^{-1} \in H$   
è di equivalenza

classi laterali **GRUPPO**  $G/H = G/H$

•  $[g] = gH = Hg \quad 1_{G/H} = H$

## sottogruppi di $\mathbb{Z}$ :

sono  $\{0\}$  o  $n\mathbb{Z}$

## TEOREMA DI LAGRANGE

$G$  finito,  $H \leq G$   
allora  $\#H \mid \#G$

## GRUPPI CICLICI

$G$  gr.  $g \in G$   $\text{ord}(g) = n \geq 1$

$\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$

$\forall d \mid n, \exists! H_d \leq \langle g \rangle$  t.c.  $\#H_d = d$

## INVERSIONE

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 6 & 7 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \uparrow & \uparrow & \uparrow & \uparrow \\ 4 & 6 & 7 & 5 \end{pmatrix}$

ciclo  $(123)^{-1} = (321)$

## COMPOSIZIONE (PRODOTTO)

$\sigma \circ \tau$ : si applica  $\tau$ , poi  $\sigma$

$\sigma = (1342), \tau = (15324)$

$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \\ \sigma & \tau & & & \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}$

## cicli a supporti disgiunti

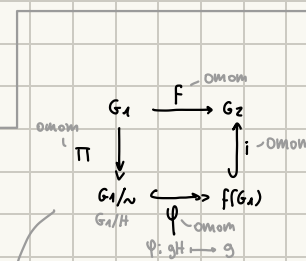
$(a_1 \dots a_s), (b_1 \dots b_t),$   
se  $\{a_1 \dots a_s\} \cap \{b_1 \dots b_t\} = \emptyset$

ogni  $\sigma \in S_n$  può essere  
decomposto in prod. di cicli

a supp. disgi. (UNICAMENTE DET,  
e che commutano)

## $n$ -ciclo

•  $\sigma = (a_1 a_2 \dots a_n) =$   
 $(a_n a_{n-1}) (a_n a_{n-2}) \dots (a_n a_1)$   
( $n-1$  fattori)



## 1o TEOR. OMOM. GRUPPI

$f$  omom  $\Rightarrow f = \underbrace{i \circ \varphi \circ \pi}_{\text{omom}}$

