(utili x esercizi, non approfondite o dimostrate)

FORMULE ALGEBRA

GENERALI

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

$a+b = b+a$ comm +

$(a+b)c = a+(b+c)$ ass. +

$a + 0_A = 0_A + a = a$ el neutro +

$a + (-a) = 0_A$ opposto

$a \cdot b = b \cdot a$ comm · (anello commutativo)

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ass ·

$a \cdot 1_A = 1_A \cdot a = a$ el neutro · (anello unitario)

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

Cancellazione in un anello A

se a non divisore di 0_A, $ab = ac \Rightarrow b = c$

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

INVERTIBILI $ab = ba = 1_A$

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

il prodotto di due invertibili è invertibile

EL. IRRIDUCIBILE

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

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

N. PRIMO

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

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

primo $\Longleftrightarrow$ irriducibile

CAMPO

A anello comm. un.

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

$a \in A^\times$

ogni campo è un dominio

DOMINIO

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

l'unico divisore di zero è 0_A

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

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

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 1o grado

GRUPPO $(G, *, e)$

- $(a*b)*c = a*(b*c)$ assoc.
- $a*e = e*a = a$ el. neutro
- $a*a' = a'*a = e$ inverso

abeliano: $a*b = b*a$ commut.

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

MONDO DELLA DIVISIBILITÀ

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

t.c. $a = qn + r$ — utile! $r < n$

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

DIVISIBILITÀ E CONGRUENZA MOD N

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

b resto a/b

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

è una rel di equivalenza $\longrightarrow$ utile! $a \equiv_n b \Longleftrightarrow b \equiv_n a$ (simm.)

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

nota:

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

$ab \equiv_n a'b'$

utili!!

nel mondo $\mathbb{Z}/n\mathbb{Z}$

$[a] + [b] = [a+b]$

$[a] \cdot [b] = [ab]$

1. Gauss: se $MCD(a,b) = 1$

allora $a | bc \Rightarrow a | c$

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

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

e $a, b | c$ allora $ab | c$

FERMAT

$n^p \equiv_p n$ (p primo)

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

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

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

MCD

$\delta = MCD(a,b)$ se

① $\delta | a$, $\delta | b$

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

allora $d' | \delta$

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

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

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

TEOREMA FONDAMENTALE ARITMETICA

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

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

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

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

conseguenze

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

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

POLINOMI (sono domini)

def polinomio

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

operazioni

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

$P\cdot Q := \sum_{k\geq 0} c_k X^k$ Cauchy, $c_k = \sum_{i+j=k} a_i b_j$

grado di un polinomio

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

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

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

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

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

C-VALORE ASSOLUTO

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

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

- $|a|_c = 0 \iff a = 0$
- $|ab|_c = |a|_c \cdot |b|_c$
- $|a+b|_c \leq \max(|a|_c, |b|_c)$ $\leq |a|_c + |b|_c$

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

$\exists! \, (q,r) \in A$ t.c. $a = qb + r$ con $\deg(r) < \deg(b)$

ovvero $|r|_c < |b|_c$

inversi

$A^\times = K^\times$

(sono le "costanti" inverse del campo)

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

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

(anche qui MCD)

POLINOMI MONICI

$P = a_0 + aX + \ldots + a_n X^n$

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

- prodotto di monici è monico

FATTORIZZAZIONE UNICA

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

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

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

VALUTAZIONE

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

$ev_x(F) = F_0 + F_1 x + \ldots + F_n x^n$

$ev: K[X] \longrightarrow K$

- $ev_x^{-1}(\{0\}) = (X-x)A$ (pol. che si annullano in x)

polinomio coniugato

dato $F = f_0 + f_1 X + \ldots + f_n X^n$,

$\overline{F} = \overline{f_0} + \overline{f_1} X + \ldots + \overline{f_n} X^n$

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

i polinomi irriducibili sono:

- in $\mathbb{C}[X]$: $\deg(P) = 1$ (forma $X - \alpha$ $\alpha \in \mathbb{C}$)
- in $\mathbb{R}[X]$ ① $\deg(P) = 1$
  ② $\deg(P) = 2$ e $\Delta = a^2 - 4b < 0$

polinomi noti:

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

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

in $K[X]$ (es. $\mathbb{Q}[X]$) campo:

- $\deg(Q) = 1$ irriducibile
- $\deg(Q) = 2$ — irriducibile / $Q = P_1 P_2$ irr. deg 1
- $\deg(Q) = 3$ — irriducibile / $Q = P_1 P_2$ $\deg(P_1) = 1$, P_2 irr. deg 2
- $\deg(Q) = 4$ — irriducibile / $Q = P_1 P_2$ — $\deg(P_1) = 1$ $\deg(P_2) = 3$ / deg

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

MOLTEPLICITÀ

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

si scrive in modo unico come:

$F = \lambda_{\in K^\times} \prod_{x\in K} (X-x)^{V_x(F)}$ → è la molteplicità di F in x

fatt. in $\mathbb{R}[X]$ $\forall F \in \mathbb{R}[X]$, $F = \lambda_{\in \mathbb{R}^\times} \prod_{x\in \mathcal{R}_{\mathbb{R}}} (X-x)^{V_x(F)} \prod_{z \in \mathcal{R}^+_{\mathbb{C}\setminus\mathbb{R}}} [\underbrace{(X-z)(X-\bar{z})}_{\deg 2 \text{ irr in } \mathbb{R}[X]}]^{V_z(F)}$

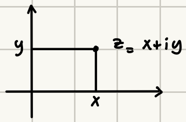
NUMERI COMPLESSI

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

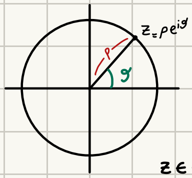
• $\mathbb{C} = \{ x+iy : x,y \in \mathbb{R} \}$ $i : \sqrt{-1}$ caratterizzato come $i^2 = -1$

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

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



RAPPRESENTAZIONE POLARE



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

OSS: cerchio delle unità

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

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

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

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

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

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

CONIUGAZIONE COMPLESSA

$\bar{z} = x - iy$

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

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

· $\overline{-z} = -\bar{z}$

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

formule fondamentali

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

reali $z \in \mathbb{R} \iff z = \bar{z}$

VAL. ASS. COMPLESSO

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

· $|z| = 0 \iff z = 0$

· $|zz'| = |z| \cdot |z'|$

· $|z+z'| \le |z| + |z'|$

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

esponenziale di Eulero

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

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

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

• $|e^{i\vartheta}| = 1$

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

inverso

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

GRUPPI

GRUPPO $(G, *, e)$

- $(a * b) * c = a * (b * c)$ assoc.
- $a * e = e * a = a$ el. neutro
- $a * a' = a' * a = e$ inverso

abeliano: $a * b = b * a$ commut.

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

omomorfismo di gruppi

$f: G_1 \to G_2$ t.c. ($\cdot, 1_{G_1}$; $\circ, 1_{G_2}$)

$f(a \cdot b) = f(a) \circ f(b)$

(quindi, ① $f(1_{G_1}) = 1_{G_2}$

② $f(a^{-1}) = f(a)^{-1}$) (inv. G_1, inv. G_2)

isomorfismo: omom. biiettivo

SOTTOGRUPPO

$H \subset G$ t.c. $\forall a, b \in H$

$a * b^{-1} \in H$

$1_G = 1_H \in H$, $ab \in H$

KERNEL

$f: G_1 \to G_2$ omom.

$H = \{g \in G_1 : f(g) = 1_{G_2}\}$

$= f^{-1}(\{1_{G_2}\})$ el. G_1 che portano a 1_{G_2}

- $\mathrm{Ker}(f) = \{1_{G_1}\} \iff f$ iniettiva

IMMAGINE

$f: G_1 \to G_2$ omom.

$f(G_1) < G_2$

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

SOTTOGRUPPI CONIUGATI

dati $H < G$, $g \in G$

$H^g := \{g' \in G : \exists h \in H \text{ t.c. } g' = g^{-1}hg\}$

- se G abeliano, $H^g = H$ ($g^{-1} \cdot g = 1_G$)

SOTTOGR. GENERATO da $I \subset G$

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

$\langle g \rangle = \bigcap_{\substack{H < G: \\ g \in H}} H = g^{\mathbb{Z}}$ ($\langle g \rangle$, $g \in G$)

se G finito, $\exists n \in \mathbb{N}^*$

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

sottogruppi di $\mathbb{Z}$:

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

SG. NORMALE $H \triangleleft G$

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

- $\cap$ sottogr è un sottogr.

($\cup$ sottogr. non per forza)

- G abeliano e $H < G \Rightarrow H \triangleleft G$
- se $f: G_1 \to G_2$ omom, $\mathrm{Ker}(f) \triangleleft G_1$

inoltre, se $H \triangleleft G$, allora $H = \mathrm{Ker}(\pi_H)$

($g \mapsto [g]$, $G \to G/H$)

ORDINE DI UN EL

G finito e $g \in G$,

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

TEOREMA DI LAGRANGE

G finito, $H < G$

allora $\#H \mid \#G$

- σ n-ciclo, $\mathrm{ord}(\sigma) = n$

quindi $\sigma^n = 1_S$

GRUPPI CICLICI

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

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

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

PERMUTAZIONI

$\mathcal{E}$ finito, $S(\mathcal{E}) = \{f: \mathcal{E} \to \mathcal{E} : f \text{ biì}\}$

$(S(\mathcal{E}), \circ, \mathrm{Id}_{\mathcal{E}})$ è un gruppo (di perm.)

- $f, g \in S(\mathcal{E}) \to g \circ f \in S(\mathcal{E})$

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

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

fisso gli el $\notin \{a_1 \ldots a_s\}$, mando gli altri:

$a_i \to a_{i+1}$, tranne $a_s \to a_1$

notazione $(a_1 a_2 a_3 \ldots a_s)$

nota: $(a_1 a_2 a_3) = (a_3 a_1 a_2)$ shift ok

$\neq (a_2 a_1 a_3)$ rimescolare no

trasposizione: 2-ciclo

INVERSIONE

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

ciclo $(1\,2\,3)^{-1} = (3\,2\,1)$

COMPOSIZIONE (PRODOTTO)

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

$\sigma = (1\,3\,4\,2)$, $\tau = (1\,5\,3\,2\,4)$

$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix}$ (τ, σ)

cicli a supporti disgiunti

$(a_1 \ldots a_s)$, $(b_1 \ldots b_s)$,

se $\{a_1 \ldots a_s\} \cap \{b_1 \ldots b_s\} = \emptyset$

$\downarrow$

ogni $\sigma \in S_n$ può essere decomposta in prod. di cicli a supp. disg. (UNICAMENTE DET, e che commutano)

anche

ogni permutazione si può decomporre in un prodotto di trasposizioni

n-ciclo

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

($n-1$ fattori)

ORD (σ)

$\mathrm{ord}(\sigma) = \mathrm{mcm}(\mathrm{ord}(c_1), \ldots, \mathrm{ord}(c_n))$

cicli a supp. disgiunti

SEGNO DI UNA PERM

s numero di trasposizioni in cui si decompone σ

$\varepsilon_\sigma = (-1)^s \in \mathbb{Z}^\times$ (+1 pari, −1 disp)

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

- $S_n \xrightarrow{\varepsilon} \mathbb{Z}^\times$ 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
- $O_{G_1 \times G_2} = (O_{G_1}, O_{G_2})$

- è abeliano se G_1, G_2 lo sono

relazione $\sim$

$H < G$, $x, x' \in G$ $\quad x \sim x' \iff x(x')^{-1} \in H$

è di equivalenza

classi laterali GRUPPO $G/\!\sim\, = G/H$

- $[g] = gH = Hg$ $\quad$ - $1_{G/H} = H$

$$\begin{tikzcd} G_1 \arrow[r, "f"', "\text{omom}"] \arrow[d, "\pi"', "\text{omom}"] & G_2 \\ G_1/\!\sim \;(G_1/H) \arrow[r, "\varphi", "\text{omom}"'] & f(G_1) \arrow[u, "i"', "\text{omom}"] \end{tikzcd}$$

$\varphi: gH \mapsto g$

1° TEOR. OMOM. GRUPP.

f omom $\Rightarrow f = i \circ \varphi \circ \pi$ (omom)

SPAZI VETTORIALI