(utili x esercizi, non approfondite o dimostrate)

## GENERALI

### anello

$a+b = b+a$ 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. $\forall a \in A \setminus \{0\}$

$a \in A^\times$

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

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

### 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 1o grado

## 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

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

è una rel di equivalenza $\longrightarrow$ utile! $a \equiv_n b \overset{\text{simm.}}{\Longleftrightarrow} b \equiv_n a$

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

nota:

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

$ab \equiv_n a'b'$

utili!!

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 $ab|c$

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

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

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

### 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

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

in $K[X]$ (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 1o grado

**MOLTEPLICITÀ**

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

si scrive in modo unico come:

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

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

Fatt in $\mathbb{R}[X]$ $\forall F \in \mathbb{R}[X]$, $F = \underset{\in \mathbb{R}^\times}{\lambda} \prod_{x \in \mathcal{R}_{\mathbb{R}}} (X - x)^{v_x(F)} \prod_{z \in \mathcal{R}^+_{\mathbb{C} \setminus \mathbb{R}}} [\overbrace{(X - z)(X - \overline{z})}^{\text{deg 2 irr in } \mathbb{R}[X]}]^{v_z(F)}$

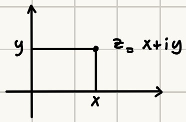
# NUMERI COMPLESSI

$\mathbb{R} \subset \mathbb{C}$ $\quad$ $\mathbb{C}$ è un campo

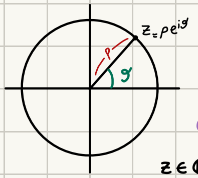
- $\mathbb{C} = \{ x + iy : x, y \in \mathbb{R} \}$ $\quad$ $i : \sqrt{-1}$ caratterizzato come $i^2 = -1$

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

numero complesso: $z = \overset{\text{parte reale}}{x} + i \underset{\text{parte immaginaria}}{y}$




## RAPPRESENTAZIONE POLARE




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

oss: cerchio delle unità

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

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

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

operazioni: $-z = -x + i(-y)$ $\quad$ 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 $z \in \mathbb{R} \Longleftrightarrow z = \bar{z}$

## VAL. ASS. COMPLESSO

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

- $|z| = 0 \Longleftrightarrow z = 0$
- $|zz'| = |z| \cdot |z'|$
- $|z + z'| \leq |z| + |z'|$

esponenziale di Eulero

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

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

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)