

DEFINIZIONE DI POLINOMIO

PREMESSA

SIA $(A, +, \cdot)$ UN ANELLO COMMUTATIVO UNITARIO
UNA FUNZIONE $f: \mathbb{N} \rightarrow A$ SI DICE SUCCESSIONE DI
ELEMENTI DI A , NOTIAMO f COME $f = (a_m)_{m \in \mathbb{N}}$.
E NOTIAMO L' m -ESIMO ELEMENTO DI f COME $f(m) = a_m$.

DEFINIZIONE

$(a_m)_{m \in \mathbb{N}}$ È UN POLINOMIO $\iff (\exists k \in \mathbb{N}) ((\forall m \geq k) (a_m = 0_A))$
A COEFFICIENTI IN A

CIOÈ, UN POLINOMIO È UNA SUCCESSIONE CHE SI
ANNULLA DOPO UN CERTO NUMERO k DI TERMINI

DEFINIAMO L'INSIEME DEI POLINOMI DEFINIBILI SU A
COME $A[x]$

CHE CAMBIA TRA SUCCESSIONE E FUNZIONE

UNA SUCCESSIONE È UN PARTICOLARE TIPO DI
FUNZIONE $f: m \in \mathbb{N} \mapsto a_m \in \mathbb{N}$

TEOREMA DIVISIONE LUNGA VR È IL GRADO DI f
 SIA $(A, +, \cdot)$ UN ANELLO COMMUTATIVO UNITARIO,
 $f, g \in A_{\Sigma^3}$

$$CD(g) \in U(A) \Rightarrow (\exists! (q, r) \in A_{\Sigma^3} \times A_{\Sigma^3} (f = gq + r \quad \forall r < v_g))$$

DIM. \exists

$$\text{SE } VR < Vg \Rightarrow (q = 0, r = f)$$

ALTRIMENTI, SIANO $m = VR, n = Vg, a_v = CDf, b_v = CDg$

$$\text{PRENDO } k = a_v b_v^{-1} x^{n-m} g, V_k = n - m + m.$$

PRENDO ORA $h = f - k, V_h < VR$. PER IPOTESI INDUTTIVA
 $\exists (q_1, r_1) \in A_{\Sigma^3} \times A_{\Sigma^3} (h = gq_1 + r_1 \quad \forall r_1 > V_{r_1})$.

$$f = h + k = gq_1 + r_1 + a_v b_v^{-1} x^{n-m} g =$$

$$= g(q_1 + a_v b_v^{-1} x^{n-m}) + r_1, \text{ CHE È LA TESI} \quad \square$$

DIM. UNICITÀ (!)

SIANO PER ASSURDO $(q_1, r_1) \neq (q_2, r_2)$ COPPIE

PER CUI VALE LA TESI, ALLORA

$$f = gq_1 + r_1 = gq_2 + r_2 \quad \& \quad V_{r_1} < Vg \quad \& \quad V_{r_2} < Vg.$$

$$g(q_1 - q_2) = r_2 - r_1 \quad \& \quad \text{PER IPOTESI } Vg > V(r_2 - r_1)$$

VALE LA REGOLA DI ADDIZIONE DEI GRADI, QUINDI
 $Vg + V(q_1 - q_2) = V(r_2 - r_1) < Vg$, CIÒ È

$$Vg + V(q_1 - q_2) < Vg, \text{ ALLORA } V(q_1 - q_2) = -\infty, \text{ CIÒ È}$$

$$q_1 - q_2 = 0 \Leftrightarrow q_1 = q_2 \quad \& \quad \text{QUINDI } (q_1, r_1) = (q_2, r_2) \quad \square$$

INDUZIONE II

$$\left(\forall X \in PC(\mathbb{N}) \setminus \{\emptyset\} \right) \left(\left(\forall m \in \mathbb{N} \right) \left(\left(\forall k \in \mathbb{N} \right) \left(m \leq k < m \Rightarrow k \in X \right) \Rightarrow m \in X \right) \right) \Rightarrow \\ x = \mathbb{N}_{\min X}$$

$$\mathbb{N}_{\min X} = \{m \in \mathbb{N} \mid m \geq \min X\}$$

DIM

SIA $m = \min X$, PER ASSURDO $X \neq \mathbb{N}_{\min X}$.

PREndo $Y = \mathbb{N}_{\min X} \setminus X$, QUINDI $Y \neq \emptyset$, SIA $n = \min Y$, $n \neq m$.

SE $m \leq k < n$ È VERO, ALLORA $k \in X$ (* PER DEFINIZIONE DI \mathbb{N}_m)

SE $(m \leq k < n \Rightarrow k \in X)$ È VERO, ALLORA $n \in X$ (**)

SE $((m \leq k < n \Rightarrow k \in X) \Rightarrow n \in X)$ È VERO, ALLORA

$\mathbb{N}_{\min X} = X$, CHE È ASSURDO. \square

COS' È UN INSIEME FINITO DI CARDINALITÀ m ?

SIA S UN INSIEME, $|S| = n$ SIGNIFICA CHE ESISTE UNA BIETTIVA $f: S \rightarrow \{1, 2, \dots, n\}$, DOVE $\{1, 2, \dots, n\} \subseteq \mathbb{N}$

DIMOSTRAZIONE CHE SE $|S| = n$, $|P(S)| = 2^n$ (PER INDUZIONE)

S INSIEME FINITO $\Rightarrow |P(S)| = 2^n$

DIM

CASI BASE: $n = 0 \Leftrightarrow S = \emptyset \Rightarrow P(S) = \{\emptyset\} \Rightarrow |P(S)| = 1 = 2^0$ ✓
 $n = 1 \Leftrightarrow S = \{x\} \Rightarrow P(S) = \{\{x\}, \emptyset\} \Rightarrow |P(S)| = 2 = 2^1$ ✓

SUPpongo LA TESI VALIDA PER $n \in \mathbb{N}$ E DIMOSTRO PER $n+1$.

$|S| = n+1 \Rightarrow S \neq \emptyset$ $\exists f: S \rightarrow \{1, 2, \dots, n+1\}$ BIETTIVA.

PREndo UN $x \in S$ E PONGO $T = S \setminus \{x\}$. ESSENDO f BIETTIVA, L'IMMAGINE DI x È COMPRESA TRA $1 \leq m \leq n+1$, QUINDI, SIA $f(x) = m$, $1 \leq m \leq n+1$.

PRESA $f_T: T \rightarrow \{1, 2, \dots, m-1, m+1, \dots, n, n+1\}$. PER IPOTESI INDUTTIVA,

$m \in A$

$|P(T)| = 2^n$. $P(x) = \{\{x\}, \emptyset\}$, DI CONSEGUENZA $|P(S)| = 2^n \cdot 2 = 2^{n+1}$

CHE È LA TESI

PARTIZIONE DI UN INSIEME

SIA S UN INSIEME, $S \neq \emptyset$, F È UNA PARTIZIONE DI S SE VALGONO LE SEGUENTI

- 1) $(\forall x \in F)(x \neq \emptyset)$
- 2) $(\forall x, y \in F)(x \neq y \Rightarrow x \cap y = \emptyset)$
- 3) $\bigcup F = S$

TEOREMA FONDAMENTALE RELAZIONI DI EQUIVALENZA E PARTIZIONI

PER OGNI INSIEME A , ESISTE $\tilde{F}: \sim \in EQ(A) \hookrightarrow \text{PART}(A)$

DIM

• DIMOSTRAO L'INVERSAZIONE DI \tilde{F} . SIANO $\sim_1, \sim_2 \in EQ(A)$ TALI CHE $\tilde{F}(\sim_1) = \tilde{F}(\sim_2)$, CIOÈ CHE $A_{\sim_1} = A_{\sim_2} \Leftrightarrow \{\{x\}_{\sim_1} \mid x \in A\} = \{\{x\}_{\sim_2} \mid x \in A\}$.

$$(\forall x, y \in A)(x \sim_1 y \Leftrightarrow \{x\}_{\sim_1} = \{y\}_{\sim_1}) \Leftrightarrow (\exists z \in A)(\{x\}_{\sim_1} = \{z\}_{\sim_2}) \wedge (\exists w \in A)(\{y\}_{\sim_1} = \{w\}_{\sim_2}) \Leftrightarrow$$

$$\Leftrightarrow w \sim_2 z \Leftrightarrow x \sim_2 y$$

• DIMOSTRAO LA SURIESSIVITÀ DI \tilde{F} : SIA $F \in \text{PART}(A)$, DEFINISCO $(\forall x, y \in A)(x \sim y \mid (\exists z \in F)(x \in z \wedge y \in z))$ CIOÈ $x \sim y$ APPARTENGONO ALLO STESSO ELEMENTO DELLA PARTIZIONE

• DIMOSTRAO CHE \sim È DI EQUIVALENZA. SIA $F \in \text{PART}(A)$

• RIFLESSIVITÀ

$$(\forall x \in A)(\exists z \in F)(x \in z \wedge x \in z) \quad \checkmark$$

• SIMMETRIA

$$(\forall x, y \in A)(\exists z \in F)(x \in z \wedge y \in z) \Rightarrow y \in z \wedge x \in z$$

• TRANSITIVITÀ

SIANO $x \sim y \wedge y \sim z$, $F \in \text{PART}(A)$, PER DEFINIZIONE

$(\exists w_1, w_2 \in F)(x \in w_1 \wedge y \in w_1 \wedge y \in w_2 \wedge z \in w_2)$, CIOÈ $w_1 \cap w_2 \neq \emptyset$, PER DEFINIZIONE DI PARTIZIONE, $w_1 = w_2 \neq \emptyset$, CIOÈ $x \sim z$.



OMOMORFISMO TRA STRUTTURE

SIANO (S, \cdot) , $(\bar{S}, \bar{\cdot})$ DUE STRUTTURE ALGEBRICHE,
 $f: S \rightarrow \bar{S}$ È UN OMOMORFISMO $\Leftrightarrow (\forall x, y \in S) (x \cdot y = f(x) \bar{\cdot} f(y))$

MONOMORFISMO OMOMORFISMO INIETTIVO

EPIMORFISMO OMOMORFISMO SURIETTIVO

ISOMORFISMO OMOMORFISMO BIETTIVO

TEOREMA FONDAMENTALE OMOMORFISMO PER INSIEMI

PREMESSA

SIANO A, B INSIEMI, $f: A \rightarrow B$

- ESISTERÀ UN INSIEME IMMAGINE DI f , SOTTOSIEME DI B . ($\text{Im } f \subseteq B$)
- ESISTE ALLORA LA FUNZIONE IMMERSIONE $i: x \in \text{Im } f \mapsto x \in B$, INIETTIVA.
- AVREMO UN INSIEME QUOTIENTE DI A DEFINITO SU $\text{Ker } f$, PRENDO
 $\pi: x \in A \mapsto [x]_{\text{Ker } f}$, SURIETTIVA (LE CLASSI DI EQUIVALENZA NON SONO MOLTIPLICABILI)
- CHIUDO IL DIAGRAMMA CON $\tilde{f}: [x]_n \in A_n \mapsto f(x) \in \text{Im } f$

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \uparrow i & \\ A_n & \xrightarrow{\tilde{f}} & \text{Im } f \end{array}$$

VOLGO A DIMOSTRARE

- \tilde{f} BIETTIVA
- $\tilde{f} = i \circ f \circ \pi$

DIM

- 1) DEFINISCO $\pi: f(x) \in \text{Im } f \mapsto [x]_{\text{Ker } f} \in A_n$, VOLGO ARIE $\pi = \tilde{f}^{-1}$
 • INIETTIVITÀ DI π
 PER DEFINIZIONE DI NUCLEO DI EQUIVALENZA
 $(\forall x, y \in A) (f(x) = f(y) \Leftrightarrow [x]_{\text{Ker } f} = [y]_{\text{Ker } f})$, (NIETTIVÀ V)

• SURGETTIVITÀ DI \tilde{f}
 VERIFICATA PERCHÉ OGNI ELEMENTO APPARTIENE
 A UNA CLASSE DI EQUIVALENZA
 $y \in A_{\eta R} \Rightarrow (\exists x \in A)(y = f(x)_{\eta R})$ ✓

\tilde{f} È BIETTIVA, \tilde{f}^{-1} LA SUA INVERSA $\Rightarrow \tilde{f}^{-1}$ BIETTIVA

2) DUE FUNZIONI SONO UGUALI SE HANNO
 STESSO DOMINIO, CODOMINIO E IMMAGINE

$$f: A \rightarrow B$$

$$i \circ \tilde{f} \circ \pi: A \rightarrow A_{\eta R} \rightarrow \text{Im } f \rightarrow B \quad \checkmark$$

$$i(\tilde{f}(\pi(c_x))) = i(\tilde{f}(c_{\eta R})) = i(f(c_x)) = f(c_x) \quad \checkmark$$



FARE UN ESEMPIO DI ANELLO BOOLEANO A 3 E 8 ELEM.
 ESSENDO (PCS, \leq) UN RETTICOLO BOOLEANO E
 (PCS, Δ, \cap) IL SUO CORRISPETTIVO ANELLO BOOLEANO,
 $|PCS| = 3$ È IMPOSSIBILE, $|PCS| = 8 \Leftrightarrow |S| = 3$

MINORANTI E MAGGIORANTI

SIA (A, P) UN INSIEME ORDINATO, $T \subseteq A$,

$m \in A$ È MINORANTE $\Leftrightarrow (\forall x \in T)(m \leq x)$
 DI $T \subseteq A$

$M \in A$ È MAGGIORANTE $\Leftrightarrow (\forall x \in T)(x \leq M)$
 DI $T \subseteq A$

COME DEFINIRE UNA RELAZIONE BINARIA
SIA $A \neq \emptyset$, $P = (A \times A, g)$, CON $g \subseteq A \times A$,

$x, y \in A$ SONO IN RELAZIONE $\Leftrightarrow xPy \Leftrightarrow (x, y) \in g$

RELAZIONE DI EQUIVALENZA

$P = (A \times A, g)$, $g \subseteq A \times A$, $A \neq \emptyset$, $P \in \text{Equiv}(A) \Leftrightarrow$

- RIFLESSIVA ($\forall x \in A$) (xPx)
- SIMMETRICA ($\forall x, y \in A$) ($xPy \Rightarrow yPx$)
- TRANSITIVA ($\forall x, y, z \in A$) ($xPy \wedge yPz \Rightarrow xPz$)

RELAZIONE D'ORDINE

$P = (A \times A, g)$ È D'ORDINE \Leftrightarrow

- ANTISIMMETRICA ($\forall x, y \in A$) ($xPy \wedge yPx \Rightarrow x=y$)
- TRANSITIVA ($\forall x, y, z \in A$) ($xPy \wedge yPz \Rightarrow xPz$)

ORDINE LARGO

• RIFLESSIVITÀ: ($\forall x \in A$) (xPx)

ORDINE STRETTO

• ANTIRIFLESSIVITÀ ($\forall x \in A$) ($\neg xRx$)

PASSARE DA ORDINE LARGO A ORDINE STRETTO

SIA $P \in \text{OLCA}$, DEFINISCO $\bar{P} \in \text{OSCA}$ TALE CHE
 $(\forall x, y \in A) (x \bar{P} y \Leftrightarrow xPy \wedge x \neq y)$

PASSARE DA ORDINE STRETTO A ORDINE LARGO

SIA $P \in \text{OSCA}$, DEFINISCO $\bar{P} \in \text{OLCA}$ TALE CHE
 $(\forall x, y \in A) (x \bar{P} y \Leftrightarrow xPy \vee x=y)$

ANELLO BOOLEANO

ANELLI BOOLEANI, RETICOLI BOOLEANI E ALGEBRE DI BOOLE SONO EQUIVALENTI, IN PARTICOLARE, UN ANELLO $(A, +, \cdot)$ È BOOLEANO SE:

- $(A, +, \cdot)$ ANELLO COMMUTATIVO UNITARIO
- $(\forall x \in A) [x^2 = x \cdot x = x]$

DATO UN ANELLO BOOLEANO, COME SI DEFINISCE UN RETICOLO BOOLEANO?

SIA $(A, +, \cdot)$ ANELLO BOOLEANO, DEFINIAMO

$$P: (\forall x, y \in A) (x P y \Leftrightarrow x \cdot y = x) \Leftrightarrow (S, P) \text{ È UN RETICOLO BOOLEANO.}$$

PER ESSERE UN RETICOLO, $P \in \Omega(A)$

- RIFLESSIVITÀ: $(\forall x \in A) (x \cdot x = x) \Rightarrow (\forall x \in A) (x P x)$
- ANTISIMMETRIA: $(\forall x, y \in A) (x P y \wedge y P x \Rightarrow x \cdot y = x \wedge y \cdot x = y)$,
IN PIÙ, • È COMMUTATIVA, QUINDI $x \cdot y = y \cdot x = x = y$
- TRANSPRINTITÀ

$$(\forall x, y, z \in A) (x P y \wedge y P z \Rightarrow x P z)$$

$$x \cdot y = x \wedge y \cdot x = y \Rightarrow x \cdot z = (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y = x$$

CIOÈ $x P z$.

Ogni coppia di elementi deve ammettere infine sup.

(A, P) DEVE ESSERE LIMITATO

(A, P) DEVE ESSERE DISTRIBUTIVO

(A, P) DEVE ESSERE COMPLEMENTATO

COME DEFINIRE INSIEMI ORDINATI

SIA $A \neq \emptyset$, (A, ρ) È UN INSIEME ORDINATO
SE ρ È UNA RELAZIONE D'ORDINE, CIOÈ:

- ANTISIMMETRICA
- TRASITIVA

MINIMALI E MASSIMALI

SIA (A, ρ) UN INSIEME ORDINATO.

$m \in A$ MINIMALE $\iff (\forall x \in A)(x \rho m \vee m \rho x \Rightarrow m \rho x)$

$M \in A$ MASSIMALE $\iff (\forall x \in A)(x \rho M \vee M \rho x \Rightarrow x \rho M)$

SOMMA TRA POLINOMI

SIA $(A, +, \cdot)$ UN ANELLO COMMUTATIVO UNITARIO

$$(a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}} = (a_n + b_n)_{n \in \mathbb{N}}$$

IN GENERE VUOLE SAPERE QUESTA

PRODOTTO TRA POLINOMI

$$(a_n)_{n \in \mathbb{N}} \cdot (b_m)_{m \in \mathbb{N}} = \sum_{n+j=m} (a_n b_j)_{n \in \mathbb{N}}$$

QUANDO \mathbb{Z}_m È UN CAMPO?

QUANDO m È PRIMO

DIM

\mathbb{Z}_m È UN CAMPO $\Rightarrow m$ È PRIMO E \mathbb{Z}

VOGLIA DEMOSTRARE CHE GLI ELEMENTI NON NULLI SONO INVERTIBILI

SUPPONGO $[a]_m \neq [0]_m$, CON $0 < av < m$
 m È IRRIDUCIBILE, COE' $\text{DIV}(m) = \{-1, +1, -m, m\}$.
 $\Rightarrow \text{MCD}(a, m) = 1$.

PER BEZOUT $(\exists u, v \in \mathbb{Z}) (1 = au + mv)$, COE'
 $[1]_m = [au + mv]_m = [av]_m = [av]_m \cdot [v]_m$.
COE' SIGNIFICA CHE v È INVERTIBILE, QUINDI
 $(\mathbb{Z}_m, +, \cdot)$ È UN CAMPO.

DIVISORE DELLO 0

SIA $(A, +, \cdot)$ UN ANELLO UNITARIO,

$x \in A \setminus \{0_A\}$ È
DIVISORE DELLO $\iff \exists y \in A \setminus \{0\} y \cdot x = 0_A$
ZERO A SX

$z \in A \setminus \{0_A\}$ È
DIVISORE DELLO $\iff \exists y \in A \setminus \{0\} z \cdot y = 0_A$
ZERO A SX

UN DIVISORE DELLO ZERO A DESTRA È
SINGOLARE SI DICHIÀ DIVISORE DELLO ZERO

COME SI DIMOстра CHE n È PRIMO?

SE n È PRIMO, AMMETTE SOLO DIVISORI BANALI,
cioè $\text{DIV}(n) = \{-n, -1, 1, n\}$

DIM

SIA OÙ EZ UN DIVISORE DI n , cioè $n = ab$,
ALLORA $n|_2 \vee n|_b$. SUPpongo $n|_b$, QUINDI
TROVO KTZ TALE CHE $a = nk$, QUINDI $n = nk b$
 $\& kb = 1$. DATO CHE $\text{U}(\mathbb{Z}) = \{1, -1\}$, $b = \pm 1$, QUINDI
 n AMMETTE SOLO DIV. BANALI

SE $(\mathbb{Z}_n, +, \cdot)$ DOMINIO DI INTEGRITÀ, n È PRIMO

DIM

SIA $(\mathbb{Z}_n, +, \cdot)$ DOMINIO DI INTEGRITÀ, ALLORA
NON AMMETTE DIVISORI DEGLI ZERO, cioè,

SIA $n = ab$, ALLORA

$$[n]_n = [0]_n = [ab]_n = [a]_n \cdot [b]_n$$

TROVANDOCI IN UN DOMINIO DI INTEGRITÀ

$\bar{a} = \bar{0} \vee \bar{b} = \bar{0}$ PER LEGGE DI ANNULLAMENTO DEL PROD.

SUPpongo $\bar{a} = \bar{0}$, QUINDI $(a \equiv_n 0) \Leftrightarrow (\exists k \in \mathbb{Z}_n)(a = kn)$

$$\Rightarrow n = ab = knb \Rightarrow knb = 1 \Rightarrow b = \pm 1 \wedge a = \pm n.$$

QUINDI n È IRREDUCIBILE PERCHÉ HA SOLO DIV BAN

TEOREMA DI Divisione EUCLIDEA

$$(\forall m, n \in \mathbb{Z}) (\underline{m \neq 0} \Rightarrow \exists! (q, r) \in \mathbb{Z} \times \mathbb{N}) (m = mq + r \wedge 0 \leq r < |m|)$$

DIM (3) IN IN

- SE $m = 0 \Rightarrow (q, r) = (0, 0)$
- SE $m = |m|$, ALLORA
 - $\bullet m = m \Rightarrow (q, r) = (1, 0)$
 - $\bullet m = -m \Rightarrow (q, r) = (-1, 0)$
- SUPPONGO $0 \leq m < |m| \Rightarrow (q, r) = (0, m)$
- SUPPONGO $m > |m|$, ALLORA:

$m - |m| < m$ E PER IP. INDUTTIVA

$m - |m| = mq_1 + r_1 \quad 0 \leq r_1 < |m|$, QUINDI

VALE $m = mq_1 + |m| + r_1$

DATO CHE $m = mq_1 + |m| + r_1$

- SE $m > 0$, $q = q_1 + 1$, $r_1 = r$
- SE $m < 0$, $q = q_1 - 1$, $r_1 = r$

L'ASSESSIO È QUINDI VALIDO $\forall m \in \mathbb{N}$ PER INDUZIONE II

DIM \exists IN \mathbb{Z}

SIA $m < 0$

VALE $-m = mq_1 + r_1$ CON $0 \leq r_1 < |m|$

QUINDI $m = m(-q_1) - r_1$, PERO $-r_1 < 0$,

QUINDI SOTTRAENDO E SONO SOTTRAGGIO $|m|$, QUINDI

$m = m(-q_1) - r_1 + |m| - |m| \in$ C' SONO DUE CASI

• $m > 0 \Rightarrow q = -q_1 - m$, $r = m - r_1$

• $m < 0 \Rightarrow q = -q_1 + m$, $r = -m - r_1$

DIM !

SIANO $(q_1, r_1) \neq (q_2, r_2)$ COPPIE PER CUI VALE

LA TESI, SUPPONGO $0 \leq r_1 \leq r_2 < |m|$ E

$m = mq_1 + r_1 = mq_2 + r_2$, ALLORA

$m(q_1 - q_2) = r_2 - r_1$, ALLORA

$|m| |q_1 - q_2| = |m(q_1 - q_2)| = |r_2 - r_1| < |m|$

QUINDI $|m(q_1 - q_2)| < |m|$, QUINDI

$q_1 - q_2 = 0 \Rightarrow q_1 = q_2$

$\Rightarrow (q_1, r_1) = (q_2, r_2)$

BEZOUT

$$\left(\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\} \right) \left(\forall d \in \text{MCD}(a, b) \right) \left(\exists u, v \in \mathbb{Z} \right) \left(d = au + bv \right)$$

DIM PROVIMENTO SU T

SIA t IL MINIMO NUMERO DI PASSAGGI TAVI CHE

$r_t = 0$, SUPPONIAMO $a/b \in \mathbb{N}$

SE $t = 1$, ALLORA $r_1 = 0 \Rightarrow au = bq_1$, ALCORDA
 $b \in \text{MCD}(a, b) \Rightarrow b = 1 \cdot a + b \cdot 1$

SE $t = 2$, ALLORA $r_1 \neq 0$, $r_2 = 0$, QUINDI $r_1 = au \cdot 1 + b(-q_1)$

SUPPONGO L'ASSERZIONE VERA PER $r_i : 0 \leq i < t$

SE $t > 1 \Rightarrow r_{t-1} \in \text{MCD}(a, b)$

QUINDI $r_{t-1} = r_{t-3} + r_{t-2}(-q_{t-1})$ E PER IPOTESI INDUTTIVA

$\exists u, v, w, x \in \mathbb{Z} : (r_{t-3} = au + bv) \wedge (r_{t-2} = aw + bx)$, QUINDI

$$r_{t-1} = r_{t-3} + r_{t-2}(-q_{t-1}) = auv + bvx + awv + bx(-q_{t-1}) =$$

$$= (-q_{t-1})(avw + bvx)$$

□

MONOIDI E FATTOREIALE

SIA (A, \cdot) UN MONOIDE COMMUTATIVO CANCELLATIVO
ESSO È FATTOREIALE SE VALE UNA TPA:

- $\forall x \in A \setminus W(A)$, x È PRODOTTO DI PRIMI
- $\forall x \in A \setminus W(A)$, x È PRODOTTO DI IRRIDUCIBILI
E OGNI IRRIDUCIBILE È PRIMO
- $\forall x \in A \setminus W(A)$, x È PRODOTTO DI IRRIDUCIBILI
E OGNI FATTOREZZAZIONE È UNICA A MENO
DELL'ORDINE.

STRUTTURE BOOLEANE

ANELLI BOOLEANI, RETTICI, BOOLEGANI E ALGEBRE DI BOOLE SONO TRA LORO EQUIVALENTI.

RETTOBOOL

UN RETTOBOOL È DEGNO BOOLEANO SE È SIA DISTRIBUTIVO CHE COMPLEMENTARIO.

ALGEBRA DI BOOLE

UN'ALGEBRA DI BOOLE È UNA QUADRUPLA $(S, \wedge_p, \vee_p, {}')$ TALE CHE

1) \wedge_p E \vee_p SONO COMMUTATIVE

2) \wedge_p E \vee_p SONO ASSOCIATIVE

3) \wedge_p E \vee_p AMMETTONO NEUTRO
 0 1

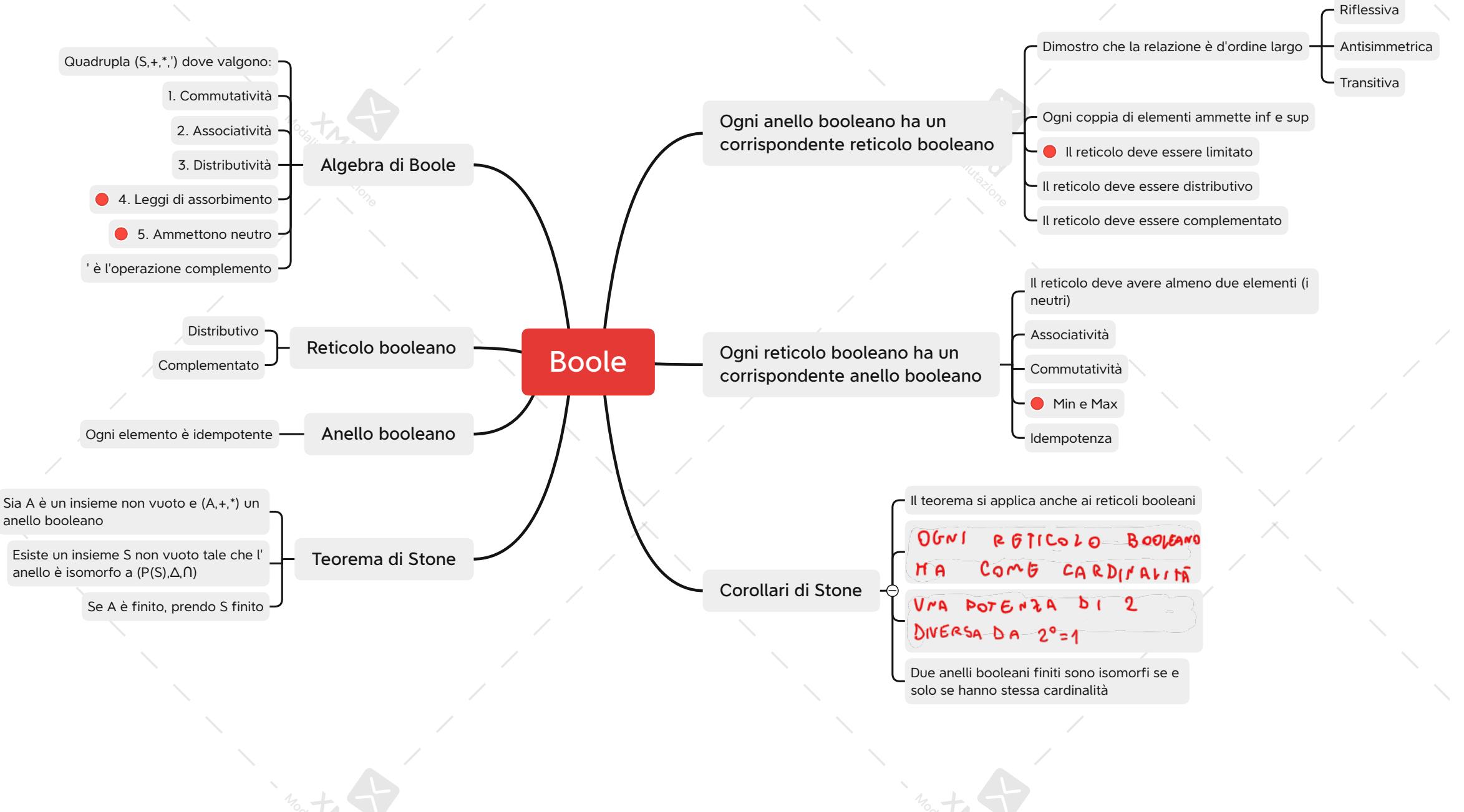
4) VALE LA DISTRIBUTIVITÀ TRA \wedge_p E \vee_p

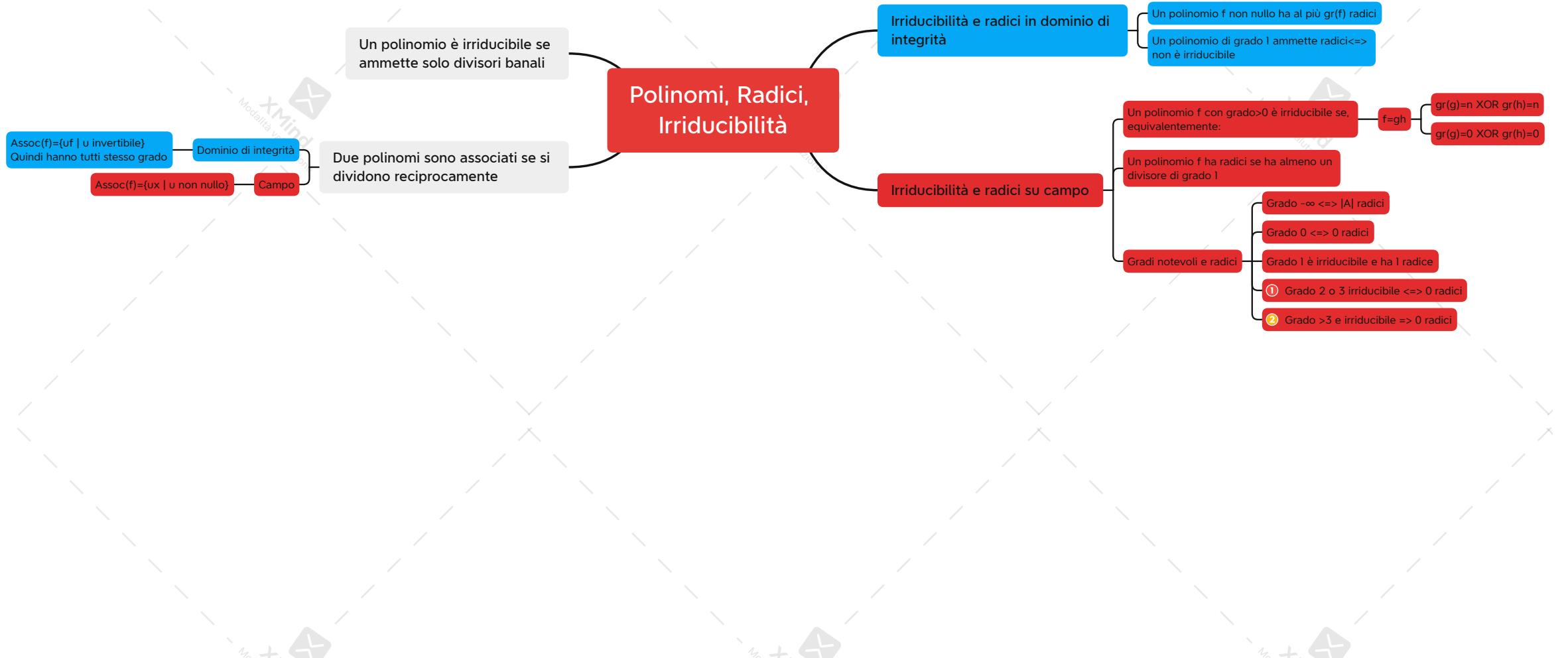
5) VALGONO LE LEGGI DI ASSORBIMENTO

6) $'$ È L'OPERAZIONE DI COMPLEMENTAZIONE

ANELLO BOOLEANO

UN ANELLO È BOOLEANO \Leftrightarrow OGNI ELEMENTO È IDEMPOTENTE





RUFFINI GENERALIZZATO

SIA A UN DOMINIO DI INTEGRITÀ, $f \in A_{\text{Ex}}$,
 $c_1, c_2, \dots, c_m \in A$

$$c_1, c_2, \dots, c_m \underset{\substack{\text{RADICI} \\ \text{DISTINTE}}}{\text{RADICI DISTINTE}} \text{ DI } f \iff \prod_{i=0}^m (x - c_i) \mid f$$

DIM PER INDUZIONE SU m

CASO BASE: $m=1$. VALE RUFFINI SEMPLICE ✓
 SUPPONGO L'ASSERTO VERO PER $m-1 \geq 1$ E DIMOSTRO
 PER m .

PER IPOTESI c_m È RADICE DI f , QUINDI $f(c_m) = 0$.
 PER TH. RESTO $\Rightarrow (x - c_m) \mid f$ PERCHÉ $f(c_m)$ È IL
 RESTO DI $f \setminus (x - c)$
 $f = (x - c_m)q$. PRENDO UN CERTO $c_i : i \in \{1, 2, \dots, m-1\}$

APPLICO OMOMORFISMO DI SOSTITUZIONE, OTTENENDO
 $f(c_i) = (c_i - c_m) q(c_i) = 0$. A È DOMINIO DI
 INTEGRITÀ, QUINDI $c_i - c_m = 0 \vee q(c_i) = 0$.

ESSENDO I c_i TUTTI DISTINTI PER IPOTESI,
 $q(c_i) = 0$. ALLORA PER IP. INDUTTIVA

$$(\exists h \in A_{\text{Ex}}) \left(q = \prod_{i=0}^{m-1} (x - c_i) h \right).$$

Con INDUZIONE SI OTTIENTA LA TESI,

INSIEME BEN ORDINATO

UN INSIEME È BEN ORDINATO SE OGNI SUA PARTE NON VUOTA AMMETTE MINIMO

INSIEME NATURALMENTE ORDINATO

UN INSIEME SI DICE NATURALMENTE ORDINATO SE È BEN ORDINATO E OGNI SUA PARTE NON VUOTA È SUPERIORMENTE LIMITATA AMMETTE MASSIMO

INSIEME LIMITATO

UN INSIEME È LIMITATO SE È SIA:

- INFERIORMENTE LIMITATO, CIOÈ AMMETTE MINORANTI.
- SUPERIORAMENTE LIMITATO, CIOÈ AMMETTE MAGGIORANTI.

INSIEME TOTALMENTE ORDINATO

È UN INSIEME SU CUI È DEFINITA UNA RELAZIONE DI ORDINE TOTALE, CIOÈ DOVE OGNI ELEMENTO

È CONFRONTABILE

BUON ORDINE \Rightarrow ORDINE TOTALE

UN INSIEME È BEN ORDINATO SE OGNI SUA PARTE NON VUOTA AMMETTE MINIMO. SIA ESSO (A, ρ)

$$(\forall x, y \in A) (\exists m \in \{x, y\}) (m = \min \{x, y\}) \Rightarrow$$

$$\Rightarrow m = x \vee m = y \Rightarrow x \rho y \vee y \rho x$$

INSIEME DELLE FUNZIONI DA A IN B
SIANO A, B INSIEMI, INDICHIAMO CON
MAP(A, B) L'INSIEME DELLE FUNZIONI DA A IN B

$$|\text{MAP}(A, B)| = |B|^{|A|}$$

MAP_{in}(A, B) È L'INSIEME DELLE INIETTIVE

$$|\text{MAP}_{in}(A, B)| > 0 \Leftrightarrow |B| \geq |A|$$

$$|\text{MAP}_{in}(A, B)| = \frac{|B|!}{(|B|-|A|)!}$$

MAP_{su}(A, B) È L'INSIEME DELLE SORRIETTIVE

$$|\text{MAP}(A, B)|_{su} \neq 0 \Leftrightarrow |A|=0=|B| \vee 0 < |B| \leq |A|$$

MAP_{bi}(A, B) È QUELLO DELLE BIGETTIVE

$$|\text{MAP}_{bi}(A, B)| \neq 0 \Leftrightarrow |A|=|B|$$

COEFFICIENTE BINOMIALE

$\forall n, k \in \mathbb{N}$

$$\binom{n}{k} = |\mathcal{P}_k(\mathcal{I}_n)|$$

CIOÈ, $\binom{n}{k}$ È IL NUMERO DI PARTI CON k ELEMENTI
DI UN INSERIMENTO DI n ELEMENTI

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

FORMULA RICORSIVA PER IL CALCOLO DI C.BIN.

$$(\forall n, k \in \mathbb{N}) (k \leq n \Rightarrow \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1})$$

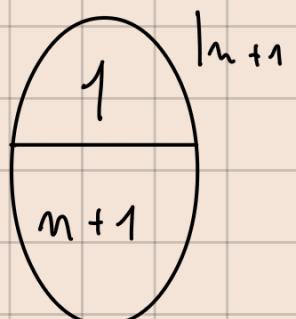
DIM

PRESO \mathcal{I}_{n+1} , DEFINISCO DUE INSIEMI A, B

$$A = \left\{ x \in \mathcal{P}_{k+1}(\mathcal{I}_{n+1}) \mid 1 \notin x \right\}$$

CIOÈ LE $k+1$ PARTI A CUI
1 NON APPARTIENE

$$B = \left\{ y \in \mathcal{P}_{k+1}(\mathcal{I}_{n+1}) \mid 1 \in y \right\}$$



$\{A, B\}$ È PART $(\mathcal{P}_{k+1}(\mathcal{I}_{n+1}))$ ALLORA

$$\binom{n+1}{k+1} = |\mathcal{P}_{k+1}(\mathcal{I}_{n+1})| = |A| + |B| \stackrel{\binom{n}{k+1}}{\hookleftarrow} \stackrel{\binom{n}{k}}{\hookrightarrow} = \binom{n}{k+1} + \binom{n}{k}$$

CDF CANCELLABILE \Rightarrow f CANCELLABILE

DIM

CDF CANCELLABILE \Leftrightarrow CDF Non È DIVISORE
DELL'0
PER LA REGOLA DI ADDIZIONE DEI GRADI

$(\forall g \in A_{\text{fin}}) (\gamma \neq 0 \Rightarrow V(f_g) = Vf + Vg \neq -\infty \Rightarrow$
 $f_g \neq 0) \Rightarrow f$ Non È DV. DELLO 0, QUINDI È
CANCELLABILE

NON INVERTIBILITÀ DI UN POLINOMIO

SE $f \in A_{\text{fin}}$ È CANCELLABILE E $Vf > 0$, f NON
È INVERTIBILE

DIM

PER ASSURDO SIA f CANCELLABILE E $g = f^{-1}$.

PER REGOLA DI ADDIZIONE GRADI

$$V(f_g) = V1 = 0 \Rightarrow Vf = 0, \text{ ASSURDO}$$

NON INVERTIBILITÀ DI X

x NON È MAI INVERTIBILE

DIM

$C\Delta x = 1_A$, L'UNITÀ DELL'ANELLO È

CANCELLABILE \Leftrightarrow non DIV 0. $Vx = 1$, QUINDI x HA

- CD CANCELLABILE \Rightarrow x CANCELLABILE \Rightarrow Non È INVERTIBILE
- GRADO > 0 PER TH. PREC.

