

# APPUNTI ALGEBRA

1 - Composizione di funzioni suriettive è suriettiva

1 - Dimostrazione

Sia  $f: A \rightarrow B$  e  $g: B \rightarrow C$  DUE FUNZIONI SURIETTIVE

PRENDIAMO UN  $y \in C$

SAPPiamo che  $g$  è suriettiva quindi

$$\exists x \in B \mid g(x) = y \quad \leftarrow$$

SAPPiamo che  $x \in B$  e  $f$  è suriettiva quindi

$$\exists k \in A \mid f(k) = x \quad \leftarrow$$

$$ORÀ \quad g(f(k)) = g(x) \quad e \quad g(x) = y$$

$\forall y$  Dunque la composta è suriettiva  $\square$

2 - Composizione di funzioni iniettive è iniettiva

2 - Dimostrazione

Sia  $f: A \rightarrow B$  e  $g: B \rightarrow C$  DUE FUNZIONI INIETTIVE

Siano  $x, y \in A$  in modo che

$$g \circ f(x) = g \circ f(y)$$

MA VUOL DIRE

$$g(f(x)) = g(f(y))$$

$g$  è iniettiva quindi

$$f(x) = f(y)$$

$f$  è iniettiva quindi

$$x = y$$

Dunque la composta è iniettiva  $\square$

3 - La composizione di funzioni biettive è biettiva

3 - Dimostrazione

SEGUÉ DAI PRECEDENTI

4 - Sezione di una funzione

DATI 2 FUNZIONI  $f: A \rightarrow B$  e  $g: B \rightarrow A$

SE  $f \circ g = id_B$ , ALLORA

$g$  SI DICE SEZIONE DI  $f$

5 - Retroazione di una funzione

DATI 2 FUNZIONI  $f: A \rightarrow B$  e  $g: B \rightarrow A$

SE  $g \circ f = id_A$ , ALLORA

$g$  SI DICE RETROAZIONE DI  $f$

6 - Caratterizzazione di Iniettività tramite Retroazione

UNA FUNZIONE È INIETTIVA  $\Leftrightarrow$  IL DOMINIO È VUOTO

o ESISTE UNA SUA RETROAZIONE

6 - Dimostrazione

$\Leftarrow$ : SE  $A = \emptyset$  INIETTIVITÀ BANALE POI

SE  $(\exists g: B \rightarrow A)(g \circ f = id_A)$  MA ESSENDO  
 $id_A$  INIETTIVA,  $f$  INIETTIVA

→ IL NOSTRO OBIETTIVO È TROVARE LA RETROAZIONE  $g$ .

DEFINIAMO  $g: Y \in B \rightarrow \begin{cases} x_y & \text{SE } y \in \text{Im } f \\ \bar{x} & \text{SE } y \notin \text{Im } f \end{cases}$

QUESTA È UNA RETROAZIONE PERCHÉ

$$g \circ f(x) = g(f(x)) = g(y) = x_y$$

MA  $f(x_y) = f(x) \rightarrow x_y = x$  PER INIEZIONE

DI  $f$ , DUNQUE  $g$  RETROAZIONE

□

## 7 - Caratterizzazione di Suriettività tramite Sezione

UNA FUNZIONE È SURIETTIVA  $\iff$  ESISTE UNA SUA SEZIONE

### 7 - Dimostrazione

$\leftarrow$ : SE  $(\exists g: B \rightarrow A)(f \circ g = id_B)$  MA ESSENDO  
 $id_B$  SURIETTIVA,  $f$  SURIETTIVA

→: SAPPIAMO CHE SE  $f$  È SURIETTIVA ALLORA

$\forall y \in B (\overleftarrow{f\{y\}} \neq \emptyset)$  OVVERO CHE ESISTE SEMPRE  
UN ELEMENTO DELLA CONTROIMMAGINE

PRENDIAMO LA FUNZIONE  $g$  COSÌ DEFINITA

$g: Y \in B \rightarrow (x \in \overleftarrow{f\{y\}}) \in A$  CHE È UNA SEZIONE

PERCHÉ

$$f \circ g(y) = f(g(y)) = f(x) = y$$

□

## 8 - Unicità dell'inversa

Se  $f$  ha una sezione  $s$  è una retroazione  $\pi$   
allora  $s = \pi$  ed essa è l'unica inversa

## 8 - Dimostrazione

$$\begin{aligned} \pi \circ f &= id_A \\ f \circ s &= id_B \end{aligned} \quad \text{ALLORA} \quad \begin{aligned} (\pi \circ f) \circ s &= id_A \circ s = s \\ \pi \circ (f \circ s) &= \pi \circ id_B = \pi \end{aligned}$$

ESSENDO LA COMPOSTA ASSOCIATIVA ABBIAMO

$$\underbrace{(\pi \circ f) \circ s}_{s} = \underbrace{\pi(f \circ s)}_{\pi}$$

## 9 - Invertibilità implica cancellabilità

DATA UNA STRUTTURA  $(S, \cdot)$  ALLORA

$$\forall x \in S \quad (x \text{ È INVERTIBILE} \rightarrow x \text{ CANCELLABILE})$$

## 9 - Dimostrazione

$x$  È INVERTIBILE

$$\text{LA CANCELLAGILITÀ DICE } \forall y, z \quad (x \cdot y = x \cdot z \rightarrow y = z)$$

ESSENDO  $x$  INVERTIBILE PUÒ ESSERE IN OPERAZIONE CON IL  
SUO INVERSO  $\bar{x}$

$$((x \cdot \bar{x}) \cdot y = (x \cdot \bar{x}) \cdot z \rightarrow y = z) = (\varepsilon \cdot y = \varepsilon \cdot z \rightarrow y = z)$$

## 10 - Omomorfismo fra strutture algebriche

SIANO  $(A, *)$  E  $(B, \square)$  2 STRUTTURE ALGEBRICHE

ALLORA  $f : A \rightarrow B$  È UN OMOMORFISMO  $\Leftrightarrow \forall x, y \in S (f(x * y) = f(x) \square f(y))$

## 11 - Isomorfismo fra strutture algebriche

L'ISOMORFISMO È UN OMOMORFISMO BIETTIVO (DA  $A \rightarrow B$  E  $B \rightarrow A$ )

## 12 - L'inverso di un Isomorfismo è un Isomorfismo

SIA  $(A, *)$  E  $(B, \square)$  2 STRUTTURE ALGEBRICHE

SE  $f : A \rightarrow B$  È UN ISOMORFISMO ALLORA  $f^{-1} : B \rightarrow A$   
È A SUA VOLTA UN ISOMORFISMO

## 12 - Dimostrazione

DATO CHE LA FUNZIONE È BIETTIVA, BASTA DEMONSTRARE CHE L'INVERSA È UN OMOMORFISMO.

SIA  $x, y \in B$ . ESSENDO  $f \circ f^{-1} = id_B \rightarrow$  (NEUTRO) ALLORA

OBIETTIVO

$f^{-1}(x \square y) = f^{-1}(x) * f^{-1}(y)$  MA COME CI ARRIVIAMO?

PROCEDIMENTO

$$f^{-1}(x \square y) = f^{-1}\left(f\left(f^{-1}(x)\right) \square f\left(f^{-1}(y)\right)\right)$$

$$f^{-1}\left(f\left(\underset{\parallel}{f^{-1}(x)} * \underset{\parallel}{f^{-1}(y)}\right)\right)$$

$$f^{-1}(x) * f^{-1}(y)$$

## BONUS 1 (Domanda iniziale) - Applicazione o funzione

SIA  $f = (\alpha \times b, g)$  con  $g \subseteq \alpha \times b$ , si verifica che

$$\forall x \in \alpha \quad (\exists ! y \in b \mid x \in f y)$$

Ovvvero per ogni elemento di  $\alpha$  esiste uno ed un solo elemento di  $b$  con cui è in corrispondenza, allora diciamo che  $f$  è un'applicazione o funzione

$$f : \alpha \rightarrow b$$

- $\alpha$  si dice **dominio**
- $b$  si dice **codominio**
- se  $x \in f y$ , scriveremo  $g(x) = y$ ,  $y$  immagine di  $x$

L'insieme di tutte le immagini  $Im(f) := \{y \in b \mid (\exists x \in \alpha)(g(x) = y)\}$   
si definisce **immagine della funzione**. Si può scrivere anche  
 $Im(f) := \{g(x) \mid x \in \alpha\}$

Dato un insieme  $s \subseteq \alpha$ , allora definiamo  $f(s) = \{y \in b \mid (\exists x \in s)(g(x) = y)\}$   
cioè l'insieme di tutte le immagini degli elementi di  $s$ .

Equivalentemente, se  $s \subseteq b$ , definiamo l'**antimmagine** o **componimagine** di  $s$  l'insieme di tutti gli elementi di  $\alpha$  che hanno immagine in  $s$

$$f^{-1}(s) = \{x \in \alpha \mid g(x) \in s\}$$

Possiamo definire una funzione attraverso una sua descrizione esplicita che ne definisce dominio, codominio, e la legge che lega gli elementi.

ESEMPIO:  $f : m \in \mathbb{N} \rightarrow (m+1) \in \mathbb{N}$

Un'applicazione è ben posta o ben definita per sottolineare che essa è effettivamente un'applicazione e non solo una corrispondenza.

## BONUS 2 (Domanda iniziale) - Applicazioni particolari

LA FUNZIONE  $\text{Id}_\alpha : x \in \alpha \rightarrow x \in \alpha$ , ELOE' LA FUNZIONE CHE ASSOCIA AD OGNI VALORE DI  $\alpha$  SE' STESSO, SI DICE FUNZIONE IDENTITÀ.

DATA  $f : x \in \alpha \rightarrow f(x) \in b$ ,  $\in S \subseteq \alpha$ , LA FUNZIONE

$$f|_S : x \in S \rightarrow f(x) \in b$$

SI DICE RESTRIZIONE DELLA FUNZIONE  $f$  AD  $S$ .

SE  $\alpha \subseteq h$ , UNA FUNZIONE  $g : h \rightarrow e$  SI DICE PROLUNGAMENTO

DI  $f$  SE  $g|_\alpha = f$  ELOE' SE  $f$  E' UNA RESTRIZIONE DI  $g$ .

SE  $S \subseteq b \wedge \text{Im}(f) \subseteq S$ , LA FUNZIONE  $p : x \in \alpha \rightarrow f(x) \in S$  SI DICE RIDOTTA  
DI  $f$  AD  $S$

PER OGNI  $f : \alpha \rightarrow b$  DEFINIAMO LE FUNZIONI:

$$\overrightarrow{f} : x \in P(\alpha) \rightarrow \{f(z) \mid z \in x\} \in P(b)$$

$$\overleftarrow{f} : y \in P(b) \rightarrow \{z \in \alpha \mid f(z) \in y\} \in P(\alpha)$$

ELOE' LE FUNZIONI IMMAGINE ED ANTIMMAGINE CHE, RISPECTIVAMENTE,  
ASSOCIANO AD OGNI SOTTOINSIEME DEL DOMINIO LA SUA IMMAGINE, E  
AD OGNI SOTTOINSIEME DEL CODOMINIO LA SUA ANTIMMAGINE.

### 13 - Legge di annullamento del prodotto

DATO UN ANELLO  $(A, +, \cdot)$  DIREMO CHE VALE LA LEGGE DI ANNULLAMENTO DEL PRODOTTO  $\Leftrightarrow \forall x, y (x \cdot y = 0_A \rightarrow (x = 0_A \vee y = 0_A))$

### 14 - Anello integro

UN ANELLO INTEGRO È UN ANELLO DOVE VALE LA LEGGE DI ANNULLAMENTO DEL PRODOTTO

### 15 - Dominio di integrità

UN ANELLO UNITARIO (ovvero con neutro  $1_A$ ) INTEGRO SI DICE DOMINIO DI INTEGRITÀ

### 16 - Divisore dello zero

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

$x \in A \setminus \{0_A\}$  È DIVISORE DELLO ZERO  $\Leftrightarrow (\exists y \in A \setminus \{0_A\}) (x \cdot y = 0_A)$

### 17 - I divisori dello zero sono non cancellabili

$x \in A$  DIVISORE DELLO ZERO  $\Leftrightarrow x$  NON E CANCELLABILE

### 17 - Dimostrazione

$\rightarrow$  SAPPIAMO CHE  $x \in A$  DIVISORE DELLO ZERO, QUINDI

$(\exists y \in A \setminus \{0_A\}) (x \cdot y = 0_A)$ . PER ASSURDO SE  $x$  FOSSE CANCELLABILE  
 $x \cdot y = x \cdot 0_A \rightarrow y = 0_A$

ASSURDO IN QUANTO IL DIV O DICE  $y \notin \{0_A\}$

$\leftarrow$  PER I POTESI (DI NON CANCELLABILITÀ)

$\exists y, z \in A (xy = xz \wedge y \neq z)$  QUINDI  $xy - xz = 0 \wedge y \neq z$

CANCELLABILITÀ

$$x(y - z) = 0$$



MA  $y \neq z$

QUINDI  $x$  DIVISORE DELLO 0

SICCOME  $y - z \neq 0$  e  $x(y - z) = 0$

□

ESEMPIO

$3$  NON CANCELLABILE

$\exists y, z \in A (\exists y: 3z \wedge y \neq z)$

$$3(y - z) = 0$$

$3$  DIV ZERO

## 18 - Anelli commutativi unitari e domini di Integrità

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

$(A, +, \cdot)$  DOMINIO DI INTEGRITÀ  $\iff (A, +, \cdot)$  PRIMO DI DIVISORI DELLO ZERO

## 18 - Dimostrazione

$\rightarrow$   $(A, +, \cdot)$  DOMINIO DI INTEGRITÀ, QUINDI VALE LA LEGGE

DI ANNULLAMENTO DEL PRODOTTO CHE VA CONTRO L'IPOTESI

di avere divisori dello zero

$\leftarrow$  SE NESSUN ELEMENTO È DIVISORE DELLO ZERO

ALLORA TUTTI GLI ELEMENTI SONO CANCELLABILI.

CONSIDERIAMO  $\forall x, y \in A (x \neq 0 \wedge xy = 0 \rightarrow y = 0)$  CHE È LA TESI

□

19 - Corpo

$(A, +, \cdot)$  si dice CORPO se  $(A - \{0\}, \cdot)$  è un GRUPPO.

20 - Campo

UN CORPO COMMUTATIVO SI DICE CAMPO

21 - Ogni Campo è Dominio di Integrità

21 - Dimostrazione

CAMPO È UN CORPO COMMUTATIVO.

OBETTIVO

IL CORPO È UN ANELLO UNITARIO.



ANELLO UNITARIO È DOMINIO DI INTEGRITÀ SE È PRIVO DI DIVISORI DELLO ZERO

OGNI ELEMENTO DI UN CAMPO ECETO LO ZERO È INVERTIBILE, DUNQUE CANCELLABILE.

UN ELEMENTO CANCELLABILE NON È DIVISORE DELLO ZERO

QUINDI NON ESISTONO DIVISORI DELLO ZERO.

DUNQUE UN CAMPO È DOMINIO DI INTEGRITÀ

## 22 - Relazione d'ordine largo

UNA RELAZIONE D'ORDINE LARGO E' RIFLESSIVA, ANTISIMMETRICA, TRANSITIVA

## 23 - Relazione d'ordine stretto

UNA RELAZIONE D'ORDINE STRETTO E' ANTIRIFLESSIVA, ANTISIMMETRICA, TRANSITIVA

## 24 - Relazione duale

DATA UNA RELAZIONE BINARIA  $\sigma$  SU UN INSIEME  $A$  DEFINIAMO

$$\bar{\sigma} : \forall x, y \in A \quad (x \bar{\sigma} y \leftrightarrow y \sigma x)$$

## 25 - Congruenza di Modulo m

DATO  $m \in \mathbb{Z}$  UNA CONGRUENZA MODULO m E'

$$\equiv_m = (\mathbb{Z} \times \mathbb{Z}, \circ_g) \text{ TALE CHE}$$

$$\forall a, b ((a, b) \in g \leftrightarrow \exists k \in \mathbb{Z} (a - b = km))$$

(LA CONGRUENZA E' UN EQUIVALENZA)

## 26 - Nucleo di equivalenza

DATA UNA  $f: A \rightarrow B$  DEFINIAMO LA RELAZIONE NUCLEO DI EQUIVALENZA :

$$Ker_f := (A \times A, \circ_g)$$

$$\forall x, y \in A ((x, y) \in g \leftrightarrow f(x) = f(y))$$

## 27 - Classe di Equivalenza

SIA  $\sigma$  UNA RELAZIONE D'EQUIVALENZA SU  $S$  E  $x \in S$  DEFINIAMO

$$[x]_\sigma = \{y \in S \mid x \sigma y\}$$

SI CHIAMA CLASSE DI EQUIVALENZA DI  $x$  DI MODOLO  $\sigma$   
E  $x$  SI CHIAMA RAPPRESENTANTE DELLA CLASSE DI RESTO

## 28 - Classe di Resto

LE CLASSI DI EQUIVALENZA DI UNA CONGRUENZA SI DICONO  
CLASSI DI RESTO.

## 29 - Insieme quoziente

DATO UN INSIEME  $S$  ED UNA RELAZIONE D'EQUIVALENZA  $\sigma$   
L'INSIEME QUOTIENTE È

$$S/\sigma = \{[x]_\sigma \mid x \in S\}$$

### 30 - Proprietà fondamentali delle classi di equivalenza

SIA  $A$  UN INSIEME,  $\mathcal{Q}$  UNA RELAZIONE D'EQUIVALENZA DEFINITA SU  $A$  E SIANO  $a \sim b \in A$ . ALLORA

- 1)  $[a]_q \neq \emptyset$
- 2)  $[a]_q \neq [b]_q \Leftrightarrow [a]_q \cap [b]_q = \emptyset$
- 3)  $\bigcup [a] \in A = A$

30 - Dimostrazione (1) ( $[a]_q \neq \emptyset$ )

$\mathcal{Q}$  È DI EQUIVALENZA  $\rightarrow \mathcal{Q}$  È RIFLESSIVA  $\rightarrow \forall a \in A (a \sim a) \rightarrow \forall a \in A ([a]_q \neq \emptyset)$

30 - Dimostrazione (2) ( $[a]_q \neq [b]_q \Leftrightarrow [a]_q \cap [b]_q = \emptyset$ )

SUPPONIAMO PER ASSURDO L'INTERSEZIONE SIA NON VUOTA.

$[a]_q \cap [b]_q \neq \emptyset \rightarrow \exists z (z \in [a]_q \wedge z \in [b]_q) \rightarrow a \sim z \wedge z \sim b \rightarrow a \sim b$

QUESTO È UN ASSURDO SICCOME  $a \sim b$  VUOL DIRÉ CHE

$$[a]_q = [b]_q$$

MA LA SECONDA PROPRIETÀ DICE

$$[a]_q \neq [b]_q \Leftrightarrow [a]_q \cap [b]_q = \emptyset$$

30 - Dimostrazione (3) ( $\bigcup [a] \in A = A$ )

PER DIMOSTRARE L'UOGUALIANZA BISOGNA DIMOSTRARE LA DOPPIA INCLUSIONE

$\bigcup [a]_q \subseteq A$  QUINDI SE  $x \in \bigcup [a]_q \rightarrow x \in [a]_q \rightarrow x \in A$

$\bigcup [a]_q \supseteq A$  QUINDI SE  $x \in A \rightarrow x \in [x]_q \rightarrow x \in \bigcup [a]_q$

ALLORA  $\bigcup [a] \in A = A$

### 31 - Proiezione canonica

SIA  $A$  UN INSIEME E  $\sigma$  UNA RELAZIONE D'EQUIVALENZA SU  $A$   
ALLORA

$$\pi: x \in A \rightarrow [x]_\sigma \in A/\sigma$$

PI SI CHIAMA PROIEZIONE CANONICA

### 32 - Proiezione canonica è suriettiva

#### 32 - Dimostrazione

SICCOME OGNI CLASSE DI EQUIVALENZA NON È VUOTA ALLORA  
È SUBETTIVA.

### 33 - Partizioni

DATO UN INSIEME  $A$  UN INSIEME  $f$  SI DICE PARTIZIONE  
DI  $A$  SE:

$$1 - \forall x \in f (x \neq \emptyset)$$

$$2 - \forall x, y \in f (x \neq y \Rightarrow x \cap y = \emptyset)$$

$$3 - \bigcup_f = A$$

### 34 - Teorema fondamentale su relazioni d'equivalenza e partizioni

SIA  $A$  UN INSIEME NON VUOTO, ALLORA

1) SE  $\mathcal{E}$  E' UNA REL. DI EQUIVALENZA DEFINITA SU  $A$ , ALLORA L'INSIEME QUOTIENTE  $\frac{A}{\mathcal{E}}$  E' UNA PARTIZIONE DI  $A$

2) SE  $F$  E' UNA PARTIZIONE DI  $A$ , ALLORA

$$\mathcal{Q}_F = \forall x, y \in A \quad x \mathcal{Q}_F y \iff \exists k \in F \mid \{x, y\} \subseteq k$$

E' UNA REL. DI EQUIVALENZA IN  $A$  E RISULTA

$$\frac{A}{\mathcal{Q}_F} = F$$

#### 34 - Dimostrazione (1)

$\frac{A}{\mathcal{E}} = \left\{ [a]_{\mathcal{E}} \mid a \in A \right\}$  E' UNA PARTIZIONE  $\iff$

1)  $\forall [a] \in \frac{A}{\mathcal{E}} \quad ([a] \neq \emptyset)$  PER LE PROPRIETÀ DELLE CLASSI

2)  $\forall [a], [b] \in \frac{A}{\mathcal{E}} \quad ([a] \neq [b] \rightarrow [a] \cap [b] = \emptyset)$  PROPRIETÀ CLASSI

3)  $\bigcup_{a \in A} [a] = A$  PROPRIETÀ CLASSI

#### 34 - Dimostrazione (2)

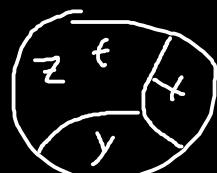
$$\mathcal{Q}_F: \forall x, y \in A, \quad x \mathcal{Q}_F y \iff \exists k \in F \mid \{x, y\} \subseteq k$$

TESI:

•  $\mathcal{Q}_F$  È DI EQUIV.

$$\frac{A}{\mathcal{Q}_F} = F$$

$$F = \{\{x\}, \{y\}, \{z, t\}\}$$



$$\mathcal{Q}_F = \{(x, x), (y, y), (z, z), (t, t), (z, t), (t, z)\}$$

$F$  È RIFLESSIVA, SIMMETRICA, TRANSITIVA, DUNQUE DI EQUIVALENZA

$$\frac{A}{\mathcal{Q}_F} = \{[x], [y], [z], [t]\} = \{\{x\}, \{y\}, \{z, t\}\} = F$$

### 35 - 1^ Tesi del Teorema fondamentale dell'aritmetica (TFA)

Ogni numero intero  $\in \mathbb{Z} \setminus \{0, 1\}$  o è primo oppure si può scrivere in modo unico (a meno dell'ordine) come prodotto di primi.

#### 35 - Dimostrazione

$P(m) = \forall m \in \mathbb{N} \setminus \{0, 1\}, m$  o è primo o è prodotto di primi

DIMOSTRIAMO CON IL PRINCIPIO DI INDUZIONE DI 2<sup>a</sup> FORMA

**BASE INDUTTIVA**  $m_0 = 2 \rightarrow P(2)$  vera perché 2 primo

**PASSO**  $\forall m > 2 (\forall h (2 \leq h < m \wedge P(h)) \rightarrow P(m))$

Sia  $m > 2$ .  $\forall h | 2 \leq h < m (P(h)$  è vera) Si distinguono 2 casi:

•  $m$  è primo  $\rightarrow P(m)$  vera

•  $m$  non è primo  $\rightarrow m$  ammette almeno un divisore non banale  $m_1 \in \mathbb{N}$

$m_1 \in \mathbb{N} (1 < m_1 < m)$

$m_1 | m \Leftrightarrow \exists x \in \mathbb{N} (m = m_1 \cdot x)$

Se  $x = 1 \rightarrow m = m_1$  ASSURDO! ( $m$  non banale)

Se  $x > 1 \rightarrow m = m_1 \cdot x \rightarrow m_1 > 1$  ASSURDO! ( $1 < m_1$ )

$1 < m_1, x < m \Leftrightarrow 2 \leq m_1, x < m$

$$\left. \begin{array}{l} 2 \leq m_1 < m \\ 2 \leq x < m \end{array} \right\}$$

$P(m_1) : m_1 = p_1 \cdot p_2 \cdot p_3 \dots p_k (k \geq 1)$

$P(x) : x = q_1 \cdot q_2 \cdot q_3 \dots q_h (h \geq 1)$

ORA PARLIAMO DEI NEGATIVI

Sia  $m \in \mathbb{N} \setminus \mathbb{Z}$  ORA  $-m \in \mathbb{N}$ .

ORA PER  $-m$  VALE LA TESI

QUINDI  $m = -(p_1) \cdot -(p_2) \cdot -(p_3) \dots$

MA UN NUMERO PRIMO RIMANE PRIMO

AUHE SE DIVENTA NEGATIVO.

36 - 2<sup>a</sup> Tesi del Teorema fondamentale dell'aritmetica (TFA)

Se  $m = q_1 \cdot \dots \cdot q_n$  ALLORA  $x = s \quad \exists f: \{1, \dots, n\} \rightarrow \{1, \dots, s\}$

BIETTIVA TALE CHE E' POSSIBILE  $(\forall i \in 1..n) (p_i = q_{f(i)})$

### 36 - Dimostrazione

DIMOSTRIAMO CON IL PRINCIPIO DI INDUZIONE DI 1° FORMA

**BASE INDUTTIVA**  $n=1$  VUOL DIRE CHE  $p_1 = m = q_1$

E  $n=s=1$  E  $p_1 = q_1$

**PASSO** IPOTIZZIAMO CHE LA TESI VALGA PER  $n-1$

DUNQUE VOGLIAMO DEMOSTRARE CHE VALGA PER  $n$

SAPPIAMO CHE:

$$p_1 \cdot p_2 \cdot \dots \cdot p_n = m = q_1 \cdot q_2 \cdot \dots \cdot q_s$$

POSSIAMO DIRE

$$p_1 \mid q_1 \cdot q_2 \cdot \dots \cdot q_s$$

MEGLIO ALLORA

$$p_1 \mid q_1 \vee p_1 \mid q_2 \vee p_1 \mid q_3 \dots \vee p_1 \mid q_s$$

SENZA PERDRE LA GENERALITÀ DIREMO:

$$p_1 \mid q_1$$

(OVVERO IMPOSTO  $q_1$  LA Q CHE VIENE DIVISA DA  $p_1$ )

ESSENDO  $q_1$  PRIMO DIREMO

$$p_1 \mid \pm q_1$$

AVREMO QUINDI

$$\cancel{p_1 \cdot p_2 \cdot \dots \cdot p_n = m = (\pm p_1) \cdot q_2 \cdot \dots \cdot q_s}$$

CANCELLANDO  $p_1$  AD ENTRAMBI I MEMBRI AVREMO

$$p_2 \cdot \dots \cdot p_n = m = (\pm p_2) \cdot q_2 \cdot \dots \cdot q_s$$

SIAMO ARRIVATI NEL CASO  $n=1$  E QUINDI VALE LA  
TESI INDUTTIVA  $\square$

37 - Elementi confrontabili

DATO UN INSIEME ORDINATO  $(S, P)$  DUE ELEMENTI  
 $X, Y \in S$  SI DICONO CONFRONTABILI  $\Leftrightarrow XPy \vee YPx$

38 - Insieme ben ordinato

UN INSIEME ORDINATO  $(S, P)$  È BEN ORDINATO  
SE OGNI SUO SOTTINSIEME NON VUOTO È DOTATO  
DI MINIMO

39 - Minimo e Massimo se esistono sono unici

39 - Dimostrazione

LA DEMOSTRAZIONE È PER IL MINIMO MA VALE SIMILARE  
PER IL MASSIMO

PER ASSURDO  $m_1, m_2$  MINIMI DI  $S$ .

ALLORA

$\forall x \in S (m_1 Px \wedge m_2 Px) \rightarrow m_1 Pm_2 \wedge m_2 Pm_1$

PER ASIMMETRIA  $m_1 = m_2 \quad \square$

## 40 - Buon ordine implica ordine totale

### 40 - Dimostrazione

$$\forall x, y \in S \quad (\exists m \mid m = \min \{x, y\}) \rightarrow_{m=x \vee m=y} x p y \vee y p x$$

## 41 - Relazione di copertura

DATO UN INSIEME ORDINATO  $(S, P)$  E DUE ELEMENTI  $x, y \in S$ .

$$y \text{ COPRE } x \leftrightarrow (x p y) \wedge (\forall z \in S)(z \neq x \wedge z \neq y \wedge x p z \wedge z p x)$$

CIOÉ NON VI SONO ELEMENTI TRA  $y \in x$

## 42 - Diagramma di Hasse

DATO UN INSIEME ORDINATO  $(S, P)$  DEFINIAMO IL DIAGRAMMA DI HASSE LA COPIA  $(S \times S, \preceq)$  TALE CHE

$$\forall x, y \in S \quad ((x, y) \in \preceq \leftrightarrow y \text{ COPRE } x)$$

## 43 - Massimo,minimo,massimale,minimale,maggiorante,minorante

Sia  $(S, P)$  UN INSIEME ORDINATO

$$m \text{ È MINIMO} \leftrightarrow \forall x \in S (m p x)$$

$$M \text{ È MASSIMO} \leftrightarrow \forall x \in S (x p M)$$

$$m \text{ È MINIMALE} \leftrightarrow \forall x \in S (m p x \vee x p m \rightarrow m p x) \\ \text{(PER OGNI ELEMENTO)} \\ \text{CHE È COMPARABILE}$$

$$M \text{ È MASSIMALE} \leftrightarrow \forall x \in S (m p x \vee x p m \rightarrow x p M) \\ \text{(PER OGNI ELEMENTO)} \\ \text{CHE È COMPARABILE}$$

Sia  $(S, P)$  UN INSIEME ORDINATO E  $T \subseteq S$  ALLORA :

$$m \in S \text{ È MINORANTE} \leftrightarrow \forall x \in T (m p x)$$

$$M \in S \text{ È MAGGIORANTE} \leftrightarrow \forall x \in T (x p M)$$

#### 44 - Insieme limitato

Sia  $(S, P)$  un insieme ordinato e  $t \in S$  allora :

$t$  è limitato inferiormente  $\Leftrightarrow \text{MINOR}_{(S, P)}(t) \neq \emptyset$

$t$  è limitato superiormente  $\Leftrightarrow \text{MAJJOR}_{(S, P)}(t) \neq \emptyset$

Cioè se è dotato di minore o maggiore

#### 45 - Insieme naturalmente ordinato

$(S, P)$  è naturalmente ordinato  $\Leftrightarrow$  È BEN ORDINATO E OGNI SUA PARTE NON VUOTA SUPERIORMENTE LIMITATA HA MASSIMO

#### 46 - Buon ordine implica Ordine largo

#### 46 - Dimostrazione

Sia  $(S, P)$  un insieme ben ordinato allora:

$\forall x \in S \left( \{x\} \text{ HA MINIMO} \rightarrow x \in x \right)$

#### 47 - Principio di induzione 1^ forma

Sia  $X \subseteq N \setminus \{0\}$   $N_{\min(x)} = \{m \in N \mid m \geq \min(x)\}$

ESEMPIO:

$$X = \{7, 9, 12\} \quad N_{\min(X)} = \{m \in N \mid m \geq 7\} \\ \{7, 8, 9, \dots\}$$

ORA INTRODUCEREMO IL PRINCIPIO DI INDUZIONE

$\forall x \in P(N) \setminus \{\emptyset\} \left( \forall m \in N \left( m \in x \rightarrow m+1 \in x \right) \right) \rightarrow (x = N_{\min(x)})$

## 47 - Dimostrazione

IPOTEZI ZIANO PER ASSURDO CHE  $X \neq N_{\min(x)}$

PONIAMO

$$m = \min(x)$$

QUINDI SE FACCIA NO  $N_m \setminus X \neq \emptyset$

PONIAMO  $Y = N_m \setminus X \neq \emptyset$

ORA PONIAMO  $m = \min(Y)$  (ESISTE PERCHÉ  $Y \subseteq N$ )

SAPPIAMO  $m < m$  PERCHÉ  $Y = N_{\min(x)} \setminus X$

ALLORA  $m \leq m-1 < m \rightarrow (m-1) \in Y$

PER IPOTESI  $(m-1)+1 \in X \rightarrow m \in X$  ASSURDO!

□

## 48 - Principio di induzione 2^ forma

$\forall x \in \mathcal{P}(\mathbb{N}) - \{\emptyset\} (\forall m \in \mathbb{N}) (\forall k \in \mathbb{N}) (\min(x) \leq k < m \rightarrow k \in x) \rightarrow m \in x \Rightarrow x = N_{\min(x)}$

## 48 - Dimostrazione

IPOTEZI ZIANO PER ASSURDO CHE  $X \neq N_{\min(x)}$

PONIAMO

$$m = \min(x)$$

$Y = N_m \setminus X \neq \emptyset$

ORA PONIAMO

$$n = \min(Y)$$

ALLORA  $\forall k \in \mathbb{N} (m \leq k < n) \rightarrow k \in Y$

ALLORA  $n \in X$  ASSURDO!

## 49 - Teorema fondamentale di Omomorfismo per insiemi

SIA  $f: A \rightarrow B$  UN'APPLICAZIONE

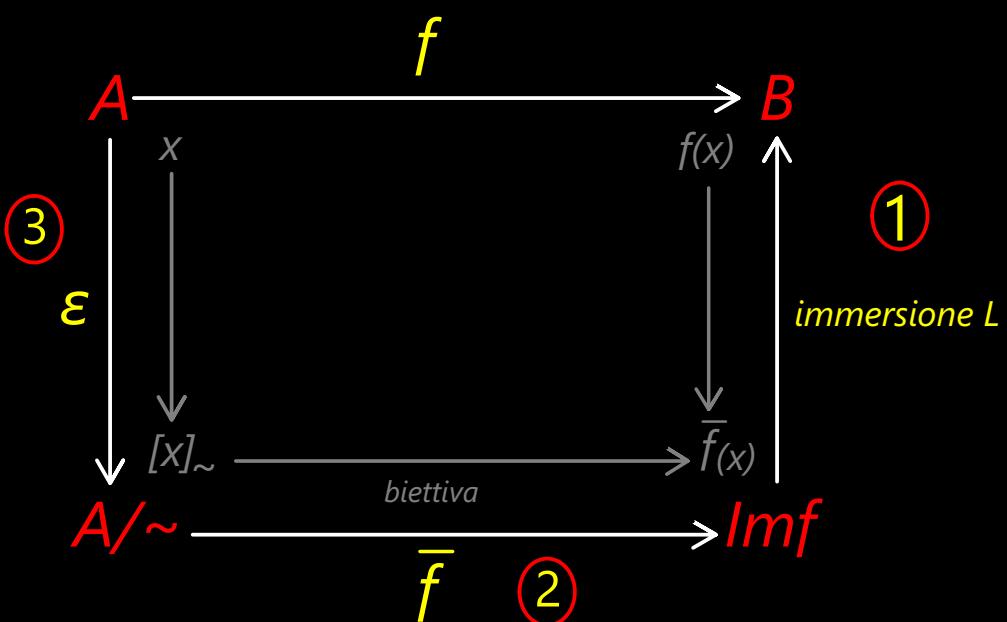
SIA  $\sim$  IL NUCLEO DI EQUIVALENZA

1)  $\exists \bar{f}: [x] \in A/\sim \rightarrow f(x) \in \text{Im } f$  (UN APPLICAZIONE) E' BIETTIVA

2) SE  $\varepsilon: A \rightarrow A/\sim$  (PROIEZIONE CANONICA  $x \rightarrow [x]$ ) E'

SE  $L$  E' UN IMMERSIONE ( $\text{Im } f \subseteq B$ ) ALLORA

$$\bar{f} = L \circ \bar{f} \circ \varepsilon$$

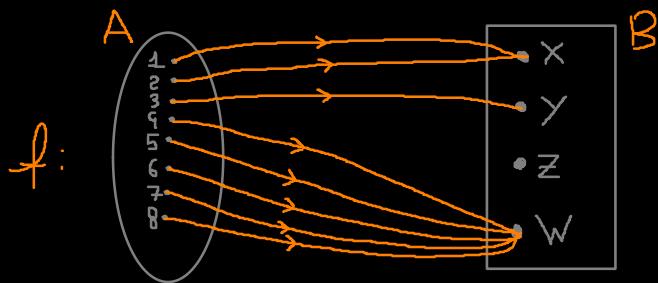


TEOREMA FONDAMENTALE  
OMOMORFISMO PER INSIEMI

ESEMPIO: SIA  $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ ,  $B = \{x, y, z, w\}$

SIA  $f: A \rightarrow B$  UN'APPLICAZIONE

SIA  $\sim$  IL NUCLEO DI  $f$



QUANTE SONO LE CLASSI DI EQUIVALENZA?  $|A/\sim| = ?$

SAPPIAMO CHE  $A/\sim = \{\overleftarrow{f}(\{x\}), \overleftarrow{f}(\{y\}), \overleftarrow{f}(\{z\}), \overleftarrow{f}(\{w\})\}$

$A/\sim = \{\{1, 2\}, \{3\}, \emptyset, \{4, 5, 6, 7, 8\}\}$

$|A/\sim| = 3$

#### 49 - Dimostrazione

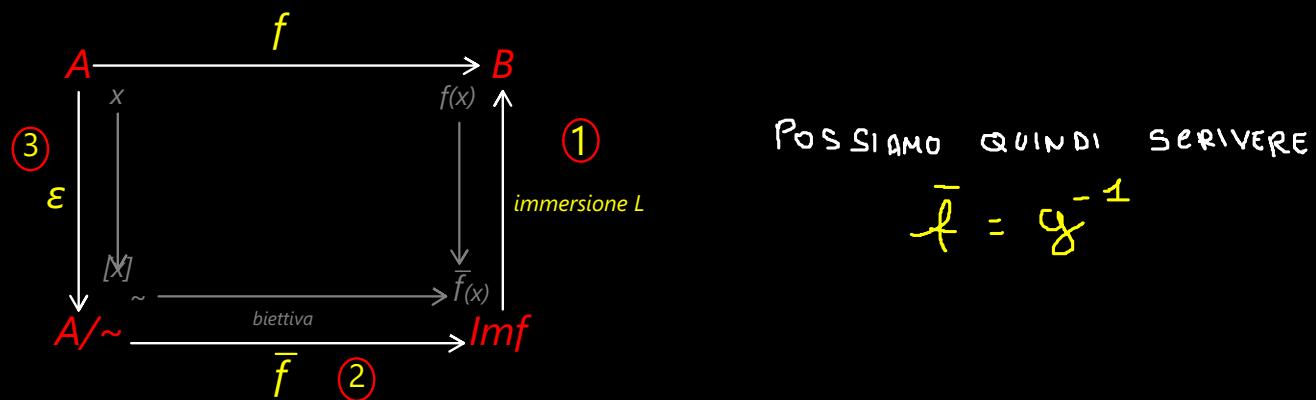
$\exists g : b \in \text{Im } f \rightarrow \overset{\leftarrow}{f}(\{b\}) \in A/\sim \quad (g \in \text{BIETTIVA})$

$\forall b, e \in \text{Im } f \quad g(b) = g(e) \iff \overset{\leftarrow}{f}(\{b\}) = \overset{\leftarrow}{f}(\{e\})$   
 $b \in \text{Im } f \quad \text{QUINDI} \quad \overset{\leftarrow}{f}(\{b\}) \neq \emptyset$

PRENDIAMO  $x \in \overset{\leftarrow}{f}(\{b\})$ , ALLORA  $f(x) = b$

PRENDIAMO  $x \in \overset{\leftarrow}{f}(\{e\})$ , ALLORA  $f(x) = e$   
 QUINDI  $e = b$

$g$  è suriettiva siccome  $A/\sim$  è una partizione di  $\forall x \in A/\sim \quad \{x\} \neq \emptyset$



$\forall a \in A$

$$\bar{f}([\underline{a}]) = g^{-1}(\overset{\leftarrow}{f}(\{f(a)\})) = f(a)$$

INOLTRE

$\forall a \in A$

$$(L \circ \bar{f} \circ \varepsilon)(a) = L(\bar{f}([\underline{a}])) = L(f(a)) = f(a)$$

PERTANTO

$$L \circ \bar{f} \circ \varepsilon = f$$

□

## 50 - Equipotenza

2 INSIEMI  $A \in B$  SI DICONO EQUIPOTENTI SE HANNO LA STESSA CARDINALITÀ

## 51 - Insieme finito

UN INSIEME SI DICE FINITO SE  $m \in \mathbb{N}$  E L'INSIEME È EQUIPOTENTE

$$\{1, 2, \dots, m\}$$

## 52 - Cardinalità di un insieme

SIA  $A$  UN INSIEME FINITO EIOÉ EQUIPOTENTE A  $\{1, 2, \dots, m\} \subseteq \mathbb{N}$

ALLORA DIREMO  $m$  LA CARDINALITÀ DI  $A$  È SCRIVEREMO

$$|A| = m$$

## 53 - Numero di applicazioni fra due Insiemi Finiti

SIANO  $A \in B$  DUE INSIEMI FINITI.

ALLORA ESISTONO  $|B|^{|A|}$  APPLICAZIONI  $f: A \rightarrow B$

## 54 - Condizione di esistenza di applicazioni iniettive fra insiemi finiti

SIANO  $A \in B$  DUE INSIEMI FINITI.

ESISTONO APPLICAZIONI INIETTIVE FRA  $A \in B$  SE E SOLO SE

$$|A| \leq |B|$$

## 55 - Numero di applicazioni iniettive fra insiemi finiti

SIANO  $A \in B$  DUE INSIEMI FINITI.

E IL NUMERO DI APPLICAZIONI INIETTIVE È UGUALE A

$$\frac{|B|!}{(|B| - |A|)!}$$

## 56 - Condizione di esistenza di applicazioni suriettive fra insiemi finiti

SIANO  $A \in B$  DUE INSIEMI FINITI.

ESISTONO APPLICAZIONI SURIETTIVE FRA  $A \in B$  SE E SOLO SE

$$A = B = \emptyset \quad \vee \quad 0 < |B| \leq |A|$$

## 57 - Condizione di esistenza di applicazioni biettive fra insiemi finiti

SIANO  $A \in B$  DUE INSIEMI FINITI.

ESISTONO APPLICAZIONI BIETTIVE FRA  $A \in B$  SE E SOLO SE

$$|A| = |B|$$

## 58 - Cancellabilità e Invertibilità in un monoide commutativo finito

SIA  $(S, \cdot)$  UN MONOIDE COMMUTATIVO FINITO E SIA  $x \in S$   
ALLORA

$$X \text{ INVERTIBILE} \Leftrightarrow X \text{ CANCELLABILE}$$

## 58 - Dimostrazione

ABBIAMO GIÁ DEMONSTRATO INVERTIBILE  $\rightarrow$  CANCELLABILE

QUINDI ORA DINOSTRIAMO CANCELLABILE  $\rightarrow$  INVERTIBILE

SE  $x \in S$  CANCELLABILE ALLORA  $f_x \in g_x$  SONO BIETTIVE

$\exists y \in S (f_x(y) = xy = 1_S)$   $y$  INVERSO A  $dx$

$\exists z \in S (g_x(z) = zx = 1_S)$   $z$  INVERSO A  $5x$

ALLORA  $y = z \in x$  INVERTIBILE

## 59 - Funzione caratteristica

SIA  $S$  UN INSIEME E  $t \subseteq S$ . ALLORA

$$\chi_{t,s} : x \in S \rightarrow \begin{cases} 0 & \text{se } x \notin t \\ 1 & \text{se } x \in t \end{cases}$$

SI DICE APPLICAZIONE CARATTERISTICA DI  $t$  IN  $S$

## BONUS BINOMIALE - Coefficiente binomiale

$$\forall m, k \quad \binom{m}{k} = |\mathcal{P}_k(\mathcal{I}_m)|$$

$$\text{SE } m < k \quad \text{ALLORA} \quad \binom{m}{k} = 0$$

## BONUS BINOMIALE - Sommatoria di Coefficienti binomiali

$$\forall m \in \mathbb{N} \quad \left( \sum_{k=0}^m \binom{m}{k} = 2^m \right)$$

### Dimostrazione - Sommatoria di Coefficienti binomiali

SAPPIAMO CHE

$$\mathcal{P}(\mathcal{I}_m) = \mathcal{P}_0(\mathcal{I}_m) \cup \mathcal{P}_1(\mathcal{I}_m) \cup \dots \cup \mathcal{P}_m(\mathcal{I}_m).$$

SI AVRÀ DUNQUE:

$$|\mathcal{P}(\mathcal{I}_m)| = |\mathcal{P}_0(\mathcal{I}_m)| \cup |\mathcal{P}_1(\mathcal{I}_m)| \dots \cup |\mathcal{P}_m(\mathcal{I}_m)| = \sum_{k=0}^m \binom{m}{k} = 2^m$$

## BONUS BINOMIALE - Equivalenza di Coefficienti binomiali

$$\forall m, k \in \mathbb{N} \quad (k \leq m \rightarrow \binom{m}{k} = \binom{m}{m-k})$$

### Dimostrazione - Equivalenza di Coefficienti binomiali

SIA  $f: X \in \mathcal{P}(\mathcal{I}_m) \rightarrow \mathcal{I}_m - X \in \mathcal{P}(\mathcal{I}_m)$ .

$f$  È BIETTIVA PERCHÉ LA FUNZIONE DIFFERENZA È BIETTIVA.

INOLTRE SE  $|\mathcal{I}_m| = m$ ,  $|X| = k \rightarrow |\mathcal{I}_m - X| = m - k$

DUNQUE:  $\overline{f}(P_k(I_m)) = P_{m-k}(I_m)$

QUINDI, LA FUNZIONE:

$f|_{P_k(I_m)}: x \in P_k(I_m) \rightarrow I_{m-x} \in P_{m-k}(I_m) \cap I_m f|_{P_k(I_m)}$

È AVEORA UNA BIJEZIONE. I DUE INSIEMI SONO EQUIPOTENTI DUNQUE UGUALI.

BONUS BINOMIALE - Formula ricorsiva per i Coefficienti Binomiali

$$\forall m, k \in \mathbb{N} \quad (k \leq m \rightarrow \binom{m+1}{k+1} = \binom{m}{k} + \binom{m}{k+1})$$

Dimostrazione - Formula ricorsiva per i Coefficienti Binomiali

Sia  $I_{m+1}$ , ALLORA:

$$Q = \{x \in P_{k+1}(I_{m+1}) \mid 1 \in x\}$$

$$b = \{y \in P_{k+1}(I_{m+1}) \mid 1 \notin y\}$$

SE RIMUOVISSIMO 1 DA OGNI  $x \in Q$ , QUESTO DIMINUIREBBE LA LORO CARDINALITÀ DI 1.

NON CONTENENDO 1, SAREBBERO POI ANCHE SOTTOSIEMI DI CARDINALITÀ K DELL'INSIEME  $I_{m+1} - \{1\}$ , E SAREBBERO QUINDI  $\binom{m}{k}$  IN NUMERO.

SIMILARMENTE, GLI INSIEMI DI b, NON CONTENENDO 1, SONO GLI INSIEMI DI CARDINALITÀ k+1 DELL'INSIEME  $I_{m+1} - \{1\}$  E QUINDI SONO  $\binom{m}{k+1}$  IN NUMERO.

$\{a, b\} \in$  UNA PARTIZIONE DI  $P_{k+1}(I_{m+1})$ , E QUINDI  
 $\binom{m+1}{k+1} = |P_{k+1}(I_{m+1})| = |a| + |b| = \binom{m}{k} + \binom{m}{k+1}$

		1					
	1	1	1				
	1	2	1	1			
	1	3	3	1			
	1	4	6	4	1		
	1	5	10	10	5	1	
1	6	15	20	15	6	1	

BONUS BINOMIALE - Formula Matematica dei coefficienti binomiali

$$\forall m, k \in \mathbb{N} \quad (k \leq m \rightarrow \binom{m}{k} = \frac{m!}{(m-k)!k!})$$

Dimostrazione - Formula Matematica dei coefficienti binomiali

USIAMO L'INDUZIONE DI 2° FORMA.

DOBBIAMO ALLINEARE I COEFFICIENTI IN

"LINEA" IN MODO CHE AD OGNI

COEFFICIENTE BINOMIALE POSSA ESSERE ASSOCIAZO UN INTERO.

$$(\forall x, y, z, w \in \{0, \dots, m\}) ((x, y) < (z, w) \iff (x < z) \wedge (y < w))$$

SONO DUNQUE COSÌ ORDINATI

$(0,0) < (1,0) < (1,1) < (2,0) < (2,1) < (2,2) < \dots$

ORA SONO IN ORDINE.

USIAMO COME CASO BASE LA ZERESIMA  
 $m=0$   $\binom{0}{0}$ . ESISTE UN SOLO INSIEME DI  
CARDINALITÀ 0 SOTTOINSIEME DEL VUOTO

$1 = \frac{0!}{(0-0)!0!}$ , LA TESI VALE.

ESTENDIAMO LA TESI  $0 \leq i < m$  PER IPOTESI  
INDUTTIVA E DIMOSTRIAMO CHE VALE IN  $m$ .

IPOTEZZIAMO SIA  $\binom{m}{k}$ .

$$\binom{m}{k} = \binom{m-1}{k-1} + \binom{m-1}{k}$$

MA PER ORDINE SONO MINORI DI  $\binom{m}{k}$

QUINDI VALE LA TESI INDUTTIVA.

$$\binom{m-1}{k-1} + \binom{m-1}{k} =$$
$$\frac{(m-1)!}{(m-1-(k-1))!(k-1)!} + \frac{(m-1)!}{(m-1-k)!(k)!}$$

$$\begin{aligned}
 & \frac{(n-1)}{(n-k)! (k-1)!} + \frac{(n-1)!}{(n-k-1)! k!} = \\
 & \frac{(n-1)! k}{(n-k)! k!} + \frac{(n-1)! (n-k)}{(n-k)! k!} = \\
 & \frac{(n-1)! (k+n-k)}{(n-k)! k!} - \frac{(n-1)! n}{(n-k)! k!} = \frac{n!}{(n-k)! k!}
 \end{aligned}$$

60 - Ogni sottoinsieme è dotato di funzione caratteristica

$$\varphi : t \in P(S) \rightarrow X_{t,s} \in \{0, 1\}^S$$

E  $\varphi$  è BIETTIVA

60 - Dimostrazione

**SURIETTIVITÀ** SIA  $t \in \{0, 1\}^S$ . Poniamo  $t = \overleftarrow{\varphi}(\{1\}) = \{x \in S \mid \varphi(x) = 1\}$

SE  $x \in t \rightarrow X_{t,s} = 1 = \varphi(x)$

SE  $x \notin t \rightarrow X_{t,s} = 0 = \varphi(x)$

QUINDI  $\varphi = X_{t,s}$  QUINDI  $\varphi$  SURIETTIVA

**INIETTIVITÀ** SIA  $t \subseteq S \wedge v \subseteq S \wedge t \neq v$ . Prendo  $x \in t - v$ . ALLORA  $X_{t,s}(x) = 1$   
 $\in X_{v,s} = 0$  QUINDI LE FUNZIONI SONO DISTINTE E  $\varphi$  È INIETTIVA

61 - Insiemi ordinati finiti sono isomorfi se e soltanto se hanno lo stesso diagramma di Hasse

62 - Principio di dualità per insiemi ordinati

DATO  $(S, P)$  È LA DUALE  $\bar{P}$ , ALLORA SI OSSERVA CHE:  $\max(S, P) = \min(S, \bar{P})$

63 - Il Minimo è l'unico Minimale e viceversa (Massimo unico massimale)

DATO UN INSIEME ORDINATO  $(S, P)$  E  $m = \min(S, P)$  ALLORA È L'UNICO MINIMALE

63 - Dimostrazione

SIA  $m \in S$  MINIMALE DI  $(S, P)$ . PER DEFINIZIONE DI MINIMO SI HA CHE  $m P m$ . QUINDI  $m, m$  SONO CONFRONTABILI, QUINDI PER DEFINIZIONE DI MINIMALE  $m P m$ . PER ASIMMETRIA, ALLORA I DUE COINCIDONO.

64 - In insiemi finiti, l'Unico Minimale è Minimo e viceversa (Unico massimale, max)

65 - Estremo superiore ed inferiore

SIA  $(S, P)$  UN INSIEME ORDINATO E  $t \subseteq S$ .

DEFINIAMO L'ESTREMO INFERIORE E SUPERIORE COME

$$\sup_{(S, P)}(t) = \min(\text{MAGGIOR}(S, P)) \quad (\text{SE ESISTE})$$

$$\inf_{(S, P)}(t) = \max(\text{MINOR}(S, P)) \quad (\text{SE ESISTE})$$

## 66 - Reticolo

SIA  $(S, P)$  UN INSIEME ORDINATO CON  $P \subseteq \text{OL}(S)$

$$(S, P) \text{ RETICOLO} \iff \forall x, y \in S (\exists_{\text{INF}_{(S, P)}} \xi_{x, y} \wedge \exists_{\text{SUP}_{(S, P)}} \xi_{x, y})$$

## 67 - Operazioni in un reticolo

DATO UN RETICOLO  $(S, P)$ ,  $\forall x, y \in S$  DEFINIAMO:

$$(\text{WEDGE}) \wedge : (x, y) \in S \times S \rightarrow \text{INF}_{(S, P)}(\xi_{x, y}) \in S$$

$$(\text{VEE}) \vee : (x, y) \in S \times S \rightarrow \text{SUP}_{(S, P)}(\xi_{x, y}) \in S$$

ALLORA POSSIAMO ESPRIMERE UN RETICOLO  
COME UNA STRUTTURA ALGEBRICA  $(S, \wedge, \vee)$

## 68 - Reticolo limitato

UN RETICOLO SI DICE LIMITATO SE E' DOTATO DI MAX E MIN

## 69 - Reticolo completo

UN RETICOLO SI DICE COMPLETO SE OGNI SUA PARTE NON VUOTA  
E' DOTATA DI ESTREMO SUPERIORE ED INFERIORE

## 70 - Principio di dualità per i reticolati

SIA  $(S, P)$  UN RETICOLO, E'  $(S, \bar{P})$  IL SUO DUALE. SE  $\sigma$  E' UN ENUNCIATO  
SUL RETICOLI, CHIAMERÒ  $\bar{\sigma}$  IL SUO ENUNCIATO DUALE  
DOVE

- ① RIMPIAZZERÒ  $P$  CON  $\bar{P}$  (E VICEVERSA)
- ② RIMPIAZZERÒ  $\vee$  CON  $\wedge$  (E VICEVERSA)

71 - Il Minimale di un Reticolo è il suo Minimo e viceversa (Massimale è il suo max)

## 71 - Dimostrazione

SIA  $(S, P)$  UN RETICOLO E  $m \in S$  MINIMALE. SIA  $x \in S$  UN ELEMENTO  
GENERALICO DEL RETICOLO. AVREMO  $(m \wedge x) \leq m$  PER LA DEFINIZIONE  
DI ESTREMO INFERIORE.  
PER LA DEFINIZIONE DI MINIMALE  $m \leq (m \wedge x)$ .  
PER ASIMETRIA  $m \wedge x = m \quad \forall x$ . ALLORA  $m$  MINIMO DI  $S$ .

72 - Ogni parte finita di un Reticolo è dotata di estremo inferiore e superiore

73 - Commutatività di Wedge e Vee

SIA  $(S, \wedge, \vee)$  UN RETICOLO.

ALLORA

$$\forall x, y \in S (x \wedge y = y \wedge x) \wedge (x \vee y = y \vee x)$$

73 - Dimostrazione

$$x \wedge y = \inf_{(S, P)} (\{x, y\}) = \inf_{(S, P)} (\{y, x\}) = y \wedge x$$

$$x \vee y = \sup_{(S, P)} (\{x, y\}) = \sup_{(S, P)} (\{y, x\}) = y \vee x$$

74 - Associatività di Wedge e Vee

SIA  $(S, \wedge, \vee)$  UN RETICOLO.

ALLORA  $\wedge, \vee$  SONO ASSOCIATIVE

74 - Dimostrazione

DIMOSTRIAMO IL TEOREMA PER  $\vee$ , LA DEMOSTRAZIONE È ANALOGA PER  $\wedge$

SIANO  $x, y, z \in S$ . PER DEFINIZIONE ABBIAMO CHE:

$$1) x \leq [x \vee (y \vee z)]$$

$$2) (y \vee z) \leq [x \vee (y \vee z)]$$

$$3) y \leq (y \vee z)$$

$$4) z \leq (y \vee z)$$

ALLORA PER TRANSITIVITÀ  $y \leq [x \vee (y \vee z)]$

$$z \leq [x \vee (y \vee z)]$$

E DUNQUE

$$(x \vee y) \leq [x \vee (y \vee z)]$$

ED INFINE

$$[(x \vee y) \vee z] \leq [x \vee (y \vee z)]$$

## 75 - Proprietà di Assorbimento

$$\forall x, y \in S \quad ((x \vee (x \wedge y) = x) \wedge (x \wedge (x \vee y) = x))$$

## 76 - Proprietà di Idempotenza

IN UN RETICOLO  $(S, P)$ ,  $x = x \vee x = x$  PER OGNI  $x \in S$

## 76 - Dimostrazione

DIMOSTRIAMO PER  $\wedge$ , ANALOGO PER  $\vee$ .

DALLE PROPRIETÀ DI ASSORBIMENTO SEGUÉ:

$$\forall y \in S \quad (x \wedge (x \vee y) = x)$$

DATO CHE  $x \wedge x \in S$  ALLORA, PONENDO  $y = x \wedge x$

APPLICHIAMO DI NUOVO L'ASSORBIMENTO

$$x = x \wedge (x \vee (x \wedge x)) = x \wedge x$$

□

## 77 - Minimo e massimo sono elementi neutri di un reticolo

SIA  $(S, P)$  UN RETICOLO. SIANO  $m, M \in S$ . ALLORA

$m$  MINIMO DI  $S \iff m$  NEUTRO DI  $\wedge_P$

$M$  MASSIMO DI  $S \iff M$  NEUTRO DI  $\vee_P$

## 77 - Dimostrazione

→ SIA  $x \in S$ . ALLORA  $x \wedge m \wedge x = x$ .

DUNQUE  $x = \min(\{x, m\}) = x \wedge_P m$ .  $m$  NEUTRO

←  $\forall x \in S \quad (m \wedge_P x = x) \rightarrow \forall x \in S \quad (x \wedge_P m)$ .

LA DEMOSTRAZIONE È ANALOGA PER IL MASSIMO

## 78 - Sottoreticolo

SIA  $(S, \wedge, \vee)$  UN RETICOLO E  $t \in \wp(S) \setminus \{\emptyset\}$ .

SE  $t$  È CHIUSO RISPETTO  $\wedge, \vee$  ALLORA SI DICE SOTTORETIColo DI  $(S, \wedge, \vee)$

## 79 - Intervallo chiuso

SIA  $(S, \leq)$  UN INSIEME ORDINATO, CON  $\leq \in \text{OL}(S)$

$i \subseteq S$  INTERVALLO:  $\Leftrightarrow \forall x, y \in i \ (\forall z \in S) (x \leq z \wedge z \leq y \rightarrow z \in i)$

## 80 - Reticolo complementato

UN RETICOLO  $(S, \wedge, \vee)$  SI DICE COMPLEMENTATO SE

$$\forall x \in S \ (\exists y \in S) \mid \boxed{x \wedge y = \min(S)} \wedge \boxed{x \vee y = \max(S)}$$

## 81 - Reticolo distributivo

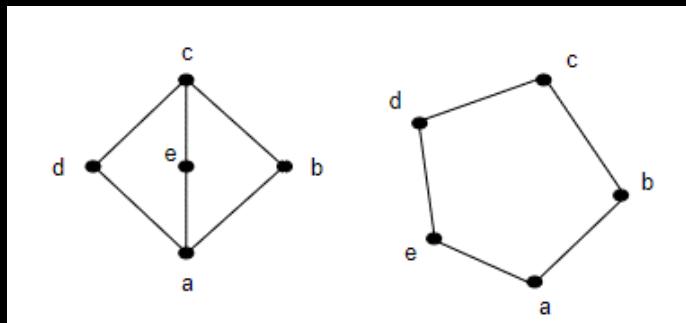
UN RETICOLO  $(S, \wedge, \vee)$  SI DICE DISTRIBUTIVO SE VALGONO

ENTRAMBE LE LEGGI DISTRIBUTIVE

$$\forall a, b, c \in S \ (a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c))$$

$$\forall a, b, c \in S \ (a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c))$$

INOLTRE UN RETICOLO È DISTRIBUTIVO  $\Leftrightarrow$  NON HA SOTTORETICOLI ISOMORFI AL RETICOLO TRIANGOLARE O AL RETICOLO PENTAGONALE



## BONUS - Anello Booleano

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

UN ANELLO È BOOLEANO  $\Leftrightarrow \forall x \in A \ (x \cdot x = x)$

## 82 - Reticolo booleano

UN RETICOLO SI DICE BOOLEANO SE E' DISTRIBUTIVO E COMPLEMENTATO.

## 83 - Algebra di boole

UNA STRUTTURA  $(S, \wedge_p, \vee_p)$  SI DICE ALGEBRA DI BOOLE SE:

1)  $\wedge_p, \vee_p$  SONO COMMUTATIVE

2)  $\wedge_p, \vee_p$  SONO ASSOCIATIVE

3) VALE LA LEGGE DI ASSORBIMENTO

4) VALE LA DISTRIBUTIVITÀ.

5)  $\wedge_p \in \vee_p$  HANNO ELEMENTI NEUTRI 0, 1.

6) E' UN'OPERAZIONE UNARIA INTERNA:  $\forall x \in S (x \vee_p x' = 1) \wedge (x \wedge_p x' = 0)$

## 84 - In un anello Booleano, ogni elemento è il proprio opposto

$$(\alpha, +, \cdot) \text{ BOOLEANO} \iff \forall x \in \alpha (x = -x)$$

## 84 - Dimostrazione

$$x + x = (x+x)^2$$

$$x + x = x^2 + 2x^2 + x^2$$

$$x + x = x + \cancel{2x^2} + x$$

QUINDI

$$2x^2 = 0$$

MA ALLORA

$$\cancel{x+x} = 0 \rightarrow x = -x$$

## 85 - Anelli booleani sono commutativi

SIA  $(\alpha, +, \cdot)$  UN ANELLO BOOLEANO. ALLORA  $\forall x, y \in \alpha (xy = yx)$

## 85 - Dimostrazione

SIANO  $x, y \in \alpha$

$$x+y = (x+y)^2$$

$$x+y = x^2 + xy + yx + y^2$$

$$x+y = x + xy + yz + y$$

MA ALLORA

$$xy + yx = 0 \rightarrow xy = -yx \text{ (OGNI ELEMENTO E' IL SUO OPP)}$$

BONUS 3 - Per ogni Anello Booleano esiste un corrispondente Reticolo Booleano  
DATO UN ANELLO  $(\mathcal{Q}, +, \cdot)$ , DEFINIAMO  $P: \forall x, y \in \mathcal{Q} (x P y \leftrightarrow xy = x)$ .

ALLORA DIMOSTRIAMO CHE  $(S, P)$  È UN RETICOLO BOOLEANO

Dimostrazione

1-  $P \in OL(\mathcal{Q})$ :

-  $\forall x \in \mathcal{Q} (x \cdot x = x) \rightarrow \forall x (x P x)$  PER LA PROPRIETÀ PRINCIPALE  
DELL'ANELLO BOOLEANO. LA REL DUNQUE È RIFLESSIVA.

-  $\forall x, y \in \mathcal{Q} (x P y \wedge y P x \rightarrow xy = x \wedge yx = y \rightarrow x = y)$  PER LA  
COMMUTATIVITÀ DELL'ANELLO BOOLEANO. LA REL DUNQUE È ASIMMETRICA

-  $\forall x, y, z \in \mathcal{Q} (x P y \wedge y P z \rightarrow xy = x \wedge yz = y \rightarrow x = xy = x(yz) = (xy)z = xz \rightarrow x P z)$   
LA REL DUNQUE È TRANSITIVA

2- VERIFICHiamo CHE PER OGNI COPPIA, INF E SUP SONO COSÌ DEFINITI

$$\forall x, y \in \mathcal{Q} (x \vee_p y = x + y + xy)$$

$$\forall x, y \in \mathcal{Q} (x \wedge_p y = xy)$$

SIANO  $x, y \in \mathcal{Q}$ . DIMOSTRIAMO CHE  $x \vee_p y$  È MAGGIORANTE.

$x \cdot (x \vee_p y) = x(x + y + xy) = x^2 + xy + x^2y$  PER LE PROPRIETÀ DELL'ANELLO  
BOOLEANO,  $x^2 = x \in xy + xy = 0$

PERTANTO  $x \cdot (x \vee_p y) = x \rightarrow x P (x \vee_p y)$

LO STESSO PROCEDIMENTO SI PUÒ EFFETTUARE PER Y.

DIMOSTRAMO CHE  $x \vee_p y$  È ESTREMO SUPERIORE, EPOÈ MINIMO DEI  
MAGGIORANTI.

SIA  $z \in \mathcal{Q}$  MAGGIORANTE DI  $\{x, y\}$ . ALLORA:

$$\begin{aligned} x P z \wedge y P z &\rightarrow xz = x \wedge yz = y \\ &\rightarrow (x + y + xy)z = xz + yz + xyz = x + y + xy \\ &\rightarrow (x + y + xy)P z \\ &\rightarrow (x \vee_p y)P z \end{aligned}$$

### 3- È LIMITATO, DISTRIBUTIVO E COMPLEMENTATO

LIMITATO -  $\forall x \in \Omega (0x=0 \rightarrow 0 \neq x)$  e/o è 0 è minimo

ANALOGAMENTE,  $\forall x \in \Omega (x1=x \rightarrow 1 \neq x)$  1 è massimo, RETICOLO LIMITATO

DISTRIBUTIVO -  $x \wedge (y \vee z) = x \wedge (y+z+yz) = x(y+z+yz) = xy+xz+xyz$

$$(x \wedge y) \vee (x \wedge z) = (xy) \vee (xz) = xy+xz+xyz = xy+xz+xyz$$

PERTANTO IL RETICOLO È DISTRIBUTIVO

COMPLEMENTATO - SIA  $x \in \Omega$ . ALLORA:

$$x \wedge (1+x) = x(1+x) = x+x^2 = x+x = x$$

$$x \vee (1+x) = x + (1+x) + x(1+x) = x + 1 + x + x + x^2 = 1$$

BONUS 4 - Per ogni Reticolo Booleano esiste un corrispondente Anello Booleano

SIA  $(S, \wedge, \vee)$  RETICOLO BOOLEANO con ALMENO 2 ELEMENTI E

DEFINIAMO:  $x+y = (x \wedge y')$   $\vee (x' \wedge y) \quad x \cdot y = (x \wedge y)$ .

ALLORA SI DIMOSTRA CHE  $(S, +, \cdot)$  È UN ANELLO BOOLEANO

BONUS 5 - L'insieme delle parti è un Anello Booleano

Dimostrazione

DATO CHE  $(P(S), \subseteq)$  È UN RETICOLO BOOLEANO, ALLORA

$(P(S), \cap, \cup, ')$  È UNA ALGEBRA DI BOOLE, DOVE

$$\forall x \in P(S) (x' = S-x)$$

PER LA CORRISPONDENZA BIUNIVOCÀ FRA RETICOLI ED ALGEBRE DI BOOLE.

ALLORA  $\forall x, y \in P(S)$ :

$$- x \cdot y = x \cap y$$

$$- x+y = (x \cap (S-y)) \cup (y \cap (S-x)) = (x-y) \cup (y-x) = x \Delta y$$

E DUNQUE  $(P(S), \Delta, \cap)$  È UN ANELLO BOOLEANO.

## BONUS 6 - Teorema di Stone

SIA  $\alpha \neq \emptyset \in (\alpha, +, \cdot)$  UN ANELLO BOOLEANO.

ALLORA:  $(\exists s \neq \emptyset)(\alpha, +, \cdot) \xrightarrow{\text{ISOMORFO}} (P(s), \Delta, \cap)$ .

SE  $\alpha$  È FINITO, POSSO SCEGLIERE ANCHE  $s$  FINITO.

## BONUS 7 - Corollari del Teorema di Stone

- 1) IL TEOREMA DI STONE SI APPLICA ANCHE FRA RETICOLI BOOLEANI  $\in (P(s), \leq)$
- 2) SE  $(\alpha, +, \cdot) \in$  UN ANELLO BOOLEANO  $\in [\alpha] = m \in \mathbb{N}_2$   
ALLORA  $(\exists_{m \in \mathbb{N} \setminus \{0\}})(m = 2^m)$
- 3) SE  $(\alpha, P) \in$  UN RETICOLO BOOLEANO  $\in [\alpha] = m \in \mathbb{N}_1$ , ALLORA  $(\exists_{m \in \mathbb{N} \setminus \{0\}})(m = 2^m)$ , E OÈ LA CARDINALITÀ DELL'INSIEME SOSTEGNO DI UN ANELLO BOOLEANO È SEMPRE UNA POTENZA DI DUE.
- 4) DUE ANELLI BOOLEANI FINITI SONO ISOMORFI  $\iff$  HANNO LA STESSA CARDINALITÀ.

## 86 - Divisori e multipli

$$\forall x, y \in S \quad x|y \iff \exists z \in S \quad (y = xz)$$

$y$  è multiplo di  $x$

DENOTIAMO

$$\text{Div}_S(x) = \{y \in S \mid y|x\}$$

$$\text{Mult}_S(x) = \{z \in S \mid x|z\}$$

## 87 - Due elementi si dicono associati se si dividono a vicenda

$$\forall x, y \in S$$

$$X, Y \text{ ASSOCIATI} \iff x \in \text{Div}_S(y) \wedge y \in \text{Div}_S(x)$$

L'INSIEME DEGLI ELEMENTI ASSOCIATI SARÀ

$$\text{Assoc}_S(x) = \{y \in S \mid x|y \wedge y|x\}$$

## 88 - Associati di un elemento cancellabile

SIA  $(S, \cdot)$  UN MONOIDE COMUTATIVO. SE  $x \in S$  È UN ELEMENTO CANCELLABILE ALLORA

$$\text{Assoc}_S(x) = \{x_u \in S \mid u \in U(S)\}$$

OVVERO TUTTI GLI ASSOCIATI DI UN ELEMENTO CANCELLABILE SONO IL PRODOTTO DI  $x$  PER UN ELEMENTO INVERTIBILE

## 89 - Divisori banali

$$B\text{DIV}_S(x) = U(S) \cup \text{Assoc}_S(x)$$

## 90 - Elementi irriducibili

SIA  $(S, +, \cdot)$  UN DOMINIO DI INTEGRITÀ E SIA  $x \in S$

$$X \text{ IRRIDUCIBILE} \iff x \notin U(S) \wedge \text{Div}_S(x) = B\text{DIV}_S(x)$$

## 91 - Elementi primi

SIA  $(S, \cdot)$  UN MONOIDE COMUTATIVO.

$$p \in S \text{ PRIMO} \iff \forall a, b \in S \quad (p|ab \rightarrow p|a \vee p|b)$$

## 92 - Elementi coprimi

SIA  $(S, \cdot, 1_S)$  UN MONOIDE COMUTATIVO.

$$x, y \in S \text{ COPRIMI} \iff 1_S \in \text{MCD}(\{x, y\})$$

EPOE' SE IL NEUTRO È UN LORO MCD.

### 93 - Monoide cancellativo

UN MONOIDE COMMUTATIVO SI DICE CANCELLATIVO SE OGNI SUO ELEMENTO È CANCELLABILE.

### 94 - Monoide fattoriale

UN MONOIDE COMMUTATIVO  $(m, \cdot)$  SI DICE FATTORIALE SE VALE:

- 1) OGNI  $x \in m \setminus U(m)$  È UN PRODOTTO DI PRIMI
- 2) OGNI  $x \in m \setminus U(m)$  È PRODOTTO DI IRRIDUCIBILI, ED OGNI IRRIDUCIBILE È PRIMO
- 3) OGNI  $x \in m \setminus U(m)$  È PRODOTTO DI IRRIDUCIBILI, ED OGNI FATTORIZZAZIONE È UNICA A MENO DELL'ORDINE DEI FATTORI E DEL PRODOTTO PER INVERTIBILI.

### 95 - Anello fattoriale

UN ANELLO COMMUTATIVO UNITARIO  $(A, +, \cdot)$  SI DICE FATTORIALE SE  $(A \setminus \{0\}, \cdot)$  È UN MONOIDE FATTORIALE.

### 96 - Proprietà di divisione lineare dei divisori comuni

SIA  $(S, +, \cdot)$  UN ANELLO COMMUTATIVO UNITARIO E SIANO  $a, b \in S$ .  
SE  $d \in \text{DIV}_{(S,+)}(a) \cap \text{DIV}_{(S,+)}(b)$ .

ALLORA

$$\forall x, y \in S \quad (d | x_a + y_b)$$

CIOE' I DIVISORI COMUNI DIVIDONO OGNI COMBINAZIONE LINEARE DEGLI ELEMENTI.

### 96 - Dimostrazione

$$d | a \wedge d | b \rightarrow \exists h, k \in \mathbb{Z} \quad (a = dk \wedge b = dh)$$

E QUINDI

$$\forall x, y \in \mathbb{Z} \quad (ax + by = dkx + dh = d(kx + hy) \rightarrow d | (ax + by))$$

### 97 - Valore assoluto

SIA  $m \in \mathbb{Z}$ . ALLORA DEFINIAMO LA FUNZIONE VALORE ASSOLUTO COME.

$$|m|: m \in \mathbb{Z} \rightarrow \begin{cases} m & \text{se } m \in \mathbb{N} \\ -m & \text{se } m \in \mathbb{Z} \setminus \mathbb{N} \end{cases}$$

## 97 - Divisione Eculidea

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

OVVERO PER OGNI COPPIA DI VALORI  $m \in \mathbb{Z}$ , CON  $n$  NON  
NULLO ESISTONO E SONO UNICI QUOTIENTE  $q$  E RESTO TALE CHE  
 $m$  PUÒ ESSERE SCRITTO COME  $m = qn + r$ . INOLTRE IL  
RESTO  $r$  È COMPRESO FRA 0 E IL VALORE ASSOLUTO DI  $n$ .

### 97 - Dimostrazione

DIVIDIAMO LA DEMOSTRAZIONE IN 3 SEZIONI:

- ① DIMOSTRIAMO CHE ESISTE LA COPPIA  $(q, r)$  SE  $m \in \mathbb{N}$
- ② DIMOSTRIAMO CHE LA COPPIA  $(q, r)$  ESISTE ANCHE SE  $m$  È NEGATIVO
- ③ DIMOSTRIAMO CHE LA COPPIA  $(q, r)$  È UNICA

1 - DIMOSTRIAMO PER INDUZIONE DI SECONDA FORMA SU  $m$ .

1 SE  $m=0$ , ALLORA SCEGLIO  $q=r=0$

2 SE  $0 < m < |n|$ , ALLORA  $q=0$ ,  $r=m$  Es.  $3|7=0+7$  e  $r=3$

3 SE  $m=|n|$ , ABBIAMO 2 POSSIBILITÀ:

- $m=n$ , ALLORA  $q=1$  E  $r=0$  Es.  $7|7=1 \cdot 7 + 0$
- $m=-n$ , ALLORA  $q=-1$  E  $r=0$  Es.  $7|-7=(-1) \cdot (-7) + 0$

Q SE  $m > |n|$  ALLORA  $0 < m - |n| < m$  QUINDI PER IPOTESI INDUTTIVA

$$\exists (q_1, r_1) \mid \underbrace{m - |n|}_{m - n} = mq_1 + r_1 \wedge 0 \leq r_1 < |n|$$

QUINDI  $m = m - |n| + |n| + r_1$  (ORA METTIAMO  $m$  IN EVIDENZA)

QUINDI SE  $m > 0$ , ALLORA  $(q, r) = (q_1 + 1, r_1)$  Es.  $7|3(7, 3) = (2, 1)$

SE  $m < 0$ , ALLORA  $(q, r) = (q_1 - 1, r_1)$  Es.  $7|-3(7, 3) = (-2, 1)$

E PER INDUZIONE LA TESI VALE  $\forall m$

## 2- DIMOSTRIAMO CASO $m \in \mathbb{Z} \setminus \mathbb{N}$

Se  $m \in \mathbb{Z} \setminus \mathbb{N}$

Allora  $-m \in \mathbb{N} \rightarrow -m = mq_1 + r_1 \wedge 0 \leq r_1 < |m| \rightarrow m = m(-q_1) - r_1$

Se  $r_1 = 0 \rightarrow q = -q_1 \in \mathbb{N} = 0$

Se  $r_1 > 0 \quad 0 < |m| - r_1 < |m| \in m = m \cdot (-q_1) - |m| + |m| - r_1$

$$m > 0 \quad (q, r) = (-q_1 - 1, m - r_1)$$

$$m < 0 \quad (q, r) = (-q_1 + 1, -m - r_1)$$

Allora la tesi vale  $\forall m \in \mathbb{Z}$

## 3- DIMOSTRAZIONE (q, r) UNICI

Sia  $(q_1, r_1), (q_2, r_2) \in \mathbb{Z} \times \mathbb{N}$  (DIRE LA TESI SOL 2)

Allora  $0 \leq r_1 \leq r_2 < |m|$ , di conseguenza

$$m = m q_1 + r_1 \quad \text{QUINDI } m = m q_1 + r_1 = m q_2 + r_2$$

$$m = m q_2 + r_2$$

Allora

$$m(q_1 - q_2) = r_2 - r_1 \in |m(q_1 - q_2)| = |r_2 - r_1| \in$$

$$0 \leq |r_2 - r_1| < |m|$$

AVERNO  $|m| |q_2 - q_1| < |m|$ , DATO CHE  $m \neq 0$  PUÒ SUCCEDERE

SOLÒ QUANDO  $|q_2 - q_1| = 0 \rightarrow q_2 = q_1$

QUINDI  $m = m q_1 + r_1 = m q_2 + r_2 \rightarrow r_1 = r_2$ . CHE È LA TESI.

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

## 98 - Teorema di Bézout

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

OVVÉRO CHE PER OGNI MCD TRA  $\alpha \in B$  ESISTE UNA COMBINAZIONE LINEARE TRA I DUE

## 98 - Dimostrazione

SIA  $t$  IL MINIMO NUMERO DI PASSI TALE CHE  $r_t = 0$   
OVVÉRO CHE TRAMITE L'ALGORITMO DELLE DIVISIONI SUCCESSIONE IL RESTO SIA 0.

SE  $t=1$  ALLORA  $r_1=0$  E  $\alpha = b q_1 \rightarrow b \in \text{MCD}(\alpha, b)$   
 $\in b = \alpha \cdot 0 + b \cdot 1$ . QUINDI  $(u, v) = (0, 1)$

$$\begin{aligned} \text{ESEMPIO: } \alpha &= 7 \quad b = 7 \\ 7 &= 7 \cdot 1 + 0 \quad (t \leq 1) \\ \alpha &= b \cdot q_1 \\ b &= \alpha \cdot 0 + b \cdot 1 \\ 7 &= 0 + 7 \cdot 1 \end{aligned}$$

IL TEOREMA DICE CHE L'MCD (IN QUESTO CASO 7) PUÒ ESSERE SCRITTO COME COMBINAZIONE LINEARE PROPRIO TRA A E B, IN QUESTO CASO USANDO COME  $(u, v) = (0, 1)$

SE  $t=2$  ALLORA  $r_1 \neq 0$  E  $r_2 = 0$  ( $r_t$ ).  
AVREMO  $r_1 \in \text{MCD}(\alpha, b) / \in r_1 = \alpha \cdot 1 + b \cdot (-q_1)$ .  
QUINDI  $(u, v) = (1, -q_1)$

$$\begin{aligned} \text{ESEMPIO: } \alpha &= 5 \quad b = 2 \\ t=1 \quad 5 &= 2 \cdot 2 + 1 \quad r_1 \\ t=2 \quad 2 &= 1 \cdot 2 + 0 \quad 1 = \alpha \cdot 1 + b \cdot (-q_1) \\ &\quad 1 = 5 - 4 \end{aligned}$$

SUPPONIAMO SEMPRE VERO L'ASSERTO  $\forall i : 1 \leq i < t$ .  
 $(r_t = 0 \rightarrow r_{t-1} \in \text{MCD}(\alpha, b))$

SAPPiamo che  $x_{t-1} = x_{t-3} + r_{t-2}(-q_{t-1})$ . (per la stessa ipotesi di  $t=2$ )

Allora ( $\exists u, v, w, x \mid x_{t-1} = (au + bv) + (qw + bx) \cdot (-q_{t-1})$ )  
 $= au + bv - qwq_{t-1} - bxq_{t-1} = \underline{a(u - wq_{t-1}) + b(v - xq_{t-1})}$ )

□

### 99 - Lemma di Euclide

SIANO  $a, b, c \in \mathbb{Z}$ . SE  $a, b$  SONO COPRIMI ALLORA

$$a \mid bc \rightarrow a \mid c$$

### 99 - Dimostrazione

$1 \in \text{MCD}(a, b)$  PERCHÉ SONO COPRIMI.

PER IL TEOREMA DI BÉZOUT.

SAREBBE

$\exists u, v \in \mathbb{Z} (au + bv = 1)$  QUINDI  $c = aeu + bcv$ .

$c = e$  SICOMÈ  
 $au + bv = 1$

DATO CHE  $a \mid ac$  (BANALMENTE) E  $a \mid bc$  (PER IPOTESI), ALLORA

$\exists h, k \in \mathbb{Z} (c = aeu + bcv = ah + akv \rightarrow c = a(h + kv) \rightarrow a \mid c)$

□

### 100 - Relazione d'equivalenza compatibile

$\sim$  COMPATIBILE A  $S*$  IN  $(S, *) \iff \forall a, b, c \in S (a \sim b \rightarrow c * a \sim c * b)$

$\sim$  COMPATIBILE A  $D*$  IN  $(S, *) \iff \forall a, b, c \in S (a \sim b \rightarrow a * c \sim b * c)$

### 101 - Congruenza

SIA  $S \neq \emptyset$  E  $*_1, *_2, \dots, *_n$  SUE OPERAZIONI BINARIE INTERNE

E SIA  $\sim$  UNA RELAZIONE D'EQUIVALENZA.

$\sim$  E' UNA CONGRUENZA SE E SOLO SE

$\forall a, b, c, d \in S (\forall i \in N (0 \leq i < n \rightarrow (a \sim b \wedge a *_i d \rightarrow c *_i c \sim b *_i d)))$

### 102 - Equazione diofantea

SIANO  $a, b, c \in \mathbb{Z}$  ALLORA LA FUNZIONE:

$$f[a, b, c] : (x, y) \in \mathbb{Z} \times \mathbb{Z} \rightarrow ax + by - c \in \mathbb{Z}$$

SI DICE EQUAZIONE DIOFANTEA DI 1° GRADO CON TERMINI  $a, b, c$ .  
(SI PUÒ SCRIVERE ANCHE COME  $ax + by = c$ )

### 103 - Soluzione di un'equazione diofantea

DATA UN'EQUAZIONE DIOFANTEA  $\exists [\alpha, b, c](m, m)$  ALLORA  
LA COPPIA  $(x, y)$  PER CUI  $\exists [\alpha, b, c](x, y) = 0 \Leftrightarrow \alpha x + b y = c$   
SI DICE SOLUZIONE DELL'EQUAZIONE DIOFANTEA.

### 104 - Equazioni congruenziali

SIANO  $m \in \mathbb{Z} \setminus \{0\}$ ,  $a, b \in \mathbb{Z}$  ALLORA LA FUNZIONE:

$$\exists \in [\alpha, b, m] : [m]_m \in \mathbb{Z}_m \rightarrow [\alpha_m - b] \in \mathbb{Z}_m$$

SI DICE EQUAZIONE CONGRUENZIALE DI 1° GRADO AD UNA INCONGNITA DI TERMINI  $a$  E  $b$  E MODULO  $m$ .

### 105 - Soluzioni di un'equazione congruenziale

SIA  $m \in \mathbb{Z}$  SI DICE SOLUZIONE DI UN'EQUAZIONE CONGRUENZIALE  $\exists \in [\alpha, b, m]$  SE  $\exists \in [\alpha, b, m](m) = [\alpha]_m$  OVVERO SE

$$\alpha_m \equiv b$$

OVVIAMENTE ESSENDO  $m$  UNA CLASSE DI RESTO, SONO SOLUZIONI ANCHE TUTTI I VALORI CONGRUI A  $[m]_m$ .

### 106 - Criterio per l'esistenza di soluzioni congruenziali

SIANO  $a, b \in \mathbb{Z}$  E  $m \in \mathbb{Z} \setminus \{0\}$   
ALLORA

$$ax \equiv_m b \text{ HA SOLUZIONI} \Leftrightarrow \text{MCD}(\alpha, m) \mid b$$

### 106 - Dimostrazione

L'EQUAZIONE CONGRUENZIALE  $ax \equiv_m b$  PUÒ ESSERE SCRITTA COME EQUAZIONE DIOFANTEA  $\alpha x + my = b$ .

TRAMITE BÉZOUT SAPPIAMO CHE SE  $d \in \text{MCD}(\alpha, m)$   
ALLORA DIVIDE  $b$

## 107 - Primo corollario del criterio d'esistenza di soluzioni congruenziali

SIA  $a, b \in \mathbb{Z}$   $m \in \mathbb{Z} \setminus \{0\}$   $d \in \text{MCD}(a, m)$  ALLORA:

$$[\frac{a}{m}] \in U(\mathbb{Z}_m) \iff a, m \text{ COPRIMI}$$

### 107 - Dimostrazione

$\rightarrow$  ESISTE  $[u]_m$  TALE CHE  $[\alpha]_m \cdot [u]_m = [1]_m$ , QUINDI  
L'EQUAZIONE CONGRUENZIALE  $\alpha x \equiv_m 1$  HA SOLUZIONE  $u$ .  
QUESTO IMPLICA CHE  $d \in \text{MCD}(a, m) | 1$   
MA  $1 | d$  QUINDI I DUE SONO ASSOCIAZI!  $\in 1 \in \text{L'MCD}$ .  
ALLORA  $a \in m$  SONO COPRIMI.

$\leftarrow$  SE  $a \in m$  SONO COPRIMI ALLORA  $1 \in \text{MCD}$   
 $\in 1 | 1$  QUINDI L'EQUAZIONE CONGRUENZIALE  
 $\alpha x \equiv_m 1$  HA SOLUZIONI.

ESISTE QUINDI UN  $[\alpha]_m$  INVERTIBILE

## 108 - Secondo corollario del criterio d'esistenza di soluzioni congruenziali

SIANO  $a, b \in \mathbb{Z}$   $m \in \mathbb{Z} \setminus \{0\}$   $d \in \text{MCD}(a, b)$  ALLORA

$$[\frac{a}{m}] \in U(\mathbb{Z}_m) \iff [\frac{a}{m}] \text{ NON E' DIVISORE DELLO ZERO}$$

### 108 - Dimostrazione

$\rightarrow$  PER ASSURDO SIA  $[\frac{a}{m}]$  DIVISORE DELLO ZERO.

$$\text{AVREMO CHE } \exists [b]_m \quad [\frac{a}{m}] [b]_m = [0]_m.$$

MA INVERTIBILITÀ IMPLICA CANCELLABILITÀ E QUINDI AVREMO  
 $[b]_m = [0]_m$  CHE E' ASSURDO

$\leftarrow$  PER ASSURDO SIA  $[\frac{a}{m}]$  NON INVERTIBILE.

ALLORA PER IL PRIMO COROLLARIO  $a, m$  NON SONO COPRIMI

ALLORA PREndo  $d \neq 1$  TALE CHE  $\exists k \in \mathbb{Z} (ad = km)$

$$[\frac{a}{m}] [\frac{d}{m}] = [\frac{ad}{m}] = [\frac{km}{m}] = [0]_m \text{ CHE E' ASSURDO}$$

## 109 - Elemento periodico

SIA  $(g, \cdot)$  UN GRUPPO.  $X \in g$  SI DICE PERIODICO SE

$$\exists m \in \mathbb{N}^{\geq 2} \mid X^m = 1_g$$

TALE  $m$  SI DICE PERIODICO DELL'ELEMENTO  $X \in g$ .  
INDICA CON  $|X|$

## 109 - Successione di elementi

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

ALLORA UNA FUNZIONE

$$f: m \in \mathbb{N} \rightarrow x \in A$$

SI DICE SUCCESSIONE DEGLI ELEMENTI DI  $A$ .

LA SUCCESSIONE LA DENOTEREMO CON

$$A_m = f(m)$$

## 110 - Polinomi

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

$(a_m)_{m \in \mathbb{N}}$  UNA SUCCESSIONE DI SUOI ELEMENTI

DIREMO CHE :

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

UN POLINOMIO E' QUINDI UNA SUCCESSIONE CHE SI ANNULLA DOPO UN CERTO NUMERO  $k$  DI TERMINI.

NOTEREMO I POLINOMI COME  $A[x]$

## 110 - Polinomio nullo

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

DEFINIREMO IL POLINOMIO NULLO COME

$$O : (O_A)_{n \in \mathbb{N}}$$

DOVE  $(O_A)_{n \in \mathbb{N}}$  È UNA SUCCESSIONE DOVE OGNI ELEMENTO  
È  $O$

$$(\forall n \in \mathbb{N}) (o_n) = O_A$$

## 111 - Grado di un polinomio

SIA  $f \in A[x] \setminus \{0\}$  (ovvero un polinomio non nullo)

IL MINIMO  $k \in \mathbb{N}$  :  $\forall n > k (a_n = 0)$  SI DICE GRADO

DI  $f$  SI DENOTEREMO CON  $gr(f)$

## 112 - Coefficiente direttore di un polinomio

SE  $f \in A[x] \setminus \{0\}$   $a_{gr(f)}$  SI DICE COEFFICIENTE

DIRETTORE DEL POLINOMIO E SI INDICA  $ed(f)$

## 113 - Grado e coefficiente direttore del polinomio nullo

$$ed(O) = 0$$

$$gr(O) = -\infty$$

## 114 - Polinomio monico

$f \in A[x]$  SI DICE POLINOMIO MONICO SE

$$ed(f) = 1_A$$

CIOÈ IL COEFFICIENTE DIRETTORE È L'UNITÀ  
DELL'ANGOLLO

## 115 - Somma e prodotto di polinomi (come successioni)

DEFINIAMO LA SOMMA E IL PRODOTTO DI POLINOMI:

SIANO  $(a_m)_{m \in \mathbb{N}}$ ,  $(b_m)_{m \in \mathbb{N}} \in A[\mathbf{x}]$  DUE POLINOMI. ALLORA

$$(a_m)_{m \in \mathbb{N}} + (b_m)_{m \in \mathbb{N}} = (a_m + b_m) \quad (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

$$(a_m)_{m \in \mathbb{N}} \cdot (b_m)_{m \in \mathbb{N}} = \sum_{i+j=m} a_i \cdot b_j \quad (a_1 \cdot (b_1, \dots, b_m), a_2 \cdot (b_2, \dots, b_m), \dots, a_n \cdot (b_1, \dots, b_m))$$

## 116 - Anello dei polinomi

DEFINITA ANCHE LA SOMMA E IL PRODOTTO POSSIAMO DIRE CHE  
L'INSIEME  $A[\mathbf{x}]$  DEFINITO SU UN ANELLO COMMUTATIVO UNITARIO  
E' A SUA VOLTA UN ANELLO. L'ANELLO DEI POLINOMI DI A.

- L'ELEMENTO NEUTRO DELLA SOMMA E'  $(0, 0, 0, 0, \dots)$  (NULLO)
- L'ELEMENTO NEUTRO DEL PRODOTTO E'  $(1, 0, 0, 0, \dots)$

## 117 - Polinomio costante

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

ALLORA IL POLINOMIO  $(\alpha, 0, 0, 0, \dots)$  SI DICE POLINOMIO COSTANTE.

VOLENDO POSSIAMO DIRE CHE  $\alpha = (\alpha, 0, 0, 0, \dots)$  O WERU

INDI CHIAMO IL POLINOMIO COSTANTE CON IL COEFFICIENTE.

## 118 - Polinomio incognita

DEFINIAMO IL POLINOMIO

$x = (0, 1_A, 0, 0, \dots)$  COME POLINOMIO INCOGNITA

## 119 - Potenze del polinomio incognita

$x = (0, 1_A, 0, 0, \dots)$

$x^2 = (0, 0, 1_A, 0, 0, \dots)$

$\vdots$

$x^m = (0, 0, 0, \dots (m VOLTE), 1_A, 0, \dots)$

## 120 - Monomio

DATO UN ANELLO  $(A, +, \cdot)$  E SIA  $\alpha \in A$  E SIA  $x = (0, 1_A, 0, 0, \dots)$   
ALLORA

$$\alpha x^m = (\alpha, 0, 0, 0, \dots) \cdot (0, 0, (m \text{ volte}), 1_A, 0, 0, \dots) = (0, 0, (m \text{ volte}), \alpha, 0, 0)$$

IL MONOMIO  $\alpha x^m$  E` QUINDI IL POLINOMIO CON TUTTI COEFFICIENTI NULLI TRAMONTE QUELLO IN POSIZIONE  $m+1$  CHE HA VALORE  $\alpha$ .

ESEMPIO:  $3x^4 = (0, 0, 0, 0, 3)$

Coeff.       $\downarrow$        $\downarrow$        $\downarrow$        $\downarrow$        $\downarrow$   
 $x^0$        $x^1$        $x^2$        $x^3$        $x^4$

## 121 - Scrivere un polinomio come somma di monomi

SIA  $f$  UN POLINOMIO E SIA  $m = \text{gr}(f)$  E

$$f = (\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_m, 0, 0, \dots)$$

POSSIAMO SCRIVERE  $f$  COME

$$f = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \dots + \alpha_m x^m$$

## 122 - Proprietà somma e prodotto di polinomi

SIANO  $f, g \in A[x]$ ,  $m = \text{gr}(f)$ ,  $n = \text{gr}(g)$ ,  $M = \max\{m, n\}$

ALLORA

$$f + g = \sum_{i=0}^M (a_i + b_i) x^i$$

$$f \cdot g = \sum_{i=0}^{m+n} \left( \sum_{j=0}^i a_j b_{i-j} \right) x^i$$

## 123 - Proprietà del grado della somma di polinomi

SIANO  $f, g \in A[x] \setminus \{0\}$

ALLORA

$$\text{SE } \text{gr}(f) = \text{gr}(g) \wedge \text{ed}(f) = -\text{ed}(g) \rightarrow \text{gr}(f+g) < \text{gr}(f) = \text{gr}(g)$$

$f = x^3 + g \rightarrow$  IL GRADO DELLA SOMMA E` PIU' PICCOLO  
 $g = -x^3 + x - 2$  DEL GRADO DI  $f$  E  $g$  (CHE HANNO LO STESSO  
GRADO)

$$\text{SE } \text{gr}(f) \neq \text{gr}(g) \vee \text{ed}(f) \neq \text{ed}(g) \rightarrow \text{gr}(f+g) = \max\{\text{gr}(f), \text{gr}(g)\}$$

$f = x^4 + 2$  OPPURE  $f = x^4$   $\rightarrow$  IL GRADO DELLA SOMMA E` IL GRADO PIU' ALTO  
 $g = x^2 + 1$                      $g = -3x^4$                     TRA  $f$  E  $g$

## 124 - Proprietà del prodotto di polinomi (PROPRIETÀ ADDIZIONE GRADI)

SIANO  $f, g \in A[x] \setminus \{0\}$

ALLORA

$$\text{SE } \text{ed}(f) \cdot \text{ed}(g) = 0 \rightarrow \text{gr}(f \cdot g) < \text{gr}(f) + \text{gr}(g)$$

SIAMO IN  $\mathbb{Z}_5$

$$f = 5x^6 + 3$$

$$g = 3x^2$$

IL GRADO DEL POLINOMIO RISULTANTE DAL PRODOTTO  
 $(15x^6 + 3x^2)$  CHE IN  $\mathbb{Z}_5$  È UGUALE A  $(9x^2)$   
 È PIÙ PICCOLO DEL GRADO DI  $f(g)$  + GRADO  
 DI  $g(2) = 6$ . INFATTI  $2 < 6$

$$\text{SE } \text{ed}(f) \cdot \text{ed}(g) \neq 0 \rightarrow \text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g) \wedge \text{ed}(f \cdot g) = \text{ed}(f) \cdot \text{ed}(g)$$

$$f = x^5 + 7$$

$$g = 3x$$

IL GRADO DEL POLINOMIO RISULTANTE DAL PRODOTTO  
 $(3x^6 + 21x)$  È UGUALE ALLA SOMMA DEL GRADO DI  $f(g)$   
 PIÙ IL GRADO DI  $g(1)$ . INFATTI  $6+1 = 6$  È INOLTRE  
 IL ED DEL POLINOMIO RISULTANTE (3) È UGUALE  
 AL PRODOTTO DEL ED( $f$ ) · ED( $g$ ). INFATTI  $3 \cdot 1 = 3$   
 E  $3 = 3$

## 125 - Coefficiente direttore cancellabile implica polinomio cancellabile

SIA  $f \in A[x] \setminus \{0\}$  SE  $\text{ed}(f)$  È CANCELLABILE ALLORA ANCHE  $f$

LO È. PER  $f$  VALE LA LEGGE DI ADDIZIONE DEI GRADI.

## 125 - Dimostrazione

ESSENDO  $\text{ed}(f)$  CANCELLABILE VUOL DIRE CHE ESSENTE NON È DIVISORE DELLO ZERO QUINDI VIENE A CADERE LA 1° PROPRIETÀ DEL PRODOTTO DI POLINOMI E VALE LA LEGGE DI ADDIZIONE DEI GRADI.

ALLORA

$$\forall g \in A[x] \neq 0$$

$$\text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g) \neq 0$$

QUINDI  $f$  NON È DIVISORE DELLO ZERO, ALLORA È CANCELLABILE

## 126 - Invertibilità del polinomio incognita

IL POLINOMIO  $x$  NON È MAI INVERTIBILE

## 126 - Dimostrazione

DATO CHE IL COEFFICIENTE DIRETTORE DI  $x$  È 1, L'UNITÀ DELL'ANELLO È SEMPRE CANCELLABILE. QUINDI  $A[x]$  NON È MAI UN CAMPO.

## 127 - Teorema della divisione lunga fra polinomio

SIA  $(A, +, \cdot)$  UN ANELLO COMMUTATIVO UNITARIO E SIANO  $f, g \in A[x]$

ALLORA

$$ed(g) \in U(A) \rightarrow \exists! (q, r) \in A[x] \times A[x] (f = gq + r \wedge gr(x) < gr(g))$$

Ovvvero se abbiamo 2 polinomi  $f \in g \in IL$   $ed(g) \in$  INVERTIBILE

ALLORA esistono 2 polinomi  $q$  (QUOTIENTE),  $r$  (RESTO) tali che

$f$  possa essere scritto come  $gq + r \in IL$  GRADO

DEL POLINOMIO  $r$  PIÙ PICCOLO DEL GRADO DEL POLINOMIO  $g$ .

### 127 - Dimostrazione

① DIMOSTRIAMO L'ESISTENZA DELLA COPPIA  $(q, r)$ .

PONIAMO  $m = gr(g)$ ,  $n = gr(f)$ . SE  $m < n$  ALLORA  $q=0$   $r=f$

SE  $m \geq n$  ( $ed(g) \neq 0$ ). PONGO  $a = ed(f)$  E  $b = ed(g)$

USIAMO INDUZIONE DI 2° FORMA SU  $n$ . PER IPOTESI DI  $ed(g)$  VALE

PONIAMO  $k = ab^{-1} \cdot x^{n-m} \cdot g$ . TRA  $ab^{-1}$ ,  $x^{n-m}$  E  $g$  VALE LA FORMULA DI

ADDITIONE DEI GRADI.

ALLORA  $gr(k) = gr(ab^{-1} \cdot x^{n-m}) + gr(g) = m$  POI IL  $ed(k) = a$

E PONIAMO  $h = f - k$

IL  $gr(h) < m$ . PER INDUZIONE  $\exists (q_1, r_1)$  ( $f - k = gq_1 + r_1$ )  $\wedge gr(r_1) < gr(g)$ .  
ALLORA:

$$f = gq_1 + r_1 + k = gq_1 + r_1 + ab^{-1} \cdot x^{n-m} \cdot g = g(q_1 + ab^{-1} \cdot x^{n-m}) + r_1$$

② DIMOSTRIAMO L'UNICITÀ DELLA COPPIA

SIANO  $(q_1, r_1), (q_2, r_2)$  DUE COPPIE.

$$\text{QUINDI } g(q_1 - q_2) = r_2 - r_1$$

$gr(r_2 - r_1) < gr(g) = m$ . VALE LA LEGGE DI ADDIZIONE DEI GRADI.

$$gr(r_2 - r_1) = gr(g) + gr(q_1 - q_2) = m + gr(q_1 - q_2) < m.$$

QUESTO È POSSIBILE SOLO SE  $gr(q_1 - q_2) < 0$  MAE  $q_1 - q_2 = 0$  ALLORA

$$q_1 = q_2 \wedge r_1 = r_2.$$

## 128 - Omomorfismo di sostituzione

SIA  $e \in A$  ANELLO COMMUTATIVO UNITARIO. ALLORA LA FUNZIONE

$$f \in A[x] \rightarrow f(e) \in A$$

E' UN OMOMORFISMO DI AVESSI DETTO OMOMORFISMO DI SOSTITUZIONE

## 129 - Applicazione polinomiale

SIA  $f \in A[x]$ . DEFINIAMO L'APPPLICAZIONE POLINOMIALE DI  $f$ :

$$\bar{f}: e \in A \rightarrow f(e) \in A$$

## 130 - Radice di un polinomio

SE  $f \in A[x]$ ,  $e \in A$ ,  $f(e) = 0_A$ , ALLORA E SI DICE RADICE (O SOLUZIONE) DEL POLINOMIO

## 131 - Applicazioni polinomiali di somme e prodotti

SIANO  $f, g \in A[x]$ , ALLORA

$$\overline{f+g}(e) = \bar{f}(e) + \bar{g}(e)$$

$$\overline{fg}(e) = \bar{f}(e) \cdot \bar{g}(e)$$

DA QUESTO DERIVA CHE SE E E' RADICE DI f ALLORA LO E' ANCHE DI fg E gf.

## 132 - Teorema del resto

SIA A UN ANELLO COMMUTATIVO UNITARIO. SIA  $f \in A[x]$  E CEA.

ALLORA  $f(e)$  E' IL RESTO DELLA DIVISIONE LUNGA TRA  $f \in (x-e)$ .

## 132 - Dimostrazione

ED  $(x-e) = 1$  CHE E' INVERTIBILE. ALLORA POSSIAMO FARE LA DIVISIONE LUNGA.

$f = (x-e)q + r \wedge q(x) < q(x-e)$ , MA  $q(x-e) = 1 \rightarrow q(x) = 0$   
POE'  $r$  E' UNA COSTANTE. ALLORA

$$f(e) = (e-e)q(e) + r(e) = 0 \cdot q(e) + \text{costante} = \text{costante}$$

### 133 - Teorema di Ruffini

SIA  $A$  UN ANELLO COMMUTATIVO UNITARIO,  $f \in A[x]$ ,  $c \in A$ . ALLORA

$c$  RADICE DI  $f \Leftrightarrow (x-c) | f$   
OPPURE

$$f(c) = 0 \Leftrightarrow \exists q \in A[x] \mid f = (x-c) \cdot q$$

### 134 - Teorema di Ruffini generalizzato

SIA  $A$  UN DOMINIO D'INTEGRITÀ. SIA  $f \in A[x]$  E  $c_1, \dots, c_m \in A$ .  
ALLORA

$c_1, \dots, c_m$  RADICI DI  $f \Leftrightarrow \prod_{i=1}^m (x-c_i) | f$

### 134 - Dimostrazione

→) DIMOSTRIAMO PER INDUZIONE SU  $m$  (CHE E' IL NUMERO DI RADICI  $c_1, \dots, c_m$ )

SE  $m = 1$ , LA TESI E' OVVIA PERCHÉ E' PROPRIO RUFFINI.

SUPPONIAMO  $m > 1$  E IPOTIZZIAMO LA TESI VERA PER  $m-1$ .

$f(c_m) = 0$  PER IPOTESI.

RUFFINI DICE  $(x-c_m) | f \rightarrow f = (x-c_m) \cdot g$ .

SE PRENDO  $1 \leq i < m \rightarrow g(c_i) = (c_i - c_m) \cdot g(c_i)$ .

SIAMO IN UN DOMINIO DI INTEGRITÀ, SAPPIAMO  $g(c_i) = 0$  E  $c_i - c_m \neq 0$

QUINDI PER LA LEGGE DI ANNULLAMENTO DEL PRODOTTO,  $g(c_i) = 0$ .

QUINDI TUTTI I  $c_i$  SONO RADICI DI  $g$ . ALLORA.

$$f = (x-c_m) \cdot g = \prod_{i=1}^m (x-c_i) \cdot h$$

CHE IMPLICA

$$\prod_{i=1}^m (x-c_i) | f$$

CHE E' LA TESI

$$\leftarrow) \text{ SE } \prod_{i=1}^m (x-c_i) | f \rightarrow \exists h \in A[x] (f = h \cdot \prod_{i=1}^m (x-c_i))$$

$$f(c_m) = h \cdot [(c_m - c_1) \cdot (c_m - c_2) \cdot \dots \cdot (c_m - c_i) \cdot \dots \cdot (c_m - c_m)] = 0$$

CHE E' LA TESI

### 135 - Numero di radici in un dominio di integrità

SIA  $A$  UN DOMINIO DI INTEGRITÀ,  $f \in A[x]$  E SIANO  $c_1, \dots, c_m$  RADICI DI  $f$ .

ALLORA

$$m \leq \text{gr}(f)$$

CIOE' IL NUMERO DELLE RADICI È MINORE O UGUALE DEL GRADO  
DEL POLINOMIO

#### 135 - Dimostrazione

SIA  $\varphi = \prod_{i=1}^m (x - c_i)$ .

PER RUFFINI GENERALIZZATO  $\exists h \in A[x] (f = h\varphi)$ .

MA  $A$  È DOMINIO DI INTEGRITÀ E  $\varphi \neq 0$ , QUINDI VALE

$$\text{gr}(f) = \text{gr}(\varphi) + \text{gr}(h) \geq \text{gr}(\varphi) = m$$

PERCHE'  $\varphi$  È IL PRODOTTO DI GRADO 1

### 136 - Rappresentante monico di un polinomio

SIA  $A$  UN CAMPO E  $f \in A[x] \setminus \{0\}$ .

ALLORA

$$\text{ASSOC}(f) = \{u \in A \setminus \{0\} \mid f = u \cdot \text{mon}(f)\}$$

ALLORA PER OGNI  $f$  NON NULLO ESISTE ED È UNICO UN  
POLINOMIO MONICO ASSOCIAZIATO AD  $f$ . TALE POLINOMIO SI DICE  
RAPPRESENTANTE MONICO DELLA CLASSE DI  $f$ .

### 137 - Criterio di irriducibilità di polinomi su un campo

SIA  $A$  UN CAMPO, E SIA  $f \in A[x] \setminus \{0\}$  E PONIAMO  $\text{gr}(f) = m$   
 ALLORA,  $f$  È IRRIDUCIBILE SE E SOLTANTE SE

- ①  $\forall g, h \in A[x] (f = gh \rightarrow \text{gr}(g) = m \oplus \text{gr}(h) = m)$
- ②  $\forall g, h \in A[x] (f = gh \rightarrow \text{gr}(g) = 0 \vee \text{gr}(h) = 0)$  (E COSTANTI)

### 137 - Dimostrazione

$\leftarrow$ ) GLI INVERTIBILI DI  $A[x]$  SONO GLI STESSI DI  $A$ . CIOÈ I POLINOMI COSTANTI.

SE  $m = \text{gr}(f) > 0$  NON È COSTANTE QUINDI  $f \notin U(A[x])$ .

SE  $f = gh$ , ALLORA PER (1) DICO  $\text{gr}(g) = m$  E PER LA FORMULA DI ADDIZIONE DEI GRADI  $\text{gr}(h) = 0 \rightarrow h \in U(A[x]) \rightarrow f$  HA SOLO DIVISORI BANALI.

$\rightarrow$ )  $f$  È IRRIDUCIBILE QUINDI  $f \notin U(A[x]) = U(A) \in \text{DIV}(f) = \text{BDIV}(f)$ .

$A$  È CAMPO QUINDI  $U(A) = A \setminus \{0\}$  E  $\text{gr}(f) > 0$ .

$f$  HA SOLO DIVISORI BANALI ED ESSENDO OGNI VALORE DI  $A$  INVERTIBILE ALLORA ANCHE CANCELLABILE.

$f$  HA COEFFICIENTE DIRETTORE CANCELLABILE QUINDI  $f$  CANCELLABILE.

$$\text{BDIV} = \left\{ u f \mid u \in A \setminus \{0\} \right\} \cup \left( A \setminus \{0\} \right)$$

### 138 - Irriducibilità di polinomi in un Dominio di integrità

SIA  $A$  UN DOMINIO DI INTEGRITÀ E  $g(x) \in A[x]$ .

SE  $\text{gr}(f) > 1$  E HA RADICI  
 ALLORA  $f$  È IRRIDUCIBILE

### 139 - Irriducibilità di polinomi di 2° e 3° grado su un campo

UN POLINOMIO DI 2° E 3° GRADO SU UN CAMPO È  
 IRREDUCIBILE SOLO SE NON HA RADICI IN  $A$

A CAMPO QUALESiasi

- 1)  $\delta(f)=1 \Rightarrow f$  irriducibile
- 2)  $\delta(f) > 1$ :  $f$  irriducibile  $\Rightarrow f$  privo di radici (non vale  $\Leftarrow$ )
- 3)  $\delta(f)=2 \vee \delta(f)=3$ :  $f$  irriducibile  $\Leftrightarrow f$  privo di radici

CAMPO R

$f$  irriducibile  $\Leftrightarrow \delta(f)=1 \vee (\delta(f)=2 \wedge \Delta < 0)$

$$f = ax^2 + bx + c \Rightarrow \Delta = b^2 - 4ac$$

CAMPO Q

Sia  $f = a_0 + a_1x + \dots + a_mx^m \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$  e  $a_m \neq 0$

Criterio di Eisenstein -  $f$  irriducibile

$\exists p = \text{numero primo tale che}$ :

- $p \nmid a_m$
- $p \mid a_0, a_1, a_2, \dots, a_{m-1}$
- $p^2 \nmid a_0$

CONSEGUENZA

TUTTI I POLINOMI

DEL TIPO

$(x^m - p)$  SONO

IRRIDUCIBILI IN  $\mathbb{Q}[x]$

141 - Radici di un polinomio di grado maggiore di 3 su un campo

SE UN POLINOMIO DI GRADO 3 SU UN CAMPO A E'

IRRIDUCIBILE ALLORA NON HA RADICI IN A

142 - Irriducibilità di polinomi reali

Ogni polinomio irriducibile di  $\mathbb{R}[x]$  ha grado minore di 3

143 - Teorema di bolzano

Ogni polinomio su  $\mathbb{R}[x]$  di grado dispari ha una radice in  $\mathbb{R}$

144 - Grafo semplice

Sia  $V \neq \emptyset$  e  $\rho$  una relazione simmetrica e antiriflessiva su  $V$ . Allora

LA COPPIA  $(V, \rho)$  SI DICE GRAFO SEMPLICE

SI PUÒ ANCHE SCRIVERE COME COPPIA DI INSIEMI

$(V, \ell)$  DOVE  $\ell$  E' :

$$\ell \subseteq \wp_2(V) = \{\{x, y\} \subseteq \wp(V) \mid x \neq y\}$$

IL GRAFO SEMPLICE SI RAPPRESENTA COME PUNTI

UNITI DA LINEE O CURVE.

IL GRAFO SI DICE SEMPLICE PERCHÉ FRA 2 VERTICI C'È

PRESA UNA SINGOLA CONNESSIONE. (CONNESSIONE A DOPPIO SENSO). COSA INVECE DIVERSA NEI MULTIGRAFI.

## 145 - Multigrafo

UNA TERNA DI INSIEMI NON VUOTI  $(V, \mathcal{L}, \sigma)$  SI DICE MULTIGRAFO SE LA FUNZIONE SIGMA E' DEL TIPO

$$\sigma: \mathcal{L} \rightarrow P_2(V)$$

LA FUNZIONE CI ASSOCIA AD OGNI GRAFO L'EFFECTIVA COPPIA ORDINATA DI VERTICI CHE ESSO CONNETTE.

VUOL DIRE CHE POSSONO ESISTERE PIÙ LATI CHE CONNETTONO GLI STESSI VERTICI.

GLI ARCHI INOLTRE SONO A SENSO UNICO IN QUANTO SE ABBIANO 2 VERTICI DOBBIAMO SPECIFICARE SE UN LATO VA DA A  $\rightarrow$  B O DA B  $\rightarrow$  A.

## 146 - Sottografo

UN SOTTOGRAFO SEMPLICE  $(V, \mathcal{L})$  E' UNA COPPIA  $(V_1, \mathcal{L}_1)$  TALE CHE  $V_1 \subseteq V$  E  $\mathcal{L}_1 \subseteq \mathcal{L}$ , PERO' SE PRENDO PARTI A CASO DI  $V \in \mathcal{L}$  NON OTTENGO UN SOTTOGRAFO.

UN SOTTOGRAFO DI UN MULTIGRAFO  $(V, \mathcal{L}, \sigma)$  E' UNA TERNA  $(V_1, \mathcal{L}_1, \sigma_1)$  TALE CHE  $V_1 \subseteq V$  E  $\mathcal{L}_1 \subseteq \mathcal{L} \in \sigma_1 \in \sigma$  UNA RESTRIZIONE DI  $\sigma$ .

### 147 - Cammini

SIA  $G = (V, L, f)$  UN MULTIGRAFO E SIANO  $a, b \in V$   
 UN CAMMINO DA  $a \rightarrow b$  E' UNA SEQUENZA DI LATI  
 $(l_1, \dots, l_m)$  TALE CHE  $l_1 = \{a, x_1\}$ ,  $l_2 = \{x_1, x_2\}, \dots$   
 $l_m = \{x_{m+1}, b\}$ . INOLTRE NON CI SONO RIPETIZIONI.  
 SE  $a = b$ , IL CAMMINO SI CHIAMA CIRCUITO (ACCO).

DUE VERTICI  $a, b$  SI DICONO CONNESSI  $\Leftrightarrow a = b$  OPPURE ESISTE  
 UN CAMMINO DA  $a \rightarrow b$

LA RELAZIONE DI CONNESSIONE E' RIFLESSIVA, SIMMETRICA, TRANSITIVA.

### 148 - Grafo completo e complementare

SIA  $G = (V, L)$  UN GRAFO. UN GRAFO COMPLETO E'  
 UN GRAFO IN CUI  $L = P_2(V)$ .

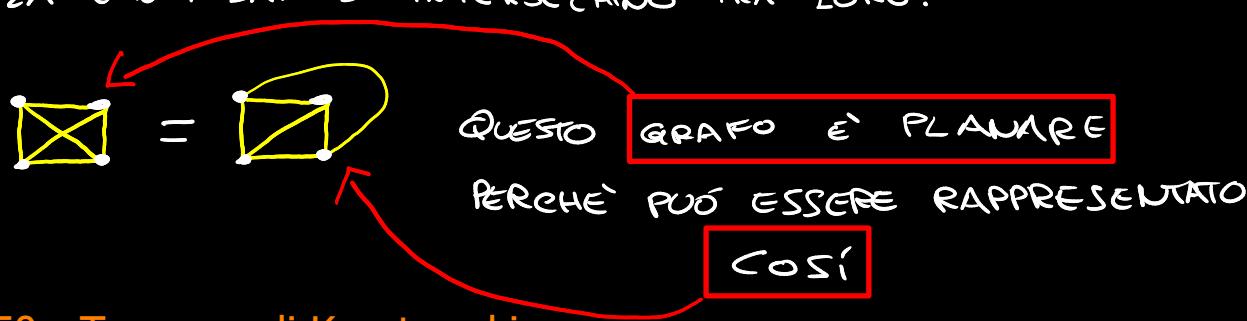
SE UN GRAFO HA  $m$  VERTICI, ESISTONO  $\binom{m}{2}$  GRAFI  
 COMPLETI CON  $m$  VERTICI.

ESEMPIO :

 SONO COMPLEMENTARI

### 149 - Grafi planari

UN GRAFO SI DICE PLANARE SE PUO' ESSERE RAPPRESENTATO  
 SENZA CHE I LATI SI INTERSECHINO TRA LORO.



### 150 - Teorema di Kuratowski

UN GRAFO E' PLANARE  $\Leftrightarrow$  NON HA SOTTOGRAFI ISOMORFI  
 A  $K_3$  E  $K_5$



## 151 - Cammino euleriano

UN CAMMINO EULERIANO FINITO SENZA CAPPI È UN CAMMINO CHE ATTRAVERSA TUTTI I LATI.

QUANDO c'è un cammino euleriano?

DEVE VERIFICARSI CHE:

- 1) ESISTE AL MASSIMO UNA COMPONENTE CONNESSA
- 2) IL NUMERO DI VERTICI CON GRADO DISPARI È 0

OPPURE 2:

- SE CI SONO ZERO VERTICI CON GRADO DISPARI, ALLORA ESISTE UN CIRCUITO EULERIANO.
- SE CI SONO DUE VERTICI CON GRADO DISPARI, ESISTONO CAMMINI EULERIANI CHE COMPRENDONO ENTRAMBI I VERTICI CON GRADO DISPARI.

## 152 - Alberi e foreste

UNA FORESTA È UN GRAFO IN EUI NON ESISTONO CIRCUITI (cicli). UNA FORESTA CONNESSA SI CHIAMA ALBERO

UN GRAFO È UNA FORESTA  $\Leftrightarrow$  SEELTI  $a, b \in G$  ESISTE O OPPURE 1 CAMMINO DA  $a - b$ .

UN GRAFO È UN ALBERO  $\Leftrightarrow$  SEELTI  $a, b \in G$  ESISTE PER FORZA 1 SOLO CAMMINO DA  $a - b$

### 153 - Lemma

IN OGNI MULTIGRAFO CONNESSO È SEMPRE POSSIBILE TROVARE UN SOTTOGRAFO CANCELLANDO DEI LATI IN MODO DA OTTENERE UN ALBERO.

QUINDI SIA  $G = (V, L, \ell)$  UN MULTIGRAFO CONNESSO. ALLORA  $G$  HA UN SOTTOALBERO MASSIMALE, OVVERO UN SOTTOGRAFO CON LO STESSO INSIEME DEI VERTICI DEL GRAFO ORIGINALE, E CHE SIA UN ALBERO.

### 153 - Dimostrazione

PARTIAMO DAL GRAFO



IL GRAFO È ANCORA CONNESSO.

SICCOME IN A È CAMMINO DA  $a \circ b$  ALLORA ESISTE ANCHE NEL SOTTOGRAFO.

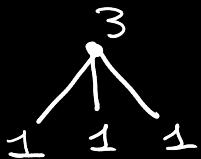
SE HO ELIMINATO IL CIRCUITO ALLORA HO UN SOTTOGRAFO MASSIMALE, ALTRIMENTI CONTINUO AD ELIMINARE I LATI.

### 154 - Teorema

SIA  $G = (V, L, \ell)$  UN MULTIGRAFO FINITO SENZA CAPPI.

ALLORA  $2|L| = \sum_{v \in V} d(v)$  DOVE  $d$  È IL GRADO DI  $v$ .

ESEMPIO :



$\sum_{v \in V} d(v) = 6$ , INFATTI CI SONO 3 LATI

### 154 - Dimostrazione

USIAMO IL METODO DEL DOPPIO CONTEGGIO:

SIA  $S = \{(v, l) \in V \times L \mid v \in \text{UN ESTREMO DI } L\}$

COUNTIAMO GLI ELEMENTI DI  $S$  CON UNA TABELLA

	$v_1$	$v_2$	... ...	$v_k$
$l_1$				
$l_2$	X			
$l_k$				

LE ERIOCETTE INDICANO SE  $v_i$  È UN ESTREMO DI  $l_j$ .

- SE COUNTO PER RIGHE, VISTO CHE OGNI LATO HA 2 ESTREMI, OGNI RIGA AVRÀ DUE X.

ALLORA  $|S| = 2L$

- SE COUNTO PER COLONNE, IN OGNI COLONNA CI SARANNO TANTE X QUANTO IL GRADO DI  $v$ .

ALLORA  $|S| = \sum_{v \in V} d(v)$ .

UNA CONSEGUENZA DEL TEOREMA È:

LA SOMMA DEI GRADI IN UN MULTIGRAFO È SEMPRE UN NUMERO PARI.

## 155 - Proprietà degli alberi

LA NOZIONE DI ALBERO È DIVERSA DALLA NOZIONE DI ALBERO CON RADICI.



QUESTA SI CHIAMA RAPPRESENTAZIONE RADICALE DELL'ALBERO.

IN UN ALBERO CON RADICI CHE ABBIA ALMENO 2 VERTICI,  
ESISTONO ALMENO DUE VERTICI CON GRADO 1.

I VERTICI DI GRADO 1 SI CHIAMANO FOGLIE.

SIA  $T = (V, L)$  UN ALBERO.

SE  $\ell \in L, v \in V \in \delta(v) = 1 \in v \in$  ADIACENTE A  $\ell$ , ALLORA  
IL GRAFO CHE OTTENGO CANCELLANDO  $v$  ED  $\ell$ .

$$(V/\{v\}, L/\{\ell\})$$

E' UN SOTTOALBERO.

SE INVECE  $\delta(v) > 1$  ALLORA NON OTTENGO UN ALBERO  
MA UNA FORESTA.

INFATTI:



$T = (V, L)$  UN ALBERO FINITO. ALLORA  $|V| = |L| + 1$

$F = (V, L)$  UNA FORESTA FINITA CON  $K$  COMPONENTI CONNESSE.

ALLORA  $|V| = |L| + K$

## CONSEQUENZE

SE  $G = (V, L, \ell)$  È UN MULTIGRAFO FINITO, SICCOME HA UN SOTTOALBERO MASSIMALE, IL NUMERO DEI LATI È  $|L| \geq |V| - 1$ . SE INVECE NON È CONNESSO, AVRA'  $|L| \geq |V| - k$ , SE K È IL NUMERO DELLE SUO COMPONENTI CONNESSE.

UN MULTIGRAFO CON K COMPONENTI CONNESSE È UNA FORESTA  $\iff |L| = |V| - k$

## 156 - Proprietà degli alberi

SIA  $G = (V, L)$  UN GRAFO FINITO. SONO EQUIVALENTI:

- 1)  $G$  È UN ALBERO
- 2)  $G$  È CONNESSO E  $|V| = |L| + 1$
- 3)  $G$  È UNA FORESTA E  $|V| = |L| + 1$

**THE END**