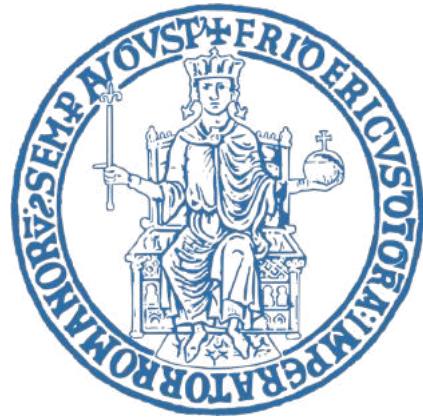


UNIVERSITA' DEGLI STUDI DI NAPOLI "FEDERICO II"
Scuola Politecnica e delle scienze di base
Dipartimento di Ingegneria Elettrica e delle Tecnologie
dell'Informazione



Appunti di
Algebra

Di

Alessia Marasco

• PREMESSÉ

Ogni teoria matematica è espressa in un **linguaggio**, costituito da:

- ↳ **ALFABETO DI SIMBOLI**, che possono essere uniti per formare stringhe di caratteri;
- ↳ **REGOLE SINTATICHE**, che permettono di distinguere tra stringhe:

$$1+1 < 0$$

$$1+1 < 3$$

CORRETTAMENTE COMPOSTE (FORMULE)

NON CORRETTAMENTE COMPOSTE

Come possiamo notare dal primo esempio quindi la sintesi prevede dall'interpretazione logica dei simboli; di questo aspetto invece si occupa la **SEMANTICA**. Analizzando semanticamente una formula è possibile, se si tratta di formule chiuse, attribuirvi un valore di verità nell'immediato; queste formule chiuse prendono anche il nome di **PROPOSIZIONI** (formule chiuse).

- | | | | |
|------|---|---|--|
| [es] | $0 < 1$ formula VERA $1 < 0$ formula FALSA | } | proposizioni (sono attribuibili un valore di verità) |
|------|---|---|--|

• CONNESSIONI PROPOSIZIONALI

Tra i simboli del linguaggio sono presenti i cosiddetti **SIMBOLI LOGICI**, che permettono di creare formule più complesse, tra cui appunto i connettivi proposizionali!

Le variabili p e q rappresentano proposizioni che vengono chiamate **VARIABILI PROPOSIZIONALI**; le formule costituite da variabili e connettivi proposizionali, e parentesi, prendono il nome di **FORME PROPOSIZIONALI**.

↳ **NEGAZIONE (NOT)**: ha come argomento una sola formula (connettivo **UNARIO**) e invertire il valore di verità del suo argomento.

↳ **CONGIUNZIONE (AND)**: è un connettivo **BINARIO**, ed è una proposizione vera se e solo se entrambi i suoi argomenti sono veri.

↳ **DISGIUNZIONE INCLUSIVA (OR)**: falsa solo quando entrambe sono false.

↳ **DISGIUNZIONE ESCLUSIVA (XOR)**: sarà sola se p o q sono vere, MA NON ENTRAMBE.

↳ **DOPPIA IMPLICAZIONE (SE E SOLO SE)**: è un'equivalenza; è vera se hanno lo stesso valore di verità,

↳ **IMPLICAZIONE (IF)**:

- se p è vero, non può essere che q sia falso;
- se p è falso, l'implicazione è sempre vera.

| p | q | $\neg p$ | $p \wedge q$ | $p \vee q$ | $p \oplus q$ | $p \Leftrightarrow q$ | $p \Rightarrow q$ |
|-----|-----|----------|--------------|------------|--------------|-----------------------|-------------------|
| V | V | F | V | V | F | V | V |
| V | F | F | F | V | V | F | F |
| F | V | V | F | V | V | F | V |
| F | F | V | F | F | F | V | V |

P.S: la tavola di verità di una forma proposizionale con un numero k di variabili richiede 2^k righe.

• TAUTOLOGIE

Si dice che una forma proposizionale è una **tautologia** se il suo valore di verità è sempre vero, indipendentemente dai valori attribuiti alle variabili.

Dualmente esistono forme proposizionali il cui valore di verità è sempre falso, e queste prendono il nome di **contraddizioni**.

Due forme proposizionali si dicono **LOGICAMENTE EQUIVALENTI** se e solo se le forme $\alpha \Leftrightarrow \beta$ è una tautologia. Se α appare come parte di una forma proposizionale è possibile quindi sostituirle con β e ottenere lo stesso valore di verità.

(es) $p \Leftrightarrow \neg(\neg p)$; se trovo $\neg(\neg p)$ posso sostituirlo con p . (**LEGGE DOPPIA NEGAZIONE**)

↳ ALCUNE TAUTOLOGIE ELEMENTARI

IDE MPOTENZA

$$(p \wedge p) \Leftrightarrow p$$

$$(p \vee p) \Leftrightarrow p$$

COMUTATIVITÀ

$$(p \wedge q) \Leftrightarrow (q \wedge p)$$

$$(p \vee q) \Leftrightarrow (q \vee p)$$

$$(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$$

$$(p \text{XOR } q) \Leftrightarrow (q \text{XOR } p)$$

ASSOCIAZIVITÀ

$$((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$$

$$((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$$

$$((p \Leftrightarrow q) \Leftrightarrow r) \Leftrightarrow (p \Leftrightarrow (q \Leftrightarrow r))$$

$$((p \text{XOR } q) \text{XOR } r) \Leftrightarrow (p \text{XOR } (q \text{XOR } r))$$

DISTRIBUTIVITÀ

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$$

$$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$$

DE MORGAN

$$\neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$$

$$\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$$

↳ TAUTOLOGIE DELL'IMPLICAZIONE

$$(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$$

$$(p \Rightarrow q) \Leftrightarrow ((\neg p) \vee q)$$

$$(p \Rightarrow q) \Leftrightarrow ((\neg q) \Rightarrow (\neg p))$$

$$(\neg(p \Rightarrow q)) \Leftrightarrow (p \wedge (\neg q))$$

$$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$$

DOPPIA IMPLICAZIONE
IN LOGICHE DISGIUNZIONE
CONTROAPPOSIZIONE
NEGAZIONE
TRANSITIVITÀ

↳ TAUTOLOGIE DELLO XOR

$$(\neg(p \Leftrightarrow q)) \Leftrightarrow ((\neg p) \Leftrightarrow q) \Leftrightarrow (p \Leftrightarrow (\neg q)) \Leftrightarrow (p \text{XOR } q)$$

$$(p \wedge (q \text{XOR } r)) \Leftrightarrow ((p \wedge q) \text{XOR } (p \wedge r))$$

NEGAZIONE EQUIVALENZA
DISTRIBUTIVITÀ

• QUANTIFICATORI

↳ QUANTIFICAZIONE UNIVERSALE $\forall \varphi(x)$ \Rightarrow afferma che $\varphi(x)$ è vera;

↳ QUANTIFICAZIONE ESISTENZIALE $\exists \varphi(x)$ \Rightarrow afferma almeno una tra le $\varphi(x)$;
 $\exists ! x (\varphi(x)) \Leftrightarrow \exists x (\forall y (\varphi(y) \Leftrightarrow y = x))$ \Rightarrow solo un valore lo rende vero.

↳ VARIABILI LIBERE E VINCOLATE

Quando una variabile x non è introdotta da un quantificatore si dice che le sue occorrenze all'interno di una formula sono **occorrenze LIBERE**, altrimenti **VINCOLATE** al "campo d'azione" espresso dalle frontiere del quantificatore.

(es) $\forall x (x > 1 \wedge x \leq y) \wedge (x \neq y)$

O vincolate o libere

Definiamo quindi una **FORMULA CHIUSA** se a solo se non contiene variabili con occorrenza libera, poiché in questo caso le formule non potrebbe avere un valore di verità.

OSSERVAZIONE: quando applico una sostituzione, questa opera solo nelle occorrenze libere delle variabili. Ad esempio osserviamo che:

- $\varphi : \forall x(x > y) \quad \varphi(0) : \forall 0(0 > y)$ non ha senso;
- $\varphi : x > 1 \Rightarrow \varphi(3) : 3 > 1$;
- $\varphi : \forall x(x > 1) \Rightarrow \varphi(3) = \varphi(x)$ perché non ci sono occorrenze libere;
- $\varphi : \forall x(x > 1) \wedge x > 7 \Rightarrow \varphi(3) = \forall x(x > 1) \wedge 3 > 7$;

Un **PREDICATO UNARIO** nelle variabile x è una formula che non contiene occorrenze libere di altre variabili diverse da x .

• QUANTIFICATORI RISTRETTI

I quantificatori possono esser accompagnati da una condizione che limita l'ambiente in cui la variabile può assumere i suoi valori.

$(\forall x \in S)(\varphi)$ abbreviazione di $\forall x(x \in S \Rightarrow \varphi(x))$

$(\exists x \in S)(\varphi)$ abbreviazione di $\exists x(x \in S \wedge \varphi(x))$

L> QUANTIFICATORI MULITPLI

$$\forall x(\forall y(\forall z(\dots))) \Leftrightarrow \forall y(\forall z(\forall x(\dots))) \Leftrightarrow \forall x,y,z(\dots)$$

$$\exists x(\exists y(\exists z(\dots))) \Leftrightarrow \exists y(\exists z(\exists x(\dots))) \Leftrightarrow \exists x,y,z(\dots)$$

Se però i quantificatori si mescolano:

$$\exists y(\forall x(\varphi)) \Rightarrow \forall x(\exists y(\varphi)) \quad \text{Non è ammesso il risparmio}$$

$\forall x(\varphi(x)) \Rightarrow \exists x(\varphi(x))$
 È sempre vero, almeno due quantificatori NON sono ristretti, in quel caso potrebbe essere falso (ad esempio se $S = \emptyset$ è falso)



L> NEGAZIONI

$$\neg(\forall x(\varphi)) \Leftrightarrow (\exists x(\neg\varphi))$$

$$\neg(\forall x \in S)(\varphi) \Rightarrow (\exists x \in S)(\neg\varphi)$$

$$\neg(\exists x(\varphi)) \Leftrightarrow (\forall x(\neg\varphi))$$

$$\neg(\exists x \in S)(\varphi) \Rightarrow (\forall x \in S)(\neg\varphi)$$

• INSIEMI

Una definizione di insieme non viene data, ma sono caratterizzati dagli elementi che li appartengono secondo l'**ASSIOMA DI ESTENSIONALITÀ**: $\forall A, B (A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B))$

Sia $\varphi = \varphi(x)$ un predicato unario nelle variabile x , si indica con $\{x \mid \varphi\}$ la totalità degli oggetti x che sostituiti a x , rendono φ vero. Questa totalità si chiama **ESTENSIONE** di φ , pensando ad φ come a una proprietà che un oggetto può o meno soddisfare, la sua estensione è la totalità degli oggetti che la soddisfano. Se avremmo di formare un insieme a partire dall'estensione di un predicato potremmo imbatterci in diverse contraddizioni; il modo per evitare ricavi di ottenere un insieme è quello di utilizzare l'estensione all'interno di un insieme S ; allora sicuramente otterriamo un insieme. Ce lo assicura l'**ASSIOMA DI SEPARAZIONE**: pren il predicato unario φ , l'estensione $\{x \mid (x \in S) \wedge \varphi(x)\}$ è un insieme, e gli indichiamo in simboli $\{x \in S \mid \varphi(x)\}$.

Vale l'equivalenza tra $A = \{x \mid \varphi(x)\}$ e $\forall x(x \in A \Leftrightarrow \varphi(x))$

↳ ALCUNE CONSEGUENZE

- Dall'assiomma di estensionalità abbiamo anche che: $A \subseteq B \Leftrightarrow \forall x (x \in A \Rightarrow x \in B)$
- Un'estensione di un predicato può anche non essere soddisfatta da nessun oggetto; in questo caso otteniamo la definizione di **INSIEME VUOTO**: $\exists \emptyset (\forall x (\neg(x \in \emptyset))) \Rightarrow \emptyset = \emptyset$
- Chiamiamo **SINGLETON** un insieme costituito da un solo elemento $\{x\}$.

ATTENZIONE!: $x \in \{x\}$, ma $x \neq \{x\}$ e $\emptyset \subseteq \{1, 2\}$, non $\emptyset \in \{1, 2\}$
infine $\{1, 2\} \subseteq \{1, 2\}$, ma $\{1, 2\} \neq \{1, 2\}$

L'**ASSIOMA DELL'UNIONE** ci garantisce che è sempre possibile fare l'unione di due insiemi per ottenere un insieme. Proprio per questo possiamo dimostrare che non esiste $\{x \mid \neg x\}$, ovvero l'estensione di una negazione di un predicato, perché ottenimenti, unendolo con $\{x \mid x\}$ otteniamo l'insieme di tutti gli insiemi che non esiste. Se però ci troviamo in un ambiente ristretto, per esempio, ad S è possibile ottenere una traduzione delle negazioni attraverso il **COMPLEMENTO**: per $A \subseteq S$, $S \setminus A = \{x \in S \mid x \notin A\}$

Vista la corrispondenza tra predicatori e insiemi, è possibile tradurre tutti i risultati che abbiamo ottenuto precedentemente per le teorie degli insiemi:

↳ LEGGI DI DE MORGAN

Sia $A \setminus B = \{x \mid x \in A \wedge x \notin B\} = \{x \in A \mid x \notin B\}$

per assorbiatività

$$\bullet A \setminus (B \cup C) = \{x \mid x \in A \wedge x \notin (B \cup C)\} = \{x \mid x \in A \wedge ((\neg B) \wedge (\neg C))\} = \{x \mid x \in A \wedge (\neg(B \wedge C))\}$$

se si trova una $\neg A$ si im
plica non comincia insieme

$$= \{x \mid x \in A \wedge x \in (\neg B) \wedge x \in (\neg C)\} = \{x \mid ((x \in A) \wedge (\neg B)) \wedge ((x \in A) \wedge (\neg C))\}$$

per assorbiatività
e commutatività

$$= \{x \mid x \in A \wedge (\neg B)\} \cap \{x \mid x \in A \wedge (\neg C)\} = (A \setminus B) \cap (A \setminus C)$$

$$\bullet A \setminus (B \cap C) = \{x \mid x \in A \wedge x \notin (B \cap C)\} = \{x \mid x \in A \wedge ((\neg B) \vee (\neg C))\}$$

per distributività

$$= \{x \mid x \in A \wedge (\neg B)\} \cup \{x \mid x \in A \wedge (\neg C)\} = (A \setminus B) \cup (A \setminus C)$$

• DIAGRAMMI DI EULERO-VENN

Sono delle rappresentazioni grafiche che agevolano le letture di alcuni insiemi; in particolare sono utili per dimostrazioni del tipo: $A, b, c (\dots = \dots)$
 $A, b, c (\dots \subseteq \dots)$.

Se ad esempio dobbiamo rappresentare un diagramma con tre insiemi $\{a, b, c\}$ dove essere rappresentato ogni parte dell'insieme $S = \{a, b, c\}$, ovvero le parti: $\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

• UNIONE E INTERSEZIONE

L'unione e l'intersezione non sono operazioni binarie, bensì unarie e le definiamo:

$\forall a \quad U_a = \{x \mid \exists y \in a (x \in y)\}$ $I_a = \{x \mid \forall y \in a (x \in y)\}$ per l'intersezione
l'insieme dove
essere NON VUOTO
[a ≠ ∅]

$\forall a, b \quad U\{a, b\} = \{x \mid \exists y \in \{a, b\} (x \in y)\} = \{x \mid x \in a \vee x \in b\} = a \cup b$

↳ OSSERVAZIONI:

$$\bullet U_b = \bigcup_{x \in b} x$$

$$\bullet a \cap (U_b) = \bigcup_{x \in b} (a \cap x)$$

$$a \cup (U_b) = \bigcap_{x \in b} (a \cup x) \quad b \neq \emptyset$$

- $(U_a) \cup (U_b) = \bigcup_{y \in a} (x \cup y) = \bigcup \{x \cup y \mid x \in a \wedge y \in b\}$
- $s \setminus U_a = \{x \in S \mid x \notin U_a\} = \{x \in S \mid \neg (\exists y \in a (x \in y))\} = \{x \in S \mid \forall y \in a (x \notin y)\} = \bigcap_{y \in a} (S \setminus y)$
- $s \setminus \bigcap_a = \bigcup_{y \in a} (s \setminus y)$

COPPIA ORDINATA

E' un termine binario con la seguente proprietà: $\forall a, b, c, d \quad (a, b) = (c, d) \Leftrightarrow (a = c \wedge b = d)$

è quindi definita da quelle che chiamiamo **PRIMA E SECONDA COORDINATA**, e a differenza degli insiemi, è fondamentale l'ordine in cui appaiono e le ripetizioni NON sono amminate.

\hookrightarrow **TERNA ORDINATA**: $(a, b, c) = (d, e, f) \Leftrightarrow ((a = d), (b = e), (c = f))$
semplice da dimostrare perché $(e, b, a) = ((e, b), a)$

PRODOTTO CARTESIANO

$$a \times b = \{(x, y) \mid x \in a \wedge y \in b\} \quad \forall a, b$$

ATTENZIONE: $a \times b \neq b \times a$; $a \times \emptyset = \emptyset$

CORRISPONDENZA

Siano a e b due insiemi; una corrispondenza da a a b è una terza ordinata (a, b, G) dove $G \subseteq a \times b$ è il GRAFICO. Per ogni $x \in a, y \in b$ si dice che y è un **CORRISPONDENTE** di x , rispetto a G , se e solo se $(x, y) \in G$.
Per descrivere in maniera immediata una corrispondenza poniamo subito:

| TABELLA | $\left\{ \begin{array}{ c c c } \hline & x & y \\ \hline 1 & \bullet & \bullet \\ 2 & & \\ 3 & & \bullet \\ \hline \end{array} \right\}$ | $G = \{(x, y) \in a \times b \mid \varphi(x, y)\}$ | FUNZIONE |
|---------|--|--|----------|
|---------|--|--|----------|

Una **RELAZIONE BINARIA** di un insieme è una corrispondenza binaria fra l'insieme e se stesso. Due corrispondenze α e β sono uguali se e solo se, dati: $\alpha = (a, b, G)$ $\beta = (c, d, G^*)$, allora $a = c \wedge b = d \wedge G = G^*$
Indichiamo $\text{Corr}(a, b) \Rightarrow \text{Corr}(a, a) = \text{Rel}(a)$

\hookrightarrow COMPOSIZIONE DI CORRISPONDENZE (PRODOTTO RELAZIONALE)

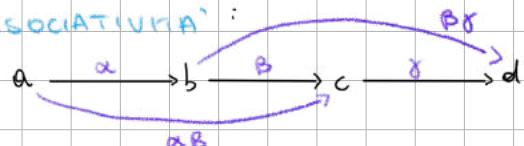
$$\alpha \in \text{Corr}(a, b) \quad \beta \in \text{Corr}(b, c)$$

$\alpha \beta \in \text{Corr}(a, c)$ è definita: $\forall x \in a, \forall z \in c \quad (x (\alpha \beta) z \Leftrightarrow \exists y \in b \quad (x \alpha y \wedge y \beta z))$

Una proprietà del prodotto relazionale è l'**ASSOCIAZIONE**:

$$\forall \alpha \in \text{Corr}(a, b), \beta \in \text{Corr}(b, c), \gamma \in \text{Corr}(c, d)$$

$$(\alpha \beta) \gamma = \alpha (\beta \gamma)$$



Dim) innanzitutto notiamo che i prodotti hanno stessi dominio (a) e codominio (d) dunque resta solo da dimostrare che hanno lo stesso grafico, ovvero che $\forall x \in a, \forall t \in d \quad (x (\alpha \beta) t \Leftrightarrow x \alpha (\beta t))$.

$$\underline{x (\alpha \beta) t \Leftrightarrow \exists z \in c \quad (x \alpha z \wedge z \beta t)} \Leftrightarrow \exists z \in c \quad (\exists y \in b \quad (x \alpha y \wedge y \beta z \wedge z \gamma t))$$

$$\underline{x \alpha (\beta t) \Leftrightarrow \exists y \in b \quad (\exists z \in c \quad (x \alpha y \wedge y \beta z \wedge z \gamma t))}$$

• APPLICAZIONI

Una applicazione f da a a b è una corrispondenza tale che $\forall x \in a \exists! y \in b (f(x) = y)$.
 Visto che ci tante numeri di corrispondenze è possibile fare la composizione di applicazioni: che resta a sua volta un'applicazione, ovvero $\forall \alpha \in \text{Map}(a, b), \forall \beta \in \text{Map}(b, c) \alpha \circ \beta \in \text{Map}(a, c)$. Nel campo delle applicazioni chiamiamo $\text{Map}(a, b)$ l'insieme di tutte le applicazioni da a a b , e $\alpha \circ \beta = \beta \circ \alpha$. L'unico corrispondente di x prende il nome di **IMMAGINE** di x .

Evvendo un'applicazione un particolare tipo di corrispondenza, anch'essa è definita da una terza ordinaria $(a, b, \{(x, y(x)) \mid x \in a \wedge y(x) \in b\})$

L'APPLICAZIONI COSTANTI

Pinotto?

$f: a \rightarrow b$ è costante se e solo se $\forall x \in a (f(x) = f(y))$; ad esempio $x \in a \mapsto b$

L'APPLICAZIONE IDENTICA: $\text{id}_a : x \in a \mapsto x \in a$

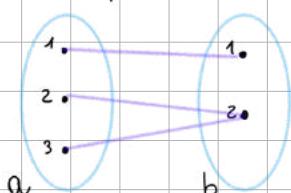
L'APPLICAZIONE COMPOSTA:

$\forall a, b, c (\forall \alpha \in \text{Map}(a, b), \forall \beta \in \text{Map}(b, c) \Rightarrow \beta \circ \alpha \in \text{Map}(a, c))$ $\beta \circ \alpha(x) = \beta(\alpha(x))$

• IMMERSIONI E RESTRIZIONI

$\forall b \subseteq a x \in b \mapsto x \in a$ è un'altra applicazione identica, ma non uguale alla precedente perché $(a, a, G) \neq (b, a, G)$, e prende il nome di **IMMERSIONE** di b in a . $\forall f \in \text{Map}(a, c), f|_b : x \in b \mapsto f(x) \in c$ è la **RESTRIZIONE** di f a b . Praticamente l'immersione è di un insieme e riguarda le sole applicazioni identiche, mentre la restrizione è di una qualunque funzione. Possiamo quindi dire che l'immersione è una restrizione di id_a a b .

(es)



$$b = \{1, 2\} \subseteq a = \{1, 2, 3\}$$

$$\text{id}_b = f|_b \quad (\text{immersione} = \text{restrizione})$$

diciamo che f è un **PROLUNGAMENTO** di id_b ad a

• IMMAGINE DI f E SURIETTIVITÀ

$f: a \rightarrow b, \text{im}(f) = \{f(x) \mid x \in a\} \subseteq b$; quest'oggetto ci permette di dare una definizione:
 f è **SURIETTIVA** $\Leftrightarrow \text{im}(f) = b \Leftrightarrow b \subseteq \text{im}(f) \Leftrightarrow \forall y \in b \exists x \in a (y = f(x)) \Leftrightarrow$

Da cui la NEGAZIONE di suriettività:
 $\exists y \in b \forall x \in a (y \neq f(x))$



L'COMPOSIZIONE DI FUNZIONI SURIETTIVE

$$f: a \rightarrow b \quad g: b \rightarrow c$$

• f e g iniettive $\Rightarrow g \circ f$ iniettiva $a \rightarrow c$

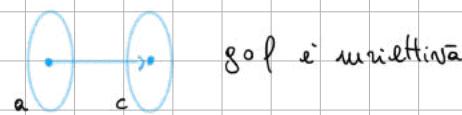
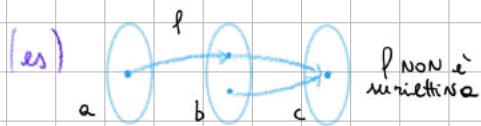
Dim) iniettivo: $\forall z \in c (\exists x \in a ((g \circ f)(x) = z))$. Fissiamo una $z \in c$; poiché g è iniettiva $\exists y \in b (g(y) = z)$. Visto che non rappresenta di quanti elementi può avere * immagine, fissiamo $y \in b$; poiché f è iniettiva $\exists x \in a (y = f(x))$. Analogamente a prima, fissiamo x , allora $(g \circ f)(x) = g(f(x)) = g(y) = z$



(*): non è detto che l'applicazione sia iniettiva, allora magari $z = g(y) = g(y')$, allora ne fissiamo 1

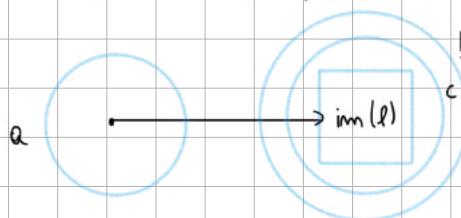
• $g \circ f$ suriettiva $\Rightarrow g$ suriettiva

Dim) obiettivo: $\forall z \in c (\exists y \in b (z = g(y)))$. Per ipotesi $\forall z \in c (\exists x \in a (z = (g \circ f)(x)))$, cioè $z = g(f(x))$. Posto $y = f(x)$ allora $z = g(y)$.



↳ APPLICAZIONE RIDOTTA

$f: a \rightarrow b$, $\forall c \in \mathcal{P}(b) (\text{im}(f) \subseteq c) \Rightarrow \forall x \in a \rightarrow f(x) \in c$. Questa descrizione è l'applicazione ridotta de f a c , può essere indicata con \overline{f} , e viene spesso usata con lo scopo di rendere le funzioni di partenza suriettive.



↳ in questo caso $\text{im}(f) = c$
e la chiamiamo RIDOTTA
ALL'IMMAGINE

• APPLICAZIONE IMMAGINE E ANTIIMMAGINE

$$\overline{f}: \mathcal{P}(a) \rightarrow \mathcal{P}(b)$$

$$x \mapsto \{f(t) \mid t \in x\} = \text{im}(f|_x)$$

$$\overleftarrow{f}: \mathcal{P}(b) \rightarrow \mathcal{P}(a)$$

$$y \mapsto \{t \in a \mid f(t) \in y\}$$

} IMMAGINE di f

} ANTIIMMAGINE di f

ATTENZIONE!
 $\overline{f}(\overline{f}(\overline{x})) \neq x$
 $\overline{f}(\{1,2,3\}) = \{x,y\}$
 $\overline{f}(\{x,y\}) = \{1,2,3\}$
 $\overline{f}(\overline{f}(\{1,2,3\})) = \{1,2,3\}$



↳ OSSERVAZIONI

$$\textcircled{1} \quad \overline{f}(\emptyset) = \emptyset = \overline{f}(\{\emptyset\})$$

$$\textcircled{2} \quad \overline{f}(\{x\}) = \text{im}(f)$$

$$\textcircled{3} \quad \overline{f}(\{b\}) = a = \overline{f}(\text{im}(f))$$

$$\textcircled{4} \quad x \subseteq y \subseteq a \Rightarrow \overline{f}(x) \subseteq \overline{f}(y)$$

$$x \subseteq y \subseteq b \Rightarrow \overleftarrow{f}(x) \subseteq \overleftarrow{f}(y)$$

$$\textcircled{5} \quad \forall t \in a (\overline{f}(\{t\}) = \{f(t)\})$$

$$\textcircled{6} \quad \forall y \in b (\overline{f}(\{y\}) = \{t \in a \mid f(t) \in \{y\}\} = \{t \in a \mid f(t) = y\})$$

$$\textcircled{7} \quad f \text{ è SURIETTIVA} \Leftrightarrow \forall y \in b (\overleftarrow{f}(\{y\}) \neq \emptyset)$$

$$\forall y \in b (y \in \text{im}(f) \Leftrightarrow \overleftarrow{f}(\{y\}) \neq \emptyset)$$

$$\textcircled{8} \quad \forall x \in \mathcal{P}(a) (x \subseteq \overline{f}(\overline{f}(x)))$$

$$\forall t \in x \quad f(t) \in \overline{f}(x) \quad \text{perché } t \in \overleftarrow{f}(\overline{f}(x)) = \{s \in a \mid f(s) \in \overline{f}(x)\}$$

• INIEZIONE

f è INIEZIONE se e solo se $\forall x, y \in a (x \neq y \Rightarrow f(x) \neq f(y))$, equivalente a:

$\forall x, y \in a (f(x) = f(y) \Rightarrow x = y)$ o ancora $\forall y \in b (|\overleftarrow{f}(\{y\})| \leq 1)$ → cardinalità



NEGAZIONE INIEZIONE:

$$\exists x, y \in a (x \neq y \wedge f(x) = f(y))$$

L> COMPOSIZIONE DI FUNZIONI INIETTIVE

- f e g iniettive $\Rightarrow g \circ f$ iniettiva

Dim) obiettivo: $\forall x, y \in a \quad ((g \circ f)(x) = (g \circ f)(y) \Rightarrow x = y)$, analizzando la prima parte $g(f(x)) = g(f(y))$, visto che g è iniettiva $\Rightarrow f(x) = f(y)$, ma ugualmente f è iniettiva $\Rightarrow x = y$.

- $g \circ f$ iniettiva $\Rightarrow f$ iniettiva

Dim) se $x \neq y \Rightarrow (g \circ f)(x) \neq (g \circ f)(y)$, cioè $g(f(x)) \neq g(f(y))$, e cioè $f(x) \neq f(y)$.
→ questa è un'implicazione logica, visto che in una funzione ogni elemento ha un'unica immagine, se esse sono diverse, anche gli elementi sono distinti.

• BIETTIVITÀ

Un'applicazione biettiva è una funzione contemporaneamente iniettiva ($\forall y \in b \quad (\exists x \in a \quad (y = f(x)))$) e suriettiva ($\forall y \in b \quad (\exists x \in a \quad f(x) = y)$), ovvero per ogni elemento del codominio esiste uno, e un unico elemento del dominio tale che $f(x) = y$ ($\forall y \in b \quad (\exists x \in a \quad y = f(x))$)

L> COMPOSIZIONE DI FUNZIONI BIETTIVE

- f e g biettive $\Rightarrow g \circ f$ biettiva;
- $g \circ f$ biettiva $\Rightarrow g$ suriettiva e f iniettiva;

• PROPRIETÀ DELLA COMPOSIZIONE DI APPLICAZIONI

① Per il prodotto relazionale vale l'associetività, il che può dire:

$$(f \circ g) \circ h = f \circ (g \circ h) \Leftrightarrow h \circ (g \circ f) = (h \circ g) \circ f$$

② $a \xrightarrow{\text{id}_a} a \xrightarrow{f} b \xrightarrow{\text{id}_b} b \quad f \in \text{corr}(a, b) \quad \sigma = \text{id}_a \circ f = f \circ \text{id}_b = f$

Dim) $\forall x \in a, \forall y \in b \quad x \circ y \Leftrightarrow \exists t \in a \quad (x \circ t \wedge t \circ y)$, ma siccome necessariamente $t = x$, allora $x \circ y \Rightarrow \sigma = f$.

Analogamente vale $\sigma = f(\text{id}_b) = \text{id}_b \circ f = f$.

③ Previ $f: a \rightarrow b$ e $g: b \rightarrow a$, se $g \circ f = \text{id}_a$ diciamo che:

↳ f è una **SEZIONE** di g ;

↳ g è una **RETRAZIONE** di f ;

Visto che l'identità è una funzione biettiva $\Rightarrow f$ iniettiva e g suriettiva. Inoltre è equivalente a dire:

$$g \circ f = \text{id}_a \Leftrightarrow \forall x \in a \quad ((g \circ f)(x) = x) \Leftrightarrow \forall x \in a \quad (g(f(x)) = x) \Leftrightarrow \forall x \in a \quad (f(x) \in \overleftarrow{g}(\{x\})).$$

L> TEORIA

① g suriettiva $\Leftrightarrow g$ ha una retziona

$$f: a \longrightarrow b \quad g \circ f = \text{id}_a$$

② f iniettiva $\Leftrightarrow f$ ha una retrazionc, oppure $a = \emptyset$

$$g: b \longrightarrow a \quad f \circ g = \text{id}_b$$

Dim 1) \Leftrightarrow verificato precedentemente (*)

Dim 2) Sia $g: b \rightarrow a$ suriettiva, cioè $\forall x \in a \quad (\exists y \in b \quad x = g(y))$; allora $\forall x \in a \quad (\overleftarrow{g}(\{x\}) \neq \emptyset)$. Allora $\forall x$ fissa una $y_x \in \overleftarrow{g}(\{x\})$, considerando l'applicazione $f: x \in a \mapsto y_x \in b$ allora posso dire che f è una retziona di g (*).

Dimm 2) se f ha una retrozione, abbiamo già dimostrato l'implicazione precedentemente, se $a = \emptyset$, allora $f: a \rightarrow b$ è sicuramente iniettiva.

\Rightarrow Se f è iniettiva $\Rightarrow \forall y \in b (\lvert \{x \mid f(x) = y\} \rvert \leq 1) \Rightarrow \forall y \in \text{im}(f) (\exists! x_y \in a (f(x_y) = y))$.

Fisso un arbitrario $c \in a$ e considero:

$$g: y \in b \mapsto \begin{cases} x_y, & \text{se } y \in \text{im}(f) \\ c, & \text{se } y \notin \text{im}(f) \end{cases}$$

Allora $g \circ f = \text{id}_a$ perché $\forall x \in a (g(f(x)) = g(f(x)) \in \text{im}g)$, ovvero x è l'unico elemento di a la cui immagine mediante f sia $f(x)$. *

• APPLICAZIONE INVERSA

Prendiamo la funzione $f: a \rightarrow b$, g è un'inversa di f se e solo se g è una retzione e una retrozione di f , cioè se $g: b \rightarrow a$, e $g \circ f = \text{id}_b$ e $f \circ g = \text{id}_a$.

↳ TEOREMA

Sia $f: a \rightarrow b$ un'applicazione, se f ha una retzione r e una retrozione s , allora $s = r$. Aggiungiamo che di conseguenza:

- s è l'unica retzione di f ;
- s è l'unica retrozione di f ;
- s è l'unica inversa di f .

Dimm)

$$\begin{array}{ccccccc} & & \text{id}_b & & & & \\ b & \xrightarrow{s} & a & \xrightarrow{f} & b & \xrightarrow{r} & a \\ & \text{id}_a & & & \text{id}_b & & \end{array} \quad f \circ s = \text{id}_b \quad r \circ f = \text{id}_a$$

$s = \text{id}_a \circ s = (r \circ f) \circ s = r \circ (f \circ s) = r \circ \text{id}_b = r$ (uso proprietà associativa)

Per dimostrare la prima conseguenza (unicità retzione) supponiamo per antros che esiste un'altra retzione t ; allora abbiamo dimostrato che retzione e retrozione coincidono $\Rightarrow t = r$, ma $s = r \Rightarrow t = s$. *

↳ TEOREMA

Sia $f: a \rightarrow b$ applicazione, sono equivalenti le seguenti affermazioni:

- ① f è biettiva;
 - ② f ha una retzione e una retrozione;
 - ③ f ha un'inversa;
 - ④ f ha esattamente una retzione;
 - ⑤ $\forall y \in b (\exists! x \in a (f(x) = y))$.
-) per definizione di retzione (iniettiva) e retrozione (suriettiva)
) definizione
) teorema precedente

Dimm) 4 \Rightarrow 5 Se f ha una retzione $\Rightarrow f$ è iniettiva $\Rightarrow \forall y \in b (\exists! x \in a (f(x) = y))$, ma se un $y \in b$ ammette due elementi distinti $x_1, x_2 \in a$ tali che $f(x_1) = y = f(x_2)$, allora f dovrebbe avere almeno due retzioni, ma da manca y in x_1 e l'altra in x_2 . (f \circ s = \text{id}_b) *

OSSERVAZIONE: sia a un singleton, se $|b| > 1$; allora esiste un'applicazione iniettiva $f: a \rightarrow b$ e questa ha una retrozione. Ma $|\text{Map}(b, a)| = 1$, ovvero esiste una sola applicazione $b \rightarrow a$, ovvero quella $y \in b \rightarrow x \in a$, dove $a = \{x\}$.

• OPERAZIONE BINARIA

Sia S un insieme, un'operazione binaria im S è un'applicazione $S \times S \rightarrow S$.

Se $*: S \times S \rightarrow S$ è un'operazione binaria, $\forall a, b \in S$ si scrive $a * b$ per intendere $*((a, b))$, e $T(a) = \text{Map}(a, a)$ si chiama insieme delle TRASFORMAZIONI di a .

Sia $*$ un'operazione binaria, si dice che:

↳ $*$ è COMMUTATIVA $\Leftrightarrow \forall x, y \in S (x * y = y * x)$,

↳ $*$ è ASSOCIAUTIVA $\Leftrightarrow \forall x, y, z \in S ((x * (y * z)) = ((x * y) * z))$,

Se l'operazione è associativa, la struttura algebrica $(S, *)$ è un SEMIGRUPPO.

↳ ELEMENTO NEUTRO

$(S, *)$, $*: S \times S \rightarrow S$, $\forall t \in S$:

↳ t è neutro a sinistra rispetto a $*$ $\Leftrightarrow \forall x \in S (t * x = x)$;

↳ t è neutro a destra rispetto a $*$ $\Leftrightarrow \forall x \in S (x * t = x)$;

t è NEUTRO se è neutro sia a destra che a sinistra $\Leftrightarrow \forall x \in S (t * x = x = x * t)$

TEOREMA (unicità del neutro)

Sia $*$ un'operazione binaria nell'insieme a , e siano s un neutro a sinistra e d un neutro a destra in $(a, *)$. Allora $s = d$, ovvero s è l'unico elemento neutro a sx e dx, ovvero l'unico neutro.

Dim) $\forall x \in a$ ① $s * x = x$ $\Rightarrow d \stackrel{\textcircled{1}}{=} s * d \stackrel{\textcircled{3}}{=} s$
 ② $x * d = x$



Siamo a un insieme a e $*: a \times a \rightarrow a$ un'operazione binaria im a . Si definisce $*^{\text{op}}: (x, y) \in a \times a \mapsto y * x \in a$ l'OPERAZIONE OPPOSTA di $*$.

↳ $*$ è commutativa $\Leftrightarrow *^{\text{op}} = *$;

↳ $*$ è associativa $\Leftrightarrow *^{\text{op}}$ è associativa;

perché $((x *^{\text{op}} y) *^{\text{op}} z) = (z * (y * x)) = ((z * y) * x) = (x *^{\text{op}} (y *^{\text{op}} z))$

↳ t è neutro in $(a, *)$ \Leftrightarrow è neutro in $(a, *^{\text{op}})$

• MONOIDÈ

Un monoidè è una struttura algebrica $(S, *, t)$ im cui:

↳ $*$ è associativa;

↳ ammette elemento neutro;

↳ ELEMENTI SIMMETRICI

Siamo $*: a \times a \rightarrow a$ e supponiamo che $(a, *)$ abbia elemento neutro. $\forall x, y \in a$:

↳ y è simmetrico sx di x in $(a, *)$ $\Leftrightarrow y * x = t$;

↳ y è simmetrico dx di x in $(a, *)$ $\Leftrightarrow x * y = t$;

y è simmetrico \Leftrightarrow è simmetrico sx e dx $\Leftrightarrow y * x = t = x * y$. In questo caso si dice che x è SIMMETRIZABILE (ovvero si ha simmetria).

L'elemento neutro è sempre simmetrizzabile perché è il simmetrico di se stesso.

TEOREMA (unicità del simmetrico)

Sia $(\alpha, *, t)$ un monoidale, sia $x \in \alpha$. Siano s un simmetrico su x e d un simmetrico di x in $(\alpha, *, t)$. Allora $s = d$.

$$\text{Dim: } \begin{cases} s * x = t \\ x * d = t \end{cases} \Rightarrow d = t * d = (s * x) * d = s * (x * d) = s * t = s$$

Siamo $(\alpha, *)$, $b \subseteq \alpha$. Diciamo che b è CHIUSO rispetto a $*$ $\Leftrightarrow \forall x, y \in b \quad (x * y \in b)$

Se b è chiuso posso definire $\cdot : (x, y) \in b \times b \rightarrow x * y \in b$, che chiameremo OPERAZIONE INDOTTA da $*$ in b (moltiplicazione di $*$ ridotta alle sue immagini).

• GRUPPI

Un gruppo è un monoidale in cui tutti gli elementi sono invertibili. Un gruppo ABELIANO è un gruppo in cui l'operazione è anche COMUTATIVA.

$(M, *, t)$ monoidale, $U(M) = \{x \in M \mid x \text{ è invertibile}\}$

$(U(M), *, t) \rightarrow$ GRUPPO DEGLI INVERTIBILI di $(M, *, t)$.

↳ PROPRIETÀ DEL GRUPPO DEGLI INVERTIBILI

① Se $\forall x \in U(M)$ indichiamo con x' il simmetrico di x in M , allora $\forall x, y \in U(M) \quad (x * y \in U(M) \wedge ((x * y)' = y' * x'))$.

Dim: Dovo dimostrare che $\forall x, y \in U(M) \quad (x * y) * (y' * x') = t = [y' * x'] * (x * y)$

↳ per associazività: $((x * y) * y') * x' = (x * (y * y')) * x' = (x + t) * x' = x * x' = t$.

↳ //: $((y' * x') * x) * y = (y' + (x' * x)) * y = (y' * t) * y = y' * y = t$.

② $U(M)$ è chiuso in $(M, *) \quad \Rightarrow U(M)$ sotto monoidale di $(M, *, t)$

③ $t \in U(M) \quad \Rightarrow (U(M), *)$ è un gruppo



• SOTTONOIDALE

$(M, *, t)$ monoidale; $H \subseteq M \quad (L, *_L, t)$ è un sottonomoidale di M se:

↳ L è chiuso rispetto a $*$;

↳ $t \in L$.

Con $*_L$ operazione indotta in L da $*$, avrò $\forall a, b \in L \quad (a *_L b = a * b)$

• SOTTOGRUPPO

$(G, *, ', t)$, com $' : x \in G \mapsto x' \in G$

$H \subseteq G$, H costituisce un sottogruppo di $(G, *, ', t)$ se e solo se:

↳ H è chiuso rispetto a $*$;

↳ $t \in H$;

↳ $\forall x \in H \quad (x' \in H)$.

$$\Leftrightarrow H \neq \emptyset \wedge \forall x, y \in H \quad (x * y') \in H$$

Dim: \Leftarrow ovvia, perché $\forall x, y \in H \quad (x', y' \in H)$ quindi $x * y' \in H$ l'operazione si chiude

$\Leftarrow \exists a \in H$, finito $a \in H$, $t = a * a' \in H$

$\forall x \in H \quad x' = t * x' \in H$

$\forall x, y \in H \quad y' \in H \Rightarrow x * y' \in H$



$U(T(a), \circ, \text{id}_a) = \{l \in T(a) \mid l \text{ è biettiva}\} \rightarrow$ insieme delle PERMUTAZIONI di a , ovvero l'insieme delle trasformazioni biettive di a .
 $= \text{Sym}(a)$ GRUPPO SIMMETRICO di a .

• TAVOLE DI CAYLEY

$(S, *) \quad * : S \times S \rightarrow S$, sia $S = \{x, y, z, \dots\}$

| | x | y | z |
|---|---------|---------|---------|
| x | $x * x$ | $x * y$ | $x * z$ |
| y | $y * x$ | $y * y$ | $y * z$ |
| z | $z * x$ | $z * y$ | $z * z$ |

↳ Commutatività: simmetria rispetto alla diagonale.
 ↳ simmetricabile: elemento neutro nelle celle.
 ↳ neutro a dx: se la colonna corrispondente è uguale agli elementi delle righe.

• ELEMENTI CANCELLABILI

Siano $* : S \times S \rightarrow S$, $a \in S$:

↳ $\sigma_a : x \in S \mapsto a * x \in S$ la TRASLAZIONE SIMMETRICA A SINISTRA

↳ $\delta_a : x \in S \mapsto x * a \in S$ la TRASLAZIONE SIMMETRICA A DESTRA

Diciamo che:

- a è cancellabile a sx in $(S, *) \Leftrightarrow \sigma_a$ è iniettiva
- a è cancellabile a dx in $(S, *) \Leftrightarrow \delta_a$ è iniettiva
- a è cancellabile in $(S, *) \Leftrightarrow$ è cancellabile a dx e a sx.

Allora a non è cancellabile \Leftrightarrow
 $\exists x, y \in S \ (x * a = y * a \wedge x \neq y)$



OVVERO: $\forall x, y \in S \ (a * x = a * y \Rightarrow x = y)$
 $\forall x, y \in S \ (x * a = y * a \Rightarrow x = y)$

OSSERVAZIONE: l'elemento neutro è sempre cancellabile.

↳ TEOREMA

Sia $(S, *, t)$ un monoidale e sia $a \in S$,

- a è simmetricabile a dx $\Rightarrow a$ cancellabile a dx;
- a è simmetricabile a sx $\Rightarrow a$ cancellabile a sx;
- a è simmetricabile $\Rightarrow a$ cancellabile;

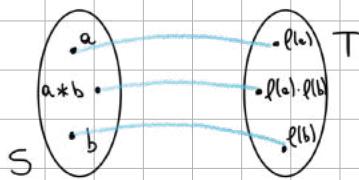
Dim) Sia a simm. a sx $\Rightarrow \exists a' \in S \ (a' * a = t)$. Allora $\forall x, y \in S, a * x = a * y$
 $\Rightarrow a' * (a * x) = a' * (a * y) \Rightarrow (a' * a) * x = (a' * a) * y \Rightarrow t * x = t * y \Rightarrow x = y$

Dimostrazione analoga per cancellabilità a dx.

• OMOMORFISMO

Siano $(S, *)$ e (T, \cdot) strutture algebriche, con $*$ e \cdot operazioni binarie.

Un'applicazione $f: S \rightarrow T$ è un omomorfismo da $(S, *)$ a (T, \cdot) se e solo se:
 $\forall x, y \in S (f(x * y) = f(x) \cdot f(y))$, ossia se f conserva le operazioni.



Un omomorfismo biettivo
si dice ISOMORFISMO

Se $f: (S, *) \rightarrow (T, \cdot)$ è un ISOMORFISMO SURGETTIVO siamo:

① Se $*$ è commutativa $\Rightarrow \cdot$ è commutativa.

Dim) $\forall x, y \in T (\exists a, b \in S (x = f(a) \wedge y = f(b)))$

se $*$ è commutativa $\Rightarrow a * b = b * a \Rightarrow f(a * b) = f(b * a)$; per def. di omomorfismo
 $\Rightarrow f(a * b) = f(a) \cdot f(b) \Rightarrow f(a) \cdot f(b) = f(b) \cdot f(a) \Rightarrow x \cdot y = y \cdot x \Rightarrow \cdot$ è commutativa
 $f(b * a) = f(b) \cdot f(a)$

② Se $*$ è associativa $\Rightarrow \cdot$ è associativa.

Dim) $\forall x, y, z \in T (\exists a, b, c \in S (f(a) = x \wedge f(b) = y \wedge f(c) = z))$

$*$ associativa $\Rightarrow a * (b * c) = (a * b) * c \Rightarrow f(a * (b * c)) = f((a * b) * c)$

$\Rightarrow f(a * (b * c)) = f(a) \cdot (f(b) \cdot f(c)) \Rightarrow x \cdot y \cdot z = (x \cdot y) \cdot z \Rightarrow \cdot$ associativa
 $f((a * b) * c) = (f(a) \cdot f(b)) * f(c)$

③ Sia $t \in S$; allora se t è neutro a sx im $(S, *) \Rightarrow f(t)$ è neutro a sx im (T, \cdot) .

Dim) per ipotesi $\forall y \in T (\exists b \in S (f(b) = y))$

$\forall a \in S (t * a = a) \Rightarrow f(t * b) = f(b) = y$; per def. omomorfismo

$f(t * b) = f(t) \cdot f(b) = f(t) \cdot y = y \Rightarrow f(t)$ neutro a sx.

Analogamente se t è neutro a dx im $(S, *) \Rightarrow f(t)$ neutro a dx im (T, \cdot) .

④ Siano $a, b \in S$ e assumiamo che S abbia neutro: se a è simmetrico a sx di b im $(S, *) \Rightarrow f(a)$ è simmetrico di $f(b)$ im (T, \cdot) .

Dim) $\forall x, y \in T (\exists a, b \in S (f(a) = x \wedge f(b) = y)) \rightarrow$ per teorema precedente i neutri im (T, \cdot)

per ipotesi $a + b = t \Rightarrow f(a + b) = f(t) \Rightarrow f(a) \cdot f(b) = x \cdot y = f(t)$

da proposizione i analoge per la simmetria a dx.

Se $f: (S, *) \rightarrow (T, \cdot)$ è un ISOMORFISMO (biettivo) siamo anche:

① $\forall a \in S$, a cancellabile a sx im $(S, *) \Rightarrow f(a)$ cancellabile a sx im (T, \cdot) .

Dim) Voglio dimostrare che: $\forall x, y \in T f(a) \cdot x = f(a) \cdot y \Rightarrow x = y$

Visto che f è biettiva posso scrivere: $f(f(a) \cdot f(l^{-1}(x))) = f(a) \cdot f(l^{-1}(y))$, che per definizione di omomorfismo equivale a $f(a * l^{-1}(x)) = f(a * l^{-1}(y))$.

Poiché f è, nello specifico, anche biettiva $\Rightarrow a * f^{-1}(x) = a * f^{-1}(y)$, e visto che a è cancellabile a sinistra $\Rightarrow f^{-1}(x) = f^{-1}(y) \Rightarrow x = y$.

La dimostrazione è equivalente per le cancellabilità a dx.

e) $f: (S, *) \rightarrow (T, \cdot)$ isomorfismo $\Leftrightarrow f^{-1}: (T, \cdot) \rightarrow (S, *)$ isomorfismo.

Dim) Se f è un isomorfismo si dimostra che f^{-1} è biettiva, dico dimostrazione
Per x, y ($f^{-1}(x \cdot y) = f^{-1}(x) * f^{-1}(y)$). Visto che f è biettiva, applica f :
 $\Leftrightarrow f(f^{-1}(x \cdot y)) = f(f^{-1}(x) * f^{-1}(y)) \Leftrightarrow (x \cdot y) = f(f^{-1}(x) * f^{-1}(y)) \Leftrightarrow$
 $(x \cdot y) = f(f^{-1}(x)) \cdot f(f^{-1}(y)) = x \cdot y$ OK!



Quando ci ha un isomorfismo tra due strutture, le proprietà algebriche di una valgono anche per l'altra.

* **TEOREMA:** tutti i gruppi di due elementi sono sempre isomorfi (nelle righe e nelle colonne delle tavole di Cayley non ci sono ripetizioni). In generale tutti i gruppi sono isomorfi se la loro cardinalità è un numero primo.

↳ **PROPOSIZIONE:** se $|a| > 2$, $(\text{Symm}(a), \circ)$ non è commutativo.

Dim) Siamo x, y, z tre elementi distinti di a ; allora:

$$\alpha \in \text{Symm}(a) \quad \alpha(x) \mapsto y, \alpha(y) \mapsto x, \forall t \in a \setminus \{x, y\} (\alpha(t) = t)$$

$$\beta \in \text{Symm}(a) \quad \beta(y) \mapsto z, \beta(z) \mapsto y, \forall t \in a \setminus \{y, z\} (\beta(t) = t)$$

$$(\alpha \circ \beta)(x) = \alpha(\beta(x)) = \alpha(x) = y \Rightarrow \alpha \circ \beta \neq \beta \circ \alpha$$

$$(\beta \circ \alpha)(x) = \beta(\alpha(x)) = \beta(y) = z$$



Sia (S, \cdot) un semigruppo, $x \in S$. Definiamo la POTENZA x^m :

① $\forall m \in \mathbb{N}^* \quad (x^m = x \cdot x \cdot \dots \cdot x) \rightarrow m \text{ volte}$

② Se (S, \cdot, t) è un monoido, $x^0 = t$;

③ Se x è invertibile (con simmetrico x'), $\forall m \in \mathbb{N}^*$ poniamo:

$$x^{-m} = (x')^m = x' \cdot x' \cdot \dots \cdot x'; \text{ il cui simmetrico è a } m \text{ volte } x^m$$

In maniera formale, se $x^1 = x$, $\forall m \in \mathbb{N}^* \quad x^{m+1} = x^m \cdot x$ e $x^1 = x^{-1}$. $\forall x \in S$, $\forall m, n \in \mathbb{Z}$, le potenze che appaiono sono definite:

$$\hookrightarrow x^{m+n} = x^m \cdot x^n;$$

$$\hookrightarrow (x^m)^n = x^{m \cdot n};$$

Se avremo assunto le nozioni sopraite:

$$\hookrightarrow mx = x+x+\dots+x;$$

$$\hookrightarrow 0x = t;$$

$$\hookrightarrow m(x') = (-m)x;$$

$$\hookrightarrow m(mx) = (mm)x;$$

PROPOSIZIONE: $(S, *)$, sia $\mathcal{J} \subseteq \mathcal{P}(S)$ e $\mathcal{J} \neq \emptyset$. Allora vale che $\forall T \in \mathcal{J}$ (T chiuso rispetto a $*$) $\Rightarrow \bigcap \mathcal{J}$ è chiuso.

Dim) $\forall T \in \mathcal{J} (a, b \in T) \Rightarrow a * b \in T$, con $a, b \in \mathcal{J}$

$$\forall T \in \mathcal{J} (a+b \in T) \Rightarrow a+b \in \bigcap \mathcal{J}$$

$$\bigcap \mathcal{J} = \{x \mid \forall T \in \mathcal{J} (x \in T)\}$$

PROPOSIZIONE: sia $X \subseteq S$ e sia $A = \{T \in S \mid x \subseteq T \wedge T \text{ chiuso rispetto a } *\}$. Allora sicuramente $S \in A \Rightarrow A \neq \emptyset$, dunque $\bigcap A$ è chiuso rispetto a $*$, contiene $X \Leftrightarrow \bigcap A \in A$

Dim) $\bigcap A$ è il più piccolo elemento di A rispetto all'inclusione (il minimo), oppure è equivalente dire che è la più piccola parte chiusa $(S, *)$ contiene X . $X = \bigcap A \Leftrightarrow X$ è chiuso.

$\bigcap A = [x]$ parte chiusa generata da X in $(S, *)$

FATTORIALE

$$\forall m \in \mathbb{N} \quad m! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot m = \prod_{i=1}^m i$$

$$\boxed{0! = 1}$$

FATTORIALE DISCENDENTE

$$\forall m, n \in \mathbb{N} \quad m^{\underline{n}} = m(m-1)(m-2) \dots (m-n+1)$$

$$m \leq n \Rightarrow m^{\underline{n}} = \frac{m!}{(m-n)!}$$

$$\text{e } m > n \Rightarrow m^{\underline{n}} = 0$$

• COMBINATORIA

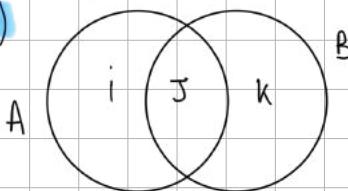
Siamo A e B insiemi finiti

$$\hookrightarrow |A \times B| = |A| \cdot |B|$$

Dim) $\forall x \in A$ esistono esattamente $|B|$ elementi in $A \times B$ che abbiano x come prima cond.

$$\hookrightarrow |A \cup B| = |A| + |B| - |A \cap B|, \text{ se non sono disgiunti;}$$

Dim)



$$i = |A \setminus B| \quad j = |A \cap B| \quad k = |B \setminus A|$$

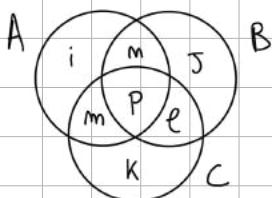
$$|A| = i + j \quad \Rightarrow |A| + |B| - |A \cap B| = i + j + k + p - j = i + j + k = |A \cup B|$$

$$|B| = j + k$$



Per tre insiemi A, B, C finiti e non disgiunti vale invece:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$



$$|A| = i + m + n + p$$

$$|B| = j + e + m + p$$

$$|C| = k + e + m + p$$

$$(i + m + n + p) + (-e + m + p) + (k + e + m + p) -$$

$$-(m + p) - (m + e) - (e + p) + p$$

$$= i + j + m + k + e + m + p = |A \cup B \cup C|$$



→ PRINCIPIO DI INCLUSIONE-UNIONE (caso generale)

Sia S un insieme finito di insiemi finiti; posto $m = |S|$, si ha:

$$|\cup S| = \sum_{i=1}^m (1-1)^{i+1} \sum_{T \in \mathcal{P}_i(S)} |\cap T|, \text{ con } \mathcal{P}_i(S) = \{x \subseteq S \mid |x|=i\}$$

(es) $m = 3$

$$i=1 \rightarrow |A| + |B| + |C| \quad T \in \mathcal{P}_1(S) \quad T \in \mathcal{P}_1(S)$$

$$i=2 \rightarrow -|A \cap B| - |A \cap C| - |B \cap C| \quad T \in \mathcal{P}_2(S)$$

$$i=3 \rightarrow +|A \cap B \cap C| \quad T \in \mathcal{P}_3(S)$$

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

Dim) Poniamo $m = |A|$ e $A = \{a_1, a_2, \dots, a_m\}$

$a_1 \mapsto$ abbiamo $|B|$ scelte per l'immagine di a_1

$a_2 \mapsto$ abbiamo $|B|$ scelte per l'immagine di a_2

:

$a_m \mapsto$ abbiamo $|B|$ scelte per l'immagine di a_m

$$|\text{Map}(A, B)| = \underbrace{|B| \cdot |B| \cdots |B|}_{m=|A|}$$



OSSERVAZIONE:

- Se $A = \emptyset \Rightarrow |\text{Map}(A, B)| = |B|^{|A|} = |B|^0 = 1$
- Se $B = A = \emptyset \Rightarrow |\text{Map}(A, B)| = 0^0 = 1 = \{\text{id}_{\emptyset}\}$
- Se $A \neq \emptyset \wedge B = \emptyset \Rightarrow |\text{Map}(A, B)| = 0^{|A|} = ? = \emptyset (*)$

$$\hookrightarrow |\mathcal{I}_{m,j}^n \text{Map}(A, B)| = |B|^{|\mathbb{A}|}$$

Dim) $a_1 \mapsto |B|$ possibili scelte;

$a_2 \mapsto |B|-1$ scelte;

:

$a_m \mapsto ?$ ci troviamo di fronte a due possibili casi:

① $|A| \leq |B|$, procediamo con l'enumerazione delle immagini fino ad ottenere $|B| - (m-1)$ possibili scelte per l'immagine di a_m . Allora:

$$|\mathcal{I}_{m,j}^n \text{Map}(A, B)| = |B| \cdot (|B|-1) \cdot (|B|-2) \dots (|B|-|A|+1) = |B|^{|\mathbb{A}|}$$

② $|A| > |B|$, arrivati ad $a_{|B|+1}$ saremmo di aver utilizzato tutti gli elementi di B come possibili immagini, quindi non potremmo procedere ulteriormente
 $\Rightarrow |\mathcal{I}_{m,j}^n \text{Map}(A, B)| = 0$

• TEOREMA

Siamo A e B insiemi finiti, e $a = |A|$ e $b = |B|$. Allora:

- ① esistono applicazioni INIETTIVE $A \rightarrow B \Leftrightarrow a \leq b$. Sono esattamente b^a applicazioni;
- ② esistono applicazioni SURGETTIVE $A \rightarrow B \Leftrightarrow a \geq b > 0 \vee a = b = 0$;
- ③ esistono applicazioni BIETTIVE $A \rightarrow B \Leftrightarrow a = b$. E sono esattamente $a!$.

Dim ①) dimostrazione prudente;

Dim ②) \Leftarrow sia f un'applicazione iniettiva $A \rightarrow B$; allora f ha una retzione $g: B \rightarrow A$, che è sicuramente iniettiva per definizione, e per conseguenza di ① $\Rightarrow b \leq a$.
 \Rightarrow Inoltre se $b=0 \Rightarrow a=0$, altrimenti $\text{Map}(A, B) = \emptyset$ (+).

\Leftarrow Viceversa, se vale la condizione a destra, allora:

\hookrightarrow se $b=0 \Rightarrow a=0 \Rightarrow$ esiste un'unica applicazione surgettiva, cioè id_A ;

\hookrightarrow se $b \neq 0$ e $a \geq b \Rightarrow$ esiste un'applicazione iniettiva $f: B \rightarrow A$ per ① e, essendo $B \neq \emptyset$, f ha una retzione $g: A \rightarrow B$ che per definizione è surgettiva.

Dim ③) \Leftarrow se esiste un'applicazione biettiva $A \rightarrow B$, allora $b \geq a$ per ① e $a \leq b$ per ② \Rightarrow ovvero $a = b$.

\Leftarrow se $a = b$, allora esistono per le ① delle applicazioni iniettive, in particolare, visto che $|\mathcal{I}_{m,j}^n \text{Map}(A, B)| = b^a = b \cdot (b-1) \cdot (b-2) \dots (b-a+1)$, ma se $b=a$, questo è uguale a $b \cdot (b-1) \dots (1) = b! = a!$, e per come sono costruite le applicazioni iniettive nella dimostrazione delle loro cardinalità, devono necessariamente essere biettive.

• TEOREMA

Siamo A e B insiemi finiti equipotenti. Allora $\forall f: A \rightarrow B$ vale:

- ① f è iniettiva;
 - ② f è surgettiva;
 - ③ f è biettiva.
- } non equivalenti

Dim) $\textcircled{1} \Rightarrow \textcircled{3}$ perché se per ipotesi so che f è iniettiva e $|A|=|B|$, per il teorema precedente ho già dimostrato l'implicazione.

$\textcircled{3} \Rightarrow \textcircled{2}$ ovvio per definizione di biiettività;

$\textcircled{2} \Rightarrow \textcircled{1}$ neppure per ipotesi che f è suriettiva $\Rightarrow f$ ha una retzione $g: B \rightarrow A$ per definizione iniettiva; ma avendo dimostrato che $\textcircled{1} \Rightarrow \textcircled{3}$, so che g è biiettiva. Ma allora f è una retzione dell'applicazione biiettiva g , e l'unica retzione di una funzione biiettiva è la sua inversa, e me nolte biiettiva $\Rightarrow f$ è iniettiva. 

OSSERVAZIONE: la parola d'ordine per tutte queste definizioni è INSIEME FINITO, perché nel caso infinito risultano false:

D: $m \in \mathbb{N} \mapsto m+1 \in \mathbb{N}$, in questo esempio gli insiemini sono equipotenti, ma la funzione non è suriettiva, perché lo 0 non è immagine di alcun elemento.

Diremo quindi che A e B sono EQUIPOTENTI se e solo se esiste un'applicazione biiettiva $A \rightarrow B$. In questo caso si sarà $|A|=|B|$ e si dice che A e B hanno la stessa cardinalità.

Si dice che A e B hanno cardinalità minore o uguale ($|A| \leq |B|$) se e solo se esiste un'applicazione iniettiva $A \rightarrow B$, o che A ha cardinalità strettamente minore di B ($|A| < |B|$) se e solo se esiste un'applicazione iniettiva $A \rightarrow B$ ma non esistono applicazioni biiettive.

↳ Ora vieni a A, B, C insieme:

- $|A|=|A|$ — poiché \rightarrow idea i biiettive;
- $|A|=|B| \Rightarrow |B|=|A|$ — poiché \rightarrow f biiettive $\Rightarrow f^{-1}$ biiettive;
- $(|A|=|B|) \wedge (|B|=|C|) \Rightarrow |A|=|C|$ — poiché \rightarrow $f \circ g$ biett $\Rightarrow g \circ f$ biett;
- $A \subseteq B \Rightarrow |A| \leq |B|$ — poiché \rightarrow immagine i iniettive;
- $|A|=|B| \Rightarrow |A| \leq |B|$ — poiché \rightarrow biettive \Rightarrow iniettive pur del;
- $(|A| \leq |B|) \wedge (|B| \leq |C|) \Rightarrow |A| \leq |C|$ — poiché \rightarrow $f \circ g$ iniettiva $\Rightarrow g \circ f$ iniettiva;

↳ Nelvo ormai come insieme:

$$|\mathbb{N}^*| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{N} \times \mathbb{N}| < |\mathbb{R}| = |\mathbb{R} \times \mathbb{R}| = |\mathcal{P}(\mathbb{N})| \xrightarrow{\text{in generale } \forall A \quad |A| < |\mathcal{P}(A)|}$$

↳ gli insiemini equipotenti a \mathbb{N} li chiamiamo NUMERABILI

• PROPOSIZIONE

Sia (S, \cdot) un semigruppo finito. Se (S, \cdot) ha qualche elemento cancellabile allora (S, \cdot) è un MONOIDE e ogni suo elemento cancellabile è simmetricabile.

N.B. = in generale non è sempre vero: abbiamo visto che in un monoido simmetricabile implica cancellabile, ma non il viceversa.

Dim) Sia a un elemento cancellabile in (S, \cdot) , allora le traslazioni simmetriche $\sigma_a: x \in S \mapsto ax \in S$ e $\sigma_a: x \in S \mapsto xa \in S$ sono iniettive. Poiché S è finito, $|\text{Im}_{\sigma_a} \text{ e } \text{Im}_{\sigma_a}| = S^S$, ma visto che $S=S$, σ_a e σ_a sono biiettive. Ciò comporta che a è simmetricabile, quindi $\exists s, d \in S \quad (a = \sigma_a(s) = \sigma_a(d))$, cioè $a = sa \wedge a = ad$.

Allora $\forall b \in S$, poiché σ_a invertibile, finisce un certo c tale che $\exists c \in S (b = \sigma_a(c) = ac)$
 $\Rightarrow sb = s(ac) = (sa)c = ac = b \Rightarrow s$ neutro sx in (S, \cdot)
 Fino un h tale che $\exists h \in S (b = \sigma_a(h) = ha)$
 $\Rightarrow bd = (ha)d = h(ad) = ha = b \Rightarrow d$ neutro dx in (S, \cdot)
 $\Rightarrow s = d$ è neutro in (S, \cdot) $\Rightarrow (S, \cdot)$ è un monoido.

Ora resta solo da dimostrare che ogni elemento cancellabile è simmetricabile.
 Allora, tenere per la invertibilità di σ_a e σ_c , $s \in \text{im}(\sigma_a) \cap \text{im}(\sigma_c)$, cioè
 $\exists p, r \in S (s = \sigma_a(p) = \sigma_c(r))$

$$\Rightarrow s = ap \wedge s = cr \Rightarrow \begin{cases} p \text{ è simmetrico dx di } a \\ r \text{ è simmetrico sx di } a \end{cases} \Rightarrow p = r \text{ è simmetrico di } a.$$



• PROPOSIZIONE

Sia $f: a \rightarrow b$ un'applicazione biettiva; allora $\tilde{f}: P(a) \rightarrow P(b)$ è biettiva, con inversa $\tilde{\tilde{f}}$.

Dim) l'obiettivo è: $\tilde{f} = (\tilde{\tilde{f}})^{-1}$, e cioè ① $\tilde{f} \circ \tilde{\tilde{f}} = \text{id}_{P(b)}$ e ② $\tilde{\tilde{f}} \circ \tilde{f} = \text{id}_{P(a)}$

① proviamo di dimostrare che $\forall y \in b (\tilde{f}(\tilde{\tilde{f}}(y)) = y)$

$$\forall y \in b (\exists y \in \tilde{f}(\tilde{\tilde{f}}(y))) \Leftrightarrow \exists x \in \tilde{f}(y) (y = f(x)) \Leftrightarrow \exists x \in a (f(x) \in y \wedge x \in f(x)) \Leftrightarrow y \in y$$

② da dimostrare: $\forall X \subseteq a (\tilde{\tilde{f}}(\tilde{f}(X)) = X)$

$$\forall x \in a (x \in \tilde{f}(\tilde{\tilde{f}}(X)) \Leftrightarrow f(x) \in \tilde{f}(X) \Leftrightarrow \exists c \in X (f(x) = f(c)) \Leftrightarrow \exists c \in X (x \in X \Leftrightarrow x = c)$$



↳ **Corollario**: $\forall a, b (|a| = |b| \Rightarrow |P(a)| = |P(b)|)$

• FUNZIONE CARATTERISTICA

Siamo S un insieme e $T \subseteq S$; si definisce:

$$\text{"chi"} \quad \chi_{T,S}: x \in S \mapsto \begin{cases} 1 & \text{se } x \in T \\ 0 & \text{se } x \notin T \end{cases} \in \{0, 1\}$$

↳ TEOREMA

Assumemmo queste notazioni, l'applicazione definita $\alpha: T \in P(S) \mapsto \chi_{T,S} \in \text{Map}(S, \{0,1\})$ è biettiva, con inversa $\beta: f \in \text{Map}(S, \{0,1\}) \mapsto \tilde{f}(\{1\}) \in P(S)$.

Dim) poniamo $H = \text{Map}(S, \{0,1\})$; obiettivi: ① $\alpha \circ \beta = \text{id}_H$ e ② $\beta \circ \alpha = \text{id}_{P(S)}$

① $\forall f \in H ((\alpha \circ \beta)(f) = \alpha(\beta(f)) = \alpha(\tilde{f}(\{1\})) = \chi_{\tilde{f}(\{1\}),S} = f)$

$$\chi_{\tilde{f}(\{1\}),S}: x \in S \mapsto \begin{cases} 1 & \text{se } x \in \tilde{f}(\{1\}) \\ 0 & \text{se } x \notin \tilde{f}(\{1\}) \end{cases} \in \{0, 1\}$$

$$\forall x \in S \begin{cases} x \in \tilde{f}(\{1\}) \Leftrightarrow f(x) = 1 \\ x \notin \tilde{f}(\{1\}) \Leftrightarrow f(x) \neq 1 \Leftrightarrow f(x) = 0 \end{cases}; \text{ allora posso ricavare:}$$

$$\chi_{\tilde{f}(\{1\}),S}: x \in S \mapsto \begin{cases} 1 & \text{se } f(x) = 1 \\ 0 & \text{se } f(x) = 0 \end{cases} \in \{0, 1\} \Leftrightarrow x \in S \mapsto f(x) \in \{0, 1\}$$

$$\Rightarrow (\alpha \circ \beta)(f) = \chi_{\tilde{f}(\{1\}),S} = f$$

② $\forall T \in P(S) ((B\alpha)(T) = (T))$

$$(B\circ\alpha)(T) = B(\alpha(T)) = B(X_{T,S}) = \overleftarrow{X}_{T,S}(\{1\}) = \{x \in S \mid X_{T,S}(x) = 1\} = T$$

\rightarrow Corollario: $\forall S (|P(S)| = |\text{Map}(S, \{0, 1\})|) = 2^{|S|}$ se S è finito

• COEFFICIENTE BINOMIALE

Com $P_k(S)$, $k \in \mathbb{N}$, ci indica l'insieme delle parti di S che abbiano esattamente k elementi: $P_k(S) = \{X \subseteq S \mid |X| = k\}$. Supponendo che S sia un insieme finito possiamo definire un coefficiente binomiale come:

$$\binom{m}{k} := |P_k(S)|$$

Alcuni di questi sono immediati da calcolare:

$$\hookrightarrow \binom{m}{0} = 1 = \binom{m}{m}$$

$$\text{Dim: } \binom{m}{0} = \emptyset \Rightarrow |P_0(S)| = 1 \quad e \quad \binom{m}{m} = S \Rightarrow |P_m(S)| = 1$$

$$\hookrightarrow \binom{m}{1} = m$$

$$\hookrightarrow \forall k \in \mathbb{N} (k > m \Rightarrow \binom{m}{k} = 0)$$

$$\hookrightarrow \sum_{k=0}^m \binom{m}{k} = 2^m$$

Dim per definizione $|P(S)| = 2^m$ [dim. più avanti]; inoltre si chiede che $P(S)$ è l'unica disgiunzione degli insiemi $P_k(S)$, pertanto scriviamo $|P(S)| = \sum_{k=0}^m |P_k(S)|$ (principio di inclusione - esclusione)

$$\Rightarrow 2^m = |P(S)| = \sum_{k=0}^m |P_k(S)| = \sum_{k=0}^m \binom{m}{k}$$

$$\hookrightarrow m, k \in \mathbb{N} \quad e \quad k \leq m, \text{ allora: } \binom{m}{m-k} = \binom{m}{k}$$

Dim consideriamo l'applicazione $\varphi: X \in P(S) \mapsto S \setminus X \in P(S)$. Poiché vale le leggi delle doppie negazioni, ovvero: $(S \setminus (S \setminus X) = X)$, φ^2 deve corrispondere $\text{id}_{P(S)}$, vale a dire che φ è l'inversa di se stessa, e dunque biettiva. L'immagine di $P_k(S)$ tramite φ è costituita dai complementi delle parti di S di cardinalità k , che avranno cardinalità $m-k$, dunque l'immagine di $P_k(S)$ è $P_{m-k}(S)$. Pertanto l'applicazione indotta da φ , $\varphi_n: X \in P(S) \mapsto S \setminus X \in P_{m-n}(S)$ è anch'essa biettiva, ciò dimostra che $|P_k(S)| = |P_{m-k}(S)| \Rightarrow \binom{m}{k} = \binom{m}{m-k}$.

• PRINCIPIO DI INDUZIONE

Sia p un predicato monico nelle variabili $m, b \in \mathbb{N}$, $\mathbb{N}_b = \{x \in \mathbb{N} \mid x \geq b\}$; se:

$\hookrightarrow p(b)$ è vera (BASE DI INDUZIONE);

$\hookrightarrow \forall m \in \mathbb{N}_b (p(m) \Rightarrow p(m+1))$

\Rightarrow ipotesi di induzione
 \Rightarrow passo induttivo

$\Rightarrow \forall m \in \mathbb{N}_b (p(m))$

Definiamo adesso α e β su S :

- $M = \{X \in P(S) \mid a \notin X\}$
- $E = \{X \in P(S) \mid a \in X\}$

$$\alpha: X \in M \mapsto X \cup \{a\} \in E$$

$$\beta: X \in E \mapsto X \setminus \{a\} \in M$$

chiaramente risulta: $P(S) = M \cup E$, $M \cap E = \emptyset$, $E = P(S) \setminus M$

PROPOSIZIONE: α e β sono una l' inversa dell'altra, quindi biettive $\Rightarrow |M| = |E|$

$$\text{Dim: } \forall X \in M \quad ((\beta \circ \alpha)(X) = \beta(\alpha(X)) = \beta(X \cup \{a\}) = (X \cup \{a\}) \setminus \{a\} = X)$$

$$\forall X \in E \quad ((\alpha \circ \beta)(X) = \alpha(\beta(X)) = \alpha(X \setminus \{a\}) = (X \setminus \{a\}) \cup \{a\} = X)$$

$$\Rightarrow \beta \circ \alpha = \text{id}_M, \alpha \circ \beta = \text{id}_E \Rightarrow \beta = \alpha^{-1}$$

• **TEOREMA:** $\forall S$ finito $\Rightarrow \forall a \in S \quad |P(S)| = 2^{|P(S \setminus \{a\})|}$

$$\text{Dim: } |P(S)| = |M| + |E| = 2|M| = 2|P(S \setminus \{a\})|$$

• **TEOREMA:** $\forall S$ finito, $|S|=m \Rightarrow |P(S)| = 2^m$

Dim: uso p. di induzione:

$$\rightarrow \text{base: } p(0) \Rightarrow |S|=0 \Leftrightarrow S=\emptyset, P(\emptyset)=\{\emptyset\} \Rightarrow |P(\emptyset)|=1=2^0 \text{ ok!}$$

$$\rightarrow \text{passo:} \text{ assumiamo vero per } m, \text{ ma } |S|=m+1 \Rightarrow S \neq \emptyset$$

$$\Rightarrow \exists a \in S \quad |P(S)| = 2|P(S \setminus \{a\})| \Rightarrow 2 \cdot 2^m = 2^{m+1}$$

$$|S \setminus \{a\}| = (m+1)-1 = m \Rightarrow |P(S \setminus \{a\})| = 2^m \text{ per ip. induttiva}$$

Definiamo adesso $\forall k \in \mathbb{N}$:

$$M_k = M \cap P_k(S) = \{X \in P_k(S) \mid a \notin X\}$$

$$E_k = E \cap P_k(S) = \{X \in P_k(S) \mid a \in X\}$$

α e β sono bijective $\Rightarrow |M_k| = |E_{k+1}|$

$$\alpha: X \in M_k \rightarrow X \cup \{a\} \in E_{k+1}$$

$$\beta: X \in E_{k+1} \rightarrow X \setminus \{a\} \in M_k$$

OSSERVAZIONE: sia $|S|=m+1$, allora: $|P_{k+1}(S)| = |M_{k+1}| + |E_{k+1}| = |M_{k+1}| + |M_k|$

$$\Rightarrow \binom{m+1}{k+1} = \binom{m}{k+1} \binom{m}{k} \quad (*)$$

• **TEOREMA**

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

Per chiarezza chiameremo questo passo nelle dimostrazione come $B(m, k)$

Dim: proviamo per induzione

\rightarrow base: per $m=0$, $p(0)$ deve essere vera; ma se $m=0$ e $k \leq m \in \mathbb{N} \Rightarrow k=0$

$\binom{0}{0} = 1$, quindi la nostra base è verificata, ma i interamente la dim. generale di:

$$B(m, 0) = \binom{m}{0} = \frac{m!}{0!(m-0)!} = \frac{m!}{m!} = 1$$

\rightarrow passo: assumiamo $p(m)$ vera $\Rightarrow p(m+1)$ deve essere verificata.

$$B(m+1, k) = \binom{m+1}{k} = \frac{(m+1)!}{k!(m+1-k)!} \quad \text{ho due possibili casi}$$

① se $k=0$, abbiamo visto che $B(m, 0)$ è verificata.

② se $k \neq 0$, applico $(*)$ a $\binom{m+1}{k}$

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

$\Delta x! = x(x-1)!$
 $= (m-k+1)(m-k)!$

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

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

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

• PARTIZIONE

Una partizione di A è un insieme F di parti non vuote di A , tale che:

$$\forall x \in A (\exists! b \in F (x \in b)) \wedge F \subseteq P(A) \setminus \{\emptyset\}.$$

Allora F è una partizione di A se e solo se valgono le tre proprietà:

$$① UF = \{x \mid \exists! b \in F (x \in b)\} = A;$$

$$② \emptyset \notin F;$$

$$③ \forall x, y \in F (x \neq y \Rightarrow x \cap y = \emptyset)$$

Dim) \Rightarrow se F per ipotesi è una partizione: da $F \subseteq P(A)$ segue $UF \subseteq A$, e da $\forall x \in A (\exists! b \in F (x \in b))$ segue $A \subseteq UF \Rightarrow A = UF$. Per definizione F è costituito da parti non vuote, dunque è verificata la seconda condizione. Per dimostrare la terza proprietà se $x \cap y \neq \emptyset \Rightarrow \exists z \in x \cap y \Rightarrow z \in x \wedge z \in y$, ma per definizione di partizione questo è possibile $\Leftrightarrow x = y$.

\Leftarrow $① \Rightarrow F \subseteq P(A)$ e $② \Rightarrow F \subseteq P(A) \setminus \{\emptyset\}$. $①$ x appartiene ad almeno un elemento b di F , per $③$ ci garantisce l'unicità. 

• LA PROIEZIONE π_F

$\forall F \in \text{Partz}(A)$ insieme di tutte le partizioni di A

$\pi_F : x \in A \mapsto b \in F$ tale che $x \in b$, ad ogni elemento associa la classe di equivalenza

↳ PROPOSIZIONE: $\forall A, \forall F \in \text{Partz}(A)$, la proiezione π_F di A su F è iniettiva.

Dim) dobbiamo provare che ogni elemento di F è nell'immagine di π_F . Sia $b \in F$, poiché per definizione $b \neq \emptyset$, esiste un $x \in b$. Finché un tale x , allora b è l'unico elemento di F a cui x appartiene, dunque $b = \pi_F(x)$ e $b \in \text{im}(\pi_F)$. 

• RELAZIONE DI EQUIVALENZA

Una relazione binaria è una relazione di equivalenza se e solo se è:

↳ RIFLESSIVA: $\forall x \in A (x \sim x)$;

↳ SIMMETRICA: $\forall x, y \in A (x \sim y \Rightarrow y \sim x)$;

↳ TRANSITIVA: $\forall x, y, z \in A ((x \sim y \wedge y \sim z) \Rightarrow x \sim z)$;

• NUCLEO DI EQUIVALENZA

applicazione

Si definisce nucleo di equivalenza di l la relazione binaria R_l che si definisce ponendo $\forall x, y \in A (x R_l y \Leftrightarrow l(x) = l(y))$.

↳ PROPOSIZIONE: sia $l: A \rightarrow B$ un'applicazione e R_l il suo nucleo di equivalenza; allora $R_l \in \text{Eq}(A)$.

Dim) riflessiva: $\forall x \in A (x R_l x)$, vere perché $l(x) = l(x)$,

simmetrica: $\forall x, y \in A (x R_l y \Rightarrow y R_l x)$

$x R_l y \Leftrightarrow l(x) = l(y) \Leftrightarrow l(y) = l(x) \Leftrightarrow y R_l x$;

transitiva: $\forall x, y, z \in A ((x R_l y \wedge y R_l z) \Rightarrow x R_l z)$

$(x R_l y \wedge y R_l z) \Rightarrow l(x) = l(y) = l(z) \Rightarrow x R_l z$; 

I nuclei di equivalenza sono sempre relazioni di equivalenza.

• CLASSI DI EQUIVALENZA

Sia $x \in A$ e $\epsilon \in \text{Eq}(A)$. La classe di equivalenza di x rispetto a ϵ è l'insieme $[x]_\epsilon = \{y \in A \mid y \epsilon x\}$, che è assialmente una parte di A .

↳ $[x]_\epsilon \neq \emptyset$ perché per la proprietà riflessiva $x \epsilon x \Rightarrow x \in [x]$;

↳ $[x]_\epsilon = \{y \in A \mid y \epsilon x\}$ per la proprietà simmetrica;
 $\Rightarrow x \epsilon y \Rightarrow x \in [y]_\epsilon \Rightarrow [x]_\epsilon = [y]_\epsilon$

↳ $[x]_\epsilon$ è l'unica classe di equivalenza a cui appartiene x ;

• INSIEME QUOTIENTE

Si chiama insieme quoziante di A rispetto a ϵ l'insieme $A/\epsilon = \{[x]_\epsilon \mid x \in A\}$ insieme di tutte le classi di equivalenza.

Per le proprietà delle classi di equivalenza, A/ϵ è un insieme di parti non vuote di A con la proprietà che ogni elemento di A appartenga a uno e un solo elemento di $A/\epsilon \Rightarrow A/\epsilon \in \text{Part}_z(A)$

↳ PROIEZIONE CANONICA

$\forall A, \epsilon \in \text{Eq}(A)$ definiamo $\Pi_\epsilon : x \in A \mapsto [x]_\epsilon \in A/\epsilon$, che è iniettiva per dimostrazione precedente. Soltre R_{Π_ϵ} nucleo di equivalenza di Π_ϵ
 $\forall x, y \in A \quad (x R_\epsilon y \Leftrightarrow \Pi_\epsilon(x) = \Pi_\epsilon(y) \Leftrightarrow [x]_\epsilon = [y]_\epsilon \Leftrightarrow x \epsilon y)$, ovvero abbiamo scoperto che il nucleo di equivalenza R_{Π_ϵ} di una proiezione canonica Π_ϵ coincide con l'applicazione ϵ .

OSSERVAZIONE: ogni relazione di equivalenza è il nucleo di equivalenza di qualche applicazione.

↳ TEOREMA

$\forall A, \alpha : \epsilon \in \text{Eq}(A) \mapsto A/\epsilon \in \text{Part}_z(A)$ è biettiva, e l'inversa è l'applicazione che ad ogni $F \in \text{Part}_z(A)$ associa il nucleo di equivalenza della proiezione $A \rightarrow F$.

Dim 1) α è iniettiva:

Siamo $\sigma, \rho \in \text{Eq}(A)$ e supponiamo che $\alpha(\sigma) = \alpha(\rho) \Rightarrow A/\sigma = A/\rho$.

$\forall x \in A \quad x \in [x]_\sigma \in A/\sigma = A/\rho \Rightarrow [x]_\sigma \in A/\rho$, ma l'unico elemento di A/ρ a cui appartiene x è $[x]_\rho$, quindi $[x]_\sigma = [x]_\rho$. Ora abbiamo che $\forall x, y \in A \quad x \sigma y \Leftrightarrow [x]_\sigma = [y]_\sigma \Leftrightarrow [x]_\rho = [y]_\rho \Leftrightarrow x \rho y \Rightarrow \sigma = \rho \Rightarrow \alpha$ è iniettiva

2) α è suriettiva:

Sia $F \in \text{Part}_z(A)$ e sia $\Pi_F : A \rightarrow F$ la proiezione di A su F , e R_{Π_F} il suo nucleo di equivalenza; abbiamo allora che $\forall x, y \in A \quad (x R_F y \Leftrightarrow \Pi_F(x) = \Pi_F(y) \Leftrightarrow y \in \Pi_F(x)) \Rightarrow [x]_F = \{y \in A \mid y \in \Pi_F(x)\} = \Pi_F(x)$

Allora $A/F = \{[x]_F \mid x \in A\} = \{\Pi_F(x) \mid x \in A\} = \text{im}(\Pi_F) = F$, perché Π_F è suriettiva
 $\Rightarrow F = \alpha(R_F)$, ormai abbiamo appena dimostrato che:

$\forall F \in \text{Part}_z(A) \quad (\exists R \in \text{Eq}(A) \quad (\alpha(R) = F)) \Rightarrow \alpha$ è suriettiva

3) inversa:

L'immagine di F tramite α^{-1} è la relazione di equivalenza R_F in A definita come nucleo di equivalenza di Π_F , cioè quella definita da:

$\forall x, y \in A \quad (x R_F y \Leftrightarrow \Pi_F(x) = \Pi_F(y)) \Leftrightarrow (x R_F y \Leftrightarrow (\exists b \in F \quad (x \in b \wedge y \in b)))$

infatti se $x \in b \Rightarrow b = \Pi_F(x)$, e se $x, y \in \Pi_F(x) \Rightarrow \Pi_F(y) = \Pi_F(x)$.



OSSERVAZIONE: le partizioni banali coincidono con le relazioni banali:

$$P: \text{uguaglianza} \longrightarrow A/P = \{\{x\} \mid x \in A\} = P_1(A)$$

$$P: \text{universale} \longrightarrow A/P = \{A\}$$

Abbiamo così che le RELAZIONI DI EQUIVALENZA si ponono riguardo da almeno tre punti di vista:

- ↳ come particolari relazioni binarie;
- ↳ come contest associato a quelli di partizione;
- ↳ come nuclei di equivalenza delle applicazioni;

• TEOREMA (di omomorfismo per immagini)

Siamo $f: A \rightarrow B$ un'applicazione e R_f il suo nucleo di equivalenze.

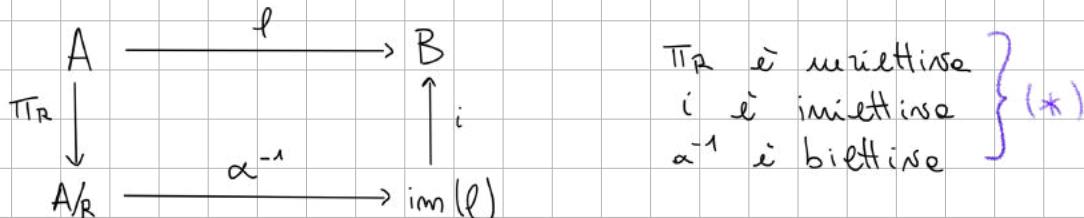
Allora $\forall x \in A$ si ha $[x]_R = \{y \in A \mid f(x) = f(y)\} = \overleftarrow{f}(\{f(x)\})$ e inoltre l'applicazione $\alpha: B \in \text{im}(f) \mapsto \overleftarrow{f}(\{b\}) \in A/R$ è biettiva.

Dimm) $\forall a \in A$ $[a]_R = \{x \in A \mid f(x) = f(a)\}$, ovvero l'insieme degli elementi che hanno la stessa immagine di a mediante f , ma chiaramente questo insieme è $\overleftarrow{f}(f(a)) = \{x \in A \mid f(x) = f(a)\}$

- **ben pote:** $\text{im}(f) = \{f(x) \mid x \in A\}$, quindi $\forall y \in \text{im}(f) (\exists x \in A (y = f(x)))$ e per l'osservazione precedente $\overleftarrow{f}(\{f(x)\}) = \overleftarrow{f}(\{y\}) = [x]_R$.
- **suriettive:** $\forall c \in A/R (\exists x \in A (c = [x]_R))$, sempre per la prima osservazione fatta $[x]_R = \overleftarrow{f}(f(x))$ e $f(x) \in \text{im}(f) \Rightarrow c = \alpha(f(x)) \Rightarrow \alpha$ è suriettiva.
- **iniettiva:** siamo $u, v \in \text{im}(f)$ tali che $\alpha(u) = \alpha(v)$. Dal momento che $u \in \text{im}(f)$, $\exists x \in A (u = f(x))$, ovvero $x \in \overleftarrow{f}(\{u\}) = \alpha(u)$; ma visto che abbiamo avuto $\alpha(u) = \alpha(v) \Rightarrow x \in \overleftarrow{f}(\{v\}) = \alpha(v)$, cioè $f(x) = v$. Pertanto $u = f(x) = v \Rightarrow \alpha$ è iniettiva.

OSSERVAZIONE: visto che α è biettiva, ha un inverso che è definito come $\alpha^{-1}: [x]_R \in A/R \mapsto f(x) \in \text{im}(f)$

La situazione presentata nel teorema può essere descritta dal diagramma:



↳ π_R è la proiezione canonica definita del nucleo di equivalenza;

↳ i è l'immersione di $\text{im}(f)$ in B ;

Rimette $f = (i \circ \alpha^{-1} \circ \pi_R)$, infatti $\forall x \in A ((i \circ \alpha^{-1} \circ \pi_R)(x) = (i(\alpha^{-1}(\pi_R(x)))) = i(\alpha^{-1}([x]_R)) = i(f(x)) = f(x))$. E siccome valgono (*) vediamo che ogni applicazione è ottenibile come composta tre un'applicazione iniettiva e una suriettiva: $f = (i \circ \alpha^{-1}) \circ \pi_R$.

• ANELLI

Un anello è una struttura algebrica $(R, +, \cdot)$ con le seguenti proprietà:

↳ $(R, +)$ è un gruppo abeliano (commutativo);

↳ (R, \cdot) è un semigruppo; (associativo);

↳ distributività rispetto a $+$;

$$\text{S} \quad \forall a, b, c \in R \quad a(b+c) = ab+ac \wedge (b+c)a = ba+ca$$

ATTENZIONE: se \cdot non è commutativa sono due proprietà differenti!

Diciamo che un anello è un **ANELLO COMMUTATIVO** se \cdot è commutativo; d'altronde l'altra operazione lo deve essere per forza. Chiamiamo invece un **ANELLO UNITARIO** se \cdot ha un elemento neutro; anche in questo caso le prime operazioni ne sono dotate.

Inoltre, se (R, \cdot) ha tutti gli elementi simmetrici rispetto a \cdot , chiamiamo:

• **INVERSO**: il simmetrico rispetto a \cdot ;

• **OPPOSTO**: il simmetrico rispetto a $+$;

Se $(R, +, \cdot)$ è unitario definio \circ :

• **ZERO** il neutro rispetto a $(R, +)$ e lo indichiamo con 0_R ;

• **UNITA'** il neutro rispetto a (R, \cdot) e lo indichiamo con 1_R ;

• SOTTOANELLI

Un sottanello $(R', +, \cdot)$ è tale se e solo se:

↳ $(R', +)$ è un sottogruppo di $(R, +)$;

↳ (R', \cdot) è chiuso rispetto a \cdot $\Leftrightarrow (R', \cdot)$ è un sottosemigruppo di (R, \cdot) .

Si dice **SOTTOANELLO UNITARIO** un sottanello che ha tra i suoi elementi il neutro dell'anello. Si dice invece **NON SOTTOANELLO UNITARIO** se $1_R \notin R'$, anche se come anello può avere unitario ($1_{R'} \in R'$).

• PROPRIETÀ DI CALCOLO DEGLI ANELLI

$$① \forall a \in R \quad a \cdot 0_R = 0_R = 0_R \cdot a$$

Dim) $a \cdot 0_R = a \cdot 0_R + 0_R$; inoltre visto che $0_R + 0_R = 0_R$, posso trarre a 0_R anche come $a(0_R + 0_R) = a \cdot 0_R + a \cdot 0_R$, per la distributività.
 $\Rightarrow a \cdot 0_R + 0_R = a \cdot 0_R + a \cdot 0_R \Rightarrow 0_R = a \cdot 0_R$

$$② \forall a, b, c \in R \quad -(a+b) = (-a)b = a(-b)$$

$$\text{Dim)} (a+b) + ((-a)b) = (a+(-a))b = 0_R b = 0_R$$

$$③ \forall a, b, c \in R \quad a(b-c) = ab - ac, \quad (b-c)a = ba - ca$$

$$\text{Dim)} a(b-c) = a(b+(-c)) = ab + a(-c) = ab + (-ac) = ab - ac$$

$$④ \forall m \in \mathbb{Z}, \forall R \text{ è unitario} \text{ vale } ma = (m \cdot 1_R)a$$

OSSERVAZIONE: non sempre negli anelli si verifica la comuta legge di annullamento del prodotto ($x \cdot y = 0 \Leftrightarrow x = 0 \vee y = 0$).

[**(es)** $(P(S), \Delta, \cap)$, in cui $P_{\{S\}} = \emptyset$

[premi $X, Y \in P(S)$ tali che $X \cap Y = \emptyset \Leftrightarrow X = \emptyset \vee Y = \emptyset$, infatti:
 $X = \{1, 2, 3\} \quad Y = \{4, 5, 6\}$ la loro intersezione è comunque vuota.

↳ OMOMORFISMI TRA ANELLI

Siamo R, S anelli e $f: R \rightarrow S$ un omomorfismo; nonostante siamo abituati a pensare che gli omomorfismi conservino le operazioni tra le due strutture, in questo caso non sempre $f(1_R) = 1_S$. Se questo accade lo chiamiamo **OMOMORFISMO DI ANELLI UNITARI**, altrimenti è semplicemente un omomorfismo tra anelli. Gli omomorfismi **SURGETIVI** sono sempre di anelli unitari.

[**(es)** $b \mapsto a$ e $f: P(b) \rightarrow P(a)$ immersione (?)

$$f(1_{P(b)}) = f(b) \neq a = 1_{P(a)}$$

• DIVISORE DELLO ZERO

Sia R un anello e a un suo elemento; allora diciamo che:

↳ a è un **divisore sx** dello zero in $R \Leftrightarrow \exists b \in R \setminus \{0_R\} (ab = 0_R)$;

↳ a è un **divisore dx** dello zero in $R \Leftrightarrow \exists b \in R \setminus \{0_R\} (ba = 0_R)$;

a è un **DIVISORE** dello zero \Leftrightarrow è divisore sinistro oppure destro.

OSSERVAZIONE: se $|R| > 1$ 0_R è un divisore sx e dx

Quindi adesso possiamo dire che la legge di annullamento del prodotto ($\forall a, b \in R \setminus \{0_R\} (ab \neq 0_R)$) vale se e solo se in $R \setminus \{0_R\}$ NON esistono divisori dello zero.

• INTEGRITÀ DI UN ANELLO

R è **INTEGRO** se e solo se 0_R è l'unico divisore dello 0_R in R , ovvero se e solo se $|R| > 1$, quindi se vale la L.A.P. (legge di annullamento del prodotto).

Chiamiamo invece R un **DOMINIO DI INTEGRITÀ** se R è integro e commutativo.

↳ TEOREMA

Siamo R un anello e $a \in R$; allora:

- a è un divisore sx $\Leftrightarrow a$ non è cancellabile a sx in R ; } **cancelleabile**
- a è un divisore dx $\Leftrightarrow a$ non è cancellabile a dx in R ; } **non è un divisore**
- a è un divisore $\Leftrightarrow a$ non è cancellabile.

Dim) \Rightarrow sia a un divisore sx dello zero, allora per definizione $\exists b \in R \setminus \{0_R\}$ tale che $(ab = 0_R)$. Fissato tale b , abbiamo $a \cdot b = 0_R = a \cdot 0_R$, ma per ipotesi $b \neq 0_R \Rightarrow a$ non è cancellabile a sx per definizione di cancellabilità e' $\forall x, y \in R (ax = ay \Rightarrow x = y)$.

\Leftarrow sia a non cancellabile a sx, cioè $\exists x, y \in R (ax = ay \wedge x \neq y)$. Per tali $x \neq y$ vole $(ax - ay = 0_R \Rightarrow a(x - y) = 0_R)$; ma se a questo punto chiamiamo $(b = x - y)$ ottengo $ab = 0_R \wedge b \neq 0_R \Rightarrow a$ è un divisore sx in R .

Quindi sono equivalenti le seguenti definizioni:

- ↳ un anello integro;
- ↳ un anello in cui vale la legge di annullamento del prodotto;
- ↳ un anello privo di divisori dello zero;
- ↳ un anello in cui ogni elemento diverso da zero è cancellabile.
Difatti zero non è cancellabile perché $0 \cdot 2 = 0 \cdot 5 \Rightarrow 2 = 5$.

- R è un **CORPO** $\Leftrightarrow R$ è un anello unitario, $|R| > 1$ e ogni elemento di R diverso da 0_R è invertibile (cioè $U(R) = R \setminus \{0_R\}$).
- \Rightarrow un corpo è un **anello integro**, in cui per ogni elemento non nullo vale cancellabile \Rightarrow rimovibile.
- R è un **CAMP** $\Leftrightarrow R$ è un campo commutativo.
- \Rightarrow un campo è un **dominio di integrità**, in cui ogni elemento non nullo è invertibile, ovvero vale (cancellabile \Rightarrow rimovibile).

PROPOSIZIONE: ogni dominio di integrità **FINITO** è un campo.

Dim: ossia anche per un semigruppo finito vale cancellabile \Rightarrow invertibile, e visto che per definizione un dominio di integrità è un anello commutativo in cui tutti gli elementi non nulli sono cancellabili $\Rightarrow R$ è un campo. 

• FORMULA DEL BINOMIO DI NEWTON

Siamo a e b due elementi di un anello **COMMUTATIVO** ($ab = ba$); allora per ogni intero positivo m :

$$(a+b)^m = \sum_{i=0}^m \binom{m}{i} a^{m-i} b^i$$

OSSERVAZIONE: questa formula chiaramente non vale se l'anello non è commutativo, e per verificarselo basta un semplice esempio:

$$\begin{aligned} (a+b)^3 &= (a+b)(a+b)(a+b) \text{ utilizzando più volte la proprietà distributiva} \\ \text{abbiamo: } &= a(a+b)(a+b) + b(a+b)(a+b) \\ &= a(a(a+b) + b(a+b)) + b(a(a+b) + b(a+b)) \\ &= a(aa+ab+ba+bb) + b(aa+ab+ba+bb) \\ &= a^2a + a^2b + ab^2 + b^2b + bab + bba + bbb \end{aligned}$$

Se a è commutativo posso unire i fattori $(aab + ab^2 + baa)$ come $3a^2b$ e ottenere la formula indicata dal binomio di Newton $a^3 + 3a^2b + 3ab^2 + b^3$; ma in caso contrario, se $ab \neq ba$ i tre fattori precedenti sono l'uno diverso dall'altro e otterrei una formula (corretta) ma ben differente.

• RELAZIONI D'ORDINE

Sia A un insieme e $\leq \in \text{Rel}(A)$ una relazione binaria; allora:

$\hookrightarrow \leq$ è ANTRIFLESSIVA $\Leftrightarrow \forall x \in A (x \neq x)$

$\hookrightarrow \leq$ è ANTISIMMETRICA $\Leftrightarrow \forall x, y \in A ((x \leq y \wedge y \leq x) \Rightarrow x = y)$

Diciamo quindi che \leq è una RELAZIONE D'ORDINE LARGO se e solo se è antiriflessiva, antisimmetrica e transitiva. Si dice invece che la relazione \leq è una RELAZIONE D'ORDINE STRETTO se è antiriflessiva e transitiva.

OSSERVAZIONE: tutte le relazioni di ordine stretto sono antisimmetriche.

Dim) $\forall x, y \in A ((x \leq y \wedge y \leq x) \Rightarrow x = y)$ per la transitività, ma per ipotesi \leq è anche antiriflessiva ($\forall x \in A (x \neq x)$). Quanto vuol dire che la proposizione $(x \leq y \wedge y \leq x)$ è falsa e quindi $(x \leq y \wedge y \leq x) \Rightarrow x = y$ è vera perché l'antecedente è falso.

Sia $OL(A)$ l'insieme di tutte le relazioni d'ordine largo in A , e $OS(A)$ tutte quelle di ordine stretto. Valgono le seguenti proposizioni:

① $\forall p \in OL(A)$ posso definire $p \neq \in \text{Rel}(A)$ in modo che $\forall x, y \in A$:

$$x \neq y \Leftrightarrow (x \neq y \wedge x \neq y) \Rightarrow p \neq \in OS(A).$$

Dim) antiriflessiva: $\forall x \in A (x \neq x)$ perché $x = x \wedge x \neq x$ (rispetto che $p \in OL(A)$),

transitività: $\forall x, y, z \in A (x \neq y \wedge y \neq z \Rightarrow x \neq z)$

$$x \neq y \wedge y \neq z \Rightarrow x \neq y \wedge x \neq y \wedge y \neq z \Rightarrow x \neq z \wedge x \neq z \Rightarrow x \neq z$$

② $\forall \sigma \in OS(A)$ posso definire $\sigma_+ \in \text{Rel}(A)$ in modo che $\forall x, y \in A$:

$$x \sigma_+ y \Leftrightarrow (x \sigma y \vee x = y) \Rightarrow \sigma_+ \in OL(A).$$

Dim) riflessiva: $\forall x \in A x \sigma_+ x$, perché $x = x$;

antisimmetrica: se nego queste proprietà ho che $\exists x, y \in A (x \sigma_+ y \wedge y \sigma_+ x \wedge x \neq y)$ (negazione di implicazione $\neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg q)$), ma questo sarebbe equivalente a $(x \sigma y \vee x = y) \wedge (y \sigma x \vee y = x) \wedge x \neq y \rightarrow$ rispetto che si devono verificare tutte le parti delle congiuntione e ho questa ultima condizione, sarebbe equivalente a $x \sigma y \wedge y \sigma x \wedge x \neq y$, ma questo è absurd perché σ è antisimmetrica.

transitività: $\forall x, y, z \in A (x \sigma_+ y \wedge y \sigma_+ z) \Rightarrow (x \sigma y \vee x = y) \wedge (y \sigma z \vee y = z)$.

Nel caso $x = y \wedge y = z \Rightarrow x = z \Rightarrow x \sigma_+ z$; altrimenti da $x \sigma y \wedge y \sigma z$ segue $x \sigma z$, per la transitività di $\sigma \Rightarrow x \sigma_+ z$.

PROPOSIZIONE: le applicazioni $p \in OL(A) \mapsto p \neq \in OS(A)$ e $\sigma \in OS(A) \mapsto \sigma_+ \in OL(A)$ sono biettive e una l'inversa dell'altra.

Dim) Sia \bar{p} la relazione duale di p , e $(\bar{p})^*$ il suo grafico; definiamo:

$\rightarrow p$ antiriflessiva $\Leftrightarrow \Delta_A \cap p^* = \emptyset$

$\rightarrow p$ antisimmetrica $\Leftrightarrow p^* \cap (\bar{p})^* \subseteq \Delta_A$

inoltre $(p_+)^* = p^* \setminus \Delta_A$ e $(\sigma_+)^* = \sigma^* \cup \Delta_A$. Allora:

il grafico di $(p_+)^* = (\bar{p})^* \setminus \Delta_A \cup \Delta_A = p^* \Rightarrow l^{-1}(l(p)) = (p_+)^* = p$.

duolmente per $(\sigma_+)^* = (\sigma^* \cup \Delta_A) \setminus \Delta_A = \sigma^* \Rightarrow (\sigma_+)^* = \sigma$

• RELAZIONE DI DIVISIBILITÀ

Sia (S, \circ) un semigruppo commutativo; la relazione di divisibilità in (S, \circ) implicata da \mid o da $|_{(S,\circ)}$ è definita dalle formule:

$$\forall a, b \in S \quad (a \mid b \Leftrightarrow \exists c \in S (b = ac))$$

↳ Se (S, \circ) è un semigruppo $\Rightarrow \mid$ è transitiva.

Dim) $\forall x, y, z \in S (x \mid y \wedge y \mid z) \Rightarrow \exists c, d \in S (y = xc \wedge z = yd)$; sostituendo y ottengo $z = (x c)d$, applico associazività $\Rightarrow z = x(cd)$. Quindi ho scoperto che $\exists (cd) \in S (z = x(cd)) \Rightarrow x \mid z$.

↳ Se (S, \circ) è un monoido $\Rightarrow \mid$ è riflessiva.

Dim) prevo t elemento neutro in (S, \circ) $\Rightarrow \forall a \in S (a = at) \Rightarrow a \mid a$

$\forall a, b \in S$ si dice che a e b sono ASSOCIATI se $(a \circ b \Leftrightarrow (a \circ b \wedge b \circ a))$

↳ Se (S, \cdot) è un monoido la relazione di divisibilità è antiriflexiva, quindi è una relazione di ordine largo, se e solo se $\forall a, b \in S (a \mid b \Leftrightarrow a = b)$, ovvero se e solo se la relazione "esse elementi associati" è l'uguaglianza.

Dim) \Leftarrow affinché la relazione \mid sia antiriflexiva deve valere: $(a \mid b \wedge b \mid a \Rightarrow a = b)$ ma per definizione di elementi associati $(a \mid b \wedge b \mid a) \Rightarrow a \circ b$

$\Leftarrow a \circ b \Rightarrow a \mid b$ ovvio, perché \mid è riflessiva.

(es) la relazione di divisibilità in (\mathbb{N}, \circ) è di ordine largo; infatti $a \mid b \Leftrightarrow a = b$, invece non è antiriflexiva in (\mathbb{Z}, \cdot) , in cui ad esempio $(1 \mid -1 \wedge -1 \mid 1)$, ma $1 \neq -1$.

• INSIEME ORDINATO

Un insieme ordinato è una coppia ordinata (S, ρ) , dove ρ è una relazione di ordine largo in S ($\rho \in OL(S)$). A differenza delle strutture algebriche, definite da operazioni, questi sono definiti da relazioni; allo stesso modo però si può parlare di sottostrutture.

ESEMPI STANDARD: (\mathbb{R}, \leq) $(\mathbb{P}(S), \subseteq)$ (\mathbb{N}, \mid)

Siamo a, b appartenenti a un insieme S in cui è definita $\rho \in OL(S)$; diciamo che a e b sono CONFRONTABILI se e solo se $(a \rho b \vee b \rho a)$. Definiamo quindi che la relazione $\rho \in OL(S)$ è TOTALMENTE ORDINATA se $\forall a, b \in S$ a e b sono confrontabili rispetto a ρ .

(es) (\mathbb{R}, \leq) è tot. ordinato;

$(\mathbb{P}(S), \subseteq)$ è tot. ordinato $\Leftrightarrow |S| \leq 1$, perché se S ha almeno due elementi distinti x e y , $\{x\} \subset \{y\}$ non sono confrontabili $\Rightarrow \exists x, y \in S (x \not\sim y \wedge y \not\sim x)$ negazione

(\mathbb{N}, \mid) non è tot. ordinato, infatti $(2 \nmid 3 \wedge 3 \nmid 2)$.

• RELAZIONE D'ORDINE INDOTTA SU UNA PARTE

Sia (S, ρ) un insieme ordinato, quindi $\rho \in OL(S)$; $\forall T \subseteq S$ si può definire la relazione binaria ρ_T indotta da ρ in T : $\forall a, b \in T (a \rho_T b \Leftrightarrow a \rho b)$. È ovvio che anche ρ_T è d'ordine, in quanto eredita tutte le proprietà di $\rho \Rightarrow \rho_T \in OL(T)$.

Allora (T, ρ_T) è un insieme ordinato e si dice che è un **SOTTOINSIETÀ ORDINATO** di (S, ρ) ; in genere si scrive direttamente (T, ρ) .

(es) (\mathbb{Q}, \leq) , (\mathbb{Z}, \leq) , (\mathbb{R}^+, \leq) sott. ordinati di (\mathbb{R}, \leq) ;
 $\forall T \subseteq S \Rightarrow (\mathcal{P}(T), \subseteq)$ sott. ordinato di $(\mathcal{P}(S), \subseteq)$.

FUNZIONI CRESCENTI

Se (S, ρ) e (T, σ) sono insiemni ordinati, ossia $\rho \in OL(S)$ e $\sigma \in OL(T)$ una applicazione $f: S \rightarrow T$ è **crecente** da (S, ρ) a (T, σ) se e solo se:

$$\forall a, b \in S (a \rho b \Rightarrow f(a) \sigma f(b))$$

ISOMORFISMI TRA INSIEMI ORDINATI

Si dice che $f: S \rightarrow T$ è un **isomorfismo** da (S, ρ) a (T, σ) se e solo se:

$\hookrightarrow f$ è biettiva;

$\hookrightarrow f$ è crecente da (S, ρ) a (T, σ) ; } $\Leftrightarrow \forall a, b \in S (a \rho b \Leftrightarrow f(a) \sigma f(b))$

$\hookrightarrow f^{-1}$ è crecente da (T, σ) a (S, ρ)

(es) applicazione identica $id_{\mathbb{N}^*}: \mathbb{N}^* \rightarrow \mathbb{N}^*$ è biettiva e crecente da $(\mathbb{N}^*, |)$ a (\mathbb{N}, \leq) , infatti $\forall a, b \in \mathbb{N}^* (a | b \Rightarrow a \leq b)$. Ma non è crecente l'insieme da (\mathbb{N}^*, \leq) a $(\mathbb{N}^*, |)$, in quanto $a \leq b \Rightarrow a | b$ ($2 \leq 3$, ma $2 \nmid 3$).

MASSIMO E MINIMO

Siano finiti un insieme S e $\rho \in OL(S)$, con $\bar{\rho}$ la relazione duale. Definiamo:

$\hookrightarrow a \in S$ è **MINITO** in (S, ρ) $\Leftrightarrow \forall x \in S (a \rho x)$; $a \leq x$

$$x \leq a \Rightarrow x = a$$

$\hookrightarrow a \in S$ è **MASSIMO** in (S, ρ) $\Leftrightarrow \forall x \in S (x \rho a)$; $x \leq a$

$$a \leq x \Rightarrow a = x$$

$\hookrightarrow a \in S$ è **MINIMALE** in (S, ρ) $\Leftrightarrow \neg (\exists x \in S (x \rho a)) \Leftrightarrow \forall x \in S (x \rho a \Rightarrow x = a)$

$\hookrightarrow a \in S$ è **MASSIMALE** in (S, ρ) \Leftrightarrow è minimale in $(S, \bar{\rho})$ $\Leftrightarrow \forall x \in S (a \bar{\rho} x \Rightarrow a = x)$

PROPOSIZIONE: se a è di minimo in (S, ρ) , allora a è l'unico minimo in (S, ρ) (e quindi anche l'unico minimo).

Dim) sia a di minimo in (S, ρ) , allora a è minima perche' $\forall x \in S (a \rho x)$, per definizione, ma se vale $x \rho a \Rightarrow x = a$ perché ρ è antisimmetrica. Supponiamo poi per absurdio che b sia un altro minimo; nole, per definizione di minimo, che $a \rho b$, ma allora $a = b$ per definizione di minimo.

Per dualità vale la stessa proposizione per massimo e massimale.

$$\Rightarrow \begin{cases} \text{min}(S, \rho) \text{ indica l'unico minimo;} \\ \text{MAX}(S, \rho) \text{ indica l'unico massimo;} \end{cases}$$

OSSERVAZIONE: non tutti gli insiemni ordinati sono dotati di minimo o di massimo, potrebbero anche avere solo minimali e maximali. Ma se (S, ρ) è **TOTALMENTE ORDINATO** a è minima (maxima) $\Leftrightarrow a$ è minimo (massimo).

• TEOREMA

Sia (S, \leq) un insieme ordinato finito non vuoto; allora ha minimi e massimi.

Dim) Supponiamo che (S, \leq) non abbia elementi minimi; poiché $S \neq \emptyset$, $\exists x_0 \in S$ e lo siamo. Per ipotesi x_0 non è minima, allora $\exists x_1 \in S (x_1 \leq x_0 \wedge x_1 \neq x_0)$, ovvero $\exists x_1 \in S (x_1 \neq x_0)$ e lo siamo; x_1 a sua volta non è minima, allora $\exists x_2 \in S (x_2 \leq x_1)$ e per transitività $x_2 \leq x_0$. Proseguendo in questo modo definiamo ricorsivamente una successione $(x_n)_{n \in \mathbb{N}}$ di elementi di S tali che $\forall i, j \in \mathbb{N} (i < j \Rightarrow x_j \leq x_i) \Rightarrow (i \neq j \Rightarrow x_j \neq x_i)$.

Allora $\{x_i \mid i \in \mathbb{N}\}$ è una parte infinita di S , il che è ASSURDO, quindi (S, \leq) ha elementi minimi, e per dualità abbiamo anche dimostrato, riferendoci a $\bar{\leq}$, che ha massimi. ■

• INTERVALLI E COPERTURA

Siamo S un insieme, $\leq \in \text{OL}(S)$, e le corrispondenti relazioni di ordine stretto, $a, b \in S$. Definiamo gli intervalli:

$$\begin{aligned} [a, b] &= \{x \in S \mid a \leq x \wedge x \leq b\} && \text{chiuso} \\ [a, b[&= \{x \in S \mid a \leq x \wedge x < b\} && \text{semiaperto} \\]a, b] &= \{x \in S \mid a < x \wedge x \leq b\} \\]a, b[&= \{x \in S \mid a < x \wedge x < b\} && \text{aperto} \end{aligned}$$

Inoltre diciamo che b copre a in $(S, \leq) \Leftrightarrow a < b \wedge]a, b[= \emptyset$; in questo caso scriviamo $a \lessdot b$. Con queste definizioni, sono equivalenti:

- ① $a \lessdot b$
- ② $a < b \wedge \neg (\exists c \in S | a < c < b)$;
- ③ a è un elemento massimo in $(\{x \in S \mid x < b\}, \leq)$;
- ④ b è un elemento minima in $(\{x \in S \mid a < x\}, \leq)$;

• TEOREMA

Sia (S, \leq) un insieme ordinato finito, e siamo $a, b \in S$. Allora $a \leq b \Leftrightarrow \exists m \in \mathbb{N}$ s.t. x_0, x_1, \dots, x_m elementi di S tali che $x_0 = a, x_m = b$ e $\forall j \in \{i \in \mathbb{N} \mid i < m\} (x_j \lessdot x_{j+1})$.

Dim) \Leftarrow se $\exists m \in \mathbb{N}$ e x_0, \dots, x_m elementi con la proprietà richiesta allora:

$$\hookrightarrow m = 0 \Rightarrow a = x_0 = b \Rightarrow a \leq b,$$

$\hookrightarrow m > 0 \Rightarrow a = x_0 \lessdot x_1 \lessdot x_2 \dots \lessdot x_m = b$ ovvero $a = x_0 < x_1 < x_2 \dots < x_m = b$; immagine in ogni caso ottengo $a \leq b$.

\Rightarrow sia $a \leq b$ per ipotesi:

$\hookrightarrow a = b$ otteniamo la conclusione richiesta ponendo $m = 0$ e $x_0 = a = b$; infatti per $m = 0$ l'insieme $\{i \in \mathbb{N} \mid i < 0\}$ è vuoto, dunque abbiamo una proposizione introdotta da un quantificatore universale ridotto all'insieme vuoto, quindi $\forall x \in S (\varphi(x)) \Leftrightarrow \forall x (x \in S \Rightarrow \varphi(x))$ è vera perché l'antecedente è falso;

$\hookrightarrow a \neq b \Rightarrow a < b$: poniamo $x_0 = a$ e consideriamo l'intervallelo $X =]a, b[$.

Siccome X è finito, o $X = \emptyset$ oppure (X, \leq) ha un elemento minima x_1 . Se $X = \emptyset$ si ha $a < b$, quindi basta porre $m = 1$ e $x_0 = a, x_1 = b$. Se invece $X \neq \emptyset$ consideriamo l'intervallelo $]x_1, b[$ (notare $x_1 \leq b$).

\hookrightarrow se $[x_1, b] = \emptyset \Rightarrow x_1 < b$ e quindi basta porre $m=2$ e $x_2=b$, così $a=x_0 \leftarrow x_1 \leftarrow x_2 = b$.
 \hookrightarrow se $[x_1, b] \neq \emptyset$, visto che il limite raggiunge un elemento minimo x_2 ; allora $a=x_0 \leftarrow x_1 \leftarrow x_2 \leq b$ e consideriamo $[x_2, b]$.
 Procedendo in questo modo costruiamo una sequenza di elementi di S tali che $a=x_0 \leftarrow x_1 \leftarrow x_2 \dots \leftarrow x_i \leftarrow x_{i+1} \leftarrow \dots \leq b$ ottenuta ricorsivamente in questo modo: se i definito x_i , se $x_i=b$ si fermiamo, altrimenti definiamo x_{i+1} come elemento minimo in $[x_i, b]$.
 Poiché S è finito e gli elementi x_i sono a due a due distinti, questa costruzione si deve necessariamente fermare, quindi troviamo un $i \in \mathbb{N}$ tale che $x_i=b$. Ponendo $m=i$ vediamo che a questo punto abbiamo costituito gli elementi x_0, x_1, \dots, x_m richiesti.

DIAGRAMMI DI HASSE

Sia (S, \leq) un insieme ordinato finito; rappresentiamo gli elementi di S come punti del piano, col simbolo che se $a, b \in S$ e $a \leq b$, il punto che rappresenta b sia disegnato più in alto di quello di a . Inoltre tracciamo una linea che $a \leq b \Leftrightarrow a \leq b$.

(es) $(P(S), \subseteq)$

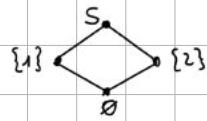
$$S = \emptyset$$

•

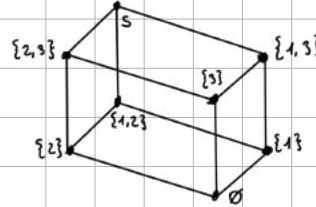
$$|S|=1$$



$$S = \{1, 2\}$$



$$S = \{1, 2, 3\}$$



Due insiemni ordinati si dicono ISOMORFI se hanno lo stesso diagramma.

Il duale di un diagramma di Hasse si ottiene ruotando il grafico di 180° .

Sia $f: S \rightarrow T$ un'applicazione, $\leq \in \text{OL}(T)$ e $\leq = (\leq)_f \in \text{OS}(T)$; definiamo le relazioni $\sigma, \rho \in \text{Rel}(S)$ usando le formule:

$\hookrightarrow \forall x, y \in S \quad x \sigma y \Leftrightarrow f(x) \leq_f f(y) \quad \Rightarrow \sigma \in \text{OS}(S)$;

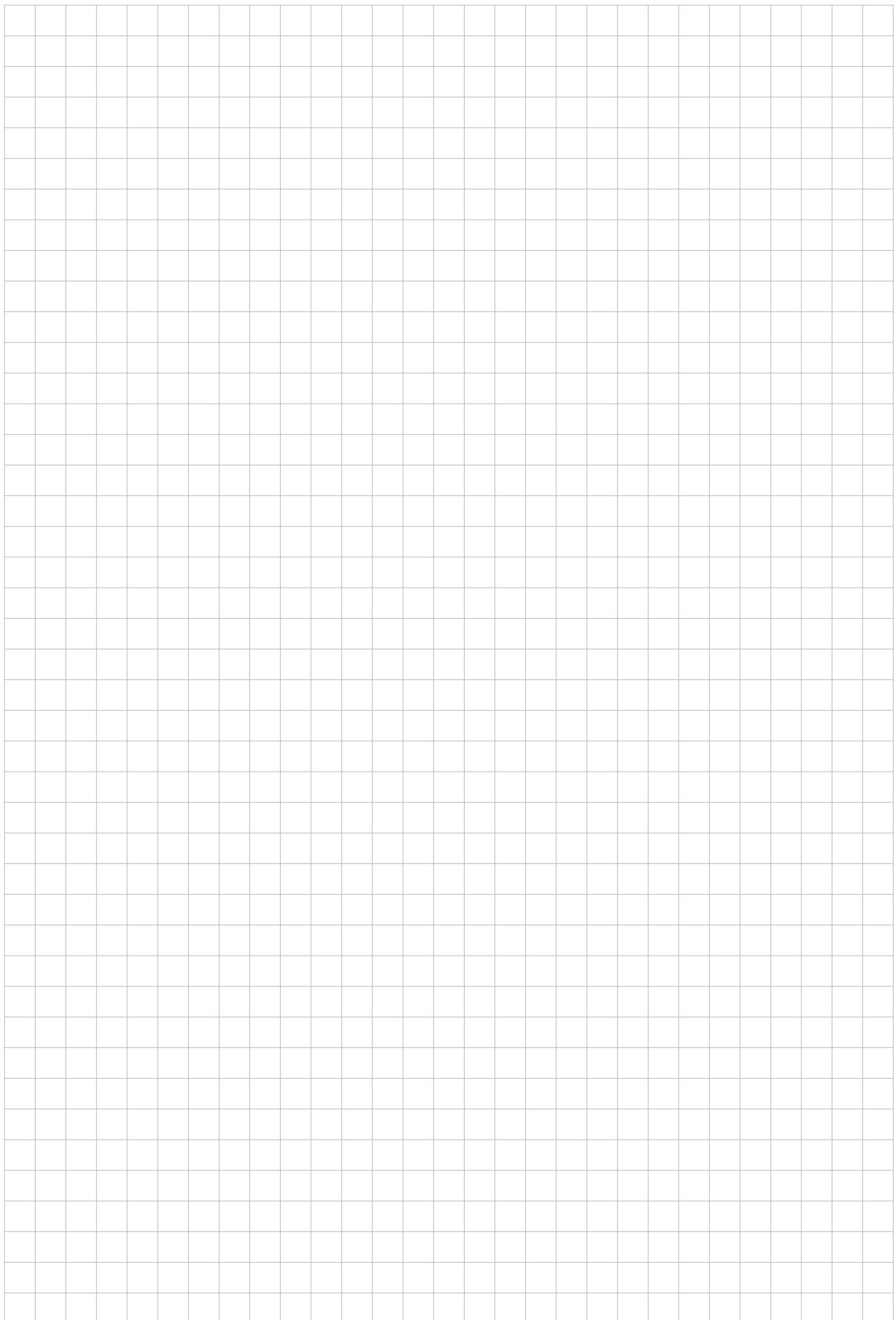
$\hookrightarrow \forall x, y \in S \quad x \rho y \Leftrightarrow (x = y \vee f(x) < f(y)) \quad \Rightarrow \rho = (\sigma) = \in \text{OL}(S)$;

OSSERVAZIONE: $\forall a \in S$, a NON è minimaile $\Leftrightarrow \exists b \in S \ (b \neq a) \ Leftrightarrow \exists b \in S \ (b \neq a)$
 $\Leftrightarrow \exists b \in S \ (f(b) < f(a)) \Leftrightarrow f(a)$ non è minimaile in $(\text{im}(f), \leq)$.

Prese quindi questi nuovi elementi che abbiamo definito, poniamo ridefinire:

$\hookrightarrow a$ è MINIMALE in $(S, \rho) \Leftrightarrow f(a)$ è minimaile in $(\text{im}(f), \leq)$;

$\hookrightarrow a$ è MASSIMALE in $(S, \rho) \Leftrightarrow f(a)$ è maximaile in $(\text{im}(f), \leq)$;



• MINORANTI E MAGGIORANTI

Moltre, dati (S, ρ) con $\rho \in \text{OL}(S)$, $\forall X \in \mathcal{P}(S)$ definiamo:

$$X^{\downarrow} = \{a \in S \mid \forall x \in X \quad a \rho x\} \quad X^{\uparrow} = \{a \in S \mid \forall x \in X \quad x \rho a\}$$

$\hookrightarrow a$ è un **MINORANTE** di X in $(S, \rho) \Leftrightarrow a \in X^{\downarrow}$;

$\hookrightarrow a$ è un **MAGGIORANTE** di X in $(S, \rho) \Leftrightarrow a \in X^{\uparrow}$,

Se premoto il caso specifico $S = \mathbb{N}$

$$X^{\uparrow} = \{y \in \mathcal{P}(S) \mid \forall c \in UX \quad (c \in y)\} = \{y \subseteq S \mid UX \subseteq y\}$$

$$X^{\downarrow} = \{y \subseteq S \mid \forall a \in X \quad (y \subseteq a)\} = \begin{cases} \{y \subseteq S \mid y \subseteq UX\} & \text{se } X \neq \emptyset \\ \{y \mid y \subseteq S\} = \mathcal{P}(S) & \text{se } X = \emptyset \end{cases}$$

• ESTREMI

$\hookrightarrow \forall a \in S$, a è **ESTREMO INFERIORE** di X in $(S, \rho) \Leftrightarrow a = \text{MAX}(X^{\downarrow(S, \rho)})$;

$\hookrightarrow \forall a \in S$, a è **ESTREMO SUPERIORE** di X in $(S, \rho) \Leftrightarrow a = \text{min}(X^{\uparrow(S, \rho)}) \Leftrightarrow a = \text{MAX}(X^{\uparrow(S, \rho)})$

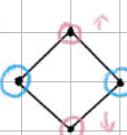
Sono equivalenti le seguenti affermazioni:

- ① $a \rho b$;
- ② $a = \text{min}\{a, b\}$;
- ③ $a = \text{inf}\{a, b\}$;
- ④ $a \in \{a, b\}^{\downarrow}$;

• RETICOLO

Diciamo che (S, ρ) è un reticolo $\Leftrightarrow \forall a, b \in S \quad [\exists \text{inf}\{a, b\} \wedge \text{sup}\{a, b\}]$.

Visto che $a \rho b$ è equivalente a $a = \text{inf}\{a, b\}$, se voglio capire se un insieme ordinato è un reticolo, mi devo solo preoccupare di verificare che tutti gli elementi siano confrontabili a due a due. Orviamente se ho un insieme totalmente ordinato, questo è sicuramente un reticolo.

(*)  per verificare che sia un reticolo guardo alle coppie non confrontabili, quindi: a 0, e in questo caso hanno sia un inf che un sup 0.

PROPOSIZIONE: sia $a \in (S, \rho)$ reticolo; a è minimo in $(S, \rho) \Leftrightarrow a = \text{min}(S, \rho)$.

Dim: si già dimostrato in generale per gli insiemi ordinati.

Fd sia a minima; $\forall b \in S$ sia $c = \text{inf}\{a, b\} = \text{MAX}(X^{\downarrow})$, allora $c \rho a$ e $c \rho b$, ma visto che a è minima $\Rightarrow c = a \Rightarrow a \rho b \quad \forall b \in S \Rightarrow a = \text{min}(S, \rho)$.

Per dualità' vale anche massima $\Leftrightarrow \text{max}$.

OSSERVAZIONE: $\forall a, b \in S \quad a \rho b \Leftrightarrow a = \text{inf}\{a, b\} \Leftrightarrow b = \text{sup}\{a, b\}$. Moltre se $X \subseteq S$ e $x = \text{inf}(X) \Rightarrow X^{\downarrow} = \{x\}^{\downarrow}$

(*) **PROPOSIZIONE:** sia (S, ρ) un insieme ordinato e $X, Y \subseteq S$. Supponiamo che esistano $x = \text{inf}(X)$ e $y = \text{inf}(Y)$; allora $(X \cup Y)^{\downarrow} = X^{\downarrow} \cap Y^{\downarrow} = \{x\}^{\downarrow} \cap \{y\}^{\downarrow} = \{xy\}^{\downarrow}$. Se inoltre (S, ρ) è un reticolo esiste $a = \text{inf}\{x, y\} = \text{MAX}(\{x, y\}^{\downarrow}) = \text{MAX}((X \cup Y)^{\downarrow}) = \text{inf}(X \cup Y)$.

Un reticolo si dice **LIMITATO** se ha minimo e massimo, un reticolo finito non vuoto è sempre limitato. Un reticolo si dice **COMPLETO** se tutti i sottoinsiemi hanno sup e inf.

• OPERAZIONI RETICOLARI

Sia (S, ρ) un reticolo; definiamo due operazioni binarie in S :

$$\begin{aligned} \wedge: (a, b) \in S \times S &\mapsto \inf\{a, b\} \in S \\ \vee: (a, b) \in S \times S &\mapsto \sup\{a, b\} \in S \end{aligned} \quad \left. \begin{array}{l} \text{hanno le seguenti proprietà:} \\ \text{1. commutativa,} \\ \text{2. associativa,} \\ \text{3. valgono le leggi di annullamento: } \forall a, b \in S \quad (a \wedge b \vee b) = a = a \vee (a \wedge b), \\ \text{4. idempotente: ogni elemento } a \text{ idempotente } \forall a \in S \quad a \wedge a = a = a \vee a, \end{array} \right\}$$

- 1 commutativa;
- 2 associativa;
- 3 valgono le **leggi di annullamento**: $\forall a, b \in S \quad (a \wedge b \vee b) = a = a \vee (a \wedge b)$;
- 4 idempotente: ogni elemento a idempotente $\forall a \in S \quad a \wedge a = a = a \vee a$;

Dimostriamo che (S, ρ) è un reticolo \Leftrightarrow valgono le operazioni reticolari con le proprietà duali.

\Rightarrow se (S, ρ) è un reticolo, le operazioni sono **commutative** perché, per come può essere definito un insieme $\{a, b\} = \{b, a\} \Rightarrow a \wedge b = \inf\{a, b\} = \inf\{b, a\} = b \wedge a$; **associative** perché: $a \wedge (b \wedge c) = a \wedge \inf\{b, c\} = \inf\{a, \inf\{b, c\}\} = \inf\{a, b, c\}$ vero per la proposizione (*), poiché sappiamo che $\inf\{x, y\} = \inf\{y, x\}$, con $i = \inf\{a, b\}$ e $j = \inf\{b, c\}$, e ovviamente $a = \inf\{a\}$ e $c = \inf\{c\}$.

Sinfine l'**idempotenza** non è altro che una conseguenza delle ③, in quanto se $\forall a \in S \quad a = (a \wedge (a \vee b)) \Rightarrow a \vee a = a \wedge (a \wedge (a \vee b)) \Rightarrow a \wedge a = a$.

come ultimo passo, notiamo a cosa corrispondono gli elementi neutri delle operazioni binarie:

$\forall a \in S \quad a$ è neutrino rispetto a $\vee \Leftrightarrow \forall b \in S \quad (a \vee b = b) \Leftrightarrow \forall b \in S \quad (a \leq b) \Leftrightarrow a = \min(S, \leq)$. Per dualità posso dire che a è neutrino rispetto a $\wedge \Leftrightarrow a = \max(S, \leq)$.

\Leftarrow Viceversa sia (S, \vee, \wedge) una struttura algebrica con due operazioni binarie \vee e \wedge che verificano ①, ②, ③. Definiamo $\rho \in \text{Rel}(S)$ con le formule $\forall a, b \in S \quad (a \rho b \Leftrightarrow a = a \wedge b)^*$, ovvero $(a \rho b \Leftrightarrow b = a \vee b)^*$, e questo perché:

$$\begin{aligned} \Rightarrow \forall a \rho b \Rightarrow a = a \wedge b \Rightarrow a \vee b = (a \wedge b) \vee b = b \quad \text{per ① e ③;} \\ \Rightarrow \forall b \rho a \Rightarrow b = a \vee b \Rightarrow a \wedge b = a \wedge (a \vee b) = a \quad \text{per ③} \Rightarrow a \rho b; \end{aligned}$$

Dimostriamo che $\rho \in \text{Rel}(S)$:

\hookrightarrow riflessiva: $\forall a \in S \quad (a \rho a)$ per ④, infatti $a = a \vee a = a \wedge a$;

\hookrightarrow antisimmetrica: $(a \rho b \wedge b \rho a) \Rightarrow a = a \wedge b = b \wedge a = b$ per ①;

\hookrightarrow transitiva: $(a \rho b \wedge b \rho c) \Rightarrow (a = a \wedge b \wedge b = b \wedge c) \Rightarrow a = a \wedge (b \wedge c)$, ma per ② $\Rightarrow a = (a \wedge b) \wedge c \Rightarrow a = a \wedge c \Rightarrow a \rho c$;

Dimostriamo adesso che (S, ρ) è un reticolo:

pongo $\forall a, b, c \in S \quad M := \{a, b\}^\downarrow$, quindi $c \in M \Leftrightarrow (c \rho a \wedge c \rho b)$, ovvero se e solo se $c = c \wedge a = c \wedge b \Rightarrow c = c \wedge b = (c \wedge a) \wedge b \stackrel{\text{②}}{=} c \wedge (a \wedge b) \Rightarrow c \rho (a \wedge b)$

Se dimostro che quando $a \wedge b$ appartiene a M , avrò dimostrato che $\forall a, b \in S \quad (a \wedge b) \rho (a \wedge b)$ ovvero che $a \wedge b = \text{MAX}(n) = \inf\{a, b\}$ $\forall a, b \in S$.

$a \wedge b \in M \Leftrightarrow ((a \wedge b) \rho a \wedge (a \wedge b) \rho b)$; ma:

$$[(a \wedge b) \rho a] = (a \wedge b) \wedge a \stackrel{\text{④}}{=} a \wedge (a \wedge b) = (a \wedge a) \wedge b \stackrel{\text{a.}}{=} a \wedge b$$

$$[(a \wedge b) \rho b] = (a \wedge b) \wedge b = a \wedge (b \wedge b) = a \wedge b$$

$$\begin{array}{c} a \wedge b \\ \uparrow \quad \uparrow \\ x \rho y \end{array} \Leftrightarrow x \wedge y = y \wedge x = x$$



$\Rightarrow a \wedge b \in M$, ovvero $\forall a, b \in S (\exists \inf\{a, b\} = a \wedge b)$. Soltanto, visto che vale (*),
 vale $\forall a, b \in S (\exists \inf\{a, b\} = a \wedge b \text{ e } \sup\{a, b\} = a \vee b) \Rightarrow (S, \leq)$ è un reticolo.

• ISOMORFISMI TRA RETICOLI

PROPOSIZIONE: siano (S, \leq) e (T, γ) reticoli con operazioni reticolari \wedge, \vee per S e \wedge, \vee per T . Sia $f: S \rightarrow T$ un'applicazione biettiva; allora f è un isomorfismo di insiami ordinati da $(S, \leq) \rightarrow (T, \gamma) \Leftrightarrow f$ è un isomorfismo di strutture algebriche $(S, \vee, \wedge) \rightarrow (T, \vee, \wedge)$.

Dimm) $\Rightarrow \forall a, b \in S a \wedge b = \inf_{(S, \leq)}\{a, b\}$ ha per immagine $f(a \wedge b) = \inf_{(T, \gamma)}\{f(a), f(b)\} = f(a) \wedge f(b)$ e dunque $f(a \vee b) = f(a) \vee f(b) \Rightarrow f$ isomorf. di struttr. algebriche.

\Leftarrow Per ipotesi $\forall a, b \in S f(a \wedge b) = f(a) \wedge f(b)$:

$a \leq b \Leftrightarrow a = a \wedge b \Leftrightarrow (a) = f(a \wedge b) = f(a) \wedge f(b) \Leftrightarrow f(a) \gamma f(b) \Rightarrow f$ è un isomorfismo di insiami ordinati.

• SOTTORETICOLI

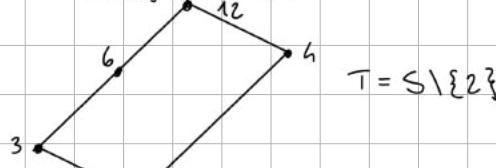
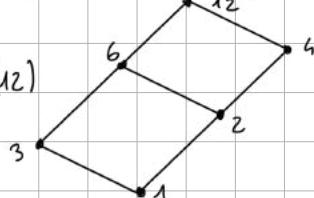
Siamo (S, \leq) un reticolo e $T \subseteq S$; definiamo (T, \leq) un sottoreticolo di (S, \leq) se e solo se T è una parte non vuota chiusa rispetto alle operazioni reticolari; gli intervalli chiusi di un reticolo sono sempre sottoreticolari.

Dimm) (S, \leq) reticolo $\Rightarrow \forall a, b \in S$ chiamo $I = [a, b] = \{x \in S \mid a \leq x \leq b\}$; allora:

$\forall x, y \in S a \leq (x \wedge y) \leq b \Rightarrow (x \wedge y) \in I \Rightarrow I$ è chiuso \Rightarrow sottoret.

(es)

$$S = \text{Distr}(12)$$



T è un reticolo, ma non è un sottoreticolo di (S, \leq) poiché non è chiuso rispetto a \wedge (estremo inferiore in S), infatti: $6 \wedge 4 = 2 \notin T$ (questo non vuol dire che in T $6 \wedge 4$ non è definito, infatti vale 1, ma l'operazione NON è chiusa perché $6 \wedge 4$ calcolato in S non appartiene a T).

• COMPLEMENTI

Sia (S, \leq) un reticolo limitato, $\forall a, b \in S$ diciamo che a è un **complemento** di $b \Leftrightarrow a \wedge b = \min(S, \leq) = \emptyset$ e $a \vee b = \max(S, \leq) = S$; non è escluso che un elemento abbia più di un complemento.

Un reticolo si dice **complementato** se ogni elemento è complementato.

(es) $(\text{P}(S), \subseteq)$ è un reticolo complementato; infatti $\min = \emptyset$ e $\max = S$ $\forall X \in \text{P}(S) (\exists S \setminus X)$ che lo complementa.

OSSERVAZIONE: $\min(S, \leq)$ e $\max(S, \leq)$ sono l'uno il complemento dell'altro; inoltre questo è l'unico caso in cui a e b possono essere complementi tra loro ed essere confrontabili.

• RETICOLI DISTRIBUTIVI

Sia (S, \leq) un reticolo con operazioni reticolari \wedge e \vee ; allora (S, \leq) è DISTRIBUTIVO \Leftrightarrow

$$\Leftrightarrow \begin{cases} \vee \text{ è distributiva rispetto a } \wedge; & \Leftrightarrow \begin{cases} a \vee(b \wedge c) = (a \vee b) \wedge (a \vee c), \\ a \wedge(b \vee c) = (a \wedge b) \vee (a \wedge c); \end{cases} \\ \wedge \text{ è distributiva rispetto a } \vee; \end{cases}$$

(es) In $(P(S), \leq)$ le operazioni reticolari sono \wedge e \vee , tre loro distributivit.

Visto che si tratta di una proprietà algebrica, se (S, \leq) è un reticolo, anche le sue sottostruzione ereditano le stesse proprietà. Attenzione, NON tutte le sue PARTI, ma solo i suoi sottoreticoli perché c'è bisogno che le operazioni reticolari siano chiuse e siano chiuse.

PROPOSIZIONE: se (S, \leq) è un reticolo limitato distributivo e $a \in S$, allora a ha al più un complemento (ma anche non avrà nemmeno).

Dim) Supponiamo per absurdum che x e y siano entrambi complementi di a , e sia $0 = \min(S, \leq)$ e $1 = \max(S, \leq)$, allora:

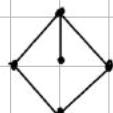
$$\begin{cases} a \wedge x = 0 = a \wedge y; \\ a \vee x = 1 = a \vee y; \end{cases} \Rightarrow x = x \wedge 1 = x \wedge (a \vee y) = (x \wedge a) \vee (x \wedge y) = 0 \vee (x \wedge y) = x \wedge y;$$

Similmente ricongraziamo che $y = y \wedge x = x \wedge y = x$.

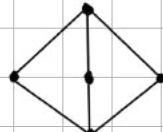
(es) in questo reticolo tutti gli elementi, eccetto uno che ne ha un unico, non hanno complementi; eppure non è distributivo, dunque il richiesto delle proposizioni non è verificato.

• TEOREMA (criterio di Birkhoff)

Sia (S, \leq) un reticolo, allora (S, \leq) è distributivo se e solo se nemmeno nessun sottoreticolo di (S, \leq) è isomorfo a un reticolo pentagonale o triangolare.



(P)ENTAGONALE



(T)RIETTANGOLO



OSSERVAZIONE: ogni reticolo con al più quattro elementi è distributivo;

• ANELLI BOOLEANI

Un anello booleano è un anello unitario in cui ogni elemento è idempotente. Se R è un anello unitario e indichiamo l'unità con 1_R , se esiste qualche intero positivo m tale che $m1_R = 1_R + 1_R + \dots + 1_R = 0_R$ allora la **CARATTERISTICA** di R è il minimo tale intero m .

Ovviamente R ha caratteristica 1 $\Leftrightarrow 1_R = 0_R$, e quindi $R = \{0_R\}$. Altrettanto banale è il caso in cui ha caratteristica 2, per cui $1_R \neq 0_R$ ma $2 \cdot 1_R = 0_R$.

PROPOSIZIONE: sia R un anello booleano; allora R è commutativo e se $|R| > 1$, R ha caratteristica 2 ($\Rightarrow \forall a \in R (2 \cdot a = a + a = 0_R)$.

Dim: $\forall a, b \in R$ $a^2 = a \cdot a = a$, $b^2 = b \cdot b = b$, $(a+b)^2 = (a+b) \cdot (a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2$, quindi, sempre per idempotenza $a+b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$; da ciò cancellando a e b si ricava $ab + ba = 0_R \Rightarrow \forall a, b \in R (ab = -ba)$. Applicandolo al caso in cui $a = b$, si ottiene $\forall a \in R (a^2 = -a^2) \Rightarrow$ per idempotenza $\Rightarrow \forall a \in R (a = -a)$ ovvero $\forall a \in R (2a = 0_R)$.

In particolare $2 \cdot 1_R = 0_R$ quindi se $1_R = 0_R$ e $R = \{0_R\}$ ha un solo elemento, oppure $|R| > 1$ e la caratteristica di R è 2.

Soltanto $\forall a, b$ sfruttando $a = -a$ per l'elemento $ba = -ba$, quindi per (*) ho scritto che $ab = ba \Rightarrow R$ è un anello commutativo. 

• TEOREMA DI STONE: sia R un anello booleano; allora:

- ↳ esiste un insieme S tale che R sia isomorfo a un sottoanello unitario di $(P(S), \Delta, \cap)$,
- ↳ se R è finito esiste un insieme S tale che R sia isomorfo a $(P(S), \Delta, \cap)$.

OSSERVAZIONE: tutti i sottoanelli unitari di $(P(S), \Delta, \cap)$ sono booleani.

↳ **Corollari:** sia R un anello booleano FINITO; allora:

- ① $\exists m \in \mathbb{N} (|R| = 2^m)$; questo perché è isomorfo a $P(S)$ e $|P(S)| = 2^{|S|}$;
- ② se T è un anello booleano e $|T| = |R|$ (sono equipotenti) $\Rightarrow T \cong R$;

• RETICOLI BOOLEANI

Un reticolo si dice booleano se e solo se è distributivo e complementato. Come raffigurare piùolare la nozione di reticolo come struttura algebrica (L, \wedge, \vee) e affinché L sia un reticolo booleano devono valere: oltre alle proprietà commutativa, associativa e alle leggi di annullamento di base, anche le proprietà distributiva (in modo che il reticolo sia distributivo), devono esistere gli elementi neutri di \wedge e \vee , ossia max e min (affinché sia limitato) e ogni elemento deve avere un complemento (consideriamo l'applicazione $' : a \in L \mapsto a' \in L$).

• ALGEBRE DI BOOLE

Si dice algebra di boole una struttura algebrica $(L, \vee, \wedge, 0, 1, ')$ tale che:

- ① $(L, \vee, 0)$ e $(L, \wedge, 1)$ sono monoidi commutativi; comm - assoc - il neutro
- ② valgono le leggi di annullamento: $\forall a, b \in L (a \vee \text{len} b) = a = a \wedge (\text{len} b)$; leggi
- ③ distributività di \wedge rispetto a \vee , e viceversa; distributività

(b) $\forall a \in L$ ($a \vee a' = 1$ e $a \wedge a' = 0$).

complemento

Per definizione quindi ogni reticolato booleano de luoghi è un'algebra di boole e, viceversa un'algebra di boole si può sempre riguardare come reticolato booleano.

OSSERVAZIONE: se prendo il duale di un reticolato complementato (-distributivo -booleano) questo sarà complementato (-distributivo -booleano).

• REGOLE DI CALCOLO

Sia $(L, V, \wedge, 0, 1, ')$ un'algebra di boole; allora $\forall a, b \in L$ valgono:

$$(i) 1 \vee a = 1 \quad e \quad 0 \wedge a = 0;$$

$$(ii) 1' = 0 \quad e \quad 0' = 1;$$

$$(iii) (a')' = a;$$

$$(iv) (a \vee b)' = a' \wedge b' \quad \left. \begin{array}{l} \\ \text{De Morgan} \end{array} \right\}$$

$$(a \wedge b)' = a' \vee b'$$

Dim) (i) e (ii) immediate perché L è un reticolato; per le (iii) e (iv) è un complemento di a e a' è un complemento di a , ma anche $(a')'$ è un complemento di a' ; quindi l'unicità dei complementi nei reticolati booleani comporta $a = (a')'$. Per le (iv) basta mostrare che $(a' \wedge b')$ è un complemento di $a \vee b$, ovvero che $(a \vee b) \vee (a' \wedge b') = 1$ e $(a \vee b) \wedge (a' \wedge b') = 0$, usando le distributività e le ①:

$$(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = (1 \vee b) \wedge (a \vee 1) = 1 \wedge 1 = 1,$$

$$(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = (0 \wedge b') \vee (0 \wedge a') = 0 \wedge 0 = 0;$$

L'altra legge di De Morgan regge per dualità $(a' \vee b')$ comp. di $a \wedge b$.



• **TEOREMA:** parlare di un anello booleano $(R, +, \cdot)$ è equivalente a parlare di un'algebra di boole $(R, V, \cdot, 0_R, 1_R, ')$.

(ex) per semplificare la dimostrazione guardiamo prima a un caso specifico: $(P(S), \Delta, \cap)$ è un anello booleano, ma $P(S)$ è anche un reticolato booleano con operazioni reticolari \vee e \wedge . La seconda operazione reticolare è proprio l'operazione di moltiplicazione dell'anello, mentre le prime si può esprimere in funzione delle operazioni dell'anello: $\forall A, B \in P(S)$

$$A \vee B = (A \Delta B) \cup (A \cap B) = (A \Delta B) \Delta (A \cap B). \quad$$
 Inoltre il min e il MAX dell'algebra di boole sono \emptyset e S , cioè lo zero e l'unità dell'anello, e un'urna $A \in P(S)$ ha come complemento $S \setminus A = S \Delta A = 1_{P(S)} \Delta A$.

Dim) \Rightarrow dobbiamo verificare che $(R, V, 0_R)$ e $(R, \cdot, 1_R)$ siano monoidi commutativi, che valgano per V e \cdot le leggi di assorbsimento e le proprietà distributive, ed infine che l'applicazione $'$ verifichi la condizione richiesta dalla definizione di complemento.

Come ci suggerisce l'esempio delimitiamo V come $a \vee b := a + b + ab$ e l'operazione $'$: $a \in R \mapsto 1_R + a \in R$.

\hookrightarrow è evidente che V sia commutativa e che 0_R ne sia l'elemento neutro, in quanto $a \vee 0_R = a + 0_R + a \cdot 0_R = a$.

\hookrightarrow assorbsività: $(a \vee b) \vee c = (a + b + ab) \vee c = a + b + ab + bc + ac + abc$
 $a \vee (b \vee c) = (b \vee c) \vee a = b + c + a + bc + ba + ca + bca$;

$\Rightarrow (R, V, 0_R)$ monoidale commutativo; che lo sia anche $(R, \cdot, 1_R)$ si già noto, in quanto R è un anello booleano.

- ↳ leggi di assorbimento: so che $\forall a, b \in R (a \vee ab = a + ab + a(ab))$, ma visto che R è booleano $\Rightarrow a(ab) = a^2b = ab$ e $ab + ab = 0_R \Rightarrow a \vee ab = a + ab + ab = a + 0_R = a$, inoltre $a \vee vb = a(e + b + eb) = a^2 + eb + a^2b = a + ab + eb = a + 0_R = a$. $\Rightarrow (R, \vee, +)$ rett. booleano
- ↳ distributività: $\forall a, b, c \in R a(b \vee c) = a(b + c + bc) = ab + ac + abc$ e $(ab) \vee (ac) = ab + ac + a^2bc = eb + ac + abc \Rightarrow a(b \vee c) = (ab) \vee (ac)$.
- ↳ resta infine da verificare che $\forall a \in R (a \vee (1_R + a) = 1_R)$ e $(aa') = 0_R$ con $a' = 1_R + a$; abbontante ovvio perché $aa' = a(1_R + a) = a + a = 0_R$ e $a \vee a' = a + a' + aa' = a + (1_R + a) + 0_R = 2a + 1_R + 0_R = 0_R + 1_R = 1_R$.

\Leftarrow (v) partendo dall'algebra $(\mathcal{B}(S), \cup, \cap, \emptyset, S)$ per esprimere le rette operazioni binarie (Δ) in funzione delle due che abbiamo a disposizione, abbiamo due possibili strade, che come vedremo, ci porteranno a uno stesso risultato:

$$A \Delta B = \begin{cases} (A \cup B) \setminus (A \cap B) & \text{(1)} \\ (A \setminus B) \cup (B \setminus A) & \text{(2)} \end{cases}$$

operazione unaria di complemento

Tornando al caso generale quindi, partendo da un'algebra $(L, \vee, \wedge, 0, 1, {}')$

$$\begin{aligned} \textcircled{1} \quad (a \wedge b)' \vee (a' \wedge b) &= (a \vee a') \wedge (a \vee b) \wedge (b \vee a') \wedge (b \vee b') \text{ per distributività di } \vee \text{ su } \wedge \\ &= 1 \wedge (a \vee b) \wedge (b \vee a') \wedge 1 = (a \vee b) \wedge (a' \vee b') = \text{uso de Morgan } (a' \vee b') = (a \wedge b)' \\ \textcircled{2} \quad &= (a \vee b) \wedge (a \wedge b)' = a + b. \end{aligned}$$

Quindi manca una qualsiasi delle formule date dall'esempio descriviamo la stessa operazione $a + b$ che si dimostra essere commutativa, associativa con 0 come elemento neutro e con ogni elemento simmetrico di se stesso $\Rightarrow (L, +)$ è un gruppo abeliano. Visto che già sappiamo che $(L, \wedge, 1)$ è un monoido commutativo e si dimostra che \wedge si distribuisce rispetto a $+$ $\Rightarrow (L, +, \wedge)$ è un anello booleano.

SOTTOALGEBRA DI BOOLE

Dunque una sottoalgebra di boole è una parte non vuota che sia chiusa rispetto a \wedge e \vee (\wedge e \vee sono rettangolari), e che contenga 0_R e 1_R , e che sia anche chiusa rispetto all'operazione $'$. Una parte è una sottoalgebra di boole \Leftrightarrow è un sottoanello booleano.

Una delle proprietà di \mathbb{N} è che è **BEN ORDINATO**, ovvero vale che:

$$\forall X \in \mathcal{P}(\mathbb{N}) (\{X \neq \emptyset\} \Rightarrow \exists \min(X, \leq))$$

OSSERVAZIONE: gli insiemini ben ordinati sono sicuramente totalmente ordinati. Quando dovo fare una dimostrazione per induzione in \mathbb{N} posso quindi fare la seguente considerazione (unica è \mathbb{N} perché è ben ordinato): sic $X = \{m \in \mathbb{N} \mid \neg(p(m))\}$, la negazione di $\forall m \in \mathbb{N} (p(m))$ è $\exists m \in \mathbb{N} (\neg(p(m))) \Rightarrow X \neq \emptyset \Rightarrow \exists \min(X, \leq)$. La conseguenza più utile e interessante di questa osservazione è la dimostrazione del principio di induzione.

TEOREMA (dim principio di induzione)

Sic p un predicato vero in m , $b \in \mathbb{N}$ e $\mathbb{N}_b = \{x \in \mathbb{N} \mid x \geq b\}$, allora vale: $(p(b) \wedge \forall m \in \mathbb{N} (p(m) \Rightarrow p(m+1))) \Rightarrow \forall m \in \mathbb{N}_b (p(m))$.

Dim) sic $X = \{m \in \mathbb{N}_b \mid (\neg(p(m)))\}$; se $X \neq \emptyset \Rightarrow \exists \min(X, \leq) = m$. Si ha $m \neq b$, perché abbiamo ammesso per ipotesi $p(b)$, cioè $b \notin X \Rightarrow m > b$.

Ma $m-1 < m = \min X$, dunque $m-1 \notin X \Rightarrow p(m-1)$ è vera. Applicando però il passo induuttivo abbiamo $p(m-1) \Rightarrow p((m-1)+1) = p(m)$, che è una contraddizione rispetto alle ipotesi, in quanto è falsa (antecedente vero, succinno falso), contraddizione mate dall'aver supposto $X \neq \emptyset$.
 $\Rightarrow X = \emptyset \Rightarrow \forall m \in \mathbb{N}_b (p(m))$.

• SECONDA FORMA DEL PRINCIPIO DI INDUZIONE

$\forall t \in \mathbb{N}_b$ definisco $M_t = \{x \in \mathbb{N}_b \mid x < t\} = [b, t]_{\mathbb{N}_b}$
 $\forall t \in \mathbb{N}_b (\forall m \in M_t (p(m)) \Rightarrow p(t)) \Rightarrow \forall m \in \mathbb{N}_b (p(m))$.

• ELEMENTI ASSOCIATI

Sia $(M, \cdot, 1)$ un monoside commutativo: si definisce la relazione di divisibilità come: $\forall a, b \in M (a|b \Leftrightarrow \exists c \in M (b = ac))$, e diciamo che due elementi sono associati se e solo se: $a|b \Leftrightarrow (a|b \wedge b|a)$. Questa relazione "due elementi associati" è chiaramente riflessiva, simmetrica e transitiva \Rightarrow è una relazione di equivalenza.

PROPOSIZIONE: $\forall a, b \in M$, siamo $a|b$ e $b|a'$; allora $a|b \Leftrightarrow a'|b'$.

Dimm) se $a|b$ abbiamo per ipotesi: $a|a, a|b, b|b' \Rightarrow a|b'$ per la transitività; il viceversa è equivalente ($a|a, a|b', b|b' \Rightarrow a|b$).

PROPOSIZIONE: $\forall a, b \in M$, $a|b \Leftrightarrow \text{Div}(a) = \text{Div}(b) \Leftrightarrow a|M = b|M$ (ovvero se hanno gli stessi divisori e gli stessi multipli); con $\text{Div}(a) = \{d \in M \mid d|a\}$ e invece $a|M = \{ax \mid x \in M\} = \{m \in M \mid a|m\}$.

Dimm) $\Rightarrow \forall d \in \text{Div}(a)$ da $d|a$ e $a|b$ segue $d|b$ per transitività, ovvero $d \in \text{Div}(b)$, $\Rightarrow \text{Div}(a) \subseteq \text{Div}(b)$. Chiaramente è analogo dimostrare che $\text{Div}(b) \subseteq \text{Div}(a) \Rightarrow \text{Div}(b) = \text{Div}(a)$.
 \Leftarrow poiché $a \in \text{Div}(a)$, se vale $\text{Div}(a) = \text{Div}(b) \Rightarrow a \in \text{Div}(b) \Rightarrow a|b$; similmente $d \in \text{Div}(b) = \text{Div}(a) \Rightarrow b|a$.

La dimostrazione per i multipli è analogo.

PROPOSIZIONE: $\forall n \in \mathbb{U}(n)$, $\forall a \in M$ ($a|an$)

Dimm) ovviamente $a|an$ e, se considero $a = (an)n \Rightarrow an|a \Leftrightarrow \{\exists i \in M \mid a = (an)i\}$.

PROPOSIZIONE: se a è cancellabile in M , si ha che $\{an \mid n \in \mathbb{U}(n)\} = [a]_n$

Dimm) ragioniamo già che $\forall n \in \mathbb{U}(n) (a|an)$, quindi si verifica un'inclusione; per verificare l'uguaglianza dobbiamo anche dimostrare che ogni associato ad a è della forma an per un opportuno $n \in \mathbb{U}(n)$.

Sia $b \in M$, se $b|a$:

$$\hookrightarrow a|b \Rightarrow \exists n \in M (b = an) \Rightarrow a \cdot 1_n = a = b \cdot n = a(n)_n$$

$$\hookrightarrow b|a \Rightarrow \exists n \in M (a = bn)$$

poiché a è cancellabile per ipotesi $\Rightarrow an = 1_n \Rightarrow n = 1 \in \mathbb{U}(n)$.

OSSERVAZIONE: in \mathbb{N} gli elementi associati devono essere per forza uguali perché esiste un solo elemento invertibile.

OSSERVAZIONE: $\forall a \in M$, tra i divisori di a ci sono:

- ↳ gli associati ad a ;
- ↳ gli elementi invertibili di M : $(a = m \text{ e } a^{-1}) \Rightarrow a \in U(M)$

Chiameremo questi: i DIVISORI BANALI di a ;

Diciamo invece che a è **IRRIDUCIBILE** in (M, \cdot) se e solo se:

- ↳ $a \notin U(M)$;
- ↳ a non ha in M divisori NON banali;

Gli irreducibili in (\mathbb{N}^*, \cdot) si chiamano numeri PRIMI.
Attenzione: 1 non è primo perché $\in U(\mathbb{N}^*)$

MONIDI FATTOREIALI

Scriviamo (supponendo se possibile farlo) a come prodotto di irreducibili come:

- $a = p_1 p_2 \dots p_t$ dove $t \in \mathbb{N}^*$ e $\forall i \in \{1, \dots, t\}$ p_i è irreducibile;
- $a = q_1 q_2 \dots q_s$ dove $s \in \mathbb{N}^*$ e $\forall i \in \{1, \dots, s\}$ q_i è irreducibile;

(*) Diciamo che queste due fattorizzazioni di a come prodotto di irreducibili sono **essenzialmente uguali** se e solo se:

$$\hookrightarrow s = t;$$

↳ i fattori p_i e q_j sono gli stessi e meno dell'ordine e delle costituzioni di alcuni di essi con elementi associati, vale a dire che $\exists \sigma \in \text{Sym}(\{1, \dots, t\})$ ($\forall i \in \{1, \dots, t\}$ $(q_{\sigma(i)} \sim p_i)$) \rightarrow fondamentale perché $p_1 \cdot p_2 = q_2 \cdot q_1 = (\mu p_1)(\mu^{-1} p_2)$

(es) in (\mathbb{N}, \cdot) abbiamo:

$$12 = 2 \cdot 2 \cdot 3$$

$$(a) 2 \cdot 3 = 3 \cdot 2 = (-1 \cdot 2)(-1 \cdot 3) \text{ quindi per l'uguaglianza}$$

$$12 = (-2) \cdot 2 \cdot (-3)$$

tra i fattori p_i e q_j non basta $p_i = q_j$, ma serve $\mu(p_i) = \mu(q_j)$

$$12 = 2 \cdot (-3) \cdot (-2)$$

Un monoido commutativo (M, \cdot) è **FATTOREIALE** se e solo se:

① è cancellativo; (ogni elemento è cancellabile)

② ogni elemento di $M \setminus U(M)$ è prodotto di irreducibili in modo essenzialmente unico. (*)

Un ANELLO FATTOREIALE è un anello unitario con olomorfismo di integrità $(R, +, \cdot)$

tole che $(R \setminus \{0_R\}, \cdot)$ sia un monoido fattoriale.

N.B.: $\exists t \in \mathbb{N}$ i gruppi d'elaborazione sono monoidi fattoriali

TEOREMA FONDAMENTALE DELL'ARITMETICA

- ① $(\mathbb{N}^*, \cdot, 1)$ è un monoido fattoriale;
- ② $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$ è un monoido fattoriale;
- ③ $(\mathbb{Z}, +, \cdot)$ è un anello fattoriale.

Di questo teorema non facciamo le dimostrazioni complete, bensì una parziale; nello specifico dimostriamo che ogni numero intero diverso da 0, 1 e -1, è prodotto di primi: $\forall m \in \mathbb{N}^* (m > 1 \Rightarrow m \text{ prodotto di primi}) \rightarrow$ irreducibili in \mathbb{Z}^*

Dim) per assurdo suppongo $X = \{m \in \mathbb{N} \mid m > 1 \wedge m \text{ non è prodotto di primi}\} \neq \emptyset$

$\Rightarrow \exists \min(X) = m$ che non è primo e, poiché $m > 1$, ha qualche divisore non banale a . Quindi $\exists b \in \mathbb{N}^* (m = ab)$, con $1 < a < m$ e $1 < b < m$. Ne segue che $a, b \notin X$ (risulta che $m = \min(X)$), cioè a e b sono prodotti di primi \Rightarrow anche m . Abbiamo quindi raggiunto l'assurdo.

OSSERVAZIONE: ossia che per $\forall m \in \mathbb{Z} \setminus \{0, 1, -1\}$ (m è prodotto di numeri primi) in quanto per $m < -1$ ($m = (-p_1)p_2 \dots p_n$) $\Rightarrow -m = p_1 p_2 \dots p_n$.

PROPOSIZIONE: $\forall p \in \mathbb{Z} (\text{p primo} \Rightarrow \forall a, b \in \mathbb{Z} (p \mid ab \Rightarrow p \mid a \vee p \mid b))$.

Dim) $a = p_1 \dots p_m$ $b = q_1 \dots q_n$; se per ipotesi $p \mid ab \Rightarrow \exists c \in \mathbb{Z} (ab = pc)$
com $c = m_1 \dots m_t \Rightarrow p m_1 \dots m_t = p_1 \dots p_m q_1 \dots q_n$

PROPOSIZIONE: sia R un anello commutativo; $\forall a, b, c \in R (a \mid b \wedge a \mid c) \Rightarrow a \mid bu + cv$:
ossvero a divide tutte le combinazioni lineari in R tra b e c .

Dim) $\exists \beta, \gamma \in R (a\beta = b \wedge a\gamma = c) \Rightarrow bu + cv = a\beta u + a\gamma v = a(bu + cv) \Rightarrow a \mid bu + cv$

PROPOSIZIONE: in \mathbb{N}^* sia $a = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, dove $t \in \mathbb{N}^* \wedge \forall i \in \{1, \dots, t\} p_i$ è primo e
inoltre per $i \neq j \Rightarrow p_i \neq p_j$, e $\alpha_i \in \mathbb{N}$. I divisori di a in \mathbb{N}^* sono tutti e soli i
numeri delle forme $p_1^{\lambda_1} \dots p_t^{\lambda_t}$ dove $\forall i \in \{1, \dots, t\} (\lambda_i \leq \alpha_i \in \mathbb{N})$; infine questi
divisori sono esattamente $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_t + 1)$.

$$(\text{es}) 12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3^1 = 2^2 \cdot 3^1 \cdot 5^0 \hookrightarrow (2+1)(1+1) = 3 \cdot 2 = 6 \text{ divisori}$$

$$\text{Divs}(12) = \{z^{\lambda_1} \cdot 3^{\lambda_2} \mid \lambda_1 \in \{0, 1, 2\} \wedge \lambda_2 \in \{0, 1\}\}$$

$$2^0 \cdot 3^0 = 1 \cdot 1 = 1$$

$$2^0 \cdot 3^1 = 1 \cdot 3 = 3$$

$$2^1 \cdot 3^0 = 2 \cdot 1 = 2$$

$$2^1 \cdot 3^1 = 2 \cdot 3 = 6$$

$$2^2 \cdot 3^0 = 4 \cdot 1 = 4$$

$$2^2 \cdot 3^1 = 4 \cdot 3 = 12$$

OSSERVAZIONE: sia $d = p_1^{\lambda_1} \dots p_t^{\lambda_t}$ un divisore di $a = p_1^{\alpha_1} \dots p_t^{\alpha_t}$; poniamo pure
 $a = db$ per un opportuno $b \in \mathbb{N}^+$. Se $\lambda_1 > \alpha_1$ otteniamo che:

$$p^{\lambda_1 - \alpha_1} p_2^{\lambda_2} \dots p_t^{\lambda_t} \cdot b = p_1^{\alpha_1} \dots p_t^{\alpha_t} \Rightarrow \text{ASSURDO!} \Rightarrow \lambda_1 \leq \alpha_1.$$

N.C.M e M.C.D

Siano $a, b \in \mathbb{N}^*$, con $a = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ e $b = p_1^{\beta_1} \dots p_t^{\beta_t}$; i divisori comuni sono i
numeri delle forme $p_1^{\lambda_1} \dots p_t^{\lambda_t}$, dove $\forall i \in \{1, \dots, t\} (\lambda_i \leq \min\{\alpha_i, \beta_i\} = s_i)$.

Allora $p^{s_1} \dots p^{s_t}$ è un MASSIMO COMUNE DIVISORE di $\{a, b\}$.

Similmente $p_1^{\alpha_1} \dots p_t^{\alpha_t}$ è un MINIMO COMUNE MULTIPLO $\forall i \in \{1, \dots, t\} (\alpha_i = \max\{\lambda_i, \beta_i\})$.

PROPOSIZIONE: se (M, \circ) un monoido commutativo con $X \subseteq M$ e $d = \text{N.C.D}(X)$ in (M, \circ) .

Allora $\forall h \in M (h \text{ è un M.C.D.} \Leftrightarrow h \sim d)$

• COMPATIBILITÀ

Sia $(S, *)$, con $* : S \times S \rightarrow S$ e $\sim \in \text{Eq}(S)$. Poniamo definire:

$\star ([a]_n, [b]_n) \in S/n \times S/n \mapsto [a * b]_n \in S/n$; che risulta ben definita se e solo se
 $\forall a, a', b, b' \in S \quad ([a]_n, [b]_n) = ([a']_n, [b']_n) \Rightarrow [a * b]_n = [a' * b']_n$, ovvero se:
 $(a \sim a' \wedge b \sim b') \Rightarrow (a * b) \sim (a' * b')$.

Se valgono queste condizioni, \star è ben definita, e dice che $* \circ \sim$ sono COMPATIBILI.

$$(\text{es}) S = \mathbb{Z}, * = +, S/0 = \{\mathbb{N}^*, \{0\}, \mathbb{Z} \setminus \mathbb{N}^*\}$$

$$\mathbb{N}^* \oplus \mathbb{Z} \setminus \mathbb{N}^* = \begin{cases} [1]_0 & \oplus [-3]_0 = [1-3]_0 = [-2]_0 \in \mathbb{Z} \setminus \mathbb{N}^* \Rightarrow + \circ \sim \text{NON compatibili} \\ [10]_0 & \oplus [-3]_0 = [10-3]_0 = [7]_0 \in \mathbb{N}^* \end{cases}$$

Ricordiamo che la proiezione canonica è l'applicazione $E : a \in S \mapsto [a]_n \in S/n$ e in
questo caso è un omomorfismo, ovvero $E(a * b) = [a * b]_n = [a]_n * [b]_n = E(a) * E(b)$.

E visto che la proiezione canonica è sempre multivoca, per gli omomorfismi si rilettino in
comunione la commutatività, l'associatività e l'eventuale elemento neutro.

$\Rightarrow (\mathbb{Z}_n, \circ)$ è un monoido commutativo

• COMPATIBILITÀ

- ↳ \sim è compatibile a \otimes con $* \Leftrightarrow \forall a, b, b' \in S (b \sim b' \Rightarrow a * b \sim a * b')$;
- ↳ \sim è compatibile a \otimes con $*$ $\Leftrightarrow \forall a, a', b \in S (a \sim a' \Rightarrow a * b \sim a' * b)$;
- \sim è compatibile con $*$ $\Leftrightarrow \sim$ è compatibile e \otimes e \otimes .

Dimm) $\forall a, b, a', b' \in S$ dimostriamo che $(a \sim a' \wedge b \sim b' \Rightarrow a * b \sim a' * b')$

$$\left. \begin{array}{l} a \sim a' \text{ (applico } \otimes \text{)} \Rightarrow a * b \sim a' * b \\ b \sim b' \text{ (applico } \otimes \text{)} \Rightarrow a * b \sim a' * b' \end{array} \right\} \Rightarrow a * b \sim a' * b' \text{ per transitività.}$$

Quindi per verificare che $*$ sia commutativa, basta vedere se \sim è compatibile e \otimes e \otimes .

N.B. = se una RELAZIONE DI EQUIVALENZA è compatibile con tutte le operazioni di una struttura algebrica, allora questa è una CONGRUENZA.

• MODULI E CONGRUENZE

$\forall m \in \mathbb{Z}$ definiamo $\equiv_m \in E_q(\mathbb{Z})$, con $a \equiv_m b \Leftrightarrow m \mid (a - b)$.

• riflessiva: $\forall a \in \mathbb{Z} (a \equiv_m a)$, infatti $m \mid a - a = 0$;

• simmetrica: $\forall a, b \in \mathbb{Z} (a \equiv_m b \Rightarrow b \equiv_m a)$, perché $m \mid a - b \Leftrightarrow m \mid -(a - b) = b - a$;

• transitiva: $\forall a, b, c \in \mathbb{Z} (a \equiv_m b \wedge b \equiv_m c \Rightarrow a \equiv_m c)$

$$\Rightarrow m \mid a - b \wedge m \mid b - c$$

$$\Rightarrow \exists u, v ((a - b) = mu \wedge (b - c) = mv)$$

$$\Rightarrow (a - b) + (b - c) = m(u + v)$$

$$\Rightarrow m \mid (a - b) + (b - c) = a - c$$

Adeguo che abbiamo dimostrato che \equiv_m è una relazione di equivalenza, non ci serve che dimostrare la compatibilità dx rispetto alle operazioni dell'anello $(\mathbb{Z}, +, \cdot)$; chiaramente basta verificare solo quelle dx perché entrambe le operazioni sono commutative.

Ora bisogna dimostrare che: $\forall a, b, c \in \mathbb{Z} (a \equiv_m b \Rightarrow (a + c) \equiv_m b + c \wedge ac \equiv_m bc)$.

→ compatibile con $+$:

$\forall a, b, c \in \mathbb{Z} a \equiv_m b \Leftrightarrow m \mid (a - b)$ per ipotesi; devo verificare che regga:

$$a + c \equiv_m b + c \Leftrightarrow m \mid (a + c) - (b + c) = a - b.$$

→ compatibile con \cdot :

$\forall a, b, c \in \mathbb{Z} a \equiv_m b \Leftrightarrow m \mid (a - b)$ devo verificare che $ac \equiv_m bc$;

$$\Rightarrow m \mid ac - bc = (a - b)c.$$

→ \equiv_m è una CONGRUENZA in $(\mathbb{Z}, +, \cdot)$, inoltre vale la proprietà distributiva:

$$[a]([b] + [c]) = [a(b + c)] = [ab + ac] = [a] \cdot [b] + [a] \cdot [c].$$

OSSERVAZIONE

- \equiv_0 è la relazione di ugualanza in \mathbb{Z} ;
- \equiv_1 è la relazione minore o uguale in \mathbb{Z} ;
- \equiv_2 è la relazione "avere le stesse parità";
- $\equiv_m = \equiv_{-m}$
- $\forall m \in \mathbb{Z}, \forall a, b \in \mathbb{Z} (a \equiv_m b \Rightarrow \forall d \in \text{Div}(m) |(a \equiv_d b)|)$

$\forall a, b$ chiamiamo COMBINAZIONE LINEARE di a e b ogni numero intero che si può scrivere come $\alpha a + \beta b$ per opportuni $\alpha, \beta \in \mathbb{Z}$.

• CLASSI DI RESTO

$\forall a, m \in \mathbb{Z}$ definiamo $[a]_m := \{b \in \mathbb{Z} \mid a \equiv_m b\} = a + m\mathbb{Z}$; questo perché se $a \equiv_m b \Rightarrow m \mid b - a \Rightarrow \exists k \in \mathbb{Z} (b - a = km) \Rightarrow b = a + mk$. Scriviamo inoltre che: $\mathbb{Z}/\equiv_m = \mathbb{Z}_m = \{[a]_m \mid a \in \mathbb{Z}\}$ è un anello commutativo unitario.

PROPOSIZIONE: Sia $m \in \mathbb{Z} \setminus \{0\}$, $\forall a \in \mathbb{Z} ([a]_m \cap \mathbb{N} \neq \emptyset)$ perché

Dim: Se l'intersezione è vuota, allora, visto che \mathbb{N} è ben ordinato, $\exists r = \min(\mathbb{N} \cap [a]_m)$ tale rispetta $r \equiv_m a$ e $0 \leq r < |m|$ questo perché $r \equiv_m r - lm$ per definizione di classe di resto $\Rightarrow (r - lm) \in [a]_m$; inoltre $r - lm < r = \min(\mathbb{N} \cap [a]_m) \Rightarrow$ per definizione di n , $r - lm \notin (\mathbb{N} \cap [a]_m) \Rightarrow r - lm \notin \mathbb{N} \Rightarrow r - lm < 0$. Verificato dal fatto che se $r < m$ ovviamente $r - m < 0$.



Quindi ogni classe mod m contiene un elemento compreso tra 0 e $m-1$ che quindi è ancora una classe. Allora $\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$ con elementi tutti diversi, infatti: siamo $i, j \in \mathbb{N}$ e supponiamo $[i]_m = [j]_m$ e $i, j < |m|$; $\Rightarrow i \equiv_m j \Rightarrow m \mid j - i \Rightarrow \exists k \in \mathbb{Z} (j - i = mk)$, ma l'unico multiplo di m positivo e minore di $|m|$ è $0 \Rightarrow j - i = 0 \Rightarrow j = i$. $\Rightarrow |\mathbb{Z}_m| = |m|$

Nell'anello \mathbb{Z}_m $[0]_m$ è l'elemento neutro e $[1]_m$ è l'unità; vogliamo:

$$\hookrightarrow c \cdot [1]_m = [c]_m;$$

$$\hookrightarrow [c]_m = [0]_m \Leftrightarrow c \equiv_m 0 \Leftrightarrow m \mid c - 0 \Leftrightarrow m \mid c;$$

Quindi $|m|$ è il periodo (caratteristico) di \mathbb{Z}_m .

• TEOREMA DELLA DIVISIONE CON RESTO

$\forall a, b \in \mathbb{Z}, b \neq 0 \Rightarrow \exists! (q, r) \in \mathbb{Z} \times \mathbb{N} (a = bq + r \wedge r < |b|)$

Dim: esistenza: sia $r \equiv_b n = \min([a]_b \cap \mathbb{N}) \Rightarrow 0 \leq r < |b|$ come abbiamo visto prima; inoltre, per definizione di classe di resto, $r = a + bk$, ovvero, se chiammo $q := -k$, ottengo: $a = m + bq$.

unicità: se esistesse un'altra coppia (q', r') ($a = bq' + r' \wedge r' < |b|$) si avrebbe $r' \equiv_b a$, ma vale anche $r \equiv_b a \Rightarrow r \equiv_b r'$, allora $r = r'$. Inoltre vale: $bq + r = a = bq' + r' \Rightarrow q = q'$.



q e r si chiamano QUOTIENTE e RESTO della divisione, e il dividendo è b il divisore.

• PERIODO NELLE CLASSI DI RESTO

Sia $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ inseribile perché $[5]_6 = [-1]_6$
 $\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$
 $0_{z_6} \quad 1_{z_6} \quad \text{divisione dello} \quad \text{zero}$ e -1 è inseribile in \mathbb{Z}

Infatti $[4]_6 \cdot [3]_6 = [12]_6 = [0]_6 = 0_{z_6} \wedge [2]_6 \cdot [3]_6 = [6]_6 = [0]_6 = 0_{z_6}$; allora \mathbb{Z}_m non è un dominio di integrità visto che non vale le leggi di annullamento del prodotto. Inoltre gli elementi inseribili sono cancellabili.

La definizione di classe di resto ha a che fare con la nozione di periodi: siamo $(G, \cdot, 1_G)$ un gruppo, $x \in G$ e m il periodo finito di x (ovvero m è il più

piccolo intero positivo tale che $x^m = 1_G$). Abbiamo che:

$$\textcircled{1} \quad \forall a \in \mathbb{Z}, \quad x^a = x^{\text{rest}(a,m)}$$

Dim) $\eta = \text{rest}(a,m) \Rightarrow \exists k \in \mathbb{Z} (a = mk + \eta)$; allora: $x^a = x^{mk+\eta} = x^{mk} \cdot x^\eta$ per quello che abbiamo appena scoperto, ma $x^{mk} = (x^m)^k = (1_G)^k = 1_G \Rightarrow x^\eta = x^\eta$

$$\textcircled{2} \quad \forall a, b \in \mathbb{Z} \quad x^a = x^b \Leftrightarrow a \equiv_m b \Leftrightarrow \text{rest}(a,m) = \text{rest}(b,m);$$

Dim) $\eta_1 \leq a = mk + b \Rightarrow a = mk + b \Rightarrow x^a = x^{mk} \cdot x^b = 1_G \cdot x^b = x^b$. Viceversa:
 $\Rightarrow a \leq b \Rightarrow x^{a-b} = 1_G = x^0 \Rightarrow a \equiv_m b$

• CRITERIO DI DIVISIBILITÀ

Banalmente seppiamo ragionare in base 10; un numero n è infatti:

$M = a_0 + 10 \cdot a_1 + 100 \cdot a_2 + \dots + 10^t \cdot a_t = \sum_{i=0}^t a_i \cdot 10^i$. Questo criterio può essere applicato a qualunque base; in quelle q ad esempio $\forall i \in \mathbb{N} \quad 10^i \equiv_q 1$, allora abbiamo $m \equiv_q \sum_{i=0}^t a_i \cdot 1 = \sum_{i=0}^t a_i$. Adesso il resto di un numero, ad esempio 271 in base 9 è $2+7+1 = 9+1$; quindi $271 \equiv_9 1$.

• DIVISORE COMUNE, MCD, mcm

Sia (S, \cdot) un semigruppo commutativo, sia $X \subseteq S$ e $d \in S$. Ricordiamo che $\forall a, b \in \mathbb{Z}$, $\forall m \in \mathbb{Z} \setminus \{0\}$, $(a \equiv_m b \Leftrightarrow \text{rest}(a,m) = \text{rest}(b,m))$, quindi \equiv_m è il nucleo di equivalentie dell'applicazione $a \in \mathbb{Z} \mapsto \text{rest}(a,m) \in \mathbb{N}$.

- d è un divisore comune degli elementi di X in (S, \cdot) $\Leftrightarrow \forall x \in X (d|x)$,
- Un MCD di X è un divisore comune a tutti gli elementi di X che è multiplo di tutti i divisori comuni di X ; ovvero per $X = \{a, b\}$, d è MCD \Leftrightarrow
 $\Leftrightarrow (d|a \wedge d|b \wedge (\forall c \in S (c|a \wedge c|b) \Rightarrow c|d))$.
- Un mcm di X è un multiplo comune a tutti gli elementi di X che è divisore di tutti i multipli comuni di X .

In un monosiale fattoriale, per come li abbiamo definiti precedentemente, esistono sempre un MCD e un mcm.

• ALGORITMO EUCLideo DELLE DIVISIONI SUCCESSIVE

Siano $a, b, q, r \in \mathbb{Z}$ tali che $a = bq + r$; allora i divisori comuni di a e b in \mathbb{Z} sono tutti e soli i divisori comuni di b e r . Osservi: $\forall d \in \mathbb{Z} (d|a \wedge d|b) \Leftrightarrow$
 $\Leftrightarrow (d|r \wedge d|b)$ perché a è combinazione lineare di b e r . Supponiamo di voler calcolare i MCD tra a e b , allora questi saranno esattamente gli stessi tra b e r . Il vantaggio è che $r < |b|$, quindi abbiamo ridotto la ricerca al numero dei naturali.

Per qualsiasi elemento x, y di un qualsiasi insieme vale che se $x|y$ allora x è un MCD(x, y), in quanto $x|x \wedge x|y \wedge (\forall c \in S (c|x \wedge c|y) \Rightarrow c|x)$.

Allora se $r = 0$, $a|b$ e ho risolto in quanto $\text{MCD}(a, b) = a$; altrimenti, se così non fosse, ho $b = qr_1 + r_1$ tale che $|b| > r > r_1$. Ma i $\text{MCD}(b, r) = \text{MCD}(r, r_1)$, quindi se $r_1 \neq 0$, procedo ricorrendo $r = r_1 q_2 + r_2$, con $|r_2| > r_1 > r_2$.

Al massimo dopo r paraggiamo a 0:

$$\begin{aligned} r_t &= r_{t+1} q_{t+2} + r_{t+2} \\ r_{t+1} &= r_{t+2} q_{t+3} + 0 \end{aligned} \quad \left. \begin{array}{l} \text{l'ultimo resto } \neq 0 \text{ è il } \text{MCD}(a, b) = \text{MCD}(r_{t+1}, r_{t+2}) = r_{t+2} \end{array} \right\}$$

• TEOREMA DI BEZOUT

Siano $a, b \in \mathbb{Z}$, ma $d \in \text{MCD}(a, b)$ e $c \in \mathbb{Z}$. Sono equivalenti:

$$\textcircled{1} \exists u, v \in \mathbb{Z} (d = au + bv) \Leftrightarrow d | (au + bv) \quad \text{e} \quad d | (a(u+k) + b(v-k)) = d;$$

$$\text{Dim: } a = bq + r \Rightarrow \text{Div}(a) \cap \text{Div}(b) = \text{Div}(b) \cap \text{Div}(r);$$

$$\forall d \in \mathbb{Z}, d \in \text{MCD}(a, b) \Leftrightarrow d \in \text{MCD}(b, r)$$

$$\forall m \in \mathbb{Z} \quad m | b \wedge m | a \Rightarrow m | r = ba + r$$

$$m | a \wedge m | b \Rightarrow m | r = a + b(-q)$$



Se MCD è combinazione lineare dei due numeri precedenti (ne ne intorno di più), vuol dire che sono associati).

$$\textcircled{2} \exists u, v \in \mathbb{Z} (c = au + bv) \Leftrightarrow d | c: \text{equivalente a: } \{au + bv \mid u, v \in \mathbb{Z}\} = d\mathbb{Z}.$$

$$\text{Dim 1} \Rightarrow 2 \quad \forall k \in \mathbb{Z}, \text{ se } d = au + bv \text{ allora } dk = a(uk) + b(vk);$$

$$\text{Dim 2} \Rightarrow 1 \quad \text{poiché } d | a \wedge d | b \Rightarrow \forall u, v \in \mathbb{Z} (d | au + bv).$$



L'insieme dei multipli dell' MCD è l'insieme di tutte le combinazioni lineari.

$$\textcircled{3} \text{ Prese } d = \text{MCD}(a, b), \text{ l'equazione diante } ax + by = c \text{ ha soluzioni re e solo re } d | c.$$

\hookrightarrow un'equazione diante è un'equazione in cui le incognite sono numeri reali.

$$\textcircled{4} a \text{ e } b \text{ sono coprimi} \Leftrightarrow \text{1 è combinazione lineare di } a \text{ e } b \Leftrightarrow \exists u, v \in \mathbb{Z} (1 = au + bv)$$

\hookrightarrow LEMMA DI EUCLIDE (conseguenze del teorema di Bezout)

$$\forall a, b, c \in \mathbb{Z} (a \text{ e } b \text{ coprimi} \wedge a | bc) \Rightarrow a | c$$

Dim per il teorema di Bezout, $\exists u, v \in \mathbb{Z} (1 = au + bv) \Rightarrow c = acu + bcv$; ma acu e bcv sono multipli di $a \Rightarrow c$ è multiplo di $a \Rightarrow a | c$.



• EQUAZIONI CONGRUENZIALI

Supponiamo di avere l'equazione $AX = C$ in un anello commutativo unitario:

- Se A è invertibile, la soluzione è $X = A^{-1}C$;
- Se A è cancellabile, esiste al massimo una soluzione;
- Se A è un divisore dello zero ha nessuna soluzione o più soluzioni.

Vediamo come si comporta l'equazione in \mathbb{Z}_m con $m \in \mathbb{N}^*$: $A = [a]_m$, $C = [c]_m$, con $a \in A$ e $c \in C$, otengo: $[a]X = [c]$. Prese $u \in \mathbb{Z}$, $[u]_m$ è soluzione dell'equazione se e solo se $[a]_m \cdot [u]_m = [c]_m \Leftrightarrow [au]_m = [c]_m \Leftrightarrow au \equiv_m c$.

Questa è chiamata equazione congruenziale e lo scopo è quello di trovare gli u che ne siano soluzioni, ovvero:

$$\Leftrightarrow m | c - au \Leftrightarrow \exists v \in \mathbb{Z} (mv = c - au) \Leftrightarrow \exists v \in \mathbb{Z} (au + mv = c)$$

$$\Leftrightarrow \exists v \in \mathbb{Z} ((u, v) \text{ è soluzione dell'equazione diante } au + mv = c).$$

Quanto, per il teorema di Bezout visto precedentemente, vuol dire che $au \equiv_m c$ ha soluzioni se e solo se il $\text{MCD}(a, m)$ divide c .

• ELEMENTI INVERTIBILI

$\forall a \in \mathbb{Z}$, $\forall m \in \mathbb{N}^*$ (equivalente a $\mathbb{Z} \setminus \{0\}$ perché $\equiv_m = \equiv_{-m}$)

$[a]_m \in U(\mathbb{Z}_m) \Leftrightarrow a$ ed m sono coprimi $\Leftrightarrow \text{MCD}(a, m) = 1$, questo perché se le classi

dunque si dice rimmetribile oppure dire che $\exists n \in \mathbb{Z} ([a]_m[n] = [1]) \Leftrightarrow a \equiv_m 1$
 $\Leftrightarrow \text{MCD}(a, m) | 1 \Leftrightarrow \exists x \in \mathbb{Z} (1 = \text{MCD}(a, m) \cdot x) \Leftrightarrow \text{MCD}(a, m) = \pm 1$.

[ex] $\mathbb{Z}_{10} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9} \}$

$\text{Div}(1) \cap \text{Div}(10) = \{1, -1\} = \text{MCD}(1, 10)$ ✓ e' invertibile

$\text{Div}(2) \cap \text{Div}(10) = \{1, -1, \bar{2}, -\bar{2}\} = \text{MCD}(6, 10)$ X NON e' invertibile

OSSERVAZIONE: ogni elemento non rimmetribile in \mathbb{Z}_m è un divisore dello zero.

Sia $a \in \mathbb{Z}$ NON coprime con m , ovvero un elemento non rimmetribile:
 $\Rightarrow \exists t \in \mathbb{Z} (t > 1 \wedge t \mid a \wedge t \mid m)$ e sia $l = \frac{m}{t}$, con $1 < l < m$, dunque visto che $t \mid a \Rightarrow tl \mid al \Rightarrow m \mid la \Rightarrow \text{primo } [a]_m \cdot [l]_m = [a \cdot l]_m = [a]_m$, se $m \mid al$, quindi al è un multiplo di m , e per definizione di classe di resto:
 $\forall x \in \mathbb{Z} [x]_m = x + m\mathbb{Z} \Rightarrow [a \cdot l]_m = [0]_m$. Per concludere, visto che $[l]_m \neq [0]_m \Rightarrow [a]_m$ è un divisore dello zero

Sempre nel caso $m \neq 0$, sono equivalenti le seguenti affermazioni:

- ① \mathbb{Z}_m è un campo;
- ② \mathbb{Z}_m è un dominio di integrità;
- ③ m è primo.

Infatti se \mathbb{Z}_m è un campo tutti gli elementi eccetto $0_{\mathbb{Z}_m}$ sono rimmetribili \Rightarrow invertibili $\Rightarrow m$ non divisori dello zero. Dunque se \mathbb{Z}_m non è un campo, m non è primo, ovvero $\forall a, b \in \mathbb{Z}_m [a]_m [b]_m = [m]_m = [0]_m$, e quindi \mathbb{Z}_m non è un dominio di int.

Chiamiamo **EQUIVALENTI** due equazioni come venziali avendo le stesse soluzioni:

- ① $\forall a, c ([a \equiv_m a' \wedge c \equiv_m c']) \Rightarrow a'x \equiv_m c'$ è equivalente a $ax \equiv_m c$
 (ex) $145x \equiv_{100} 96$ è equivalente a $45x \equiv_{100} -4$.
- ② $\forall k \in \mathbb{Z} \setminus \{0\}$, $ax \equiv_m c$ equivale a $axk \equiv_m ck$; questo perché $\forall s, t \in \mathbb{Z}$
 $s \equiv_m t \Leftrightarrow m \mid t-s \Leftrightarrow m \mid ((t-s)k) \Leftrightarrow t \equiv_m sk$.
 (ex) $45x \equiv_{100} 30$ è equivalente a $9x \equiv_5 6$ (dato che $\text{MCD}(45, 100) = 5$).
- ③ $\forall t \in \mathbb{Z}$, se t è coprimo con $m \Rightarrow ax \equiv_m c$ è equivalente a $axt \equiv_m ct$.

• ALGORITMO PER LA RISOLUZIONE (equazioni congruentiali)

- (I) trovo un $\text{MCD}(a, m) = d$;
- (II) d divide c ? $\begin{cases} \text{no} \Rightarrow S = \{\text{soluzioni dell'equazione}\} = \emptyset, \\ \text{sì} \Rightarrow \text{(III)} \end{cases}$;
- (III) dividendo a, m e c per d , in modo da ottenere la RIDOTTA.

• PERIODO

Sia (G, \cdot) un gruppo con $x \in G$, $\varphi : m \in \mathbb{Z} \mapsto x^m \in G$ è un omomorfismo da $(\mathbb{Z}, +)$ a (G, \cdot) . Con la convenzione che x si dice periodico se $\exists a, b \in \mathbb{Z}$ tali che $(a > b \wedge x^a = x^b) \rightarrow$ ovvero $x^{a-b} = 1_G$.

↳ x è iniettiva $\Leftrightarrow x$ ha periodo infinito / non è periodico.

↳ se non è iniettiva $\Leftrightarrow x$ è periodico $\Rightarrow A = \{m \in \mathbb{N}^* \mid x^m = 1_G\} \neq \emptyset$

Se x è periodico $\text{o}(x) := \min(A)$ si chiama PERIODO di x in G .

OSSERVAZIONE: $\forall x, \forall m \in \mathbb{N}^*$ in $\text{Sym}(x)$, gli m -cicli hanno periodo m .

Se $m = \text{o}(x)$, $\forall h \in \mathbb{Z}$ ($x^h = x^{h \bmod m}$)

Dim) $\exists h \in \mathbb{Z}$ tali che $r = h \bmod m = h + mk$

$$\Rightarrow x^r = x^{h+mk} = x^h \cdot x^{mk} = x^h \cdot (x^m)^k = x^h \cdot 1_G = x^h$$

↳ come conseguenza $x^a = x^b \Leftrightarrow a \equiv_m b$.

Allora, in virtù di ciò, $\{x^t \mid t \in \mathbb{Z}\}$ ha esattamente m elementi, ovvero le classi di resto, e corrisponde al sottogruppo generato da x .

Diciamo CARATTERISTICA, in un anello unitario, se x è periodico, in $(\mathbb{R}, +)$, il suo periodo. Se c è la caratteristica, $\forall a \in \mathbb{R}$ ($ca = 0_R$).

• POLINOMI

ATTENZIONE! i polinomi NON sono funzioni; possono essere considerati tali solo in campi infiniti.

Sia A un anello commutativo unitario, chiamiamo $A[x]$ un ANELLO DI POLINOMI a coefficienti in A per una determinata x , ovvero $A[x]$ è un anello commutativo unitario tale che:

- ① A sia un sottoanello unitario di $A[x]$ ($1_{A[x]} = 1_A$);
 - ② $x \in A[x]$
 - ③ $\forall f \in A[x] (\exists ! (a_i)_{i \in \mathbb{N}} \in A^{\mathbb{N}} (\exists m \in \mathbb{N} : f = \sum_{i=0}^m a_i x^i \wedge \forall i \in \mathbb{N} (i > m \Rightarrow a_i = 0_A)))$
- \downarrow SUCCESSIONE DEI COEFFICIENTI DI f

[es] Se $A = \mathbb{Z}$, per $x = \sqrt{2}$ NON ho una sola soluzione a darmi lo stesso risultato

- $0 + 0 \cdot (\sqrt{2}) + 1 \cdot (\sqrt{2})^2 = 2$
- $2 + 0 \cdot (\sqrt{2}) = 2$

la parola chiave dunque è UNICITÀ. Per ogni A è possibile trovare un anello di polinomi con le tre proprietà richieste:

$A[x]$ esiste sempre e, a meno di isomorfismi, è unico.

$$\begin{aligned} f &= \sum_{i=0}^m a_i x^i & \forall i \in \{0, \dots, m\} a_i = b_i \\ \text{Siamo} \quad f &= \sum_{i=0}^m b_i x^i & \Rightarrow \text{se } m \geq m \\ && \forall i \in \{m+1, \dots, n\} a_i = 0_A \end{aligned}$$

\Rightarrow non c'è un unico modo per scrivere un polinomio, infatti una volta scritti i coefficienti noti, si può aggiungere infiniti coefficienti nulli. In questo modo si ottengono, anche se banali, più scritture dello stesso polinomio

Gli elementi di A si dicono POLINOMI COSTANTI, di cui uno è proprio lo zero dell'anello, ed è detto polinomio nullo.

$[0_A = 0_{A[x]}]$ POLINOMIO NULLO successione di coefficienti $(0_i)_{i \in \mathbb{N}}$

• GRADO DEL POLINOMIO

Se $f \in A[x] \setminus \{0_A\}$ e $(a_i)_{i \in \mathbb{N}}$ è la successione dei coefficienti di f

$S_f = \{i \in \mathbb{N} \mid a_i \neq 0_A\}$ è finito e non vuoto, quindi ha MASSIMO. Possiamo definire allora:

$\text{MAX}(S_f) = \text{GRADO DI } f$, detto anche:

$\hookrightarrow \nu f$ "mi",

\rightarrow il coefficiente con il grado
più alto

$\hookrightarrow S_f$;

o νf è il COEFFICIENTE DIRETTORE di $f = cd(f)$

$\hookrightarrow \deg f$;

Il coefficiente di grado $i=0$ si chiama TERMINE NOTO

\rightarrow dato di resto

[es] in $\mathbb{Z}_5[x]$ $f = [2]_5 + [3]_5 x + [10]_5 x^3$ per il polinomio nullo si pone:
 $\Rightarrow \nu f = 1$ $cd(f) = 0_A$ (unico caso in cui $i=0$)
 $cd(f) = [3]_5$ $\nu(0_A) = -\infty$

Si dice che il polinomio f è MONICO $\Leftrightarrow cd(f) = 1_A$ (in \mathbb{Z}_2 tutti i $f \neq 0_{\mathbb{Z}_2}$ sono monici)

$$[0]_2 \quad 1_{2^1} = [1]_2$$

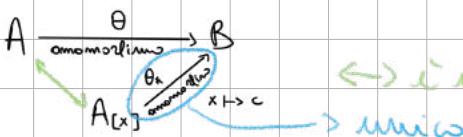
• PROPRIETÀ UNIVERSALE

Siamo A e B anelli commutativi unitari; definisco Θ omomorfismo di anelli unitari da A a B , cioè $\Theta(1_A) = 1_B$. $A[x]$ è un anello di polinomi in x ad una indeterminata x . Allora: $\forall c \in B, \exists! \Theta_*$ omomorfismo di anelli unitari $A[x] \rightarrow B$ tale che $(\Theta_*)_A = \Theta$, $\Theta_*(x) = c$

$$\Theta_*: \sum_{i=0}^n a_i x^i \in A[x] \mapsto \sum_{i=0}^n \Theta(a_i)c^i \in B$$

osserva Θ è la restrizione di Θ_* ad A

$$\sum_{i=0}^n a_i x^i = \sum_{i=0}^n \Theta_*(a_i) \Theta_*(x^i) = \sum_{i=0}^n \Theta_*(a_i) (\Theta_*(x))^i = \sum_{i=0}^n \Theta_*(a_i) \Theta_* x^i$$



\leftrightarrow è un omomorfismo ed è l'immersione di A in $A[x]$

Come applicazioni delle proprietà universale abbiamo:

① Unità dell'anello dei polinomi a meno di isomorfismi:

Siamo $A[x]$ e $A[y]$ anelli di polinomi; poniamo $B = A[y]$; come omomorfismo restringo $\Theta = A \xrightarrow{\text{isomorfismo}} A[y]$ e come c prendo y .

$$\begin{array}{ccccc} A & \xleftarrow{\quad} & A[y] & \xrightarrow{\quad} & \\ \nearrow & \searrow & \nearrow \alpha & \searrow & \\ A & & & & \end{array}$$

$\alpha: \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n a_i y^i$

In questo caso $\alpha(a_i) = a_i$ perché come omomorfismo è stato scelta l'immersione

N.B. = se ho gli stessi coefficienti, cambiando solo la x , ho praticamente lo stesso oggetto

Ottengono quindi un unico omomorfismo α per cui $\alpha(x) = y$ è l'immersione di A in $A[y]$ ma la restrizione di α ad A .

Poiché anche $A[y]$ è un anello di polinomi, poniamo ripetere le stesse contrazioni scambiando i ruoli di $A[x]$ e x con $A[y]$ e y . Quindi ottengono:

$$\begin{array}{ccccc} A & \xleftarrow{\quad} & A[x] & \xrightarrow{\quad} & \\ \nearrow & \searrow & \nearrow \beta & \searrow & \\ A & & & & \end{array}$$

$\beta: \sum_{i=0}^n a_i y^i \mapsto \sum_{i=0}^n a_i x^i$

E' facile verificare che α e β sono l'uno l'inverso dell'altro; dunque ammogliati due anelli di polinomi ad una indeterminata in A esiste un isomorfismo tra questi due che manda l'indeterminata di uno nell'indeterminata dell'altro e manda in re stessa ogni elemento di A . Poniamo quindi dire che due anelli di polinomi in A possono sol più differire per il nome dell'indeterminata.

② Omomorfismo di sostituzione

In questo caso, applicando le proprietà per $A=B$ e $\Theta=\text{id}_A$, raffidiamo che $\forall c \in A$, esiste unica

$$\begin{array}{ccccc} A & \xrightarrow{\text{id}_A} & A & \xrightarrow{\quad} & \\ \nearrow & \searrow & \nearrow p & \searrow & \\ A & & & & \end{array}$$

$p: x \mapsto c$

$$\begin{aligned} f: \sum_{i=0}^n a_i x^i &\mapsto \sum_{i=0}^n a_i c^i = f(c) \\ \Rightarrow f: p(x) \in A[x] &\mapsto p(c) \in A \end{aligned}$$

③ Sia $m \in \mathbb{N}^*$, $A = \mathbb{Z}$, $B = \mathbb{Z}_m[x]$, $c = x$, e prendo:

↳ le proiezioni canoniche $\mathcal{E}_m : a \in \mathbb{Z} \mapsto [a]_m = \bar{a} \in \mathbb{Z}_m$; (omomorfismo suriettivo)

↳ l'immersione $\mathcal{S} : \bar{a} \in \mathbb{Z}_m \mapsto \bar{a} \in \mathbb{Z}_m[x]$:

e le componego, ottenendo $\theta = \mathcal{S} \circ \mathcal{E}_m : a \in \mathbb{Z} \mapsto \bar{a} \in \mathbb{Z}_m[x]$

$$\mathbb{Z} \xrightarrow{\theta} \mathbb{Z}_m[x]$$

$$\begin{array}{ccc} & \nearrow & \\ \mathbb{Z}[x] & \xrightarrow{x \mapsto x} & \end{array}$$

$$f : \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^m \bar{a}_i x^i \quad (\text{omomorfismo suriettivo})$$

Attenzione però: perché applicando f non ci garantisce che si conservino grado e cd.

¶ $f(p) = 2 + 3x + 10x^3 \in \mathbb{Z}[x]$

$p_5 = \bar{2} + \bar{3}x + \bar{10}x^3 \in \mathbb{Z}_5[x] = \bar{2} + \bar{3}x$ perché $\bar{10} = \bar{5} = \bar{0}$

potrebbe semplificare: calcoli ma NON conserva il grado.

• SOMMA DI POLINOMI

¶ $f, g \in A[x] \setminus \{0_A\}$ poniamo $M = \nu f$, $m = \nu g$, $a = \text{cd}(f)$, $b = \text{cd}(g)$, $f = \sum a_i x^i$, $g = \sum b_i x^i$; abbiamo che $a = a_m \neq 0_A$ e $b = b_m \neq 0_A$. Siamo infine in $(a_i)_{i \in \mathbb{N}}$ la successione dei coefficienti di f e $(b_i)_{i \in \mathbb{N}}$ quella di g ; Allora:

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

Da questo risultato ottieniamo anche:

① $\nu(f+g) \leq \max\{M, m\} = M$

↳ $M \neq m \Rightarrow \nu(f+g) = M$

↳ $m = M$ e $a_m + b_m \neq 0_A \Rightarrow \nu(f+g) = M$

↳ $m = M$ e $a_m + b_m = 0_A \Rightarrow \nu(f+g) < M$

$\Rightarrow a_m = -b_m$

\Rightarrow il grado delle somme non supera mai quello dei singoli

② $\nu(f-g) \leq M$

la dimostrazione è equivalente a quella precedente: $\nu(f-g) < M \Leftrightarrow (m = M \wedge a = b)$; ovvero se notiamo anche che $f-g = f+(-g)$.

• PRODOTTO DI POLINOMI

Assumendo le stesse ipotesi di prima, descriviamo il prodotto di due polinomi come:

$$f \cdot g = (a_0 b_0) + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \dots + (a_m b_m) x^{m+m}$$

o anche:

$$f \cdot g = \sum_{i=0}^{m+m} c_i x^i, \text{ per cui } \forall i \in \mathbb{N} \left(c_i = \sum_{j=0}^i a_j b_{i-j} \right).$$

E per questo vale:

③ $\nu(f \cdot g) \leq m+m$

$$\nu(f \cdot g) = m+m \Leftrightarrow (a_m b_m \neq 0_A)$$

Se si verifica $r(fg) = r_f + r_g$, quindi se $ab \neq 0_A$, si dice che per i polinomi f e g vale la **REGOLA DI ADDIZIONE DEI GRADI**. Ovviamente queste regole vale sempre nel caso in cui uno dei due sia il polinomio nullo; se ad esempio $f = 0_A$, $r(f \cdot g) = r(0_A) = -\infty = -\infty + r_g = r_f + r_g$.

COME MANIPOLARE IL GRADO DEI POLINOMI: (corollari delle regole)

Sia A un anello commutativo unitario, e sia $f \in A[x]$; allora vale:

(*) ① Se il cd(f) è cancellabile in A , allora f è cancellabile in $A[x]$ e $\forall g \in A[x]$, vale la regola di addizione dei gradi;

② Sono equivalenti:

- i) A è un dominio di integrità;
- ii) $\forall f, g \in A[x] \quad (r(fg) = rf + rg)$;
- iii) $A[x]$ è un dominio di integrità.

Dim) (i) \Rightarrow (ii) $\forall f \in A[x]$:

$f \neq 0_A \Rightarrow$ cd è cancellabile in A e sarà il primo corollario;

$f = 0_A \Rightarrow$ come abbiamo notato prima, $\forall g \in A[x]$ vale la R.A.G. per f e g .

Ovviamente (ii) \Rightarrow (iii), in quanto ne vale R.A.G. $\forall f, g \in A[x] \quad (fg \neq 0_A)$, ovvero vale la legge di annullamento del prodotto in $A[x]$, che quindi è un dominio di integrità.

(iii) \Rightarrow (i) perché se $A[x]$ è un dominio di integrità, come visto nell'implicazione precedente, ne vale la L.A.P. \Rightarrow ne vale R.A.G. $\Rightarrow \forall f, g \in A[x] \setminus \{0\} \quad (ab \neq 0_A) \Rightarrow$ ne vale L.A.P. in A . 

Inoltre, se vale la proprietà appena dimostrata, $\mathcal{U}(A[x]) = \mathcal{U}(A)$.

Dim) ovviamente $\mathcal{U}(A) \subseteq \mathcal{U}(A[x])$, in quanto $\forall a \in \mathcal{U}(A)$, com'è il suo inverso, $ab = 1_A = 1_{A[x]} \Rightarrow b$ è l'inverso di a in $A[x]$.

Viceversa: sia $f \in \mathcal{U}(A[x])$ e sia g il suo inverso in $A[x]$. Allora: $fg = 1_{A[x]}$, quindi per le R.A.G. $rf + rg = r(1_{A[x]}) = 0$, dunque $rf = rg = 0$, ovvero f e g sono polinomi costanti e $f, g \in A$, e sono uno l'inverso dell'altro $\Rightarrow f \in \mathcal{U}(A) \Rightarrow \mathcal{U}(A[x]) \subseteq \mathcal{U}(A)$. 

(es) $\mathcal{U}(\mathbb{Z}_{[x]}) = \mathcal{U}(\mathbb{Z}) = \{1, -1\}$

Oppure, per ogni campo K ($\mathcal{U}(K[x]) = \mathcal{U}(K) = K \setminus \{0_K\}$).

Per concretizzare effettivamente del fatto che quello che abbiamo dimostrato non vale sempre ma solo nei DOMINI DI INTEGRITÀ basta prendere un semplice controesempio:

(es) Sia $f = \bar{1} + \bar{2}x \in \mathbb{Z}_2[x]$, non vale la regola di addizione dei gradi:

$$f^2 = \bar{1} + \bar{2} \cdot \bar{2}x + \bar{4}x^2 = \bar{1} + \bar{0}x + \bar{0}x^2 = \bar{1} \Rightarrow 0 = r(f^2) \neq r(f) + r(f) = 1+1=2.$$

e inoltre $f \cdot f = f^2 = \bar{1} = 1_{\mathbb{Z}_2} \Rightarrow f = f^{-1} \Rightarrow f \in \mathcal{U}(\mathbb{Z}_{2,[x]})$ pur non essendo f un polinomio costante $\Rightarrow \mathcal{U}(\mathbb{Z}_{2,[x]}) \neq \mathcal{U}(\mathbb{Z}_2)$

OSSERVAZIONE: se cd f è cancellabile in A e $rf > 0 \Rightarrow f \notin \mathcal{U}(A[x])$. Allora per ogni scelta di A non nullo, in $A[x]$ esistono elementi non inseribili e diversi dallo zero $\Rightarrow A[x]$ NON è un campo.

DIVISIONE CON RESTO TRA POLINOMI

$\forall f, g \in A[x]$, se $g \neq 0_A$, diciamo che in $A[x]$ è possibile effettuare la divisione di f (divisando) per g (divisore) se e solo se esistono $q, r \in A[x]$ tali che $f = qg + r$ e $\deg r < \deg g$.

non può essere 0 perché
non è invertibile

PROPOSIZIONE: siamo $f, g \in A[x]$, e supponiamo che $b := cd(g) \in U(A)$, allora:

$$\Rightarrow \exists (q, r) \in A[x] \times A[x] \{ f = qg + r \wedge \deg r < \deg g \}$$

Dim 1) Esistenza: poniamo $a = cd(f)$, $b = cd(g)$, $m = \deg f$, $n = \deg g$

- caso I: $m = \deg f < \deg g = n \Rightarrow$ basta porre $q = 0_A$ e $r = f$

- caso II: $m \geq n$; procediamo per induzione su m , quindi supponiamo che $f \in A[x]$ tale che $\deg f < m$ sia possibile fare la divisione di f per g .

Prendiamo in esame il polinomio $ab^{-1}x^{m-n}$; poniamo forse in quanto, se $m = n$
 $\Rightarrow m - n \geq 0 \in \mathbb{N}$ e quindi rispetta le ipotesi per essere una potenza; inoltre $cd(g) = b$
è invertibile quindi possiamo prendere b^{-1} .

Quindi questo polinomio ha grado $m - n$ e $cd = ab^{-1}$. Se prendo $(ab^{-1}x^{m-n}) \cdot g := k$,
il coefficiente direttore di questo prodotto risulta $ab^{-1}b = a \cdot 1_A = a \neq 0_A$,
e quindi vale la R.A.G., ovvero $\deg(k) = \deg(ab^{-1}x^{m-n}) + \deg(g) = m - n + n = m$.

Quindi se faccio $f - k := l_1$, sto facendo la differenza tra polinomi con lo stesso grado e
lo stesso coefficiente direttore $\Rightarrow \deg(l_1) < \deg(f) = \deg(k) = m$

L'ipotesi induttiva quindi garantisce che $\exists (\bar{q}, \bar{r})$ tali che $f_1 = \bar{q}g + \bar{r}$ e $\deg \bar{r} < \deg g$.

Visto che $f = ((ab^{-1}x^{m-n}) \cdot g) + f_1$

$$\begin{aligned} \Rightarrow f &= (ab^{-1}x^{m-n} \cdot g) + f_1 \\ &= (ab^{-1}x^{m-n} \cdot g) + g \cdot \bar{q} + \bar{r} \\ &= (ab^{-1}x^{m-n} + \bar{q}) g + \bar{r} \quad \Rightarrow f = g \cdot \bar{q} + \bar{r} \quad \text{e} \quad \deg \bar{r} = \deg \bar{r}_1 < \deg g. \end{aligned}$$

2) Unicità: siamo $q_1, q_2, r_1, r_2 \in A[x]$ tali che $f = q_1g + r_1 = q_2g + r_2$ e $\deg r_1 < \deg g$ e $\deg r_2 < \deg g$
 $g \cdot (q_1 - q_2) = r_2 - r_1$ ha grado $< \deg g$

Vede R.A.G. perché $cd(g) \in U(A)$ e rimarrà così, per $(*) \Rightarrow$ ha grado $\deg g + \deg(q_1 - q_2)$.

$$\Rightarrow \deg g + \deg(q_2 - q_1) < \deg g \Rightarrow \deg(q_2 - q_1) < 0$$

Allora questo non è in \mathbb{N} , dunque $\deg(q_1 - q_2) = -\infty$, cioè $q_2 - q_1 = 0_A \Rightarrow q_2 = q_1$; e inoltre:

$$g \cdot 0_A = q_2 - q_1 \Rightarrow 0_A = q_2 - q_1 \Rightarrow q_2 = q_1.$$

$$\text{Esempio: } A = \mathbb{Q} \quad f = 3x^4 + 2 \quad g = 2x - 1 \quad \Rightarrow \quad f_1 = f - \frac{3}{2}x^3 \cdot g = f - \left(3x^4 - \frac{3}{2}x^2\right) = 2 + \frac{3}{2}x^3$$

| | |
|-------|-------|
| $m=4$ | $n=1$ |
| $a=3$ | $b=2$ |

$$\begin{array}{r} 3x^4 \quad / \quad / \quad / \quad + 2 \\ - 3x^4 \quad + \frac{3}{2}x^3 \\ \hline \end{array} \quad \begin{array}{r} 2x - 1 \\ \frac{3}{2}x^3 + \frac{3}{2}x^2 \\ \hline \end{array}$$

$$\begin{array}{r} \xrightarrow{\quad} \quad / \quad \frac{3}{2}x^3 \quad + 2 \\ - \frac{3}{2}x^3 + \frac{3}{2}x^2 \\ \hline \end{array}$$

$$\begin{array}{r} \xrightarrow{\quad} \quad / \quad \frac{3}{2}x^2 \quad + 2 \\ \hline \end{array}$$

N.B.: se A è un campo, la condizione $cd(g) \in U(A)$ implica che $g \neq 0_A$, in quanto ogni elemento non nullo di A è invertibile, quindi $cd(g) \neq 0$. Il fatto che ogni polinomio e coefficienti in un campo non nullo sia divisibile ci permette di eseguire l'algoritmo euclideo finché non otteniamo un resto uguale a 0, questo perché ci fermiamo solo quando m è stabile, cioè la divisione, ovvero quando il resto è 0.

• APPLICAZIONI POLINOMIALI

$\forall f \in A[x], \forall c \in A$ posto $f = \sum_{i=0}^m a_i x^i$ $f(c) = \sum_{i=0}^m a_i c^i$ ($i \in \{0, 1, \dots, n\}$ $a_i \in A$)

diciamo $\tilde{f}: c \in A \mapsto f(c) \in A$ è l'**APPLICAZIONE POLINOMIALE** definita da f , che è differente da l'omomorfismo di sostituzione, questa applicazione non è, in generale, un omomorfismo.

Si dice che c è **RADICE** di $f \Leftrightarrow f(c) = 0_A$.

PROPOSIZIONE: $\forall f, g \in A[x]$ re $f \mid g \Rightarrow$ ogni radice di f è radice di g .

Dim) se $f \mid g \Rightarrow \exists h \in A[x]$ ($g = fh$). Allora applicando l'omomorfismo di sostituzione definito da g , abbiamo $g(c) = f(c)h(c) = 0_A \cdot h(c) = 0_A$. 

(*) **PROPOSIZIONE:** Se A è un dominio di integrità, $\forall c \in A$, c è radice di $fg \Leftrightarrow c$ è radice di $f \circ g$.

Dim) \Leftarrow per la proposizione precedente se c è radice di $g \circ f$ di $f \Rightarrow c$ è radice di fg .

Fd' insiemere, se c è una radice di $fg \Rightarrow f(c)g(c) = fg(c) = 0_A$, e visto che se A è un dominio di integrità, come abbiamo già dimostrato, lo è anche $A[x]$ e quindi solo le L.A.P., se $f(c)g(c) = 0_A \Rightarrow$ uno tra $f(c)$ e $g(c)$ è $0_A \Rightarrow c$ è radice di almeno uno di loro. 

• TEOREMA DEL RESTO

Ω_n

Sia $f \in A[x]$ e $c \in A$; allora $f(c)$ è il resto della divisione di f per $x - c$.

Dim) la prima cosa da provare è che è certamente possibile effettuare la divisione in quanto $x - c$ è un polinomio monico, quindi $\text{cd}(x - c) = 1 \in U(A)$ (*).

$\Rightarrow \exists (q, r)$ tali che $f = q(x - c) + r$ e $\deg r < \deg(x - c) = 1$; quest'ultima condizione equivale a dire che r è un polinomio costante, quindi $r(c) = r$.

Applicando l'omomorfismo di sostituzione otteniamo: $f(c) = (q(x - c))(c) + r(c) = q(c) \cdot (c - c) + r(c) = q(c) \cdot 0_A + r(c) = r(c) = r \Rightarrow f(c) = r$. 

• TEOREMA DI RUFFINI (conseguenza immediata del teorema del resto)

Siano $f \in A[x]$ e $c \in A$. Allora c è una radice di $f \Leftrightarrow (x - c) \mid f$ in $A[x]$.

Da dimostrazione è ovvia perché per il teorema del resto, c è radice di f se e solo se il resto della divisione di f per $x - c$ è zero, cioè se e solo se $x - c$ divide f .

• TEOREMA DI RUFFINI GENERALIZZATO

Sia A un dominio di integrità unitario, $m \in \mathbb{N}^*$, c_1, c_2, \dots, c_m elementi di A a due a due distinti, $f \in A[x]$. Allora si ha che esistono degli elementi a_i i radice di f se e solo se $\prod_{i=1}^m (x - c_i)$ divide f in $A[x]$.

Dim) \Leftarrow ovvio perché se $\prod_{i=1}^m (x - c_i)$ divide f , allora ciascuno degli elementi c_i è radice di f , in quanto $(x - c_i)$ divide f .

\Rightarrow proveremo per induzione su m .

base: $m = 1 \Rightarrow \prod_{i=1}^1 (x - c_i) = x - c_1 \Rightarrow$ risulta per il teorema di Ruffini.

Sia $m > 1$ e assumiamo l'enunciato vero per $m - 1$; allora, poiché $f(c_m) = 0_A$, per il teorema di Ruffini $x - c_m \mid f$, ovvero $\exists h \in A[x]$ ($f = (x - c_m)h$). Sia ora $1 \leq i \leq m$; poiché c_i è radice di f per ipotesi, e A è un dominio di integrità, per la (*), ci dà che

essere radice di $(x - c_m)$ o di h . Ma $c_i \neq c_m$ per come abbiamo definito i, dunque andiamolo a verificare se c_i è radice di $(x - c_m)$ risulta: $(x - c_m)(c_i) = c_i - c_m \neq 0_A$
 $\Rightarrow c_i$ è radice di $h \Rightarrow h(c_i) = 0_A$; e questo dimostramente vale $\forall i \in \{1, \dots, (m-1)\}$.
Applicandolo quindi l'ipotesi induzione concludo che $\prod_{i=1}^{m-1} (x - c_i)$ divide h , quindi esiste $g \in A[x]$ tale che $h = g \cdot \prod_{i=1}^{m-1} (x - c_i)$. Allora:
 $f = h(x - c_m) = g \cdot \prod_{i=1}^{m-1} (x - c_i) \cdot (x - c_m) = g \cdot \prod_{i=1}^m (x - c_i) \Rightarrow \prod_{i=1}^m (x - c_i)$ divide f .

COROLLARI

domini di integrità unici

① Sia $f \in A[x] \setminus \{0_A\}$; allora f ha al massimo νf radici in A .

Dim) Se f ha n radici, per il teorema di Ruff. gen., f è multiplo di $g := \prod_{i=1}^n (x - c_i)$, quindi $f = qg$, per un opportuno $q \in A[x]$. Essendo $f \neq 0_A \Rightarrow q \neq 0_A$, ma $\nu g = n$, e visto che nei domini di integrità vale la R.A.G., $\nu f = \nu g + \nu q = n + \nu q \geq n$.

② PRINCIPIO DI IDENTITÀ DEI POLINOMI: sia A un dominio di integrità infinito. Allora $\forall f, g \in A[x]$ si ha $\tilde{f} = \tilde{g} \Leftrightarrow f = g$ (cioè $f \in A[x] \mapsto \tilde{f} \in \text{Map}(A, A)$ è iniettiva). $\tilde{f}: c \in A \mapsto f(c) \in A$
Dim) \Leftarrow ovviamente se $f = g \Rightarrow \tilde{f}: c \in A \mapsto f(c) \in A = \tilde{g}: c \in A \mapsto g(c) \in A = \tilde{g}$.
 \Rightarrow viceversa, se $\tilde{f} = \tilde{g} \Rightarrow \forall c \in A (f(c) = g(c))$. Sia $h = f - g \Rightarrow \forall c \in A h(c) = f(c) - g(c) = 0_A$, ovvero ogni elemento di A è radice di $h \Rightarrow h$ ha infinite radici. Ma per la proposizione precedente, se $h \neq 0_A$ il numero delle sue radici è finito, perch'è parso essere al mo · mo $\nu h = \nu h = 0_A \Rightarrow f = g$.

CONTROESEMPI:

- ① Sia $A = \mathbb{Z}_{6[x]}$, ovvero A NON è un dominio di integrità; sia $f = \bar{2}x$. Sia $[0]_6$ che $[3]_6$ sono radici di f , ma il grado di f è 1.
- ② Nel caso degli anelli finiti, il numero delle applicazioni da A ad A è finito, mentre $A[x]$ è infinito, quindi l'applicazione $f \in A[x] \mapsto \tilde{f} \in \text{Map}(A, A)$ è sicuramente non iniettiva.
- ③ Anche nel caso degli anelli infiniti che non sono intesi, il principio può non valere; ad esempio se A è un anello booleano e $f = x^2 - x$, poiché ogni elemento di A è idempotente, $f(c) = c^2 - c = 0_A \Rightarrow$ tutti gli elementi sono radici di f . Allora $\tilde{f} = 0_A$, nonostante $f \neq 0_A$.

• FATTORIZZAZIONE

Un teorema che non dimostreremo ci assicura che se A è l'anello, allora anche $A[x]$ è fattoriale (ovvero è un monoidale commutativo cancellativo, in cui ogni elemento non invertibile è prodotto di elementi irriducibili in maniera univocamente unica). Ricordiamo inoltre che se A è un dominio di integrità unitario $\Rightarrow U(A[x]) = U(A)$, allora $f \in A[x]$ gli associati a f in $A[x]$ sono tutti e soli i polinomi delle forme $u f$ al variare di u in $U(A[x]) = U(A)$, quindi hanno lo stesso grado di f .

Se A è un campo K , $U(K[x]) = U(K) = K \setminus \{0_K\}$, quindi l'insieme di tutti i polinomi associati ad $f \in K[x] \setminus \{0_K\}$ è $\{f | 0_K \neq u \in K\}$. Se $a = cd f$, si ha $cd(u) = u$. Allora f ha esattamente un associato con coefficiente diretto K (con $K \in K^*$), e sicuramente $(Ka^{-1})f$, inoltre $\forall u \in K^*$, $cd(u) = ua = K \Leftrightarrow u = Ka^{-1}$. $\Rightarrow f$ ha esattamente un associato con coefficiente diretto K .

PROPOSIZIONE (conseguenza di th di ciò che abbiamo dimostrato): sia K un campo; in ogni classe di elementi associati ai polinomi non nulli in $K[x]$, esiste un solo polinomio monico (con $K = 1_K$), che chiameremo **RAPPRESENTANTE MONICO**.

PROPOSIZIONE: sia K un campo; allora ogni polinomio non nullo si fattorizza come prodotto di un invertibile (quindi un elemento di K , e nello specifico il suo coefficiente diretto), e polinomi irriducibili monici, in modo unico e meno dell'ordine dei fattori.

Dim) l'unicità della fattorizzazione segue dal fatto che $K[x]$ è fattoriale e dal fatto che ogni classe di polinomi associati non nulli contiene un solo rappresentante monico.

L'esistenza è ovvia nei casi dei polinomi costanti; sia allora $f \in K[x] \setminus K$ e sia $f = p_1 p_2 \dots p_m$ una fattorizzazione di f di polinomi irriducibili. $\forall i \in \{1, \dots, m\}$ sia $a_i = cd(p_i) \Rightarrow p_i = q_i \cdot a_i$ dunque $q_i = p_i \cdot a_i^{-1}$ è associato a p_i (\Rightarrow invertibile) ed è monico. Punto $a = a_1 \dots a_m \Rightarrow f = a q_1 \dots q_m$.

• CARATTERIZZAZIONE DEI POLINOMI IRRIDUCIBILI

Sia $f \in K[x]$, $m = \nu f$. Allora f è **IRRIDUCIBILE** in $K[x]$ se e solo se $m > 0$ e vale una tra:

- ↳ $\exists g, h \in K[x] (f = gh \wedge \nu g < m \wedge \nu h < m)$;
- ↳ $\exists g, h \in K[x] (f = gh \wedge \nu g > 0 \wedge \nu h > 0)$; } equivalenti

Dim) \Rightarrow se f è irriducibile, per definizione, $f \in U(K[x]) = K \setminus \{0_K\} \Rightarrow f \notin K$, ovvero non f è un polinomio costante, e inoltre non può essere nullo perché per definizione, se è irriducibile \Rightarrow non è invertibile e non ha divisori non banali, ma il polinomio nullo ha tutti gli elementi di $K[x] \setminus K$ come divisori $\Rightarrow m > 0$.

Siamo $h, g \in K[x]$ e $f = gh \Rightarrow g \mid f$ e visto che f è irriducibile, g deve essere un divisore banale. Ci sono quindi due possibilità:

- * se g è invertibile $\Rightarrow g \in K \setminus \{0_K\} \Rightarrow \nu g = 0$;
- * se g è associato ad $f \Rightarrow \nu g = \nu f = m$;

\Leftarrow Viceversa, assumiamo per anturro che f non sia irriducibile. Visto che per ipotesi $m > 0 \Rightarrow f \notin K \setminus \{0_K\} = U(K[x]) \Rightarrow f$ non è invertibile. Inoltre se f riducibile ha un divisore non banale $g \Rightarrow g \neq 0_K$ (altrimenti $f = 0_K$) e non è invertibile $\Rightarrow \nu g > 0$. Ora sìmette $h \neq 0_K$ e non è invertibile poiché $g \mid f \Rightarrow \nu h > 0$. Assurdo!

OSSERVAZIONE NECESSARIA: due polinomi associati hanno lo stesso grado.

OSSERVAZIONE: sia A un dominio di integrità unitario, $f \in A[x]$ e $\sqrt{f} > 1$. Allora per il teorema di Ruffini, se f ha una radice $c \in A$, allora $x - c$ è un divisore non banale di f . Allora l'esistenza di una radice per un polinomio di grado maggiore al primo, ci avverte che non è irriducibile.

• METODI DI RICERCA DI RADICI

Sia K un campo, $f \in K[x] \setminus \{0_K\}$ e $\sqrt{f} = m$. Valgono:

① f ha una radice in $K \Leftrightarrow f$ ha un divisore di primo grado in $K[x]$

② $m = 0 \Rightarrow f$ non ha radici, non irriducibile e invertibile;

$m = 1 \Rightarrow f$ ha una radice ed è irriducibile;

$m \in \{2, 3\} \Rightarrow (f \text{ è irriducibile} \Leftrightarrow f \text{ non ha radici});$

$m > 3 \Rightarrow (f \text{ è irriducibile} \Rightarrow f \text{ non ha radici}); *$

> Dim) sia f privo di radici \Rightarrow non ha divisori di primo grado; ma $g, h \in K[x]$ e $f = gh \Rightarrow \sqrt{g} + \sqrt{h} = \sqrt{f} = m$ e $\sqrt{g} \neq 1 \neq \sqrt{h}$: allora:

se $m = 2 \{ \sqrt{g}, \sqrt{h} \} = \{ 0, 2 \}$ l'altra possibilità sarebbe $\{1, 2\}$ ma non

$m = 2 \{ \sqrt{g}, \sqrt{h} \} = \{ 0, 3 \}$ ha radici di grado uno.



* **CONTROESEMPIO:** $(x^2 + 1)^2$ ha grado 4 ed è ovviamente riducibile in quanto prodotto di $x^2 + 1$ irriducibili, e mi $x^2 + 1$ mi $(x^2 + 1)^2$ hanno radici.

• LISTA DI POLINOMI IRRIDUCIBILI IN $\mathbb{Z}_2[x]$

grado 1: x ; $x + \bar{1}$

grado 3: $x^3 + x^2 + \bar{1}$; $x^3 + x + \bar{1}$

grado 2: $x^2 + x + \bar{1}$

grado 4: $x^4 + x^3 + \bar{1}$; $x^4 + x + \bar{1}$



OSSERVAZIONE:

① tutti i polinomi di grado dispari in \mathbb{R} hanno radici;

② in $\mathbb{R}[x]$ i polinomi irriducibili hanno grado massimo 2;

③ $\forall f \in \mathbb{Q}[x] (\exists l_1 \in \mathbb{Z}[x] (l_1 \approx f)) \Rightarrow$ hanno la stessa radice

• CRITERIO DI EISENSTEIN

Sia $f = \sum a_i x^i$ un polinomio non nullo di grado n in $\mathbb{Z}[x]$. Se esiste p primo tale che:

$\left. \begin{array}{l} p \mid a_i \quad \forall i \in \{1, \dots, n-1\}; \\ p \nmid a_n; \\ p^2 \nmid a_0; \end{array} \right\}$

$\Rightarrow f$ è irriducibile in $\mathbb{Q}[x]$

OSSERVAZIONE: $\forall m \in \mathbb{N}^*$ $x^m - p$ è irriducibile in $\mathbb{Q}[x]$

CONTROESEMPIO: $x-1$ è irriducibile ma non soddisfa le condizioni.

PROPOSIZIONE: sia $f = \sum a_i x^i$ un polinomio non nullo di grado n in $\mathbb{Z}[x]$, sia c una radice di f in \mathbb{Q} . Scritto c come frazione ridotta $\frac{u}{v}$ (u, v interi coprimi e $v \neq 0$), si ha:
 $v \mid a_m$ e $u \mid a_0$.

Dim) $0 = f(c) = a_m \frac{u^m}{v^m} + a_{m-1} \frac{u^{m-1}}{v^{m-1}} + \dots + a_1 \frac{u}{v} + a_0$

$\Rightarrow 0 = a_m u^m + a_{m-1} u^{m-1} v + a_{m-2} u^{m-2} v^2 + \dots + a_1 u v^{m-1} + a_0 v^m$

$v \mid a_0 v^m$, visto che u e v^m sono coprimi $\Rightarrow v \mid a_0$; analogamente $v \mid a_m u^m \Rightarrow v \mid a_m$

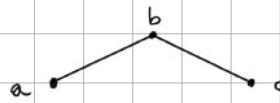
multipi di v multipli di v



• GRAFI

Un grafo **SEMPLICE** lo definiamo come una coppia ordinata (V, L) , dove V è un insieme non vuoto, $L \subseteq P_2(V)$, tra due vertici c'è al massimo un solo e non ci sono coppi.

$$\left(\begin{array}{c} \{\{a,b,c\}, \{\{a,b\}, \{a,c\}\} \\ \text{VERTICI} \quad \text{LATI} \end{array} \right) = (V, L)$$

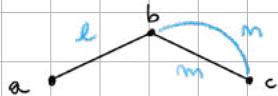


Definiamo **MULTIGRAFO SEMPLICE** una terza ordinata (V, L, l) dove $l: L \rightarrow P_2(V)$.

$$e \mapsto \{\{a,b\}\}$$

$$m \mapsto \{\{b,c\}\}$$

$$n \mapsto \{\{b,c\}\}$$



i grafî semplici sono multigrafi in cui l è iniettiva.

OSSERVAZIONE: $\forall V, A = \{ p \in \text{Rel}(V) \mid p \text{ è antiriflessiva e simmetrica} \}$; e definiamo inoltre l'applicazione biettiva $L \in P(P_2(V)) \mapsto p_L \in A$ che ha per inversa l'applicazione $p \in A \mapsto \{\{\{a,b\} \mid a \neq b\} \in P_2(V)\}$.

Poniamo definire a questo punto la relazione di **ADIAZENZA**: due estremi sono adiacenti se e solo se sono estremi dello stesso lato, ovvero $a \sim b \Leftrightarrow \{\{a,b\}\} \in L$. Se considero $L = \{\{x,y\} \in P(V) \mid x \neq y\} \subseteq P_2(V)$ posso anche definire il grafo come la coppia $(V, p) = G$.

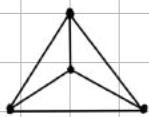
Due lati si dicono **INCIDENTI** se hanno un vertice in comune; un vertice e un lato si delimitano tali se il vertice è un estremo del lato. Inoltre il **GRADO** di un vertice è il numero dei lati di cui un vertice è estremo, ovvero $\forall x \in V \text{ deg}(x) = \{e \in L \mid x \text{ è estremo di } e\}$

• GRAFO COMPLETO

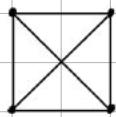
Sia $G = (V, L)$ un grafo; quest'è completo quando $L = P_2(V)$. Se un grafo ha n vertici, $|P_2(V)| = \binom{n}{2}$, quindi normalmente $|L| \leq \binom{n}{2}$; se il grafo è completo vale l'uguaglianza.

• GRAFO PLANARE

È un grafo che può essere rappresentato senza che i lati si intersechino tra loro. Ad esempio:



è plausore



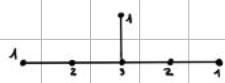
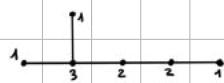
non è plausore

• ISOMORFISMO

Siano $G = (V, L, l)$ e $G' = (V', L', l')$ due multigrafi; un isomorfismo è una coppia di applicazioni bietteive $\alpha: V \rightarrow V'$ e $\beta: L \rightarrow L'$ tali che $\forall l \in L, \forall a, b \in V, a \sim b$ sono gli estremi di $l \Leftrightarrow \alpha(a) \sim \alpha(b)$ sono gli estremi di $\beta(l)$.

Per i grafî semplici basta che $\forall a, b \in V \quad \{\{a,b\} \in L \Leftrightarrow \{\{\alpha(a), \alpha(b)\}\} \in L'$.

\Rightarrow due grafî isomorfi hanno lo stesso numero di vertici e di lati.



questi due grafi non sono isomorfi perché non si mantengono l'adiacenza dei grafi.

questi sono isomorfi: stesso numero di vertici, però si mantengono l'adiacenze.

e sempre pari

• **TEOREMA**: sia $G = (V, L, \ell)$ un multigrafo limitato; allora $\sum_{v \in V} \deg(v) = 2|L|$

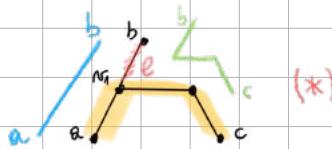
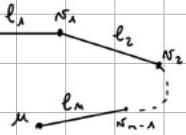
Dimostrazione: si può dimostrare per induzione, oppure alternativamente prendo:

$\ell_1, \ell_2, \dots, \ell_n \in S = \{(\nu, e) \in V \times L \mid \nu \text{ estremo di } e\}$. Le uscite indicano ν , i vertici estremi di e .
Se conto per colonne, visto che ogni lato ha due estremi, ogni colonna avrà due $x \Rightarrow 2L = |S|$. Se conto per righe, in ogni riga ci saranno tante x quanto il grado di ν , $\Rightarrow |S| = \sum_{v \in V} \deg(v)$.

Un vertice si dice **puro** se ha gradi pari, **dispari** se ha gradi dispari. Come conseguenza del teorema i vertici puro possono avere di un numero arbitrario, quelli dispari devono avere di numero pari.

CAMMINI

Se $\nu, u \in V$, un cammino γ da ν a u di lunghezza $m \in \mathbb{N}$ è una m -upla $(l_1, \dots, l_m) \in L^m$ di lati a due a due distinti, tali che: $l_1 = \{\nu, \nu_1\}, l_2 = \{\nu_1, \nu_2\}, \dots, l_m = \{\nu_{m-1}, u\}$.



Un **CIRCUITO** è un cammino da un vertice a se stesso ($u = \nu$). Se un cammino passa per ogni lato di un multigrafo una ed una sola volta, allora si dice **CAMMINO EULERIANO**.

↳ **condizioni necessarie e sufficienti** → tutti gli elementi sono comuni a due a due

- in un multigrafo limitato e connesso esiste un circuito euleriano \Leftrightarrow ogni vertice ha gradi pari;
- $\forall \nu \Leftrightarrow$ il numero di vertici con gradi dispari è 0 o 2;

Due vertici a, b si dicono **connessi** $\Leftrightarrow a = b$ oppure esiste un cammino da a a b .

La relazione di connessione si riflette, simmetrice e transitiva, dunque è una relazione di equivalenza. La proprietà transitiva è garantita anche nel caso in cui non ci sia la ripetizione di un lato; se ad esempio nel cammino da a a b e nel cammino da b a c incontriamo l , passiamo per il vertice ν , che corrisponde al minimo tra i vertici in comune. (*)

Visto che la relazione è di equivalenza possiamo definire le classi di equivalenza, che chiameremo **COMPONENTI CONNESSE**, e sono formate da vertici comuni e dai lati che formano i cammini che li connettono, e un insieme quoziente.

SOTTOGRAFI

Sia $G = (V, L)$ un grafo; allora $G' = (V', L')$ è un sottografo se e solo se $V' \subseteq V$, $L' \subseteq L$ e forma a sua volta un grafo. Per i multigrafi è necessario che l' sia una riduzione di l .

• FORESTE E ALBERI

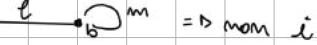
Un grafo è una **foresta** \Leftrightarrow non esistono cicli (circuiti). Una foresta comune si dice **albero**.

TEOREMA: un grafo finito è una foresta $\Leftrightarrow \forall (a,b) \in G$, con $a \neq b$, esiste al più un comune cammino da a a b ;

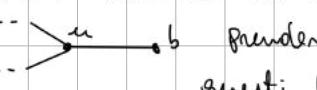
N.B.: una foresta è necessariamente un grafo semplice.

Dimo) Siamo $a, b \in V$, dove V è l'insieme dei vertici della foresta G ; supponiamo esistano due cammini diversi da a a b : $l = (l_1, l_2, \dots, l_m)$ e $m = (m_1, m_2, \dots, m_n)$

$\Rightarrow \exists v \in V$ tale che da v in poi i due cammini l, m non coincidono.

L) se $v = b$  \Rightarrow non è un grafo acchico \Rightarrow contraddizione!

U) se $v \neq b$ $\exists u \in V$ tale che da u in poi i due cammini coincidono.

 prendendo in considerazione da v a u e da u a v questi formano un circuito \Rightarrow contraddizione!

• RAPPRESENTAZIONE RADICALE DI UN ALBERO

Si può rappresentare un albero scegliendo un suo vertice r e disegnando al di sotto di esso quelli a distanza uno, poi due, etc..., collegandoli per avere un grafo isomorfo.

OSSERVAZIONE: una foresta finita è necessariamente un grafo albero.

Se un albero ha albero due vertici in rappresentazione radicale, quelli a distanze massime hanno grado 1 (detti **FOGLIE**). In generale il numero di foglie $i \geq \deg(r)$.

Lemma: sia $T = (V, L)$ un albero, $v \in V$ ($\deg(v) = 1$) $\Rightarrow v$ è una foglia; sia $l \in L$ tale che v è un estremo di l . Allora $T' = (V \setminus \{v\}, L \setminus \{l\})$ è ancora un albero.

Dimo) $\forall a, b \in T'$, $a \neq v \wedge b \neq v \Rightarrow$ il cammino da a a b non è l , quindi ogni vertice in un cammino ha grado ≥ 2 se non è un estremo.

PROPOSIZIONE: se T è finito $\Rightarrow |V| = |L| + 1$.

Dimo) procediamo per induzione: posto $|L| = 0 \Rightarrow |V| = 1 = 1$ è verificato.

Ammesso $|L_{t'}| = m$ e verifichiamo $|L_{t'}'| = m - 1$.

Per il lemma precedente, se a t' togliamo una foglia e il letto ad essa incidente, abbiamo ancora un albero, di $m+1-1 = m$ leti, e $|V_{t'}|-1$ foglie. Per ipotesi le foglie di quell'albero sono $m+1 \Rightarrow |V_{t'}|-1 = m+1 \Rightarrow |V_{t'}| = m+1+1 = |L_{t'}'| + 1$.

• SOTTOALBERI MASSIMALI

Sia $G = (V, L, l)$ un multografo finito. Un sottografo massimale di G è un sottografo di G con insieme di verti- V che è un albero; è unico $\Leftrightarrow G$ è conexo. Si dimostra facilmente che se eliminiamo un letto da un circuito i $v \in V$ rimangono tutti comuni.

OSSERVAZIONE: sia $G = (V, L, l)$ un multografo conexo; se $l_0 \in L$ tale che l è ponte di un circuito in G . Allora il sottografo di G , $G' = (V, L', l')$ con $L' = L \setminus \{l_0\}$ è ancora conexo.

Dimo) diamo $a, b \in G$; se a, b comuni da un circuito \Rightarrow esistono almeno due cammini diversi ($m \neq n$) da a a b . Se l_0 è in $m \Rightarrow a, b$ non sono in m in G' , o viceversa.

TEOREMA CONCLUSIVO

Sia $G = (V, L, \ell)$ multigrado finito con sottostante K componenti connesse. Allora:

① G connesso $\Rightarrow |L| \geq |V| - 1$;

② $|L| \geq |V| - K$;

③ $|L| = |V| - K \Leftrightarrow G$ è una foresta;

④ Sono equivalenti:

a $\hookrightarrow G$ è un albero;

b $\hookrightarrow G$ è connesso e $|V| = |L| + 1$

c $\hookrightarrow G$ è una foresta e $|V| = |L| + 1$;

Dim ①) G connesso $\Rightarrow G$ ha un sottobraccio massimale (V, L') con $L' \subseteq L$.

$\Rightarrow |V| = |L'| + 1 \Rightarrow |L'| = |V| - 1$ e visto che $|L'| \leq |L| \Rightarrow |L| \geq |V| - 1$ avremo
sempre $|V| = |L| + 1 \Leftrightarrow |L| = |L'| \Leftrightarrow L = L'$

Dim ②) Siamo $(V_1, L_1, \ell_1), (V_2, L_2, \ell_2), \dots, (V_K, L_K, \ell_K)$ le componenti connesse di G .

$\forall i \in \{1, \dots, K\}$, $|L_i| \geq |V_i| - 1$ per ①

$$|L| = \sum_{i=1}^K |L_i|, \quad |V| = \sum_{i=1}^K |V_i|, \quad \sum_{i=1}^K -1 = -K \Rightarrow |L| \geq |V| - K.$$

Dim ③) Se $\forall i \in \{1, 2, \dots, K\}$ $|L_i| = |V_i| - 1 \Rightarrow |L| = |V| - K$ per lo ②. Inoltre

$G_i = (V_i, L_i)$ è un albero $\Rightarrow G$ è una foresta.

Dim ④) b \Rightarrow a per ①; a \Rightarrow b già dimostrato.

a \Rightarrow c: se G è un albero, allora G è anche una foresta, inoltre per ③ $|V| = |L| + K$,
dunque K sono le componenti connesse in G . Essendo G un albero, $K = 1$,

c \Rightarrow a: per ③ G è una foresta con $K = 1$ componenti connesse, dunque è un albero. //