APPUNTI DI LOGICA, ALGEBRA E GEOMETRIA

Anno Accademico 2020/2021

Autore: Arlind Pecmarkaj

Questi appunti son stati scritti nel primo semestre dell'anno accademico 2020/21, perciò in piena pandemia Covid: sono la trasposizione in formato pdf degli appunti presi in tutte le lezioni a cui ho partecipato.

Volevo condividerli poiché quando ero ancora una matricola, appunti di questo corso non esistevano e pensavo potessero essere utili a tutti i nuovi studenti che devono sostenere il "primo" esame matematico a Informatica applicata.

Parto col dire che non sono il massimo, ma forniscono un'idea generale della materia.
Da soli non bastano a passare l'esame, rileggendoli ho notato molti errori; perciò, vi consiglio caldamente di integrare il tutto con i vostri appunti e seguire le lezioni costantemente.
Inoltre è possibile che il vostro programma sia differente (anche sostanzialmente) a ciò che è scritto qui: in quel caso questo file non sarebbe molto utile.

Noterete che all'avanzare delle pagine la formattazione del testo migliora. Questo è da spiegarsi nel fatto che ho imparato a usare Word man mano che scrivevo gli appunti. Perciò le prime pagine son piuttosto brutte da vedere.

Ovviamente potete modificare gli appunti e farci quel che volete tranne venderli o spacciarli per vostri.
Concludo augurandovi il meglio nella vostra carriera universitaria.

Data ultima modifica: 14 dicembre 2020

ALGEBRA

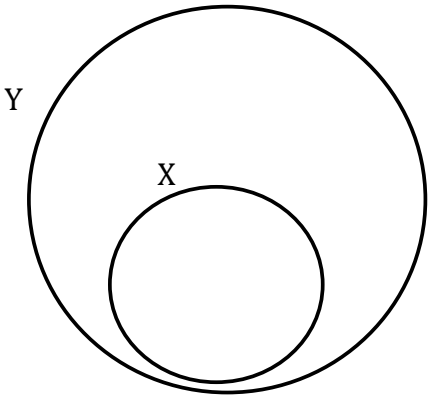
La definizione di insieme è piuttosto difficile da ricercare in quanto se si definisce come "gruppo di elementi" si arriva a un circolo vizioso. Cosa vuol dire gruppo? Un insieme. E un insieme? Un gruppo e così via.
Bisogna prima di iniziare definire la differenza tra sintassi e semantica:
- SINTASSI: modo di scrivere delle formule, la grammatica.
- SEMANTICA: ciò che da significato/valore o interpretazione agli oggetti o sintassi

Per definire gli insiemi si arrivò alla TEORIA INGENUA DEGLI INSIEMI di G. Cantor che non definisce l'insieme, ma lo usa.
Cantor disse che se un insieme esiste, esso è costituito dai suoi elementi.
In caso l'insieme sia senza elementi, esso si chiama insieme vuoto → definito dal simbolo Ø
Gli insiemi nascono dal concetto di appartenenza

$\in$ → appartiene $\quad\quad$ $\notin$ → non appartiene

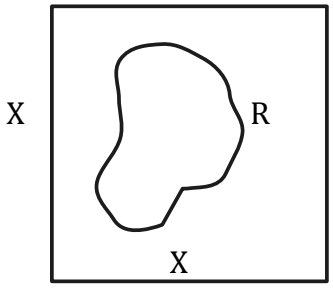
Supponendo che X sia un insieme e x un suo elemento si può dire che x $\in$ X
La teoria ha dei limiti e porta a paradossi e contraddizioni (vedi paradosso di Russel)

X $\subseteq$ Y vuol dire X è un <u>sottoinsieme</u> o <u>proprietà</u> di Y



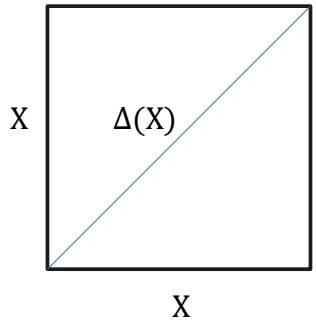
Una proprietà può essere chiamata anche <u>relazione unaria</u>
es. "Allo studente x è piaciuta la lezione di matematica."
In questo caso lo studente x è parte di un sottoinsieme degli studenti totali.
Definendo x si ha una <u>sentenza</u> o una <u>relazione zeroaria.</u>

Prendiamo invece per esempio questa frase:
"Allo studente x è piaciuta la lezione y"
Questa si chiama <u>relazione binaria</u> e in tal caso è una relazione binaria sul prodotto cartesiano dell'insieme degli studenti e dell'insieme delle lezioni.
Continuando con i prodotti cartesiani, supponiamo di farne uno tra l'insieme X e sé stesso: avremo questo



Con R $\subseteq$ X x X

Adesso supponiamo di prendere una relazione binaria dove son presenti le coppie di valori "uguali"



Questa relazione la possiamo chiamare diagonale, relazione diagonale o UGUAGLIANZA ed è indicata da Δ(X)

$\Delta(X) = \{(x, x): x \in X\}$

Prendendo per esempio x e y → x = y <=> (x, y) ∈ Δ(X) ovvero x e y sono uguali se la loro coppia è presente della diagonale.

∈ si assume come simbolo primitivo.

Il sottoinsieme che definisce la relazione viene anche chiamato grafo della relazione.

Ritornando alle relazioni esse possono essere definite anche come sottoinsiemi di prodotti cartesiani.

Considerando che una relazione zeroaria è il sottoinsieme di un prodotto cartesiano di zero insiemi, unaria di un solo insieme, binaria di due insiemi e così via possiamo chiamarle anche relazioni n-aria dove n è il numero di insiemi coinvolti nel prodotto cartesiano.

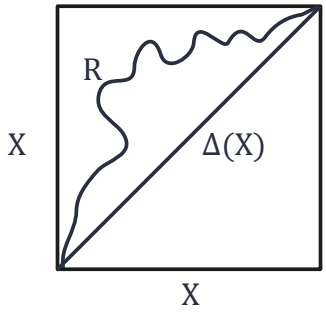
$R \subseteq \underbrace{X \times \ldots \times \ldots \times X}_{\text{n-volte}}$

Le relazioni in base a certe proprietà possono essere chiamate in determinati modi

R. RIFLESSIVA

Una relazione è detta riflessiva <=> Δ(X) ⊆ R

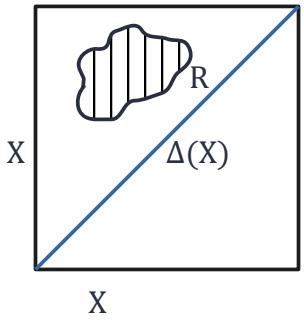
Esempi di relazioni riflessive applicate nella vita reale possono essere le amicizie, parallelismo, tolleranza e uguaglianza (Δ(X) ⊆ Δ(X))



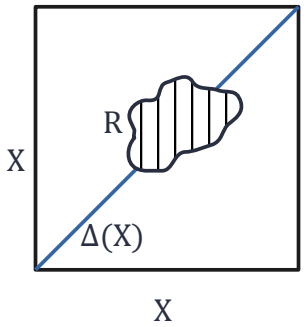
L'area interna del poligono rappresenta una relazione riflessiva

R. ANTIRIFLESSIVA

Una relazione è detta antiriflessiva <=> $\Delta(X) \cap R = \emptyset$



Esempio di relazione antiriflessiva



Esempio di relazione che non è né riflessiva ne antiriflessiva
$\Delta(X) \cap R \neq \emptyset$
$\Delta(X) \not\subset R$

R. SIMMETRICA

Una relazione è simmetrica <=> $R^{-1} = R$

R. ANTISIMMETRICA

Una relazione è antisimmetrica <=> $R^{-1} \cap R \subseteq \Delta(X)$

R. TRANSITIVA

Una relazione è transitiva <=> $(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

Le relazioni che sono:
- riflessive
- simmetriche
- transitive

si dicono EQUIVALENZE.

Una R è un PREORDINE in X se e solo se:
- R è riflessiva.
- R è transitiva.

Una R è un ORDINE in X se e solo se:
- R è un preordine
- R è antisimmetrica.

Consideriamo una relazione d'ordine possiamo scrivere
$(x, y) \in R \Leftrightarrow x \leq y$
Il simbolo $\leq$ assume come significato di appartenenza a R
Possiamo anche scrivere
$x < y \Leftrightarrow (x, y) \in R \wedge (x, y) \notin \Delta(x)$
$x \geq y$ e $x > y$ è l'ordine inverso delle relazioni definite in precedenza.

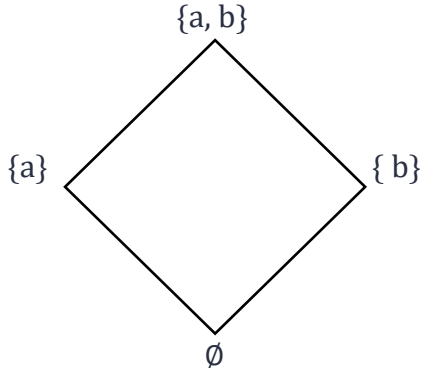
L'insieme X munito di un ordine $\leq$ è un insieme ordinato che può essere rappresentato così:
$X := (X, \leq)$ (POSET, partially ordered set)

Un ordinamento $\leq$ X è detto totale quando si verifica la proprietà di tricotomia ovvero:
Data la coppia $x, y \in X$ si verifica solo una di queste condizioni:

- $x < y$
- $x = y$
- $x > y$

Un insieme totalmente ordinato si può scrivere così $(X, \leq)$ ed è chiamato anche catena.
Il vocabolario può essere considerato come un insieme totalmente ordinato.

Esempio di insieme parzialmente ordinato, ma non totalmente:
Sia $X := \{a, b\}$, considero P(X) come l'insieme dei sottoinsiemi di X
$P(X) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
Introduco la relazione di inclusione classica $\subseteq$
$(P(X), \subseteq)$ è un POSET



P(X) non è totalmente ordinato poiché gli elementi {a} e {b} non sono confrontabili tramite $\subseteq$ nel diagramma di Hasse.

Sia $(X, \leq)$, $Y \subseteq X \longrightarrow (Y, \leq)$ ordine indotto
I sottoinsiemi di un insieme totalmente ordinati lo sono a loro volta.

Prendendo sempre $Y \subseteq X$ possiamo affermare che
$b \in X$ è un maggiorante per $Y \Leftrightarrow x \leq b, \forall x \in Y$
$a \in X$ è un minorante per $Y \Leftrightarrow a \leq x, \forall x \in Y$

----- a -------|-------Y-------|-----b---- X
Si ha
Y limitato superiormente $\Leftrightarrow \exists$ un maggiorante di Y in X
Y limitato inferiormente $\Leftrightarrow \exists$ un minorante di Y in X
Se Y è contemporaneamente limitato superiormente e inferiormente si dice che è limitato in X

e' := inf Y $\longrightarrow$ estremo inferiore
X
Un estremo inferiore è tale se:

- e' è un minorante di Y in X ($e' \leq x, \forall x \in Y$)
- $a \leq e' \ \forall$ a minorante di Y

Si può dire che e' è il più grande dei minoranti.
Se e' è un elemento di Y si chiama minimo e lo indichiamo con 'm'.

Non è detto che dato un insieme un suo sottoinsieme abbia un minimo, però esiste sempre un ordine che lo rende un buon ordinamento, ovvero in un insieme si può trovare almeno un sottoinsieme che ammette un minimo.

e'' := $\sup_X Y$ ⟶ estremo superiore

Un estremo superiore è tale se:

- e'' è un maggiorante di Y in X ($x \leq e'', \forall x \in Y$)
- $e'' \leq b \ \forall$ b maggiorante di Y

Si può dire in questo caso che e'' è il più piccolo dei maggioranti.
Se è un elemento di Y si chiama massimo e lo indichiamo con 'M'.

Un elemento è detto massimale ⇔ $x \leq y \Rightarrow x = y$
Un elemento è detto minimale ⇔ $x \geq y \Rightarrow x = y$

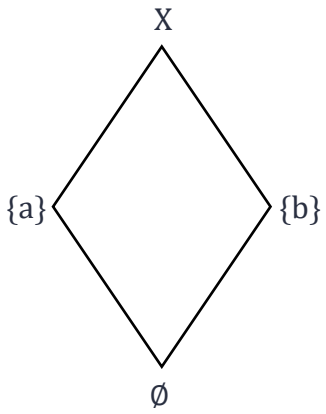
RETICOLI

I reticoli sono POSET particolari. Un reticolo può essere chiamato anche lattice.
$(X, \leq)$ in cui $\forall x, y \in X$ si trova contemporaneamente un sup{x, y} e un inf{x, y}.

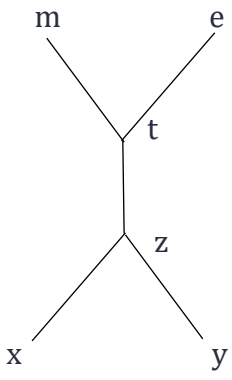
$x \vee y := \sup\{x, y\}$
$x \wedge y := \inf\{x, y\}$

Ogni insieme totalmente ordinato è un reticolo.
Con i diagrammi di Hasse possiamo visualizzare se un insieme è un reticolo o no:

1)



2)



Nell'es. 1, l'insieme è un reticolo poiché prendendo una coppia qualsiasi si riesce a trovare sempre un sup e un inf.
Ciò non accade invece nell'insieme dell'es. 2.

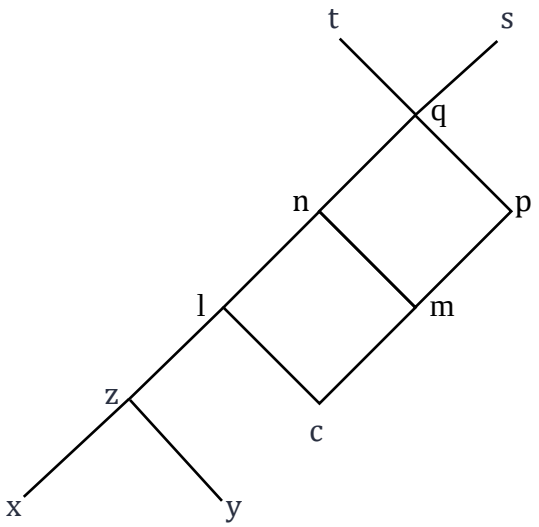
In un insieme possiamo definire delle operazioni, per esempio definiamo come operazioni nel prodotto cartesiano "vel" ed "et":
$(X, \vee, \wedge)$ $\vee: X \times X \longrightarrow X$ $\wedge: X \times X \longrightarrow X$
$(x, y) \in X \times X \longrightarrow x \vee y$
$(x, y) \in X \times X \longrightarrow x \wedge y$
Un insieme X con operazioni viene definito reticolo se e solo se gode di queste 4 proprietà:

1) Legge commutativa
   $x \wedge y = y \wedge x$
   $x \vee y = y \vee x$
   $\forall\, x, y \in X$
2) Legge associativa
   $x \vee (y \vee z) = (x \vee y) \vee z$
   $x \wedge (y \wedge z) = (x \wedge y) \wedge z$
   $\forall\, x, y, z \in X$
3) Legge di assorbimento
   $x \vee (x \vee y) = x$
   $x \wedge (x \wedge y) = x$
   $\forall\, x, y \in X$
4) Legge di idempotenza
   $x \vee x = x$
   $x \wedge x = x$
   $\forall\, x \in X$

Con $\wedge = \inf(x, y)$ e $\vee = \sup(x, y)$ si può notare che la prima definizione di reticolo è comunque esatta.

Esercizio di ripasso:

X =



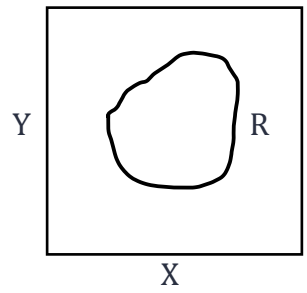
- X non è un lattice o reticolo perché esistono coppie che non ammettono un sup o un inf; per esempio {t, s} non ha un sup.
- {t, s} sono i massimali, {x, y} i minimali dell'insieme.

Consideriamo adesso Y = {q, n, p, l, m, c} con Y ⊆ X

- Si può definire un buon' ordine poiché ammette un minimo ⟶ {c}
- E' un reticolo perché prese due coppie qualsiasi dell'insieme si trova sempre un sup e un inf.
- E' limitato superiormente (e'' = {q}) e inferiormente (e' = {c}) e perché i due estremi sono appartenenti a Y essi sono rispettivamente il massimo M e il minimo m.
- I maggioranti di Y sono {t, s, q} e i minoranti {z, c, x, y}.

RELAZIONI TRA DUE INSIEMI X E Y

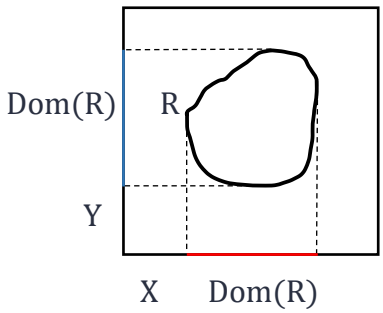
Siano dati due insiemi X e Y non vuoti, X, Y ≠ ∅, la relazione del prodotto cartesiano è definita come R ⊆ X x Y



Dato R abbiamo un:

- Dominio o Dom(R) := {x | ∃ y ∈ Y ∧ (x, y) ∈ R}
- Codominio o Cod(R) := {y | ∃ x ∈ X ∧ (x, y) ∈ R}
- Dom(R) ⊆ X, Cod(R) ⊆ Y

Si può dire che il dominio è la proiezione della relazione su X, il codominio è la proiezione della relazione su Y. Il codominio viene definito anche come immagine o Imm(R).
Si possono visualizzare graficamente:



La linea colorata di rosso è il dominio, quella di blu è il codominio.

Sia x ∈ X, y ∈ Y per definizione abbiamo x R y ⇔ (x, y) ∈ R
Dati X ed Y e il predicato P(x, y) è definita estensione:
E := {(x, y) : (x, y) ∈ X x Y ∧ P(x, y)}
L'estensione è costituita dalle coppie x, y che soddisfano il predicato P.
P(x, y) ⟶ R ⊆ X x Y Da un predicato nasce una relazione e viceversa.

Dati X, Y ≠ ∅; T ⊆ X x Y

T^{-1} := {(y, x) | (x, y) ∈ T } inversa
T^{C} := {(x, y) | (x, y) ∉ T } complementare (ovvero tutte le coppie non presenti in T in X x Y)

Proprietà delle relazioni nel prodotto cartesiano tra X e Y

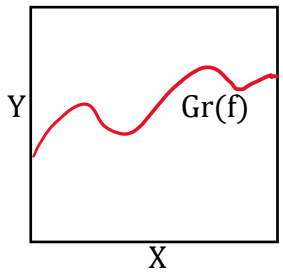
Dati $R, S \subseteq X \times Y$

- Se $R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$
- Se $R \subseteq S \Rightarrow S^C \subseteq R^C$
- $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$
- $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$
- $(R \cap S)^C = R^C \cup S^C$
- $(R \cup S)^C = R^C \cap S^C$

Le ultime due proprietà vengono anche chiamate leggi di De Morgan.
Dati tre insiemi X, Y, Z con le seguenti relazioni:
$R \subseteq X \times Y, S \subseteq Y \times Z$
Viene definita relazione composta:
$S \circ R \subseteq X \times Z$ (R "indica" S)
$\Leftrightarrow (x, z) \in S \circ R \Leftrightarrow \exists\, y \in Y : (x, y) \in R \wedge (y, z) \in S$
n.b. La composizione tra relazioni non è commutativa.

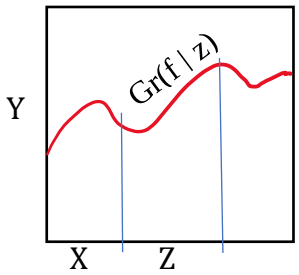
Concetto di funzione definito come insieme

Sia un grafo di f $Gr(f) \subseteq X \times Y$, esso esiste se e solo se:
$\forall\, x \in X\ \exists!\, y \in Y : (x, y) \in Gr(f)$
La formula scritta sopra può essere anche scritta così:
$f : X \longrightarrow Y$
Ogni funzione deve rispettare la seguente regola:
$(x, y) \in Gr(f) \wedge (x, z) \in Gr(f) \Rightarrow y = z$
Il dominio di una funzione equivale a $X \longrightarrow Dom(Gr(f)) = X$
$Cod(f) = f(x) = Cod(Gr(f))$
Per "abuso di scrittura" $\forall\, x \in X\ \exists!\, y \in Y : (x, y) \in Gr(f)$ può essere scritto anche:
$\forall\, x \in X\ \exists!\, y \in Y : y = f(x)$



Esempio di funzione (linea rossa)
Si nota che per ogni x è associato un solo elemento y

Si dice che una funzione è limitata su Z quando:
$Z \subseteq X \quad f : X \longrightarrow Y \quad f \mid z : Z \longrightarrow Y$
$Gr(f \mid z) = Gr(f) \cap (Z \times Y)$



La parte di Gr(f) limitata da Z è Gr(f | z)

- $f : X \longrightarrow Y$ è suriettiva $\Leftrightarrow f(x) = Y$ (il codominio è tutto Y)
- $f : X \longrightarrow Y$ è iniettiva $\Leftrightarrow \forall\, x, y \in X, x \neq y \Rightarrow f(x) \neq f(y)$
- $f : X \longrightarrow Y$ è biettiva $\Leftrightarrow$ f è iniettiva e suriettiva allo stesso tempo

- una funzione f è detta invertibile se e solo se la sua relazione inversa è una funzione. Ciò accade solo con le funzioni biettive, perciò possiamo dire una funzione è invertibile se e solo se la funzione è biettiva e viceversa.

Funzione identica: $id_x : X \longrightarrow X, \ \forall x \in X \ id_x(x) = x$
Funzione composta:
$f : X \longrightarrow Y$
$g : Y \longrightarrow Z$
$(g \circ f)(x) = g(f(x)) \ \forall x \in X$

STRUTTURE ALGEBRICHE

Sia $X \neq \emptyset$, un operazione interna binaria su X è una funzione definita così:
$* : X \times X \longrightarrow X$
$(x, y) \in X \times X \longrightarrow x * y \in X$

Strutture algebriche fondamentali

Sia $A \neq \emptyset$, in esso si introducono due operazioni binarie
$+_A : A \times A \longrightarrow A$ somma in A
$\cdot_A : A \times A \longrightarrow A$ prodotto in A
L'operazione di somma deve soddisfare queste quattro proprietà:

1) $(x +_A y) +_A z = x +_A (y +_A z) \ \ \forall x, y, z \in A$ (proprietà associativa)
2) $x +_A y = y +_A x \ \ \forall x, y \in A$ (proprietà commutativa)
3) $\exists \ 0_A \in A : x +_A 0_A = x, \forall x \in A$ (esistenza dell'elemento neutro 0_A)
4) $\forall x \in A, \exists \ y_x \in A : x +_A y = 0$ (esistenza degli opposti; $y_x = -x$)

Invece rispetto al prodotto $\cdot_A$ si assume esso goda queste proprietà:

1) $(x \cdot_A y) \cdot_A z = x \cdot_A (y \cdot_A z) \ \ \forall x, y, z \in A$ (proprietà associativa)
2) $(x \cdot_A y) = (y \cdot_A z) \ \forall x, y \in A$ (proprietà commutativa)
3) $\exists \ 1_A \in A : x \cdot_A 1_A = x, \forall x \in A$ (esistenza dell'elemento neutro 1_A)

Entrambe le operazioni devono soddisfare le leggi o assiomi di distribuzione:

1) $x \cdot_A (y +_A z) = (x \cdot_A y) +_A (x \cdot_A z) \ \ \forall x, y, z \in A$
2) $(x +_A y) \cdot_A z = (x \cdot_A z) +_A (y \cdot_A z) \ \ \forall x, y, z \in A$

La coppia logica $A := (A, +_A, \cdot_A)$ è un anello commutativo con identità 1_A (o Abeliano).

LEGARE LA TEORIA DEGLI ANELLI A QUELLA DEI RETICOLI

Un anello $(A, +, \cdot)$ è detto booleano se:

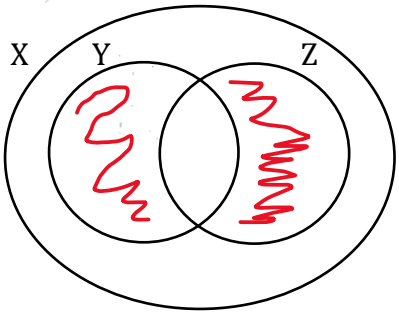
1) È unitario, ossia $1_A \in A$
2) Ogni elemento di A è idempotente, ossia $\forall x \in A\ x$

Sia $X \neq \emptyset$ un insieme e $P(X)$ l'insieme dei sottoinsiemi delle sue parti si considerino le seguenti operazioni:

$\Delta : P(X) \times P(X) \longrightarrow P(X)$

Tale che $\forall Y, Z \in P(X), (Y, Z) \longrightarrow Y \Delta Z$

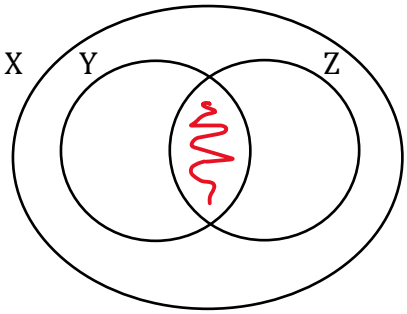
Dove $Y \Delta Z = (Y \setminus Z) \cup (Z \setminus Y)$ è la differenza simmetrica



Le aeree col rosso indicano la differenza simmetrica.

$\cap : P(X) \times P(X) \longrightarrow P(X)$

Tale che $\forall Y, Z \in P(X), (Y, Z) \longrightarrow Y \cap Z$



L'area col rosso indica l'intersezione.

Ciò che abbiamo ottenuto è la struttura $(P(X), \Delta, \cap)$.

Si può dimostrare che esso è un anello booleano poiché:

1) Ha un elemento unitario 1_A che è X ($\forall Y \in P(X), Y \cap X = Y$)
2) Ogni suo elemento è idempotente ($\forall Y \in P(X), Y \cap Y = Y$)

Dalle osservazioni precedenti le strutture vengono indicate con $(P(X), \leq, \vee, \wedge)$

Si noti che $(P(X), \subseteq)$ è un reticolo limitato ovvero esiste un $\min P(X) = \emptyset$ e $\max P(X) = X$ rispetto a $\subseteq$.

Dato un reticolo limitato $(R, \leq, \vee, \wedge)$ e sia $a \in R$, un elemento $b \in R$ è detto complemento di a in R se e solo se:

- $a \vee b = \max R$
- $a \wedge b = \min R$

Dato a, può esistere più di un complemento di a in R.

Ciò non succede in $(P(X), \subseteq, \cup, \cap)$ poiché:

$\forall Y \in P(X)$

$Y \cup (X \setminus Y) = X = \max P(X)$

$Y \cap (X \setminus Y) = \emptyset = \min P(X)$

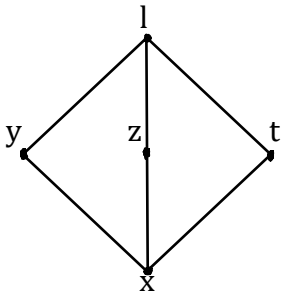
Ossia in P(X) per ogni Y esiste un unico complemento che è $X \setminus Y$

Ricapitolando un reticolo $(R, \leq, \vee, \wedge)$ è definito complementato se e solo se $\forall x \in R$ esiste almeno un complemento.

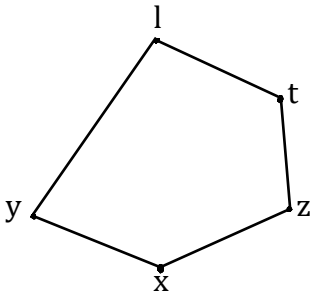
Un reticolo $(R, \leq, \vee, \wedge)$ è detto distributivo se e solo se per definizione valgono le seguenti leggi $\forall\, x, y, z \in R$:

1) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
2) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

I reticoli trirettangolo e pentagonali non sono mai distributivi



$y \wedge (z \vee t) = y \wedge l = y$
$(y \wedge z) \vee (y \wedge t) = x \vee x = x$
In questo caso $y \wedge (z \vee t) \neq (y \wedge z) \vee (y \wedge t)$



$z \vee (y \wedge t) = z \vee x = z$
$(z \vee y) \wedge (z \vee t) = l \wedge t = t$
Anche qui non viene rispettata la legge distributiva
TEOREMA DI BIRKHOFF: Un reticolo $(R, \leq, \vee, \wedge)$ è distributivo se e solo se non esistono sottoreticoli di R isomorfi al reticolo trirettangolo o pentagonale

Un reticolo $(R, \leq, \vee, \wedge)$ è detto booleano se e solo se per definizione esso è:

1) distributivo
2) complementato

Dunque $(P(X), \subseteq, \cup, \cap)$ è un reticolo booleano poiché si può dimostrare che è complementato e distributivo. Dunque, valgono i seguenti fatti:

1) $(P(X), \cup, \emptyset)$ e $(P(X), \cap, X)$ sono monoidi commutativi.
2) $Y \cup (Y \cap Z) = Y$ e $Y \cap (Y \cup Z) = Y \quad \forall\, Y, Z \in P(X)$ (Leggi di assorbimento)
3) Valgono le leggi distributive
4) $\forall\, Y \in P(X) \longrightarrow Y \cap (X \setminus Y) = \emptyset$ e $Y \cup (X \setminus Y) = X$

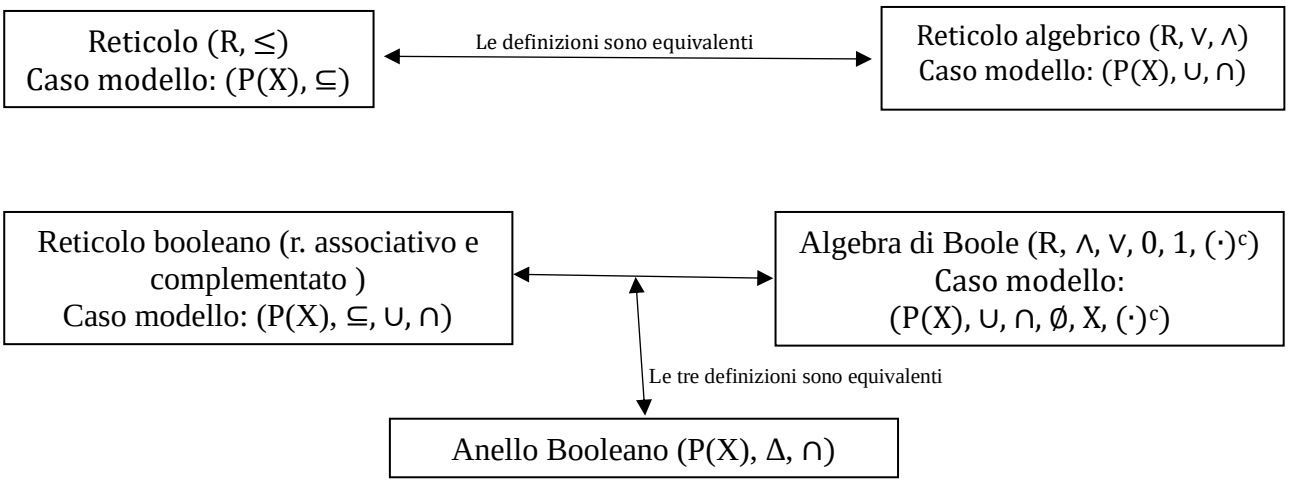
Una struttura algebrica $(R, \wedge, \vee, 0, 1, (\cdot)^c)$ è detta algebra di Boole se e solo se:

- $0, 1 \in R$ sono costanti o relazioni 0-arie
- $(\cdot)^c : R \longrightarrow R$ è un operazione unaria
- $\wedge, \vee : R \times R \longrightarrow R$ sono operazioni binarie

Tali che:

1) $(R, \vee, 0)$ e $(R, 1, 1)$ sono monoidi commutativi
2) Valgono le leggi di assorbimento
3) Valgono le leggi distributive
4) $x \vee x^c = 1, x \wedge x^c = 0 \quad \forall\, x \in R$

Pertanto $(P(X), \cup, \cap, \emptyset, X, (\cdot)^c)$ è un algebra di Boole.
In generale vale che le nozioni di reticolo booleano e algebra di Boole sono equivalenti



L'anello booleano $(P(X), \Delta, \cap)$ è un' algebra di Boole poiché esso può essere definito come la seguente struttura: $(P(X), ?, \cap, \emptyset, X, (\cdot)^c)$.
In '?' possiamo usare Δ e $\cap$ per definire $\cup$ in questo modo: $Y \cup Z = (Y \Delta Z) \Delta (Y \cap Z)$

EQUIVALENZE TRA GLI ANELLI BOOLEANI E ALGEBRE DI BOOLE

Sia $(R, +, \cdot)$ un anello booleano, ovvero esiste l'elemento unitario 1_R in R e ogni elemento dell'insieme è idempotente possiamo per definizione strutturarlo come algebra di Boole: $(R, \vee, \wedge, 0, 1, (\cdot)^c)$

Tale che:
$x \vee y := x + y + xy$
$x \wedge y := xy$
$0 = 0_R$ $\forall x, y \in R$
$1 = 1_R$
$x^c = 1 + x$

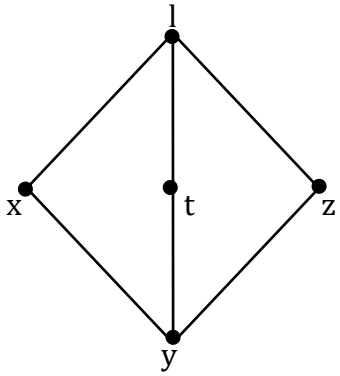
Poiché caratterizzando in questo modo le operazioni si può provare che esse soddisfano tutte le proprietà delle algebre di Boole.
Viceversa, da un algebra di Boole si può provare che esso è un anello booleano:
$(R, \vee, \wedge, 0, 1, (\cdot)^c) \Rightarrow (R, +, \cdot)$

Tale che:
$x + y := (x \wedge y^c) \vee (x^c \wedge y)$ $\forall x, y \in R$
$x \cdot y := x \wedge y$

Le operazioni così definite soddisfano le proprietà degli anelli di Boole.
Ciò dimostra che si può passare da anello di Boole ad algebra booleana e viceversa, dimostrando che le due definizioni sono equivalenti.
La dimostrazione prende il nome di Teorema di caratterizzazione di Stone.

DEFINIZIONE DI SOTTORETICOLO

Prendiamo un reticolo R rappresentato dal diagramma di Hasse così:

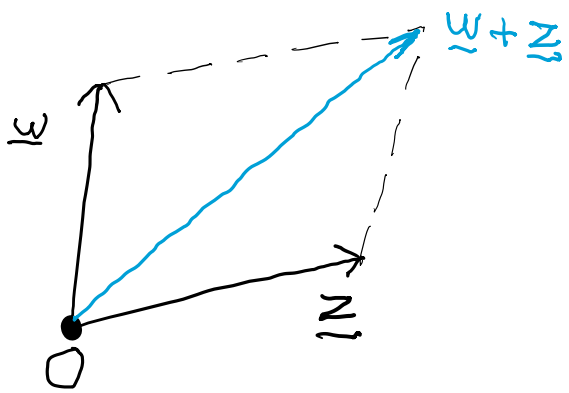


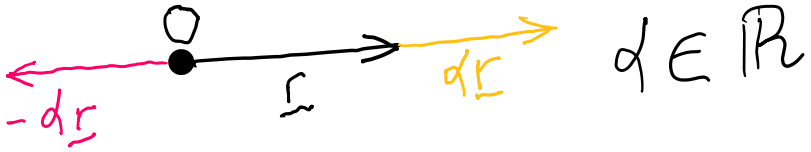
Il sottoinsieme X = {x, t, z} è un sottoreticolo? No, poiché esso non soddisfa le proprietà dei reticoli. Per esempio: sup{x, t} = l, l ∉ X
Si può dire che un sottoinsieme X di un reticolo R è un sottoreticolo se e solo se:
∀ x, y ∈ X
x ∧ y ∈ X, x ∨ y ∈ X
ovvero X è stabile rispetto alle operazioni ∧ e ∨.

OPERAZIONI INTERNE ED ESTERNE

Sia S ≠ ∅, in esso possiamo definire un'operazione
⊥ : S x S ⟶ S
L'immagine ⊥(x, y) delle coppie (x, y) ∈ S x S viene detto composto di x e y e si indica con x ⊥ y.
Si usano anche i simboli *, f (es. * : S x S ⟶ S) e per i composti i simboli + o · (es. x ⊥ y diventa x + y)
Generalmente la scrittura ⊥ : S x S ⟶ S indica un'<u>operazione interna</u>

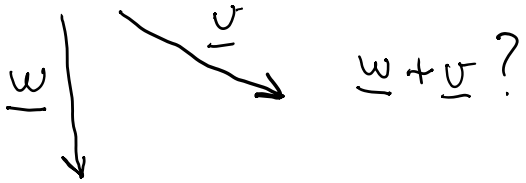
Siano S, Ω ≠ ∅
⊥ : Ω x S ⟶ S
In questo caso ⊥ è un <u>operazione esterna</u> (applicazione) in cui Ω è il dominio degli operatori
Osservazione: se Ω = S si ha che ogni legge interna in S può essere vista come una legge esterna speciale in cui il dominio degli operatori è S.
Esempio:
Si consideri V2 l'insieme dei vettori geometrici di centro O nel piano Euclideo E2 e lo muniamo di operazioni
+ : V2 x V2 ⟶ V2
· : R x V2 ⟶ V2



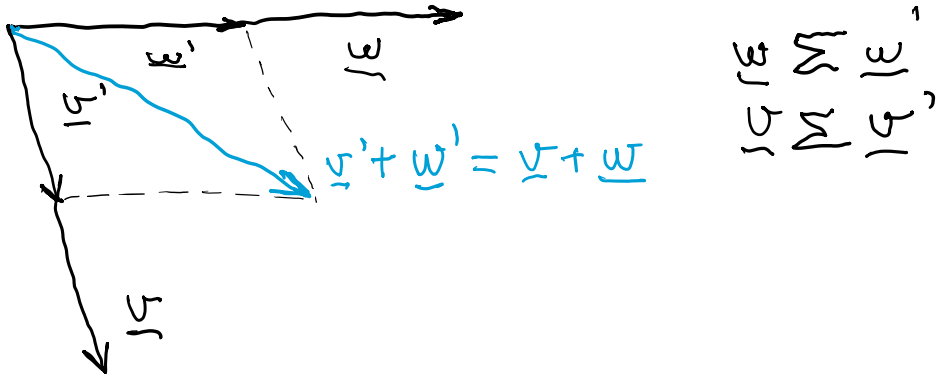


'+' è una legge interna, mentre '·' è una legge esterna.

Sia V l'insieme dei vettori geometrici di un piano euclideo con le seguenti operazioni.
$+ : V \times V \longrightarrow V$
$\cdot : R \times V \longrightarrow V$
Sorge un problema con l'operazione '+'
Prendiamo due vettori e proviamo a fare la somma.



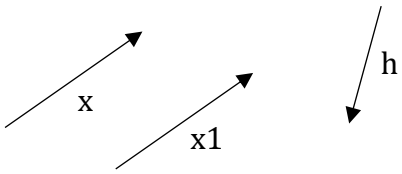
Con gli strumenti a disposizione ciò non è possibile.
Proviamo allora a introdurre la relazione $\sum$ di equivalenza tale che:
$\underline{v} \sum \underline{v'} \Leftrightarrow \underline{v}$ e $\underline{v'}$ hanno stesso modulo, intensità e verso (equipollenza)



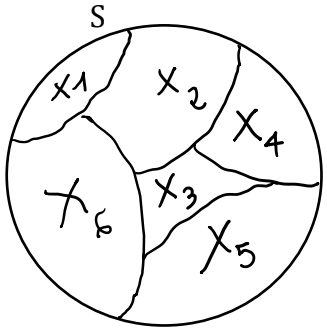
Grazie al passaggio di quoziente v + w è equipollente a v' + w' anche se ciò non è sempre vero per tutte le strutture

INSIEME QUOZIENTE

Sia $(S, +)$, $S \neq \emptyset$ munito di relazione di equivalenza $\sum$, l'insieme quoziente indica un insieme tale che:
$S/\sum := \{ [x]_\sum , x \in S \}$
$[x]_\sum := \{ y \in S : y \sum x \}$
$[x]_\sum$ è la classe di equivalenza di x modulo $\sum$



Prendendo l'insieme V di prima possiamo dire:
$x \in [x]_\sum$
$x1 \in [x]_\sum$
$h \notin [x]_\sum$
Per transitività si può cambiare rappresentate della classe di equivalenza ed essa non cambierebbe:
$[x]_\sum = [x1]_\sum$
Viceversa, da un insieme partizionato si può arrivare a una relazione di equivalenza:



S è formata dai sottoinsiemi di tipo (X_α) dove $\alpha \in \Lambda$ (in questo esempio $\Lambda := \{1, 2, 3, 4, 5, 6\}$) in cui l'intersezione tra due sottoinsiemi di S da $\emptyset$ e l'unione di tutti i sottoinsiemi da S.
Si può dire allora che $\forall x, y \in S$:
$x \sum y \Leftrightarrow \exists \alpha \in \Lambda : x, y \in X_\alpha$

ELEMENTI DI UN INSIEME DOTATO DI OPERAZIONE

Dato un insieme $(S, \perp)$
$\perp : S \times S \longrightarrow S$
Possiamo trovare tre tipi di elementi

1) Elemento neutro
2) Elementi simmetrizzabili
3) Elementi regolari

ELEMENTO NEUTRO

Un elemento $e \in S$ è neutro se e solo se per definizione:
$e \perp x = x \perp e = x \quad \forall x \in S$
Si può dimostrare che l'elemento neutro 'e' in S è unico:
$e' \in S \Leftrightarrow e' \perp x = x \perp e' = x \quad \forall x \in S$
$e \in S \Leftrightarrow e \perp x = x \perp e = x \quad \forall x \in S$
$e = e \perp e' = e'$
$e = e'$

Esistono elementi che sono neutri solo a destra:
$x \perp e = x$
ed elementi che sono neutri solo a sinistra:
$e \perp x = x$
Non è detto che essi siano unici! Possiamo avere più elementi neutri a destra o a sinistra. Però se un insieme ha un elemento e' neutro a destra e uno e'' a sinistra si può provare che essi sono un unico elemento che è l'elemento neutro:
$e' \perp x = x \quad \forall x \in S$
$x \perp e'' = x \quad \forall x \in S$
allora
$e' \perp e'' = e''$
ma anche
$e' \perp e'' = e'$
dunque
$e' = e''$
Nelle strutture commutative ciò è banale.
Si nota che se esistono più elementi neutri a sinistra (o destra) non esistono elementi neutri a destra (o sinistra)
Per esempio:

$\perp$	a	b	c
a	a	c	a
b	b	a	b
c	c	b	c

In questo caso non esiste l'elemento neutro, ma due elementi neutri a destra 'a' e 'c'

Infatti:
$a \perp a = a \qquad a \perp c = a$
$b \perp a = b \qquad b \perp c = b$
$c \perp a = c \qquad c \perp c = c$

ELEMENTI SIMMETRIZZABILI

Un elemento $x \in S$ è detto simmetrizzabile in S se e solo se per definizione
$\exists\, x' \in S : x' \perp x = x \perp x' = e$
Se $\perp$ viene rappresentato come '+' , x' viene indicato come -x mentre se $\perp$ viene rappresentato come '·' allora x' viene indicato come x^{-1}
Possono esistere più elementi simmetrici tranne nelle strutture associative dove si può dimostrare che il simmetrico è unico:
se per assurdo oltre a x' abbiamo un secondo x'' simmetrico e $\perp$ è associativo:
$x'' \perp x = x \perp x''$
$x'' = e \perp x''$
$e = x' \perp x$
dunque
$x'' = (x' \perp x) \perp x''$
per associatività possiamo anche scrivere
$x'' = x' \perp (x \perp x'')$
però $x \perp x'' = e$
$x'' = x' \perp e$
$x'' = x'$

Un elemento è detto simmetrizzabile a sinistra se $x' \perp x = e \;\forall\, x \in S$, mentre è detto simmetrizzabile a destra se $x \perp x' = e \;\forall\, x \in S$
Proposizione: se $\perp$ è associativo in S allora se x ha un x' simmetrico a sinistra e x'' simmetrico a destra allora x' = x'' ed è l'elemento simmetrico di x e si verifica:
$x' \perp x = e$
$x \perp x'' = e$
allora
$x' \perp x = x \perp x''$
possiamo scrivere
$(x' \perp x) \perp x'' = x' \perp (x \perp x'')$
Sappiamo che $(x' \perp x)$ e $(x \perp x'')$ equivalgono a 'e'.
$e \perp x'' = x' \perp e$
$x'' = x'$

ELEMENTI REGOLARI (O CANCELLABILI)

Un elemento $a \in S$ è detto regolare a sinistra se:
$a \perp x = a \perp y => x = y$
Un elemento $a \in S$ è detto regolare a destra se:
$x \perp a = y \perp a => x = y$
In una struttura commutativa un elemento regolare a destra lo è anche a sinistra.
Se un elemento 'a' è regolare a destra e regolare sinistra si dice semplicemente che è regolare (o cancellabile).
Si può dimostrare che in una struttura associativa un elemento simmetrizzabile è anche regolare:
$(S, \perp)$ $\perp$ associativo

- ➔ $a \in S$ è simmetrizzabile $\Leftrightarrow \exists\, a' \in S : a' \perp a = a \perp a' = e$
- ➔ a è regolare $\Leftrightarrow a \perp x = a \perp y => x = y \;\; \forall\, x, y \in S$

$a \perp x = a \perp y$
segue che
$a' \perp (a \perp x) = a' \perp (a \perp y)$

$(a' \perp a) \perp x = (a' \perp a) \perp y$
$e \perp x = e \perp y \Rightarrow x = y$

Gli elementi regolari di S rispetto a $\perp$ associativo sono tutti elementi simmetrizzabili assunto che S sia finito.
Premesse:

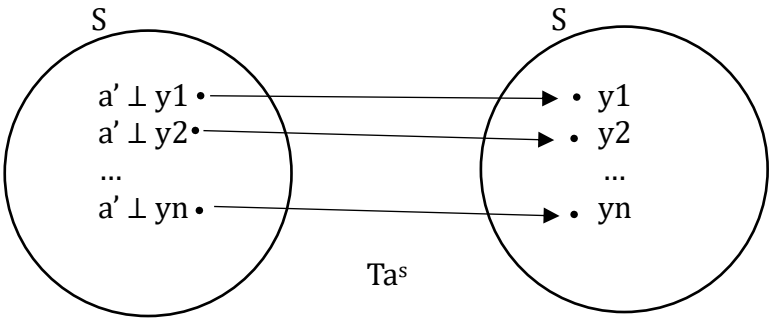
- a è regolare a destra se e solo se per definizione la funzione traslazione a destra in a è iniettiva:
  $Ta^d : S \longrightarrow S$
  $Ta^d(x) = x \perp a$
  $Ta^d(x) = Ta^d(y) \Leftrightarrow (x \perp a = y \perp a \Rightarrow x = y)$
- a è regolare a sinistra se e solo se per definizione la funzione traslazione a sinistra in a è iniettiva:
  $Ta^s : S \longrightarrow S$
  $Ta^s(x) = a \perp x$
  $Ta^s(x) = Ta^s(y) \Leftrightarrow (a \perp x = a \perp y \Rightarrow x = y)$

Proposizione: sia $\perp$ una legge associativa in S per un elemento $a \in S$ le seguenti tre affermazioni sono equivalenti

1) 'a' è simmetrizzabile
2) Ta^s e Ta^d sono biettive
3) Ta^s e Ta^d sono suriettive

Premessa:
Una funzione $f : S \longrightarrow S$ è suriettiva se $\forall z \in S \; \exists y \in S : f(y) = z$

Dimostrazione (1) $\longrightarrow$ (2):
Se 'a' è simmetrizzabile, poiché $\perp$ è associativo si ha che è anche regolare, ossia le funzioni di traslazione destra e sinistra in a sono iniettive. Proviamo allora che esse sono suriettive:
Sia a' il simmetrico di a in S, allora $\forall y \in S, \exists a' \perp y \in S$ tale che
$Ta^s (a' \perp y) = a \perp (a' \perp y) = (a \perp a') \perp y = e \perp y = y$
Ciò si può visualizzare graficamente:



Analogamente $\forall y \in S, \exists y \perp a' \in S$ tale che
$Ta^d (y \perp a') = (y \perp a') \perp a = y \perp (a' \perp a) = y \perp e = y$
Poiché le funzioni di traslazione sono sia iniettive che suriettive esse sono biettive.
(2) => (3) è banale (se le funzioni sono biettive allora sono certamente suriettive)
(3) => (1)
Ta^d è suriettiva $\Leftrightarrow a \in S \; \exists x \in S : Ta^d (x) = x \perp a = a$
x è l'elemento neutro a sinistra
Ta^s è suriettiva $\Leftrightarrow \forall a \in S \; \exists x \in S : y = Ta^s (x) = a \perp x = a$

Si ha allora
$u \perp y = u \perp (a \perp x) = (u \perp a) \perp x = Ta^d(u) \perp x = a \perp x = y$
Allo stesso modo
Ta^s è suriettiva $\Leftrightarrow a \in S \; \exists \, v \in S : Ta^s(v) = a \perp v = a$
Poiché 'u' è elemento neutro a sinistra e 'v' elemento neutro a destra per la dimostrazione fatta in precedenza $v = u = e$ che è l'elemento neutro di $\perp$ in S.
Resta da dimostrare che $\exists \, a' \in S : a' \perp a = a \perp a' = e$
Poiché Ta^s è suriettiva $\Rightarrow \exists \, a1 \in S : Ta^s(a1) = a \perp a1 = e$
Analogamente Ta^d è suriettiva $\Rightarrow \exists \, a2 \in S : Ta^d(a2) = a2 \perp a = e$
Pertanto:
$a2 = a2 \perp e = a2 \perp (a \perp a1) = (a2 \perp a) \perp a1 = e \perp a1 = a1$
e si ha
$a1 \perp a = e = a \perp a2$
In conclusione, $a1 = a2 = a'$ che è il simmetrico di a in S

Per dimostrare che le funzioni di traslazione sono suriettive posso per assurdo assumere che esse non siano suriettive. Prendiamo per esempio Ta^s.
Se Ta^s non fosse suriettiva, l'immagine della funzione sarebbe un sottoinsieme di S.
Però visto che la funzione è iniettiva si ha che il numero di elementi di essi equivale a quello di S. Ciò vuol dire che la funzione deve essere per forza suriettiva.
Analogamente ciò vale lo stesso per Ta^d.

NUMERI NATURALI

Assumiamo per buona qualche teoria di insiemi in cui esiste $\emptyset := 0$
Considero che $\{\emptyset\} = \{0\} := 1$
$\{0, 1\} = \{\emptyset, \{\emptyset\}\} := 2$
$\{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} : = 3$
$\{0, 1, 2, 3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} : = 4$
E così via… (ricorsione)
In generale possiamo dire che:
$n := \{0, 1, \dots, n-1\}$
Tramite questo modello posso definire i numeri naturali tramite il vuoto.
Preso un 'n' qualsiasi chiamo successivo di $n \longrightarrow (n+1)$ o $s(n)$ tale che
$s(n) = n+1 = \{0, 1, \dots, n\}$
Per esempio
$s(6) = 6+1 = \{0, 1, 2, 3, 4, 5, 6\} = 7$
In generali $n+1 = n \cup \{n\}$
Nel modello valgono gli assiomi di Peano:
$\exists$ un insieme $\mathbb{N}$ ed una funzione $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$ tale che:

1) $0 \in \mathbb{N}$ $(\mathbb{N} \neq \emptyset)$
2) La funzione $\sigma : \mathbb{N} \longrightarrow \mathbb{N} \setminus \{0\}$ è iniettiva
3) Vale il principio di induzione matematica
   Se $X \subseteq \mathbb{N}$ tale che: $0 \in X$ e $\forall x \in X \Rightarrow \sigma(x) \in X$ implica che $X = \mathbb{N}$

Riprendendo il principio di induzione:
$X \subseteq \omega$
$0 \in X$
$\sigma(x) = x + 1 : X \longrightarrow X$
Dunque, $\forall x \in X \Rightarrow x + 1$
Ciò implica che $X = \omega$
Si nota come il principio definisca in astratto che l'insieme è infinito.
Possiamo vedere inoltre che $(X, +)$ è stabile e che ω è un buon ordine.

Sia ω e $\mathbb{N}$ indicano i numeri naturali e dunque sono lo stesso insieme, soltanto che ω viene usato quando si usa la teoria degli insiemi di Von Neumann mentre $\mathbb{N}$ è un modello astratto.

Posso introdurre somma e prodotto tramite ricorsione:
$(\mathbb{N}, +, \cdot)$
Somma e prodotto funzionano come ci è sempre stato insegnato.
Ciò che otteniamo è un semianello.
Possiamo introdurre un ordine tale che $n \leq m \Leftrightarrow n \subseteq m \ \ \forall n, m \in \mathbb{N}$
Verifichiamo se $\leq$ soddisfa le proprietà degli ordini:

1) Riflessività – $n \leq n \Rightarrow n = n$
   $n \subseteq n \Rightarrow n = n$
2) Antisimmetria – $n \leq m$ e $m \leq n \Rightarrow n = m$
   $n \subseteq m$ e $m \subseteq n \Rightarrow n = m$ (doppia inclusione)
3) Transitività – $n \leq m$, $m \leq t \Rightarrow n \leq t$
   $n \subseteq m$, $m \subseteq t \Rightarrow n \subseteq t$

Poiché l'ordine verifica le proprietà di tricotomia, $(\mathbb{N}, \leq)$ è un insieme totalmente ordinato.

Se in ($\mathbb{N}, +, \cdot, \leq$) valgono le seguenti proprietà

1) $\forall$ n, m, t $\in \mathbb{N}$ n $\leq$ m $\Leftrightarrow$ n + t $\leq$ m + t
2) $\forall$ n, m, t $\in \mathbb{N}$ n $\leq$ m $\Leftrightarrow$ nt $\leq$ mt

Ossia le operazioni sono compatibili con l'ordine allora si può dire che è un semianello totalmente ordinato. $\mathbb{N}$ non è un anello poiché non ci sono opposti.

Problema:

$1 + 2 + 3 + \ldots + n = \frac{(n+1)\,n}{2}$

Come lo si dimostra?

Per fare ciò si usa il principio di induzione.

Supponiamo di avere un predicato P(n) dipendente da n $\in \mathbb{N}$.

1) Si suppone che $P(n_0)$ sia vero
2) Se P(n-1) è vero allora P(n) è vero $\forall$ n >= n_0

In questo caso $n_0 = 0$ e $P(n_0) = \frac{(0+1)0}{2} = 0$ ed è vero.

$P(n\text{-}1) = 1 + 2 + \ldots + (n - 1) = \frac{(n-1)\,n}{2}$

Dunque:

$P(n) = \frac{(n-1)\,n}{2} + n = \frac{(n+1)\,n}{2}$

La formula è dimostrata.

DEFINIZIONE DELL'INSIEME DEI NUMERI INTERI Z

$N := \{0, 1, 2, \ldots\}$

$N \times N = N^2 := \{(n, m) : n, m \in N\}$

In N^2 si introducono due operazioni:

$(m, n) + (s, t) := (m + s, n + t)$

$(m, n) \cdot (s, t) := (ms + mt, ns + nt)$

Es.

$(2, 1) + (3, 5) = (5, 6)$

$(2, 1) \cdot (3, 5) = (16, 8)$

N^2 non è un anello poiché mancano gli opposti.

Introduciamo una relazione di equivalenza $\sum$ tale che:

$(m, n) \sum (s, t) \Leftrightarrow m + t = n + s$

Es.

$(2, 3) \sum (2, 3)$ vero

Si crea l'insieme quoziente $N^2/\sum := \{ [m, n]_\sum : (m, n) \in N^2 \}$

(Da ora in poi nelle scritture del tipo $[x, y]_\sum$, $\sum$ sarà implicito per praticità)

$[(1, 0)] = \{[m, n] : (m, n) \sum (1, 0)\} = \{[(m, n)] : m + 0 = n + 1 \longrightarrow m = n + 1\} =$

$= \{[(n +1, n)] : n \in N\}$

Es.

$(3, 2) \in [(1, 0)]$

$(7, 2) \notin [(1, 0)]$

Adesso si troverà la classe nulla o neutra sull'addizione in $(N^2/\sum, +, \cdot)$
Sappiamo che
$[(m, n)] + [(s, t)] := [(m + t, n + s)]$
$[(m, n)] \cdot [(s, t)] := [(ms + mt, ns + nt)]$
Dobbiamo trovare $[(x, y)]$ tale che:
$[(m, n)] + [(x, y)] = [(m, n)]$
$[(m + y, n + x)] = [(m, n)]$
Ovvero
$(m + y, n + x) \sum (m, n)$
$m + y + n = n + x + m$
si arriva che
$y = x$
Dunque, tutte le classi del tipo $[(x, x)]$ sono nulle rispetto all'addizione (es. $[(0, 0)]$)
L'unità del prodotto invece è $[(1, 0)]$ (es. $[(m, n)] \cdot [(1, 0)] = [(m, n)]$)

Adesso si cercherà di trovare una classe $[(x, y)]$ tale che:
$[(m, n)] + [(x, y)] = [(0, 0)]$
$[(m + y, n + x)] = [(0, 0)]$
$m + y = 0$
$n + x = 0$
dunque
$y = m$
$x = n$
Si può affermare allora che per ogni classe del tipo $[(m, n)]$, l'elemento opposto è la classe del tipo $[(n, m)]$
$[(m, n)] + [(n, m)] = [(0, 0)]$
$[(n, m)] := -[(m, n)]$

Nell' insieme quoziente introduco un ordine $\leq$ tale che:
$[(m, n)] \leq [(s, t)] \Leftrightarrow m + t \leq n + s$
Es.
$[(1, 0)] < [(2, 0)]$
$[(0, 1)] > [(0, 2)]$
$-[(0, 1)] > [(0, 2)]$
Poiché l'ordine è totale esso è una catena
$\ldots < -[(2, 0)] < -[(1, 0)] < [(0, 0)] < [(1, 0)] < [(2, 0)] < \ldots$
$\ldots \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad \ldots$
Per ogni classe assegniamo un simbolo, ciò che otteniamo è Z, l'insieme dei numeri interi
$Z := (N^2/\sum, +, \cdot, \leq)$
Poiché esistono gli opposti, Z è un anello totalmente ordinato.

CAMPO DEI RAZIONALI Q

Sia $Z = (Z, +, \cdot, \leq)$ l'anello commutativo degli interi. In Z x N* considero la relazione di equivalenza $\sim$ definita da:
$\forall (m, n), (s, t) \in Z \times N^*, \ (m, n) \sim (s, t) \Leftrightarrow m \cdot t = n \cdot s$
L'insieme quoziente $Q := (Z \times N^*)/\sim$ viene dotato delle operazioni $+$ e $\cdot$ definite
$\forall [(m, n)], [(s, t)] \in Q$

- $[(m, n)] + [(s, t)] := [(t \cdot m + s \cdot n, n \cdot t)]$
- $[(m, n)] \cdot [(s, t)] := [(m \cdot s, n \cdot t)]$

Definiamo in Q un ordine totale tale che:
$[(m, n)] \leq [(s, t)] \Leftrightarrow m \cdot t \leq n \cdot s$ per definizione.
Sappiamo che $[(m, n)] \cdot [(n, m)] = [(1, 1)]$ con m diverso da 0.
Ogni anello commutativo ordinato con unità in cui ogni suo elemento non nullo ammette inverso è detto campo.
Perciò, per questa definizione $Q := (Q, +, \cdot, \leq)$ è un campo che rappresenta i numeri razionali.
Per convezione le classi di Q del tipo [(m, n)] verranno scritte in questo modo: $\frac{m}{n}$

TEORIA DEI CAMPI

Per definizione un campo è un dominio di integrità, ovvero un anello in cui si verifica la proprietà $x \cdot y = 0 \Leftrightarrow x = 0$ oppure $y = 0$
Se in un campo $K = (K, +, \cdot, \leq)$ l'ordine è compatibile con le operazioni, allora il campo è totalmente ordinato.

Morfismo. Un morfismo è una funzione tra anelli.
Considero due anelli commutativi con unità A e R e una funzione φ

$\varphi : A \longrightarrow R$ è detto omomorfismo di anelli se si verificano
$\varphi(x +_A y) = \varphi(x) +_R \varphi(y)$ per ogni $x, y \in A$
$\varphi(x \cdot_A y) = \varphi(x) \cdot_R \varphi(y)$ per ogni $x, y \in A$
$\varphi(1_A) = 1_R$

Un omomorfismo di anelli $\varphi : A \longrightarrow R$ è detto:
monomorfismo se φ è iniettivo.
epimorfismo se φ è suriettivo.
Isomorfismo se φ è biettivo.

Si può dare una caratterizzazione di estremo inferiore e superiore tramite i campi:
Sia K un campo totalmente ordinato e dia Y un sottoinsieme di K non vuoto.
Sia $e' \in K$ allora $e' := \inf_K Y$ se e solo se:

i) $e' \leq y \ \ \forall y \in Y$
ii) $\forall \varepsilon > 0, \exists y \in Y : y < e' + \varepsilon$

Sia $e'' \in K$ allora $e'' := \sup_K Y$ se e solo se:

i) $y \leq e'' \ \forall \ y \in Y$
ii) $\forall \varepsilon > 0 \ \exists y \in Y : e'' - \varepsilon < y$

Dato un anello con integrità di dominio $A = (A, +, \cdot)$. Costruiremo un campo chiamato campo delle frazioni di A, che contiene A e che non ha sottocampi che contengono A.
Più precisamente in $A \times (A \setminus \{0\})$ considero la relazione di equivalenza tilde tale che:

$$\forall\ (a, b), (c, d) \in A \times (A \setminus \{0\}), (a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c$$

La classe di equivalenza definita come Q(A) associata alla relazione può essere trasformata in anello se l'insieme viene dotata di somma e prodotto in questo modo:

$$[(a, b)] +_{Q(A)} [(c, d)] := [(a \cdot d + c \cdot b, b \cdot d)]$$

e

$$[(a, b)] \cdot_{Q(A)} [(c, d)] := [(a \cdot c, b \cdot d)]$$

Per ogni $[(a, b)], [(c, d)] \in Q(A)$.
Se viene osservato che le operazioni soddisfano le proprietà degli anelli e che ogni elemento ha un inverso sul prodotto si può dire che Q(A) è un campo.
La mappa $j : A \to Q(A), x \in A \to [(x, 1)] \in Q(A)$ è iniettiva e dimostra che c'è una copia di A in Q(A). Se identifichiamo A come la sua immagine in Q(A), A è uno sottoanelli di Q(A). Dunque, la somma e la moltiplicazione degli elementi è uguale nei due insiemi.
In particolare, il campo Q dei razionali può esser visto come il campo delle frazioni dell'anello degli interi Z.

La caratteristica n di un anello $A = (A, +, \cdot)$ è l'elemento n appartenente a N* tale che

$$n \cdot 1 := 1 + 1 + ... + 1 \text{ (n volte)} = 0$$

Ogni campo ordinato ha caratteristica 0.

STRUTTURA METRICA DI CAMPI ORDINATI

Per ogni campo ordinato $K = (K, +, \cdot, \leq)$ definisco il concetto di distanza in A.
Sia $| \cdot | : K \to K$ tale che:

$$|x| := \max\{x, -x\} \text{ per ogni } x \in K.$$

L'immagine |x| è chiamata valore assoluto di x appartenente a K
Un sottoinsieme di K è chiamato intervallo se per alcuni $a, b \in K$ coincide con uno di questi insiemi:

$[a, b] := \{x : x \in X \wedge a \leq x \leq b\}$
$(a, b) := \{x : x \in X \wedge a < x < b\}$
$[a, b) := \{x : x \in X \wedge a \leq x < b\}$
$(a, b] := \{x : x \in X \wedge a < x \leq b\}.$

a e b sono gli estremi dell'intervallo, b - a è la lunghezza dell'intervallo.
Per ogni $a \in K$ possiamo definire gli intervalli illimitati

$(-\infty, a] := \{x : x \in X \wedge x \leq a\}$
$(-\infty, a) := \{x : x \in X \wedge x < a\}$
$[a,\infty) := \{x : x \in X \wedge x \geq a\}$
$(a,\infty) := \{x : x \in X \wedge x > a\}.$

Topologia di un campo. L'ordine induce la metrica o distanza in un campo ordinato K
$d : K \times K \to K$ dato da:

$$d(x, y) := |x - y| \text{ per ogni } x, y \in K.$$

La distanza segue delle proprietà dovute all'ordine:

(i) $d(x, y) \geq 0$;
(ii) $d(x, y) = 0$ se e solo se $x = y$;
(iii) $d(x, y) = d(y, x)$;
(iv) $d(x, y) \leq d(x, z) + d(z, y)$.

Ogni campo K totalmente ordinato può esser visto come uno spazio metrico (K, d), dove d è la metrica indotta dall'ordine totale.

Per ogni $x \in K$ e $\varepsilon > 0$ una **palla aperta** o **boccia** con centro x e raggio ε in K è l'insieme:

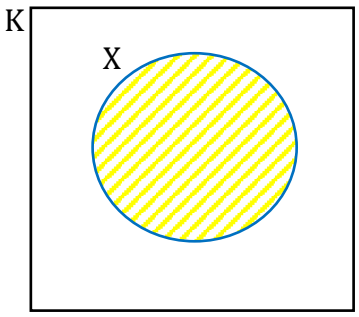
$$B\varepsilon(x) := \{y \in K : d(x, y) < \varepsilon\}$$

Sia X un sottoinsieme non vuoto di K, un elemento $x \in K$ è detto:

- **punto interno** si X se esiste $\varepsilon > 0$ tale che $B\varepsilon(x) \subseteq X$;
- **punto esterno** si X se esiste $\varepsilon > 0$ tale che $B\varepsilon(x) \subseteq K \setminus X$;
- **punto di frontiera** di X se per ogni $\varepsilon > 0$ ci sono $y, z \in B\varepsilon(x)$ tale che $y \in X$, $z \in K \setminus X$;
- **punto di accumulazione** (o **punto limite**) per X se per ogni $\varepsilon > 0$ esiste $y \in B\varepsilon(x) \setminus \{x\}$ tale che $y \in X$
- **punto isolato** di X se esiste $\varepsilon > 0$ tale che $X \cap B\varepsilon(x) = \{x\}$.

Per convezione

- $\dot{X}$ denota l'insieme dei punti interni di X
- ∂X denota l'insieme dei punti di frontiera di X
- $\bar{X} := X \cup \partial X$ denota la chiusura o aderenza di X
- DX indica l'insieme dei punti di accumulazione di X e denota l'insieme derivato di X
  Si sa che $\dot{X} \subseteq DX$



La linea blu indica ∂X, *il motivo giallo indica* $\dot{X}$. *L'unione dei due insiemi è* $\bar{X}$ *(che in questo caso esempio equivale a X).*

Per ogni $x \in K$, $\varepsilon > 0$ una palla chiusa di centro x e raggio ε è definita da:

$$\bar{B}\varepsilon(x) = \{y \in K : d(x, y) \leq \varepsilon\}$$

Un insieme $X \subseteq K$ è detto

aperto se e solo se $X = \dot{X}$;
chiuso se e solo se $X = \bar{X}$;

Proposizione a. Sia $K = (K, +, \cdot, \leq)$ un campo totalmente ordinato. Valgono i seguenti fatti:

(1) K e $\emptyset$ sono aperti;

(2) Se $(X_\alpha)_{\alpha \in J}$ è una famiglia di insiemi aperti, allora $\bigcup_{\alpha \in J} X_\alpha$ è un insieme aperto;

(3) Se $X_1, \ldots, X_k$ $(k \in N^*)$ sono insiemi aperti, allora $\bigcap_{k}^{i=1} X_i$ è un insieme aperto;

Proposizione b. Sia $K = (K, +, \cdot, \leq)$ un campo totalmente ordinato. Valgono i seguenti fatti:

(1) K e $\emptyset$ sono chiusi;

(2) Se $(X_\alpha)_{\alpha \in J}$ è una famiglia di insiemi chiusi, allora $\bigcap_{\alpha \in J} X_\alpha$ è un insieme chiuso;

(3) Se $X_1, \ldots, X_k$ $(k \in N^*)$ sono insiemi chiusi, allora $\bigcup_{k}^{i=1} X_i$ è un insieme chiuso;

CAMPI ARCHIMEDI

Sia $K = (K, +, \cdot, \leq)$ un campo totalmente ordinato. K è detto archimedeo se e solo se per definizione per ogni $x > 0$ e $y \in K$ esiste $n \in N$ tale che $n \cdot x > y$.

Proposizione. In un campo K totalmente ordinato valgono i seguenti fatti:

(i) K è archimedeo;

(ii) Per ogni $y \in K$ esiste $n \in N$ tale che $n > y$;

(iii) Q è denso in K, ossia per ogni $x, y \in K$ con $x < y$ esiste $c \in Q$ tale che $x < c < y$

Da ciò si assume che Q è un campo archimedeo: per ogni $x, y \in Q$ con $x < y$ allora $x < c < y$ dove $c := \frac{x+y}{2}$.

SUCCESSIONI IN K

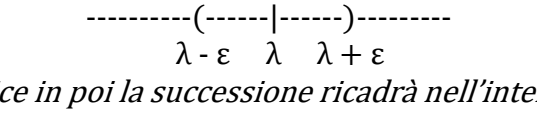
Prendiamo in K una funzione $x : N \longrightarrow K$ tale che $n \in N \longmapsto x(n) \in K$.
Il simbolo x(n) verrà scritto come x_n e prende il nome di successione.
Le successioni $(x_n)_n$ son contenute in K e la loro cardinalità equivale a quella di N:

$$|(x_n)_n| = |N| = \aleph_0$$

$(x_n)_n$ è convergente in $\lambda \in K$ se per ogni $\varepsilon > 0$ in K, esiste $\nu_\varepsilon \in N$ tale che

$$d(x_n, \lambda) < \varepsilon \text{ in K per ogni } n \geq \nu_\varepsilon \text{ in N;}$$

Chiamiamo λ limite di $(x_n)_n$ e scriveremo $\lambda = \lim_{n \to \infty} x_n$.



Graficamente, da un indice in poi la successione ricadrà nell'intervallo per avvicinarsi a λ.

Denotiamo con K^N l'insieme di tutte le successioni di K.
Es. $Q^N := \{(\frac{1}{n})_n, (\frac{n+1}{n})_n, \ldots\}$

Possiamo costruire $K^N = (K^N, +, \cdot)$ e ciò è un anello commutativo con unità con le operazioni definite per ogni $(x_n)_n,(y_n)_n \in K^N$

$$(x_n)_n + (y_n)_n := (x_n +_K y_n)_n$$

e

$$(x_n)_n \cdot (y_n)_n := (c_n)_n$$

Dove $c_n := \sum_{k=0}^{n} x_k \cdot_K y_{n-k} = (x_0 \cdot_K y_n) +_K (x_1 \cdot_K y_{n-1}) +_K \dots +_K (x_n \cdot_K y_0)$

In K^N

$(0)_n = 0_{K^N}$
$(x_n)_n + (-x_n)_n = 0$
$(1)_n = 1_{K^N}$

Non esiste un inverso poiché K^N non è un campo.

Introduco l'anello delle serie formali a coefficienti in K

$$K[[X]] := x_0 + x_1X + x_2X^2 + \dots + x_nX^n = \sum_{n=0}^{\infty} x_nX^n$$

$\sum_{n=0}^{\infty} x_nX^n$ prende il nome di serie formale
In $K[[X]] = (K[[X]], +, \cdot)$ le operazione sono definite in questo modo:

$$(\sum_{n=0}^{\infty} x_nX^n) + (\sum_{n=0}^{\infty} y_nX^n) = \sum_{n=0}^{\infty} (x_n + y_n) X^n$$

e

$$(\sum_{n=0}^{\infty} x_nX^n) \cdot (\sum_{n=0}^{\infty} y_nX^n) = (\sum_{n=0}^{\infty} c_nX^n)$$

Se si ha una serie formale, si ha anche una successione e viceversa. Infatti, si può definire un isomorfismo tra i due anelli:
$f : K[[X]] \longrightarrow K^N$
Dove $f(\sum_{n=0}^{\infty} x_nX^n) = (x_n)_n$

COMPLETEZZA DI UN CAMPO K

Siano X, Y due insiemi non vuoti, $X \leq Y$ se e solo se per definizione per ogni $x \in X$ e per ogni $y \in Y$ si verifica che $x \leq y$

Dedekind completezza (o D-completezza). Un campo totalmente ordinato K è detto Dedekind completo (o D-completo) se e solo se per definizione per ogni sottoinsieme X, Y non vuoto di K esiste $z \in K$ tale che $X \leq z \leq Y$

Visualizzazione grafica di un campo K D-completo.

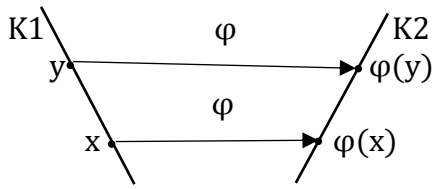
Sia X un sottoinsieme non vuoto di K indicheremo con:
U_x l'insieme dei maggioranti di X in K;
L_x l'insieme dei minoranti di X in K;

Proposizione. Sia K un campo totalmente ordinato. Valgono i seguenti fatti.

(1) K è D-completo
(2) Per ogni sottoinsieme X di K non vuoto, se U_x non è vuoto allora esiste $\sup_K X$, se L_x non è vuoto allora esiste $\inf_K X$

Siano $K_1 = (K_1, +_1, \cdot_1, \leq_1)$ e $K_2 = (K_2, +_2, \cdot_2, \leq_2)$ due campi totalmente ordinati.
Una funzione $\varphi : K1 \to K2$ è detta isomorfismo di campi crescenti quando:

$x \leq_1 y$ in $K_1 \Rightarrow \varphi(x) \leq_2 \varphi(y)$ in K_2



Visualizzazione grafica dell'isomorfismo.

Teorema fondamentale. *Esiste un unico campo K totalmente ordinato e D-completo a meno di isomorfismo crescenti.*

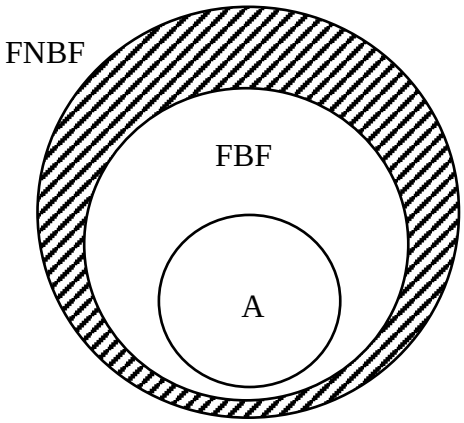
Ovvero tutti i campi totalmente ordinati e D-completi sono isomorfi tra loro (ogni campo è l'immagine dell'altro).
All'unico campo totalmente ordinato e D-completo si da il nome di campo dei numeri reali e lo si indica con R.
Per esplicitare il modello si fa l'insieme quoziente con le successioni.

Si dimostra che Q non è D-completo:

Sia $X := \{ q \in Q : q \geq 0 \text{ e } q^2 < 2\}$.
X è un sottoinsieme di Q e U_X non è vuoto. Però in questa situazione, $\sup_Q X$ non esiste.

LOGICA

Non è corretto dire che esiste un'unica logica, ma tante diverse.
Una logica è semplicemente una teoria formale e viceversa.
Consideriamo un insieme di simboli A che indica un alfabeto. (A numerabile).
Da questo alfabeto le lettere come p, q o r sono suoi elementi. Attraverso queste sequenze di elementi posso costruire un linguaggio.
Queste sequenze si chiamano **formule ben formate** o **FBF**.
Un linguaggio, dunque, è semplicemente un alfabeto e le FBF che si creano con esso.



L'intero insieme rappresenta tutte le possibili sequenze dell'alfabeto comprendendo formule ben formate e non. Un linguaggio però comprende l'insieme dell'alfabeto e delle formule ben formate.

Possiamo dire che una logica è un **linguaggio** con un **sistema deduttivo**. Un sistema deduttivo è composto da **assiomi** (particolari FBF) e regole di **inferenza** (sistemi dimostrativi).
Una logica inoltre ha due livelli di lettura: il primo riguarda la sintassi (si controlla se la sequenza scritta è una FBF) e il secondo riguarda la semantica (cha valore/significato diamo alla sintassi).

LOGICA PROPOSIZIONALE

La logica proposizionale non è altro che la codifica della logica basata sulle proposizioni. Le proposizioni sono semplicemente oggetti di un insieme. In essa ritroviamo diversi simboli.

Simboli delle proposizioni: A, B, C, …
Simboli connettivi: $\neg$, $\wedge$, $\vee$, $\longrightarrow$
Parentesi: ( )

Per comodità, $\perp$ indicherà il falso.

Ora si stabiliscono le regole per la sintassi:

- A, B, C, $\perp$, … sono FBF (proposizioni atomiche).
- Allora ($\neg$ A), (A $\wedge$ Q), (P $\vee$ Q), (P $\longrightarrow$ Q) sono FBF (proposizioni composte).

Per adesso i simboli non hanno alcun valore semantico e si manipolano solo in maniera formale rispettando la sintassi definita.
Poiché ci potrebbero essere un eccessivo uso di parentesi in alcune forme si stabilisce una priorità tra simboli:

(minor priorità) $\longrightarrow$ $\vee$ $\wedge$ $\neg$ (massima priorità)

Esempio. Dunque, la formula

$$\neg A \vee B$$

Viene intesa come

$$((\neg A) \vee B)$$

Si può introdurre la semantica, attribuendo un significato (VERO o FALSO) a ogni FBF. I valori di verità VERO verranno indicati con 1, quelli di falsità FALSO con 0.
Ciò non è altro che la definizione di una funzione

$$v : FBF \longrightarrow \{0, 1\}$$

che associa a una FBF P il suo valore di verità v(P).
Dunque, possiamo dire che v(A), dove A è una proposizione atomica qualsiasi, vale 1 se A è vera e 0 se A è falsa. Inoltre, v(⊥) è sempre 0 poiché ⊥ indica la falsità.
Assegnando il valore alle proposizioni lo si assegna alle FBF.
Per verificare come si comportano i connettivi invece, assegniamo ad essi delle *tavole di verità* :

¬ = NOT	
P	¬ P
0	1
1	0

∧ = AND		
P	Q	P ∧ Q
0	0	0
0	1	0
1	0	0
1	1	1

∨ = OR		
P	Q	P ∨ Q
0	0	0
0	1	1
1	0	1
1	1	1

⟶ = implicazione		
P	Q	P⟶Q
0	0	1
0	1	1
1	0	0
1	1	1

Da queste tavole possiamo poi risalire a qualsiasi altra di ogni FBF.
In una tavola di verità ogni riga è un *interpretazione* che è assimilabile a una funzione v : FBF ⟶ {0, 1}. L'interpretazione v può avere valore 0 o 1 in base alla configurazione delle proposizioni atomiche. Se P è una FBF e v(P) equivale a 1, allora si dirà che P *è soddisfatta da* v, o v è *un modello* per P e si scriverà v ⊨ P (P è vera nell'interpretazione v).

Se una forma ben formata P ha almeno un modello (ovvero esiste un'interpretazione che soddisfa P) allora si dirà che P è *soddisfacibile*. In caso contrario si dirà che P è *insoddisfacibile*.
Esempio.

$$(A \wedge \neg B) \vee (B \longrightarrow A)$$

Questa forma è soddisfacibile

$$A \wedge \neg A$$

Invece questa forma no. Non esiste nessuna interpretazione che la rende vera.

Se P è una FBF che è sempre soddisfacibile in qualsiasi interpretazione v, allora si dirà che P è una *tautologia* e si scriverà $\vDash P$.

Proposizione. Una formula ben formata P è una tautologia se $\neg P$ *è insoddisfacibile.*

Sia Γ un insieme di formule ben formate. Γ è soddisfacibile se esiste un'interpretazione v tale che $v(P) = 1$ per ogni $P \in \Gamma$ (Ovvero esiste almeno un modello o un interpretazione in comune che soddisfa tutte le proposizione) e si scriverà $\vDash \Gamma$.
Γ è insoddisfacibile se, per ogni interpretazione v, esiste almeno una proposizione $P \in \Gamma$ tale che $v(P) = 0$.
Una proposizione Q è conseguenza (semantica) di Γ, e scriveremo $\Gamma \vDash Q$, se per ogni interpretazione v tale che $v(P) = 1$ per ogni $P \in \Gamma$, si ha anche $v(Q) = 1$. Ovvero i modelli di Γ lo sono anche per Q.

Teorema (Deduzione semantica). Per ogni intero $n \geq 1$, si ha

$$P_1, P_2, \ldots, P_n \models Q \text{ se e solo se } P_1, P_2, \ldots, P_{n-1} \models P_n \to Q.$$

Teorema di Compattezza. Un insieme Γ di formule ben formate è soddisfacibile se e solo se lo è ogni suo sottoinsieme finito.

Un'altra formulazione è questa:

Un insieme Γ di formule ben formate `e insoddisfacibile se e solo se esiste un sottoinsieme finito di $\Gamma$ che `e insoddisfacibile.

Due forme ben formate si dicono *semanticamente equivalenti* quando coincidono nelle interpretazioni, ovvero hanno la stessa tavola di verità.
Nasce quindi la definizione: Due formule ben formate P e Q si dicono (semanticamente) equivalenti se, per ogni interpretazione v, si ha $v(P) = v(Q)$. In tal caso scriveremo $P \equiv Q$.
Teorema. Si hanno le seguenti equivalenze:

idempotenza

$$P \vee P \equiv P \qquad P \wedge P \equiv P$$

commutatività

$$P \vee Q \equiv Q \vee P \qquad P \wedge Q \equiv Q \wedge P$$

associatività

$$(P \vee Q) \vee R \equiv P \vee (Q \vee R) \qquad (P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$$

assorbimento

$$P \vee (P \wedge Q) \equiv P \qquad P \wedge (P \vee Q) \equiv P$$

distributività

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R) \qquad P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

leggi di De Morgan

$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q \qquad \neg(P \wedge Q) \equiv \neg P \vee \neg Q$$

doppia negazione

$$\neg\neg P \equiv P$$

Poiché i connettivi, se assimilati a operazioni di un insieme, soddisfano le proprietà delle algebre di Boole, si può costruire l'algebra di Boole della logica proposizionale.

Completezza Funzionale

Sia P una FBF contenente n proposizioni atomiche distinte $A_1, A_2, \ldots, A_n$.
La funzione $f_P : \{0, 1\}^n \to \{0, 1\}$ tale che, per ogni $(a_1, a_2, \ldots, a_n) \in \{0, 1\}^n$,
si ha $f_P(a1, a2, \ldots, an) = v(P)$, dove v è una interpretazione tale che $v(A_i) = a_i$,
per ogni $i = 1, \ldots, n$, è detta la funzione di verità di P.
La funzione di verità di una proposizione P è equivalente alla tavola di verità di P.
Adesso si vedrà quante tavole di verità una proposizione P di n proposizioni atomiche: se abbiamo n proposizioni atomiche, in virtù del fatto che abbiamo due valori da assegnare ad ognuna di esse, avremo 2^n configurazioni possibili. Perciò, avremo 2^{2n} diverse configurazioni della tavola di verità per una proposizione P n-aria.

Dato un insieme di connettivi logici C e un connettivo $c \notin C$, c si dice (semanticamente) derivabile da C se esiste una formula proposizionale P costruita con i soli connettivi di C tale che $f_P = f_c$. In altre parole, un connettivo c è derivabile dall'insieme di connettivi C se è possibile esprimerlo mediante connettivi di C.
È possibile fare degli esempi a dimostrazione di ciò.
Prendiamo per esempio $P \vee Q$. Sappiamo che grazie alle leggi di De Morgan essa è semanticamente equivalente a $\neg(\neg P \wedge \neg Q)$.
Dunque, il connettivo $\vee$ è derivabile dall'insieme di connettivi $\{\neg, \wedge\}$.

Diremo che un insieme C di connettivi logici si dice funzionalmente completo se, per ogni $n \geq 1$ e per ogni funzione $f : \{0, 1\}^n \to \{0, 1\}$, esiste una formula ben formata P, costruita utilizzando solo i connettivi di C, tale che $f = f_P$. Più semplicemente si dirà che un insieme C di connettivi logici è funzionalmente completo se ogni altro connettivo è derivabile da C.

Forme normali.
Un *letterale* è una proposizione atomica o la sua negazione.
Diremo inoltre che una congiunzione di formule ben formate $P_1, P_2, \ldots, Pn$ è una formula del tipo $P_1 \wedge P_2 \wedge \cdots \wedge P_n$.
La disgiunzione delle formule $P_1, P_2, \ldots, P_n$ è invece la formula $P_1 \vee P_2 \vee \cdots \vee P_n$.

Una formula ben formata P è detta in *forma normale congiuntiva* (fnc) se P è della forma $P_1 \wedge P_2 \wedge \cdots \wedge P_n$ (per qualche $n \geq 1$), dove ciascuna P_i è una disgiunzione di letterali.
Invece è detta in forma normale disgiuntiva (fnd) se P è della forma $P_1 \vee P_2 \vee \ldots \vee P_n$ (per qualche $n \geq 1$), dove ciascuna P_i è una congiunzione di letterali.

$A \wedge \neg B \wedge (A \vee C)$
$(\neg A \vee B \vee C) \wedge (\neg C \vee A)$
Esempio di fnc.

$A \vee (\neg B \wedge C \wedge \neg A)$
$(A \wedge B) \vee (C \wedge \neg A) \vee C$
Esempio di fnd.

Se una proposizione è del tipo $A_1 \wedge A_2 \wedge \cdots \wedge A$ o $A_1 \vee A_2 \vee \cdots \vee A_n$, dove $A_1, A_2, \ldots, A_n$ sono letterali essa, può esser vista sia in forma normale congiuntiva che disgiuntiva!
Tali tipi di forme normali sono importanti in vista del prossimo risultato

Teorema. Per ogni formula ben formata P esistono una formula in forma normale congiuntiva P^C e una formula in forma normale disgiuntiva P^D tali che $P \equiv P^C$ e $P \equiv P^D$.

Esempio. *Sia $P = (A \vee \neg B) \rightarrow C$. Per trovare PC si procederà così:*

$$\begin{aligned}(A \vee \neg B) \rightarrow C &\equiv \neg(A \vee \neg B) \vee C \\ &\equiv (\neg A \wedge \neg\neg B) \vee C \\ &\equiv (\neg A \wedge B) \vee C \\ &\equiv (\neg A \vee C) \wedge (B \vee C) = PC\end{aligned}$$

Per trovare PD invece:

$$\begin{aligned}(A \vee \neg B) \rightarrow C &\equiv \neg(A \vee \neg B) \vee C \\ &\equiv (\neg A \wedge \neg\neg B) \vee C \\ &\equiv (\neg A \wedge B) \vee C = PD\end{aligned}$$

Data una proposizione P formata da letterali A1, A2, …, An è possibile trovare PD e PC riferendosi alle tavole di verità.
Per P^D è sufficiente la somma di min termini già trattata in Reti Logiche.
Per P^C il funzionamento è simile. Vediamo con un esempio semplice:

A	B	P	
0	0	0	A ⋁ B
0	1	1	
1	0	0	¬A ⋁ B
1	1	1	

P^C sarà (A ⋁ B) ⋀ (¬A ⋁ B).
Prendiamo ogni riga in cui P è 0 e facciamo la disgiunzione dei letterali della riga. Se essi valgono 1 essi vengono negati. Avremo n disgiunzioni che devono corrispondere alle volte in cui 0 compare nella tavola di verità. Se ciò risulta facciamo la congiunzione di tutte le disgiunzioni.