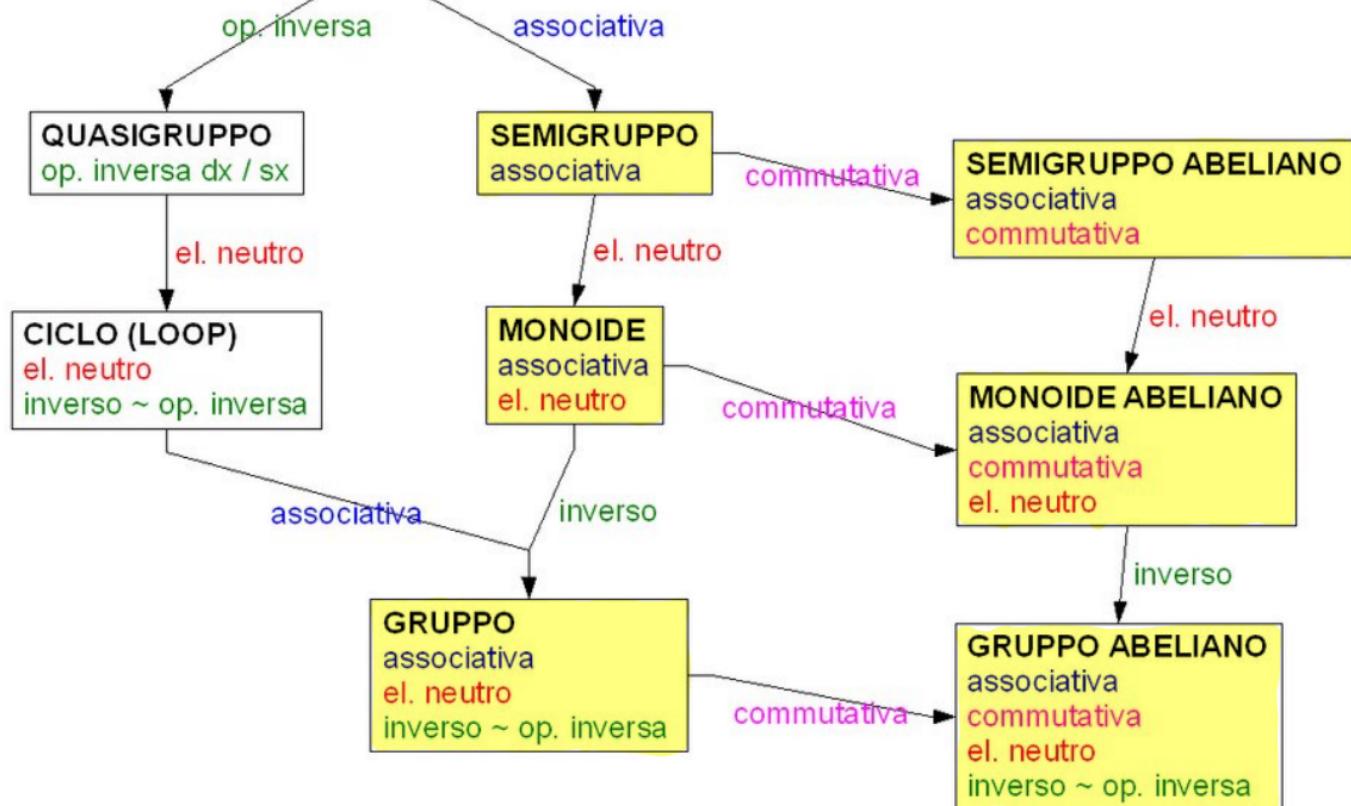




**MAGMA / GRUPPOIDE =  $(A, *)$**



**ANELLOIDE =  $(A, +, *)$**

$*$

\* distributiva su  $+$

$+$  : associativa, commutativa, el. neutro  $e_+ := 0$

$*$  : associativa

0 annichila \*

**SEMIANELLO**

$(A, +)$  monoide abeliano

$(A, *)$  semigruppo

0 annichila \*

\* distributiva su  $+$

$+$  : inverso

**ANELLO [PSEUDOANELLO]**

$(A, +)$  gruppo abeliano

$(A, *)$  semigruppo

(0 annichila \*)

\* distributiva su  $+$

$*$  : el. neutro  $e_* := 1$

$*$  : el. neutro  $e_* := 1$

**SEMIANELLO UNITARIO**

$(A, +)$  monoide abeliano

$(A, *)$  monoide

0 annichila \*

\* distributiva su  $+$

$+$  : inverso

**ANELLO UNITARIO [ ANELLO ]**

$(A, +)$  gruppo abeliano

$(A, *)$  monoide

(0 annichila \*)

\* distributiva su  $+$

$*$  : commutativa

$*$  : inverso (tranne 0)

**ANELLO UNITARIO COMMUTATIVO**

$(A, +)$  gruppo abeliano

$(A, *)$  monoide abeliano

(0 annichila \*)

\* distributiva su  $+$

**CORPO**

$(A, +)$  gruppo abeliano

$(A - \{0\}, *)$  gruppo

(0 annichila \*)

\* distributiva su  $+$

$*$  : inverso (tranne 0)

$*$  : commutativa

**CAMPO**

$(A, +)$  gruppo abeliano

$(A - \{0\}, *)$  gruppo abeliano

(0 annichila \*)

\* distributiva su  $+$

## ■ Struttura Algebrica

- Sia  $S$  un insieme, e  $*$  un'operazione binaria. Allora  $(S, *)$  è una Struttura Algebrica.

Una struttura può avere anche più operazioni binarie.

Si chiama insieme di sostegno

- Chiamiamo operazione una qualsiasi funzione  $*: S \times S \rightarrow S$

Quindi le operazioni hanno la proprietà di chiusura, cioè l'operazione tra due elementi di un insieme darà un elemento dell'insieme

- Teorema di Associazività

Se  $*$  è associativa, è possibile omettere le parentesi

$$a * b * c = (a * b) * c = a * (b * c)$$

- Teorema di commutatività

Se  $*$  è commutativa, è possibile scambiare di posto gli operandi

$$a * b = b * a$$

## ■ Semigruppo

$(S, *)$  è un semigruppo  $\Leftrightarrow *$  è associativa

## ■ Elemento neutro

Sia  $*: S \times S \rightarrow S$

$\forall t \in S$

- $t$  è neutro a sx  $\Leftrightarrow \forall a \in S (t * a = a)$
- $t$  è neutro a dx  $\Leftrightarrow \forall a \in S (a * t = a)$
- $t$  è neutro  $\Leftrightarrow t$  neutro a sx  $\wedge$  a dx  $\Leftrightarrow \forall a \in S (a * t = a = t * a)$

- Teorema dell'elemento neutro

- Sia  $*$  un op. binaria su  $S$ , ed esistono:  $x$  elemento neutro a sx, ed  $y$  elemento neutro a dx, allora

- $(x = y)$  ed  $x$  è
  - l'unico neutro a sx
  - l'unico neutro a dx
  - l'unico neutro

- Quindi sappiamo che è possibile avere più elementi neutri a sx  $\Leftrightarrow$  Non ce ne sono a dx

Dualmente per la dx

- Dimostrazione

$$x * y = x \text{ (perché } y \text{ neutro a dx)}$$

$$x * y = y \text{ (perché } x \text{ neutro a sx)}$$

Quindi  $x = y$

## Monoide

- Sia  $(S, *)$  un semigruppo, e sia  $t$  un neutro, allora  $(S, *, t)$  è un monoide
- $t$  è un **operazione nulla**, cioè un'operazione senza alcun operando, non c'è altro che un elemento di  $S$ . La selezione di un elemento neutro è un'operazione nulla.

## Operazione opposta

- Sia  $*^o: (a, b) \in S \mapsto b * a \in S$ , allora  $*^o$  è detta **operazione opposta**. L'operazione opposta ha le stesse proprietà dell'op. iniziale.
- In termini di tavola di Cayley significa ribaltare la tavola rispetto a righe e colonne. Neutri a sx diventano neutri a dx, e viceversa.
- Risulta comoda per teoremi: e proprietà che valgono solo per elementi neutri a sx o dx.

## Elemento simmetrico

- Sia  $(S, *, t)$  un monoide,
- $\forall x, y \in S$ :
  - $x$  è simmetrico a dx d:  $y \Leftrightarrow y * x = t$
  - $x$  è simmetrico a sx d:  $y \Leftrightarrow x * y = t$
  - $x$  è simmetrico d:  $y \Leftrightarrow y * x = t = x * y$
- Il neutro è sempre simmetrico di sé stesso ( $t * t = t$ )

NB: In mancanza di elemento neutro non può esistere alcun simmetrico.

NB: Un elemento **simmetrizzabile** è un elemento che ha un simmetrico (dx/sx)

Possono esistere più elementi simmetrizzabili.

## Teorema dell'elemento simmetrico

- Sia  $(S, *, t)$  un monoide
- $\forall x \in S$ , se esistono  $s$  simmetrico sx di  $x$ , e  $d$  simmetrico destro di  $x$ , allora  $(s=d)$  ed  $s$  è l'unico simmetrico  $(dx, sx)$  di  $x$
- **Dimostrazione**

$$x * d = t \quad (d \text{ è simmetrico } dx)$$

$$s * x = t \quad (s \text{ è simmetrico } sx)$$

$$\text{Quindi } s = (s * t) = s * (x * d) = (s * x) * d = t * d = d$$

## ■ Gruppo

- Un gruppo è un monoide dove ogni elemento è simmetrizzabile

$$G = \bigcup \{G\}$$

## ■ Parte chiusa

- Sia  $(S, *)$  una struttura algebrica

$T \subseteq S$  è una parte chiusa, o stabile, di  $S \Leftrightarrow \forall a, b \in T (a * b \in T)$

- Possiamo definire la seguente applicazione:  $(a, b) : T \times T \mapsto a * b \in T$

Tale funzione si dice **operazione indotta** sulla parte stabile

- Vengono conservate le proprietà, ma è possibile perdere neutrî ( $s_x / d_x$ ) o simmetrizzabili ( $d_x / s_x$ )

## ■ Gruppo degli invertibili:

Sia  $(S, *, t)$  un monoide,  $\mathcal{U}(S) = \{x \mid x \text{ è simmetrizzabile in } (S, *, t)\}$  è una parte chiusa

$\mathcal{U}(S) \neq \emptyset$ , perché  $t \in \mathcal{U}(S)$  che è anche il neutro degli invertibili

Allora il gruppo degli invertibili è un sottomonoide (conserva il neutro) ed anche un **gruppo** (tutti gli el. simmetrizzabili)

Quindi in un monoide gli elementi simmetrizzabili costituiscono un **sotto-gruppo** (parte chiusa)

- Il prodotto tra elementi simmetrizzabili è ancora simmetrizzabile

### Dimostrazione

$$\forall a, b \in \mathcal{U}(S)$$

$\exists a', b' \in (S \setminus \mathcal{U}(S))$  con  $a'$  simm. di  $a$ ,  $b'$  simm. di  $b$  in  $(S, *, t)$

$$(a * b) * (b' * a') = a * (b * b') * a' = a * t * a' = a * a' = t$$

Quindi  $(b' * a')$  è un elemento simmetrico  $d_x$  di  $(a * b)$

Vediamo che anche simmetrico  $s_x$

$$(b' * a') * (a * b) = b' * (a * a) * b = b' * t * b = b' * b = t$$

Quindi  $(b' * a')$  è simmetrico di  $(a * b)$

ex)

$$(\mathcal{P}(S), \cap, S) \quad \mathcal{U}(\mathcal{P}(S)) = \{S\} \quad \text{Si dice gruppo identico perché ha un solo elemento}$$

$$(\mathcal{P}(S), \cup, \emptyset) \quad \mathcal{U}(\mathcal{P}(S)) = \{\emptyset\}$$

$$(\mathbb{Z}, \cdot) \quad \mathcal{U}(\mathbb{Z}) = \{1, -1\}$$

$$(Q, \cdot) \quad \mathcal{U}(Q) = \{Q \setminus \{0\}\} = Q^*$$

## Sottogruppo

•  $(S, *, t, ')$  è un gruppo se ogni elemento è simmetrico.

L'operazione  $'$  è la scelta del simmetrico.

Si dice sottogruppo di  $(S, *, t, ')$  una struttura  $(T, \bar{*}, \bar{t}, \bar{'})$  in cui  $T$  è parte chiusa di  $S$

e  $\bar{*}$  l'operazione indotta da  $*$  su  $T$ . Poi  $t \in T$  e  $\forall a \in T (a' \in T = a^{\bar{'}})$

ex)  $(\mathbb{Z}, +, 0, -)$  è un gruppo abeliano.

Un suo sottogruppo dei multipli di  $n$  in  $\mathbb{Z}$ ,  $\forall n \in \mathbb{Z} \setminus \{0\} \{ nk \mid k \in \mathbb{Z}\}$

Se sommo due multipli di  $n$ , poi  $0 \in n\mathbb{Z}$ , e  $-nk = n(-k)$

Quindi è chiuso rispetto a  $(+, t, ')$  per cui è sottogruppo.

## Teorema

• Sia  $(S, *, t, ')$  un gruppo, e sia  $\emptyset \neq T \subseteq S$

Allora  $T$  è un sottogruppo di  $S \Leftrightarrow \forall a, b \in T (a * b \in T)$

Dimostrazione  $\Rightarrow$

$T$  è sottogruppo di  $S$ , quindi  $\forall a, b \in T (a * b \in T)$  per def.  $\forall a \in T (a' \in T) \Rightarrow (a' * b \in T)$

Dimostrazione  $\Leftarrow$

$T \neq \emptyset$ , per ipotesi

Quindi  $\exists a \in T$ , allora  $(a * a' \in T)$  cioè  $t \in T$

•  $\forall x \in T (x * t \in T)$  ma  $x * t = x$ , quindi  $T$  è chiuso rispetto la scelta del simmetrico

•  $\forall x, y \in T, x' \in T$  per cui  $(x') * y \in T$ , ma  $(x') * y = x * y$ . Quindi  $T$  è chiuso rispetto a \*

Allora  $T$  è un sottogruppo

## Anello

### • Definizione

Un anello  $(R, +, \cdot)$  è una struttura algebrica tale che:

- 1  $(R, +)$  è un gruppo abeliano
  - Esiste un neutro  $0_R$
  - Tutti gli elementi hanno opposto
  - $+$  è associativa e commutativa

- 2  $(R, \cdot)$  è un semigruppo

- 3
  - è doppiamente distributivo rispetto a  $+$
  - distributivo a sx :  $\forall a, b, c \in R (a \cdot (b+c) = (a \cdot b) + (a \cdot c))$
  - distributivo a dx :  $\forall a, b, c \in R ( (a+b) \cdot c = (a \cdot c) + (b \cdot c))$

• Un anello è **commutativo**  $\Leftrightarrow (R, \cdot)$  è una struttura abeliana

• Un anello è **unitario**  $\Leftrightarrow$  In  $(R, \cdot)$  esiste un neutro  $1_R$   $\Leftrightarrow (R, \cdot)$  è un monoido

ex)

Sono anelli :  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$

Non è un anello  $(N, +, \cdot)$  perché  $(N, +)$  non è un gruppo (non esistono opposti in  $(N, +)$ )

NB:  $(\mathcal{P}(S), \Delta, \cap)$  si chiama **anello delle parti**,  $(\mathcal{P}(S), \Delta)$  è un gruppo abeliano, e  $(\mathcal{P}(S), \cap)$  è un Semigruppo  
Inoltre  $\cap$  è distributivo risp.  $\Delta$

## Nozioni e Terminologia

- In un anello si indica con  $0_R$  il neutro risp.  $+$ . E con  $1_R$  quello rispetto al  $\cdot$ .

Rispettivamente zero ed uno dell'anello.

- Inoltre  $\forall x \in R$  :  $-x$  è l'opposto, mentre  $\frac{1}{x}$  è l'inverso (sono i simmetrici di  $x$  risp.  $+$  e  $\cdot$ )

- Un sottoanello è una parte chiusa rispetto  $+$  e  $\cdot$ .

Un sottoanello si dice **unitario** se conserva l'unità.

Nb: Un sottoanello può essere unitario, ma non è detto che sia un sottoanello unitario

ex)  $(S, +, \cdot)$ ,  $T \subseteq S$ ,  $\mathcal{P}(T)$  è un sottoanello di  $\mathcal{P}(S)$ , esso è anche unitario ( $I_T = T$ ) ma non è un sottoanello unitario  
 $(I_{\mathcal{P}(T)} \neq I_{\mathcal{P}(S)})$

Fun fact: Anello in inglese = Ring, per indicare un anello non unitario si usa Ring

## ■ Proprietà degli anelli

### I) Proprietà di assorbimento

Sia  $R$  un anello,  $\forall a \in R$   $a \cdot 0_R = 0_R = 0_R \cdot a$

#### Dimostrazione

$0_R \cdot a$ , ma  $0$  è elemento neutro rispetto alla somma, quindi posso scriverlo

$(0_R + 0_R) \cdot a$  che per distributività è:  $0_R a + 0_R a$

quindi  $0_R + 0_R a = 0_R a + 0_R a$  ma  $(R, +)$  è un gruppo  $\Rightarrow$  tutti gli elementi sono cancellabili

quindi:  $0_R = 0_R a$

Quindi, dato un generico anello  $R$ ,  $\forall x \in R$  ( $x + x = x + 0_R$ )

### 2) $-(a b) = -a(b) = a(-b)$

#### Dimostrazione

$(-a)b + ab$  per distributività "inversa" è  $b \cdot (a - a)$  cioè  $b \cdot 0_R$

quindi  $(-a)b$  è l'opposto di  $ab$

- Ma il simmetrico è unico, quindi vale la proprietà generale  $\forall x, y \in R$ :

a)  $x \cdot 0 = 0 \cdot x = 0$

b)  $-(x y) = -x(y) = x(-y)$

c)  $x - y = x + (-y)$  Sottrarre è come sommare con l'opposto di un numero

d)  $x(y - z) = xy - xz \wedge (y - z)x = yx - zx$

Dim:  $x(y - z) = x(y + (-z)) = xy + x(-z) = xy + (-xz) = xy - xz$

## ■ Divisore dello zero

- Sia  $(R, +, \cdot)$  un anello, un elemento  $a \in R$  si dice:

divisore sx dello zero  $\Leftrightarrow \exists b \in R \setminus \{0\}$  ( $a \cdot b = 0_R$ )

divisore dx dello zero  $\Leftrightarrow \exists b \in R \setminus \{0\}$  ( $b \cdot a = 0_R$ )

divisore dello zero  $\Leftrightarrow$  è un divisore sx or dx dello zero

- Lo  $0_R$  è sempre un divisore dello zero, ammenoché  $R = \{0_R\}$  cioè  $|R| = 1$

- Legge di annullamento del prodotto

$$\forall a, b \in R \quad (a \cdot b = 0 \Rightarrow a = 0 \vee b = 0)$$

Questa legge non vale in tutti gli anelli, perché se ci sono divisori dello zero

allora può capitare che  $(a \cdot b = 0 \wedge a \neq 0 \wedge b \neq 0)$

$$-ab + ab$$

(NB + commutatività)  
↳ Simmetrico a sx  
↳ Commutatività di +  
↳ Simmetrico e basta)

NB: Quando parliamo di simmetrizzabili/cancellabili ci riferiamo all'operazione moltiplicativa, perché in quella additiva valgono sempre (in quanto gruppo abeliano)

## • Teorema

Sia  $R$  un anello,  $\forall a \in R$

- Se  $a$  è divisore di  $x$  dello zero  $\Leftrightarrow a$  non è cancellabile a  $sx$
- Se  $a$  è divisore di  $x$  dello zero  $\Leftrightarrow a$  non è cancellabile a  $dx$
- Se  $a$  è divisore dello zero  $\Leftrightarrow a$  non è cancellabile

Dimostrazione  $\Rightarrow$

Sia  $a$  un divisore di  $x$  dello zero, allora  $\exists b \in R \setminus \{0\} (ab = 0)$

Allora posso scrivere  $ab = 0_R$ , perché in ogni anello  $\forall x \in R (x \cdot 0_R = 0_R)$

Ma  $b \neq 0_R$ , quindi  $a$  non è cancellabile a  $sx$

Dimostrazione  $\Leftarrow$

Supponiamo  $a$  non cancellabile a  $sx$ , quindi  $\exists x, y \in R (ax = ay \wedge x \neq y)$

ma possiamo scrivere  $ax = ay$  come  $ax - ay = 0_R$

quindi  $a(x - y) = 0_R$ , ma  $x - y \neq 0_R$

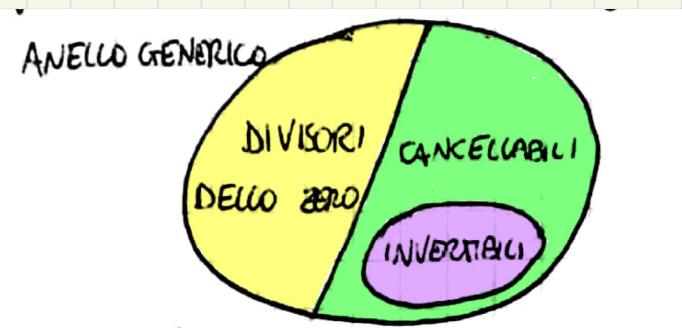
Allora  $a$  è un divisore dello zero

## Gesù aiuto

- Un elemento di un anello è esclusivamente un divisore dello zero o cancellabile

Inoltre in un anello unitario, l'unità è invertibile  $\Rightarrow$  cancellabile

ex) In  $(\mathbb{Z}, +, \cdot)$ : zero è l'unico divisore dello zero,  
tutti sono cancellabili, ma solo  $\{-1, 1\} \subset U(\mathbb{Z})$



## Campo

Sia  $(R, +, \cdot)$  un anello.

$|R| > 1 \Leftrightarrow 0_R$  è un divisore dello zero (quindi non invertibile)

Si chiama **corpo** un anello unitario in cui ogni elemento diverso da zero è invertibile

Si chiama **campo** un corpo commutativo

ex) Alcuni campi

- $(\mathbb{Q}, +, \cdot)$   $(\mathbb{R}, +, \cdot)$
- $(\mathbb{F}(S), \Delta, \cap)$  non è un campo perché ha divisori dello zero diversi da zero
- $(\mathbb{F}(S), \cap, \Delta)$  è un campo solo se  $|S| = 1$  in quanto  $\mathbb{F}(S) = \{\emptyset, \{a\}\}$



R: Anello commutativo unitario in cui ogni elemento ( $\neq 0_R$ ) è invertibile

**Integro:** Ogni elemento diverso da zero è cancellabile, commutativo, non per forza unitario

**Campo:** Ogni elemento diverso da zero è invertibile, commutativo, unitario

## ■ Domini di Integrità

- Sia  $(R, +, \cdot)$  un anello

$R$  è integro  $\Leftrightarrow$  ogni elemento di  $R \setminus \{0_R\}$  è cancellabile

cioè se  $R$  non ha divisori dello zero diversi da  $0_R$

- $R$  è un dominio di integrità  $\Leftrightarrow R$  è un anello integro commutativo

- $R$  è un dominio di integrità  $\Leftrightarrow$  Vale la legge di annullamento del prodotto

- Un anello integro finito è sempre un corpo. I corpi finiti sono sempre commutativi, quindi campi

- Teorema

$R$  è integro  $\Leftrightarrow \forall a, b \in R (ab=0 \Rightarrow a=0 \vee b=0)$

### Dimostrazione

Se  $R$  non è integro, allora ha divisori dello zero diversi da zero

Supponiamo che  $a$  sia un divisore sx dello zero, allora  $\exists b \in R (ab=0 \neq b)$

Ma vale che  $a=0 \vee b=0$ , quindi abbiamo una contraddizione, ed  $R$  non può avere divisori dello zero diversi da zero per cui è integro.

Gli anelli integri sono quelli per cui vale la LAP

## ■ Anello booleano

- Sia  $R$  un anello

$R$  è booleano  $\Leftrightarrow R$  è unitario ed ogni elemento è idempotente

ex)  $(P(S), \Delta, \cap)$  perché  $\forall x \in P(S) (x^2 = x \cap x = x)$ , ed esiste l'unità  $I_{P(S)} = S$

- Se  $R$  è un anello booleano, allora è commutativo e  $\forall a \in R (0_R a = 0_R)$  ed ogni elemento coincide al suo opposto

### Dimostrazione

$\forall a, b \in R (a+b)^2 = a^2 + ab + ba + b^2$ , ma vale l'idempotenza, quindi  $a+b = a+ab+ba+b$

Perché valga l'identità  $ab$  e  $ba$  devono essere opposti, ovvero  $0_R = ab + ba \Rightarrow ba = -ab$

Se  $b=I$  oppure  $b=a$ , allora  $a=-a$ , ovvero  $2a=0_R$

Quindi  $-ba = ab = -ab$

Allora l'anello è commutativo

- L'idempotenza della moltiplicazione è la causa della commutatività in un anello unitario

ex)  $(P(S), \Delta, \cap)$

$$(a \Delta b)^2 = (a \cap a) \Delta ab \Delta ba \Delta (b \cap b) = a \Delta (a \cap b) \Delta (b \cap a) \Delta b = a \Delta b$$

$(Z_2, +, \cdot)$  sono Anelli booleani

- Sia  $R$  un anello unitario, si chiama caratteristica il periodo dell'unità. Cioè la caratteristica è l'inf

tale che  $(h \cdot I = 0_R)$

ex)  $h=I \Leftrightarrow I = 0_R$

$h=2 \Leftrightarrow I + I = 0 \quad (P(S), \Delta), (Z_2, +)$

## Reticolo

- Sia  $(S, \leq)$  un reticolo, se considero le applicazioni:

$$\wedge: (a, b) \in S \times S \mapsto \inf_{(S, \leq)} (\{a, b\}) \in S \quad \text{intersezione reticolare, cap, inf}$$

$$\vee: (a, b) \in S \times S \mapsto \sup_{(S, \leq)} (\{a, b\}) \in S \quad \text{unione reticolare, cup, sup}$$

Possiamo definire una struttura algebrica  $(S, \wedge, \vee)$

## Proprietà

- $\wedge$  e  $\vee$  sono commutative

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

- $\wedge$  e  $\vee$  sono associative

$$\forall x, y, z \in S \quad x \wedge (y \wedge z) = \inf(\{a, b, c\}) = (x \wedge y) \wedge z$$

- Valgono le leggi di assorbimento

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

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

- Ogni elemento è idempotente (proprietà iterativa) deriva algebricamente dall'assorbimento

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

- Se consideriamo una struttura algebrica reticolo con queste due operazioni, e con le proprietà di sopra:

Possiamo definire una rel. d'ordine, e avere un reticolo

Quindi possiamo definire un reticolo sia come struttura che come ins. ordinato.

## Booleanerie

### Proposizione 1

Sia  $R$  un anello booleano:  $R$  è commutativo, e  $(|R| > 1) \Rightarrow R$  ha caratteristica 2

#### Dimostrazione

Ricordando che l'anello è idempotente, ma come ogni anello:

$$(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2$$

$$\text{Quindi } a+b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b, \text{ cancelliamo } a \text{ e } b \quad (\text{perché } a+b = a+ab+ba+b)$$

$$\text{cioè } ab + ba = 0,$$

$$\text{Ricaviamo quindi } \forall a, b \in R \quad (ab = -ba)$$

Applicandola nel caso di  $a=b$  diventa  $(aa = -aa)$  cioè  $(a^2 = -a^2)$ , ma  $a^2 = a$

$$\text{Quindi } (a = -a) \quad \forall a \in R$$

$$\text{Che diventa } \forall a \quad (2a = 0)$$

• In particolare:  $(2 \cdot 1 = 0_R)$  quindi  $(1 = 0 \wedge |R| = 1) \vee (|R| > 1 \wedge \text{ha caratteristica 2})$

• Sapendo che ogni elemento coincide con il suo opposto:

$$(-ba = ba), \text{ ma prima abbiamo trovato che } \forall a, b \quad (ab = -ba)$$

Cioè dimostra la commutatività

## Teorema di Stone

• Sia  $R$  un anello booleano:

• Esiste un insieme  $S$  tale che  $R$  è isomorfo ad un sottoanello unitario di  $(\mathcal{P}(S), \Delta, \cap)$

• Se  $R$  è finito, allora è isomorfo a  $(\mathcal{P}(S), \Delta, \cap)$

• Tutti i sottoanelli di  $(\mathcal{P}(S), \Delta, \cap)$  sono anelli booleani

Infatti: Ogni sottoanello unitario di un anello booleano è booleano

## Conseguenza T. di Stone

• Sia  $R$  un anello booleano

•  $|R|$  è una potenza di 2

• Se  $A$  è un Anello booleano, e  $|A| = |R| \Rightarrow A \cong R$

#### Dimostrazione

Sappiamo che  $R$  è isomorfo ad un  $(\mathcal{P}(S), \Delta, \cap)$  per un determinato  $S$

Ora  $|\mathcal{P}(S)| = 2^{|S|}$ , quindi anche  $R$  avrà la stessa cardinalità.

Per Stone abbiamo che  $A \cong (\mathcal{P}(T), \Delta, \cap)$  cioè  $|A| = |\mathcal{P}(T)|$ , quindi  $|\mathcal{P}(T)| = 2^n$  e  $|T| = n$

Dunque  $|T| = |S|$  comporta  $(\mathcal{P}(T), \Delta, \cap) \cong (\mathcal{P}(S), \Delta, \cap)$  cioè  $A \cong R$

esercizio)

$f: S \rightarrow T$  con  $f$  biettiva  $\Rightarrow |S| = |T|$ , quindi  $|\mathcal{P}(S)| = |\mathcal{P}(T)|$

Può esistere un  $\vec{g}: \mathcal{P}(S) \rightarrow \mathcal{P}(T)$  tale che  $(\vec{g}(x \Delta y) = g(x) \Delta g(y))$  e  $(\vec{g}(x \cap y) = g(x) \cap g(y)) \quad \forall x, y \in \mathcal{P}(S)$

- Nel caso di anelli booleani infiniti, esistono anelli booleani infiniti non isomorfi a  $(\mathcal{P}(S), \Delta, \cap)$  per alcun  $S$
- ex)**  $P = \{x \in \mathcal{P}(N) \mid x \text{ finito} \vee N \setminus x \text{ finito}\}$
- $P \subseteq (\mathcal{P}(N), \Delta, \cap)$  quindi  $P$  è booleano
- L'unità  $(\emptyset) \in P$ , e per def.  $(\forall y \in P \Rightarrow y \in \mathcal{P}(N))$
- Ma per ogni insieme  $S$ ,  $P$  non esistono applicazioni bigettive da  $P$  a  $\mathcal{P}(S)$ , quindi  $P$  non è isomorfo a  $(\mathcal{P}(S), \Delta, \cap)$

## Reticoli booleani

### Proposizione 5

Siano  $a, b$  elementi del reticolo  $(L, \leq)$ :

- $\{x \in L \mid a \leq x\}$  è un sottoreticolo di  $L$
- $\{x \in L \mid x \leq b\}$  è un sottoreticolo di  $L$
- $(a \leq b) \Rightarrow [a, b] \subseteq L$  è un sottoreticolo di  $L$

### Dimostrazione

Sia  $X = \{x \in L \mid a \leq x\} \Rightarrow X \neq \emptyset$ . Siano  $x, y \in X$ , sappiamo che  $(x \geq a \wedge y \geq a)$  quindi  $a \in \text{Minor}(\{x, y\})$

Quindi  $a \leq x \wedge y$ , concludiamo che  $x \wedge y \in X$ . Inoltre  $a \leq x \leq x \vee y$  cioè  $x \vee y \in X$

Abbiamo provato che  $X$  è chiuso rispetto a  $\wedge, \vee$ . Quindi  $X$  è un sottoreticolo di  $L$ .

Per dualità la seconda è vera per un determinato  $y$

E la terza è  $X \cap Y = [a, b] \neq \emptyset$

### ex) $\forall n \in \mathbb{N}$

$\text{Div}(n)$  e  $n\mathbb{N}$  sono sottoreticoli di  $(\mathbb{N}, \mid)$

Similmente:  $T \subseteq S$ ,  $\mathcal{P}(T)$  e  $\mathcal{P}(S) \setminus T$  sono sottoreticoli di  $(\mathcal{P}(S), \subseteq)$

- Se un sottoinsieme di un reticolo è ordinato risp. l'ord. indotto, non è detto che sia un sottoreticolo

### Proposizione 7

- Sia  $(L, \leq, \vee, \wedge)$  un reticolo:

- Il min è il neutro rispetto  $\vee$
- Il max è il neutro rispetto  $\wedge$

### Dimostrazione

$x = \min(L)$ ,  $\forall a \in L (x \leq a)$  quindi  $x \vee a = x$

Dualmente per il max

- Dunque se  $L$  è limitato:  $(L, \vee)$  e  $(L, \wedge)$  sono monoidi commutativi

**ex)**  $(\mathcal{P}(S), \cup, \cap)$   $\min = \emptyset$   $\max = S$

### Ex reticoli complementati

- $(\mathcal{P}(S), \subseteq)$  ogni elemento ha un complemento:  $\forall X \in \mathcal{P}(S) (S \setminus X \text{ è il complemento di } X)$
- Se  $L$  è totalmente ordinato allora è limitato, gli unici complementi sono min e max
- $(\mathbb{N}, \mid)$  le operazioni  $\vee, \wedge$  corrispondono a mcm e MCD. Gli unici complementi sono 0, 1
- Ci possono essere più complementi: per lo stesso elemento  $M_3, N_5$

## Algebra di Boole (Reticolo Booleano)

### • Struttura

- Sia  $(L, \leq)$  un reticolo, con operazioni:  $\vee, \wedge$ ; Se  $(L, \leq)$  è booleano, allora valgono delle proprietà extra, e possiamo definire la struttura  $(L, \vee, \wedge, O_L, I_L, ')$ , dove:
  - $O_L$  e  $I_L$  sono operazioni nullarie (costanti), e  $'$  è un'operazione unaria
  - 1)  $(L, \vee)$  è un semigruppo abeliano, ma con il neutro diventa il monoido  $(L, \vee, O_L)$   
Lo stesso anche per  $(L, \wedge, I_L)$
  - 2) Valgono le leggi di assorbimento  $(\forall a, b \in L \quad a \wedge (a \vee b) = a = a \vee (a \wedge b))$
  - 3)  $\wedge, \vee$  sono distributivi tra loro
  - 4)  $\forall a \in L \quad (a \wedge a = O_L) \text{ e } (a \vee a = I_L)$   
ex)  $(\mathcal{P}(S), \cup, \cap) \Rightarrow (\mathcal{P}(S), \cup, \cap, \emptyset, S, {}^c)$   ${}^c: x \in \mathcal{P}(S) \mapsto S \setminus x \in \mathcal{P}(S)$
- L'applicazione  $' : L \rightarrow L$ , che ad ogni elemento associa il suo complemento (in  $L$ )

• La 1 e 2 esprimono che  $(L, \vee, \wedge)$  sia limitato

La 3 che è distributivo

La 4 che è complementato

• Quindi l'algebra di Boole è la nozione 'puramente algebrica' di un reticolo booleano

## Isomorfismo tra Algebre

Un isomorfismo tra Algebre di Boole è un'applicazione biettiva tra  $(L_1, \vee_1, \wedge_1, O_1, I_1, {}^1)$  e  $(L_2, \vee_2, \wedge_2, O_2, I_2, {}^2)$  tale che:

$$1) f(a \vee_1 b) = f(a) \vee_2 f(b) \text{ e } f(a \wedge_1 b) = f(a) \wedge_2 f(b)$$

$$2) f(O_1) = O_2, f(I_1) = I_2$$

$$3) f(a') = (f(a))^2$$

• La 1 esprime un isomorfismo tra reticolati

Ma se i due reticolati sono isomorfi, vale la 2

•  $\forall x \in L_1$  ( $x'$  è il complemento di  $x$ ) quindi la sua immagine sarà il complemento di  $f(x) \in L_2$

• Due Algebre di Boole sono isomorfe  $\Leftrightarrow$  Sono isomorfe come reticolati

Quindi lo studio delle algebre di Boole equivale allo studio dei reticolati booleani

## Sottoalgebra

- Sia  $L$  un'algebra di Boole,  $\emptyset \neq M \subseteq L$   
 $M$  è una sottoalgebra di Boole  $\Leftrightarrow$  [è chiusa rispetto a  $(\wedge, \vee)$  ed a  $'$  (cioè  $\forall a \in M (a' \in M)$ ), e  $(\{0_L, 1_L\}) \subseteq M$ ]
- L'ultimo punto segue dalle precedenti, infatti: siccome  $0_L = a \wedge a'$ , allora se ( $M$  è chiusa rispetto a  $\wedge$  e  $'$ )  $\Rightarrow 0_L \in M$   
Similmente per  $1_L$ .

ex)  $T \subseteq S$ ,  $\mathcal{O}(T)$  non è una sottoalgebra di  $\mathcal{O}(S)$ , perché non ha  $1_S \in T$ , ma  $\mathcal{O}(T)$  è un sottoreticolato di  $\mathcal{O}(S)$   
Cioè perché la sottoalgebra deve essere chiusa rispetto i complementi:

NB: La nozione di **Sottoalgebra** differisce da quella di **sottoreticolato**.

Ad un sottoreticolato basta essere chiuso rispetto le operazioni reticolari.

Una sottoalgebra necessita anche di chiusura rispetto a max, min e complementi.

## De Morgan e regole di calcolo

Sia  $(L, \vee, \wedge, 0, 1, ')$  un'algebra di Boole. Allora per ogni  $a, b \in L$ :

1)  $1 \vee a = 1$  e  $0 \wedge b = 0$

2)  $1' = 0$  e  $0' = 1$

3)  $(a')' = a$

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

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

• La 1 segue dalle leggi di assorbimento, la 2 dal fatto che  $L$  è un reticolato complementato.

La 3 significa che  $'$  è involutoria, cioè l'inversa di se stesso (segue dall'unicità dei comp. nei reticolati booleani)

### Dimostrazione 4/5 (De Morgan)

Dimostriamo che  $a' \wedge b'$  è il complemento di  $(a \vee b)'$

Cioè che:  $(a \vee b) \vee \underbrace{(a' \wedge b')}_{\rightarrow} = 1$  e che  $(a \vee b) \wedge (a' \wedge b') = 0$

Usiamo la distributività:

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

Simmetricamente:

$$(a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = (0 \wedge b') \vee (a' \wedge 0) = 0 \vee 0 \quad \text{che è una bella faccina}$$

La 5 segue per dualità

ex) Se la nostra algebre è  $(\mathcal{O}(S), \cup, \cap, \emptyset, S, {}^c)$ , allora questa proposizione esprime che  $\forall a, b \in \mathcal{O}(S)$

1)  $S \cup a = S$  e  $a \cap \emptyset = \emptyset$

2)  $S \setminus S = \emptyset$  e  $S \setminus \emptyset = S$

3)  $S \setminus (S \setminus a) = a$

4)  $S \setminus (a \cup b) = (S \setminus a) \cap (S \setminus b)$

5)  $S \setminus (a \cap b) = (S \setminus a) \cup (S \setminus b)$

## ■ Interscambiabilità tra Algebre ed Anelli Booleani

- Idea generale: Partire dall'esempio

Sia  $(R, +, \cdot)$  un anello booleano, vogliamo definire una struttura di reticolo booleano su  $R$ .

Partiamo dall'anello delle parti di un insieme:  $(\mathcal{P}(S), \Delta, \cap)$  che è comunque un anello booleano,

E con  $\mathcal{P}(S)$  reticolo booleano. Adesso l'operazione moltiplicativa è la stessa, dobbiamo definire quella additiva, cioè:  $\forall a, b \in \mathcal{P}(S) \quad a \cup b = (a \Delta b) \Delta (\Delta a b)$

Abbiamo min e max  $(\emptyset, S)$ . Ed ogni elemento ha complemento  $a' = S \setminus a = S \Delta a = I \Delta a$

### • Da Anello ad Algebra

In un arbitrario anello booleano  $(R, +, \cdot, 0, 1)$  definiamo:

- L'operazione  $\vee$ :  $\forall a, b \in R \quad a \vee b = a + b + ab$
- L'applicazione  $'$ :  $\forall a \in R \quad a' = I + a$

### • Proposizione

Quella descritta qui sopra è un'Algebra di Boole

#### Dimostrazione

Ecco la lista della spesa:

- Verificare che  $(R, \vee, 0)$  e  $(R, \cdot, I)$  siano monoidi abeliani
- Che valgano per  $\vee, \cdot$  le leggi di assorbimento e la distributività
- Che l'applicazione  $'$  verifichi la condizione richiesta

1)  $(R, \vee, 0)$  è sicuramente commutativo, e  $(\forall a \in R)(a \vee 0 = a + 0 + a0 = a)$

Proviamo l'associalità:  $\forall a, b, c \in R \quad a \vee (b \vee c) = (a \vee b) \vee c$

$$(a \vee b) \vee c = (a + b + ab) \vee c = (a + b + ab) + c + (a + b + ab) \cdot c = a + b + ab + c + ac + bc + abc$$

$$a \vee (b \vee c) = a \vee (b + c + bc) = a + (b + c + bc) + a(b + c + bc) = a + b + c + bc + ab + ac + abc$$

Quindi  $(R, \vee, 0)$  è un monoide abeliano

Che  $(R, \cdot, I)$  sia un monoide abeliano lo sappiamo perché siamo partiti da un Anello booleano

2) Vediamo le leggi di assorbimento:

$$\forall a, b \in R \quad a \vee (a \cdot b) = a + ab + aa \cdot b = a + ab + ab = a \quad (\text{ogni elemento è il suo inverso})$$

$$\forall a, b \in R \quad a(a \vee b) = a(a + b + ab) = a^2 + ab + ab = a$$

Quindi sappiamo che  $R$  è un reticolo limitato.

Verifichiamo la distributività:

$$\forall a, b, c \in R \quad a \cdot (b \vee c) = a(b + c + bc) = ab + ac + abc$$

$$\text{Ed } (a \cdot b) \vee (a \cdot c) = ab + ac + aabc = ab + ac + abc$$

3) Infine  $\forall a \in R \quad a \cdot a' = I + a$  deve verificare la def.

$$\text{Cioè } a \vee a' = I : a \vee a' = a + a' + aa' = a + (I + a) + 0 = I$$

$$\text{E } \forall a \in R \quad a \cdot a' = a \cdot (I + a) = a + a = 0$$

## • Da Algebra ad Anello

Partiamo dall'esempio di:  $(\mathcal{C}(S), \vee, \wedge, \emptyset, S, {}^c)$  dobbiamo ottenere  $(\mathcal{C}(S), \Delta, \cap)$

Abbiamo già l'operazione moltiplicativa, dobbiamo ottenere quella additiva

$$\text{Definiamo } \Delta : (A \setminus B) \cup (B \setminus A) = (A \cap B^c) \cup (B \cap A^c) = (A \cup B) \setminus (A \cap B)$$

## • Lemma

Sia  $(L, \vee, \wedge, \emptyset, I, {}^c)$  un'algebra di Boole, allora  $\forall a, b \in L (a \wedge b^c) \vee (a^c \wedge b) = (a \vee b) \wedge (a \wedge b)^c$

### Dimostrazione

Usando la distributività:

$$(a \wedge b^c) \vee (a^c \wedge b) = a \vee a^c \wedge a \vee b \wedge b^c \wedge b \vee b^c = I \wedge a \vee b \wedge b^c \wedge I = (a \vee b) \wedge (a \wedge b)^c$$

## • Osservazione

Sia  $(L, \vee, \wedge, \emptyset, I, {}^c)$  un'algebra di Boole, allora  $\forall a, b, c \in L (a \wedge b)^c \wedge (a \wedge c) = a \wedge b^c \wedge c$

### Dimostrazione

Usando De Morgan:

$$(a \wedge b)^c \wedge (a \wedge c) = (a^c \vee b^c) \wedge a \wedge c = (a^c \vee b^c \vee a) \wedge c$$

$$((a^c \vee b^c \vee a) \wedge c) = (b^c \wedge a) \wedge c = a \wedge b^c \wedge c$$

## • Proposizione

Sia  $(L, \vee, \wedge, \emptyset, I, {}^c)$  un'Algebra di Boole, se definiamo l'operazione  $+$ :

$\forall a, b \in L (a + b = (a \wedge b^c) \vee (a^c \wedge b))$  allora  $L$  diventa un anello booleano con  $\emptyset, I$

### Dimostrazione $\Delta$

Verifichiamo che  $(L, +, \emptyset)$  sia un gruppo abeliano, (dato che  $\wedge, \vee$  sono commutative, anche  $+$  lo è)

$$\forall a, b, c \in L a + b + c = (a \wedge b^c) \vee (a^c \wedge b) + c$$

$$(((a \wedge b^c) \vee (a^c \wedge b)) \wedge c^c) \vee (((a \wedge b^c) \vee (a^c \wedge b))^c \wedge c) =$$

Usiamo il  $\forall a, b \in L (a \wedge b^c) \vee (a^c \wedge b) = (a \vee b) \wedge (a \wedge b)^c$  quindi: "spostiamo il complemento"

$$(((a \wedge b^c) \vee (a^c \wedge b)) \wedge c^c) \vee (((a \vee b) \wedge (a \wedge b)^c)^c \wedge c) =$$

Adesso De Morgan

$$(((a \wedge b^c) \vee (a^c \wedge b)) \wedge c^c) \vee (((a \wedge b^c) \vee (a^c \wedge b))^c \wedge c) =$$

Infine la distributività:

$$((a \wedge b^c \wedge c^c) \vee (a^c \wedge b \wedge c^c)) \vee ((a \wedge b^c \wedge c) \vee (a^c \wedge b \wedge c))$$

Togliamo le parentesi:

$$(a \wedge b^c \wedge c^c) \vee (a^c \wedge b \wedge c^c) \vee (a \wedge b^c \wedge c) \vee (a^c \wedge b \wedge c)$$

Adesso, per la commutatività di  $\vee, \wedge$  anche  $+$  è commutativa, ed associativa

$\forall a \in L (a + \emptyset = (a \wedge I \vee a \wedge \emptyset) = a \vee \emptyset = a)$  quindi  $\emptyset$  è neutro rispetto a  $+$  neutro

$\forall a \in L (a + a = (a \wedge a^c) \vee (a^c \wedge a) = \emptyset \vee \emptyset = \emptyset)$  ogni elemento è il simmetrico di se stesso inversi

Quindi  $(L, +)$  è un gruppo abeliano

Per def  $(L, \wedge)$  è un monoido commutativo

Ci serve verificare la distributività di  $\wedge$  rispetto a  $+$ .

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

Usando due volte la formula  $(a \wedge b) \wedge (a \wedge c) = a \wedge b \wedge c$  otteniamo

$$((a \wedge b) \wedge (a \wedge c)) \vee ((a \wedge c) \wedge (a \wedge b))$$

Quindi:  $a \wedge (b + c) = (a \wedge b) + (a \wedge c)$  cioè la distributività

Ecco dimostrato che è un anello, il resto segue dalla def. di Alg. di Boole

- Quindi abbiamo visto che è possibile definire da un anello booleano un'algebra, e poi da un'algebra un anello.

E' anche possibile dimostrare che l'operazione additiva è la stessa

Quindi riotteniamo lo stesso anello da cui eravamo partiti, lo stesso vale per il discorso inverso

### Teorema

Sia  $L$  un insieme. E sia  $A$  l'insieme delle coppie ordinate  $(\vee, \wedge)$  di op. binarie in  $L$  che strutturano  $L$  un'Algebra di Boole. E sia  $B$  l'insieme delle coppie ordinate  $(\vee, \wedge)$  di op. binarie in  $L$  che strutturano  $L$  come un Anello booleano.

Allora si possono definire due applicazioni  $(f: A \rightarrow B, g: B \rightarrow A)$  che sono inverse tra loro, quindi biettive

Questa corrispondenza tra algebre ed anelli booleani conserva la nozione di isomorfismo

### Proposizione

Siano  $(L_1, \vee_1, \wedge_1, 0_1, 1_1, ')$  e  $(L_2, \vee_2, \wedge_2, 0_2, 1_2, '')$  algebre di Boole,

e siano  $(L_1, +_1, \wedge_1)$  e  $(L_2, +_2, \wedge_2)$  i corrispettivi anelli booleani.

Sia poi  $f: L_1 \rightarrow L_2$  un'applicazione biettiva.

$f$  è un isomorfismo tra algebre di Boole  $\Leftrightarrow$  E' un isomorfismo tra anelli booleani

Dimostrazione  $\Rightarrow$

Sia  $f$  un isomorfismo tra Algebre, allora  $\forall a, b \in L_1$  si ha

$$\begin{aligned} f(a +_1 b) &= f((a \vee_1 b') \wedge_1 (a \vee_1 b)) = \\ &= (f(a) \vee_2 f(b')) \wedge_2 (f(a) \wedge_2 f(b)) = f(a) +_2 f(b) \end{aligned}$$

$$\text{Ovviamente } f(a \vee_1 b) = f(a) \vee_2 f(b)$$

Quindi  $f$  è un isomorfismo di anelli booleani

Dimostrazione  $\Leftarrow$

Se  $f$  è un isomorfismo di anelli booleani, allora  $\forall a, b \in L_1$

$$f(a \wedge_1 b) = f(a) \wedge_2 f(b)$$

$$f(a \vee_1 b) = f(a +_1 b + (a \wedge_1 b)) = f(a) +_2 f(b) +_2 (f(a) \wedge_2 f(b)) = f(a) \vee_2 f(b)$$

- Dunque  $f$  conserva le op reticolari, quindi è un isomorfismo di reticolati. Che come abbiamo visto sopra è anche un isomorfismo tra Algebre

## Proposizione

Sia  $(L, \vee, \wedge, 0, 1, ')$  un'algebra di Boole, sia  $(L, +, \wedge)$  il suo anello booleano.

Sia  $K \subseteq L$ . Allora  $K$  è una sottoalgebra  $\Leftrightarrow K$  è un sottoanello unitario di  $(L, +, \wedge)$

### Dimostrazione

Sia  $K$  una sottoalgebra di  $L$

Allora  $\forall a, b \in K (a+b = (a \wedge b') \vee (a' \wedge b) \in K)$  quindi  $K$  è chiusa rispetto a  $+$

Dato che  $(L, +, \wedge)$  è booleano, ogni elemento coincide con il suo opposto

Quindi  $K$  è un sottogruppo di  $L$ ,  $(K, \wedge, 1)$  è anche un sottomonoido (in quanto sottoalgebra di  $L$ )

### Dimostrazione $\Leftarrow$

Se  $K$  è un sottoanello unitario di  $(L, +, \wedge)$ . Allora  $K$  è un sottomonoido di  $(L, \wedge, 1)$ , inoltre  $0 \in K$

e  $\forall a \in K (a' = a+1 \in K)$

Dunque  $\forall a, b \in K (a \vee b = (a \wedge b') + (a' \wedge b) \in K)$

Concludiamo che  $K$  è un sottomonoido di  $(L, \vee, 0)$  e contiene in  $L$  il complemento di ogni suo elemento.

Dunque  $K$  è una sottoalgebra

## Teorema di Stone (per Algebre di Boole)

Sia  $L$  un'Algebra di Boole, allora:

- Esiste un insieme  $S$  tale che  $L$  sia isomorfa ad una sottoalgebra di Boole dell'algebra delle parti di  $S$   $(\wp(S), \cup, \cap, \emptyset, S, ')$
- Se  $L$  è finita, esiste un insieme  $S$  tale che  $L$  sia isomorfa all'algebra  $(\wp(S), \cup, \cap, \emptyset, S, ')$

## Teorema di Stone (per reticolati booleani)

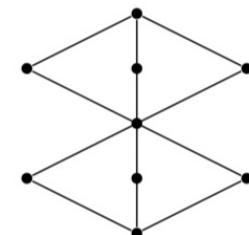
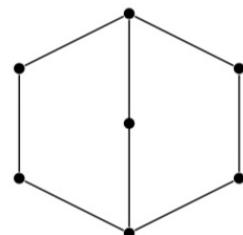
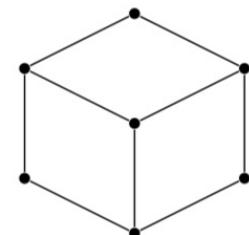
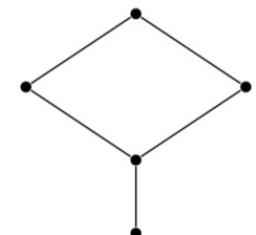
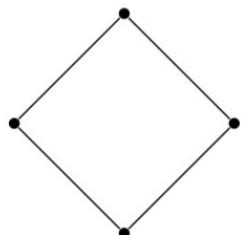
Sia  $L$  un reticolo booleano, allora:

- Esiste un insieme  $S$  tale che  $L$  sia isomorfo ad un sottoreticolo del reticolo  $(\wp(S), \subseteq)$
- Se  $L$  è finito, esiste un insieme  $S$  tale che  $L$  sia isomorfo a  $(\wp(S), \subseteq)$

**Esercizio 8.** Per ogni  $n \in \mathbb{N}$ , sia  $D_n$  il reticolo dei divisori di  $n$  in  $\mathbb{N}$  (che è, ricordiamo, un sottoreticolo di  $(\mathbb{N}, |)$ ). Lo scopo di questo esercizio è riconoscere che  $D_n$  è complementato se e solo se  $n$  è un intero *libero da quadrati*, cioè un intero non divisibile per il quadrato di alcun primo.<sup>(4)</sup>

- (i) Sia  $d$  un divisore (in  $\mathbb{N}$ ) di  $n$ . Se  $d$  e  $n/d$  sono coprimi, allora  $n/d$  è un complemento di  $d$  in  $D_n$ . [Suggerimento: basta calcolare MCD e mcm tra  $d$  e  $n/d$ .]
- (ii) Dedurre dal punto precedente che se  $n$  è libero da quadrati allora  $D_n$  è complementato. [Suggerimento: pensare alla scomposizione di  $n$  in fattori primi e descrivere i divisori di  $n$ .]
- (iii) Supponiamo che esista un primo  $p$  tale che  $p^2$  divida  $n$ . Allora  $p$  non ha complemento in  $D_n$ . [Suggerimento: se  $a$  è un complemento di  $p$ ,  $p$  divide o non divide  $a$ ?]
- (iv) A questo punto la conclusione è facile:  $D_n$  è complementato se e solo se  $n$  è libero da quadrati.

Ulteriori esempi: dei reticolati qui rappresentati sono complementati il primo, ed il quarto, non gli altri tre.



### In sintesi

Si definiscono tre tipi di strutture che fanno riferimento nel loro nome a quello di George Boole. Abbiamo gli *anelli booleani*, che sono per definizione gli anelli unitari i cui elementi sono tutti idempotenti, i *reticolati booleani*, che sono invece i reticolati distributivi e complementati, le *algebre di Boole*, che sono particolari strutture algebriche la cui definizione è riportata più avanti, nella terza sezione di queste note.

Ciò che lega queste strutture tra loro è che definire su un insieme una struttura di uno di questi tre tipi (anello booleano, reticolo booleano, algebra di Boole) equivale definirne una di ciascuno degli altri due tipi; in modo che risulti del tutto equivalente lo studio degli anelli booleani, quello delle algebre di Boole e quello dei reticolati booleani.

L'*esempio* da avere come *riferimento* è quello dell'insieme  $\mathcal{P}(S)$  delle parti di un insieme  $S$ . Come dovrebbe essere ben noto,  $(\mathcal{P}(S), \subseteq)$ , cioè l'insieme  $\mathcal{P}(S)$  ordinato per inclusione, è un reticolo, che risulta essere un *reticolo booleano*. Lo stesso insieme, munito delle operazioni di differenza simmetrica ed intersezione,  $(\mathcal{P}(S), \Delta, \cap)$ , è un *anello booleano*. Infine,  $\mathcal{P}(S)$  si può strutturare come *algebra di Boole* mediante le *operazioni di unione, intersezione e l'operazione unaria di complemento*:  $X \in \mathcal{P}(S) \mapsto S \setminus X \in \mathcal{P}(S)$ ; l'algebra di Boole così ottenuta è  $(\mathcal{P}(S), \cup, \cap, \emptyset, S, {}^c)$ .

Questo esempio è particolarmente importante per almeno due motivi. Uno di tipo pratico: il modo in cui si può, in  $\mathcal{P}(S)$ , passare da uno dei tre tipi di struttura booleana a ciascuno degli altri due illustra molto bene come si può effettuare l'analogo passaggio a partire da una struttura booleana arbitraria; questo esempio può essere quindi di grande aiuto nello studio della situazione generale. Il secondo motivo, di carattere teorico e di importanza ancora maggiore, è che quello fornito dagli insiemi  $\mathcal{P}(S)$  non è un esempio particolare ma, in qualche modo, *quello tipico*. Infatti un importante teorema (dovuto a M.H. Stone) mostra che *ogni anello booleano finito è isomorfo a  $(\mathcal{P}(S), \Delta, \cap)$  per un opportuno insieme  $S$*  (per gli anelli infiniti il teorema è un po' più debole: ogni anello booleano è isomorfo ad un sottoanello unitario di  $(\mathcal{P}(S), \Delta, \cap)$ , per un opportuno insieme  $S$ ). Analoghi enunciati valgono per i reticolati booleani e per le algebre di Boole. Questo vuol dire, ad esempio, che se sappiamo descrivere il reticolo delle parti degli insiemi finiti, conosciamo, a meno di isomorfismi, tutti i reticolati booleani finiti. Una conseguenza del teorema di Stone è che gli anelli booleani finiti (ma lo stesso vale per i reticolati booleani finiti o per le algebre di Boole finite) hanno per cardinalità una potenza di 2, e che due anelli booleani finiti con lo stesso numero di elementi sono necessariamente isomorfi.