

# **Algebra & Logica**

**Appunti**

Galizzi Francesco & Scandella Matteo

18 giugno 2014

# Indice

<b>I. Algebra</b>	<b>5</b>
<b>1. Relazioni su un insieme</b>	<b>6</b>
1.1. Introduzione . . . . .	6
1.2. Grafo associato ad una relazione . . . . .	6
1.3. Proprietà . . . . .	6
1.3.1. Restrizione ad un sottoinsieme . . . . .	8
1.4. Relazioni di equivalenza . . . . .	9
1.4.1. Classi di equivalenza . . . . .	9
1.4.2. Insieme quoziente . . . . .	10
1.4.3. Congruenza modulo $n$ . . . . .	11
1.4.4. Rappresentanti e buona definizione . . . . .	13
1.4.5. Somma e prodotto in $\mathbb{Z}/n\mathbb{Z}$ . . . . .	14
1.5. Relazioni di ordine . . . . .	14
1.5.1. Ordine totale . . . . .	14
1.5.2. Estremanti . . . . .	14
1.5.3. Reticolo . . . . .	16
1.5.4. Proprietà dei reticoli . . . . .	16
<b>2. Strutture algebriche</b>	<b>17</b>
2.1. Leggi di composizione . . . . .	17
2.1.1. Definizione . . . . .	17
2.1.2. Proprietà . . . . .	17
2.2. Strutture con una lci . . . . .	19
2.2.1. Base . . . . .	19
2.2.2. Il monoide delle parole . . . . .	21
2.2.3. Sottogruppi . . . . .	21
2.2.4. Gruppo quoziente . . . . .	22
2.3. Gruppi finiti . . . . .	23
2.3.1. Elementi di ordine finito . . . . .	23
2.3.2. Gruppi finiti . . . . .	25
2.4. Morfismi . . . . .	25
<b>3. Aritmetica</b>	<b>27</b>
3.1. Richiami . . . . .	27
3.2. Ideali di $\mathbb{Z}$ . . . . .	27
3.2.1. Definizione . . . . .	27
3.2.2. $\mathbb{Z}$ è principale . . . . .	29
3.2.3. Intersezione e somma . . . . .	29
3.2.4. $MCD$ , $mcm$ . . . . .	30
3.2.5. Proprietà di $MCD$ e $mcm$ . . . . .	30

3.2.6.	Teorema di Bezout . . . . .	30
3.3.	Equazioni diofantee . . . . .	31
3.3.1.	Teorema cinese dei resti . . . . .	31
3.3.2.	Equazioni diofantee . . . . .	31
3.3.3.	Invertibili in $\mathbb{Z}/n\mathbb{Z}$ . . . . .	32
3.4.	Algoritmo di Euclide . . . . .	32
<b>4.</b>	<b>Strutture algebriche (2)</b>	<b>34</b>
4.1.	Applicazioni della teoria dei gruppi . . . . .	34
4.1.1.	Teoremi di Fermat ed Eulero . . . . .	34
4.1.2.	Diffie-Hellman . . . . .	34
4.1.3.	RSA (Ronald Rivest, Adi Shamir, Leonard Adleman, 1978) . . . . .	35
4.2.	Strutture algebriche con 2 lei . . . . .	36
4.2.1.	Anello . . . . .	36
4.2.2.	Proprietà . . . . .	37
4.2.3.	Ideali . . . . .	37
4.2.4.	Anelli di polinomi . . . . .	39
4.2.5.	Campi . . . . .	39
<b>II.</b>	<b>Logica</b>	<b>42</b>
<b>5.</b>	<b>Logica proposizionale</b>	<b>43</b>
5.1.	Il linguaggio . . . . .	43
5.1.1.	Base . . . . .	43
5.1.2.	Induzione . . . . .	45
5.1.3.	Albero sintattico . . . . .	45
5.1.4.	Semantica . . . . .	46
5.1.5.	Equivalenza semantica . . . . .	49
5.1.6.	Completezza funzionale . . . . .	51
5.1.7.	Dualità . . . . .	51
5.2.	Forme normali . . . . .	52
5.2.1.	Definizione . . . . .	52
5.2.2.	Esistenza . . . . .	52
5.3.	Sistemi deduttivi . . . . .	53
5.3.1.	Idea . . . . .	53
5.3.2.	Deduzione naturale . . . . .	53
5.3.3.	Rappresentazione ad albero . . . . .	55
5.3.4.	Interpretazione semantica . . . . .	56
5.3.5.	Risoluzione a clausole . . . . .	56
<b>6.</b>	<b>Logica dei predicati o del primo ordine</b>	<b>59</b>
6.1.	Il linguaggio . . . . .	59
6.1.1.	Base . . . . .	59
6.1.2.	Sottoformule . . . . .	60
6.1.3.	Principi di induzione . . . . .	61
6.1.4.	Variabili libere e vincolate . . . . .	61
6.1.5.	Semantica . . . . .	65
6.1.6.	Soddisfacibilità, validità e modelli . . . . .	66
6.1.6.1.	Definizione . . . . .	66

## *Indice*

6.1.6.2.	Chiusure . . . . .	69
6.1.6.3.	Proprietà delle chiusure . . . . .	69
6.1.7.	Equivalenza semantica . . . . .	69
6.1.8.	Forma normale prenessa . . . . .	70
6.1.9.	Forma di Skolem . . . . .	70
6.2.	Sistemi deduttivi . . . . .	71
6.2.1.	Deduzione naturale . . . . .	71
6.2.2.	Risoluzione . . . . .	71
6.3.	Complementi . . . . .	75
6.3.1.	Decidibilità . . . . .	75
6.3.2.	Gödel . . . . .	75
 <b>III. Appendici</b>		<b>76</b>
 <b>A. La prova del 9</b>		<b>77</b>
 <b>B. Divertimenti</b>		<b>78</b>

**Parte I.**

**Algebra**

# 1. Relazioni su un insieme

## 1.1. Introduzione

### Definizione

- Una **corrispondenza** tra 2 insiemi  $A$  e  $B$  è una parte  $f$  di  $A \times B$ .
- Un'**applicazione** da un insieme  $A$  a un insieme  $B$  è una corrispondenza  $f$  tra  $A$  e  $B$  tale che  $\forall a \in A \exists$  un solo  $b \in B$  tale che  $(a, b) \in f$ .
- Una **relazione** su un insieme  $A$  è una parte  $\rho$  di  $A \times A$  (quindi una corrispondenza tra  $A$  e  $A$ ). Se  $(a, b) \in \rho$  si scrive  $a \rho b$  e si dice che  $a \rho b$  è vera (se no che è falsa).

**Esempi** N.B.:  $(a, b) \neq (b, a)$  se  $b \neq a$ , mentre  $\{a, b\} = \{b, a\}$ .

- $A = \mathbb{N} (\mathbb{Z}, \mathbb{Q}, \mathbb{R}), \leq = \{(a, b) \in A \times A \mid \exists c \in \mathbb{R} \mid b = a + c^2\}$
- $A$  qualsiasi,  $\rho = =$  (la relazione  $\rho$  è l'uguaglianza)  
 $= = \{(a, a) \in A \times A \mid a \in A\}$
- $A = \mathbb{N} (\mathbb{Z}), \mid = \{(a, b) \in A \times A \mid \exists k \in A \mid b = a \cdot k\}$ <sup>I</sup>  
 $\Rightarrow a \mid b$  se e solo se  $\exists k \in A \mid b = a \cdot k$
- se  $X$  è un qualsiasi insieme,  $A = \mathcal{P}(X)$ <sup>II</sup>,  $\subseteq$  è una relazione su  $A$   
 $\subseteq = \{(B, C) \in A \times A \mid \exists Z \in A \mid C = B \cup Z\}$
- $A = \text{piano}, \rho = \{(P, Q) \in A \times A \mid P \text{ e } Q \text{ hanno la stessa ordinata}\}$

## 1.2. Grafo associato ad una relazione

Data una relazione  $\rho$  su un insieme  $A$ , le associamo un grafo orientato nel modo seguente:

- i vertici sono gli elementi di  $A$  (punto);
- $C'$  è uno spigolo da  $a$  verso  $b$  se e solo se  $a \rho b$  (freccia).

## 1.3. Proprietà

Sia  $A$  un insieme e  $\rho$  una relazione su  $A$ .

**Riflessività** Si dice che  $\rho$  è **riflessiva** se e solo se  $\forall a \in A, a \rho a$  (cioè  $(a, a) \in \rho$ ).

Sul grafo c'è una freccia, detta *cappio*, da ogni elemento verso se stesso.

Se si sa che  $\rho$  è riflessiva si omettono i cappi dal grafo.

---

<sup>I</sup>La relazione " $\mid$ " si legge "divide".

<sup>II</sup>Insieme delle parti di  $X$ , ossia l'insieme di tutti i possibili sottoinsiemi di  $X$ .

## 1. Relazioni su un insieme

**Simmetria** Si dice che  $\rho$  è **simmetrica** se  $\forall (a, b) \in A \times A, a \rho b \Rightarrow b \rho a$  (cioè se  $(a, b) \in \rho$  allora  $(b, a) \in \rho$ ).

Sul grafo per ogni freccia esiste quella nel verso opposto; posso tracciarne una sola togliendo l'estremità.

**Transitività** Si dice che  $\rho$  è **transitiva** se e solo se  $\forall (a, b, c) \in A^3, a \rho b \wedge b \rho c \Rightarrow a \rho c$  (se  $(a, b) \in \rho$  e  $(b, c) \in \rho$  allora  $(a, c) \in \rho$ ).

Nel grafo significa che “ci sono le scorciatoie”; se si sa che  $\rho$  è transitiva non si indicano le frecce che conseguono dalle altre.

**Antisimmetria** Si dice che  $\rho$  è **antisimmetrica** se e solo se  $\forall (x, y) \in A^2, x \rho y \wedge y \rho x \Rightarrow x = y$  (cioè se  $(x, y) \in \rho$  e  $(y, x) \in \rho \Rightarrow x = y$ ).

Non ci sono frecce in versi opposti, tranne eventuali cappi.

N.B.: non è il contrario di simmetrico (una relazione può essere sia simmetrica che antisimmetrica, nel qual caso potrà contenere solo cappi).

**Equivalenza** Si dice che  $\rho$  è una **relazione di equivalenza** (o un'**equivalenza**) se e solo se è riflessiva, simmetrica e transitiva.

Sul grafo si “chiudono i cerchi”.

**Ordine** Si dice che  $\rho$  è una **relazione di ordine** (o un **ordine**) se e solo se è riflessiva, antisimmetrica e transitiva.

Sul grafo si dispongono gli elementi in modo che tutte le frecce siano rivolte verso l'alto e si omettono le estremità (albero).

### Osservazione

- Esistono relazioni sia simmetriche che antisimmetriche (sono formate da soli cappi).
- L'uguaglianza è l'unica relazione che possiede tutte le proprietà ed è sia un'equivalenza che un ordine.

**Esempi**  $A = \mathbb{N}(\mathbb{Z})$ .

= riflessiva, simmetrica, transitiva, antisimmetrica, equivalenza, ordine

$\leq \{(a, b) \in A \times A \mid \exists c \in \mathbb{R} \mid b = a + c^2\}$

R sia  $a \in A$ , allora con  $c = 0$ ,  $a = a + c^2$ , quindi è riflessiva

S  $2 \leq 3$  ma  $3 \not\leq 2$

T siano  $a, b, c \in A$  tali che  $a < b$  e  $b < c$ , allora:  
 $\exists k, l \in \mathbb{R}$  tali che  $b = a + k^2$  e  $c = b + l^2 = a + k^2 + l^2$ .  
 Dato che  $\sqrt{k^2 + l^2} \in \mathbb{R}$ ,  $a \leq c$ , quindi è transitiva

A siano  $a, b \in A$  tali che  $a \leq b$  e  $b \leq a$ , allora:  
 $\exists k, l \in \mathbb{R}$  tali che  $b = a + k^2$  e  $a = b + l^2 = a + k^2 + l^2$   
 $\Rightarrow k^2 = -l^2 \Rightarrow k = l = 0 \Rightarrow a = b$ , quindi è antisimmetrica

quindi è un ordine

$\subseteq \{(B, C) \in \mathcal{P}(X) \times \mathcal{P}(X) \mid \exists Z \in \mathcal{P}(X) \mid C = B \cup Z\}$

R sia  $A \in \mathcal{P}(X)$ , allora con  $B = \emptyset$   $A = A \cup B$ , quindi è riflessiva

## 1. Relazioni su un insieme

<u>S</u>	$A = \{1, 2\}, B = \{2\} \Rightarrow B \subseteq A$ ma $A \not\subseteq B$ quindi non è simmetrica
<u>T</u>	Siano $A, B, C \in \mathcal{P}(X)$ tali che $A \subseteq B$ e $B \subseteq C$ , allora: $\exists X, Y \in \mathcal{P}(X)$ tali che $B = A \cup X$ e $C = B \cup Y = A \cup X \cup Y$ . Dato che $X \cup Y \in \mathcal{P}(X)$ , $A \subseteq C$ , quindi è transitiva
<u>A</u>	Siano $A, B \in \mathcal{P}(X)$ tali che $A \subseteq B$ e $B \subseteq A$ , allora: $\exists X, Y \in \mathcal{P}(X)$ tali che $B = A \cup X$ e $A = B \cup Y = A \cup X \cup Y$ , quindi $X \cup Y = \emptyset \Rightarrow X = Y = \emptyset \Rightarrow B = A$ , quindi è antisimmetrica

quindi è un ordine

< dato che la definizione di < non è facilmente formulabile è difficile trovare una dimostrazione formale

R

S

T

A

"stessa ordinata" riflessiva, simmetrica, transitiva, ~~antisimmetrica~~  $((2, 0) \neq (4, 0))$

Le dimostrazioni si ricavano da quelle dell'uguaglianza

|  $\{(a, b) \in A \times A \mid \exists k \in A \mid b = a \cdot k\}$

R sia  $a \in A$ . Allora  $a = 1 \cdot a$ , quindi  $a \mid a$

S  $2 \mid 4$  ma  $4 \nmid 2$  perché  $\forall k \in A, 4k \geq 4$  se  $k > 0, 4k \leq 0$  se  $k < 0$  quindi  $\forall k \in A, 4k \neq 2$

T siano  $a, b, c \in A$  tali che  $a \mid b$  e  $b \mid c \Rightarrow \exists k, l \in A$  tali che  $b = k \cdot a$  e  $c = l \cdot b = l \cdot k \cdot a, l \cdot k = m \in A$ , quindi  $a \mid c$ , quindi è transitiva

A siano  $a, b \in A$  tali che  $a \mid b$  e  $b \mid a$ , cioè tali che  $\exists k, l$  tali che  $b = k \cdot a, a = l \cdot b$ .  
Quindi  $a = l \cdot k \cdot a$ .

Se  $a = 0, b = k \cdot a = 0 = a$ .

Se  $a \neq 0, k \cdot l = 1$ . Questo è possibile se e solo se  $k = l = \pm 1$ .

Per  $A = \mathbb{N}, k = l = 1$  quindi  $b = a$  e  $\mid$  è antisimmetrica.

Per  $A = \mathbb{Z}, a = 2$  e  $b = -2$  sono tali che  $a \mid b$  e  $b \mid a$  con  $a \neq b$  quindi  $\mid$  non è antisimmetrica.

$\mid$  è una relazione d'ordine per  $\mathbb{N}$  ma non per  $\mathbb{Z}$

### 1.3.1. Restrizione ad un sottoinsieme

**Definizione** Sia  $R$  una relazione su un insieme  $A$  e sia  $B$  un sottoinsieme di  $A$ . La **restrizione di  $R$  a  $B$**  è la relazione  $R_B$  su  $B$  definita da  $R_B = R \cap (B \times B)$ , cioè  $\forall b_1, b_2 \in B, b_1 R_B b_2 \Leftrightarrow b_1 R b_2$ .

**Proposizione** Siano  $A, B, R$  e  $R_B$  come sopra, allora:

- Se  $R$  è riflessiva  $\Rightarrow R_B$  è riflessiva
- Se  $R$  è simmetrica  $\Rightarrow R_B$  è simmetrica
- Se  $R$  è transitiva  $\Rightarrow R_B$  è transitiva
- Se  $R$  è antisimmetrica  $\Rightarrow R_B$  è antisimmetrica



## 1.4. Relazioni di equivalenza

### 1.4.1. Classi di equivalenza

Sia  $A$  un insieme,  $\sim$  una relazione di equivalenza su  $A$ .  $\forall a \in A$  la **classe di equivalenza** di  $a$  per  $\sim$  è

$$[a]_{\sim} = [a] = a^{\sim} = \bar{a} = \{b \in A \mid a \sim b\}$$

#### Osservazione

- Siccome  $\sim$  è una relazione di equivalenza è riflessiva, quindi  $\forall a \in A, a \in [a]_{\sim}$ . In particolare nessuna classe d'equivalenza è vuota.
- Per la simmetria,  $b \in [a]_{\sim} \Rightarrow a \in [b]_{\sim}$ .
- La definizione non è strettamente legata alle relazioni di equivalenza, ma ha senso studiarle solo in questo caso.

#### Esempi

"="  $[a]_{\sim}$  è  $\{a\}$

"stessa ordinata"  $[P]_{\sim}$  è la retta orizzontale passante per  $P$

"stessa cardinalità" con  $A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ :

- $[\emptyset]_{\sim} = \{\emptyset\}$
- $[\{a\}]_{\sim} = \{\{a\}, \{b\}\}$
- $[\{b\}]_{\sim} = \{\{a\}, \{b\}\}$
- $[\{a, b\}]_{\sim} = \{\{a, b\}\}$

**Proposizione** Sia  $A$  un insieme e sia  $\sim$  una relazione di equivalenza su  $A$ . Siano  $a \in A, b \in A \Rightarrow$ :

1.  $a \sim b \Leftrightarrow [a]_{\sim} = [b]_{\sim}$
2.  $[a]_{\sim} \neq [b]_{\sim} \Leftrightarrow [a]_{\sim} \cap [b]_{\sim} = \emptyset$

#### Dimostrazione

**1 ( $\Leftarrow$ )** Siccome  $b \in [b]_{\sim}$  e  $[b]_{\sim} = [a]_{\sim}, b \in [a]_{\sim}$  quindi  $a \sim b$ .

**1 ( $\Rightarrow$ )** Supponiamo  $a \sim b$ . Vogliamo dimostrare che  $[a]_{\sim} = [b]_{\sim}$  dimostrando che  $[a]_{\sim} \subseteq [b]_{\sim}$  e  $[b]_{\sim} \subseteq [a]_{\sim}$ .

Sia  $c \in [b]_{\sim} \Rightarrow b \sim c$ ; siccome  $\sim$  è transitiva,  $a \sim c$ , cioè  $c \in [a]_{\sim}$  quindi  $[b]_{\sim} \subseteq [a]_{\sim}$ .

Siccome  $\sim$  è simmetrica si può dimostrare la seconda parte in modo analogo, quindi  $[a]_{\sim} = [b]_{\sim}$ .

**2 ( $\Leftarrow$ )** Immediato perché  $a \in [a]_{\sim}, [a]_{\sim} \cap [b]_{\sim} = \emptyset \Rightarrow a \notin [b]_{\sim} \Rightarrow [a]_{\sim} \neq [b]_{\sim}$ .

**2 ( $\Rightarrow$ )** Facciamo la dimostrazione contrapposta, cioè che se  $[a]_{\sim} \cap [b]_{\sim} \neq \emptyset \Rightarrow [a]_{\sim} = [b]_{\sim}$ .

Se  $[a]_{\sim} \cap [b]_{\sim} \neq \emptyset, \exists c \in [a]_{\sim} \cap [b]_{\sim} \Rightarrow a \sim c$  e  $b \sim c$ , cioè  $a \sim c$  e  $c \sim b \Rightarrow a \sim b \Rightarrow$  dalla (1)  $[a]_{\sim} = [b]_{\sim}$ .

### Osservazione

- La relazione di equivalenza suddivide  $A$  in un certo numero di “pacchetti”, le classi di equivalenza.
- Due elementi sono in relazione se e solo se condividono una certa proprietà.

### 1.4.2. Insieme quoziente

Ciascuna delle classi di equivalenza è un sottoinsieme di  $A$ , quindi un elemento di  $\mathcal{P}(A)$ .

### Definizione

- Sia  $A$  un insieme e  $\sim$  una relazione di equivalenza su  $A$ . L'*insieme quoziente* di  $A$  per  $\sim$  è  $A/\sim = \{[a]_{\sim} \mid a \in A\}$ . ( $A/\sim \subseteq \mathcal{P}(A)$ )
- L'applicazione  $\pi_{\sim}$ :

$$\begin{aligned} A &\rightarrow A/\sim \\ a &\mapsto \pi_{\sim}(a) = [a]_{\sim} \end{aligned}$$

si chiama *proiezione canonica* da  $A$  su  $A/\sim$ .

### Esempi

- “=”
  - $A/\sim = \{\{a\}, \{b\}, \dots\}$
  - $\pi_{\sim}(a) = \{a\}$
- “stessa ordinata”
  - $\text{piano}/\sim = \{\text{rette orizzontali}\}$
  - $\pi_{\sim}(P) = \text{retta orizzontale passante per } P$
- “stesso cardinale” con  $A = \mathcal{P}(\{a, b\})$ 
  - $A/\sim = \{\{\emptyset\}, \{\{a\}, \{b\}\}, \{a, b\}\}$
  - $\pi_{\sim}(\emptyset) = \{\emptyset\}$ ,  $\pi_{\sim}(\{a\}) = \pi_{\sim}(\{b\}) = \{\{a\}, \{b\}\}$  e  $\pi_{\sim}(\{a, b\}) = \{a, b\}$

**Definizione** Sia  $A$  un insieme e  $F$  un sottoinsieme di  $\mathcal{P}(A)$ . Si dice che  $F$  è una *partizione* di  $A$  se e solo se:

1.  $\emptyset \notin F$
2.  $\bigcup_{X \in F} X = A$  (ciascun elemento di  $A$  sta in almeno un elemento di  $F$ )
3.  $\forall X \in F, \forall Y \in F$ , se  $X \neq Y \Rightarrow X \cap Y = \emptyset$  (un elemento di  $A$  non sta in due elementi diversi di  $F$ )

### Osservazione

- L'insieme quoziente è una partizione.
- Ogni relazione di equivalenza definisce una partizione dell'insieme su cui è definita.
- Un insieme vuoto non può avere nessuna partizione perchè  $\mathcal{P}(\emptyset) = \{\emptyset\}$  e quindi l'unico sottoinsieme di  $\mathcal{P}(\emptyset)$  che non vada contro la (1) della definizione è l'insieme vuoto stesso, ma questo contraddice la (2) della definizione.

## 1. Relazioni su un insieme

**Proposizione** Sia  $A$  un insieme non vuoto e  $F$  una partizione di  $A$  allora esiste una relazione di equivalenza  $\sim_F$ , con  $A/\sim_F = F$ .

$$\sim_F = \{(a, b) \in A \times A \mid \exists X \in F \mid a \in X \text{ e } b \in X\}$$

**Dimostrazione** Bisogna mostrare che  $\sim_F$  è un'equivalenza e  $A/\sim_F = F$ . Per comodità al posto di  $\sim_F$  scriviamo  $\sim$ .

- R Sia  $a \in A$ , dalla (2) della definizione di partizione,  $\exists X \in F$  tale che  $a \in X$  e dalla definizione di  $\sim$ ,  $a \sim a$ .
- S Siano  $a \in A, b \in A$  tali che  $a \sim b$ . Quindi  $\exists X \in F$  tale che  $a \in X$  e  $b \in X$ . Quindi  $b \in X$  e  $a \in X$ . Quindi  $b \sim a$ .  
Dato che non c'è stato bisogno di sfruttare il fatto che  $F$  è una partizione per dimostrare la simmetria si dice che è simmetrica per definizione.
- T Siano  $a, b, c \in A$  tali che  $a \sim b$  e  $b \sim c$ , allora  $\exists X \in F$  tale che  $a \in X$  e  $b \in X$ ,  $\exists Y \in F$  tale che  $b \in Y$  e  $c \in Y$ .  
Dato che  $b \in X$  e  $b \in Y$  allora  $X \cap Y \neq \emptyset$ .  
Se  $X \neq Y$  allora per il punto (3) della definizione di partizione varrebbe che  $X \cap Y = \emptyset$  e quindi si creerebbe una contraddizione, quindi  $X = Y$ .  
Quindi  $a \in X$  e  $c \in X$ , perciò  $a \sim c$  e quindi  $\sim$  è transitiva.

Quindi  $\sim$  è un'equivalenza.

Inoltre bisogna dimostrare che  $A/\sim = F$ .

sia  $a \in A$ , allora  $[a]_{\sim} = \{b \in A \mid a \sim b\} = \{b \in A \mid \exists X \in F \mid a \in X \text{ e } b \in X\}$ .

Essendo  $F$  una partizione esiste un solo insieme  $X$  che contiene  $a$  quindi  $[a]_{\sim} = X$ , con  $X \in F$  e  $a \in X$ . Quindi ogni elemento di  $A$  ha la classe di equivalenza in  $F$  e quindi  $A/\sim \subseteq F$ .

Sia  $Y \in F$  allora  $\exists b \in A$  tale che  $b \in Y$  quindi  $[b]_{\sim} = Y$  per ciò che è stato detto prima, quindi tutti gli elementi di  $F$  sono una classe di equivalenza e quindi  $F \subseteq A/\sim$  e quindi  $A/\sim = F$ .

### 1.4.3. Congruenza modulo $n$

**Definizione** Siano  $a, b, n \in \mathbb{Z}$ . Si dice che “ $a$ ” è **congruo a “ $b$ ” modulo  $n$**  se e solo se  $n \mid b - a$ , cioè se e solo se  $\exists k \in \mathbb{Z}$  tale che  $b = a + k \cdot n$ .

In tal caso si denota:  $a \equiv_n b$ ,  $a \equiv b$ ,  $a \equiv b \pmod{n}$ ,  $a \equiv b \text{ mod } n$ .

**Proposizione**  $\forall n \in \mathbb{Z}$ ,  $\equiv_n$  è una relazione di equivalenza.

**Dimostrazione** Sia  $n \in \mathbb{Z}$ .

- R Sia  $a \in \mathbb{Z}$ , con  $k = 0$  otteniamo  $a = a + 0 \cdot n = a$  e quindi  $a \equiv_n a$ .
- S Siano  $a, b \in \mathbb{Z}$  tali che  $a \equiv_n b$  e quindi  $\exists k \in \mathbb{Z}$  tali che  $b = a + kn$ , allora  $a = b - kn = b + (-k)n$ ,  $(-k) \in \mathbb{Z}$  e quindi  $b \equiv_n a$ , quindi  $\equiv_n$  è simmetrica.
- T Siano  $a, b, c \in \mathbb{Z}$  tali che  $a \equiv_n b$  e  $b \equiv_n c \Rightarrow \exists k, l$  tali che  $b = a + kn$  e  $c = b + ln$ .  
 $c = a + kn + ln = a + (k + l)n$ . Siccome  $(k + l) \in \mathbb{Z}$ ,  $c \equiv_n a$ . Quindi  $\equiv_n$  è transitiva.

Quindi  $\equiv_n$  è un'equivalenza.

## 1. Relazioni su un insieme

**Osservazione** Dato  $a \in \mathbb{Z}$ :

- $[a]_{\equiv_n} = \{\dots, a - 2n, a - n, a, a + n, a + 2n, \dots\}$
- $[a]_{\equiv_0} = \{a\}$ , quindi  $\equiv_0$  è  $=$
- $[a]_{\equiv_1} = \mathbb{Z}$ , quindi  $\forall a, b \in \mathbb{Z}, a \equiv_1 b$

**Osservazione** Siano  $n \in \mathbb{Z}$  e  $m = -n$ ,  $[a]_m = [a]_n$  ovvero  $\equiv_m$  e  $\equiv_n$  sono la stessa relazione. Supporremo sempre (implicitamente)  $n \geq 0$ .

**Definizione** Sia  $n \in \mathbb{N}$ , con  $n \neq 0$ , e  $a \in \mathbb{Z}$ , allora si definisce **classe di resto** della divisione euclidea di  $a$  per  $n$  l'insieme di tutti i numeri interi che divisi per  $n$  danno resto  $a$  e si indica con:

$$[a]_n = \{x \in \mathbb{Z} \mid x = nq + a\}.$$

**Proposizione** Sia  $n \in \mathbb{N}$  con  $n \geq 1$  e  $a \in \mathbb{Z}$ , allora  $[a]_n = [a]_{\equiv_n}$ .

**Dimostrazione** Per dimostrare che 2 insiemi sono uguali bisogna dimostrare che  $[a]_n \subseteq [a]_{\equiv_n}$  e  $[a]_{\equiv_n} \subseteq [a]_n$ .

- $[a]_n \subseteq [a]_{\equiv_n}$   
Sia  $x \in [a]_n$  allora per la divisione euclidea si ha  $x = qn + a$  dove  $q$  è il quoziente e  $a$  il resto.  
Allora  $a \equiv_n x \Rightarrow x \in [a]_{\equiv_n} \Rightarrow [a]_n \subseteq [a]_{\equiv_n}$ .
- $[a]_{\equiv_n} \subseteq [a]_n$   
Sia  $x \in [a]_{\equiv_n}$  allora  $a \equiv_n x \Rightarrow \exists k \in \mathbb{Z}$  tale che  $x = kn + a$   
Quindi per la divisione euclidea il quoziente è  $k$  e il resto è  $a$ , quindi  $x \in [a]_n \Rightarrow [a]_{\equiv_n} \subseteq [a]_n$ .

**Definizione** Sia  $n \in \mathbb{Z}$ , allora l'insieme quoziente  $\mathbb{Z}/\equiv_n$  è detto **insieme delle classi di resto modulo  $n$** , e si indica con  $\mathbb{Z}/n\mathbb{Z}$ .

**Osservazione**  $\mathbb{Z}/0\mathbb{Z}$  ha infiniti elementi, ma tutti con un solo elemento dato che:

$$[a]_0 = [a]_{\equiv_0} = \{a\} \Rightarrow \mathbb{Z}/0\mathbb{Z} = \{\{0\}, \{1\}, \dots\}$$

**Proposizione** Se  $n \geq 1$ ,  $\mathbb{Z}/n\mathbb{Z}$  ha  $n$  elementi.

**Dimostrazione** Per la definizione di divisione euclidea il resto può valere solo  $n$  valori, infatti:  $0 \leq r \leq n - 1$ . Quindi possono esserci massimo  $n$  classi di resto.

Si deve ora verificare che ci siano esattamente  $n$  classi di resto, verificando che dati 2 resti con la stessa classe si ottiene che i 2 resti sono uguali, e quindi gli  $n$  resti danno  $n$  classi distinte.

Se  $r_1$  e  $r_2$  sono tali che  $0 \leq r_1 \leq n - 1$ ,  $0 \leq r_2 \leq n - 1$ ,  $[r_1]_n = [r_2]_n$  cioè  $\exists k \in \mathbb{Z}$  tale che  $r = r_1 + kn$  ( $r_2 - r_1 = kn$ ).

$$0 \leq r_2 \leq n - 1, 1 - n \leq -r_1 \leq 0$$

$$1 - n \leq r_2 - r_1 \leq n - 1$$

$$1 - n \leq kn \leq n - 1$$

Siccome  $k \in \mathbb{Z}$ :

- se  $k \geq 1 \Rightarrow kn \geq n > n - 1$ ;
- se  $k \leq -1 \Rightarrow kn \leq -n < 1 - n$ ;

quindi  $k$  è per forza uguale a 0, di conseguenza  $r_2 = r_1$ .

Quindi ci sono esattamente  $n$  classi.

### Esempi

- $\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$
- $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$

### 1.4.4. Rappresentanti e buona definizione

#### Definizione

- Sia  $A$  un insieme,  $\sim$  un'equivalenza su  $A$  e  $C$  una classe di equivalenza per  $\sim$ . Ogni  $a \in C$  si chiama **rappresentante** di  $C$  (quindi  $C = [a]_\sim$  se e solo se  $a$  è un rappresentante di  $C$ ).
- Un sottoinsieme  $R$  di  $A$  tale che ogni classe di  $A$  per  $\sim$  abbia un unico elemento in  $R$  si chiama **sistema completo di rappresentanti** per  $\sim$ .

### Esempi

- "stessa ordinata":
  - un rappresentante della classe "retta  $y = 3$ " è un qualsiasi punto che si trovi sulla retta, come  $P_1(-1, 3)$ , o  $P_2(7, 3)$
  - un sistema completo di rappresentanti è l'asse  $y$ , oppure "retta  $x = 2$ ", oppure la curva  $y = x^3$ ; invece non vanno bene:
    - \*  $y = \arctan x$  perché  $\forall x \in \mathbb{R}, -\pi/2 < y < \pi/2$ , quindi non contiene un rappresentante per ogni classe
    - \*  $y = x^3 - 3x$  perché contiene, per alcune classi, più di un rappresentante
- $\equiv_n, n \geq 1$ :
  - $[7]_{18}$  ammette rappresentanti  $7, 25, 43, -11, -29, \dots$
  - Un sistema completo di rappresentanti per  $\mathbb{Z}/n\mathbb{Z}$  è  $\{0, 1, \dots, n-1\}$  o  $\{n, n+1, \dots, 2n-1\}$
  - Un sistema completo di rappresentanti per  $\mathbb{Z}/(2n)\mathbb{Z}$  è  $\{-n+1, -n+2, \dots, -1, 0, 1, \dots, n-1, n\}$
  - Un sistema completo di rappresentanti per  $\mathbb{Z}/(2n+1)\mathbb{Z}$  è  $\{-n, -n+1, \dots, -1, 0, 1, \dots, n-1, n\}$

**Funzioni mal definite** Quando si definiscono delle funzioni tra classi di resto bisogna stare attenti ai rappresentanti usati. Ad esempio:

$$g: \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$$

$$[a]_2 \mapsto g([a]_2) = [2a]_3$$

non è ben definita perché:

$$[0]_2 = [2]_2$$

$$g([0]_2) = [2 \cdot 0]_3 = [0]_3$$

$$g([2]_2) = [2 \cdot 2]_3 = [4]_3 = [1]_3 \neq [0]_3$$

Quindi per uno stesso valore del dominio otteniamo 2 valori del codominio e quindi questa funzione è mal definita.

Questo succede perché per calcolare  $g([0]_2)$  usiamo un rappresentante di  $[a]_2$ , e se si cambia il rappresentante cambia il risultato.

## 1. Relazioni su un insieme

### 1.4.5. Somma e prodotto in $\mathbb{Z}/n\mathbb{Z}$

**Proposizione** Siano  $a, b, c, d, n \in \mathbb{Z}$  tali che  $a \equiv_n c$  e  $b \equiv_n d$  (cioè  $[a]_n = [c]_n$  e  $[b]_n = [d]_n$ ), allora:

- $a + b \equiv_n c + d$  (cioè  $[a + b]_n = [c + d]_n$ );
- $ab \equiv_n cd$  (cioè  $[ab]_n = [cd]_n$ ).

**Dimostrazione** Esistono  $k, l \in \mathbb{Z}$  tali che  $c = a + kn$  e  $d = b + ln$ . Allora:

- $c + d = a + b + (k + l)n$ ,  $(k + l) \in \mathbb{Z} \Rightarrow a + b \equiv_n c + d$ ;
- $cd = ab + bkn + aln + kln^2 = ab + (kb + al + kln)n$ ,  $(kb + al + kln) \in \mathbb{Z} \Rightarrow cd \equiv_n ab$ .

**Definizione** Siano  $a, b, n \in \mathbb{Z}$  allora:

- $[a]_n + [b]_n = [a + b]_n$ ;
- $[a]_n \cdot [b]_n = [ab]_n$ .

**Osservazione**  $[a + b]_n$  e  $[a \cdot b]_n$  sono insiemi ben definiti per la proposizione di prima, quindi ha senso definire tale somma e prodotto.

- $[0]_n + [a]_n = [a]_n$
- $[0]_n \cdot [a]_n = [0]_n$
- $[1]_n \cdot [a]_n = [a]_n$

Può capitare che con  $a \neq 0$  e  $b \neq 0$ ,  $[a]_n \cdot [b]_n = [0]_n$ , quando  $a \cdot b = 0 + k \cdot n = k \cdot n$  con  $k \in \mathbb{Z}$  quindi quando il prodotto è multiplo di  $n$ .

## 1.5. Relazioni di ordine

### 1.5.1. Ordine totale

**Definizione** Sia  $A$  un insieme e  $\preceq$  una relazione di ordine su  $A$ , si dice che l'**ordine**  $\preceq$  è **totale** se e solo se  $\forall a, b \in A$ ,  $a \preceq b$  o  $b \preceq a$ .

#### Esempi

- $\leq$  su  $\mathbb{R}$  è totale
- $\subseteq$  su  $\mathcal{P}(X)$  non è (in generale) totale. Se  $a = \{x, z\}$ ,  $b = \{y, z\}$ , con  $x \neq y$ ,  $y \neq z$ ,  $z \neq x$  non è vero che  $a \subseteq b$  e non è vero che  $b \subseteq a$
- $|$  su  $\mathbb{N}$  non è un ordine totale ( $6 \nmid 15$  e  $15 \nmid 6$ )

### 1.5.2. Estremanti

Sia  $A$  un insieme,  $\preceq$  una relazione di ordine su  $A$  ed  $E$  un sottoinsieme di  $A$ .

**Definizione**

- Un elemento  $M$  di  $E$  si dice **massimo** di  $E$  se e solo se  $\forall a \in E, a \preceq M$ .
- Un elemento  $m$  di  $E$  si dice **minimo** di  $E$  se e solo se  $\forall a \in E, m \preceq a$ .
- Un elemento  $M$  di  $A$  si dice **maggiorante** di  $E$  se e solo se  $\forall a \in E, a \preceq M$ .
- Un elemento  $m$  di  $A$  si dice **minorante** di  $E$  se e solo se  $\forall a \in E, m \preceq a$ .
- L'**estremo superiore** di  $E$  è, se esiste, il minimo dei suoi maggioranti.
- L'**estremo inferiore** di  $E$  è, se esiste, il massimo dei suoi minoranti.
- Un elemento  $M$  di  $E$  si dice **massimale** di  $E$  se e solo se l'unico elemento  $a \in E$  tale che  $M \preceq a$  è  $a = M$ .
- Un elemento  $m$  di  $E$  si dice **minimale** di  $E$  se e solo se l'unico elemento  $a \in E$  tale che  $a \preceq m$  è  $a = m$ .

**Osservazione** Negli ordini totali i massimi sono anche i massimali e viceversa.

**Proposizione**

- Se esiste un massimo è unico.
- Se esiste un minimo è unico.

**Dimostrazione** Supponiamo che  $M_1$  e  $M_2$  siano massimi per  $E$ , allora:

- $M_1$  è massimo:  $M_2 \in E \Rightarrow M_2 \preceq M_1$ ;
- $M_2$  è massimo:  $M_1 \in E \Rightarrow M_1 \preceq M_2$ .

Ma  $\preceq$  è antisimmetrica quindi  $M_1 = M_2$ .

La dimostrazione per il minimo è analoga.

**Osservazione** Dato che l'estremo superiore (inferiore) è definito come un minimo (massimo) è anch'esso unico.

**Proposizione**

- Se c'è un massimo è l'unico elemento massimale.
- Se c'è un minimo è l'unico elemento minimale.

**Dimostrazione** Sia  $M$  il massimo di  $E, \Rightarrow \forall a \in E a \preceq M$ .

Siano  $M_1$  e  $M_2$  massimali di  $E$ , allora se  $a \in E$ :

- Se  $M_1 \preceq a \Rightarrow M_1 = a$ ;
- se  $M_2 \preceq a \Rightarrow M_2 = a$ ,

Quindi dato che  $M \in E$ :

- $M_1 \preceq M \Rightarrow M_1 = M$ ;
- $M_2 \preceq M \Rightarrow M_2 = M$ ;

$\Rightarrow M_1 = M_2 = M$ .

La dimostrazione per il minimale è analoga.

## 1. Relazioni su un insieme

### Proposizione

- Se  $c$  è un massimo allora è anche l'estremo superiore.
- Se  $c$  è un minimo allora è anche l'estremo inferiore.

**Dimostrazione** Sia  $M$  il massimo di  $E$ ,  $\Rightarrow \forall a \in E, a \preceq M$ .

Quindi  $M$  è anche un maggiorante, inoltre dato che tutti gli elementi dell'insieme sono “minori” del massimo gli altri maggioranti sono per forza “maggiori” del massimo, quindi  $M$  è il minimo dei maggioranti e quindi è l'estremo superiore.

La dimostrazione per l'estremo inferiore è analoga.

### 1.5.3. Reticolo

**Definizione** Un *reticolo* è una coppia  $(E, \rho)$  dove  $E$  è un insieme e  $\rho$  è una relazione d'ordine su  $E$  tale che  $\forall a \in E, b \in E, \{a, b\}$  ha un estremo superiore e un estremo inferiore per  $\rho$ .

Se  $(E, \rho)$  è un reticolo, per  $(a, b) \in E^2$  denotiamo:

- $\inf(a, b) = a \wedge b = \inf \{a, b\}$ ;
- $\sup(a, b) = a \vee b = \sup \{a, b\}$ .

### 1.5.4. Proprietà dei reticoli

**Proposizione** Sia  $(E, \rho)$  un reticolo. Valgono:

1. **Idempotenza:**  $\forall a \in E, a \vee a = a \wedge a = a$ .
2. **Commutatività:**  $\forall a, b \in E, a \vee b = b \vee a, a \wedge b = b \wedge a$ .
3. **Associatività:**  $\forall a, b, c \in E, (a \vee b) \vee c = a \vee (b \vee c) = \sup \{a, b, c\}, (a \wedge b) \wedge c = a \wedge (b \wedge c) = \inf \{a, b, c\}$ .

**Definizione** Sia  $(E, \rho)$  un reticolo. Il reticolo  $(E, \rho)$  si dice *limitato* se e solo se esistono il massimo  $I$  e il minimo  $O$  di  $E$  per  $\rho$ .

**Proposizione** Se  $(E, \rho)$  è limitato,  $\forall a \in E$  valgono:

- $O \vee a = a$  e  $O \wedge a = O$ ;
- $I \vee a = I$  e  $I \wedge a = a$ .

**Definizione** Sia  $(E, \rho)$  un reticolo limitato e  $a \in E$ , allora se esiste  $b \in E$  tale che  $a \vee b = I$  e  $a \wedge b = O$  l'elemento  $b$  si dice *complemento* di  $a$ .

Se tutti gli elementi di  $E$  hanno un complemento il reticolo si dice *complementato*.

**Teorema** Il reticolo  $(\mathbb{N}, |)$  è un reticolo limitato.

**Dimostrazione** È chiaro che 1 è il minimo e 0 è il massimo di  $\mathbb{N}$  per  $|$ .

Siano  $a, b \in \mathbb{N}$ . Allora i maggioranti di  $\{a, b\}$  saranno gli elementi divisibili sia per  $a$  che per  $b$ , cioè i multipli comuni di  $a$  e  $b$ . Quindi  $a \wedge b = mcm(a, b)$ .

Per l'inf e i minoranti è lo stesso: i minoranti sono i divisori comuni e quindi  $a \vee b = MCD(a, b)$ .

La definizione rigorosa e la dimostrazione dell'esistenza di  $mcm$  e  $MCD$  è trattata più avanti, per questa dimostrazione basta il significato intuitivo.



## 2. Strutture algebriche

### 2.1. Leggi di composizione

#### 2.1.1. Definizione

Sia  $E$  un insieme. Una *legge di composizione interna* su  $E$  (o *lci*, *legge di composizione*, *legge di composizione binaria*, *operazione*, ...) è un'applicazione da  $E \times E$  in  $E$ .

Se  $\star$  è lci su  $E$  e  $a, b \in E$ ,  $\star(a, b)$  si scrive  $a \star b$ .

#### Esempi

- $+$ ,  $\cdot$  su  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , matrici (quadrate per il  $\cdot$ ) e  $\mathbb{Z}/n\mathbb{Z}$
- $-$  su  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , matrici e  $\mathbb{Z}/n\mathbb{Z}$
- $/$  su  $\{\pm 1\}$ ,  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$ ,  $\mathbb{C}^{*I}$
- $\cap$ ,  $\cup$  su  $\mathcal{P}(X)$
- $\circ^{\text{II}}$  su  $\text{appl}(X, X)$ ,  $\text{iniez}(X, X)$ ,  $\text{suriez}(X, X)$ ,  $\text{biez}(X, X)$ , crescenti in  $(\mathbb{R}, \mathbb{R})$
- $\wedge$ ,  $\vee$  su un reticolo  $(E, \rho)$

Non sono lci:

- $-$  su  $\mathbb{N}$ , perchè dati 2 elementi in  $\mathbb{N}$  non è detto che si possa fare la sottrazione
- $/$  su  $\mathbb{N}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , perchè la divisione su 0 non è definita
- $\circ$  su decrescenti in  $(\mathbb{R}, \mathbb{R})$  perchè la composizione tra 2 funzioni decrescenti forma una funzione crescente

#### 2.1.2. Proprietà

**Definizione** Sia  $E$  un insieme e  $\star$  una lci su  $E$ .

- La lci  $\star$  è detta **commutativa** se e solo se  $\forall a \in E, \forall b \in E, a \star b = b \star a$ .
- La lci  $\star$  è detta **associativa** se e solo se  $\forall a \in E, \forall b \in E, \forall c \in E, (a \star b) \star c = a \star (b \star c)$ .
- L'elemento  $e \in E$  si dice **neutro** o **unità** per  $\star$  se e solo se  $\forall a \in E, a \star e = e \star a = a$ .
- L'elemento  $z \in E$  si dice **elemento assorbente** per  $\star$  se e solo se  $\forall a \in E, a \star z = z \star a = z$ .
- Se  $e$  è un neutro per  $\star$  e  $a \in E$ , un elemento  $b \in E$  tale che  $a \star b = b \star a = e$  si dice **inverso** o **simmetrico** di  $a$  per  $\star$ .  
Si denota  $a^{-1}$ . Se  $\exists$  un tale  $b$ ,  $a$  si dice **invertibile**.
- Se  $\star$  ammette un neutro in  $E$ , allora l'insieme degli elementi invertibili per  $\star$  si indica  $E^*$ .

<sup>I</sup>L'asterisco come apice indica che l'insieme viene preso escludendo lo 0; successivamente questo concetto viene spiegato meglio.

<sup>II</sup>Il simbolo " $\circ$ " indica la composizione di funzioni.

## 2. Strutture algebriche

### Esempi

LCI	Insieme di definizione	Comm.	Ass.	Neutro	Assorbente	Inverso di a
+	$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ , matrici, $\mathbb{Z}/n\mathbb{Z}$	Sì	Sì	0	Nessuno	-a
$\cdot$	$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$	Sì	Sì	1	0	$\frac{1}{a}$
$\cdot$	Matrici $n \times n$	No	Sì	$I_n$	Matrice nulla	Matrice inversa
—	$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	No	No	Nessuno	Nessuno	—
$\cup$	$\mathcal{P}(X)$	Sì	Sì	$\emptyset$	$X$	Non c'è
$\cap$	$\mathcal{P}(X)$	Sì	Sì	$X$	$\emptyset$	Non c'è
$\circ$	Funzioni $\mathbb{R} \rightarrow \mathbb{R}$	No	Sì	$id(x) = x$	Funzione nulla	Funzione inversa
$\wedge$	Reticolo non limitato $(E, \rho)$	Sì	Sì	Nessuno	Nessuno	—
$\vee$	Reticolo non limitato $(E, \rho)$	Sì	Sì	Nessuno	Nessuno	—
$\wedge$	Reticolo limitato $(E, \rho)$	Sì	Sì	$O$	$I$	Complemento
$\vee$	Reticolo limitato $(E, \rho)$	Sì	Sì	$I$	$O$	Complemento

**Proposizione** Sia  $E$  un insieme e  $\star$  una lci su  $E$ , se esiste un neutro per  $\star$  è unico.

**Dimostrazione** Siano  $e_1, e_2$  due neutri per  $\star$ . Allora:

- $e_1 \star e_2 = e_2$  perché  $e_1$  è neutro;
- $e_1 \star e_2 = e_1$  perché  $e_2$  è neutro;

$\Rightarrow e_1 = e_2$ .

**Proposizione** Sia  $E$  un insieme e  $\star$  una lci su  $E$ , se esiste un elemento assorbente per  $\star$  è unico.

**Dimostrazione** Siano  $z_1, z_2$  due elementi assorbenti per  $\star$ . Allora:

- $z_1 \star z_2 = z_1$  perché  $z_1$  è assorbente;
- $z_1 \star z_2 = z_2$  perché  $z_2$  è assorbente;

$\Rightarrow z_1 = z_2$ .

**Proposizione** Sia  $E$  un insieme e  $\star$  una lci associativa su  $E$ , se un elemento ammette un inverso e  $\star$  è associativa allora detto inverso è unico.

**Dimostrazione** Supponiamo  $e$  neutro,  $\star$  associativa,  $a \in E$  e  $b_1$  e  $b_2$  inversi di  $a$ , allora:

- $b_1 \star (a \star b_2) = b_1 \star e = b_1$ ;
- $b_1 \star (a \star b_2) = (b_1 \star a) \star b_2 = e \star b_2 = b_2$ ;

$\Rightarrow b_1 = b_2$ .

### Definizione

- Sia  $E$  un insieme e  $k \geq 0$  intero. Un'**operazione di arità  $k$**  su  $E$  è un'applicazione da  $E^k$  in  $E$  (per  $k = 0$  si tratta delle costanti, cioè degli elementi di  $E$ ).
- Una **struttura algebrica** è una  $(n + 1)$ -upla  $(E, \star_1, \dots, \star_n)$  dove  $E$  è un insieme e ciascuna  $\star$  è un'operazione di arità  $k \geq 0$  su  $E$ .

### Esempi

- Le *lci* sono operazioni di arità 2
- Il simmetrico è un'operazione di arità 1
- Il neutro è un'operazione di arità 0
- $(\mathbb{R}, +, \cdot, 0, 1, -, ^{-1})$  è una struttura algebrica dove:
  - $\mathbb{R}$  è l'insieme di definizione
  - $+$  è la *lci* della somma tra reali e quindi ha arità 2
  - $\cdot$  è la *lci* del prodotto tra reali e quindi ha arità 2
  - $0$  è una costante (il neutro della somma) e quindi ha arità 0
  - $1$  è una costante (il neutro della moltiplicazione) e quindi ha arità 0
  - $-$  è l'operazione che restituisce il simmetrico della somma e quindi ha arità 1
  - $^{-1}$  è l'operazione che restituisce il simmetrico della moltiplicazione e quindi ha arità 1

Questa struttura è un campo come verrà spiegato in seguito

## 2.2. Strutture con una lci

### 2.2.1. Base

**Definizione** Sia  $(E, \star)$  una struttura algebrica.

- Se  $\star$  è associativa,  $(E, \star)$  si dice **semigrupp**.
- Se  $\star$  è associativa e ammette un neutro,  $(E, \star)$  si dice **monoide**.
- Se  $\star$  è associativa, ammette un neutro e ogni elemento è invertibile,  $(E, \star)$  si dice **gruppo**.
- Se inoltre  $\star$  è commutativa si dice che  $(E, \star)$  è un semigrupp (rispettivamente monoide o gruppo) **abeliano** o **commutativo**. In quel caso si dice anche che la *lci* è **abeliana**.

### Esempi

- $(\text{appl}(X, X), \circ)$  è un monoide con neutro  $id_x$
- $\left( \begin{matrix} \mathbb{N} \\ \mathbb{Z} \\ \mathbb{Q} \\ \mathbb{R} \\ \mathbb{C} \end{matrix}, \begin{matrix} + \\ \cdot \end{matrix} \right)$  sono monoidi abeliani
- $\left( \begin{matrix} \mathbb{Z} \\ \mathbb{Q} \\ \mathbb{R} \\ \mathbb{C} \\ \mathbb{Z}/n\mathbb{Z} \end{matrix}, + \right)$  e  $\left( \begin{matrix} \mathbb{Q}^* \\ \mathbb{R}^* \\ \mathbb{C}^* \end{matrix}, \cdot \right)$  sono gruppi abeliani

## 2. Strutture algebriche

**Definizione** Sia  $(G, \star)$  un gruppo, il **centro** di  $(G, \star)$  è  $Z(G) = \{z \in G \mid \forall g \in G, z \star g = g \star z\}$ .

**Osservazione** Se  $(G, \star)$  è un gruppo abeliano allora  $Z(G) = G$ .

**Osservazione** Un monoide (e quindi un gruppo) non è mai vuoto perché contiene sempre almeno il neutro.

**Proposizione** Se  $(S, \star)$  è un monoide, allora  $(S^*, \star)$  è un gruppo.

**Dimostrazione** Per dimostrare che una struttura algebrica è un gruppo bisogna controllare se:

- $\star$  sia una lci in  $S^*$ , quindi se  $\forall a, b \in S^* \Rightarrow a \star b \in S^*$ :  
 $a \star b \in S^*$  se è invertibile, quindi bisogna capire se esiste tale inverso.  
Dato che  $a, b \in S^*$  allora esistono  $a^{-1}$  e  $b^{-1}$ . Inoltre  $(a \star b)^{-1} = b^{-1} \star a^{-1}$  infatti:  
$$\begin{aligned} - a \star b \star b^{-1} \star a^{-1} &= a \star e \star a^{-1} = a \star a^{-1} = e; \\ - b^{-1} \star a^{-1} \star a \star b &= b^{-1} \star e \star b = b^{-1} \star b = e; \end{aligned}$$
  
quindi l'inverso esiste e quindi  $a \star b \in S^*$ .
- $\star$  sia associativa, quindi se  $\forall a, b, c \in S^* \Rightarrow a \star (b \star c) = (a \star b) \star c$ :  
dato che  $\star$  è associativa in  $S$  lo è anche nel suo sottoinsieme  $S^*$ .
- $S^*$  contenga il neutro di  $\star$ :  
bisogna controllare se il neutro è invertibile, ma l'inverso del neutro è il neutro stesso:  $e \star e = e$ .
- $S^*$  contenga gli inversi per  $\star$  quindi se  $\forall a \in S^* \Rightarrow a^{-1} \in S^*$ :  
per la definizione di  $S^*$  se un elemento  $a \in S$  è invertibile allora  $a \in S^*$ , ma non si è sicuri che anche  $a^{-1} \in S^*$ .  
L'inverso di  $a^{-1}$  è  $a$  infatti:  
 $a \star a^{-1} = a^{-1} \star a = e$ .  
Quindi  $a^{-1} \in S^*$  e quindi tutti gli inversi appartengono a  $S^*$ .

**Notazione** Se  $(E, \star)$  è un monoide:

- $g^0 = e$  è il neutro;
- $\forall n \geq 0, g^{n+1} = g \star g^n$ ;
- se  $g$  è invertibile e  $n < 0, g^n = (g^{-1})^{-n}$ .

**Esempi**

- $(\mathbb{Z}, +)$ 
  - $g^0 = 0$
  - $g^1 = g + 0, g^2 = g + g = 2 \cdot g, g^n = \underbrace{g + \dots + g}_{n \text{ volte}} = n \cdot g$
  - $g^{-1} = -g, g^{-2} = -2 \cdot g, g^{-n} = \underbrace{(-g) + \dots + (-g)}_{n \text{ volte}} = -n \cdot g$
- $(\mathbb{Q}, \cdot)$

## 2. Strutture algebriche

$$\begin{aligned}
 - g^0 &= 1 \\
 - g^1 &= g \cdot 1, g^2 = g \cdot g, g^n = \underbrace{g \cdot \dots \cdot g}_{n \text{ volte}} \\
 - g^{-1} &= \frac{1}{g}, g^{-2} = \frac{1}{g} \cdot \frac{1}{g}, g^{-n} = \underbrace{\frac{1}{g} \cdot \dots \cdot \frac{1}{g}}_{n \text{ volte}}
 \end{aligned}$$

**Proposizione** Sia  $(E, \star)$  un monoide,  $g \in E$  e  $k, l \in \mathbb{Z}$ , allora se  $g$  è invertibile o  $k \geq 0$  e  $l \geq 0$ :

- $g^{k+l} = g^k \star g^l$ ;
- $g^{kl} = (g^k)^l$ .

Inoltre se  $(E, \star)$  è abeliano allora:

- $(g \star h)^k = g^k \star h^k$ .

### 2.2.2. Il monoide delle parole

**Definizione** Sia  $A$  un insieme non vuoto.

- Una **parola nell'alfabeto  $A$**  è una successione  $w = (w_1, \dots, w_n)$  finita di elementi di  $A$ . L'intero  $n$  si chiama **lunghezza** della parola  $w$  e si denota  $l(w)$ .  
La parola di lunghezza 0 è la parola  $\varepsilon = ()$  (indicata anche con  $\epsilon$ ) e si chiama **parola vuota**.  
L'insieme delle parole nell'alfabeto  $A$  si denota  $W(A)$

- Sia  $W(A)$  un insieme di parole e  $v, w \in W(A)$  con  $v = (v_1, \dots, v_m)$  e  $w = (w_1, \dots, w_n)$ .  
Si definisce la **lci concatenazione** di  $v$  e  $w$ :

$$x = v \circ w = (x_1, \dots, x_{m+n}) \text{ con } \begin{cases} x_i = v_i & 1 \leq i \leq m \\ x_i = w_{i-m} & m+1 \leq i \leq m+n \end{cases}$$

**Osservazione**  $(w_1, \dots, w_n)$  si scrive  $w_1 \dots w_n$  e  $v \circ w$  si scrive  $vw$ .

**Proposizione**  $(W(A), \circ)$  è un monoide di neutro  $\varepsilon$ .

**Dimostrazione** Che  $\circ$  sia interna è chiaro dalla definizione.

Che sia associativa è relativamente evidente:  $(vw)x$  e  $v(wx)$  sono i caratteri di  $v$  seguiti da quelli di  $w$  seguiti da quelli di  $x$ .

Che  $\varepsilon$  sia il neutro è abbastanza chiaro: non modifico la parola se antepongo o postpongo nessun carattere.

**Osservazione**  $l(vw) = l(v) + l(w)$  e quindi l'unico elemento invertibile è  $\varepsilon$ .

### 2.2.3. Sottogruppi

N.B.: se  $(E, \star_1, \dots, \star_n)$  è una struttura algebrica che si chiama un “coso” esiste la nozione di “sotto-coso”, un sottoinsieme  $V$  di  $E$  tale che  $(V, \star_1, \dots, \star_n)$  sia ancora un “coso”.

**Definizione** Sia  $(G, \star)$  un gruppo. Un **sottogruppo** di  $(G, \star)$  è un sottoinsieme  $H$  di  $G$  tale che:

1.  $H \neq \emptyset$ ;
2.  $\forall a \in H, b \in H, a \star b^{-1} \in H$ .

## 2. Strutture algebriche

**Proposizione** Se  $(G, \star)$  è un gruppo e  $H$  un suo sottogruppo allora  $(H, \star)$  è un gruppo.

**Dimostrazione** Per dimostrare che una struttura algebrica è un gruppo bisogna controllare se:

- $H$  contiene il neutro di  $\star$ :  
per la (1)  $\exists c \in H$ ;  
per la (2) con  $c = b = a$ ,  $c \star c^{-1} \in H \Rightarrow e \in H$ .
- $\star$  è associativa, quindi se  $\forall x, y, z \in H \Rightarrow x \star (y \star z) = x \star (y \star z)$ :  
dato che  $\star$  è associativa in  $G$ , allora è associativa in  $H$ .
- $H$  contiene gli inversi per  $\star$ , quindi se  $\forall x \in H \Rightarrow x^{-1} \in H$ :  
per la (2) con  $a = e$  e  $b = x$  si ottiene  $e \star x^{-1} \in H \Rightarrow x^{-1} \in H$ .
- $\star$  è una lci in  $H$ , quindi se  $\forall x, y \in H \Rightarrow x \star y \in H$ :  
per il punto prima  $x^{-1} \in H$  e  $y^{-1} \in H$  e usando la (2) con  $a = x$  e  $b = y^{-1}$  otteniamo:  
 $x \star (y^{-1})^{-1} \in H \Rightarrow x \star y \in H$ .

### 2.2.4. Gruppo quoziente

Sia  $(G, \star)$  un gruppo e  $H$  un suo sottogruppo. Definiamo su  $G$  due relazioni di equivalenza  $\lambda_H$  e  $\rho_H$ :  
 $\forall a \in G, \forall b \in G$ :

- $a \lambda_H b \Leftrightarrow \exists h \in H$  tale che  $b = h \star a$ <sup>III</sup>;
- $a \rho_H b \Leftrightarrow \exists h \in H$  tale che  $b = a \star h$ <sup>IV</sup>.

**Notazione** Se  $(G, \star)$  è un gruppo e  $H$  è un suo sottogruppo, allora:

- $G/\lambda_H = H \backslash G$ ; (notazione incerta)
- $G/\rho_H = G/H$ .

**Proposizione**  $\lambda_H$  e  $\rho_H$  sono relazioni di equivalenza.

**Dimostrazione** Per  $\lambda_H$ :

R Sia  $a \in G$ , e il neutro di  $\star \in H$ , quindi  $a = e \star a$  per  $e \in H$  e quindi  $a \lambda_H a$  è riflessiva.

S Siano  $a, b \in G$  tali che  $a \lambda_H b$ .  
Quindi  $\exists h \in H$  tale che  $b = h \star a$ .  
Se  $h \in H$ , allora  $h^{-1} \in H$ , quindi  $h^{-1} \star b = h^{-1} \star h \star a = e \star a = a$ .  
Quindi  $a = h^{-1} \star b$  con  $h^{-1} \in H$ , cioè  $b \lambda_H a$  e quindi  $\lambda_H$  è simmetrica.

T Siano  $a, b, c \in G$  tali che  $a \lambda_H b$  e  $b \lambda_H c$ .  
Quindi  $\exists h, k \in H$  tali che  $b = h \star a$  e  $c = k \star b = k \star h \star a$ .  
Dato che  $k \star h \in H$ ,  $a \lambda_H c$  e quindi  $\lambda_H$  è transitiva.

Per  $\rho_H$ :

R Sia  $a \in G$ , e il neutro di  $\star \in H$ , quindi  $a = a \star e$  per  $e \in H$  e quindi  $a \rho_H a$  è riflessiva.

<sup>III</sup>Si usa  $\lambda$  per indicare che la  $h$  va a sinistra (left).

<sup>IV</sup>Si usa  $\rho$  per indicare che la  $h$  va a destra (right).

## 2. Strutture algebriche

S Siano  $a, b \in G$  tali che  $a \rho_H b$ .  
 Quindi  $\exists h \in H$  tale che  $b = a \star h$ .  
 Se  $h \in H$ , allora  $h^{-1} \in H$ , quindi  $b \star h^{-1} = a \star h \star h^{-1} = a \star e = a$ .  
 Quindi  $a = b \star h^{-1}$  con  $h^{-1} \in H$ , cioè  $b \rho_H a$  e quindi  $\rho_H$  è simmetrica.

T Siano  $a, b, c \in H$  tali che  $a \rho_H b$  e  $b \rho_H c$ .  
 Quindi  $\exists h, k \in H$  tali che  $b = a \star h$  e  $c = b \star k = a \star h \star k$ .  
 Dato che  $h \star k \in H$ ,  $a \rho_H c$  e quindi  $\rho_H$  è transitiva.

**Attenzione** Gli insiemi quozienti  $G/\lambda_H$  e  $G/\rho_H$  non sono in generale gruppi per un'ipotetica *lci*  $[a]_{\lambda_H} \star [b]_{\lambda_H} = [a \star b]_{\lambda_H}$ . Anzi, questa legge non è ben definita.

**Definizione** Un sottogruppo  $H$  di  $(G, \star)$  è detto **normale** se e solo se  $\forall g \in G$  vale  $\{g \star h \star g^{-1} \mid h \in H\} = H$ .

### Osservazione

- Tutti i sottogruppi di gruppi abeliani sono normali dato che  $\forall g, h \in G$  vale:  
 $g \star h \star g^{-1} = g \star g^{-1} \star h = e \star h = h$ .
- Se  $H$  è un sottogruppo normale allora  $G/\lambda_H = G/\rho_H$ .
- Se  $H$  è un sottogruppo normale allora la *lci* definita come  $[a]_{\lambda_H} \star [b]_{\lambda_H} = [a \star b]_{\lambda_H}$  è ben definita.
- Se  $H$  è un sottogruppo normale allora  $(G/\lambda_H, \star) = (G/\rho_H, \star)$  è un gruppo.

## 2.3. Gruppi finiti

### 2.3.1. Elementi di ordine finito

**Definizione** Sia  $(E, \star)$  un monoide di neutro  $e$ . Un elemento  $g \in E$  si dice di **ordine finito** se e solo se  $\exists n > 0$  tale che  $g^n = e$ . In tal caso l'**ordine di  $g$**  si denota  $o(g)$  ed è il minimo  $n > 0$  tale che  $g^n = e$ . In caso contrario  $g$  si dice di **ordine infinito**.

**Osservazione** Sia  $(E, \star)$  un monoide di neutro  $e$ ,  $g \in E$  allora:  
 $g$  è di ordine finito se e solo se  $\exists n, m \in \mathbb{Z}$  tali che  $g^n = g^m$ .

**Dimostrazione** Per semplicità prendiamo  $n > m$  (il contrario sarebbe comunque analogo).

- $g$  di ordine finito  $\Rightarrow \exists n, m \in \mathbb{Z}$  tali che  $g^n = g^m$  :  
 mettendo  $n = o(g)$  e  $m = 0$  si ottiene  $g^{o(g)} = g^0 = e$  quindi l'affermazione è vera.
- Siano  $n, m \in \mathbb{Z}$  tali che  $g^n = g^m \Rightarrow g$  è di ordine finito:  
 $g^n \star (g^m)^{-1} = g^n \star (g^m)^{-1} \Rightarrow g^{n-m} = e$ , quindi  $g$  è di ordine finito.

**Proposizione** Sia  $(G, \star)$  un gruppo di neutro  $e$ . Se  $G$  ha un numero pari di elementi allora esiste  $g \in G$  tale che  $g \neq e \wedge g^2 = e$ .

**Dimostrazione** Sappiamo che l'inverso del neutro è il neutro stesso, perché  $e \star e = e$ .

Il fatto che  $G$  abbia un numero pari di elementi significa che esiste un altro elemento  $g \in G$  oltre al neutro tale che  $g^{-1} = g$ , perciò  $g^2 = g \star g = g \star g^{-1} = e$ .

## 2. Strutture algebriche

**Proposizione** Sia  $(E, \star)$  un monoide di neutro  $e$ ,  $g \in E$ , allora l'insieme  $Z_g = \{n \in \mathbb{Z} \mid g^n = e\}$  è un sottogruppo di  $(\mathbb{Z}, +)$ .

**Dimostrazione** Per dimostrare che  $Z_g$  è un sottogruppo di  $(\mathbb{Z}, +)$  bisogna controllare se:

1.  $Z_g \neq \emptyset$ :  
 $g^0 = e$  quindi  $0 \in Z_g \Rightarrow Z_g \neq \emptyset$ .
2.  $\forall a \in Z_g, b \in Z_g, a + b^{-1} \in Z_g \Rightarrow a - b \in Z_g$ :  
 siano  $a, b \in Z_g$  allora  $g^a = e$  e  $g^b = e$ .  
 $g^{a-b} = g^a \star g^{-b} = g^a \star (g^b)^{-1} = e \star e^{-1} = e \star e = e \Rightarrow a - b \in Z_g$ .

### Osservazione

- Dato che  $Z_g$  è un sottogruppo di  $(\mathbb{Z}, +)$  è anche un ideale di  $\mathbb{Z}^V$ .
- Dato che il numero più basso maggiore di 0 contenuto in  $Z_g$  è  $o(g)$  si ha:  $Z_g = (o(g))$ .
- $o(g)$  è il numero di elementi di  $\mathbb{Z}/Z_g$ , e rimane vero anche se  $g$  è di ordine infinito.
- Se  $g^n = e$  allora  $o(g) \mid n$ .
- $g = e$  se e solo se  $o(g) = 1$ .

**Attenzione** Sia  $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2) \mid ad - bc \neq 0 \right\}$  con lci il prodotto fra matrici. Allora  $(G, \times)$  è un gruppo.

Siano  $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  e  $h = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ .

- $g \times g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow o(g) = 4$
- $h \times h \times h = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow o(h) = 3$
- $k = g \times h = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$
- $k^2 = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$
- $k^3 = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ 0 & -1 \end{pmatrix}$
- per induzione:  $k^n = \begin{pmatrix} (-1)^n & (-1)^{n+1}n \\ 0 & (-1)^n \end{pmatrix} \neq I_2$  per  $n \neq 0$

Quindi  $g$  e  $h$  sono di ordine finito ma il loro prodotto non lo è.

Da questo esempio si può dedurre che se due elementi possiedono una certa proprietà, non è detto che anche il loro prodotto, o qualsiasi altro risultato di operazione su di essi, la possieda.

---

<sup>V</sup>Gli ideali di  $\mathbb{Z}$  verranno introdotti in seguito nel capitolo di Aritmetica.



### 2.3.2. Gruppi finiti

**Definizione** Un gruppo  $(G, \star)$  è **finito** se e solo se  $G$  è un insieme finito<sup>VI</sup>.

Se  $(G, \star)$  è un gruppo finito l'**ordine di  $G$**  è il numero di elementi di  $G$ ; si denota  $o(G)$ ,  $\#G$  o  $|G|$ .

**Osservazione** Se  $(E, \star)$  è un monoide e  $g \in E$  è di ordine finito,  $\langle g \rangle = \{g^n \mid n \in \mathbb{N}\}$  è un gruppo. L'elemento  $g$  è invertibile e il suo inverso è  $g^{o(g)-1}$ . Abbiamo visto che questo gruppo ha  $o(g)$  elementi, quindi in questo caso l'ordine di  $\langle g \rangle$  è l'ordine di  $g$ . È la ragione per cui si usa il termine ordine sia per il gruppo che per un elemento.

**Proposizione** Sia  $(G, \star)$  un gruppo finito e  $H$  un suo sottogruppo. Allora  $\#H \mid \#G$ .

**Dimostrazione** Ricordiamo la relazione di equivalenza  $\rho_H$ :  $\forall a, b \in G, a \rho_H b \Leftrightarrow \exists h \in H$  tale che  $b = a \star h$ .

Sia  $g \in G$ ,  $[g]_{\rho_H} = \{b \in G \mid \exists h \in H \mid b = g \star h\} = \{g \star h \mid h \in H\}$ . Essendo  $(G, \star)$  un gruppo,  $g \star h_1 = g \star h_2$  se e solo se  $h_1 = h_2$ .

Quindi  $[g]_{\rho_H}$  ha  $\#H$  elementi. Quindi, visto che l'insieme quoziente è sempre una partizione di  $G$ ,  $\#G = \#(G/\rho_H) \cdot \#H$ . Quindi  $\#G$  è un multiplo di  $\#H$ .

**Osservazione** Se  $(G, \star)$  è un gruppo finito allora ogni  $g \in G$  ha un ordine finito e  $o(g) \mid \#G$ .

**Definizione** Sia  $(G, \star)$  un gruppo. Se esiste  $g \in G$  tale che  $\forall h \in G, \exists n \in \mathbb{Z}$  tale che  $h = g^n$ , cioè  $G = \{g^n \mid n \in \mathbb{Z}\}$  allora  $G$  si dice **ciclico di generatore  $g$** .

## 2.4. Morfismi

N.B.: se c'è una nozione di struttura algebrica che è un "coso" allora c'è la corrispondente nozione di "morfismo di coso".

Se  $(G, \star_1, \dots, \star_n)$  e  $(H, \diamond_1, \dots, \diamond_n)$  sono 2 cosi, un **morfismo di cosi** è un'applicazione  $f : G \rightarrow H$  tale che  $\forall g \in G, \forall g' \in G, f(g \star_i g') = f(g) \diamond_i f(g')$ .

**Definizione** Siano  $(G, \star)$  e  $(H, \diamond)$  due gruppi.

Un **morfismo di gruppi** tra  $(G, \star)$  e  $(H, \diamond)$  è un'applicazione  $f : G \rightarrow H$  tale che  $\forall g \in G, \forall g' \in G, f(g \star g') = f(g) \diamond f(g')$ .

Se  $f$  è una biiezione si dice un **isomorfismo di gruppi**.

Se  $(G, \star) = (H, \diamond)$ ,  $f$  si dice essere un **endomorfismo di gruppi**.

Se  $f$  è sia un isomorfismo che un endomorfismo allora si dice essere un **automorfismo di gruppi**.

**Proposizione** Se  $f : G \rightarrow H$  è un morfismo di gruppi tra due gruppi di neutri rispettivi  $e_G$  e  $e_H$  allora  $f(e_G) = e_H$  e  $\forall g \in G, f(g^{-1}) = f(g)^{-1}$  ( $g^{-1}$  calcolato in  $G$ ,  $f(g)^{-1}$  calcolato in  $H$ ).

**Dimostrazione**  $f(e_G) = f(e_G \star e_G) = f(e_G) \diamond f(e_G)$ .

Siccome  $(H, \diamond)$  è un gruppo esiste l'inverso di  $f(e_G)$ .

$e_H = f(e_G) \diamond f(e_G)^{-1} = f(e_G) \diamond f(e_G) \diamond f(e_G)^{-1} = f(e_G)$ .

Sia  $g \in G, e_H = f(e_G) = f(g \star g^{-1}) = f(g) \diamond f(g^{-1})$ .

Esiste  $f(g)^{-1}$  in  $H$ , quindi  $f(g)^{-1} = f(g)^{-1} \diamond e_H = f(g)^{-1} \diamond f(g) \diamond f(g^{-1}) = f(g^{-1})$ .

<sup>VI</sup>Un insieme si dice finito se ha un numero finito di elementi.

## 2. Strutture algebriche

**Definizione** Siano  $(G, \star)$  e  $(H, \diamond)$  due gruppi di neutri rispettivamente  $e_G$  e  $e_H$  e  $f : G \rightarrow H$  un morfismo di gruppi.

Il **nucleo** di  $f$  è l'insieme  $\ker f = \{g \in G \mid f(g) = e_H\}$ .

L'**immagine** di  $f$  è l'insieme  $\text{Im} f = \{f(g) \mid g \in G\}$ .

**Proposizione**  $\ker f$  è un sottogruppo normale di  $(G, \star)$ .

**Dimostrazione** Per dimostrare che  $\ker f$  è un sottogruppo di  $(G, \star)$  bisogna dimostrare che:

- $\ker f \neq \emptyset$ :  
 $e_G \in \ker f$  quindi  $\ker f \neq \emptyset$ .
- $\forall g, h \in \ker f, g \star h^{-1} \in \ker f$ :  
siano  $g, h \in \ker f$ ,  $f(g \star h^{-1}) = f(g) \diamond f(h^{-1}) = f(g) \diamond f(h)^{-1} = e_H \diamond e_H^{-1} = e_H$ .

Per dimostrare che è un sottogruppo normale bisogna dimostrare che:

- $\forall g \in G$  vale  $\{g \star h \star g^{-1} \mid h \in \ker f\} = \ker f$ :  
sia  $g \in G$  e  $h \in \ker f$  allora  $f(g \star h \star g^{-1}) = f(g) \diamond f(h) \diamond f(g^{-1}) = f(g) \diamond e_H \diamond f(g)^{-1} = f(g) \diamond f(g)^{-1} = e_H$ , quindi  $\ker f$  è un sottogruppo normale di  $(G, \star)$ .

**Proposizione**  $\text{Im} f$  è un sottogruppo di  $(H, \diamond)$ .

**Dimostrazione** Per dimostrare che un insieme è un sottogruppo bisogna dimostrare che:

- $\text{Im} f \neq \emptyset$ :  
 $f(e_G) = e_H \in \text{Im} f$  quindi  $\text{Im} f \neq \emptyset$ .
- $\forall g, h \in \text{Im} f, g \star h^{-1} \in \text{Im} f$ :  
siano  $g, h \in \text{Im} f$ , quindi  $\exists a, b \in G$  tali che  $f(a) = g$  e  $f(b) = h$ , quindi  $g \diamond h^{-1} = f(a) \diamond f(b^{-1}) = f(a \star b^{-1})$ . Dato che  $(G, \star)$  è un gruppo  $a \star b^{-1} \in G$ , quindi  $g \diamond h^{-1} \in \text{Im} f$ .

## 3. Aritmetica

### 3.1. Richiami

**Teorema (fondamentale dell'aritmetica)** Sia  $n \in \mathbb{Z}$ ,  $n \neq 0$ , allora  $\exists \varepsilon = \pm 1$  e  $p_1, \dots, p_k$  primi (positivi) tali che  $n = \varepsilon p_1 \dots p_k$ .

Inoltre  $\varepsilon$  e i  $p_i$  sono unici (a meno del riordinamento dei primi).

**Osservazione** L'unicità della decomposizione non è così scontata:

$$\underbrace{(1 + i\sqrt{5})(1 - i\sqrt{5})}_{\text{interi algebrici}} = 1 - (i\sqrt{5})^2 = 1 - (-5) = 6 = 2 \cdot 3$$

**Definizione (divisione euclidea)** Siano  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ , allora esistono e sono unici  $q, r \in \mathbb{Z}$  tali che  $a = bq + r$  e  $0 \leq r < |b|$ .

**Osservazione** Tramite la divisione euclidea si può dimostrare che i numeri primi sono infiniti:

sia  $S = \{p_1, \dots, p_s\}$  un insieme finito di primi, allora  $\exists n \in \mathbb{Z}$  tale che  $n = \rho_1 \cdot \dots \cdot \rho_s + 1$ .

$n$  non è divisibile per nessun  $\rho \in S$  perchè la divisione euclidea dà sempre resto 1.

Quindi i numeri primi che dividono  $n$  sono fuori da  $S$  e quindi ogni insieme finito non può contenere tutti i primi.

### 3.2. Ideali di $\mathbb{Z}$

#### 3.2.1. Definizione

**Definizione** Un *ideale di  $\mathbb{Z}$*  è un sottoinsieme  $I$  di  $\mathbb{Z}$  tale che:

1.  $I \neq \emptyset$
2.  $\forall x \in I, \forall y \in I, x + y \in I$
3.  $\forall a \in \mathbb{Z}, \forall x \in I, ax \in I$

I punti (2) e (3) possono anche essere riassunti come segue:

$$\forall a, b \in \mathbb{Z}, \forall x, y \in I, ax + by \in I$$

**Osservazione** Un ideale è  $\neq \emptyset$ , quindi c'è  $x \in I$ .

Usando la (3) della definizione di ideale di  $\mathbb{Z}$  con  $a = 0$  vediamo che  $0 = 0 \cdot x \in I$

**Proposizione**  $I$  è un sottogruppo di  $(\mathbb{Z}, +)$ .

### 3. Aritmetica

**Dimostrazione** Sia  $I$  un ideale, allora per essere un sottogruppo di  $(\mathbb{Z}, +)$ , deve valere:

- $I \neq \emptyset$ :  
per la 1;
- dati  $x, y \in I \Rightarrow x + y^{-1} \in I \Rightarrow x - y \in I$ :  
dai punti (2) e (3) combinati con  $a = 1$  e  $b = -1$  si ottiene:  
 $ax + by \in I \Rightarrow x - y \in I$ .

**Proposizione** I sottogruppi  $H$  di  $(\mathbb{Z}, +)$  sono ideali di  $\mathbb{Z}$ .

**Dimostrazione**

- 1  $H \neq \emptyset$ :  
dalla definizione di sottogruppo.
- 2 Dati  $x, y \in H \Rightarrow x + y \in H$ :  
dato che  $(H, +)$  è un gruppo,  $x + y \in H$  dato che  $+$  è una *lci* su  $H$ .
- 3 Dati  $a \in \mathbb{Z}$  e  $x \in H \Rightarrow a \cdot x \in H$ :  
distinguiamo 3 casi:
  - $a > 0$   
 $x \in H \Rightarrow x + x = 2 \cdot x \in H \Rightarrow x + 2 \cdot x = 3 \cdot x \in H \Rightarrow x + (a - 1) \cdot x = a \cdot x \in H$
  - $a = 0$   
 $0 \cdot x = 0 = \text{neutro}$ , ma  $\text{neutro} \in H$  per la definizione di gruppo
  - $a < 0$   
 $a \cdot x = -b$  con  $b > 0$   
 $b = (-a) \cdot x$  dato che  $-a > 0 \Rightarrow b \in H$ .  
Dato che nei gruppi ci sono sempre i complementari:  
 $-b \in H \Rightarrow a \cdot x \in H$

Dalle 2 proposizioni precedenti si deduce che parlare di ideali di  $\mathbb{Z}$  o di sottogruppi di  $(\mathbb{Z}, +)$  è equivalente.

**Definizione** Sia  $n \in \mathbb{Z}$ , l'*ideale principale* generato da  $n$  è  $(n) = \{kn \mid k \in \mathbb{Z}\}$ .

**Proposizione**  $\forall n \in \mathbb{Z}$ ,  $(n)$  è un ideale di  $\mathbb{Z}$ .

**Dimostrazione** Perché  $(n)$  sia un ideale di  $\mathbb{Z}$  deve valere:

- $(n) \neq \emptyset$ :  
se si prende  $k = 0$ ,  $0 \cdot n \in (n) \Rightarrow (n) \neq \emptyset$ ;
- dati  $a, b \in (n) \Rightarrow a + b \in (n)$ :
  - $a \in (n) \Rightarrow \exists k \in \mathbb{Z}$  tale che  $a = k \cdot n$ ;
  - $b \in (n) \Rightarrow \exists l \in \mathbb{Z}$  tale che  $b = l \cdot n$ ; $\Rightarrow a + b = k \cdot n + l \cdot n = (k + l) \cdot n$ .  
Dato che  $k + l \in \mathbb{Z}$ ,  $a + b \in (n)$ ;
- dato  $a \in \mathbb{Z}$  e  $x \in (n) \Rightarrow a \cdot x \in (n)$ :  
 $x \in (n) \Rightarrow \exists k \in \mathbb{Z}$  tale che  $x = k \cdot n \Rightarrow a \cdot x = a \cdot k \cdot n$ .  
Dato che  $a \cdot k \in \mathbb{Z}$ ,  $a \cdot x \in (n)$ .

### 3. Aritmetica

**Osservazione**  $(n) = (-n)$  perché basta usare i “ $k$ ” opposti:

$$\begin{array}{cccccc} -2n & -n & 0 & n & 2n & n > 0 \\ \hline 2n & n & 0 & -n & -2n & n < 0 \end{array}$$

#### 3.2.2. $\mathbb{Z}$ è principale

**Teorema** Per qualsiasi  $I$  ideale di  $\mathbb{Z}$  esiste  $n \in \mathbb{Z}$  tale che  $I = (n)$ .

**Dimostrazione** Se  $I = \{0\}$  allora  $I = (0)$ .

Altrimenti in  $I$  c'è un elemento  $x \neq 0$ , se è negativo  $-x > 0$ , quindi in  $I$  c'è sempre un elemento maggiore di 0.

Sia  $n$  il più piccolo elemento di  $I$  maggiore di 0. Vogliamo dimostrare che  $I = (n)$ .

Sia  $x \in I$ , per la divisione euclidea tra  $x$  e  $n$  si ha:

$$x = n \cdot q + r \text{ con } 0 \leq r < n$$

Per la definizione di ideale  $n \cdot q \in I \Rightarrow x - nq \in I \Rightarrow r = x - nq \in I$ .

Siccome  $n$  è il più piccolo intero positivo in  $I$  allora  $r = 0$ , cioè  $x = nq \in (n)$ . Quindi  $I \subseteq (n)$ .

Siccome  $n \in I$ ,  $(n) \subseteq I$ . (per la (3) della definizione di ideale di  $\mathbb{Z}$ )

Perciò  $I = (n)$ .

#### 3.2.3. Intersezione e somma

**Proposizione** Se  $I$  e  $J$  sono ideali di  $\mathbb{Z}$ ,  $I \cap J$  è un'ideale di  $\mathbb{Z}$ .

**Dimostrazione** Perché  $I \cap J$  sia un ideale deve valere:

- $I \cap J \neq \emptyset$ :  
abbiamo già osservato che un ideale contiene sempre lo 0, quindi  $0 \in I$  e  $0 \in J$ , quindi non sono disgiunti;
- dati  $a, b \in \mathbb{Z}$  e  $x, y \in I \cap J \Rightarrow a \cdot x + b \cdot y \in I \cap J$ :  
 $x, y \in I$  e  $x, y \in J \Rightarrow a \cdot x + b \cdot y \in I$  e  $a \cdot x + b \cdot y \in J \Rightarrow a \cdot x + b \cdot y \in I \cap J$ .

**Definizione** Siano  $I$  e  $J$  due ideali di  $\mathbb{Z}$ , la **somma** di  $I$  e  $J$  è  $I + J = \{x + y \mid x \in I, y \in J\}$ .

**Osservazione**

- Sia  $a \in I$ , dato che  $0 \in J$ ,  $a + 0 = a \in I + J$  e quindi  $I \subseteq I + J$ .
- Sia  $b \in J$ , dato che  $0 \in I$ ,  $0 + b = b \in I + J$  e quindi  $J \subseteq I + J$ .
- Sia  $I = (a)$  e  $J = (b)$  allora  $(a) + (b) = \{x + y \mid x \in (a), y \in (b)\} = \{x + y \mid x = n \cdot a, y = m \cdot b \mid n, m \in \mathbb{Z}\} = \{n \cdot a + m \cdot b \mid n, m \in \mathbb{Z}\}$ .

**Proposizione** Siano  $I$  e  $J$  due ideali di  $\mathbb{Z}$ , allora  $I + J$  è un ideale di  $\mathbb{Z}$ .

**Dimostrazione** Perché  $I + J$  sia un ideale deve valere:

1.  $I + J \neq \emptyset$ :  
 $I$  e  $J$  non sono vuoti, siano  $x \in I$  e  $y \in J$ , allora  $x + y \in I + J$ , quindi  $I + J \neq \emptyset$ ;

### 3. Aritmetica

2. dati  $a, b \in \mathbb{Z}$  e  $x, y \in I + J \Rightarrow a \cdot x + b \cdot y \in I + J$ :  
 siano  $a, b \in \mathbb{Z}$ ,  $x + y \in I + J$  e  $x' + y' \in I + J$ .  
 $a(x + y) + b(x' + y') = ax + ay + bx' + by' = \underbrace{ax + bx'}_{\in I} + \underbrace{ay + by'}_{\in J} \in I + J$ .

#### 3.2.4. MCD, mcm

**Definizione** Siano  $a, b \in \mathbb{Z}$ . L'**MCD** e l'**mcm** di  $a$  e  $b$  sono gli interi  $M$  e  $m$  positivi tali che  $(a) \cap (b) = (m)$ ,  $(a) + (b) = (M)$ .

**Proposizione**  $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, MCD(a, b) \cdot mcm(a, b) = |ab|$ .

**Osservazione** Si può facilmente dimostrare usando la definizione di **MCD** e **mcm** che usa la scomposizione in fattori primi, ma è abbastanza difficile usando la definizione che usa gli ideali di  $\mathbb{Z}$ .

- $MCD(a, 0) = (a) + (0) = (a) \Rightarrow MCD(a, 0) = a$ .
- $mcm(a, 0) = (a) \cap (0) = (0) \Rightarrow mcm(a, 0) = 0$ .

#### 3.2.5. Proprietà di MCD e mcm

1.  $mcm(a, b)$  è un multiplo di  $a$  e  $b$  ed è il più piccolo dei multipli comuni positivi (se  $a \neq 0, b \neq 0$ ).  
 Infatti  $(a)$  è l'insieme dei multipli di  $a$  e  $(b)$  è l'insieme dei multipli di  $b$ , quindi  $(a) \cap (b)$  è l'insieme dei multipli comuni di  $a$  e  $b$ .  
 Dato che  $(a) \cap (b)$  è un ideale di  $\mathbb{Z}$  il suo principale sarà l'**mcm**.
2.  $MCD(a, b)$  è un divisore comune di  $a$  e  $b$  ed è il più grande divisore comune; infatti:
  - $a \in (a)$  e  $0 \in (b) \Rightarrow a + 0 = a \in (a) + (b) = (MCD(a, b))$ ;
  - $0 \in (a)$  e  $b \in (b) \Rightarrow 0 + b = b \in (a) + (b) = (MCD(a, b))$ ;

quindi  $MCD(a, b) \mid a$  e  $MCD(a, b) \mid b$  e quindi è un divisore comune di  $a$  e  $b$ .

Sia  $d$  un divisore comune di  $a$  e  $b$  allora  $d \mid a$  e  $d \mid b$  e quindi  $a \in (d)$  e  $b \in (d)$ .

Quindi  $\exists k, l \in \mathbb{Z}$  tali che  $a = k \cdot d$  e  $b = l \cdot d$ .

Sia  $x \in (a) + (b)$  allora  $\exists m, n \in \mathbb{Z}$  tali che  $m \cdot a + n \cdot b = x$  (dall'osservazione sulla somma degli ideali).

Ma  $a = k \cdot d$  e  $b = l \cdot d$  quindi  $m \cdot k \cdot d + n \cdot l \cdot d = x \Rightarrow x = (m \cdot k + n \cdot l) \cdot d$ .

Dato che  $m \cdot k + n \cdot l \in \mathbb{Z}$ ,  $x \in (d)$ , tutti gli elementi di  $(a) + (b)$  sono elementi di  $(d)$ .

quindi  $(a) + (b) \subseteq (d)$  cioè  $(MCD(a, b)) \subseteq (d)$ .

Sapendo che  $MCD(a, b) \in (MCD(a, b))$ ,  $\exists p \in \mathbb{Z}$  tale che  $MCD(a, b) = d \cdot p$  e quindi  $d \mid MCD(a, b)$ .

Quindi tutti i divisori comuni di  $a$  e  $b$  sono divisori di  $MCD(a, b)$  che è anch'esso un divisore e quindi è per forza il più grande.

#### 3.2.6. Teorema di Bezout

**Teorema (di Bezout)** Siano  $a$  e  $b \in \mathbb{Z}$  e  $d = MCD(a, b)$ . Esistono  $m$  e  $n \in \mathbb{Z}$  tali che  $ma + nb = d$ . Inoltre:

1. se  $a \neq 0$  o  $b \neq 0$ ,  $d$  è il più piccolo positivo per il quale si possano trovare  $m, n \in \mathbb{Z}$  tali che  $m \cdot a + n \cdot b = d$ ;
2. se esistono  $m$  e  $n \in \mathbb{Z}$  tali che  $ma + nb = 1$ , allora  $MCD(a, b) = 1$ .

### 3. Aritmetica

**Dimostrazione**  $(d) = (a) + (b)$ ,  $d \in (d) \Rightarrow d = ma + nb$  per qualche  $m$  e  $n \in \mathbb{Z}$ .

Sia  $p \in \mathbb{Z}$  tale che  $\exists m, n \in \mathbb{Z}$  tali che  $n \cdot a + m \cdot b = p$ , allora  $p \in (d)$ , ma il più piccolo  $p > 0$  tale che  $p \in (d)$  è  $d$  quindi vale la (1).

Il (2) dice che  $\exists m, n \mid ma + nb = 1 \Rightarrow 1 \in (d)$ . Non ci può essere un positivo più piccolo di  $d$  in  $(d) \Rightarrow d = 1$ .

## 3.3. Equazioni diofantee

### 3.3.1. Teorema cinese dei resti

**Teorema** Siano  $a, b, m, n \in \mathbb{Z}$ , con  $MCD(m, n) = 1$ . Allora esiste  $x \in \mathbb{Z}$  tale che  $x \equiv_n a$  e  $x \equiv_m b$ . Inoltre se  $x$  e  $y$  soddisfano entrambe le condizioni,  $x \equiv_{m \cdot n} y$ .

**Dimostrazione** Per dimostrare che  $x \equiv_n a$  e  $x \equiv_m b$  bisogna trovare  $k, l \in \mathbb{Z}$  tali che

$$x = k \cdot n + a \text{ e } x = l \cdot m + b \Rightarrow k \cdot n + a = l \cdot m + b \Rightarrow a - b = l \cdot m - k \cdot n.$$

Per il teorema di Bezout  $\exists p, q \in \mathbb{Z}$  tali che  $pm + qn = 1 = MCD(m, n)$

quindi moltiplicando da entrambe le parti per  $(a - b)$  si ottiene:

$$p \cdot m \cdot (a - b) + q \cdot n \cdot (a - b) = (a - b) \Rightarrow k = p(a - b) \text{ e } l = -q(a - b) = q(b - a).$$

Quindi  $x = p \cdot (a - b) \cdot n + a = q \cdot (b - a) \cdot m + b$ , quindi  $x \equiv_n a$  e  $x \equiv_m b$ .

Siano  $x, y \in \mathbb{Z}$  tali che  $x \equiv_n a$ ,  $x \equiv_m b$ ,  $y \equiv_n a$  e  $y \equiv_m b$ , per mostrare che  $x \equiv_{n \cdot m} y$  bisogna trovare  $k \in \mathbb{Z}$  tale che  $x = y + k \cdot m \cdot n \Rightarrow x - y = k \cdot m \cdot n$

$$\text{Si sa che } \exists k_x, l_x, k_y, l_y \in \mathbb{Z} \text{ tali che } x = k_x \cdot n + a = l_x \cdot m + b \text{ e } y = k_y \cdot n + a = l_y \cdot m + b$$

$$\Rightarrow x - y = k_x \cdot n + k_y \cdot n \Rightarrow k \cdot n \cdot m = k_x \cdot n + k_y \cdot n = (k_x + k_y) \cdot n.$$

Se  $n = 0 \Rightarrow x = a$  e  $y = a$  quindi  $x = y \Rightarrow x \equiv_{0 \cdot m} y \Rightarrow x \equiv_0 y$ .

Se  $m = 0 \Rightarrow x = b$  e  $y = b$  quindi  $x = y \Rightarrow x \equiv_{n \cdot 0} y \Rightarrow x \equiv_0 y$ .

$$\text{Se } m \neq 0 \text{ e } n \neq 0 \text{ allora } k = (k_x + k_y) \cdot \frac{n}{n \cdot m} = \frac{k_x + k_y}{m}.$$

Bisogna però verificare se il  $k$  così trovato  $\in \mathbb{Z}$ ; per farlo bisogna dimostrare che  $m \mid (k_x + k_y)$ .

Si sa che  $x - y = (k_x + k_y) \cdot n = (l_x + l_y) \cdot m$  quindi  $(k_x + k_y) \cdot n$  è un multiplo di  $m$ , ma  $MCD(n, m) = 1$ , quindi  $(k_x + k_y)$  è multiplo di  $m$  e quindi  $\frac{k_x + k_y}{m} \in \mathbb{Z}$ .

Quindi  $x \equiv_{m \cdot n} y$ .

### 3.3.2. Equazioni diofantee

Sono equazioni nella forma  $ax + by = c$ , con  $a, b, c \in \mathbb{Z}$  dati e  $x, y \in \mathbb{Z}$  incognite.

**Teorema** L'equazione  $ax + by = c$  in  $x, y \in \mathbb{Z}$  con dati  $a, b, c \in \mathbb{Z}$  ha soluzione se e solo se  $MCD(a, b) \mid c$ .

**Dimostrazione** Dato che bisogna dimostrare un "se e solo se" bisogna dimostrare che la condizione è sia necessaria che sufficiente:

- **C.N.:**  
dato che  $(MCD(a, b)) = \{a \cdot x + b \cdot y \mid x, y \in \mathbb{Z}\}$ , allora  $c$  deve appartenere a  $(MCD(a, b))$  e quindi  $MCD(a, b) \mid c$ ;
- **C.S.:**  
se  $MCD(a, b) \mid c$ , allora  $c \in (MCD(a, b)) = \{a \cdot x + b \cdot y \mid x, y \in \mathbb{Z}\}$  e quindi  $\exists x, y \in \mathbb{Z}$  tali che  $a \cdot x + b \cdot y = c$ .

### Procedimento di risoluzione

1. Si ricava in qualche modo  $d = MCD(a, b)$
2. Si ricavano in qualche modo  $p, q \in \mathbb{Z}$  tali che  $p \cdot a + q \cdot b = d$ , che esistono per il teorema di Bezout
3. Dato che  $c \in (d) \exists k \in \mathbb{Z}$  tale che  $d \cdot k = c$  da cui:  
 $p \cdot a + q \cdot b = d \Rightarrow k \cdot p \cdot a + k \cdot q \cdot b = k \cdot d \Rightarrow k \cdot p \cdot a + k \cdot q \cdot b = c$ .  
 Quindi  $x_0 = k \cdot p$  e  $y_0 = k \cdot q$  sono una soluzione, ma le soluzioni sono infinite

Procedimento per trovare le altre soluzioni:

Supponiamo che  $(x, y)$  sia un'altra soluzione, quindi:

$$c = ax + by = ax_0 + by_0 \Rightarrow a(x - x_0) = b(y_0 - y).$$

Dato che  $d \mid a$  e  $d \mid b \exists a', b'$  tali che  $a = a'd$  e  $b = b'd$ .

$$\Rightarrow a'd(x - x_0) = b'd(y_0 - y)$$

Si può ipotizzare che  $a \neq 0$  e  $b \neq 0$ , altrimenti risolvere l'equazione diofantea non presenterebbe nessun problema.

$$\text{Quindi } d \neq 0 \Rightarrow a'(x - x_0) = b'(y_0 - y)$$

Da cui si osserva che:

- $a'(x - x_0)$  è multiplo di  $b'$
- $b'(y_0 - y)$  è multiplo di  $a'$

Ricordando che  $p \cdot a + q \cdot b = d \Rightarrow p \cdot d \cdot a' + q \cdot d \cdot b' = d \Rightarrow p \cdot a' + q \cdot b' = 1 \Rightarrow MCD(a', b') = 1$

$$x - x_0 \text{ è multiplo di } b' \Rightarrow \exists l \in \mathbb{Z} \text{ tale che } x - x_0 = l \cdot b' \Rightarrow x = x_0 + l \cdot b'$$

Ricordando che  $a'(x - x_0) = b'(y_0 - y) \Rightarrow a' \cdot l \cdot b' = b'(y_0 - y) \Rightarrow a' \cdot l = y_0 - y \Rightarrow y = y_0 - a' \cdot l$   
 l'insieme delle soluzioni è quindi:

$$\{(x_0 + l \cdot b', y = y_0 - a' \cdot l) \mid l \in \mathbb{Z}\} = \left\{ \left( x_0 + l \cdot \frac{b}{d}, y = y_0 - \frac{a}{d} \cdot l \right) \mid l \in \mathbb{Z} \right\}$$

### 3.3.3. Invertibili in $\mathbb{Z}/n\mathbb{Z}$

Per  $[a]_n \in \mathbb{Z}/n\mathbb{Z}$  cerchiamo se esiste  $[b]_n$  tale che  $[a]_n [b]_n = [ab]_n = [1]_n$ , cioè se esiste un  $b$  tale che  $\exists k$  tale che  $ab + nk = 1$ .

Questa equazione ha soluzioni se e solo se  $MCD(a, n) \mid 1$ , quindi se e solo se  $MCD(a, n) = 1$ .

Le soluzioni sono  $b = p + ln$  ( $k = q - la$ , ma a noi non interessa), con  $l \in \mathbb{Z}$  e  $pa + qn = 1$ ;  $[b]_n = [p]_n$ .

Quindi  $[a]_n$  è invertibile (per il prodotto) se e solo se  $MCD(a, n) = 1$  e  $[a]_n^{-1} = [p]_n$  per  $p$  tale che  $pa + qn = 1$  con  $q \in \mathbb{Z}$ .

**Osservazione**  $[a]_n$  è invertibile se e solo se  $MCD(a, n) = 1$ .

Quindi se  $n$  è primo, tutte le classi sono invertibili tranne  $[0]_n$ .

Al contrario, se  $n$  non è primo, esistono  $a$  e  $b$  tra 2 e  $n-1$  tali che  $ab = n$ . Allora  $MCD(a, n) = a \geq 2$ . Quindi  $[a]_n$  non è invertibile.

Quindi  $n$  è primo se e solo se tutte le classi  $[a]_n$ , con  $1 \leq a \leq n-1$ , sono invertibili.

### 3.4. Algoritmo di Euclide

Questo algoritmo permette di ricavare l' $MCD$  senza scomporre in fattori primi e può essere anche utilizzato per ricavare i coefficienti di Bezout.

Si basa sulla seguente



### 3. Aritmetica

**Osservazione** Sia  $d = MCD(a, b)$ . Quindi  $(a) + (b) = (d) = \{ax + by \mid x, y \in \mathbb{Z}\}$ .

Sia  $q \in \mathbb{Z}$ ,  $(a) + (b) = (d) = \{ax + qay - qay + yb \mid x, y \in \mathbb{Z}\} = \{(x + qy)a + y(b - qa) \mid x, y \in \mathbb{Z}\}$ .

Dato che  $(x + qy)$  con  $x, y \in \mathbb{Z}$  è un qualsiasi numero in  $\mathbb{Z}$  si può effettuare un cambio di variabile, quindi:

$$(d) = \{za + y(b - qa) \mid z, y \in \mathbb{Z}\} = (a) + (b - qa).$$

$$\text{Quindi } \forall q \in \mathbb{Z}, MCD(a, b) = MCD(a, b - qa).$$

**Procedimento** Siano dati  $b \geq a \geq 0$ . Per calcolare l' $MCD(a, b)$  definiamo due successioni  $(a_n)$  e  $(b_n)$  nel modo seguente:

- $b_0 = b, a_0 = a$ ;
- se  $a_n$  e  $b_n$  esistono, se  $a_n = 0$ ,  $MCD(a, b) = b_n$ ;  
se no si calcolano  $q_n$  e  $r_n$  tali che  $b_n = q_n a_n + r_n$  con  $0 \leq r_n \leq a_n - 1$  e prendiamo  $b_{n+1} = a_n$  e  $a_{n+1} = r_n$ .

**Esempio**  $MCD(91, 117) = ?$

$n$	$b_n$	$a_n$	$q_n$	$r_n$	divisione
0	117	91	1	26	$117 = 1 \cdot 91 + 26$
1	91	26	3	13	$91 = 3 \cdot 26 + 13$
2	26	13	2	0	$26 = 2 \cdot 13 + 0$
3	13	0			

Quindi  $MCD(91, 117) = 13$ .

Inoltre si possono ricavare i coefficienti di Bezout usando i valori appena ricavati, infatti (dal passaggio 1):

$$13 = 91 - 3 \cdot 26 = 91 - 3 \cdot (117 - 1 \cdot 91) = (1 + 3 \cdot 1) \cdot 91 - 3 \cdot 117 = 4 \cdot 91 - 3 \cdot 117.$$

## 4. Strutture algebriche (2)

### 4.1. Applicazioni della teoria dei gruppi

#### 4.1.1. Teoremi di Fermat ed Eulero

**Definizione** Sia  $n \in \mathbb{Z}$ ,  $n \geq 2$ , il numero  $\varphi(n)$  di elementi invertibili in  $\mathbb{Z}/n\mathbb{Z}$  si chiama *indicatore di Eulero*.

**Osservazione** Se  $p$  è primo,  $\varphi(p) = p - 1$ .

Il teorema cinese dei resti permette di dimostrare che se  $MCD(m, n) = 1$  allora  $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ .

Si verifica in modo semplice che se  $p$  è primo,  $k \geq 1$ ,  $\varphi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p - 1) = p^k \cdot \left(1 - \frac{1}{p}\right)$ .

**Teorema (Fermat)** Siano  $p$  e  $n$  interi con  $p$  primo e  $p \nmid n$ , allora  $n^{p-1} \equiv_p 1$ .

**Dimostrazione**  $p \nmid n \Rightarrow MCD(p, n) = 1 \Rightarrow [n]_p$  è invertibile in  $\mathbb{Z}/p\mathbb{Z}$  e quindi  $[n]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$  (insieme degli invertibili in  $\mathbb{Z}/p\mathbb{Z}$ ).

Sappiamo che  $\#(\mathbb{Z}/p\mathbb{Z})^\times = \varphi(p) = p - 1$  e quindi il gruppo  $\left((\mathbb{Z}/p\mathbb{Z})^\times, \times\right)^1$  è un gruppo finito, quindi:  $\left([n]_p\right)^{\varphi(p)} = \left([n]_p\right)^{p-1} = \text{neutro} = [1]_p$  e quindi  $[n^{p-1}]_p = [1]_p \Rightarrow n^{p-1} \equiv_p 1$ .

**Osservazione** Dato che  $[n]_p$  è invertibile  $[n^{p-1}]_p = [1]_p \Rightarrow [n^p]_p \cdot [n]_p^{-1} = [1]_p \Rightarrow [n^p]_p \cdot [n]_p^{-1} \cdot [n]_p = [1]_p \cdot [n]_p \Rightarrow [n^p]_p = [n]_p$ .

**Teorema (Eulero)** Siano  $m$  e  $n$  interi tali che  $MCD(m, n) = 1$ . Allora  $n^{\varphi(m)} \equiv_m 1$ .

**Dimostrazione**  $MCD(m, n) = 1 \Rightarrow [n]_m$  è invertibile in  $\mathbb{Z}/m\mathbb{Z}$  e quindi  $[n]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$  (insieme degli invertibili in  $\mathbb{Z}/m\mathbb{Z}$ ).

Sappiamo che  $\#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(m)$  e quindi il gruppo  $\left((\mathbb{Z}/m\mathbb{Z})^\times, \times\right)$  è un gruppo finito, quindi:  $\left([n]_m\right)^{\varphi(m)} = \text{neutro} = [1]_m$  e quindi  $\left[n^{\varphi(m)}\right]_m = [1]_m \Rightarrow n^{\varphi(m)} \equiv_m 1$ .

#### 4.1.2. Diffie-Hellman

L'*algoritmo di Diffie-Hellman* permette lo scambio tra 2 persone (Andrea e Bartolomeo) di una chiave segreta su una linea aperta.

---

<sup>1</sup>“ $\times$ ” indica il prodotto; non usiamo il simbolo solito “ $\cdot$ ” perché come apice non si vedrebbe.

#### 4. Strutture algebriche (2)

Persona	Azione	Dato comunicato
Andrea	Scegli un numero primo $p$	$p$
Andrea	Sceglie $g$ tale che $(\mathbb{Z}/p\mathbb{Z})^\times = \langle [g]_p \rangle$	$g$
Andrea	Sceglie un intero $a$ tale che $1 \leq a \leq p-1$	
Andrea	Calcola un rappresentante $x$ della classe $[g]_p^a = [g^a]_p$	$x$
Bartolomeo	Sceglie un intero $b$ tale che $1 \leq b \leq p-1$ .	
Bartolomeo	Calcola un rappresentante $y$ della classe $[g]_p^b = [g^b]_p$	$y$
Andrea	Calcola un rappresentante della classe $[y]_p^a = [g^b]_p^a = [g^{ab}]_p$	
Bartolomeo	Calcola un rappresentante della classe $[x]_p^b = [g^a]_p^b = [g^{ab}]_p$	

La chiave di sicurezza comune è il rappresentante della classe  $[g^{ab}]_p$ .

Non esiste un algoritmo efficace che permetta di calcolare  $a$  da  $p$ ,  $g$  e  $x$  e quindi è estremamente sicuro, ma allo stesso tempo ricavare tali dati è estremamente semplice rendendo questo un ottimo algoritmo di comunicazione.

Per aumentare l'efficacia dell'algoritmo il numero  $p$  deve essere grande (circa 1024 bit o più).

##### 4.1.3. RSA (Ronald Rivest, Adi Shamir, Leonard Adleman, 1978)

L'algoritmo RSA permette di criptare un messaggio e di comunicarlo su una linea aperta in totale sicurezza.

Se Andrea vuole aprire una comunicazione con Bartolomeo deve:

1. Scegliere  $p$  e  $q$  primi distinti
2. Calcolare  $n = p \cdot q$
3. Scegliere un numero  $e$  tale che  $MCD(e, \varphi(n)) = 1$ .  
Si può notare che  $\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$  dato che sono entrambi numeri primi
4. Calcolare  $d$  tale che  $[d]_{\varphi(n)} = [e]_{\varphi(n)}^{-1}$ .  
Si può notare che moltiplicando a destra e a sinistra per  $[e]_{\varphi(n)}$  si ottiene:  
 $[d]_{\varphi(n)} \cdot [e]_{\varphi(n)} = [e]_{\varphi(n)}^{-1} \cdot [e]_{\varphi(n)} \Rightarrow [d \cdot e]_{\varphi(n)} = [1]_{\varphi(n)} \Rightarrow d \cdot e \equiv_{\varphi(n)} 1$
5. Comunicare a Bartolomeo la coppia  $(n, e)$

Se Bartolomeo vuole mandare un messaggio ad Andrea deve:

1. Suddividere il messaggio in pezzi  $a_i$  di lunghezza inferiore a  $\log_2 n$ .  
Quindi  $a_i$  ha un numero di bit inferiore a quello di  $n$  e quindi  $a_i < n$
2. Calcolare  $b_i$  tale che  $[b_i]_n = [a_i]_n^e$
3. Comunicare ad Andrea  $b_i$

Andrea per decifrare il messaggio deve:

1. Calcolare  $[b_i]_n^d$ .  
Si può notare che  $[b_i]_n^d = ([a_i]_n^e)^d = [a_i]_n^{ed}$
2. L'elemento positivo più piccolo della classe appena calcolata è  $a_i$

## 4. Strutture algebriche (2)

Per capire come funziona bisogna suddividere il problema in vari casi in base al valore di  $MCD(a_i, n)$ .  
Dato che  $n = p \cdot q$  ha come divisori solo 1,  $p$ ,  $q$  e  $n$ ,  $MCD(a_i, n)$  può assumere solo quei quattro valori:

1.  $MCD(a_i, n) = n$  :  
questo caso capita solo se  $a_i = 0$ ;
2.  $MCD(a_i, n) = p$  :  
questo caso capita solo se  $a_i = k \cdot p$  dove  $0 \leq k \leq q - 1$ , dato che per  $k = q$ ,  $a_i = p \cdot q = n$  che è impossibile dato che  $a_i < n$ ;
3.  $MCD(a_i, n) = q$  :  
questo caso capita solo se  $a_i = l \cdot q$  dove  $0 \leq l \leq p - 1$  dato che per  $l = p$ ,  $a_i = q \cdot p = n$  che è impossibile dato che  $a_i < n$ ;
4.  $MCD(a_i, n) = 1$ :  
per tutti gli altri valori di possibili di  $a_i$ .

Dato che  $a_i$  può assumere  $n$  valori diversi le probabilità che  $MCD(a_i, n) \neq 1$  sono molto basse, in particolare sono solo  $\frac{p-1+q-1+1}{n} = \frac{p+q-1}{n}$ , quindi se l'algoritmo funziona per il caso (4) allora funziona nella quasi totalità dei casi.

Se ci si trova in un altro caso si può modificare leggermente il messaggio per uscire da quel caso dato che è altamente improbabile ricapitare in un caso in cui non funzioni.

Quindi si suppone che  $MCD(a_i, n) = 1$  e quindi vale il teorema di Eulero:

$$a^{\varphi(n)} \equiv_n 1 \Rightarrow [a_i]_n^{\varphi(n)} = [1]_n.$$

Dato che  $d \cdot e \equiv_{\varphi(n)} 1 \Rightarrow \exists k \in \mathbb{Z}$  tale che  $d \cdot e = \varphi(n) \cdot k + 1$ .

$$\text{Quindi } [a_i]_n^{ed} = [a_i]_n^{\varphi(n) \cdot k + 1} = \left([a_i]_n^{\varphi(n)}\right)^k \cdot [a_i]_n^1 = \left([a_i]_n^{\varphi(n)}\right)^k \cdot [a_i]_n$$

Dato che  $\varphi(n)$  è il numero di invertibili in  $\mathbb{Z}/n\mathbb{Z}$  allora se si prende il gruppo  $\left((\mathbb{Z}/n\mathbb{Z})^\times, \cdot\right)$  avrà  $\varphi(n)$  elementi e quindi è un gruppo finito e in un gruppo finito l'ordine di un elemento è un divisore dell'ordine del gruppo.

Dato che  $MCD(a_i, n) = 1$  allora  $[a_i]_n$  ha un inverso e quindi  $[a_i]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$  e quindi  $[a_i]_n^{\varphi(n)} = [1]_n$ , quindi:

$$[a_i]_n^{ed} = \left([a_i]_n^{\varphi(n)}\right)^k \cdot [a_i]_n = [1]_n^k \cdot [a_i]_n = [a_i]_n$$

Dato che  $a_i < n$  e che  $[a_i]_n = \{\dots, a_i - 2n, a_i - n, a_i, a_i + n, a_i + 2n, \dots\}$  allora l'elemento positivo più piccolo della classe appena calcolata è il messaggio decifrato.

### Osservazione

- In realtà l'algoritmo funziona anche se ci si trova nei casi 2 e 3, ma il motivo è radicalmente diverso, dato che  $[a_i]_n \notin (\mathbb{Z}/n\mathbb{Z})^\times$ , e anche più complicato.
- La sicurezza è data dal fatto che è lungo calcolare  $p$  e  $q$  noto solo  $n = pq$ .

## 4.2. Strutture algebriche con 2 lci

### 4.2.1. Anello

**Definizione** un *anello* è una struttura algebrica  $(A, +, \cdot)$  o  $(A, +, \cdot, 0_A, 1_A, -)$  (dove “ $-$ ” indica l'opposto) tale che:

1.  $(A, +, 0_A, -)$  è un gruppo abeliano<sup>II</sup>;

---

<sup>II</sup>Questa è una notazione un po' diversa da quella usata fin ad ora per i gruppi, ma sono equivalenti; in questa si mettono solo in evidenza il neutro e l'operazione di arità 1 per ottenere l'inverso.

#### 4. Strutture algebriche (2)

2.  $(A, \cdot, 1_A)$  è un monoide;
3.  $\forall a, b, c \in A, (a + b) \cdot c = (a \cdot c) + (b \cdot c), a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  ossia vale la doppia distributività.

#### Esempi

- $\left( \begin{matrix} \mathbb{Z} & \mathbb{Q} \\ \mathbb{R} & \mathbb{C} \end{matrix}, +, \cdot \right), (M(n), +, \cdot)^{\text{III}}, (\mathbb{Z}/n\mathbb{Z}, +, \cdot), (\mathcal{P}(X), \Delta, \cap)$  (dove  $A \Delta B = (A \cup B) \setminus (A \cap B)$  (“ $\setminus$ ” indica l’esclusione)).

#### 4.2.2. Proprietà

**Proposizione** Se  $(A, +, \cdot)$  è un anello, allora  $\forall a \in A, a \cdot 0_A = 0_A \cdot a = 0_A^{\text{IV}}$ .

**Dimostrazione** Sia  $a \in A$ .

$$a \cdot 0_A = a \cdot (0_A + 0_A) = a \cdot 0_A + a \cdot 0_A$$

$$a \cdot 0_A - a \cdot 0_A = a \cdot 0_A + a \cdot 0_A - a \cdot 0_A$$

dato che  $-a \cdot 0_A$  è l’inverso di  $a \cdot 0_A$  per il  $+$ :

$$0_A = a \cdot 0_A.$$

Analoghi passaggi per il  $0_A \cdot a$ .

**Osservazione** Cosa succede se  $0_A = 1_A$ ?

Sia  $a \in A$ , allora  $a = 1_A \cdot a = 0_A \cdot a = 0_A$ .

Quindi  $A = \{0_A\}$ .

L’anello  $\{0_A\}$  si chiama **anello nullo**. In tutti gli altri  $0_A \neq 1_A$ .

**Osservazione** Se  $A \neq \{0_A\}$ ,  $0_A$  non è invertibile (per  $\cdot$ ) perché  $\forall a \in A, a \cdot 0_A = 0_A \neq 1_A$ .

**Definizione** Se  $(A, +, \cdot)$  è un anello e il prodotto è commutativo l’anello si dice **commutativo**.

#### 4.2.3. Ideali

**Definizione** Sia  $(A, +, \cdot)$  un anello commutativo, allora un **ideale** di  $(A, +, \cdot)$  è un sottoinsieme  $I$  tale che:

1.  $I \neq \emptyset$ ;
2.  $\forall a, b \in I, a + b \in I$ ;
3.  $\forall x \in I, \forall a \in A, a \cdot x \in I$ .

I punti (2) e (3) possono anche essere riassunti come segue:

$$\forall a, b \in A, \forall x, y \in I, ax + by \in I.$$

**Proposizione** Se  $I$  è un ideale di un anello  $(A, +, \cdot)$ ,  $0_A \in I$ .

**Dimostrazione** Per la (1)  $\exists c \in I$  e per la (3) della definizione ponendo  $a = 0_A$  si ottiene che  $c \cdot 0_A = 0_A \in I$ .

<sup>III</sup>Matrici quadrate di ordine  $n$  con la somma tra matrici e il prodotto matriciale.

<sup>IV</sup>È equivalente a dire che il neutro della somma è l’elemento assorbente della moltiplicazione.

#### 4. Strutture algebriche (2)

##### Osservazione

- Se  $1_A \in I$ ,  $I = A$  (per il punto (3) della definizione con  $x = 1_A$ ).
- Se un invertibile  $x \in I$ , usando il punto (3) della definizione con  $a = x^{-1}$  si vede che  $1_A \in I \Rightarrow I = A$ .

**Proposizione**  $I$  è un sottogruppo di  $(A, +)$ .

**Dimostrazione** Per dimostrare che  $I$  è un sottogruppo di  $(A, +)$  bisogna controllare se:

1.  $I \neq \emptyset$ :  
data dalla (1) della definizione di ideale;
2.  $\forall a \in I, b \in I, a + b^{-1} \in I \Rightarrow a - b \in I$ :  
siano  $a, b \in I$ .  
Quindi prendendo i punti (2) e (3) della definizione di ideale combinati con  $x = 1_A$  e  $y = -1_A$  si ottiene:  
 $1_A \cdot a + (-1_A) \cdot b \in I \Rightarrow a - b \in I$ .

**Definizione** Sia  $I$  un ideale di un anello definito sull'insieme  $A$  allora si definisce la relazione  $\rho_I$ :

$a \rho_I b \Leftrightarrow \exists x \in I$  tale che  $b = a + x$ .

Inoltre la classe di equivalenza  $[a]_{\rho_I} = [a]_I = \{b \in A \mid b - a \in I\}$ .

**Osservazione** È quello che abbiamo fatto con la congruenza modulo  $n$ , l'ideale è  $n\mathbb{Z} = (n) = \{\text{multipli di } n\}$ .

**Proposizione** Siano  $(A, +, \cdot)$  un anello commutativo,  $I$  un ideale e  $a, b, c, d \in A$  tale che  $[a]_I = [c]_I$ ,  $[b]_I = [d]_I$ .

- $[a + b]_I = [c + d]_I$
- $[a \cdot b]_I = [c \cdot d]_I$

**Dimostrazione** Dato che  $[a]_I = [c]_I$  allora  $\exists k \in I$  tale che  $a = c + k$ .

Dato che  $[b]_I = [d]_I$  allora  $\exists l \in I$  tale che  $b = d + l$ .

$a + b = c + k + d + l = c + d + (k + l)$  ma  $k + l \in I$ , quindi  $[a + b]_I = [c + d]_I$ .

$a \cdot b = (c + k) \cdot (d + l)$ .

Per la proprietà distributiva degli anelli si ha:

$a \cdot b = c \cdot (d + l) + k \cdot (d + l) = c \cdot d + c \cdot l + k \cdot d + k \cdot l = c \cdot d + (c \cdot l + k \cdot d + k \cdot l)$ .

Ma  $c \cdot l + k \cdot d \in I$  per i punti (2) e (3) della definizione di ideale combinati.

$k \cdot l \in I$  per il punto (3), quindi per la (2)  $c \cdot l + k \cdot d + k \cdot l \in I$  e quindi  $[a \cdot b]_I = [c \cdot d]_I$ .

**Definizione** Sull'insieme  $A/I = A/\rho_I$  si definiscono 2 *lci*, una somma  $[a]_I + [b]_I = [a + b]_I$  e un prodotto  $[a]_I [b]_I = [ab]_I$ .

**Proposizione**  $(A/I, +, \cdot)$  è un anello e si dice *anello quoziente*.

**Osservazione** Se  $a \in A$ ,  $(a) = \{a \cdot x \mid x \in A\}$  è un ideale di  $A$  se  $(A, +, \cdot)$  è un anello commutativo.

#### 4. Strutture algebriche (2)

**Dimostrazione** per dimostrare che  $(a)$  è un ideale di  $A$  dobbiamo dimostrare che:

- $(a) \neq \emptyset$ :  
dato che  $0_A \in A$  allora  $a \cdot 0_A = 0_A \in (a)$ ;
- $\forall b, c \in (a), a + b \in (a)$ :  
siano  $b, c \in (a)$  allora  $\exists k, l \in A$  tali che  $a \cdot k \in (a)$  e  $a \cdot l \in (a)$ .  
 $b + c = a \cdot k + a \cdot l$  per la proprietà distributiva degli anelli  $b + c = a \cdot (k + l)$  ma  $k + l \in A$  quindi  $c + d \in (a)$ ;
- $\forall x \in (a), \forall a \in A, a \cdot x \in (a)$ :  
sia  $x \in (a)$  allora  $\exists k \in A$  tale che  $a \cdot k = x$ .  
Sia  $l \in A$  allora  $l \cdot x = l \cdot a \cdot k$  dato che l'anello è commutativo  $l \cdot x = a \cdot l \cdot k$  ma  $l \cdot k \in A$  e quindi  $l \cdot x \in A$ .

**Definizione** Se tutti gli ideali di  $(A, +, \cdot)$  sono della forma  $(a)$  l'anello si dice *principale*.

#### 4.2.4. Anelli di polinomi

Sia  $(A, +, \cdot)$  un anello commutativo.

Definiamo  $A[X]$  l'insieme delle successioni  $(a_i)_{i \geq 0}^V$  con ogni  $a_i \in A$  tale che esista  $n_0$  tale che  $\forall i > n_0, a_i = 0_A$ .

Il numero  $n_0$  viene chiamato *grado del polinomio* e si denota  $d(P)$  (dall'inglese degree).

Su  $A[X]$  definiamo una somma e un prodotto:

- $(a_i)_{i \geq 0} + (b_i)_{i \geq 0} = (a_i + b_i)_{i \geq 0}$ ;
- $(a_i)_{i \geq 0} \cdot (b_i)_{i \geq 0} = (c_i)_{i \geq 0}$  dove  $\forall i \geq 0, c_i = \sum_{j=0}^i a_j b_{i-j}$ .

Si denota  $X = (0_A, 1_A, 0_A, \dots, 0_A, \dots)$ .

Si definisce un prodotto esterno:  $\forall t \in A, \forall (a_i)_{i \in I} \in A[X], t \cdot (a_i)_{i \in I} = (t \cdot a_i)_{i \in I}$ .

**Osservazione**  $X^n = \left( \underbrace{0_A, \dots, 0_A}_{n \text{ volte}}, 1_A, 0_A, \dots, 0_A, \dots \right)$  e allora  $(a_i)_{i \geq 0} = a_0 \cdot X^0 + a_1 \cdot X^1 + \dots + a_{n_0} \cdot X^{n_0}$ .

**Proposizione**  $(A[X], +, \cdot)$  è un anello commutativo, il neutro per la somma è  $(0_A, \dots, 0_A, \dots)$ , il neutro per il prodotto è  $(1_A, 0_A, \dots, 0_A, \dots)$ . L'opposto di  $(a_i)_{i \geq 0}$  è  $(-a_i)_{i \geq 0}$ .

**Osservazione** Se  $A = \mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$ , per semplicità consideriamo  $[0]_2 = 0$  e  $[1]_2 = 1$ .

Sia  $P(X) = X^2 + X = (0, 1, 1, 0, \dots, 0, \dots) \in \mathbb{Z}/2\mathbb{Z}[X]$ .

$P(0) = 0^2 + 0 = 0$ .

$P(1) = 1^2 + 1 = 1 + 1 = 0$ .

Quindi come funzione  $P$  è la funzione nulla, come polinomio non lo è.

#### 4.2.5. Campi

**Definizione** Un *campo* è un anello commutativo  $(K, +, \cdot)$  tale che  $1_K \neq 0_K$  e ogni  $x \in K, x \neq 0_K$ , è invertibile.

<sup>V</sup>Con questa notazione si intende che la successione ha solo indici positivi.

#### 4. Strutture algebriche (2)

**Esempi**  $\begin{pmatrix} \mathbb{Q} \\ \mathbb{R} \\ \mathbb{C} \end{pmatrix}, +, \cdot$  sono campi,  $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$  è un campo se e solo se  $p$  è primo.

Un campo non commutativo viene detto **corpo**.

##### Osservazione

- Dato che in un campo ogni elemento ha un inverso, per l'osservazione fatta sugli anelli, in un campo ci sono solo 2 ideali:  $\{0_K\} = (0_K)$  e  $K = (1_K)$ .
- Come sugli anelli si definiscono i polinomi su un campo  $(K, +, \cdot)$  e il corrispettivo anello dei polinomi  $K[X]$  su  $K$ .
- Su  $K[X]$  si definisce una divisione euclidea:  $\forall A \in K[X], B \in K[X]$  con  $B \neq 0$ , esistono  $Q$  e  $R \in K[X]$  tali che  $A = B \cdot Q + R$  e  $R = 0$  o  $d(R) < d(B)$ . Inoltre  $Q$  e  $R$  sono unici.

**Proposizione**  $(K[X], +, \cdot)$  è un anello principale. Un generatore per l'ideale  $I$  è uno qualsiasi degli elementi di  $I$  diversi da 0 e di grado minimo.

**Osservazione** Se  $P \neq 0$  e  $Q \neq 0$  allora  $PQ \neq 0$  e  $d(PQ) = d(P) + d(Q)$ .

$$\begin{aligned} (a_0 + a_1 \cdot X + \dots + a_m \cdot X^m) \cdot (b_0 + b_1 \cdot X + \dots + b_n \cdot X^n) = \\ = (a_0 \cdot b_0 + (a_0 \cdot b_1 + a_1 \cdot b_0) \cdot X + \dots + (a_m \cdot b_{n-1} + a_{m-1} \cdot b_n) \cdot X^{m+n-1} + a_m \cdot b_n \cdot X^{m+n}) \\ c_i = \sum_{j=0}^i a_j \cdot b_{i-j} \end{aligned}$$

- $i = m + n + 1 \Rightarrow b_{i-j} \neq 0$  solo se  $j \geq m + 1$ , ma allora  $a_j = 0_K$ , quindi  $c_{m+n+1} = 0_K$  (e i successivi nello stesso modo);
- $i = m + n, b_{i-j} \neq 0_K$  solo se  $j \geq m$ , ma  $a_j = 0_K$  per  $j \geq m + 1$ , quindi  $c_{m+n} = a_m \cdot b_n$ .

**Osservazione**  $a_m \neq 0_K$  e  $b_n \neq 0_K \Rightarrow a_m \cdot b_n \neq 0_K$  perché  $(a_m \cdot b_n)^{-1}$  esiste ed è  $b_n^{-1} \cdot a_m^{-1}$  ( $= a_m^{-1} \cdot b_n^{-1}$ ).

**Corollario** Gli invertibili di  $(K[X], +, \cdot)$  sono i polinomi “costanti”  $a_0$ , con  $a_0 \in K, a_0 \neq 0_K$  quindi sono quelli di grado 0.

**Definizione** Un polinomio  $P$  è detto **irriducibile** se e solo se  $\forall Q \in K[X], \forall R \in K[X], P = QR \Leftrightarrow Q$  o  $R$  “costante” (cioè invertibile), e inoltre  $P$  non è invertibile (cioè non è “costante”).

**Teorema**  $(K[X]/(P), +, \cdot)$  è un campo se e solo se  $P$  è irriducibile. (con  $(P)$  si intende l'ideale con principale il polinomio  $P$ )

**Esempio**  $K = \mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$ , dove per semplicità scriviamo  $[0]_2 = 0$  e  $[1]_2 = 1$ .

Grado

$$K[X] = \left\{ \begin{array}{llll} 0 & 0 & 1 & \\ 1 & X & X+1 & \\ 2 & X^2 & X^2+X & X^2+1 \quad X^2+X+1 \\ 3 & X^3 & \dots & \end{array} \right\}$$

Per vedere se quelli di secondo grado siano riducibili o no bisogna controllare che non possano essere scritti come il prodotto di 2 polinomi di primo grado, quindi:

- $X \cdot X = X^2$ , quindi  $X^2$  è riducibile



#### 4. Strutture algebriche (2)

- $X \cdot (X + 1) = X^2 + X$ , quindi  $X^2 + X$  è riducibile
- $(X + 1) \cdot (X + 1) = X^2 + X + X + 1 = X^2 + 1$ , quindi  $X^2 + 1$  è riducibile

quindi  $X^2 + X + 1$  è irriducibile.

Quindi  $(K[X]/(X^2+X+1), +, \cdot)$  è un campo.

**Osservazione** Sia  $I = (X^2 + X + 1)$ . Allora se  $P = a_0 + a_1 \cdot X + \dots + a_n \cdot X^n$ ,  
 $X^2 = X^2 + X + 1 - X - 1 = \underbrace{X^2 + X + 1}_{\in I} + X + 1$ ; quindi  $[X^2]_I = [X + 1]_I$ .

Quindi se  $n \geq 2$ ,  $[X^n]_I = [X^{n-2}]_I \cdot [X^2]_I = [X^{n-2}]_I \cdot [X + 1]_I$  quindi  $\exists k \in I$  tale che  $X^n = X^{n-2} \cdot (X + 1) + k = X^{n-1} + X^{n-2} + k$ .

Si può proseguire per induzione riducendo i gradi e sommando i vari " $k$ " e si ottiene  $P = a'_1 \cdot X + a'_0 \cdot k'$  con  $a'_1, a'_0 \in K$  e  $k' \in I$ . Quindi  $[P]_I = [a'_1 \cdot X + a'_0]_I$ .

Quindi  $K[X]/(P) = \{[0]_I, [1]_I, [X]_I, [X + 1]_I\}$ .  $K[X]/(P)$  ha 4 elementi, è un campo.

Essendo solo 4 elementi si possono esplicitare somme e moltiplicazioni (escludendo quelle che includono termini costanti che sono banali):

- somma:

- $[X] + [X] = [0]$
- $[X] + [X + 1] = [X] + [X] + [1] = [1]$
- $[X + 1] + [X + 1] = [X] + [X] + [1] + [1] = [0]$
- $[X]^3 = [1]$

– prodotto:

- $[X][X] = [X^2] = [X + 1]$
- $[X][X + 1] = [X^2 + X] = [X^2] + [X] = [X + 1] + [X] = [X] + [1] + [X] = [1]$
- $[X + 1][X + 1] = [X^2 + 2 \cdot X + 1] = [X^2 + 1] = [X^2] + [1] = [X + 1] + [1] = [X] + [1] + [1] = [X]$
- $[X]^3 = [1]$

**Parte II.**

**Logica**

## 5. Logica proposizionale

### 5.1. Il linguaggio

#### 5.1.1. Base

Per noi una proposizione è una frase che può essere soltanto vera o falsa.

**Esempi** Sono proposizioni:

- Parigi è in Francia;
- l'Italia è in Europa;
- l'India è una regione della Spagna;
- $3 < 4$ .

Non lo sono:

- la pasta è buona;
- la Grecia è grande;
- gli occhi sono blu.

**Definizione** Un *alfabeto per un linguaggio della logica proposizionale* è costituito dai seguenti simboli:

1. un numero al massimo numerabile di simboli atomici di proposizione:  $A_1, A_2, A_3, \dots$  o  $A, B, C, \dots$ ;
2. connettivi:  $\neg$  (not),  $\vee$  (or),  $\wedge$  (and),  $\rightarrow$  (implica),  $\perp$  (falso)<sup>I</sup>;
3. simboli ausiliari: “(” e “)”.

Con questo alfabeto abbiamo un monoide delle parole. Alcune sono “sintatticamente corrette”, altre (la maggioranza) no.

**Definizione**

- L'*insieme  $\mathcal{F}$  delle formule ben formate* (fbf) è il “minimo” (per la relazione di ordine “ $\subseteq$ ”) insieme  $X$  che soddisfa:
  1. i simboli atomici di proposizione appartengono a  $X$ ;
  2.  $\perp \in X$ ;
  3. se  $\mathcal{P} \in X$  allora  $(\neg \mathcal{P}) \in X$ ;
  4. se  $\mathcal{P}_1 \in X, \mathcal{P}_2 \in X$ , allora  $(\mathcal{P}_1 \vee \mathcal{P}_2) \in X, (\mathcal{P}_1 \wedge \mathcal{P}_2) \in X, (\mathcal{P}_1 \rightarrow \mathcal{P}_2) \in X$ .

---

<sup>I</sup>Questo simbolo rappresenta una T di True al contrario.

## 5. Logica proposizionale

- Un elemento qualsiasi di  $\mathcal{F}$  è detto **formula ben formata** (anche abbreviato con “fbf”).
- Una fbf del tipo (1) si dice **fbf atomica**.
- Nelle formule del tipo  $(\neg \mathcal{P})$ ,  $(\mathcal{P}_1 \vee \mathcal{P}_2)$ ,  $(\mathcal{P}_1 \wedge \mathcal{P}_2)$ ,  $(\mathcal{P}_1 \rightarrow \mathcal{P}_2)$ , il connettivo  $\neg$ ,  $\vee$ ,  $\wedge$ ,  $\rightarrow$  si dice **connettivo principale**.  
Nella formula  $\perp$ , il simbolo stesso è il connettivo principale.

### Osservazione

- A volte per scrivere meno si usa la notazione  $\top = \neg \perp$ .
- Il “minimo” insieme  $X$  esiste.  
Un tale insieme  $X$  esiste: il monoide completo delle parole.  
Consideriamo  $\mathcal{F}$  l’intersezione di tutti gli  $X$  che soddisfano (1), (2), (3) e (4). Questo  $\mathcal{F}$  soddisfa (1) e (2). Sappiamo che  $\mathcal{P} \in \mathcal{F}$ , allora  $\mathcal{P}$  appartiene a ciascun  $X$ . Quindi  $(\neg \mathcal{P})$  appartiene a ciascun  $X$ , quindi  $(\neg \mathcal{P}) \in \mathcal{F}$ .  
Stesso procedimento per il punto (4).
- È facile verificare che una data formula è una fbf.  
Sia  $\mathcal{P} = ((A \vee B) \rightarrow (C \wedge D))$ .  
Se  $\mathcal{P}_1 = (A \vee B) \in \mathcal{F}$  e  $\mathcal{P}_2 = (C \wedge D) \in \mathcal{F}$  allora  $\mathcal{P} = (\mathcal{P}_1 \rightarrow \mathcal{P}_2)$  per il punto (4).  
Se  $A \in \mathcal{F}$  e  $B \in \mathcal{F}$  allora  $\mathcal{P}_1 \in \mathcal{F}$  per il punto (4). Ma per il punto (1)  $A \in \mathcal{F}$  e  $B \in \mathcal{F}$ .  
Se  $C \in \mathcal{F}$  e  $D \in \mathcal{F}$  allora  $\mathcal{P}_2 \in \mathcal{F}$  per il punto (4). Ma per il punto (1)  $C \in \mathcal{F}$  e  $D \in \mathcal{F}$ .  
Invece, dimostrare che una formula non appartiene a  $\mathcal{F}$  è più complicato.  
Sia  $\mathcal{P} = (\rightarrow)$ . Sia  $X = \mathcal{F} \setminus \{\varepsilon\}$ ,  $\varepsilon = ()$  parola vuota, e sia  $Y = X \setminus \{(\rightarrow)\}$ <sup>II</sup>.  
Possiamo verificare che  $Y$  soddisfa i punti (1), (2), (3) e (4).  
Quindi per definizione di  $\mathcal{F}$ ,  $\mathcal{F} \subseteq Y$ . Ma per costruzione  $Y \subseteq \mathcal{F}$ . Quindi  $Y = \mathcal{F}$ , perciò  $\varepsilon \notin \mathcal{F}$ ,  $(\rightarrow) \notin \mathcal{F}$ .  
Dimostrare che una formula non appartiene a  $\mathcal{F}$  non è semplice, ma dato che è intuitivo capirlo non è un argomento di studio interessante.

### Definizione

- Sia  $\mathcal{P}$  una fbf di un linguaggio della logica proposizionale. L’insieme  $S(\mathcal{P})$  delle sottoformule di  $\mathcal{P}$  è definito da:
  1. se  $\mathcal{P}$  è atomica,  $S(\mathcal{P}) = \{\mathcal{P}\}$ ;
  2. se  $\mathcal{P}$  è  $\perp$ ,  $S(\mathcal{P}) = \{\perp\} = \{\mathcal{P}\}$ ;
  3. se  $\mathcal{P} = (\neg \mathcal{P}_1)$ ,  $S(\mathcal{P}) = \{\mathcal{P}\} \cup S(\mathcal{P}_1)$ ;
  4. se  $\mathcal{P} = (\mathcal{P}_1 \vee \mathcal{P}_2)$ ,  $\mathcal{P} = (\mathcal{P}_1 \wedge \mathcal{P}_2)$  o  $\mathcal{P} = (\mathcal{P}_1 \rightarrow \mathcal{P}_2)$ ,  $S(\mathcal{P}) = \{\mathcal{P}\} \cup S(\mathcal{P}_1) \cup S(\mathcal{P}_2)$ .
- Una **sottoformula** di  $\mathcal{P}$  è un elemento di  $S(\mathcal{P})$ .

### Osservazione

- Per qualsiasi fbf  $\mathcal{P}$ ,  $\mathcal{P}$  è una sottoformula di  $\mathcal{P}$ .
- Nella formula  $\mathcal{P} = ((\neg(A \vee B)) \rightarrow (A \vee B))$ :  
 $S(\mathcal{P}) = \{\mathcal{P}, (\neg(A \vee B)), (A \vee B), A, B\}$   
 $(A \vee B)$  compare due volte nella formula. Ci sono quindi due “istanze” della sottoformula nella formula.

<sup>II</sup>Siccome  $\varepsilon \notin X$ , togliere anche  $(\rightarrow)$  non toglie implicazioni.

## 5. Logica proposizionale

**Notazione** Nella scrittura di una fbf si possono togliere le parentesi esterne e quelle rese inutili dalle seguenti regole di precedenza:

$\neg > \wedge > \vee > \rightarrow$  (“ $>$ ” significa “ha precedenza maggiore”).

Ricordiamo che  $\rightarrow$  è associativa a sinistra:  $\mathcal{P}_1 \rightarrow \mathcal{P}_2 \rightarrow \mathcal{P}_3$  é  $(\mathcal{P}_1 \rightarrow \mathcal{P}_2) \rightarrow \mathcal{P}_3$ .

### Esempi

- $A \vee B \wedge C = (A \vee (B \wedge C))$
- $\neg A \vee B = ((\neg A) \vee B)$
- $\neg A \wedge B \vee C \rightarrow D = (((\neg A) \wedge B) \vee C) \rightarrow D$

### 5.1.2. Induzione

Ricordiamo il principio di induzione “classico”.

**Teorema** Sia  $\mathcal{P}(n)$  una proposizione dipendente da una variabile  $n$ .  $\mathcal{P}(n)$  è vera per ogni  $n \geq n_0$ ,  $n_0 \in \mathbb{N}$ , se per  $n_0$ :

1.  $\mathcal{P}(n_0)$  è vera; *passo base*
2. per qualsiasi  $n \geq n_0$ , se  $\mathcal{P}(n)$  è vera allora  $\mathcal{P}(n+1)$  è vera. *passo induttivo*

C’è un analogo per le fbf.

**Teorema** Sia  $\mathcal{A}(\mathcal{P})$  una proposizione che dipende da una proposizione variabile  $\mathcal{P}$ .  $\mathcal{A}(\mathcal{P})$  è vera per ogni fbf se:

1.  $\mathcal{A}(\mathcal{P})$  è vera per ogni fbf atomica  $\mathcal{P}$ ; *passo base*
2.  $\mathcal{A}(\perp)$  è vera; *passo base*
3. se per una fbf  $\mathcal{P}$ ,  $\mathcal{A}(\mathcal{P})$  è vera, allora  $\mathcal{A}(\neg \mathcal{P})$  è vera; *passo induttivo*
4. se per due fbf  $\mathcal{P}_1$  e  $\mathcal{P}_2$ ,  $\mathcal{A}(\mathcal{P}_1)$  e  $\mathcal{A}(\mathcal{P}_2)$  sono vere allora  $\mathcal{A}(\mathcal{P}_1 \vee \mathcal{P}_2)$ ,  $\mathcal{A}(\mathcal{P}_1 \wedge \mathcal{P}_2)$ ,  $\mathcal{A}(\mathcal{P}_1 \rightarrow \mathcal{P}_2)$  sono vere. *passo induttivo*

**Esempio**  $\mathcal{A}(\mathcal{P})$  è “l’insieme delle sottoformule  $S(\mathcal{P})$  è stato definito”.

Dalla definizione data di  $S(\mathcal{P})$  non si può avere la certezza che non esistano delle sottoformule “nascoste” che non conosciamo direttamente, ma dato che le ipotesi del teorema dell’induzione sono tutte verificate si ha la certezza che l’insieme  $S(\mathcal{P})$  sia completo.

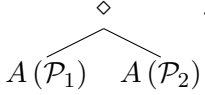
Analoghi ragionamenti permettono di dimostrare la “completezza” di molte definizioni sulle proposizioni.

### 5.1.3. Albero sintattico

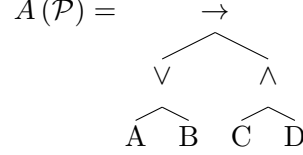
Se  $\mathcal{P}$  è una formula il suo albero sintattico  $A(\mathcal{P})$  si costruisce in questo modo:

- se  $\mathcal{P}$  è  $\perp$  o atomica,  $A(\mathcal{P}) = \mathcal{P}$ ;
- se  $\mathcal{P} = \neg \mathcal{P}_1$ ,  $A(\mathcal{P}) = \begin{array}{c} \neg \\ | \\ A(\mathcal{P}_1) \end{array}$ ;

## 5. Logica proposizionale

- se  $\mathcal{P} = \mathcal{P}_1 \diamond \mathcal{P}_2$ , dove  $\diamond$  è uno tra  $\vee$ ,  $\wedge$  e  $\rightarrow$ ,  $A(\mathcal{P}) =$  .

**Esempio**  $\mathcal{P} = A \vee B \rightarrow C \wedge D$ :



**Osservazione** Si ha la certezza di aver definito bene un albero per tutte le formule ben formate grazie al teorema di induzione.

### 5.1.4. Semantica

**Definizione** Un'*interpretazione* (o *valutazione*) è un'applicazione  $v : \mathcal{F} \rightarrow \{0, 1\}$  che soddisfa:

1.  $v(\perp) = 0$ ;
2.  $\forall \mathcal{P} \in \mathcal{F}, v(\neg \mathcal{P}) = 1 - v(\mathcal{P})$ ;
3.  $\forall \mathcal{P}_1 \in \mathcal{F}, \forall \mathcal{P}_2 \in \mathcal{F}, v(\mathcal{P}_1 \vee \mathcal{P}_2) = \max(v(\mathcal{P}_1), v(\mathcal{P}_2))$ ;
4.  $\forall \mathcal{P}_1 \in \mathcal{F}, \forall \mathcal{P}_2 \in \mathcal{F}, v(\mathcal{P}_1 \wedge \mathcal{P}_2) = \min(v(\mathcal{P}_1), v(\mathcal{P}_2))$ ;
5.  $\forall \mathcal{P}_1 \in \mathcal{F}, \forall \mathcal{P}_2 \in \mathcal{F}, v(\mathcal{P}_1 \rightarrow \mathcal{P}_2) = \max(1 - v(\mathcal{P}_1), v(\mathcal{P}_2))$ .

**Osservazione**

- La notazione usata nel punto (2) è un modo per scrivere in modo sintetico il concetto voluto, ossia che:
  - se  $v(\mathcal{P}) = 0$  allora  $v(\neg \mathcal{P}) = 1$ ;
  - se  $v(\mathcal{P}) = 1$  allora  $v(\neg \mathcal{P}) = 0$ .
- La notazione usata nel punto (3) è un modo per scrivere in modo sintetico il concetto voluto di  $\vee$ , ossia che basta che una delle 2 proposizioni abbia interpretazione 1 per far valere 1 l'interpretazione della  $\vee$  tra le 2.
- La notazione usata nel punto (4) è un modo per scrivere in modo sintetico il concetto voluto di  $\wedge$ , ossia che basta che una delle 2 proposizioni abbia interpretazione 0 per far valere 0 l'interpretazione della  $\wedge$  tra le 2.
- La notazione usata nel punto (5) è un modo per scrivere in modo sintetico il concetto voluto di  $\rightarrow$ , ossia che l'interpretazione vale 0 solo se  $v(\mathcal{P}_1) = 1$  e  $v(\mathcal{P}_2) = 0$ ; in tutti gli altri casi  $v(\mathcal{P}_1 \rightarrow \mathcal{P}_2) = 1$ .  
Alternativamente possiamo dire che  $v(\mathcal{P}_1 \rightarrow \mathcal{P}_2) = 0 \Leftrightarrow v(\mathcal{P}_1) = 1 \wedge v(\mathcal{P}_2) = 0$ .

**Proposizione** Siano  $v$  e  $v'$  due interpretazioni. Allora  $v = v'$  se e solo se per ogni formula atomica  $\mathcal{P}$  vale  $v(\mathcal{P}) = v'(\mathcal{P})$ .

## 5. Logica proposizionale

**Dimostrazione** Si usa il principio di induzione con  $\mathcal{A}(\mathcal{P}) = "v(\mathcal{P}) = v'(\mathcal{P})"$ .

Si può verificare senza particolare difficoltà che una volta assegnati dei valori  $v_0(A_i) \in \{0, 1\}$  per ogni simbolo atomico  $A_i$  esiste una (e una sola) interpretazione  $v$  tale che  $\forall i, v(A_i) = v_0(A_i)$ .

In pratica se una formula  $\mathcal{P}$  contiene  $n$  simboli atomici distinti, per sapere i valori delle interpretazioni mi basta considerare i  $2^n$  casi corrispondenti ai possibili valori 0 e 1 per i simboli atomici. Si organizzano in una cosiddetta “tabella di verità”.

$A$	$\neg A$	$A$	$B$	$A \vee B$	$A \wedge B$	$A \rightarrow B$
0	1	0	0	0	0	1
0	1	0	1	1	0	1
1	0	1	0	1	0	0
1	0	1	1	1	1	1

Attenzione per l'implicazione: se l'implicazione è vera e l'ipotesi è vera allora la tesi è vera.

Se l'ipotesi è falsa l'implicazione è vera indipendentemente dalla tesi: la tesi può essere vera o falsa. La riga in cui  $A = 0$  e  $B = 1$  si legge provocatoriamente “il falso implica il vero”.

È stato scelto di usare questa regola per distinguere la normale implicazione dall'uguaglianza o dall'implicazione a doppio verso in cui se l'ipotesi  $A$  è falsa allora deve esserlo anche l'implicazione  $B$  per rendere vera la tesi.

### Esempi

- “Se sono ricco allora sono intelligente” è un'implicazione vera, ma siccome non sono ricco non si può dire niente sulla mia intelligenza.
- “Se  $f$  è dispari e  $f(0)$  è definita allora  $f(0) = 0$ ”, se  $f$  non è dispari, per esempio  $f = x^2 + x$ , può darsi che  $f(0) = 0$ .

**Attenzione** Abbiamo tendenza a procedere per deduzione: sappiamo qualcosa, ne deduciamo qualcos'altro.

L'implicazione non è simmetrica: se  $A \rightarrow B$  non si può sapere se  $B \rightarrow A$ , per cui è meglio non partire dalla tesi per riportarsi alle ipotesi.

### Definizione

- Sia  $\mathcal{P}$  una fbf e  $v$  un'interpretazione. Si dice che  $\mathcal{P}$  è **soddisfatta in**  $v$ , oppure che  $v$  è un **modello per**  $\mathcal{P}$ , se e solo se  $v(\mathcal{P}) = 1$ . Si scrive  $v \models \mathcal{P}$ .
- Una fbf si dice **soddisfacibile** se e solo se ammette un modello.
- Una fbf si dice **insoddisfacibile** (o **contraddittoria**) se e solo se non ammette nessun modello.
- Una fbf  $\mathcal{P}$  si dice una **tautologia** se e solo se è soddisfatta in tutte le interpretazioni. Si scrive  $\models \mathcal{P}$ .

### Proposizione

- Una fbf  $\mathcal{P}$  è insoddisfacibile se e solo se  $\neg \mathcal{P}$  è una tautologia.
- Una fbf  $\mathcal{P}$  è una tautologia se e solo se  $\neg \mathcal{P}$  è insoddisfacibile.

## 5. Logica proposizionale

**Definizione** Sia  $\Gamma$  un insieme di fbf.

- Si dice che un'interpretazione  $v$  è un **modello per**  $\Gamma$  se e solo se per ogni  $\mathcal{P} \in \Gamma$ ,  $v(\mathcal{P}) = 1$  (cioè  $v$  è un modello per ogni  $\mathcal{P} \in \Gamma$ ).
- Si dice che  $\Gamma$  è **soddisfacibile** se e solo se ammette almeno un modello. Altrimenti si dice **insoddisfacibile** (o **contraddittorio**).
- Sia  $\mathcal{P}$  una fbf. Si dice che  $\mathcal{P}$  è una **conseguenza semantica** di  $\Gamma$  se e solo se ogni modello di  $\Gamma$  è un modello di  $\mathcal{P}$ . Si scrive  $\Gamma \models \mathcal{P}$ .

### Esempi

- $\Gamma = \{\neg A\}$ ,  $\mathcal{P} = A \rightarrow B$

$A$	$B$	$\neg A$	$A \rightarrow B$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	1

$\mathcal{P}$  è conseguenza semantica di  $\Gamma$

- $\Gamma = \{\neg A\}$ ,  $\mathcal{P}' = A \vee B$

$A$	$B$	$\neg A$	$A \vee B$
0	0	1	0
0	1	1	1
1	0	0	1
1	1	0	1

$\mathcal{P}'$  non è conseguenza semantica di  $\Gamma$

- Per verificare che una proposizione  $\mathcal{P}$  è conseguenza semantica di un insieme di proposizioni  $\Gamma$  basta seguire i seguenti passi:
  - si prepara la tabella di verità con tutti i possibili valori dei simboli atomici presenti nelle proposizioni di  $\Gamma$ ;
  - si procede a scrivere l'interpretazione per ogni proposizione presente in  $\Gamma$  nella tabella: se un'interpretazione vale 0 allora si cancella la riga ed è inutile continuare a calcolare l'interpretazione delle proposizioni successive su quella riga; se si cancellano tutte le righe prima di passare al punto dopo allora l'insieme  $\Gamma$  è insoddisfacibile e quindi tutte le proposizioni sono conseguenza semantica;
  - nelle righe non cancellate si calcola l'interpretazione di  $\mathcal{P}$ : se una è 0 allora ci si ferma perchè vuol dire che  $\mathcal{P}$  non è conseguenza semantica di  $\Gamma$ ; se invece tutte le interpretazioni valgono 1  $\mathcal{P}$  è conseguenza semantica di  $\Gamma$ .

**Notazione**  $\{\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_n\} \models \mathcal{P}$  si scrive  $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_n \models \mathcal{P}$ .

**Lemma** Siano  $\Gamma$  un insieme di fbf e  $\mathcal{P}$  una fbf. Allora  $\Gamma \models \mathcal{P}$  se e solo se  $\Gamma \cup \{\neg \mathcal{P}\}$  è insoddisfacibile.

### Dimostrazione

- Supponiamo  $\Gamma \models \mathcal{P}$ . Vogliamo mostrare che  $\Gamma \cup \{\neg \mathcal{P}\}$  è insoddisfacibile, cioè che nessuna interpretazione è un modello, ovvero che per ogni interpretazione  $v$  c'è almeno una formula in  $\Gamma \cup \{\neg \mathcal{P}\}$  che non è soddisfatta.  
Sia quindi  $v$  un'interpretazione. Se tutte le fbf in  $\Gamma$  sono soddisfatte allora  $v(\mathcal{P}) = 1$  perché  $\mathcal{P}$



## 5. Logica proposizionale

è conseguenza semantica di  $\Gamma$ , per cui  $v(\neg\mathcal{P}) = 0$ . Quindi in tutti i casi c'è almeno una fbf di  $\Gamma \cup \{\neg\mathcal{P}\}$  che non è soddisfatta in  $v$ .

- Supponiamo  $\Gamma \cup \{\neg\mathcal{P}\}$  insoddisfacibile, e sia  $v$  un'interpretazione che è un modello per  $\Gamma$ . Siccome  $\Gamma \cup \{\neg\mathcal{P}\}$  è insoddisfacibile, c'è almeno una fbf in  $\Gamma \cup \{\neg\mathcal{P}\}$  che non è soddisfatta in  $v$ . Siccome  $v$  è un modello per  $\Gamma$ , la suddetta fbf è per forza  $\neg\mathcal{P}$ , quindi  $v(\neg\mathcal{P}) = 0$  e quindi  $v(\mathcal{P}) = 1$ .  
Quindi  $\mathcal{P}$  è conseguenza semantica di  $\Gamma$ .

**Lemma** Siano  $\mathcal{P}_1$  e  $\mathcal{P}_2$  due fbf. Allora  $\mathcal{P}_1 \models \mathcal{P}_2$  se e solo se  $\mathcal{P}_1 \rightarrow \mathcal{P}_2$ .

### Dimostrazione

- Supponiamo  $\mathcal{P}_1 \models \mathcal{P}_2$ . Sia  $v$  un'interpretazione. Se  $v(\mathcal{P}_1) = 0$  allora  $v(\mathcal{P}_1 \rightarrow \mathcal{P}_2) = 1$  indipendentemente da  $v(\mathcal{P}_2)$ . Se invece  $v(\mathcal{P}_1) = 1$ , siccome  $\mathcal{P}_2$  è conseguenza semantica di  $\mathcal{P}_1$ ,  $v(\mathcal{P}_2) = 1$  e quindi  $v(\mathcal{P}_1 \rightarrow \mathcal{P}_2) = 1$ .  
Quindi  $\mathcal{P}_1 \rightarrow \mathcal{P}_2$  è una tautologia.
- Sia  $v$  un'interpretazione, se  $\mathcal{P}_1 \rightarrow \mathcal{P}_2$  è una tautologia allora se  $v(\mathcal{P}_1) = 1$ ,  $v(\mathcal{P}_2) = 1$ , e quindi  $\mathcal{P}_1 \models \mathcal{P}_2$ .

**Teorema (deduzione semantica)** Siano  $\mathcal{P}_1, \dots, \mathcal{P}_n$  e  $\mathcal{P}$  fbf,  $n \geq 1$ , allora  $\mathcal{P}_1, \dots, \mathcal{P}_n \models \mathcal{P}$  se e solo se  $\mathcal{P}_1, \dots, \mathcal{P}_{n-1} \models \mathcal{P}_n \rightarrow \mathcal{P}$ .

**Dimostrazione** Si sfrutta il teorema dell'induzione "classico", quindi bisogna dimostrare il passo base e il passo induttivo:

- per  $n = 1$ , bisognerebbe dimostrare che  $\mathcal{P}_1 \models \mathcal{P}$  se e solo se  $\mathcal{P}_1 \rightarrow \mathcal{P}$ , che è quello che si è dimostrato nel lemma precedente;
- se l'affermazione è vera per un  $n \geq 1$  allora è vera anche per  $n + 1$ .  
Sapendo che  $\mathcal{P}_1, \dots, \mathcal{P}_n \models \mathcal{P}$  se e solo se  $\mathcal{P}_1, \dots, \mathcal{P}_{n-1} \models \mathcal{P}_n \rightarrow \mathcal{P}$ , allora :  
dato che  $\mathcal{P}_1, \dots, \mathcal{P}_n \models \mathcal{P}$  allora  $\mathcal{P}_1, \dots, \mathcal{P}_n, \mathcal{P}_{n+1} \models \mathcal{P}$  è vera se e solo se  $\mathcal{P}_{n+1} \rightarrow \mathcal{P}$  e quindi  $\mathcal{P}_1, \dots, \mathcal{P}_n \models \mathcal{P}_{n+1} \rightarrow \mathcal{P}$ .

Quindi per il teorema di induzione il teorema è verificato per tutte le  $n \geq 1$ .

### 5.1.5. Equivalenza semantica

**Definizione** Siano  $\mathcal{P}_1$  e  $\mathcal{P}_2$  due fbf. Si dice che  $\mathcal{P}_1$  e  $\mathcal{P}_2$  sono *semanticamente equivalenti* se e solo se per ogni interpretazione  $v$  vale  $v(\mathcal{P}_1) = v(\mathcal{P}_2)$ . Si indica con  $\mathcal{P}_1 \equiv \mathcal{P}_2$ .

**Equivalenze semantiche fondamentali** Siano  $p, q$  e  $r$  tre formule fbf. Allora valgono:

## 5. Logica proposizionale

	$p \vee \neg p \equiv \top$	$p \wedge \neg p \equiv \perp$
<b>doppia negazione</b>	$\neg(\neg p) \equiv p$	
<b>contrapposizione</b>	$p \rightarrow q \equiv \neg q \rightarrow \neg p$	
	$p \rightarrow q \equiv \neg q \vee p$	
<b>cancellazione</b>	$p \wedge \top \equiv p$	$p \vee \perp \equiv p$
<b>dominanza</b>	$p \wedge \perp \equiv \perp$	$p \vee \top \equiv \top$
<b>idempotenza</b>	$p \vee p \equiv p$	$p \wedge p \equiv p$
<b>commutatività</b>	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
<b>associatività</b>	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
<b>doppia distributività</b>	$(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$	$(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$
<b>leggi di De Morgan</b>	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
<b>assorbimento</b>	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
<b>doppia ipotesi</b>	$p \rightarrow (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$	

**Dimostrazione** Le dimostrazioni si fanno tutte nello stesso modo facendo la tabella di verità e verificando che i risultati siano uguali. Esplicitiamo solo quella della contrapposizione perché è la più interessante.

$p$	$q$	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg q \rightarrow \neg p$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	0	0
1	1	0	0	1	1

per ogni  $v$ ,  $v(p \rightarrow q) = v(\neg q \rightarrow \neg p)$ .

**Definizione** Siano  $\mathcal{P}_1$  e  $\mathcal{P}_2$  due fbf e  $A$  un simbolo atomico. Definiamo  $\mathcal{P}_1[\mathcal{P}_2/A]$  per induzione:

1. se  $\mathcal{P}_1$  è atomica:
  - a) se  $\mathcal{P}_1 = A$ , allora  $\mathcal{P}_1[\mathcal{P}_2/A] = \mathcal{P}_2$ ;
  - b) se  $\mathcal{P}_1 \neq A$ , allora  $\mathcal{P}_1[\mathcal{P}_2/A] = \mathcal{P}_1$ ;
2. se  $\mathcal{P}_1 = \perp$ ,  $\mathcal{P}_1[\mathcal{P}_2/A] = \mathcal{P}_1 = \perp$ ;
3. se  $\mathcal{P}_1 = \neg \mathcal{Q}_1$ ,  $\mathcal{P}_1[\mathcal{P}_2/A] = \neg(\mathcal{Q}_1[\mathcal{P}_2/A])$ ;
4. se  $\mathcal{P}_1 = \mathcal{Q}_1 \diamond \mathcal{Q}_2$ , dove  $\diamond$  è uno tra  $\vee$ ,  $\wedge$  e  $\rightarrow$ ,  $\mathcal{P}_1[\mathcal{P}_2/A] = (\mathcal{Q}_1[\mathcal{P}_2/A]) \diamond (\mathcal{Q}_2[\mathcal{P}_2/A])$ .

### Osservazione

- Il teorema dell'induzione ci assicura di aver scritto una definizione completa.
- Con  $\mathcal{P}_1[\mathcal{P}_2/A]$  si intende la proposizione  $\mathcal{P}_1$  sostituendo al simbolo atomico  $A$  la proposizione  $\mathcal{P}_2$ .

**Teorema** Siano  $\mathcal{P}_1$ ,  $\mathcal{P}_2$ ,  $\mathcal{P}_3$  fbf,  $A$  un simbolo atomico e  $v$  un'interpretazione. Se  $v(\mathcal{P}_1) = v(\mathcal{P}_2)$  allora  $v(\mathcal{P}_3[\mathcal{P}_1/A]) = v(\mathcal{P}_3[\mathcal{P}_2/A])$ .

**Corollario** Se  $\mathcal{P}_1 \equiv \mathcal{P}_2$  allora per qualsiasi  $A$  e  $\mathcal{P}_3$ ,  $\mathcal{P}_3[\mathcal{P}_1/A] \equiv \mathcal{P}_3[\mathcal{P}_2/A]$ .

### 5.1.6. Completezza funzionale

#### Definizione

- Sia  $\mathcal{P}$  una fbf, e  $A_1, \dots, A_n$  i simboli atomici che compaiono in  $\mathcal{P}$ . Si definisce l'applicazione  $f_{\mathcal{P}}$  da  $\{0, 1\}^n$  in  $\{0, 1\}$  e  $f_{\mathcal{P}}(v(A_1), v(A_2), \dots, v(A_n)) = v(\mathcal{P})$  dove  $v$  è una qualsiasi interpretazione.
- Se  $\mathcal{P} = \neg A$  allora  $f_{\mathcal{P}}$  si denota  $f_{\neg}$ ;  
se  $\mathcal{P} = A \diamond B$ , dove  $\diamond$  è uno tra  $\vee, \wedge$  e  $\rightarrow$ , allora  $f_{\mathcal{P}}$  si denota  $f_{\diamond}$ .

#### Osservazione

- Questa funzione  $f_{\mathcal{P}}$  va interpretata come una funzione che trasferisce il vettore delle interpretazioni dei simboli atomici sull'interpretazione della proposizione  $\mathcal{P}$ .  
Quindi è la funzione che rappresenta la tabella di verità.
- $\mathcal{P}_1 \equiv \mathcal{P}_2$  se e solo se  $f_{\mathcal{P}_1} = f_{\mathcal{P}_2}$ .

**Definizione** Sia  $\mathcal{C}$  un insieme di connettivi e sia  $c$  un connettivo. Si dice che  $c$  è **derivabile** da  $\mathcal{C}$  se e solo se esiste una fbf  $\mathcal{P}$  i cui connettivi sono in  $\mathcal{C}$  tale che  $f_c = f_{\mathcal{P}}$ .

#### Osservazione

- Un connettore  $c$  è derivabile in  $\mathcal{C}$  se può essere scritto in modo equivalente usando solo i connettori in  $\mathcal{C}$ .  
Ad esempio se  $\mathcal{C} = \{\neg, \vee\}$  e  $c = \wedge$  per il teorema di De Morgan  $A \wedge B = \neg(\neg A \vee \neg B)$  con  $A$  e  $B$  simboli atomici e quindi  $\wedge$  è derivabile in  $\mathcal{C}$ .
- I connettori contenuti nell'insieme sono sempre derivabili per quell'insieme, per ovvie ragioni e quindi ha poco senso parlarne.

**Definizione** Si dice che  $\mathcal{C}$  è **funzionalmente completo** se e solo se tutti i connettivi sono derivabili da  $\mathcal{C}$ .

**Osservazione** Se tutti i connettivi sono derivabili da  $\mathcal{C}$  vuol dire che tutte le formule ben formate possono essere scritte in modo equivalente usando solo i connettori presenti in  $\mathcal{C}$ .

**Proposizione** I seguenti insiemi di connettivi sono funzionalmente completi:  $\{\neg, \vee\}$ ,  $\{\neg, \wedge\}$ ,  $\{\neg, \rightarrow\}$ ,  $\{\perp, \rightarrow\}$ ,  $\{\nabla\}^{\text{III}}$ ,  $\{\bar{\wedge}\}^{\text{IV}}$ .

**Dimostrazione** Si può fare utilizzando le equivalenze semantiche fondamentali.

### 5.1.7. Dualità

**Definizione** Sia  $\mathcal{P}$  una fbf i cui connettivi sono in  $\{\neg, \vee, \wedge\}$ . La fbf **duale** di  $\mathcal{P}$  è la fbf  $\mathcal{P}^{\vee}$  tale che:

1. se  $\mathcal{P}$  è atomica,  $\mathcal{P}^{\vee} = \mathcal{P}$ ;
2. se  $\mathcal{P} = \neg \mathcal{P}_1$ ,  $\mathcal{P}^{\vee} = \neg(\mathcal{P}_1^{\vee})$ ;
3. se  $\mathcal{P} = \mathcal{P}_1 \vee \mathcal{P}_2$ ,  $\mathcal{P}^{\vee} = \mathcal{P}_1^{\vee} \wedge \mathcal{P}_2^{\vee}$ ;  
se  $\mathcal{P} = \mathcal{P}_1 \wedge \mathcal{P}_2$ ,  $\mathcal{P}^{\vee} = \mathcal{P}_1^{\vee} \vee \mathcal{P}_2^{\vee}$ .

<sup>III</sup>È il simbolo di NOR:  $(A \nabla B) \equiv \neg(A \vee B)$ .

<sup>IV</sup>È il simbolo di NAND:  $(A \bar{\wedge} B) \equiv \neg(A \wedge B)$ .

## 5.2. Forme normali

### 5.2.1. Definizione

- Un **letterale** è una fbf atomica o la negazione di un simbolo atomico.
- Una fbf  $\mathcal{P}$  è detta in **forma normale congiuntiva** (anche abbreviato con “fnc”) se e solo se  $\mathcal{P} = \mathcal{P}_1 \wedge \mathcal{P}_2 \wedge \dots \wedge \mathcal{P}_n$  con  $n \geq 0$  e ogni  $\mathcal{P}_i = \mathcal{R}_{i,1} \vee \dots \vee \mathcal{R}_{i,k_i}$  con  $k_i \geq 1$  e ogni  $\mathcal{R}_{i,j}$  è un letterale.
- Una fbf  $\mathcal{P}$  è detta in **forma normale disgiuntiva** (anche abbreviato con “fnd”) se e solo se  $\mathcal{P} = \mathcal{P}_1 \vee \mathcal{P}_2 \vee \dots \vee \mathcal{P}_n$  con  $n \geq 0$  e ogni  $\mathcal{P}_i = \mathcal{R}_{i,1} \wedge \dots \wedge \mathcal{R}_{i,k_i}$  con  $k_i \geq 1$  e ogni  $\mathcal{R}_{i,j}$  è un letterale.
- $\mathcal{P} = \neg \perp$  è in fnc con  $n = 0$ .
- $\mathcal{P} = \perp$  è in fnd con  $n = 0$ .

### Esempi

- $A \wedge \neg B \wedge (A \vee C)$  è in fnc, con  $n = 3$ ,  $k_1 = 1$ ,  $k_2 = 1$ ,  $k_3 = 2$ ;
- $A \vee (B \wedge \neg C) \vee \neg C$  è in fnd, con  $n = 3$ ,  $k_1 = 1$ ,  $k_2 = 2$ ,  $k_3 = 1$ ;
- $A \wedge \neg B \wedge \neg C \wedge D$  è:
  - in fnc, con  $n = 4$ ,  $k_1 = k_2 = k_3 = k_4 = 1$ ;
  - in fnd, con  $n = 1$ ,  $k_1 = 4$ .

### 5.2.2. Esistenza

**Teorema** Sia  $\mathcal{P}$  una fbf. Allora esistono  $\mathcal{P}^c$  e  $\mathcal{P}^d$  fbf rispettivamente in fnc e fnd tali che  $\mathcal{P} \equiv \mathcal{P}^c$  e  $\mathcal{P} \equiv \mathcal{P}^d$ .

**Dimostrazione** Costruiamo  $\mathcal{P}^c$  e  $\mathcal{P}^d$ . A tal fine, fare la tavola di verità di  $\mathcal{P}$  e:

- per la fnd: per ogni riga in cui l’interpretazione  $v$  vale 1, costruire la congiunzione  $\mathcal{R}_i = L_1 \wedge L_2 \wedge \dots \wedge L_k$  con  $L_i = A_i$  se  $v(A_i) = 1$  e  $L_i = \neg A_i$  se  $v(A_i) = 0$ ; in questo modo le  $\mathcal{R}_i$  costruite hanno un solo modello ed è l’interpretazione della riga in esame. Facendo la disgiunzione  $\mathcal{P}^d$  (ossia la  $\vee$ ) di tutte le  $\mathcal{R}_i$  si ottiene una fbf che ha come modelli quelli delle singole  $\mathcal{R}_i$  e quindi la disgiunzione  $\mathcal{P}^d$  ha gli stessi modelli di  $\mathcal{P}$ .
- per la fnc: per ogni riga in cui l’interpretazione  $v$  vale 0, costruire la disgiunzione  $\mathcal{R}_i = L_1 \vee L_2 \vee \dots \vee L_k$  con  $L_i = A_i$  se  $v(A_i) = 0$  e  $L_i = \neg A_i$  se  $v(A_i) = 1$ ; in questo modo le  $\mathcal{R}_i$  costruite non sono soddisfatte solo nell’interpretazione della riga in esame. Facendo la congiunzione  $\mathcal{P}^c$  (ossia la  $\wedge$ ) di tutte le  $\mathcal{R}_i$  si ottiene una fbf che non è soddisfatta dalle interpretazioni che non sono soddisfatte nelle singole  $\mathcal{R}_i$ ; quindi la  $\mathcal{P}^c$  non è soddisfatta dalle interpretazioni dove non è soddisfatta la  $\mathcal{P}$ , e quindi ha gli stessi modelli.

### Osservazione

- Il teorema garantisce l’esistenza di una fnc e una fnd equivalenti, ma non dice che sono uniche; infatti ne esistono più di una equivalenti.
- Questo teorema dimostra anche che l’insieme  $\{\neg, \vee, \wedge\}$  è funzionalmente completo, infatti tutte le fbf possono essere scritte usando solo quei 3 connettivi.

### 5.3. Sistemi deduttivi

#### 5.3.1. Idea

Consideriamo la formula  $\mathcal{P} = (A \rightarrow B) \wedge (A \rightarrow (B \rightarrow C)) \rightarrow (A \rightarrow C)$ . Questa fbf è una tautologia.

Piuttosto che fare la tavola di verità possiamo analizzare  $\mathcal{P}$ . È un'implicazione di cui l'ipotesi è la congiunzione di  $A \rightarrow B$  e  $A \rightarrow (B \rightarrow C)$  e la tesi è  $A \rightarrow C$ .  $\mathcal{P}$  può essere falsa solo se la sua ipotesi è vera e la tesi falsa.

Per avere la tesi falsa dobbiamo avere  $A$  vera e  $C$  falsa.

Per avere l'ipotesi vera le due implicazioni che la compongono devono essere vere, per cui nella prima  $B$  è vera. Nella seconda viene che  $B \rightarrow C$  dev'essere vera, ma ciò è falso perché  $B$  è vera e  $C$  è falsa.

Per cui non c'è nessuna interpretazione in cui  $\mathcal{P}$  è falsa.

$\mathcal{P}$	$($	$A$	$\rightarrow$	$B$	$)$	$\wedge$	$($	$A$	$\rightarrow$	$($	$B$	$\rightarrow$	$C$	$)$	$\rightarrow$	$($	$A$	$\rightarrow$	$C$	$)$
1															F					
2						V												F		
3			V					V									V		F	
4		V					V				V	F								
5				V																
6																				

Un sistema deduttivo è un insieme di regole che formalizzano ragionamenti di questo tipo.

Che cosa si considera di un sistema deduttivo:

- la **correttezza**: che si possano dimostrare solo le tautologie (o le conseguenze semantiche);
- la **completezza**: che si permetta di dimostrare tutte le tautologie (o le conseguenze semantiche).

La correttezza è più importante della completezza, perché è inutile avere un sistema deduttivo da cui si può dedurre tutto ma non sai se stai deducendo correttamente.

#### 5.3.2. Deduzione naturale

Se  $\Gamma = \{\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n\}$  è un insieme di fbf e  $\mathcal{B}$  una fbf, indicheremo con  $\Gamma \vdash \mathcal{B}$  o  $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n \vdash \mathcal{B}$  che dalle fbf  $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n$  si può dedurre  $\mathcal{B}$  nel sistema della deduzione naturale.

Il sistema si presenta come una serie di deduzioni che permettono di introdurre o eliminare un connettivo, più due regole “fuori serie”.

( $\wedge e$ )

( $\wedge e.1$ )  $\mathcal{A}_1 \wedge \mathcal{A}_2 \vdash \mathcal{A}_1$   
Se  $\mathcal{A}_1 \wedge \mathcal{A}_2$  è vero si può dedurre che  $\mathcal{A}_1$  è vero

( $\wedge e.2$ )  $\mathcal{A}_1 \wedge \mathcal{A}_2 \vdash \mathcal{A}_2$   
Se  $\mathcal{A}_1 \wedge \mathcal{A}_2$  è vero si può dedurre che  $\mathcal{A}_2$  è vero

( $\wedge i$ )  $\mathcal{A}_1, \mathcal{A}_2 \vdash \mathcal{A}_1 \wedge \mathcal{A}_2$   
Se sia  $\mathcal{A}_1$  che  $\mathcal{A}_2$  sono veri allora si può dedurre che  $\mathcal{A}_1 \wedge \mathcal{A}_2$  è vero

\*( $\vee e$ ) se  $\mathcal{A}_1 \vdash \mathcal{A}_3$  e  $\mathcal{A}_2 \vdash \mathcal{A}_3$  allora  $\mathcal{A}_1 \vee \mathcal{A}_2 \vdash \mathcal{A}_3$   
Se quando  $\mathcal{A}_1$  è vero si può dedurre che  $\mathcal{A}_3$  è vero e quando  $\mathcal{A}_2$  è vero si può dedurre che  $\mathcal{A}_3$  è vero allora  
se  $\mathcal{A}_1 \vee \mathcal{A}_2$  è vero (ossia almeno una tra  $\mathcal{A}_1$  e  $\mathcal{A}_2$  è vera) si può dedurre che  $\mathcal{A}_3$  è vero

## 5. Logica proposizionale

( $\vee i$ )

( $\vee i.1$ )  $\mathcal{A}_1 \vdash \mathcal{A}_1 \vee \mathcal{A}_2$

Se  $\mathcal{A}_1$  è vero si può dedurre che  $\mathcal{A}_1 \vee$  "qualsiasi cosa" è vero

( $\vee i.2$ )  $\mathcal{A}_2 \vdash \mathcal{A}_1 \vee \mathcal{A}_2$

( $\rightarrow e$ )  $\mathcal{A}_1, \mathcal{A}_1 \rightarrow \mathcal{A}_2 \vdash \mathcal{A}_2$

Se  $\mathcal{A}_1 \rightarrow \mathcal{A}_2$  è vero e  $\mathcal{A}_1$  è vero si può dedurre che  $\mathcal{A}_2$  è vero

\*( $\rightarrow i$ ) se  $\mathcal{A}_1 \vdash \mathcal{A}_2$  allora  $\vdash \mathcal{A}_1 \rightarrow \mathcal{A}_2$

Se quando  $\mathcal{A}_1$  è vero si può dedurre che  $\mathcal{A}_2$  è vero allora si può dedurre che  $\mathcal{A}_1 \rightarrow \mathcal{A}_2$  è sempre vera

( $\perp e$ )  $\perp \vdash \mathcal{A}_1$

Dato che il  $\perp$  non è mai vero allora tutto è vero quando il  $\perp$  è vero (dato che non lo è mai) e quindi dal  $\perp$  si può dedurre qualsiasi cosa

( $\neg e$ )  $\mathcal{A}_1, \neg \mathcal{A}_1 \vdash \perp$

In nessun caso  $\mathcal{A}_1$  e  $\neg \mathcal{A}_1$  sono veri entrambi quindi si può dedurre il  $\perp$  (che è falso sempre)

\*( $\neg i$ ) se  $\mathcal{A}_1 \vdash \perp$  allora  $\vdash \neg \mathcal{A}_1$

Se quando  $\mathcal{A}_1$  è vero si può dedurre che il  $\perp$  è vero allora  $\mathcal{A}_1$  è sempre falso e quindi si può dedurre che  $\neg \mathcal{A}_1$  è sempre vero

\*(taglio) se  $\Gamma \vdash \mathcal{A}_1$  e  $\Gamma, \mathcal{A}_1 \vdash \mathcal{A}_2$  allora  $\Gamma \vdash \mathcal{A}_2$

Se quando tutte le fbf di  $\Gamma$  sono vere si può dedurre che  $\mathcal{A}_1$  è vero, e quando tutte le fbf di  $\Gamma$  e  $\mathcal{A}_1$  sono vere si può dedurre che  $\mathcal{A}_2$  è vera allora

se tutte le fbf di  $\Gamma$  sono vere si può dedurre che  $\mathcal{A}_2$  è vero

\*(RAA) se  $\neg \mathcal{A}_1 \vdash \perp$  allora  $\vdash \mathcal{A}_1$

Se quando  $\neg \mathcal{A}_1$  è vero si può dedurre che il  $\perp$  è vero allora  $\neg \mathcal{A}_1$  è sempre falso e quindi si può dedurre che  $\mathcal{A}_1$  è sempre vero

### Osservazione

- I nomi delle regole (escluso il taglio e la RAA) si formano mettendo il connettore coinvolto seguito da "*i*" se si inserisce il connettore o "*e*" se lo si elimina (si aggiunge "*n*" se ce ne sono più d'una di quel tipo).
- La regola del taglio formalizza la tecnica "del lemma": si dimostra un risultato intermedio che aiuta nella dimostrazione di un risultato più grosso.
- Le regole asteriscate sono più complicate delle altre. Si chiamano regole **condizionali**, mentre le altre si chiamano regole **semplici**.  
Nel caso in cui  $\mathcal{A}_1 \vdash \mathcal{A}_2$  è nelle ipotesi di una regola condizionale la fbf  $\mathcal{A}_1$  si chiama **premessa sussidiaria**, mentre  $\mathcal{A}_2$  si chiama **conclusione sussidiaria** della regola.
- La RAA si chiama riduzione all'assurdo. Tramite ( $\perp e$ ) e ( $\neg e$ ) si può verificare che è equivalente alla cosiddetta **regola di Peirce**: se da  $\neg \mathcal{A} \vdash \mathcal{A}$  allora  $\vdash \mathcal{A}$ .
- La RAA o la regola di Peirce possono essere eliminate dal sistema. Il sistema è allora detto "intuizionistico".

### 5.3.3. Rappresentazione ad albero

Le regole semplici si rappresentano come una “frazione” in cui le ipotesi sono sopra la riga e la conclusione sotto. Se la conclusione di una regola coincide con la premessa di un’altra si collegano le regole per formare un albero.

$(\wedge e)$

$$(\wedge e.1) \quad \frac{\mathcal{A}_1 \wedge \mathcal{A}_2}{\mathcal{A}_1}$$

$$(\wedge e.2) \quad \frac{\mathcal{A}_1 \wedge \mathcal{A}_2}{\mathcal{A}_2}$$

$$(\wedge i) \quad \frac{\mathcal{A}_1 \quad \mathcal{A}_2}{\mathcal{A}_1 \wedge \mathcal{A}_2}$$

$(\vee i)$

$$(\vee i.1) \quad \frac{\mathcal{A}_1}{\mathcal{A}_1 \vee \mathcal{A}_2}$$

$$(\vee i.2) \quad \frac{\mathcal{A}_2}{\mathcal{A}_1 \vee \mathcal{A}_2}$$

$$(\rightarrow e) \quad \frac{\mathcal{A}_1 \quad \mathcal{A}_1 \rightarrow \mathcal{A}_2}{\mathcal{A}_2}$$

$$(\perp e) \quad \frac{\perp}{\mathcal{A}_1}$$

$$(\neg e) \quad \frac{\mathcal{A}_1 \quad \neg \mathcal{A}_1}{\perp}$$

La regola del taglio dice che le premesse della dimostrazione sono le foglie dell’albero e la conclusione la radice.

**Esempio** L’albero seguente rappresenta la deduzione  $A \wedge B, B \wedge A \rightarrow C \vdash C \vee D$ :

$$\frac{\frac{\frac{A \wedge B}{B} (\wedge e.2) \quad \frac{A \wedge B}{A} (\wedge e.1)}{B \wedge A} (\wedge i) \quad \frac{B \wedge A \rightarrow C}{C} (\rightarrow e)}{C \vee D} (\vee i.1)$$

Le regole condizionali si rappresentano aggiungendo le conclusioni sussidiarie come premesse “supplementari”, e si scrivono sopra le conclusioni sussidiarie le premesse sussidiarie tra parentesi quadre.

$$(\vee e) \quad \frac{\mathcal{A}_1 \vee \mathcal{A}_2 \quad \begin{array}{c} [\mathcal{A}_1] \\ \mathcal{A}_3 \end{array} \quad \begin{array}{c} [\mathcal{A}_2] \\ \mathcal{A}_3 \end{array}}{\mathcal{A}_3}$$

$$(\rightarrow i) \quad \frac{\begin{array}{c} [\mathcal{A}_1] \\ \mathcal{A}_2 \end{array}}{\mathcal{A}_1 \rightarrow \mathcal{A}_2}$$

$$(\neg i) \quad \frac{\begin{array}{c} [\mathcal{A}_1] \\ \perp \end{array}}{\neg \mathcal{A}_1}$$

$$(RAA) \quad \frac{\begin{array}{c} [\neg \mathcal{A}_1] \\ \perp \end{array}}{\mathcal{A}_1}$$

## 5. Logica proposizionale

La regola del taglio si modifica in questo modo: nel sottoalbero che ha come radice una conclusione sussidiaria possiamo mettere la corrispondente ipotesi sussidiaria tra parentesi quadre. Tutte le foglie tra parentesi quadre sono considerate cancellate e non fanno più parte delle premesse della deduzione.

**Esempio**  $\frac{A}{B \rightarrow A} (\rightarrow i)$

Riapplico la regola:

$$\frac{\frac{[A]}{B \rightarrow A} (\rightarrow i)}{A \rightarrow (B \rightarrow A)} (\rightarrow i)$$

dimostra  $\vdash A \rightarrow (B \rightarrow A)$ .

### 5.3.4. Interpretazione semantica

**Definizione** Un insieme  $\Gamma$  di fbf è detto *inconsistente* se e solo se  $\Gamma \vdash \perp$ , *consistente* nel caso contrario.

**Lemma** Le seguenti condizioni risultano equivalenti:

1.  $\Gamma$  è inconsistente;
2. esiste una fbf tale che  $\Gamma \vdash \mathcal{P}$  e  $\Gamma \vdash \neg \mathcal{P}$ ;
3. per qualsiasi fbf  $\mathcal{P}$ ,  $\Gamma \vdash \mathcal{P}$ .

**Corollario (correttezza)** se  $\vdash \mathcal{P}$  allora  $\models \mathcal{P}$ .

**Definizione** Se una fbf  $\mathcal{P}$  è tale che  $\vdash \mathcal{P}$ ,  $\mathcal{P}$  si dice un *teorema* del sistema di deduzione naturale.

Vale il teorema: se  $\Gamma$  è un insieme di fbf e  $\mathcal{P}$  una fbf, se  $\Gamma \models \mathcal{P}$  allora  $\Gamma \vdash \mathcal{P}$ .

### Confronto di concetti

lato semantico	lato sistemi deduttivi
$\Gamma \models \mathcal{A}$ conseguenza semantica	$\Gamma \vdash \mathcal{A}$ derivabilità
$\models \mathcal{A}$ tautologia	$\vdash \mathcal{A}$ teorema
$\Gamma \not\models \perp$ soddisfacibile	$\Gamma \not\vdash \perp$ consistente
$\Gamma \models \perp$ insoddisfacibile	$\Gamma \vdash \perp$ inconsistente

### 5.3.5. Risoluzione a clausole

#### Definizione

- Una *clausola* è una disgiunzione di letterali.
- La *clausola vuota* è  $\perp^V$ .
- Una fbf in fnc si dice in *forma a clausole*.
- Se  $R$  è un letterale denoteremo  $\sim R$  il letterale “opposto”, cioè se  $R = A_i$ ,  $\sim R = \neg A_i$ , se  $R = \neg A_i$ ,  $\sim R = A_i$ .

---

<sup>V</sup>In questo modo  $v(\{\{\}, \{A\}\}) = v(\{\} \vee \{A\}) = \max(v(\perp), v(A)) = \max(0, v(A)) = v(A)$ .



## 5. Logica proposizionale

**Osservazione**  $\sim R \equiv \neg R$  ma non è necessariamente uguale.

### Notazione

- La clausola vuota si rappresenta con un  $\square$ .
- Una clausola si rappresenta come l'insieme dei letterali che la compongono.
- Una fbf in forma a clausole si rappresenta come l'insieme delle sue clausole.

**Esempio**  $A \wedge (\neg B \vee A) \wedge (\neg A \vee B \vee \neg C)$  si rappresenta  $\{\{A\}, \{\neg B, A\}, \{\neg A, B, \neg C\}\}$ .

**Definizione** Se  $\mathcal{C}_1$  e  $\mathcal{C}_2$  sono due clausole si dice che  $\mathcal{R}$  è una **risolvente** per  $\mathcal{C}_1$  e  $\mathcal{C}_2$  se e solo se esiste un letterale  $L$  tale che  $L \in \mathcal{C}_1$ ,  $\sim L \in \mathcal{C}_2$  e  $\mathcal{R} = (\mathcal{C}_1 \setminus \{L\}) \cup (\mathcal{C}_2 \setminus \{\sim L\})$ .

**Esempio**  $\mathcal{C}_1 = \{\neg A, \neg B, C\}$  e  $\mathcal{C}_2 = \{A, \neg B, \neg C\}$ .

Con  $L = \neg A$ ,  $\mathcal{R} = \{\neg B, C, \neg C\}$ .

Con  $L = C$ ,  $\mathcal{R} = \{\neg A, \neg B, A\}$ .

**Lemma** Se  $\mathcal{C}_1$  e  $\mathcal{C}_2$  sono due clausole e  $\mathcal{R}$  una risolvente per  $\mathcal{C}_1$  e  $\mathcal{C}_2$  allora  $\mathcal{C}_1, \mathcal{C}_2 \models \mathcal{R}$ .

**Dimostrazione** Siano  $\mathcal{C}_1 = L_0 \vee L_{1,1} \vee \dots \vee L_{1,n}$  e  $\mathcal{C}_2 = \sim L_0 \vee L_{2,1} \vee \dots \vee L_{2,m}$  dove  $m, n \in \mathbb{N}$ ,  $L_{i,j}$  dei letterali distinti e  $L_0$  è il letterale (diverso dagli altri) comune che permette di creare la risolvente  $\mathcal{R} = L_{1,1} \vee \dots \vee L_{1,n} \vee L_{2,1} \vee \dots \vee L_{2,m}$ .

Supponiamo  $L_0 = A$  e quindi  $\sim L_0 = \neg A$ ; se fosse il contrario si otterrebbe un risultato semanticamente equivalente.

$\mathcal{C}_1$  ha solo una interpretazione  $v_1$  tale per cui  $v_1(\mathcal{C}_1) = 0$  e in cui  $v_1(L_0) = 0$  in quanto è una disgiunzione di letterali.

$\mathcal{C}_2$  ha solo una interpretazione  $v_2$  tale per cui  $v_2(\mathcal{C}_2) = 0$  e in cui  $v_2(\sim L_0) = 0$  (cioè  $v_2(L_0) = 1$ ) in quanto è una disgiunzione di letterali.

Perché sia vero che  $\mathcal{C}_1, \mathcal{C}_2 \models \mathcal{R}$ ,  $\mathcal{R}$  dovrà essere soddisfatta da tutte le interpretazioni escluse  $v_1$  e  $v_2$ .

Sia  $v$  una interpretazione dove  $v(\mathcal{R}) = 0$ , allora  $\max(v(L_{1,1} \vee \dots \vee L_{1,n}), v(L_{2,1} \vee \dots \vee L_{2,m})) = 0$  e quindi  $v(L_{1,1} \vee \dots \vee L_{1,n}) = 0$  e  $v(L_{2,1} \vee \dots \vee L_{2,m}) = 0$ .

Se  $v(L_0) = 0$  e  $v(L_{1,1} \vee \dots \vee L_{1,n}) = 0$  allora  $v = v_1$  e quindi non ci interessa.

Se  $v(L_0) = 1$  e  $v(L_{2,1} \vee \dots \vee L_{2,m}) = 0$  allora  $v = v_2$  e quindi non ci interessa.

Quindi non esiste una interpretazione  $v$  diversa da  $v_1$  e  $v_2$  tale che  $v(\mathcal{R}) = 0$ , quindi  $\mathcal{C}_1, \mathcal{C}_2 \models \mathcal{R}$ .

### Osservazione

- Per la semantica,  $\mathcal{P}_1 \wedge \mathcal{P}_2$  ha gli stessi modelli dell'insieme  $\{\mathcal{P}_1, \mathcal{P}_2\}$ .
- Per la deduzione naturale, se  $\mathcal{P}_1 \wedge \mathcal{P}_2 \vdash \mathcal{P}_3$  allora  $\mathcal{P}_1, \mathcal{P}_2 \vdash \mathcal{P}_3$  e se  $\mathcal{P}_1, \mathcal{P}_2 \vdash \mathcal{P}_3$  allora  $\mathcal{P}_1 \wedge \mathcal{P}_2 \vdash \mathcal{P}_3$ .

**Notazione** Un insieme di fbf in forma a clausole si rappresenta come l'unione degli insiemi di clausole delle singole fbf:

$$\{(A \vee B) \wedge (\neg A \vee C), (A \vee B \vee \neg C) \wedge (B \vee C)\}$$

si rappresenta con

$$\{\{A, B\}, \{\neg A, C\}, \{A, B, \neg C\}, \{B, C\}\}$$

che è equivalente per l'osservazione precedente.

## 5. Logica proposizionale

**Definizione** Siano  $\Gamma$  un insieme di forme a clausole e  $\mathcal{C}$  una clausola.

Una **derivazione di  $\mathcal{C}$  per risoluzione da  $\Gamma$**  è una successione  $(\Gamma_i)_{1 \leq i \leq n}$  di insiemi di forme a clausole tale che:

- $\Gamma_1 = \Gamma$ ;
- $\forall i, \Gamma_{i+1} = \Gamma_i \cup \{\mathcal{R}_i\}$  e  $\mathcal{R}_i$  è una risolvente per due clausole di  $\Gamma_i$ ;
- $\mathcal{C} \in \Gamma_n$ .

In tal caso si scrive  $\Gamma \vdash_{\mathcal{R}} \mathcal{C}$ .

**Teorema (correttezza)** Un insieme di fbf  $\Gamma$  è insoddisfacibile se e solo se  $\Gamma \vdash_{\mathcal{R}} \square$ .

Il sistema di risoluzione non è completo: esistono insiemi di fbf  $\Gamma$  e clausole  $\mathcal{C}$  tali che  $\Gamma \models \mathcal{C}$  ma  $\Gamma \not\vdash_{\mathcal{R}} \mathcal{C}$ .

**Corollario (completezza per refutazione)** Se  $\Gamma$  è un insieme di fbf e  $\mathcal{P}$  una fbf,  $\Gamma \models \mathcal{P}$  se e solo se  $\Gamma \cup \{\neg \mathcal{P}\} \vdash_{\mathcal{R}} \square$ .

### Esempi

- $A \models A \vee B$ .  
 $\Gamma = \{\{A\}\}, \mathcal{C} = \{A, B\}$ .  
 Da  $\Gamma$  non possiamo “fabbricare” risolventi, per cui da  $\Gamma$  non possiamo derivare niente (inoltre non ci sarebbe nessun modo di far “compare”  $B$ ).
- $A \models \mathcal{P}, \mathcal{P} = A \vee B$ .  
 $\Gamma' = \{A, \neg(A \vee B)\}, \Gamma'^c = \{A, \neg A \wedge \neg B\}, \Gamma'^{clausole} = \{\{A\}, \{\neg A\}, \{\neg B\}\}$ .  
 Scegliamo  $\mathcal{C}_1 = \{A\}, \mathcal{C}_2 = \{\neg A\}, L = A$ , quindi  $\mathcal{R} = (\mathcal{C}_1 \setminus \{A\}) \cup (\mathcal{C}_2 \setminus \{\neg A\}) = \emptyset = \square$ .

**Osservazione** Da un insieme di clausole  $\Gamma$  si può derivare soltanto un numero finito di clausole. Quindi per verificare se  $\Gamma \vdash_{\mathcal{R}} \square$  mi basta procedere finché si possono fare nuove risoluzioni. Se si trova la clausola vuota  $\Gamma \vdash_{\mathcal{R}} \square$ , se no  $\Gamma \not\vdash_{\mathcal{R}} \square$ .

### Dimostrazione parziale del teorema

- ( $\Leftarrow$ ) Se  $\Gamma$  è soddisfacibile, c'è un modello  $v$ . Vogliamo mostrare che  $\forall i, v$  è un modello per  $\Gamma_i$ .  
 È sicuramente vero per  $\Gamma_1 = \Gamma$ .  
 Se  $v$  è un modello per  $\Gamma_i$ , siano  $\mathcal{C}_{1,i}, \mathcal{C}_{2,i}, L_i$  e  $\mathcal{R}_i$  tali che  $\mathcal{C}_{1,i} \in \Gamma_i, \mathcal{C}_{2,i} \in \Gamma_i, \mathcal{R}_i = (\mathcal{C}_{1,i} \setminus \{L_i\}) \cup (\mathcal{C}_{2,i} \setminus \{\sim L_i\})$  e  $\Gamma_{i+1} = \Gamma_i \cup \{\mathcal{R}_i\}$ .  
 $v$  è un modello per  $\mathcal{C}_{1,i}$  e  $\mathcal{C}_{2,i}$ , quindi per il lemma è un modello per  $\mathcal{R}_i$ . Quindi  $v$  è un modello per  $\Gamma_{i+1}$ .  
 Quindi per il teorema dell'induzione “classico” tutti gli insiemi  $\Gamma_i$  hanno come modello  $v$ .  
 Quindi  $\perp \notin \Gamma_i$ , cioè  $\Gamma \not\vdash_{\mathcal{R}} \square$ .
- ( $\Rightarrow$ ) (completezza parziale) È più difficile.  
 Si deve usare un teorema che non abbiamo enunciato, per riportarsi al caso in cui  $\Gamma$  è finito.  
 Procedendo per induzione sul numero dei simboli atomici contenuti in  $\Gamma$  si riesce a fare la dimostrazione.

## 6. Logica dei predicati o del primo ordine

### 6.1. Il linguaggio

#### 6.1.1. Base

**Definizione** Un *alfabeto per un linguaggio della logica del primo ordine* è costituito da:

1. un insieme di simboli costante:  $a_1, a_2, \dots$ ;
2. un insieme infinito numerabile di simboli di variabile:  $x_1, x_2, \dots$ ;
3. un insieme al massimo numerabile di simboli di funzione:  $f_i^n, i \geq 1, n \geq 1$ ;
4. un insieme al massimo numerabile di simboli di predicato:  $A_i^n, i \geq 1, n \geq 0$ ;
5. un insieme di connettori:  $\perp, \neg, \wedge, \vee$  e  $\rightarrow$ ;
6. un insieme di quantificatori:  $\forall$  e  $\exists$ ;
7. un insieme di simboli ausiliari: “(” e “)”.

#### Definizione

- L'*insieme  $\mathcal{T}$  dei termini* di un linguaggio del primo ordine è il minimo insieme  $X$  che verifica:
  1. ogni simbolo di costante appartiene a  $X$ ;
  2. ogni simbolo di variabile appartiene a  $X$ ;
  3. se  $f_i^n$  è un simbolo di funzione e  $t_1, \dots, t_n \in X$  allora  $f_i^n(t_1, \dots, t_n) \in X$ .
- Per il simbolo di funzione  $f_i^n$  l'esponente  $n$  si chiama **arietà** del simbolo<sup>1</sup>.

**Osservazione** Una costante è una funzione di arietà 0, e quindi potrebbero essere rimosse dalla definizione ammettendo funzioni con arietà 0, ma per maggiore chiarezza si usa la definizione più “lunga”.

#### Definizione

- L'*insieme  $\mathcal{F}$  delle fbf* di un linguaggio del primo ordine è il minimo insieme  $X$  che verifica:
  1. se  $A_i^n$  è un simbolo di predicato e  $t_1, \dots, t_n \in \mathcal{T}$  allora  $A_i^n(t_1, \dots, t_n) \in X$ ;
  2.  $\perp \in X$ ;
  3. se  $\mathcal{P} \in X$  allora  $(\neg \mathcal{P}) \in X$ ;
  4. se  $\mathcal{P}_1 \in X$  e  $\mathcal{P}_2 \in X$  allora  $(\mathcal{P}_1 \vee \mathcal{P}_2) \in X$ ,  $(\mathcal{P}_1 \wedge \mathcal{P}_2) \in X$ ,  $(\mathcal{P}_1 \rightarrow \mathcal{P}_2) \in X$ ;
  5. se  $\mathcal{P} \in X$  e  $x_i$  è un simbolo di variabile  $((\exists x_i) \mathcal{P}) \in X$  e  $((\forall x_i) \mathcal{P}) \in X$ .
- Per un simbolo di predicato  $A_i^n$  l'esponente  $n$  si chiama **arietà** del simbolo.

---

<sup>1</sup>In pratica  $n$  indica il numero di variabili di  $f_i^n$ , mentre la  $i$  serve solo per distinguere due funzioni con stessa arietà, dato che nella teoria si usa  $f$  per tutte le funzioni.

### Osservazione

- Un predicato di arietà 0 è una semplice proporzione.
- Una fbf  $\mathcal{P}$  nella forma  $\mathcal{P} = A_i^n(t_1, \dots, t_n)$  è detta **fbf atomica**.

### Esempi

- I simboli di predicato sono delle relazioni sull'insieme. Esprimono il fatto che i termini  $t_1, \dots, t_n$  soddisfano una certa proprietà:
  - $A_1^2(x, y)$  può significare “ $x < y$ ”
  - $A_2^2(x, y)$  può significare “ $x$  è fratello di  $y$ ”
  - $A_1^1(x)$  può significare “ $x$  è un intero”
- I simboli di funzione sono le funzioni:
  - $f_1^2(x, y)$  può significare “ $x + y$ ”
  - $f_1^1(x)$  può significare “ $\ln(x)$ ”
- Esempi di cosa si può esprimere:
  - “ogni numero naturale è un numero razionale”:  
 $(\forall x_1) (A_1^1(x_1) \rightarrow A_2^1(x_1))$  dove:
    - \*  $A_1^1(x)$  è “ $x$  è un numero naturale”
    - \*  $A_2^1(x)$  è “ $x$  è un numero razionale”
  - “esiste un numero che non è un numero naturale”:  
 $(\exists x_1) (\neg A_1^1(x_1))$  dove:
    - \*  $A_1^1(x)$  è “ $x$  è un numero naturale”
  - “per ogni numero esiste un numero maggiore di lui”:  
 $(\forall x_1) ((\exists x_2) A_1^2(x_1, x_2))$  dove:
    - \*  $A_1^2(x, y)$  è “ $x < y$ ”

**Notazione** Omettiamo le parentesi rese inutili dalle seguenti regole di precedenza:

$$\forall = \exists = \neg > \wedge > \vee > \rightarrow.$$

Ricordiamo che  $\rightarrow$  è associativa a sinistra:  $\mathcal{P}_1 \rightarrow \mathcal{P}_2 \rightarrow \mathcal{P}_3$  é  $(\mathcal{P}_1 \rightarrow \mathcal{P}_2) \rightarrow \mathcal{P}_3$ .

#### 6.1.2. Sottoformule

**Definizione** L'insieme delle sottoformule  $S(\mathcal{P})$  di una fbf  $\mathcal{P}$  è definito per induzione da:

1. se  $\mathcal{P}$  è atomica,  $S(\mathcal{P}) = \{\mathcal{P}\}$ ;
2. se  $\mathcal{P} = \perp$ ,  $S(\mathcal{P}) = \{\perp\} = \{\mathcal{P}\}$ ;
3. se  $\mathcal{P} = (\neg \mathcal{P}_1)$ ,  $S(\mathcal{P}) = \{\mathcal{P}\} \cup S(\mathcal{P}_1)$ ;
4. se  $\mathcal{P} = \mathcal{P}_1 \vee \mathcal{P}_2$ ,  $\mathcal{P} = \mathcal{P}_1 \wedge \mathcal{P}_2$  o  $\mathcal{P} = \mathcal{P}_1 \rightarrow \mathcal{P}_2$ ,  $S(\mathcal{P}) = \{\mathcal{P}\} \cup S(\mathcal{P}_1) \cup S(\mathcal{P}_2)$ ;
5. se  $\mathcal{P} = ((\exists x_i) \mathcal{P}_1)$  o  $\mathcal{P} = ((\forall x_i) \mathcal{P}_1)$ ,  $S(\mathcal{P}) = \{\mathcal{P}\} \cup S(\mathcal{P}_1)$ .

### 6.1.3. Principi di induzione

Abbiamo due principi di induzione: uno per i termini e uno per le fbf.

**Teorema** Sia  $\mathcal{A}(t)$  una proprietà che può essere soddisfatta da un termine  $t$ . Allora  $\mathcal{A}(t)$  è vera per ogni termine se e solo se:

1. per ogni simbolo di costante  $a_i$ ,  $\mathcal{A}(a_i)$  è vera; passo base
2. per ogni simbolo di variabile  $x_i$ ,  $\mathcal{A}(x_i)$  è vera; passo base
3. se  $f_i^n$  è un simbolo di funzione,  $t_1, \dots, t_n \in \mathcal{T}$  e  $\mathcal{A}(t_1), \dots, \mathcal{A}(t_n)$  sono vere allora  $\mathcal{A}(f_i^n(t_1, \dots, t_n))$  è vera. passo induttivo

**Teorema** Sia  $\mathcal{A}(\mathcal{P})$  una proprietà che può essere soddisfatta da una fbf  $\mathcal{P}$ . Allora  $\mathcal{A}(\mathcal{P})$  è vera per ogni fbf se e solo se:

1. per ogni formula atomica  $\mathcal{P}$ ,  $\mathcal{A}(\mathcal{P})$  è vera; passo base
2.  $\mathcal{A}(\perp)$  è vera; passo base
3. se  $\mathcal{A}(\mathcal{P}_1)$  è vera allora  $\mathcal{A}(\neg \mathcal{P}_1)$  è vera; passo induttivo
4. se  $\mathcal{A}(\mathcal{P}_1)$  e  $\mathcal{A}(\mathcal{P}_2)$  sono vere allora sono vere  $\mathcal{A}(\mathcal{P}_1 \vee \mathcal{P}_2)$ ,  $\mathcal{A}(\mathcal{P}_1 \wedge \mathcal{P}_2)$  e  $\mathcal{A}(\mathcal{P}_1 \rightarrow \mathcal{P}_2)$ ; passo induttivo
5. se  $\mathcal{A}(\mathcal{P}_1)$  è vera e  $x_i$  è un simbolo di variabile,  $\mathcal{A}((\exists x_i) \mathcal{P}_1)$  e  $\mathcal{A}((\forall x_i) \mathcal{P}_1)$  sono vere. passo induttivo

### 6.1.4. Variabili libere e vincolate

La formula  $(\forall x) \mathcal{P}$  esprime il fatto che  $\mathcal{P}$  è vera per ogni valore di  $x$ .

Se scriviamo  $\mathcal{P}[y/x]$  intendendo “ $\mathcal{P}$  in cui ogni  $x$  è stato sostituito da  $y$ ” allora ci aspettiamo che  $(\forall x) \mathcal{P}$  e  $(\forall y) \mathcal{P}[y/x]$  abbiano lo stesso valore di verità.

Purtroppo non è (sempre) così.

Esempio:  $f(y) = \int_0^2 t \cdot y \, dt$ .

$$f(y) = \left[ \frac{t^2 \cdot y}{2} \right]_{t=0}^{t=2} = 2 \cdot y$$

Qualsiasi variabile io sostituisca a  $t$ :  $\int_0^2 \square \cdot y \, d\square = 2 \cdot y = f(y)$

ma  $\int_0^2 y \cdot y \, dy = \int_0^2 y^2 \, dy = \frac{8}{3} \neq f(y)$  (tranne che per  $y = \frac{4}{3}$ ).

Quindi al posto di  $t$  nell'integrale posso mettere qualsiasi simbolo tranne  $y$ , perché l' $y$  all'interno dell'integrale perde il valore dato all'esterno dell'integrale e prende il valore della variabile dell'integrale.

Altro esempio:

- $(\forall x) (\exists y) (x < y)$  è vera;
- $(\forall x) (\exists t) (x < t)$  è vera;
- $(\forall x) (\exists x) (x < x)$  è falsa.

Quindi bisogna stabilire quali sostituzioni sono possibili e quali no. Per farlo introduciamo i concetti di variabili libere e variabili vincolate.

**Definizione**

- Definiamo l'*insieme delle variabili libere*  $\mathcal{L}(t)$  di un termine  $t$  per induzione:
  - se  $t = a_i$ ,  $\mathcal{L}(t) = \emptyset$ ;
  - se  $t = x_i$ ,  $\mathcal{L}(t) = \{x_i\}$ ;
  - se  $t = f_i^n(t_1, \dots, t_n)$  con  $t_1, \dots, t_n$  termini allora  $\mathcal{L}(t) = \mathcal{L}(t_1) \cup \dots \cup \mathcal{L}(t_n)$ .
- Definiamo l'*insieme delle variabili libere*  $\mathcal{L}(\mathcal{P})$  e l'*insieme delle variabili vincolate*  $\mathcal{V}(\mathcal{P})$  di una fbf  $\mathcal{P}$ :
 

se $\mathcal{P} = A_i^n(t_1, \dots, t_n)$ ,	$\mathcal{L}(\mathcal{P}) = \mathcal{L}(t_1) \cup \dots \cup \mathcal{L}(t_n)$ ,	$\mathcal{V}(\mathcal{P}) = \emptyset$ ;
se $\mathcal{P} = \perp$ ,	$\mathcal{L}(\mathcal{P}) = \emptyset$ ,	$\mathcal{V}(\mathcal{P}) = \emptyset$ ;
se $\mathcal{P} = (\neg \mathcal{P}_1)$ ,	$\mathcal{L}(\mathcal{P}) = \mathcal{L}(\mathcal{P}_1)$ ,	$\mathcal{V}(\mathcal{P}) = \mathcal{V}(\mathcal{P}_1)$ ;
se $\mathcal{P} = (\mathcal{P}_1 \diamond \mathcal{P}_2)$ ,	$\mathcal{L}(\mathcal{P}) = \mathcal{L}(\mathcal{P}_1) \cup \mathcal{L}(\mathcal{P}_2)$ ,	$\mathcal{V}(\mathcal{P}) = \mathcal{V}(\mathcal{P}_1) \cup \mathcal{V}(\mathcal{P}_2)$ ;
se $\mathcal{P} = ((\mathcal{Q} x_i) \mathcal{P}_1)$ ,	$\mathcal{L}(\mathcal{P}) = \mathcal{L}(\mathcal{P}_1) \setminus \{x_i\}$ ,	$\mathcal{V}(\mathcal{P}) = \mathcal{V}(\mathcal{P}_1) \cup \{x_i\}$ ;

dove:

  - $\diamond$  è uno tra  $\vee, \wedge$  e  $\rightarrow$ ;
  - $\mathcal{Q}$  è uno tra  $\forall$  e  $\exists$ .

**Attenzione** Una variabile può essere sia libera che vincolata per una formula:

$$\begin{aligned} \mathcal{P} &= A(x) \rightarrow (\forall x) B(x) \\ \mathcal{L}(\mathcal{P}) &= \mathcal{L}(A(x)) \cup \mathcal{L}((\forall x) B(x)) = \mathcal{L}(x) \cup (\mathcal{L}(B(x)) \setminus \{x\}) = \{x\} \cup (\mathcal{L}(x) \setminus \{x\}) = \{x\} \cup (\{x\} \setminus \{x\}) = \{x\} \\ \mathcal{V}(\mathcal{P}) &= \mathcal{V}(A(x)) \cup \mathcal{V}((\forall x) B(x)) = \emptyset \cup (\mathcal{V}(B(x)) \cup \{x\}) = \emptyset \cup \{x\} = \{x\} \end{aligned}$$

**Definizione** Si dice *campo d'azione di un quantificatore* la sottoformula alla sua destra.

**Esempi**

- $(\forall x) \overbrace{A(x)}^{\text{campo d'azione}} \rightarrow B(x)$
- $(\forall x) \overbrace{(A(x) \rightarrow B(x))}^{\text{campo d'azione}}$

**Osservazione** In questa definizione si sono fatte 2 grosse semplificazioni:

- “alla sua destra” non vuol dire nulla dal punto di vista matematico, ma permette di afferrare il concetto;
- quando abbiamo definito il concetto di sottoformula lo abbiamo fatto tramite un insieme che essendo tale “elimina i duplicati”; per questo motivo la definizione di campo d'azione si riferisce alla singola istanza della sottoformula e non alla vera e propria sottoformula come sembra trapelare dalla definizione.

Per esempio se si prende

$$\mathcal{P} = (\forall x) A(x) \rightarrow A(x) \text{ abbiamo che } S(\mathcal{P}) = \{(\forall x) A(x) \rightarrow A(x), (\forall x) A(x), A(x)\}$$

quindi seguendo rigorosamente la definizione e notando che la sottoformula a destra di  $(\forall x)$  è  $A(x)$  il campo d'azione di  $(\forall x)$  è  $A(x)$  e indicandolo sulla fbf si ottiene:

$$(\forall x) \overbrace{A(x)}^{\text{campo d'azione}} \rightarrow \overbrace{A(x)}^{\text{campo d'azione}}$$

## 6. Logica dei predicati o del primo ordine

perchè ci sono 2 istanze di  $A(x)$ , ma in realtà il campo d'azione è solo la prima istanza:

$$(\forall x) \quad \overbrace{A(x)}^{\text{campo d'azione}} \rightarrow A(x).$$

**Definizione** Una *variabile*  $y$  è *libera per una variabile*  $x$  *in una fbf*  $\mathcal{P}$  se e solo se tutte le sottoformule di  $\mathcal{P}$  in cui compaiono  $x$  e  $y$  con  $x$  libera sono nel campo d'azione di un quantificatore di variabile  $x$ .

**Esempi** In tutti questi esempi si vuole capire se la variabile  $y$  è libera per la variabile  $x$ .

- $\mathcal{P}_1 = A^2(y, x)$ :  
Calcoliamo l'insieme delle sottoformule:  
 $S(\mathcal{P}_1) = \{A^2(y, x)\}$ 
  - In  $A^2(y, x)$  compaiono sia la  $x$  che la  $y$  e la  $x$  è una variabile libera, ma questa sottoformula non è in un campo d'azione di un quantificatore quindi  $y$  non è libera per  $x$ .
- $\mathcal{P}_2 = (\forall x) A^2(y, x)$ :  
Calcoliamo l'insieme delle sottoformule:  
 $S(\mathcal{P}_2) = \{A^2(y, x), (\forall x) A^2(y, x)\}$ 
  - In  $A^2(y, x)$  compaiono sia la  $x$  che la  $y$  e la  $x$  è una variabile libera, ma questa formula è nel campo d'azione di  $(\forall x)$  e quindi non contraddice la definizione.
  - In  $(\forall x) A^2(y, x)$  compaiono sia la  $x$  che la  $y$ , ma la  $x$  non è una variabile libera e quindi non contraddice la definizione.

Dato che nessuna sottoformula va contro la definizione allora  $y$  è libera per  $x$ .

- $\mathcal{P}_3 = A^1(x) \rightarrow (\forall x) A^2(y, x)$ :  $y$  non è libera per  $x$   
Calcoliamo l'insieme delle sottoformule:  
 $S(\mathcal{P}_3) = \{A(y, x), A^1(x), (\forall x) A^2(y, x), A^1(x) \rightarrow (\forall x) A^2(y, x)\}$ 
  - In  $A^2(y, x)$  compaiono sia la  $x$  che la  $y$  e la  $x$  è una variabile libera, ma questa formula è nel campo d'azione di  $(\forall x)$  e quindi non contraddice la definizione.
  - In  $A^1(x)$  non compare la  $y$  quindi non contraddice la definizione.
  - In  $(\forall x) A^2(y, x)$  compaiono sia la  $x$  che la  $y$ , ma la  $x$  non è una variabile libera e quindi non contraddice la definizione.
  - In  $A^1(x) \rightarrow (\forall x) A^2(y, x)$  compaiono sia la  $x$  che la  $y$ , e la  $x$  è sia libera che vincolata (e quindi compare libera), ma questa sottoformula non è in un campo d'azione di un quantificatore quindi  $y$  non è libera per  $x$ .
- $\mathcal{P}_4 = (\exists x) A^1(x) \rightarrow (\forall x) A^2(y, x)$ :  $y$  è libera per  $x$   
Calcoliamo l'insieme delle sottoformule:  
 $S(\mathcal{P}_4) = \{A(y, x), A^1(x), (\forall x) A^2(y, x), (\exists x) A^1(x), (\exists x) A^1(x) \rightarrow (\forall x) A^2(y, x)\}$ 
  - In  $A^2(y, x)$  compaiono sia la  $x$  che la  $y$  e la  $x$  è una variabile libera, ma questa formula è nel campo d'azione di  $(\forall x)$  e quindi non contraddice la definizione.
  - In  $A^1(x)$  non compare la  $y$  quindi non contraddice la definizione.
  - In  $(\forall x) A^2(y, x)$  compaiono sia la  $x$  che la  $y$ , ma la  $x$  non è una variabile libera e quindi non contraddice la definizione.
  - In  $(\exists x) A^1(x)$  non compare la  $y$  quindi non contraddice la definizione.

## 6. Logica dei predicati o del primo ordine

- In  $(\exists x) A^1(x) \rightarrow (\forall x) A^2(y, x)$  compaiono sia la  $x$  che la  $y$ , ma la  $x$  non è libera quindi non contraddice la definizione.

Dato che nessuna sottoformula va contro la definizione allora  $y$  è libera per  $x$ .

- $\mathcal{P}_5 = (\exists x) (A^1(x) \rightarrow (\forall x) A^2(y, x))$ :  $y$  è libera per  $x$

Calcoliamo l'insieme delle sottoformule:

$$S(\mathcal{P}_5) = \{A(y, x), A^1(x), (\forall x) A^2(y, x), A^1(x) \rightarrow (\forall x) A^2(y, x), (\exists x) (A^1(x) \rightarrow (\forall x) A^2(y, x))\}$$

- In  $A^2(y, x)$  compaiono sia la  $x$  che la  $y$  e la  $x$  è una variabile libera, ma questa formula è nel campo d'azione di  $(\forall x)$  e quindi non contraddice la definizione.
- In  $A^1(x)$  non compare la  $y$  quindi non contraddice la definizione.
- In  $(\forall x) A^2(y, x)$  compaiono sia la  $x$  che la  $y$ , ma la  $x$  non è una variabile libera e quindi non contraddice la definizione.
- In  $A^1(x) \rightarrow (\forall x) A^2(y, x)$  compaiono sia la  $x$  che la  $y$ , e la  $x$  è sia libera che vincolata (e quindi compare libera), ma questa formula è nel campo d'azione di  $(\exists x)$  e quindi non contraddice la definizione.
- In  $(\exists x) (A^1(x) \rightarrow (\forall x) A^2(y, x))$  compaiono sia la  $x$  che la  $y$ , ma la  $x$  non è libera quindi non contraddice la definizione.

Dato che nessuna sottoformula va contro la definizione allora  $y$  è libera per  $x$ .

### Osservazione

- Per poter capire se una variabile è libera per un'altra bisogna stare attenti al campo d'azione, infatti negli esempi  $\mathcal{P}_4$  e  $\mathcal{P}_5$  il motivo per cui la variabile è libera è diverso, nonostante le formule siano molto simili.
- Per poter capire se una variabile è libera per un'altra bisogna stare attenti a non confondere libera con il contrario di vincolata, dato che una variabile può essere sia libera che vincolata come negli esempi  $\mathcal{P}_3$ ,  $\mathcal{P}_4$  e  $\mathcal{P}_5$ .

**Definizione** Un *termine*  $t$  è *libero per una variabile*  $x$  se e solo se tutte le sue variabili libere sono libere per  $x$ .

### Definizione

- Siano  $s$  e  $t$  due termini e  $x$  un simbolo di variabile. Definiamo per induzione la sostituzione di  $t$  al posto di  $x$  in  $s$  scritto  $s[t/x]$ :
  1. se  $s = a_i$ ,  $s[t/x] = s = a_i$ ;
  2. se  $s$  è un simbolo di variabile:
    - se  $s \neq x$ ,  $s[t/x] = s$ ;
    - se  $s = x$ ,  $s[t/x] = t$ ;
  3. se  $s = f_i^n(t_1, \dots, t_n)$  allora  $s[t/x] = f_i^n(t_1[t/x], \dots, t_n[t/x])$ .
- Siano  $\mathcal{P}$  una fbf e  $x$  un simbolo di variabile. Se  $t$  è libero per  $x$  in  $\mathcal{P}$  definiamo per induzione la sostituzione di  $t$  al posto di  $x$  in  $\mathcal{P}$ :
  1. se  $\mathcal{P} = A_i^n(t_1, \dots, t_n)$ ,  $\mathcal{P}[t/x] = A_i^n(t_1[t/x], \dots, t_n[t/x])$ ;



## 6. Logica dei predicati o del primo ordine

2. se  $\mathcal{P} = \perp$ ,  $\mathcal{P} [t/x] = \perp$ ;
3. se  $\mathcal{P} = \neg \mathcal{P}_1$ ,  $\mathcal{P} [t/x] = \neg (\mathcal{P}_1 [t/x])$ ;
4. se  $\mathcal{P} = \mathcal{P}_1 \diamond \mathcal{P}_2$ , dove  $\diamond$  è uno tra  $\vee$ ,  $\wedge$  e  $\rightarrow$ ,  $\mathcal{P} [t/x] = (\mathcal{P}_1 [t/x]) \diamond (\mathcal{P}_2 [t/x])$ ;
5. se  $\mathcal{P} = (\mathcal{Q} x_i) \mathcal{P}_1$ , dove  $\mathcal{Q}$  è uno tra  $\forall$  e  $\exists$ :
  - se  $x_i \neq x$ ,  $\mathcal{P} [t/x] = (\mathcal{Q} x_i) (\mathcal{P}_1 [t/x])$ ;
  - se  $x_i = x$ ,  $\mathcal{P} [t/x] = \mathcal{P}$ .

### 6.1.5. Semantica

La semantica di un linguaggio della logica del primo ordine è molto più complessa di quella di un linguaggio della logica proposizionale.

**Definizione** Una *struttura per un linguaggio del primo ordine* è una coppia  $\mathcal{A} = (D_{\mathcal{A}}, I_{\mathcal{A}})$  dove  $D_{\mathcal{A}}$ , detto **dominio** di  $\mathcal{A}$ , è un insieme e  $I_{\mathcal{A}}$  è un'*applicazione* (o *funzione*) che associa:

- ad ogni simbolo di costante  $a_i$  un elemento  $I_{\mathcal{A}}(a_i) = a_i^{\mathcal{A}} \in D_{\mathcal{A}}$ ;
- ad ogni simbolo di funzione  $f_i^n$  una funzione  $I_{\mathcal{A}}(f_i^n) = f_i^{n,\mathcal{A}} : D_{\mathcal{A}}^n \rightarrow D_{\mathcal{A}}$ ;
- ad ogni simbolo di predicato  $A_i^n$  una funzione  $I_{\mathcal{A}}(A_i^n) = A_i^{n,\mathcal{A}} : D_{\mathcal{A}}^n \rightarrow \{0, 1\}$ .

**Osservazione** È consueto indicare con  $A_i^{n,\mathcal{A}}$  il sottoinsieme di  $D_{\mathcal{A}}^n$  in cui  $A_i^{n,\mathcal{A}}$  assume il valore 1. Per esempio:

- se il dominio  $D_{\mathcal{A}} = \{0, 1, 2, 3, 4, 5\}$  e  $A_1^{1,\mathcal{A}}(x)$  vale 1 se  $x$  è pari, si indica  $A_1^{1,\mathcal{A}} = \{0, 2, 4\}$ ;
- se il dominio  $D_{\mathcal{A}} = \mathbb{N}$  e  $A_1^{2,\mathcal{A}}(x, y)$  vale 1 se  $x \mid y$ , si indica  $A_1^{2,\mathcal{A}} = \{(x, y) \text{ tali che } x \mid y\}$ .

### Definizione

- Un *ambiente* (o *assegnamento*) *per un linguaggio del primo ordine in una struttura*  $\mathcal{A} = (D_{\mathcal{A}}, I_{\mathcal{A}})$  è una funzione  $\xi^{\mathcal{A}}$  che ad ogni simbolo di variabile  $x_i$  fa corrispondere un elemento di  $D_{\mathcal{A}}$ :  $\xi^{\mathcal{A}}(x_i) \in D_{\mathcal{A}}$ .
- Se  $\xi^{\mathcal{A}}$  è un ambiente nella struttura  $\mathcal{A}$  e  $a \in D_{\mathcal{A}}$ ,  $\xi^{\mathcal{A}}[a/x_i]$  è l'ambiente  $\Psi^{\mathcal{A}}$  tale che:
  - $\Psi^{\mathcal{A}}(x_i) = a$ ;
  - $\Psi^{\mathcal{A}}(x_j) = \xi^{\mathcal{A}}(x_j)$  per ogni  $x_j \neq x_i$ .

### Definizione

- Un'*interpretazione per un linguaggio del primo ordine* è una coppia  $\mathcal{I} = (\mathcal{A}, \xi^{\mathcal{A}})$  dove  $\mathcal{A}$  è una struttura e  $\xi^{\mathcal{A}}$  un assegnamento in  $\mathcal{A}$ .
- Ad ogni termine  $t$  si associa il suo valore in  $\mathcal{I}$  per induzione:
  1. se  $t = a_i$ ,  $\llbracket t \rrbracket_{\xi}^{\mathcal{A}} = a_i^{\mathcal{A}}$ ;
  2. se  $t = x_i$ ,  $\llbracket t \rrbracket_{\xi}^{\mathcal{A}} = \xi^{\mathcal{A}}(x_i)$ ;
  3. se  $t = f_i^n(t_1, \dots, t_n)$ ,  $\llbracket t \rrbracket_{\xi}^{\mathcal{A}} = f_i^{n,\mathcal{A}}(\llbracket t_1 \rrbracket_{\xi}^{\mathcal{A}}, \dots, \llbracket t_n \rrbracket_{\xi}^{\mathcal{A}})$ .

## 6. Logica dei predicati o del primo ordine

- Ad ogni fbf  $\mathcal{P}$  si associa il suo valore in  $\mathcal{I}$  per induzione:
  1. se  $\mathcal{P} = A_i^n(t_1, \dots, t_n)$ ,  $v_\xi^{\mathcal{A}}(\mathcal{P}) = A_i^{n,\mathcal{A}}(\llbracket t_1 \rrbracket_\xi^{\mathcal{A}}, \dots, \llbracket t_n \rrbracket_\xi^{\mathcal{A}})$ ;
  2. se  $\mathcal{P} = \perp$ ,  $v_\xi^{\mathcal{A}}(\mathcal{P}) = 0$ ;
  3. se  $\mathcal{P} = \neg \mathcal{P}_1$ ,  $v_\xi^{\mathcal{A}}(\mathcal{P}) = 1 - v_\xi^{\mathcal{A}}(\mathcal{P}_1)$ ;
  4. se  $\mathcal{P} = \mathcal{P}_1 \vee \mathcal{P}_2$ ,  $v_\xi^{\mathcal{A}}(\mathcal{P}) = \max(v_\xi^{\mathcal{A}}(\mathcal{P}_1), v_\xi^{\mathcal{A}}(\mathcal{P}_2))$ ;  
 se  $\mathcal{P} = \mathcal{P}_1 \wedge \mathcal{P}_2$ ,  $v_\xi^{\mathcal{A}}(\mathcal{P}) = \min(v_\xi^{\mathcal{A}}(\mathcal{P}_1), v_\xi^{\mathcal{A}}(\mathcal{P}_2))$ ;  
 se  $\mathcal{P} = \mathcal{P}_1 \rightarrow \mathcal{P}_2$ ,  $v_\xi^{\mathcal{A}}(\mathcal{P}) = v_\xi^{\mathcal{A}}(\neg \mathcal{P}_1 \vee \mathcal{P}_2)$ ;
  5. se  $\mathcal{P} = ((\forall x_i) \mathcal{P}_1)$ ,  $v_\xi^{\mathcal{A}}(\mathcal{P}) = \min \{v_{\xi[a/x_i]}^{\mathcal{A}}(\mathcal{P}_1) \mid a \in D_{\mathcal{A}}\}$ ;  
 se  $\mathcal{P} = ((\exists x_i) \mathcal{P}_1)$ ,  $v_\xi^{\mathcal{A}}(\mathcal{P}) = \max \{v_{\xi[a/x_i]}^{\mathcal{A}}(\mathcal{P}_1) \mid a \in D_{\mathcal{A}}\}$ .

### Osservazione

- $\forall$  è una congiunzione iterata mentre  $\exists$  è una disgiunzione iterata.
- Se  $D_{\mathcal{A}}$  è infinito, non si possono calcolare min e max calcolando tutti gli elementi dell'insieme.
- Il valore di un termine  $t$  o di una fbf  $\mathcal{P}$  dipende soltanto dalla parte di  $\xi^{\mathcal{A}}$  che riguarda  $\mathcal{L}(t)$  o  $\mathcal{L}(\mathcal{P})$ .

**Proposizione** Se  $\mathcal{I} = (\mathcal{A}, \xi)$  è un'interpretazione,  $t$  un termine (rispettivamente  $\mathcal{P}$  una fbf) e  $y$  è libera per  $x$  in  $t$  (rispettivamente  $\mathcal{P}$ ),

$$\llbracket t \rrbracket_\xi^{\mathcal{A}} = \llbracket t[y/x] \rrbracket_{\xi[y/x]}^{\mathcal{A}}$$

$$v_\xi^{\mathcal{A}}(\mathcal{P}) = v_{\xi[\xi(x)/y]}^{\mathcal{A}}(\mathcal{P}[y/x])$$

**Osservazione** Questa proposizione conferma che la sostituzione come è stata definita non varia il valore di verità della fbf.

### 6.1.6. Soddisfacibilità, validità e modelli

#### 6.1.6.1. Definizione

**Definizione** Sia  $\mathcal{P}$  una fbf.

- Si dice che  $\mathcal{P}$  è **soddisfatta nell'interpretazione**  $\mathcal{I} = (\mathcal{A}, \xi)$  o che  $\mathcal{I}$  è un **modello** per  $\mathcal{P}$  se e solo se  $v_\xi^{\mathcal{A}}(\mathcal{P}) = 1$  e si scrive  $\mathcal{I} \models \mathcal{P}$ .
- Si dice che  $\mathcal{P}$  è **soddisfacibile nella struttura**  $\mathcal{A}$  se e solo se esiste un assegnamento  $\xi$  in  $\mathcal{A}$  tale che  $(\mathcal{A}, \xi)$  sia un modello per  $\mathcal{P}$ .
- si dice che  $\mathcal{P}$  è **vera nella struttura**  $\mathcal{A}$  se e solo se per ogni assegnamento  $\xi$  in  $\mathcal{A}$ ,  $(\mathcal{A}, \xi)$  è un modello per  $\mathcal{P}$  e si scrive  $\mathcal{A} \models \mathcal{P}$ . In tal caso si dice anche che  $\mathcal{A}$  è un modello per  $\mathcal{P}$ .
- Si dice che  $\mathcal{P}$  è **soddisfacibile** se e solo se esiste un modello per  $\mathcal{P}$ .
- Si dice che  $\mathcal{P}$  è **valida** se e solo se è vera in ogni struttura  $\mathcal{A}$ , cioè se e solo se ogni interpretazione è un modello per  $\mathcal{P}$ .

## 6. Logica dei predicati o del primo ordine

**Osservazione** È impossibile verificare la validità di una fbf  $\mathcal{P}$  per elenco esplicito delle possibilità (perché ci sono infiniti insiemi possibili) (tranne se  $\mathcal{P}$  è della logica proposizionale).

**Definizione** Sia  $\Gamma$  un insieme di fbf.

- $\Gamma$  è **soddisfacibile** se e solo se esiste un'interpretazione  $\mathcal{I}$  che sia un modello per tutte le fbf  $\mathcal{P} \in \Gamma$ .
- Una struttura  $\mathcal{A}$  è un **modello** per  $\Gamma$  se e solo se è un modello per ogni  $\mathcal{P} \in \Gamma$ .
- $\Gamma$  è **valido** se e solo se tutte le  $\mathcal{P} \in \Gamma$  sono valide.

**Definizione** Siano  $\Gamma$  un insieme di fbf e  $\mathcal{P}$  una fbf, si dice che  $\mathcal{P}$  è **conseguenza semantica** di  $\Gamma$  se e solo se ogni interpretazione  $\mathcal{I}$  che sia un modello per tutte le  $\mathcal{Q} \in \Gamma$  è un modello per  $\mathcal{P}$ . Si scrive allora  $\Gamma \models \mathcal{P}$  o  $\mathcal{Q}_1, \dots, \mathcal{Q}_n \models \mathcal{P}$  dove  $\Gamma = \{\mathcal{Q}_1, \dots, \mathcal{Q}_n\}$ .

**Definizione**

- Una fbf  $\mathcal{P}$  è **falsa in una struttura**  $\mathcal{A}$  se e solo se non è soddisfacibile in  $\mathcal{A}$ , ovvero se e solo se per qualsiasi ambiente  $\xi$  in  $\mathcal{A}$ ,  $v_{\xi}^{\mathcal{A}}(\mathcal{P}) = 0$ .
- Una fbf  $\mathcal{P}$  è **insoddisfacibile** o (**contraddittoria**) se e solo se non è soddisfacibile (cioè se è falsa in ogni struttura, cioè se è insoddisfatta in tutte le interpretazioni).
- Un insieme  $\Gamma$  di fbf è **falso in una struttura** se e solo se per ogni ambiente  $\xi$  in  $\mathcal{A}$  esiste (almeno) una  $\mathcal{P} \in \Gamma$  tale che  $v_{\xi}^{\mathcal{A}}(\mathcal{P}) = 0$ .
- Un insieme  $\Gamma$  di formule è **insoddisfacibile** se e solo se è falso in ogni struttura.

**Esempi**

- $(\forall x)(\forall y)(\exists z)C(f(x, y), z)$  è soddisfatta in  $(\mathcal{A}, \xi)$  con:
  - $D_{\mathcal{A}} = \mathbb{N}$
  - $f_{\mathcal{A}}(x, y) = x + y$
  - $C^{\mathcal{A}} = \{(n, n) \mid n \in \mathbb{N}\}$  (è l'uguaglianza)
  - $\xi$  ambiente qualsiasi

Non è però valida perché in una struttura in cui  $C$  è sempre falsa, la fbf non risulta soddisfatta.

- $(\exists x)(A(x) \rightarrow B(x)) \rightarrow ((\exists x)A(x) \rightarrow (\exists x)B(x))$  non è soddisfatta nell'interpretazione:
  - $D_{\mathcal{A}} = \mathbb{N}$
  - $A^{\mathcal{A}} = \{0\}$
  - $B^{\mathcal{A}} = \emptyset$
  - $\xi$  ambiente qualsiasi

Non è però insoddisfacibile perché in una struttura in cui  $A$  e  $B$  sono sempre vere (o sempre false) la fbf è soddisfatta.

- $(\exists x)(\forall y)A(x, y) \rightarrow (\forall y)(\exists x)A(x, y)$  è valida:
  - se  $D_{\mathcal{A}} = \emptyset$  l'ipotesi non è soddisfatta (non esiste  $x$ ). Quindi la formula è soddisfatta;

## 6. Logica dei predicati o del primo ordine

– se  $D_{\mathcal{A}} \neq \emptyset$ :

- \* se l'ipotesi non è soddisfatta, la fbf è soddisfatta;
- \* se l'ipotesi è soddisfatta, esiste  $a \in D_{\mathcal{A}}$  tale che, per qualsiasi  $b \in D_{\mathcal{A}}$ ,  $A^{\mathcal{A}}(a, b) = 1$ .  
Ora dato  $b \in D_{\mathcal{A}}$ , se scelgo  $x = a$ , risulta  $A^{\mathcal{A}}(a, b) = 1$ , quindi  $(\exists x) A^{\mathcal{A}}(x, b)$  è soddisfatta.

- **Paradosso del barbiere:**

In un paese c'è un barbiere che rade tutti e solo coloro che non si radono da soli. Un giorno un forestiero gli chiede chi lo rade.

Ha deciso di lasciarlo crescere la barba.

Per codificare in un linguaggio del primo ordine ci serve un predicato  $R$ ,  $R(x, y)$  significa “ $x$  rade  $y$ ” e un simbolo di costante  $b$ , il barbiere.

“tutti”:  $(\forall x) (\neg R(x, x) \rightarrow R(b, x)) = \mathcal{P}_t$

“solo”:  $(\forall x) (R(b, x) \rightarrow \neg R(x, x)) = \mathcal{P}_s$

Non c'è un modello di  $\Gamma = \{\mathcal{P}_t, \mathcal{P}_s\}$ . Se ci fosse,  $D_{\mathcal{A}}$  avrebbe almeno un elemento  $\mathcal{G}$ ; scegliamo  $b^{\mathcal{A}} = \mathcal{G}$ .

Se  $R^{\mathcal{A}}(\mathcal{G}, \mathcal{G}) = 1$ ,  $\mathcal{P}_s$  non è soddisfatta (perché l'implicazione non è soddisfatta per  $x = \mathcal{G}$ ).

Se  $R^{\mathcal{A}}(\mathcal{G}, \mathcal{G}) = 0$ ,  $\mathcal{P}_t$  non è soddisfatta (perché l'implicazione non è soddisfatta per  $x = \mathcal{G}$ ).

**Attenzione** “ $\mathcal{P}$  non è valida” non significa “ $\mathcal{P}$  è insoddisfacibile”.

- “ $\mathcal{P}$  non è valida”: non  $(\forall \mathcal{I}, v^{\mathcal{I}}(\mathcal{P}) = 1)$ , cioè  $\exists \mathcal{I}, v^{\mathcal{I}}(\mathcal{P}) = 0$ .
- “ $\mathcal{P}$  è insoddisfacibile”:  $\forall \mathcal{I}, v^{\mathcal{I}}(\mathcal{P}) = 0$ .

“ $\mathcal{P}$  non è valida” è equivalente a “ $\neg \mathcal{P}$  è soddisfacibile”.

**Osservazione** La differenza tra vera in una struttura  $\mathcal{A}$  e soddisfacibile in una struttura  $\mathcal{A}$  sta nell'assegnamento: per “vera” dev'essere soddisfatta per qualsiasi assegnamento, per “soddisfacibile” dev'essere soddisfatta per almeno un assegnamento.

Siccome l'assegnamento serve solo per le variabili libere, se una fbf non ha variabili libere è soddisfacibile in  $\mathcal{A}$  se e solo se è vera in  $\mathcal{A}$ .

**Teorema** Siano  $\Gamma$  un insieme di fbf e  $\mathcal{P}$  una fbf. Allora:

1.  $\mathcal{P}$  è valida se e solo se  $\neg \mathcal{P}$  è insoddisfacibile;
2.  $\mathcal{P}$  è soddisfacibile se e solo se  $\neg \mathcal{P}$  non è valida;
3.  $\Gamma \models \mathcal{P}$  se e solo se  $\Gamma \cup \{\neg \mathcal{P}\}$  è insoddisfacibile.

**Osservazione**

- I primi 2 punti sono la formalizzazione dei concetti spiegati sopra.
- Il terzo punto si dimostra in modo analogo a quanto fatto per lo stesso teorema nella logica proposizionale.

### 6.1.6.2. Chiusure

#### Definizione

- Una fbf  $\mathcal{P}$  è detta chiusa se e solo se  $\mathcal{L}(\mathcal{P}) = \emptyset$ .
- Sia  $\mathcal{P}$  una fbf tale che  $\mathcal{L}(\mathcal{P}) = \{x_1, \dots, x_k\}$ . Allora:
  - la **chiusura esistenziale** di  $\mathcal{P}$  è la fbf  $\mathcal{E}x(\mathcal{P}) = \mathcal{E}s(\mathcal{P}) = (\exists x_1) \dots (\exists x_k) \mathcal{P}$ ;
  - la **chiusura universale** di  $\mathcal{P}$  è la fbf  $\mathcal{C}l(\mathcal{P}) = \mathcal{C}h(\mathcal{P}) = (\forall x_1) \dots (\forall x_k) \mathcal{P}$ .

### 6.1.6.3. Proprietà delle chiusure

**Lemma** Siano  $\mathcal{P}$  una fbf e  $\mathcal{A}$  una struttura, allora  $\mathcal{A} \models \mathcal{P}$  se e solo se  $\mathcal{A} \models \mathcal{C}l(\mathcal{P})$ .

**Teorema** Sia  $\mathcal{P}$  una fbf, allora:

- $\mathcal{P}$  è valida se e solo se  $\mathcal{C}l(\mathcal{P})$  è valida;
- $\mathcal{P}$  è soddisfacibile se e solo se  $\mathcal{E}x(\mathcal{P})$  è soddisfacibile.

### 6.1.7. Equivalenza semantica

**Definizione** Siano  $\mathcal{P}_1$  e  $\mathcal{P}_2$  due fbf. Si dice che  $\mathcal{P}_1$  e  $\mathcal{P}_2$  sono semanticamente equivalenti se e solo se per qualsiasi interpretazione  $(\mathcal{A}, \xi)$  vale  $v_\xi^{\mathcal{A}}(\mathcal{P}_1) = v_\xi^{\mathcal{A}}(\mathcal{P}_2)$ . Si scrive  $\mathcal{P}_1 \equiv \mathcal{P}_2$ .

**Osservazione**  $\mathcal{P}_1 \equiv \mathcal{P}_2$  se e solo se:

- $\mathcal{P}_1 \models \mathcal{P}_2$  e  $\mathcal{P}_2 \models \mathcal{P}_1$ ;
- $\models (\mathcal{P}_1 \rightarrow \mathcal{P}_2) \wedge (\mathcal{P}_2 \rightarrow \mathcal{P}_1)$ ;
- $\models (\mathcal{P}_1 \wedge \mathcal{P}_2) \vee (\neg \mathcal{P}_1 \wedge \neg \mathcal{P}_2)$ .

**Teorema** Oltre alla lista di equivalenze semantiche della logica proposizionale, valgono anche le seguenti, dove  $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$  sono fbf e  $x_1, x_2, x_3, x_4$  sono simboli di variabile:

1.  $(\exists x_1) \mathcal{P}_1 \equiv (\exists x_2) \mathcal{P}_1 [x_2/x_1]$  (se  $x_2 \in \mathcal{L}(\mathcal{P}_1)$ )
2.  $(\forall x_1) \mathcal{P}_1 \equiv (\forall x_2) \mathcal{P}_1 [x_2/x_1]$  (se  $x_2 \in \mathcal{L}(\mathcal{P}_1)$ )
3.  $\neg(\exists x_1) \mathcal{P}_1 \equiv (\forall x_1) \neg \mathcal{P}_1$  (legge di De Morgan generalizzata)
4.  $\neg(\forall x_1) \mathcal{P}_1 \equiv (\exists x_1) \neg \mathcal{P}_1$  (legge di De Morgan generalizzata)
5.  $(\forall x_1)(\forall x_2) \mathcal{P}_1 \equiv (\forall x_2)(\forall x_1) \mathcal{P}_1$
6.  $(\exists x_1)(\exists x_2) \mathcal{P}_1 \equiv (\exists x_2)(\exists x_1) \mathcal{P}_1$
7.  $(\exists x_1) \mathcal{P}_1 \equiv \mathcal{P}_1$  (se  $x_1 \notin \mathcal{L}(\mathcal{P}_1)$ )
8.  $(\forall x_1) \mathcal{P}_1 \equiv \mathcal{P}_1$  (se  $x_1 \notin \mathcal{L}(\mathcal{P}_1)$ )
9.  $(\exists x_1)(\mathcal{P}_1 \vee \mathcal{P}_2) \equiv ((\exists x_1) \mathcal{P}_1) \vee ((\exists x_1) \mathcal{P}_2)$
10.  $(\forall x_1)(\mathcal{P}_1 \wedge \mathcal{P}_2) \equiv ((\forall x_1) \mathcal{P}_1) \wedge ((\forall x_1) \mathcal{P}_2)$

## 6. Logica dei predicati o del primo ordine

11.  $((Q x_1) \mathcal{P}_1) \vee \mathcal{P}_2 \equiv (Q x_1) (\mathcal{P}_1 \vee \mathcal{P}_2)$  (se  $x_1 \notin \mathcal{L}(\mathcal{P}_2)$ ) dove  $Q$  è uno tra  $\exists$  e  $\forall$
12.  $((Q x_1) \mathcal{P}_1) \wedge \mathcal{P}_2 \equiv (Q x_1) (\mathcal{P}_1 \wedge \mathcal{P}_2)$  (se  $x_1 \notin \mathcal{L}(\mathcal{P}_2)$ ) dove  $Q$  è uno tra  $\exists$  e  $\forall$
13.  $((\exists x_1) \mathcal{P}_1) \rightarrow \mathcal{P}_2 \equiv (\forall x_1) (\mathcal{P}_1 \rightarrow \mathcal{P}_2)$  (se  $x_1 \notin \mathcal{L}(\mathcal{P}_2)$ )
14.  $((\forall x_1) \mathcal{P}_1) \rightarrow \mathcal{P}_2 \equiv (\exists x_1) (\mathcal{P}_1 \rightarrow \mathcal{P}_2)$  (se  $x_1 \notin \mathcal{L}(\mathcal{P}_2)$ )
15.  $\mathcal{P}_2 \rightarrow ((\exists x_1) \mathcal{P}_1) \equiv (\exists x_1) (\mathcal{P}_2 \rightarrow \mathcal{P}_1)$  (se  $x_1 \notin \mathcal{L}(\mathcal{P}_2)$ )
16.  $\mathcal{P}_2 \rightarrow ((\forall x_1) \mathcal{P}_1) \equiv (\forall x_1) (\mathcal{P}_2 \rightarrow \mathcal{P}_1)$  (se  $x_1 \notin \mathcal{L}(\mathcal{P}_2)$ )

**Osservazione** Riguardo ai punti (9), (10), (11), (12):

$$(\forall n) (\text{Pari}(n) \vee \text{Dispari}(n)) \not\equiv ((\forall n) \text{Pari}(n)) \vee ((\forall n) \text{Dispari}(n))$$

### 6.1.8. Forma normale prenessa

**Definizione** Una fbf è detta in **forma normale prenessa** (anche abbreviato in “fnp”) se e solo se  $\mathcal{P} = (Q_1 x_1) \dots (Q_k x_k) \mathcal{P}_1$  con  $Q_i \in \{\exists, \forall\}$  e in  $\mathcal{P}_1$  non ci sono quantificatori.

La parte  $(Q_1 x_1) \dots (Q_k x_k)$  si chiama **prefisso** di  $\mathcal{P}$  e  $\mathcal{P}_1$  si chiama **matrice** di  $\mathcal{P}_1$ .

**Teorema** Per qualsiasi fbf  $\mathcal{P}$  esiste una fbf  $\mathcal{P}^P$  in fnp tale che  $\mathcal{P} \equiv \mathcal{P}^P$ .

**Dimostrazione** Usare i punti (3), (4) e dall’(11) al (16) del precedente teorema.

### 6.1.9. Forma di Skolem

**Definizione** Una fbf  $\mathcal{P}$  è detta in **forma di Skolem** se e solo se  $\mathcal{P}$  è in fnp e gli unici quantificatori nel prefisso sono quantificatori universali, cioè il prefisso di  $\mathcal{P}$  è  $(\forall x_1) \dots (\forall x_k)$ .

**Proposizione** Sia  $\mathcal{P}$  una fbf con  $\mathcal{L}(\mathcal{P}) = \{y_1, \dots, y_r\}$ . Il seguente procedimento produce una fbf  $\mathcal{P}^S$  in forma di Skolem:

- sia  $\mathcal{P}_1$  la formula in fnp prodotta dal teorema della sezione precedente;
- finché il quantificatore iniziale di  $\mathcal{P}_i$  è  $(\exists x_i)$ , si sostituisce in  $\mathcal{P}_i$  la variabile  $x_i$  con un nuovo simbolo di funzione  $f_i^r(y_1, \dots, y_r)$  e si toglie l’ $(\exists x_i)$ . Il risultato sarà  $\mathcal{P}_{i+1}$ .  
Se  $\mathcal{L}(\mathcal{P}) = \emptyset$  il nuovo simbolo di funzione ha arità 0 e quindi è un simbolo di costante;
- ogni volta che  $\mathcal{P}_i$  è della forma  $(\forall x_1) \dots (\forall x_k) (\exists x_{k+1}) (Q_{k+2} x_{k+2}) \dots (Q_n x_n) \mathcal{R}_i$  togliamo  $(\exists x_{k+1})$  dal prefisso e in  $\mathcal{R}_i$  sostituiamo  $x_{k+1}$  con un nuovo simbolo di funzione  $f_i^{k+r}(x_1, \dots, x_k, y_1, \dots, y_r)$ . Il risultato si denota  $\mathcal{P}_{i+1}$ .

**Osservazione** Il risultato  $\mathcal{P}^S$  non è semanticamente equivalente alla  $\mathcal{P}$  (perché nella semantica i valori scelti per le costanti e/o le funzioni che sostituiscono i quantificatori esistenziali possono essere sbagliati).

Ma  $\mathcal{P}$  è soddisfacibile se e solo se  $\mathcal{P}^S$  lo è.

**Esempio**  $\mathcal{P} = A(x) \vee (\exists x) (\forall y) (\exists z) B(x, y, z)$ .

$$\begin{aligned} \mathcal{P} &\equiv A(x) \vee (\exists t) (\forall y) (\exists z) B(t, y, z) \equiv \\ &\equiv (\exists t) (A(x) \vee (\forall y) (\exists z) B(t, y, z)) \equiv \\ &\equiv (\exists t) (\forall y) (A(x) \vee (\exists z) B(t, y, z)) \equiv \\ &\equiv (\exists t) (\forall y) (\exists z) (A(x) \vee B(t, y, z)) \text{ fnp.} \\ \mathcal{P}^S &\equiv (\forall y) (A(x) \vee B(f(x), y, g(x, y))) \text{ forma di Skolem.} \end{aligned}$$

## 6.2. Sistemi deduttivi

### 6.2.1. Deduzione naturale

Agli assiomi della deduzione naturale si aggiungono i quattro seguenti (meta)assiomi:

$$(\forall i) \quad \frac{\mathcal{A}[x_j/x_i]}{(\forall x_i) \mathcal{A}}$$

con  $x_i$  e  $x_j$  simboli di variabile; inoltre  $x_j$  non può comparire libera nelle foglie non cancellate di  $\mathcal{A}[x_j/x_i]$ .

$$(\forall e) \quad \frac{(\forall x_i) \mathcal{A}}{\mathcal{A}[t/x_i]}$$

con  $x_i$  simbolo di variabile e  $t$  termine.

$$(\exists i) \quad \frac{\mathcal{A}[t/x_i]}{(\exists x_i) \mathcal{A}}$$

con  $x_i$  simbolo di variabile e  $t$  termine.

$$(\exists e) \quad \frac{(\exists x_i) \mathcal{A} \quad \frac{\mathcal{A}[x_j/x_i]}{\mathcal{B}}}{\mathcal{B}}$$

con  $x_i$  e  $x_j$  simboli di variabile; inoltre  $x_j$  non può comparire libera né in  $\mathcal{B}$  né in nessuna delle foglie non cancellate nel sottoalbero di radice  $\mathcal{B}$ .

**Esempio** L'albero seguente rappresenta la deduzione  $(\forall x) (A \rightarrow B(x)) \vdash A \rightarrow (\forall x) B(x)$ :

$$\frac{\frac{[A] \quad \frac{(\forall x) (A \rightarrow B(x))}{A \rightarrow B(x)} (\forall e)}{B(x)} (\rightarrow e)}{\frac{(\forall x) B(x)}{A \rightarrow (\forall x) B(x)} (\forall i)} (\rightarrow i)$$

**Teorema (correttezza)** Siano  $\Gamma$  un insieme di fbf e  $\mathcal{P}$  una fbf.

$\Gamma \models \mathcal{P}$  se e solo se  $\Gamma \vdash \mathcal{P}$ .

### 6.2.2. Risoluzione

#### Definizione

- Un **letterale** è una formula atomica o la sua negazione.
- Una **clausola** è una disgiunzione di letterali.
- La **clausola vuota** si scrive  $\square$  e corrisponde a  $\perp$ .
- Una fbf in forma di Skolem si dice in **forma a clausole** se la sua matrice è una congiunzione di clausole (cioè è in fnc).

### Notazione

- Se  $\mathcal{R}$  è un letterale denotiamo  $\sim \mathcal{R}$  il letterale “opposto”, cioè:
  - se  $\mathcal{R} = A_i^n(t_1, \dots, t_n)$ ,  $\sim \mathcal{R} = \neg A_i^n(t_1, \dots, t_n)$ ;
  - se  $\mathcal{R} = \neg A_i^n(t_1, \dots, t_n)$ ,  $\sim \mathcal{R} = A_i^n(t_1, \dots, t_n)$ .
- Una clausola si rappresenta come l’unione dei suoi letterali.
- Una fbf in forma a clausole si rappresenta come l’insieme delle clausole della sua matrice.

**Definizione** Una **sostituzione** è un insieme  $\sigma = \{t_1/x_1, \dots, t_n/x_n\}$  dove gli  $x_i$  sono simboli di variabile e i  $t_i$  termini. Se  $t$  è un termine e  $\mathcal{P}$  una fbf si denota  $t.\sigma$  o  $\mathcal{P}.\sigma$  rispettivamente  $t[t_1/x_1][t_2/x_2] \dots [t_n/x_n]$  o  $\mathcal{P}[t_1/x_1][t_2/x_2] \dots [t_n/x_n]$ .

### Osservazione

- Con  $\mathcal{P}[t_1/x_1][t_2/x_2] \dots [t_n/x_n]$  si intende  $((\mathcal{P}[t_1/x_1])[t_2/x_2]) \dots [t_n/x_n]$  ossia le sostituzioni sono in fila, se si cambia l’ordine il risultato cambia. Lo stesso vale per  $t[t_1/x_1][t_2/x_2] \dots [t_n/x_n]$ .
- Data l’osservazione di prima, ad essere fiscali,  $\sigma$  non è un insieme dato che l’ordine conta.

**Definizione** Sia dato  $\Gamma = \{\mathcal{P}_1, \dots, \mathcal{P}_n\}$  insieme di fbf.

- Si dice che  $\Gamma$  è **unificabile** se e solo se esiste una sostituzione  $\sigma$ , detta **unificatore** di  $\Gamma$ , tale che  $\mathcal{P}_1.\sigma = \mathcal{P}_2.\sigma = \dots = \mathcal{P}_n.\sigma$ .
- Nel caso contrario  $\Gamma$  si dice **non unificabile**.

**Esempio**  $\Gamma = \{A(x, a), A(y, z)\}$ .

- $\sigma_1 = \{x/y, a/z\}$  unifica con risultato  $A(x, a)$
- $\sigma_2 = \{y/x, a/z\}$  unifica con risultato  $A(y, a)$
- $\sigma_3 = \{t/x, t/y, a/z\}$  unifica con risultato  $A(t, a)$
- $\sigma_4 = \{f(a, a)/x, f(a, a)/y, a/z\}$  unifica con risultato  $A(f(a, a), a)$
- $\sigma_5 = \{f(g(u), a)/x, f(g(u), a)/y, a/z\}$  unifica con risultato  $A(f(g(u), a), a)$

Un unificatore, se esiste, non è praticamente mai unico.

Nell’esempio le tre prime sostituzioni sono sostanzialmente identiche e sono migliori delle altre perché da ciascuna di esse si possono ottenere tutte le altre mediante un’ulteriore sostituzione.

### Definizione

- Siano  $\sigma = \{t_1/x_1, \dots, t_m/x_m\}$  e  $\tau = \{u_1/y_1, \dots, u_n/y_n\}$  due sostituzioni. Si denota  $\sigma.\tau$ , **composizione di sostituzioni**, la sostituzione  $\{t_1.\tau/x_1, \dots, t_m.\tau/x_m, u_1/y_1, \dots, u_n/y_n\}$  da cui si tolgono gli  $u_i/y_j$  se esiste un  $i$  tale che  $x_i = y_j$  e i  $t_i.\tau/x_i$  se  $t_i.\tau = x_i$ .
- Dato  $\Gamma$  un insieme di fbf unificabile, se  $\sigma$  è un unificatore di  $\Gamma$  tale che per ogni altro unificatore  $\tau$  esista un’ulteriore sostituzione  $\vartheta$  tale che  $\tau = \sigma.\vartheta$ ,  $\sigma$  si dice **unificatore più generale** di  $\Gamma$ .



**Proposizione** Se  $\Gamma$  è un insieme di fbf unificabile allora esiste un unificatore più generale di  $\Gamma$ .

**Dimostrazione** L'algoritmo seguente costruisce l'unificatore più generale di  $\Gamma$  o dimostra che non esiste. Supponiamo, per semplificare, che  $\Gamma = \{\mathcal{P}_1, \mathcal{P}_2\}$ .

- Si leggono  $\mathcal{P}_1$  e  $\mathcal{P}_2$  simbolo per simbolo;
- se il primo simbolo che differisce tra  $\mathcal{P}_1$  e  $\mathcal{P}_2$  è un simbolo di variabile in una delle due (diciamo  $x_i$  in  $\mathcal{P}_1$ ) allora in  $\mathcal{P}_2$  il simbolo è il primo simbolo di un termine  $t_i$  e sostituiamo allora  $\mathcal{P}_1$  e  $\mathcal{P}_2$  con  $\mathcal{P}_1[t_i/x_i]$  e  $\mathcal{P}_2[t_i/x_i]$ , e ricominciamo da capo;
- se il primo simbolo che differisce tra  $\mathcal{P}_1$  e  $\mathcal{P}_2$  non è un simbolo di variabile in una delle due allora  $\Gamma$  non è unificabile;
- se tra  $\mathcal{P}_1$  e  $\mathcal{P}_2$  non c'è differenza allora  $\Gamma$  è stato unificato.

Questo algoritmo può essere semplicemente generalizzato per qualsiasi insieme  $\Gamma$ , ma nella maggior parte delle situazioni basta unificare 2 formule.

Per completare la dimostrazione per un insieme  $\Gamma = \{\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_n\}$  si procede così:

- si unificano  $\mathcal{P}_1$  e  $\mathcal{P}_2$  con la sostituzione  $\sigma_2$  ottenendo  $\mathcal{P}_{12} = \mathcal{P}_1.\sigma_2 = \mathcal{P}_2.\sigma_2$ , se non si può l'insieme non è unificabile;
- si unificano  $\mathcal{P}_{12}$  e  $\mathcal{P}_3$  con la sostituzione  $\sigma_3$  ottenendo  $\mathcal{P}_{123} = \mathcal{P}_{12}.\sigma_3 = \mathcal{P}_1.\sigma_2.\sigma_3 = \mathcal{P}_2.\sigma_2.\sigma_3 = \mathcal{P}_3.\sigma_2.\sigma_3$ , se non si può l'insieme non è unificabile;
- ...
- si unificano  $\mathcal{P}_{12\dots(n-1)}$  e  $\mathcal{P}_n$  con la sostituzione  $\sigma_n$  ottenendo  $\mathcal{P}_{12\dots n} = \mathcal{P}_{12\dots(n-1)}.\sigma_n = \mathcal{P}_n.\sigma_2.\sigma_3 \dots \sigma_{n-1}.\sigma_n$ , se non si può l'insieme non è unificabile;
- l'insieme è unificabile con unificatore  $\sigma_2.\sigma_3 \dots \sigma_{n-1}.\sigma_n$ .

**Esempio** Siano:

- $\mathcal{P}_1 = A(x, y, f(a, x))$
- $\mathcal{P}_2 = A(b, x, f(a, c))$
- $\mathcal{P}_3 = A(z, u, f(a, v))$

dove  $u, v, x, y, z$  sono simboli di variabile e  $a, b, c$  sono simboli di costante.

- Unificare  $\Gamma_1 = \{\mathcal{P}_1, \mathcal{P}_2\}$  :

$$\begin{array}{l} \mathcal{P}_1 = A(x, y, f(a, x)) \\ \mathcal{P}_2 = A(b, x, f(a, c)) \end{array}$$

La prima colonna diversa è  $(x, b)$  dove  $x$  è una variabile e  $b$  una costante, quindi si fa la sostituzione  $\sigma_1 = \{b/x\}$  ottenendo:

$$\begin{array}{l} \mathcal{P}_1.\sigma_1 = A(b, y, f(a, b)) \\ \mathcal{P}_2.\sigma_1 = A(b, x, f(a, c)) \end{array}$$

La prima colonna diversa è  $(y, x)$  dove  $x$  e  $y$  sono variabili, quindi si fa la sostituzione  $\sigma_2 = \{x/y\}$  ottenendo:

$$\begin{array}{l} \mathcal{P}_1.\sigma_1.\sigma_2 = A(b, x, f(a, b)) \\ \mathcal{P}_2.\sigma_1.\sigma_2 = A(b, x, f(a, c)) \end{array}$$

La prima colonna diversa è  $(b, c)$  dove  $b$  e  $c$  sono costanti, quindi non sono unificabili.

## 6. Logica dei predicati o del primo ordine

- Unificare  $\Gamma_2 = \{\mathcal{P}_2, \mathcal{P}_3\}$ :

$$\mathcal{P}_2 = A \quad ( \quad b, \quad x, \quad f \quad ( \quad a, \quad c \quad ) \quad )$$

$$\mathcal{P}_3 = A \quad ( \quad z, \quad u, \quad f \quad ( \quad a, \quad v \quad ) \quad )$$

La prima colonna diversa è  $(b, z)$  dove  $z$  è una variabile e  $b$  una costante, quindi si fa la sostituzione  $\sigma_1 = \{b/z\}$  ottenendo:

$$\mathcal{P}_2.\sigma_1 = A \quad ( \quad b, \quad x, \quad f \quad ( \quad a, \quad c \quad ) \quad )$$

$$\mathcal{P}_3.\sigma_1 = A \quad ( \quad b \quad u, \quad f \quad ( \quad a, \quad v \quad ) \quad )$$

La prima colonna diversa è  $(x, u)$  dove  $x$  e  $u$  sono variabili, quindi si fa la sostituzione  $\sigma_2 = \{x/u\}$  ottenendo:

$$\mathcal{P}_2.\sigma_1.\sigma_2 = A \quad ( \quad b, \quad x, \quad f \quad ( \quad a, \quad c \quad ) \quad )$$

$$\mathcal{P}_3.\sigma_1.\sigma_2 = A \quad ( \quad b, \quad x, \quad f \quad ( \quad a, \quad v \quad ) \quad )$$

La prima colonna diversa è  $(c, v)$  dove  $v$  è una variabile e  $c$  è una costante, quindi si fa la sostituzione  $\sigma_3 = \{c/v\}$  ottenendo:

$$\mathcal{P}_2.\sigma_1.\sigma_2.\sigma_3 = A \quad ( \quad b, \quad x, \quad f \quad ( \quad a, \quad c \quad ) \quad )$$

$$\mathcal{P}_3.\sigma_1.\sigma_2.\sigma_3 = A \quad ( \quad b, \quad x, \quad f \quad ( \quad a, \quad c \quad ) \quad )$$

Che sono unificate con  $\sigma = \{b/z, x/u, c/v\}$ .

- Unificare  $\Gamma_1 = \{\mathcal{P}_1, \mathcal{P}_3\}$  :

$$\mathcal{P}_1 = A \quad ( \quad x, \quad y, \quad f \quad ( \quad a, \quad x \quad ) \quad )$$

$$\mathcal{P}_3 = A \quad ( \quad z, \quad u, \quad f \quad ( \quad a, \quad v \quad ) \quad )$$

La prima colonna diversa è  $(x, z)$  dove  $x$  e  $z$  sono variabili, quindi si fa la sostituzione  $\sigma_1 = \{x/z\}$  ottenendo:

$$\mathcal{P}_1.\sigma_1 = A \quad ( \quad x, \quad y, \quad f \quad ( \quad a, \quad x \quad ) \quad )$$

$$\mathcal{P}_3.\sigma_1 = A \quad ( \quad x \quad u, \quad f \quad ( \quad a, \quad v \quad ) \quad )$$

La prima colonna diversa è  $(y, u)$  dove  $y$  e  $u$  sono variabili, quindi si fa la sostituzione  $\sigma_2 = \{y/u\}$  ottenendo:

$$\mathcal{P}_1.\sigma_1.\sigma_2 = A \quad ( \quad x, \quad y, \quad f \quad ( \quad a, \quad x \quad ) \quad )$$

$$\mathcal{P}_3.\sigma_1.\sigma_2 = A \quad ( \quad x, \quad y, \quad f \quad ( \quad a, \quad v \quad ) \quad )$$

La prima colonna diversa è  $(x, v)$  dove  $x$  e  $v$  sono variabili, quindi si fa la sostituzione  $\sigma_3 = \{x/v\}$  ottenendo:

$$\mathcal{P}_1.\sigma_1.\sigma_2.\sigma_3 = A \quad ( \quad x, \quad y, \quad f \quad ( \quad a, \quad x \quad ) \quad )$$

$$\mathcal{P}_3.\sigma_1.\sigma_2.\sigma_3 = A \quad ( \quad x, \quad y, \quad f \quad ( \quad a, \quad x \quad ) \quad )$$

Che sono unificate con  $\sigma = \{x/z, y/u, x/v\}$ .

- Unificare  $\Gamma = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$  :

$$\mathcal{P}_1 = A \quad ( \quad x, \quad y, \quad f \quad ( \quad a, \quad x \quad ) \quad )$$

$$\mathcal{P}_2 = A \quad ( \quad b, \quad x, \quad f \quad ( \quad a, \quad c \quad ) \quad )$$

$$\mathcal{P}_3 = A \quad ( \quad z, \quad u, \quad f \quad ( \quad a, \quad v \quad ) \quad )$$

La prima terna di simboli che differiscono è  $(x, b, z)$  che contiene due simboli di variabile, per cui usiamo  $\sigma_1 = \{b/x, b/z\}$  ottenendo:

$$\mathcal{P}_1.\sigma_1 = A \quad ( \quad b, \quad y, \quad f \quad ( \quad a, \quad x \quad ) \quad )$$

$$\mathcal{P}_2.\sigma_1 = A \quad ( \quad b, \quad x, \quad f \quad ( \quad a, \quad c \quad ) \quad )$$

$$\mathcal{P}_3.\sigma_1 = A \quad ( \quad b, \quad u, \quad f \quad ( \quad a, \quad v \quad ) \quad )$$

La prima terna di simboli che differiscono è  $(y, b, u)$ , usiamo quindi  $\sigma_2 = \{b/y, b/u\}$  ottenendo:

$$\mathcal{P}_1.\sigma_1.\sigma_2 = A \quad ( \quad b, \quad y, \quad f \quad ( \quad a, \quad x \quad ) \quad )$$

$$\mathcal{P}_2.\sigma_1.\sigma_2 = A \quad ( \quad b, \quad x, \quad f \quad ( \quad a, \quad c \quad ) \quad )$$

$$\mathcal{P}_3.\sigma_1.\sigma_2 = A \quad ( \quad b, \quad u, \quad f \quad ( \quad a, \quad v \quad ) \quad )$$

La prima terna di simboli che differiscono è  $(b, c, v)$  che contiene due simboli di costante, quindi  $\Gamma$  non è unificabile.

Se al posto di  $c$  ci fosse  $b$ , sarebbe unificabile usando  $\sigma_3 = \{b/v\}$  con risultato  $A(b, b, f(a, b))$  e  $\sigma_1.\sigma_2.\sigma_3 = \{b/x, b/z, b/y, b/u, b/v\}$ .

**Definizione** Siano  $\mathcal{C}_1$  e  $\mathcal{C}_2$  due clausole:

- effettuiamo, se necessario, sostituzioni  $\sigma_1$  e  $\sigma_2$  su  $\mathcal{C}_1$  e  $\mathcal{C}_2$  in modo tale che  $\mathcal{C}_1.\sigma_1$  e  $\mathcal{C}_2.\sigma_2$  non abbiano variabili libere in comune;
- siano  $L_1, \dots, L_r$  letterali di  $\mathcal{C}_1.\sigma_1$  e  $M_1, \dots, M_s$  letterali di  $\mathcal{C}_2.\sigma_2$  tali che  $\{L_1, \dots, L_r, \sim M_1, \dots, \sim M_s\}$  sia unificabile e sia  $\sigma$  un unificatore più generale di quell'insieme;
- allora  $\mathcal{R} = (\mathcal{C}_1.\sigma_1 \setminus \{L_1, \dots, L_r\}) . \sigma \cup (\mathcal{C}_2.\sigma_2 \setminus \{M_1, \dots, M_s\}) . \sigma$  è una **risolvente** per  $\mathcal{C}_1$  e  $\mathcal{C}_2$ .

Il procedimento iterativo è lo stesso della logica proposizionale: si aggiungono risolventi di coppie di clausole dell'insieme.

**Teorema** Sia  $\Gamma$  un insieme di fbf.

- $\Gamma$  è insoddisfacibile se e solo se  $\Gamma \vdash_{\mathcal{R}} \square$ .
- Se  $\mathcal{P}$  è una fbf,  $\Gamma \models \mathcal{P}$  se e solo se  $\Gamma \cup \{\neg \mathcal{P}\} \vdash_{\mathcal{R}} \square$ .

Al contrario della logica proposizionale non può esistere un algoritmo che riesca a dedurre la clausola vuota per tutti gli insiemi di clausole insoddisfacibili. Infatti un tale algoritmo darebbe una soluzione al problema dell'arresto.

## 6.3. Complementi

### 6.3.1. Decidibilità

**Teorema (Church)** Non esiste alcun algoritmo che consenta di decidere la validità di una qualsiasi fbf in un linguaggio della logica del primo ordine.

### 6.3.2. Gödel

**Teorema (1° teorema d'incompletezza)** Sia  $\mathcal{T}$  una teoria assiomatizzabile (cioè in cui esiste un numero finito di assiomi) e sufficientemente espressiva da poter codificare gli interi.

Allora esiste in  $\mathcal{T}$  una formula chiusa  $\varphi$  tale che se  $\varphi$  non è contraddittoria, né  $\varphi$  né  $\neg \varphi$  sono dimostrabili.

**Teorema (2° teorema d'incompletezza)** Sia  $\mathcal{T}$  una teoria assiomatizzabile (cioè in cui esiste un numero finito di assiomi) e sufficientemente espressiva da poter codificare gli interi.

Sia  $\text{Cons}_{\mathcal{T}}$  una fbf chiusa che esprime la consistenza di  $\mathcal{T}$ .

Se  $\mathcal{T}$  è consistente (cioè non contraddittoria) non esiste in  $\mathcal{T}$  una dimostrazione di  $\text{Cons}_{\mathcal{T}}$ .

**Parte III.**

**Appendici**

## A. La prova del 9

Sia da verificare l'operazione  $a \star b = c$  con  $\star = +, -, \cdot$ .

Si scrive una croce  $\times$ , in alto si mette la somma delle cifre di  $a$ , in basso la somma delle cifre di  $b$ , a sinistra la somma delle cifre di  $c$  e a destra la somma delle cifre di  $[a]_9 \star [b]_9$ . Devono risultare uguali la destra e la sinistra.

Verifichiamo che se  $n = c_k \dots c_0$  con  $1 \leq c_i \leq 9$  in scrittura decimale allora  $[n]_9 = \left[ \sum_{i=0}^k c_i \right]$ .

$$n = \sum_{i=0}^k (c_i \cdot 10^i)$$

$$[n]_9 = \left[ \sum (c_i \cdot 10^i) \right]_9 = \sum [c_i \cdot 10^i]_9 = \sum [c_i]_9 \cdot [10]_9^i = \sum [c_i]_9 \cdot [1]_9^i = \sum [c_i]_9$$

sostituendo 3 al posto di 9 viene  $[10]_3 = [1]_3$  e quindi lo stesso risultato:  $[n]_3 = \sum [c_i]_3$ . Sostituendo 2, 5, 10 al posto di 9 viene  $[10]_{2,5,10} = [0]_{2,5,10}$ , quindi scompaiono gli  $i \geq 1$  e rimane  $[n]_{2,5,10} = [c_0]_{2,5,10}$ .

Sostituendo 11 al posto di 9, viene  $[10]_{11} = [-1]_{11}$  quindi  $[n]_{11} = \left[ \sum ((-1)^i c_i) \right]_{11}$ .

Possiamo quindi fare la prova del 9 (con la somma delle cifre), la prova del 10 (con la cifra delle unità) e la prova dell'11 (con la somma alternata delle cifre) e se tutte e 3 sono soddisfatte, dal teorema cinese dei resti l'operazione è giusta modulo  $990 = 9 \cdot 10 \cdot 11$ .

## B. Divertimenti

### Ci sono più reali che interi

$\mathbb{N}$ ,  $\mathbb{Z}$  e  $\mathbb{Q}$  hanno “lo stesso numero” di elementi perché le frazioni  $\frac{a}{b}$  corrispondono ad una coppia  $(a, b)$  con  $b > 0$  e  $MCD(a, b) = 1$ .

In  $\mathbb{R}$  invece ci sono più elementi.

Consideriamo l'intervallo  $I = [0, 1)$  e supponiamo di avere una successione  $(a_n)_{n \geq 1}$  di elementi di  $I$ . Sia  $x = 0, c_1 c_2 \dots c_n$  con  $c_n = 0$  se e solo se la  $n$ -esima cifra di  $a_n$  è dispari, e  $c_n = 1$  nell'altro caso.  $x$  è un elemento di  $I$ . Inoltre la  $n$ -esima cifra di  $x$  è diversa da quella di  $a_n$ , quindi  $\forall n \ x \neq a_n$ .

$x$  è anche detto *argomento diagonale di Cantor*.

### Non esiste l'insieme degli insiemi

Supponiamo che ci sia un insieme  $I$  degli insiemi. Allora ci deve essere l'insieme  $A$  degli insiemi  $X$  tali che  $X \notin X$ . Ma:

- se  $A \in A$ , per la definizione di  $A$ ,  $A$  non è un elemento di  $A$ , quindi è una contraddizione;
- se  $A \notin A$ , per la definizione di  $A$ ,  $A$  è un elemento di  $A$ , quindi è una contraddizione.

Quindi  $A$  non esiste, e di conseguenza neppure  $I$ .

# Indice analitico

- alfabeto per un linguaggio della logica del primo ordine, 59
- alfabeto per un linguaggio della logica proposizionale, 43
- algoritmo di Diffie-Hellman, 34
- algoritmo di Euclide, 32
- algoritmo RSA, 35
- ambiente (o assegnamento) per un linguaggio del primo ordine in una struttura, 65
- anello, 36
- anello commutativo, 37
- anello di polinomi, 39
- anello nullo, 37
- anello principale, 39
- anello quoziente, 38
- antisimmetria, 7
- applicazione, 6
- automorfismo di gruppi, 25
- campo, 39
- campo d'azione di un quantificatore, 62
- cappio, 6
- centro di un gruppo, 20
- chiusura esistenziale di una fbf della logica del primo ordine, 69
- chiusura universale di una fbf della logica del primo ordine, 69
- classe di resto, 12
- classe di equivalenza, 9
- clausola, 56, 71
- clausola vuota, 71
- complemento di un elemento di un reticolo limitato, 16
- completezza di un sistema deduttivo, 53
- composizione di sostituzioni, 72
- concatenazione di parole, 21
- congruenza modulo  $n$ , 11
- connettivo derivabile, 51
- connettivo principale, 44
- conseguenza semantica, 48, 67
- consistenza di un insieme di fbf, 56
- corpo, 40
- correttezza di un sistema deduttivo, 53
- corrispondenza, 6
- derivazione di una clausola per risoluzione, 58
- divisione euclidea, 27
- elemento assorbente, 17
- elemento invertibile, 17
- endomorfismo di gruppi, 25
- equazioni diofantee, 31
- equivalenza, 7
- equivalenza semantica tra fbf, 49
- equivalenza semantica tra fbf della logica del primo ordine, 69
- estremo inferiore, 15
- estremo superiore, 15
- fbf atomica, 44
- fbf del linguaggio del primo ordine atomica, 60
- fbf del linguaggio del primo ordine falsa in una struttura, 67
- fbf del linguaggio del primo ordine insoddisfacibile (o contraddittoria), 67
- fbf del linguaggio del primo ordine soddisfacibile, 66
- fbf del linguaggio del primo ordine soddisfacibile in una struttura, 66
- fbf del linguaggio del primo ordine valida, 66
- fbf del linguaggio del primo ordine vera in una struttura, 66
- fbf duale, 51
- fbf insoddisfacibile (o contraddittoria), 47
- fbf soddisfacibile, 47
- forma a clausole, 56, 71
- forma di Skolem, 70
- forma normale congiuntiva, 52
- forma normale disgiuntiva, 52
- forma normale prenessa, 70
- formula ben formata, 44
- grado di un polinomio, 39

- gruppo, 19
- gruppo finito, 25
- ideale di un anello, 37
- ideale di  $\mathbb{Z}$ , 27
- ideale principale, 28
- immagine di un morfismo, 26
- indicatore di Eulero, 34
- insieme dei termini di un linguaggio del primo ordine, 59
- insieme delle fbf di un linguaggio del primo ordine, 59
- insieme delle formule ben formate, 43
- insieme delle variabili libere di un termine, 62
- insieme delle variabili libere di una fbf, 62
- insieme delle variabili vincolate di una fbf, 62
- insieme di connettivi funzionalmente completo, 51
- insieme di fbf del linguaggio del primo ordine falso in una struttura, 67
- insieme di fbf del linguaggio del primo ordine insoddisfacibile, 67
- insieme di fbf del linguaggio del primo ordine soddisfacibile, 67
- insieme di fbf del linguaggio del primo ordine valido, 67
- insieme di fbf non unificabile, 72
- insieme di fbf unificabile, 72
- insieme ciclico di generatore  $g$ , 25
- insieme delle classi di resto modulo  $n$ , 12
- insieme quoziente, 10
- interpretazione (o valutazione), 46
- interpretazione per un linguaggio del primo ordine, 65
- inverso per una lci, 17
- isomorfismo di gruppi, 25
- lci abeliana, 19
- lci associativa, 17
- lci commutativa, 17
- legge di composizione interna, 17
- letterale, 52, 71
- lunghezza di una parola, 21
- maggiorante, 15
- massimale, 15
- massimo, 15
- MCD, 30
- mcm, 30
- minimale, 15
- minimo, 15
- minorante, 15
- modello per un insieme di fbf, 48
- modello per un insieme di fbf del linguaggio del primo ordine, 67
- modello per una fbf, 47
- modello per una fbf del linguaggio del primo ordine, 66
- monoide, 19
- morfismo di gruppi, 25
- neutro di una lci, 17
- nucleo di un morfismo, 26
- operazione di arit   $k$ , 18
- ordine, 7
- ordine di un elemento, 23
- ordine di un gruppo, 25
- ordine totale, 14
- parola nell'alfabeto  $A$ , 21
- parola vuota, 21
- partizione, 10
- polinomio, 39
- polinomio irriducibile, 40
- prodotto tra classi di resto, 14
- proiezione canonica, 10
- rappresentante di una classe di resto, 13
- regola di Peirce, 54
- relazione, 6
- restrizione ad un sottoinsieme, 8
- reticolo, 16
- reticolo complementato, 16
- reticolo limitato, 16
- riflessivit , 6
- risolvente di clausole, 57, 75
- semigrupp , 19
- simmetria, 7
- sistema completo di rappresentanti, 13
- somma tra classi di resto, 14
- somma di ideali di  $\mathbb{Z}$ , 29
- sostituzione, 72
- sottoformula, 44
- sottogruppo, 21
- sottogruppo normale, 23
- struttura algebrica, 18
- struttura per un linguaggio del primo ordine, 65



tautologia, 47  
teorema cinese dei resti, 31  
teorema del sistema di deduzione naturale, 56  
teorema di Bezout, 30  
termine libero per una variabile, 64  
transitività, 7  
  
unificatore per un insieme di fbf, 72  
unificatore più generale di un insieme di fbf, 72  
  
variabile libera per una variabile in una fbf, 63