Algebra e logica - esercizi

Silviu Filote

September 18, 2021

Contents

1 Capitolo I

Dimostrazione Posti A ipotesi e B tesi

$$A \Rightarrow B$$

$$\text{"}Se\ A\ allora\ B\text{"}$$

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

Figure 1: tabella di verità

Osservazione

- Gli elementi sono indicati con la lettera minuscola, mentre gli insiemi con la lettera maiuscola;
- Gli elementi appartengono a un insisme, es: $a \in F$;
- $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3\}$;
- $\mathbb{N} = \mathbb{Z}^+$;
- $\mathbb{Q} = frazioni$;
- $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$;

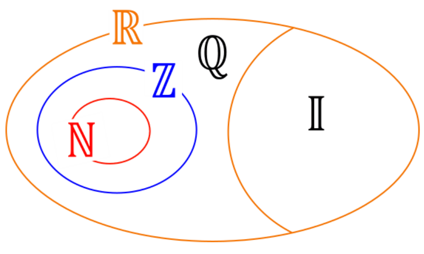


Figure 2: insiemistica

Osservazione Dimostrare un teorema significa trovare un argomentazione logica che abbia validità generale, al contrario basta un solo caso per dimostrare la sua falsità.

Osservazione Un insieme è una collezione di oggetti tale che per ogni oggetto si possa dire con certezza che è dentro o fuori l'insieme.

Esempio L'ordine e la duplicazioni di elementi all'interno di un insime non contano.

$$A = \{1, 2, 3, 4\}$$
$$B = \{2, 1, 1, 3, 4\}$$
$$A = B$$

Paradosso di Russel Supponiamo che esista l'insieme $\mathcal{I}$ di tutti gli insiemi. Dentro $\mathcal{I}$ andiamo a considerare il sottoinsieme A dove:

$$A = \{X \in \mathcal{I} : X \notin X\}$$

ossia l'insieme di tutti gli insiemi che non appartengono a sé stessi

A questo punto A è un insieme e quindi $A \in \mathcal{I}$, ci sono quindi due possibilità:

- $A \in A$ non è possibilie perchè gli elementi di A sono quelli che non appartengolo a se stessi
- $A \notin A \quad \Rightarrow \quad A \in A$ assurdo

L'errore è ammettere che si possa considerare l'insieme di tutti gli insiemi.

Definizione Dati 2 insiemi A e B il loro **prodotto cartesiano** è:

$$A \times B$$

è l'insieme di tutte le coppie:

$$(a, b) \quad a \in A \quad b \in B$$

Esempio

$$A \times A \textit{ si indica con } A^2$$
$$A \times A \times ... \times A = A^{\mathrm{n}}$$

$$\{(a, b, c, .., z) : a \in A, b \in B, ..., z \in Z\}$$
$$\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$$

Definizione Dati 2 insiemi A e B una **corrispondenza** f da un insieme A verso un insieme B è un sottoinsieme di $A \times B$. Scriveremo anche

$$f \subseteq A \times B$$

L'insime A si chiama insieme di partenza e B codominio. Se $(a, b) \in f$ allora:

$$afb$$

Osservazione A differenza delle funzioni $f(a)$ è un insieme che può contenere anche più di un elemento.

Definizione **Una applicazione** da A verso B è una corrispondenza f da A verso B tale che $\forall a \in A$ esiste **esattamente** $b \in B$ tale che $(a, b) \in f$. Equivalentemente $\forall a \in A$, $f(a)$ contiene esattamente un elemento.

Definizione Una **funzione** f da un insieme A verso un insieme B è una applicazione da un sottoinsieme $D \subseteq A$ verso B. D è detto **dominio** della funzione.

Osservazione $(a, b) \neq (b, a)$ se $b \neq a$, mentre $\{a, b\} = \{b, a\}$

Definizione Una **relazione** è una corrispondenza di un insieme con se stesso.

$$\rho \subseteq A \times A = A^2$$

$$x, y \in A,\ (x, y) \in \rho \Rightarrow x\rho y.$$
$$\text{Se invece } (x, y) \notin \rho \Rightarrow x\not\rho y.$$

Esempio La relazione è un'operazione che comprende

- $A = \mathbb{N}\ (\mathbb{Z}, \mathbb{Q}, \mathbb{R})$, $(\rho, \leq) = \{(a, b) \in A \times A : a \leq b\}$
  $\{(a, b) \in A \times A : \exists c \in \mathbb{R} : b = a + c^2\}$
- A qualsiasi, $(\rho, =) = \{(a, a) \in A \times A : a \in A\}$
- $A = \mathbb{N}\ (\mathbb{Z})$, $(\rho, |) = \{(a, b) \in A^2 : a|b\}$
  $\{(a, b) \in A^2 : \exists k \in A : b = a \cdot k\}$
  $\Rightarrow a|b$ se e solo se $\exists k \in A : b = a \cdot k$
  chiave lettura, a divide b

- Sia X un insieme e sia $\mathcal{P}(X)$ l'insieme delle parti di X
  $\subseteq\ = \{(F, G) \in \mathcal{P}(X) \times \mathcal{P}(X) : \ \textit{se } x \in F \textit{ allora } x \in G\}$

- $A =$ piano, ossia $\mathbb{R}^2$, $\rho = \{(P, Q) \in A \times A : \ P \textit{ e } Q \textit{ stessa ordinata}\}$

Osservazione Gli elementi che soddisfano la relazione $\in \rho$, dove ρ è una delle operazioni citate sopra, per cui
$\rho = \{=, \leq, \subseteq, |,$ *un'equazione, una frase*$\}$ e si legge esempio: $\subseteq$ **è una relazione** su A. La relazione è un'insieme.

2 Capitolo II

Definizione Data una relazione ρ su un insieme A, le associamo un **grafo orientato** nel modo seguente:

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

Proprietà Sia A un insieme e sia ρ una relazione su A.

- Si dice che ρ è **riflessiva** se e solo se $\forall a \in A \Rightarrow a\rho a$.
  Sul grafo c'è una freccia, detta **cappio**, da ogni elemento verso se stesso.
- Si dice che ρ è **simmetrica** se tutte le volte che vale $a\rho b$ vale anche $b\rho a$, ossia: $\forall a, b \in A$ se $a\rho b \Rightarrow b\rho a$.
  Sul grafo se esiste uno spigolo da a verso b allora esisterà anche lo spigolo da b verso a.
- Si dice che ρ è **transitiva** se e solo se $\forall (a, b, c) \in A^3$ valgono $a\rho b \wedge b\rho c \Rightarrow a\rho c$.
  Nel grafo significa che ci sono le **scorciatoie**.
- Si dice che ρ è **antisimmetrica** se e solo se $\forall (a, b) \in A^2$ valgono $a\rho b \wedge b\rho a \Rightarrow a = b$.
  Non ci sono frecce in versi opposti, tranne eventuali cappi.
- Si dice che ρ è una relazione di **equivalenza** se ρ è
  - riflessiva;
  - transitiva;
  - simmetrica;

  Sul grafo si "chiudono i cerchi".
- Si dice che ρ è una relazione di **d'ordine** se ρ è
  - riflessiva;
  - transitiva;
  - antisimmetrica;

Sul grafo si dispongono i vertici in modo che tutte le frecce siano rivolte verso l'alto e si può omettere le frecce utilizzando solo segmenti.

Esempi

$=$	equivalenza e ordine;
$\leq$	ordine;
$\subseteq$	ordine;
$<$	transitiva e antisimmetrica;
"stessa odinata"	uguaglianza;
$\mid$	è una relazione d'ordine per $\mathbb{N}$ ma non per $\mathbb{Z}$;

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

$$[a]_\sim = [a] = \{b \in A : b \sim a\}$$

- Poichè ρ è riflessiva, quindi $\forall a \in A$, $a \in [a]_\sim$. In particolare nessuna classe di equivalenza è vuota $\Rightarrow [a]_\sim \neq \varnothing$;
- Poichè $\sim$ è simmetrica se $b \in [a] \Rightarrow b \sim a \Rightarrow a \sim b$ e quindi $a \in [b]$;

Proposizione fondamentale Siano A un insieme e sia $\sim$ una relazione di equivalenza su A. Se $a, b \in A$ allora:

1. $[a] = [b] \Leftrightarrow a \sim b$
2. $[a] \neq [b] \Leftrightarrow [a] \cap [b] = \varnothing$

Dimostrazione

1 $(\Rightarrow)$ Siccome $b \in [b]_\sim$ per la priprietà riflessiva e $[b]_\sim = [a]_\sim$ per ipotesi, allora $b \in [a]_\sim$ quindi $a \sim b$.

1 $(\Leftarrow)$ 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 $c \in [b] \to b \sim c$; siccome $\sim$ è transitiva, $a \sim c$, cioè $c \in [a]$ quindi $[b] \subseteq [a]$. Siccome $\sim$ è simmetrica si può dimostrare la seconda parte in modo analogo, quindi $[a] = [b]$.

2 ($\Leftarrow$) Immediato perchè $a \in [a]$, $[a] \cap [b] = \varnothing \Rightarrow a \notin [b] \Rightarrow [a] \neq [b]$.

2 ($\Leftarrow$) Facciamo la dimostrazione contrapposta, cioè che se $[a] \cap [b] \neq \varnothing$ $\Rightarrow [a] = [b]$.
Se $[a] \cap [b] \neq \varnothing$, allora $\exists c \in [a] \cap [b] \Rightarrow a \sim c$ e $b \sim c$, cioè $a \sim c$ e $c \sim b \Rightarrow a \sim b \Rightarrow$ dalla (1) $[a] = [b]$.

Definizione **L'insieme quoziente** di A per $\sim$ è l'insieme delle classi di equivalenza

$$A/_{\sim} = \{[a]_{\sim} : a \in A\}$$

L'applicazione

$$\pi : A \to A/_{\sim}$$
$$a \to [a]_{\sim}$$

Si chiama **proiezione canonica**.

3 Capitolo III

Definizione Sia A un insieme e sia F un insieme di **sottoinsiemi** di A, si dice che F è una **partizione** di A se valgono le seguenti Proprietà:

1. $\varnothing \notin F$
2. $\bigcup_{X \in F} X = A$
3. Se $X, Y \in F$ e $X \cap Y \neq \varnothing$ allora $X = Y$

Dimostrazione Siano A insieme e $\sim$ una relazione di equivalenza su A. Dobbiamo dimostrare che $F = A_{/\sim}$ è una partizione di A.

1. $F = \{[a]_\sim, a \in A\}$, poichè $[a]_\sim = \{b \in A : a \sim b\} \Rightarrow a \in [a]_\sim$ **per la proprietà riflessiva** $a \sim a$ e quindi $[a]_\sim \neq \varnothing$
2. É ovvio perchè ogni elemento $a \in A$ appartiene alle classi di equivalenza di $[a]_\sim \Rightarrow \bigcup_{X \in F} X = \bigcup [a]_\sim = A$.
   L'unione delle classi di equivalenza di A danno proprio A.
3. $[a]_\sim, [b]_\sim \in F,\ \ [a]_\sim \cap [b]_\sim \neq \varnothing$ **Per la proposizione fondamentale** $\Rightarrow [a]_\sim = [b]_\sim$

NB

- La condizione **1)** mi dice che la partizione non è mai vuota;
- La condizione **2)** mi dice che ogni elemento di A sta in un elemento delle partizioni;
- La condizione **3)** mi dice che un elemento $a \in A$ non può appartenere a due elementi X e Y diversi;

Osservazione Le classi di equivalenza sono una partizione su A.

Osservazione Dati $a, b \in A$ diciamo che

$$a \sim b \ \textit{sse} \ \exists X \in F : a, b \in X$$

Congruenza modulo n Presi $a, b, n \in \mathbb{Z}$ diremo che a **è congruo a** b **modulo** n se e solo se:

$$\exists K \in \mathbb{Z} : a = b + k \cdot n$$

Scriveremo

$$a \equiv_n b \qquad a \equiv b \ mod\ n \qquad a \equiv b(n)$$

Osservazione La posizione della lettura coincide con la formula matematica

$$\text{" } a \textit{ congruo } b \textit{ modulo } n \text{ "}$$
$$a \equiv b \ mod\ n$$

Definizione Per ogni $n \in \mathbb{Z}$ la relazione $\equiv_n$ è una relazione di equivalenza su $\mathbb{Z}$.

Dimostrazione $\equiv_n$ sia riflessiva, transitiva e simmetrica.

<u>R</u> Sia $a \in \mathbb{Z}$, con $k = 0$ otteniamo $a = a + 0 \cdot n = a$ e quindi $a \equiv_n a$

<u>S</u> Siano $a, b \in \mathbb{Z}$ tali che $b \equiv_n a$ e quindi $\exists k \in \mathbb{Z}$ tali che $b = a + k \cdot n$, allora $a = b - k \cdot n = b + (-k) \cdot n$, $(-k) \in \mathbb{Z}$ e quindi $a \equiv_n b$, quindi $\equiv_n$ è simmetrica

<u>T</u> Siano $a, b, c \in \mathbb{Z}$ tali che $a \equiv_n b$ e $b \equiv_n c \Rightarrow \exists k, l \in \mathbb{Z} : a = b + k \cdot n$ e $b = c + l \cdot n$. Allora $a = c + k \cdot n + l \cdot n = c + (k + l) \cdot n$. Siccome $(k + l) \in \mathbb{Z}, a \equiv_n c$. Quindi $\equiv_n$ è transitiva.

Osservazioni

- $\equiv_n$ e $\equiv_{-n}$ sono la stessa cosa, per cui prenderemo $\Rightarrow n \geq 0$;

$$a = b + k \cdot n = b + (-k) \cdot (-n)$$

- Con $n = 0 \Rightarrow a \equiv b \ mod\ 0 \Rightarrow \exists k \in \mathbb{Z} : b = a + k \cdot 0 = b$, quindi $\equiv_0$ **è l'uguaglianza** $b = a$

$$[a]_{\equiv_0} = \{a\}, \ \textit{quindi} \ \equiv_0 \ \textit{è} \ =$$

- $[a]_{\equiv_1} = \mathbb{Z}$, quindi $\forall a, b \in \mathbb{Z}, a \equiv_1 b$, relazione nella quale tutti gli elementi sono in realzione tra loro, perchè posso sempre calcolare:

$$k = a - b$$

- Con $n = 2$, avremo $a \equiv_2 b$ ossia $a = b + 2k \Rightarrow a - b$ **è pari**;

Definzione Sia $n \geq 1$ e $a \in \mathbb{Z}$ la **classe di** a è:

$$[a]_n = [a]_{\equiv_n} = \{\ ..,\ a\ \text{-}\ 2n,\ a\ \text{-}\ n,\ \boldsymbol{a},\ a\ +\ n,\ a\ +\ 2n,\ ..\ \}$$

$$[3]_7 = \{..,\ \text{-}11,\ \text{-}4\ ,\ \boldsymbol{3},\ 10,\ 17,\ ..\} \Rightarrow 3 \pm 7 \cdot k$$

Osservazione Data una relazione di equivalenza $\sim$, $[a]_\sim$ classe di equivalenza. Nel caso delle congruenza modulo n, $\equiv_n$ le classi di equivalenza per $\equiv_n$ si chiamano **classi di congruenza modulo n**.

Divisione Euclidea Dato $a \geq 0$ e $n \geq 1$ esistono q e r, con $0 \leq r < n$ tali che

$$a = q \cdot n + r$$

- q, quoziente;
- r, resto sempre positivo;

Proposizione In realtà la condizione $a \geq 0$ non è necessaria. Dato $a \in \mathbb{Z}$ e $n \geq 1$ esistono **e sono unici** $q \in \mathbb{Z}$ e r tale che $0 \leq r < n$ per cui

$$a = q \cdot n + r$$

Proposizione **1)** Sia $n \geq 1$, fissato. Ci sono n classi di equivalenza per la congruenza modulo n. Sono $[0]_n, [1]_n, .., [n-1]_n$.
2) Se $a \in \mathbb{Z}$ e r è il resto della divisione per n allora $[a]_n = [r]_n$.

Dimostrazione 1) e **2)**.

1. Per la definizione di divisione euclidea il resto può valore solo n valori, infatti: $0 \leq r < n$, 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. Presi allora $0 \leq r_1 < n$ e $0 \leq r_2 < n$, **NON** può valore che $r_2 \equiv_n r_1$. Supponiamo che $r_1 > r_2$ se valesse $r_2 \equiv_n r_1$ avremmo

$$r_1 = r_2 + k \cdot n \quad ma$$

$$r_1 - r_2 = k \cdot n$$

L'unico risulato in grado di dare un multiplo è con $k = 0$, per cui:

$$r_1 = r_2$$

Per cui ci sono esattamente n classi.

2. Sia $a \in \mathbb{Z}$ possiamo scrivere:

$$a = q \cdot n + r = r + q \cdot n \Rightarrow a \in [r]_n$$

$$[a]_n = [r]_n$$

Le uniche classi di equivalenza sono:

$$[0]_n, [1]_n, .., [n-1]_n$$

e queste vengono indicate con

$$\mathbb{Z}/_{\equiv_n} \quad = \quad \mathbb{Z}/n\mathbb{Z} \quad = \quad \mathbb{Z}_n$$

Si chiamano anche **classi di resti** (dove $\mathbb{Z}/_{\equiv_n}$ è l'insieme quoziente di $\equiv_n$, ossia comprende tutti i possibili risultati, quindi le n classi).

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

Esempio $\mathbb{Z}/6\mathbb{Z}$

$$[a]_6 = [a]_{\equiv_6} \Rightarrow \mathbb{Z}/6\mathbb{Z} = \{\textit{[0], [1], [2], [3], [4], [5]}\}$$

Definzione 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 $C = [a]_\sim$ sse a è un rappresentante di C).

Definzione 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 $\sim$.

Esempio Qualunque numeri pari è un rappresentanto di $[0]_2$. Qualunque numero numero dispari è un rappresentante di $[1]_2$

Osservazione Il rappresentate di per se risulta essere un solo numero, quindi può essere un qualsiasi numero all'interno della classe di equivalenza.

Definizione Quando si definiscono delle funzioni tra classi di resto bisogna stare attenti ai rapprensentanti usati.

4 Capitolo IV

Def: Una *relazione* è una corrispondenza di un insieme con se stesso

$$\rho \subseteq A \times A = A^2$$

$$x, y \in A \quad (x, y) \in \rho$$

$$x\rho y \quad altrimenti \quad x\not\rho y$$

$$interpretiamo\ \rho\ come\ un\ insieme$$

Proprietà:

- Riflessiva → sse $\forall a \in A \Rightarrow a\rho a$
- Simmetrica → $\forall (a, b) \in A^2,\ \ se\ vale\ \ a\rho b \Rightarrow b\rho a$
- Transitiva → $\forall (a, b, c) \in A^3,\ \ se\ vale\ \ a\rho b\ e\ b\rho c \Rightarrow a\rho c$
- Antisimmetrica → $\forall (a, b) \in A^3,\ \ se\ vale\ \ a\rho b\ e\ b\rho a \Rightarrow a = b$

Proposizione: Se la proposizione

$$nRm \Rightarrow mRn$$

- Risulta essere **vera** per il fatto che nRm non è mai vera
- Infatti non siamo in grado di esibira un caso in cui $nRmn$ è vera ma mRn è falsa

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

Figure 3: tabella di verità implicazione

<u>Accorgimenti:</u>

- Non esiste coppie di elementi tali per cui $a < b$ e $b < a$
- Nel caso in non siamo in grado di dire direttamente se la proposizione sia falsa o vera andiamo per **tentativi numerici**. Solitamente la cosa semplice da fare è **sostituire** 0 **a una delle incognite** e vedere il comportamento dell'equazione.
- Nel caso transitivo aRb e $bRc \Rightarrow aRc$ ***Dobbiamo dimostrare la validità di*** aRb ***e*** bRc ***e poi vedere come si comporta*** aRc. Facciamo questo perchè ci poniamo nel solo caso della tabella di verità in cui l'implicazione risulta essere **FALSA** nel caso in cui aRc sia falsa.
- **<u>Ragionare con la tabella di verità nel caso di implicazione</u>**
- **Cercare sempre di dimostrare la falsità, perchè basta un solo caso, nel caso contrario diventa una dimostrazione e bisogna commentarla**

Accorgimenti proprietá riflessiva:

- La Proprietà riflessiva vale se

$$(x^2 + 4)(x^4 + 7) = (x^2 + 4)(x^4 + 7)$$

- La Proprietà riflessiva vale se

$$x^2 - x^2 = x - x$$

$$0 = 0$$

- La relazione riflessiva ***deve*** valere $\forall a$ se viene imposto un limite su a risulta essere non riflessiva. Esempio:

$$aRa = 2 \cdot a - a < 3 = a < 3$$

$$4R4 = 8 - 4 < 3 = 4 < 3$$

$$\textit{impossibile, non vale } \forall a$$

Accorgimenti proprietá simmetrica:

- La Proprietà simmetrica si dimostra se l'equazione:

$$x\rho y \to x^2 - y^2 = x - y$$

$$y\rho x \to y^2 - x^2 = y - x$$

basterebbe vedere $x\rho y$ come una funzione $f(x)$ la sua simmetrica è $-f(x)$, opposto tende ad essere simmetrico.

Accorgimenti proprietá transitiva:

- Transitiva *tramite somma*: $x\rho y$ e $y\rho w \Rightarrow x\rho w$

$$x\rho y \to x^2 - y^2 = x - y$$

$$y\rho w \to y^2 - w^2 = y - w$$

sommando $x\rho y$ e $y\rho w$ ottengo:

$$x^2 - \cancel{y^2} + \cancel{y^2} - w^2 = x - \cancel{y} + \cancel{y} - w$$

$$x^2 - w^2 = x - w$$

*Sommando quindi 2 relazioni che per **definizione devono valere**, si ottiene quella finale.*

- Transitiva *tramite prodotto - sostituzione: $x\rho y$ e $y\rho z \Rightarrow x\rho z$*

$$\begin{aligned}(x^3+2)(y^2+1) &= (y^3+2)(x^2+1) \quad && xRy\\ (y^3+2)(z^2+1) &= (z^3+2)(y^2+1) && yRz\\ (x^3+2)(z^2+1) &= (z^3+2)(x^2+1) && xRz\end{aligned}$$

$$(x^3+2)(z^2+1)\frac{(y^2+1)}{y^2+1} =$$

$$(x^3+2)(y^2+1)\frac{(z^2+1)}{y^2+1} = (y^3+2)(x^2+1)\frac{(z^2+1)}{y^2+1}$$

$$(y^3+2)(z^2+1)\frac{(x^2+1)}{y^2+1} = (z^3+2)(y^2+1)\frac{(x^2+1)}{y^2+1}$$

$$(z^3+2)\cancel{(y^2+1)}\frac{(x^2+1)}{\cancel{y^2+1}} = (z^3+2)(x^2+1)$$

- Transitiva *tramite somma $\pm$ e sostituzione:* $x\rho y$ *e* $y\rho z \Rightarrow x\rho z$

$$x = (a, b) \in A = \mathbb{N} \times \mathbb{N}$$

$$y = (c, d) \in A = \mathbb{N} \times \mathbb{N}$$
$$z = (e, f) \in A = \mathbb{N} \times \mathbb{N}$$

$$(a, b) \sim (c, d) \to a + d = b + c$$
$$(c, d) \sim (e, f) \to c + f = d + e$$
$$(a, b) \sim (e, f) \to a + f = b + e$$

$$a + d = b + c$$
$$a + d + f - f = b + c$$
$$a + f + d = b + c + f$$
$$a + f + \cancel{d} = b + \cancel{d} + e$$
$$a + f = b + e$$

- Tramite sostituzione effettiva di numeri e vedere se viene rispettata la relazione $2R1$

Oppure si parte dal primo pezzo finale

$$a + f = a + f + d - d =$$
$$= a + d + f - d = b + c + f - d =$$
$$= \cancel{d} + e + b - \cancel{d} = e + b$$

Accorgimenti proprietá antisimmetrica:

- Per quanto riguarda la Proprietà antisimmetrica se vale aRb e bRa, allora $a = b$ ma se troviamo un solo caso in cui $a \neq b$ allora non è antisimmetrica

Def: Si dice che ρ è una *relazione di equivalenza* se ρ è

- riflessiva
- transitiva
- simmetrica

Def: Si dice che ρ è una *relazione d'ordine* se ρ è

- riflessiva
- transitiva
- antisimmetrica

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

$$[a]_{\sim} = \{b \in A : b \sim a\}$$

Accorgimenti:

- La classe di equivalenza dato $\sim$, va scritta in base a all'elemento di rifermento (quello che sta dentro le quadre)

$$[x]_{\sim} = \{x, x+1\}$$

- Coincide esattamente con la classe di congruenza modulo n

$$[x]_{\equiv n} = \{x, x+n, x+2n\}$$

$$y = x + k \cdot n$$

- Se $a \sim [x]_{\sim}$ allora:

$$a \sim x \to x \sim a \to x \sim [a]_{\sim}$$

<u>Def:</u> Una funzione si dice **suriettiva** se ogni elemento del secondo insieme é raggiunto da almeno un elemento del primo

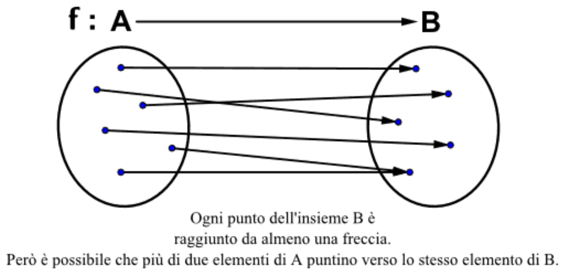


Figure 4: funzione suriettiva

<u>Def:</u> Una funzione si dice **iniettiva** se ogni elemento del dominio ha immagini distinte

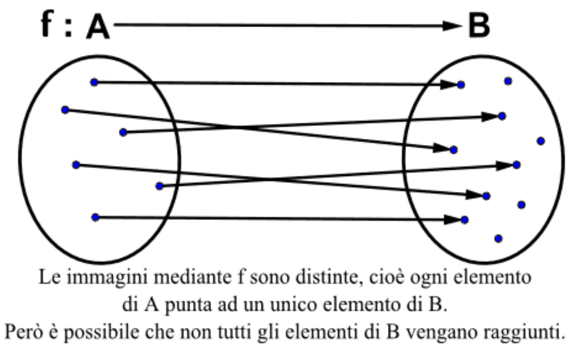
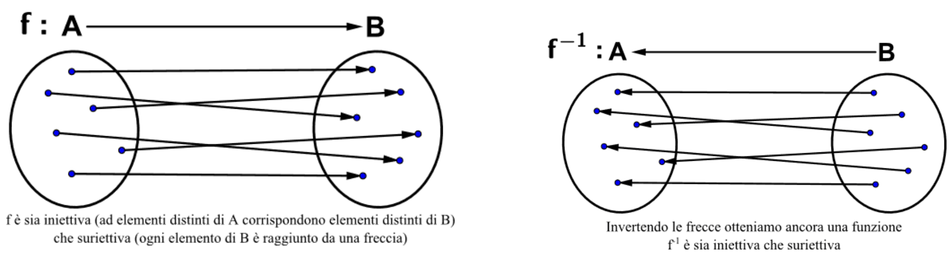


Figure 5: funzione iniettiva

<u>Def:</u> Una funzione si dice **biunivoca** se é una fuzione iniettiva e suriettiva. Inoltre una *una funzione biunivoca é invertibile e presenta una funzione inversa*



Dimostrare che una funzione sia ben definita

- Data un funzione f
- Cambiando il rappresentante della classe il risultato non deve cambiare
- Esempio

$$f : \mathbb{Z}_2 \to \mathbb{Z}_4$$
$$[a]_2 \to [a]_4$$

Se io prendo a = 0

$$[0]_2 = \{..., -4, -2, 0, 2, 4, ...\}$$

Applicando g risulta

$$[0]_4 = \{..., -8, -4, 0, 4, 8, ...\}$$

Se invece prendo a = 2

$$[2]_2 = [0]_2 = \{..., -4, -2, 0, 2, 4, ...\}$$

Applicando g risulta $[2]_4$ *che é diverso da* $[0]_4$

$$[2]_4 = \{..., -6, -2, 2, 6, 10, ...\}$$

- Se cambiando rappresentante cambia l'immagine della funzione (cambia codominio) allora la funzione non é ben definita
- Il dominio della funzione di partenza dev'essere interamente contenuto in quello di arrivo, indipendenetemente che ci siano anche altri elementi al suo interno

NB

- ρ indica una relazione che puó essere d'ordine o di equivalenza
- $\sim$ indica una relazione di equivalenza su un insieme

$$=, \quad \equiv_n$$

- Le relazione d'ordine sono

$$=, \quad \leq, \quad \subseteq, \quad |$$

5 Risoluzione lezione 5

- **Definizioni:**
  - **definizione:** Data una generica relazione di ordine su A insieme, diremo che due elementi $a, b \in A$ sono **confrontabili** se vale $a\rho b$ e $b\rho a$
  - **definizione:** Una relazione di ordine si dice **totale** se due elementi sono sempre *confrontabili*
  - **definizione:** Nel caso delle relazione di ordine si puó fare un grafo **semplificato** che prende il nome di **Diagramma di Hasse**
    a. Non si metto i *cappi*
    b. Non si mettono le *scorciatoie*
    c. Gli elementi piú grandi si mettono in alto
    d. La direzione é implicita, non si mettono frecce
  - **osservazione:** Dato un insieme A e una relazione d'ordine ρ su A, se $B \subseteq A$ allora ρ é una relazione d'ordine anche su B
  - **definizione**: Un elemento $m \in A$ si dice **minimo** se $\forall a \in A$ vale $m\rho a$.
    Un elemento $M \in A$ si dice **massimo** se $\forall a \in A$ vale $a\rho M$.
  - **definizione:** Il minimo quando esiste si denota con $MinA$ e il massimo con $MaxA$
  - **osservazione:** il minimo e il massimo se esistono sono unici.
  - **definizione:** Un elemento $m \in A$ si dice **elemento minimale** di A per ρ se e solo se

$$\forall a \in A \ \textit{se vale} \ a\rho m \rightarrow a = m$$

  - **definizione:** Un elemento $M \in A$ si dice **elemento massimale** di A per ρ se e solo se

$$\forall a \in A \ \textit{se vale} \ M\rho a \rightarrow a = M$$

  - **osservazione:** Se esiste $MinA$ questo é l'unico elemento minimale, e se esiste $MaxA$ questo é l'unico elemento massimale.
  - **definizione:** Sia $B \subseteq A$ un elemento $m \in A$ é detto **minorante di** B se

$$\forall b \in B \rightarrow m\rho b$$

- **definizione:** Sia $B \subseteq A$ un elemento $M \in A$ é detto **maggiore di** B se
$$\forall b \in B \rightarrow b\rho M$$
- **osservazione:** Indicheremo con
$$MinorB = \{ \text{ minoranti di } B\}$$
$$MaggiorB = \{ \text{ maggioranti di } B\}$$
- **definizione:** Sia $B \subseteq A$ **l'estremo inferiore** di B per la relazione di ordine ρ
$$inf(B) = Max(MinorB)$$
- **definizione:** Sia $B \subseteq A$ **l'estremo superiore** di B per la relazione di ordine ρ
$$sup(B) = Min(MaggiorB)$$
- **definizione:** Se esiste $MinB = infB$, e se esiste $MaxB = supB$
- **definizione:** Diremo che A con la relazione di ordine ρ forma un **reticolo** se $\forall a \in A$ esistono sempre $inf(a, b)$ e $sup(a, b)$
- **definizione:** Un reticolo A, ρ si dice **limitato** se esistono
  * minA = O
  * maxA = I
- **definizione:** Sia A, ρ un reticolo limitato e sia $a \in A$. $b \in A$ é detto **complemento di** a se
  * $inf(a, b) = MinA = O$
  * $sup(a, b) = MaxA = I$

- **Nozioni**
  - Quando devo trovare i minoranti e i maggioranti devo analizzare quello che ho e non trovarli di mia iniziativa se non viene dato un altro insieme che contiene quello di rifermento analizzo quindi quello che ho
  - In generale dentiamo con
$$inf(a, b) = inf\{a, b\}$$
$$sup(a, b) = sup\{a, b\}$$

potrebbero non esistere

- *Minor* $\{a,b\}$ = $\{\ c \in A : c\rho a$ ***e*** $c\rho b\ \}$
- Poiché in $\mathbb{N}$ con la relazione $\leq$ 2 elementi sono sempre confrontabili $\rightarrow$ **Ordine totale** $\leq$ esiste sempre *inf e sup*

$$Se\ a \leq b \Rightarrow inf(a,b) = a$$

$$Se\ a \geq b \Rightarrow inf(a,b) = b$$

$$sup(a,\ b) = max(a,\ b)$$

$$inf(a,\ b) = min(a\ ,\ b)$$

- Sia X un insieme e sia $A = \mathbb{P}(X)$ con $\rho = \subseteq$

$$E, F \in \mathbb{P}(X)$$

$$minor\{E,F\} = \{G \in A : G \subseteq E, G \subseteq F\} = E \cap F$$

$$x \in G \Rightarrow x \in E, x \in F \Rightarrow x \in E \cap F$$

$$maggior\{E,F\} = \{G \in A : E \subseteq G, F \subseteq G\} = E \cup F$$

$$inf\{E,F\} = E \cap F$$

$$sup\{E,F\} = E \cup F$$

$$\mathbb{P}(X)\ \textit{é un reticolo rispetto a} \subseteq$$

- Sia $A = \mathbb{N}$ o $D_n = \{k \in \mathbb{N} : k|n\}$ con $\rho = |$ e con $a, b \in A$

$$maggior\{a,b\} = \{\textit{multipli comuni di a e b}\}$$

$$minor\{a,b\} = \{\textit{divisori comuni}\}$$

$$sup\{a,b\} = m.c.m.(a,b)$$

$$inf\{a,b\} = MCD(a,b)$$

$$D_n\ \textit{é un reticolo rispetto a}\ |$$

- Sia $A = D_{36} - \{6\} = \{1, 2, 3, 4, 9, 12, 18, 36\}$ diagramma di Hasse con $\rho = |$

$$Maggior\{2,\ 3\} = \{12,\ 18,\ 36\}$$

In questo caso non esiste minimo dei maggioranti ossia il sup perché 12 e 18 non sono confrontabili $12 \not\rho 18$ *e viceversa*

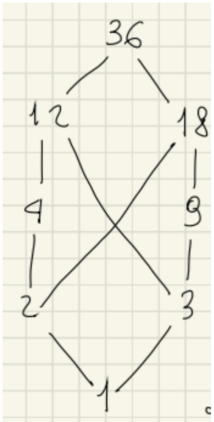


Figure 6: diagramma di Hasse

- Dato $k \in D_{30}$ trovare il suo **complemento** (dove $h \in D_{30}$)
  * inf(k, h) = minA
  * sup(k, h) = maxA
- La somma con classi uguali

$$[2]_5 + [3]_5 = [5]_5 = [0]_5$$

- $x \in [a]_n$

$$k \equiv a \ mod \ n$$

$$k = a + k \cdot n$$

6 Risoluzione lezione 7

- Se $\forall b \in [a]_n$, dividendo a e b per n ottengo lo stesso resto

$$b = a + k \cdot n$$
$$b = \frac{a + k \cdot n}{n} = \frac{a + \cancel{k \cdot n}}{\cancel{n}} \qquad r = a$$

- Insieme quoziente si indica con $\mathbb{Z}_n$

$$\mathbb{Z}_n = \{[0]_n, [1]_n, ..., [n-1]_n\}$$

- Per le classi di conguenza modulo n valgono
  - $[n]_n = [0]_n \to r = 0$ *la divisione non da resto* $\frac{(k+1)n}{n}$
  - $[k]_n + [l]_n = [k+l]_n$
  - $[k]_n \cdot [l]_n = [k \cdot l]_n$

- Trucco risuluzione

$$[3]_4 \cdot [x]_4 = [2]_4$$
$$[3]_4 = [-1]_4$$
$$-x = 2 + 4 \cdot k \qquad k \in \mathbb{Z}$$
$$x = -2 - 4 \cdot k \qquad k \in \mathbb{Z}$$
$$x = [-2]_4 = [2]_4$$

- $2x = 3 + 4k \to 2x - 4k = 3 \to$ non ha soluzioni perché $2x - 4k$ é pari ma 3 é dispari

- la parte che viene trasformata data la def di congruo mod n é la parte di destra senza incognita

- **Def:** Sia $I \subseteq \mathbb{Z}$. Diremo che I é un **ideale se**
  a. $I \neq \varnothing$
  b. Se $x, y \in I$ allora $x + y \in I$
  c. $\forall k \in \mathbb{Z}$ se $x \in I$ allora $k \cdot x \in I$
  d. NB: dato $k = 0$ per l'ultima condizione $0 \in I$

- **Def:** Con $a \in \mathbb{Z}$ si chiama ideale principale generato da a **l'insieme**

$$(a) = \{k \cdot a : k \in \mathbb{Z}\}$$

- **Def:** Sia $a \in \mathbb{Z}$ allora (a) é un ideale

- **Def:** Sia I un ideale e sia $a \in I$ per la c) se $k \in \mathbb{Z} \Rightarrow k \cdot a \in I$

$$(a) \subseteq I$$

- Dato un ideale I
  - se $I = \{0\} \rightarrow I = (0)$
  - se $I \neq \{0\} \rightarrow$ prendo a il piú piccolo elemento positivo di I
- Dati 2 ideali (a) e (b)
  - $(a) + (b)$ é un ideale
    - $(a) + (b) = \{k \cdot a + h \cdot b : k, h \in \mathbb{Z}\}$
    - $(a) + (b) = (a, b) = (M)$
    - $M = MCD(a, b)$
    - M divide sia a e b
    - M é il numero positivo piú piccolo ($\boldsymbol{M \geq 0}$)
  - $(a) \cap (b)$ é un ideale
    - $(a) \cap (b) = (m)$
    - $m \geq 0$
    - m sta per minimo comune multiplo

7 Risoluzione lezione 8

- Per trovare **MCD** tra due numeri utilizzare l'algoritmo di Euclide e ***L'MCD é l'ultimo resto non nullo***
- Per calcolare **mcm** tra due numeri utilizzare la seguente formula

$$mcm(a,b) = \frac{a \cdot b}{MCD(a,b)}$$

- **MCD(a,b) va fatto sui valori assoluti di a, b, infatti:**

$$MCD(|a|,|b|)$$

- **Teorema:** Dati $a, b \in \mathbb{Z}$, $MCD(a,b) = 1$ (quindi a,b coprimi) se e solo se $\exists n, m \in \mathbb{Z}$ tali che

$$a \cdot m + b \cdot n = 1$$

- $MCD(a,b)$ é il generatore positivo di $(a) + (b)$

$$MCD(a,b) = (a) + (b)$$

$$\exists m, n \in \mathbb{Z} : MCD(a,b) = ma + nb$$

- **Algoritmo di Euclide**
  - Determinare MCD(a, b)
  - eseguo la divisione
    - pongo $a = a_0$ e $b = b_0$
    - $a_0 : b_0$ avremo poi un r_0 e k_0
    - $a_0 = k_0 \cdot b_0 + r_0$
  - poi
    - pongo $a_1 = b_0$ e $b_1 = r_0$
    - $b_0 : r_0$ ossia $a_1 : b_1$
    - $a_1 = k_1 \cdot b_1 + r_1$
  - Continuo fino quando non ottengo $r = 0$
  - **L'MCD é l'ultimo resto non nullo**

- **Come determinare** m, n
  - Si rileggono i passaggi all'indietro dell'algoritmo di Euclide
  - Partendo dal fondo, ossia dal *ultimo resto non nullo*

$$resto_n = a_n - q_n \cdot b_n$$

$$ricordarsi\ che\ i\ b_n\ sono\ i\ resti$$

$$resto_n = a_n - q_n \cdot (a_{n-1} - q_{n-1} \cdot b_{n-1})$$

- **Risoluzione equazioni Diofantee**
  - Vogliamo risolvere equazioni del tipo, dati $a, b, c \in \mathbb{Z}$

$$a \cdot x + b \cdot y = c$$

  - Significa andare a trovare tutte le coppie $(x, y) \in \mathbb{Z}^2$ che risolvono l'equazione
  - L'equazione ammette soluzioni se e solo se *c é un multiplo di* $MCD(a, b)$
  - Se $MCD(a, b) = 1$ ammette soluzioni indipendenetemente dal valore di c
  - *Risoluzione*
    - Verificare che l'equazione sia resolvibile
      - c multiplo di $MCD(a, b)$
      - $MCD(a, b) = 1$
    - Trovare una soluzione
    - Calcolo $MCD(a, b)$
    - Divido l'equazione per $MCD(a, b)$
    - Eseguo l'algoritmo di Euclide
    - Calcolo x e y rileggono i passaggi all'indietro dell'algoritmo di Euclide
    - Moltiplico per x in modo tale che il c dell'equazione di partenza coincida con quella trovata
    - Trovo la soluzione

$$x_0 = x \quad trovata\ tramite\ Euclide$$

$$y_0 = y \quad trovata\ tramite\ Euclide$$

    - Trovare ora le altre soluzioni che sono della forma

$$x = x_0 + b \cdot k$$

$$y = y_0 - a \cdot k$$

- **Risoluzione equazione Dionfantee in $\mathbb{Z}_n$**
  - Sostituzione della x con $[a]_n$ con n dell'esercizio
  - Trascrizione dell'equazione in questa maniera $6 \cdot a - 27 \cdot k = 3$
  - Verifica se l'equazione é risolvibile
  - Divido l'equazione per il MCD
  - Effettuo la sostituzione $x = a$ e $y = k$
  - Eseguo l'algoritmo di Euclide
  - Calcolo x e y rileggono i passaggi all'indietro dell'algoritmo di Euclide
  - Moltiplico perxin modo tale che il c dell'equazione dipartenza coincida con quella trovata
  - Trovo la prima soluzione in x e y
  - Effettuo la sostuzione rendono $x = a$ e $y = k$ riportandola in a e k
  - Effettuo il controllo tramite sostituzione e verifica dell'identitá
  - Cerco le soluzione per a che rappresenta la nostra incognita e tiro fuori tutte le classi pertinenti
- **Attraverso il metodo di risoluzione delle equazioni Diofantee**
  - Utilizziamo tale metodo anche nella risoluzione in $\mathbb{Z}_n$
  - Prima dobbiamo risriverla nella forma $a \cdot x + b \cdot y = c$

$$[6]_{27} \cdot x + [7]_{27} = [0]_{27}$$

poniamo $x = [a]_{27}$ *otteniamo:*

$$[6 \cdot a + 7]_{27} = [0]_{27}$$

$$6 \cdot a + 7 = 0 + k \cdot 27$$

$$6 \cdot a - 27 \cdot k = -7$$

$MCD(6, 27) = 3$ *-7 non é un multiplo di MCD*

l'equazione non ha soluzioni 3 $\nmid$ -7

- **Altro esempio -** $\mathbb{Z}_n$

$$[6]_{27} \cdot x + [3]_{27} = [0]_{27}$$

$$\textit{poniamo } x = [a]_{27} \textit{ otteniamo:}$$

$$[6 \cdot a + 3]_{27} = [0]_{27}$$

$$6 \cdot a + 3 = 0 + k \cdot 27$$

$$6 \cdot a - 27 \cdot k = 3$$

$$MCD(6, 27) = 3 \quad 3| - 3 \text{ esistono soluzioni}$$

Divido per MCD, ottengo

$$2 \cdot a - 9 \cdot k = -1$$

sostituzione, pongo

$$x = a \qquad y = -k$$

$$2 \cdot x + 9 \cdot y = -1$$

Calcolo Euclide e ripercorrendo ottengo

$$4 \cdot 2 - 1 \cdot 9 = -1$$

$$x_0 = 4 \qquad y_0 = -1$$

Trovo le altre soluzioni

$$\begin{cases} x = 4 + 9 \cdot h \\ y = -1 - 2 \cdot h \end{cases} \tag{1}$$

sostituisco x = a e y = -k

$$\begin{cases} a = 4 + 9 \cdot h \\ y = 1 + 2 \cdot h \end{cases} \tag{2}$$

Effettuo il controllo

$$2 \cdot a - 9 \cdot k = 1$$

$$2(4 + 9 \cdot k) - 9(1 + 2 \cdot h) = -1$$

$$-1 = -1$$

Calcolo le soluzioni dell'equazione, e nel nostro caso l'incognita é a

$$[a]_{27} = [4 + 9 \cdot h]_{27}$$

$$h = 0 \qquad [a]_{27} = [4]_{27}$$

$$h = 1 \qquad [a]_{27} = [13]_{27}$$

$$h = 2 \qquad [a]_{27} = [22]_{27}$$

$$h = 3 \qquad [a]_{27} = [4]_{27}$$

Abbiamo solo 3 soluzioni

$$[4]_{27}, \quad [13]_{27}, \quad [22]_{27}$$

- **Altri metodi di risoluzione**
  - Quando n é un numero basso di $\mathbb{Z}_n$ tramite sostituzione andiamo a verificare l'identitá, nel caso l'identitá del dato $[a]_j$ risulta essere verificata quest'ultima rappresenta una soluzione

    $$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$$

  - nel caso di classi $\mathbb{Z}_n$ es come $n = 27$ dove $27 = 3^3$ posso trasformare l'equazione in classe 3 e utilizzare il metodo sopra
  - Dato una classe di congruenza $[a]_n$ che moltiplica x incognita si puó moltiplicare l'equazione per un $[b]_n$ in modo tale da ottenere $[x]_n$ con coefficiente 1

    dato un elemento $[a]_n$ devo trovare $[b]_n$:

    $$[a]_n \cdot [b]_n = [1]_n$$

    $$[a \cdot b]_n = [1]_n$$

    $$a \cdot b = 1 = k \cdot n$$

    $$a \cdot b - k \cdot n = 1$$

    *E questa equazione diofantea ha c = 1, quindi esiste una soluzione se e solo (a,n) sono **coprimi,** ossia se MCD(a, n) = 1 $\rightarrow$ MCD$|c$*

    $$[a]_n \cdot [b]_n = [1]_n$$

  - Esempio del punto prima

    $$[a]_n \cdot x + [b]_n = [0]_n \qquad [a]_n \cdot [c]_n = [1]_n$$

    $$[a]_n \cdot x \cdot [c]_n + [b]_n \cdot [c]_n = [0]_n \qquad \rightarrow x = -[b]_n \cdot [c]_n$$

8 Risoluzione lezione 9

- 0 é divisibile per qualunque numero $\frac{0}{n} = 0$
- Rappresentazione del numero 143

$$143 = 10^2 + 4 \cdot 10^1 + 3$$

- Divisibilitá per 9
  - n é divisibile per 9 se $[n]_9 = 0_9$
  - n é divisibile per 9 se la somma delle cifre del numero é divisibile per 9
  - Funziona anche per 3
  - Sapendo che $[10]_9 = [1]_9$

$$[143]_9 = [10^2]_9 + [4]_9 \cdot [10^1]_9 + [3]_9$$

$$[143]_9 = [1]_9 + [4]_9 \cdot [1]_9 + [3]_9$$

$$[143]_9 = [1 + 4 + 3]_9 = [8]_9$$

- Divisibilitá per 11
  - n é divisibile per 11 se $[n]_{11} = 0_{11}$
  - Sapendo che $[10]_{11} = [-1]_{11}$

$$[143]_{11} = [10^2]_{11} + [4]_{11} \cdot [10^1]_{11} + [3]_{11}$$

$$[143]_{11} = [1]_{11} + [4]_{11} \cdot [-1]_{11} + [3]_{11}$$

$$[143]_{11} = [1 - 4 + 3]_{11} = [0]_{11}$$

9 Risoluzione lezione 10

- **Definizione:** La *legge di composizione interna (lci)* su un insieme E é una **funzione** da $E \times E$ su E e la indicheremo con $*$

$$* : E \times E \to E$$

Significa che dati $a, b \in E$ anche $a * b \in E$

- Esempio

"-" non é una lci in $\mathbb{N}$ perché $n - m$ non é sempre definito
"/" non é lci, non posso dividere per 0

- **Diremo che *lci* é**
  - **associativa** se $\forall a, b, c \in E$ si ha che

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

  - **commutativa** se presi $a, b \in E$ vale

$$a * b = b * a$$

- Un elemento $e \in E$ é detto **elemento neutro** per $*$ se $\forall a \in E$ vale
  - Se $*$ non é commutativa é necessario verificarle entrambe, altrimenti ne basta una
  - e é unico

$$e * a = a * e = a$$

- Si dice che $a' \in E$ é un **inverso / simmetrico** di a se
  - inverso quando esiste si indica con a^{-1} ed é **unico** per ogni elemento a se **la legge é associativa**
  - Se *lci* é una somma l'inverso é $-a$

$$a * a' = a' * a = e$$

- *L'elemento neutro é **l'inverso** di se stesso*

$$e * e = e \to e^{-1} = e$$

- **Considerazioni:**
  - Su $\mathbb{N}$ l'unico elemento che ammette inverso é 1
  - In $\mathbb{Q}$ gli elementi inveribili $\frac{n}{m}$ sono quelli con $n, m \neq 0$
  - $I(X)$ é la funzione **identitá**, non fa nulla $f \circ I = I \circ f = f$
  - La funzione inversa é f^{-1}
- **Sia E un insieme e sia $*$ una *lci* su E:**
  - Se $*$ é <u>*associativa*</u> diremo che $(E, *)$ é un **semigruppo**
  - Se $*$ é <u>*associativa*</u>, *ammette* <u>*neutro*</u> *e* diremo che $(E, *)$ o $(E, *, e)$ é un **monoide**
  - Se $*$ é <u>*associativa*</u>, *ammette* <u>*neutro*</u> *e, ogni elemento é* <u>*invertibile*</u> diremo che $(E, *)$ o $(E, *, e, .^{-1})$ é un **gruppo**
- **Definizione:**
  - Se l'operazione $*$ é commutativa si dice che, *il semigruppo* o *il monoide* o *il gruppo* é **abeliano / commutativo**
- **Esercizi:**
  - Dimostrare sempre che $*$ é una *lci* su E

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	$\varnothing$	X	Non c'è
$\cap$	$\mathcal{P}(X)$	Sì	Sì	X	$\varnothing$	Non c'è
$\circ$	Funzioni $\mathbb{R} \to \mathbb{R}$	No	Sì	$id(x) = x$	Funzione nulla	Funzione inversa
$\wedge$	Reticolo non limitato(E, ρ)	Sì	Sì	Nessuno	Nessuno	—
$\vee$	Reticolo non limitato(E, ρ)	Sì	Sì	Nessuno	Nessuno	—
$\wedge$	Reticolo limitato (E, ρ)	Sì	Sì	O	I	Complemento
$\vee$	Reticolo limitato (E, ρ)	Sì	Sì	I	O	Complemento

Figure 7: riassunto

10 Risoluzione lezione 11

- **Monoide delle parole**
  - Gli elementi di A sono i simboli dell'alfabeto $A = a, b, c$
  - **Parola**, $w = a_1 a_2 ... a_n$
  - n indica la lunghezza della parola
  - La parola vuota o di lunghezza 0 si indica con ε
  - Insieme delle parole $W(A)$
  - *lci* $\circ$

$$w_1, w_2 \in w(A)$$

$$w_1 = a_1 a_2 ... a_n \qquad w_2 = b_1 b_2 ... b_n$$

$$w_1 \circ w_2 = a_1 a_2 ... a_n b_1 b_2 ... b_n$$

  - $W(A)$ non é un gruppo
  - Costruire un **gruppo** partendo da $W(A)$. **Gruppo libero**

$$\textit{Dato } A = \{a_1, a_2, ...\}$$
$$\textit{consideriamo l'insieme } A^{-1} = \{a_1^{-1}, a_2^{-1}, ...\}$$
$$W(A \cup A^{-1}) \rightarrow \textit{gruppo libero}$$

  - La **riduzione**

$$w_1 a a^{-1} w_2 \rightarrow \cancel{aa^{-1}} = w_1 w_2$$

  - La parola ridotta si indica con r_w
  - L'insieme delle parole ridotte $F(A)$

- **Definizione**
  - Sia $(G, *, e, .^{-1})$ un gruppo ed e elemento neutro. Un **sottogruppo** di G é un **sottoinsieme** $H \subseteq G$ tale che
    - $H \neq \varnothing$
    - $e \in H$
    - se $h, k \in H \Rightarrow h * k \in H$
    - $h \in H \Rightarrow h^{-1} \in H$
  - Un sottoinsieme $H \subseteq G$ é un sottogruppo se e solo se
    - $H \neq \varnothing$
    - $\forall h, k \in H \Rightarrow h * k^{-1} \in H$

– Sia $(G, *)$ un gruppo e sia $g \in G$. $< g >$ é un sottogruppo, che prende il nome di **sottogruppo ciclico**

$$(G, \times) \qquad < g > = \{g^n : n \in \mathbb{Z}\}$$
$$(G, +) \qquad < g > = \{g \cdot n : n \in \mathbb{Z}\}$$

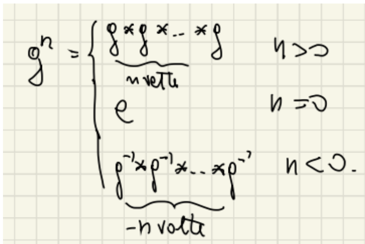


Figure 8: esempio

– Fissato un sottogruppo H. Definiamo su G due relazioni di equivalenza λ, ρ (λ_H, ρ_H) nel modo seguente:

$$\textit{Presi } x, y \in G$$
$$x\lambda y \textit{ sse } \exists h \in H : y = h * x$$
$$x\rho y \textit{ sse } \exists k \in H : y = x * k$$
$$\textit{se il gruppo é abeliano } \lambda \textit{ e } \rho \textit{ coincidono}$$

– Le classi di equivalenza

$$[x]_\lambda = \{y \in G : x\lambda y\}$$
$$= \{y \in G : \exists h : y = h * x\}$$
$$= \{h * x : h \in H\} = H * x$$

$$[x]_\rho = \{x * h : h \in H\} = x * H$$

$$[e]_{\rho,\lambda} = \{h * e : h \in H\} = \{h : h \in H\} = H$$

– Dato un gruppo G e un sottogruppo H considerano le classi di equivalenze rispetto alle relazioni λ, ρ.

$$G/_\lambda \textit{ si indica con } H \setminus G$$
$$G/_\rho \textit{ si indica con } G/H$$

- Esempio

$$(\mathbb{Z}, +) \qquad H = <n> = \{k \cdot n : k \in \mathbb{Z}\} = n\mathbb{Z}$$
$$x, y \in \mathbb{Z}$$
$$x\lambda y \ sse \ \exists h \in H : y = h + x$$
$$essendo \ che \ h \in H \ allora$$
$$x\lambda y \ sse \ \exists k \in \mathbb{Z} : y = x + k \cdot n$$
$$[x]_\lambda \ sono \ le \ classi \ di \ resti \ modulo \ n$$

- Sia H un sottogruppo di G diremo che H é un sottogruppo **normale** se

$$\forall y \in G \ e \ \forall h \in H \ si \ ha$$
$$y^{-1} * h * y \in H$$

- Sia $H \subseteq G$ sottogruppo normale allora G/H é un gruppo con *lci*

$$[x]_\rho * [y]_\rho = [x * y]_\rho$$

- Esempio

$$(\mathbb{Z}, +) \qquad H = <n> = n\mathbb{Z}$$
$$gruppo \ é \ \mathbb{Z}$$
$$sottogruppo \ é \ n\mathbb{Z}$$
$$\mathbb{Z}/n\mathbb{Z} \ classi \ di \ resto \ mod \ n \ \mathbb{Z}_n$$

- **Nozioni**
  - Se il sottogruppo H é normale allora λ e ρ coincidono

$$[x]_\lambda = [x]_\rho$$
$$questo \ mi \ permette \ di \ definire$$
$$[x]_\rho * [y]_\rho = [x * y]_\rho$$

  - Se G é commutativo ogni sottogruppo é normale

$$y^{-1} * h * y \in H = h * y * y^{-1} = h * e = h \in H$$

  - Le classi $[n]_n$ sono un gruppo commutativo di n elementi

$$[0]_n, ..., [n-1]_n$$

  - L'inverso del gruppo G viene convertito nel sottogruppo H, mentre l'elemento neutro appartiene anche a H

11 Risoluzione lezione 12

- $[x]_n$ é invertibile se e solo se

$$MCD(x,n) = 1$$

Per cui esiste una classe $[y]_n$ tale che

$$[x]_n \cdot [y]_n = [1]_n$$

$[y]_n$ é la classe inversa di $[x]_n$ e l'elemento netro é $[1]_n$ per $(\mathbb{Z}_n, \cdot)$

- Ogni classe $[x]_n$ possiede un inverso unico e diverso da ogni altra classe
- Gli elementi invertibili $[x]_n$ sono gli unici inversi
- Esercizi di verifica che dato un insieme E e una $*$ verificare che sia un **gruppo o ....**

  1. Verificare che $*$ sia una ***lci***

     $$x, y \in E \Rightarrow x * y \in E$$

  2. Verificare che $*$ sia **associativa**

     $$x, y, z \in E \Rightarrow (x * y) * z = x * (y * z)$$

  3. verificare che esista elemento **neutro** e (NB: é unico)

     $$\forall x \in E \Rightarrow x * e = x \wedge e * x = x$$

     se é $*$ é commutativa ne basta verificare una

     *Ricordarsi che l'incognita non é **x** bensí **e***
     *effettuare verifica sostiuendo alla **e** il dato trovare e vedere se*
     $x * e = x$

  4. Verificare che esista l'**inverso**

     $$\forall x \in E \Rightarrow \exists y \in E : x * y = y * x = e$$

     *Ricordarsi che l'incognita non é **x** bensí **y***
     *effettuare verifica sostiuendo alla **y***

  5. Verificare che il gruppo,... sia **abeliano**

     $$x * y = y * x$$

  - **NB:** Quando ci viene dato $(-1, 1)$ non é una coppia bensí un intervallo infatti $(-1, 1) = E$

- $\mathbb{R}^{\times} = \{x \in \mathbb{R} : x \neq 0\} \qquad \mathbb{R}^{\times}_{+} = \{x \in \mathbb{R} : x > 0\}$
- Dato un esercizio dove $G = \mathbb{R}^{\times} \times \mathbb{R}$

determinare il neutro

$$a = (x, y) \in G \exists e = (e, f) \in G : a * e = a$$
$$(xx', x'y + y') = (x, y)$$
$$xx' = x \Rightarrow x' = 1$$
$$x'y + y' = y \text{ dove } x' = 1 \Rightarrow y' = 0$$

Verificare sempre che *e* ***trovato*** $\in G$

- Dato un gruppo G il suo centro

$$Z(G) = \{z \in G : \forall g \in G : z * g = g * z\}$$

Z é un sottogruppo.
Il gruppo é ***abeliano*** *sse Z(G) = G.*
Cerchiamo gli elementi $(a, b) : \forall (x, y) \in G$

$$(a, b) * (x, y) = (x, y) * (a, b)$$

Le mie incognite sono (a,b), e devo dare valori di (x,y) per trovarli, infatti $\forall (x, y) \in G$

- **Definizioni**
  - Se $< g >$ ha un numero finito di elementi diremo che $< g >$ é di **ordine finito** e indicheremo con $o(g)$ il numero di elementi di $< g >$.
  - **Gruppo finito** é un gruppo con un numero finito di elementi.
  - Il numero di elementi si chiama **ordine del gruppo** e si indica con $o(G)$
  - Sia G un gruppo finito e sia H un sottogruppo di G allora

$$o(H) | o(G)$$

  - Se $o(G)$ é primo allora

$$H = \{e\}$$

oppure

$$H = G$$

12 Risoluzione lezione 13

- **Definizioni**
  - Sia $(G, *, e, .^{-1})$ un gruppo. Sia $g \in G$ un elemento di ordine finito $n = o(g)$, allora
$$g^n = e$$
$$< g > = \{e, g, g^2, ..., g^{n-1}\}$$
$$\textit{Avendo n elementi vuol dire che si ripetono dopo una determinata potenza}$$
  - Sia $n = o(g)$, allora
$$g^k = e \quad sse \quad n|k$$
  - Due gruppi $(G_1, *_1)$ e $(G_2, *_2)$ si dicono **isomorfi** se esiste una funzione invertibile
$$f : G_1 \to G_2$$
$$tale\ che\ \forall g_1, g_2 \in G_1\ si\ ha$$
$$f(g_1 *_1 g_2) = f(g_1) *_2 f(g_2)$$

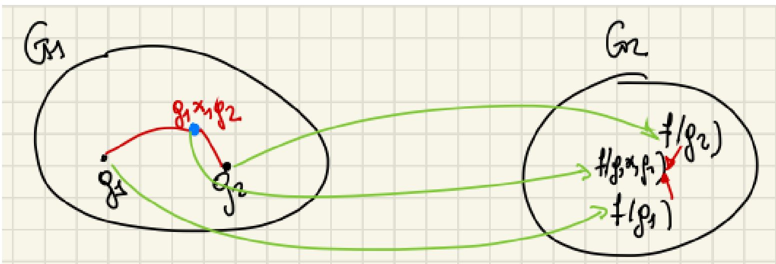


Figure 9: schema

- **Esercizio isomorfismo**
  - Mostrare che i gruppi $(\mathbb{R}, +)$ e $(\mathbb{R}^{\times}_{+}, \times)$ sono isomorfi
$$f : \mathbb{R} \to \mathbb{R}^{\times}_{+} = (0, +\infty)$$
$$f(x + y) = f(x) \times f(y)$$
$$Poniamo f(x) = e^x$$
$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$
$$Poniamo f^{-1}(x) = log(x)$$
$$log(x \cdot y) = log(x) + log(y)$$

– Mostrare che $(\mathbb{R}^\times, \times)$ e $(\mathbb{C}^\times, \times)$ non sono isomorfi

Supponiamo per assurdo che esista un isomorfismo

$$f : \mathbb{C}^\times \to \mathbb{R}^\times$$

$$-1 \in \mathbb{R}^\times \qquad \exists z \in \mathbb{C}^\times : f(z) = -1$$

$$\exists w \in \mathbb{C}^\times : w^2 = z$$

$$-1 = f(z) = f(w \cdot w) = f(w) \cdot f(w)$$

$$[f(w)]^2 = -1 \text{ \textit{impossibile in} } \mathbb{R}^\times \Rightarrow \text{ \textit{Assurdo}}$$

13 Lezione 14

- **Nozioni**
  - Se la legge é associativa l'inverso é unico
  - Sia A un insieme di n elementi. Una **permutazione** é una funzione iniettiva tale che $f : A \to A$.

$$A = \{a_1, a_2, a_3, ..., a_n\}$$

$$f : A \to A$$

ad ogni elemento del dominio corrisponde un'immagine che appartiene al dominio

  - Se $f : A \to A$ é **iniettiva** $\Rightarrow$ é automativamente **suriettiva**
    - **iniettiva:** ogni elemento del dominio ha immagini distinte
    - **suriettiva:** ogni elemento del codominio é ragginto almeno da un elemento del dominio
    - Dominio e codomio in questo cosa coincidono
  - Con $S_n = \{f : \ f \text{ permutazioni di } A\}$ consideriamo **l'insieme delle funzioni** che realizzano tutte le possibili permutazioni su A
    - n rappresenta il numero di elementi di A coinvoilti
  - Con la legge di composizione interna data dalla composizione delle funzioni

$$f, g \in S_n$$

$$f : A \to A$$

$$g : A \to A$$

$$f * g = f \circ g : A \to A$$

  - complessivamente possiamo fare $n!$ funzioni diverse

$$S_{10} = 10! = 3628800 \ \textit{funzioni}$$

  - S_n é un gruppo finito di n elementi
  - La composizione di funzioni é sempre associativa

$$f, k, l \in S_n$$

$$(h \circ k) \circ l = h \circ (k \circ l)$$

– Esempio:

$$n = 3 \quad S_3 \; con \; A = \{1, 2, 3\}$$
$$S_3 \; ha \; 6 \; elementi$$

$$f_5 \; effettua \; la \; seguente \; permutazione$$
$$1 \to 3$$
$$2 \to 2$$
$$3 \to 1$$

$$f_6 \; effettua \; la \; seguente \; permutazione$$
$$1 \to 3$$
$$2 \to 1$$
$$3 \to 2$$

$$f_3 \; effettua \; la \; seguente \; permutazione$$
$$1 \to 2$$
$$2 \to 1$$
$$3 \to 3$$

$$f_5 * f_6 = f_3$$
$$1 \to 3 \to 2$$
$$2 \to 2 \to 1$$
$$3 \to 1 \to 3$$

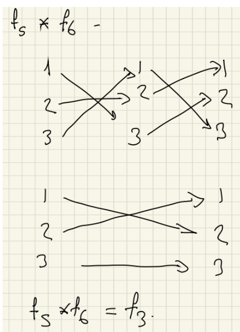


Figure 10: schema

14 Lezione 15

- **Definizioni:**
  - **definizione:** Un **anello** é una struttura algebrica $(A, +, \cdot)$ in cui A é un insieme e $+, \cdot$ sono *lci* tali che
    a. A é un gruppo abeliano rispetto a $+$, l'elemento neutro di questo gruppo lo indicheremo con O_A
    b. A é un monoide rispetto a $\cdot$, l'elemento neutro del monoide lo indicheremo con 1_A
    c. Per ogni $a, b, c \in A$ vale la **proprietá distributiva**

$$(a+b) \cdot c = (a \cdot c) + (b \cdot c)$$

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$

  - **osservazione:** il prodotto ha precedenza sulla somma (per utilizzare la proprietá distributiva)
  - Indicheremo con
    * $+$ la somma dell'anello
    * $\cdot$ il prodotto dell'anello
    * O_A lo zero dell'anello
    * 1_A l'unitá dell'anello
  - **definizione:** quando il prodotto é commutativo diremo che l'anello é **commutativo**
  - **osservazione:** Non é detto che nell'anello gli elementi siano invertibili
  - **osservazione:** L'opposto invece esiste sempre e lo indicheremo con $-a$

$$a + (-a) = O_A$$

$$(-a) + a = O_A$$

  - **definizione:** Dato un anello commutativo $(F, +, \cdot)$ se tutti gli elementi $f \in F$, $f \neq O_A$ sono invertibili diremo che F é un **campo**
  - **osservazione:** Gli unici elementi invertibili di $\mathbb{Z}$ sono 1 e -1. $\mathbb{Z}$ **non é un campo.**
    In $\mathbb{Q}$ ogni elemento non nullo é invertibile $\Rightarrow$ $\mathbb{Q}$ é un **campo**

- **proposizione:** Sia $(A, +, \cdot)$ un anello. Allora
  - $\forall a \in A \qquad a \cdot O_A = O_A \cdot a = O_A$
  - A ha almeno 2 elementi se e solo se $O_A \neq 1_A$
- **osservazione:** $A = \{O_A\}$ é un anello banale
- **osservazione:** In un anello A gli elementi che hanno prodotto O_A si dicono **divisori dello zero**.

$$es \ \ in \ \ \mathbb{Z}_6$$

$$[2]_6 \cdot [3]_6 = [0]_6$$

- **osservazione:** Un anello pivo di divisori dello zero é detto **integro**
- **Polinomi su un anello A commutativo:** Si considera l'insieme $A[x]$ delle successioni di elementi di A che sono uguali a O_A da un certo punto in poi.

$$A[x] = \{(a_n)_{n \in \mathbb{N}} : \exists n_0 : \forall n > n_0, a_n = O_A\}$$

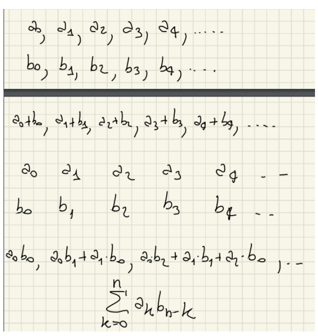
$$A[x] = a_0, a_1, a_2, .., a_{n_0}, O_A, O_A, ..$$

n_0 si chiama grado del polinomio.

- Su $A[x]$ definiamo 2 *lci* presi $(a_n), (b_n) \in A[x]$, definiamo

$$(a_n) + (b_n) = (a_n + b_n)$$

$$(a_n) \cdot (b_n) = (c_n) \ \ dove \ c_n = \sum_{k=0}^{n} a_k \cdot b_{n-k}$$



- $(A[x], +)$ é un gruppo con elemento neutro $(O_A, O_A, ...)$.
- $(A[x], \cdot)$ é un monoide con elemento neutro $1_{A[x]} = (1_A, O_A, O_A, ...)$.
- si verifica inoltre la Proprietà distributiva $\Rightarrow A[x]$ é un anello commutativo.

$$
\begin{aligned}
(a_n) &= (a_0, a_1, a_2, a_3, \dots) \\
&= (a_0, O_A, O_A, \dots) + (O_A, a_1, O_A, O_A, \dots) \\
&\quad + (O_A, O_A, a_2, O_A, O_A, \dots) + \dots \\
&= a_0 + a_1 \cdot (O_A, 1_A, O_A, O_A, \dots) + a_2 \cdot (O_A, O_A, 1_A, O_A, \dots) \\
&= a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \dots
\end{aligned}
$$

- Dove $x = (O_A, 1_A, O_A, ..)$ e $a_1 \cdot x = (O_A, a_1, O_A, ..)$
- Dato un polinomio $P \in A[x]$ della forma

$$a_0 + a_1 \cdot x + a_2 \cdot x^2 + .. + a_{n_0} \cdot x^n$$

  e preso un $b \in A$, calcolare $P(b)$

$$a_0 + a_1 \cdot b + a_2 \cdot b^2 + .. + a_{n_0} \cdot b^n$$

- Trovare una radice di P volu dire quindi trovare $b \in A$ tale che

$$a_0 + a_1 \cdot b + a_2 \cdot b^2 + .. + a_{n_0} \cdot b^n = O_A$$

15 lezione 16

- **Definizioni**
  - **Teorema di Fermat:** Sia p primo e $a \in \mathbb{Z}$ allora p divide $a^p - a$
  - **Funzione di Eulero:** Fissiamo $n \geq 1$, sia

$$\varphi(n) = card\{\mathbb{Z}_n^x\} = card\{1 \leq j \leq n : MCD(j, n) = 1\}$$

Esempio: n = 12

$$\mathbb{Z}_1 2^x = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$$

$$\varphi(12) = 4$$

Vado a prendere tutte le classi in $\mathbb{Z}_{12}^x$ che hanno MCD = 1

  - Se p é primo $\varphi(p) = p - 1$
  - **Formule di eulero**, per calcolare $\varphi(n)$

$$\varphi(n) = n \cdot \prod_{p|d} (1 - \frac{1}{p})$$

dove il prodotto é fatto su tutti i primi che dividono n

$$\varphi(12) = 12 \cdot (1 - \frac{1}{2} - \frac{1}{3}) = 4$$

Siano p,q primi e n = p · q allora la formala semplificata é

$$\varphi(n) = p \cdot q \cdot (1 - \frac{1}{p}) \cdot (1 - \frac{1}{q}) = (p - 1) \cdot (q - 1)$$

  - **Teorema di Eulero:** Sia $n \geq 1$ e $a \in \mathbb{Z}$ tale che $MCD(a, n) = 1$ allora

$$[a^{\varphi(n)}]_n = [1]_n$$

- **Scambio di chiavi Diffie - Hellman 1976**
  - Alice e Bob scelgono un numero **primo** p molto grande $\approx 10^{100}$
  - $\mathbb{Z}_{p^x}$ ha $p-1$ elementi ed é ciclico

$$\mathbb{Z}_p^x = \{[g]_p^k : k = 1, ..., p-1\}$$

  - Alice e Bob si accordano su un **generatore** g, solitamente molto piccolo
  - Alice sceglie un numero a compreso $1 \leq a \leq p-1$
  - Bob sceglie un numero b compreso $1 \leq b \leq p-1$
  - Alice calcola e lo comunica a Bob

$$[g^a]_p = [a']_p \qquad 0 \leq a' \leq p-1$$

  - Bob calcola e lo comunica ad Alice

$$[g^b]_p = [b']_p \qquad 0 \leq b' \leq p-1$$

  - Alice calcola un numero x, dove $0 \leq x \leq p-1$

$$[b'^a]_p = [g^{ab}]_p$$

  - Bob calcola un numero y, dove $0 \leq y \leq p-1$

$$[a'^b]_p = [g^{ab}]_p$$

  - Quindi $x = y$

- **Codice RSA**
  - Alice sceglie 2 numeri **primi** p, q
  - Alice calcola $n = p \cdot q$
  - Alice sceglie un numero e chiamato **esponente pubblico** tale che
    $$MCD(e, \varphi(n)) = 1$$
  - Alice sceglie un numero d chiamato **esponenete segreto** tale che
    $$[e]_{\varphi(n)} \cdot [d]_{\varphi(n)} = [1]_{\varphi(n)}$$
  - Bob vuole mandare un messaggio ad Alice, possiamo pensare che il messaggio di Bob sia un numero a tale che $0 \leq a < n$
  - Bob calcola e spedisce il messaggio ad Alice
    $$[a^e]_n = [a']_n$$
  - Alice calcola
    $$\textit{Sapendo che}$$
    $$ed = 1 + k \cdot \varphi(n)$$
    $$[a']_n^d = [a^{ed}]_n = [a^{1+k\cdot\varphi(n)}]_n = [a]_n \cdot [a^{\varphi(n)}]_n$$
    $$\textit{Se MCD(a,n) = 1, per il teorema di Eulero}$$
    $$[a^{\varphi(n)}]_n = [1]_n$$
  - Alice ha quindi decodificato il messaggio
    $$[a]_n \cdot [a^{\varphi(n)}]_n = [a]_n \cdot [1]_n = [a]_n$$
  - NB
    * Se $MCD(a, n) > 1$ succede se e solo se
      $$a = p \ \ o \ a = q$$
      $$\textit{questo perché}$$
      $$n = p \cdot q$$
    * La probabilitá che il messaggio sia p o q
      $$\frac{1}{p} + \frac{1}{q}$$

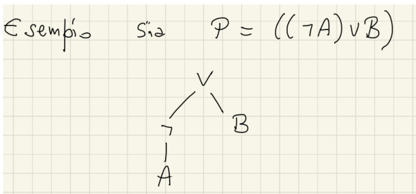
16 Lezione 17

- **Definizioni**
  - **Una proposizione** é una frase che poú essere solo vera o falsa
  - **Definizione:** Un **alfabeto** per un linguaggio della logica proposizionale é costituito da
    * **Simboli atomici:** $A, B, C, ..., A_1, B_2, A_7$
    * **Connettivi:**
      - $\perp$ *contraddizione* *falso*
      - $\neg$ *negazione* *non*
      - $\vee$ *disgiunzione* *o*
      - $\wedge$ *congiunzione* *and*
      - $\rightarrow$ *implicazione* *implica*
    * **Connettivi ausiliari:**
      - $()$ *parentesi per le precedenze*
  - Indicheremo con F l'insieme delle parole che sono fbf (*formula ben formata*)
  - **Definzione:** F é il piú piccolo insieme di parole che ha le seguenti proprietá
    1. I simboli atomici sono in F
    2. $\perp \in F$
    3. Se $P \in F \Rightarrow (\neg P) \in F$
    4. Se $P_1, P_2 \in F \Rightarrow (P_1 \vee P_2), (P_1 \wedge P_2), (P_1 \rightarrow P_2)$
  - F é il **piú piccolo insieme** con le proprietá (1,2,3,4), significa che se ci fosse un altro insieme X per cui valgano (1,2,3,4)

$$F \subseteq X$$

  - la parola vuota ε e $\rightarrow$ non sono fbf
  - **Precedenza degli operatori**
    * Quando le parentesi sono suerflue le togliamo, ossia seguono le prioritá
    1. $\neg$
    2. $\wedge$
    3. $\vee$
    4. $\rightarrow$

- **Definizione:** Sia P una *fbf*. L'insieme delle **sottoformule** di P, $S(P)$ é cosí definito
  * Se P é una fbf atomica allora $S(P) = \{P\}$
  * Se $P = \perp$ allora $S(P) = \{\perp\}$
  * Se $P = (\neg P_1)$ allora $S(P) = \{P\} \cup S(P_1)$
  * Se $P = (P_1 \vee P_2)$ oppure $P = (P_1 \wedge P_2)$ oppure $P = (P_1 \rightarrow P_2)$ allora $S(P) = \{P\} \cup S(P_1) \cup S(P_2)$
- **Albero sintattico** rappresentazione grafica di una *fbf*. Si puó partire da quella piú esterna oppure da quella piú interna.



- **Definzione: Un'interpretazione o valutazione** di un linguaggio della logica proposizionale é una applicazione $V : fbf \rightarrow \{0, 1\}$ che soddisfi
  * $v(\perp) = 0$
  * $v(\neg P) = 1 - v(P) \qquad \forall P \in F$
  * $v(P_1 \vee P_2) = max(v(P_1), v(P_2))$
  * $v(P_1 \wedge P_2) = min(v(P_1), v(P_2))$
  * $v(P_1 \rightarrow P_2) = 0$ se e solo se $v(P_1) = 1$ e $v(P_2) = 0$
- **Definzione:** Sia P una fbf e sia v una interpretazione. Si dice che P é **soddisfatta** nell'interpretazione v oppure che v é un modello per P se $v(P) = 1$. Scriveremo

$$v \models P$$

- Una *fbf*
  * é **soddisfacibile** se ha almeno un modello
  * é **insoddisfacibile** o **contradditoria** se non ha alcun modello
  * é **una tautologia** se é soddisfatta in ogni modello, $\models P$
- **Definzione:** Sia $\Gamma \subseteq F$. Si dice che una interpretazione v é un **modello** per Γ se $\forall P \in \Gamma$, $v(P) = 1$.

$$v \models \Gamma$$

- Se Γ ammette un modello é **soddisfacibile** altrimenti **insoddisfacibile**.
- Data una $P \in F$ e $\Gamma \subseteq F$ se per ogni modello v di Γ si ha $v(P) = 1$ diremo che P é una **conseguenza semantica** di Γ

$$\Gamma \models P$$

- **Nozioni**
  - Per **modello di** v si intende la combinazione di valori di 0,1 che attribuiamo alle P
  - $\Gamma \models P$ si legge da destra a sinistra quindi

    P é conseguenza semantica di Γ

  - v é un modello di Γ se $\forall P \in \Gamma \Rightarrow v(P) = 1$

    si legge da destra a sinistra

$$v \models \Gamma$$

- **Esempio**

$$\Gamma = \{\neg A \vee B, \neg A \vee \neg B\} \qquad P = A \to B$$

Verifichiamo che $\Gamma \models P$

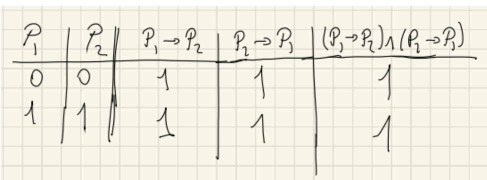
A	B	$\neg A$	$\neg B$	$\neg A \vee B$	$\neg A \vee \neg B$	$A \to B$	$A \vee B$
0	0	1	1	1	1	1	0
0	1	1	0	1	1	1	
1	0	0	1	0			
1	1	0	0	1	0		

1) Dato il modello $A = 0$ e $B = 0$, $v \models \Gamma$ perché $\forall P \in \Gamma \to v(P) = 1$
2) Per ogni modello di v di Γ la $v(P) = 1$, ossia quando é vera Γ é vera anche P

Ne segue che P é conseguenza semantica di Γ.
$A \vee B$ non é conseguenza semantica di Γ, perché quando $\forall P \in \Gamma \to v(P) = 1$ la $v(A \vee B) = 0$

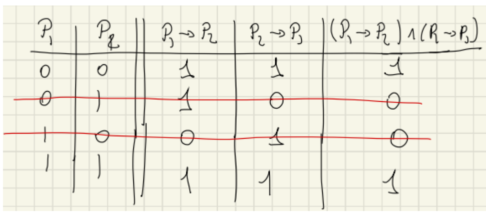
17 Lezione 18

- **Definizioni**
  - **Notazione:** Se $\Gamma = \{P_1, P_2, ..., P_n\}$ invece di scrivere $\Gamma \models K$ si scrive anche
  $$P_1, P_2, ..., P_n \models K$$
  - **Proposizione:** Sia $\Gamma \subseteq F$ e $P \in F$. Allora $\Gamma \models P$ se e solo se
  $$\Gamma \cup \{\neg P\} \textit{ é insoddisfacibile}$$
  - **Proposizione:** Siano $P_1, P_2 \in F$. Allora $P_1 \models P_2$ se e solo se
  $$\models P_1 \to P_2$$
  - **Teorema:** Sia $n \geq 1$ e siano $P_1, P_2, .., P_n \in F$ e $K \in F$ allora
  $$P_1, P_2, ..., P_n \models K \quad sse \quad P_1, ..., P_{n-1} \models P_n \to K$$
  $$\models P_1 \to (P_2 \to ..(P_n \to K))$$
  - **Definizione:** Siano $P_1, P_2 \in F$ diremo che P_1, P_2 sono **semanticamente equivalenti** e scriveremo $P_1 \equiv P_2$ se per ogni valutazione v si ha $v(P_1) = v(P_2)$
  - **Osservazione:** $P_1 \equiv P_2$ é equivalente a
    1. $P_1 \models P_2$ e $P_2 \models P_1$
    2. $\models (P_1 \to P_2) \wedge (P_2 \to P_1)$



P_1	P_2	$P_1 \to P_2$	$P_2 \to P_1$	$(P_1 \to P_2) \wedge (P_2 \to P_1)$
0	0	1	1	1
1	1	1	1	1

(a) Supponiamo di sapere che $P_1 \equiv P_2$



P_1	P_2	$P_1 \to P_2$	$P_2 \to P_1$	$(P_1 \to P_2) \wedge (P_2 \to P_1)$
0	0	1	1	1
~~0~~	~~1~~	~~1~~	~~0~~	~~0~~
~~1~~	~~0~~	~~0~~	~~1~~	~~0~~
1	1	1	1	1

(b) Supponiamo di sapere che $\models (P_1 \to P_2) \wedge (P_2 \to P_1)$ e restano le righe in cui $v(P_1) = v(P_2)$

- **Equivalenze semantiche fondamentali**
  - T é una abbreviazione per $\neg\perp$ e significa sempre vero

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

- **Definizione:** Siano $P, R \in F$ e sia A un simbolo atomico. La fbf, $P[R/A]$ é ottenuta **sostituendo** a tutte le occurrenze di A in P con R.
  a. Se P é la *fbf* atomica A allora $P[R/A] = R$
  b. Se P é la *fbf* atomica $\neq A$ allora $P[R/A] = P$
  c. Se $P = \perp$ allora $P[R/A] = \perp$
  d. Se $P = \neg P_1$ allora $P[R/A] = \neg P_1[R/A]$
  e. Se $P = P_1 \vee P_2$ allora $P[R/A] = P_1[R/A] \vee P_2[R/A]$
     $P = P1 \wedge P_2$ allora $P[R/A] = P_1[R/A] \wedge P_2[R/A]$
     $P = P_1 \rightarrow P_2$ allora $P[R/A] = P_1[R/A] \rightarrow P_2[R/A]$
- **Teorema:** Se due *fbf* P_1, P_2 sono semanticamente equivalenti ($P_1 \equiv P_2$), allora per ogni simbolo atomico A e per ogni *fbbf* R

$$R_1[P_1/A] \equiv R_2[P_2/A]$$

$$P_1[R_1/A] \equiv P_2[R_2/A]$$

- **Defizione:** Sia $P \in F$ i cui connettori sono solo $\neg, \vee, \wedge$. Il **duale** di P é la *fbf* P^V definita da
  a. se P é atomica allora $P^V = P$
  b. Se $P = \neg P_1$ allora $P^V = \neg(P_1^V)$
  c. Se $P = P_1 \vee P_2$ allora $P^V = P_1^V \wedge P_2^V$
     $P = P_1 \wedge P_2$ allora $P^V = P_1^V \vee P_2^V$

- **Definizione:** Un **letterale** é un *fbf* atomica o la negazione di una *fbf* atomica

$$A, B, C, ..., \neg A, \neg B, \neg C \qquad \textit{é un letterale}$$

$$A \to B \qquad \textit{non é un letterale}$$

- Una *fbf* é detta ***forma normale congiuntiva (fnc)*** se

$$P = P_1 \wedge P_2 \wedge ... \wedge P_n \quad con \quad n \geq 0$$

$$e\ ogni\ P_i = Q_{i,1} \vee Q_{i,2} \vee ... \vee Q_{i,k_i} \quad con \quad k_i \geq 0$$
$$dove\ ogni\ Q_{i,j}\ \textit{é un letterale}$$

Esempio

$$A \wedge \neg B \wedge (A \vee C) \quad \textit{é in fnc}$$

$$(A \vee D) \wedge (A \vee \neg C) \wedge B \quad \textit{é in fnc}$$

- Una *fbf* é detta ***forma normale disgiuntiva (fnd)*** se

$$P = P_1 \vee P_2 \vee ... \vee P_n \quad con \quad n \geq 0$$

$$e\ ogni\ P_i = Q_{i,1} \wedge Q_{i,2} \wedge ... \wedge Q_{i,k_i} \quad con \quad k_i \geq 0$$
$$dove\ ogni\ Q_{i,j}\ \textit{é un letterale}$$

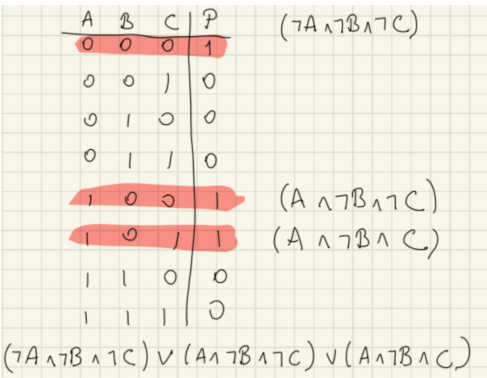
Esempio

$$A \vee (B \wedge C) \vee D \quad \textit{é in fnd}$$

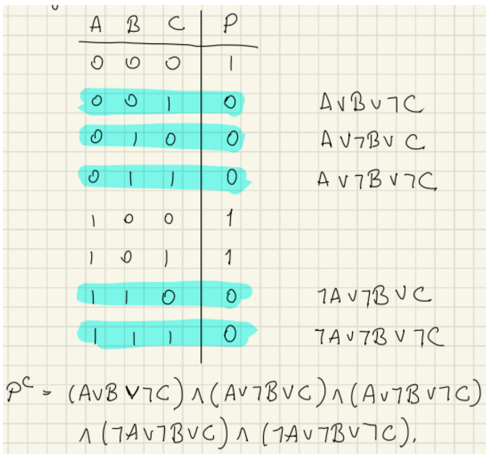
$$A \vee B \vee \neg C \quad \textit{é in fnc e fnd}$$

- **teorema:** Per ogni fbf, P esistono una P^C in fnc e una P^D in fnd tale che
$$P \equiv P^C \equiv P^D$$

- **Metodo pratico**
  - Si costruisce la tabella di veritá e
  - **per la fnd**
    - Si individuano le righe la cui valutazione é 1
    - Si costruisce la **congiunzione** $K_i = L_1 \wedge L_2 \wedge ... \wedge L_n$ per ogni riga la cui valutazione é pari a 1
      - se $v(A) = 1 \Rightarrow L_i = A_i$
      - se $v(A) = 0 \Rightarrow L_i = \neg A$
    - Si fa poi la **disgiunzione** delle congiunzioni K_i
  - **per la fnc**
    - Si individuano le righe la cui valutazione é 0
    - Si costruisce la **disgiunzione** $K_i = L_1 \vee L_2 \vee ... \vee L_n$ per ogni riga la cui valutazione é pari a 1
      - se $v(A) = 0 \Rightarrow L_i = A_i$
      - se $v(A) = 1 \Rightarrow L_i = \neg A$
    - Si fa poi la **congiunzione** delle disiunzioni K_i



(c) P^D



(d) P^C

18 Lezione 19

- **Esericizi e nozioni**
  - Per evitare di riscrivere l'intera *fbf* nella tabella di veritá porre $P_i = fbf$ e scrivere lo P_i nella tabella
  - Per verificare che P sia una tautologia basta cercare un caso in cui sia falsa per dire che P non lo é.
  - Il connettico $A \longleftrightarrow B = (A \to B) \land (B \to A)$

$$V(A \longleftrightarrow B) = 1 \quad sse \quad A{,}B \textit{ hanno lo stesso valore}$$

$$V(A \longleftrightarrow B) = V(B \longleftrightarrow A)$$

A	B	A → B	B → A	A ↔ B
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

  - Se i simboli atomici sono n $(A, B, C.....)$ avremo quindi 2^n combinazioni
  - P_1 e P_2 sono semanticamente equivalenti se per ogni combinazione hanno la stessa interpretazione
  - Seguire sempre le prioritá delle operazioni
  - Se dobbiamo scrivere una *fbf* semanticamente equivalente a quella data individuiamo nella tabella le $v(P) = 1$ *o* 0 che abbia minor cardinalitá e utilizzaimo la *fnc o fnd*
  - La *fnc, fnd* utilizzano solo i simboli $\neg, \lor, \land$
  - Per mostrare che $P \models K$ devo pcostruire la tavola di veritá e vedere che se v é un modello per P lo sia anche per K

- **Definizioni**
  - **definizione:** Una disgiunzione di letterali é detta **clausola**.

$$A \lor B \lor \neg C, \qquad A, \qquad \neg A$$

  - La **clusola vuota** si rappresenta con $\Box$ e corrisponde a $\bot$.

- Una *fbf* in *fnc* si dice anche in **forma a clausole**
- Se Q é un letterale il letterale opposto é indicato con $\sim Q$

$$\textit{chiaramente} \sim Q \equiv \neg Q$$

- Una clausola si denota con l'insieme dei suoi letterali.

$$\neg A \vee B \vee \neg C \qquad \rightarrow \qquad \{\neg A, B, \neg C\}$$

- Una *fbf* in fnc la posso rappresentare con l'insieme delle sue clausole e quindi con **un insieme di insiemi**.

$$P = (\neg A \vee B \vee \neg B) \wedge (\neg A \vee C \vee \neg B) \wedge (\neg C \vee A \vee \neg B)$$

$$\textit{si denota con}$$

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

- **Definizione:** Se C_1, C_2 e R sono clausole si dice che **R é una risolvente** per C_1 e C_2 se esiste un letterale L tale che

$$L \in C_1 \qquad e \qquad \sim L \in C_2 \qquad e$$

$$R = (C_1 \backslash \{L\}) \cup (C_2 \backslash \{\sim L\})$$
$$R = (C_1 - \{L\}) \cup (C_2 - \{\sim L\})$$

- **Lemma:** Se C_1, C_2, R sono clausole tali che R é una risolvente per C_1 e C_2 allora
$$C_1, C_2 \models R$$
- **Definizione:** Siano Γ un insieme di clausole e C una clausola. Una **derivazione di** C **per risoluzione di** Γ é una successione Γ_i con $i = 1, ..., n$ di insiemi di clausole tali che
  * $\Gamma_1 = \Gamma$
  * $\Gamma_{i+1} = \Gamma_i \cup \{R_i\}$ dove R_i é una risolvente di clausole di Γ_i
  * $C \in \Gamma_n$

  In questo caso si scrive $\Gamma \vdash_R C$
- **Teorema:** Un insieme di clausole é insoddisfacibile se e solo se $\Gamma \vdash_R \Box$

19 Lezione 20

- **Nozioni**
  - $A \to B \equiv \neg A \vee B$
  - $P_1, P_4 \models P_2$
    - Ogni volta che P_1 e P_4 sono vere allora lo é anche P_2
  - $F \models K \quad \Rightarrow \quad P_1, P_2, ..., P_n \in F \models K$
  - **Proposizione:** Sia $\Gamma \subseteq F$ e $P \in F$. Allora $\Gamma \models P$ se e solo se

    $$\Gamma \cup \{\neg P\} \ \textit{é insoddisfacibile}$$

  - Vogliamo mostrare $P_1, P_2, P_3 \models P_4$ questo equivale a mostrare che

    $$\Gamma = \{P_1, P_2, P_3, \neg P_4\} \quad \textit{é insoddisfacibile}$$

  - dobbiamo trasformare la P in P^C
    - $P_1 = A \vee B \to D \vee F$
    - $P_1 \equiv \neg(A \vee B) \vee D \vee F \equiv (\neg A \wedge \neg B) \vee D \vee F \equiv$ $(\neg A \vee D \vee F) \wedge (\neg B \vee D \vee F)$
    - Ora questa é in fnc
  - Dato Γ verificare che sia soddisfacibile, ossia dobbiamo trovare un modello, ossia un v t.c. $\forall P \in \Gamma \Rightarrow v(P) = 1$

    esempio: V(A) = 0, V(B) = 0, V(C) = 0 é un modello per Γ

    Quindi data questa combinazione $\forall P \in \Gamma$ *é soddisfatta*

  - **Risoluzione, passi da seguire**
    - Calcolare $P_1^C, P_2^C, P_3^C, \neg P_4^C$
    - Ricordandosi che di rappresentare la *fnc* in forma a clausole.
    - Quando compare la $\wedge$ all'interno dalla fbf creo un'altro insieme nell'insieme
    - $\Gamma^C = P_1^C \cup P_2^C \cup P_3^C \cup \neg P_4^C$
    - Semplificazioni, ossia $\neg A, A$ possono semplificarsi e dare origine a un nuovo gruppo senza i 2
    - Se le semplificazioni danno origine alla clausola vuota $\to P_1, P_2, P_3 \models P_4$

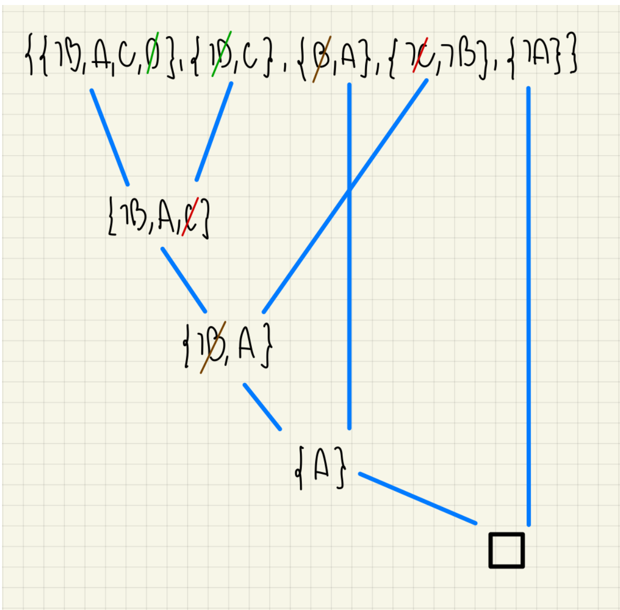
– **Esempio**

$$P_1 = B \to A \vee C \vee D$$
$$P_2 = D \to C$$
$$P_3 = (B \vee A) \wedge (C \to \neg B)$$
$$P_4 = A$$

Vogliamo mostrare $P_1, P_2, P_3 \models P_4$

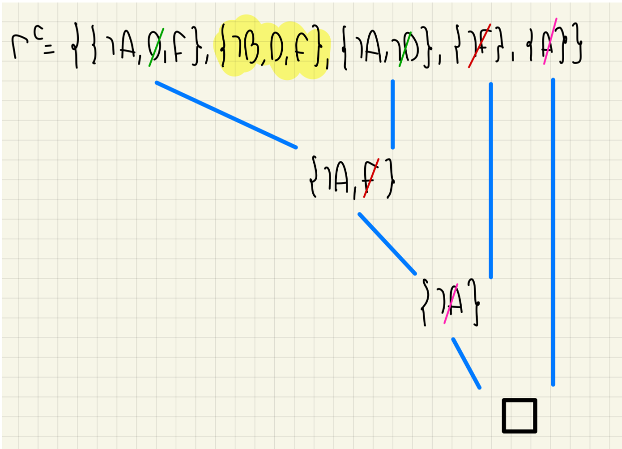
$$P_1 = B \to A \vee C \vee D \equiv \neg B \vee A \vee C \vee D \qquad P_1^C\{\{A, \neg B, C, D\}\}$$
$$P_2 = D \to C \equiv \neg D \vee C \qquad P_2^C = \{\{\neg D, C\}\}$$
$$P_3 = (B \vee A) \wedge (C \to \neg B) \equiv (B \vee A) \wedge (\neg C \vee \neg B) \qquad P_3^C = \{\{B, A\}, \{\neg C, \neg B\}\}$$
$$\neg P_4 = \neg A \qquad \neg P_4^C = \{\{\neg A\}\}$$

$$\Gamma^C = P_1^C \cup P_2^C \cup P_3^C \cup \neg P_4^C$$
$$\Gamma^C = \{\{A, \neg B, C, D\}, \{\neg D, C\}, \{B, A\}, \{\neg C, \neg B\}, \{\neg A\}\}$$



Abbiamo dimostrato che Γ^C *é insoddisfacibile. Quindi* $P_1, P_2, P_3 \models P_4$

– Posso anche non utilizzarle tutte per la risoluzione



– Determinare l'insieme delle sottoformule di P

  * Si parte da P per poi scendere sempre di un livello fino ad arrivare ai simboli atomici

$$P = (\neg A \vee C \to B) \wedge (B \to \neg A \vee C)$$

$$S(P) = \{P, (\neg A \vee C \to B), (B \to \neg A \vee C), \neg A \vee C, \neg A, A, C, B, \}$$

– **teorema:** Per ogni fbf, P esistono una P^C in fnc e una P^D in fnd tale che

$$P \equiv P^C \equiv P^D$$

20 Lezione 21

- **Definzioni:**
  - $\forall$: **quantificatore universale**
  - $\exists$: **quantificatore esistenziale**
  - **Il linguaggio della logica del primo ordine**
    - simboli di costante $a,\ b,\ c,\ \ldots\ (a_1, a_2, a_3, \ldots)$
    - simboli di variabili $x,\ y,\ z,\ \ldots\ (x_1, x_2, x_3, \ldots)$
    - simboli di funzione $f,\ g,\ h,\ \ldots\ (f_1, f_2, f_3, \ldots)$
    - simboli di predicato $A,\ B,\ C,\ \ldots\ (A_1, A_2, A_3, \ldots)$
    - connettivi $\neg, \vee, \wedge, \rightarrow$
    - Simbolo $\perp$
    - Quantificatori $\forall, \exists$
    - Simboli ausiliari "(", ")", ","
  - Dobbiamo definire i **termini**
    a) Ogni costante é un termine
    b) Ogni variabile é un termine
    c) Se $t_1, t_2, ..., t_n$ sono termini e $f^{(n)}$ é un simbolo di funzione allora $f^{(n)}(t_1, t_2, ..., t_n)$ é un termine
  - **Esempio**
    a) 0 costante
    b) x, y, z variabili
    c) $s^{(n)}, p^{(n)}, m^{(n)}$ sono funzione di con n **termini**

$$s^{(1)}, p^{(2)}, m^{(2)}$$

$$s(0) \quad s(s(0)) \quad m(s(s(0)), s(s(0))) \quad s(x) \quad s(p(0, y))$$

  - **Le formule atomiche** si costruiscono con le seguenti regole
    a) $\perp$
    b) Ogni **termine** é una formula atomica
    c) Se $t_1, t_2, ..., t_n$ sono **termini** e $A^{(n)}$ é un simbolo di predicato allora $A^{(n)}(t_1, t_2, ..., t_n)$ é una formula atomica
  - **Esempio**

$$P^{(2)} \qquad P(x, y \qquad P(x, 0))$$

- Possiamo definire le ***fbf***
  a) Ogni formula atomica é una *fbf*
  b) Se P e Q sono *fbf* allora anche
     * $\neg P$
     * $P \vee Q$
     * $P \wedge Q$
     * $P \to Q$
  c) Se P é una *fbf* e x é una variabile allora anche
     * $\forall x P$
     * $\exists x P$
- **Prioritá** (dalla piú alta alla piú bassa)
  1. $\forall, \exists, \neg$
  2. $\wedge$
  3. $\vee$
  4. $\to$
- **Sottoformule:** Sia P una *fbf* l'insieme delle sottoformule $S(P)$ é cosí definito
  a) Se P é una formula atomica allora $S(P) = \{P\}$
  b) Se $P = \perp$ allora $S(P) = \{P\} = \{\perp\}$
  c) Se $P = \neg P_1$ allora $S(P) = \{P\} \cup \{P_1\}$
  d) Se $P = P_1(\vee, \wedge, \to)P_2$ allora $S(P) = \{P\} \cup \{P_1\} \cup \{P_2\}$
  e) Se $P = (\exists x / \forall x P_1)$ allora $S(P) = \{P\} \cup \{P_1\}$
- **Proposizione:** $\forall x P$ oppure $\exists x P$ si dice che la variabile x é **vincolata o legata**.
- **proposizione:** Ogni quantificatore introduce un legame con le variabili prensenti nel suo **campo di azione**.
  In generale il **campo di azione** di un quantificatore é la **sottoformula** che compare immediatamente a destra del quantificatore.
- Una variabili che non é vincolata si dice **libera**
- Indicheremo con ***FV(p)*** le *free variables*, ossia l'insieme delle variabili libere
- Indicheremo con ***BV(p)*** le *bounded variables*, ossia l'insieme delle variabili vincolate

- **Definzione:** Sia t un **termine**, allora $\boldsymbol{FV(t)}$ é definita dal
  a) se $t = c$ $\quad FV(c) = \varnothing$
  b) se $t = x$ $\quad FV(x) = \{x\}$
  c) se $t = f^{(n)}(t_1, t_2, .., t_n)$

$$FV(t) = FV(t_1) \cup FV(t_2) \cup .... \cup FV(t_n)$$

  Sia ora P una *fbf* allora
  a) se $P = \perp$ $\quad FV(\perp) = \varnothing$
  b) se $P = t$ $\quad$ guardare sopra
  c) se $P = A^{(n)}(t_1, t_2, .., t_n)$

$$FV(P) = FV(t_1) \cup FV(t_2) \cup .... \cup FV(t_n)$$

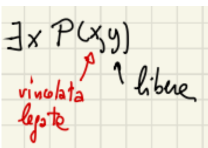
  d) $FV(\neg P) = FV(P)$

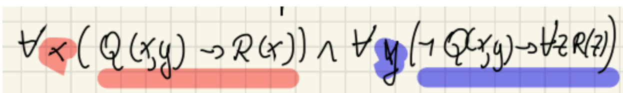
$$FV(P_1(\vee, \wedge, \rightarrow)P_2) = FV(P_1) \cup FV(P_2)$$

  e) $FV(\exists x P) = FV(P) - \{x\}$
  f) $FV(\forall x P) = FV(P) - \{x\}$
- **Definzione:** Consideriamo ora $\boldsymbol{BV}$
  a) Se t é un termine, allora $BV(t) = \varnothing$
  b) $BV(\perp) = \varnothing$
  c) $BV(A^{(n)}(t_1, t_2, .., t_n)) = \varnothing$
  d) $BV(\neg P) = BV(P)$

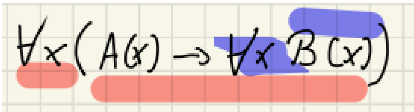
$$BV(P_1(\vee, \wedge, \rightarrow)P_2) = BV(P_1) \cup BV(P_2)$$

  e) $FV(\exists x P) = FV(P) \cup \{x\}$
  f) $FV(\forall x P) = FV(P) \cup \{x\}$
- **NB:** É possibile che $FV(P) \cap BV(P) \neq \varnothing$. Una variabile puó essere sia libera che vincolata all'interno della stessa P questo vuol dire che il fanno riferimento a diversi campi di azione





- **Osservazione:** Puó accadere che una variabile compaia nel campo di azione di piú quantificatori



- **Definizione:** Sia P una *fbf*. Diremo che P é **chiusa** se non contiene variabili libere ovvero $FV(P) = \varnothing$.
- **Definizione:** Al contrario se $BV(P) = \varnothing$ diremo che P é **aperta**.

- **Nozioni:**
  - Se x é un elemento di un dato insieme scriveremo $P(x)$ per indicare che la Proprietà P vale per l'elemento x

    P(x) potrebbe essere l'asserzione "x é un numero primo" dove x é un numero naturale

    $$P(5) = vera \qquad P(6) = falsa$$
  - $\forall x P(x)$ servirá ad indicare che la proprietá P vale per ogni elemento x (di un qualche insieme prefissato)
  - $\exists x P(x)$ servirá ad indicare che la proprietá P vale per qualche x
  - $f^{(n)}$ per indicare una funzione di n variabili. Diremo che la funzione é n-aria
  - $A^{(n)}$ per indicare un predicato n-ariario
  - Interpretazione ()

$$(\forall x(P(x) \rightarrow ((\exists y Q(x,y)) \vee (\neg P(x)))))$$

$$\forall x(P(x) \rightarrow \exists y Q(x,y) \vee \neg P(x))$$

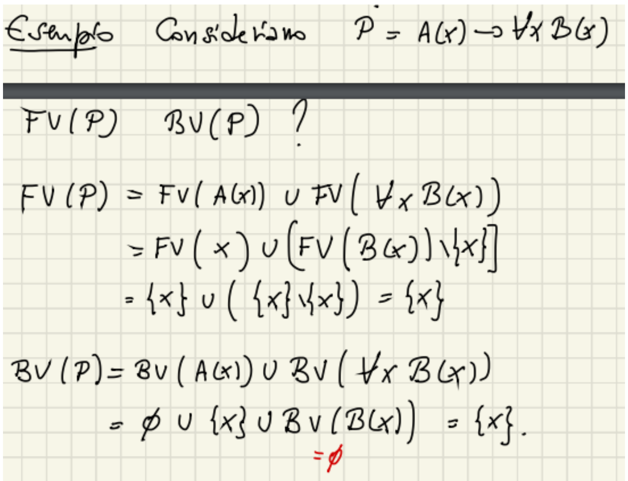
$$Mentre\ questa$$

$$\forall x P(x) \rightarrow \exists y Q(x,y) \vee \neg P(x)$$

$$sarebbe$$

$$(\forall x P(x)) \rightarrow \exists y Q(x,y)$$

- Ogni variabile che compare nel campo di azione di un quantificatore puó essere sostituita con un'altra a patto che quest'ultima **non compaia** come variabile libera nella formuala



<u>Esempio</u> Consideriamo $P = A(x) \to \forall x\, B(x)$

$FV(P)$ $BV(P)$?

$$
\begin{aligned}
FV(P) &= FV(A(x)) \cup FV(\forall x\, B(x)) \\
&= FV(x) \cup \left[FV(B(x)) \setminus \{x\}\right] \\
&= \{x\} \cup (\{x\} \setminus \{x\}) = \{x\}
\end{aligned}
$$

$$
\begin{aligned}
BV(P) &= BV(A(x)) \cup BV(\forall x\, B(x)) \\
&= \emptyset \cup \{x\} \cup \underbrace{BV(B(x))}_{=\emptyset} = \{x\}.
\end{aligned}
$$

21 Lezione 22

- **Definizioni:**
  - **definizione:** Siano t e s due termini e x una variabile. Il termine $s[t/x]$ é definito mediante le seguenti regole
    1. Se s é una **costante** c allora $s[t/x] = c$
    2. Se s é una **variabile** y allora
    $$s[t/x] = \begin{cases} y & y \neq x \\ t & y = x \end{cases}$$
    3. Se $t_1, t_2, ..., t_n$ sono termini e $f^{(n)}(t_1, t_2, ..., t_n)$ é una **funzione n-aria** allora
    $$f^{(n)}(t_1, t_2, ..., t_n)[t/x] = f^{(n)}(t_1[t/x], t_2[t/x], ..., t_n[t/x])$$
    per indicare la sostituzione si pone alla fine $[t/x]$
  - **definizione:** Siano P una *fbf*, t un termine e x una variabile. La formula $P[t/x]$ é definita dalle seguenti regole
    1. $\perp[t/x] = \perp$
    2. Se $t_1, t_2, ..., t_n$ sono termini e $A^{(n)}(t_1, t_2, ..., t_n)$ é un **predicato n-ario** allora
    $$A^{(n)}(t_1, t_2, ..., t_n)[t/x] = A^{(n)}(t_1[t/x], t_2[t/x], ..., t_n[t/x])$$
    3. Se $P = P_1 \to P_2$ allora $P[t/x] = P_1[t/x] \to P_2[t/x]$
    Se $P = P_1 \vee P_2$ allora $P[t/x] = P_1[t/x] \vee P_2[t/x]$
    Se $P = P_1 \wedge P_2$ allora $P[t/x] = P_1[t/x] \wedge P_2[t/x]$
    Se $P = \neg P_1$ allora $P[t/x] = \neg(P_1[t/x])$
    4. $$(\forall y P)[t/x] = \begin{cases} \forall y(P[t/x]) & x \neq y \ se \ y \notin FV(t) \\ \forall z(P[z/y] \ \ P[t/x]) & x \neq y \ se \ y \in FV(t), \\ & z \ non \ occorre \ in \ P \ e \ t \\ \forall y P & x = y \end{cases}$$
    5. $$(\exists y P)[t/x] = \begin{cases} \exists y(P[t/x]) & x \neq y \ se \ y \notin FV(t) \\ \exists z(P[z/y] \ \ P[t/x]) & x \neq y \ se \ y \in FV(t), \\ & z \ non \ occorre \ in \ P \ e \ t \\ \exists y P & x = y \end{cases}$$

- **Semantica del calcolo dei predicati:** Dobbiamo dare un valore di veritá alle *fbf.*
- **definizione:** Una **struttura** $\mathcal{A}$ é data da un insieme D detto *dominio* e una *applicazione* che associa
  1. ad ogni **simbolo di costante** $\boldsymbol{c}$ un elemento $c^{\mathcal{A}} \in D$
  2. ad ogni **simbolo di funzione** $\boldsymbol{f}^{(n)}$ una funzione
  $$f^{(\mathcal{A})} : D \times D \times ... \times D \to D$$
  una funzione che sia definita su D e vada in D
  3. ad ogni **predicato** $\boldsymbol{B}^{(n)}$ una funzione
  $$B^{(\mathcal{A})} : D \times D \times ... \times D \to \{0, 1\}$$
- **NB:** Poiché una *fbf* puó contenere delle **variabili libere** bisognerá assegnare loro dei valori
- **definizione:** Data una struttura $\mathcal{A}$ con dominio D chiameremo **ambiente (o assegnemento)** una *funzione* $\mathcal{E} = \mathcal{E}^{\mathcal{A}}$ definita su D.
  $$\mathcal{E} : VAR \to D$$
  L'insieme di tutti i possibili ambienti lo indichiamo con
  $$ENV_D = \{\mathcal{E} : VAR \to D\}$$
  Se $\mathcal{E}$ é un ambiente per la struttura $\mathcal{A}$ e $a \in D$ indicheremo con $\mathcal{E}[a/x]$ **l'ambiente modificato** per fare in modo che alla variabile x sia associato il valore a. Ossia
  $$\mathcal{E}[a/x] = \begin{cases} \mathcal{E}(y) & y \neq x \\ a & y = x \end{cases}$$
- **definizione:** Una **interpretazione** $\mathcal{F} = (\mathcal{A}, \mathcal{E})$ é data da una struttura $\mathcal{A}$ e da un ambiente $\mathcal{E}$ per tale struttura. Se $a \in D$ scriveremo $\mathcal{F}[a/x]$ per indicare l'interpretazione data da $(\mathcal{A}, \mathcal{E}[a/x])$.
- **defizione:** Fissiamo una interpretazione $\mathcal{F} = (\mathcal{A}, \mathcal{E})$ e dato un **termine** t denotiamo con
  $$[\![t]\!]^{\mathcal{A}}_{\mathcal{E}}$$
  il suo valore nell'interpretazione definito induttivamente con le seguenti regole:

1. se t é un simbolo di **costante** c allora

$$[\![t]\!]^{\mathcal{A}}_{\mathcal{E}} = c^{\mathcal{A}}$$

2. se t é una **variabile** x allora

$$[\![t]\!]^{\mathcal{A}}_{\mathcal{E}} = \mathcal{E}(x)$$

3. se t e una **funzione** $f^{(n)}(t_1, t_2, ..., t_n)$ dove $(t_1, t_2, ..., t_n)$ sono termini, allora

$$[\![t]\!]^{\mathcal{A}}_{\mathcal{E}} = f^{\mathcal{A}}([\![t_1]\!]^{\mathcal{A}}_{\mathcal{E}}, [\![t_2]\!]^{\mathcal{A}}_{\mathcal{E}}, ..., [\![t_n]\!]^{\mathcal{A}}_{\mathcal{E}})$$

- *Indicheremo il valore di veritá con* $v^{\mathcal{F}}(P) = v^{(\mathcal{A},\mathcal{E})}(P)$
- **Definzione:** La funzione di valutazione $v^{\mathcal{F}} : fbf \rightarrow \{0, 1\}$ é definita induttivamente come segue: (sia B un predicato)
  1. $v^{\mathcal{F}}(\perp) = 0$
  2. $v^{\mathcal{F}}(B^{(n)}(t_1, t_2, ..., t_n)) = B^{\mathcal{F}}([\![t_1]\!]^{\mathcal{A}}_{\mathcal{E}}, [\![t_2]\!]^{\mathcal{A}}_{\mathcal{E}}, ..., [\![t_n]\!]^{\mathcal{A}}_{\mathcal{E}})$
  3. $v^{\mathcal{F}}(\neg P) = 1 - v^{\mathcal{F}}(P)$
  4. $v^{\mathcal{F}}(P_1 \vee P_2) = max(v^{\mathcal{F}}(P_1), v^{\mathcal{F}}(P_2))$
  5. $v^{\mathcal{F}}(P_1 \wedge P_2) = min(v^{\mathcal{F}}(P_1), v(^{\mathcal{F}}P_2))$
  6. $v^{\mathcal{F}}(P_1 \rightarrow P_2) = max(1 - v^{\mathcal{F}}(P_1), v^{\mathcal{F}}(P_2))$
  7. $v^{\mathcal{F}}(\forall x P) = min\{v^{\mathcal{F}[a/x]}(P) : a \in D\}$
  8. $v^{\mathcal{F}}(\exists x P) = max\{v^{\mathcal{F}[a/x]}(P) : a \in D\}$

- **Oseervazione:** il **quantificatore universale** $\forall x$ puó essere pensato come un **congiunzione iterata**

$$\forall x P(x) \Rightarrow P(a_1) \wedge P(a_2) \wedge .. \qquad (a_1, a_2...) \in D$$

Analogamente il **quantificatore esistenziale** $\exists x$ puó essere pensato come **disgiunzione iterata**

$$\exists x P(x) \Rightarrow P(a_1) \vee P(a_2) \vee .. \qquad (a_1, a_2...) \in D$$

- **Teorema:** Sia P una *fbf* e $\mathcal{A}$ una struttura. Sia $FV(P) = \{y_1, y_2, ..., y_n\}$ l'insieme delle variabili libere. La valutazione dipende solo dal valore assegnato dall'ambiente $\mathcal{E}$ alle variabili libere di P.

22 Lezione 23

- **Definizioni:** Sia P una *fbf* diremo che

  a. P é **soddisfatta** in una data struttura $\mathcal{A}$ rispetto all'ambiente $\mathcal{E}$ se $v^{(\mathcal{A},\mathcal{E})}(P) = 1$.
  $$(\mathcal{A}, \mathcal{E}) \models P$$

  b. P é **soddisfacibile** in una data struttura $\mathcal{A}$ se esiste un ambiente $\mathcal{E}$ per cui
  $$(\mathcal{A}, \mathcal{E}) \models P$$

  c. P é **soddisfacibile** se esistono una struttura $\mathcal{A}$ e un ambiente $\mathcal{E}$ tale che
  $$(\mathcal{A}, \mathcal{E}) \models P$$

  d. P é **vera** in una struttura $\mathcal{A}$ se per ogni ambiente $\mathcal{E}$ si ha
  $$(\mathcal{A}, \mathcal{E}) \models P$$

  e. P é **valida** se é vera in ogni struttura
  $$\models P$$

  f. P é **falsa** in una struttura $\mathcal{A}$ se non esiste alcun ambiente $\mathcal{E}$ tale che $v^{(\mathcal{A},\mathcal{E})}(P) = 1$. In altre parole $v^{(\mathcal{A},\mathcal{E})}(P) = 0$ qualunque sia $\mathcal{E}$.
  $$\mathcal{A} \not\models P$$

  g. P é **insoddisfacibile (o contraddittoria)** se é falsa in ogni struttura

- **Definizioni:** Sia Γ un insieme di *fbf* diremo che

  a. Γ é **soddisfatta** in una data struttura $\mathcal{A}$ se esiste un ambiente $\mathcal{E}$ tale che $\forall P \in \Gamma$ si abbia $v^{(\mathcal{A},\mathcal{E})}(P) = 1$.
  $$(\mathcal{A}, \mathcal{E}) \models P$$

  b. Γ é **soddisfacibile** se esiste una struttura $\mathcal{A}$ in cui Γ é soddisfacibile

  c. Una struttura $\mathcal{A}$ é un **modello** per Γ se $\forall P \in \Gamma$ si ha
  $$\mathcal{A} \models P$$

  d. Γ é **valido** se ogni struttura é un modello per Γ

- **definizione:** Dato un insieme di *fbf* Γ ed una *fbf* Q, diremo che Q é **conseguenza semantica** di Γ e scriveremo $\Gamma \models Q$ se per ogni struttura $\mathcal{A}$ e ambiente $\mathcal{E}$ tali che si abbia

$$v^{(\mathcal{A},\mathcal{E})}(P) = 1 \qquad \forall P \in \Gamma \Rightarrow v^{(\mathcal{A},\mathcal{E})}(Q) = 1$$

- **definizione:** Sia P una *fbf* e sia $FV(P) = \{x_1, x_2, ..., x_n\}$ l'insieme delle variabili libere di P. La **chiusura universale** di P é la formula

$$Ce(P) = \forall x_1 \forall x_2 ... \forall x_n$$

la **chiusura esistenziale** di P é la formula

$$Ex(P) = \exists x_1 \exists x_2 ... \exists x_n$$

- **definizione:** Sia P una *fbf*. Allora P **é valida** se e solo se $Ce(P)$ lo é.
- **definizione:** Sia P una *fbf*. Allora P **é soddisfacibile** se e solo se $Ex(P)$ lo é.
- **definizione:** Due *fbf* P e Q sono **semanticamente equivalenti** se per tutte le interpretazioni $\mathbb{F} = (\mathcal{A}, \mathcal{E})$ si ha

$$v^{\mathcal{F}}(P) = v^{\mathcal{F}}(Q) \Rightarrow P \equiv Q$$

- **Teorema:** Sia P una *fbf*, valgono le seguenti equivalenze semantiche

  a. $\neg \forall x P \equiv \exists x \neg P$
  b. $\neg \exists x P \equiv \forall x \neg P$
  c. $\forall x P \equiv \neg \exists x \neg P$
  d. $\exists x P \equiv \neg \forall x \neg P$
  e. $\forall x \forall y P \equiv \forall y \forall x P \qquad \forall x, y P$
  f. $\exists x \exists y P \equiv \exists y \exists x P \qquad \exists x, y P$
  g. $\forall x \exists y P \;\not\equiv\; \exists y \forall x P$
  h. $\forall x P \equiv P \qquad se\ x \neq FV(P)$
  i. $\exists x P \equiv P \qquad se\ x \neq FV(P)$
  j. $\forall x (P_1 \wedge P_2) \equiv \forall x P_1 \wedge \forall x P_2$
  k. $\exists x (P_1 \vee P_2) \equiv \exists x P_1 \vee \exists x P_2$
  l. $\forall x (P_1 \vee P_2) \equiv \forall x P_1 \vee P_2 \qquad x \neq FV(P_2)$
  m. $\exists x (P_1 \wedge P_2) \equiv \exists x P_1 \wedge P_2 \qquad x \neq FV(P_2)$

Attenzione in generale

$$\forall x (P_1 \vee P_2) \not\equiv \forall x P_1 \vee \forall x P_2.$$

$$\exists x (P_1 \wedge P_2) \not\equiv \exists x P_1 \wedge \exists x P_2.$$

Consideriamo due formule ben formate P_1, P_2 e due quantificatori $Q_1, Q_2 \in \{\exists, \forall\}$

$$Q_1 x P_1 \vee Q_2 x P_2 \equiv Q_1 x\, Q_2 z (P_1 \vee P_2[z/x])$$

$$Q_1 x P_1 \wedge Q_2 x P_2 \equiv Q_1 x\, Q_2 z (P_1 \wedge P_2[z/x])$$

a condizione che $z \notin FV(P_1) \cup FV(P_2)$.

23 Lezione 24

- **Nozioni**
  - Data P, una fbf, vogliamo dare un valore di veritá alla P
    a. **Scegliere una struttura** $\mathcal{A}$, la struttura definisce
       * Dominio
       * costanti
       * le funzioni
       * i predicati
    b. Definire un **ambiente** $\mathcal{E}$, si occupa di assegnare un valore
       * Variabili libere
       * Variabili vincolate

         Anche se si occupa solo di assegnare un valore alle ***variabili libere****, perché quelle vincole vengono sostituite con un valore del dominio.*

$$\mathcal{E}(y) = 4$$

    c. **L'interpretazione** $\mathcal{F} = (\mathcal{A}, \mathcal{E})$, assegna i valori dettati dalla struttura e dal ambiente scelti.

$$v^{\mathcal{F}}(P)$$

  - l'interpretazione nel caso in cui t sia un termine, questo vale per
    * variabile
    * costante
    * funzione

$$[\![t]\!]^{\mathcal{A}}_{\mathcal{E}}$$

  - una volta che io incontro un **quantificatore** la fbf interna ad esso porta con se **l'ambiente modificato**

$$\mathcal{E}[a/x]$$

  - Il predicato A é interpretato come $=$

$$A(x, y) \Rightarrow x = y$$

  - la funzione f é interpretata come $\times$

$$f(x, y) \Rightarrow x \times y$$

- Le variabili voncolate vengono introdotte dai quantificatori $\forall x, \exists x$, e introduce l'**ambiente modificato** $[a/x]$
- Esempio variabili vincolate

$$v^{\mathcal{A}}_{\mathcal{E}(a/x)} = ((\forall y)A(x,y)) = 1$$

$$= min\{v^{\mathcal{A}}_{\mathcal{E}[a/x][b/y]}(A(x,y) : b \in D)\}$$

- Trovare una formual di logica proposizionale $f(A,B,C)$ che non sia una contraddizione e tale che Γ sia insoddisfacibile.

$$\Gamma = \{\neg A, \neg A \to (B \vee C), B \to (A \vee C), f(A,B,C)\}$$

$$f(A,B,C) = \neg \ di \ una \ P \ di \ \Gamma$$

$$f(A,B,C) = \neg(\neg A \to (B \vee C)) \equiv \neg(A \vee B \vee C) \equiv (\neg A \wedge \neg B \wedge \neg C)$$