ARGOMENTI D'ESAME LOGICA E ALGEBRA 2

Dagli appunti del professor Paolo Sentinelli

Autori Pietro Pizzoccheri Lorenzo Bardelli

Document formatting by ${\rm L_{UCA~ZANI}}$

 $\begin{array}{c} {\rm Politecnico~di~Milano} \\ {\rm A.Y.~2024/2025} \end{array}$

© The authors. Some rights reserved. This work is licensed under CC BY-NC-SA 4.0. http://creativecommons.org/licenses/by-nc-sa/4.0/
In particular, without the authors' permission, it is forbidden to make digital or printed copies to sell them.
Document created on 8 gennaio 2025
DEVELOPED BY: LUCA ZANI PIETRO PIZZOCCHERI
Lorenzo Bardelli

Indice

1	Can	npi Finiti e Tensori	1					
	1.1	I sottogruppi di un gruppo ciclico sono ciclici	1					
	1.2	Un anello è un campo se e solo se i suoi ideali sono banali	2					
	1.3	Teorema di isomorfismo per anelli commutativi	3					
	1.4	Insieme degli ideali dell'anello \mathbb{Z} e dell'anello \mathbb{Z}_n	4					
	1.5	Teorema cinese dei resti	5					
	1.6	Costruzione di un campo finito di cardinalità p^n	6					
	1.7	Tutti i polinomi irriducibili di grado n a coefficienti in \mathbb{F}_p sono fattori di $X^{p^n} - X \in \mathbb{F}_p[X]$	7					
	1.8	Sottocampi di un campo finito	8					
	1.9	Algoritmo di Berlekamp	9					
	1.10		13					
2	Logica modale							
	2.1	.1 Sintassi della logica modale e semantica di Kripke						
			15					
			18					
		2.1.3 Semantica dei mondi possibili (semantica di Kripke)	18					
	2.2		20					
	2.3		21					
	2.4	Esprimibilità della proprietà transitiva	22					
	2.5	Morfismi di modelli + Lemma 1	23					
	2.6		25					
	2.7	Logiche modali normali, dimostrazioni, teoremi e validità della logica K	27					

Capitolo 1

Campi Finiti e Tensori

1.1 I sottogruppi di un gruppo ciclico sono ciclici

 $extbf{Teorema 1.1}$ — di struttura per i gruppi ciclici. Sia G un gruppo ciclico. Allora ogni sottogruppo di G è ciclico.

DIMOSTRAZIONE. Sia $g \in G$ tale che $G = \langle g \rangle$. La funzione $\varphi : (\mathbb{Z}, +) \to G$ definita da $\varphi(g) = g^n, \forall n \in \mathbb{Z}$ è un morfismo suriettivo di gruppi.

- a) G è infinito: allora $Ker(f) = \{0\}$ e quindi φ è iniettivo. Dunque φ è un isomorfismo di gruppi. Tutti i sottogruppi di $\mathbb Z$ sono ciclici.
- b) G è finito: sia $H \subseteq G$ un sottogruppo. Allora $\varphi^{-1}(H) := \{n \in \mathbb{Z} : \varphi(n) \in H\} \subseteq \mathbb{Z}$ è un sottogruppo di \mathbb{Z} , quindi esiste $\varphi^{-1}(H) = \langle k \rangle$ con $k \in \mathbb{N}$.

La restrizione $\varphi:k\mathbb{Z}\to H$ è un morfismo suriettivo di gruppi e

$$\varphi(hk) = \varphi(\underbrace{k+k+\ldots+k}_{h \text{ volte}}) = \varphi(k)\varphi(k)\ldots\varphi(k) = [\varphi(k)]^h \quad \forall h \in \mathbb{Z}$$

Quindi $H = \langle \varphi(k) \rangle$.

1.2 Un anello è un campo se e solo se i suoi ideali sono banali

Proposizione 1.2. Sia A un anello commutativo e $I \subseteq A$ un ideale. Allora:

- I=A se e solo se I contiene un elemento invertibile
- A è un campo sse i suoi unici ideali sono $\langle 0 \rangle$ e $A = \langle 1_A \rangle$

DIMOSTRAZIONE.

• se I = A allora $1_A \in I$ e 1_A è invertibile.

Sia $u \in I$ un elemento invertibile.

Allora $u^{-1} \in A$ e quindi $1_A u u^{-1} \in I$.

Ne segue che $A = \langle 1_A \rangle \subseteq I$. e quindi I = A.

• Sia A un campo e sia $I \neq \langle 0 \rangle$. se $n \in I$ e $x \neq 0$ allora x è invertibile e quindi I = A per il punto sopra.

Viceversa, se $\langle 0 \rangle$ e A sono gli unici ideali di A, e se $x \in A \setminus \{0\}$, allora $\langle x \rangle = \langle 1_A \rangle$, ossia $ax = 1_A$ per qualche $a \in A$. Quindi x è invertibile.

1.3 Teorema di isomorfismo per anelli commutativi

Teorema 1.3 — di isomorfismo per gruppi abeliani. Sia $f:G_1 \to G_2$ un morfismo di gruppi abeliani. Allora esiste un morfismo iniettivo $\varphi: G_1/Ker(f) \to G_2$ tale che il seguente diagramma è commutativo:

$$G_1 \xrightarrow{f} G_2$$

$$\downarrow \qquad \qquad \downarrow \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \downarrow \qquad \qquad \downarrow$$

In particolare, $G_1/Ker(f) \simeq Im(f)$.

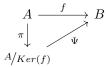
DIMOSTRAZIONE. L'assegnazione $[g] \mapsto f(g), \forall g \in G$, definisce una funzione $\varphi : G_1/Ker(\varphi) \to G_2$. Infatti, se $g' \sim g$, ossia [g] = [g'], allora $g = g' + h, h \in Ker(f)$.

Dunque f(g) = f(g' + h) = f(g') + f(h) = f(g'). Poiché f è morfismo di gruppi, anche φ lo è.

Inoltre $Ker(f) = \{[g] \in G/Ker(f) : \varphi([g]) = e_2\} = \{[g] \in G/Ker(f) : f(g) = e_2\} = [e_1]$. Quindi φ è iniettiva.

Infine, $\varphi: G_1/Ker(f) \to Im(f)$ è un morfismo di gruppi, iniettivo e suriettivo, quindi un isomorfismo.

Teorema 1.4 — di isomorfismo per anelli commutativi. Sia $f:A\to B$ un morfismo di anelli commutativi. Allora esiste un morfismo iniettivo di anelli $\Psi: {}^{A}\!/{}_{Ker(f)}\to B$ tale che il seguente diagramma è commutativo:



in particolare, se f è suriettivo, allora Ψ è un isomorfismo di anelli.

.

Insieme degli ideali dell'anello \mathbb{Z} e dell'anello \mathbb{Z}_n

PROPOSIZIONE 1.5. L'insieme dei sottogruppi di $(\mathbb{Z}, +)$ è $\{n\mathbb{Z} : n \in \mathbb{N}\}$.

DIMOSTRAZIONE. Sia $H\subseteq\mathbb{Z}$ un sottogruppo non banale. Sia $k:=min(H_{>0})$ dove $H_{>0}:=\{h\in H:h>0\}$. Sia $h\in H_{>0}, h\neq k$. Allora h>k e h=nk+r, $n\in\mathbb{N}, 0\leq r< k$. Dunque $r=h-nk\in H\to r=0$ per la minimalità di k.

COROLLARIO 1.6. L'insieme dei sottogruppi di $\mathbb{Z}_n, n \in \mathbb{N}$ è:

$$\{\langle \overline{m} \rangle : \overline{m} \in \mathbb{Z}_n\}$$

ESEMPIO. Abbiamo già visto che ogni sottogruppo di $(\mathbb{Z},+)$ è del tipo $n\mathbb{Z}=\{kn:k\in\mathbb{Z}\}$, dove

Inoltre, se $a \in \mathbb{Z}$ e $x \in n\mathbb{Z}$, ossia x = kn per qualche $k \in \mathbb{Z}$, si ha che $ax = akn \in n\mathbb{Z}$.

Quindi $n\mathbb{Z}$ è un ideale di $\mathbb{Z}, \forall n \in \mathbb{N},$ e tutti gli ideali di \mathbb{Z} sono di questo tipo.

1.5 Teorema cinese dei resti

TEOREMA 1.7 — **Teorema cinese dei resti.** siano $n_1, n_2, \dots, n_k \in \mathbb{N} \setminus \{0, 1\}$ tali che $MCD\{n_i, n_j\} = 1$ per ogni $1 \le i, j \le k, i \ne j$.

Sia $n := n_1 \cdot n_2 \cdot \ldots \cdot n_k$.

Allora la funzione

$$\Psi: \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

che mappa

$$x \bmod n \mapsto (x \bmod n_1, x \bmod n_2, \dots, x \bmod n_k)$$

è un isomorfismo di anelli.

DIMOSTRAZIONE. vediamo prima di tutto che Ψ è un morfismo di anelli dove $f: \mathbb{Z} \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ è definita da $f(x) = (x \mod n_1, x \mod n_2, \ldots, x \mod n_k) \forall x \in \mathbb{Z}$.

•

$$f(a+b) = ((a+b) \bmod n_1, \dots, (a+b) \bmod n_k)$$

$$= (a \bmod n_1 + b \bmod n_1, \dots, a \bmod n_k + b \bmod n_k)$$

$$= (a \bmod n_1, \dots, a \bmod n_k) + (b \bmod n_1, \dots, b \bmod n_k)$$

$$= f(a) + f(b), \forall a, b \in \mathbb{Z}$$

• $f(1) = (1 \mod n_1, \dots, 1 \mod n_k)$ e $(1 \mod n_1, \dots, 1 \mod n_k)$ è l'unità del prodotto diretto di anelli $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$

•

$$f(a \cdot b) = ((a \cdot b) \bmod n_1, \dots, (a \cdot b) \bmod n_k)$$

$$= (a \bmod n_1 \cdot b \bmod n_1, \dots, a \bmod n_k \cdot b \bmod n_k)$$

$$= (a \bmod n_1, \dots, a \bmod n_k) \cdot (b \bmod n_1, \dots, b \bmod n_k)$$

$$= f(a) \cdot f(b), \forall a, b \in \mathbb{Z}$$

Ora mostriamo che f è suriettivo:

sia $(a_1 \bmod n_1, \ldots, a_k \bmod n_k) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$.

Osserviamo che $MCD\{n_i, n_1 n_2 \dots n_{i-1} n_{i+1} \dots n_k\} = 1, \forall 1 \leq i \leq k.$

Quindi abbiamo le identità di Bézout: $c_i n_i + b_i \frac{n}{n_i} = 1$ ossia $u_i + v_i = 1$ dove $u_i = c_i n_i \in < n_i >$ e $v_i = b_i \frac{n}{n_i} \in < \frac{n}{n_i} >$.

Definiamo $x := a_1v_1 + \ldots + a_kv_k$ e abbiamo che $f(x) = (a_1 \mod n_1, \ldots, a_k \mod n_k)$. infatti:

$$v_i \bmod n_j = \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}$$

dal teorema di isomorfismo abbiamo che $\mathbb{Z}/Ker(f) \simeq \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ come anelli. ma abbiamo che $Ker(f) = \langle n_1 \rangle \cap \langle n_2 \rangle \cap \ldots \cap \langle n_k \rangle = \langle mcm\{n_1, \ldots, n_k\} \rangle = \langle n_1 n_2 \ldots n_k \rangle$ dato che n_i e n_j sono coprimi $\forall i \neq j$.

Quindi $\mathbb{Z}/Ker(f) = \mathbb{Z}/\langle n \rangle = \mathbb{Z}_n$ e l'isomorfismo $\Psi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ è quello dell'enunciato del teorema.

1.6 Costruzione di un campo finito di cardinalità p^n

PROPOSIZIONE 1.8. sia K un campo e $P(X) \in K[X]$ un poliniomio irriducibile. Allora l'anello quoziente $K[X]/\langle P(X)\rangle$ è un campo.

DIMOSTRAZIONE. Sia $[f] \in K[X]/\langle P(X) \rangle$ tale che $[p] \neq [0]$ ossia p(X) non divide f(X).

Dunque $MCD\{f(X), p(X)\} = 1$ perchè p(X) è irriducibile.

Quindi abbiamo un'identità di Bézout a(X)f(X) + b(X)p(X) = 1.

Ossia $[a(X)] = [f(X)]^{-1}$ in $K[X]/\langle P(X)\rangle$.

PROPOSIZIONE 1.9. Tutti e soli i polinomi irriducibili su \mathbb{F}_p di grado n dividono $X^{p^n} - X \in \mathbb{F}_p[X]$.

DIMOSTRAZIONE. Sia $P(X) \in \mathbb{F}_p[X]$ irriducibile di grado n e sia $K := \mathbb{F}_p[Y]/\langle P(Y) \rangle$.

Allora K ha p^n elementi che sono le radici di $X^{p^n} - X \in K[X]$.

Poichè $Y \in K$ è una radice $P(X) \in K[X]$, P(X) e $X^{p^n} - X$ hanno una radice in comune in K, allora per il teorema di Ruffini hanno un fattore comune $X - Y \in K[X]$.

Quindi, poiché $\mathbb{F}_p \subseteq K$ e MCD in $\mathbb{F}_p = MCD$ in $K[X] \implies P(X), X^{p^n} - X$ hanno $MCD \neq 1$ in $\mathbb{F}_p[X]$.

Poiché P(X) è irriducibile in $\mathbb{F}_p[X]$, P(X) divide $X^{p^n} - X$.

Adesso vogliamo costruire un isomorfismo di campi

$$f: \mathbb{F}_p[X]/\langle P(X)\rangle \to \mathbb{F}_p[X]/\langle Q(X)\rangle$$

Dove $P(X), Q(X) \in \mathbb{F}_p[X]$ sono monici irriducibili di grado n.

Basta costruire un isomorfismo di anelli.

Infatti un morfismo di anelli che sono campi è iniettivo. Inoltre:

$$|\mathbb{F}_p[X]/\langle P(X)\rangle| = |\mathbb{F}_p[X]/\langle Q(X)\rangle| = p^n$$

Quindi tale morfismo è biunivoco, ossia è isomorfismo.

Si ha che, se $y \in \mathbb{F}_p[Y]/\langle P(Y) \rangle$ allora $P(X) \in \mathbb{F}_p[X]$ è il polinomio minimo di y su \mathbb{F}_p .

Quindi, se P(X) ha una radice in $\mathbb{F}_p[Y]/\langle Q(Y)\rangle$, possiamo usare la proposizione sull'estensione di morfismi di campi per definire il morfismo f, che sarà un isomorfismo. Infatti $\mathbb{F}_p \subseteq \mathbb{F}_p[X]/\langle Q(X)\rangle$.

Inoltre $\mathbb{F}_p[X]/\langle P(X)\rangle = \mathbb{F}_p([X])$, dove [X] è la classe di X in $\mathbb{F}_p[X]/\langle P(X)\rangle$.

Poiché $\mathbb{F}_p[Y]/\langle Q(Y)\rangle$ è un campo di spezzamento di $X^{p^n}-X$ e P(X) divide $X^{p^n}-X$, allora P(X) si fattorizza in fattori di grado 1 in $\mathbb{F}_p[Y]/\langle Q(Y)\rangle$.

Sia $\beta \in \mathbb{F}_p[Y]/\langle Q(Y) \rangle$ tale che $p(\beta) = 0$.

Allora l'assegnazione

$$c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \mapsto c_0 + c_1 \beta + \ldots + c_{n-1} \beta^{n-1}$$

definisce un morfismo di anelli

$$f: \mathbb{F}_p[X]/\langle P(X)\rangle \to \mathbb{F}_p[X]/\langle Q(X)\rangle$$

1.7 Tutti i polinomi irriducibili di grado n a coefficienti in \mathbb{F}_p sono fattori di $X^{p^n}-X\in\mathbb{F}_p[X]$

PROPOSIZIONE 1.10. Tutti e soli i polinomi irriducibili su \mathbb{F}_p di grado n dividono $X^{p^n} - X \in \mathbb{F}_p[X]$.

DIMOSTRAZIONE. Sia $P(X) \in \mathbb{F}_p[X]$ irriducibile di grado n e sia $K := \mathbb{F}_p[Y]/\langle P(Y) \rangle$.

Allora K ha p^n elementi che sono le radici di $X^{p^n} - X \in K[X]$.

Poichè $Y \in K$ è una radice $P(X) \in K[X]$, P(X) e $X^{p^n} - X$ hanno una radice in comune in K, allora per il teorema di Ruffini hanno un fattore comune $X - Y \in K[X]$.

Quindi, poiché $\mathbb{F}_p\subseteq K$ e MCD in $\mathbb{F}_p=MCD$ in $K[X]\implies P(X), X^{p^n}-X$ hanno $MCD\neq 1$ in $\mathbb{F}_p[X]$.

Poiché P(X) è irriducibile in $\mathbb{F}_p[X]$, P(X) divide $X^{p^n}-X$.

Sottocampi di un campo finito

Lемма 1.11. sia F un campo. Il polinomio X^d-1 divide il polinomio X^n-1 s.s.e. d divide n.

DIMOSTRAZIONE. Se $n = qd + r, 0 \le r \le d$, in $\mathbb{F}[X]$ si ha:

$$(x^{n}-1) = (X^{d}-1)(X^{n-d} + X^{n-2d} + \dots + x^{n-(p-1)d} + X^{r}) + (X^{r}-1)$$

 $(x^n-1)=(X^d-1)(X^{n-d}+X^{n-2d}+\ldots+x^{n-(p-1)d}+X^r)+(X^r-1)$ quindi X^d-1 divide X^n-1 s.s.e. X^r-1 è il polinomio nullo, cioè s.s.e. r=0

COROLLARIO 1.12. d divide $n \iff (X^{p^d} - X)$ divide $(X^{p^n} - X)$ in $\mathbb{F}_p[X]$.

DIMOSTRAZIONE. Per il lemma precedente, $X^d - 1$ divide $X^n - 1$.

Calcolando in p si ottiene che $p^d - 1$ divide $p^n - 1$.

Quindi sempre per il lemma, $X^{p^{d-1}} - 1$ divide $X^{p^n-1} - 1$.

Viceversa se $X^{p^{d-1}}-1$ divide $X^{p^n-1}-1$, allora p^d-1 divide $p^n-1\implies d$ divide n.

Proposizione 1.13. Tutti e soli i sottocampi di \mathbb{F}_{p^n} sono i campi \mathbb{F}_{p^d} dove d divide n.

DIMOSTRAZIONE. Abbiamo che, se $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, allora tutte le radici di $X^{p^d} - X$ in \mathbb{F}_{p^d} sono radici di $X^{p^n} - X$ in \mathbb{F}_{p^n} , ossia $X^{p^d} - X$ divide $X^{p^n} - X$ $\Longrightarrow_{\text{corollario}} d$ divide n.

Se d divide n, $X^{p^d} - X$ divide $X^{p^n} - X$ e l'insieme delle radici di $X^{p^d} - X$ (è un campo) sta in \mathbb{F}_{p^n} .

1.9 Algoritmo di Berlekamp

TEOREMA 1.14. Sia $f(x) \in \mathbb{F}_p[x]$ di grado d > 1, sia $h(x) \in \mathbb{F}_p[x]$ di grado 1 < deg(h) < d tale che f(x) divide $h(x)^p - h(x)$. allora:

$$f(x) = MCD\{f(x), h(x)\} \cdot MCD\{f(x), h(x) - 1\} \cdot \dots \cdot MCD\{f(x), h(x) - (p-1)\}$$

è una fattorizzazione non banale di f(x) in $\mathbb{F}_p[x]$.

DIMOSTRAZIONE. Supponiamo che f(x) divida $h(x)^p - h(x)$. il polinomio $X^p - X \in \mathbb{F}_p[X]$ si fattorizza come:

$$X^{p} - X = X(X - 1)(X - 2) \dots (X - (p - 1))$$

mettendo h(x) al posto di X si ha:

$$h(x)^p - h(x) = h(x)[h(x) - 1][h(x) - 2] \dots [h(x) - (p-1)]$$

Abbiamo che $MCD\{h(x)-i,h(x)-j\}=1 \forall i,j\in\mathbb{F}_p,i\neq j.$

Infatti, se $MCD\{h(x) - i, h(x) - j\} = D(x)$ allora

$$\begin{cases} h(x) - i = D(x) \cdot H_i(x) \\ h(x) - j = D(x) \cdot H_j(x) \end{cases} \implies D(x)[H_i(x) - H_j(x)] = j - i \in \mathbb{F}_p \implies deg(D) = 0, i \neq j$$

inoltre, se $MCD\{a,b\} = 1$ si ha che $MCD\{f,ab\} = MCD\{f,a\} = MCD\{f,b\}$. Per induzione si ha che

$$MCD\{f, a_1 \cdot \ldots \cdot a_k\} = MCD\{f, a_1\} \cdot \ldots \cdot MCD\{f, a_k\}$$

dato che f(x) divide $h(x)^p - h(x)$, abbiamo che

$$f(x) = MCD\{f(x), h(x)^p - h(x)\}\$$

poiché, se $i \neq j$, $MCD\{h(x) - i, h(x) - j\} = 1$, si ha

$$f(x) = MCD\{f(x), h(x)^p - h(x)\} =$$

$$= MCD\{f(x), h(x)[h(x) - 1] \cdot \dots \cdot [h(x) - p + 1]\} =$$

$$= MCD\{f, h\} \cdot MCD\{f, h - 1\} \cdot \dots \cdot MCD\{f, h - p + 1\}$$

Poiché $deg(h-i) < deg(f), MCD\{f, h-i\} \neq f(x), \forall i \in \mathbb{F}_p$.

Quindi nella fattoriazzazione precedente appaiono solo polinomi di grado < d, perciò è non banale.

Proposizione 1.15. Un polinomio $h(x) \in \mathbb{F}_p[x]$ che soddisfa le condizioni del teorema esiste sempre.

DIMOSTRAZIONE. Sia

$$h(x) = b_0 + b_1 x + \dots + b_{d-1} x^{d-1} \in \mathbb{F}_p[X]$$

allora

$$h(x)^p = b_0^p + b_1^p x + \ldots + b_{d-1}^p x^{p(d-1)}$$

(avendo dimostrato che $(X+Y)^p=x^p+Y^p$ e induttivamente che $(\sum_{i=1}^k x_i)^p=\sum_{i=1}^k x_i^p)$, ma

$$b_i^p = b_i \forall 0 \le i \le d-1$$
 quindi $h(x)^p = b_0 + b_1 x^p + \ldots + b_{d-1} x^{p(d-1)}$

si ha che

$$h(x)^p \mod f(x) = b_0(\mod f) + b_1(x^p \mod f) + \ldots + b_{d-1}(x^{p(d-1)} \mod f)$$

Sia $x^{ip} = f(x)q_i(x) + r_i(x)$ con $deg(r_i) < d, 0 \le i \le d-1$. Abbiamo che

$$[h(x)^p - h(x)] \mod f = 0 \mod f$$

$$\iff h(x)^p \mod f = h(x) \mod f$$

$$\iff b_0 r_0(x) + b_1 r_1(x) + \ldots + b_{d-1} r_{d-1}(x) = b_0 + b_1 x + \ldots + b_{d-1} x^{d-1}$$
amo così un sistema lineare di d'equazioni nelle incognite b_0 b_1

Otteniamo così un sistema lineare di d equazioni nelle incognite $b_0, b_1, \ldots, b_{d-1}$.

Dobbiamo mostrare che esistono soluzioni non nulle.

Sia $f(x) = p_1(x) \dots p_k(x)$ una fattoriazzazione di $f(x) \in \mathbb{F}_p[x]$ in fattori irriducibili.

Supponiamo che f non habbia fattori multipli (verificabile con Teorema seguente).

Teorema 1.16. sia K un campo.

- a) se $f(x) \in K[x]$ è ha un fattore multiplo, allora $MCD\{f,f'\} \neq 1$, dove f' è la derivata di f rispetto a x.
- b) se K ha caratteristica 0 o p, e $MCD\{f, f'\} \neq 1$, allora f(x) ha un fattore multiplo.

Abbiamo una versione in $\mathbb{F}_p[x]$ del teorema cinese dei resti.

$$MCD{p_i(x), p_j(x)} = 1, \forall \le i \le k, 1 \le j \le k, i \ne j$$

$$\implies \mathbb{F}_p[x] / \langle f \rangle \underbrace{\simeq}_{\text{Isomorfismo di anelli}} \mathbb{F}_p[x] / \langle p_1(x) \rangle \times \ldots \times \mathbb{F}_p[x] / \langle p_k(x) \rangle$$

Dato $(s_1, \ldots, s_k) \in \mathbb{F}_p^k$, esiste un'unica classe $[h(x)] \in \mathbb{F}_p[x]/\langle f \rangle$ tale che

$$\begin{cases} [h(x)] = s_1 & \text{in} & \mathbb{F}_p[x]/\langle p_1(x) \rangle \\ \vdots \\ [h(x)] = s_k & \text{in} & \mathbb{F}_p[x]/\langle p_k(x) \rangle \end{cases}$$

ossia $h(x) - s_i$ è divisibile per $p_i(x), \forall 1 \leq i \leq k$.

Quindi $p_i(x)$ divide $h(x)[h(x)-1]\dots[h(x)-(p-1)]=h(x)^p-h(x), \forall 1\leq i\leq k$.

Ossia f(x) divide $h(x)^p - h(x)$.

Sia
$$f(x)\mathbb{F}_p[x], deg(f) = d$$
.

Sia $f(x) = p_1(x) \cdot \ldots \cdot p_k(x)$ una fattoriazzazione di f(x) in fattori irriducibili, non banali (cioè di grado ≥ 1) e aventi molteplicità 1. siano

$$r_0 = 1 \mod f(x)$$

$$r_1 = x^p \mod f(x)$$

$$\vdots$$

$$r_{d-1} = x^{p(d-1)} \mod f(x)$$

Con
$$deg(r_i) < d \forall 0 \le i \le d-1$$
.

Definiamo la matrice $A \in Mat_{d \times d}(\mathbb{F}_p)$ nel segueente modo:

 $A_{ij} = \text{coefficiente del termine di grado i del polinomio } r_j(x)$

ESEMPIO. Considerando l'esempio precedente, si ha:

$$A \in Mat_{5 \times 5}(\mathbb{F}_3) = \begin{bmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 \end{bmatrix}$$

la matrice A-I è la matrice del sistema che abbiamo risolto, ossia $(A-I)\overrightarrow{b}=\overrightarrow{0}$

TEOREMA 1.17. Il numero di fattori irriducibili k nella fattorizzazione di f è uguale alla dimensione del nucleo di A-I. Ossia:

$$k = d - rk(A - I)$$

(dove il rango è calcolato sul campo \mathbb{F}_{p}).

DIMOSTRAZIONE. Osserviamo innanzitutto che $dim(Ker(A-I)) \ge 1$.

Infatti la d-tupla $(b_0, 0, \dots, 0)$ è sempre soluzione del sistema $\forall b_0 \in \mathbb{F}_p$.

Abbiamo visto che l'Insieme

$$H = \{ h \in \mathbb{F}_p[x] : deg(h) < d, f \mid h^p - h \}$$

è uno spazio vettoriale su \mathbb{F}_p isomorfo a Ker(A-I).

Sia k il numero di fattori irriducibili non banali di f, aventi tutti molteplicità 1.

Dimostriamo che \mathbb{F}_n^k è isomorfo a H.

Abbiamo già dimostrato che per ogni $(s_1, \ldots s_k) \in \mathbb{F}_p^k$ troviamo un unico elemento di H, usando il Teorema cinese dei resti per l'anello $\mathbb{F}_p[X]$.

Quindi abbiamo definito una funzione $\varphi: \mathbb{F}_p^k \to H$

- a) φ è un morfismo si spazi vettoriali.
- b) φ è iniettiva:

$$Ker(\varphi) = \{(s_1, \dots s_k) \in \mathbb{F}_p^k : s_i \mod p_i = 0, \forall 1 \le i \le k\}$$

= $\{(0, \dots, 0)\}$

c) φ è suriettiva:

Se $h \in H$, abbiamo visto che $h^p - h = h(h-1)(h-2)\dots(h-(p-1))$.

Questi fattori sono coprimi a coppie, quindi se $f|h^p-h$, allora $p_i(x)|(h-s_i)$ per un unico $s_i \in \mathbb{F}_p, \forall 1 \leq i \leq k$.

Quindi h è soluzione del sistema

$$\begin{cases} h \equiv s_1 \bmod p_1 \\ \vdots \\ h \equiv s_k \bmod p_k \end{cases}$$

Abbiamo dimostrato che $\varphi:\mathbb{F}_p^k\to H$ è un isomorfismo do spazi vettoriali, quindi $\mathbb{F}_p^k\simeq H\simeq Ker(A-I)$

$$\mathbb{F}^k \simeq H \simeq Ker(A-I)$$

ossia dim(Ker(A-I)) = k = d - rk(A-I)

ESEMPIO. Sempre considerando l'esempio precedente, si ha che

$$\underbrace{2}_{\text{fattori irriducibili di }f(x)} = \underbrace{5}_{\text{grado di }f(x)} - rk(A-I)$$

Se $f \in \mathbb{F}_p[x]$ ha fattori irriducibili di molteplicità > 1, procediamo come segue:

Abbiamo che $D = MCD\{f, f'\} \neq 1$.

Osserviamo che il polinomio $\frac{f}{D}$ ha fattori irriducibili tutti di molteplicità 1. Infatti se p_1,\dots,p_k sono tutti distinti

$$f' = (p_1^{e_1}(x) \dots p_k^{e_k}(x))' = e_1 p_1^{e_1 - 1} p_1' p_2^{e_2} \dots p_k^{e_k} + \dots + e_k p_1^{e_1} p_2^{e_2} \dots p_k^{e_k - 1} p_k'$$

e
$$D = p_1^{e_1-1} \dots p_k^{e_k-1}$$
 quindi $\frac{f}{D} = p_1 \dots p_k$.

Allora fattorizziamo $\frac{f}{D}$ poi fattorizziamo D, eventualmente ripetendo con D, D'.

Finché non otteniamo $MCD\{D_i, D_i'\} = 1$.

1.10 Rango di un tensore

Ogni elemento di $V_1 \otimes V_2 \otimes \ldots \otimes V_h$ si scrive come combinazione lineare di tensori di rango 1. Infatti la base $\{v_{j_1}^1 \otimes v_{j_2}^2 \otimes \ldots \otimes v_{j_h}^h\}$ è costituita da tensori di rango 1.

DEFINIZIONE 1.18 — Rango di un tensore. Sia $T \in V_1 \otimes V_2 \otimes ... \otimes V_k$. definiamo rango di T e lo indichiamo rk(T) il minimo $r \in \mathbb{N}$ tale che:

$$T = \sum_{i=1}^{r} T_i$$

 $\sum_{i=1}$ dove $T_i \in V_1 \otimes V_2 \otimes \ldots \otimes V_k$ sono di rango 1 $\forall \, 1 \leq i \leq r.$

ESEMPIO. Sia U con base $\{u_1, u_2\}$, V con base $\{v_1, v_2\}$ e W con base $\{w_1, w_2\}$.

- $T: u_1 \otimes v_1 \otimes w_1 + u_1 \otimes v_2 \otimes w_1 \in U \otimes V \otimes W$ ha rango 1. infatti $T = u_1 \otimes (v_1 + v_2) \otimes w_1$.
- $T: u_1 \otimes v_1 \otimes w_1 + u_2 \otimes v_2 \otimes w_1$ ha rango 2. Infatti l'unica fattorizzazione possibile è $T = (u_1 \otimes v_1 + u_2 \otimes v_2) \otimes w_1$ che non è un tensore di rango 1.
- $T = u_1 \otimes v_1 \otimes w_1 + u_2 \otimes v_2 \otimes w_2 \in U \otimes V \otimes W$ ha rango 2.

Poiché $dim(\bigotimes_{i=1}^h V_i) = \prod_{i=1}^h dim(V_i)$, abbiamo che, se $T \in \bigotimes_{i=1}^h V_i$ allora $rk(T) \leq \prod_{i=1}^h dim(V_i)$, poiché $\bigotimes_{i=1}^h V_i$ ha una base fatta di tensori di rango 1.

Ora verifichiamo che la nozione di rango di un Tensore è coerente con quella di rango di una matrice interpretando una matrice come forma bilineare, e quindi come un tensore.

Vediamo subito che una matrice di rango 1 corrisponde ad un tensore di rango 1.

Una matrice $m \times n$ di rango 1 h come colonne multipli di un vettore $v \in K^m \setminus \{0\}$.

La prima colonna sia a_1v , la seconda $a_2v, \ldots, a_nv, a_i \in K$.

Quindi tale matrice di rango 1 si scrive come

$$A = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix} = \overrightarrow{v} \overrightarrow{a}^T$$

Come forma bilineare è il seguente elemento di $(K^m)^* \otimes (K^n)^*$:

$$v_1 a_1 e_1^* \otimes e_1^* + v_2 a_1 e_2^* \otimes e_1^* + \dots + v_1 a_2 e_1^* \otimes e_2^* + v_2 a_2 e_2^* \otimes e_2^* + \dots + v_1 a_n e_1^* \otimes e_n^* + \dots + v_m a_n e_m^* \otimes e_n^* = \\ = (v_1 e_1^* + \dots + v_m e_m^*) \otimes a_1 e_1^* + (v_1 e_1^* + \dots + v_m e_m^*) \otimes a_2 e_2^* + \dots + (v_1 e_1^* + \dots + v_m e_m^*) \otimes a_n e_n^* = \\ = (v_1 e_1^* + \dots + v_m e_m^*) \otimes (a_1 e_1^* + \dots + a_n e_n^*)$$

Dunque una matrice $A \in Mat_{m \times n}(K)$ tale che rk(A) = 1 corrisponde ad un tensore $T_A \in (K^m)^* \otimes (K^n)^*$ tale che $rk(T_A) = 1$.

ESEMPIO. La matrice

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 0 & 1 \end{pmatrix} \in Mat_{2\times 3}(\mathbb{F}_3)$$

Ha rango 1 perchè $\binom{2}{1}=2\binom{1}{2}$ in $(\mathbb{F}_3)^2.$

Ad A corrisponde la forma bilineare $T_A:(\mathbb{F}_3)^2\times(\mathbb{F}_3)^3\to\mathbb{F}_3$ definita da

$$T_A(u,v) = u^T A v$$
 $\forall u \in (\mathbb{F}_3)^2, v \in (\mathbb{F}_3)^3$ $(u^T$ è il trasposto del vettore colonna u)

come elemento di $(\mathbb{F}_3^2)^* \otimes (\mathbb{F}_3^3)^*$ si scrive

$$T_A = e_1^* \otimes e_1^* + 2e_2^* \otimes e_1^* + 2e_1^* \otimes e_3^* + e_2^* \otimes e_3^*$$
$$= (e_1^* + 2e_2^*) \otimes e_1^* + (2e_1^* + e_2^*) \otimes e_3^*$$
$$= (e_1^* + 2e_2^*) \otimes (e_1^* + e_3^*)$$

D'altra parte avevamo che $A=\begin{pmatrix}1&0&2\\2&0&1\end{pmatrix}=\begin{pmatrix}1\\2\end{pmatrix}\begin{pmatrix}1&0&2\end{pmatrix}$ sul campo \mathbb{F}_3

Ovviamente ad un Tensore di rango 1 $v_1 \otimes v_2 \in (K^m)^* \otimes (K^n)^*$ corrisponde una matrice di rango 1 $v_1v_2^T \in Mat_{m \times n}(K)$ dove v_i sono i vettori colonna delle coordinate nella base duale.

ESEMPIO. Sia $(2e_1^* + 3e_2^*) \otimes (e_2^* + 4e_3^*) \in (\mathbb{F}_5^2)^* \otimes (\mathbb{F}_5^3)^*$. La matrice corrispondente è

$$\begin{pmatrix} 2\\3 \end{pmatrix}\begin{pmatrix} 0 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 3\\0 & 3 & 2 \end{pmatrix} \in Mat_{2\times 3}(\mathbb{F}_5)$$

Quindi abbiamo dato una corrispondenza biunivoca tra matrici di rango $1 \in Mat_{m \times n}(K)$ e tensori di rango $1 \in (K^m)^* \otimes (K^n)^*$.

Dalla caratterizzazione del rango di una matrice in termini di combinazioni lineari di matrici di rango 1, e dalla definizione di rango di un tensore, segue che le matrici di rango r in $Mat_{m\times n}(K)$ stanno in corrispondenza con i tensori di rango r in $(K^m)^*\otimes (K^n)^*$.

Capitolo 2

Logica modale

Sintassi della logica modale e semantica di Kripke 2.1

Introduciamo il linguaggio della logica proposizionale. L'alfabeto è costituito da:

- 1. Insieme numerabile di variabili
- 2. Connettivi logici: \neg, \land, \lor

le parole del linguaggio possono essere:

- 1. Un Letterale: variabile x o la sua negazione $\neg x$
- 2. Una Clausola: disgiunzione finita di letterali $l_1 \vee \ldots \vee l_n$
- 3. Una Formula CNF (forma normale congiuntiva): congiunzione finita di clausole $C_1 \wedge \ldots \wedge C_n$ Per ogni letterale L definiamo

$$\overline{L} = \begin{cases} \neg x & \text{se } L \ge x \\ x & \text{se } L \ge \neg x \end{cases}$$

Indichiamo con VAR(F) l'insieme delle variabili che appaiono in una formula CNF F.

Useremo anche le parentesi (,) come simboli ausiliari per rendere chiara la lettura delle formule

Еѕемрю. $(\neg x_1 \lor x_2) \land x_1 \land (x_2 \lor x_3)$ è una formula CNF. Chiamiamola F. Allora VAR(F) =

Le clausole di Fsono $\{\neg x_1 \vee x_2, x_1, x_2 \vee x_3\}$ e i letterali di Fsono $\{x_1, x_2, x_3, \neg x_1\}$

2.1.1Semantica

Definizione 2.1 — Assegnazione appropriata. Sia F una formula CNF. Una assegnazione

$$V: X \to \{0, 1\}$$

dove $X \supseteq VAR(F)$.

L'insieme {0,1} è l'insieme dei valori di verità di F e può essere interpretato come {falso, vero}.

DEFINIZIONE 2.2 — Soddisfacibilità. Sia F una formula e V un'assegnazione appropriata a F. Diciamo che **V soddisfa F**, scritto $V \vDash F$, se

- 1. <u>F è una variabile X</u>: $V \vDash X$, significa che V(X) = 1
- F è il letterale ¬X: V ⊨ ¬X, significa che V(X) = 0
 F è una clausola L₁ ∨ ... ∨ L_n: V ⊨ F, significa che V soddisfa almeno uno dei letterali L_i

4. \underline{F} è una congiunzione di clausole $C_1 \wedge \ldots \wedge C_n$: $V \models F$, significa che V soddisfa tutte le clausole C_i

In questo modo abbiamo dato un significato al linguaggio definito precedentemente.

Se V non soddisfa F, scriveremo $V \nvDash F$.

ESEMPIO. Sia F la formula CNF $(\neg x_1 \lor x_2) \land x_1 \land (x_2 \lor x_3)$ e sia $U : \{x_1, x_2, x_3\} \rightarrow \{0, 1\}$ tale che $U(x_1) = U(x_2) = 1, U(x_3) = 0.$

Dunque

$$U(\neg x_1) = 0$$

$$U(\neg x_1 \lor x_2) = 1$$

$$U(x_2 \lor x_3) = 1$$

$$U(F) = 1$$

Quindi $U \models F$.

Sia $V: \{x_1, x_2, x_3\} \to \{0, 1\}$ tale che $V(x_1) = 1, V(x_2) = V(x_3) = 0$.

Allora

$$V(\neg x_1) = 0$$

$$V(\neg x_1 \lor x_2) = 0$$

$$V(x_2 \lor x_3) = 0$$

$$V(F) = 0$$

quindi $V \nvDash F$.

DEFINIZIONE 2.3 — Formula soddisfacibile. Diciamo che una formula è soddisfacibile se esiste un'assegnazione $V: VAR(F) \to \{0,1\}$ che la soddisfa $(V \vdash F)$.

Altrimenti è insoddisfacibile.

La formula dell' esempio precedente è soddisfacibile, $x \wedge \neg x$ è insoddisfacibile.

Definizione 2.4 — **Tautologia.** Una formula F è una **tautologia** se per ogni assegnazione V si ha $V \models F$.

La formula $x \vee \neg x$ è una tautologia, la formula dell' esempio precedente no

DEFINIZIONE 2.5 — Conseguenza logica. Date due formule F, G diciamo che G è conseguenza logica di F, se per ogni assegnazione V appropriata ad entrambe si ha che $V \models F \implies V \models G$.

Esempio. La formula y è conseguenza logica della formula $F := (\neg x \lor y) \land x$.

Infatti l'unica assegnazione che soffisfa F è $x \to 1, y \to 1$.

Tale assegnazione soddisfa anche y.

DEFINIZIONE 2.6 — Implicazione logica. Definiamo l'implicazione logica tra due formule F, G

come

Definizione 2.7 — Equivalenza logica. Due formule F, G sono logicamente equivalenti se F è conseguenza logica di G e G è conseguenza logica di F. In tal caso scriviamo $F \equiv G$.

Esempio. Nell'esempio precedente abbiamo visto che y è conseguenza logica di $F:=(\neg x\vee y)\wedge x,$ che possiamo ricrivere come $(x \implies y) \land x$.

Poiché $x \mapsto 0, y \mapsto 1$ soddisfa y ma non F, abbiamo che F non è conseguenza logica di y.

ESEMPIO.

- $l_1 \vee l_2 \equiv l_2 \vee l_1$ (la disgiunzione è commutativa)
- $c_1 \wedge c_2 \equiv c_2 \wedge c_1$ (la congiunzione è commutativa)
- $c \wedge c \equiv c \in l \vee l \equiv l$ (congiunzione e disgiunzione sono idempotenti)

Diamo altre definizioni:

DEFINIZIONE 2.8 — Doppia implicazione.

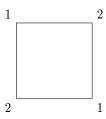
$$x \iff y := (x \implies y) \land (y \implies x)$$

Definizione 2.9 — Negazione di formule CNF. 1. l letterale: $\neg l = \overline{l}$ 2. $\neg (l_1 \lor \ldots \lor l_n) := \neg l_1 \land \ldots \land \neg l_n$ 3. $\neg (c_1 \land \ldots \land c_n) := \neg c_1 \lor \ldots \lor \neg c_n$

L'interpretazione di questa definizione di negazione è quella corretta grazie alle leggi di De Morgan e alla proprietà distributiva di \vee e \wedge .

ESEMPIO. Consideriamo il problema di colorare i vertici di un quadrato con due colori in modo che i vertici su uno stesso lato abbiano colori diversi.

Tale problema ha ovviamente una soluzione:



Formuliamo il problema come una formula CNF.

Potremo così dire che il problema è soddisfacibile se e solo se tale formula CNF è soddisfacibile. x_{ij}

indica "il vertice i ha colore j" $\forall 1 \leq i \leq 4, 1 \leq j \leq 2$

$$F := (x_{11} \lor x_{12}) \land (x_{21} \lor x_{22}) \land (x_{31} \lor x_{32}) \land (x_{41} \lor x_{42}) \land \\ \land (\neg x_{11} \lor \neg x_{12}) \land (\neg x_{21} \lor \neg x_{22}) \land (\neg x_{31} \lor \neg x_{32}) \land (\neg x_{41} \lor \neg x_{42}) \land \\ \land (\neg x_{11} \lor \neg x_{21}) \land (\neg x_{12} \lor \neg x_{22}) \land (\neg x_{21} \lor \neg x_{31}) \land (\neg x_{22} \lor \neg x_{32}) \land (\neg x_{31} \lor \neg x_{41}) \end{cases}$$

l'assegnazione $x_{11}\mapsto 1, x_{12}\mapsto 0, x_{21}\mapsto 0, x_{22}\mapsto 1, x_{31}\mapsto 1, x_{32}\mapsto 0, x_{41}\mapsto 0, x_{42}\mapsto 1$ soddisfa F

2.1.2 Sintassi

La logica modale è una estensione della logica proposizionale.

L'alfabeto è quello della logica proposizionale a cui si aggiungono i connettivi modali:

- 1. Un insieme numerabili di variabili (o formule atomiche)
- 2. I connettivi logici $\neg, \land, \lor, \Longrightarrow, \iff$
- 3. I simboli ausiliari (,)
- 4. I connettivi modali □ (Scatola o Box) e ♦ (Diamante o Diamond)

Le parole del lingiaggio sono le formule ben formate (FBF) definite in modo ricorsivo:

- 1. Ogni variabile è una FBF
- 2. Se A è una FBF, allora $\neg A$, $\Box A$, $\Diamond A$ sono FBF
- 3. Se A, B sono FBF, allora $(A \wedge B)$, $(A \vee B)$, $(A \Longrightarrow B)$, $(A \Longleftrightarrow B)$ sono FBF

Alcune letture dei simboli \square e \diamond :

• La lettura piu comune è: $\Box A$:"è necessario che A", $\Diamond A$: "è possibile che A". Secondo questa lettura i connettivi modali possono essere definiti uno in termini dell'altro:

$$\Box A \equiv \neg \diamondsuit \neg A$$
$$\diamondsuit A \equiv \neg \Box \neg A$$

- Logiche modali epistemiche: $\Box A$: "si sa che A"
- Logiche modali deonetiche: $\Box A$: "è obbligatorio che A"
- Logiche modali doxastiche: $\Box A$: "si crede che A"
- Logica modale dimostrativa: $\Box A$: "è dimostrabile che A"

Come abbiamo visto, la logica proposizionale è una logica vero-funzionale: assegnando valori "0" e "1" alle variabili possiamo assegnare un valore "0" o "1" ad una formula in modo univoco, che corrisponde alla nostra inutizione di negazione, disgiunzione, congiunzione.

Per la logica modale la situazione è più complicata.

Interpretando il simbolo "□" come operatore di necessità, ossia "♦" come operatore di possibilità, possiamo essere, ad esempio, d'accordo che le formule

$$\Box A \implies \Diamond A, \quad A \implies \Diamond A$$

siano vere, ma è vera la formula

$$A \Longrightarrow \Box \Diamond A$$
 ?

Non è chiaro se sia vera o falsa. Nel caso della logica epistemica, l'operatore " \square " si indica di solito con "K" (da "knowledge").

In questo contesto, la formula $KA \implies A$ (se si sa che A allora A vale) sembra dover essere vera.

Invece la formula $A \implies KA$ (se vale A allora si sa che A) sembra essere falsa perchè non si è onniscenti.

2.1.3 Semantica dei mondi possibili (semantica di Kripke)

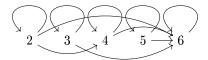
DEFINIZIONE 2.10 — Frame. Un Frame è una coppia (S, R), dove S è un insieme non vuoto detto insieme dei mondi e $R \subseteq S \times S$ è una relazione su S, detta relazione di accessibilità (se $(x, y) \in R$ si dice che y è accessibile da x).

Un Frame può essere rappresentato con un grafo diretto con cappi (loop) i cui vertici sono gli elementi dell'insieme S e ho una freccia da x a y se $(x,y) \in R$.

ESEMPIO. Il frame (\mathbb{N}, R) , dove $R = \{(n, n+1) : n \in \mathbb{N}\} \subseteq \mathbb{N} \times \mathbb{N}$ è rappresentato dal seguente grafo diretto:

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow \cdots$$

ESEMPIO. Il frame (S,R) dove $S=\{2,3,4,5,6\}$ e $R=\{(x,y)\in S\times S: x$ divide $y\}$ è rappresentato dal seguente grafo diretto:



ESEMPIO. Il frame $(\{1,2,3\},R)$ dove $R=\{(x,y)\in\{1,2,3\}\times\{1,2,3\}:y=f(x)\}$ essedo $f:\{1,2,3\}\to\{1,2,3\}$ la funzione definita da f(1)=2,f(2)=3,f(3)=1 è

$$1 \stackrel{\frown}{\sim} 2 \stackrel{\frown}{\sim} 3$$

DEFINIZIONE 2.11 — Modello. Un modello su un frame (S,R) è una terna (S,R,V) dove $V:Var \to \mathcal{P}(S)$, ci dice in quali mondi le variabili valgono 1 è detta funzione di valutazione.

Definizione 2.12. Una formula F si dice **Vera in un mondo x del modello M** e scriviamo $M \vDash_x F$ se e solo se:

- 1. F è una variabile: $M \vDash_x F$ significa che $x \in V(F)$
- 2. F è $\neg y$ e y è una variabile: $M \vDash_x F$ significa che $x \notin V(y)$
- 3. F è del tipo $\neg G$, dove G è una formula: $M \vDash_x F$ significa che $M \nvDash_x G$
- 4. F è del tipo $G_1 \wedge G_2$: $M \vdash_x F$ significa che $M \vdash_x G_1$ e $M \vDash_x G_2$
- 5. F è del tipo $G_1 \vee G_2$: $M \vdash_x F$ significa che $M \vdash_x G_1$ o $M \vDash_x G_2$
- 6. Fè del tipo $\Box G$: $M \vDash_x F$ significa che $M \vDash_y G$, per ogni $y \in S : (x,y) \in R$, ossia per ogni mondo y raggiungibile da x.
- 7. F è del tipo $\Diamond G$: $M \vDash_x F$ significa che $M \vDash_y G$ per qualche $y \in S : (x, y) \in R$, ossia per almeno un mondo raggiungibile da x.

DEFINIZIONE 2.13 — Soddisfacibilità. Una formula F è soddisfacibile se esiste un modello M = (S, R, V) e un mondo $x \in S$, tali che $M \vDash_x F$.

TEOREMA 2.14. Se una formula modale F è soddisfacibile, allora è soddisfacibile in una struttura di Kripke (S,R) tale che $|S| \leq 2^{|F|}$, |F| ="lunghezza di F".

Quindi il problema di soddisfacibilità di una formula modale è decidibile.

2.2 Esprimibilità della proprietà riflessiva

TEOREMA 2.15. Lo schema $\Box A \implies A$ è valido in un frame (S, R) se e solo se R è riflessiva.

DIMOSTRAZIONE. perché sia sempre vera la formula $\Box x \implies x$, la relazione R del frame deve essere riflessiva, ossia $(y,y) \in R \forall y \in S$.

Infatti, se R non fosse riflessiva ci sarebbe un mondo $y \in S$ tale che $(y, y) \notin R$.

Sia $Z=V(x), Z\subseteq S$, tale che $y\notin Z$ (cioè x è falsa nel mondo y).

Sia $Z\supseteq\{z\in S:(y,z)\in R\}$ cio
è x sia vera in tutti i mondi accessibili da y.

Allora se $M = (S, R, V), M \vDash_y \Box x$ ma $M \nvDash_y x$.

2.3 Esprimibilità della proprietà simmetrica

Teorema 2.16. Lo schema $A \implies \Box \Diamond A$ è valido in un frame (S,R) se e solo se R è simmetrica.

DIMOSTRAZIONE. Sia R simmetrica, ossia $(x,y) \in R \implies (y,x) \in R$.

Sia $M \vDash_w A$ e $(w,v) \in R$. Dunque $(v,w) \in R$ e $M \vDash_v \Diamond A \forall v \in S$ t.c. $(w,v) \in R$, ossia $M \vDash_w \Box \Diamond A$.

Adesso assumiamo che lo schema $A \implies \Box \Diamond A$ sia valido in (S, R).

Sia x una variabile e $V(X) = \{s\};$

sia $t \in S$ t.c. $(s,t) \in R$. Quindi $M \vDash_s X$.

Dalla validità dello schema segue allora che $M \vDash_s \Box \Diamond X$, da cui $M \vDash_t \Diamond X$.

Quindi esiste $r \in S$ t.c. $(t,r) \in ReM \vDash_r x,$ ossia r = s

2.4 Esprimibilità della proprietà transitiva

Teorema 2.17. Lo schema $\Box A \Longrightarrow \Box \Box A$ è valido in un frame (S,R) se e solo se R è transitiva.

Dimostrazione. Sia R transitiva, ossia $(x,y) \in R, (y,z) \in R \implies (x,z) \in R.$

Sia $M \vDash_w \Box A$, ossia $M \vDash_v A \forall v \in S \text{ t.c. } (w, v) \in R$.

Sia $u \in S$ t.c. $(v, u) \in R$, con $(w, v) \in R$.

Allora $(w, u) \in R$ e quindi $M \vDash_v \Box A, \forall v \in S$ t.c. $(w, v) \in R$, ossia $M \vDash_w \Box \Box A$.

Assumiamo adesso che sia valido lo schema $\Box A \implies \Box \Box A$ su un frame (S, R).

Sia x una variabile, $s \in S$ e $V(x) = \{w \in S : (s, w) \in R\}$.

Allora $M \vDash_s \Box x$ e quindi per la validità dello schema, $M \vDash_s \Box \Box x$, da cui $M \vDash_t \Box x \forall t \in S$ t.c. $(s,t) \in R$, ossia $M \vDash_r x \forall r \in S$ t.c. $(t,r) \in R$, $(s,t) \in R$.

Da ciò segue che $r \in V(x)$ ossia $(s,t) \in R$ e $(t,r) \in R \implies (s,r) \in R$

2.5Morfismi di modelli + Lemma 1

DEFINIZIONE 2.18 — Morfismo di Frame. Siano (S_1, R_1) e (S_2, R_2) due frame. una funzione f: $S_1 \to S_2$ è un morfismo di frame se:

$$(x,y) \in R_1 \implies (f(x), f(y)) \in R_2 \qquad \forall x, y \in S_1$$

ESEMPIO. Siano (\mathbb{N}, R_1) e (\mathbb{N}, R_2) i frame tali che

$$R_1 = R_2 = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x < y\}$$

allora la funzione

$$f: \mathbb{N} \to \mathbb{N}$$
$$n \mapsto n^2$$

è un morfismo di frame.

DEFINIZIONE 2.19 — Morfismo di modelli. siano $M_1 = (S_1, R_1, V_1)$ e $M_2 = (S_2, R_2, V_2)$ due modelli.

Un morfismo di frame $f:(S_1,R_1)\to (S_2,R_2)$ è un morfismo di modelli se:

- 1. $w \in V_1(x) \iff f(w) \in V_2(x) \ \forall w \in S_1, x \in Var$ 2. $(f(w), y) \in R_2 \implies \exists v \in S_1 t.c.(w, v) \in R_1, f(v) = y \ \forall w \in S_1, y \in S_2$

Nota. I morfismi di modelli sono solitamente detti p-morfismi.

ESEMPIO. Siano $M_1 = (\mathbb{N}, R_1, V_1)$ e $M_2 = (\{0, 1\}, \{0, 1\}, V_2)$ dove $R_1 = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x \leq 1\}$ y}, $Var = \{x\} \in V_1(x) = \{2n : n \in \mathbb{N}\}, V_2(x) = \{0\}$. Sia

$$f: \mathbb{N} \to \{0, 1\}$$
$$n \mapsto n \bmod 2$$

Allora f è un morfismo di modelli, infatti:

- 1. $x \le y \implies (x \mod 2, y \mod 2) \in \{0, 1\} \times \{0, 1\}$
- 2. $w \in V_1(x) \iff w \in \{2n : n \in \mathbb{N}\}; \text{ allora } w \in V_1(x) \implies f(w) = 0.$

$$f(w) \in V_2(x) \iff f(w) = 0$$
; allora $f(w) \in V_2(x) \implies w \in V_1(x)$

- 3. $(f(w), y) \in R_2 = \{0, 1\} \times \{0, 1\}$:
 - (a) f(w) = 0: se y = 0 allora $w \le w$ e f(w) = 0 = y.

Se
$$y = 1$$
 allora $w \le w + 1$ e $f(w + 1) = 1 = y$.

(b) f(w) = 1: se y = 0 allora $w \le w + 1$ e f(w + 1) = 0 = y.

Se
$$y = 1$$
 allora $w \le w$ e $f(w) = 1 = y$.

LEMMA 2.20 — Lemma 1. Sia $f:(S_1,R_1,V_1)\to (S_2,R_2,V_2)$ un morfismo dal modello M_1 al modello M_2 . Allora

$$M_1 \vDash_w F \iff M_2 \vDash_{f(x)} F$$

 $\forall w \in S_1 \text{ e ogni formula } F$

DIMOSTRAZIONE. Se F è una variabile allora $M_1 \vDash_w F$ se e solo se $w \in V_1(F)$ se e solo se $f(w) \in V_1(F)$ $V_2(F)$ (per il punto 1 nella definizone di morfismo di modelli) se e solo se $M_2 \vDash_{f(w)} F$.

Per tutti gli altri tipi di formule, si dimostra induttivamente sulla costruzione della formula.

Vediamo dsolo il caso in cui $F = \Diamond G$.

Sia $M_1 \vDash_w \Diamond G$, allora esiste $v \in S_1$ t.c. $(w, v) \in R_1$ e $M_1 \vDash_v G$.

Poiché $(f(w),f(v))\in R_2$ perchè f è un morfismo di modelli e induttivamente $M_2\vDash_{f(v)}G$, allora $M_2\vDash_{f(w)}\diamondsuit G$.

Sia ora $M_2 \vDash_{f(w)} \Diamond G$, allora esiste $u \in R_2$ t.c. $(f(w), u) \in R_2$ e $M_2 \vDash_u G$.

Per la condizione 2 nella definizione di morfismo di modelli, esiste $v \in S_1$ t.c. $(w,v) \in R_1$ e f(v) = u.

Per ipotesi induttiva $M_1 \vDash_v G$, e quindi $M_1 \vDash_w \diamondsuit G$.

2.6 Lemma 2 + Lemma 3 + Lemma 4 + non esprimibilità della proprietà antisimmetria

Lemma 2.21 — **Lemma 2.** Sia $f:(S_1,R_1,V_1)\to (S_2,R_2,V_2)$ un morfismo dal modello M_1 al modello M_2 . se f è suriettiva, allora

$$M_1 \vDash F$$
 se e solo se $M_2 \vDash F$

per ogni formula F.

DIMOSTRAZIONE. $M_1 \vDash F$ se e solo se $M_1 \vDash_w F, \forall w \in S_1$.

Se e solo se $M_2 \vDash_{f(w)} F, \forall w \in S_1$ (per il lemma 1).

Se e solo se $M_2 \models F$, perchè f è suriettivo.

Lemma 2.22 — **Lemma 3.** Sia M_2 un modello su S_2, R_2 e $f: (s_1, R_1) \to (S_2, R_2)$ un morfismo di frame tale che valga la condizione 2 della definizione di morfismo di modelli.

Allora esiste un modello M_1 su S_1, R_1 tale che $f: M_1 \to M_2$ è un morfismo di modelli.

DIMOSTRAZIONE. Basta definire $M_1 = (S_1, R_1, V_1)$ con $V_1(x) = \{w \in S_1 : M_2 \vDash_{f(w)} x\} \forall x \in Var.$

Lemma 2.23 — **Lemma 4.** Sia $f:(S_1,R_1)\to (S_2,R_2)$ un morfismo di frame tale che valga la condizione 2 della definizione di morfismo di modelli.

Se f è suriettivo, si ha $(S_1, R_1) \models F \implies (S_2, R_2) \models F$, per ogni formula F.

DIMOSTRAZIONE. Sia $S_2, R_2 \nvDash F$. Allora esiste un modello M_2 su (S_2, R_2) tale che $M_2 \nvDash F$. Per il lemma 3 esiste un modello M_1 su (S_1, R_1) tale che $f: M_1 \to M_2$ è un morfismo di modelli.

Dato che f è suriettivo, per il lemma 2 si ha $M_1 \nvDash F$, ossia $(S_1, R_1) \nvDash F$.

DEFINIZIONE 2.24 — Relazione antisimmetria. Una relazione R su un insieme X si dice antisimmetrica se

$$(x,y) \in R, (y,x) \in R \implies x = y \qquad \forall x,y \in X$$

Esempio. L'ordinamento \leq dei numeri naturali è una relazione antisimmetrica su \mathbb{N} .

Esempio. La relazione $x \mid y$ su \mathbb{N} è antisimmetrica.

Esempio. La relazione $A \subseteq B$ su $\mathcal{P}(X)$ di un insieme X è antisimmetrica.

Teorema 2.25. L'antisimmetria non è esprimibile, ossia non esiste una formula F tale che $(S, R) \models F$ se e solo se R è antisimmetrica.

DIMOSTRAZIONE. Sia $(S_1, R_1) = (\mathbb{N}, \leq)$ e $(S_2, R_2) = (\{0, 1\}, \{0, 1\} \times \{0, 1\})$.

Nell'esempio di morfismo di modelli abbiamo visto che la funzione

$$f: \mathbb{N} \to \{0, 1\}$$
$$n \mapsto n \bmod 2$$

è un morfismo dal frame (\mathbb{N},\leq) al frame $(\{0,1\},\{0,1\}\times\{0,1\})$ che soffisfa la condizione 2 della definizione di morfismo di modelli.

La relazione \leq su $\mathbb N$ è antisimmetrica.

Supponiamo per assurdo che esista una formula ${\cal F}$ come nell'enunciato del teorema. Allora:

$$(\mathbb{N}, \leq) \vDash F$$

Per il lemma 4 si ha che $(\{0,1\},\{0,1\}\times\{0,1\}) \vDash F$.

Da cui seguirebbe che R_2 è antisimmetrica, il che è falso.

2.7 Logiche modali normali, dimostrazioni, teoremi e validità della logica K

Abbiamo già mostrato che lo schema di formule

$$K: \Box (A \Longrightarrow B) \Longrightarrow (\Box A \Longrightarrow \Box B)$$

è valido, $\vDash K$.

Adesso viediamo che lo schema di formule

$$def_{\Diamond}: \Diamond A \iff \neg \Box \neg A$$

è valido, $\vDash def_{\diamondsuit}$.

DIMOSTRAZIONE. Sia (S, R) un frame, M un modello su (S, R) e $w \in S$.

Allora $M \vDash_w \Diamond A$ se e solo se esiste $v \in St.c.(w,v) \in R$ e $M \vDash_v A$.

 $M \vDash_w \neg \Box \neg A$ se e solo se $M \nvDash_w \Box \neg A$, se e solo se esiste $v \in St.c.(w,v) \in R$ e $M \nvDash_v \neg A$, se e solo se esite $v \in St.c.(w,v) \in R$ e $M \nvDash_v A$.

Abbiamo quindi dimostrato che $\models def_{\diamondsuit}$

DEFINIZIONE 2.26 — **Sostituzione uniforme.** Sia x una variabile e F una formula. Definiamo l'operzione di sostituzione uniforme di F al posto di x in una formula G, indicato come

La formula ottenuta da G dove ogni occorrenza di x è stata sostituita con F.

ESEMPIO. Sia G la formula $\Box x \implies x \land y \in F$ la formula $\Diamond y \iff \neg \Box \neg y$. Allora $G[F/x] = \Box(\Diamond y \iff \neg \Box \neg y) \implies (\Diamond y \iff \neg \Box \neg y) \land y$

DEFINIZIONE 2.27 — Logica Modale Normale. Una logica modale normale è un insieme Γ di formule tale che:

- 1. Γ contiene tutte le tautologie della logica proposizionale
- 2. Γ contiene tutte le istanze dello schema $K: \Box(A \Longrightarrow B) \Longrightarrow (\Box A \Longrightarrow \Box B)$
- 3. Γ contiene tutte le istanze dello schema $def_{\Diamond}: \Diamond A \iff \neg \Box \neg A$
- 4. Γ è chiuso sotto **modus ponens** se $A \in \Gamma$ e $(A \Longrightarrow B) \in \Gamma$, allora $B \in \Gamma$
- 5. Γ è chiuso sotto **necessitazione** se $A \in \Gamma$, allora $\Box A \in \Gamma$
- 6. Γ è chiuso sotto sostituzione uniforme se $A \in \Gamma$, allora $A[B/x] \in \Gamma$

ESEMPIO. Se (S,R) è un frame, $\{F:(S,R) \models F\}$ è una logica normale.

ESEMPIO. $\{F : \models F\}$ è una logica normale.

ESEMPIO. Se M è un modello su un frame (S,R), $\{F: M \models F\}$ NON è una logica normale.

DEFINIZIONE 2.28 — Logica Modale K. La logica modale K è definita dai seguenti schemi di assioni e regole:

1. Schemi di assiomi:

- (a) Tutte le tautologie della logica proposizionale
- (b) $K: \Box(A \Longrightarrow B) \Longrightarrow (\Box A \Longrightarrow \Box B)$
- (c) $def_{\diamondsuit} : \diamondsuit A \iff \neg \Box \neg A$
- 2. Regole di inferenza:
 - (a) Modus ponens
 - (b) Necessitazione
 - (c) Sostituzione uniforme

Definizione 2.29 — Dimostrazione in una logica modale. Data una logica modale L una dimostrazione in L è una successione finita di formule tali che ognuna di esse o è un assioma o è ottenuta da formule precedenti tramite una regola di inferenza

DEFINIZIONE 2.30 — Teorema di una logica modale. Una formula F si dice teorema di L, scritto $\vdash_L F$ se e solo se esite una dimostrazione in L in cui la ultima formula è F

Esempio. $\Box(A \land B) \implies \Box A$ è un teorema della logica K:

- 1. $\vdash_K A \land B \implies A$ (Tautologia)
- 2. $\vdash_K \Box (A \land B \implies A)$ (Necessitazione)
- 3. $\vdash_K \Box (A \land B \implies A) \implies (\Box (A \land B) \implies \Box A)$ (K)
- 4. $\vdash_K \Box(A \land B) \implies \Box A \text{ (Modus Ponens)}$

Quindi la logica basata su principi episistemici che abbiamo considerato ragionevoli si supporta su frame che sono relazioni di equivalenza.

DEFINIZIONE 2.31 — Logica Valida. Una logica L è valida (sound) se

$$\vdash_L A \implies \models A$$

Теоrема 2.32. La logica K è valida.

DIMOSTRAZIONE. Sia B_1, B_2, \dots, B_n una dimostrazione di A in K, con $B_n \equiv A$.

 B_1 è valida perchè è un assioma.

Se i > 1, allora B_i è un assioma o è ottenuta da formule precedenti tramite necessitazione o modus ponens.

- 1. $\vdash_K B_j$, per induzione $\vDash B_j$ e allora $\vDash \Box B_j$, quindi $B_i = \Box B_j$ è valida.
- 2. $\vdash_K B_j, \vdash_K B_h$ dove $B_h \equiv B_i \implies B_i$. Allora per induzione $\vDash B_j, \vDash B_j \implies B_i$ e quindi $\vDash B_i$

DEFINIZIONE 2.33 — Logica Completa. Una logica L è completa se

$$\models A \implies \vdash_L A$$

TEOREMA 2.34. La logica K è completa.

DIMOSTRAZIONE. vedee cap.4 "Corso di Logica modale proposizionale"