Appunti di

Logica e Algebra 2

Dagli appunti del professor Paolo Sentinelli

Autori
Pietro Pizzoccheri
Lorenzo Bardelli

Document formatting by
Luca Zani

Politecnico di Milano
A.Y. 2024/2025

Document created on 8 gennaio 2025

Developed by:
Luca Zani
Pietro Pizzoccheri
Lorenzo Bardelli

Indice

Capitolo 1

Teoria degli anelli commutativi e dei campi

1.1 Insiemi

Un insieme è una collezione di oggetti, detti elementi dell'insieme.

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\} \qquad \text{(Naturali)}$$

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \qquad \text{(Interi)}$$

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\} \qquad \text{(Razionali)}$$

$$\mathbb{R} = \{x \mid x \text{ is a real number}\} \qquad \text{(Reali)}$$

$$\mathbb{C} = \left\{ a + bi \mid a, b \in \mathbb{R}, i^2 = -1 \right\} \qquad \text{(Complessi)}$$

1.1.1 Operazioni tra insiemi

- $\subseteq$ (Inclusione tra insiemi)
- $\subsetneq$ (Inclusione propria tra insiemi)

$X \subseteq Y$ si legge X è sottoinsieme di Y o X è incluso in Y.

Se X è un insieme finito, indico con $|X|$ il numero di elementi di X, detto anche la **cardinalità di** X.

Definizione 1.1 — Insieme vuoto. L'insieme $\varnothing$ è l'insieme che non contiene alcun elemento. $\varnothing = \{\}$ e $|\varnothing| = 0$

Definizione 1.2 — Prodotto Cartesiano. Siano X e Y due insiemi. L'insieme $X \times Y := \{(x, y) : x \in X, y \in Y\}$ lo chiamiamo **prodotto cartesiano** di X e Y.

Definizione 1.3 — Insieme delle parti. Sia $A \in \mathcal{P}(x)$, dove $\mathcal{P}(X) := \{A : A \subseteq X\}$ è detto **Insieme delle parti di** X

Definizione 1.4 — Complementare. L'insieme $A^{\mathrm{C}} := X \setminus A$ è detto **complementare** di A

1.2 Funzioni

Siano X e Y due insiemi. **Una funzione** f **da** X **a** Y è un sottoinsieme $F \subseteq X \times Y$ tale che:

- $(x, y_1) \in F$, $(x, y_2) \in F \implies y_1 = y_2$, $\forall\, x \in X$, $y_1, y_2 \in Y$.
- $x \in X \implies \exists\, y \in Y$ tale che $(x, y) \in F$

Una funzione $F \subseteq X \times Y$ la indichiamo con $f : X \to Y$. E scriviamo $f(x) = y$ se $(x, y) \in F$.

Definizione 1.5 — Funzione identità. La funzione $Id_x : X \to X$ tale che $Id_x(x) = x, \forall\, x \in X$ la chiamiamo **funzione identità su** X

Definizione 1.6 — Funzione iniettiva. Una funzione $f : X \to Y$ è **iniettiva** se $\forall\, x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2$

Definizione 1.7 — Funzione suriettiva. Una funzione $f : X \to Y$ è **suriettiva** se $Im(f) = Y$, dove $Im(f) = \{y \in Y : \exists\, x \in X \text{ tale che } f(x) = y\}$ è detta **immagine di** f

Definizione 1.8 — Funzione biunivoca. Una funzione $f : X \to Y$ è **biunivoca** se è sia iniettiva che suriettiva.

1.2.1 Composizione di funzioni

Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni. La **composizione di** f **e** g è la funzione $g \circ f : X \to Z$ tale che $(g \circ f)(x) = g(f(x))$, $\forall\, x \in X$.

Definizione 1.9 — Funzione invertibile. una funzione $f : X \to Y$ è detta **invertibile** se esiste una funzione $g : Y \to X$ tale che

- $g \circ f = Id_X$
- $f \circ g = Id_Y$

la funzione g è detta **funzione inversa di** f e la indichiamo con f^{-1}.

Osservazione. Una funzione $f : X \to Y$ è invertibile se e solo se è biunivoca.

1.2.2 Operazioni su insiemi

Definizione 1.10 — Operazione. Una funzione $f : X \times X \to X$ è detta **operazione su** X. Invece di $f(x, y)$ scriveremo $x \cdot y$.

Definizione 1.11 — Operazione associativa. Un'operazione $\cdot$ su X è detta **associativa** se $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\forall\, x, y, z \in X$.

Definizione 1.12 — Operazione commutativa. Un'operazione $\cdot$ su X è detta **commutativa** se $x \cdot y = y \cdot x$, $\forall\, x, y \in X$.

Esempio.

- $\mathcal{P}(X)$con l'operazione di unione $\cup$ è associativa e commutativa, così come lo è con l'intersezione $\cap$.
- $A \backslash B := A \cup B^C$ **(differenza insiemistica)** è un'operazione su $\mathcal{P}(X)$.
  non è associativa: sia $A \neq \varnothing$. Allora $A \backslash (A \backslash A) = A \neq (A \backslash A) \backslash A = \varnothing$
  non è commutativa: $A \backslash \varnothing = A \neq \varnothing \backslash A = \varnothing$, se $A \neq \varnothing$
- $A \Delta B := (A \backslash B) \cup (B \backslash A)$ **(differenza simmetrica)** è un'operazione su $\mathcal{P}(X)$.
  è commutativa e anche associativa, facilmente verificabile coi diagrammi di Venn.

- Sia $F(X) := \{f : X \to X\}$.
  La composizione" $\circ$" è un'operazione su $F(X)$.
  è associativa, ma non è commutativa.
- $a \circ b = \frac{a+b}{2}$ è un'operazione commutativa su $\mathbb{Q}$, ma non associativa.

Definizione 1.13 — Identità. Sia $\cdot$ un'operazione su X. Un elemento $e \in X$ tale che $e \cdot x = x \cdot e = x$, $\forall x \in X$ è detto **elemento neutro** o **identità**.

L'identità è unica; se $e, e' \in X$ sono due identità, allora $e = e \cdot e' = e'$.

1.3 Monoidi e Gruppi

Definizione 1.14 — Monoide. Un insieme X con un'operazione associativa e un'identità è detto **monoide**.

Esempio.

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con l'addizione e identità 0 sono monoidi.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con la moltiplicazione e identità 1 sono monoidi.
- $\mathcal{P}(X)$ con $\cup$ e come identità l'insieme X è un monoide.
- $\mathcal{P}(X)$ con $\cap$ e come identità l'insieme vuoto è un monoide.
- $F(X) := \{f : X \to X\}$ con la composizione" $\circ$ "e come identità la funzione identità (Id_X) è un monoide.

Definizione 1.15 — Inverso. Sia X un monoide. Un elemento $x \in X$ è detto **invertibile** se esiste $y \in X$ tale che $x \cdot y = y \cdot x = e$, dove e è l'identità di X. L'elemento y è detto **inverso** di x.

Se $x \in X$ è invertibile, il suo inverso è unico e lo indichiamo con x^{-1}.

Osservazione. L'identità del monoide è invertibile e il suo inverso è l'identità stessa.

Esempio.

- L'insieme degli elementi invertibili di $(\mathbb{N}, +)$ è $\{0\}$.
- L'insieme degli elementi invertibili di $(\mathbb{Z}, +)$ è $\mathbb{Z}$, di $(\mathbb{Q}, +)$ è $\mathbb{Q}$, di $(\mathbb{R}, +)$ è $\mathbb{R}$, di $(\mathbb{C}, +)$ è $\mathbb{C}$.
- L'insieme degli elementi invertibili di $(\mathbb{N}, \cdot)$ è $\{1\}$, di $(\mathbb{Z}, \cdot)$ è $\{1, -1\}$, di $(\mathbb{Q}, \cdot)$ è $\mathbb{Q} \setminus \{0\}$, di $(\mathbb{R}, \cdot)$ è $\mathbb{R} \setminus \{0\}$, di $(\mathbb{C}, \cdot)$ è $\mathbb{C} \setminus \{0\}$.
- L'insieme degli elementi invertibili di $F(X) = \{f : X \to X\}$ è l'insieme delle funzioni invertibili.

Definizione 1.16 — Gruppo. Un monoide X è detto **gruppo** se ogni suo elemento è invertibile.

Definizione 1.17 — Gruppo Abeliano. Se l'operazione è commutativa, il gruppo è detto **gruppo abeliano**.

Esempio.

- $(\mathcal{P}(x), \Delta)$ è un gruppo abeliano. L'identità è l'insieme vuoto e l'inverso di $A \in \mathcal{P}(x)$ è A stesso. $(A^2 = \varnothing, \forall A \subseteq X)$
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sono gruppi abeliani

- $(\mathbb{Q}\backslash\{0\},\cdot)$, $(\mathbb{R}\backslash\{0\},\cdot)$, $(\mathbb{C}\backslash\{0\},\cdot)$ sono gruppi abeliani
- sia $X = \{1,2,\ldots,n\}$ l'insieme delle funzioni invertibili $f : X \to X$ è il **Gruppo delle permutazioni di n elementi (o gruppo simmetrico)**.Lo indiciamo con $|S_n|$. $|S_n| = m!$. Non è abeliano se $n \geq 3$.

Definizione 1.18 — Sottomonoide e Sottogruppo. Sia X un monoide con identità e. Un sottoinsieme $Y \subseteq X$ tale che $e \in Y$ e Y è chiuso rispetto all'operazione di X è detto **sottomonide di** X. Analogamente definiamo la nozione di **sottogruppo di** X. il gruppo $\{e\}$ è detto **sottogruppo banale di** X.

Esempio.

- Con l'addizione, $\{0\}$ è un sottomonoide di $\mathbb{N}$. $\{0\}$ è anche sottogruppo banale.
- Con la moltiplicazione abbiamo la catena di sottomonoidi $\{1\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq insiemeR \subseteq \mathbb{C}$ e di sottogruppi $\{1\} \subseteq \mathbb{Q}\backslash\{0\} \subseteq \mathbb{R}\backslash\{0\} \subseteq \mathbb{C}\backslash\{0\}$
- con l'addizione abbiamo la catena di sottogruppi $\{0\} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Definizione 1.19 — Sottomonoide e Sottogruppo generati. Sia X un monoide e $S \subseteq X$ un sottoinsieme, l'insieme

$$\langle S \rangle := \{x_1 \cdot x_2 \cdot \ldots \cdot x_n : n \in \mathbb{N}, x_1, x_2, \ldots, x_n \in S\}$$

è detto **sottomonoide generato da** S (intersezione di tutti i sottomonoidi di X che contengono S). Se X è un gruppo, $\langle S \rangle$ è detto **sottogruppo generato da** S.

Esempio.

- $S = \{1\} \subseteq (\mathbb{N},+)$. Allora $\langle S \rangle = \{0,1,2,\ldots\} = \mathbb{N}$
- sia $S := \{p \in \mathbb{N} : p \text{ è primo}\} \cup \{0\} \subseteq (\mathbb{N},\cdot)$. allora $\langle S \rangle = \mathbb{N}$
- $S = \{0,1\} \subseteq (\mathbb{N},\ldots)$. Allora $\langle S \rangle = \{0,1\}$
- sia $S = \{1\} \subseteq (\mathbb{Z},+)$. il sottogruppo generato da S è $\langle S \rangle = \mathbb{Z}$
- uno spazio vettoriale V è un gruppo abeliano se consideriamo l'operazione di addizione fra vettori. Prendiamo $V = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Sia $v = (1,1) \in \mathbb{R}^2$. Il sottogruppo $\langle \{v\} \rangle = \{(n,n) : n \in \mathbb{Z}\}$ è un sottogruppo proprio del sottospazio generato da $\{v\}$. Sia $v_1 = (1,0)$ ed $v_2 = (0,1)$, allora il sottogruppo $\langle \{v_1, v_2\} \rangle$ è $\mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{R} \times \mathbb{R}$

Definizione 1.20 — Prodotto diretto. Siano M_1, M_2 con identità e_1, e_2 rispettivamente. Si definisce **prodotto diretto di** M_1 **e** M_2 l'insieme $M_1 \times M_2$ con l'operazione $(m_1, m_2) \cdot (m_1', m_2') = (m_1 \cdot m_1', m_2 \cdot m_2')$ e identità (e_1, e_2). Analogamente si definisce prodotto diretto di gruppi G_1 e G_2.

L'inverso di una coppia $(a,b) \in G_1 \times G_2$ è (a^{-1}, b^{-1}).

1.4 Morfismi

Definizione 1.21 — Morfismo di Monoidi. Siano M_1 e M_2 monoidi con identità e_1 e e_2. Una funzione $f : M_1 \to M_2$ è un **morfismo di monoidi** se:

(i) $f(e_1) = e_2$

(ii) $f(xy) = f(x)f(y)$

Definizione 1.22 — Morfismo di Gruppi. Siano G_1 e G_2 gruppi con identità e_1 e e_2. Una funzione $f : G_1 \to G_2$ è un **morfismo di gruppi** se:

(i) $f(e_1) = e_2$

(ii) $f(xy) = f(x)f(y)$

Definizione 1.23 — Nucleo. Il **nucleo** di un morfismo di monoidi $f : M_1 \to M_2$ è il sottomonoide di M_1 definito come

$$Ker(f) := \{x \in M_1 : f(x) = e_2\}$$

Osservazione. Il nucleo di un morfismo di gruppi $f : G_1 \to G_2$ è il sottogruppo di G_1 definito come: $Ker(f) := \{x \in G_1 : f(x) = e_2\}$. **Il nucleo è un sottogruppo di** G_1. e $Im(f)$ **è un sottogruppo di** G_2.

Definizione 1.24 — Isomorfismo. Un **isomorfismo di monoidi (e di gruppi)** è un morfismo biunivoco, tale che la funzione inversa sia un morfismo.

Proposizione 1.25. Sia $f : M_1 \to M_2$ un morfismo di monoidi. Se f è biunivoco, allora è un isomorfismo. Questo vale anche per i gruppi.

Dimostrazione. Dobbiamo far vedere che la funzione inversa $f^{-1} : M_2 \to M_1$ è un morfismo di monoidi.

Poiché $f(e_1) = e_2$, allora $f^{-1}(e_2) = e_1$. Siano $x_2, y_2 \in M_2$, allora esistono $x_1, y_1 \in M_1$ tali che $f(x_1) = x_2, f(y_1) = y_2$. Quindi $f^{-1}(f(x_1)f(y_1)) = f^{-1}(f(x_1y_1)) = x_1y_1 = f^{-1}(x_2)f^{-1}(y_2)$ ■

Esempio.

- Siano $M_1 = (\mathcal{P}(X), \cap)$ e $M_2 = (\mathcal{P}(X), \cup)$, dove X è un insieme. Sia $f : M_1 \to M_2$ definita ponendo $f(A) = A^C, \forall A \subseteq X$. la funzione f è biunivoca. Inoltre, dalle formule di De Morgan segue che $f(A \cap B) = (A \cap B)^C = A^C \cup B^C = f(A) \cup f(B)$. Quindi f è un isomorfismo di monoidi, poiché $f(X) = X^C = \varnothing$, essendo X l'identità di M_1 e $\varnothing$ l'identità di M_2.
- Sia $\mathbb{Z}_2 := \{0, 1\}$ con l'operazione definita come: $0 + 0 = 0, 0 + 1 = 1 + 0 = 1, 1 + 1 = 0$. Sia $X := \{1, 2, \dots, n\}, n \in \mathbb{N}$. La funzione $f : \mathcal{P}(X) \to \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2$ (n volte) definita da: $f(A) = (a_1, a_2, \dots, a_n)$, dove $a_i = 1$ se $i \in A$ e $a_i = 0$ se $i \notin A$.
è un isomorfismo del gruppo $(\mathcal{P}(X), \Delta)$ con il gruppo $\mathcal{P}(X) \to \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2 = (\mathbb{Z}_2)^n$

Vediamo ora come ogni monoide finito è isomorfo a un monoide di matrici quadrate, dove l'operazione è il prodotto righe per colonne.

Sia $M = \{x_1, \dots, x_n\}$ un monoide, $|M| = n \in \mathbb{N}$, con identità $e = x_1$.

Per ogni $x \in M$ definiamo una matrice $A(x) \in Mat_{n\times n}(\mathbb{Z})$ nel seguente modo:

- $A(x)_{ij} = 1$ se $x_i \cdot x = x_j$
- $A(x)_{ij} = 0$ altrimenti.

La funzione $F : M \to Mat_{n\times n}(\mathbb{Z})$ $(x \mapsto A(x))$ è iniettiva.

Infatti, se $A(x) = A(y)$, allora $A(x)_{i1} = A(y)_{i1}\ \forall\, i \in \{1, \dots, n\}$.

Quindi se $A(x)_{i1} = A(y)_{i1} = 1$, allora $xx_1 = xe = x = yx_1 = y$.

Risulta inoltre facile vedere che $A(xy) = A(x)A(y)$ (prodotto righe per colonne), ossia che F è un morfismo di monoidi ($Mat_{n\times n}(\mathbb{Z})$ è un monoide con l'operazione di prodotto righe per colonne, la cui identità è la matrice I_n).

Quindi $F : M \to Im(F)$ è un isomorfismo di monoidi.

Esempio. Sia $M = (\mathbb{Z}_2, \cdot)$ il monoide definito da:

$\cdot$	0	1
0	0	0
1	0	1

Costruiamo un sottomonoide di $\mathrm{Mat}_{4\times 4}(\mathbb{Z})$ isomorfo a $M \times M = \{(0,0),(0,1),(1,0),(1,1)\}$.

$$(0,0) \mapsto \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \ (0,1) \mapsto \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \ (1,0) \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \ (1,1) \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$\cdot$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$
$(1,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$
$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$

Si può verificare direttamente che le matrici hanno la stessa tabella moltiplicativa.

Abbiamo quindi visto che un monoide finito di cardinalità n è isomorfo a un monoide di matrici $n \times n$ le cui colonne hanno un unico "1" e altrove sono "0".

Ognuna di queste matrici può essere vista come una funzione da $X = \{1, \dots, n\} \in X$:

$$A_{ij} = 1 \iff f(j) = i$$
$$A_{ij} = 0 \iff f(j) \neq i$$

Il prodotto righe per colonne corrisponde alla composizione di funzioni.

Quindi un monoide finito di cardinalità n è isomorfo a un sottomonoide del monoide delle funzioni f da $\{1, \dots, n\}$ in $\{1, \dots, n\}$ con l'operazione di composizione.

Notiamo che un elemento $x \in M$ di un monoide finito M è invertibile se e solo se la matrice associata è invertibile (una matrice $A \in Mat_{n\times n}(\mathbb{Z})$ è invertibile se e solo se il suo determinante è invertibile su $\mathbb{Z}$, ossia se e solo se $det(a) \in \{-1, 1\}$).

Da ciò segue che un gruppo finito G di cardinalità $|G| = n$, è isomorfo a un gruppo di matrici le cui componenti sono "0" e "1" e che hanno un unico "1" in ogni riga e ogni colonna (matrici di permutazioni).

Il gruppo G è inoltre isomorfo a un sottogruppo del gruppo delle funzioni biunivoche da $\{1, \dots, n\}$ in $\{1, \dots, n\}$, che abbiamo chiamato **gruppo simmetrico** S_n.

Gli elementi di S_n in notazione a una linea sono indicati nel modo seguente: sia $\sigma \in S_n$ una funzione biunivoca da $\{1, \dots, n\}$ in $\{1, \dots, n\}$, allora σ è indicata come $\sigma(1)\sigma(2)\dots\sigma(n)$.

Teorema 1.26 — Teorema di Cayley. Ogni sottogruppo finito di cardinalità $n \in \mathbb{N}\backslash\{0\}$ è isomorfo a un sottogruppo di S_n

Esempio.

- $S_2 = \{12, 21\}, S_3 = \{123, 132, 213, 231, 312, 321\}$
- vediamo il gruppo $(\mathbb{Z}_2, +)$ come gruppo di matrici e come gruppo di permutazioni.

$$(\mathbb{Z}_2, +) \simeq \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} \underbrace{\simeq}_{\text{Isomorfismo di gruppi}} \{12, 21\} = S_2$$

1.5 Relazioni

Definizione 1.27 — Relazione. Sia X un insieme. Un sottoinsieme $R \subseteq X \times X$ è detto **relazione su X**.

Definizione 1.28 — Relazione di equivalenza. Una relazione $R \subseteq X \times X$ è detta **relazione di equivalenza** se soddisfa le seguenti proprietà:

(i) **riflessità**: $(x, x) \in R, \forall x \in X$

(ii) **simmetria**: $(x, y) \in R \implies (y, x) \in R, \forall x, y \in X$

(iii) **transitività**: $(x, y) \in R$ e $(y, z) \in R \implies (x, z) \in R, \forall x, y, z \in X$

Se R è una relazione di equivalenza su X e $(x, y) \in R$, scriviamo $x \sim y$, che si legge "x è equivalente a y".

Definizione 1.29 — Classe di equivalenza. Sia X un insieme e $R \subseteq X \times X$ una relazione di equivalenza su X. L'insieme

$$[x]_R := \{y \in X : x \sim y\}$$

è detto **classe di equivalenza di x rispetto a R**.

Definizione 1.30 — Insieme quoziente. L'insieme ${}^{X}\!/\!_{\sim} := \{[x] : x \in X\}$ è detto **insieme quoziente**.

Definizione 1.31 — Proiezione canonica. La funzione

$$\begin{aligned} \pi : X &\longrightarrow {}^{X}\!/\!_{\sim} \\ x &\longmapsto [x] \end{aligned}$$

è detta **proiezione canonica**.

Definizione 1.32 — Partizione. Siano $x, y \in X$. Allora se $x \sim y$ abbiamo che $[x] = [y]$. Se $x \nsim y$ abbiamo che $[x] \cap [y] = \varnothing$. Quindi $X = \biguplus_{[x] \in {}^{X}\!/\!_{\sim}} [x]$, ossia ${}^{X}\!/\!_{\sim}$ è una partizione di X.

Esempio.

- L'uguaglianza "=" è una relazione di equivalenza su ogni insieme X.
- Sia $X = \{1, 2, \dots, n\}$. Definiamo su $\mathcal{P}(X)$ la seguente relazione: $A \sim B \iff |A| = |B|, \forall A, B \subseteq X$. Questa è una relazione di equivalenza e ${}^{\mathcal{P}(X)}\!/\!_{\sim} \equiv \{0, 1, \dots, n\}$. Se $A \subseteq X$ è tale che $|A| = k \leq n$ allora $|[A]| = \binom{n}{k} := \frac{n!}{k!(n-k)!}$
- Sia G un gruppo e $H \subseteq G$ un sottogruppo. La relazione $\sim$ su G definita da $g_1 \sim g_2 \iff g_1 = g_2 h$ per qualche $h \in H$ è una relazione di equivalenza.
  1. $g \sim g : g \cdot e$, $\forall g \in G, e \in H$
  2. $g_1 \sim g_2 \to g_2 \sim g_1 : g_1 = g_2 h \to g_1 h^{-1} = g_2$ $(h^{-1} \in H)$
  3. $g_1 \sim g_2, g_2 \sim g_3 \to g_1 \sim g_3 : g_1 = g_2 h, g_2 = g_3 h' \to g_1 = g_3 h h' = g_3 h'', \forall g_1, g_2, g_3 \in G$

  In questo caso l'insieme quoziente lo indichiamo con ${}^{G}\!/\!_{H}$.

Definizione 1.33 — Coefficiente binomiale. Il numero $\binom{n}{k}$ è chiamato **coefficiente binomiale**, questo perché $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^n y^{n-k}, \forall x, y \in \mathbb{C}$

Se G è un gruppo abeliano e H un suo sottogruppo, possiamo definire la seguente operazione "+" su ${}^{G}\!/\!_{H}$: $[g_1] + [g_2] := [g_1 + g_2]$, vediamo che è ben definita: se $g_1' = g_1 + h_1$ e $g_2' = g_2 + h_2$, allora $[g_1'] = [g_1]$,

$[g_2'] = [g_2]$ e $g_1' + g_2' = g_1 + h_1 + g_2 + h_2 = g_1 + g_2 + h$, dove $h = h_1 + h_2 \in H$. Quindi $[g_1' + g_2'] = [g_1 + g_2]$.
L'operazione è ovviamente associativa e commutativa, perché lo è quella su G. Inoltre $[g]+[0] = [g]$, $\forall\,[g] \in {}^{G}\!/_{H}$ dove con "0" abbiamo indicato l'identità di G. Quindi la classe $[0]$ dell'identità di $({}^{G}\!/_{H}, +)$.

Infine $[g] + [-g] = [g - g] = [0]$, dove con $-g$ abbiamo indicato l'inverso di g in G.

Quindi $-[g] = [-g], \forall\,[g] \in {}^{G}\!/_{H}$, ossia $({}^{G}\!/_{H}, +)$ è un gruppo abeliano.

Esempio.

- Se $H = \{0\} \subseteq G$, allora ${}^{G}\!/_{H}$ è isomorfo a G. ($\{0\}$ gruppo banale e G gruppo abeliano)
- Sia $G = (\mathbb{Z}, +)$, $n \in \mathbb{N}$. il sottoinsieme $n\mathbb{Z} := \{kn : k \in \mathbb{Z}\}$ è un sottogruppo di $\mathbb{Z}$.
  - $0\mathbb{Z} = \{0\}$
  - $1\mathbb{Z} = \{\mathbb{Z}\}$
  - $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$
  - $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$
  - $\dots$

  Definiamo il gruppo abeliano $\mathbb{Z}_n := {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ per $\mathbb{Z}_0 = {}^{\mathbb{Z}}\!/_{0\mathbb{Z}} = {}^{\mathbb{Z}}\!/_{\{0\}} \simeq \mathbb{Z}$.
  Sia $n \geq 0$ e siano $x, y \in \mathbb{Z}$. Allora $x \sim y \iff x = y + h$ $(h \in n\mathbb{Z}) \iff x - y = kn$ (per $k \in \mathbb{Z}$) $\iff$ il resto della divisione di x per n è uguale al resto della divisione di y per n.

  I possibili resti della divisione per n sono $0, 1, \dots, n-1$.

  Quindi $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. ($\{[0], [1], \dots, [n-1]\}$ sono le classi di resto)

  - $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, $\begin{array}{c|c|c} + & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & \overline{1} \\ \hline \overline{1} & \overline{1} & \overline{0} \end{array}$ $\overline{1} + \overline{1} = [1 + 1] = [2] = [0]$
  - $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, $\begin{array}{c|c|c|c} + & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{1} & \overline{1} & \overline{2} & \overline{0} \\ \hline \overline{2} & \overline{2} & \overline{0} & \overline{1} \end{array}$

Definizione 1.34 — Morfismo suriettivo di gruppi. Sia G un gruppo abeliano e $H \subseteq G$ un sottogruppo. La proiezione canonica $\pi : G \to {}^{G}\!/_{H}$ è un **morfismo suriettivo di gruppi**

Se G è un gruppo finito e $H \subseteq G$ è un sottogruppo, allora $[g] \in {}^{G}\!/_{H} \to |[g]| = |H|$.

Infatti $[g] = \{gh : h \in H\}$ e $gh_1 = gh_2 \to h_1 = h_2$.

Poiché le classi di equivalenza sono una partizione di G , abbiamo $|G| = |{}^{G}\!/_{H}| \cdot |H|$.

In particolare la cardinalità o (**ordine**) di un sottogruppo di un gruppo finito divide la cardinalità del gruppo.

Teorema 1.35. Sia $f : G_1 \to G_2$ un morfismo di gruppi. Allora f è iniettivo se e solo se $Ker(f) = \{e_1\}$ (Questo non vale per i morfismi di monoidi.)

Dimostrazione. Sia f iniettivo. Sia $x \in Ker(f)$. Allora $f(x) = e_2$ e quindi, poiché anche $f(e_1) = e_2$, si ha che $x = e_1$ per l'ipotesi di iniettività.
Sia $Ker(f) = \{e_1\}$. Siano $x, y \in G_1$ tali che $f(x) = f(y)$.
Allora $f(x)f(y^{-1}) = e_2 \to f(xy^{-1}) = e_2 \to xy^{-1} \in Ker(f) \to xy^{-1} = e_1 \to x = y$, ■

Esempio.

- $G = \mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$,

- $\langle\overline{0}\rangle = \overline{0}$ sottogruppo banale $\simeq \mathbb{Z}_1$
- $\langle\overline{1}\rangle = \mathbb{Z}_4$
- $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}\} \simeq \mathbb{Z}_2$ $(2 + 2 = 0)$
- $\langle\overline{3}\rangle = \mathbb{Z}_4$ $(3, 3 + 3 = 6 = 2, 3 + 2 = 5 = 1, 3 + 1 = 4 = 0)$

I sottogruppi di $\mathbb{Z}_4$ possono avere cardinalità $1, 2, 4$. L'insieme dei sottogruppo di $\mathbb{Z}_4$ è $\{\{\overline{0}\}, \{\overline{0}, \overline{2}\}, \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbb{Z}_4\}$

- $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$,
  - $\langle\overline{0}\rangle = \overline{0}$ sottogruppo banale $\simeq \mathbb{Z}_1$
  - $\langle\overline{1}\rangle = \mathbb{Z}_6$
  - $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}\} \simeq \mathbb{Z}_3$
  - $\langle\overline{3}\rangle = \{\overline{0}, \overline{3}\} \simeq \mathbb{Z}_2$
  - $\langle\overline{4}\rangle = \{\overline{0}, \overline{2}, \overline{4}\} \simeq \mathbb{Z}_3$
  - $\langle\overline{5}\rangle = \mathbb{Z}_6$

  I sottogruppi di $\mathbb{Z}_6$ possono avere cardinalità $1, 2, 3, 6$. L'insieme dei sottogruppo di $\mathbb{Z}_6$ è $\{\{\overline{0}\}, \{\overline{0}, \overline{2}, \overline{4}\}, \{\overline{0}, \overline{3}\}, \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \mathbb{Z}_6\}$

Caso generale: consideriamo il gruppo $\mathbb{Z}_n = (\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}, +)$ sia $m \in \mathbb{N}, m < n$.

Se $m = 0$, $\langle\overline{0}\rangle = \{\overline{0}\}$.

Sia $m > 0$ e $z := \frac{mcm\{m,n\}}{m}$. (mcm = minimo comune multiplo)

$$\overline{m} + \overline{m} + \ldots = \overline{m} = \overline{zm} = \overline{mcm\{m, n\}} = \overline{0}$$

Se $i \leq i \leq z$: $im < zm = mcm\{m, n\} \to n$ non divide im.

$\overline{m} + \overline{m} + \ldots = \overline{m} = \overline{im} \neq \overline{0}$ perché im è multiplo di m e $im < mcm\{m, n\}$, quindi im non è multiplo di n.

Dunque $|\langle\overline{m}\rangle| = z = \frac{mcmc\{m,n\}}{m}$.

In particolare, $\langle\overline{m}\rangle = \mathbb{Z}_n \iff z = n \iff MCD\{m, n\} = 1$.

Ossia **l'insieme $\{\langle \overline{m}\rangle\}$ genera il gruppo $\mathbb{Z}_n$ sse m e n sono coprimi.**

Definizione 1.36 — Funzione di Eulero. La funzione definita da $\varphi : \mathbb{N}\backslash\{0\} \to \mathbb{N}\backslash\{0\}$, $\varphi(n) := |\{m \in \mathbb{N}\backslash\{0\} : m < n \text{ e } MCD\{m, n\} = 1\}|$ è detta **funzione di Eulero**.

Quindi ci sono $\varphi(n)$ elementi $\overline{m}$ tali che $\langle\overline{m}\rangle = \mathbb{Z}_n$.

Proposizione 1.37. 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. ■

Definizione 1.38 — Gruppo ciclico. Un gruppo G è detto **ciclico** se esiste $g \in G$ tale che $\langle g\rangle = G$.

Un gruppo ciclico è anche abeliano

Esempio.

- $\mathbb{Z} = \langle 1\rangle$ è ciclico

- $\mathbb{Z}_n = \langle \overline{1} \rangle$ è ciclico
- $\mathbb{Z} \times \mathbb{Z} = \langle (1,0), (0,1) \rangle$ non è ciclico, infatti in $\mathbb{Z} \times \mathbb{Z}$, se $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, $\langle (a,b) \rangle = \{(ka, kb) : k \in \mathbb{Z}\} = \{(x,y) : a \text{ divide } x, b \text{ divide } y\} \subsetneq \mathbb{Z} \times \mathbb{Z}$.
- $\mathbb{Z}_2 \times \mathbb{Z}_2$ non è ciclico. Infatti, in $\mathbb{Z}_2 \times \mathbb{Z}_2$ si ha:
  - $\langle (\overline{0}, \overline{0}) \rangle = \{(\overline{0}, \overline{0})\}$
  - $\langle (\overline{0}, \overline{1}) \rangle = \{\overline{0}\} \times \mathbb{Z}_2$
  - $\langle (\overline{1}, \overline{0}) \rangle = \mathbb{Z}_2 \times \{\overline{0}\}$
  - $\langle (\overline{1}, \overline{1}) \rangle = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{1})\}$

  Quindi nessun elemento di $\mathbb{Z}_2 \times \mathbb{Z}_2$ genera $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Teorema 1.39 — di isomorfismo per gruppi abeliani. Sia $f : G_1 \to G_2$ un morfismo di gruppi abeliani. Allora esiste un morfismo iniettivo $\varphi : {}^{G_1}/_{Ker\varphi} \to G_2$ tale che il seguente diagramma è commutativo:

$$\begin{tikzcd} G_1 \arrow[r, "f"] \arrow[d, "\pi"'] & G_2 \\ {}^{G_1}/_{Ker(f)} \arrow[ur, "\varphi"'] & \end{tikzcd}$$

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 $Ker(f) = \{[g] \in {}^{G}/_{Ker(f)} : \varphi([g]) = O_2\} = \{[g] \in {}^{G}/_{Ker(f)} : f(g) = O_2\} = [O_1]$. 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 1.40 — 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

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

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

∎

Corollario 1.41. L'insieme dei sottogruppi di $\mathbb{Z}_n, n \in \mathbb{N}$ è:

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

Proposizione 1.42. Sia $n \in \mathbb{N}$ e sia d/n (d divide n).
Allora esiste al più un unico sottogruppo di $\mathbb{Z}_n$ di cardinalità d.

Dimostrazione. Sia $H \subseteq \mathbb{Z}_n$ sottogruppo tale che $|H| = d$. Si considerino le proiezioni canoniche $\mathbb{Z} \to^{\pi_1} \mathbb{Z}_n \to^{\pi_2} \mathbb{Z}_n/H$.

Poiché $\pi_1^{-1}(H) = \{m \in \mathbb{Z} : \pi_1(m) \in H\}$ è un sottogruppo di $\mathbb{Z}$, allora esiste $k \in \mathbb{N}$ tale che $\pi_1^{-1}(H) = k\mathbb{Z}$.

Inoltre $Ker(\pi_1 \cdot \pi_2) = \pi_1^{-1}(H)$ e quindi, essendo $\pi_1 \cdot \pi_2$ un morfismo suriettivo di gruppi, $\mathbb{Z}_n/H \simeq \mathbb{Z}/\pi^{-1}(H) = \mathbb{Z}/k\mathbb{Z} = \mathbb{Z}_k$.

Quindi $|\mathbb{Z}_k| = k = |\mathbb{Z}_n/H| = |\mathbb{Z}_n|/|H| = \frac{n}{d}$, ossia k è univocamente determinato, e allora $H = \pi_1(k\mathbb{Z})$ è univocamente determinato. ■

Esempio. I sottogruppi di $\mathbb{Z}_{899}$ sono quattro, perché $899 = 31 \cdot 29$, quindi c'è un sottogruppo di cardinalità 1 (il sottogruppo banale), uno di cardinalità 31, uno di cardinalità 29 e $\mathbb{Z}_{899}$.
Sono: $\{\{0\}, \langle\overline{29}\rangle, \langle\overline{31}\rangle, \mathbb{Z}_{899}\}$.

1.6 Anelli

Definizione 1.43 — Anello. Sia X un insieme su cui sono definite due operazioni $+$ e $\cdot$. X è un **anello** con unità 1_X se:

(i) $(X, +)$ è un gruppo abeliano

(ii) $(X, \cdot)$ è un monoide con unità 1_X

(iii) vale la proprietà distributiva:

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(a + b) \cdot c = a \cdot c + b \cdot c$, $\forall a, b, c \in X$

Definizione 1.44 — Anello commutativo. Diciamo che un anello X è **commutativo** se il monoide $(X, \cdot)$ è commutativo.

Indichiamo con "0" l'identità del gruppo $(X, +)$.

Esempio.

- Gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con le operazioni di addizione e moltiplicazione sono anelli commutativi con unità, che è il numero "1".
- L'insieme delle matrici $n \times n, n > 1$ a valori su $\mathbb{Z}$, su $\mathbb{Q}$, su $\mathbb{R}$ o su $\mathbb{C}$, con l'operazione di somma e il prodotto righe per colonne, è un anello **non commutativo**, con unità la matrice identità.

  In generale, se A è un anello commutativo con unità, l'insieme $Mat_{n\times n}(A)$ delle matrici a valori in $\mathbb{R}$ con le operazioni di somma e prodotto righe per colonne, è un anello non commutativo con unità.
- $\{X\}$ è un anello, detto **anello nullo**. Le due operazioni sono la stessa e $0 = 1_{\{X\}} = x$.

Considereremo sempre $0 \neq 1_A$ e studieremo solo anelli commutativi con unità. Quindi quando diremo "anello" intendiamo "anello con unità".

Definizione 1.45 — Zero divisore in un anello. Sia A un anello commutativo. Un elemento $x \in A$ è detto **zero divisore** se esiste $y \in A\backslash\{0\}$ tale che $xy = 0$.

Definizione 1.46 — Elemento invertibile in un anello. Diciamo che un elemento $x \in A$ è **invertibile** se è un elemento invertibile del monoide $(A, \cdot)$.

Proposizione 1.47. Sia A un anello commutativo. Allora l'insieme degli elementi invertibili di A è disgiunto dall'insieme degli zero-divisori di A.

Dimostrazione. Siano $x, y \in A$ tali che $xy = 0$. Se X è invertibile, allora $x^{-1}xy = y = 0$, quindi x non è uno zero-divisore. ■

Proposizione 1.48 — Legge di cancellazione. Sia A un anello commutativo e sia $x \in A$ un elemento che non è uno zero-divisore. Allora:

$$\cancel{x}y = \cancel{x}z \to y = z \qquad \forall\, y, z \in A$$

Dimostrazione. Se $xy = xz$ allora $x(y - z) = 0$. Poiché x non è uno zero-divisore, allora $y - z = 0$, ossia $y = z$. ■

Definizione 1.49 — Dominio di integrità. Un anello commutativo privo di zero-divisori non nulli è detto **dominio di integrità**.

Definizione 1.50 — Campo. Un anello commutativo i cui elementi non nulli sono tutti invertibili è detto **campo**.

Esempio. L'anello $\mathbb{Z}$ è un dominio di integrità, ma non è un campo.
Gli anelli $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi.

1.7 Ideali

Definizione 1.51 — Ideale. Sia A un anello commutativo. Un sottoinsieme $I \subseteq A$ è detto **ideale** di A se:

(i) I è un sottogruppo di $(A, +)$

(ii) $ax \in I, \forall\, a \in A, x \in I$

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

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.

Osservazione. Siano $I, J \subseteq A$ ideali di un anello commutativo A. Allora:

- $I \cap J$ è un ideale di A
- $I + J := \{x + y : x \in I, y \in J\}$ è un ideale di A
- $IJ := \langle\{xy : x \in I, y \in J\}\rangle$ è un ideale di A

Definizione 1.52 — Ideale generato da un insieme. Sia $S \subseteq A$ un sottoinsieme di un anello commutativo. **L'ideale generato da** S è l'intersezione di tutti gli ideali di A che contengono S e lo indichiamo con $\langle S \rangle$.

Se $S = \{x\}$, diciamo che $\langle S \rangle$ è **l'ideale principale generato da** $x \in A$.

Esempio. Abbiamo visto che gli ideali di $\mathbb{Z}$ sono tutti e soli i sottoinsiemi $n\mathbb{Z} = \langle n \rangle, n \in \mathbb{N}$. Quindi gli ideali di $\mathbb{Z}$ sono tutti principali.

Definizione 1.53 — Anello ad ideali principali. un anello i cui ideali sono tutti principali si dice **anello ad ideali principali**.

Proposizione 1.54. 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 $1_A uu^{-1} \in I$.

  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 $x \in A \backslash \{0\}$, allora $\langle x \rangle = \langle 1_A \rangle$, ossia $ax = 1_A$ per qualche $a \in A$. Quindi x è invertibile.

■

1.8 Anelli quoziente

Sia A un anello commutativo e $I \subseteq A$ un ideale.

In particolare, A con l'operazione "+" è un gruppo abeliano e I è un sottogruppo di A.

Allora possiamo definire il gruppo quoziente $^{A}/_{I}$.

Con l'operazione $[x] \cdot [y] := [xy]$, per ogni $[x], [y] \in {}^{A}/_{I}$, abbiamo che $^{A}/_{I}$ è un anello commutativo con unità $[1_A]$.

Infatti, mostriamo che l'operazione è ben definita. Siano $x' \in [x]$ e $y' \in [y]$. Allora esistono $i_x \in I$ e $i_y \in I$ tali che $x' = x + i_x$ e $y' = y + i_y$.

Quindi $x'y' = (x + i_x)(y + i_y) = xy + \underbrace{xi_y + yi_x + i_x i_y}_{\in I \text{ perché } I \text{ è un ideale di } A}$

Quindi $[x'y'] = [xy]$.

Inoltre $[1_A][x] = [1_A x] = [x]$, per ogni $[x] \in {}^{A}/_{I}$, quindi $[1_A]$ è l'unità di $^{A}/_{I}$.

Esempio. Abbiamo visto che $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ è un ideale dell'anello $\mathbb{Z}$. Quindi il quoziente $\mathbb{Z}_n = {}^{\mathbb{Z}}/_{n\mathbb{Z}}$ ha la struttura di anello.

- $\mathbb{Z}_0 \simeq \mathbb{Z}$
- $\mathbb{Z}_1 \simeq \{0\}$ anello nullo.
- $\mathbb{Z}_2 \simeq \{\overline{0}, \overline{1}\}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

- $\mathbb{Z}_3 \simeq \{\overline{0}, \overline{1}, \overline{2}\}$ è un campo perché $\overline{1}$ è invertibile e $\overline{2} \cdot \overline{2} = \overline{1}$, quindi anche $\overline{2}$ è invertibile.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

- $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ dove $\overline{2} \cdot \overline{2} = \overline{0}$, quindi $\mathbb{Z}_4$ non è un dominio di integrità. In particolare non è un campo.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Vediamo che $\mathbb{Z}_n$ è un campo se e solo se $n \in \mathbb{N} \backslash \{0, 1\}$ è un numero primo (per $n = 0$ abbiamo $\mathbb{Z}_0 \simeq \mathbb{Z}$ e per $n = 1$ abbiamo l'anello nullo).

Un ideale di $\mathbb{Z}_n$ è un sottogruppo di $\mathbb{Z}_n$.

Poiché $\mathbb{Z}_n$ è ciclico, i suoi sottogruppi sono ciclici e sono $\{\langle\overline{m}\rangle : \overline{m} \in \mathbb{Z}_n\}$.

Inoltre $\langle\overline{m}\rangle \subseteq \mathbb{Z}_n$ è un ideale, $\forall\, \overline{m} \in \mathbb{Z}_n$.

Infatti, se $\overline{a} \in \mathbb{Z}$, allora $\overline{a m} = \overline{am} = \underbrace{\overline{m} + \overline{m} + \ldots + \overline{m}}_{a \text{ volte}} \in \langle\overline{m}\rangle$.

Quindi $\{\langle\overline{m}\rangle : \overline{m} \in \mathbb{Z}_n\}$ è l'insieme degli ideali di $\mathbb{Z}_n$ ($\mathbb{Z}_n$ è anello ad ideali principali).

Inoltre, se $n > 1, \{\langle\overline{m}\rangle \overline{m} \in \mathbb{Z}_n\} = \{\{\overline{0}\}, \mathbb{Z}_n\} \cup \{\langle\overline{m}\rangle : MCD_{m \neq 0}\{m, n\} \neq 1\}$.

Quindi $\mathbb{Z}_n$ è un campo se e solo se $\{\langle\overline{m}\rangle : \overline{m} \in \mathbb{Z}_n\} = \{\{\overline{0}\}, \mathbb{Z}_n\}$ se e solo se n è un numero primo.

Esempio. $\mathbb{Z}_3$ è un campo, si ha che $\overline{2}^{-1} = \overline{2}$. Infatti:

$$\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$$

Invece $\mathbb{Z}_4$ non lo è, infatti:

$$\overline{2} \cdot \overline{2} = \overline{0}$$

e quindi $\overline{2}$ non è invertibile.

1.9 Algoritmo di Euclide e identità di Bézout su $\mathbb{Z}$

Vogliamo calcolare il massimo comun divisore tra 1876 e 365. Usiamo l'algoritmo di Euclide:

$$\begin{aligned} 1876 &= 5 \cdot 365 + 51 \\ 365 &= 7 \cdot 51 + 8 \\ 51 &= 6 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Quindi $MCD\{1876, 365\} = 1$.

Adesso vogliamo trovare due numeri $x, y \in \mathbb{Z}$ tali che $1876x + 365y = 1$.

Definizione 1.55 — Identità di Bézout. Un'identità del tipo $ax + by = MCD\{a, b\}$ si chiama **identità di Bézout**.

Dall'algoritmo di Euclide abbiamo:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 2 &= 8 - 3 \cdot 2 \\ 3 &= 51 - 6 \cdot 8 \\ 8 &= 365 - 7 \cdot 51 \\ 51 &= 1876 - 5 \cdot 365 \end{aligned}$$

Quindi

$$\begin{aligned} 1 &= 3 - 2 = \\ &= 3 - (8 - 3 \cdot 2) = 3 \cdot 3 - 8 \\ &= 3 \cdot (51 - 8 \cdot 6) - 8 = 3 \cdot 51 - 8 \cdot 19 \\ &= 3 \cdot 51 - 19(365 - 51 \cdot 7) \\ &= 136 \cdot 51 - 19 \cdot 365 \\ &= 136 \cdot (1876 - 365 \cdot 5) - 19 \cdot 365 \\ &= 136 \cdot 1876 - 699 \cdot 365 \end{aligned}$$

Quindi $x = -699$ e $y = 136$. In generale possiamo enunciare il seguente teorema:

Teorema 1.56. siano $a, b \in \mathbb{N} \setminus 0$, se $a \mid b$, allora $a = MCD\{a, b\}$. se $a \nmid b$ e r è l'ultimo resto non nullo dell'algoritmo di Euclide, allora $r = MCD\{a, b\}$.

Inoltre esistono $x, y \in \mathbb{Z}$ tali che $ax + by = MCD\{a, b\}$.

1.10 Equazioni diofantee lineari

sono equazioni del tipo $ax + by = c$, con $a, b, c \in \mathbb{Z}$.

Proposizione 1.57. siano $a, b, c \in \mathbb{Z}$. allora esistono $x, y \in \mathbb{Z}$ tali che $ax + by = c$ se e solo se $MCD\{a, b\} \mid c$.

Dimostrazione. Se $ax + by = c$, allora $MCD\{a, b\} \mid c$.

Viceversa, se $d := MCD\{a, b\} \mid c$, allora abbiamo un'identità di Bézout

$$ax + by = d \qquad \forall\, x, y \in \mathbb{Z}$$

Se $d \mid c$ cioè se $c = d \cdot k$ per qualche $k \in \mathbb{Z}$, $a(kx) + b(ky) = kd = c$ ∎

Esempio. l'equazione diofantea: $365x - 1876y = 24$ ha soluzione perché $MCD\{365, 1876\} = 1$ e $1 \mid 24$.

Avevamo l'identità di Bézout $365(-699) - 1876(-136) = 1$, moltiplicando per 24 otteniamo $365(-699 \cdot 24) - 1876(-136 \cdot 24) = 24$.

Ossia una soluzione è $x = -699 \cdot 24$ e $y = -136 \cdot 24$.

Esempio. in $\mathbb{Z}_{1876}$ calcolare, se esiste, l'inverso moltiplicativo di $\overline{365}$. abbiamo che $\overline{365} \cdot \overline{a} = \overline{1}$ in $\mathbb{Z}_{1876}$ se e solo se esistono $a, b \in \mathbb{Z}$ t.c. $365 \cdot a = 1 + b \cdot 1876 \iff 365 \cdot a - 1876 \cdot b = 1$.

Una soluzione è $a = -699$ e $b = 136$, ossia $\overline{365}^{-1} = \overline{-699} = \overline{1177}$.

Osservazione. se $p \in \mathbb{N}$ è un numero primo, scriviamo $\mathbb{F}_p := \mathbb{Z}_p$.
Il campo $\mathbb{F}_p$ ha p elementi.

1.11 Morfismi di anelli

Definizione 1.58 — Morfismo di anelli. Siano A, B due anelli. Un'applicazione $f : A \to B$ è un **morfismo di anelli** se:

(i) $f : (A, +) \to (B, +)$ è un morfismo di gruppi.

(ii) $f : (A, \cdot) \to (B, \cdot)$ è un morfismo di monoidi.

Definizione 1.59 — Nucleo di un morfismo di anelli. il nucleo di un morfismo di anelli $f : A \to B$ è l'insieme:

$$Ker(f) := \{a \in A : f(a) = 0\}$$

Osservazione. $Ker(f)$ è un ideale di A con A anello commutativo.

Esempio. sia $I \subseteq A$ un ideale di un anello commutativo A.

$$\begin{aligned} \pi : \ & A \to {}^{A}/_{I} \\ & a \mapsto [a] \end{aligned}$$

è un morfismo di anelli il cui nucleo è I.

Esempio. si consideri l'anello dei numeri complessi $\mathbb{C}$.
Allora il coniugio $\overline{z} = \overline{a + bi} = a - bi$ è un morfismo di anelli da $\mathbb{C}$ in $\mathbb{C}$:

$$\overline{1} = 1, \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$$

Teorema 1.60 — 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:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ {}^{A}/_{Ker(f)} \arrow[ur, "\Psi"'] & \end{tikzcd}$$

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

Notazione: $\overline{x} \in \mathbb{Z}_n$. La classe di equivalenza $\overline{x}$ la scriveremo anche $x \bmod n$.

Teorema 1.61 — Teorema cinese dei resti. siano $n_1, n_2, \ldots, n_k \in \mathbb{N} \backslash \{0, 1\}$ tali che $MCD\{n_i, n_j\} = 1$ per ogni $1 \leq i, j \leq k, i \neq j$.

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

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

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 $f(x) = (x \bmod n_1, x \bmod n_2, \ldots, x \bmod n_k) \forall\, x \in \mathbb{Z}$.

- $$\begin{aligned} f(a+b) &= ((a+b) \bmod n_1, \ldots, (a+b) \bmod n_k) \\ &= (a \bmod n_1 + b \bmod n_1, \ldots, a \bmod n_k + b \bmod n_k) \\ &= (a \bmod n_1, \ldots, a \bmod n_k) + (b \bmod n_1, \ldots, b \bmod n_k) \\ &= f(a) + f(b), \forall\, a, b \in \mathbb{Z} \end{aligned}$$
- $f(1) = (1 \bmod n_1, \ldots, 1 \bmod n_k)$ e $(1 \bmod n_1, \ldots, 1 \bmod n_k)$ è l'unità del prodotto diretto di anelli $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$
- $$\begin{aligned} f(a \cdot b) &= ((a \cdot b) \bmod n_1, \ldots, (a \cdot b) \bmod n_k) \\ &= (a \bmod n_1 \cdot b \bmod n_1, \ldots, a \bmod n_k \cdot b \bmod n_k) \\ &= (a \bmod n_1, \ldots, a \bmod n_k) \cdot (b \bmod n_1, \ldots, b \bmod n_k) \\ &= f(a) \cdot f(b), \forall\, a, b \in \mathbb{Z} \end{aligned}$$

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

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 $x := a_1 v_1 + \ldots + a_k v_k$ e abbiamo che $f(x) = (a_1 \bmod n_1, \ldots, a_k \bmod n_k)$. 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 $Ker(f) =< n_1 > \cap < n_2 > \cap \ldots \cap < n_k > =< mcm\{n_1, \ldots, n_k\} > =< n_1 n_2 \ldots n_k >$ dato che n_i e n_j sono coprimi $\forall\, i \neq j$.

Quindi $\mathbb{Z}/_{Ker(f)} = \mathbb{Z}/_{<n>} = \mathbb{Z}_n$ 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. ■

Esempio. Siano $n_1 = 3, n_2 = 7 e n_3 = 10$. Allora $n := n_1 n_2 n_3 = 210$ e abbiamo l'isomorfismo di anelli $\mathbb{Z}_{210} \simeq \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{10}$.

Sia $(2 \bmod 3, 5 \bmod 7, 4 \bmod 10) \in \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{10}$, questa terna corrisponde ad un elemento $x \bmod 210 \in \mathbb{Z}_{210}$ che soddisfa il sistema

$$\begin{cases} x \bmod 3 = 2 \bmod 3 \\ x \bmod 7 = 5 \bmod 7 \\ x \bmod 10 = 4 \bmod 10 \end{cases}$$

La dimostrazione del teorema cinese dei resti ci dice come trovare x.

$$x = 2v_1 + 5v_2 + 4v_3$$

dove, se

$$\begin{aligned} 3a + 70b &= 1 \\ 7a + 30b &= 1 \\ 10a + 21b &= 1 \end{aligned}$$

sono identità di Bézout, allora $v_1 = 70b, v_2 = 30b = 30, v_3 = 21b$

$$\begin{aligned}
3a + 70b = 1 &\quad : \quad a = -23, b = 1 \implies v_1 = 70 \\
7a + 30b = 1 &\quad : \quad 30 = 4 \cdot 7 + 2, 7 = 3 \cdot 2 + 1 \\
&\qquad\qquad 1 = 7 - 3 \cdot 2 = 7 - 3(30 - 4 \cdot 7) = \\
&\qquad \implies \quad = 13 \cdot 7 - 3 \cdot 30 = 91 - 90 = 1 \implies a = 13, b = -3 \\
&\qquad\qquad \implies v_2 = -3 \cdot 30 \\
10a + 21b = 1 &\quad : \quad a = -2, b = 1 \to v_3 = 21
\end{aligned}$$

Quindi $x = 2 \cdot 70 - 5 \cdot 3 \cdot 30 + 4 \cdot 21 = 194 \bmod 210$

Corollario 1.62. Sia $U(\mathbb{Z}_n)$ il gruppo degli elementi invertibili dell'anello $\mathbb{Z}_n$.
Sia $n := n_1 \dots n_k$ dove $MCD\{n_i, n_j\} = 1 \forall 1 \le i, j \le k, i \ne j$ e $n_i \in \mathbb{N} \setminus \{0, 1\} \forall 1 \le i \le k$.
Allora come i gruppi

$$U(\mathbb{Z}_n) \simeq U(\mathbb{Z}_{n_1}) \times \dots \times U(\mathbb{Z}_{n_k})$$

Dimostrazione. l'isomorfismo Ψ del teo. cinese dei resti, ristretto a $U(\mathbb{Z}_n)$ dà un isomorfismo di gruppi ■

Poiché un elemento $\overline{x} \in \mathbb{Z}_n$ è invertibile s.s.e. esiste un'identità di Bézout $ax + bn = 1$ abbiamo che $\overline{x}$ è invertibile s.s.e. $MCD\{x, n\} = 1$. Quindi

$$|U(\mathbb{Z}_n)| = \varphi(n) \qquad \text{(con } \varphi \text{ funzione di Eulero)}$$

Dal precedente Corollario e da questo segue un altro Corollario:

Corollario 1.63. Sia $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ la funzione φ di Eulero.
Siano $x, y \in \mathbb{N} \setminus \{0\}$ tali che $MCD\{x, y\} = 1$, allora:

$$\varphi(xy) = \varphi(x) \cdot \varphi(y)$$

Dimostrazione. dal Corollario precedente abbiamo che $U(\mathbb{Z}_{xy}) \simeq U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)$ come i gruppi, quindi:

$$\begin{aligned}
\varphi(xy) &= |U(\mathbb{Z}_{xy})| = \\
&= |U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)| = \\
&= |U(\mathbb{Z}_x)| \cdot |U(\mathbb{Z}_y)| = \varphi(x)\varphi(y)
\end{aligned}$$

■

Come conseguenza del corollario precedente otteniamo una formula per calcolare la funzione φ di Eulero.
Se p è un numero primo, allora ci sono p^k numeri $1 \le n \le p^k$.
Di questi numeri $p, 2p, \dots, p^{k-1}p$ hanno fattori comuni con p^k e quindi

$$\varphi(p^k) = p^k - p^{k-1}.$$

se $n = p^{k_1} \dots p^{k_s}$ per il corollario precedente ($n > 1$):

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{k_1} \dots \varphi(p_s^{k_s}) = \\ &= (p_1^{k_1} - p_1^{k_1-1}) \dots (p_s^{k_s} - p_s^{k_s-1}) = \\ &= p_1^{k_1} \dots p_s^{k_s} \prod_{\substack{p \mid n \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right) = n \prod_{\substack{p \mid n \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right)\end{aligned}$$

Teorema 1.64 — di Eulero. Sia $n \in \mathbb{N} \setminus \{0\}$ ed $a \in \mathbb{N} \setminus \{0\}$ tale che $MCD\{a, n\} = 1$. Allora:

$$a^{\overline{\varphi(n)}} = \overline{1} \quad \text{in} \quad \mathbb{Z}_n$$

(diciamo che $a^{\varphi(n)} \equiv 1 \bmod n$ ossia che $a^{\varphi(n)}$ e 1 sono equivalenti modulo n).

Dimostrazione. Sappiamo che la cardinalità del gruppo degli elementi invertibili di $\mathbb{Z}_n$ è $\varphi(n)$.

Sia $\langle \overline{a} \rangle \subseteq U(\mathbb{Z}_n)$ il sottogruppo generato da $\overline{a} \in U(\mathbb{Z}_n)$. allora $|\langle \overline{a} \rangle|$ divide $\varphi(n)$ ossia $\varphi(n) = k|\langle \overline{a} \rangle|$, per qualche $k \in \mathbb{N}$.

Sia $c := |\langle \overline{a} \rangle|$ abbiamo che

$$\overline{1} = \overline{a}^c = (\overline{a^c})^k = \overline{a^{ck}} = \overline{a^{\varphi(n)}}$$

■

Corollario 1.65 — Piccolo Teorema di Fermat. Sia p un numero primo e $a \in \mathbb{N}$.

Allora in $\mathbb{Z}_p$ abbiamo che $\overline{a} = \overline{a^p}$ ($a^p \equiv a \bmod p$).

Dimostrazione. Se p è primo si ha che $\varphi(p) = p - 1$. Allora dal Teo. di Eulero segue che, se $a \neq 0, p \nmid a$, $a^{\varphi(p) \equiv 1 \bmod p} \implies a^{p-1} \equiv 1 \bmod p \implies a^p \equiv a \bmod p$.

Se $a = 0$ o $p \mid a$ l' uguaglianza si riduce a $\overline{0} = \overline{0}$. ■

1.12 Caratteristica di un anello

Definizione 1.66 — Caratteristica di un anello. sia A un anello. Il sottogruppo $\langle 1_A \rangle \subseteq (A, +)$è un gruppo ciclico.

Quindi esiste un $n \in \mathbb{N}$ tale che $\langle 1_A \rangle \simeq \mathbb{Z}_n$. n è detto la caratteristica dell'anello A.

Esempio. La caratteristica di $\mathbb{Z}$ è 0, infatti $\langle 1 \rangle = \mathbb{Z} \simeq \mathbb{Z}_0$.

La caratteristica degli anelli $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ è sempre 0 poiché $\langle 1 \rangle = \mathbb{Z} \simeq \mathbb{Z}_0$ in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

Esempio. Sia $n \in \mathbb{N}$ allora la caratteristica dell'anello $\mathbb{Z}_n$ è n.

Infatti $\langle \overline{1} \rangle = \mathbb{Z}_n$, rispetto all'operazione $+$

Indichiamo con $CHAR(A)$ la caratteristica di un anello A.

Definizione 1.67 — Sottoanello Fondamentale. Sia A un anello e sia $\langle 1_A \rangle$ il sottogruppo di $(A, +)$ generato da 1_a.

L'intersezione di tutti i sottoanelli di A contenenti $\langle 1_a \rangle$ si chiama **sottoanello fondamentale di A**.

Esempio. Il sottoanello fondamentale di $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ è $\mathbb{Z}$

Definizione 1.68 — Sottocampo Fondamentale. sia K un campo, l'intersezione di tutti i sottocampi di K contenenti il gruppo $\langle 1_k \rangle \subseteq (K, +)$ si chiama **sottocampo fondamentale di K**.

Esempio. Il sottocampo fondamentale di $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ è $\mathbb{Q}$.

Se $p \in \mathbb{N}$ è primo, il sottocampo fondamentale di $\mathbb{F}_p$ è $\mathbb{F}_p$ perché $\langle \overline{1} \rangle = \mathbb{F}_p$.

1.13 Anello dei polinomi in una indeterminata a coefficienti in un campo

Definizione 1.69 — Successione a valori di un campo. Sia K un campo. una funzione $f : \mathbb{N} \to K$ si chiama **successione a valori in** K.

ad una successione a valori in K corrisponde una serie formale nella variabile x su K:

$$\sum_{n=0}^{\infty} f(n) x^n$$

Se l'insieme $\{m \in \mathbb{N} : f(n) \neq 0\}$ è finito diciamo che la serie formale è **un polinomio in** x **di grado** $deg(P) := MAX\{n \in \mathbb{N} : f(n) \neq 0\}$.

Il grado del polinomio 0 non è definito.

L'insieme dei polinomi in x a coefficienti in K si indica con $K[x]$ ed è un anello commutativo con le operazioni:

- somma: $(\sum_{n=0}^{\infty} a_n X^n) + (\sum_{n=0}^{\infty} b_n X^n) = \sum_{n=0}^{\infty} (a_n + b_n) X^n$
- prodotto: $(\sum_{n=0}^{\infty} a_n X^n) \cdot (\sum_{n=0}^{\infty} b_n X^n) = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k b_{n-k}) X^n$

L'unità di $K[x]$ è il polinomio 1_k.

Esempio. in $\mathbb{F}_2[x]$ siano $P := 1 + X^2 + X^3$ e $Q := X + X^2$.

Allora $P + Q = 1 + X + X^3$ e $P \cdot Q = (1 + X^2 + X^3)(X + X^2) = X + X^2 = X^3 + X^4 + X^4 + X^5 = X + X^2 + X^3 + X^5$

Proposizione 1.70. Siano $P, Q \in K[x]$ polinomi non nulli. Allora:

$$deg(P \cdot Q) = deg(P) + deg(Q).$$

In particolare $K[x]$ è un dominio di integrità.

Definizione 1.71 — Polinomio monico. Un polinomio si dice **monico** se il coefficiente del termine di grado massimo è 1.

Definizione 1.72. sia K un campo. un polinomio $P \in K[x]$ si dice **irriducibile** se i suoi unici divisori sono del tipo a, aP con $a \in K \setminus \{0\}$.

Altrimenti si dice **riducibile**.

Esempio. In $\mathbb{F}_2[X]$ il polinomio $X^2 + 1$ è irriducibile, infatti $X^2 + 1 = (X + 1)^2$.

Quindi $X + 1$ divide $X^2 + 1$ e $X + 1 \notin K \setminus \{0\}$.

Esempio. In $K[X]$ ogni polinomio di grado 1 è irriducibile, infatti se $deg(P) = 1$ allora $P = aX + b$ con $a, b \in K, a \neq 0$.

I suoi divisori sono c e $c^{-1}(aX + b), c \in K \setminus \{0\}$.

Definizione 1.73 — Radice di un polinomio. Sia $\alpha \in K$. L'elemento α è detto **radice** del polinomio $P = \sum_{n=0}^{\infty} a_n X^n \in K[X]$ se $P(\alpha) = \sum_{n=0}^{\infty} a_n \alpha^n = 0$.

Anche nell'anello $K[X]$ come in $\mathbb{Z}$ abbiamo un algoritmo di divisione Euclidea.

Se $f(X), g(X) \in K[X]$ sono polinomi non nulli allora esistono unici polinomi $q(X), r(X) \in K[X]$ tali che:

$f(X) = q(X) \cdot g(X) + r(X)$ e $r(X) = 0$ oppure $deg(r) < deg(g)$.

$q(X)$ si chiama **quoziente** e $r(X)$ si chiama **resto** della divisione.

Ne segue il seguente teorema, dimostrato come in $\mathbb{Z}$:

Teorema 1.74. L'anello $K[X]$ è a ideali principali. Se $I = \langle p(X) \rangle$ allora esiste un unico generatore monico di I.

Definizione 1.75 — Massimo Comune Divisore. Definiamo il **massimo comune divisore** di due polinomi $f(X), g(X) \in K[X]$ come l'unico massimo comune divisore monico.

Come in $\mathbb{Z}$ possiamo trovarlo con l'algoritmo delle divisioni successive che dà anche un identità di Bézout.

Esempio. $f(X) = X^4 - X^3 - 4X^2 + 4X + 1$ e $g(X) = X^2 - 1$ in $\mathbb{Q}[X]$, allora:

$$\begin{aligned} f(X) &= g(X)(X^2 - 3) + (X - 2) \\ g(X) &= (X - 2)(X + 1) + 1 \implies MCD(f, g) = 1 \end{aligned}$$

inoltre

$$\begin{aligned} 1 &= g(X) - (X - 2)(X + 1) = \\ &= g(X) - [f(X) - g(X)(X^2 - 3)](X + 1) = \\ &= -(X - 1)f(X) + (X^3 + X^2 - 3X - 2)g(X) \end{aligned}$$

Proposizione 1.76. sia K un campo e $P(X) \in K[X]$ un polinomio 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 $MCD\{f(X), p(X)\} = 1$ perché $p(X)$ è irriducibile.

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

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

Esempio. In $\mathbb{F}_2[X]$ il polinomio $P(X) = 1 + X + X^2$ è irriducibile.

Infatti non ha radici in $\mathbb{F}_2$.

Quindi l'anello ${}^{\mathbb{F}_2[X]}/_{\langle 1+X+X^2 \rangle}$ è un campo, che chiamiamo $\mathbb{F}_4$.

Un elemento di $\mathbb{F}_4$ è della forma $a_0 + a_1 X$ con $a_0, a_1 \in \mathbb{F}_2$.

La tavola moltiplicativa è la seguente:

·	0	1	X	1 + X
0	0	0	0	0
1	0	1	X	1 + X
X	0	X	1 + X	1
1 + X	0	1 + X	1	X

L'inverso di X è $1 + X$.

Esempio. In $\mathbb{F}_3[X]$ il polinomio $P(X) = 1 + X^2$ è irriducibile.

Indichiamo con $\mathbb{F}_9$ il campo $\mathbb{F}_3[X]/\langle 1+X^2\rangle$.

Un elemento di $\mathbb{F}_9$ è della forma $a_0 + a_1X$ con $a_0, a_1 \in \mathbb{F}_3$ quindi sono 9.

La tavola moltiplicativa è la seguente:

·	0	1	2	X	1 + X	2 + X	2X	1 + 2X	2 + 2X
0	0	0	0	0	0	0	0	0	0
1	0	1	2	X	1 + X	2 + X	2X	1 + 2X	2 + 2X
2	0	2	1	2X	2 + 2X	1 + 2X	X	2 + X	1 + X
X	0	X	2X	2	2 + X	2 + 2X	1	1 + X	1 + 2X
1 + X	0	1 + X	2 + 2X	2 + X	2X	1	1 + 2X	2	X
2 + X	0	2 + X	1 + 2X	2 + 2X	1	X	1 + X	2X	2
2X	0	2X	X	1	1 + 2X	1 + X	2	2 + 2X	2 + X
1 + 2X	0	1 + 2X	2 + X	1 + X	2	2X	2 + 2X	X	1
2 + 2X	0	2 + 2X	1 + X	1 + 2X	X	2	2 + X	1	2X

Teorema 1.77 — di Ruffini. Sia $f(X) \in K[X]$ un polinomio non nullo.

Se $\alpha \in K$, il resto della divisione di $f(X)$ per $X - \alpha$ è $f(\alpha)$, in particolare α è una radice di $f(X)$ s.s.e. $X - \alpha$ divide $f(X)$ in $K[X]$.

Dimostrazione. $f(X) = (X - \alpha)q(X) + r(X)$ con $r(X) = 0$ oppure $deg(r(X)) < 1$.

Quindi $r(X)$ è un polinomio costante, $r(X) = x \in K$.

Calcolando in α otteniamo $f(\alpha) = c$. ■

Esempio. Il polinomio $X^2 + 1 \in \mathbb{R}[X]$ non ha radici in $\mathbb{R}$ quindi è irriducibile e $\mathbb{R}[X]/\langle X^2+1\rangle$ è un campo isomorfo a $\mathbb{C}$, dove l'isomorfismo è dato dall'assegnazione $1 \mapsto 1$ e $x \mapsto i$

Enunciamo il seguente importante risultato, senza fornire la dimostrazione.

Proposizione 1.78. Se K è un campo, ogni sottogruppo finito del gruppo moltiplicativo $K \setminus \{0\}$ è ciclico. In particolare, se K è un campo finito, $K \setminus \{0\}$ è un gruppo ciclico.

Esempio.

- In $\mathbb{F}_4 = \mathbb{F}_2/\langle 1+X+X^2\rangle$ si ha che $\{X, X^2, X^3\} = \{X, 1 + X, 1\} = \mathbb{F}_4 \setminus \{0\}$ quindi X è un generatore del gruppo moltiplicativo $\mathbb{F}_4 \setminus \{0\}$, l'altro è $1 + X$
- in $\mathbb{F}_9 = \mathbb{F}_3/\langle 1+X^2\rangle$ abbiamo:

$$\begin{aligned}
\langle X\rangle &= \{X, X^2, X^3, X^4\} = \{X, 2, 2X, 1\} \\
\langle 1+X\rangle &= \{1+X, (1+X)^2, (1+X)^3, (1+X)^4, (1+X)^5, (1+X)^6, (1+X)^7, (1+X)^8\} = \\
&= \{1+X, 2X, 1+2X, 2, 2+2X, X, 2+X, 1\} \\
&= \mathbb{F}_9 \setminus \{0\}
\end{aligned}$$

Quindi $1 + X$ genera il gruppo moltiplicativo $\mathbb{F}_9 \setminus \{0\}$.

Sia $p \in \mathbb{N}$ un numero prima e sia $n \in \mathbb{N} \setminus \{0\}$.

Sia $Q(X), \mathbb{F}_p[X]$ un qualsiasi polinomio irriducibile di grado n. Definiamo il campo

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

Vogliamo ora mostrare che se $Q(X), Q'(X) e \mathbb{F}_p[X]$ sono polinomi irriducibili di grado n, allora:

$$^{\mathbb{F}_p[X]}/_{\langle Q(X) \rangle} \underbrace{\simeq}_{\text{Isomorfismo di campi}} {}^{\mathbb{F}_p[X]}/_{\langle Q'(X) \rangle}$$

Quindi la definizione di $\mathbb{F}_p$ è ben posta, a meno di isomorfismi.

Definizione 1.79 — Elementi Algebrici e Trascendenti. Siano $F \subseteq K$ due campi (ampliamento di campi).

Un elemento $\alpha \in K$ si dice **algebrico** su F se è radice di qualche polinomio non nullo su $f(X) \in F(X)$, altrimenti si dice **trascendente** su F.

Dato un ampliamento di campi $F \subseteq K$ e $\alpha \in K$, si consideri il morfismo di anelli

$$\begin{aligned} v_\alpha : \ & F[X] \to K \\ & f(X) \mapsto f(\alpha) \end{aligned}$$

$Ker(v_\alpha)$ è l'ideale di $F[X]$ costituito dai polinomi che si annullano in α.

Quindi α è algebrico su F s.s.e. $Ker(v_\alpha)$ è un ideale non nullo di $F[X]$.

Poiche $F[X]$ è ad ideali principali, $Ker(v_\alpha) = \langle m(X) \rangle$ dove $m(X)$ è l'unico polinomio monico di grado minimo in $Ker(v_\alpha)$.

Definizione 1.80 — Polinomio Minimo. Se $\alpha \in K$ è algebrico su F, il polinomio $m(X)$ definito sopra si chiama **polinomio minimo di α su F**, se $deg(m(X)) = n$, α si dice algebrico di grado n

Nota. sia $\alpha \in K$ e $P(X) \in F[X] \setminus \{0\})$ tale che $p(\alpha) = 0$, allora $p(X)$ è il polinomio minimo di α su F s.s.e. $p(X)$ è monico e irriducibile.

Esempio. Si consideri l'ampliamento $\mathbb{R} \subseteq \mathbb{C}$. allora $1 + X^2 \in \mathbb{R}[X]$ è il polinomio minimo di $i \in \mathbb{C}$ su $\mathbb{R}$.

Proposizione 1.81. Sia $F \in K$ un ampliamento di campi e $\alpha \in K$.

Si consideri il morfismo di anelli $v_\alpha : F[X] \to K$.

Allora $Im(v_\alpha)$ è il più piccolo sottoanello di K contenente sia F che α

Dimostrazione. Si osservi che l'immagine di un morfismo di anelli è un sottoanello.

Di conseguenza $Im(v_\alpha)$ è un sottoanello di K.

Sia $c \in F$ e si consideri il polinomio costante $c \in F[X]$. Allora $v_\alpha(c) = c$.

Quindi $F \subseteq Im(v_\alpha)$ e $v_\alpha(X) = \alpha \implies \alpha \in Im(v_\alpha)$ d'altra parte per chiusura additiva e moltiplicativa, ogni sottoanello di K contenete sia F che α contiene anche $Im(v_\alpha)$. ■

Proposizione 1.82. Sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$.

Il più piccolo sottocampo di K contenente sia F che α si chiama **ampliamento di F in K generato da α** e si indica con $\mathbf{F(\alpha)}$ tale ampliamento si dice **semplice** (poiché generato da un solo elemento)

da questa proposizione segue questo Corollario:

Corollario 1.83. Sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$. Allora:

$$F(\alpha) = \{f(\alpha)g(\alpha)^{-1} : f(X), g(X) \in F[X], g(\alpha) \neq 0\}$$

Dimostrazione. Per la proposizione precedente il più piccolo sottoanello di K contenente sia F che α è $Im(v_\alpha = \{f(\alpha) : f(X) \in F[X]\})$.

Prendendo gli inversi in K si ottiene la tesi. ■

Se $\alpha \in K$ è algebrico su F si ha che $Im(v_\alpha \simeq {}^{F[X]}/_{\langle m(X) \rangle})$, dove $m(X)$ è il polinomio minimo di α. quindi $Im(v_\alpha)$ è un campo e $F(\alpha) = Im(v_\alpha)$.

Se n è il grado di α si ha quindi:

$$F(\alpha) = \{c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} : c_i \in F\}$$

Esempio. Si consideri l'ampliamento $\mathbb{Q} \subseteq \mathbb{R}$.

L'elemento $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ è algebrico su $\mathbb{Q}$ con polinomio minimo $X^2 - 2$.

Quindi $\sqrt{2}$ ha grado 2 su $\mathbb{Q}$ e

$$\mathbb{Q}(\sqrt{2}) = \{c_0 + c_1\sqrt{2} : c_0, c_1 \in \mathbb{Q}\}).$$

Adesso mostriamo che il campo $\mathbb{F}_{p^n}$ è un ampliamento semplice di $\mathbb{F}_p$.

Proposizione 1.84. Sia $\alpha \in \mathbb{F}_{p^n}$ un generatore del campo moltiplicativo $\mathbb{F}_{p^n} \setminus \{0\}$. Allora:

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$$

Dimostrazione. $\mathbb{F}_p(\alpha)$ è il più piccolo sottocampo di $\mathbb{F}_{p^n}$ contenente sia $\mathbb{F}_p$ che α quindi $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$.

Poiché α genera il gruppo moltiplicativo $\mathbb{F}_{p^n} \setminus \{0\}$ anche $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p(\alpha)$ ■

Ora, se $P(X), Q(X) \in \mathbb{F}_p[X]$ sono due polinomi irriducibili di grado n, vogliamo costruire un isomorfismo

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

Ci serve il seguente risultato:

Proposizione 1.85. Siano $F \subseteq K$ e $F \subseteq K'$ due ampliamenti di campi.

Se $\alpha \in K$ è algebrico di grado n su F, con polinomio minimo $m(x)$,esiste un morfismo di campi $\varphi : F(\alpha) \to K'$ che fissa F in K'.

In questo caso i morfismi φ sono tanti quante le radici distinte $\beta_1, \ldots, \beta_s$ di $m(X)$ in K'.

Sono tutti e soli quelli definiti da:

$$c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} \to c_0 + c_1\beta_i + \ldots + c_{n-1}\beta_i^{n-1}$$

Dimostrazione. Se α è algebrico di grado n su F con polinomio minimo $m(X)$ e $\varphi : F(\alpha) \to K'$ è isomorfismo, allora $0 = \varphi(0) = \varphi(m(\alpha)) = m(\varphi(\alpha))$ quindi $\varphi(\alpha)$ deve essere radice di $m(X)$ in K'.

Viceversa, sia β una radice di $m(X)$ in K' e consideriamo il morfismo di anelli

$$\begin{aligned} v_\beta : \ & F[X] \to K' \\ & f(X) \to f(\beta) \end{aligned}$$

Poiché $m(X) \in Ker(v_\beta)$, dal Teorema di isomorfismo per anelli abbiamo che il seguente diagramma è commutativo:

$$\begin{tikzcd}
F[X] \arrow[r, "v_\beta"] \arrow[d, "\pi"] & K' \\
F(\alpha) \simeq F[X]/\langle m(X)\rangle \arrow[ur, "\varphi"] &
\end{tikzcd}$$

Infatti $Ker(v_\beta) = \langle m(X)\rangle$, essendo $m(X)$ irriducibile.

Quindi abbiamo trovato un morfismo iniettivo $\varphi : F(\alpha) \to K'$ che soddisfa le proprietà dell'enunciato. ■

Definizione 1.86 — Campo di spezzamento. Sia F un campo e $f(X) \in F[X]$ un polinomio di grado $n \geq 1$.

Un campo K, ampliamento di F, si dice **campo di spezzamento di f(X) su F** se:

- $f(X)$ fattorizza in polinomi di grado 1 su $K[X]$
- non ci sono campi intermedi $F \subseteq L \subsetneq K$ con la stessa proprietà.

Esempio. $\mathbb{Q}(\sqrt{2})$ è un campo di spezzamento di $X^2 - 2 \in \mathbb{Q}[X]$.

$\mathbb{C}$ è un campo di spezzamento di $X^2 + 1 \in \mathbb{R}[X]$.

Ora vogliamo mostrare che un campo che ha cardinalità p^n è un campo di spezzamento del polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$.

Infatti se K è un campo e $|K| = p^n$, allora il suo gruppo moltiplicativo $K \setminus \{0\}$ ha cardinalità $p^n - 1$ e quindi oer ogni $\alpha \in K \setminus \{0\}$ si ha $\alpha^{p^n-1} = 1$.

Quindi ogni elemento di K è radice del polinomio $X^{p^n} - X$.

Per il teorema di Ruffini, K è un campo di spezzamento di $X^{p^n} - X$.

Adesso mostriamo che ogni polinomio di grado n irriducibile in $\mathbb{F}_p[X]$ divide $X^{p^n} - X \ \in \mathbb{F}_p[X]$.

Proposizione 1.87. 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 $X^{p^n} - X \in K[X]$.

Poiché $Y \in K$ 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:

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

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

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

Esempio. In $\mathbb{F}_3[X]$ si considerino i polinomi irriducibili

$$1 + X^2 \qquad \text{e} \qquad 2 + X + X^2.$$

Il polinomio minimo di X in ${}^{\mathbb{F}_3[X]}/_{\langle 1+X^2\rangle} := K$ su $\mathbb{F}_3$ è $1 + X^2$.

In $K' := {}^{\mathbb{F}_3[Y]}/_{\langle 1+Y+Y^2\rangle}$ si ha che

$$1 + X^2 = (X + Y + 2)(X + 2Y + 1)$$

quindi in $K'[X]$ $1 + X^2$ ha due radici:

$$-Y - 2 = 2Y + 1 \qquad \text{e} \qquad -2Y - 1 = y + 2.$$

Abbiamo quindi due isomorfismi

$$f : K \to K' \qquad a_0 + a_1 x \mapsto a_0 + a_1(2Y + 1)$$

$$g : K \to K' \qquad a_0 + a_1 x \mapsto a_0 + a_1(Y + 2)$$

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(2) &= 2 \\ f(X) &= 2Y + 1 \\ f(1 + X) &= f(1) + f(X) = 2Y + 2 \\ f(2 + X) &= f(2) + f(X) = 2Y \\ f(2X) &= f(2)f(X) = 2f(X) = y + 2 \\ f(1 + 2X) &= f(1) + f(2X) = Y \\ f(2 + 2X) &= f(2) + f(2X) = y + 1 \end{aligned}$$

$$\begin{aligned} g(0) &= 0 \\ g(1) &= 1 \\ g(2) &= 2 \\ g(X) &= Y + 2 \\ g(1 + X) &= g(1) + g(X) = Y \\ g(2 + X) &= g(2) + g(X) = Y + 1 \\ g(2X) &= g(2)g(X) = 2g(X) = 2Y + 1 \\ g(1 + 2X) &= g(1) + g(2X) = 2Y + 2 \\ g(2 + 2X) &= g(2) + g(2X) = 2Y \end{aligned}$$

Osservazione. $X \in K$ non è un generatore di $K \setminus \{0\}$.

Infatti il sottogruppo del gruppo moltiplicativo $K \setminus \{0\}$ generato da X è

$$\langle X \rangle = \{X, 2, 2X, 1\} \subsetneq K \setminus \{0\}$$

Lemma 1.88. se K è un anello commutativo di caratteristica prima p, allora

$$(X+Y)^{p^h} = X^{p^h} + Y^{p^h}$$

per ogni $x, y \in K, h \geq 1$

Dimostrazione. Sia $h = 1$. se $p > k > 0$, p divide tutti i coefficienti binomiali $\binom{p}{k} := \frac{p!}{k!(p-k)!}$ perché non divide $k!(p-k)!$. Allora:

$$(X+Y)^p = \sum_{k=0}^{p} \binom{p}{k} X^k Y^{p-k} = X^p + Y^p$$

la tesi segue per induzione. ∎

Definizione 1.89 — Automorfismo di Frobenius. Dal lemma precedente segue che se K è un campo di caratteristica p, allora la funzione

$$\begin{aligned} \Phi : \ & K \to K \\ & x \mapsto x^p \end{aligned}$$

è un morfismo di campi. Infatti $\forall\, x, y \in K$:

$$\begin{aligned} \Phi(x+y) &= (x+y)^p = x^p + y^p = \Phi(x) + \Phi(y) \\ \Phi(xy) &= (xy)^p = x^p y^p = \Phi(x)\Phi(y) \end{aligned}$$

Se $K = \mathbb{F}_{p^n}, \Phi$ è un automorfismo (essendo morfismo iniettivo da un campo di cardinalità finita in se stesso) detto **automorfismo di Frobenius**.

Teorema 1.90. Il gruppo degli automorfismi di $\mathbb{F}_{p^n}, AUT(\mathbb{F}_p^n)$ è ciclico di cardinalità n, generato dall'automorfismo di Frobenius.

Lemma 1.91. sia F un campo. Il polinomio $X^d - 1$ divide il polinomio $X^n - 1$ s.s.e. d divide n.

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

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

quindi $X^d - 1$ divide $X^n - 1$ s.s.e. $X^r - 1$ è il polinomio nullo, cioè s.s.e. $r = 0$ ∎

Lemma 1.92. Sia F un campo. Il polinomio $X^d - 1$ divide il polinomio $X^n - 1$ s.s.e. d divide n.

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

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

Quindi $X^d - 1$ divide $X^n - 1$ s.s.e. $X^r - 1$ è il polinomio nullo, cioè s.s.e. $r = 0$ ∎

Dalla fattorizzazione nella dimostrazione del lemma otteniamo che, calcolando in p, se $p^d - 1$ divide $p^n - 1$ allora d divide n.

Corollario 1.93. 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 1.94. 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 $X^{p^n} - X \underbrace{\implies}_{\text{corollario}} d$ 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 $\mathbb{F}_{p^n}$. ■

Finora, dato un numero primo p e un numero naturale $n \neq 0$, abbiamo costruito il campo $\mathbb{F}_{p^n}$ di cardinalità p^n prendendo un polinomio irriducibile $Q \in \mathbb{F}_p$ e facendo il quoziente:

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

Abbiamo visto che due campi costruiti in questo modo sono isomorfi.

Facciamo alcune osservazioni e un discorso più generale.

1. Sia K un campo finito. qual'è la caratteristica di K?

   Prendiamo il sottogruppo $\langle 1_K \rangle \subseteq K$. Poiché $\langle 1_K \rangle$ è finito, $\langle 1_K \rangle \simeq \mathbb{Z}_n$ per qualche $n > 1$.

   Dato che gli elementi di $\langle 1_K \rangle$ sono di un campo, non sono divisori dello zero, quindi n è primo, ossia un campo finito ha caratteristica prima p e il suo sottocampo fondamentale è $\mathbb{F}_p$

2. Sia K un campo finito. Abbiamo detto nel punto 1. che $\mathbb{F}_p \subseteq K$ per qualche primo p.

   Inoltre il gruppo moltiplicativo $K \setminus \{0\}$ è ciclico e quindi, come precedentemente dimostrato, $se K \setminus \{0\} = \alpha, K = \mathbb{F}_p(\alpha)$.

   Quindi, se il grado di α su $\mathbb{F}_p$ è n, abbiamo che: $|K| = p^n$, ossia ogni campo finito ha cardinalità p^n, per qualche p primo e $n \neq 0$.

3. Siano K_1 e K_2 due campi finiti di cardinalità p^n.

   Sia $K_1 = \mathbb{F}_p(\alpha)$ dove α è un generatore del gruppo $K_1 \setminus \{0\}$ e ha grado n su K_1.

   Sia $Q \in \mathbb{F}_p[X]$ il suo polinomio minimo. Quindi $deg(Q) = n$, e Q è irriducibile.

   a) K_1 e K_2 sono campi di spezzamento di $X^{p^n} - X \in \mathbb{F}_p[X]$.
   b) Ogni polinomio irriducibile di grado n in $\mathbb{F}_p[X]$ è fattore di $X^{p^n} - X$.
   c) Da b) segue che Q ha una radice in K_2, la chiamiamo β.
   d) L'assegnazione $\alpha \to \beta$ definisce un morfismo di campi da K_1 in K_2.

      Poiché un morfismo tra campi è sempre iniettivo, ed essendo anche suriettivo, perché K_1 e K_2 hanno la stessa cardinalità, è un isomorfismo:

      $$K_1 \simeq K_2$$

1.14 Algoritmo di Berlekamp

Teorema 1.95. 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:

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

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

$$\begin{aligned} f(x) &= MCD\{f(x), h(x)^p - h(x)\} = \\ &= MCD\{f(x), h(x)[h(x)-1]\cdot\ldots\cdot[h(x)-p+1]\} = \\ &= MCD\{f,h\}\cdot MCD\{f,h-1\}\cdot\ldots\cdot MCD\{f,h-p+1\} \end{aligned}$$

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

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

Proposizione 1.96. Un polinomio $h(x) \in \mathbb{F}_p[x]$ che soddisfa le condizioni del teorema esiste sempre.

Dimostrazione. Sia

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

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

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

si ha che

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

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

$$\begin{aligned} &[h(x)^p - h(x)] \bmod f = 0 \bmod f \\ &\iff h(x)^p \bmod f = h(x) \bmod f \\ &\iff b_0 r_0(x) + b_1 r_1(x) + \ldots + b_{d-1}r_{d-1}(x) = b_0 + b_1 x + \ldots + b_{d-1}x^{d-1} \end{aligned}$$

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 fattorizzazione di $f(x) \in \mathbb{F}_p[x]$ in fattori irriducibili.
Supponiamo che f non abbia fattori multipli (verificabile con Teorema seguente). ■

Teorema 1.97. 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.

$$MCD\{p_i(x), p_j(x)\} = 1, \forall \quad \leq i \leq k, 1 \leq j \leq k, i \neq j$$

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

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

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

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 $h(x)^p - h(x)$.

Esempio. Fattorizziamo $f = x^5 + x^2 + 2x + 1 \in \mathbb{F}_3[x]$.
Verifichiamo che $MCD\{f, f'\} = MCD\{x^5 + x^2 + 2x + 1, 2x^4 + 2x + 2\} = 1$ poi calcoliamo i resti:

$$\begin{aligned} x^{3(5-1)} &= x^{12} \equiv (x^2 + 2) \bmod f \\ x^{3\cdot 3} &= x^9 \equiv (2x^4 + x^3 + x^2 + 2x + 2) \bmod f \\ x^{3\cdot 2} &= x^6 \equiv (2x^3 + x^2 + 2x) \bmod f \\ x^3 &\equiv x^3 \bmod f \\ 1 &\equiv 1 \bmod f \end{aligned}$$

$$\begin{aligned} \implies b_0 + b_1 x^3 + b_2(2x^3 + x^2 + 2x) +& \\ + b_3(2x^4 + x^3 + x^2 + 2x + 2) +& \\ + b_4(x^2 + 2) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4& \end{aligned}$$

$$\begin{cases} 2b_3 + 2b_4 = 0 \\ 2b_2 + 2b_3 - b_1 = 0 \\ \cancel{b_2} + b_3 + b_4 - \cancel{b_2} = 0 \\ b_1 + 2b_2 = 0 \\ 2b_3 - b_4 = 0 \end{cases} \iff \begin{cases} b_3 = 2b_4 \\ b_1 + b_2 + b_3 = 0 \\ b_1 = b2 \end{cases} \iff b_1 = b_2 = b_3 = 2b_4$$

Una soluzione è dunque $(0, 1, 1, 1, 2)$, ossia $h(x) = x + x^2 + x^3 + 2x^4$. quindi:

$$\begin{aligned} f(x) &= MCD\{f, x + x^2 + x^3 + 2x^4\} \cdot MCD\{f, 1 + x^2 + x^3 + 2x^4\} \cdot MCD\{f, 2 + x^2 + x^3 + 2x^4\} = \\ &= (1 + x^2)(x^3 + 2x + 1) \end{aligned}$$

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

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

$$\begin{aligned} r_0 &= 1 \bmod f(x) \\ r_1 &= x^p \bmod f(x) \\ &\vdots \\ r_{d-1} &= x^{p(d-1)} \bmod f(x) \end{aligned}$$

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

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

A_{ij} = 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 1.98. 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 $dim(Ker(A - I)) \geq 1$.

Infatti la d-tupla $(b_0, 0, \ldots, 0)$ 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 $\mathbb{F}_p^k$ 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:

$$\begin{aligned} Ker(\varphi) &= \{(s_1, \ldots s_k) \in \mathbb{F}_p^k : s_i \bmod p_i = 0, \forall\, 1 \leq i \leq k\} \\ &= \{(0, \ldots, 0)\} \end{aligned}$$

c) φ è suriettiva:

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

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

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

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 $p_1, \ldots, p_k$ sono tutti distinti

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

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

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

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

Esempio. In $\mathbb{F}_3[x]$ consideriamo il polinomio $f = 1 + 2x + 2x^2 + x^5 + x^6 + x^7$.

Si ha che

$$f' = 2 + 4x + 5x^4 + 7x^6 = 2 + x + 2x^4 + x^6$$

e

$$\begin{aligned} MCD\{f, f'\} = 1 + 2x + x^3 =: D \\ \frac{f}{D} = 1 + 2x^2 + x^3 + x^4 \end{aligned}$$

fattorizzando $\frac{f}{D}$ otteniamo $\frac{f}{D} = (x+1)(1 + 2x + x^3)$.

Dato che D non ha radici in $\mathbb{F}_3$, D è irriducibile. Allora

$$f = \frac{f}{D} \cdot D = (x+1)(1 + 2x + x^3)^2$$

Capitolo 2

Tensori

2.1 Prodotto tra matrici

Definizione 2.1 — Prodotto righe per colonne di matrici 2 x 2. Sia

$$Mat_{2\times 2}(K) = \{\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} : x_i \in K\}$$

l'insieme delle matrici 2 x 2 a coefficienti in un campo K.

Diamo all'insieme una struttura di anello:

- Somma: $\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} + \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} = \begin{pmatrix} x_1+y_1 & x_2+y_2 \\ x_3+y_3 & x_4+y_4 \end{pmatrix}$
- Prodotto: $\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \cdot \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} = \begin{pmatrix} x_1y_1+x_2y_3 & x_1y_2+x_2y_4 \\ x_3y_1+x_4y_3 & x_3y_2+x_4y_4 \end{pmatrix}$

Con queste operazioni $Mat_{2\times 2}(K)$ è un anello con unità $\begin{pmatrix} 1_k & 0 \\ 0 & 1_k \end{pmatrix}$.

Il prodotto così definito richiede di eseguire 8 moltiplicazioni.

Analogamente possiamo dotare $Mat_{n\times n}(K)$ di una struttura di anello.

La moltiplicazione righe per colonne richiede l'esecuzione di n^3 moltiplicazioni.

Esempio. In $Mat_{3\times 3}(\mathbb{F}_2)$ abbiamo

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Definizione 2.2 — Algorimo di Strassen per il prodotto di matrici 2 x 2. Sia

$$A = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} \quad \text{e} \quad AB = \begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix}$$

Definiamo

$$\begin{aligned}
\mathrm{I} &:= (x_1 + x_4)(y_1 + y_4) \\
\mathrm{II} &:= (x_3 + x_4)y_1 \\
\mathrm{III} &:= x_1(y_2 + y_4) \\
\mathrm{IV} &:= x_4(-y_1 + y_3) \\
\mathrm{V} &:= (x_1 + x_2)y_4 \\
\mathrm{VI} &:= (-x_1 + x_3)(y_1 + y_2) \\
\mathrm{VII} &:= (x_2 - x_4)(y_3 + y_4)
\end{aligned}$$

Allora

$$\begin{aligned}
z_1 &= \mathrm{I} + \mathrm{IV} - \mathrm{V} + \mathrm{VII} \\
z_2 &= \mathrm{III} + \mathrm{V} \\
z_3 &= \mathrm{II} + \mathrm{IV} \\
z_4 &= \mathrm{I} + \mathrm{III} - \mathrm{II} + \mathrm{VI}
\end{aligned}$$

Esempio. In $Mat_{2\times 2}(\mathbb{F}_2)$ siano

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Allora

$$\mathrm{I} := 0,\ \mathrm{II} := 0,\ \mathrm{III} := 1,\ \mathrm{IV} := 0,\ \mathrm{V} := 0,\ \mathrm{VI} := 0,\ \mathrm{VII} := 0$$

Quindi

$$AB = \begin{pmatrix} \mathrm{I} + \mathrm{IV} - \mathrm{V} + \mathrm{VII} & \mathrm{III} + \mathrm{V} \\ \mathrm{II} + \mathrm{V} & \mathrm{I} + \mathrm{III} - \mathrm{II} + \mathrm{VI} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

Nell'algoritmo di Strassen per matrici 2 x 2 si eseguono 7 moltiplicazioni.

L'algoritmo può anche essere usato ricorsivamente per moltiplicare matrici più grandi. Ad esempio, se $M, N \in Mat_{4\times 4}(K)$, possiamo scrivere:

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad \text{e} \quad N = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \qquad \text{dove} \quad A, B, C, D, A', B', C', D' \in Mat_{2\times 2}(K)$$

poiche $MN = \begin{pmatrix} AA' + BC' & AB' + BD' \\ CA' + DC' & CB' + DD' \end{pmatrix}$ Possiamo usare l'algoritmo in due passi.

Primo passo:

$$\begin{aligned}
\mathrm{I} &:= (A + D)(A' + D') \\
\mathrm{II} &:= (C + D)A' \\
\mathrm{III} &:= A(B' + D') \\
\mathrm{IV} &:= D(-A' + C') \\
\mathrm{V} &:= (A + B)D' \\
\mathrm{VI} &:= (-A + C)(A' + B') \\
\mathrm{VII} &:= (B - D)(C' + D')
\end{aligned}$$

E quindi

$$MN = \begin{pmatrix} \mathrm{I} + \mathrm{IV} - \mathrm{V} + \mathrm{VII} & \mathrm{II} + \mathrm{V} \\ \mathrm{III} + \mathrm{IV} & \mathrm{I} + \mathrm{III} - \mathrm{II} + \mathrm{VI} \end{pmatrix}$$

Secondo passo: calcoliamo il prodotto in $\mathrm{I}, \mathrm{II}, \mathrm{III}, \ldots, \mathrm{VII}$ con l'algoritmo di Strassen.

Quindi l'algoritmo di Strassen per il prodotto tra due matrici 4 x 4 richiede 7^2 moltiplicazioni.

Se vogliamo moltiplicare matrici 3 x 3 possiamo aggiungere una riga e una colonna di zeri e considerarle 4 x 4.

In generale la moltiplicazione di due matrici n x n usando l'algoritmo di Strassen richiede 7^k moltiplicazioni. Se $n = 2^k$ abbiamo che:

$$7^k = 2^{\log_2 7^k} = 2^{k \log_2 7} \approx 2^{2.81}$$

Definizione 2.3 — Esponente w della moltiplicazione di matrici.

$$w := \inf\{h \in \mathbb{R} : Mat_{n\times n}(K) \text{ può essere moltiplicato con } O(n^h) \text{ operazioni aritmetiche}\}$$

L'algoritmo di Strassen mostra che $w \leq 2.81$.

Se $n = 2$ l'algoritmo di Strassen è ottimale (dal Teorema di Brockett-Dobkin).

Non è noto un algoritmo ottimale per la moltiplicazione matrici 3 x 3.

Nel 2022 è stato pubblicato un algoritmo trovato da Alphatensor per matrici 4 x 4 su $\mathbb{F}_2$.

che richiede l'esecuzione di 47 moltiplicazioni, l'algoritmo di Strassen ne richiederebbe 49.

2.2 Anello degli endomorfismi

Definizione 2.4 — Endomorfismo di spazi vettoriali. Siano V, W spazi vettoriale su un campo K.

Una funzione $f : V \to W$ è un endomorfismo di spazi vettoriali se:

$$f(av_1 + bv_2) = af(v_1) + bf(v_2) \qquad \forall\, a, b \in K \quad v_1, v_2 \in K$$

Un morfismo $f : V \to V$ di spazi vettoriali è detto endomorfismo di V.

L'insieme $End(V) = \{f : V \to V : f \text{ è un endomorfismo di } V\ \}$.

E' un anello con le operazioni di somma e composizione di funzioni con unità la funzione identità $Id_v : V \to V$.

Se $dim(V) > 1$ l'anello non è commutativo.

Definizione 2.5. Sia $Mat_{n\times n}(K)$ l'insieme delle matrici $n \times n$ a coefficienti in K con le operazioni di somma e prodotto righe per colonne.

L'insieme $Mat_{n\times n}(K)$ è un anello, con unità la matrice identità

$$Id_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Ad un endomorfismo $f \in End(V)$, se $dim(V) = n$, possiamo associare una matrice nel seguente modo:

Sia $\{e_1, \dots e_n\}$ una base di V.

Sia

$$f(e_1) = a_{1i}e_1 + a_{2i}e_2 + \dots + a_{ni}e_n \quad a_{1i}, \dots, a_{ni} \in K \quad \forall\, 1 \leq i \leq n$$

Allora la matrice $M(f)$ associata a f è:

$$\begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix}$$

Teorema 2.6. Sia V uno spazio vettoriale di dimensione n su un campo K.
Allora la funzione

$$\begin{aligned} M: \ End(V) &\to Mat_{n\times n}(K) \\ f &\mapsto M(f) \end{aligned}$$

è un isomorfismo di anelli.

Esempio. Si consideri il campo

$$\mathbb{F}_4 := {}^{\mathbb{F}_2[x]}\big/_{\langle 1+x+x^2\rangle}$$

$\mathbb{F}_4$ è uno spazio vettoriale di dimensione 2 sul campo $\mathbb{F}_2$. Nella base $\{1, x\}$ di $\mathbb{F}_4$ l'automorfismo di Frobenius

$$\begin{aligned} \Phi: \ \mathbb{F}_4 &\to \mathbb{F}_4 \\ v &\mapsto v^2 \end{aligned}$$

che è un morfismo di spazi vettoriali ($\Phi(y) = y \; \forall\, y \in \mathbb{F}_2$) è rappresentato dalla matrice

$$M(\Phi) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

infatti $\Phi(1) = 1, \Phi(x) = x^2 = 1 + x$. Dato che $[(\Phi)]^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ una rappresentazione matriciale di $Aut(\mathbb{F}_4)$ è

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

in rappresentazione matriciale gli endomorfismi di $\mathbb{F}_4$, come spazio vettoriale, sono l'insieme di 16 matrici

$$Mat_{2\times 2}(\mathbb{F}_2) = \left\{ \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} : x_i \in \mathbb{F}_2 \right\}$$

Esempio — automorfismi di $\mathbb{F}_4$ come s.v su $\mathbb{F}_2$. Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ una matrice invertibile a coefficienti in $\mathbb{F}_2$.

A rappresenta un automorfismo di $\mathbb{F}_4$ come spazio vettoriale.

A è invertibile se e solo se

$$detA = ad - bc \neq 0 \iff detA = 1$$

$$\begin{aligned} a = 0 &\implies bc = 1 \implies b = c = 1 \\ b = 0 &\implies ad = 1 \implies a = d = 1 \\ c = 0 &\implies ad = 1 \implies a = d = 1 \\ d = 0 &\implies bc = 1 \implies b = c = 1 \end{aligned}$$

quindi, come spazio vettoriale,

$$Aut(\mathbb{F}_4) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

invece, come campo, avevamo che

$$Aut(\mathbb{F}_4) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{\text{Identità}} \quad , \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_{\text{Automorfismo di Frobenius}} \right\}$$

2.3 Spazio duale di uno spazio vettoriale

Definizione 2.7 — Spazio Duale. Sia V uno spazio vettoriale di dimensione n su un campo K.
Sia $\{e_1, \ldots, e_n\}$ una base di V.
L'insieme

$$V^* = \{f : V \to K : \ f \text{ è un morfismo di spazi vettoriali}\}$$

è detto **spazio duale di V**.
Sia

$$e_i^*(e_j) = \begin{cases} 1 \text{ se } i = j \\ 0 \text{ se } i \neq j \end{cases} \qquad \forall\, 1 \leq i \leq n$$

L'insieme $\{e_1^*, \ldots, e_n^*\}$ è una base di V^*, in particolare $dim(V^*) = dim(V) = n$.

Esempio. Sia $V = (\mathbb{F}_2)^4$ e sia $f \in V^*$ definita da

$$f(x) = \langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, x \rangle$$

dove $\langle \ldots \rangle$ è il prodotto scalare canonico su $(\mathbb{F}_2)^4$.
Dunque, se

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \qquad f(x) = x_1 + x_2 + x_3 + x_4 \quad \text{e} \quad f = e_1^* + e_2^* + e_3^* + e_4^*$$

ad esempio

$$f \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 1 + 1 + 1 + 1 = 0 \qquad f \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 0 + 1 + 1 + 1 = 1$$

2.4 Forme bilineari e prodotto tensoriale

Definizione 2.8 — Forma bilineare. Sia V uno spazio vettoriale di dimensione n su un campo K.
Indichiamo con $\{e_1, \ldots, e_n\}$ una base di V.
Una funzione $f : V \times V \to K$ è detta **forma bilineare** su V se:

1. $f(av_1, v_2) = f(v_1, av_2) = af(v_1, v_2), \forall\, a \in K, v_1, v_2 \in V$
2. $f(v_1 + v_2, w) = f(v_1, w) + f(v_2, w)$
   $f(w, v_1 + v_2) = f(w, v_1) + f(w, v_2) \quad \forall\, v_1, v_2, w \in V$

Definizione 2.9 — Prodotto Tensoriale. Siano $f, f_1, f_2 : V \times V \to K$ forme bilineari.
Se definiamo

- $f_1 + f_2 : V \times V \to K$ con $(f_1 + f_2)(v, w) = f_1(v, w) + f_2(v, w)\ \forall\, v, w \in V$

- $af : V \times V \to K$ con $(af)(v,w) = af(v,w)\ \forall\, v,w \in V$ e $a \in K$

allora $f_1 + f_2$ e af sono forme bilineari.

Quindi l'insieme delle forme bilineari su V è uno spazio vettoriale che denotiamo con

$$V^* \otimes V^*$$

e chiamiamo **Prodotto tensoriale di V^* con V^***

Siano $1 \leq i,j \leq n$. Indichiamo con $e_i^* \otimes e_j^* : V \times V \to K$ la forma bilineare su V tale che:

$$e_i^* \otimes e_j^*(e_h, e_k) = \delta_{ih}\delta_{jk} = \begin{cases} 1_k & \text{se } i = h, j = k \\ 0 & \text{altrimenti} \end{cases}$$

dove

$$\delta_{ih} = \begin{cases} 1 & \text{se } i = h \\ 0 & \text{altrimenti} \end{cases} \qquad \text{(delta di Kronecker)}$$

L'insieme $\{e_i^* \otimes e_j^* : 1 \leq i,j \leq n\}$ è una base dello spazio vettoriale $V^* \otimes V^*$.

Abbiamo che

$$e_i^* \otimes e_j^*(e_h, e_k) = e_i^*(e_h)e_j^*(e_k)$$

Se $u, v \in V^*$ allora $u \otimes v(x,y) = u(x)v(y), \forall\, x, y \in V$.

$$\text{Se } u = u_1 e_1^* + \ldots + u_n e_n^* \text{ e}$$
$$v = v_1 e_1^* + \ldots + v_n e_n^*$$

allora

$$u \otimes v = \sum_{j=1}^{n}\sum_{i=1}^{n} u_i v_j e_i^* \otimes e_j^*(x,y)$$

Quindi

$$(u_1 e_1^* + \ldots + u_n e_n^*) \otimes (v_1 e_1^* + \ldots + v_n e_n^*) =$$
$$= \sum_{j=1}^{n}\sum_{i=1}^{n} u_i v_j e_i^* \otimes e_j^*$$

Esempio. Sia $\langle \ldots \rangle$ il prodotto scalare canonico su K^n, ossia

$$\text{se } v = v_1 e_1 + \ldots + v_n e_n \text{ e}$$
$$w = w_1 e_1 + \ldots + w_n e_n$$

allora $\langle v, w \rangle = v_1 w_1 + \ldots + v_n w_n$.

Il prodotto scalare canonico è una forma bilineare simmetrica su V e come elemento di $(K^n)^* \otimes (K^n)^*$ si scrive

$$e_1^* \otimes e_1^* + e_2^* \otimes e_2^* + \ldots + e_n^* \otimes e_n^*$$

Ad una forma bilineare f su V possiamo associare una matrice $M(f)$ in $Mat_{n \times n}(K)$ nel seguente modo.

La componente $M(f)_{ij}$ di coordinate i, j è l'elemento $f(e_i, e_j) \in K$, In tal modo $f(u,v) = \langle u, M(f)v \rangle$ $\forall\, u, v \in V$.

Cioè $M(f)_{ij}$ = coordinata di f nella base $\{e_i^* \otimes e_j^*\}$ di $V^* \otimes V^*$

Esempio.

- la matrice del prodotto scalare canonico è la matrice identità.
- alla forma bilineare

$$e_1^* \otimes e_2^* - e_2^* \otimes e_1^* \in (K^2)^* \otimes (K^2)^*$$

corrisponde la matrice

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

si nota che è una forma bilineare antisimmetrica.

- La forma bilineare antisimmetrica

$$e_1^* \otimes e_3^* - e_3^* \otimes e_1^* + e_2^* \otimes e_4^* - e_4^* \otimes e_2^* \in (K^4)^* \otimes (K^4)^*$$

è detta forma simplettica, e la sua matrice associata è

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

Abbiamo quindi definito un isomorfismo di spazi vettoriali

$$\begin{aligned} M: \ V^* \otimes V^* &\to Mat_{n\times n}(K) \\ f &\mapsto M(f) \end{aligned}$$

Quindi se

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in Mat_{n\times n}(K)$$

La forma bilineare $f \in V^* \otimes V^*$ associata a A è

$$f = (a_{11}e_1^* + \ldots + a_{n1}e_n^*) \otimes e_1^* + \ldots + (a_{1n}e_1^* + \ldots + a_{nn}e_n^*) \otimes e_n^*$$

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

$$\begin{aligned} f &= (e_1^* + 2e_2^*) \otimes e_1^* + (2e_1^* + e_2^*) \otimes e_2^* = \\ &= e_1^* \otimes e_1^* + 2e_2^* \otimes e_1^* + 2e_1^* \otimes e_2^* + e_2^* \otimes e_2^* \end{aligned}$$

Nota. Essendo $v^* \otimes V^*$ lo spazio vettoriale delle forme bilineare su V, si ha che:

1. $a(e_i^* \otimes e_j^*) = (ae_i^*) \otimes e_j^* = e_i^* \otimes (ae_j^*)$
2. $e_i^* \otimes (e_j^* + e_k^*) = e_i^* \otimes e_j^* + e_i^* \otimes e_k^*$

Esempio. Siano $v_1 := 3e_1^* + 2e_2^* + e_3 \in (\mathbb{R}^3)^*$ e $v_2 := e_2^* - \sqrt{3}e_3^* \in (\mathbb{R}^3)^*$.
Allora

$$\begin{aligned} v_1 \otimes v_2 &= (3e_1^* + 2e_2^* + e_3^*) \otimes (e_2^* - \sqrt{3}e_3^*) = \\ &= 3e_1^* \otimes e_2^* - 3\sqrt{3}e_1^* \otimes e_3^* + 2e_2^* \otimes e_2^* - 2\sqrt{3}e_2^* \otimes e_3^* + e_3^* \otimes e_2^* - \sqrt{3}e_3^* \otimes e_3^* \end{aligned}$$

Definizione 2.10 — Forma multilineare. Siano $V_1, V_2, \ldots, V_k$ spazi vettoriali su un campo $\mathbb{F}$. Una funzione

$$f: V_1 \times V_2 \times \ldots \times V_k \to \mathbb{F}$$

è detta **forma multilineare** se è lineare rispetto ad ogni variabile, cioè se:

1.

$$\begin{aligned} f(av_1, \ldots, v_k) &= f(v_1, av_2, \ldots, v_k) = \\ &= f(v_1, \ldots, av_k) = \\ &= af(v_1, \ldots v_k) \qquad \forall\, a \in \mathbb{F}, v_i \in V_i \end{aligned}$$

2.

$$\begin{aligned} f(v_1 + w_1, v_2, \ldots, v_k) &= f(v_1, \ldots, v_k) + f(w_1, \ldots, v_k) \\ &\vdots \\ f(v_1, v_2, \ldots, v_k + w_k) &= f(v_1, \ldots, v_k) + f(v_1, \ldots, w_k) \qquad \forall\, v_i, w_i \in V_i \end{aligned}$$

2.4.1 Prodotto tensoriale di spazi vettoriali

Definizione 2.11. Siano $V_1, V_2, \ldots, V_k$ spazi vettoriali su un campo $\mathbb{F}$.
Definiamo $V_1 \otimes V_2 \otimes \ldots \otimes V_k$ lo spazio vettoriale delle forme multilineari

$$f : V_1 \times V_2 \times \ldots \times V_k \to \mathbb{F}$$

Una base di $V_1 \otimes V_2 \otimes \ldots \otimes V_k$ è l'insieme

$$\{e_{i_1}^{1^*} \otimes e_{i_2}^{2^*} \otimes \ldots \otimes e_{i_k}^{k^*} : 1 \leq i_1 \leq dim(V_1), \ldots, 1 \leq i : k \leq dim(V_k)\}$$

dove $\{e_{i_1}^{1^*}\}$ è una base di V_1^*, ecc.

2.5 Rango di una matrice

Definizione 2.12. Sia $A \in Mat_{h \times k}(\mathbb{F})$ una matrice $h \times k$.
Il rango di A è definito come:

$$\begin{aligned} rk(A) &:= \text{ n° massimo di colonne linearmente indipendenti} \\ &:= \text{ n° massimo di righe linearmente indipendenti} \end{aligned}$$

Si verifica facilmente che ogni matrice si può scrivere come combinazione lineare di matrici di rango 1.
Sia $X = \{A \in Mat_{h \times k}(\mathbb{F}) : rk(A) = 1\}$, allora si ha che

$$rk(A) = min\{k \in \mathbb{N} : A = \sum_{i=1}^{k} M_i, M_i \in X, \forall\, 1 \leq i \leq k\}$$

Esempio. La matrice

$$A = \begin{pmatrix} 1 & -1 & 3 \\ 2 & 4 & -6 \\ 3 & 0 & 3 \end{pmatrix}$$

ha rango 2, e si ha che:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 3 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -1 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & -6 \\ 0 & 0 & 3 \end{pmatrix}$$

che è una combinazione lineare di matrici di rango 1, un altra è:

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 2 \\ 3 & 0 & 3 \end{pmatrix} + \begin{pmatrix} 0 & -1 & 2 \\ 0 & 4 & -8 \\ 0 & 0 & 0 \end{pmatrix}$$

ovviamente è la minima perché $rk(A) = 2$

Come è fatta una matrice di rango 1 in $Mat_{a\times b}(K)$?

Tutte le sue colonne sono proporzionali ad un vettore colonna $\overrightarrow{v} \in K^a \setminus \{\overrightarrow{0}\}$.

Quindi, se $A \in Mat_{a\times b}(K)$ e $rk(A) = 1$, esistono $a_1, \dots, a_b \in K$ tali che:

$$A = \begin{pmatrix} a_1\overrightarrow{v} & a_2\overrightarrow{v} & \dots & a_b\overrightarrow{v} \end{pmatrix}$$

Quindi

$$A = \overrightarrow{v}\begin{pmatrix} a_1 & a_2 & \dots & a_b \end{pmatrix} = \overrightarrow{v}\,\overrightarrow{a}^T \quad \text{dove} \quad \overrightarrow{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_b \end{pmatrix} \in K^b \setminus \{\overrightarrow{0}\}$$

Come è fatta una matrice $A \in Mat_{a\times b}(K)$ di rango k?

Siano $\overrightarrow{v_1}, \dots, \overrightarrow{v_k} \in K^a \setminus \{\overrightarrow{0}\}$ colonne linearmente indipendenti.

Le altre colonne sono combinazione lineare di queste e quindi esistono $\overrightarrow{a_1}, \dots, \overrightarrow{a_k} \in K^b \setminus \{\overrightarrow{0}\}$ tali che:

$$A = \overrightarrow{v_1}\overrightarrow{a_1}^T + \dots + \overrightarrow{v_k}\overrightarrow{a_k}^T$$

Cioè A si scrive come somma di k matrici di rango 1.

Se si potesse scrivere con meno addendi avrebbe rango $< k$.

Quindi $rk(A) = min\{k \in N : A = \sum_{i=1}^{k} M_i, rk(M_i) = 1 \forall\, 1 \le i \le k\}$

D'ora in poi se $V_1, \dots, V_h$ sono spazi vettoriali su un campo K con basi

$$\{v_1^1, \dots v_{i_1}^1\}, \{v_1^2, \dots v_{i_2}^2\}, \dots, \{v_1^h, \dots v_{i_h}^h\}$$

allora $V_1 \otimes V_2 \otimes \dots \otimes V_h$ è uno spazio vettoriale con base

$$\{v_{j_1}^1 \otimes v_{j_2}^2 \otimes \dots \otimes v_{j_h}^h : 1 \le j_1 \le i_1, \dots, 1 \le j_h \le i_h\}$$

che soddisfa le seguenti Relazioni:

1.
$$\begin{aligned} a(v_{j_1}^1 \otimes v_{j_2}^2 \otimes \dots \otimes v_{j_h}^h) &= (av_{j_1}^1) \otimes v_{j_2}^2 \otimes \dots \otimes v_{j_h}^h = \\ &= \dots = v_{j_1}^1 \otimes v_{j_2}^2 \otimes \dots \otimes (av_{j_h}^h) \quad \forall\, a \in K, 1 \le j_1 \le i_1, \dots, 1 \le j_h \le i_h \end{aligned}$$

2.
$$\begin{aligned} (v_1 + w_1) \otimes v_2 \otimes \dots \otimes v_h &= v_1 \otimes v_2 \otimes \dots \otimes v_h + w_1 \otimes v_2 \otimes \dots \otimes v_h \\ &\vdots \\ v_1 \otimes v_2 \otimes \dots \otimes (v_h + w_h) &= v_1 \otimes v_2 \otimes \dots \otimes v_h + v_1 \otimes v_2 \otimes \dots \otimes w_h \\ \forall\, v_i, w_i \in V_i, 1 \le i \le h \end{aligned}$$

L'insieme $\{v_1 \otimes v_2 \otimes \dots \otimes v_h : v_i \in V_i \forall\, 1 \le i \le h\}$ è **L'insieme dei tensori di rango 1 di** $V_1 \otimes V_2 \otimes \dots \otimes V_h$

2.5.1 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 $\{v^1_{j_1} \otimes v^2_{j_2} \otimes \ldots \otimes v^h_{j_h}\}$ è costituita da tensori di rango 1.

Definizione 2.13 — Rango di un tensore. Sia $T \in V_1 \otimes V_2 \otimes \ldots \otimes V_k$.
definiamo **rango di T** e lo indichiamo $\mathbf{rk(T)}$ il minimo $r \in \mathbb{N}$ tale che:

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

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 $dim(\otimes_{i=1}^{h} V_i) = \prod_{i=1}^{h} dim(V_i)$, abbiamo che, se $T \in \otimes_{i=1}^{h} V_i$ allora $rk(T) \leq \prod_{i=1}^{h} dim(V_i)$, poiché $\otimes_{i=1}^{h} V_i$ 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 $a_1 v$, la seconda $a_2 v, \ldots, a_n v, a_i \in K$.

Quindi tale matrice di rango 1 si scrive come

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

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

$$\begin{aligned} & v_1 a_1 e_1^* \otimes e_1^* + v_2 a_1 e_2^* \otimes e_1^* + \ldots + v_1 a_2 e_1^* \otimes e_2^* + v_2 a_2 e_2^* \otimes e_2^* + \ldots + v_1 a_n e_1^* \otimes e_n^* + \ldots + v_m a_n e_m^* \otimes e_n^* = \\ & = (v_1 e_1^* + \ldots + v_m e_m^*) \otimes a_1 e_1^* + (v_1 e_1^* + \ldots + v_m e_m^*) \otimes a_2 e_2^* + \ldots + (v_1 e_1^* + \ldots + v_m e_m^*) \otimes a_n e_n^* = \\ & = (v_1 e_1^* + \ldots + v_m e_m^*) \otimes (a_1 e_1^* + \ldots + a_n e_n^*) \end{aligned}$$

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 perché $\begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ 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

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

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

$$\begin{aligned} T_A &= e_1^* \otimes e_1^* + 2e_2^* \otimes e_1^* + 2e_1^* \otimes e_3^* + e_2^* \otimes e_3^* \\ &= (e_1^* + 2e_2^*) \otimes e_1^* + (2e_1^* + e_2^*) \otimes e_3^* \\ &= (e_1^* + 2e_2^*) \otimes (e_1^* + e_3^*) \end{aligned}$$

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 $v_1 v_2^T \in Mat_{m\times n}(K)$ 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 $(K^m)^* \otimes (K^n)^*$.

2.6 Endomorfismi di V come elementi di $V^* \otimes V$

Sia V uno spazio vettoriale su un campo K con base $\{e_1, \dots, e_n\}$.

Gli elementi di $V^* \otimes V = span\{e_i^* \otimes e_j\}$ possono essere interpretati come endomorfismi di V nel seguente modo: definiamo il morfismo di spazi vettoriali

$$e_i^* \otimes e_j : V \to V \quad \text{ponendo}$$
$$e_i^* \otimes e_j(v) = \begin{cases} e_j & \text{se } h = i \\ 0 & \text{altrimenti} \end{cases}$$

ossia

$$(e_i^* \otimes e_j)(e_h) = e_i^*(e_h)e_i \qquad \forall\, 1 \leq i, j, h \leq n$$

Se $f \in END(V)$ è rappresentato dalla matrice

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

allora come elemento di $V^* \otimes V$ si scrive

$$\begin{aligned} f = {} & e_1^* \otimes (a_{11}e_1 + a_{21}e_2 + \dots + a_{n1}e_n) + \\ & + e_2^* \otimes (a_{12}e_1 + a_{22}e_2 + \dots + a_{n2}e_n) + \\ & + \dots + e_n^* \otimes (a_{1n}e_1 + \dots + a_{nn}e_n) \end{aligned}$$

viceversa, ogni elemento di $V^* \otimes V$ può essere interpretato come un endomorfismo di V e tale corrispondenza biunivoca è un isomorfismo di spazi vettoriali

$$END(V) \to V^* \otimes V$$

Esempio. Sia $V \in Mat_{2\times 2}(\mathbb{R})$ lo spazio vettoriale delle matrici 2×2 a coefficienti reali. La funzione

$$\begin{aligned} f : Mat_{2\times 2}(\mathbb{R}) &\to Mat_{2\times 2}(\mathbb{R}) \\ A &\mapsto A^T \end{aligned}$$

è un morfismo di spazi vettoriali.

Una base di V è $\{E_{ij} : 1 \leq i, j \leq 2\}$, dove

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

la matrice di f in questa base è

$$M(f) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad rk(M(f) = 4)$$

Come elemento di $V^* \otimes V$ la trasposizione si scrive

$$f = E_{11}^* \otimes E_{11} + E_{12}^* \otimes E_{21} + E_{21}^* \otimes E_{12} + E_{22}^* \otimes E_{22} \qquad rk(f) = 4$$

Invece l'elemento $g \in V^* \otimes V$ definito da

$$\begin{aligned} g &= 2E_{11}^* \otimes E_{11} + E_{12}^* \otimes (E_{12} + E_{21}) + E_{21}^* \otimes (E_{12} + E_{21}) + 2E_{22}^* \otimes E_{22} = \\ &= 2E_{11}^* \otimes E_{11} + (E_{12}^* + E_{21}^*) \otimes (E_{12} + E_{21}) + 2E_{22}^* \otimes E_{22} \qquad rk(g) = 3 \end{aligned}$$

corrisponde all'endomorfismo

$$\begin{aligned} g : Mat_{2\times 2}(\mathbb{R}) &\to Mat_{2\times 2}(\mathbb{R}) \\ A &\mapsto A + A^T \end{aligned}$$

In generale i morfismi di spazi vettoriali $f : V \to W$ sono in corrispondenza biunivoca con $V^* \otimes W$ e tale corrispondenza è un isomorfismo di spazi vettoriali

$$\underbrace{Hom(V,W)}_{\text{spazio vettoriale dei morfismi } f\,:\,V\to W} \to V^* \otimes W$$

Il rango di un morfismo $f : V \to W$ (come dimensione della sua immagine o come rango della sua matrice associata) corrisponde al rango del tensore $f \in V^* \otimes W$.

Ancora più in generale, ogni forma multilineare $f : V_1 \times \ldots \times V_h \to W$ è un elemento di $V_1^* \otimes \ldots \otimes V_h^* \otimes W$ posto

$$\begin{gathered} e_{i_1}^{1^*} \otimes e_{i_2}^{2^*} \otimes \ldots \otimes e_{i_h}^{h^*} \otimes w(v_1, v_2, \ldots v_h) = e_{i_1}^{1^*}(v_1) e_{i_2}^{2^*}(v_2) \ldots e_{i_h}^{h^*}(v_h)\, w \in W \\ \forall\, 1 \leq i_1 \leq dimV_1, \ldots, 1 \leq i_h \leq dimV_h, v_i \in V_i, w \in W \end{gathered}$$

Adesso andiamo a considerare la moltiplicazione di matrici 2×2.
Questa è una forma bilineare

$$M_{2,2,2} : Mat_{2\times 2}(K) \times Mat_{2\times 2}(K) \to Mat_{2\times 2}(K)$$

definita da $M_{2,2,2}(A, B) = AB$ (AB prodotto righe per colonne). E' una forma bilineare perché

1. $x(AB) = (xA)B = A(xB)\ \forall\, x \in K, A, B \in Mat_{2\times 2}(K)$
2. $$\begin{aligned} A(B_1 + B_2) &= AB_1 + AB_2 \\ (A_1 + A_2)B &= A_1B + A_2B \qquad \forall\, A_1, A_2, B_1, B_2, A, B, \in Mat_{2\times 2}(K) \end{aligned}$$

quindi $M_{2,2,2} \in (Mat_{2\times 2}(K))^* \otimes (Mat_{2\times 2}(K))^* \otimes Mat_{2\times 2}(K)$. In generale la moltiplicazione di matrici è un elemento

$$M_{n,n,n} \in (Mat_{n\times n}(K))^* \otimes (Mat_{n\times n}(K))^* \otimes Mat_{n\times n}(K)$$

vediamo come scrivere $M_{2,2,2}$ nella base $\{E^*_{ij} \otimes E^*_{h,k} \otimes E_{uv}\}$, dove

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

abbiamo che $E_{11}E_{11} = E_{11}, E_{12}E_{12} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \dots, E_{22}E_{22} = E_{22}$, ossia

$$E_{ij}E_{hk} = \begin{cases} E_{ik} & \text{se } j = h \\ 0 & \text{altrimenti} \end{cases}$$

quindi

$$\begin{aligned} M_{2,2,2} = {} & E^*_{11} \otimes E^*_{11} \otimes E_{11} + E^*_{12} \otimes E^*_{21} \otimes E_{11} + \\ & + E^*_{11} \otimes E^*_{12} \otimes E_{12} + E^*_{12} \otimes E^*_{22} \otimes E_{12} + \\ & + E^*_{21} \otimes E^*_{11} \otimes E_{21} + E^*_{21} \otimes E^*_{12} \otimes E_{22} + \\ & + E^*_{22} \otimes E^*_{22} \otimes E_{22} + E^*_{22} \otimes E^*_{21} \otimes E_{21} \end{aligned}$$

abbiamo anche che $rk(M_{2,2,2}) \leq 8$

$$\begin{aligned} M_{2,2,2} = {} & (E^*_{11} + E^*_{22}) \otimes (E^*_{11} + E^*_{22}) \otimes (E_{11} + E_{22}) + \\ & + (E^*_{21} + E^*_{22}) \otimes E^*_{11} \otimes (E_{21} - E_{22}) + \\ & + E^*_{11} \otimes (E^*_{12} - E^*_{22}) \otimes (E_{12} + E_{22}) + \\ & + E^*_{22} \otimes (-E^*_{11} + E^*_{21}) \otimes (E_{12} + E_{22}) + \\ & + (E^*_{11} + E^*_{12}) \otimes E^*_{22} \otimes (-E_{11} + E_{12}) + \\ & + (-E^*_{11} + E^*_{21}) \otimes (E^*_{11} + E^*_{12}) \otimes E_{22} + \\ & + (E^*_{12} - E^*_{22}) \otimes (E^*_{21} + E^*_{22}) \otimes E_{11} \end{aligned}$$

da questa fattorizzazione si ha che $rk(M_{2,2,2}) \leq 7$.

Questa fattorizzazione è l'algoritmo di Strassen per la moltiplicazione di matrici 2×2.

Notiamo che, se $A, B \in Mat_{2,2}(K)$,

$$E^*_{ij} \otimes E^*_{hk} \otimes E^*_{uv}(A, B) = E_{ij}(A)E_{hk}(B)E_{uv}$$

Quindi ogni addendo in una fattorizzazione del tensore $M_{2,2,2}$ corrisponde ad una moltiplicazione di elementi del campo K.

Allora il rango del tensore $M_{2,2,2}$ è il numero massimo di moltiplicazioni necessarie per calcolare il prodotto di due matrici 2×2.

Alcuni risultati generali. Consideriamo il campo $K = \mathbb{C}$

Teorema 2.14 — di Brockett-Dobkin (1978).

$$rk(M_{n,n,n} \geq 2n^2 - 1)$$

($M_{n,n,n}$ è il tensore della moltiplicazione di due matrici $n \times n$ sul campo $\mathbb{C}$)

Corollario 2.15.

$$rk(M_{2,2,2}) \geq 7$$

Infatti dall'algoritmo di Strassen segue che $rk(M_{2,2,2}) \leq 7$ e dal teorema di Brockett-Dobkin segue che $rk(M_{2,2,2}) \geq 7$.

Teorema 2.16 — di Bläser (1999).

$$rk(M_{n,n,n}) \geq \frac{5}{2}n^2 - 3n$$

Teorema 2.17 — di Laderman (1976).

$$rk(M_{n,n,n}) \leq 23$$

Teorema 2.18 — Deepmind (2022). Sul campo $\mathbb{F}_2$

$$rk(M_{4,4,4}) \leq 47$$
$$rk(M_{5,5,5}) \leq 96$$

Teorema 2.19 — di Kauers e Moosbauer (2022). Sul campo $\mathbb{F}_2$

$$rk(M_{5,5,5}) \leq 95$$

Capitolo 3

Logica Proposizionale

3.1 Sintassi

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

1. Insieme numerabile di variabili
2. Connettivi logici: $\neg, \wedge, \vee$

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

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

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 CNF.

Esempio. $(\neg x_1 \vee x_2) \wedge x_1 \wedge (x_2 \vee x_3)$ è una formula CNF. Chiamiamola F. Allora $VAR(F) = \{x_1, x_2, x_3\}$.
Le clausole di F sono $\{\neg x_1 \vee x_2, x_1, x_2 \vee x_3\}$ e i letterali di F sono $\{x_1, x_2, x_3, \neg x_1\}$

3.2 Semantica

Definizione 3.1 — Assegnazione appropriata. Sia F una formula CNF. Una **assegnazione appropriata a F** è una funzione

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

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

1. F è una variabile X: $V \models X$, significa che $V(X) = 1$
2. F è il letterale $\neg X$: $V \models \neg X$, significa che $V(X) = 0$
3. F è una clausola $L_1 \vee \ldots \vee L_n$: $V \models F$, significa che V soddisfa almeno uno dei letterali L_i

4. 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 $V \not\models F$.

Esempio. Sia F la formula CNF $(\neg x_1 \vee x_2) \wedge x_1 \wedge (x_2 \vee x_3)$ e sia $U : \{x_1, x_2, x_3\} \to \{0,1\}$ tale che $U(x_1) = U(x_2) = 1, U(x_3) = 0$.

Dunque

$$\begin{aligned} U(\neg x_1) &= 0 \\ U(\neg x_1 \vee x_2) &= 1 \\ U(x_2 \vee x_3) &= 1 \\ U(F) &= 1 \end{aligned}$$

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

$$\begin{aligned} V(\neg x_1) &= 0 \\ V(\neg x_1 \vee x_2) &= 0 \\ V(x_2 \vee x_3) &= 0 \\ V(F) &= 0 \end{aligned}$$

quindi $V \not\models F$.

Definizione 3.3 — 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 3.4 — 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 3.5 — 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 $F := (\neg x \vee y) \wedge x$.

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

Tale assegnazione soddisfa anche y.

Definizione 3.6 — Implicazione logica. Definiamo l'**implicazione logica** tra due formule F, G

come

$$x \implies y := \neg x \vee y$$

x	y	$x \implies y$
0	0	1
0	1	1
1	0	0
1	1	1

Definizione 3.7 — 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 riscrivere come $(x \implies y) \wedge x$.

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)
- $c \wedge c \equiv c$ e $l \vee l \equiv l$ (congiunzione e disgiunzione sono idempotenti)

Diamo altre definizioni:

Definizione 3.8 — Doppia implicazione.

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

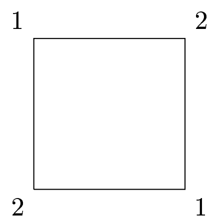
Definizione 3.9 — Negazione di formule CNF. 1. l letterale: $\neg l = \bar{l}$

2. $\neg(l_1 \vee \ldots \vee l_n) := \neg l_1 \wedge \ldots \wedge \neg l_n$
3. $\neg(c_1 \wedge \ldots \wedge c_n) := \neg c_1 \vee \ldots \vee \neg c_n$

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" $\forall\, 1 \leq i \leq 4, 1 \leq j \leq 2$

$$\begin{aligned} F := &(x_{11} \vee x_{12}) \wedge (x_{21} \vee x_{22}) \wedge (x_{31} \vee x_{32}) \wedge (x_{41} \vee x_{42}) \wedge \\ &\wedge (\neg x_{11} \vee \neg x_{12}) \wedge (\neg x_{21} \vee \neg x_{22}) \wedge (\neg x_{31} \vee \neg x_{32}) \wedge (\neg x_{41} \vee \neg x_{42}) \wedge \\ &\wedge (\neg x_{11} \vee \neg x_{21}) \wedge (\neg x_{12} \vee \neg x_{22}) \wedge (\neg x_{21} \vee \neg x_{31}) \wedge (\neg x_{22} \vee \neg x_{32}) \wedge (\neg x_{31} \vee \neg x_{41}) \end{aligned}$$

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

Capitolo 4

Logica Modale

4.1 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 $\neg, \wedge, \vee, \implies, \iff$
3. I simboli ausiliari $(,)$
4. I connettivi modali $\Box$ (**Scatola o Box**) e $\Diamond$ (**Diamante o Diamond**)

Le parole del linguaggio 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 $(A \wedge B), (A \vee B), (A \implies B), (A \iff B)$ sono FBF

Alcune letture dei simboli $\Box$ 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:

$$\Box A \equiv \neg \Diamond \neg A$$
$$\Diamond A \equiv \neg \Box \neg A$$

- 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 intuizione di negazione, disgiunzione, congiunzione.

Per la logica modale la situazione è più complicata.

Interpretando il simbolo "$\Box$" come operatore di necessità, ossia "$\Diamond$" 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

$$A \implies \Box \Diamond A \quad ?$$

Non è chiaro se sia vera o falsa. Nel caso della logica epistemica, l'operatore "$\Box$" 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 perché non si è onniscienti.

4.2 Semantica dei mondi possibili (semantica di Kripke)

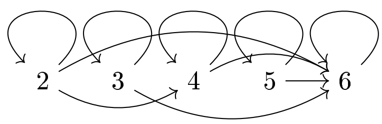
Definizione 4.1 — Frame. Un **Frame** è una coppia (S, R), dove S è un insieme non vuoto detto **insieme dei mondi** e $R \subseteq S \times S$ è una relazione su S, detta **relazione di accessibilità** (se $(x, y) \in R$ si dice che y è accessibile da x).

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 $(x, y) \in R$.

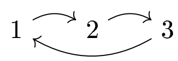
Esempio. Il frame $(\mathbb{N}, R)$, dove $R = \{(n, n+1) : n \in \mathbb{N}\} \subseteq \mathbb{N} \times \mathbb{N}$ è rappresentato dal seguente grafo diretto:

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

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



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



Definizione 4.2 — 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 4.3. 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. F è 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 4.4 — 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 4.5. 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.

Se come frame prendiamo $(0, R)$ dove $R \subseteq S \times S = \{(0,0)\}$ è quindi S stesso, una funzione di valutazione è $V : Var \to \mathcal{P}(S) = \{\varnothing, \{0\}\} \simeq \{0,1\}$.

In questo modo i connettivi modali diventano superflui e ritroviamo la logica modale che abbiamo già studiato.

La verità di una formula del linguaggio della logica modale dipenderà quindi dal frame scelto, in particolare dalla relazione R.

Ad esempio nella logica della necessità vogliamo che sia sempre vera la formula

$$\Box x \implies x \qquad \text{"è necessaria che } x\text{, allora } x\text{"}$$

Nella logica deontica la stessa formula la leggiamo "è obbligatorio che x, allora x" e non vogliamo che questa affermazione sia sempre vera.

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

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

Nella logica deontica, dove non vogliamo che sia sempre vera la formula $\Box x \implies x$, non prenderemo una relazione riflessiva.

Definizione 4.6. Una formula F si dice **vera in un modello M**, scritto $M \vDash F$, se $M \vDash_x F, \forall x \in S$, ossia se è vera in tutti i mondi di S.

Definizione 4.7. Una formula si dice **valida in un frame** (S, R), scritto $(S, R) \vDash F$, se è vera in tutti i modelli costruiti su (S, R).

Esempio. La formula $\Box x \implies x$ è valida solo nel frame (S, R) in cui R è riflessiva.

Definizione 4.8 — Formula Valida. Una formula F è **valida** se e solo se è valida su ogni frame, e scriviamo $\vDash F$

Definizione 4.9 — Schema di Formule. Uno **schema di formule** è una collezione di formule aventi tutte la stessa forma sintattica.

Ad esempio, con lo schema $\Box x \implies x$ si intendono tutte le formule di questa forma, come $\Box x \implies x$, x variabile, o $\Box(\neg\Diamond\neg x) \implies \neg\Diamond\neg x$.

Le tautologie della logica proposizionale sono valide su ogni frame.

Vediamo ora che lo schema di formule $\Box(A \implies B) \implies (\Box A \implies \Box B)$
è valido su ogni frame.

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

Sia $M \vDash_w \Box(A \implies B)$ e $M \vDash_w \Box A$. (dobbiamo solo controllare che quando $\Box(A \implies B)$ è vera, allora se è vera $\Box A$, è vera $\Box B$).

$M \vDash_w \Box(A \implies B)$ significa che $M \vDash_v A \implies B, \forall v \in S t.c. (w, v) \in R$.

$M \vDash_w \Box A$ significa che $M \vDash_v A, \forall v \in S t.c. (w, v) \in R$.

Dunque $M \models_v B, \forall\, v \in S t.c. (w,v) \in R$, ossia $M \models_w \Box B$.

Abbiamo dimostrato che

$$\models \Box(A \implies B) \implies (\Box A \implies \Box B)$$

Chiameremo K tale schema.

Mostriamo che i seguenti schemi sono validi:

1. $\Box(A \wedge B) \iff (\Box A \wedge \Box B)$
2. $\Diamond(A \vee B) \iff (\Diamond A \vee \Diamond B)$
3. $\Box(A \implies B) \implies (\Diamond A \implies \Diamond B)$
4. $\Diamond(A \implies B) \implies (\Box A \implies \Diamond B)$

1. $M \models_w \Box(A \wedge B)$ se e solo se $M \models_v A \wedge B, \forall\, v \in S t.c. (w,v) \in R$,
   se e solo se $M \models_v A$ e $M \models_v B \forall\, v \in S t.c. (w,v) \in R$,
   se e solo se $M \models_w \Box A$ e $M \models_w \Box B$,
   se e solo se $M \models_w (\Box A \wedge \Box B)$, dove M è un modello su un frame (S,R) e $w \in S$
2. $M \models_w \Diamond(A \vee B)$ se e solo se $M \models_v A \vee B, \exists\, v \in S t.c. (w,v) \in R$,
   se e solo se $M \models_v A$ o $M \models_v B \exists\, v \in S t.c. (w,v) \in R$,
   se e solo se $M \models_w \Diamond A$ o $M \models_w \Diamond B$,
   se e solo se $M \models_w (\Diamond A \vee \Diamond B)$, dove M è un modello su un frame (S,R) e $w \in S$
3. $M \models_w \Box(A \implies B)$ e $M \models_w \Diamond A$ implicano che $M \models_v (A \implies B), \forall\, v \in S t.c. (w,v) \in R$,
   e $M \models_v A, \exists\, v \in S t.c. (w,v) \in R$.
   Quindi $M \models_v B, \exists\, v \in S$ t.c. $(w,v) \in R$,
   ossia $M \models_w \Diamond B$, dove M è un modello su un frame (S,R) e $w \in S$
4. $M \models_w \Diamond(A \implies B)$ e $M \models_w \Box A$ implicano che $M \models_v (A \implies B), \exists\, v \in S t.c. (w,v) \in R$, e $M \models_v A, \forall\, v \in S t.c. (w,v) \in R$.

   Quindi $M \models_v B, \exists\, v \in S t.c. (w,v) \in R$, ossia $M \models_w \Diamond B$, dove M è un modello su un frame (S,R) e $w \in S$

Abbiamo già mostrato che se M è un modello su un frame (S,R) con R non riflessiva, allora $\Box x \implies x$ non è vera nel modello M. Quindi la formula $\Box x \implies x$ non è valida.

$$\not\models \Box x \implies x$$

Mostriamo che i seguenti schemi di formule non sono validi:

1. $\Diamond A \implies \Box A$
2. $\Box A \implies A$ (già visto)
3. $\Box A \implies \Box\Box A$
4. $\Box(A \implies B) \implies (\Box A \implies \Diamond B)$
5. $\Box(\Box A \implies B) \vee \Box(\Box B \implies A)$
6. $\Box(A \vee B) \implies (\Box A \vee \Box B)$
7. $\Box(\Box A \implies A) \implies \Box A$

1.
$$\begin{tikzcd} 1 \arrow[loop above] \arrow[r] & 2 \end{tikzcd} \qquad M = (\{1,2\}, \{(1,2),(1,1)\}, V)$$

   $V(x) = 2$ (ossia la formula x è vera solo nel mondo 2) quindi $M \models_! \Diamond x$ e $M \not\models_1 \Box x$, ossia $M \not\models_1 (\Diamond x \implies \Box x)$
2. già visto.
3.
$$1 \longrightarrow 2 \longrightarrow 3 \qquad M = (\{1,2,3\}, \{(1,2),(2,3)\}, V)$$

$V(x) = \{2\}$ Quindi $M \vDash_1 \Box x$.

Abbiamo che $M \vDash_1 \Box\Box x$ se e solo se $M \vDash_2 \Box x$, se e solo se $M \vDash_3 x$, ma $M \nvDash_3 x$, quindi $M \nvDash_1 \Box\Box x$

4.
$$\begin{tikzcd} 1 \arrow[r] & 2 \end{tikzcd} \qquad M = (\{1,2\}, V)$$

$V(x) = \{1\}$ $M \vDash_2 \Box(A \implies B)$, $M \vDash_2 \Box A$, ma $M \nvDash_2 \Diamond B$, perché non esiste $v \in \{1,2\} t.c M \vDash_v$ $, (2, v) \in R$

5. prendiamo $A = B = x$ nel frame
$$\begin{tikzcd} 1 \arrow[r] & 2 \arrow[r] & 3 \end{tikzcd} \qquad M = (\{1,2,3\}, \{(1,2),(2,3)\}, V)$$

$V(x) = \{3\}$, si ha $M \vDash_1 \Box(\Box x \implies x)$ se e solo se $M \vDash_2 \Box x \implies x$, se e solo se $M \vDash_3 x$ e $M \nvDash_2 x$, ma $M \nvDash_2 \Box x$, quindi $M \nvDash_1 \Box(\Box x \implies x)$

6.
$$\begin{tikzcd} 1 \arrow[loop above] \arrow[r] & 2 \end{tikzcd} \qquad M = (\{1,2\}, \{(1,2),(1,1),\}, V)$$

$V(x) = \{1\}, V(y) = \{2\}$ $M \vDash_1 \Box(x \vee y)$ se e solo se $M \nvDash_1 (x \vee y)$ e $M \nvDash_2 (x \vee y)$.

Quindi abbiamo che $M \nvDash_1 \Box(x \vee y)$.

Invece $M \vDash_1 (\Box x \vee \Box y)$ se e solo se $M \vDash_1 x$ e $M \vDash_2 x$ o $M \vDash_1 y$ e $M \vDash_2 y$, Dunque $M \nvDash_1 (\Box x \vee \Box y)$

7.
$$\begin{tikzcd} 1 \arrow[loop above] \arrow[r] & 2 \arrow[r] & 3 \end{tikzcd} \qquad M = (\{1,2,3\}, \{(1,2),(2,3)\}, V)$$

$V(x) = \{2,3\}$ $M \vDash_1 \Box(\Box x \implies x)$ se e solo se $M \vDash_1 (\Box x \implies x)$ e $M \vDash_2 (\Box x \implies x)$, che sono entrambe vere, quindi $M \vDash_1 \Box(\Box x \implies x)$ invece $M \nvDash_1 \Box x$ perché $M \nvDash_1 x$.

4.3 Corrispondenza e Non Esprimibilità

Definizione 4.10. diciamo che un frame (S, R) gode di una certa proprietà se ne gode la relazione R.

In molti casi una proprietà di un frame equivale alla validità di uno schema di formule modali nei frame con quella proprietà.

Teorema 4.11. Lo schema $\Box A \implies A$ è valido in un frame (S, R) se e solo se R è riflessiva.

Dimostrazione. Già visto. ■

Teorema 4.12. 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. $(t, r) \in R e M \vDash_r x$, ossia $r = s$ ■

Teorema 4.13. Lo schema $\Box A \implies \Box\Box A$ 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 $M \vDash_v A \forall v \in S$ 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 $(t, r) \in R \implies (s, r) \in R$
■

Adesso vediamo che ci sono anche proprietà dei frame non esprimibili in termini di validità di schemi di formule modali.

4.4 Morfismi di modelli

Definizione 4.14 — 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

$$\begin{aligned} f :\ & \mathbb{N} \to \mathbb{N} \\ & n \mapsto n^2 \end{aligned}$$

è un morfismo di frame.

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

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

Allora la funzione

$$\begin{aligned} f :\ & \mathbb{N} \to \mathbb{N} \\ & n \mapsto n + 1 \end{aligned}$$

non è un morfismo di frame.

Definizione 4.15 — 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 $M_2 = (\{0,1\}, \{0,1\} \times \{0,1\}, V_2)$ dove $R_1 = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x \leq y\}$, $Var = \{x\}$ e $V_1(x) = \{2n : n \in \mathbb{N}\}, V_2(x) = \{0\}$. Sia

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

Allora f è un morfismo di modelli, infatti:

1. $x \leq y \implies (x \bmod 2, y \bmod 2) \in \{0,1\} \times \{0,1\}$
2. $w \in V_1(x) \iff w \in \{2n : n \in \mathbb{N}\}$; 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 $w \leq w$ e $f(w) = 0 = y$.
   Se $y = 1$ allora $w \leq w + 1$ e $f(w + 1) = 1 = y$.
   (b) $f(w) = 1$: se $y = 0$ allora $w \leq w + 1$ e $f(w + 1) = 0 = y$.
   Se $y = 1$ allora $w \leq w$ e $f(w) = 1 = y$.

Lemma 4.16 — 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

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

$\forall\, w \in S_1$ 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 $f(w) \in V_2(F)$ (per il punto 1 nella definizione 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 solo 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 $(f(w), f(v)) \in R_2$ perché f è un morfismo di modelli e induttivamente $M_2 \vDash_{f(v)} G$, allora $M_2 \vDash_{f(w)} \Diamond G$.

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 $M_1 \vDash_w \Diamond G$. ■

Lemma 4.17 — 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

$$M_1 \vDash F \text{ se e solo se } M_2 \vDash F$$

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 $M_2 \vDash F$, perché f è suriettivo. ■

Lemma 4.18 — 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 4.19 — 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 $(S_1, R_1) \vDash F \implies (S_2, R_2) \vDash F$, 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 4.20 — 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 4.21. L'antisimmetria non è esprimibile, ossia non esiste una formula F tale che $(S, R) \vDash F$ 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

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

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

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

Supponiamo per assurdo che esista una formula 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. ■

4.5 Logiche Modali Normali

Abbiamo già mostrato che lo schema di formule

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

è valido, $\models K$.

Adesso vediamo che lo schema di formule

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

è valido, $\models def_\Diamond$.

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

Allora $M \models_w \Diamond A$ se e solo se esiste $v \in S t.c. (w, v) \in R$ e $M \models_v A$.

$M \models_w \neg\Box\neg A$ se e solo se $M \not\models_w \Box\neg A$, se e solo se esiste $v \in S t.c. (w, v) \in R$ e $M \not\models_v \neg A$, se e solo se esiste $v \in S t.c. (w, v) \in R$ e $M \models_v A$.

Abbiamo quindi dimostrato che $\models def_\Diamond$ ■

Definizione 4.22 — Sostituzione uniforme. Sia x una variabile e F una formula. Definiamo l'operazione di sostituzione uniforme di F al posto di x in una formula G, indicato come

$$G[F/x]$$

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

Esempio. Sia G la formula $\Box x \implies x \wedge y$ e F la formula $\Diamond y \iff \neg\Box\neg y$.

Allora $G[F/x] = \Box(\Diamond y \iff \neg\Box\neg y) \implies (\Diamond y \iff \neg\Box\neg y) \wedge y$

Definizione 4.23 — 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 $K : \Box(A \implies B) \implies (\Box A \implies \Box B)$
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 $(A \implies B) \in \Gamma$, 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 4.24 — Logica Modale K. La **logica modale K** è definita dai seguenti schemi di assiomi e regole:

1. Schemi di assiomi:
   (a) Tutte le tautologie della logica proposizionale

(b) $K : \Box(A \implies B) \implies (\Box A \implies \Box B)$

(c) $def_\Diamond : \Diamond A \iff \neg\Box\neg A$

2. Regole di inferenza:
   (a) Modus ponens
   (b) Necessitazione
   (c) Sostituzione uniforme

Definizione 4.25 — 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 4.26 — Teorema di una logica modale. Una formula F si dice **teorema di L**, scritto $\vdash_L F$ se e solo se esiste una dimostrazione in L in cui la ultima formula è F

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

1. $\vdash_K A \wedge B \implies A$ (Tautologia)
2. $\vdash_K \Box(A \wedge B \implies A)$ (Necessitazione)
3. $\vdash_K \Box(A \wedge B \implies A) \implies (\Box(A \wedge B) \implies \Box A)$ (K)
4. $\vdash_K \Box(A \wedge B) \implies \Box A$ (Modus Ponens)

Teorema 4.27. L'insieme $\{F : \vdash_K F\}$ è chiuso sotto sostituzione uniforme.

Nelle logiche Epistemiche si estende la logica K aggiungendo lo schema di assiomi

$$\Box F \implies F \quad \text{(se si sa che } F\text{, allora } F \text{ vale)}$$

che, come abbiamo visto, non vogliamo come assioma in una logica Deontica (se F è obbligatorio non è detto che F valga).

La logica K a cui aggiungiamo l'assioma $\Box F \implies F$ si chiama logica T.

Dato lo schema di formule $\Box F \implies F$, i teoremi della logica T sono validi su frame riflessivi. Se accettiamo il **principio di introspezione epistemica positiva**, ossia se assumiamo che ogni volta che si sa qualcosa si sa di saperla, aggiungiamo l'assioma $\Box F \implies \Box\Box F$.

Avremmo così definito la logica S4.

I teoremi della logica S4 sono validi su frame riflessivi e transitivi, perché lo schema di formule $\Box F \implies \Box\Box F$ esprime la transitività.

Se accettiamo anche il **principio di introspezione epistemica negativa**, ossia se ogni volta che non si sa qualcosa si sa di non saperla, aggiungiamo l'assioma $\neg\Box F \implies \Box\neg\Box F$. Avremmo così definito la logica S5.

I teoremi della logica S5 sono validi su frame riflessivi, transitivi e simmetrici ossia sulle relazioni di equivalenza.

Dobbiamo solo far vedere la validità sui frame simmetrici.

Deriviamo lo schema di formule $F \implies \Box\Diamond F$ da S5:

1) $\vdash_{S5} \neg\Box\neg F \implies \Box\neg\Box\neg F$

2) $\vdash_{S5} \Diamond F \implies \Box\Diamond F$ (1 + $def_\Diamond$)

3) $\vdash_{S5} \Box\neg F \implies \neg F$ (assioma T)

4) $\vdash_{S5} \neg\neg F \implies \neg\Box\neg F$ (3 + tautologia)

5) $\vdash_{S5} F \implies \Diamond F$ (4 + $def_\Diamond$ + tautologia)

6) $\vdash_{S5} F \implies \Box\Diamond F$ (transitività implicazione + 5 + 2)

Quindi $F \implies \Box\Diamond F$ è un teorema di S5.

Adesso facciamo vedere che $\neg\Box F \implies \Box\neg\Box F$ è un teorema di K + 1), 2), 3):

1. $\Box F \implies F$
2. $\Box F \implies \Box\Box F$
3. $F \implies \Box\Diamond F$
4. $\vdash \Box\Box F \iff \Box F$ (1 e 2)
5. $\vdash \neg\Box\neg\neg\Box\neg F \implies \neg\Box\neg F$ (4 + tautologia)
6. $\vdash \Diamond\Diamond F \implies \Diamond F$ ($def_\Diamond$)
7. $\vdash \Diamond F \implies \Box\Diamond\Diamond F$ (3)
8. $\vdash \Box(\Diamond\Diamond F \implies \Diamond F)$ (6 + necessitazione)
9. $\vdash \Box\Diamond\Diamond F \implies \Box\Diamond F$ (schema K + modus ponens)
10. $\vdash \Diamond F \implies \Box\Diamond F$ (7 + 9)
11. $\vdash \neg\Box\neg F \implies \Box\neg\Box\neg F$ ($def_\Diamond$)
12. $\vdash \neg\Box F \implies \Box\neg\Box F$ (tautologia)

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

Definizione 4.28 — Logica Valida. Una logica L è **valida (sound)** se

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

Teorema 4.29. La logica K è valida.

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

B_1 è valida perché 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 $\models B_j$ e allora $\models \Box B_j$, 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 $\models B_j, \models B_j \implies B_i$ e quindi $\models B_i$

■

Definizione 4.30 — Logica Completa. Una logica L è **completa** se

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

Teorema 4.31. La logica K è completa.

4.6 Logiche multimodali e connettivi modali n-ari

Finora abbiamo studiato logiche modali con un solo connettivo modale 1-ario, $\Box$.

(come abbiamo visto, l'altro connettivo modale, $\Diamond$ può essere definito usando $\Box$).

Il connettivo $\Box$ era 1-ario nel senso che si applicava ad una sola formula.

Adesso consideriamo Logiche modali con più di un connettivo modale:

$$\Box_1, \Box_2, \ldots$$

e connettivi modali n-ari ossia

$$\Box(F_1, F_2, \ldots, F_n) \qquad \text{dove } F_i \text{ sono formule}$$

Vediamo qual'è la semantica dei connettivi modali n-ari.

Sia S un insieme, $R \subseteq \underbrace{S \times \ldots \times S}_{(n+1 \text{ volte})}$ una relazione $(n+1)$-aria su S e M un modello su S, R.

Sia $w \in S$, scriviamo

$$M \vDash_w \Box(F_1, F_2, \ldots, F_n)$$

se e solo se $\forall\, v_1 \in S, \ldots, v_n \in S$ tali che $(w, v_1, \ldots, v_n) \in R$, si ha $M \vDash_{v_1} F_1, \ldots, M \vDash_{v_n} F_n$.

4.6.1 Logiche Temporali LTL (Linear-time Temporal Logic)

Queste logiche hanno tre connettivi modali 1-ari:

$$X, F, G$$

- X significa "neXt state" (anche indicato con "O")
- F significa "some Future state"
- G significa "all future states (Globally)"

e tre connettivi modali 2-ari:

$$U, W, R$$

- U significa "Until"
- W significa "Weak-until"
- R significa "Release"

4.6.1.1 Semantica

Sia S un insieme, $R \subseteq S \times S$ e M un frame tale che R non è riflessiva.

Con R^* indichiamo la chiusura riflessiva e transitiva di R, ossia ogni volta che in R abbiamo

$$\text{x} \longrightarrow \text{y} \longrightarrow \text{z}$$

in R^* abbiamo

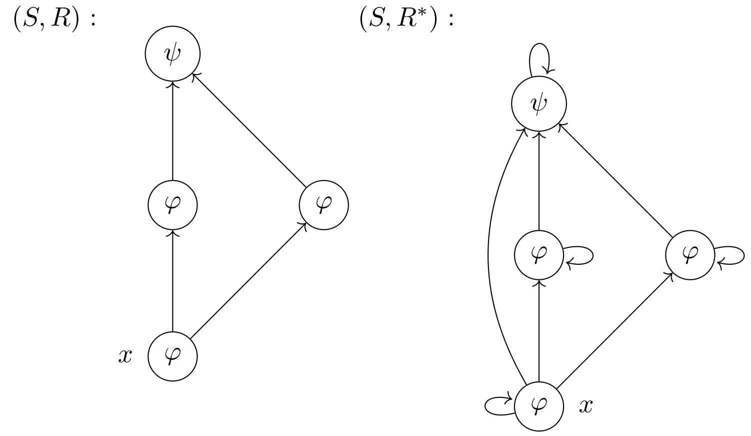
$$\begin{tikzcd} \text{x} \arrow[r] \arrow[loop above] \arrow[rr, bend right] & \text{y} \arrow[r] \arrow[loop above] & \text{z} \arrow[loop above] \end{tikzcd}$$

1) X è da considerare come $\Box$ sul frame (S, R)
2) G è da considerare come $\Box$ sul frame (S, R^*)
3) F è da considerare come $\Diamond$ sul frame (S, R^*), quindi $F\varphi = \neg G \neg \varphi$ per ogni formula φ
4) U è un connettivo modale 2-ario. è definito da $M \vDash_x U(\varphi, \psi)$ se e solo se
   a) $\exists\, z \in S t.c. (x, z) \in R^*$ e $M \vDash_z \psi$
   b) $M \vDash_y \varphi \forall\, y \in S t.c. (x, y) \in R^*, (y, z) \in R^*, y \neq z$
5) $W(\varphi, \psi)$ se e solo se $U(\varphi, \psi)$ oppure $G\varphi$
6) $R(\varphi, \psi)$ se e solo se $\neg U(\neg\varphi, \neg\psi)$

Quindi gli unici connettivi modali per definire questa logica solo X, G e U.

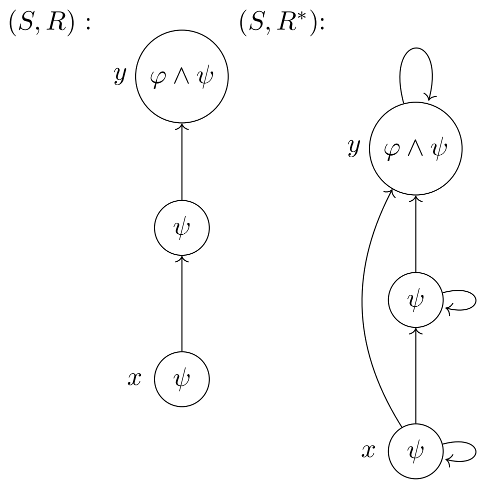
Gli altri sono esprimibili in termini di questi.

Esempio. Consideriamo la relazione:



$M \vDash_x X\varphi,\ M \nvDash_x G\varphi$
$M \vDash_x F\varphi,\ M \vDash_x U(\varphi, \psi)$
$M \vDash_x W(\varphi, \psi),\ M \vDash_x R(\varphi, \psi)$

Esempio. Consideriamo la relazione:



$M \vDash_x X\psi,\ M \vDash_x G\psi,\ M \vDash_y G\psi$
$M \nvDash_x X\varphi,\ M \nvDash_x G\varphi,\ M \vDash_y G\varphi$
$M \vDash_x F\varphi,\ M \vDash_x U(\psi, \varphi)$
$M \vDash_x W(\psi, \varphi),\ M \vDash_x R(\varphi, \psi)$

$\varphi R \psi : \neg U(\neg\varphi, \neg\psi)$.
$M \vDash_x \neg U(\neg\varphi, \neg\psi) \iff M \nvDash_x U(\neg\varphi, \neg\psi) \iff$
o $\forall z \in S$ t.c $(x,z) \in R^*, M \vDash_z \psi$
o $\forall z \in S$ t.c $(x,z) \in R^*. M \vDash_z \neg\psi, \exists\, y \in S$ t.c $(x,y) \in R^*, (y,z) \in R^*, y \neq z, M \vDash_y \varphi$
ψ deve essere vere fino al punto in cui inizia ad essere vera φ (φ rilascia ψ)

4.6.2 Logiche Temporali CTL (Computation Tree Logic)

In queste logiche modali, quantifichiamo sui cammini del grafo diretto che rappresenta il frame (S, R).
I connettivi modali sono:

$$AX, EX, AF, EF, AG, EG \qquad \text{(1-ari)}$$
$$AU, EU \qquad \text{(2-ari)}$$

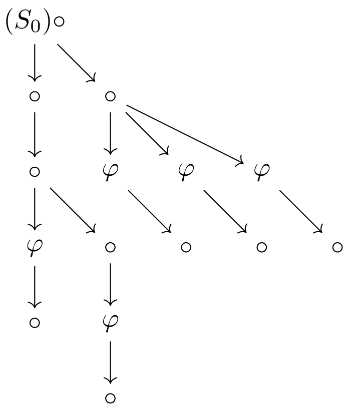
A sta per "Along all paths", E sta per "along at least one path (there Exists)"

4.6.2.1 Semantica

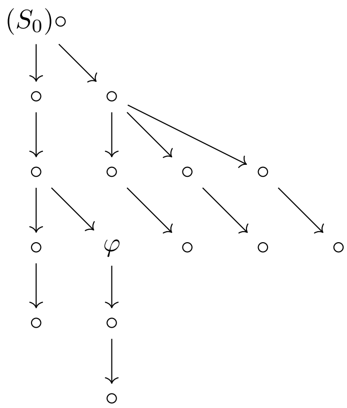
1) $M \vDash_w AX\psi$ se e solo se $\forall\, v \in S$ t.c $(w, s) \in R$(c'è un arco)$, M \vDash_s \psi$, ossia si comporta come $\Box$ su (S, R)
2) $M \vDash_w EX\psi$ se e solo se $\exists\, s \in S$ t.c $(w, s) \in R$(c'è un arco)$, M \vDash_s \psi$, ossia si comporta come $\Diamond$ su (S, R)
3) AG si comporta come $\Box$ su (S, R^*)
4) $M \vDash_w EG\varphi$ se e solo se esiste un cammino $s_0 := w \to s_1 \to s_2 \to \ldots$ in (S, R) tale che $M \vDash_{s_i} \varphi$ (lungo il cammino)
5) $M \vDash_w EU(\varphi, \psi)$ se e solo se esiste un cammino in (S, R) tale che $M \vDash_{s_i} U(\varphi, \psi)$ (lungo il cammino, possiamo intenderlo come sotto-frame)

Analogamente si definiscono gli altri connettivi modali.

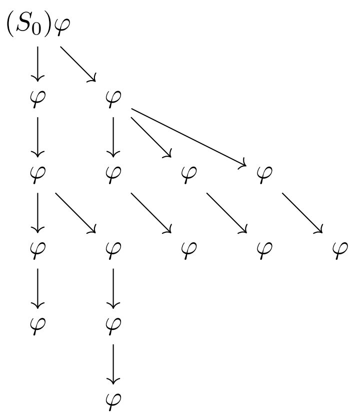
Esempio. Nei grafi:



$M \vDash_{S_0} AF\varphi$



$M \vDash_{S_0} EF\varphi$



$M \vDash_{S_0} AG\varphi$

4.6.3 Logiche CTL*

Le logiche CTL* hanno la stessa semantica delle LTL, a cui aggiungiamo i quantificatori A "Along all paths" ed E "Along at least one path".

Quindi CTL* contiene LTL e CTL.

In LTL possiamo esprimere l'affermazione "su tutti i cammini in cui appare ψ appare anche φ":

$$F\varphi \implies F\psi$$

in CTL non possiamo esprimerla, ma in CTL* si, dato che contiene LTL.

$$E(GF\varphi)$$

ovviamente tale affermazione non è esprimibile in LTL a meno che il frame (S, R) non abbia un solo cammino.

Non è esprimibile neanche in CTL; infatti ha un altro significato:

Esempio. in CTL:

$$\begin{tikzcd}
(S_0)\varphi \arrow[d] \arrow[dr] & & & & \\
\circ \arrow[d] & \circ \arrow[d] \arrow[dr] \arrow[drr] & & & \\
\circ \arrow[d] \arrow[dr] & \varphi \arrow[dr] & \varphi \arrow[dr] & \varphi \arrow[dr] & \\
\varphi \arrow[d] & \circ \arrow[d] & \circ & \circ & \circ \\
\circ & \varphi \arrow[d] & & & \\
& \circ & & &
\end{tikzcd}$$

$$M \vDash_{S_0} EG(EF\varphi) \text{ in CTL}$$

4.6.4 Model Checking

Esempio. Quando più processi eseguono in contemporanea, se condividono una risorsa potrebbe essere necessario assicurare che non vi accedano nello stesso momento.

Ad esempio non vorremmo che più di un processo modifichi un file nello stesso momento.

Definiamo delle "sezioni critiche" per ogni codice del processo e le disponiamo in modo che due processi non si trovino nella stessa sezione critica nello stesso momento.

Vogliamo che valga la seguente proprietà:

Sicurezza: "Un processo alla volta può stare nella sezione critica"

per due processi $P1$ e $P2$, consideriamo le variabili:

- n_1 := "processo 1 non sta in stato critico"
- n_2 := "processo 2 non sta in stato critico"
- c_1 := "processo 1 sta in stato critico"
- c_2 := "processo 2 sta in stato critico"
- t_1 := "processo 1 prova a entrare in stato critico"
- t_2 := "processo 2 prova a entrare in stato critico"

Sicurezza è esprimibile in LTL come: $\varphi_1 = G\neg(c_1 \wedge c_2)$ ossia $M \vDash_{S_0} G\neg(c_1 \wedge c_2)$.

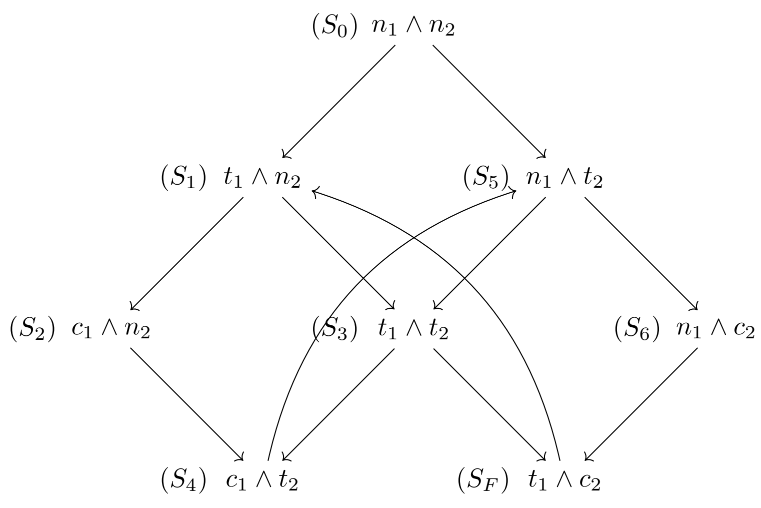
Un'altra condizione che vogliamo sia verificata è:

Vitalità: "Ogni volta che un processo chiede di entrare nella sua sezione critica, gli sarà permesso in un altro momento"

Questa condizione è esprimibile in CTL come:

$$M \vDash_{S_0} (AGt_1 \implies EFc_1) \wedge (AGt_2 \implies EFc_2) \equiv \varphi_2$$

considerando il seguente frame:



abbiamo che vale $M \vDash_{S_0} \varphi_1 \wedge \varphi_2$