Logica e Algebra 2

Niccoló Didoni

September 2022

Contents

Part I

Algebra

Chapter 1

Definizioni

Prima di affrontare i temi principali di questo corso è bene dare alcune definizioni di base.

1.1 Insiemi

Iniziamo dagli insiemi. I principali insiemi numerici con cui andremo a lavorare sono

- L'insieme dei **numeri naturali** $\mathbb{N}$.

$$\mathbb{N} = \{0, 1, 2, 3, \dots\} \tag{1.1}$$

- L'insieme dei **numeri interi** $\mathbb{Z}$.

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \tag{1.2}$$

- L'insieme dei **numeri razionali** $\mathbb{Q}$.

$$\mathbb{R} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in Z, b \neq 0 \right\} \tag{1.3}$$

- L'insieme dei **numeri reali** $\mathbb{R}$.
- L'insieme dei **numeri complessi** $\mathbb{C}$.

$$\mathbb{C} = \{a + \imath b : a \in \mathbb{R}, b \in \mathbb{R}, \imath^2 = -1\} \tag{1.4}$$

Passiamo ora alle relazioni tra insiemi. In particolare, indichiamo con:

- $\subseteq$ l'inclusione tra insiemi. Se X e Y sono due insiemi possiamo quindi scrivere $X \subseteq Y$ per dire che X è incluso, o uguale a, Y. Equivalentemente possiamo dire che X è sottoinsieme di Y.
- $\subsetneq$ l'inclusione propria tra insiemi. Se X e Y sono due insiemi possiamo quindi scrivere $X \subsetneq Y$ per dire che X è incluso in (ma mai uguale a) Y. Equivalentemente possiamo dire che X è sottoinsieme di Y.

Analizziamo ora un'altra proprietà di un'insieme: la sua cardinalità.

Definizione 1 (Cardinalità)**.** *Sia X un insieme finito, allora chiamiamo cardinalità il numero di elementi di X e scriviamo $|X|$.*

Grazie alla definizione di cardinalità (Definizione 1) possiamo definire cosa intendiamo per insieme vuoto.

Definizione 2 (Insieme vuoto)**.** *L'insieme vuoto $\emptyset$ è l'insieme che ha cardinalità 0.*

$$|\emptyset| = 0$$

Passiamo ora ad analizzare le principali operazioni tra insiemi, partendo dal prodotto cartesiano, che indicheremo con il simbolo $\times$.

Definizione 3 (Prodotto cartesiano)**.** *Siano X e Y due insiemi, allora il prodotto cartesiano $X \times Y$ tra i due insiemi è definito come l'insieme delle coppie il cui primo elemento appartiene a X e il secondo a Y.*

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

La cardinalità del prodotto cartesiano di due insiemi X e Y è il prodotto delle cardinalità dei singoli insiemi.

$$|X \times Y| = |X| \cdot |Y| \tag{1.5}$$

Questo è vero perché per ogni elemento di X (i.e., per $|X| = n$ volte) possiamo scegliere un diverso elemento di Y (i.e., $|Y| = m$ elementi). Notiamo infine che il prodotto cartesiano tra un insieme non vuoto X e l'insieme vuoto è l'insieme vuoto stesso.

$$X \times \emptyset = \emptyset \tag{1.6}$$

A conferma di questa affermazione, la cardinalità di $X \times \emptyset$, può essere calcolata come

$$|X \times \emptyset| = |X| \cdot |\emptyset| = |X| \cdot 0 = 0$$

Quindi effettivamente il risultato è l'insieme vuoto, ossia l'insieme con cardinalità 0.

Definiamo ora il concetto di insieme delle parti.

Definizione 4 (Insieme delle parti)**.** *Sia X un insieme, allora l'insieme delle parti $\wp(X)$ di X è l'insieme di tutti i sottoinsiemi A di X.*

$$\wp(X) = \{A : A \subseteq X\} \tag{1.7}$$

Passiamo ora ad introdurre il concetto di complementare di un insieme.

Definizione 5 (Insieme complementare)**.** *Sia X un insieme, se A appartiene all'insieme delle parti di A, allora il complementare di A, e scriviamo A^c è l'insieme di tutti gli elementi che non appartengono ad A.*

$$A^c = \{x \in X : x \notin A\} \tag{1.8}$$

1.2 Funzioni

Dopo aver introdotto gli insiemi e le loro principali caratteristiche, è arrivato il momento di parlare di funzioni.

Definizione 6 (Funzione)**.** *Siano X e Y due insiemi, una funzione da X a Y è un sottoinsieme di $F = X \times Y$ tale che*

1. *Se $(x, y_1) \in F$ e $(x, y_2) \in F$, allora $y_1 = y_2$ per ogni $x \in X$ e $y_1, y_2 \in Y$. In pratica, ad ogni elemento di X, assegniamo un solo elemento di Y.*
2. *Se $x \in X$, allora esiste un elemento $y \in Y$ tale per cui la coppia (x, y) appartiene a F.*

Se le condizioni sopra valgono, allora possiamo scrivere

$$F : X \to Y$$

per indicare una funzione F che va da X in Y.

Si noti che, quando definiamo una funzione, dobbiamo sempre definire

- L'**insieme di partenza** (i.e., X).
- L'**insieme d'arrivo** (i.e., Y).
- La relazione tra gli elementi di X e quelli di Y.

Tra tutte le funzioni, la funzione identità è molto importante ed è quindi bene definirla. La funzione identità su X, che indicheremo con Id_X è una funzione

$$Id_X : X \to X$$

che manda gli elementi $x \in X$ in loro stessi. In altre parole, la relazione tra insieme di partenza e insieme di arrivo è

$$Id_X(x) = x$$

Occupiamoci ora delle proprietà di alcune funzioni. La prima proprietà che andremo ad analizzare è la suriettività.

Definizione 7 (Funzione suriettiva)**.** *Una funzione $f : X \to Y$ si dice suriettiva se l'immagine di f, $Im(f) = \{f(x) : x \in X\}$, coincide con l'insieme di arrivo Y.*

In altre parole, una funzione è suriettiva se ogni elemento di Y è raggiunto da almeno un elemento di X. Graficamente, possiamo rappresentare una funzione suriettiva come in Figura 1.1.

Una funzione può essere anche iniettiva.

Definizione 8 (Funzione iniettiva)**.** *Una funzione $f : X \to Y$ si dice iniettiva se*

$$f(x) = f(y) \Rightarrow x = y \quad \forall x, y \in X \tag{1.9}$$

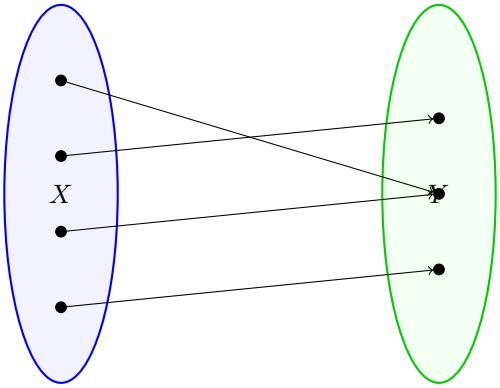


Figure 1.1: Una funzione suriettiva.

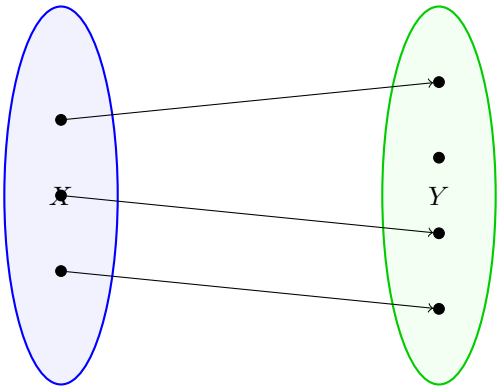


Figure 1.2: Una funzione iniettiva.

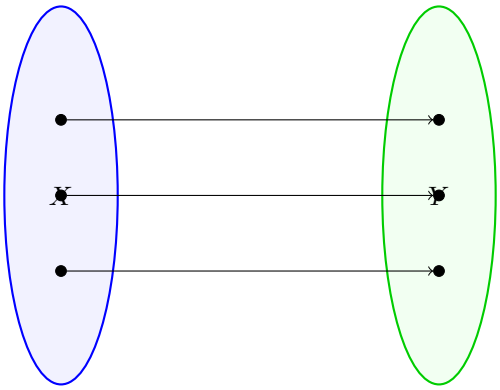


Figure 1.3: Una funzione biettiva.

In altre parole una funzione è iniettiva se ogni elemento di X va in un solo elemento di Y. Un esempio di funzione iniettiva è mostrato in Figura 1.2.

I concetti di funzione iniettiva e suriettiva possono essere utilizzati per definire una funzione biettiva.

Definizione 9 (Funzione biettiva)**.** *Una funzione $f : X \to Y$ si dice biettiva se e solo se è sia iniettiva che suriettiva.*

In altre parole, in una funzione biettiva, tutti gli elementi di Y sono raggiunti da uno e un solo elemento di X. Un esempio grafico di funzione biettiva è mostrato in Figura 1.3.

La prossima definizione ci permette di comporre funzioni per ottenere nuove funzioni.

Definizione 10 (Funzione composta)**.** *Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni, allora la funzione*

$$g \circ f : X \to Z$$

definita come

$$(g \circ f)(x) = g(f(x)) \quad \forall x \in X$$

prende il nome di composta tra f e g.

Come ultimo concetto relativo alle funzioni, introduciamo la definizione di funzione invertibile.

Definizione 11 (Funzione invertibile)**.** *Una funzione $f : X \to Y$ è detta invertibile se esiste una funzione $g : Y \to X$ tale per cui*

$$g \circ f = Id_X$$

e

$$f \circ g = Id_Y$$

La funzione g è detta inversa di f.

Per ricordare la definizione di funzione invertibile, possiamo notare che g va da Y a X, mentre x va da X a Y. Componendo g e f si ottiene una funzione che va da X a X, per la Definizione 10 e quindi l'identità deve necessariamente essere su X. Infatti f, calcolata inizialmente porta da X in Y e g, calcolata sul risultato di f, porta nuovamente Y in X.

Un'importante proprietà delle funzioni invertibili è la seguente.

Teorema 1. *Una funzione è invertibile se e solo se è biunivoca (biettiva).*

1.3 Operazioni

Le funzioni possono essere utilizzate per definire il concetto di operazione.

Definizione 12 (Operazione)**.** *Una funzione $f : X \times X \to X$ è un'operazione su X che indichiamo con*

$$f(x, x)$$

In altre parole, un'operazione è una funzione che prende due elementi di un insieme X e ritorna un altro elemento dell'insieme X. In alcuni casi useremo la notazione infissa per indicare un'operazione. Ad esempio, l'operazione $\times$ tra due elementi a e b può essere scritta come

$$a \times b$$

Passiamo ora all'enumerazione delle proprietà di un'operazione. Un'operazione può essere:

- **Associativa**. Un'operazione $*$ è associativa se

  $$x * (y * z) = (x * y) * z$$

  In altre parole un'operazione è associativa se l'ordine in cui viene eseguita non cambia il risultato. Quando un'operazione è associativa possiamo evitare di usare le parentesi.

- **Commutativa**. Un'operazione $*$ è commutativa se

  $$x * y = y * x$$

  In altre parole, cambiando l'ordine degli operandi, il risultato non cambia.

1.3.1 Esempi

Differenza simmetrica

Un'operazione molto interessante tra insiemi è la differenza simmetrica $\triangle$ definita come segue.

Definizione 13 (Differenza simmetrica)**.** *Dati due insiemi A e B, la differenza simmetrica $\triangle$ tra A e B è*

$$A \triangle B = (A \setminus B) \cup (B \setminus A) \tag{1.10}$$

Chapter 2

Strutture algebriche

2.1 Identità

Ora che conosciamo il concetto di operazione, possiamo iniziare a costruire un po' di strutture algebriche. Prima abbiamo però bisogno del concetto di identità di un'operazione.

Definizione 14 (Identità di un'operazione)**.** *Sia $*$ un'operazione su X, un elemento $e \in X$ tale per cui*

$$e * x = x$$

prende il nome di identità.

Dalla definizione di identità, non è ben chiaro quanti siano i possibili elementi per cui vale $e * x = x$. Il seguente teorema serve per chiarire questo punto.

Teorema 2 (Unicità dell'identità)**.** *L'identità di un'operazione è unica.*

Per dimostrare questo teorema basta ipotizzare, per assurdo che esistano due identità e_1 ed e_2. A questo punto potremmo scrivere

$$e_1 * x = x$$

e

$$e_2 * x = x$$

Sostituendo la x a destra nella prima equazione otterremmo

$$e_1 * x = e_2 * x$$

Dato che $x = x$, allora deve essere anche che $e_1 = e_2$, quindi le due identità coincidono ed esiste una sola identità.

2.2 Monoide

Grazie al concetto di identità possiamo definire la nostra prima struttura algebrica.

Definizione 15 (Monoide)**.** *Un insieme X con un'operazione associativa $\cdot$ e con un'identità e rispetto all'operazione $\cdot$ è detto monoide.*

$$(X, \cdot, e)$$

Un monoide è quindi una tripletta $(X, \cdot, e)$ in cui

- X è un **insieme**.
- $\cdot$ è un'**operazione associativa** definita su X.
- e è l'**identità** rispetto a $\cdot$.

Togliendo l'identità da un monoide si ottiene un semigruppo.

Definizione 16 (Semigruppo)**.** *Un semigruppo è un monoide senza identità e. In particolare, un insieme X con un'operazione associativa $\cdot$*

$$(X, \cdot)$$

è un semigruppo.

Dato che un monoide include un'operazione, possiamo definire il concetto di elemento invertibile di un monoide.

Definizione 17 (Elemento invertibile di un monoide)**.** *Sia $(X, \cdot, e)$ un monoide, un elemento $x \in C$ è invertibile se esiste un valore $y \in X$ tale per cui*

$$x \cdot y = y \cdot x = e$$

L'elemento $y = x^{-1}$ prende il nome di inverso ed è unico.

Data la definizione di elemento invertibile di un monoide, possiamo scrivere, dato un monoide, l'insieme di tutti gli elementi del monoide che sono invertibili. Prendiamo ad esempio il monoide $(\mathbb{N}, +, 0)$. L'unico intero x tale per cui esiste un intero y che sommato a x da 0 (ossia l'identità) è $x = 0$. Se prendiamo invece il monoide $(\mathbb{Z}, +, 0)$ allora il suo insieme degli elementi invertibili è $\mathbb{Z}$ stesso perché dato un qualsiasi numero $n \in \mathbb{Z}$, ci basta prendere $-n$ per avere $n + (-n) = 0$. Un altro esempio molto importante è il monoide formato dall'insieme $F(X) = \{f : X \to X\}$ delle funzioni da X in X. In questo caso l'insieme degli elementi invertibili è l'insieme delle funzioni biunivoche. In particolare, se X ha N elementi, allora l'insieme degli elementi invertibili è l'insieme delle permutazioni di N elementi.

2.3 Gruppo

Un'altra importante struttura algebrica è il gruppo.

Definizione 18 (Gruppo)**.** *Un gruppo è un monoide tale che tutti i suoi elementi siano invertibili. Se l'operazione del gruppo è commutativa diciamo che il gruppo è commutativo o abeliano.*

2.3.1 Esempi

Numeri interi

Un esempio di gruppo è $(\mathbb{Z}, +, 0)$, dato che l'insieme degli elementi invertibili è $\mathbb{Z}$. Il gruppo $(\mathbb{Z}, +, 0)$ è anche commutativo perché la somma è commutativa.

Differenza simmetrica

L'insieme delle parti $\wp(X)$ con la differenza simmetrica $\triangle$ (Definizione 13) è un gruppo abeliano. Più precisamente, il monoide $(\wp(X), \triangle, \emptyset)$ è un monoide in cui tutti gli elementi di $\wp(X)$ hanno inverso. Dimostriamo quindi quest'ultima affermazione, ossia che per ogni insieme $A \in \wp(X)$ esiste un altro insieme $B \in \wp(X)$ tale per cui

$$A \triangle B = \emptyset$$
$$(A \setminus B) \cup (B \setminus A) = \emptyset$$

L'unico elemento che soddisfa questa uguaglianza è A stesso, infatti $A \setminus A = \emptyset$. Quindi l'inverso, rispetto all'operazione $\triangle$, di $A \in \wp(X)$ è $A \in \wp(X)$.

Funzioni invertibili

Prendiamo un insieme $X = \{1, 2, 3, \ldots, n\}$, per un qualche $n \in \mathbb{N}$. L'insieme delle funzioni $f : X \to X$ invertibili è un gruppo e prende il nome di **insieme delle permutazioni** di n elementi o **gruppo simmetrico**. Un gruppo simmetrico viene tipicamente indicato con S_n, la cui cardinalità è $n!$. Se $n \geq 3$, allora il gruppo non è abeliano. Se consideriamo ad esempio $X = \{1, 2\}$, allora S_2 contiene:

- L'identità, che manda 1 in 1 e 2 in 2.
- La funzione che manda 1 in 2.
- La funzione che manda 2 in 1.

Questo gruppo è importante perché tutti i gruppi finiti possono essere visti come sottogruppi di un gruppo simmetrico.

2.4 Sottomonoide

Dalla definizione di monoide possiamo ricavare quella di sottomonoide.

Definizione 19 (Sottomonoide)**.** *Sia $(X, \cdot, e)$ un monoide. Chiamo sottomonoide un sottoinsieme $Y \subseteq X$ che, con l'operazione indotta (i.e., con la stessa operazione) $\cdot$ e la stessa identità e, è un monoide a sua volta.*

In maniera analoga possiamo definire un sottogruppo.

Definizione 20 (Sottogruppo)**.** *Sia $(X, \cdot, e)$ un gruppo. Chiamo sottogruppo un sottoinsieme $Y \subseteq X$ che, con l'operazione indotta (i.e., con la stessa operazione) $\cdot$ e la stessa identità e, è un gruppo a sua volta.*

Un'altra importante definizione riguardante i sottomonoidi è qualla di sottomonoide generato da un insieme.

Definizione 21 (Sottomonoide generato da un insieme)**.** *Sia $(X, \cdot, e)$ un monoide e $S \subseteq X$, definiamo*

$$\langle S \rangle$$

il sottomonoide di X generato da S come il più piccolo sottomonoide di X che contiene S.

In altre parole, il sottomonoide di X generato da S è la più piccola intersezione di tutti i sottomonoidi di X che contengono S. In maniera analoga possiamo definire

Definizione 22 (Sottogruppo generato da un insieme)**.** *Sia $(X, \cdot, e)$ un gruppo e $S \subseteq X$, definiamo*

$$\langle S \rangle$$

il sottogruppo di X generato da S, come il più piccolo sottogruppo di X che contiene S.

Quando vogliamo definire il sottomonoide generato da un insieme S (sottoinsieme dell'insieme di un monoide), dobbiamo svolgere l'operazione del monoide su tutti gli elementi di S, ricordandoci però di aggiungere l'identità nel caso questa non sia ottenuta svolgendo l'operazione su tutti gli elementi dell'insieme. Al contrario, per i sottogruppi, non è necessario controllare la presenza dell'identità perché, per definizione, ogni elemento ha un inverso e quindi sicuramente è presente l'identità (per definizione di inverso, per ogni x, esiste y tale per cui xy da l'identità).

Sempre parlando di monoidi, possiamo introdurre una nuova operazione tra monoidi.

Definizione 23 (Prodotto diretto di monoidi)**.** *Siano M_1 e M_2 due monoidi con identità e_1 ed e_2 rispettivamente, chiamiamo prodotto diretto di M_1 con M_2, l'insieme $M_1 \times M_2$ con l'operazione*

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2) \quad \forall a_1, a_2 \in M_1 \ \forall b_1, b_2 \in M_2$$

Il prodotto diretto di monoidi è un monoide e ha identità (e_1, e_2). L'operazione di prodotto diretto può essere fatta anche tra gruppi.

Definizione 24 (Prodotto diretto tra gruppi)**.** *Siano G_1 e G_2 due gruppi con identità e_1 ed e_2 rispettivamente, chiamiamo prodotto diretto di G_1 con G_2, l'insieme $G_1 \times G_2$ con l'operazione*

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2) \quad \forall a_1, a_2 \in G_1, b_1, b_2 \in G_2$$

Come per il prodotto diretto di monoidi, anche il prodotto diretto tra gruppi è un gruppo con

- Identità (e_1, e_2).

- Inverso $(a, b)^{-1} = (a^-1, b^{-1}) \in G_1 \times G_2$

2.4.1 Esempi

Sottogruppo banale

Ogni gruppo ha un sottogruppo formato dalla sola identità e,

$$\{e\}$$

che è detto sottogruppo banale.

Catena di sottomonoidi

L'insieme formato dall'elemento 1 è un sottomonoide per tutti i monoidi con moltiplicazione sugli insiemi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

$$\{1\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Sottomonoide generato da un insieme con singolo elemento

Consideriamo ad esempio, $S = \{0, 1\} \subseteq (\mathbb{N}, +, 0)$. Per ottenere il sottomonoide generato da S, dobbiamo prendere il più piccolo sottomonoide di $(\mathbb{N}, +)$ che contiene S. Quindi

$$\langle S \rangle = \mathbb{N}$$

Si noti che $\langle S \rangle$ non può essere $\{0, 1\}$ perché $1+1 = 2 \notin \{0, 1\}$, quindi $(\{0, 1\}, +, 0)$ non è un monoide. Se invece considerassimo la moltiplicazione, il sottomonoide generato da S sarebbe

$$\langle S \rangle = \{0, 1\}$$

2.4.2 Morfismi

Un morfismo tra due monoidi è una funzione che rispetta la struttura algebrica del monoide. Più formalmente

Definizione 25 (Morfismo di monoidi)**.** *Siano $(M_1, \cdot, e_1)$ e $(M_2, \cdot, e_2)$ due monoidi. Una funzione $f : M_1 \to M_2$ è un morfismo di monoidi se*

1. *f manda l'identità di M_1 nell'identità di M_2.*

$$f(e_1) = e_2$$

2. *La struttura algebrica del monoide è rispettata.*

$$f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in M_1$$

Prima di fare alcuni esempi riguardanti i morfismi di monoidi, è utile introdurre il concetto di nucleo (o kernel)

Definizione 26 (Nucleo)**.** *Il nucleo di un morfismo $f : M_1 \to M_2$ di spazi vettoriali è il sottomonoide $Ker(f)$ degli elementi $x \in M_1$ che tramite f, vengono mandati in e_2 (ossia nell'elemento neutro di M_2).*

$$ker(f) = \{x \in M_1 : f(x) = e_2\} \subseteq M_1 \tag{2.1}$$

Sempre considerando un morfismo, possiamo considerare la seguente affermazione.

Teorema 3 (Immagine di un morfismo)**.** *L'immagine di un morfismo $f : M_1 \to M_2$ è un sottomonoide di M_2*

$$\Im(f) = \{f(x) : x \in M_1\} \subseteq M_2$$

Proviamo a dimostrare il teorema appena enunciato. Sicuramente $\Im(f)$ contiene e_2, per la prima proprietà di morfismo (Definizione 25). Per verificare che $\{f(x) : x \in M_1\}$ sia un morfismo dobbiamo poi dimostrare che presi due elementi qualsiasi $f(x_1)$ e $f(x_2)$ in $\Im(f)$, applicando l'operazione del monoide M_1 ottengo un elemento di $\Im(f)$, ossia

$$f(x_1) \cdot f(x_2) \in \Im(f)$$

Per la seconda proprietà dei morfismi tra monoidi possiamo dire che

$$f(x_1) \cdot f(x_2) = f(x_1 \cdot x_2)$$

e dato che $x_1 \cdot x_2 \in M_1$, essendo M_1 un monoide, allora $f(x_1 \cdot x_2)$ appartiene a $\Im(f)$.

Un morfismo può essere definito, allo stesso modo, anche per i gruppi. In questo caso la prima proprietà non è necessaria essendo assicurata dalla seconda. Formalmente

Definizione 27 (Morfismo di gruppi)**.** *Siano $(G_1, \cdot, e_1)$ e $(G_2, \cdot, e_2)$ due gruppi. Un morfismo di gruppi $g : G_1 \to G_2$ è un morfismo di monoidi (Definizione 25)*

Applicando le proprietà dei morfismi di gruppi, possiamo scrivere che

$$e_2 = f(e_1)$$

Siccome stiamo parlando di gruppi, tutti gli elementi di G_1 hanno inverso, quindi possiamo scrivere e_1 come il prodotto (o, in generale con l'operazione del gruppo) tra un elemento $x \in G_1$ e il suo inverso $x^{-1} \in G_1$.

$$e_2 = f(e_1) = f(x \cdot x^{-1})$$

Per la seconda proprietà dei morfismi tra monoidi possiamo anche dire che

$$e_2 = f(e_1) = f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1})$$

Ma quindi, dato che l'immagine di un morfismo $f : M_1 \to M_2$ tra monoidi è un sottomonoide di M_2, allora l'elemento invertibile di M_2 è

$$\big[f(x)\big]^{-1} = f(x^{-1})$$

Ora che sappiamo un po' di cose sui morfismi tra monoidi e gruppi possiamo definire il concetto di morfismo biunivoco.

Definizione 28 (Morfismo biunivoco di monoidi (o gruppi))**.** *Un isomorfismo di monoidi (o gruppi) è un morfismo biunivoco, ossia un morfismo tale che il morfismo inverso sia un morfismo di monoidi (o gruppi).*

In realtà, per i monoidi, un morfismo biunivoco è direttamente un isomorfismo. In particolare vale la seguente proposizione

Proposizione 1 (Inversa di un morfismo di monoidi)**.** *Sia $f : M_1 \to M_2$ un morfismo biunivoco di monoidi (o di gruppi), allora $f^{-1} : M_2 \to M_1$ è un morfismo di monoidi (o di gruppi).*

Per dimostrare questa proposizione possiamo partire dal far vedere che

$$f^{-1}(e_2) = e_1$$

perché $f(e_1) = e_2$. Ora dobbiamo dimostrare che dati due elementi $x_2, y_2 \in M_2$, se esistono $x_1, y_1 \in M_1$ tali che

$$f(x_1) = x_2$$

e

$$f(y_1) = y_2$$

allora

$$f^{-1}(x_2 \cdot y_2) = f^{-1}(f(x_1) \cdot f(y_1)) = f^{-1}(f(x_1 \cdot y_1)) = x_1 \cdot y_1$$

Chapter 3

Relazioni su un insieme

3.1 Relazioni di equivalenza

Dato che stiamo studiando le relazioni tra insiemi, iniziamo con il definire cosa intendiamo per relazione.

Definizione 29 (Relazione su un insieme)**.** *Sia X un insieme. Un sottoinsieme $R \subseteq X \times X$ è una relazione su X.*

Una relazione molto importante è la relazione di equivalenza.

Definizione 30 (Relazione di equivalenza)**.** *Una relazione $R \subseteq X \times X$ è detta relazione di equivalenza se soddisfa le proprietà*

1. ***Riflessiva****. Ogni $x \in X$ deve essere in relazione con se stesso.*

$$(x, x) \in R \quad \forall x \in X$$

   Quindi, ogni elemento è equivalente a se stesso.

2. ***Simmetrica****. Se $x \in X$ è in relazione con $y \in X$, allora y è in relazione con x.*

$$(x, y) \in R \Rightarrow (y, x) \in R \quad \forall x, y \in X$$

   Quindi, se un elemento x è equivalente ad un elemento y, allora anche y è equivalente ad x.

3. ***Transitiva****. Se $x \in X$ è in relazione con $y \in X$ e y è in relazione con $z \in X$, allora anche x è in relazione con z.*

$$(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R \quad \forall x, y, z \in X$$

Se le proprietà di cui sopra sono valide, allora scriviamo

$$x \sim y$$

per indicare $(x, y) \in R$.

Grazie alla definizione di equivalenza possiamo definire un classe di equivalenza di un elemento, ossia l'insieme di tutti gli elementi equivalenti a quell'elemento. Formalmente

Definizione 31 (Classe di equivalenza)**.** *Sia x un elemento dell'insieme X. La classe di equivalenza di x, che indichiamo con $[x]$, è l'insieme degli elementi $y \in X$ che sono equivalenti ad x.*

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

La seguente proprietà permette di eguagliare classi di equivalenza di elementi che sono tra di loro equivalenti.

Proposizione 2 (Uguaglianza delle classi di equivalenza)**.** *Siano x e y due elementi dell'insieme X, se x è equivalente ad y allora la classe di equivalenza di x è uguale alla classe di equivalenza di y.*

Per dimostrare la proposizione basta considerare un elemento $z \in [x]$. Dato che z è nella classe di equivalenza di x, allora z è equivalente ad x. Ma x è equivalente a y, quindi per la proprietà transitiva delle relazioni di equivalenza z è equivalente a y. Se $z \sim y$ allora z è nella classe di equivalenza di y. Dato che questo ragionamento può essere ripetuto per ogni $z \in [x]$, allora le classi di equivalenza $[x]$ e $[y]$ devono necessariamente contenere gli stessi elementi. L'insieme delle classi di equivalenza è chiamato insieme quoziente ed è definito come segue.

Definizione 32 (Insieme quoziente)**.** *Sia X un insieme, l'insieme quoziente $X/\sim$ rispetto ad X è l'insieme degli insiemi di equivalenza di ogni elemento $x \in X$.*

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

Notiamo che l'insieme quoziente è un insieme di insiemi, e non di elementi di X. Per fare chiarezza, consideriamo l'insieme X con l'uguaglianza come relazione di equivalenza. L'insieme quoziente è $X/\sim = \{\{1\}, \{2\}, \{3\}\}$ e non $\{1, 2, 3\}$. Un'altra importante proprietà delle classi di equivalenza è che se due elementi $x, y \in X$ non sono equivalenti, allora le loro classi di equivalenza sono disgiunte (i.e. $[x] \cap [y] = \emptyset$). Questo significa che

Proposizione 3. *Sia X una partizione e $X/\sim$ un insieme quoziente. L'insieme quoziente è una partizione di X dato che l'unione disgiunta degli elementi di $X/\sim$ è X stessa.*

$$\biguplus_{[x] \in X/\sim} [x] = X$$

Dato un insieme e il suo insieme quoziente, possiamo definire un'importante funzione, chiamata funzione canonica, che lega questi due insiemi.

Definizione 33 (Funzione canonica)**.** *La funzione*

$$\pi : X \to {}^{X}\!/_{\sim}$$

che manda gli elementi di $x \in X$ nel proprio insieme di equivalenza $[x] \in {}^{X}\!/_{\sim}$ è detta funzione canonica.

3.1.1 Esempio

Consideriamo il classico insieme

$$X = \{1, 2, \dots, n\}, \quad n \in \mathbb{N} \setminus \{0\}$$

e diciamo che due insiemi sono equivalenti se hanno stessa cardinalità.

$$A \sim B \iff |A| = |B|$$

Iniziamo descrivendo l'insieme quoziente dell'insieme delle parti di X. L'insieme quoziente ${}^{\wp(X)}\!/_{\sim}$ è

$${}^{\wp(X)}\!/_{\sim} = \{\{\emptyset\}, \{\{1\}, \{2\}, \dots, \{n\}\}, \dots, X\}$$

A questo punto possiamo dire che, se consideriamo un sottoinsieme $A \in \wp(X)$ con cardinalità k, allora la cardinalità dell'insieme di equivalenza di A è

$$|A| = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

3.2 Gruppo quoziente

Ora che conosciamo il concetto di insieme quoziente, possiamo utilizzare tale insieme per costruire un gruppo. Prima di dare la definizione di gruppo quoziente, consideriamo un gruppo $(G, *, e)$ (che per semplicità indicheremo solo con G) e un suo sottogruppo $(H, *, e)$. Definiamo su G la relazione $\sim$ come

$$g_1 \sim g_2 \iff g_2 = g_1 * h$$

per qualche $h \in H$ e per ogni $g_1, g_2 \in G$. Iniziamo a mostrare che la relazione appena definita è effettivamente una relazione di equivalenza:

1. Proprietà riflessiva. Per provare la proprietà riflessiva dobbiamo mostrare che $g \sim g$ per ogni $g \in G$. Dato che l'identità di G è la stessa di H, essendo H sottogruppo di G, allora possiamo scrivere

   $$g = g * e = g$$

   quindi esiste un h, in particolare $h = e$, per cui $g = g$.

2. Proprietà simmetrica. Per provare la proprietà simmetrica dobbiamo mostrare che

   $$g_1 \sim g_2 \Rightarrow g_2 \sim g_1 \quad \forall g_1, g_2 \in G$$

Iniziamo con lo scrivere la relazione di equivalenza come $g_1 = g_2 h$. Dato che H è un sottogruppo, allora ogni elemento di H ha un inverso, quindi possiamo moltiplicare a destra e sinistra per h^{-1} e ottenere

$$g_1 * h^{-1} = g_2 * h * h^{-1}$$

Per definizione di inverso $h * h^{-1} = e$, ed essendo e la stessa in H e G (H è sottogruppo di G), allora otteniamo

$$g_1 * h^{-1} = g_2$$

Ma h^{-1} è un elemento di H, allora g_2 è equivalente a g_1.

3. Proprietà transitiva. Per provare la proprietà transitiva iniziamo scrivendola esplicitamente.

$$g_1 = g_2 * h, g_2 = g_3 * h' \Rightarrow g_1 = g_3 * h''$$

Sostituendo g_2 della seconda relazione nella prima otteniamo

$$g_1 = g_3 * h' * h$$

Ma dato che H è un gruppo, $h' * h$ appartiene ad H, quindi $g_1 \sim g_3$.

L'insieme quoziente della relazione di equivalenza appena descritta viene indicato con G/H. Proviamo ora a dimostrare che l' insieme quoziente è anche un gruppo. Per essere un gruppo, l'insieme quoziente deve avere un'operazione, che che definiamo come

$$[g_1] + [g_2] = [g_1 + g_2] \quad \forall g_1, g_2 \in G$$

Mostriamo ora che l'operazione è ben definita. Sia $g_1' = g_1 + h$ e $g_2' = g_2 + h$, allora, per la relazione di equivalenza definita sopra, possiamo dire $g_1' \sim g_1$ e $g_2' \sim g_2$. Ma se g_1' è equivalente a g_1, allora la classe di equivalenza di g_1 è equivalente a quella di g_1', per la Proposizione 2

$$[g_1] = [g_1']$$

e la stessa cosa può essere detta per g_2 e g_2', quindi

$$[g_2] = [g_2']$$

Ciò significa che possiamo scrivere

$$[g_1] + [g_2] = [g_1'] + [g_2']$$

Per come abbiamo definito la somma su G/H, allora possiamo scrivere

$$[g_1'] + [g_2'] = [g_1' + g_2']$$

Se l'operazione di somma è stata ben definita allora dobbiamo dimostrare che $[g_1 + g_2]$ e $[g_1' + g_2']$ sono uguali, perché $[g_i] = [g_i']$. Iniziamo espandendo la somma $g_1' + g_2'$.

$$g_1' + g_2' = g_1 + h_1 + g_2 + h_2 = (g_1 + g_2) + (h_1 + h_2)$$

Ma $h_1 + h_2$ è un elemento di H, perché $(H, +, 0)$ è un gruppo (Definizione 34), quindi per come abbiamo definito l'equivalenza

$$(g_1' + g_2') \sim (g_1 + g_2)$$

e quindi, per la Proposizione 2, le due classi di equivalenza sono uguali

$$[g_1 + g_2] = [g_1' + g_2']$$

e quindi l'operazione di somma su G/H è ben definita. L'operazione + su G/H che abbiamo appena definito

- È commutativa.
- È associativa.
- Ha identità la classe di equivalenza dell'identità di G: $[0]$.
- Ha inverso, per ogni elemento $[g]$ che indichiamo come $[-g]$.

Ora che siamo sicuri che l'insieme quoziente ${}^{G}\!/_{H}$ abbia identità e un'operazione, possiamo finalmente definire il gruppo quoziente.

Definizione 34 (Gruppo quoziente)**.** *Sia $(G, +, 0)$ un gruppo abeliano (che per semplicità indicheremo solo con G) e sia $(H, +, 0)$ un sottogruppo di G. Indichiamo con*

$$ {}^{G}\!/_{H} $$

l'insieme quoziente con relazione di equivalenza tra gli elementi di G

$$ g_1 \sim g_2 \iff g_2 = g_1 + h $$

per ogni $g_1, g_1 \in G$ e qualche $h \in H$, con operazione

$$ [g_1] + [g_2] = [g_1 + g_2] \quad \forall [g_1], [g_2] \in {}^{G}\!/_{H} $$

e identità

$$ e = [0] $$

3.2.1 Esempi

Sottogruppo banale

Consideriamo un gruppo abeliano $(G, +, 0)$ e il suo sottogruppo banale $H = \{0\}$. L'insieme quoziente in questo caso è l'insieme di tutti gli insiemi di un solo elemento perché, dato che H contiene solo l'elemento neutro, allora ogni $g \in G$ è equivalente a se stesso.

$$ {}^{G}\!/_{H} = \{\{g\} : g \in G\} $$

3.2.2 Classi di resto

Sia $G = (\mathbb{Z}, +, 0)$ un gruppo abeliano e $n \in \mathbb{N}$ un numero naturale. Consideriamo poi l'insieme

$$ n\mathbb{Z} = \{kn : k \in \mathbb{Z}\} \subseteq \mathbb{Z} $$

dei multipli interi di n. Si noti che $n\mathbb{Z}$ è un sottogruppo di $(\mathbb{Z}, +, 0)$. Dato che abbiamo un gruppo e un suo sottogruppo, possiamo definire l'insieme quoziente che, in questo caso, indichiamo con $\mathbb{Z}_n$

$$ \mathbb{Z}_n = {}^{\mathbb{Z}}\!/_{\mathbb{Z}_n} $$

Prima di vedere il caso generico, consideriamo degli esempi pratici, partendo da $n = 0$. In questo caso, l'unico elemento di $n\mathbb{Z}$ è 0, quindi ci riduciamo al caso di sottogruppo banale visto nell'esempio precedente e quindi otteniamo

$$ \mathbb{Z}_0 = \{\{x\} : x \in \mathbb{Z}\} $$

Passiamo ora a $n = 1$. In questo caso, $n\mathbb{Z}$ è $\mathbb{Z}$ stesso e quindi

$$\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z} = \{[0]\}$$

perché, essendo $\mathbb{Z}$ un gruppo possiamo sempre scegliere $h = g$ (dato che $G = H$) così da scrivere

$$g = 0 + g$$

e quindi ogni g è equivalente a 0. Consideriamo infine $\mathbb{Z}_2$. In questo caso, $n\mathbb{Z}$ è l'insieme dei numeri pari, quindi otteniamo

$$\mathbb{Z}_2 = \{[0], [1]\}$$

perché definiamo la relazione di equivalenza come

$$a \sim b \iff a = b + h \quad h \in 2\mathbb{Z}$$

Quindi ogni numero pari $a \in \mathbb{Z}$ è equivalente a 0 se prendiamo $h = a$, mentre i numeri dispari sono equivalenti a 1 prendendo $h = a - 1$ (ossia il numero pari prima di a). Più precisamente,

$$h = 2k = a - b$$

k appartiene a $\mathbb{Z}$ (ossia $a - b$ è divisibile per 2) se e sono se il resto della divisione di a per 2 è uguale al resto della divisione di b per 2. Per vedere questo fatto possiamo scrivere a e b come

$$a = 2h_a + r_a$$

e

$$b = 2h_b + r_b$$

La loro differenza è

$$a - b = 2h_a + r_a - (2h_b + r_b) = 2(h_a - h_b) + r_a - r_b$$

e quindi $a - b$ è un multiplo di 2 se e solo se i due resti r_a e r_b sono uguali. Dunque se a è pari anche b lo deve essere e quindi tutti i numeri pari sono equivalenti tra loro (e prendiamo 0 come rappresentante della classe). Analogamente, se a è dispari anche b lo deve essere, allora tutti i numeri dispari sono equivalenti tra loro.

Generalizzando per n qualsiasi, $\mathbb{Z}_n$ è la classe dei resti della divisione per n, ossia

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \big\{[0], [1], \ldots, [n-1]\big\} = \{\hat{0}, \hat{1}, \ldots, n \hat{-} 1\}$$

Per la Definizione 34, l'insieme quoziente $\mathbb{Z}_n$ delle classi di resto modulo n con la somma $+$ (definita in 34) è un gruppo.

3.2.3 Proiezione canonica

In precedenza abbiamo definito una funzione canonica (Definizione 33) come una funzione che manda un elemento nella sua classe di equivalenza. Ora possiamo fare la stessa cosa con i gruppi e definire la proiezione canonica.

Definizione 35 (Proiezione canonica)**.** *Sia G un gruppo abeliano e $H \subseteq G$ un sottogruppo, la funzione*

$$\pi : G \to {}^{G}\!/_{H}$$

che manda gli elementi di G nella propria classe di equivalenza dell'insieme quoziente

$$\pi(g) = [g]$$

prende il nome di proiezione canonica.

Si noti che, per come abbiamo costruito questa funzione, π è un morfismo di gruppi. Per dimostrare questa affermazione dobbiamo dimostrare che

$$\pi(g1 + g2) = \pi(g_1) + \pi(g_2)$$

Per farlo basta scrivere che, per definizione di proiezione canonica,

$$\pi(g1 + g2) = [g_1 + g_2]$$

Poi per come abbiamo definito l'operazione nel gruppo quoziente (Definizione 34), possiamo scrivere

$$[g_1 + g_2] = [g_1] + [g_2] = \pi(g_1) + \pi(g_2)$$

e quindi π è un morfismo di gruppi.

3.2.4 Cardinalità di una classe di equivalenza

Sia G è un gruppo finito e $H \subseteq G$ è un sottogruppo. Se prendiamo la classe di equivalenza $[g]$ di un elemento $g \in G$, allora è lecito chiedersi quale sia la cardinalità di tale classe, ossia

$$|[g]| : [g] \in {}^{G}\!/_{H}$$

Per valutare la cardinalità di $[g]$, possiamo scrivere esplicitamente la classe di equivalenza. Se indichiamo con $*$ (non stiamo più considerando solo gruppi abeliani) l'operazione di G, allora possiamo scrivere una classe di equivalenza come

$$[g] = \{g' = g * h : h \in H\} = \{g * h : h \in H\}$$

perché $g \sim g' \iff g' = g * h$. Prendiamo ora due elementi $g * h_1$ e $g * h_2$ in $[g]$. Se questi elementi sono uguali,

$$g * h_1 = g * h_2$$

allora deve essere $h_1 = h_2$. Ma se $h_1 = h_2$, allora esiste un solo h per cui vale l'equivalenza e quindi sicuramente non possiamo avere più di un h per cui vale l'equivalenza, ossia $[g]$ non può avere cardinalità maggiore di $|H|$. La cardinalità di $[g]$ non può essere neanche minore di $|H|$, infatti avremmo $g_1 = g * h_1$ e $g_2 = g * h_2$ con $h_1 = h_2$ (cardinalità minore di $|H|$) ma $g_1 \neq g_2$. Quindi ogni elemento di ${}^{G}\!/_{H}$ contiene tanti elementi quanti ne contiene H.

$$|[g]| = |H|$$

Dato che valgono gli stessi ragionamenti fatti quando abbiamo introdotto l'insieme quoziente, allora G/H è una partizione di G, ossia

$$G = \biguplus_{[g] \in G/H} [g]$$

Quindi il numero di elementi di G è dato dal numero di partizioni, ossia la cardinalità di G/H, per il numero di elementi di ogni partizione, ossia $|[g]| = |H|$

$$|G| = \left|G/H\right||H|$$

Questo significa che, dato un gruppo G e un suo sottogruppo H, la cardinalità del sottogruppo divide quella del gruppo. In pratica, dato un gruppo di 7 elementi, non possiamo trovare un sottogruppo di 3 elementi perché 3 non divide 7.

3.2.5 Elementi generatori di una classe di resti

Fino ad ora abbiamo definito un gruppo $\mathbb{Z}_n$ chiamato gruppo dei resti modulo n definito come il gruppo quoziente di $\mathbb{Z}$ e l'insieme dei multipli di n, $n\mathbb{Z}$. Abbiamo poi delineato la cardinalità del gruppo $\mathbb{Z}_n$, appurando che fosse un multiplo della cardinalità dei suoi sottogruppi. Un gruppo $\mathbb{Z}_n$ ha quindi un sottogruppo, di cardinalità d, per ogni divisore d di $|\mathbb{Z}_n|$. Se consideriamo ad esempio $\mathbb{Z}_4$, dato che i divisori di 4 sono 1, 2 e 4, allora $\mathbb{Z}_4$ ha 3 sottogruppi, il primo di un elemento, il secondo di 2 elementi e il terzo di 4 elementi (ossia $\mathbb{Z}_4$ stesso). Volgiamo ora estendere questo ragionamento ad un qualsiasi gruppo $\mathbb{Z}_n$ e capire quali elementi generano i sottogruppi di $\mathbb{Z}_n$. Consideriamo quindi un numero naturale $m \in \mathbb{N}$ minore di n. Se $m = 0$, allora il sottogruppo generato dalla classe $[0]$ è il sottogruppo banale $\{[0]\}$. Consideriamo ora $m > 0$ e definiamo

$$z = \frac{\text{mcm}\{m, n\}}{m}$$

Se sommiamo la classe di m, ossia $[m] = \bar{m}$, z volte otteniamo

$$\bar{m} + \bar{m} + \cdots + \bar{m} = \overline{m + m + \cdots + m} = \overline{zm}$$

Ma per come abbiamo definito z, possiamo scrivere

$$\bar{m} + \bar{m} + \cdots + \bar{m} = \overline{m + m + \cdots + m} = z\bar{m} = \overline{\frac{\text{mcm}\{m, n\}}{m} m} = \overline{\text{mcm}\{m, n\}}$$

Ma per definizione, il minimo comune multiplo tra m e n è sicuramente divisore di n, quindi cade nella classe di resto $\bar{0}$.

$$\bar{m} + \bar{m} + \cdots + \bar{m} = \overline{m + m + \cdots + m} = z\bar{m} = \overline{\frac{\text{mcm}\{m, n\}}{m} m} = \overline{\text{mcm}\{m, n\}} = \bar{0}$$

Se invece consideriamo un numero naturale i minore di z, allora la somma di $\bar{m}$ per i volte è

$$\bar{m} + \bar{m} + \cdots + \bar{m} = \overline{im}$$

ed è diverso dalla classe $\bar{0}$. Questo perché $\overline{im}$ è un multiplo di m, ma non è divisibile per n, perché è più piccolo del minimo comune multiplo tra n e m. Quindi il gruppo generato da $\bar{m}$ ha z elementi

$$|\langle \bar{m} \rangle| = z = \frac{\text{mcm}\{m, n\}}{m}$$

Dalla formula appena enunciata possiamo capire che $\bar{m}$ genera tutto $\mathbb{Z}_n$ quando $z = n$ (perché $\mathbb{Z}_n = \{\bar{0}, \dots, \overline{n-1}\}$ ha cardinalità n), ossia quando $\text{mcm}\{m, n\} = mn$, che otteniamo quando m e n sono coprimi tra loro. Se ad esempio prendiamo $\mathbb{Z}_{14}$, gli elementi che generano $\mathbb{Z}_{14}$ stesso sono tutti tranne $\bar{0}$, $\bar{2}$ e $\bar{7}$, che non sono coprimi con $\overline{14}$. Formalmente otteniamo il seguente risultato.

Proposizione 4 (Generatori della classe di resto)**.** *Sia $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. Gli elementi che generano $\mathbb{Z}_n$ sono tutti i $\bar{m} \in \mathbb{Z}_n$ tali per cui m e n sono coprimi.*

Per capire quanti sono gli elementi di $\mathbb{Z}_n$ che generano $\mathbb{Z}_n$ possiamo utilizzare la funzione di Eulero, definita come segue.

Definizione 36 (Funzione di Eulero)**.** *La funzione*

$$\phi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$$

definita da

$$\phi(n) = \left|\{m \leq n : MCD(m, n) = 1\}\right|$$

prende il nome di funzione di Eulero e calcola il numero di valori m, minori di n, coprimi con n.

Quindi, ci sono $\phi(n)$ elementi $\bar{m}$ tali che il gruppo generato da $\bar{m}$ è $\mathbb{Z}_n$.

3.2.6 Sottogruppi di numeri interi con l'addizione

Consideriamo il classico gruppo $(\mathbb{Z}, +, 0)$ e proviamo a capire quali sono i suoi sottogruppi.

Proposizione 5 (Sottogruppi del gruppo degli interi con addizione)**.** *L'insieme dei sottogruppi di $(\mathbb{Z}, +, 0)$ è*

$$\{n\mathbb{Z} : n \in N\}$$

e non ce ne sono altri.

Proviamo ora a dimostrare la Proposizione 5. Prendiamo un sottogruppo non banale $H \subseteq \mathbb{Z}$ (per definizione con stessa operazione $+$ e identità 0). Prendiamo poi

$$k = \min\{h \in H : h > 0\}$$

e un elemento $h \geq 0$ del sottogruppo H diverso da k. Se k è il più piccolo elemento positivo di H e h deve essere diverso da k, allora h è sicuramente maggiore di k (ricordando che $h > 0$). Se $h > k$ allora posso fare la divisione con resto tra h e k e scrivere

$$h = nk + r \quad , n \in \mathbb{N}, 0 \leq r < k$$

Se esplicitiamo r, otteniamo

$$r = h - nk$$

Sia h che nk stanno in H, il primo per definizione, il secondo perché somma, n volte, dell'elemento k, che a sua volta sta in H (e H è un gruppo). Ma quindi r è la somma di due valori che stanno in

H (in realtà il secondo valore è l'inverso, ma comunque parlando di un gruppo non è un problema lavorare con l'inverso dato che questo fa sempre parte del gruppo), quindi anche r appartiene ad H. Ma dato che k era il minimo valore positivo di H, il resto è un valore compreso tra 0 e k e $r \in H$, allora il resto deve essere necessariamente 0. Per assurdo, se r fosse un numero $0 < r < k$, allora avremmo che esiste un numero $r > 0$ in H più piccolo di k, che è impossibile perché k è il minimo. Quindi $h = kn$ e dato che $h \in H$, allora H contiene tutti i multipli di k, dove k è il più piccolo valore positivo di H. In definitiva, H è il sottogruppo dei multipli di $\mathbb{Z}$.

3.3 Gruppi ciclici

Un'importante categoria di gruppi sono i gruppi ciclici. Vediamo cosa sono.

Definizione 37 (Gruppo ciclico)**.** *Un gruppo G si dice ciclico se può essere generato da un solo elemento*

$$\exists g \in G : G = \langle g \rangle$$

Un gruppo ciclico è anche abeliano.

Ad esempio, il nostro amico $(\mathbb{Z}, +, 0)$ è ciclico perché generato da 1.

$$(\mathbb{Z}, +, 0) = \langle 1 \rangle$$

Infatti, $(\mathbb{Z}, +)$ è il più piccolo sottogruppo che contiene l'elemento 1.

3.3.1 Teoremi importanti

Iniettività di un morfismo di gruppi

Teorema 4 (Iniettività di un morfismo di gruppi)**.** *Sia $f : G_1 \to G_2$ un morfismo di gruppi, allora f è iniettivo se e solo se il nucleo di f (26), $ker(f)$, contiene solo l'identità di G_1.*

$$f \text{ iniettivo} \iff ker(f) = \{e_1\}$$

Passiamo subito a dimostrare il teorema appena enunciato. Partiamo con il dimostrare che, se f è iniettivo, prendendo un elemento nel nucleo, questo elemento è l'identità e_1. Prendendo $x \in \ker(f)$, per definizione di nucleo (26),

$$f(x) = e_2$$

Dunque, siccome f è iniettivo ed è un morfismo di gruppi, l'unico elemento di G_1 che può andare in e_2 è e_1 e quindi $x = e_1$. Dimostriamo ora l'implicazione inversa, ossia che, se il nucleo contiene solo e_1, allora la funzione è iniettiva. Prendiamo quindi $\ker(f) = \{e_1\}$ e $x, y \in G_1$ tali che $f(x) = f(y)$. Per dimostrare che f è iniettiva dobbiamo mostrare che $x = y$. Allora, moltiplicando $f(x)$ per l'inverso di $f(y)$ (possibile perché f è un morfismo di gruppi, e $f(x)$ è un elemento di un gruppo), otteniamo

$$f(x)\big[f(y)\big]^{-1}$$

Si noti che con $\big[f(y)\big]^{-1}$ indentiamo l'elemento inverso di $f(y)$ e non la funzione inversa da G_2 a G_1. Per le proprietà dei morfismi di gruppi (Definizione 27) possiamo scrivere che

$$f(x)\big[f(y)\big]^{-1} = f(x)f(y^{-1})$$

e per definizione di morfismo (25)

$$f(x)\big[f(y)\big]^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

Inoltre, dato che $f(x) = f(y)$, allora moltiplicando $f(x)$ per il suo inverso $\big[f(y)\big]^{-1}$ otteniamo e_2.

$$e_2 = f(x)\big[f(y)\big]^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

Ma quindi, se $f(xy^{-1}) = e_2$, allora xy^{-1} deve appartenere al nucleo

$$xy^{-1} \in \ker(f)$$

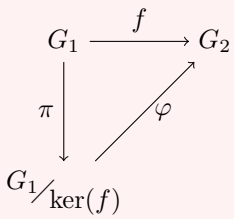
Ma il nucleo di f è per ipotesi solo e_1, quindi

$$\begin{aligned} xy^{-1} &= e_1 \\ x &= e_1 y \\ x &= y \end{aligned}$$

Teorema del diagramma

Un altro teorema fondamentale è il seguente.

Teorema 5. *Sia $f : G_1 \to G_2$ un morfismo di gruppi abeliani. Allora esiste un morfismo iniettivo di gruppi $\varphi : {}^{G}\!/_{\ker(f)} \to G_1$ tale che il diagramma*



è commutativo. In particolare ${}^{G_1}\!/_{\ker(f)}$ è isomorfo all'immagine di f.

$$G_1/\ker(f) \simeq \Im(f) \tag{3.1}$$

Questo significa che, partendo da G_1, possiamo andare in G_2 sia tramite f che, tramite π e φ, passando per il gruppo quoziente ${}^{G_1}\!/_{\ker f}$. Proviamo ora a dimostrare il teorema appena enunciato. Prendiamo l'assegnazione

$$[g] \to f(g)$$

con $[g] \in {}^{G_1}\!/_{\ker(f)}$, $g \in G_1$ e $f(g) \in G_2$. Questo assegnamento definisce una funzione $\phi : {}^{G_1}\!/_{\ker(f)} \to G_2$. Dobbiamo quindi dimostrare che ϕ sia effettivamente una funzione, ossia che, vale per qualsiasi $g \in G_1$. Infatti, se $g' \in [g]$ è un altro elemento della classe di equivalenza di g, allora $g' = g + h$ con $h \in \ker(f)$. Applicando f ottengo

$$f(g') = f(g + h)$$

Per le proprietà dei morfismi tra gruppi possiamo scrivere

$$f(g') = f(g + h) = f(g) + f(h)$$

Ma dato che h sta nel nucleo, allora $f(h) = e_2$ e quindi

$$\begin{aligned} f(g') &= f(g + h) \\ &= f(g) + f(h) \\ &= f(g) + e_2 \\ &= f(g) \end{aligned}$$

Quindi g e g' vengono mandati nello stesso valore e quindi φ è ben definita perché, prendendo qualsiasi valore di una classe di equivalenza, tale valore viene mandato nell'immagine del rappresentante della classe. Abbiamo quindi capito che φ è una funzione. Ora dobbiamo far vedere che è un morfismo di gruppi e che è iniettivo. Per dimostrare che φ è un morfismo di gruppi dobbiamo far vedere che

$$\varphi([g_1] + [g_2]) = \varphi([g_1]) + \varphi([g_2])$$

Iniziamo svolgendo la somma tra classi di equivalenza

$$\varphi([g_1] + [g_2]) = \varphi([g_1 + g_2])$$

Applichiamo poi la funzione φ

$$\begin{aligned} \varphi([g_1] + [g_2]) &= \varphi([g_1 + g_2]) \\ &= f(g_1 + g_2) \end{aligned}$$

Ma f è un morfismo di gruppi (noi vogliamo dimostrare che anche φ lo è), quindi

$$\begin{aligned} \varphi([g_1] + [g_2]) &= \varphi([g_1 + g_2]) \\ &= f(g_1 + g_2) \\ &= f(g_1) + f(g_2) \\ &= \varphi([g_1]) + \varphi([g_2]) \end{aligned}$$

Quindi, finalmente, possiamo affermare che φ è un morfismo di gruppi. L'ultimo passo per concludere la dimostrazione è dimostrare che ϕ è iniettivo. Per dimostrarlo possiamo usare il Teorema 4 e quindi verificare che il nucleo di φ contenga solo l'identità di ${}^{G_1}\!/_{\ker f}$. Il nucleo di φ è

$$\ker \varphi = \left\{ [g] \in {}^{G_1}\!/_{\ker f} : \varphi([g]) = f(g) = 0_2 \right\}$$

in cui 0_2 è l'identità di G_2. Ma quindi, dato che il nucleo di φ contiene tutti gli elementi g per cui $f(g) = 0_2$, allora è equivalente al nucleo di f.

$$\ker \varphi = \left\{ [g] \in {}^{G_1}\!/_{\ker f} : \varphi([g]) = f(g) = 0_2 \right\} = \ker f = \{[0_1]\}$$

Quindi il nucleo di φ contiene solo l'identità e quindi φ è iniettivo.

Ciclicità di sottogruppi

Passiamo ora ad un altro teorema molto importante che riguarda i gruppi ciclici (37), ossia quei gruppi che possono essere generati da un solo elemento.

Teorema 6 (Ciclicità dei sottogruppi di gruppi ciclici)**.** *Sia G un gruppo ciclico. Allora ogni sottogruppo di G è ciclico.*

Dimostriamo quindi il teorema. Prendiamo un elemento $g \in G$ tale che G è generato da g, ossia

$$G = \langle g \rangle$$

Prendiamo poi la funzione $\phi : (\mathbb{Z}, +) \to G$ definita come segue

$$\phi(n) = g^n$$

con $g^0 = e$ ed e identità di G. Inoltre vale $g^{-2} = (g^2)^{-1} = g^{-1}g^{-1}$. La funzione ϕ che abbiamo definito è un suriettivo morfismo di gruppi, perché G è generato da g. Vediamo prima il caso in cui G ha un numero infinito di elementi. In questo caso, il nucleo di ϕ è

$$\ker \phi = \{0\}$$

e quindi ϕ è iniettivo, per il Teorema 4. Essendo ϕ anche suriettivo, per ipotesi, allora ϕ è un isomorfismo (i.e., è biettivo). Quindi stiamo dicendo che un gruppo ciclico G è isomorfo al gruppo $(\mathbb{Z}, +)$, che è anch'esso ciclico (generato da $\langle 1 \rangle$) e quindi i sottogruppi di un gruppo ciclico sono ciclici. Consideriamo ora il caso finito. Prendiamo un sottogruppo $H \subseteq G$ di G e

$$\phi^{-1}(H) = \{n \in \mathbb{Z} : \phi(n) = g^n \in H\}$$

che è un sottogruppo di $\mathbb{Z}$. Ma se $\varphi^{-1}(H)$ è un sottogruppo di $\mathbb{Z}$, allora si può scrivere come

$$\phi^{-1}(H) = k\mathbb{Z}$$

per qualche k naturale. Consideriamo ora la restrizione

$$\varphi : k\mathbb{Z} \to H$$

ossia il morfismo suriettivo di gruppi che manda i multipli di k in H. A questo punto possiamo scrivere

$$\varphi(hk) = \varphi(k + k + \ldots_{h \text{ volte}} + k) = \varphi(k)\varphi(k)\ldots_{h \text{ volte}} \varphi(k) = \big[\varphi(k)\big]^n$$

Ma quindi H è generato da $\varphi(k)$

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

cioè H è ciclico.

Il seguente corollario deriva dal Teorema 6.

Teorema 7 (Ciclictà dei sottogruppi di gruppi ciclici (corollario)). *L'insieme dei sottogruppi di $\mathbb{Z}_n$, con $n \in \mathbb{N}$, è l'insieme dei sottogruppi generati dalle classi di resto di $\mathbb{Z}_n$.*

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

L'ultimo importante risultato che dobbiamo analizzare permette di definire quali sono i sottogruppi di $\mathbb{Z}_n$.

Proposizione 6 (Sottogruppi di classi di resto). *Sia $n \in N$ e sia d un divisore di n, i.e., $d|n$. Allora esiste un unico sottogruppo di $\mathbb{Z}_n$ di cardinalità d, generato da $\bar{d}$.*

La proposizione appena enunciata ci dice che, dato $\mathbb{Z}_n$, questo ha tanti sottogruppi quanti sono i suoi divisori, e ogni sottogruppo la cardinalità di un divisore di n. Inoltre, per la Proposizione 4, i sottogruppi propri sono quelli generati da $\bar{d}$ con d divisore di n. Proviamo a dimostrare questa affermazione. Prendiamo un sottogruppo H di $\mathbb{Z}_n$ tale che la sua cardinalità sia d. Consideriamo le proiezioni canoniche

$$\mathbb{Z} \xrightarrow{\pi_1} \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \xrightarrow{\pi_2} Z_n/H$$

che portano gli elementi di $\mathbb{Z}$ nella propria classe dei resti e gli elementi di $\mathbb{Z}_n$ nel proprio gruppo quoziente. Per costruzione, le proiezioni canoniche sono morfismi di gruppi, quindi la composizione di π_1 e π_2

$$\pi_2 \circ \pi_1 : \mathbb{Z} \to \mathbb{Z}_n/H$$

e un morfismo e dato che le proiezioni canoniche sono suriettive, allora anche la loro composta lo è. In definitiva, $\pi_2 \circ \pi_1$ è un morfismo di gruppi suriettivo. Consideriamo

$$\pi_1^{-1}(H) = \{m \in \mathbb{Z} : \pi_1(m) \in H\}$$

che è sottogruppo di $\mathbb{Z}$ e che quindi può essere scritto, essendo un sottogruppo di $\mathbb{Z}$, come

$$\pi_1^{-1}(H) = \{m \in \mathbb{Z} : \pi_1(m) \in H\} = k\mathbb{Z}$$

per qualche $k \in \mathbb{N}$. Proviamo ora a scrivere il nucleo della composta delle proiezioni. Partiamo dallo scrivere il nucleo di π_2, ossia gli elementi che vengono mandati in $[0]$. Un elemento g appartiene alla classe di equivalenza $[0]$ se e solo se, per come abbiamo definito l'operazione sul gruppo quoziente, $g = 0 + h$

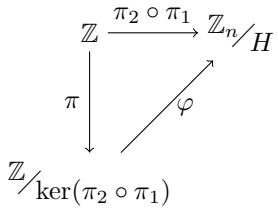
$$g \in [0] \iff g = 0 + h$$

Quindi, il nucleo di π è composto da tutti e soli gli elementi di H.

$$\ker \pi_2 = H$$

Quindi il nucleo della composta sono tutti gli elementi che da $\mathbb{Z}$ vanno in H, sottogruppo di $\mathbb{Z}_n$ di cardinalità d. Questi elementi sono $\pi_1^{-1}(H) = k\mathbb{Z}$. Ora, per dimostrare che sia solo uno il sottogruppo di cardinalità d, dobbiamo provare che k è unico. Consideriamo il morfismo suriettivo

di gruppi



Come visto nel Teorema 5, $\mathbb{Z}/\ker(\pi_2 \circ \pi_1)$ è isomorfo all'immagine di $\pi_2 \circ \pi_1$,

$$\Im(\pi_2 \circ \pi_1) = \mathbb{Z}_n/H \simeq \mathbb{Z}/\ker(\pi_2 \circ \pi_1) = \mathbb{Z}_k$$

Se $\mathbb{Z}_k$ è isomorfo a $\mathbb{Z}_n/H$, allora le loro cardinalità devono coincidere, e quindi possiamo scrivere

$$\begin{aligned} |\mathbb{Z}_k| &= \left|\mathbb{Z}_n/H\right| \\ |\mathbb{Z}_k| &= \frac{|\mathbb{Z}_n|}{|H|} \\ k &= \frac{n}{d} \end{aligned}$$

e quindi esiste un solo k, che è il risultato della divisione tra n e d, e così lo è H, che è

$$H = \pi_1(k\mathbb{Z})$$

3.3.2 Esempi

Applichiamo tutti i teoremi visti fin'ora nel seguente esempio. Vogliamo trovare tutti i sottogruppi di $\mathbb{Z}_{899}$. Dato che $899 = 29 \cdot 31$, allora i sottogruppi di $\mathbb{Z}_{899}$ sono 4 e sono

- $\langle \bar{0} \rangle$.
- $\langle \bar{29} \rangle$.
- $\langle \bar{31} \rangle$.
- $\mathbb{Z}_{899}$.

Chapter 4

Anelli

4.1 Introduzione

Iniziamo subito dando la definizione di anello.

Definizione 38 (Anello)**.** *Sia X un insieme su cui sono definite due operazioni $+$ (commutativa) e $\cdot$. X è un anello con unità 1_X se*

1. *$(X, +, 0)$ è un **gruppo abeliano**.*
2. *$(X, \cdot, 1_X)$ è un **monoide** la cui identità è 1_X.*
3. *Valgono le proprietà distributive (non è detto che $\cdot$ sia commutativa)*

$$(x + y) \cdot z = x \cdot z + y \cdot z \quad \forall x, y, z \in X$$

e

$$z \cdot (x + y) = z \cdot x + z \cdot y \quad \forall x, y, z \in X$$

Se il monoide $(X, \cdot)$ è commutativo, allora l'anello prende il nome di anello commutativo.

Notiamo che le operazioni $+$ e $\cdot$ potrebbero non avere nulla a che vedere con l'addizione e la moltiplicazione e sono semplicemente la notazione che usiamo per indicare due generiche operazioni di cui la prima è sempre commutativa.

Qualsiasi insieme di un solo elemento è un anello, se utilizziamo la stessa operazione per il gruppo e per il monoide. Un anello con un solo elemento prende il nome di **anello nullo**.

4.1.1 Zero divisore

Tra tutti gli elementi di un anello, uno in particolare ha grande importanza ed è quindi importante definirlo formalmente.

Definizione 39 (Zero divisore)**.** *Sia A un anello commutativo con 0 identità del gruppo $(A, +)$. Un elemento $x \in A$ di A è detto zero divisore se esiste un elemento non nullo*

$y \in A \setminus \{0\}$ *di* A *tale che*

$$x \cdot y = 0$$

Se avessimo preso un anello non commutativo avremmo dovuto specificare se lo zero divisore fosse destro o sinistro. Dato che l'anello in questo caso è commutativo, non è necessario specificare il lato dell'operazione. Se consideriamo l'anello delle matrici 2×2 con somma elemento per elemento e prodotto riga-colonna allora l'elemento

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

è uno zero divisore (sia destro che sinistro in questo caso, ma in generale non necessariamente) perché esiste

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

tale per cui

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

4.1.2 Elemento invertible

Un altro importante elemento di un anello è l'elemento invertibile, rispetto all'operazione di monoide.

Definizione 40 (Elemento invertible)**.** *Sia A un anello commutativo. Diciamo che un elemento $x \in A$ è invertible se è un elemento invertibile (17) del monoide $(A, \cdot)$.*

Se consideriamo ad esempio l'anello $A = (\mathbb{Z}, +, \cdot)$, in cui $+$ e $\cdot$ sono le classiche operazioni di somma e moltiplicazione, gli elementi invertibili di A sono l'insieme

$$\{1, -1\}$$

perché gli unici elementi $x \in \mathbb{Z}$ per cui possiamo trovare un altro elemento $y \in \mathbb{Z}$ tale per cui $x \cdot y = 1$ (con 1 identità dell'operazione $\cdot$).

Si noti che

Proposizione 7 (Invertibilità degli elementi zero-divisori)**.** *Sia A un anello commutativo. Allora, l'insieme degli elementi invertibili di A è disgiunto da quello degli elementi zero-divisori.*

In pratica, se un elemento $x \in A$ è uno zero-divisore, allora non è invertibile e quindi un elemento di un anello che non è uno zero divisore può non essere invertibile. Dimostriamo questa proposizione. Consideriamo uno zero divisore x, ossia una coppia $x, y \in A$ tale che $x \cdot y = 0$. Prendiamo ora x e, per assurdo assumiamo sia anche invertibile. Allora se moltiplico x per il suo inverso x^{-1} ottengo

$$x^{-1} \cdot x \cdot y = x^{-1} \cdot 0 = 0$$

Ma dato che x^{-1} è inverso di x, allora possiamo anche scrivere

$$0 = x^{-1} \cdot x \cdot y = 1 \cdot y = y$$

E quindi $y = 0$. Ma per la Definizione 39 di zero-divisore, y deve essere diverso da 0, quindi è assurdo affermare che x è uno zero-divisore e dunque x non può essere uno zero-divisore.

Un'altra importante proposizione riguardante gli anelli è la seguente.

Proposizione 8 (Legge di cancellazione)**.** *Sia A un anello commutativo e sia $x \in A$ un elemento non zero-divisore. Allora*

$$x \cdot y = x \cdot z \Rightarrow y = z \quad \forall x, y, z \in A$$

Per dimostrare questa affermazione ci basta scrivere

$$x \cdot y = x \cdot z \Rightarrow x \cdot y - x \cdot z = 0$$

Queste sono tutte operazioni che si possono fare perché l'operazione di somma (in cui la sottrazione è la somma per l'inverso) è definita nel gruppo e quindi abbiamo sempre un inverso e il prodotto di due elementi è sempre in $(A, \cdot)$, quindi anche in $(A, +)$. Raccogliendo x (dato che le operazioni sono associative) possiamo scrivere

$$\begin{aligned} x \cdot y = x \cdot z &\Rightarrow x \cdot y - x \cdot z = 0 \\ &\Rightarrow x \cdot (y - z) = 0 \end{aligned}$$

Ma dato che x non è uno zero divisore, allora $(y - z)$ deve essere uno zero divisore, quindi

$$y - z = 0 \iff y = z$$

e abbiamo mostrato che $y = z$.

4.1.3 Dominio di integrità

Definizione 41 (Dominio d'integrità)**.** *Un anello commutativo A privo di zero divisori (senza considerare lo zero, ossia l'identità di $(A, +)$) è detto dominio di integrità.*

Un esempio di dominio d'integrità è l'anello $(\mathbb{Z}, +, \cdot)$ perché non esiste elemento diverso da 0 che, moltiplicato per un altro elemento da 0.

4.1.4 Campi

Un'importante struttura algebrica definita a partire da un anello è quella di campo.

Definizione 42 (Campo)**.** *Un anello commutativo A i cui elementi non nulli sono tutti invertibili è detto campo.*

L'anello $(\mathbb{Z}, +, \cdot)$ è un esempio di anello che non è un campo mentre $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ sono sia anelli che campi. Dalla Proposizione 7 consegue

Proposizione 9 (Integrità di un campo)**.** *Un campo è un dominio di integrità.*

perché, abbiamo dimostrato che l'insieme di elementi invertibili e zero-divisori è disgiunto, quindi un elemento è in uno o nell'altro insieme. Se tutti gli elementi sono nell'insieme degli elementi zero divisori, allora quello degli elementi invertibili è vuoto (o al più ha solo lo 0), e quindi se tutti gli elementi sono invertibili nessuno è zero-divisore e quindi l'anello è un dominio di integrità.

4.2 Ideali

Definizione 43 (Ideale di un anello commutativo)**.** *Sia $(A, +, \cdot)$ un anello commutativo. Un sottoinsieme $I \subseteq A$ è detto ideale se*

1. *I è un sottogruppo di $(A, +)$.*
2. *Moltiplicando un elemento di I per un elemento di A, si ottiene un altro elemento in I.*

$$a \cdot x \in I, \quad \forall a \in A, \forall x \in I$$

Proviamo, ad esempio, a capire chi sono tutti gli ideali dell'anello $(Z, +, \cdot)$. Dato che un ideale di $\mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$, allora dobbiamo cercare gli ideali tra i sottogruppi di $\mathbb{Z}$. Come abbiamo già visto, i sottogruppi di $\mathbb{Z}$ sono tutti e soli

$$\{n\mathbb{Z} : n \in \mathbb{N}\} = \{\langle n \rangle : n \in \mathbb{N}\}$$

Tra tutti questi sottogruppi, vogliamo capire quali sono ideali. Prendiamo un elemento $x \in n\mathbb{Z}$ che quindi può essere scritto come $x = kn$, per qualche $k \in \mathbb{Z}$. Se ora prendiamo un altro elemento $a \in \mathbb{Z}$ allora possiamo scrivere

$$a \cdot x = a \cdot k \cdot n \in n\mathbb{Z}$$

Questo perché $\mathbb{Z}$ è un gruppo, e quindi $a \cdot k$ appartiene a $\mathbb{Z}$. Se $a \cdot k \in \mathbb{Z}$, allora $a \cdot k \cdot n \in n\mathbb{Z}$. Ma quindi abbiamo appena mostrato la definizione di ideale e, dato che questa vale per ogni n, allora tutti i sottogruppi $n\mathbb{Z}$ di $\mathbb{Z}$ sono ideali.

4.2.1 Proprietà

Se prendiamo un anello commutativo A e due suoi ideali $I, J \subseteq A$, allora

- L'intersezione di I e J è un ideale di A a sua volta.

$$I \cap J \subseteq A$$

- La somma di ideali I e J è un ideale di A a sua volta.

$$I + J = \{x + y : x \in I, y \in J\} \subseteq A$$

- Il prodotto di ideali I e J è un ideale di A a sua volta.

$$I \cdot J = \{x \cdot y : x \in I, y \in J\} \subseteq A$$

Facciamo degli esempi per convincerci del fatto che le proprietà elencate sopra sono vere. Consideriamo sempre $(\mathbb{Z}, +, \cdot)$ e i suoi ideali $I = \langle 2 \rangle$ e $J = \langle 3 \rangle$ (ricordando che i sottogruppi di $\mathbb{Z}$ sono tutti e soli quelli nella forma $\langle n \rangle$ e per lo più sono tutti ideali). L'intersezione di I e J è l'insieme di tutti gli elementi pari che sono divisibili per 3, ossia quelli generati da 6

$$I \cap J = \langle \text{mcm}\{2, 3\} \rangle = \langle 6 \rangle$$

che è in effetti un ideale di $(\mathbb{Z}, +, \cdot)$. Se consideriamo invece la somma di ideali, otteniamo

$$I + J = \mathbb{Z}$$

perché $-2 + 3 = 1 \in I + J$. Ma se $I + J$ contiene 1, allora può essere scritto come

$$I + J = \langle 1 \rangle$$

e dato che 1 genera tutto $\mathbb{Z}$, allora $I + J = \mathbb{Z}$. Concludiamo con il prodotto di ideali. Il prodotto di I e J è

$$I \cdot J = \langle 6 \rangle$$

Definizione 44 (Ideale generato da un sottoinsieme di un anello)**.** *Sia $S \subseteq A$ un sottoinsieme di un anello commutativo A. L'ideale generato da S è l'intersezione di tutti gli ideali di A che contengono S e lo indichiamo con*

$$\langle S \rangle$$

L'ideale generato da S è quindi il più piccolo ideale contenente S.

Definizione 45 (Ideale principale)**.** *Se $S \subseteq A$, sottoinsieme dell'anello A, è un insieme con un solo elemento, i.e., $|S| = 1$, allora diciamo che l'ideale generato da S è un ideale principale.*

Tra tutti gli anelli, possiamo distinguere un sottogruppo di anelli, detti anelli a ideali principali, che hanno delle proprietà molto interessanti.

Definizione 46 (Anello ad ideali principali)**.** *Un anello i cui ideali sono tutti principali prende il nome di anello ad ideali principali.*

Ora che conosciamo ideali e ideali principali, possiamo iniziare ad elencare alcune importanti proposizioni.

Proposizione 10. *Siano A un anello commutativo e $I \subseteq A$ un suo ideale. Allora*

1. *I coincide con A se e solo se I contiene un elemento invertibile.*

$$I = A \iff \exists x \in I : \exists y \in I : x \cdot y = 1$$

2. *A è un campo se e solo se i suoi unici ideali sono $\{0\}$ e l'ideale $A = \langle 1_A \rangle$ generato dall'unità 1_A.*

Dimostriamo la proposizione appena enunciata partendo dal primo punto. Iniziamo con mostrare l'implicazione da destra a sinistra, ossia che, se $I = A$ allora I contiene un elemento invertibile. Se $I = A$, allora $1_A \in I$ e 1_A è invertibile ($1_A \cdot 1_A = 1_A$), e quindi abbiamo dimostrato che almeno un elemento invertibile esiste. Dimostriamo ora l'implicazione inversa. Per ipotesi esiste un elemento invertibile $u \in I$. Allora $u^{-1} \in A$ (per definizione di elemento invertibile) e $1_A = u \cdot u^{-1}$ (sempre per definizione di elemento invertibile). Inoltre $1_A = u \cdot u^{-1} \in I$ perché I è un ideale e per definizione di ideale esiste un elemento $a \in A$ (in questo caso $a = u^{-1}$) tale per cui $a \cdot u \in I$. Ma se $1_A \in I$, allora I è generato da 1_A stesso e quindi $I = A$ perché 1_A genera A.

Dimostriamo ora il secondo punto, partendo dall'implicazione da destra a sinistra. Assumiamo quindi che A sia un campo (42) e dimostriamo che i suoi unici ideali sono quelli banali, ossia $\{0\}$ e A stesso. Prendiamo quindi per assurdo un ideale $I \neq \langle 0 \rangle$ e un suo elemento $x \in I \setminus \{0\}$. Dato che A è un campo, allora x è invertibile, quindi possiamo trovare un elemento $a = x^{-1} \in A$ tale per cui $x \cdot x^{-1} = 1_A \in I$, e quindi $I = A$ (come al punto precedente). Questo significa che se I non è $\{0\}$ allora I è tutto il campo. Mostriamo ora l'implicazione inversa. Ipotizziamo che gli unici ideali di A siano $\{0\}$ e A. Se prendiamo un qualsiasi elemento $x \in A \setminus \{0\}$, dobbiamo dimostrare che questo è invertibile (ossia che A è un campo). Se $x \in A$, allora possiamo dire che A è generato da x. Ma dato che A è generato anche da 1_A, allora possiamo scrivere

$$\langle x \rangle = \langle 1_A \rangle = A$$

Dato che A è anche ideale di se stesso, e sicuramente $1 \in A$ (altrimenti non sarebbe anello), allora 1 sta anche nell'ideale. Ma per definizione (43) di ideale, per ogni elemento $x \in A$ deve esistere un elemento $a \in I$ tale che $xa \in I$. Ma dato che $1 \in I$, allora la proprietà deve essere vera anche per 1, quindi deve esistere $\tilde{a}$ tale che $x\tilde{a} = 1$. e quindi x è invertibile (e il suo inverso è a). Poiché il ragionamento vale per ogni x, allora ogni elemento di A è invertibile e quindi A è un campo.

4.3 Anelli quoziente

Per i gruppi abbiamo definito il gruppo quoziente (34) rispetto ad un suo sottogruppo. La stessa cosa può essere fatta per gli anelli, in particolare possiamo definire l'anello quoziente rispetto ad un ideale. In particolare, possiamo prendere un anello, un suo ideale e definire il quoziente che, a sua volta, è un anello. Dati un anello commutativo $(A, +, \cdot, 1_A)$ e un suoi ideale $I \subseteq A$, per mostrare che A/I è un anello dobbiamo dimostrare che

- A/I con l'operazione $+$ è un gruppo.
- A/I con l'operazione $\cdot$ è un monoide, ossia che l'operazione è ben definita.

Dato che $(A, +)$ e $(I, +)$ sono gruppi (per definizione di anello e ideale, rispettivamente) allora anche il quoziente A/I è un gruppo, ed in particolare è il gruppo quoziente con operazione $+$. Concentriamoci quindi sull'operazione $\cdot$. Definiamo su A/I un'operazione $\cdot$ in modo da avere un anello, ossia tali per cui

$$[x] \cdot [y] = [xy] \quad \forall x, y \in A/I$$

Con questa operazione, A/I è un anello commutativo con unità $[1_A]$. Mostriamo che l'operazione $\cdot$ è ben definita, ossia che prendendo un qualsiasi rappresentante delle due classi, l'operazione è sempre valida. Prendiamo $x' \in [x]$ e $y' \in [y]$. Allora, per definizione di classe di equivalenza possiamo scrivere, ricordando che per i gruppi scrivevamo $g' \sim g \iff g' = g + h$,

$$x' = x + i_x \quad i_x \in I$$

e

$$y' = y + i_y \quad i_y \in I$$

Ma quindi

$$\begin{aligned} x' \cdot y' &= (x + i_x) \cdot (y + i_y) \\ &= x \cdot y + x \cdot i_y + y \cdot i_x + i_x \cdot i_y \end{aligned}$$

Ma dato che I è un ideale possiamo dire che $x \cdot i_y$, $y \cdot i_x$ e $i_x \cdot i_y$ stanno tutti in I (per definizione di ideale, $\exists a \in A, x \in I : ax \in I$) e quindi anche la loro somma sta in I. Questo implica che possiamo scrivere $x' \cdot y'$ come

$$x' \cdot y' = (x \cdot y) + i_{xy}$$

e quindi

$$(x' \cdot y') \sim (x \cdot y) \iff [x' \cdot y'] = [x \cdot y]$$

Se $[x' \cdot y'] = [x \cdot y]$, allora l'operazione $\cdot$ è ben definita per qualsiasi rappresentante prendiamo delle due classi, e quindi l'operazione in se è ben definita.

Definizione 47 (Anello quoziente)**.** *Sia $(A, +, \cdot, 1_A)$ un anello commutativo e sia $I \subseteq A$ un ideale di A. L'insieme quoziente A/I con le operazioni*

- $+$*, quindi* $[x] + [y] = [x + y]$.
- $\cdot$*, definita come* $[x] \cdot [y] = [xy] \quad \forall x, y \in A/I$.

e relazione di equivalenza

$$x \sim y \iff \exists i \in I : y = x + i \qquad \forall x, y \in A$$

è un anello con identità $[1_A]$.

L'anello quoziente A/I contiene quindi le classi di equivalenza di A, in cui ogni classe contiene tutti gli elementi uguali, a meno di multipli di un qualsiasi $i \in I$.

4.3.1 Esempi

Analizziamo ora alcuni esempi di anelli quoziente.

Anelli quoziente sui numeri interi

Se consideriamo l'anello $(\mathbb{Z}, +, \cdot)$, sappiamo bene che i suoi ideali sono tutti e soli quelli generati da $\langle n \rangle$, ossia

$$\{\langle n \rangle : n \in \mathbb{N}\}$$

Possiamo dunque definire l'anello quoziente

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n \rangle$$

4.3.2 Classi dei resti e campi

Ora che sappiamo che la classe di resti modulo n, i.e., $\mathbb{Z}_n$ è un anello quoziente, possiamo cercare di capire quando questa è un campo. Sicuramente $\mathbb{Z}_0$ non è un campo perché è isomorfo a $\mathbb{Z}$, che a sua volta non è un campo. L'anello $\mathbb{Z}_1 = \{0\}$, non contenendo elementi non nulli (contiene solo l'elemento nullo 0), potrebbe essere definito campo, anche se noi non lo considereremo come tale. Consideriamo ora $\mathbb{Z}_n$ con $n > 1$. Per dimostrare che $\mathbb{Z}_n$ è un campo, possiamo utilizzare la seconda condizione della Proposizione 10. Più precisamente, vogliamo vedere quali $\mathbb{Z}_n$ hanno come unici ideali quelli banali. L'insieme dei sottogruppi $\mathbb{Z}_n$ è

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

Cerchiamo di capire ora se i sottogruppi di $\mathbb{Z}_n$ sono degli ideali. Per definizione di ideale (43), ci basta trovare un elemento $\bar{a} \in \mathbb{Z}_n$ che moltiplicato per un elemento $\bar{m}$ di un sottogruppo $\langle \bar{m} \rangle$ di $\mathbb{Z}_n$ ritorna un altro elemento di $\langle \bar{m} \rangle$. In formule,

$$\begin{aligned} \bar{a} \cdot \bar{m} &= \overline{a \cdot m} \\ &= \bar{m} + \ldots_{a \text{ volte}} + \bar{m} \end{aligned}$$

Quindi possiamo scrivere $\bar{a} \cdot \bar{m}$ come la somma, a volte di $\bar{m}$ che è un elemento di $\langle \bar{m} \rangle$, e quindi $\langle \bar{m} \rangle$ è un ideale. Dato che il ragionamento funziona sul generatore dell'ideale, allora funziona su ogni elemento dell'ideale.

Quindi abbiamo capito che i sottoinsiemi $\langle \bar{m} \rangle$ sono ideali, ma che i sottoinsiemi banali $\mathbb{Z}_1 = \{0\}$ e $\mathbb{Z}_n$ non lo sono. Quindi vogliamo capire quali sottoinsiemi $\langle \bar{m} \rangle$ non coincidono con quelli banali. Per la Proposizione 4, sappiamo che gli elementi $\langle \bar{m} \rangle$ che generano $\mathbb{Z}_n$ sono tutti quelli per cui m e n sono coprimi, quindi possiamo scrivere i sottoinsiemi di $\mathbb{Z}_n$ come

$$\{\bar{m} : \bar{m} \in \mathbb{Z}_n\} = \{\{0\}, \mathbb{Z}_n\} \cup \{\langle \bar{m} \rangle : m \neq 0, MCD(m, n) \neq 1\}$$

Otteniamo quindi il seguente risultato.

Proposizione 11 (Classe di resto che è anche campo)**.** *$\mathbb{Z}_n$ è un campo se e solo se n è un numero primo.*

$$\mathbb{Z}_n \text{ campo} \iff \{\langle \bar{m} \rangle : \bar{m} \in \mathbb{Z}_n\} = \{\{0\}, \mathbb{Z}_n\}$$

Il campo appena trovato può essere indicato come segue.

Definizione 48 (Campo dell'insieme dei resti)**.** *Se $p \in \mathbb{N}$ è un numero primo, scriviamo*

$$\mathbb{F}_p = \mathbb{Z}_p$$

per indicare il campo $\mathbb{Z}_p$. Il campo $\mathbb{F}_p$ ha p elementi.

4.4 Algoritmo di Euclide e identità di Bézout

Per capire l'algoritmo di Euclide è utile partire da un esempio. Diciamo di voler calcolare il massimo comune divisore tra 365 e 1876. Per trovare $MCD\{365, 1876\}$ dobbiamo:

1. Dividere 1876 per 365, quello che otteniamo è 5 con resto 51.
$$1876 = 365 \cdot 5 + 51$$
2. Dividere 365 per il resto della divisione precedente, i.e., 51. Quello che otteniamo è 7 con resto 8.
$$365 = 51 \cdot 7 + 8$$
3. Dividere 51 per il resto della divisione precedente, i.e., 8. Quello che otteniamo è 6 con resto 3.
$$51 = 8 \cdot 6 + 3$$
4. Dividere 8 per il resto della divisione precedente, i.e., 3. Quello che otteniamo è 2 con resto 2.
$$8 = 3 \cdot 2 + 2$$
5. Dividere 3 per il resto della divisione precedente, i.e., 2. Quello che otteniamo è 1 con resto 1.
$$3 = 2 \cdot 1 + 1$$
6. Dividere 2 per il resto della divisione precedente, i.e., 1. Quello che otteniamo è 2 con resto 0.
$$2 = 2 \cdot 1 + 0$$
7. Terminare l'algoritmo perché il resto ottenuto è 0. Il massimo comune divisore è l'ultimo resto prima di ottenere resto 0, ossia
$$MCD\{365, 1876\} = 1$$

L'algoritmo di Euclide può essere utilizzato anche per trovare due numeri $x, y \in \mathbb{Z}$ tali che

$$365x + 1876y = MCD\{365, 1876\} = 1$$

Questi due numeri prendono il nome di **identità di Bézout**. In generale possiamo definire l'identità di Bézout come segue.

Definizione 49 (Identità di Bézout)**.** *Un'identità del tipo*

$$ax + by = MCD\{a, b\}$$

si chiama identità di Bézout.

Vediamo ora come calcolare l'identità di Bézout, dati due numeri a, b. Per calcolare l'identità di Bézout ci basta scrivere i resti ottenuti con l'algoritmo di Euclide in ordine inverso, ossia

1. $1 = 3 - 2 \cdot 1$
2. $2 = 8 - 3 \cdot 2$
3. $3 = 51 - 8 \cdot 6$
4. $8 = 365 - 51 \cdot 7$

5. $51 = 1876 - 365 \cdot 5$

Ora possiamo sostituire nell'equazione i il resto dell'equazione successiva. Partendo dalla prima equazione, sostituiamo il 2 con il valore nella seconda equazione. Poi il 3 nella seconda con il valore nella terza equazione e così via. Infine otteniamo

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (8 - 3 \cdot 2) \cdot 1 \\ &= 3 - (8 - 3 \cdot 2) \end{aligned}$$

A questo punto possiamo raccogliere a fattor comune il 3 per ottenere

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (8 - 3 \cdot 2) \cdot 1 \\ &= 3(1 + 2) - 8 \\ &= 3 \cdot 3 - 8 \end{aligned}$$

Sostituendo ora il 3 ottenuto dalla terza equazione possiamo scrivere

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (8 - 3 \cdot 2) \cdot 1 \\ &= 3(1 + 2) - 8 \\ &= 3 \cdot 3 - 8 \\ &= (51 - 8 \cdot 6) \cdot 3 - 8 \\ &= 51 \cdot 3 - 8(6 \cdot 3 + 1) \\ &= 51 \cdot 3 - 8 \cdot 19 \end{aligned}$$

Continuando a sostituire in questo modo otteniamo

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

Questo significa che se prendiamo $x = 136$ e $y = -699$, allora possiamo scrivere

$$1876 \cdot x + 365 \cdot y = 1$$

e quindi $x = 136$ e $y = -699$ sono l'identità di Bézout dei numeri 1876 e 365. In generale, vale il seguente teorema.

Teorema 8 (di Bézout)**.** *Siano $a, b \in \mathbb{N} \setminus \{0\}$ due numeri naturali non nulli.*

- *Se $a|b$ (a divide b), allora a è il massimo comune divisore tra a e b.*
$$MCD\{a, b\} = a$$
- *Se $a \not| b$ e r è l'ultimo resto non nullo nell'algoritmo di Euclide per a e b, allora r è il massimo comune divisore.*
$$MCD\{a, b\} = r$$

Inoltre esistono due numeri interi $x, y \in \mathbb{Z}$ tali che

$$ax + by = MCD\{a, b\}$$

4.4.1 Equazioni diofantee lineari

Siccome vogliamo studiare le equazioni diofantee lineari, conviene iniziare a definirle formalmente.

Definizione 50 (Equazione diofantea lineare)**.** *Un'equazione del tipo*

$$ax + bx = c \quad a, b, c \in \mathbb{Z}$$

è detta equazione diofantea lineare (perché entrambe le incognite hanno grado 1).

Dal Teorema 8 di Bézout, possiamo ricavare la seguente proposizione per le equazioni diofantee lineari.

Proposizione 12. *Siano $a, b, c \in \mathbb{Z}$ numeri interi, allora esistono $x, y \in \mathbb{Z}$ numeri interi tali che*

$$ax + by = c$$

se e solo se il massimo comune divisore tra a e b divide c.

$$ax + by = c \iff MCD\{a, b\}|c$$

Si noti che le soluzioni possono essere anche più di una, infatti la proposizione assicura solo che ne esiste almeno una. Proviamo a dimostrare ora la proposizione. Iniziamo dal dimostrare che, se esistono $x, y \in \mathbb{Z}$ allora $\text{MCD}\{a, b\}$ divide c. Se un numero r divide sia a che b, allora possiamo scrivere $a = r \cdot q_1$ e $b = r \cdot q_2$. Ma quindi l'equazione diventa

$$\begin{aligned}(r \cdot q_1) \cdot x + (r \cdot q_2) \cdot y &= c \\ r \cdot (q_1 \cdot x + q_2 \cdot y) &= c\end{aligned}$$

e quindi r divide anche c. Consideriamo poi l'implicazione inversa, ossia che se $d = \text{MCD}\{a, b\}$ divide c, allora esistono due interi x e y tali per cui $ax + by = c$. Per il Teorema 8 di Bézout possiamo dire

che

$$ax + by = d = \text{MCD}\{a, b\}$$

Ma se d divide c (per ipotesi), allora $c = kd$ con $k \in \mathbb{Z}$ e quindi possiamo scrivere

$$\begin{aligned} ax + by &= d \\ ax + by &= \frac{c}{k} \\ kax + kby &= c \\ a \cdot (kx) + b \cdot (ky) &= c \end{aligned}$$

e quindi i due numeri che stavamo cercando sono kx e ky.

4.4.2 Esempi

Esempio

Se consideriamo i numeri utilizzati per il teorema di Bézout possiamo scrivere l'equazione diofantea

$$365x - 1876y = 24$$

che ha soluzione, per la Proposizione 12, dato che $MCD365, 1876 = 1$ divide 24. Le soluzioni possono essere trovate sfruttando l'identità di Bézout, infatti, dall'esempio di prima sappiamo che

$$365 \cdot -699 + 1876 \cdot 136 = 1$$

e applicando la Proposizione 12, possiamo scrivere

$$\begin{aligned} 365 \cdot -699 + 1876 \cdot 136 &= 1 \\ 365 \cdot -699 + 1876 \cdot 136 &= \frac{24}{24} \\ 365 \cdot (24 \cdot -699) + 1876 \cdot (24 \cdot 136) &= \frac{24}{24} \end{aligned}$$

e quindi le soluzioni dell'equazione diofantea sono $x = -699 \cdot 24$ e $y = 24 \cdot 136$.

Classi di resto

In $\mathbb{Z}_{1876}$ calcoliamo, se esiste, l'inverso moltiplicativo di $\overline{365}$, ovvero cerchiamo $\bar{a} \in Z_{1876}$ tale che

$$\begin{aligned} \bar{a} \cdot \overline{365} &= \bar{1} \\ \overline{a \cdot 365} &= \bar{1} \end{aligned}$$

Per definizione di classe di resto, $365 \cdot a$ appartiene alla classe di resto 1 modulo 1876 (i.e., le due classi di resto sono uguali) se possiamo scrivere $365 \cdot a$ come 1876 per qualche intero b più 1, ossia

$$365 \cdot a = 1 + 1876 \cdot b$$

Ma quindi, riarrangiando i termini, possiamo scrivere l'identità di Bézout

$$365 \cdot a - 1876 \cdot b = 1$$

che ha soluzione $a = -699$, $b = -136$, quindi, l'inverso moltiplicativo di $\overline{365}$ è la classe $\bar{a} = \overline{-699} = \overline{1876 - 699} = \overline{1176}$.

4.4.3 Morfismi di anelli

Come abbiamo definito un morfismo tra gruppi e monoidi, allo stesso modo possiamo definire un morfismo tra anelli.

Definizione 51 (Morfismo di anelli)**.** *Siano A e B due anelli. Una funzione $f : A \to B$ è un morfismo di anelli se*

1. *$f : (A, +) \to (B, +)$ è un morfismo di gruppi.*
2. *$f : (A, \cdot) \to (B, \cdot)$ è un morfismo di monoidi.*

Definizione 52 (Nucleo di un morfismo di anelli)**.** *Siano A, B due anelli. Il nucleo di un morfismo di anelli $f : A \to B$ è il nucleo del morfismo di gruppi $f : (A, +) \to (B, +)$, ossia l'insieme*

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

Anche in questo caso vale quello che abbiamo detto per i morfismi di gruppi (Teorema 4), quindi se il nucleo di un morfismo di anelli è il nucleo banale, allora il morfismo è biettivo. Inoltre, vale anche la seguente proprietà.

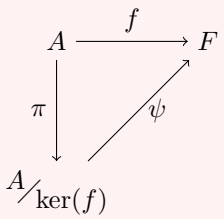
Proposizione 13 (Nucleo di un morfismo di anelli come ideale)**.** *Siano A, B due anelli commutativi e $f : A \to B$ un morfismo di anelli. Il nucleo $\ker(f) \subseteq A$ di f è un ideale di A.*

Come per i gruppi, possiamo definire un teorema (simile al Teorema 4) riguardante gli isomorfismi tra anelli.

Teorema 9 (Isomorfismo di 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.



Questo significa che, prendendo un elemento $a \in A$ e mandandolo in B tramite f, oppure prendendo lo stesso elemento $a \in A$ e mandandolo in ${}^{A}\!/_{\ker(f)}$ tramite π e poi in B tramite ψ, ottengo lo stesso elemento. In particolare,

Proposizione 14. *Se, nel diagramma del Teorema 9, f è suriettiva, allora anche ψ è suriettivo. Ma quindi, ψ è sia iniettivo (per il Teorema 9) che suriettivo, e dunque è iniettivo.*

4.4.4 Teorema cinese del resto

Prima di enunciare il teorema cinese dei resti, è necessario introdurre una nuova notazione. In particolare, indichiamo con $x \mod n$ la classe di equivalenza $\overline{x} \in Z_n$.

Teorema 10 (Cinese dei resti)**.** *Siano $n_1, \dots, n_k \in \mathbb{N} \setminus \{0, 1\}$ numeri naturali tali che*

$$MCD\{n_i, n_j\} = 1 \quad \forall 1 \leq i, j \leq k, i \neq j$$

Sia n il prodotto di tutti i numeri $n_1, \dots, n_k$

$$n = n_1 n_2 \dots n_k$$

Allora la funzione

$$\psi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$$

definita come

$$x \mod n \mapsto (x \mod n_1, \dots, x \mod n_k)$$

è un isomorfismo di anelli.

In pratica, la funzione ψ manda un elemento $x \mod n$ nell'insieme $(x \mod n_1, \dots, x \mod n_k)$. In altre parole, per ogni insieme $(x \mod n_1, \dots, x \mod n_k)$ esiste un solo $x \mod n$, e viceversa. Passiamo ora a dimostrare il teorema.

Proof. Sia $f : \mathbb{Z} \to \mathbb{Z}_{n_1} \times \dots Z_{n_k}$ definita come

$$f(x) = (x \mod n_1, \dots, x \mod n_k) \quad \forall x \in \mathbb{Z}$$

Dimostriamo che f è anche un morfismo di anelli. In particolare, partiamo dal mostrare che l'operazione di somma è ben definita

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

Sviluppando $f(a + b)$ otteniamo

$$\begin{aligned} f(a+b) &= \big((a+b) \mod n_1, \dots, (a+b) \mod n_k\big) \\ &= \big(a \mod n_1 + b \mod n_1, \dots, a \mod n_k + b \mod n_k\big) && \mathbb{Z}_{n_i}\text{anelli} \\ &= \big(a \mod n_1, \dots, a \mod n_k\big) + \big(b \mod n_1, \dots, b \mod n_k\big) \\ &= f(a) + f(b) \end{aligned}$$

Dimostriamo ora che anche l'operazione di moltiplicazione è ben definita.

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

Sviluppando $f(a \cdot b)$ otteniamo

$$\begin{aligned} f(a \cdot b) &= \big((a \cdot b) \mod n_1, \dots, (a \cdot b) \mod n_k\big) \\ &= \big(a \mod n_1 \cdot b \mod n_1, \dots, a \mod n_k \cdot b \mod n_k\big) && \mathbb{Z}_{n_i}\text{anelli} \\ &= \big(a \mod n_1, \dots, a \mod n_k\big) \cdot \big(b \mod n_1, \dots, b \mod n_k\big) \\ &= f(a) \cdot f(b) \end{aligned}$$

Mostriamo infine che l'identità venga mandata nell'identità.

$$\begin{aligned} f(1) &= (1 \mod n_1, \dots, 1 \mod n_k) \\ &= (1_{Z_{n_1}}, \dots, 1_{Z_{n_1}}) \end{aligned}$$

Dato che $(1_{Z_{n_1}}, \dots, 1_{Z_{n_1}})$ è l'identità di $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, allora l'identità di $\mathbb{Z}$ viene mandata nell'identità di $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

A questo punto possiamo notare che il massimo comune divisore tra n_i e $\frac{n}{n_i}$ è uguale a 1 perché, avendo diviso n per n_i, allora n_i non è divisore di $\frac{n}{n_i}$ e, tutti gli altri divisori n_j non dividono n_i, poiché $\text{MCD}\{n_i, n_j\} = 1$. In formule

$$\text{MCD}\left\{n_i, \frac{n}{n_i}\right\} = 1 \quad \forall 1 \leq i \leq k$$

Grazie all'identità di Bézout (49), possiamo scrivere

$$an_i + b\frac{n}{n_i} = 1$$

Possiamo ora definire

$$v_i = b\frac{n}{n_i}$$

che è un elemento dell'ideale generato da $\frac{n}{n_i}$, ossia dall'ideale $\langle \frac{n}{n_i} \rangle$. Sia poi un elemento $(\overline{a}_1, \dots, \overline{a}_k) \in (\mathbb{Z}_{n_1}, \dots, \mathbb{Z}_{n_k})$ nell'immagine e sia x definito come segue

$$x = a_1v_1 + a_2v_2 + \cdots + a_kv_k$$

Allora proviamo a dimostrare che

$$f(x) = (\overline{a}_1, \dots, \overline{a}_k)$$

Dato che f è un morfismo di anelli, possiamo scrivere

$$f(x) = f(a_1)f(v_1) + \cdots + f(a_k)f(v_k)$$

A questo punto ci serve sapere chi è $v_i \mod n_j$:

- Se $i = j$, allora $v_i = v_j = b\frac{n}{n_j}$, allora per l'identità di Bézout abbiamo $v_i \mod n_j = b\frac{n}{n_j} \mod n_j = 1$, perché $\text{MCD}(n_j, \frac{n}{n_j}) = 1$. In particolare, scrivendo l'identità di Bézout

  $$an_i + b\frac{n}{n_i} = 1$$

  e applicando l'operazione di modulo, otteniamo

  $$\begin{aligned} an_i \mod n_i + b\frac{n}{n_i} \mod n_i &= 1 \mod n_i \\ 0 + b\frac{n}{n_i} \mod n_i &= 1 \mod n_i \end{aligned}$$

- Se $i \neq j$, allora $v_i = b\frac{n}{n_i}$, quindi n contiene il fattore n_j e quindi n è divisibile per n_j (i.e., il resto della divisione è 0).

Riassumendo,

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

Ma dato che $f(v_i) = (v_i \mod n_1, \ldots, v_i \mod n_k)$, allora tutte le componenti di $f(v_i)$ sono nulle, tranne per $v_i \mod n_i$:

$$f(v_i) = (0, \ldots, 1 \mod n_i, \ldots, 0)$$

Quindi abbiamo un morfismo suriettivo di anelli commutativi

$$f : \mathbb{Z} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

e dal teorema di isomorfismo (9), abbiamo che esiste un isomorfismo

$$\psi : \mathbb{Z}/\ker\{f\} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

Il nucleo di f è l'insieme dei numeri in $x \in \mathbb{Z}$ tali che $f(z) = (0, \ldots, 0)$, ossia l'intersezione degli ideali $\langle n_i \rangle$ dove $\langle n_i \rangle$ è l'ideale dei multipli di n_i.

$$\ker\{f\} = \langle n_1 \rangle \cap \cdots \cap \langle n_k \rangle = \langle \text{mcm}\{n_1, \ldots, n_k\} \rangle = \langle n \rangle$$

dato che n_i sono tutti coprimi tra loro. Quindi

$$\mathbb{Z}/\ker(f) = \mathbb{Z}/\langle n \rangle = \mathbb{Z}_n$$

Ma quindi abbiamo mostrato che ϕ è un morfismo iniettivo e suriettivo che va da $\mathbb{Z}_n$ a $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, ossia il morfismo ϕ che stavamo dimostrando essere un isomorfismo. □

Si noti che tutta questa dimostrazione si basa sul fatto che n_i sono tutti coprimi tra loro, altrimenti non avremmo potuto scrivere l'identità di Bézout.

Esempio

Siano $n_1 = 3$, $n_2 = 7$ ed $n_3 = 10$, quindi $n = 3 \cdot 7 \cdot 10 = 210$. Per il Teorema cinese dei resti (10), essendo n_1, n_2 e n_3 coprimi tra loro,

$$Z_{210} = Z_3 \times Z_7 \times Z_{10}$$

Essendo Z_{210} isomorfo a $Z_3 \times Z_7 \times Z_{10}$ allora prendendo un elemento nel secondo insieme, possiamo trovare il corrispondente nel primo. Sia, ad esempio $(2 \mod 3, 5 \mod 7, 4 \mod 10)$ un elemento in $Z_3 \times Z_7 \times Z_{10}$. Tramite l'isomorfismo definito nel Teorema cinese dei resti (10), possiamo ottenere il corrispondente valore in Z_{210}, ossia l'unico elemento $x \mod 210$ tale che

$$\begin{cases} x \mod 3 \equiv 2 \mod 3 \\ x \mod 7 \equiv 5 \mod 7 \\ x \mod 10 \equiv 4 \mod 10 \end{cases}$$

Dalla dimostrazione del teorema cinese dei resti, sappiamo che possiamo scrivere x come

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

e quindi ci basta trovare v_1, v_2 e v_3. Sempre dalla dimostrazione del teorema cinese dei resti, e alla identità di Bézout, possiamo scrivere le equazioni

$$an_i + b\frac{n}{n_i} = 1$$

Sostituendo con i valori presi in considerazione nel nostro esempio otteniamo

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

Dato che nella dimostrazione abbiamo definito $v_i = b\frac{n}{n_i}$, allora possiamo ricavare v_1, v_2 e v_3 dal precedente sistema come

$$\begin{aligned} v_1 &= 70b \\ v_2 &= 30b \\ v_3 &= 21b \end{aligned}$$

Iniziamo a risolvere la prima equazione. Per $b = 1$, otteniamo

$$\begin{aligned} 3a + 70 &= 1 \\ 3a &= 1 - 70 \\ 3a &= -69 \end{aligned}$$

Ma dato che 69 è divisibile per 3, allora possiamo calcolare $a = -23$. Quindi sappiamo che

$$v_1 = 70b = 70$$

La soluzione della seconda equazione di Bézout è $a = 7$, $b = -30$, quindi

$$v_2 = -3 \cdot 30 = -90$$

Infine, il risultato della terza equazione è $a = -2$, $b = 1$ e quindi

$$v_3 = 21$$

Sostituendo i valori di v_i appena trovati, possiamo calcolare x come

$$\begin{aligned} x &= 2v_1 + 5v_2 + 4v_3 \\ &= 2 \cdot 70 - 5 \cdot 90 + 4 \cdot 21 \\ &= 194 \end{aligned}$$

e quindi

$$\begin{cases} 194 \mod 3 \equiv 2 \mod 3 \\ 194 \mod 7 \equiv 5 \mod 7 \\ 194 \mod 10 \equiv 4 \mod 10 \end{cases}$$

Corollari

I seguenti sono corollari del teorema cinese dei resti.

Teorema 11 (Teorema cinese dei resti (Corollario)). *Sia $U(\mathbb{Z}_n)$ il gruppo, rispetto alla moltiplicazione, degli elementi invertibili dell'anello $\mathbb{Z}_n$. Sia $n = n_1 \cdot \cdots \cdot n_k$ con tutti i numeri n_i, n_j coprimi tra loro. Allora come gruppi*

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

Per dimostrare questo teorema basta restringere l'isomorfismo del teorema cinese dei resti al solo gruppo $U(\mathbb{Z}_n)$ dell'anello.

Teorema 12 (Teorema cinese dei resti (Corollario)). *Un elemento $x \in \mathbb{Z}_n$ è invertibile se e solo se esiste l'identità di Bézout*

$$ax + bn = 1$$

In più, la cardinalità degli elementi invertibili è data dalla funzione di Eulero $\varphi(n)$.

$$|U(\mathbb{Z}_n)| = \varphi(n)$$

Come conseguenza del corollario 11, otteniamo il seguente corollario.

Teorema 13 (Teorema cinese dei resti (Corollario)). *Sia $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ la funzione di Eulero. Siano $x, y \in \mathbb{N} \setminus \{0\}$ tali che $MCD\{x, y\} = 1$, allora*

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

Proof. Siccome x e y sono coprimi, allora per il Corollario 11 abbiamo

$$U(\mathbb{Z}_{xy}) \simeq U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)$$

Ma per il Corollario 12,

$$\varphi(xy) = |U(\mathbb{Z}_{xy})|$$

Ma essendo $U(\mathbb{Z}_{xy})$ isomorfo a $U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)$, allora la cardinalità del primo è uguale a quella di $U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)$. Possiamo quindi scrivere

$$\varphi(xy) = |U(\mathbb{Z}_{xy})| = |U(\mathbb{Z}_x) \times U(\mathbb{Z}_y)|$$

Ma la cardinalità del prodotto cartesiano è il prodotto delle cardinalità dei singoli insiemi e quindi possiamo scrivere

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

□

Grazie a questo corollario, possiamo trovare un modo per calcolare il numero di Eulero. In particolare, se consideriamo un numero primo p, allora la funzione di Eulero di p^k può essere calcolata come la differenza tra tutti i numeri più piccoli di p^k (i.e., tutti i possibili divisori) e i numeri che

hanno almeno un divisore in comune con p^k. I numeri minori di o uguali a p^k sono, in totale, p^k. I numeri che hanno un fattore in comune con p^k sono invece

$$1, p, 2p, 3p, \dots, p^{k-1}p$$

e quindi sono, in numero, p^{k-1}. Sottraendo il secondo numero al primo otteniamo che

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

In generale, dato un numero $n = p_1^{k_1} \cdot \dots \cdot p_h^{k_h}$, possiamo scrivere

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1}) \cdot \varphi(p_h^{k_h}) \\
&= (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_h^{k_h} - p_h^{k_h-1}) \\
&= p_1^{k_1} \cdot \dots \cdot p_k^{k_h} (1 - \frac{p_1^{k_1-1}}{p_1^{k_1}}) \cdot \left(1 - \frac{p_h^{k_h-1}}{p_h^{k_h}}\right) \\
&= p_1^{k_1} \cdot \dots \cdot p_k^{k_h} \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_h}\right) \\
&= n \prod_{p|n} \left(1 - \frac{1}{p}\right)
\end{aligned}$$

4.4.5 Teorema di Eulero

Teorema 14 (Eulero)**.** *Siano $n \in \mathbb{N}\backslash\{0\}$, $a \in \mathbb{N}$ due numeri naturali tali che $MCD\{a, n\} = 1$. Allora, in $\mathbb{Z}_n$,*

$$\overline{a^{\phi(n)}} = \overline{1}$$

oppure, scritto in un altro modo,

$$a^{\phi(n)} \equiv 1 \mod n$$

in cui ϕ è la funzione di Eulero (36).

Proof. Dal Teorema 10 sappiamo che $\varphi(n)$ è la cardinalità del gruppo degli elementi invertibili di $\mathbb{Z}_n$ (rispetto alla moltiplicazione), ossia

$$\varphi(n) = |U(\mathbb{Z}_n)|$$

Prendiamo ora il sottogruppo $\langle \bar{a} \rangle \subseteq U(\mathbb{Z}_n)$. La cardinalità di questo sottogruppo divide quella di $U(\mathbb{Z}_n)$ e quindi divide $\varphi(n)$. Possiamo quindi scrivere

$$\varphi(n) = k|\langle \bar{a} \rangle| = kc$$

dove abbiamo definito $c \coloneqq |\langle \bar{a} \rangle|$. A questo punto possiamo scrivere a^c come

$$\begin{aligned}
\overline{a^c} &= \overline{1} \\
&= \overline{a^c} \\
&= \left(\overline{a^c}\right)^k && \mathbb{Z}_n \text{ ciclico} \\
&= \overline{a^{\phi(n)}}
\end{aligned}$$

□

Come corollario di questo teorema, abbiamo il piccolo teorema di Fermat.

Teorema 15 (Piccolo teorema di Fermat)**.** *Sia p un numero primo e $a \in \mathbb{N}$. Allora in $\mathbb{Z}_p$ abbiamo*

$$\overline{a} = \overline{a^p}$$

ossia

$$a^p \equiv a \mod p$$

Proof. Iniziamo a considerare il caso in cui $a \in \{0, 1\}$ e p non divide a. In questo caso è immediato vedere che le due classi $\overline{a}$ e $\overline{a^p}$ sono equivalenti. Consideriamo ora il caso in cui p divide a. Per il Teorema di Eulero (14), abbiamo che

$$a^{\varphi(p)} = 1 \mod p$$

Ma la funzione di Eulero di un numero primo p vale $p - 1$ (applicando la formula p ha un solo divisore, con molteplicità 1, che è p stesso). Possiamo quindi scrivere

$$a^{p-1} = 1 \mod p$$

Moltiplicando per a a destra e a sinistra otteniamo

$$a^p \equiv a \mod p$$

□

Esempi

Si vogliono calcolare le ultime due cifre di 7^{500000} usando il teorema di Eulero. Dato che siamo interessati solo alle ultime due cifre, possiamo calcolare $7^{500000} \mod 100$ ($89172 = 891 \cdot 100 + 72$). Per calcolare

$$7^{500000} \mod 100$$

possiamo sfruttare il fatto che

$$7^{\varphi(100)} \equiv 1 \mod 100$$

Calcoliamo quindi la funzione di Eulero di 100. Dato che $100 = 5^2 \cdot 2^2$, allora

$$\varphi(100) = (5^2 - 5^1) \cdot (2^2 - 2^1) = (25 - 5) \cdot (4 - 2) = 20 \cdot 2 = 40$$

Dato che 500000 è divisibile per 40, allora possiamo scrivere

$$\begin{aligned} 7^{500000} \mod 100 &= 7^{\phi(100) \cdot x} \mod 100 \\ &= 1^x \mod 100 \\ &= 1 \mod 100 \end{aligned}$$

e quindi le ultime due cifre di 7^{500000} sono 01.

4.4.6 Caratteristica

La caratteristica di un anello è la cardinalità del sottogruppo additivo generato dall'unità. Più precisamente,

Definizione 53 (Caratteristica di un anello)**.** *Sia A un anello (con unità). Il sottogruppo abeliano*

$$\langle 1_A \rangle \subseteq (A, +)$$

è un gruppo ciclico. Quindi esiste un numero naturale $n \in \mathbb{N}$ tale che $\langle 1_A \rangle$ è isomorfo a $\mathbb{Z}_n$, ossia

$$\langle 1_A \rangle \simeq \mathbb{Z}_n$$

Il numero n così definito è detto caratteristica dell'anello e scriviamo

$$\mathrm{char}(A) = n$$

Consideriamo subito degli esempi per capire meglio come funziona la caratteristica di un anello. Calcoliamo ad esempio la caratteristica dell'anello $\mathbb{Z}$. Dato che $\mathbb{Z}$ è generato da 1, allora

$$\mathbb{Z} \simeq \langle 1 \rangle = \mathbb{Z}_0$$

quindi

$$\mathrm{char}(\mathbb{Z}) = 0$$

Allo stesso modo, anche la caratteristica di $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ è 0. Vediamo ora casi di caratteristica diversa da 0. Consideriamo ad esempio la caratteristica di $\mathbb{Z}_n$ dove n è un numero naturale qualsiasi. La caratteristica di $\mathbb{Z}_n$ è n,

$$\mathrm{char}(\mathbb{Z}_n) = n$$

perché il sottogruppo additivo $(\mathbb{Z}_n, +)$ è generato da $\langle \bar{1} \rangle$.

4.4.7 Sottocampi e sottoanelli fondamentali

Diamo ora la definizione di sottocampo di un campo.

Definizione 54 (Sottoanello fondamentale)**.** *Sia A un anello (anche non commutativo) e sia $\langle 1_A \rangle \subseteq (A, +)$ il sottogruppo generato dall'unità. L'intersezione di tutti i sottoanelli di A contenenti $\langle 1_A \rangle$ si chiama sottoanello fondamentale di A.*

Si noti che $\langle 1_A \rangle$ è un gruppo, ma non necessariamente un anello. Il più piccolo anello di A che contiene $\langle 1_A \rangle$ è il sottoanello fondamentale.

Ad esempio, il sottoanello fondamentale di $\mathbb{Z}$ è $\mathbb{Z}$ stesso. La stessa cosa vale per $\mathbb{Q}$, $\mathbb{C}$ ed $\mathbb{R}$, infatti in tutti questi casi il sottoanello fondamentale è $\mathbb{Z}$. Definiamo ora il sottocampo fondamentale di un campo.

Definizione 55 (Sottocampo fondamentale)**.** *Sia K un campo e sia $\langle 1_K \rangle \subseteq (K, +)$ il sottogruppo generato dall'unità. L'intersezione di tutti i sottocampi di K contenenti $\langle 1_K \rangle$ si chiama sottocampo fondamentale di K.*

Ad esempio, il sottocampo fondamentale di $\mathbb{Q}$ è $\mathbb{Q}$ perché è il più piccolo sottocampo di $\mathbb{Q}$ che contiene $\mathbb{Z}$ (ossia $\langle 1_{\mathbb{Q}} \rangle$). La stessa cosa vale anche per $\mathbb{R}$ e $\mathbb{C}$, il cui sottocampo fondamentale è $\mathbb{Q}$, in entrambi i casi. Consideriamo ora un altro esempio. Sia $p \in \mathbb{N}$ un numero primo, allora il sottocampo fondamentale di $\mathbb{F}_p$ è $\mathbb{F}_p$ stesso, perché $\langle \bar{1} \rangle$ genera $\mathbb{F}_p$ stesso.

4.5 Polinomi

Vogliamo dare la definizione di polinomi in una sola indeterminata (o incognita) a coefficienti in un campo. Prima però dobbiamo definire il concetto di successione.

Definizione 56 (Successione)**.** *Sia K un campo. Una funzione*

$$f : \mathbb{N} \to K$$

è chiamata successione a valori in K.

Ad esempio, una successione in $\mathbb{Q}$,

$$1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}$$

può essere scritta come

$$\begin{aligned} a_0 &= 1 \\ a_1 &= \frac{1}{2} \\ a_2 &= \frac{1}{3} \\ &\vdots \\ a_n &= \frac{1}{n} \end{aligned}$$

La successione può quindi essere scritta anche come una funzione f definita come

$$\begin{aligned} f(0) &= 1 \\ f(1) &= \frac{1}{2} \\ f(2) &= \frac{1}{3} \\ &\vdots \\ f(n) &= \frac{1}{n} \end{aligned}$$

Grazie alle successioni, possiamo definire il concetto di serie formale, che è una generalizzazione del concetto di serie (i.e., non ci interessa se la serie formale converge o diverge).

Definizione 57 (Serie formale)**.** *Ad una successione a valori in K corrisponde una serie formale nell'indeterminata x che indichiamo come*

$$\sum_{n \in \mathbb{N}} f(n) \cdot x^n$$

Definizione 58 (Polinomio)**.** *Se l'insieme*

$$\{n \in N : f(n) \neq 0\}$$

è finito diciamo che la serie formale

$$\sum_{n \in \mathbb{N}} f(x)x^n$$

è un polinomio P nell'indeterminata x di grado

$$\deg(P) = \max\{n \in N : f(n) \neq 0\}$$

Si noti che noi non definiremo il grado del polinomio 0, ossia del polinomio generato dalla successione di tutti 0.

4.5.1 Insieme dei polinomi

L'insieme dei polinomi in x a coefficienti nel campo K può essere indicato come $K[x]$. L'insieme $K[x]$ ha struttura di anello commutativo con le operazioni di somma e prodotto. Andiamo dunque a definire la somma e il prodotto di polinomi.

Definizione 59 (Anello di polinomi)**.** *L'insieme $K[x]$ dei polinomi nell'indeterminata x su un campo K è un anello con:*

- *Somma di $P = \sum_n a_n x^n$ e $Q = \sum_n b_n x^n$ definita come*

$$P + Q = \sum_n (a_n + b_n)x^n$$

- *Prodotto di $P = \sum_n a_n x^n$ e $Q = \sum_n b_n x^n$ definita come*

$$P + Q = \sum_n \big(\sum_i^n a_i \cdot b_{n-i} \big) \cdot x^n$$

- *Unità di $K[x]$ il polinomio 1, ossia la successione*

$$1 + 0x + 0x^2 + 0x^3 + \dots$$

Si noti che, dato che entrambe le serie usate per definire P e Q, anche la serie definita dalla somma e dal prodotto di P e Q termina. Facciamo ora un esempio. Prendiamo i polinomi a coefficienti in $\mathbb{F}_2[x]$,

$$P = 1 + x^2 + x^3$$

e

$$Q = x + x^2$$

La somma dei due polinomi è

$$P + Q = (1 + 0) + (0 + 1)x + (1 + 1)x^2 + (1 + 0)x^3 = 1 + x + x^3$$

Il prodotto dei due polinomi è invece

$$P \cdot Q = (1 + x^2 + x^3)(x + x^2) = x + x^2 + x^3 + x^4 + x^4 + x^5 = x + x^2 + x^3 + x^5$$

Si noti che, essendo in $\mathbb{F}_2$, allora vale $1 + 1 = 0$. Essenzialmente, i polinomi in $\mathbb{F}_2[x]$ sono quelli a coefficienti 0 o 1. Enunciamo ora un'importante proprietà dei polinomi.

Proposizione 15. *Siano P e Q due polinomi non nulli in un campo $K[x]$ (i.e., $P, Q \in K[x] \setminus \{0\}$). Il grado del prodotto dei polinomi è la somma dei gradi.*

$$\deg(PQ) = \deg(P) + \deg(Q)$$

In particolare, l'anello $K[x]$ è un dominio d'integrità (Definizione 41).

Dato che ci servirà poi, conviene definire subito cos'è un polinomio monico.

Definizione 60 (Polinomio monico)**.** *Un polinomio si dice monico se il coefficiente del termine di grado massimo è 1.*

Quindi ad esempio il polinomio $2 + 3x + 4x^2 + x^3$ è monico. Chiarito questo concetto, dobbiamo definire quando un polinomio è riducibile e quando invece è irriducibile.

Definizione 61 (Polinomio irriducibile)**.** *Sia $P \in K[x]$ un polinomio, $a \in K$, allora P si dice irriducibile se i suoi unici divisori sono del tipo*

$$a$$

e

$$a \cdot P$$

Altrimenti diciamo che P è riducibile.

In altre parole, i fattori di un polinomio sono o un numero a (nel campo) o il polinomio stesso moltiplicato per un valore a (nel campo). Questo significa che non otteniamo mai divisori di grado minore di quelli del polinomio. Facciamo un esempio per capire meglio. In $\mathbb{F}_2[x]$, il polinomio

$$x^2 + 1$$

è riducibile, infatti può essere scritto come $(x + 1)^2$

$$\begin{aligned}(x + 1)^2 &= x^2 + 1^2 + 2x \\ &= x^2 + 1\end{aligned}$$

e quindi esiste un polinomio diverso da $x^2 + 1$, ossia $(x + 1)$ che divide $x^2 + 1$.

Un'importante proprietà riguardante la riducibilità dei polinomi con coefficienti in un campo è la seguente.

Proposizione 16. *In $K[x]$, ogni polinomio di grado 1 è irriducibile.*

4.5.2 Radici di un polinomio

Definizione 62 (Radice di un polinomio)**.** *Sia $\alpha \in K$ un elemento del campo K. α è una radice di*

$$P = \sum_{n=0}^{\deg(P)} a_n x^n \quad \in K[x]$$

se

$$\sum_{n=0}^{\deg(P)} a_n \alpha^n = 0$$

Passiamo ora a definire la divisione tra polinomi.

Definizione 63 (Divisione tra polinomi)**.** *Se $f(x) \in K[x] \setminus \{0\}$ e $g(x) \in K[x] \setminus \{0\}$ sono polinomi non nulli, allora esistono unici $q(x) \in K[x]$ e $r(x) \in K[x]$, detti rispettivamente quoziente e resto della divisione, tali che*

$$f(x) = g(x) \cdot q(x) + r(x)$$

e

- $r(x) = 0$, *oppure*
- $\deg(r(x))\langle\deg(g(x))$

Dal fatto che è possibile dividere polinomi, segue

Teorema 16. *L'anello $K[x]$ è ad ideali principali (Definizione 46). Se I è l'ideale generato da un polinomio $\langle p(x)\rangle$, ossia*

$$I = \langle p(x)\rangle$$

allora esiste un unico generatore monico di I.

4.5.3 Massimo comune divisore tra polinomi

Dato che è possibile dividere polinomi, possiamo anche definire il massimo comune divisore tra polinomi. In particolare, definiremo il massimo comune divisore monico (tra i tanti MCD di due polinomi). Per trovare l'MCD possiamo utilizzare l'algoritmo delle divisioni successive (di Euclide). Applichiamo subito quanto detto con un esempio. Consideriamo i polinomi

$$f(x) = x^4 - x^3 - 4x^2 + 4x + 1$$

e

$$g(x) = x^2 - x - 1$$

Utilizzando l'algoritmo di Euclide otteniamo

$$f(x) = g(x)(x^2 - 3) + x - 2$$
$$g(x) = (x - 2)(x + 1) + 1$$

Dato che il resto della divisione tra $g(x)$ e $(x-2)$ è 1, ci possiamo fermare e dire che il massimo comune divisore tra $f(x)$ e $g(x)$ è 1, ossia che i due polinomi sono coprimi tra loro. Possiamo ora applicare le sostituzioni successive per ottenere l'identità di Bézout.

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

e quindi abbiamo la nostra identità di Bézout.

Proposizione 17. *Sia K un campo e $p \in K[x]$ un polinomio irriducibile (61), allora l'anello quoziente*

$$K[x]\big/\langle p(x)\rangle$$

è un campo.

Ricordiamo che, per come è stato definito l'anello quoziente, $\langle p(x)\rangle$ è un ideale e che la relazione di equivalenza tra due elementi $a(x)$, $b(x)$ dell'anello quoziente è definita come

$$a(x) \sim b(x) \iff \exists q(x) \in \langle p(x)\rangle : b(x) = a(x) + q(x)$$

quindi il campo $K[x]\big/\langle p(x)\rangle$ è il campo di classi di polinomi $K[x]$ uguali a meno di multipli di $p(x)$. In altre parole, due polinomi stanno nella stessa classe se entrambi, divisi per $p(x)$, hanno stesso resto.

Proof. Sia $[f] \in K[x]\big/\langle p(x)\rangle$ tale che $[f] \neq [0]$ perché, per Definizione 42 di campo, vogliamo far vedere che tutti gli elementi diversi da 0 sono invertibili. Ricordiamo che la classe di 0 sono tutti i polinomi divisibili per $p(x)$, quindi prendere $[f] \neq [0]$ significa prendere i polinomi $f(x)$ che non hanno $p(x)$ come divisore. Ma se $p(x)$ non divide $f(x)$, allora il massimo comune divisore tra $f(x)$ e $p(x)$ è

$$\mathrm{MCD}\big(p(x), f(x)\big) = 1$$

perché p è irriducibile e non divide f. Quindi abbiamo un'identità di Bézout

$$a(x)f(x) + b(x)p(x) = 1$$

che in $K[x]\big/\langle p(x)\rangle$ diventa

$$[a(x)]\cdot[f(x)] + [b(x)]\cdot[p(x)] = 1$$

Ma dato che la classe di $p(x)$ è la classe di 0, perché $p(x)$ irriducibile e quindi è divisibile solo per $a \in K$ o $ap(x)$, allora l'identità diventa

$$[a(x)][f(x)] = 1$$

e l'inverso della classe di $f(x)$ è la classe di $a(x)$, ossia

$$[f(x)]^{-1} = [a(x)] \in K[x]\big/\langle p(x)\rangle$$

□

Esempi

Facciamo ora un esempio molto importante. Prendiamo l'anello dei polinomi a coefficienti reali, i.e., $\mathbb{R}[x]$, e un polinomio x^2+1. Il polinomio è irriducibile, infatti non possiamo trovare dei valori a, b, c e d tali per cui

$$(ax+b)(cx+d) = x^2+1$$

La Proposizione 17 è quindi vera e possiamo dire che

$$\mathbb{R}[x]/\langle x^2+1\rangle$$

è un campo, in particolare, è il campo dei polinomi a meno di polinomi multipli di x^2+1. Questo significa che in $\mathbb{R}[x]/\langle x^2+1\rangle$:

- $\overline{x^2+1} = \overline{0}$
- $\overline{x^2} = \overline{-1}$
- $\overline{x^3+x^2} = \overline{-x-1}$ perché
  - $\overline{x^2} = \overline{-1}$
  - $x^3 = x \cdot x^2$ e $\overline{x^2} = \overline{-1}$.

Ma quindi tutti gli elementi maggiori o uguali a due scompaiono e quindi il campo contiene solo gli elementi nella forma

$$a+bx$$

e $x^2 = -1$ e quindi il campo è isomorfo a $\mathbb{C}$.

$$\mathbb{R}[x]/\langle x^2+1\rangle \simeq \mathbb{C}$$

Consideriamo ora un altro esempio. Prendiamo il polinomio

$$p(x) = 1+x+x^2$$

in $\mathbb{F}_2[x]$, che è irriducibile perché non ha radici in $\mathbb{F}_2$. Chiamiamo ora $\mathbb{F}_{2^2} = \mathbb{F}_4$ il quoziente

$$\mathbb{F}_4 = \mathbb{F}_2[x]/\langle p(x)\rangle$$

che, come abbiamo dimostrato, è un campo. La classe di equivalenza di $p(x)$ è 0, quindi possiamo scrivere

$$1+x+x^2 = 0$$

che ci porta ad affermare che

$$x^2 = -1-x = 1+x$$

Quindi ogni polinomio può essere ridotto usando l'equivalenza appena scritta fino ad ottenere solo polinomi di grado due. Per questo motivo possiamo dire che $\mathbb{F}_4$ è

$$\mathbb{F}_4 = \{a_0 + a_1 x : a_0, a_1 \in \mathbb{F}_2\}$$

Dato che a_0 e a_1 possono essere solo 0 o 1 (perché prendono valori in $\mathbb{F}_2$), allora la cardinalità di $\mathbb{F}_4$ è 2^2, ossia 4.

$$|\mathbb{F}_4| = \left|\mathbb{F}_2/\langle 1+x+x^2\rangle\right| = 4$$

Ecco quindi perché chiamiamo $\mathbb{F}_4$ l'anello quoziente.

4.5.4 Teorema di Ruffini

Teorema 17 (Ruffini)**.** *Sia $f(x) \in K[x] \setminus \{0\}$. Se $\alpha \in K$, il resto della divisione di $f(x)$ per $x - \alpha$ è $f(\alpha)$, ossia*

$$f(x) = (x - \alpha) \cdot q(x) + f(\alpha)$$

In particolare, se α è una radice del polinomio, ossia $f(\alpha) = 0$, allora $x - \alpha$ divide $f(x)$.

Proof. Iniziamo scrivendo $f(x)$ come

$$f(x) = (x - a)q(x) + r(x)$$

con $r(x) = 0$ oppure $\deg(r(x)) < \deg((x - \alpha))$. Ma dato che il grado di $x - \alpha$ è 1, allora $r(x) = 0$ oppure $\deg(r(x)) < 1$. Questo significa che, in ogni caso, $r(x)$ è una costante, ossia $c = r(x) \in K$. Possiamo quindi scrivere

$$f(x) = (x - a)q(x) + c$$

Calcolando f in α otteniamo

$$f(\alpha) = (\alpha - \alpha)q(x) + c = c$$

e quindi $r(x) = c = f(\alpha)$. □

Proposizione 18. *Se K è un campo, ogni sottogruppo finito del gruppo moltiplicativo $K \setminus \{0\}$ è ciclico. In particolare, se K è un campo finito, allora $K \setminus \{0\}$ è ciclico.*

Esempio

Consideriamo nuovamente l'esempio di prima, ossia

$$\mathbb{F}_4 = {}^{\mathbb{F}_2[x]}\!\!\diagup_{\langle 1 + x + x^2 \rangle}$$

e troviamo i suoi generatori. Innanzitutto, dato che $\mathbb{F}_4$ contiene le classi di resto della divisione per $1 + x + x^2$, allora $\mathbb{F}_4$ contiene tutti i polinomi di grado 1 o 0 (per Definizione 63), ossia

$$\mathbb{F}_4 = \{1, x, 1 + x\}$$

Troviamo ora i generatori di $\mathbb{F}_4$. Ad esempio, x è un generatore del gruppo moltiplicativo $\mathbb{F}_4 \setminus \{0\}$, perché i valori generati da x sono

$$\langle x \rangle = \{x, x^2, x^3\}$$

che è genera tutto l'insieme $\mathbb{F}_4 = {}^{\mathbb{F}_2[x]}\!\!\diagup_{\langle 1 + x + x^2 \rangle}$, tranne lo 0, infatti

- $1 + x + x^2 = 0$
- $x = 1 + x^2 = 1 + 1 + x = 2 + x = x$.
- $x^2 = 1 + x$.
- $x^3 = x(x^2) = x(1 + x) = x + x^2 = x + 1 + x = 1$.

e quindi

$$\{x, x^2, x^3\} = \{x, 1 + x, 1\} = \{0 + x, 1 + x, 1 + 0x\} = \mathbb{F}_4 \setminus \{0\}$$

L'altro generatore è $x + 1$.

Definizione 64. *Sia $p \in \mathbb{N}$ un numero primo e $n \in \mathbb{N} \setminus \{0\}$. Sia $Q(x) \in \mathbb{F}_p[x]$ un polinomio irriducibile di grado n. Definiamo il campo*

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

Il campo $\mathbb{F}_{p^n}$ è quindi il campo di classi di polinomi a coefficienti in $\mathbb{F}_p$ in cui due polinomi sono equivalenti se sono uguali a meno di un multiplo di $Q(x)$, polinomio di grado n.

4.5.5 Isomorfismi di campi

Vogliamo ora dimostrare la seguente proposizione.

Proposizione 19 (Isomorfismo di campi)**.** *Sia $p \in \mathbb{N}$ numero primo e siano $Q(x)$ e $Q'(x)$, due polinomi in $\mathbb{F}_p[x]$. Se $Q(x)$ e $Q'(x)$ sono irriducibili e di grado n, allora*

$${}^{\mathbb{F}_p[x]}\!/_{\langle Q(x) \rangle} \simeq {}^{\mathbb{F}_p[x]}\!/_{\langle Q'(x) \rangle}$$

ossia che esiste un isomorfismo di campi tra ${}^{\mathbb{F}_p[x]}\!/_{\langle Q(x) \rangle}$ e ${}^{\mathbb{F}_p[x]}\!/_{\langle Q'(x) \rangle}$.

Proof. Iniziamo con dire che $\mathbb{F}_p$ è isomorfo ad $\mathbb{F}_p[x]$ modulo un qualsiasi polinomio di grado 1, ossia

$$\mathbb{F}_p \simeq {}^{\mathbb{F}_p[x]}\!/_{a + bx}$$

□

Definizione 65 (Elemento algebrico)**.** *Siano $F \subseteq K$ due campi (in cui K è un ampliamento di F). Un elemento α in K si dice **algebrico** su F se è radice (62) di un polinomio non nullo $f(x) \in F[x]$. Altrimenti, α si dice elemento **trascendente**.*

Si noti che gli elementi in F sono tutti algebrici su F stesso, quindi di solito consideriamo elementi $\alpha \in K \setminus F$. Ad esempio, se consideriamo $\mathbb{Q} \subseteq \mathbb{R}$ e $\alpha = \sqrt{2}$, α è algebrico perché è radice di $x^2 - 2 \in \mathbb{Q}[x]$. L'elemento $\alpha = \pi$ è invece trascendente perché $x - \pi \notin \mathbb{Q}[x]$.

Definizione 66 (Valutazione)**.** *Sia $F \subseteq K$ un ampliamento di campi, $\alpha \in K$ e $f(x) \in F[x]$. Il morfismo di anelli*

$$v_\alpha : F[x] \to K$$

definito come

$$f(x) \mapsto f(\alpha)$$

prende il nome di valutazione dei polinomi in α.

Il nucleo di v_α è l'ideale di $F[x]$ costituito da tutti i polinomi in $F[x]$ annullati da α. Quindi,

- Se α è **algebrico** su F allora ci sono dei polinomi che si annullano in α e quindi il nucleo non è banale, i.e. $\ker(v_a) \neq \{0\}$. Inoltre, conoscendo l'algoritmo di divisione dei polinomi, sappiamo

che l'anello di un polinomio è ad ideali principali e quindi $\ker(v_a)$ sarà un ideale generato da un solo polinomio. Questo significa che

$$\ker(v_\alpha) = \langle m(x) \rangle$$

dove $m(x)$ è l'unico polinomio monico di grado minimo di $\ker(v_a)$.

- Se α è **trascendente** allora il nucleo è banale.

Definizione 67 (Elemento algebrico di grado n)**.** *Sia $F \subseteq K$, $\alpha \in K$ algebrico su F. Il polinomio $m(x)$, definito come l'unico polinomio monico di grado minimo di $\ker(v_a)$, si chiama polinomio minimo di α su F. Se $\deg\big(m(x)\big) = n$, α si dice algebrico di grado n su F.*

Ad esempio, se consideriamo $\mathbb{Q} \subseteq \mathbb{C}$ allora $\alpha = \imath \in \mathbb{C} \setminus \mathbb{Q}$ è algebrico su $\mathbb{Q}$ e il polinomio minimo di $\imath$ è $x^2 + 1$ perché

- É monico.
- Annulla $\imath$.
- É irriducibile su $\mathbb{Q}$.

Proposizione 20 (Immagine della valutazione)**.** *Sia $F \subseteq K$ un ampliamento di campi e $\alpha \in K$. Si consideri il morfismo di anelli*

$$v_\alpha : F[x] \to K$$

ossia la valutazione dei polinomi in α. Allora l'immagine di v_α è il più piccolo sottoanello di K contenente sia F che α.

Proof. Iniziamo osservando che l'immagine di un morfismo di anelli è un anello. Quindi l'immagine di v_α è un sottoanello di K. Ora vogliamo mostrare che F sta nell'immagine e α sta nell'immagine. Partiamo prendendo un elemento $c \in F$ e il polinomio costante c. Se valutiamo il polinomio in α otteniamo la costante stessa.

$$v_\alpha(c) = c$$

Questo significa che c sta nell'immagine di v_α e, essendo $c \in F$, un elemento di F sta nell'immagine di v_α.

$$F \subseteq \Im(v_a)$$

Inoltre, se valutiamo il polinomio di grado 1 x in α, otteniamo α e quindi anche α sta nell'immagine di v_α.

$$\alpha \in \Im(v_\alpha)$$

Per chiusura additiva e moltiplicativa, ogni sottoanello di K contenente sia F che α contiene $\Im(v_a)$. In pratica, dato che v_α valuta il polinomio in α, allora l'immagine di v_α contiene somme di potenze di α. Inoltre, ogni sottoanello che contiene F e α contiene anche tutte le somme e i prodotti di potenze di α, e quindi anche l'immagine di v_α. □

Definizione 68 (Ampliamento semplice)**.** *Sia $F \subseteq K$ un ampliamento di campi e $\alpha \in K$. Il più piccolo sottocampo di K contenente si F che α si chiama ampliamento di F in K generato da α e lo indichiamo come segue.*

$$F(\alpha)$$

Un tale ampliamento lo chiamiamo semplice (perché generato da un solo elemento α).

In altre parole $F(\alpha)$ è il più piccolo sottocampo di K che contiene sia F che α. Ad esempio, l'ampliamento semplice $\mathbb{Q} \subseteq \mathbb{C}$, è l'insieme

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$$

dei numeri complessi a coefficienti razionali.

Teorema 18. *Sia $F \subseteq K$ un ampliamento di campi e sia $\alpha \in K$. Allora l'ampliamento semplice $F(\alpha)$ è*

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

Proof. Per la definizione di ampliamento semplice, l'immagine di v_α è

$$\Im(v_\alpha) = \{f(\alpha) : f(x) \in F[x]\}$$

Prendiamo gli inversi in K e otteniamo

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

□

Se α è algebrico su F, si ha che l'immagine di v_α, per il Teorema 9 di isomorfismo di anelli, è isomorfa a $F[x]/\langle m(x)\rangle$

$$\Im(v_\alpha) \simeq F[x]/\langle m(x)\rangle$$

dove $m(x)$ è il polinomio minimo di α. Questo quoziente è un campo se $m(x)$ è irriducibile. Quindi $\Im(v_\alpha)$ è un campo e

$$F(\alpha) = \Im(v_\alpha)$$

Se $\deg(m(x)) = n$, ossia n è il grado di α, si ha che

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

Passiamo ora ad un esempio. Prendiamo l'ampliamento $\mathbb{Q} \in \mathbb{R}$ e $\alpha = \sqrt{3}$. α è algebrico su $\mathbb{Q}$ con polinomio minimo $x^2 - 3$. Quindi $\sqrt{3}$ ha grado 2 su $\mathbb{Q}$. L'ampliamento semplice di $\sqrt{3}$ è quindi

$$\mathbb{Q}(\sqrt{3}) = \{c_0 + c_1\sqrt{3} : c_0, c_1 \in \mathbb{Q}\} \simeq \mathbb{Q}[x]/\langle x^2 - 3\rangle$$

Si noti che, se lavoriamo in $\mathbb{Q}[x]/\langle x^2 - 3\rangle$ possiamo fare il prodotto tra due elementi

$$(c_0 + c_1x)(c_0' + c_1'x) = (c_0c_0' + c_0c_1'x + c_0'c_1x + c_1c_1'x^2)$$

Ma in questo quoziente $x^2 - 3 = 0$, quindi $x^2 = 3$ e il prodotto diventa

$$(c_0 + c_1x)(c_0' + c_1'x) = (c_0c_0' + c_0c_1'x + c_0'c_1x + 3c_1c_1')$$

Proposizione 21. *Sia $\alpha \in \mathbb{F}_{p^n}$ un generatore per il gruppo moltiplicativo $\mathbb{F}_{p^n} \setminus \{0\}$. Allora $\mathbb{F}_{p^n}$ è un ampliamento semplice di $\mathbb{F}_p$ generato da α, ossia*

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

Si noti che $\mathbb{F}_{p^n}$ è un ampliamento di $\mathbb{F}_p$, ossia $\mathbb{F}_p$ è incluso in $\mathbb{F}_{p^n}$ perché i polinomi di grado 0 sono contenuti nell'insieme di tutti i polinomi.

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$$

Proof. $\mathbb{F}_p(\alpha)$, per definizione, deve essere il più piccolo sottocampo che contiene sia F_p che α, quindi

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

Poiché α genera $\mathbb{F}_{p^n} \setminus \{0\}$ (facendo tutte le potenze possibili di α, otteniamo tutti gli elementi di $\mathbb{F}_{p^n}$), si ha che

$$\mathbb{F}_{p^n} \subseteq F_p(\alpha)$$

Ma quindi

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

□

4.5.6 Isomorfismi tra quozienti di polinomi

Ora vogliamo costruire un isomorfismo tra i quozienti $\mathbb{F}_{p^n}$, ossia un isomorfismo tra il quoziente di $\mathbb{F}_p$ e un polinomio irriducibile in $\mathbb{F}_p$ di grado n.

Proposizione 22 (Isomorfismi tra quozienti di polinomi)**.** *Siano $F \subseteq K$ e $F \subseteq K'$ due ampliamenti di campi. Se $\alpha \in K$ algebrico di grado n su F con polinomio minimo $m(x)$, allora esiste un morfismo φ di campi dall'ampliamento semplice generato da α, $F(\alpha)$, a K' che fissa F (ossia che facendo $\varphi(f)$ con $f \in F$, ottengo f stesso)*

$$\varphi : F(\alpha) \to K'$$

se e solo se $m(x)$ ha una radice in K'. In questo caso, i morfismi sono tanti quanti le radici distinte $\beta_1, \ldots, \beta_s$ di $m(x)$ e sono tutti e soli quelli definiti da

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mapsto c_0 + c_1\beta_i + \cdots + c_{n-1}\beta_i^{n-1}$$

Proof. Iniziamo a dimostrare l'implicazione diretta. Assumiamo che

$$\varphi : F(\alpha) \to K'$$

sia un morfismo e vediamo che

$$0 = \varphi(0)$$

Dato che $m(x)$ è il polinomio minimo di α, allora φ valutata in $m(\alpha)$ è 0, quindi

$$0 = \varphi(0) = \varphi(m(\alpha))$$

Ma dato che φ è un morfismo allora possiamo anche dire che

$$0 = \varphi(0) = \varphi(m(\alpha)) = m(\varphi(\alpha))$$

Ma quindi, dato che $m(\varphi(\alpha)) = 0$, allora $\varphi(\alpha)$ è una radice di $m(x)$ in K' (perché $\varphi(\alpha) \in K'$). Mostriamo ora l'implicazione inversa. Prendiamo una radice β di m in K', ossia un $\beta \in K'$ tale che

$$m(\beta) = 0$$

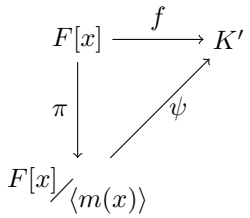
Consideriamo la valutazione in β, v_β, (che è un morfismo)

$$v_\beta : F[x] \to K'$$

definita come segue

$$f(x) \mapsto f(\beta)$$

poiché $m(x)$ sta nel nucleo di v_β, dal teorema di isomorfismo, possiamo scrivere



Ma abbiamo detto che $F[x]/\langle m(x)\rangle \simeq F(\alpha)$, e quindi possiamo dire che esiste un isomorfismo da $F(\alpha)$ a K'. □

4.5.7 Campo di spezzamento di un polinomio

Definiamo ora un campo di spezzamento di un polinomio

Definizione 69 (Campo di spezzamento di un polinomio)**.** *Sia F un campo e $f(x) \in F[X]$ un polinomio di grado $n \geq 1$ a coefficienti in F. Un campo K tale che $F \subseteq K$ si dice campo di spezzamento di f su F se:*

1. *$f(x)$ si fattorizza in polinomi di grado 1 su $K[x]$ e*
2. *non ci sono campi intermedi $F \subseteq L \subsetneq K$ con questa proprietà (i.e., K è il più piccolo che rispetta questa proprietà).*

In altre parole, dobbiamo guardare se tutte le radici di F stanno anche in K, considerando solo i polinomi di grado 1.

Esempio

Consideriamo $\mathbb{Q}(\sqrt{2})$, ossia l'ampliamento semplice generato da $\sqrt{2}$. $\mathbb{Q}(\sqrt{2})$ è un campo di spezzamento di $x^2 - 2 \in \mathbb{Q}[x]$. Si noti che $x^2 - 2$ è irriducibile in $\mathbb{Q}[x]$ ma può essere fattorizzato in $\mathbb{Q}(\sqrt{2})$. Infatti possiamo fattorizzare $x^2 - 2$ come

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}) \in \mathbb{Q}(\sqrt{2})[x]$$

Proprietà

Proposizione 23. *Un campo di cardinalità p^n è un campo di spezzamento di $x^{p^n} - x \in \mathbb{F}_p[x]$*

Proof. La cardinalità di $K \setminus \{0\}$ è $p^n - 1$ e

$$\alpha \in K \setminus \{0\} \Rightarrow \alpha^{p^n - 1} = 1$$

perché K è ciclico. Quindi α è radice di $x^{p^n} - x$ e per il Teorema 17 di Ruffini, K è un campo di spezzamento di $x^{p^n} - x$. □

Proposizione 24. *Tutti e soli i polinomi irriducibili su $\mathbb{F}_p$ di grado n sono i fattori irriducibili di grado n di $x^{p^n} - x \in \mathbb{F}_p[x]$.*

Questo ci serve perché se vogliamo trovare un polinomio di grado n irriducibile, possiamo cercarlo nella fattorizzazione di $x^{p^n} - x$.

Proof. Sia $p(x) \in \mathbb{F}_p[x]$ un polinomio irriducibile di grado n e sia

$$K \coloneqq {}^{\mathbb{F}_p[y]}\!/_{p(y)}$$

Allora K è un campo con p^n elementi che sono anche radici del polinomio $x^{p^n} - x \in K[x]$. $y \in K$ è una radice sia di $p(x)$ che di $x^{p^n} - x$, quindi per il Teorema 17 di Ruffini, hanno un fattore comune che è $x - y$ in cui y è un elemento del campo e x è l'indeterminata dell'anello di polinomi. Poiché $\mathbb{F}_p \subseteq K$ e il massimo comune divisore in $\mathbb{F}_p[x]$ è lo stesso che in $K[x]$, allora $p(x)$ e $x^{p^n} - x$ hanno MCD $\neq 1$ in $\mathbb{F}_p[x]$ (avendo un fattore in comune). Poiché $p(x)$ irriducibile, allora $p(x)$ divide $x^{p^n} - x$. □

Isomorfismo

Vogliamo ora costruire un isomorfismo

$$f : {}^{\mathbb{F}_p[x]}\!/_{\langle p(x) \rangle} \to {}^{F_p[x]}\!/_{\langle q(x) \rangle}$$

Più precisamente, ci basta costruire un morfismo di anelli, dato che

- Un morfismo di campi è sempre iniettivo.
- I campi ${}^{\mathbb{F}_p[x]}\!/_{\langle p(x) \rangle}$ e ${}^{F_p[x]}\!/_{\langle q(x) \rangle}$ hanno stessa cardinalità p^n e quindi il morfismo è anche suriettivo.

Sia $\alpha \in {}^{\mathbb{F}_p[x]}\!/_{\langle p(x) \rangle}$ un generatore del gruppo moltiplicativo ${}^{\mathbb{F}_p[x]}\!/_{\langle p(x) \rangle} \setminus \{0\}$. Sia $h(x) \in \mathbb{F}_p[x]$ il polinomio minimo di α. Poiché

$${}^{\mathbb{F}_p[x]}\!/_{\langle p(x) \rangle} \simeq \mathbb{F}_p(\alpha)$$

è l'ampliamento semplice generato da α, il quale, essendo $h(x)$ il polinomio minimo di α, è isomorfo anche a ${}^{\mathbb{F}_p[x]}\!/_{\langle h(x) \rangle}$.

$${}^{\mathbb{F}_p[x]}\!/_{\langle p(x) \rangle} \simeq \mathbb{F}_(\alpha) \simeq {}^{\mathbb{F}_p[x]}\!/_{\langle h(x) \rangle}$$

Ma allora il grado di $h(x)$ è n. Poiché il campo ${}^{\mathbb{F}_p[y]}\!/_{\langle q(y)\rangle}$ è un campo di spezzamento di $x^{p^n} - x$ e $h(x)$ divide $x^{p^n} - x$, allora $h(x)$ si fattorizza in fattori di grado 1 in ${}^{\mathbb{F}_p[y]}\!/_{\langle q(y)\rangle}$. Ossia $h(x)$ ha una radice in ${}^{\mathbb{F}_p[y]}\!/_{\langle q(y)\rangle}$. In pratica dobbiamo

1. Prendere il generatore del gruppo ciclico ${}^{\mathbb{F}_p[x]}\!/_{\langle p(x)\rangle} \setminus \{0\}$.
2. Prendere il suo polinomio minimo $h(x)$.
3. Considerare $h(x)$ come polinomio nel campo ${}^{\mathbb{F}_p[y]}\!/_{\langle q(y)\rangle}$ in cui $h(x)$ ha una radice.
4. Mandare α nella radice trovata al punto precedente.

In altre parole, sia $\beta \in {}^{\mathbb{F}_p[y]}\!/_{\langle q(y)\rangle}$ tale che $h(\beta) = 0$. Allora l'assegnazione

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mapsto c_0 + c_1\beta + \dots c_{n-1}\beta^{n-1}$$

definisce un morfismo di anelli, che è iniettivo e suriettivo, quindi biettivo.

Esempio

Consideriamo i seguenti polinomi in $\mathbb{F}_3[x]$:

$$p(x) = 1 + x^2$$

e

$$q(x) = 2 + 2x + x^2$$

I polinomi $p(x)$ e $q(x)$ sono irriducibili in $\mathbb{F}_3$ (basta controllare, per ogni possibile valore di x, che nessuna x è una radice).

Consideriamo ora il polinomio

$$1 + x \in {}^{\mathbb{F}_3[x]}\!/_{\langle 1 + x^2\rangle} = K_1$$

Questo polinomio è un generatore del gruppo moltiplicativo $K_1 \setminus \{0\}$. Per definire un isomorfismo, dobbiamo

1. Prendere un generatore del gruppo ciclico K_1, ad esempio $1 + x$.
2. Prendere il suo polinomio minimo nell'anello $\mathbb{F}_3[y]$.
3. Fattorizzare il polinomio minimo nell'anello ${}^{\mathbb{F}_3[x]}\!/_{\langle 2 + 2x + x^2\rangle} = K_2$.

Il primo punto è fatto, ora dobbiamo trovare il polinomio minimo di $1 + x$ in $\mathbb{F}_3[y]$. Il polinomio minimo è

$$2 + y + y^2$$

perché

- É irriducibile, infatti sostituendo a y tutti i possibili valori, il polinomio non si annulla mai.
- É monico.

- Si annulla in $1+x$, infatti

$$\begin{aligned} 2+(1+x)+(1+x)^2 &= 2+1+x+1+x^2+2x \\ &= 1+x^2 \\ &= 0 \end{aligned}$$

Trovato il polinomio minimo, dobbiamo fattorizzarlo in $\mathbb{F}_3[x]/\langle 2+2x+x^2\rangle$. Una sua fattorizzazione è

$$2+y+y^2 = (y+x)(y+2x-1)$$

in $K_2[y]$ e quindi le radici di $2+y+y^2$ in K_2 sono $-x = 2x$ e $-2x-1 = x+2$. Possiamo quindi definire i seguenti morfismi:

- $f_1 : K_1 \to K_2$ definito come $1+x \mapsto 2x$.
- $f_2 : K_1 \to K_2$ definito come $1+x \mapsto 2+x$.

Per applicare i morfismi, ci basta scrivere l'argomento della funzione nella base della funzione. Se consideriamo f_1, vogliamo scrivere l'argomento come combinazione lineare delle basi 1 e $1+x$. Otteniamo quindi i seguenti risultati:

- $f_1(0) = f_1(0+0\cdot(1+x)) = 0$
- $f_1(1) = f_1(1+0\cdot(1+x)) = 1$
- $f_1(2) = f_1(2+0\cdot(1+x)) = 2$
- $f_1(x) = f_1(2+1\cdot(1+x)) = 2+2x$
- $f_1(1+x) = f_1(0+\cdot(1+x)) = 2x$
- $f_1(2+x) = f_1(1+1\cdot(1+x)) = 1+2x$
- $f_1(2x) = f_1(1+2\cdot(1+x)) = 1+4x = 1+x$

Proposizione 25. *Se K è un anello commutativo di caratteristica prima p, allora*

$$(x+y)^{p^h} = x^{p^h} + y^{p^h} \quad \forall x, y \in K, h \geq 1$$

Proof. Se $h = 1$ e $0 \leq k \leq p$, p divide tutti i coefficienti binomiali

$$\binom{p}{k} := \frac{p!}{k!(p-k)!}$$

perché p non divide $k!(p-k)!$. Allora, in un anello commutativo,

$$(x+y)^p = \sum_{K=0}^{p} \binom{p}{k} x^k y^{p-k}$$

Ma i coefficienti binomiali sono tutti 0, tranne gli estremi, e quindi otteniamo

$$x^p + y^p$$

Se $h > 1$, andiamo per induzione. □

Da questo fatto segue

Definizione 70 (Automorfismo di Fröbenius)**.** *Se K è un campo di caratteristica p, la funzione*

$$\Phi : K \to K$$

definita come

$$x \mapsto x^p$$

è un morfismo di campi iniettivo (ma non necessariamente suriettivo), infatti

$$\Phi(x+y) = (x+y)^p = x^p + y^p = \Phi(x) + \Phi(y)$$

e

$$\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$$

Se $K = \mathbb{F}_p$, allora Φ è un isomorfismo da K in K e quindi è un automorfismo che prende il nome di automorfismo di Fröbenius.

L'automorfismo di Fröbenius è importante perché ci permette di enunciare il seguente teorema.

Teorema 19 (Gruppo degli automorfismi di $\mathbb{F}_{p^n}$)**.** *Il gruppo* $\mathrm{Aut}(\mathbb{F}_{p^n})$ *degli automorfismi di $\mathbb{F}_{p^n}$ è un gruppo ciclico generato dall'automorfismo di Fröbenius.*

Part II

Tensori

Chapter 5

Introduzione

Iniziamo a definire alcuni concetti base dell'algebra lineare. Per prima cosa, diciamo cosa si intende per spazio vettoriale.

Definizione 71 (Spazio vettoriale)**.** *Sia K un campo, V un insieme, $+ : V \times V \to V$ associativa e commutativa con elemento 0 e per cui ogni $v \in V$ ha elemento neutro e $\cdot : K \times V \to V$ con elemento neutro 1. Valgano poi le proprietà:*

- $a \cdot (v + u) = av + au \quad \forall a \in K, \forall u, v \in V$
- $(a + b) \cdot v = av \cdot bv \quad \forall a, b \in K, \forall v \in V$
- $(a \cdot b) \cdot v = a \cdot (b \cdot v) \quad \forall a, b \in K, \forall v \in V$

Allora V è uno spazio vettoriale.

Definizione 72 (Matrice 2×2)**.** *Sia*

$$\mathrm{Mat}_{2\times 2}(K) = \left\{ \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} : x_1, x_2, x_3, x_4 \in K \right\}$$

l'insieme delle matrici quadrate 2×2 a coefficienti in K. Diamo all'insieme $\mathrm{Mat}_{2\times 2}(K)$ una struttura di anello, tramite le seguenti operazioni:

- *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 righe per colonne.*
$$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \cdot \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} = \begin{pmatrix} x_1y_1 + x_2y_3 & x_1y_2 + x_2y_4 \\ x_3y_1 + x_4y_3 & x_3y_2 + x_4y_4 \end{pmatrix}$$

Con queste operazioni, $\mathrm{Mat}_{2\times 2}(K)$ è un anello con unità

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

Notiamo una cosa interessante. Computazionalmente, la moltiplicazione righe per colonne tra matrici 2×2 richiede di calcolare 8 prodotti (la complessità delle addizioni è irrilevante per il calcolo della complessità totale).

Analogamente, possiamo associare una struttura di anello alle matrici quadrate $n \times n$ sul campo K.

Proposizione 26 (Anelli di matrici)**.** *L'insieme* $\mathrm{Mat}_{n\times n}(K)$ *ha una struttura di anello (non commutativo, a meno che* $n = 1$*).*

Si noti che la moltiplicazione righe per colonne tra matrici in $\mathrm{Mat}_{2\times 2}(K)$ richiede l'esecuzione di n^3 moltiplicazioni. Inoltre, la moltiplicazione righe per colonne può essere applicata anche tra matrici $n \times m$ compatibili, ma in questo caso la struttura non è di anello perché l'operazione non è chiusa. Più precisamente, possiamo far diventare rettangolari le matrici quadrate aggiungendo degli zeri.

5.1 Algoritmo di Strassen

L'algoritmo di Strassen permette di calcolare il prodotto righe per colonne tra matrici $n \times n$ utilizzando però meno operazioni rispetto all'algoritmo che deriva direttamente dalla definizione di prodotto righe per colonne. Ad esempio, la moltiplicazione righe per colonne di matrici in $\mathrm{Mat}_{2\times 2}(K)$ richiede 7 moltiplicazioni anziché 8.

5.1.1 Matrici 2 per 2

Iniziamo analizzando l'algoritmo per matrici 2×2 per poi generalizzare a matrici $n\times n$. Consideriamo due matrici

$$A = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$$

e

$$B = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}$$

Il prodotto $A \cdot B$ avrà componenti:

$$A \cdot B = \begin{pmatrix} x_1y_1 + x_2y_3 & x_1y_2 + x_2y_4 \\ x_3y_1 + x_4y_3 & x_3y_2 + x_4y_4 \end{pmatrix} = \begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix}$$

Definiamo ora 7 numeri, che indichiamo I, II, III, IV, V, VI, VII, come

- $I \coloneqq (x_1 + x_4)(y_1 + y_4)$
- $II \coloneqq (x_3 + x_4)y_1$
- $III \coloneqq x_1(y_2 + y_4)$
- $IV \coloneqq x_4(-y_1 + y_3)$
- $V \coloneqq (x_1 + x_3)y_4$
- $VI \coloneqq (-x_1 + x_3)(y_1 + y_2)$

- $VII \coloneqq (x_2 - x_4)(y_3 + y_4)$

In ognuno di questi numeri troviamo una sola moltiplicazione. Inoltre, possiamo scrivere le componenti delle componenti di $A \cdot B$ come somme di questi numeri. In particolare

- $z_1 = I + IV - V + VII$
- $z_2 = III + V$
- $z_3 = II + IV$
- $z_4 = I - II + III + VI$

5.1.2 Matrici quadrate generiche

L'algoritmo di Strassen può essere applicato ricorsivamente per moltiplicare generiche matrici $n \times n$. Iniziamo considerando due matrici $M, N \in \mathrm{Mat}_{4\times 4}(K)$. Le matrici M, N possono essere scritte come matrici di matrici 2×2, ossia

$$M = \begin{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{13} & x_{14} \end{pmatrix} & \begin{pmatrix} x_{21} & x_{22} \\ x_{23} & x_{24} \end{pmatrix} \\ \begin{pmatrix} x_{31} & x_{32} \\ x_{33} & x_{34} \end{pmatrix} & \begin{pmatrix} x_{41} & x_{42} \\ x_{43} & x_{44} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

e

$$N = \begin{pmatrix} \begin{pmatrix} x'_{11} & x'_{12} \\ x'_{13} & x'_{14} \end{pmatrix} & \begin{pmatrix} x'_{21} & x'_{22} \\ x'_{23} & x'_{24} \end{pmatrix} \\ \begin{pmatrix} x'_{31} & x'_{32} \\ x'_{33} & x'_{34} \end{pmatrix} & \begin{pmatrix} x'_{41} & x'_{42} \\ x'_{43} & x'_{44} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$$

Il prodotto righe per colonne può essere fatto anche considerando solo i blocchi, quindi,

$$M \cdot N = \begin{pmatrix} AA' + BC' & AB' + BD' \\ CA' + DC' & CB' + DD' \end{pmatrix}$$

Ma quindi possiamo applicare l'algoritmo di Strassen sulle sotto-matrici di M e N (i.e., A, A', B, B', ...), e poi applicare nuovamente l'algoritmo per calcolare i prodotti tra le sotto-matrici. Più precisamente:

1. Al primo passo calcoliamo i numeri $I, \ldots, VII$ per il prodotto $M \cdot N$ usando le sotto-matrici. Abbiamo quindi:
   - $I \coloneqq (A + D)(A' + D')$
   - $II \coloneqq (C + D)A'$
   - $III \coloneqq A(B' + D')$
   - $IV \coloneqq D(-A' + C')$
   - $V \coloneqq (A + C)D'$
   - $VI \coloneqq (-A + C)(A' + B')$
   - $VII \coloneqq (B - D)(C' + D')$

2. Utilizziamo l'algoritmo di Strassen sulle sotto-matrici 2×2 per eseguire i calcoli al punto precedente. Quindi ad esempio, $I = (A + D)(A' + D')$ viene calcolato utilizzando l'algoritmo di Strassen sulle matrici $(A + D)$ e $(A' + D')$.

3. Calcolati i numeri $I, \ldots, VII$ possiamo scrivere

$$M \cdot N = \begin{pmatrix} I + IV - V + VII & III + V \\ II + IV & I - II + III + VI \end{pmatrix}$$

Ma quindi, ad ognuno dei due passi abbiamo 7 moltiplicazioni (per calcolare i numeri $I, \ldots, VII$) e quindi in totale è necessario fare $7^2 = 49$ moltiplicazioni, che sono già molte meno rispetto a quelle dell'algoritmo diretto (righe per colonne), che sono $4^3 = 64$. Consideriamo quindi il caso generico di matrici $n \times n$.

- Se n dispari, aggiungiamo una colonna e una riga di 0 così da far diventare il numero di righe e colonne pari. A questo punto possiamo ricondurci al caso n pari.
- Se n pari, applico ricorsivamente l'algoritmo di Strassen.

L' Algoritmo 1 mostra un implementazione dell'algoritmo di Strassen in pseudocodice.

Algoritmo 1 Algoritmo di Strassen.

procedure STRASSEN(A, B)
  if DIM(A) $= 1 \wedge$ DIM(B) $= 1$ **then**
    return $A \cdot B$ ▷ A e B sono valori in K, ritorniamo direttamente il loro prodotto
  end if
  if DIM(A) mod $2 \neq 0$ **then**
    $A \leftarrow$ PAD(A) ▷ Aggiungi una riga e una colonna di 0
  end if
  if DIM(B) mod $2 \neq 0$ **then**
    $B \leftarrow$ PAD(B) ▷ Aggiungi una riga e una colonna di 0
  end if
  $I \leftarrow$ STRASSEN$((x_1 + x_4), (y_1 + y_4))$
  $II \leftarrow$ STRASSEN$((x_3 + x_4), y_1)$
  $III \leftarrow$ STRASSEN$(x_1, (y_2 + y_4))$
  $IV \leftarrow$ STRASSEN$(x_4, (-y_1 + y_3))$
  $V \leftarrow$ STRASSEN$((x_1 + x_3), y_4)$
  $VI \leftarrow$ STRASSEN$((-x_1 + x_3), (y_1 + y_2))$
  $VII \leftarrow$ STRASSEN$((x_2 - x_4), (y_3 + y_4))$
  return $\begin{pmatrix} I + IV - V + VII & III + V \\ II + IV & I - II + III + VI \end{pmatrix}$
end procedure

Se $n = 2^k$, dobbiamo eseguire k volte l'algoritmo di Strassen (ogni volta la dimensione delle matrici viene dimezzata) e quindi l'algoritmo di Strassen per moltiplicare matrici $2^k \times 2^k$ esegue 7^k moltiplicazioni. Il numero di moltiplicazioni può essere scritto anche come

$$7^k = 2^{\log_2 7^k} = 2^{k \log_2 7} = n^{\log_2 7} \simeq n^{2.81}$$

Quindi asintoticamente, l'algoritmo di Strassen ha una complessità migliore di quella della moltiplicazione righe per colonne.

$$T_{Strassen}(n) = \mathcal{O}(n^{2.81}) < \mathcal{O}(n^3) = T_{righe,colonne}(n)$$

5.1.3 Esponente

Definizione 73 (Esponente della moltiplicazione di matrici)**.** *L'esponente ω della moltiplicazione di matrici è*

$$\omega := \inf\{h \in \mathbb{R} : \mathrm{Mat}_{n\times n}(K) \text{ può essere moltiplicata usando} \mathcal{O}(n^h) \text{ operazioni aritmetiche}\}$$

Per operazioni aritmetiche intendiamo addizione e moltiplicazione.

L'esponente è un numero in generale non noto, però sappiamo, dall'algoritmo di Strassen, che

$$\omega \leq \log_2 7 < 2.81$$

Inoltre, sappiamo anche che

Proposizione 27 (Ottimalità dell'algoritmo di Strassen)**.** *Per $n = 2$, l'algoritmo di Strassen è ottimale.*

Questa affermazione deriva dal fatto che è stato provato che ω deve essere maggiore di 2^{n-1} e dal teorema di Brockett-Dobnin per cui segue che il numero di moltiplicazioni per calcolare il prodotto di matrici deve essere maggiore di $2n^2 - 1$. Se per $n = 2$ sappiamo che l'algoritmo di Strassen è ottimale, per $n = 3$ non conosciamo l'algoritmo ottimale.

5.2 Algebra lineare

5.2.1 Isomorfismo tra endomorfismi di spazi vettoriali e matrici

Definizione 74 (Morfismo di spazi lineari)**.** *Siano V, W due spazi vettoriali su un campo K qualsiasi. Una funzione*

$$f : V \to W$$

è un morfismo di spazi vettoriali se

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

e prende il nome di applicazione lineare o funzione lineare.

Definizione 75 (Endomorfismo)**.** *Sia V uno spazio vettoriale su un campo K. Un morfismo*

$$f : V \to V$$

è detto endomorfismo di V. L'insieme degli endomorfismi di V lo indichiamo con

$$\mathrm{End}(V)$$

Ora che conosciamo l'insieme degli endomorfismi, vogliamo definire una somma ed un prodotto su $\mathrm{End}(V)$ così da dare una struttura di anello a $\mathrm{End}(V)$.

Definizione 76 (Anello di endomorfismi)**.** *Con le operazioni di somma e composizione di funzioni,* $\mathrm{End}(V)$ *è un anello con unità l'endomorfismo identità Id_V. Se la dimensione di V è maggiore di 1, l'anello non è commutativo.*

Sia V uno spazio vettoriale su K e $\dim(V) = n \in \mathbb{N}$, possiamo associare ad f, endomorfismo di V, una matrice $M(f) \in \mathrm{Mat}_{n\times n}(K)$ nel seguente modo. Sia

$$\{e_1, \dots, e_n\}$$

la base canonica di V. Si noti che, se $V = K^n$, allora la base canonica è

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \cdots \quad , \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\}$$

Sia poi $f(e_i)$ un elemento di V, allora $f(e_i)$ può essere scritto come composizione lineare delle basi di V

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

Allora $M(f)$ è la matrice la cui colonna i-esima è

$$\begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ni} \end{pmatrix}$$

ossia

$$M(f) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

Teorema 20 (Isomorfismo tra endomorfismi e matrici)**.** *Sia V uno spazio vettoriale di dimensione n su un campo K. Allora la funzione*

$$M : \mathrm{End}(V) \to \mathrm{Mat}_{n\times n}(K)$$

definita come

$$f \mapsto M(f)$$

è un isomorfismo di anelli.

Quindi, fare la composizione di endomorfismi in $\mathrm{End}(V)$ o il prodotto righe per colonne di matrici in $\mathrm{Mat}_{n\times n}(K)$ è la stessa cosa.

Esempio

Consideriamo il campo $\mathbb{F}_4$ definito come

$$\mathbb{F}_4 = {}^{\mathbb{F}_2[x]}\!\diagup_{\langle 1+x+x^2\rangle}$$

Questo è un campo, ma anche uno spazio vettoriale sul campo $\mathbb{F}_2$ perché può essere scritto come

$$\mathbb{F}_4 = \{a_0 + a_1 x : a_0, a_1 \in \mathbb{F}_2\}$$

che è isomorfo, come insieme, allo spazio vettoriale $(\mathbb{F}_2)^2$. Una base di $\mathbb{F}_4$ è $\{1, x\}$. Vediamo ora chi è la matrice dell'automorfismo di Fröbenius rispetto alla base $\{1, x\}$. L'automorfismo di Fröbenius $\Phi : \mathbb{F}_4 \to \mathbb{F}_4$ è un automorfismo di $\mathbb{F}_4$ definito come

$$v \mapsto v^2$$

essendo $4 = 2^2$. L'automorfismo Φ è un morfismo di spazi vettoriali perché

- $\Phi(a+b) = \Phi(a) + \Phi(b) \quad \forall a, b \in \mathbb{F}_4$ perché Φ è morfismo di anelli.
- $\Phi(ca) = c\Phi(a) \quad \forall c \in \mathbb{F}_2, a \in \mathbb{F}_4$. Questa proprietà non è immediata e va verificata. Essendo Φ un morfismo di anelli, abbiamo che

  $$\Phi(ca) = \Phi(c)\Phi(a)$$

  Ma l'automorfismo di Fröbenius fissa gli elementi del sottocampo fondamentale, quindi quelli di $\mathbb{F}_2$, e quindi $\Phi(c) = c$ e segue che

  $$\Phi(ca) = \Phi(c)\Phi(a) = c\Phi(a)$$

Scriviamo ora la matrice di Φ nella base $\{1, x\}$. Applicando Φ alla base otteniamo:

- $\Phi(1) = 1^2 = 1$
- $\Phi(x) = x^2 = 1 + x$

e quindi $M(\Phi)$ si costruisce mettendo sulle colonne i coefficienti di Φ applicata sulle basi.

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

Gli automorfismi di $\mathbb{F}_4$ possono essere visti anche come spazi vettoriali su $\mathbb{F}_2$. In particolare,

$$\mathbb{F}_4 \approx (\mathbb{F}_2 \times \mathbb{F}_2)$$

Sia ora

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{F}_2)$$

La matrice A è invertibile solo se il suo determinante è diverso da 0, ossia se

$$ad - bc \neq 0$$

Si noti che, se la matrice fosse in $\mathbb{Z}_4$, che non è un campo, avremmo dovuto assicurarci che il determinante fosse invertibile, altrimenti non averemmo potuto calcolare l'inversa di A. Ma fortunatamente siamo in $\mathbb{F}_4$, quindi possiamo proseguire senza verificare che $\det A$ sia invertibile perché, per definizione di campo, lo è. Dato che la matrice A ha valori in $\mathbb{F}_2$, allora $\bar{-1} = \bar{1}$ e quindi possiamo scrivere il determinante come

$$\det A = ad - bc = ad + bc$$

Essendo in $\mathbb{F}_2$, il determinante è diverso da 0 quando vale 1, quindi possiamo scrivere

$$\det A = 1$$
$$ad + bc = 1$$

Questo significa che:

- Se $a = 0$, allora necessariamente $b = c = 1$.
- Se $b = 0$, allora necessariamente $a = d = 1$.
- Se $c = 0$, allora necessariamente $a = d = 1$.
- Se $d = 0$, allora necessariamente $b = c = 1$.

Quindi, gli automorfismi di $\mathbb{F}_4$ possono essere scritti, come spazio vettoriale, come

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

Si noti che una matrice 2×2 in $\mathbb{F}_2$ è linearmente indipendente se

- Le righe e le colonne sono diverse.
- Nessuna riga o colonna è uguale a 0.

Come campo avevamo invece

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

5.2.2 Spazio duale di uno spazio vettoriale

Definizione 77 (Spazio duale di uno spazio vettoriale)**.** *Sia V uno spazio vettoriale di dimensione n su un campo K e sia $\{e_1, \ldots, e_n\}$ una sua base. L'insieme V^**

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

delle funzioni da V in K è detto duale di V.

Si noti che i morfismi in V^* sono funzioni che mandano un vettore $v \in V$ da uno spazio vettoriale V in un numero in K.

Definizione 78 (Base duale di uno spazio vettoriale)**.** *Chiamiamo il morfismo di spazi vettoriali*

$$e_i^* : V \to K$$

definito da

$$e_i^*(e_j) = \begin{cases} 1_K & \text{se } j = 1 \\ 0 & \text{altrimenti} \end{cases} \forall i = 1, \dots, n$$

base duale. L'insieme

$$\{e_1^*, \dots, e_n^*\}$$

è una base di V^*. In particolare,

$$\dim V^* = \dim V = n$$

Notiamo che abbiamo definito e_i^* solo sulle basi perché un vettore v in V può essere scritto come combinazione lineare delle sue basi, ossia

$$v = a_1 e_1 + a_2 e_2 + \cdots + a_n e_n$$

Dato che e_i^* è un morfismo di spazi vettoriali, per definizione (74), possiamo scrivere $e_i^*(v)$ come

$$e_i^*(v) = e_i^*(a_1 e_1 + a_2 e_2 + \cdots + a_n e_n) = a_1 e_1^*(e_1) + a_2 e_1^*(e_2) + \cdots + a_n e_1^*(e_n)$$

e quindi ci interessa solo definire e_i^* sulle basi di V.

Esempio

Consideriamo lo spazio vettoriale $V = \left(\mathbb{F}_2\right)^4$ che è isomorfo, come spazio vettoriale, a $\mathbb{F}_{16}$, quindi

$$V = \left(\mathbb{F}_2\right)^4 \approx \mathbb{F}_{16}$$

definito da

$$f(x) = < \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} ; x >$$

dove $< \cdot ; \cdot >$ è il prodotto scalare canonico su $(\mathbb{F}_2)^4$. Quindi, se

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

allora

$$f(x) = x_1 + x_2 + x_3 + x_4$$

Le basi di V sono

$$\{e_1, e_2, e_3, e_4\} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Se volessimo calcolare $e_1^*(x)$ scriveremmo

$$\begin{aligned} e_1^*(x) &= e_1^* \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \\ &= e_1^* \left(x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right) \\ &= e_1^*(x_1 e_1 + x_2 e_2 + x_3 e_3 + x_4 e_4) \\ &= e_1^*(x_1 e_1) + e_1^*(x_2 e_2) + e_1^*(x_3 e_3) + e_1^*(x_4 e_4) \\ &= e_1^*(x_1 e_1) \\ &= x_1 \end{aligned}$$

Ripetendo lo stesso ragionamento per tutte le basi di V^* otteniamo

$$f = e_1^* + e_2^* + e_3^* + e_4^*$$

Provando a chiamare f su x otteniamo, come aspettato,

$$f(x) = e_1^*(x) + e_2^*(x) + e_3^*(x) + e_4^*(x) = x_1 + x_2 + x_3 + x_4$$

Quindi effettivamente, f può essere scritta tramite la base duale di V.

5.3 Forme bilineari

Definizione 79 (Forma bilineare)**.** *Sia V uno spazio vettoriale di dimensione n su K. Sia $\{e_1, \dots, e_n\}$ una base di V. Una funzione da $V \times V \to K$ è detta forma bilineare se:*

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

Ad esempio, il prodotto scalare canonico su $\mathbb{R}^n$ è una forma bilineare.

5.3.1 Prodotto tensoriale bilineare

L'insieme delle forme bilineari su V forma uno spazio vettoriale. In particolare, siano $f_1, f_2, f : V \times V \to K$ forme bilineari, allora se definiamo

$$f_1 + f_2 : V \times V \to K$$

con

$$(f_1 + f_2)(v, w) \coloneqq f_1(v, w) + f_2(v, w) \quad \forall v, w \in V$$

e

$$af : V \times V \to K$$

con

$$(af)(v, w) \coloneqq af(v, w)$$

allora $f_1 + f_2$ e af sono forme bilineari. Ma quindi $f, f_1, f_2 \in \{f : V \times V \to K\}$ rispettano le proprietà della Definizione 71 perché sommando due elementi in $\{f : V \times V \to K\}$ otteniamo un altro elemento in $\{f : V \times V \to K\}$ (ossia un'altra forma bilineare) e moltiplicando un elemento di $\{f : V \times V \to K\}$ per un valore del campo K, otteniamo un'altra forma bilineare. In definitiva, l'insieme $\{f : V \times V \to K\}$ delle forme bilineari su V è uno spazio vettoriale e lo indichiamo come

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

e lo chiamiamo prodotto tensoriale tra V^* e V^*. In altre parole

Definizione 80 (Prodotto tensoriale bilineare)**.** *Sia V uno spazio vettoriale su un campo K. Lo spazio vettoriale delle forme bilineari su V*

$$V^* \otimes V^* = \{f : V \times V \to K\}$$

prende il nome di prodotto tensoriale.

Dalla definizione di prodotto tensoriale possiamo capire che

- Una forma monolineare è un elemento di V^*.
- Una forma bilineare è un elemento di $V^* \otimes V^*$.

Definizione 81 (Basi di una forma bilineare)**.** *Siano $1 \leq i, j \leq n$, indichiamo con*

$$e_i^* \otimes e_j^* : V \times V \to K$$

una forma bilineare definita come

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

dove δ_{ih} è il delta di Kroneker, definito come

$$\delta_{ih} = \begin{cases} 1 & \text{if } i = h \\ 0 & \text{altrimenti} \end{cases}$$

L'insieme

$$\{e_i^* \otimes e_j^* : 1 \leq i \leq n, 1 \leq j \leq n\}$$

è una base del prodotto tensoriale $V^* \otimes V^*$.

Esempio

Sia $< \cdot; \cdot >$ il prodotto scalare canonico su V. Quindi, se

$$v \coloneqq v_1 e_1 + \cdots + v_n e_n$$

e

$$w \coloneqq w_1 e_1 + \cdots + w_n e_n$$

allora

$$< v; w >= v_1 w_1 + \cdots + v_n w_n \in K$$

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

$$e_1^* \otimes e_1^* + \cdots + e_n^* \otimes e_n^*$$

5.3.2 Associare una matrice ad una forma bilineare

Data una forma bilineare è interessante associarvi una matrice. Sia $f : V \times V \to K$ una forma bilineare sullo spazio vettoriale V, ossia $f \in V^* \otimes V^*$. Allora possiamo creare una matrice $M(f) \in \mathrm{Mat}_{n\times n}(K)$ i cui elementi sono definiti come

$$M(f)_{r,c} = f(e_r, e_c) \in K$$

In questo modo, otteniamo che

$$f(u, v) =< u; M(f)v > \quad \forall u, v \in V$$

con $<;>$ prodotto scalare. Cerchiamo di ottenere questa scrittura considerando uno spazio vettoriale V di dimensione 2.

$$\begin{aligned}
f(u,v) &= f(u_1e_1 + u_2e_2, v_1e_1 + v_2e_2) \\
&= f(u_1e_1, v_1e_1 + v_2e_2) + f(u_2e_2, v_1e_1 + v_2e_2) && \text{linearità forma bilineare} \\
&= f(u_1e_1, v_1e_1 + v_2e_2) + f(u_2e_2, v_1e_1 + v_2e_2) && \text{linearità forma bilineare} \\
&= f(u_1e_1, v_1e_1) + f(u_1e_1, v_2e_2) + f(u_2e_2, v_1e_1) + f(u_2e_2, v_2e_2) && \text{linearità forma bilineare} \\
&= u_1v_1f(e_1, e_1) + u_1v_2f(e_1, e_2) + u_2v_1f(e_2, e_1) + u_2v_2f(e_2, e_2) && \text{linearità forma bilineare} \\
&= u_1\big(v_1f(e_1, e_1) + v_2f(e_1, e_2)\big) + u_2\big(v_1f(e_2, e_1) + v_2f(e_2, e_2)\big)
\end{aligned}$$

Se chiamiamo

$$w_1 = v_1 f(e_1, e_1) + v_2 f(e_1, e_2)$$

e

$$w_2 = v_1 f(e_2, e_1) + v_2 f(e_2, e_2)$$

allora

$$w = (w_1, w_2)$$

e $f(u, v)$ può essere scritto come

$$f(u, v) =< u; w >$$

Cerchiamo ora di capire chi è w. w_1 è il prodotto della prima riga della matrice $M(f)$ con il vettore colonna v mentre w_2 è il prodotto della seconda riga della matrice $M(f)$ con il vettore colonna v, quindi w è il prodotto riga-colonna tra $M(f)$ e v. Abbiamo quindi

$$f(u,v) =< u; M(f)v >$$

Abbiamo quindi definito un isomorfismo di spazi vettoriali da $V^* \otimes V^*$ a $\mathrm{Mat}_{n\times n}(K)$

$$M : V^* \otimes V^* \to \mathrm{Mat}_{n\times n}(K)$$

definito come

$$f \mapsto M(f)$$

Inoltre, essendo $V^* \otimes V^*$ lo spazio vettoriale delle forme bilineari su V, si ha che:

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

Esempi

Esempio 1 La matrice del prodotto scalare canonico è la matrice identità Id_n.

Esempio 2 Consideriamo la forma bilineare

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

La matrice associata a f è

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

Questo è un esempio di forma bilineare antisimmetrica. Per costruire questa matrice ci basta valutare f per tutte le combinazioni delle basi di $V \times V$. In particolare,

- $f(e_1, e_1) = e_1^* \otimes e_2^*(e_1, e_1) - e_2^* \otimes e_1^*(e_1, e_1) = 0 - 0 = 0$
- $f(e_1, e_2) = e_1^* \otimes e_2^*(e_1, e_2) - e_2^* \otimes e_1^*(e_1, e_2) = 1 - 0 = 1$
- $f(e_2, e_1) = e_1^* \otimes e_2^*(e_2, e_1) - e_2^* \otimes e_1^*(e_2, e_1) = 0 - 1 = -1$
- $f(e_2, e_2) = e_1^* \otimes e_2^*(e_2, e_2) - e_2^* \otimes e_1^*(e_2, e_2) = 0 - 0 = 0$

5.3.3 Forma multilineare

Definizione 82 (Forma multilineare)**.** *Siano $V_1, \ldots, V_K$ spazi vettoriali su un campo $\mathbb{F}$. Una funzione*

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

è detta forma multilineare se

1. $f(av_1, v_2, \ldots, v_k) = f(v_1, av_2, \ldots, v_k) = \cdots = af(v_1, v_2, \ldots, v_k) \quad \forall a \in \mathbb{F}, v_i \in V$

2.

$$\begin{aligned} f(v_1 + w, v_2, \dots, v_k) &= f(v_1, v_2, \dots, v_k) + f(w, v_2, \dots, v_k) \\ f(v_1, v_2 + w, \dots, v_k) &= f(v_1, v_2, \dots, v_k) + f(v_1, w, \dots, v_k) \\ &\vdots \\ f(v_1, v_2, \dots, v_k + w) &= f(v_1, v_2, \dots, v_k) + f(v_1, v_2, \dots, w) \end{aligned}$$

5.3.4 Prodotto tensoriale

Definizione 83 (Prodotto tensoriale)**.** *Siano $V_1, V_2, \dots, V_k$ spazi vettoriali su un campo $\mathbb{F}$. Definiamo*

$$V_1^* \otimes V_2^* \otimes \cdots \otimes V_k^*$$

lo spazio vettoriale delle forme multilineari

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

Definizione 84 (Base del prodotto tensoriale)**.** *Una base di $V_1^* \otimes V_2^* \otimes \cdots \otimes V_k^*$ è l'insieme*

$$\{e_{i_1}^{1^*} \otimes e_{i_2}^{2^*} \otimes \cdots \otimes e_{i_k}^{k^*} : 1 \le i_1 \le \dim V_1, \dots, 1 \le i_k \le \dim V_k\}$$

in cui

$$e_{i_1}^{1^*} \otimes e_{i_2}^{2^*} \otimes \cdots \otimes e_{i_k}^{k^*}(e_{j_1}^1, e_{j_2}^2, \dots, e_{j_k}^k) = e_{i_1}^{1^*}(e_{j_1}^1) \cdot e_{i_2}^{2^*}(e_{j_2}^2) \cdot \cdots \cdot e_{i_k}^{k^*}(e_{j_k}^k)$$

e

$$\{e_1^{1^*}, \dots, e_{\dim V_1}^{1^*}\}$$

è una base di V_1^*.

In pratica, per costruire una base del prodotto tensoriale, dobbiamo prendere, per ogni duale V_i^*, un suo elemento della base e fare il prodotto tensoriale tra tutti questi elementi.

5.3.5 Rango di una matrice

Definizione 85 (Rango di una matrice)**.** *Sia $A \in \mathrm{Mat}_{h\times k}(\mathbb{F})$ una matrice $h \times k$. Il rango di A è il numero massimo di colonne linearmente indipendenti o equivalentemente il numero massimo di righe linearmente indipendenti e lo indichiamo con* $\mathrm{rk}(A)$.

Inoltre, si può verificare che ogni matrice può essere scritta come somma di matrici di rango 1. Grazie a questo fatto possiamo dare un'altra definizione di rango.

Definizione 86 (Rango di una matrice)**.** *Sia*

$$X \coloneqq \{A \in \mathrm{Mat}_{h\times k}(\mathbb{F}) : \mathrm{rk}(A) = 1\}$$

allora il rango di una matrice $A \in \mathrm{Mat}_{h\times k}(\mathbb{F})$ è il minimo numero di matrici di rango 1 la cui somma da A, ossia

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

Da adesso in poi, se $V_1, \dots, V_k$ 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

$$V_1 \otimes V_2 \otimes \cdots \otimes V_k$$

è lo spazio vettoriale con base

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

che soddisfa le seguenti relazioni:

1. Per ogni $a \in K$, $1 \leq j_1 \leq i_1, \dots, 1 \leq j_h \leq i_h$

$$a(v_{j_1}^1 \otimes v_{j_2}^2 \otimes \cdots \otimes v_{j_h}^h) = a(v_{j_1}^1) \otimes v_{j_2}^2 \otimes \cdots \otimes v_{j_h}^h = \cdots = v_{j_1}^1 \otimes v_{j_2}^2 \otimes \cdots \otimes a(v_{j_h}^h)$$

2. Per ogni $v_i, w_i \in V$

$$\begin{aligned}
&(v_1 + w_1) \otimes \cdots \otimes v_h = (v_1 \otimes \cdots \otimes v_h) + (w_1 \otimes \cdots \otimes v_h) \\
&v_1 \otimes (v_2 + w_2) \otimes \cdots \otimes v_h = (v_1 \otimes v_2 \otimes \cdots \otimes v_h) + (v_1 \otimes w_2 \otimes \cdots \otimes v_h) \\
&v_1 \otimes \cdots \otimes (v_h + w_h) = (v_1 \otimes \cdots \otimes v_h) + (v_1 \otimes \cdots \otimes w_h)
\end{aligned}$$

Inoltre,

Definizione 87 (Tensori di rango 1)**.** *L'insieme*

$$\{v_1 \otimes v_2 \otimes \cdots \otimes v_h : v_i \in V_i \ \ \forall 1 \leq i \leq h\}$$

è l'insieme dei tensori di rango 1.

5.3.6 Rango di un tensore

Dato che per le matrici abbiamo definito il rango come il numero minimo di matrici di rango 1 da sommare per ottenere la matrice stessa, ed esiste un modo per associare una matrice ad un tensore (ossia ad una forma bi- o multi-lineare), allora possiamo definire il rango di un tensore analogamente. In particolare,

Definizione 88 (Rango di un tensore)**.** *Sia $T \in V_1 \otimes \cdots \otimes V_k$ un tensore. Il rango di T è il minimo numero $r \in \mathbb{N}$ tale che T può essere scritto come somma di r tensori $T_i \in_1\otimes \cdots \otimes V_k$*

di rango 1, ossia

$$\mathrm{rk}(T) = \min\{r \in \mathbb{N} : T = \sum_{i=1}^{r} T_i, \quad \mathrm{rk}(T_i) = 1, T_i \in V_1 \otimes \cdots \otimes V_k \ \forall i = 1, \ldots, r\}$$

Esempio

Siano U, V, W tre spazi vettoriali con basi $\{u_1, u_2\}$, $\{v_1, v_2\}$ e $\{w_1, w_2\}$, rispettivamente. Il tensore

$$T = u_1 \otimes v_1 \otimes w_1 + u_1 \otimes v_2 \otimes w_1 \in U \otimes V \otimes W$$

può essere riscritto, raccogliendo a fattor comune, come

$$T = u_1 \otimes (v_1 + v_2) \otimes w_1 \in U \otimes V \otimes W$$

e quindi T ha rango 1 perché è un solo tensore (i.e., la somma di un solo tensore). Se prendiamo invece

$$T' = u_1 \otimes v_1 \otimes w_1 + u_2 \otimes v_2 \otimes w_2 \in U \otimes V \otimes W$$

T' non può essere fattorizzato e quindi ha rango 2 perché è somma di due tensori di rango 1.

Rango e dimensione di un tensore

Osserviamo ora un fatto interessante. La dimensione del prodotto tensoriale di h spazi vettoriali V_1 è il prodotto delle dimensioni dei singoli spazi vettoriali, ossia

$$\dim\left(\bigotimes_{i=1}^{h} V_i\right) = \prod_{i=1}^{h} \dim(V_i)$$

Questo perché la dimensione di uno spazio vettoriale è data dal numero di basi dello spazio, ma le basi di $\bigotimes_{i=1}^{h} V_i$ sono tutte le possibili combinazioni di $e_{i_1}^{1+}, e_{i_2}^{2+}, \ldots, e_{i_k}^{k+}$ per $1 \leq i_1 \leq \dim V_1$, $1 \leq i_2 \leq \dim V_2$ fino a $1 \leq i_k \leq \dim V_k$. Se $T \in \bigotimes_{i=1}^{h} V_i$ allora il suo rango è sicuramente inferiore al prodotto delle dimensioni dei singoli V_i perché il rango è definito come somma di tensori di rango 1, e ne servono al massimo h, quindi

$$\mathrm{rk}T \leq \prod_{i=1}^{h} \dim(V_i)$$

5.3.7 Matrice come tensore

Abbiamo visto che dato un tensore è sempre possibile associargli una matrice. Vediamo ora come fare l'operazione inversa, ossia, come associare un tensore ad una matrice.

Iniziamo notando che una matrice $m \times n$ di rango 1 ha come colonne multipli di un qualche vettore

$$v \in K^m \setminus \{0\}$$

poiché tutte le colonne della matrice sono linearmente dipendenti da v. Se chiamiamo la prima colonna $a_1 v$, la seconda $a_2 v$ e l'n-esima $a_n v$, con $a_i \in K$ allora possiamo scrivere una matrice $A \in \mathrm{Mat}_{m\times n}(K)$ di rango 1 come

$$A = \mathbf{v}\cdot\mathbf{a} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} = \begin{pmatrix} v_1a_1 & v_1a_2 & \cdots & v_1a_n \\ v_2a_1 & v_2a_2 & \cdots & v_2a_n \\ \vdots & & & \\ v_ma_1 & v_ma_2 & \cdots & v_ma_n \end{pmatrix}$$

La matrice A, come forma bilineare, è il seguente elemento (ossia la forma bilineare) di $(K^m)^* \otimes (K^n)^*$,

$$\begin{aligned} t = {} & v_1a_1e_1^* \otimes e_1^* + v_1a_2e_1^* \otimes e_2^* + \cdots + v_1a_ne_1^* \otimes e_n^* \\ & + v_2a_1e_2^* \otimes e_1^* + v_2a_2e_1^* \otimes e_2^* + \cdots + v_2a_ne_1^* \otimes e_n^* \\ & + \dots \\ & + v_ma_1e_2^* \otimes e_1^* + v_ma_2e_1^* \otimes e_2^* + \cdots + v_1a_ne_1^* \otimes e_n^* \end{aligned}$$

Raccogliendo a fattor comune $a_ie_1^*$ otteniamo

$$\begin{aligned} t = {} & (v_1e_1^* + v_2e_2^* + \dots v_me_m^*) \otimes a_1e_1^* \\ & + (v_1e_1^* + v_2e_2^* + \dots v_me_m^*) \otimes a_2e_2^* \\ & + \dots \\ & + (v_1e_1^* + v_2e_2^* + \dots v_me_m^*) \otimes a_ne_n^* \end{aligned}$$

Raccogliendo nuovamente il fattore comune abbiamo

$$t = (v_1e_1^* + v_2e_2^* + \dots v_me_m^*) \otimes (a_1e_1^* + a_2e_2^* + \cdots + a_ne_n^*) \in (K^m)^* \otimes (K^n)^*$$

che è un tensore di rango 1, e quindi la matrice A di rango 1 può essere scritta come un tensore di rango 1. Quindi, una matrice $A \in \mathrm{Mat}_{m\times n}(K)$ tale che $\mathrm{rk}(A) = 1$ corrisponde ad un tensore $T_A \in (K^m)^* \otimes (K^n)^*$ tale che $\mathrm{rk}(T_A) = 1$. In pratica, ad un tensore di rango 1

$$v_1 \otimes v_2 \in (K^m)^* \otimes (K^n)^*$$

corrisponde una matrice di rango 1

$$v_1v_2^T \in \mathrm{Mat}_{m\times n}(K)$$

Quindi, data una matrice, possiamo sempre ottenere il suo tensore corrispondente e viceversa. Questo risultato è espresso nella seguente proposizione

Proposizione 28. *Data una matrice $A \in \mathrm{Mat}_{m\times n}(K)$ e un tensore $T_A \in (K^m)^* \otimes (K^n)^*$, entrambi di rango 1, A e T_A sono isomorfi.*

$$A \simeq T_A$$

Esiste quindi una corrispondenza biunivoca tra matrici di rango 1 in $\mathrm{Mat}_{m\times n}(K)$ e tensori

di rango 1 in $(K^m)^* \otimes (K^n)^*$.

Ma dato che una matrice può essere scritta come combinazione lineare di matrici di rango 1, un tensore può essere scritto come combinazione lineare di tensori di rango 1 ed esiste una biezione tra matrici di rango 1 e tensori di rango 1, allora possiamo affermare che:

Proposizione 29. *Data una matrice* $A \in \mathrm{Mat}_{m\times n}(K)$ *e un tensore* $T_A \in (K^m)^* \otimes (K^n)^*$, *A e* T_A *sono isomorfi.*

$$A \simeq T_A$$

Esiste quindi una corrispondenza biunivoca tra matrici in $\mathrm{Mat}_{m\times n}(K)$ *e tensori in* $(K^m)^* \otimes (K^n)^*$.

In pratica stiamo dicendo che una matrice di rango 1 può essere univocamente associata ad una sola forma multilineare. Questa associazione è ottenuta come combinazione lineare delle basi di del tensore. In particolare, la base $e_i^* \oplus e_j^*$ viene moltiplicata per il valore in posizione (i, j) della matrice. In questo modo, l'associazione tra matrice e tensore è univoca.

Esempio

Consideriamo, ad esempio, la matrice

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

Dato che i coefficienti sono in $\mathbb{F}_3$, allora $2 \cdot 2 = 4 = 1$ e $2 \cdot 1 = 2$ e quindi la prima e la terza colonna non sono linearmente indipendenti. Inoltre, la seconda colonna, essendo di tutti 0, non è linearmente indipendente rispetto alle altre due. In definitiva, la matrice ha rango 1. Come abbiamo visto, possiamo associare ad A una forma bilineare

$$T_A : \mathbb{F}_3^2 \times \mathbb{F}_3^3 \to \mathbb{F}_3$$

definita da

$$T_A(u, v) = u^T A v \quad \forall u \in \mathbb{F}_3^2, v \in \mathbb{F}_3^3$$

Ma non è tutto, infatti possiamo anche associare un tensore T_A di $(\mathbb{F}_3^2)^* \times (\mathbb{F}_3^3)^*$. In particolare,

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

Possiamo ora raccogliere a fattor comune per ottenere,

$$\begin{aligned} T_A &= e_1^* \otimes e_1^* + 2e_1^* \otimes e_3^* + 2e_2^* \otimes e_1^* + e_2^* \otimes e_3^* \\ &= (e_1^* + 2e_1^*) \otimes e_1^* + (2e_1^* + e_2^*) \otimes e_3^* \\ &= (e_1^* + 2e_1^*) \otimes e_1^* + 2(e_1^* + 2e_2^*) \otimes e_3^* \\ &= (e_1^* + 2e_1^*) \otimes (e_1^* + 2e_3^*) \in (\mathbb{F}_3^2)^* \times (\mathbb{F}_3^3)^* \end{aligned}$$

La matrice A può quindi essere scritta come

$$A = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 2 \end{pmatrix}$$

5.3.8 Isomorfismi di uno spazio vettoriale come elementi del prodotto tensoriale

Vogliamo ora interpretare Mat come morfismo di spazi vettoriali, così da poterlo poi interpretarlo come tensore.

Sia V uno spazio vettoriale su un campo K con base $\{e_1, \dots, e_n\}$. Gli elementi di $V^* \otimes V$

$$V^* \otimes V = \text{span}\{e_i^* \otimes e_j : 1 \leq i, j \leq n\}$$

ossia quelli generati dalle basi $e_i^* \otimes e_j$, possono essere interpretati come bimorfismi di V. Il morfismo di spazi vettoriali

$$e_i^* \otimes e_j : V \to V$$

è definito come

$$\begin{aligned} e_i^* \otimes e_j(e_h) &= \begin{cases} e_j & \text{se } h = i \\ 0 & \text{altrimenti} \end{cases} \\ &= e_i^*(e_h)e_j \quad \forall 1 \leq i, j, h \leq n \end{aligned}$$

La seconda scrittura ha senso perché $e_j^*(e_h)$ vale 1_K se $j = h$, 0 altrimenti e moltiplicando questo valore per e_j otteniamo proprio e_j.

Consideriamo ora un endomorfismo $f \in \text{END}(V)$ rappresentato dalla matrice

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

La matrice A può essere scritta come elemento di $V^* \otimes V$ e in particolare abbiamo

$$\begin{aligned} f = {} & e_1^* \otimes (a_{11}e_1 + a_{21}e_2 + \cdots + a_{n1}e_n) \\ & + e_2^* \otimes (a_{12}e_1 + a_{22}e_2 + \cdots + a_{n2}e_n) \\ & \vdots \\ & + e_n^* \otimes (a_{1n}e_1 + a_{2n}e_2 + \cdots + a_{nn}e_n) \end{aligned}$$

Viceversa, ogni elemento di $V^* \otimes V$ può essere interpretato come un endomorfismo di V, infatti basta scriverlo come sopra per poi ottenere la matrice che rappresenta l'endomorfismo. Abbiamo quindi definito un isomorfismo di spazi vettoriali tra $\text{END}(V)$ e $V^* \otimes V$,

$$\text{END}(V) \simeq V^* \otimes V$$

In altre parole abbiamo una corrispondenza biunivoca che è un isomorfismo di spazi vettoriali.

$$\text{END}(V) \to V^* \otimes V$$

Esempio matrice trasposta

Sia $V = \text{Mat}_{2\times 2}(\mathbb{R})$ lo spazio vettoriale delle matrici a componenti in $\mathbb{R}$. La funzione

$$f : \text{Mat}_{2\times 2}(\mathbb{R}) \to \text{Mat}_{2\times 2}(\mathbb{R})$$

definita da

$$A \mapsto A^T$$

è un morfismo di spazi vettoriali. Una base di V è

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

La matrice di f nella base $\{E_{11}, E_{12}, E_{21}, E_{22}\}$ (ossia la matrice associata all'endomorfismo f) è

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

che ha rango 4. La matrice $M(f)$ è stata ottenuta

1. applicando la trasposta alle basi,
2. scrivendo le basi trasposte come vettori colonna, da sinistra a destra e dall'alto in basso,
3. come matrice che ha per colonne i vettori ottenuti al punto precedente.

L'endomorfismo f (ossia la trasposizione di matrici), come tensore, può essere scritto come

$$f = E_{11}^* \otimes E_{11} + E_{12}^* \otimes E_{21} + E_{21}^* \otimes E_{12} + E_{22}^* \otimes E_{22}$$

Esempio somma con la trasposta

Consideriamo ora un elemento $g \in V^* \otimes V$ definito da

$$g = 2E_{11}^* \otimes E_{11} + E_{12}^* \otimes \big(E_{12} + E_{21}\big) + E_{21}^* \otimes \big(E_{12} + E_{21}\big) + 2E_{22}^* \otimes E_{22}$$

Raccogliendo a fattor comune otteniamo

$$g = 2E_{11}^* \otimes E_{11} + (E_{12}^* + E_{21}^*) \otimes \big(E_{12} + E_{21}\big) + 2E_{22}^* \otimes E_{22}$$

Che è un tensore di rango 3 e corrisponde all'endomorfismo

$$g : \mathrm{Mat}_{2\times 2}(\mathbb{R}) \to \mathrm{Mat}_{2\times 2}(\mathbb{R})$$

definito da

$$A \mapsto A + A^T$$

Corrispondenza di isomorfismo con il prodotto tensoriale

In generale, i morfismi

$$f : V \to W$$

sono in corrispondenza con il prodotto tensoriale

$$V^* \otimes W$$

Tale corrispondenza ci da un isomorfismo di spazi vettoriali dai morfismi $\mathrm{HOM}(V, W)$ a $V^* \otimes W$

$$\mathrm{HOM}(V, W) \simeq V^* \otimes W$$

Inoltre, il rango di un morfismo $f : V \to W$, inteso come dimensione della sua immagine o come rango della sua matrice associata, corrisponde al rango del tensore $f \in V^* \otimes W$. In generale

Proposizione 30 (Corrispondenza tra isomorfismi e tensori)**.** *Siano $V_1, V_2, \dots, V_h, W$ spazi vettoriali su K, una forma multilineare*

$$f : V_1 \times V_2 \times \cdots \times V_h \to W$$

è un elemento di

$$V_1^* \times V_2^* \times \cdots \times V_h^* \times W$$

posto

$$e^*_{i_1} \otimes e^*_{i_2} \otimes \cdots \otimes e^*_{i_h} \otimes w(v_1, v_2, \dots, v_h) = e^{1^*}_{i_1}(v_1) e^{2^*}_{i_2}(v_2) \cdots e^{h^*}_{i_h}(v_h) w \in W$$

$$\forall 1 \le i_1 \le \dim(V_1), \dots, 1 \le i_h \le \dim(V_h), w \in W, v_i \in V_i$$

5.3.9 Algoritmo di Strassen con i tensori

Qualche pagina fa abbiamo definito l'algoritmo di Strassen per calcolare il prodotto tra matrici più rapidamente rispetto all'algoritmo che moltiplica righe per colonne (chiamiamolo *algoritmo standard*, per brevità). Con le conoscenze che abbiamo acquisito fino ad ora, possiamo ora interpretare l'algoritmo di Strassen in termini di prodotti tensoriali. Partiamo dal notare che la moltiplicazione tra matrici $\mathrm{Mat}_{2\times 2}(K)$ (iniziamo con il caso semplice della moltiplicazione 2×2, per poi generalizzare) è una forma bilineare (79)

$$M_{2,2,2} : \mathrm{Mat}_{2\times 2}(K) \times \mathrm{Mat}_{2\times 2}(K) \to \mathrm{Mat}_{2\times 2}(K)$$

definita da

$$M_{2,2,2}(A, B) = A \cdot B \quad \forall A, B \in \mathrm{Mat}_{2\times 2}(K)$$

in cui $\cdot$ indica il prodotto righe per colonne. Mostriamo che $M_{2,2,2}$ è effettivamente una forma lineare. Come da definizione 79 dobbiamo mostrare che:

1. $x(AB) = (xA)B = A(xB) \quad \forall x \in K$
2. $(A_1 + A_2)B = A_1B + A_2B$
3. $B(A_1 + A_2) = BA_1 + BA_2$

Quindi, essendo $M_{2,2,2}$ una forma bilineare, possiamo associarvi un tensore

$$M_{2,2,2} \in (\mathrm{Mat}_{2\times 2}(K))^* \otimes (\mathrm{Mat}_{2\times 2}(K))^* \otimes \mathrm{Mat}_{2\times 2}(K)$$

Dato che le proprietà sopra valgono per matrici quadrate di dimensione arbitraria, allora, in generale, la moltiplicazione tra due matrici $\mathrm{Mat}_{n\times n}(K)$ è una forma bilineare, quindi un elemento in

$$\big(\mathrm{Mat}_{n\times n}(K)\big)^* \otimes \big(\mathrm{Mat}_{n\times n}(K)\big)^* \otimes \mathrm{Mat}_{n\times n}(K)$$

Torniamo ora a considerare il caso 2×2. Data una base canonica di $\mathrm{Mat}_{2\times 2}$, vogliamo scrivere il tensore associato alla forma bilineare $M_{2,2,2}$. Un base di $\mathrm{Mat}_{2\times 2}(K)$, con K campo qualsiasi, è

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

Possiamo quindi scrivere un tensore nella base

$$\left\{E_{ij}^* \otimes E_{hk}^* \otimes E_{uv} : 1 \leq i, j, h, k, u, v \leq 2\right\}$$

di

$$\left(\mathrm{Mat}_{2\times 2}(K)\right)^* \otimes \left(\mathrm{Mat}_{2\times 2}(K)\right)^* \otimes \mathrm{Mat}_{2\times 2}(K)$$

Se calcoliamo tutti i prodotti tra le basi otteniamo, ad esempio

- $E_{11}E_{11} = E_{11}$
- $E_{12}E_{12} = \mathbf{0}$
- $E_{22}E_{22} = E_{22}$

generalizzando abbiamo quindi

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

Possiamo quindi scrivere $M_{2,2,2}$ come

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

Per ottenere questa scrittura abbiamo utilizzato i risultati che vogliamo ottenere moltiplicando due basi. Prendiamo ad esempio $E_{11}E_{11}$. Il risultato di questa moltiplicazione vogliamo sia E_{11}, quindi sappiamo che $E_{11}^* \otimes E_{11}^* \otimes E_{11}$ è non nullo perché

$$E_{11}^* \otimes E_{11}^* \otimes E_{11}(E_{11}, E_{11}) = E_{11}^*(E_{11}) \otimes E_{11}^*(E_{11}) \otimes E_{11} = E_{11}$$

Considerando nuovamente $M_{2,2,2}$, ogni riga rappresenta una componente del prodotto tra matrici. Consideriamo ad esempio la prima, che restituisce l'elemento in posizione $(1, 1)$. Applicando $M_{2,2,2}$ a due matrici A e B con componenti a_{ij} e b_{ij} abbiamo che la prima riga ritorna

$$\begin{aligned} E_{11}^* \otimes E_{11}^* \otimes E_{11}(A, B) + E_{12}^* \otimes E_{21}^* \otimes E_{11}(A, B) &= E_{11}^* \otimes E_{11}^*(A, B) \cdot E_{11} + E_{12}^* \otimes E_{21}^*(A, B) \cdot E_{11} \\ &= E_{11}^*(A) \cdot E_{11}^*(B) \cdot E_{11} + E_{12}^*(A) \cdot E_{21}^*(B) \cdot E_{11} \\ &= a_{11} \cdot b_{11} \cdot E_{11} + a_{12} \cdot b_{21} \cdot E_{11} \\ &= (a_{11} \cdot a_{11} + a_{12} \cdot b_{21})E_{11} \end{aligned}$$

ed infatti l'elemento in posizione $(1, 1)$ del prodotto tra A e B si calcola come $a_{11} \cdot a_{11} + a_{12} \cdot b_{21}$.

Notiamo ora che il rango di $M_{2,2,2}$ è minore o uguale ad 8, che è anche il numero di operazioni necessarie per calcolare il prodotto di matrici 2×2 con l'algoritmo standard. Questo ci fa pensare che, se riuscissimo a fattorizzare $M_{2,2,2}$ in modo tale da avere un tensore di rango strettamente minore di 8, allora potremmo trovare un algoritmo per eseguire la moltiplicazione tra matrici con

meno operazioni. Una possibile fattorizzazione di $M_{2,2,2}$ è

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

Questa fattorizzazione ci permette di dire che $\mathrm{rk}(M_{2,2,2})$ è minore o uguale a 7, e corrisponde all'algoritmo di Strassen. Cerchiamo ora di capire perché il rango di $M_{2,2,2}$ corrisponde al numero di moltiplicazioni ed in particolare, perché ogni addendo della fattorizzazione corrisponde ad una moltiplicazione nell'algoritmo di Strassen. Se valutiamo la base di $\big(\mathrm{Mat}_{2\times 2}(K)\big)^* \otimes \big(\mathrm{Mat}_{2\times 2}(K)\big)^* \otimes \mathrm{Mat}_{2\times 2}(K)$ su due matrici A e B otteniamo

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

in cui $E_{ij}^*(A)$ e $E_{ij}^*(A)$ sono due valori di K, quindi $E_{ij}^*(A)E_{hk}^*(B)$ è una moltiplicazione tra due valori di K. Segue che il rango del tensore $M_{2,2,2}$ è il numero massimo di moltiplicazioni necessarie per eseguire la moltiplicazione di due matrici 2×2.

Risultati sui ranghi di tensori

Di seguito alcuni teoremi che mostrano i ranghi di alcuni tipi di tensori.

Teorema 21 (Brokett-Dobkin)**.**

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

Teorema 22 (Brokett-Dobkin)**.**

$$\mathrm{rk}(M_{2,2,2}) = 7$$

Proof. Abbiamo dimostrato, fattorizzando $M_{2,2,2}$ che $\mathrm{rk}(M_{2,2,2}) \leq 7$. Dal Teorema 21 abbiamo che $\mathrm{rk}(M_{2,2,2}) \geq 2 \cdot 4 - 1 = 7$ e quindi $\mathrm{rk}(M_{2,2,2}) = 7$. □

Teorema 23 (Blasser)**.**

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

Teorema 24 (Laderman)**.**

$$\mathrm{rk}(M_{3,3,3}) \leq 23$$

Teorema 25 (Deepmind). *Sul campo* $\mathbb{F}_2$

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

Teorema 26 (Kauers-Moosbauer).

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

Tutti questi risultati sono stati ottenuti fattorizzando il tensore che rappresenta la moltiplicazione tra matrici perché trovare il rango di una matrice equivale a trovare la fattorizzazione del tensore.

5.4 Tensori simmetrici e antisimmetrici

Vogliamo ora definire cosa si intende per tensore simmetrico e antisimmetrico. Partiamo dalla seguente definizione:

Definizione 89 (Gruppo di permutazione di n oggetti). *Sia* $n \in \mathbb{N} \setminus \{0\}$. *Definiamo*

$$[n] \coloneqq \{1, 2, \dots, n\}$$

L'insieme delle funzioni

$$f : [n] \to [n]$$

biunivoche con operazione di composizione è un gruppo che indichiamo con S_n *ed è detto gruppo di permutazione di* n *oggetti o gruppo simmetrico. La cardinalità del gruppo* S_n *è* $n!$*,*

$$|S_n| = n!$$

Un elemento σ di S_n può essere rappresentato come una stringa di n numeri,

$$\sigma(1)\sigma(2)\dots\sigma(n)$$

Questa notazione prende il nome di **notazione ad una linea** e σ è una funzione da $[n]$ in $[n]$. Ad esempio, la funzione $213 \in S$ è una funzione

$$f : [3] \to [3]$$

tale che

$$1 \mapsto 2$$
$$2 \mapsto 1$$
$$3 \mapsto 3$$

perché

- $\sigma(1) = 2$
- $\sigma(2) = 1$
- $\sigma(3) = 3$

Notiamo anche che, se $\sigma = 45132$, allora $\sigma^{-1} = 34512$ perché

- $\sigma(1) = 4$, quindi $\sigma(4)^{-1} = 1$
- $\sigma(2) = 5$, quindi $\sigma(5)^{-1} = 2$
- $\sigma(3) = 1$, quindi $\sigma(1)^{-1} = 3$
- $\sigma(4) = 2$, quindi $\sigma(2)^{-1} = 4$
- $\sigma(5) = 3$, quindi $\sigma(3)^{-1} = 5$

Infine, dovrebbe essere chiaro che la funzione identità può essere scritta come 12345.

Definiamo ora il numero di inversioni che possono essere fatte data una permutazione.

Definizione 90 (Numero di inversioni di una permutazione)**.** *Sia $\sigma \in S_n$. La cardinalità dell'insieme*

$$\{(i,j) \in [n] \times [n] : i < j, \sigma(i) \geq \sigma(j)\}$$

è il numero di inversioni di σ e lo indichiamo con

$$\mathrm{inv}(\sigma)$$

Sia V uno spazio vettoriale su K, con base $\{e_1, \dots, e_n\}$ e $\sigma \in S_h$. La permutazione σ può essere vista come un endomorfismo di

$$\bigotimes_{i=0}^{h} V_i$$

nel seguente modo

$$\sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \otimes \sigma_{i_h} = e_{i_{\sigma^{-1}(1)}} \otimes e_{i_{\sigma^{-1}(2)}} \otimes \cdots \otimes e_{i_{\sigma^{-1}(h)}} \qquad \forall 1 \leq i_1 \leq n, \dots, 1 \leq i_h \leq n$$

Quindi, ad ogni $\sigma \in S_h$ possiamo associare un endomorfismo,

$$\sigma \in S_n \mapsto \sigma \in \mathrm{END}\left(\bigotimes_{i=0}^{h} V_i\right)$$

Allora, possiamo definire i seguenti endomorfismi (idempotenti) di $\bigotimes_{i=0}^{h} V_i$:

1. $p^+ := \frac{1}{h!} \sum_{\sigma \in S_h} \sigma$
2. $p^- := \frac{1}{h!} \sum_{\sigma \in S_h} (-1)^{wv(\sigma)} \sigma$

Grazie a questi endomorfismi, possiamo definire i tensori simmetrici e antisimmetrici.

Definizione 91 (Tensore simmetrico)**.** *L'immagine dell'endomorfismo* p^+*,*

$$\mathrm{Im}(p^+) \subseteq \bigotimes_{i=1}^{h} V$$

è il sottospazio dei tensori simmetrici in $\bigotimes_{i=1}^{h} V$ *e lo indichiamo con* $S^h V$*.*

Definizione 92 (Tensore antisimmetrico)**.** *L'immagine dell'endomorfismo* p^-*,*

$$\mathrm{Im}(p^-) \subseteq \bigotimes_{i=1}^{h} V$$

è il sottospazio dei tensori antisimmetrici in $\bigotimes_{i=1}^{h} V$ *e lo indichiamo con* $\Lambda^h V$*.*

5.4.1 Esempi

Associazione di un endomorfismo ad una permutazione

Sia $\sigma = 321 \in S_3$ e $V = \mathbb{R}^2$ con base $\{e_1, e_2\}$. Vogliamo calcolare $\sigma(e_1 \otimes e_1 \otimes e_2)$ in cui $i_1 = 1$, $i_2 = 1$, $i_3 = 2$. Allora

$$\begin{aligned}\sigma(e_1 \otimes e_1 \otimes e_2) &= e_{i_{\sigma^{-1}(1)}} \otimes e_{i_{\sigma^{-1}(2)}} \otimes e_{i_{\sigma^{-1}(3)}} \\ &= e_{i_3} \otimes e_{i_2} \otimes e_{i_3} \\ &= e_2 \otimes e_1 \otimes e_1\end{aligned}$$

Quindi

$$\sigma(u \otimes v \otimes w) = w \otimes v \otimes u \quad \forall u, v, w \in \mathbb{R}^2$$

Tensori simmetrici

Consideriamo lo spazio vettoriale $V = \mathbb{R}^2$ con base $\{e_1, e_2\}$ e definiamo l'endomorfismo $p^+ : \mathbb{R}^2 \otimes \mathbb{R}^2 \to \mathbb{R}^2 \otimes \mathbb{R}^2$. Iniziamo calcolando

$$\begin{aligned}p^+(e_1 \otimes e_2) &= \frac{1}{2!} \sum_{\sigma \in S_2} \sigma(e_1 \otimes e_2) \\ &= \frac{1}{2} 12(e_1 \otimes e_2) + \frac{1}{2} 21(e_1 \otimes e_2) \\ &= \frac{1}{2} e_{i_{\sigma^{-1}(1)}} \otimes e_{i_{\sigma^{-1}(2)}} + \frac{1}{2} e_{i_{\sigma^{-1}(1)}} \otimes e_{i_{\sigma^{-1}(2)}} \\ &= \frac{1}{2} e_{i_1} \otimes e_{i_2} + \frac{1}{2} e_{i_2} \otimes e_{i_1} \\ &= \frac{1}{2}\big(e_1 \otimes e_2 + e_2 \otimes e_1\big)\end{aligned}$$

Allo stesso modo otteniamo

$$p^+(e_1 \otimes e_1) = \frac{1}{2}\big(e_1 \otimes e_1 + e_1 \otimes e_1\big) = e_1 \otimes e_1$$
$$p^+(e_2 \otimes e_1) = \frac{1}{2}\big(e_1 \otimes e_2 + e_2 \otimes e_1\big)$$
$$p^+(e_2 \otimes e_2) = \frac{1}{2}\big(e_2 \otimes e_2 + e_2 \otimes e_2\big) = e_2 \otimes e_2$$

Quindi, un elemento di $S^2\mathbb{R}^2$, è del tipo

$$x_{11}e_1 \otimes e_1 + x_{12}\big(e_1 \otimes e_2 + e_2 \otimes e_1\big) + x_{22}e_2 \otimes e_2$$

che, interpretato come forma bilineare, può essere scritto, sotto forma di matrice, come

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{12} & x_{22} \end{pmatrix}$$

In generale abbiamo un isomorfismo di spazi vettoriali

$$S^2K^n \simeq M \in \mathrm{Mat}_{n\times n}(K) : M = M^T$$

Tensori antisimmetrici

Consideriamo lo spazio vettoriale $V = \mathbb{R}^2$ con base $\{e_1, e_2\}$ e scriviamo l'endomorfismo $p^- : \mathbb{R}^2 \otimes \mathbb{R}^2 \to \mathbb{R}^2 \otimes \mathbb{R}^2$ come

$$p^-(e_1 \otimes e_1) = 0$$
$$p^-(e_1 \otimes e_2) = \frac{1}{2}(12 + 21)(e_1 \otimes e_2) = \frac{1}{2}(e_1 \otimes e_2 - e_2 \otimes e_1)$$
$$p^-(e_2 \otimes e_2) = \frac{1}{2}(12 + 21)(e_2 \otimes e_1) = \frac{1}{2}(-e_1 \otimes e_2 + e_2 \otimes e_1)$$
$$p^-(e_2 \otimes e_2) = 0$$

Una base di $\Lambda^2\mathbb{R}^2$ è

$$\{e_1 \otimes e_2 - e_2 \otimes e_1\} = e_1 \wedge e_2$$

ed un elemento di $\Lambda^2\mathbb{R}^2$ è del tipo

$$x_{12}e_1 \wedge e_2$$

Interpretato come forma bilineare, $\Lambda^2\mathbb{R}^2$ può essere scritto, in forma matriciale, come

$$\begin{pmatrix} 0 & x_{12} \\ -x_{12} & 0 \end{pmatrix}$$

In generale abbiamo un isomorfismo di spazi vettoriali

$$\lambda^2\mathbb{R}^2 \simeq \{M \in \mathrm{Mat}_{n\times n}(K) : M = -M^T\}$$

5.4.2 Equazione parametrica dell'insieme dei tensori di rango 1

Consideriamo $\mathbb{R}^3 \otimes \mathbb{R}^3$ ed il tensore

$$T = (a_1 e_1 + a_2 e_2 + a_3 e_3) \otimes (b_1 e_1 + b_2 e_2 + b_3 e_3)$$

Il rango di T è 1 se

$$(a_1, a_2, a_3) \neq (0, 0, 0) \neq (b_1, b_2, b_3)$$

Il tensore può essere scritto anche come

$$\begin{aligned} T = & a_1 b_1 e_1 \otimes e_1 + a_1 b_2 e_1 \otimes e_2 + a_1 b_3 e_1 \otimes e_3 \\ & + a_2 b_1 e_2 \otimes e_1 + a_2 b_2 e_2 \otimes e_2 + a_2 b_3 e_2 \otimes e_3 \\ & + a_3 b_1 e_3 \otimes e_1 + a_3 b_2 e_3 \otimes e_2 + a_3 b_3 e_3 \otimes e_3 \end{aligned}$$

Part III

Logica

Chapter 6

Logica proposizionale

6.1 Sintassi

Il nostro obiettivo è quello di studiare la logica modale. Dato che la logica modale è un estensione della logica proposizionale, dobbiamo prima introdurre quest'ultima.

Per prima cosa, iniziamo a studiare cosa è possibile scrivere in logica proposizionale e quali sono i simboli per farlo.

6.1.1 Alfabeto

L'alfabeto usato in logica proposizionale, i.e., l'insieme di simboli consentiti è definito come segue.

Definizione 93 (Alfabeto della logica proposizionale)**.** *L'alfabeto della logica proposizionale è:*

1. *Un* ***insieme numerabile di variabili****.*
2. *I* ***connettivi logici***
   - $\neg$*, che chiamiamo negazione.*
   - $\wedge$*, che chiamiamo congiunzione.*
   - $\vee$*, che chiamiamo disgiunzione.*

Notiamo che per ora non abbiamo introdotto i simboli di implicazione e doppia implicazione perché questi possono essere scritti con $\neg$, $\wedge$ e $\vee$. Da questo alfabeto, possiamo costruire le parole del linguaggio, che possono essere:

Definizione 94 (Parola in logica proposizionale)**.** *Una parola del linguaggio in logica proposizionale è:*

1. *Un* ***letterale*** *che è una variabile X o la sua negazione $\neg X$.*
2. *Una* ***clausola****, ossia una disgiunzione di letterali. Se L_1 e L_2 sono letterali, allora $L_1 \vee L_2$ è una clausola.*

3. *Una **formula in forma normale congiuntiva** (CNF, Conjuntive Normal Form) che è una congiunzione di clausole. Se C_1 e C_2 sono clausole, allora $C_1 \wedge C_2$ è una formula in CNF.*

Come notazione, per ogni letterale L definiamo

$$\bar{L} = \begin{cases} \neg X & \text{se } L = X \\ X & \text{se } L = \neg X \end{cases}$$

Inoltre, indichiamo con

$$\mathrm{Var}(F)$$

l'insieme delle variabili di una formula F. Infine aggiungiamo all'alfabeto, come simboli ausiliari, le parentesi tonde che possono aiutarci a leggere correttamente le formule.

Esempio

Ad esempio

$$F = (\neg X_1 \vee X_2) \wedge X_1 \wedge (X_2 \vee X_3)$$

è una formula. Le sue variabili sono

$$\mathrm{Var}(F) = \{X_1, X_2, X_3\}$$

e le sue clausole sono

$$\neg X_1 \vee X_2$$
$$\neg X_1$$
$$X_2 \vee X_3$$

6.2 Semantica

Vogliamo ora dare un significato alle formule della logica proposizionale. Per farlo dobbiamo introdurre il concetto di assegnazione appropriata ad una formula.

Definizione 95 (Assegnazione appropriata)**.** *Sia F una formula in CNF e $\mathrm{Var}(F) \subseteq Y$ (quindi Y insieme delle possibili variabili). Una assegnazione appropriata ad F è una funzione*

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

L'insieme dei valori $\{0, 1\}$ è l'insieme dei valori di verità di F (i.e., falso e vero). La funzione V assegna quindi un valore di verità $\{0, 1\}$ ad una variabile della formula.

Definizione 96 (Assegnazione che soddisfa una formula)**.** *Sia F una formula. Una assegnazione V di F soddisfa F e scriviamo*

$$V \models F$$

se

1. *F è una variabile X, allora $V \models F$ significa che $V(X) = 1$.*
2. *F è il letterale $\neg X$, allora $V \models F$ significa che $V(X) = 0$.*
3. *F è una clausola $L_1 \vee L_2 \vee \cdots \vee L_n$, allora $V \models F$ significa che V soddisfa almeno uno dei letterali L_i (usando la definizione ai punti 1 e 2).*
4. *F è una congiunzione di clausole $C_1 \wedge C_2 \wedge \cdots \wedge C_n$, allora $V \models F$ significa che V soddisfa tutte le clausole C_i (usando la definizione al punto 3).*

Ora che sappiamo dire se una certa assegnazione (ossia una funzione che assegna ad ogni variabile un valore in $\{0, 1\}$) di una formula soddisfa la formula, possiamo definire quando una formula è soddisfacibile.

Definizione 97 (Formula soddisfacibile)**.** *Una formula F è detta soddisfacibile se esiste almeno un'assegnazione V appropriata ad F che soddisfa F, ossia*

$$F \text{ soddisfacibile} \iff \exists V : V \models F$$

Altrimenti diciamo che F è insoddisfacibile.

Definizione 98 (Tautologia)**.** *Una formula F è una tautologia se ogni assegnazione V appropriata ad F soddisfa F.*

Un esempio di tautologia è $X \vee \neg X$ perché prendendo $f(X) = 1$ o $f(X) = 0$, in entrambi i casi la formula è soddisfatta. Al contrario abbiamo

Definizione 99 (Contraddizione)**.** *Una formula F è una contraddizione se nessuna assegnazione V appropriata ad F soddisfa F.*

Un esempio di contraddizione è $X \wedge \neg X$ perché prendendo $f(X) = 1$ o $f(X) = 0$, in entrambi i casi la formula non è soddisfatta.

6.2.1 Conseguenza ed implicazione logica

Vogliamo ora definire il concetto di conseguenza logica.

Definizione 100 (Conseguenza logica)**.** *Date due formule F e G, G è conseguenza logica di F se per ogni assegnazione V appropriata di F e G allora si ha $V \models F$ implica $V \models G$.*

In altre parole, diciamo che G è conseguenza logica di F se, data una assegnazione soddisfa V, allora questa deve soddisfare anche G. Oltre alla conseguenza logica, è comodo definire anche il concetto di implicazione logica. In particolare, abbiamo

Definizione 101 (Implicazione logica)**.** *Definiamo*

$$X \Rightarrow Y \coloneqq \neg X \vee Y$$

L'implicazione logica ci dice che:

- Se X è falso, allora la formula è sicuramente vera.
- Se X è vero, allora Y deve essere vero affinché la formula sia vera.

e quindi effettivamente abbiamo definito l'implicazione logica. Grazie al concetto di conseguenza logica, possiamo definire l'equivalenza logica come la conseguenza logica considerando entrambe le direzioni. Più formalmente:

Definizione 102 (Equivalenza logica)**.** *Siano F e G due formule. F e G sono logicamente equivalenti, e scriviamo*

$$F \equiv G$$

se G è conseguenza logica di F e F è conseguenza logica di G.

Oltre all'equivalenza può essere utile definire il concetto di doppia implicazione. In particolare, abbiamo

Definizione 103 (Doppia implicazione)**.** *Definiamo:*

$$X \iff Y \coloneqq (X \implies Y) \wedge (Y \implies X)$$

6.2.2 Negazione di una formula

Vogliamo definire ora come negare una formula. In particolare, abbiamo:

1. Sia L letterale, $\neg L = \bar{L}$.
2. Sia $L_1, \ldots, L_n$ letterali, $\neg(L_1 \vee \cdot \vee L_n) \coloneqq \neg L_1 \wedge \cdot \wedge \neg L_n$.
3. Sia $C_1, \ldots, C_n$ clausole, $\neg(C_1 \wedge \cdot \wedge C_n) \coloneqq \neg C_1 \vee \cdot \vee \neg C_n$. Si noti che, da questa formula, bisogna applicare la proprietà distributiva per ottenere una formula CNF.

6.3 Verifica di soddisfacibilità

6.3.1 Definizioni utili

Data una formula F, vogliamo vedere se è soddisfacibile in maniera automatica. Per comodità, indicheremo una clausola $C = L_1 \vee L_2 \vee \cdots \vee L_n$ come

$$\{L_1, L_2, \ldots, L_n\}$$

Allo stesso modo, possiamo scrivere una formula come un insieme di clausole, ossia un insieme di insiemi. Inoltre indicheremo con $\varnothing$ la clausola vuota, ossia

$$\varnothing = L_1 \vee L_2 \vee \cdots \vee L_n \quad n = 0$$

ossia la disgiunzione di 0 letterali. Si noti che nessuna assegnazione soddisfa $\varnothing$, ossia $\varnothing$ è una contraddizione. Indichiamo poi con $\not{1}$ la congiunzione di 0 clausole, ossia

$$\not{1} = C_1 \wedge C_2 \wedge \cdots \wedge C_n \quad n = 0$$

Tutte le assegnazioni soddisfano $\not{1}$, ossia $\not{1}$ è una tautologia.

Proposizione 31. *Sia S' l'insieme ottenuto da un insieme di clausole S dopo la cancellazione di una tautologia. Allora*

$$S \equiv S'$$

6.3.2 Algoritmo di Davis-Putnam

L'algoritmo di Davis-Putnam permette di verificare se una formula F è soddisfacibile. Prima di vedere l'algoritmo in se, dobbiamo introdurre alcune definizioni accessorie. Iniziamo a dire cosa si intende per risolvente di due clausole.

Definizione 104 (Risolvente di clausole)**.** *Siano C_1 e C_2 clausole, e supponiamo che un letterale L soddisfi $L \in C_1$ e $\bar{L} \in C_2$. Il risolvente di C_1 e C_2 su L e $\bar{L}$ è la clausola*

$$R(C_1, C_2, L, \bar{L}) = (C_1 \setminus \{L\}) \cup (C_2 \setminus \{\bar{L}\})$$

In altre parole, il risolvente è la clausola ottenuta togliendo L da C_1 e $\bar{L}$ da C_2 e unendo le due clausole.

Lemma 1. *Sia C_1, C_2 clausole e $L \in C_1, \bar{L} \in C_2$, allora il risolvente di C_1 e C_2 su L e $\bar{L}$ è conseguenza logica di $C_1 \wedge C_2$.*

Proof. Chiamiamo

$$D \coloneqq R(C_1, C_2, L, \bar{L}).$$

D non ha nuove variabili rispetto a quelle di C_1 e C_2 perché abbiamo semplicemente tolto L dalle clausole. Allora, ogni assegnazione appropriata a $C_1 \wedge C_2$ è appropriata a D perché D non ha più variabili di $C_1 \wedge C_2$. Sia poi α un'assegnazione che soddisfa entrambe le clausole ossia, $\alpha \models C_1$ e $\alpha \models C_2$. Dato che α soddisfa entrambe le clausole, questa soddisfa anche la congiunzione delle clausole, ossia $\alpha \models C_1 \wedge C_2$. Vogliamo quindi mostrare che $\alpha \models D$. Per ipotesi $\alpha \models M$ per qualche letterale M della clausola C_1 e $\alpha \models N$ per qualche N letterale di C_2. Non è possibile che $M = L$ e $N = \bar{L}$ perché α soddisferebbe L e la sua negazione, quindi se $M = L$, allora $N \neq \bar{L}$, e viceversa. Questo significa che o $L \in D$ o $\bar{L} \in D$, ma non entrambi e quindi concludiamo che $\alpha \models D$. □

Lemma 2. *La formula $C_1 \wedge C_2$ è logicamente equivalente alla formula $C_1 \wedge C_2 \wedge R(C_1, C_2, L, \bar{L})$.*

$$C_1 \wedge C_2 \equiv C_1 \wedge C_2 \wedge R(C_1, C_2, L, \bar{L})$$

Algoritmo

Data una formula

$$F = C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

in CNF, possiamo verificare se F è soddisfacibile tramite il seguente algoritmo:

1. Eliminiamo le clausole con un letterale l (ossia per cui l'unica assegnazione che le rende vere è 1). In particolare:
   (a) Eliminiamo le clausole con un solo letterale l, assegnando $l = 1$.
   (b) Eliminiamo tutte le clausole che contengono l.
   (c) Eliminiamo $\bar{l}$ da tutte le clausole che lo contengono (eliminiamo solo $\bar{l}$, non tutta la clausola).
2. Se la formula F contiene le clausole $C_1 = \{L\}$ e $C_2 = \{\bar{L}\}$, la formula non è soddisfacibile.
3. Se nella formula appare solo il letterale l, ma non appare $\bar{l}$, allora possiamo assegnare $l = 1$ ed eliminare tutte le clausole in cui compare l.
4. Eliminiamo le tautologie.
5. Scegliamo una variabile che occorre nella clausola più corta e la chiamiamo p_1. Calcoliamo tutti i possibili risolventi su $\bar{p}_1$ e p_1 e li mettiamo insieme alle clausole in cui non appare p_1.
6. Reiteriamo fino a che non otteniamo $\{\emptyset\}$ o $\not{\Lambda}$ e
   - Se otteniamo $\emptyset$, la formula non è soddisfacibile perché la clausola vuota non è mai soddisfacibile.
   - Se otteniamo $\not{\Lambda}$, la formula è soddisfacibile, perché $\not{\Lambda}$ è una tautologia.

L'algoritmo di Davis-Putnam ritorna anche un'assegnazione che soddisfa la formula.

Chapter 7

Logica modale

7.1 Sintassi

La logica modale è un estensione della logica proposizionale. Per questo motivo, i simboli usati in logica modale sono un'estensione di quelli usati in logica proposizionale. In particolare, abbiamo

Definizione 105 (Alfabeto della logica modale)**.** *L'alfabeto della logica modale è:*

- *Un insieme numerabile di variabili* Var*.*
- *I connettivi logici* $\neg$, $\vee$, $\wedge$, $\Rightarrow$ *e* $\iff$ *.*
- *I simboli ausiliari* (*e*)*.*
- *I connettivi* $\Box$ *e* $\Diamond$*.*

La novità introdotta dalla logica modale è data dai simboli $\Box$ e $\Diamond$. Per ora questi simboli non hanno significato, ma analizzeremo più avanti come interpretarli. Le parole del linguaggio sono le formule ben formate (FBF) definite ricorsivamente come segue.

Definizione 106 (Formula ben formata)**.** *Una formula ben formata è definita ricorsivamente:*

1. *Ogni variabile è una formula ben formata.*
2. *Se* A *è una formula ben formata, allora* $\neg A$, $\Box A$ *e* $\Diamond A$ *sono formule ben formate.*
3. *Se* A *e* B *sono formule ben formate, allora* $A \wedge B$, $A \vee B$, $A \Rightarrow B$ *e* $A \iff B$ *sono formule ben formate.*

7.1.1 Interpretazione dei nuovi connettivi

Prima di analizzare la semantica della logica modale, diamo delle interpretazioni dei connettivi $\Box$ e $\Diamond$ introdotti dalla logica modale.

Logica classica

La lettura più comune dei simboli $\Box$ e $\Diamond$ è:

- $\Box A$ lo leggiamo come *è necessario che A*.
- $\Diamond A$ lo leggiamo come *è possibile che A*.

Possiamo notare che queste affermazioni non possono essere tradotte in logica proposizionale. Inoltre, possiamo definire un simbolo in termini dell'altro e viceversa:

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

Logica modale epistemica

Nelle logiche modali epistemiche:

- $\Box A$ lo leggiamo come *si sa che A*. In questo caso si può anche scrivere $\Box_1 A$ per dire che *la persona 1 sa che A*.

Logica modale deontica

Nelle logiche modali deontiche:

- $\Box A$ lo leggiamo come *è obbligatorio che A*.
- $\Diamond A$ lo leggiamo come *è facoltativo che A*.

Logica modale doxastica

Nelle logiche modali doxastiche:

- $\Box A$ lo leggiamo come *si crede che A*.

Logica modale dimostrativa

Nelle logiche modali dimostrativa:

- $\Box A$ lo leggiamo come *è dimostrabile che A*.

Una nota importante

La logica proposizionale è una logica vero-funzionale, ossia assegnando i valori 0 e 1 alle variabili possiamo assegnare un valore 0 o 1 ad una formula nel modo univoco stabilito dalla semantica della logica proposizionale. Questo assegnamento corrisponde alla nostra intuizione di negazione, disgiunzione e congiunzione.

Per la logica modale la situazione è più complicata. Interpretando il simbolo $\Box$ come operatore di necessità e $\Diamond$ come operatore di possibilità, possiamo essere, ad esempio, d'accordo sul fatto che le formule

$$\Box A \Rightarrow \Diamond A$$

e

$$A \Rightarrow \Diamond A$$

siamo vere. Questo perché ha senso dire che *se è necessario che sia vera A, allora è possibile che sia vera A*. Ha anche senso affermare che *se è vera A allora è possibile che sia vera A*. Non è invece chiaro se sia vera la formula

$$A \Rightarrow \Box\Diamond A$$

perché non è chiaro se sia vero che *se è vera A, allora è necessario che sia possibile che A*. Nel caso della logica epistemica, in cui $\Box$ si indica con K, la formula $KA \Rightarrow A$ sembra essere vera perché è vero che *se si sa A allora vale A*. Nella stessa logica sembra invece falsa la formula $A \Rightarrow KA$, interpretata come **se vale A allora si sa che** A, perché non si è onniscenti.

7.2 Semantica dei mondi possibili

La logica modale introduce la semantica dei mondi possibili, o di Kircke. Per descrivere questa semantica abbiamo bisogno del concetto di frame.

Definizione 107 (Frame)**.** *Un frame è una coppia (S, R) dove*

- *S è un insieme non vuoto detto **insieme dei mondi**.*
- *R è una relazione su S, ossia $R \subseteq S \times S$ con $R \neq \emptyset$, detta **relazione di accessibilità**.*

Definizione 108 (Accessibilità di un frame)**.** *Sia (S, R) un frame e $x, y \in S$. Se $(x, y) \in R$ allora diciamo che y è accessibile da x.*

Un frame (S, R) può essere rappresentato come un grafo diretto con cappi (per indicare un mondo raggiungibili dal mondo stesso) in cui:

- I nodi sono i valori di S.
- È presente un arco da x a y se $(x, y) \in R$.

Se consideriamo ad esempio il frame

$$\big(\{2, 3, 4, 5, 6\}, \{(x, y) : x|y\}\big)$$

questo può essere rappresentato come in Figura 7.1.

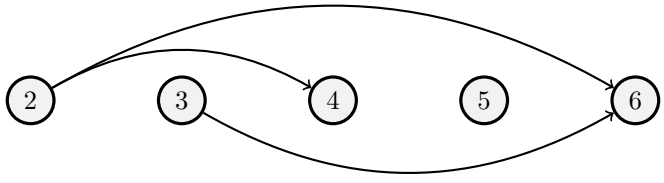


Figure 7.1: Il grafo rappresentante il frame $\big(\{2, 3, 4, 5, 6\}, \{(x, y) : x|y\}\big)$

Grazie alla definizione di frame possiamo definire un modello su un frame. Un modello ci consente di dire quando una certa formula è vera.

Definizione 109 (Modello su un frame)**.** *Un modello su un frame (S, R) è una terna*

$$(S, R, V)$$

con

$$V : \text{Var} \to \wp(S)$$

funzione, detta ***funzione di valutazione****, che associa a una variabile un insieme di mondi, ossia i mondi in cui la variabile è vera.*

La funzione di valutazione associa le variabili di una formula ai mondi in cui sono vere, ossia in quali mondi la formula vale 1. Possiamo quindi dire quando una formula ben formata F è vera in un mondo. In particolare:

Definizione 110 (Formula ben formata vera in un mondo)**.** *Una formula ben formata F si dice vera in un mondo $x \in S$ del modello $M = (S, R, V)$ e scriviamo*

$$M \models_x F$$

se e solo se

1. *Se F è una variabile, allora $M \models_x F$ significa che il mondo x è nei mondi in cui F è vera, i.e.,*
$$x \in V(F)$$
2. *Se $F = \neg y$ con y variabile, allora $M \models_x F$ significa che il mondo x non appartiene ai mondi in cui y è vera, i.e.,*
$$x \notin V(y)$$
3. *Se $F = \neg G$ con G formula ben formata, allora $M \models_x F$ significa che*
$$M \not\models_x G$$
4. *Se $F = G_1 \wedge G_2$ con G_1, G_2 formule ben formate, allora $M \models_x F$ significa*
$$M \models_x G_1 \wedge M \models_x G_2$$
5. *Se $F = G_1 \vee G_2$ con G_1, G_2 formule ben formate, allora $M \models_x F$ significa*
$$M \models_x G_1 \vee M \models_x G_2$$
6. *Se $F = \Box G$ con G formula ben formata, allora $M \models_x F$ significa che, per ogni mondo y raggiungibile da x (i.e., $\forall y \in S : (x, y) \in R$),*
$$M \models_y G$$
7. *Se $F = \Diamond G$ con G formula ben formata, allora $M \models_x F$ significa che, per qualche mondo y raggiungibile da x,*
$$M \models_y G$$

Dalla logica modale a quella proposizionale

Se come frame prendiamo il frame

$$(\{\emptyset\}, R)$$

dove

$$R \subseteq S \times S = \{(\emptyset, \emptyset)\}$$

Una funzione di valutazione è

$$V : \text{Var} \to \wp(S) = \{\emptyset, \{\emptyset\}\} \simeq \{0, 1\}$$

In questo modo i connettori modali diventano superflui e ritroviamo la logica proposizionale. La verità di una formula del linguaggio modale dipenderà quindi dal frame scelto. In particolare, dalla relazione R.

7.2.1 Relazioni e formule

Consideriamo la formula $\Box X \Rightarrow X$. Nella logica classica, questa formula viene interpretata come **se è necessario che X, allora vale X**, e quindi noi vorremmo che sia vera. La veridicità di questa formula, dato che contiene il connettore $\Box$, dipende dalla relazione R del modello che stiamo considerando. In particolare vale il seguente risultato

Proposizione 32. *La formula $\Box X \Rightarrow X$ è vera sul frame (S, R) se e solo se la relazione R è riflessiva, ossia ogni mondo $x \in S$ è in relazione con se stesso,*

$$(x, x) \in R \quad \forall x \in S$$

Proof. Assumiamo che R non sia riflessiva e mostriamo che la formula non è vera. Se R non è riflessiva, esiste $y \in S$ tale che $(y, y) \notin R$. Vediamo ora che c'è un modello su un frame tale per cui la formula non è vera. Sia $Z \coloneqq V(X) \subseteq S$, con X variabile, tale che $y \notin Z$. Ossia X è falsa nel mondo y. Sia $\{z \in S : (y, z) \in R\} \subseteq Z$, ossia che Z contiene tutti i mondi accessibili da y. Si noti che, dato che $(y, y) \notin R$, allora $y \notin Z$. Allora, il modello $M = (S, R, V)$ soddisfa $M \models_y \Box X$. Questo perché X è vera in tutti i mondi accessibili da y, essendo $Z = V(X)$. Ma $M \not\models_y X$ perché $y \notin Z$.

Se R è riflessiva, ossia $(w, w) \in R \forall w \in S$, allora X è vera per tutti i mondi accessibili da w ed in particolare per w (essendo R riflessiva). Quindi $M \models_w \Box X$ implica $M \models_w X$ per ogni modello su (S, R). □

Questa proposizione offre uno spunto interessante, infatti vedremo che è possibile esprimere alcune proprietà di una relazione, come la simmetria in questo caso, sotto forma di formula in logica modale.

7.2.2 Veridicità e validità

Definizione 111 (Formula vera)**.** *Una formula F si dice vera su un modello M e scriviamo*

$$M \models F$$

se è vera in ogni mondo, ossia

$$M \models_x F \quad \forall x \in S$$

Definizione 112 (Formula valida su un frame)**.** *Una formula F si dice valida su un frame (S, R) e scriviamo*

$$(S, R) \models F$$

se è vera su tutti i modelli su (S, R).

Definizione 113 (Formula valida)**.** *Una formula F si dice valida e scriviamo*

$$\models F$$

se è vera su tutti i frame.

Le tautologie della logica proposizionale sono valide per ogni frame.

7.2.3 Schema di formule

Un altro concetto nuovo rispetto alla logica proposizionale è l'idea di schema di formule.

Definizione 114 (Schema di formule)**.** *Uno schema di formule è una collezione di formule aventi tutte la stessa forma sintattica.*

In uno schema di formule possiamo sostituire una variabile con una qualsiasi altra parola del linguaggio, quindi anche con un'altra formula. Ad esempio, con lo schema

$$\Box F \Rightarrow F$$

intendiamo tutte le formule di questa forma, quindi anche

$$\Box X \Rightarrow X$$

e

$$\Box(\neg\Diamond\neg X) \Rightarrow (\neg\Diamond\neg X)$$

Schemi di formule validi su ogni frame

Lo schema di formule

$$\Box(A \Rightarrow B) \Rightarrow (\Box A \Rightarrow \Box B)$$

è vero su ogni frame. Dato che abbiamo delle implicazioni, ci interessa solo verificare che, quando l'antecedente è vero, allora anche il conseguente lo è. In particolare, vogliamo verificare che, quando sono vere $\Box A$ e $\Box(A \Rightarrow B)$, allora è vera $(\Box A \Rightarrow \Box B)$. Sia (S, R) un frame qualsiasi, M un modello su tale frame e $w \in S$. Assumiamo che

$$M \models_w \Box(A \Rightarrow B)$$

e

$$M \models_w \Box A$$

Con la prima ipotesi, stiamo dicendo che $M \models_v A \Rightarrow B$ per ogni mondo v accessibile da w, ossia $(w, v) \in R$. Nel secondo caso diciamo invece che $M \models_v A$ per ogni mondo v accessibile da w, ossia

$(w, v) \in R$. Ma quindi $M \models_v B$ per ogni mondo v accessibile da w, quindi $M \models_w \Box B$. Abbiamo quindi mostrato

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

7.3 Corrispondenza e non esprimibilità

Un frame (S, R) gode di una certa proprietà se la relazione R del frame gode di quella proprietà. In alcuni casi, la proprietà di un frame equivale ad avere una formula valida sul frame.

7.3.1 Riflessività

Teorema 27 (Riflessività di un frame)**.** *Lo schema*

$$\Box A \Rightarrow A$$

è valido in un frame (S, R) se e solo se R è riflessiva.

La dimostrazione è la stessa della Proposizione 32, infatti abbiamo semplicemente generalizzato il risultato ad uno schema.

7.3.2 Simmetria

Teorema 28 (Simmetria di un frame)**.** *Lo schema*

$$A \Rightarrow \Box\Diamond A$$

è valido in un frame (S, R) se e solo se R è simmetrica.

Proof. Sia R simmetrica, ossia $(x, y) \in R \implies (y, x) \in R$. Sia poi A vera in un mondo w qualsiasi del modello M, ossia $M \models_w A$. Prendiamo poi un elemento $v \in S$ in relazione con w, ossia $(w, v) \in R$. Per ipotesi, essendo R simmetrica, abbiamo anche $(v, w) \in R$. Ma quindi esiste un mondo w accessibile da v per cui è vera A (ricordando che $M \models_w A$) e quindi $M \models_v \Diamond A$ (perché esiste un mondo w, raggiungibile da v in cui A è vera). Questo ragionamento può essere ripetuto per ogni v raggiungibile da w e quindi $M \models_v A$ per ogni v accessibile da w e quindi $M \models_w \Box\Diamond A$.

Assumiamo, viceversa, che sia valido lo schema $A \Rightarrow \Box\Diamond A$ su un frame (S, R). Dato che stiamo considerando uno schema di formule, possiamo prendere A come una variabile. In particolare, sia $X \in Var$ e $V(X) = \{s\}$ con $s \in S$. Sia $t \in S$ tale che $(s, t) \in R$. Quindi $M \models_s X$, perché X vera in s. Dalla validità dello schema segue che $M \models_s \Box\Diamond X$. Ma quindi, per definizione di $\Box$ abbiamo $M \models_t \Diamond X$. Ossia esiste $r \in S$, con $(t, r) \in R$ tale che $M \models_r X$. Ma siccome X era vera solo su s, allora $s = r$ e quindi $(t, s) \in R$. $\Box$

7.3.3 Transitività

Teorema 29 (Transitività di un frame)**.** *Lo schema*

$$\Box A \Rightarrow \Box\Box A$$

è valido sul frame (S, R) se e solo se R è transitiva.

Proof. Sia R transitiva, ossia, per ogni $x, y, z \in S$, se $(x, y) \in R$ e $(y, z) \in R$, allora $(x, z) \in R$. Sia $\Box A$ vera nel mondo w nel modello M, ossia $M \models_w \Box A$. Questo accade se e solo se $M \models_v A$ per ogni mondo $v \in S$ raggiungibile da w, ossia $(w, v) \in R$. Sia ora u un mondo raggiungibile da v, ossia $(v, u) \in R$. A questo punto abbiamo:

$$(w, v) \in R \qquad (v, u) \in R$$

quindi $(w, u) \in R$ per transitività di R. Quindi $M \models_v \Box A$ per ogni $v \in S$ tale che $(w, v) \in R$, ossia $M \models_w \Box\Box A$. Quello che abbiamo detto vale per ogni w, quindi abbiamo $M \models \Box\Box A$.

Assumiamo ora che sia valido lo schema $\Box A \Rightarrow \Box\Box A$ su un frame (S, R). Sia X una variabile e $s \in S$ tale che

$$V(X) = \{w \in S : (s, w) \in R\}$$

ossia vera in tutti i mondi raggiungibili da s. Dato che lo schema è valido, allora

$$M \models_s \Box X$$

perché X è vera in ogni mondo raggiungibile da s, e quindi

$$M \models_s \Box\Box X$$

perché $\Box A \Rightarrow \Box\Box A$. Segue quindi,

$$M \models_t \Box X \quad \forall t \in S, (s, t) \in R$$

ossia

$$M \models_r X \quad \forall r \in S, (t, r) \in R$$

Ma se X è vero su ogni mondo r, allora r deve stare in $V(X)$ (altrimenti non sarebbe vero $M \models_r X$) e quindi $(s, r) \in R$. Sapevamo già che $(s, t) \in R$ e $(t, r) \in R$, quindi aggiungendo $(s, r) \in R$, abbiamo R transitiva. □

7.4 Morfismi di modelli

Un morfismo di modelli è una funzione tra due oggetti del mondo.

7.4.1 Morfismo di frame

Prima di definire un morfismo di modelli, dobbiamo introdurre il concetto di morfismo di frame.

Definizione 115 (Morfismo di frame)**.** *Siano $(S_1, R_1), (S_2, R_2)$ due frame. Una funzione f da S_1 a S_2 è un morfismo di frame se*

$$(x, y) \in R_1 \implies \big(f(x), f(y)\big) \in R_2 \quad \forall x, y \in S$$

Esempio

Ad esempio, siano $(\mathbb{N}, R)$ e $(\mathbb{N}, R)$ due frame, con

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

allora la funzione $f : \mathbb{N} \to \mathbb{N}$ data da

$$n \mapsto n + 1$$

è un morfismo perché rispetta la relazione d'ordine imposta da R (se $n_1 < n_2$, allora anche $n_1 + 1 < n_2 + 1$).

7.4.2 Morfismo di modelli

Grazie alla definizione di morfismo di frame possiamo definire un morfismo di modelli.

Definizione 116 (Morfismo di modelli)**.** *Siano $M_1 \coloneqq (S_1, R_1, V_1)$ e $M_2 \coloneqq (S_2, R_2, V_2)$ due modelli. Un morfismo di frame*

$$f : (S_1, R_1) \to (S_2, R_2)$$

è un morfismo di modelli se:

1. $w \in V_1(X) \iff f(w) \in V_2(X)$
2. $(f(w), y) \in R_2 \Rightarrow \exists v \in S_1 : (w, v) \in R_1, f(v) = y \quad \forall w \in S_1, y \in S_2$

Esempio

Consideriamo ad esempio due modelli

$$M_1 = (\mathbb{N}, R_1, V_1)$$

con

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

e

$$M_2 = (\{0, 1\}, \{0, 1\} \times \{0, 1\}, V_2)$$

Sia inoltre

$$\text{Var} = \{X\}$$

che è vera nei mondi:

$$V_1(X) = \{2n : n \in N\}$$
$$V_2(X) = \{0\}$$

Sia infine

$$f : \mathbb{N} \to \mathbb{N}$$

definita da

$$n \mapsto \begin{cases} 0 & \text{if } n \text{ pari} \\ 1 & \text{if } n \text{ dispari} \end{cases}$$

Mostriamo che f è un morfismo di modelli verificando le proprietà date dalla Definizione 116:

1. Il mondo w sta in $V_1(X)$ se e solo se è pari. Ma $f(n) = 0$ per ogni n pari, quindi w sta in $V_1(X)$ se e solo se $f(n) = 0$ e la proprietà è verificata.
2. $f(w)$ e y possono avere due valori, per un totale di 4 combinazioni, allora proviamo a mostrare la proprietà per ogni combinazione.
   - Se $f(w) = 0$ e $y = 0$, allora $y = f(v) = 0$ significa che v pari. Dato che w è pari possiamo prendere $v = w$, quindi $w \leq w$ e $f(w) = 0 = y$.
   - Se $f(w) = 0$ e $y = 1$, allora $y = f(v) = 1$ significa che v dispari. Dato che w è pari possiamo prendere $v = w + 1$, quindi $w \leq w + 1$ e $f(w + 1) = 1 = y$.
   - Se $f(w) = 1$ e $y = 0$, allora $y = f(v) = 0$ significa che v pari. Dato che w è dispari possiamo prendere $v = w + 1$, quindi $w \leq w + 1$ e $f(w + 1) = 0 = y$.
   - Se $f(w) = 1$ e $y = 1$, allora $y = f(v) = 1$ significa che v dispari. Dato che w è dispari possiamo prendere $v = w$, quindi $w \leq w$ e $f(w) = 1 = y$.

7.4.3 Lemmi

Enunciamo ora una serie di lemmi.

Lemma 3. *Sia*

$$f : (S_1, R_1, V_1) \to (S_2, R_2, V_2)$$

un morfismo tra modelli, allora

$$M_1 \models_w F \iff M_2 \models_{f(w)} F$$

Proof. Dimostriamo il lemma per induzione:

- Se F è una variabile, ossia $F \coloneqq X$, allora $M_1 \models_w F$ se e solo se $w \in V_1(X)$. Dato che f è un morfismo di modelli, per definizione, $w \in V_1(X)$ se e solo se $f(w) \in V_2(X)$ e quindi se e solo se $M_2 \models_{f(w)} F$. In formule:

$$\begin{aligned} M_1 \models_w X &\iff w \in V_1(X) \\ &\iff f(w) \in V_2(X) \\ &\iff M_1 \models_{f(w)} X \end{aligned}$$

- Se $F \coloneqq \neg G$ con G formula ben formata, per ipotesi induttiva abbiamo

$$M_1 \models_w G \iff M_2 \models_{f(w)} G$$

Sia $M_1 \models_w \neg G$, allora

$$M_1 \not\models_w G$$

Ma, per ipotesi induttiva, G è vera in w per M_1 se e solo se G è vera in $f(w)$ per M_2. Quindi, dato che G non è vera in w per M_1, allora non lo è neanche in $f(w)$ per M_2. Otteniamo quindi

$$M_2 \not\models_{f(w)} G$$

ossia

$$M_2 \models_{f(w)} \neg G$$

Lo stesso ragionamento può essere applicato partendo dall'ipotesi $M_2 \models_{f(w)} \neg G$.

- Se $F \coloneqq G_1 \vee G_2$, con G_1, G_2 formule ben formate, per ipotesi induttiva abbiamo

$$M_1 \models_w G_1 \iff M_2 \models_{f(w)} G_1 \quad e \quad M_1 \models_w G_2 \iff M_2 \models_{f(w)} G_2 \quad e \quad \forall w \in S_1$$

Sia $M_1 \models_w F$. Questo è vero se e solo $M_1 \models_w G_1$ o $M_1 \models_w G_2$. Ma per ipotesi induttiva $M_2 \models_{f(w)} G_1$ e $M_2 \models_{f(w)} G_2$ e quindi $M_2 \models_{f(w)} G_1 \vee G_2$. In formule:

$$\begin{aligned} M_1 \models_w G_1 \vee G_2 &\iff M_1 \models_w G_1 \text{ o } M_1 \models_w G_2 \\ &\iff M_2 \models_{f(w)} G_1 \text{ o } M_2 \models_{f(w)} G_2 \\ &\iff M_2 \models_{f(w)} G_1 \vee G_2 \end{aligned}$$

- Se $F \coloneqq G_1 \wedge G_2$, con G_1, G_2 formule ben formate, per ipotesi induttiva abbiamo

$$M \models_w G_1 \iff M \models_{f(w)} G_1 \qquad M \models_w G_2 \iff M \models_{f(w)} G_2 \qquad \forall w \in S_1$$

Sia $M_1 \models_w F$. Questo è vero se e solo $M_1 \models_w G_1$ e $M_1 \models_w G_2$. Ma per ipotesi induttiva $M_2 \models_{f(w)} G_1$ e $M_2 \models_{f(w)} G_2$ e quindi $M_2 \models_{f(w)} G_1 \wedge G_2$. In formule:

$$\begin{aligned} M_1 \models_w G_1 \wedge G_2 &\iff M_1 \models_w G_1 \text{ e } M_1 \models_w G_2 \\ &\iff M_2 \models_{f(w)} G_1 \text{ e } M_2 \models_{f(w)} G_2 \\ &\iff M_2 \models_{f(w)} G_1 \wedge G_2 \end{aligned}$$

- Se $F \coloneqq \Diamond G$, con G formula ben formata. Per ipotesi induttiva abbiamo

$$M_1 \models_w G \iff M_2 \models_{f(w)} G \qquad \forall w \in S_1$$

Sia $M_1 \models_w \Diamond G$. Questo è vero se e solo se esiste un mondo v raggiungibile da w in cui è vera G, ossia

$$\exists v \in S_1 : (w, v) \in R_1, \quad M_1 \models_v G$$

Per definizione di morfismo di frame, abbiamo che $(f(w), f(v)) \in R_2$, visto che $(w, v) \in R_1$. Ma per ipotesi induttiva, dato che $M_1 \models_v G$, allora $M_2 \models_{f(v)} G$. Combinando questi due risultati abbiamo che

$$\exists f(v) \in S_2 : (f(w), f(v)) \in R_2, \quad M_2 \models_{f(v)} G$$

ossia

$$M_2 \models_{f(w)} \Diamond G$$

Sia ora $M_2 \models_{f(w)} \Diamond G$. Questo implica che esiste $y \in S_2$, raggiungibile da $f(w)$, per cui la formula è vera. Per la condizione 2 della definizione di morfismo di frame, se y è raggiungibile da $f(w)$, allora esiste $v \in S_1$ tale che $y = f(v)$ e v è raggiungibile da w. Inoltre, per ipotesi induttiva, $M_1 \models_v G$. Abbiamo quindi che $(f(w), f(v)) \in R_2$, $(w, v) \in R_1$ e $M_1 \models_v G$, dunque

$$\exists v \in S_1 : (w, v) \in R_1, \quad M_1 \models_v G$$

ossia

$$M_1 \models_w \Diamond G$$

- Se $F \coloneqq \Box G$, con G formula ben formata. Per ipotesi induttiva abbiamo

$$M_1 \models_w G \iff M_2 \models_{f(w)} G \qquad \forall w \in S_1$$

Dimostriamo l'implicazione $\implies$. In particolare, mostriamo che, quando il conseguente è falso, allora anche l'antecedente è falso. Sia quindi

$$M_2 \not\models_{f(w)} \Box G$$

Questo significa che esiste un mondo y, raggiungibile da $f(w)$, tale per cui

$$M_2 \not\models_y G$$

Ma per la proprietà 2 della definizione di morfismo di frame, se $(f(w), y) \in R_2$, allora esiste un $v \in S_1$, raggiungibile da w, tale che $y = f(v)$. Quindi abbiamo $(w, v) \in R_1$. Per ipotesi induttiva G è vera in w per il modello M_1 se e solo se G è vera in $f(w)$ per M_2. Ma quindi, se G non è vera in $f(w)$ per M_2, allora non deve esserlo neanche in w per M_1. Possiamo quindi scrivere, unendo questa affermazione e la precedente (ossia $(w, v) \in R_1$):

$$\exists v : (w, v) \in R_1, \quad M_1 \not\models_w G$$

e quindi

$$M_1 \not\models_w \Box G$$

Dimostriamo ora l'implicazione $\impliedby$, mostrando che quando il conseguente è falso, lo è anche l'antecedente. Sia quindi

$$M_1 \not\models_w \Box G$$

ossia, esiste un mondo v, raggiungibile da w, per cui

$$M_1 \not\models_v G$$

Per ipotesi induttiva, se $(w, v) \in R_1$, allora $(f(w), f(v)) \in R_2$. Vediamo ora che $\Box G$ non è vera in $f(v)$ per M_2. Per ipotesi induttiva,

$$M_2 \models_{f(v)} G \iff M_1 \models_v G$$

Ma dato che per ipotesi $M_1 \not\models_v G$, allora deve essere anche

$$M_2 \not\models_{f(v)} G$$

Ma $f(v)$ è raggiungibile da $f(w)$, quindi

$$\exists f(v) \in S_2 : (f(w), f(v)) \in R_2 \qquad M_2 \not\models_{f(v)} G$$

ossia

$$M_2 \not\models_{f(w)} \Box G$$

□

Lemma 4. *Sia*

$$f : (S_1, R_1, V_1) \to (S_2, R_2, V_2)$$

un morfismo di modelli. Se f è suriettivo, allora

$$M_1 \models F \text{ sse } M_2 \models F$$

Proof.

$$\begin{aligned} M_1 \models F \text{ se e solo se } & M_1 \models_w F \ \forall w \in S_1 && \text{Definizione 111} \\ \text{se e solo se } & M_2 \models_{f(w)} F \ \forall w \in S_1 && \text{Lemma 3} \\ \text{se e solo se } & M_2 \models_z F \ \forall z \in S_2 && f \text{ suriettivo} \\ \text{se e solo se } & M_2 \models F \end{aligned}$$

□

Lemma 5. *Sia M_2 modello su (S_2, R_2) e*

$$f : (S_1, R_2) \to (S_2, R_2)$$

un morfismo di frame che soddisfa la condizione 2 della Definizione 116 di morfismo di modelli. Allora esiste M_1 modello su (S_1, R_1) tale che $f : M_1 \to M_2$ sia un morfismo di modelli.

Proof. Definiamo $M_1 \coloneqq (S_1, R_1, V_1)$ con

$$V_1(X) = \{w \in S_1 : M_2 \models_{f(w)} X\} \quad \forall X \in \text{Var}$$

□

Lemma 6. *Sia*

$$f : (S_1, R_1) \to (S_2, R_2)$$

un morfismo di frame che soddisfa la condizione 2 della Definizione 116 di morfismo di modelli. Se f suriettivo, allora

$$(S_1, R_1) \models F \Rightarrow (S_2, R_2) \models F \quad \forall F$$

Proof. Sia $(S_2, R_2) \not\models F$. Allora esiste un modello M_2 su (S_2, R_2) tale che $M_2 \not\models F$. Per il Lemma 5 esiste un modello M_1 su (S_1, R_1) tale che $f : M_1 \to M_2$ è un morfismo di modelli. Poiché f suriettivo, per il Lemma 4, abbiamo $M_1 \not\models F$, quindi $(S_1, R_1) \not\models F$. □

7.4.4 Relazioni non associabili a schemi modali

Prima di proseguire, diamo la definizione di relazione antisimmetrica, che ci servirà poi per ottenere alcuni risultati importanti.

Definizione 117 (Relazione antisimmetrica)**.** *Una relazione $R \subseteq X \times X$ su un insieme X si dice antisimmetrica se*

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

Teorema 30 (Antisimmetria frame)**.** *L'antisimmetria non è esprimibile, ossia non esiste una formula F tale che*

$$(S, R) \models F \text{ se e solo se } R \text{ antisimmetrica}$$

Questo significa che per ogni formula F, o F è vera ma R non è antisimmetrica, o R è antisimmetrica ma F non è vera. Ossia non è possibile trovare uno schema F che è vero quando la relazione R è antisimmetrica.

Proof. Sia $(S_1, R_1) = (\mathbb{N}, \leq)$ e $(S_2, R_2) = (\{0, 1\}, \{0, 1\} \times \{0, 1\})$. Si noti che R_1 è simmetrica ma R_2 no. La funzione $f : \mathbb{N} \to \{0, 1\}$ definita da $n \mapsto n \mod 2$ è un morfismo dal frame (S_1, R_1) al frame (S_2, R_2) che soddisfa la condizione 2 della Definizione 116. La relazione $\leq$ su $\mathbb{N}$ è antisimmetrica. Supponiamo, per assurdo, che esista una formula F come nell'enunciato del teorema. Allora

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

Per il Lemma 6, $(S_2, R_2) \models F$. Per ipotesi (assurda), dato che F è vero per (S_2, R_2) allora R_2 è antisimmetrica, che è falso. □

7.5 Logiche modali normali

Abbiamo già mostrato che lo schema di formule

$$K : \Box(A \Rightarrow B) \implies (\Box A \Rightarrow \Box B)$$

è valido, i.e., $\models K$. Vogliamo ora mostrare che anche lo schema

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

è valido, ossia $\models def_\Diamond$. Per mostrarlo, consideriamo un frame (S, R) e un modello M su (S, R). Sia $w \in S$. Allora

$$M \models_w \Diamond A$$

se e solo se esiste un mondo $v \in S$, raggiungibile da w tale che $M \models_v A$. Poi,

$$M \models_w \neg\Box\neg A$$

se e solo se $M \not\models_w \Box\neg A$, ossia se e solo se esiste un mondo $v \in S$, raggiungibile da w, per cui $M \not\models_v \neg A$. Questo significa che esiste un mondo $v \in S$, raggiungibile da w, per cui $M \models_v A$. Abbiamo quindi mostrato che

$$\models def_\Diamond$$

Definizione 118 (Sostituzione uniforme)**.** *Sia X una variabile e F una formula. La sostituzione uniforme di F al posto X in una formula G, indicata come*

$$G[F/X]$$

è la formula ottenuta da G dove ogni occorrenza di X è sostituita da F.

Definizione 119 (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 $K : \Box(A \Rightarrow B) \Rightarrow (\Box A \Rightarrow \Box B)$.*
3. *Γ contiene tutte le istanze dello schema $def_{\Diamond} : \Diamond A \iff \neg\Box\neg A$.*
4. *Γ è chiuso sotto modus ponens, ossia se $A \in \Gamma$ e $A \Rightarrow B \in \Gamma$, allora $B \in \Gamma$.*
5. *Γ è chiuso sotto necessitazione, ossia se $A \in \Gamma$, allora $\Box A \in \Gamma$.*
6. *Γ è chiuso sotto sostituzione uniforme, ossia se $A \in \Gamma$ e $B \in \Gamma$, allora $A[B/X] \in \Gamma$.*

7.5.1 Logica modale K

Definizione 120 (Logica modale K)**.** *La logica modale K è definita dai seguenti schemi di assiomi e regole:*

1. *Assiomi:*
   - *Le tautologie della logica proposizionale.*
   - *$K : \Box(A \Rightarrow B) \Rightarrow (\Box A \Rightarrow \Box B)$*
   - *$def_{\Diamond} : \Diamond A \iff \neg\Box\neg A$*
2. *Regole di inferenza:*
   - *Modus ponens.*
   - *Necessitazione.*
   - *Sostituzione uniforme.*

Definizione 121 (Dimostrazione)**.** *Data una logica modale L, una dimostrazione in L è una successione finita di formule tali che ognuna di esse è un assioma o è ottenuta dalle formule precedenti della successioni via applicazione di una delle regole di inferenza.*

Definizione 122 (Teorema)**.** *Una formula F si dice teorema di L, e scriviamo*

$$\vdash_L F$$

se e solo se esiste una dimostrazione in L la cui ultima formula è F.

Teorema 31. *L'insieme*

$$\{F : \vdash_K F\}$$

dei teoremi della logica K è chiuso sotto sostituzione uniforme.

Proof. Vogliamo mostrare che, dati due teoremi F_1 e F_2, il teorema ottenuto da F_1 sostituendo ogni istanza della variabile X con F_2, è un teorema a sua volta. In formule

$$F_1[F_2/X] \in \{F : \vdash_K F\}$$

Per definizione di logica K, sappiamo che $F_1[F_2/X]$ appartiene alle formule della logica. Dobbiamo ora dimostrare che è anche un teorema. □

Nelle logiche epistemiche, si estende la logica K aggiungendo lo schema di assiomi

$$\Box F \Rightarrow F$$

ossia, *se si sa che F, allora vale F* che non vogliamo come assioma di una logica deontica, infatti se F è obbligatorio, non è detto che valga F.

Chapter 8

Logiche multimodali

8.1 Connettivi n-ari

Fino ad ora abbiamo visto connettivi unari, ossia che possono essere applicati ad una sola formula. Consideriamo ora connettivi che possono essere applicati a più formule. Le logiche, estese dalla logica modale, che usano connettivi n-ari prendono il nome di logiche multimodali. Più precisamente, andiamo ad aggiungere alla logica modale

- Diversi connettivi modali 1-ari
$$\Box_1, \Box_2, \Box_3, \ldots, \Box_i$$
- Connettivi modali n-ari, ossia che vengono applicati su più formule
$$\Box(F_1, F_2, \ldots, F_n)$$

Questi connettivi hanno diverso significato, a seconda della logica modale che consideriamo. Ad esempio, nella logica epistemica, i connettivi 1-ari $\Box_i$ vengono interpretati come *la persona i sa che una formula F è vera*.

8.1.1 Semantica dei connettivi n-ari

Avendo introdotto un nuovo tipo di connettivo, applicato su più formule, dobbiamo definirne la semantica. Si noti che lo stesso non vale per $\Box_i$ dato che la semantica è uguale a quella della logica modale, ma stiamo solo considerando agenti diversi.

Per interpretare $\Box(F_1, F_2, \ldots, F_n)$ dobbiamo definire, invece che una relazione binaria sui mondi, una relazione $n+1$-aria. In particolare,

Definizione 123 (Connettivi n-ari veri in un mondo)**.** *Sia S un insieme di mondi e R una relazione*
$$R \subseteq \underbrace{S \times S \times \cdot \times S}_{n+1 \text{ volte}}$$
Sia M un modello su (S, R) e $w \in S$. Allora diciamo che
$$M \models_w \Box(F_1, \ldots, F_n)$$

se e solo se

$$\forall v_1 \in S, v_2 \in S, \ldots, v_n \in S : (w, v_1, v_2, \ldots, v_n) \in R$$

si ha che

$$M \models_{v_1} F_1, M \models_{v_2} F_2, \ldots M \models_{v_n} F_n$$

Questa, in realtà, è una delle possibili definizioni di soddisfacibilità. In particolare, noi abbiamo applicato il connettivo $\Box$ ad ogni formula, ma in realtà potremmo definire connettivi n-ari che si comportano diversamente per ogni formula. Ad esempio un operatore può comportarsi come $\Box$ nella prima formula e come $\Diamond$ nella seconda. In questo caso, basta applicare, ad ogni formula, la definizione (110) di formula vera in un mondo del corrispondente connettivo. Quindi, nel nostro esempio, applichiamo alla prima formula la definizione di verità di $\Box$ in un mondo e alla seconda la definizione di verità di $\Diamond$ in un mondo.

8.2 Logiche LTL (Linear-time Temporal Logic)

Le logiche LTL, che sono logiche multimodali, descrivono stati di un sistema nel tempo. Parliamo di logiche al plurale perché dipendono dal frame che consideriamo.

8.2.1 Sintassi

Le logiche LTL utilizzano tre connettivi modali 1-ari

- **X**, che sta per *neXt state*, quindi questo connettivo indica che una formula vale nello stato successivo allo stato che stiamo considerando.
- **F**, che sta per *some Future state*, quindi questo connettivo indica che una formula è vera per qualche istante successivo rispetto a quello che stiamo considerando.
- **G**, che sta per *all future states, Globally*, quindi questo connettivo indica che una formula è vera in tutti gli stati futuri.

e tre connettivi modali binari

- **U**, che sta per *Until*, quindi questo connettivo indica che una formula ϕ vale fino a che non vale un'altra formula ψ.
- **W**, che sta per *Weak until*.
- **R**, che sta per *Release*.

In realtà, i connettivi binari possono essere scritti in relazione agli altri, ma torna comunque comodo definirli comunque.

8.2.2 Semantica

Prima di definire la semantica della logica LTL, abbiamo bisogno delle seguenti definizioni.

Definizione 124 (Chiusura transitiva)**.** *Sia S un insieme e $R \in S \times S$ una relazione binaria, la chiusura transitiva di R è*

$$R^t = R \cup \{(s_1, s_{n+1}) : \exists s_2, \ldots, s_n \in S : (s_i, s_{i+1}) \in R \forall i = 1, \ldots, n\}$$

Definizione 125 (Chiusura riflessiva)**.** *Sia S un insieme e $R \in S \times S$ una relazione binaria, la chiusura riflessiva di R è*

$$R^r = R \cup \{(x, x) : x \in S\}$$

Definizione 126 (Formula LTL vera in un mondo)**.** *Sia (S, R) un frame tale che $R \subseteq S \times S$ non sia riflessiva. Sia R^* la chiusura riflessiva e transitiva in R. Allora,*

1. *X è il connettivo modale $\Box$ sul frame (S, R). Quindi $M \models_w X\phi$ significa che X vale su tutti i mondi (i.e., stati) successivi a w.*
2. *G è il connettivo modale $\Box$ sul frame (S, R^*). Quindi $M \models_w G\phi$ significa che X vale su tutti i mondi (i.e., stati) successivi a w e anche in w (grazie alla chiusura riflessiva).*
3. *F è il connettivo modale $\Diamond$ sul frame (S, R^*). Dato che possiamo sempre scrivere il connettivo $\Diamond$ in termini di $\Box$ ($\Diamond F = \neg\Box\neg F$), allora possiamo anche scrivere*

   $$F\phi = \neg G\neg\phi \quad \forall\phi$$

   Quindi, la formula ϕ vale per qualche stato futuro del sistema.
4. *Scriviamo $M \models_w U(\phi, \psi)$ se e solo se*
   (a) *esiste uno stato $z \in S$ tale che $(w, z) \in R^*$ e $M \models_z \psi$.*
   (b) *$M \models_y \phi$ per ogni $y \in S$ tale che $(w, y) \in R^*$, $(y, z) \in R^*$ e $y \neq z$.*

   In pratica, ϕ vale sicuramente fino all'ultimo istante in cui non vale ψ, poi ϕ potrebbe valere ancora oppure no.
5. *Scriviamo $M \models_w W(\phi, \psi)$ se e solo se $U(\phi, \psi)$ o $G\phi$. In pratica, ϕ o vale sicuramente fino all'ultimo istante in cui non vale ψ oppure vale sempre.*
6. *Scriviamo $M \models_w W(\phi, \psi)$ se e solo se $\neg U(\neg\phi, \neg\psi)$. In pratica, ϕ o vale sicuramente fino all'ultimo istante in cui non vale ψ oppure vale sempre.*

Si noti che gli unici connettivi modali necessari per definire una logica LTL sono X, G e U perché gli altri possono essere espressi tramite questi ultimi.

8.3 Logiche CTL (Computation Tree Logic)

Le logiche CTL introducono quantificatori per i cammini da uno stato ad un altro di un sistema.

8.3.1 Sintassi

Le logiche CTL estendono la logica modale aggiungendo i seguenti connettivi unari:

- **AX** e **EX**.
- **AF** e **EF**.
- **AG** e **EG**.

e i connettivi binari:

- **AU** ed **EU**.
- **AW** ed **EW**.
- **AR** ed **ER**.

La sintassi e simile a quella vista nelle logiche LTL, con la differenza che ogni connettore è sdoppiato. In particolare, viene aggiunta una lettera prima di ogni connettore il cui significato è:

- *per ogni percorso* (*along All paths*) quando usiamo la lettera A.
- *esiste un cammino* (*Exists at least a path* o *along at least a path*) quando usiamo la lettera E.

8.3.2 Semantica

Analizziamo ora la semantica dei connettivi appena aggiungi.

Definizione 127 (Formula CTL vera in un mondo)**.** *Sia (S, R) un frame tale che $R \subseteq S \times S$ non sia riflessiva. Sia R^* la chiusura riflessiva e transitiva in R. Allora,*

1. *Scriviamo $M \models_w AX\phi$ se e solo se, per ogni stato $s \in S$ successivo a w, abbiamo $M \models_s \phi$. AX si comporta quindi come $\Box$ in (S, R).*
2. *Scriviamo $M \models_w EX\phi$ se e solo se, esiste $s \in S$ successivo a w per cui $M \models_s \phi$. EX si comporta quindi come $\Diamond$ in (S, R).*
3. *Scriviamo $M \models_w AG\phi$ se e solo se, per ogni stato $s \in S$ raggiungibile da w (ossia con $(w, s) \in R^*$), abbiamo $M \models_s \phi$. AG si comporta quindi come $\Box$ in (S, R^*).*
4. *Scriviamo $M \models_w EG\phi$ se e solo se, esiste esiste un cammino $w \to s_1 \to s_2 \to \cdots \to s_f$ tale che $M \models_{s_i} \phi$ per tutti gli i del cammino.*
5. *Scriviamo $M \models_w EU(\phi, \psi)$ se e solo se esiste un cammino $w \to s_1 \to s_2 \to \cdots \to s_f$ tale che $M \models_{s_i} U(\phi, \psi)$ su questo cammino.*

Gli altri connettivi possono essere definiti a partire da quelli definiti sopra.

8.4 Logiche CTL*

Le logiche CTL* contengono le logiche LTL e CTL. Questo significa che le logiche CTL hanno i connettivi modali sia delle logiche LTL (ossia X, F, G ed U) che quelli delle logiche CTL (ossia AX, EX, AF, EF, AG, EG, AU, EU) e aggiungono i quantificatori:

- **A** che indica *per ogni cammino.*
- **E** che indica *esiste un cammino.*

Possiamo dire che le logiche CTL* sono logiche modali predicative.

Consideriamo ora le seguente affermazione: *su tutti i cammini in cui appare la formula ϕ, appare la formula ψ.* In logica LTL possiamo scrivere questa formula come

$$F\phi \Rightarrow F\psi$$

La stessa affermazione non può essere espressa in CTL.

L'affermazione *c'è un cammino in cui ϕ appare infinite volte* può essere espressa in CTL* come

$$A(GF\phi)$$

ossia esiste un cammino in cui ogni stato futuro ha un cammino in cui appare ϕ. Si noti che non volgiamo che ϕ valga sempre nel cammino, ma solo che sia vera infinite volte (e quindi in alcuni stati potrebbe essere falsa). Questa affermazione non può essere espressa in LTL perché non è presente il quantificatore E. L'affermazione non può essere espressa neanche in CTL perché abbiamo i connettori EF e EG, ma non il solo connettore E.

8.5 Model checking

Vediamo ora come applicare praticamente le logiche multimodali.

8.5.1 Sezioni critiche

In un sistema con molti processi contemporaneamente in esecuzione potrebbe essere necessario assicurare che questi processi non accedano ad una risorsa nello stesso istante. Ad esempio potremmo volere che una variabile venga scritta da un solo processo per volta. Le condizioni, come quella appena descritta, che devono essere vere nel sistema possono essere specificate come formule della logica multimodale.

Le parti di codice in cui una risorsa può essere modificata o letta da un solo processo prendono il nome di sezioni critiche.

Consideriamo, ad esempio due processi e le variabili

- n_i che rappresentano: il processo i non è in uno stato critico.
- c_i che rappresentano: il processo i è in uno stato critico.
- t_i che rappresentano: il processo i chiede di accedere ad uno stato critico.

Consideriamo ora il frame in Figura 8.1 e immaginiamo di voler forzare la condizione di sicurezza, ossia che due processi non possono stare contemporaneamente in uno stato critico. Questa condizione può essere espressa con la seguente formula della logica LTL:

$$G\neg(c_1 \wedge c_2)$$

e quindi deve valere

$$M \models_{s_0} G\neg(c_1 \wedge c_2)$$

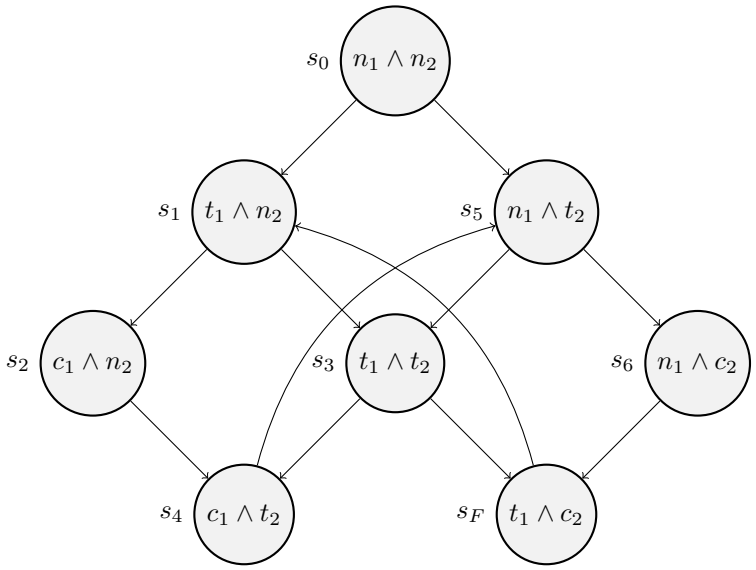


Figure 8.1: Il frame che rappresenta gli stati di un sistema con due processi.

Un'altra proprietà che si potrebbe voler soddisfare è la vitalità, ossia che ogni volta che un processo vuole entrare in una sezione critica, questo gli sarà concesso, in qualche momento nel futuro. Questa proprietà è esprimibile con la formula della logica CTL

$$\phi = (AFt_1 \Rightarrow EFc_1) \wedge (AGt_2 \Rightarrow EFc_2)$$

e quindi si vuole verificare

$$M \models_{s_0} \phi$$

Definite le proprietà che ci interessa soddisfare, possiamo verificare se il frame in Figura 8.1 le soddisfa. In questo caso possiamo verificarlo a mano, ma per sistemi più complessi questo è impossibile. Fortunatamente, esistono tool automatici, chiamati model checkers, che, dato un frame e un insieme di formule, permettono di verificare la validità di tali formule. Un esempio è *NuSMV* (New Symbolic Model Checker).

Definizioni

Teoremi

Proposizioni