Appunti di Algebra

Michele Laurenti
asmeikal@me.com

21 Luglio 2015

Indice

I Algebra **2**

1 Nozioni e concetti fondamentali **3**
1.1 Insiemi . . . 3
1.1.1 Proprietà delle funzioni . . . 4
1.2 Relazioni su un insieme . . . 5
1.2.1 Diagramma di Hasse . . . 7
1.2.2 INF e SUP . . . 8
1.3 Reticoli . . . 9
1.3.1 Teorema di dualità . . . 11
1.4 Partizioni di A . . . 12
1.4.1 Classi di equivalenza . . . 12
1.4.2 Congruenza modulo n su $\mathbb{Z}$ . . . 13
1.4.3 Relazioni di equivalenza e partizioni . . . 13
1.4.4 Teorema di omomorfismo per gli insiemi . . . 16
1.5 Morfismi . . . 18
1.5.1 Morfismi di insiemi parzialmente ordinati . . . 18
1.5.2 Morfismi di reticoli . . . 19
1.5.3 Isomorfismi . . . 20
1.6 Numeri Naturali . . . 22
1.6.1 Iterazioni . . . 22
1.6.2 Operazioni su $\mathbb{N}$ . . . 23
1.6.3 Ordine naturale su $\mathbb{N}$ . . . 24
1.6.4 Altre forme del principio di induzione . . . 25
1.7 Principi del calcolo combinatorio . . . 25
1.7.1 Principio della somma . . . 25
1.7.2 Principio del prodotto . . . 26
1.7.3 Dimostrazioni biettive . . . 27
1.7.4 Fattoriale decrescente . . . 28
1.7.5 Coefficienti binomiali . . . 29
1.7.6 Teorema binomiale . . . 30
1.7.7 Coefficienti multinomiali . . . 30
1.7.8 Teorema multinomiale . . . 32
1.7.9 Principio dei cassetti . . . 32
1.7.10 Principio di inclusione/esclusione . . . 34
1.7.11 Numeri di Stirling di prima e seconda specie . . . 34
1.7.12 Anagrammi . . . 36

2 Strutture algebriche **40**

2.1 Strutture algebriche con un'operazione . . . 40
2.1.1 Classificazione delle strutture algebriche con una operazione . . . 41
2.1.2 Gruppo simmetrico . . . 41
2.2 Monoidi . . . 42
2.2.1 Morfismi di monoidi . . . 42
2.2.2 Teorema di omomorfismo per i monoidi . . . 42
2.2.3 Potenze (iterazioni sui monoidi) . . . 43
2.2.4 Congruenze . . . 44
2.3 Gruppi . . . 45
2.3.1 Sottogruppi . . . 45
2.3.2 Morfismi di gruppi . . . 46
2.3.3 Nucleo di un morfismo di gruppi . . . 47
2.3.4 Teorema di omomorfismo per i gruppi . . . 48
2.3.5 Classi laterali . . . 51
2.3.6 Permutazioni come cicli . . . 54
2.3.7 Trasposizioni . . . 56
2.4 Strutture algebriche con due operazioni . . . 60
2.4.1 Anelli . . . 60
2.4.2 Teorema di divisione . . . 61
2.4.3 Minimo comune multiplo e massimo comun divisore . . . 62
2.4.4 Algoritmo di Euclide per il calcolo del MCD . . . 63
2.4.5 Anello degli interi . . . 65
2.4.6 Anello degli interi modulo n intero . . . 66
2.4.7 Funzione di Eulero . . . 69
2.4.8 Equazioni di primo grado in $\mathbb{Z}_n$ . . . 71
2.4.9 Equazioni diofantee . . . 75
2.4.10 Strutture algebriche e reticoli . . . 77
2.4.11 Gruppi ciclici . . . 80
2.4.12 Morfismo di anelli . . . 82
2.4.13 Morfismo di campi . . . 82
2.4.14 Teorema di omomorfismo per gli anelli . . . 83
2.4.15 Anello dei polinomi . . . 83
2.4.16 Teorema di divisione in $\mathbb{K}[x]$ . . . 84
2.5 Matrici . . . 85
2.5.1 Gruppo delle matrici m per n . . . 85
2.5.2 Anello delle matrici quadrate . . . 86

II Algebra lineare **91**

3 Spazi vettoriali **92**
3.1 Spazi vettoriali su un campo $\mathbb{K}$ . . . 92
3.1.1 Sottospazi vettoriali . . . 94
3.1.2 Reticolo dei sottospazi vettoriali . . . 95
3.1.3 Combinazioni lineari e indipendenza lineare . . . 96
3.1.4 Esempi di combinazioni lineari . . . 97
3.1.5 Indipendenza lineare . . . 99
3.1.6 Caratterizzazione degli insiemi indipendenti . . . 100
3.1.7 Base di uno spazio vettoriale . . . 101

3.1.8 Caratterizzazione delle basi . . . 102

4 Applicazioni lineari **105**
4.1 Applicazione lineari . . . 105
4.1.1 Teorema di omomorfismo per gli spazi vettoriali . . . 105
4.1.2 Basi e applicazioni lineari . . . 108
4.1.3 Isomorfismi fra spazi vettoriali . . . 108
4.1.4 Analogia tra cardinalità e dimensione . . . 110
4.2 Rappresentazione di applicazioni lineari (con matrici) . . . 111
4.2.1 Spazio vettoriale delle applicazioni lineari . . . 117
4.2.2 Altre proprietà delle applicazioni lineari come matrici . . . 117
4.3 Cambiamento di base . . . 118
4.4 Diagonalizzazione . . . 119
4.4.1 Criterio di diagonalizzazione . . . 124

5 Risoluzione di sistemi lineari **129**
5.1 Sistemi lineari . . . 129
5.2 Matrici a scala . . . 129
5.3 Risoluzione dei sistemi lineari . . . 130
5.4 Risoluzione con il metodo di Gauss . . . 131
5.4.1 Calcolo del rango per righe di A con il metodo di Gauss . . . 131
5.5 Matrici invertibili . . . 134
5.5.1 Caratterizzazione delle matrici invertibili . . . 135
5.6 Determinante di una matrice . . . 136
5.6.1 Regola di Laplace per il calcolo del determinante . . . 136
5.6.2 Proprietà del determinante . . . 137
5.6.3 Calcolo della matrice inversa di una matrice A . . . 138

6 Esercizi ed esempi **141**

Sommario

I riferimenti a teoremi, proposizioni, proprietà e altro sono ipertestuali (ci puoi clickare). Anche altri elementi del pdf lo sono, come i siti internet indicati di seguito, l'indice, o la mia mail in prima pagina.

Il sito della professoressa Venezia è: `http://twiki.di.uniroma1.it/twiki/view/Algebra/MZ/WebHome`.

Gli appunti non sono privi di errori. Non farci troppo affidamento. Se ne trovi, dimmelo.

Parte I

Algebra

Capitolo 1

Nozioni e concetti fondamentali

Insiemi, relazioni, funzioni, numeri naturali e principio di induzione, calcolo combinatorio.

1.1 Insiemi

L'insieme è un concetto primitivo senza definizione. Ma definiamo come si fa ad assegnare un insieme. Il modo più semplice è quello di elencarne gli elementi.

$$A = \{\text{giallo}, \text{rosso}, \text{blu}\}$$

Un altro modo è definendo una proprietà.

$$A = \{x \in X : P(x)\}$$

Un insieme fondamentale è quello delle coppie ordinate. A, B insiemi. $A \times B =$ insieme delle coppie ordinate.

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

C'è una differenza fondamentale fra insiemi e coppie ordinate.

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$$
$$\{a, b\} = \{c, d\} \Leftrightarrow (a = c \wedge b = d) \vee (a = d \wedge b = c)$$

Il concetto può essere generalizzato da coppie a terne, quaterne, e in generale n-uple.

Una relazione binaria tra due insiemi è un sottonisieme di $A \times B$. Il prodotto cartesiano non è associativo, ma i due insiemi $A \times B$ e $B \times A$ hanno la stessa cardinalità.

Una funzione da un'insieme A ad un insieme B è una terna (A, B, f), indicata tipicamente con $f : A \to B$, dove A si dice Dominio, B si dice Codominio, ed f è una relazione ($f \subseteq A \times B$) tale che $\forall\ a \in A\ \exists$ un solo $b \in B$ t.c. $(a, b) \in f$, ossia tale per che $b = f(a)$.

Esiste una funzione da $A = \emptyset$ a $B \neq \emptyset$? Sì, la funzione $(\emptyset, B, \emptyset)$. Viceversa, una funzione da $A \neq \emptyset$ a $B = \emptyset$ non esiste.

$$R_1 = \left\{(m, n) \in \mathbb{N}^2 : m = n^2\right\}$$

Non è una funzione. Perché?

$$R_2 = \left\{(r, s) \in \mathbb{R}^+ \times \mathbb{R} : r = s^2\right\}$$

Non è una funzione. Perché?

$$R_3 = \left\{(r, s) \in \mathbb{R}^+ \times \mathbb{R}^+ : r = s^2\right\}$$

È una funzione. Perché?

Definizione 1.1.1 (*Uguaglianza tra funzioni*)

Due funzioni sono uguali solo se coincidono come terne.

Per definire una funzione bisogna definire l'insieme del Dominio, definire l'insieme del Codominio, e una relazione che gode della proprietà che ogni elemento del dominio ha una sola immagine.

Sia $f : A \to B$ una funzione, si indica con Im_f l'immagine di f.

$$Im_f = \{b \in B : \ \exists\ a \in A \text{ t.c. } f(a) = b\}$$

$$f : \mathbb{N} \to \mathbb{N} \text{ t.c. } \ \forall\ n \in \mathbb{N}\ f(n) = \begin{cases} n-1 & \text{se } n \text{ è pari} \\ n+1 & \text{se } n \text{ è dispari} \end{cases}$$

Non è una funzione perché lo zero non ha immagine.

$$f : \mathbb{R} \to \mathbb{R} \text{ t.c. } \ \forall\ r \in \mathbb{R}\ f(r) = \begin{cases} r^2+1 & \text{se r} \leq 0 \\ r & \text{se r} \geq 0 \end{cases}$$

Non è una funzione perché lo zero ha due immagini.

1.1.1 Proprietà delle funzioni

Suriettiva Ogni elemento di B è immagine di un elemento di A, ossia $Im_f = B$.

Iniettiva Due elementi diversi di A non hanno la stessa immagine.

È più facile dimostrare l'iniettività di una funzione in un altro modo.

f è iniettiva $\Leftrightarrow a, a' \in A$, se $f(a) = f(a')$ allora $a = a'$.

Una funzione iniettiva e suriettiva è detta "biunivoca".

$$f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \text{ t.c. } f(x, y) = \sqrt{2}x + y$$

Non è iniettiva, perché $(1, 0)$ e $(0, \sqrt{2})$ hanno la stessa immagine. È suriettiva. Per l'immagine:

$$\forall\ r \in \mathbb{R}\ \exists\ (x, y) \in \mathbb{R} \times \mathbb{R} \text{ t.c. } f(x, y) = \sqrt{2}x + y = r$$

Infatti basta scegliere $(0, r)$ e $f(0, r) = r$.

Determiniamo le immagini della funzione per i domini dati.

$$A = \left\{ \left(a, -\sqrt{2}a \right) : a \in \mathbb{R} \right\}$$
$$f(A) = \left\{ r \in \mathbb{R} : \ \exists \ (a, -\sqrt{2}a) \text{ t.c. } f(a, -\sqrt{2}a) = r \right\} = \{0\}$$

$$C = \left\{ (a, \sqrt{2}b) : a, b \in \mathbb{Z} \right\}$$
$$f(C) = \left\{ r \in \mathbb{R} : \ \exists \ (a, \sqrt{2}b) \text{ t.c. } f(a, \sqrt{2}b) = r \right\}$$
$$r = f(a, \sqrt{2}b) = \sqrt{2}a + \sqrt{2}b = \sqrt{2}(a + b)$$
$$(a + b) \in \mathbb{Z}$$
$$r \in \sqrt{2}\mathbb{Z} = \left\{ z \in \mathbb{R} : z = \sqrt{2} \cdot t \text{ con } t \in \mathbb{Z} \right\}$$

L'insieme delle funzioni da A in B si indica con B^A. Questo insieme verifica tutte le proprietà delle potenze. Alla somma corrisponde l'unione, al prodotto corrisponde il prodotto cartesiano. Inoltre $|B| = m$, $|A| = n$, $\left|B^A\right| = m^n$.

Composizione

Date le funzioni $f : A \to B$ e $g : B \to C$, la composizione di f e g ("f composto g") è una funzione $g \circ f : A \to C$ definita come:

$$\forall \ a \in A, \ g \circ f(a) = g(f(a))$$

L'operazione di composizione è una funzione $\circ : B^A \times C^B \to C^A$.

Inversa destra Data $f : X \to Y$, $g : Y \to X$ è un'inversa destra se $f \circ g = id_Y$ (funzione identità)

Inversa sinistra Data $f : X \to Y$, $g : Y \to X$ è un'inversa destra se $g \circ f = id_X$

1.2 Relazioni su un insieme

Una relazione su un insieme A è un sottoinsieme $R \subseteq A \times A$. I tipi di relazioni su un insieme sono due:

Relazioni d'ordine Si indica con $\leq$, $a \leq b$ indica che a è in relazione con b. Proprietà:

Riflessiva $\forall \ x \in A : x \leq x$

Antisimmetrica $\forall \ x, y \in A$ se $x \leq y$ e $y \leq x \Rightarrow x = y$

Transitiva $\forall \ x, y, z \in A$ se $x \leq y$ e $y \leq z \Rightarrow x \leq z$

Relazioni di equivalenza Si indica con ε, $a \varepsilon b$ indica che a è in relazione con b. Proprietà:

Riflessiva (vedi sopra), posso scriverla anche come $\forall \ a \in A \ \exists \ x \in A : a \varepsilon x$

Simmetrica $x \varepsilon y \Rightarrow y \varepsilon x$.

Transitiva (vedi sopra)

Le tre proprietà di una relazione d'ordine (riflessiva, antisimmetrica e transitiva) sono *indipendenti*, ossia nessuna proprietà deriva dalle altre. Per dimostrarlo, forniamo degli esempi.

- Antisimmetrica e transitiva, ma non riflessiva: $x \leq y \Leftrightarrow x \neq y$. *A me sembra sia invece simmetrica e transitiva.* $x \leq y \Leftrightarrow x < y$ *è antisimmetrica e transitiva, essendo una relazione di ordine stretto.*
- Riflessiva e transitiva, ma non antisimmetrica: definita su $A = \{\text{insieme di persone}\}$, $aRb \Leftrightarrow a$ ha la stessa età di b.
- Riflessiva e antisimmetrica, ma non transitiva: definita su $\mathbb{N}$, $x\ R\ y \Leftrightarrow x - y \leq 2$. *Non è antisimmetrica, prendendo 1 e 2 sono* $1\ R\ 2$ *e* $2\ R\ 1$.

Esercizio 1

Trovare altri esempi.

Anche le proprietà delle relazioni d'equivalenza sono indipendenti. Potrebbe sembrare che la proprietà riflessiva sia conseguenza della proprietà simmetrica e della proprietà transitiva.

$$x \varepsilon y \Rightarrow y \varepsilon x \text{ per la proprietà simmetrica}$$
$$x \varepsilon y, y \varepsilon x \Rightarrow x \varepsilon x \text{ per la proprietà transitiva}$$

L'errore è che $x \varepsilon y$ non è dato *per ogni* x: la relazione è riflessiva se $\forall\ x \in A\ \exists\ y : x \varepsilon y \Leftrightarrow$ la relazione è riflessiva.

Altri esempi di relazioni con solo alcune delle proprietà delle relazioni d'ordine:

- Relazione transitiva e simmetrica, ma non riflessiva:

$$(m, n) \in \mathbb{N} \times \mathbb{N},\ (m, n) R (p, q) \Leftrightarrow \frac{m}{p} = \frac{n}{q}$$

  La coppia $(m, 0)$ non è in relazione con nessuno se $m \neq 0$.
- Relazione riflessiva e transitiva, ma non simmetrica: una qualsiasi relazione d'ordine (essendo tutte antisimmetriche).
- Relazione riflessiva, simmetrica ma non transitiva: dato l'insieme delle rette nello spazio euclideo, $rRs \Leftrightarrow r$ è complanare a s ($r // s$ - r parallela ad s - oppure $r \cap s = \{P\}$ - si incontrano in un punto).

Esercizio 2

Verificare le proprietà delle seguenti relazioni.
- *Parallelismo tra rette dello spazio*
- $\mathbb{N} \times \mathbb{N}, (m, n) \rho (p, q) \Leftrightarrow (m + q) = (p + n)$, *ossia* $m - n = p - q$.
- $a, b \in \mathbb{Z}, a \equiv_n b \Leftrightarrow n \mid (a - b) \Leftrightarrow (a - b) = kn$ *(congruenza modulo* $n \in \mathbb{N}, n \geq 2$*)*
- *Data una funzione* $f : A \to B$, $\varepsilon_f =$ *è relazione di equivalenza individuata da* f*, detta "nucleo di* f*". È una relazione su* A *t.c.* $a, a' \in A, a \varepsilon_f a' \Leftrightarrow f(a) = f(a')$.

Data una relazione $R \subseteq A \times B$, possiamo definire R^*, la relazione duale di R. Due elementi $(a, b) \in A \times B$ sono $a\ R^*\ b \Leftrightarrow b\ R\ a$. Ad esempio, se A è un insieme di persone e R è la relazione a figlio di b, la relazione duale è R^* per cui b è genitore di a.

La duale di una relazione d'ordine è ancora una relazione d'ordine, e viene tipicamente indicata con $\geq$.

La coppia $(P, \leq)$ data dall'insieme $P \neq \emptyset$ con una relazione d'ordine $\leq$ si dice insieme parzialmente ordinato.

Definizione 1.2.1 (*Insieme totalmente (linearmente) ordinato*)

Se $\forall\, x, y \in P$ e si ha che $x \leq y \vee y \leq x$, $(P, \leq)$ si dice linearmente ordinato (o totalmente ordinato).

L'insieme dei numeri naturali $\mathbb{N}$ con la relazione d'ordine naturale $(\mathbb{N}, \leq)$ è totalmente ordinato. Ma possiamo prendere anche l'insieme dei numeri naturali con la relazione di divisibilità $(\mathbb{N}, \mid)$, ossia $m \mid n \Leftrightarrow m$ divide $n \Leftrightarrow \exists\, k \in \mathbb{N}$ tale per cui $n = k \cdot m$. Rispetto a questa relazione d'ordine, $\mathbb{N}$ non è totalmente ordinato.

L'insieme delle parti di un insieme Γ qualunque con la relazione "è sottoinsieme di" $(\mathbb{P}(\Gamma), \subseteq)$ è un insieme parzialmente ordinato.

Come si costruisce in modo naturale una relazione su un prodotto cartesiano? Ad esempio, prendo la relazione d'ordine naturale sui reali $(\mathbb{R}, \leq)$, e voglio definire naturalmente la relazione d'ordine $(\mathbb{R}^2, \leq)$, ho che $(a, b) \leq (c, d) \Leftrightarrow a \leq c \wedge b \leq d$.

$$B = \{n \in \mathbb{N} : n = 2^r \cdot 3^s \text{ con } r, s \in \mathbb{N}\}$$

Definisco ρ su B come $2^r \cdot 3^s \leq 2^t \cdot 3^u \Leftrightarrow r \leq t \wedge s \leq u$. È una relazione d'ordine parziale. Perché?

Definizione 1.2.2 (*Ordine naturale sul prodotto cartesiano*)

Dati due insiemi parzialmente ordinati $(P_1, \leq_1)$ e $(P_2, \leq_2)$, posso definire naturalmente una relazione d'ordine sul prodotto dei due insiemi $(P_1 \times P_2, \leq)$ come:

$$(x_1, x_2) \leq (y_1, y_2) \Leftrightarrow x_1 \leq_1 y_1 \wedge x_2 \leq_2 y_2$$

Si può generalizzare anche a $(P^n, \leq)$, prendendo le n-uple al posto delle coppie.

Definizione 1.2.3 (*Ordine fra funzioni*)

Se prendo un insieme parzialmente ordinato $(P, \leq)$ e un insieme qualsiasi A, posso definire una relazione su $(P^A, \leq)$ (ricordando che P^A è l'insieme di tutte le funzioni da A a P). Come faccio a dire che date $f, g \in P^A$ $f \leq g$? Se $\forall\, a \in A$ $f(a) \leq g(a)$.

1.2.1 Diagramma di Hasse

Dato un insieme e una relazione di ordine parziale su di esso $(A, \leq)$, rappresento gli elementi di A con dei punti sul piano. Posiziono il punto $x \in A$ più in basso di $y \in A$ se $x \leq y$. Congiungo con un segmento gli elementi x, y se y "copre" x, ossia se l'intervallo individuato dagli estremi $x, y = [x, y] = \{z \in A : x \leq z \leq y\}$ contiene solo x ed y. Si dice y "copre" x o x "è coperto" da y e si indica con $x <\cdot\, y$.

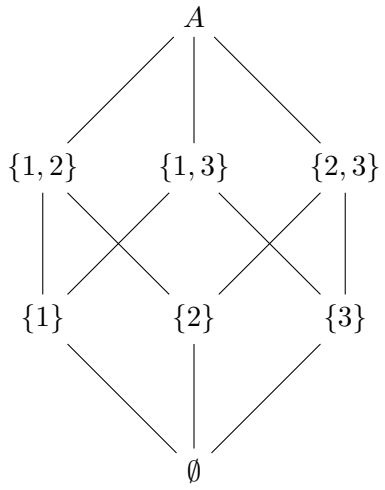

Figura 1.1: Diagramma di Hasse della relazione $(\mathbb{P}(A), \subseteq)$ sull'insieme $A = \{1, 2, 3\}$

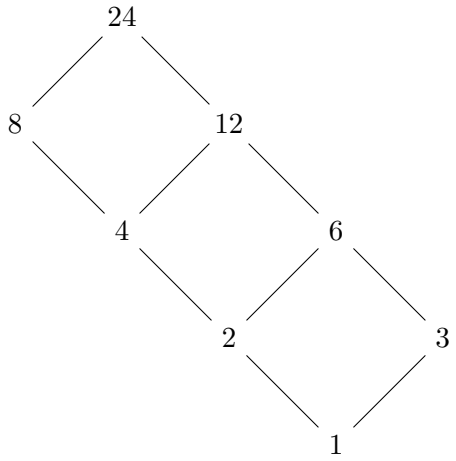

Figura 1.2: Diagramma di Hasse della relazione $(A, |)$ sull'insieme $A = \{n \in \mathbb{N} : n \mid 24\} = \{1, 2, 3, 4, 6, 8, 12, 24\}$

Teorema 1.2.1 (*Ordinamento totale*)

Ogni insieme è suscettibile di un ordine totale, ossia si può totalmente ordinare.

Esercizio 3

Determinare due ordini diversi su $\mathbb{Q}$.

1.2.2 INF e SUP

Definizione 1.2.4 (*INF*)

Dato un insieme $(P, \leq)$ *parzialmente ordinato, e due elementi* $x, y \in P$*, si dice INF di* x *e* y *l'elemento* $\inf(x, y)$ *tale che:*
INF1 $\inf(x, y) \leq x$ *e* $\inf(x, y) \leq y$
INF2 $z \in P$*, se* $z \leq x, y \Rightarrow z \leq \inf(x, y)$

Definizione 1.2.5 (*SUP*)

Analogamente possiamo definire il SUP di x, y, un elemento di P che si indica con $\sup(x, y)$ *tale che:*
SUP1 $\sup(x, y) \geq x$ *e* $\sup(x, y) \geq y$
SUP2 $z \in P$, *se* $z \geq x, y \Rightarrow z \geq \sup(x, y)$

Ossia, $\inf(x, y)$ è il più grande dei minoranti di x, y e $\sup(x, y)$ è il più piccolo di tutti i maggioranti di x, y.

Prendiamo l'insieme Γ, il suo insieme delle parti e la relazione "è sottoinsieme di" $(\mathbb{P}(\Gamma), \subseteq)$, e due sottoinsiemi $A, B \subseteq \Gamma$, l'$\inf(A, B) = A \cap B$. Il $\sup(A, B) = A \cup B$.

Prendiamo $(\mathbb{N}, |)$ e due elementi m, n. L'$\inf(m, n) = \text{MCD}(m, n)$, mentre il $\sup(m, n) = \text{mcm}(m, n)$.

1.3 Reticoli

Definizione 1.3.1 (*Reticolo*)

L'insieme parzialmente ordinato $(L, \leq)$ *è un reticolo se* $\forall\, x, y \in L$ *esiste* $\inf(x, y)$ *ed esiste* $\sup(x, y)$.

Posso interpretare i reticoli anche come strutture algebriche. Si possono definire due operazioni su L.

Definizione 1.3.2 (*Operazione di* inf)

Indicata con $\wedge : L \times L \to L$, *definita come* $\forall\, (x, y) \in L \times L,\ x \wedge y = \inf(x, y)$.

Definizione 1.3.3 (*Operazione di* sup)

L'operazione di sup, *indicata con* $\vee : L \times L \to L$, *definita come* $\forall\, (x, y) \in L \times L,\ x \vee y = \sup(x, y)$.

Ho definito quindi la struttura algebrica $(L, \wedge, \vee)$. Le due operazioni hanno le seguenti proprietà, dette **proprietà dei reticoli**:

R1 Idempotenza: $x \wedge x = x;\ x \vee x = x$.

R2 Commutativa: $x \wedge y = y \wedge x;\ x \vee y = y \vee x$.

R3 Associativa: $x \wedge (y \wedge z) = (x \wedge y) \wedge z;\ x \vee (y \vee z) = (x \vee y) \vee z$.

R4 Assorbimento: $x \wedge (x \vee y) = x;\ x \vee (x \wedge y) = x$.

Sono le proprietà classiche dell'unione e dell'intersezione.

Dimostrazione della proprietà R3: Equivale a dimostrare, per doppia inclusione, che $x \wedge (y \wedge z) \leq (x \wedge y) \wedge z$ e che $(x \wedge y) \wedge z \leq x \wedge (y \wedge z)$. La prima parte equivale a dire che

$$x \wedge (y \wedge z) \leq \begin{cases} (x \wedge y) \\ z \end{cases}$$

Il primo caso equivale a dimostrare che

$$x \wedge (y \wedge z) \leq x, y \Rightarrow x \wedge (y \wedge z) \leq x \wedge y$$

Il secondo caso si dimostra subito perché $y \wedge z \leq z, y \Rightarrow y \wedge z \leq z$ è vero per definizione di inf. ■

Teorema 1.3.1 (*Relazioni d'ordine sui reticoli*)

Data una struttura algebrica $(L, \wedge, \vee)$ verificante le quattro proprietà dei reticoli, è possibile definire su L una relazione d'ordine $\leq$ t.c. $x \wedge y = \inf(x, y)$ e $x \vee y = \sup(x, y)$ in $(L, \leq)$, ossia $x \leq y \Leftrightarrow x \wedge y = x$ (o anche $x \vee y = y$).

Dimostrazione: Dimostriamo che è una relazione d'ordine.

- Proprietà riflessiva: $x \leq x$ per R1.
- Antisimmetrica: $\forall\ x, y \in A$ se $x \leq y$ e $y \leq x \Rightarrow x = y$. Dimostrazione: $x \leq y \Rightarrow x \wedge y = x$, e $y \leq x \Rightarrow y \wedge x = y$. Per R2 $x = x \wedge y = y \wedge x = y$, per cui $x = y$.
- Transitiva: $\forall\ x, y, z \in A$ se $x \leq y \wedge y \leq z \Rightarrow x \leq y$. Dimostrazione: $x \leq y \Rightarrow x \wedge y = x$, $y \leq z \Rightarrow y \wedge z = y$, da cui $x \leq z$. Devo quindi dimostrare che $x \wedge z = x$, quindi che $(x \wedge y) \wedge z = x$. Per R3 $(x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$.

Rimane da dimostrare che $x \wedge y = \inf(x, y)$. Devo dimostrare due cose:

1. $x \wedge y \leq x, y$. Infatti $(x \wedge y) \wedge x = (x \wedge y) \Rightarrow (x \wedge y) \leq x$, e analogamente $x \wedge y \leq y$.
2. $z \leq x, y \Rightarrow z \leq (x \wedge y)$. La tesi mi dice che $z \wedge x = z$ e che $z \wedge y = z$. Devo dimostrare quindi $z \wedge (x \wedge z) = z \wedge z = z$. ■

Lemma 1.3.2

$x \leq y \Leftrightarrow x \vee y = y$

Dimostrazione del lemma 1.3.2: Sostituendo in $x \wedge y = x$ in $x \vee y$ otteniamo $(x \wedge y) \vee y = y$, per la proprietà R4. ■

Per dimostrare $x \vee y = \sup(x, y)$ basta sfruttare il lemma 1.3.2, ripercorrendo le stesse tappe e sostituendo sup al posto di inf.

I reticoli possono quindi essere visti come strutture algebriche in cui le operazioni sono l'inf e il sup, o come insiemi parzialmente ordinati.

Ci sono altre due proprietà dei reticoli:

R5 Le relazioni sono *isotoniche*.

$$x \leq y, z \in L \Rightarrow \begin{cases} x \wedge z \leq y \wedge z \\ x \vee z \leq y \vee z \end{cases}$$

R6 Disuguaglianza distributiva. In ogni reticolo $(L, \leq)$ $\forall\ x, y, z \in L$ si ha:

$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$$

Dimostrazione di R5: Devo dimostrare che $(x \wedge z) \wedge (y \wedge z) = x \wedge z$. Per ipotesi $x \leq y \Rightarrow x \wedge y = x$.

$$\begin{aligned} (x \wedge z) \wedge (y \wedge z) = \\ (x \wedge z) \wedge (z \wedge y) = \\ x \wedge (z \wedge z) \wedge y = \\ (x \wedge z) \wedge y = \\ (x \wedge y) \wedge z = \\ x \wedge z \end{aligned}$$

■

Dimostrazione di R6 : Per definizione di inf bisogna dimostrare:

$$x \vee (y \wedge z) \leq \begin{cases} (x \vee y) \\ (x \vee z) \end{cases}$$

Poichè $\vee$ è un'operazione isotonica:

$$(y \wedge z) \leq y \Rightarrow x \vee (y \wedge z) \leq x \vee y$$

■

1.3.1 Teorema di dualità

Data una stringa $E(\wedge, \vee)$ contenente gli elementi del reticolo, $\wedge, \vee, (,)$, posso creare la sua stringa duale $E^*(\vee, \wedge)$ in cui ogni $\wedge$ è sostituita da $\vee$, e le relazioni d'ordine sono scambiate.

$$(x \wedge y) \vee y = E(\wedge, \vee)$$
$$(x \vee y) \wedge y = E^*(\vee, \wedge)$$

Vediamo che le proprietà dei reticoli sono formule duali.

Perchè bisogna scambiare le relazioni d'ordine? Dato un reticolo $(L, \leq)$ e il suo duale $(L, \geq)$, il $\sup^*(x, y) = \inf(x, y)$, e l'$\inf^*(x, y) = \sup(x, y)$.

Teorema 1.3.3 (*Dualità*)

Se in un reticolo $(L, \leq)$ è vero un enunciato ξ relativo a stringhe del tipo $E(\wedge, \vee) \Rightarrow$ è vero l'enunciato duale ξ^* di ξ che si ottiene da ξ sostituendo ad ogni stringa $E(\wedge, \vee)$ la stringa $E^*(\vee, \wedge)$, e se $E_i(\wedge, \vee) \leq E_2(\wedge, \vee)$, allora $E_i^*(\vee, \wedge) \geq E_2^*(\vee, \wedge)$.

Ogni volta che dimostro un teorema sui reticoli, è vero anche il teorema duale.

La duale della disuguaglianza distributiva è:

$$x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$$

Che è anche la proprietà di disuguaglianza distributiva in $(L^*, \geq)$.

Esercizio 4

ξ: in un reticolo $(L, \leq)$ si ha che $x \leq z, y \in L \Rightarrow x \vee (y \wedge z) \leq (x \vee y) \wedge z$ (disuguaglianza modulare). Dimostrarlo.

Definizione 1.3.4 (*Reticolo distributivo*)

Se in $(L, \leq)$ vale l'identità $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, il reticolo si dice distributivo. Vale anche la duale.

Ogni reticolo distributivo è modulare. Esistono reticoli modulari ma non distributivi.

Prendiamo ad esempio il reticolo in figura 1.3: $(x \wedge y) \vee z = 0 \vee z = z$, $(x \vee z) \wedge (y \vee z) = 1 \wedge 1 = 1 \neq z$, quindi non è distributivo.

Mentre è modulare: prendiamo la coppia $0 \leq x$ in relazione e $y \in L$ non in relazione con x (lo scegliamo non in relazione con x perché altrimenti sarebbe banale la dimostrazione). $0 \vee (y \wedge x) = 0 \vee 0 = 0$, e $(0 \vee y) \wedge x = 0 \wedge x = 0$. Quindi, è modulare.

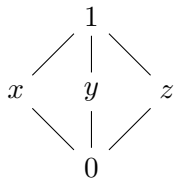

Figura 1.3: Reticolo modulare ma non distributivo

Esercizio 5

L'insieme delle parti è un reticolo distributivo, e quindi anche modulare. Dimostrarlo.

Esercizio 6

$(\mathbb{N}, |)$ *è un reticolo distributivo?*

1.4 Partizioni di A

Definizione 1.4.1 (*Partizione*)

Una partizione di A è un insieme di sottoinsiemi di A, indicato con π, tale che:
P1 $\forall\ B \in \pi,\ B \neq \emptyset$
P2 $B, C \in \pi,\ B \cap C \neq \emptyset \Rightarrow B = C$
P3 $\forall\ a \in A\ \exists\ B \in \pi : a \in B$

Una partizione π è un insieme di sottoinsiemi non vuoti di A t.c. hanno intersezione disgiunta e la loro unione è A. In altre parole, ogni elemento di A appartiene a un solo elemento di π.

Gli elementi di una partizione sono chiamati "blocchi".

Prendiamo $A = \mathbb{R}^2$. Posso pensare due partizioni banali: $\pi_0 = \left\{B \subseteq \mathbb{R}^2 : |B| = 1\right\}$, $\pi_1 = \left\{\mathbb{R}^2\right\}$.

Esercizio 7

Indicare altre partizioni su $\mathbb{R}^2$.

1.4.1 Classi di equivalenza

Definizione 1.4.2 (*Classe di equivalenza*)

Prendiamo una relazione di equivalenza $\varepsilon \subseteq A \times A$. Definisco le classi di equivalenza come, dato un $a \in A$:

$$[a] = \{x \in A : a \varepsilon x\}$$

$[a]$ si chiama "classe di equivalenza rappresentata da a".

Proposizione 1.4.1 (*Insieme quoziente*)

Se considero l'insieme delle classi di equivalenza A/ε, chiamato "insieme quoziente", questo insieme è una partizione di A.

$$A/\varepsilon = \{[a] \subseteq \mathbb{P}(A) : [a] \text{ è una classe di equivalenza}\}$$

Dimostrazione della proposizione 1.4.1 : Bisogna dimostrare le tre proprietà specificate nella definizione 1.4.1.

- $[a] \neq \emptyset$ è vero perché la relazione è riflessiva, ed a è in relazione almeno con sé stesso.
- $[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$. Supponiamo esista $z \in [a] \cap [b] \Rightarrow a \varepsilon z$ e $b \varepsilon z$. Essendo la relazione simmetrica e transitiva, $z \varepsilon b \Rightarrow a \varepsilon b$. Per la proprietà simmetrica, di nuovo, $b \varepsilon a$. Quindi $\forall\, x \in [a] \Rightarrow a \varepsilon x$ e per transitività $b \varepsilon x$.
- $\forall\, a \in A\ \exists\, B \in \pi : a \in B$. Banalmente, ogni $\forall\, a \in A : a \in [a]$ con $[a] \in \mathbb{P}(A)$ per la proprietà riflessiva. ■

1.4.2 Congruenza modulo n su $\mathbb{Z}$

Consideriamo l'insieme quoziente $\mathbb{Z}/\equiv_n$, con $\equiv_n$ simbolo per la relazione di congruenza modulo n.

$\equiv_n$ con $n \in \mathbb{N}, n \geq 2$, è definita, con $k \in \mathbb{Z}$, come:

$$\forall\, a, b \in \mathbb{Z}, a \equiv_n b \Leftrightarrow n \mid (a - b) \Leftrightarrow (a - b) = kn$$

Posso definire quindi l'insieme quoziente sulla relazione di congruenza modulo n:

$$\mathbb{Z}/\equiv_n$$
$$a \in \mathbb{Z}$$
$$[a] = \{z \in \mathbb{Z} : a \equiv_n z\}$$

Teorema 1.4.2 (*Teorema di divisione su* $\mathbb{Z}$)

$a, n \in \mathbb{Z}$ con $n > 0$, esiste un'unica coppia di interi $q, r \in \mathbb{Z}$ tale che:
- $a = nq + r$
- $0 \leq r < n$

Cosa significa $z \in [a]$, con a e z interi? Per il teorema di divisione, $a = nq + r$ e $z = np + r'$. $a \varepsilon z$ significa che $(a - z) = kn \Rightarrow n(q - p) + (r - r') = kn$. Essendo $r - r' < n$, necessariamente $r - r' = 0 \Rightarrow r = r'$. Ossia, se la differenza fra a e z è multiplo di n, devono avere lo stesso resto nella divisione per n.

Le classi di equivalenza hanno come rappresentante il resto della divisione modulo n. $Z/\equiv_2 = \{[0], [1]\}$. $Z/\equiv_3 = \{[0], [1], [2]\}$. In generale, $Z/\equiv_n$ ha n classi di equivalenza.

1.4.3 Relazioni di equivalenza e partizioni

Il concetto di relazione di equivalenza è analogo al concetto di partizione. Data una relazione di equivalenza è data una partizione, e una partizione individua una relazione di equivalenza.

Proposizione 1.4.3 (*Relazioni di equivalenza e partizioni*)

Sia $A \neq \emptyset$ e ε una relazione di equivalenza su A, allora ε individua una partizione di A data da $A/\varepsilon = \{[a] :$ è una classe di equivalenza$\}$. Viceversa, data una partizione π di A, π individua una relazione di equivalenza ε_π su A, tale che $A/\varepsilon_\pi = \pi$, ossia è possibile stabilire una biezione $F : \mathcal{E}(A) \to \Pi(A)$ dove $\mathcal{E}(A)$ è l'insieme delle relazioni di equivalenza su A e $\Pi(A)$ è l'insieme delle partizioni di A.

Dimostrazione: Definisco F come $\forall\ \varepsilon \in \mathcal{E}(A)\ F(\varepsilon) = A/\varepsilon$. Esiste la funzione G inversa di F, $G : \Pi(A) \to \mathcal{E}(A)$, $G(\pi) = \varepsilon_\pi$ con $a\varepsilon_\pi b \Leftrightarrow a, b \in B \in \pi$.

$$\varepsilon \xrightarrow{F} A/\varepsilon \xrightarrow{G} \varepsilon$$
$$\pi \xrightarrow{G} \varepsilon_\pi \xrightarrow{F} \pi = A/\varepsilon_\pi$$

■

Esercizio 8

Dimostrare che F è iniettiva e suriettiva.

Una semplice biezione non implica l'equivalenza. Prendo un insieme $E = \{e_1, e_2, \dots e_n\}$ di cardinalità $|E| = n$, l'insieme delle relazioni d'ordine $L(E)$, e l'insieme delle sue permutazioni $S(E)$ di cardinalità $n!$. Una permutazione è una biezione di un insieme finito. I due insiemi sono in corrispondenza biunivoca. Ho un'applicazione $F : S(E) \to L(E)$ che data un'occupazione σ associa ad ogni elemento di E il suo ordine associato $\sigma(e_1), \sigma(e_2), \dots \sigma(e_n)$.

Ad ogni biezione posso associare un ordine. Ma i due concetti non sono analoghi (ossia equivalenti). Non ho un'unica biezione: per definire la biezione devo stabilire un ordine degli elementi di E. A seconda di come li ordino ho una biezione diversa.

Definizione 1.4.3 (*Biezione naturale*)

Le biezioni naturali non dipendono dall'ordine lineare degli insiemi.

Come è fatta la classe $[(a, b)] = \{(c, d) \in \mathbb{N} \times \mathbb{N} : a + d = b + c\}$?

Se $a = b \Rightarrow [(a, a)] = \{(c, c) \in \mathbb{N} \times \mathbb{N} : c \in \mathbb{N}\} = [(0, 0)]$ (la coppia $(0, 0)$ la scelgo come "rappresentante standard" o "rappresentante canonico").

Se $a < b \Rightarrow b = a + m \Rightarrow [(a, a + m)] = \{(c, c + m) \in \mathbb{N} \times \mathbb{N} : c \in \mathbb{N}\} = [(0, m)]$.

Se $a > b \Rightarrow a = b + m \Rightarrow [(b + m, b)] = \{(c + m, c) \in \mathbb{N} \times \mathbb{N} : c \in \mathbb{N}\} = [(m, 0)]$.

Ciascuno dei tre tipi di classi di equivalenza ha un rappresentante canonico.

$\mathbb{N} \times \mathbb{N}/\rho$ è in corrispondenza biunivoca con $\mathbb{Z}$, associando $[(0, 0)]$ a 0, $[(0, m)]$ a $-m$ e $[(m, 0)]$ a m. Posso quindi costruire $\mathbb{Z}$ da $\mathbb{N}$.

Esercizio 9

$(\mathbb{N} \times \mathbb{N}, \rho)$ con $(a, b)\rho(c, d) \Leftrightarrow a + d = b + c$. Dimostrare che ρ è una relazione di equivalenza.

Proiezione di A sul suo insieme quoziente, e sezione

Definizione 1.4.4 (*Proiezione*)

Dato un insieme A, una relazione di equivalenza ε e l'insieme quoziente A/ε, definiamo $p : A \to A/\varepsilon$ come $p(a) = [a]$.

p è detta proiezione canonica, o naturale, ed è necessariamente suriettiva, ma in generale non è iniettiva (a meno che le classi abbiano tutte cardinalità 1). Ad ogni elemento di A associa la sua classe di equivalenza $[a]$.

Posso definire una famiglia di applicazioni $s : A/\varepsilon \to A$ "contrarie" a p tali che $s([a]) = a$, chiamate sezioni.

Definizione 1.4.5 (*Sezione*)

$\forall\ B \in A/\varepsilon, s(B) = a$ con $a \in B$. La sezione sceglie un elemento "rappresentante" da ogni classe di equivalenza.

In generale non è suriettiva (a meno che le classi abbiano tutte cardinalità 1), ma è necessariamente iniettiva.

È possibile comporre le due applicazioni:

- $p \circ s : A/\varepsilon \to A/\varepsilon$. Questa composizione mi restituisce l'identità dell'elemento che "passo" a s.
- $s \circ p : A \to A$. Questa composizione mi restituisce il rappresentante dell'elemento a nella sua classe di equivalenza, ossia manda tutti gli elementi di una classe di equivalenza in un unico elemento di quella classe.

Teorema 1.4.4 (*Assioma della scelta*)

Per ogni partizione è possibile scegliere un rappresentante in ogni classe, ossia si può definire una sezione. Equivale a dire che ogni applicazione suriettiva ha un'inversa destra, che equivale a dire che ogni applicazione iniettiva ha un'inversa sinistra, che equivale a dire che dato A insieme infinito è possibile ordinare totalmente A.

Una conseguenza dell'assioma della scelta è che tutte le applicazioni suriettive hanno un'inversa destra, e tutte le applicazioni iniettive hanno un'inversa sinistra.

- f è iniettiva $\Leftrightarrow$ f ha un'inversa sinistra.
- f è suriettiva $\Leftrightarrow$ f ha un'inversa destra.

Se una funzione ha sia un'inversa sinistra sia un'inversa destra, è biunivoca.

L'assioma della scelta permette di ordinare totalmente un insieme infinito. Scelgo un elemento $x_1 \in A$, dopodiché scelgo un elemento $x_2 \in A \setminus \{x_1\}$, e via dicendo.

Nuclei di funzioni

Ogni funzione f definisce una relazione di equivalenza ε_f.

Definizione 1.4.6 (*Partizione individuata da una funzione*)

Data $f : A \to B$, definiamo ε_f su A. ε_f è definita da:

$$\forall\ x, y \in A,\ x\ \varepsilon_f\ y \Leftrightarrow f(x) = f(y)$$

Definizione 1.4.7 (*Nucleo di una funzione*)

L'insieme quoziente A/ε_f è chiamato "nucleo di f", e si indica con $\ker f$.

Proposizione 1.4.5 (*Funzioni come composizione di funzioni suriettive con iniettive*)

Ogni funzione $f : A \to B$ si può esprimere come composta di una funzione suriettiva con una iniettiva.

Dimostrazione: Considero la funzione $F : \ker f \to Im_f$, che ad un elemento del nucleo di f associa l'immagine del rappresentante di quell'elemento, ossia $b = F([a]) = f(c)\ \forall\ c \in [a] = f(a)$.

La funzione F viene poi composta con $i : Im_f \to B$, detta "immersione". Da wikipedia:

Definizione 1.4.8 (*Immersione*)

Una struttura A si dice immersa nella struttura B se esiste una funzione iniettiva $f : A \to B$ tale che l'immagine $f(A)$ conserva tutte o parte delle strutture matematiche presenti in A, ereditandole da quelle di B. La funzione prende anch'essa il nome di immersione.

In questo caso la funzione di immersione i è la funzione identità $\ \forall\ b \in Im_f\ i(b) = b$, poiché $Im_f \subseteq B$.

La funzione identità composta F, composta con la proiezione p di f, dà proprio f.

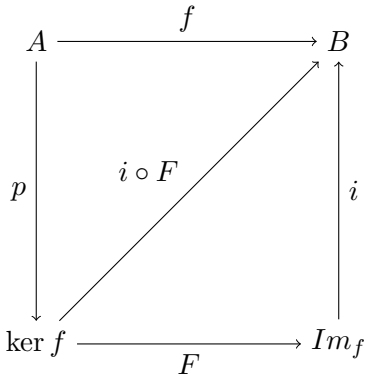

Figura 1.4: f come composizione di p e di $i \circ F$

Esempio:

Consideriamo la funzione $f : \mathbb{R}^2 \to \mathbb{R}^3$ definita da $f(x, y) = (x, x, 0)$.

Le classi di equivalenza individuate in $\ker f$ saranno $[(x, y)] = \{(z, t) \in \mathbb{R}^2 \mid z = x\}$. Per ogni classe possiamo individuare un rappresentante canonico del tipo $[(x, 0)]$ con $x \in \mathbb{R}$.

Ad ogni classe devo associare la sua immagine, quindi a $[(x, y)]$ è associato $(x, x, 0)$.

1.4.4 Teorema di omomorfismo per gli insiemi

Proposizione 1.4.6 (*Corrispondenza biunivoca fra immagine e nucleo*)

Per ogni $f : A \to B$ si ha $|Im_f| = |\ker f|$, ossia esiste una biezione $F : \ker f \to Im_f$.

Dimostrazione: Per le definizioni di immagine di una funzione e nucleo di una funzione:

$$Im_f = \{b \in B :\ \exists\ a \in A \text{ t.c. } f(a) = b\} \subseteq B$$

$$\ker f = \{[a] :\ \forall\ x \in [a]\ f(x) = f(a)\}$$

$\forall$ classe di $\ker f$ $F([a]) = f(a) = F([b]) \Rightarrow [a] = [b]$ e $\forall\ b \in Im_f\ b = f(a) \Rightarrow F([a]) = b$. F è una funzione suriettiva e iniettiva, quindi gli elementi del $\ker f$ sono tanti quanti gli elementi di Im_f.

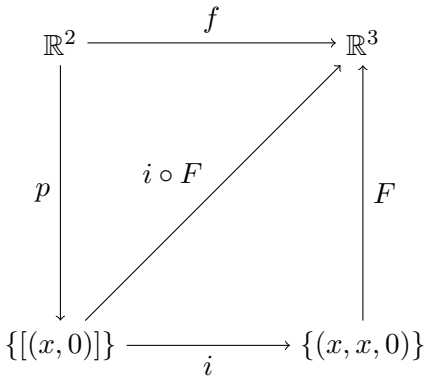

Figura 1.5: $f(x,y) = (x,x,0)$ come composizione di una funzione suriettiva con una iniettiva

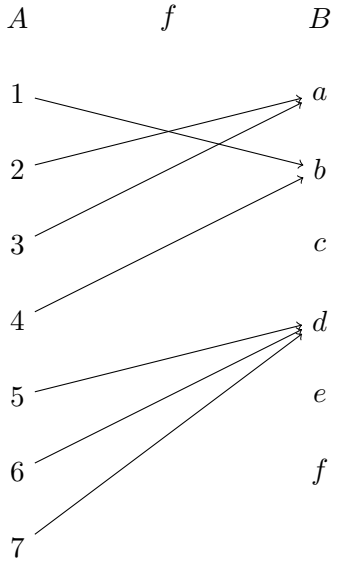

Figura 1.6: $\ker f = \{[1],[2],[5]\}$, $Im_f = \{a,b,d\}$

Partizioni come reticoli

$\Pi(A)$ è insieme delle partizioni di A, $\subseteq$ è una relazione di raffinamento.

Dati $\pi, \sigma \in \Pi(A)$, $\pi \subseteq \sigma \Leftrightarrow \ \forall\, B \in \pi$ si ha che B è contenuto in un blocco di $\sigma \Leftrightarrow$ ogni blocco di σ è unione di blocchi di $\pi \Leftrightarrow \ \forall\, x, y \in A,\ x\ \varepsilon_\pi\ y \Rightarrow x\ \varepsilon_\sigma\ y$.

Proposizione 1.4.7 (*Partizione come reticolo*)

$(\Pi(A), \subseteq)$ è *un insieme parzialmente ordinato ed è un reticolo, ossia presi comunque due elementi c'è l'*inf *e il* sup.

Dimostrazione: $(\pi \wedge \sigma)$ è dato dalla relazione $x\ \varepsilon_{(\pi\wedge\sigma)}\ y \Leftrightarrow x\ \varepsilon_\pi\ y$ e $x\ \varepsilon_\sigma\ y$. Quindi per definizione $\pi \wedge \sigma$ è $\inf(\pi, \sigma)$. ■

Verifichiamone le proprietà:

- $\pi \wedge \sigma \leq \pi, \sigma$, vero per definizione di $\leq$.

- $\pi \leq \sigma \Leftrightarrow$ se $x\ \varepsilon_\pi\ y$ allora $x\ \varepsilon_\sigma\ y$
- $\tau \leq \pi, \sigma \Rightarrow \tau \leq (\pi \wedge \sigma)$, infatti:

$$x\ \varepsilon_\tau\ y \Rightarrow x\ \varepsilon_\pi\ y \text{ e } x\ \varepsilon_\sigma\ y \Rightarrow x\ \varepsilon_{(\pi\wedge\sigma)}\ y$$

Definizione 1.4.9 (sup *fra partizioni*)

$x\ \varepsilon_{(\pi\vee\sigma)}\ y \Leftrightarrow\ \exists\ x = a_1, a_2 \ldots a_n = y$ tale che $a_i\ \varepsilon_\pi\ a_j$ oppure $a_i\ \varepsilon_\sigma\ a_j$ con $i \in [1, n-1]$, ossia ho una catena che mette in relazione a_i con a_j passando per π o σ.

Poiché $(\pi \vee \sigma) = \sup(\pi, \sigma)$, allora:

- $\pi, \sigma \leq (\pi\vee\sigma)$, ossia $\pi \leq (\pi\vee\sigma)$ e $\sigma \leq (\pi\vee\sigma)$, vero per definizione perché $x\ \varepsilon_\pi\ y \Rightarrow x\ \varepsilon_{\pi\vee\sigma}\ y$.
- $\pi, \sigma \leq \tau \Rightarrow (\pi \vee \sigma) \leq \tau$, ossia $x\ \varepsilon_\pi\ y \Rightarrow x\ \varepsilon_\tau\ y$ e $x\ \varepsilon_\sigma\ y \Rightarrow x\ \varepsilon_\tau\ y$. Quando dico $x\ \varepsilon_{(\pi\vee\sigma)}\ y$, allora $x\ \varepsilon\ a_2\ \varepsilon \ldots \varepsilon\ y$, in cui ogni ε è o ε_π o ε_σ, quindi in ogni caso $a_i\ \varepsilon_\pi\ a_j$ o $a_i\ \varepsilon_\sigma\ a_j$ per cui necessariamente $a_i\ \varepsilon_\tau\ a_j$. Segue per transitività che $x\ \varepsilon_\tau\ y$.

Esercizio 10

$(\Pi(A), \subseteq)$ è un reticolo e $\subseteq$ è una relazione d'ordine. Dimostrare che non è modulare.

1.5 Morfismi

Sono delle funzioni $f : A \to B$ che partono da A con una struttura e arrivano a B con la stessa struttura.

1.5.1 Morfismi di insiemi parzialmente ordinati

Detti anche "morfismi d'ordine" o funzioni monotone.

Definizione 1.5.1 (*Morfismo d'ordine*)

Un morfismo di un insieme parzialmente ordinato è un'applicazione $f : P_1 \to P_2$ dove $(P_1, \leq_1)$ e $(P_2, \leq_2)$ sono insiemi particolarmente ordinati, tale che $\forall\ x, y \in P_1$ con $x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$. f è una funzione monotona (ossia f conserva l'ordine).

Quindi un morfismo va da un'insieme con una struttura ad un altro insieme con la sua struttura. Lo indicheremo con questa notazione:

$$f : (P_1, \leq_1) \to (P_2, \leq_2)$$

Esempio :

Dati $P_1 = P_2 = \mathbb{P}(\Gamma)$ e la relazione $(\mathbb{P}(\Gamma), \subseteq)$, definisco $f : \mathbb{P}(\Gamma) \to \mathbb{P}(\Gamma)$ come, fissato A sottoinsieme finito di Γ, $\forall\ X \in \mathbb{P}(\Gamma) f(X) = A \cap X$.

f è un morfismo $f : (\mathbb{P}(\Gamma), \subseteq) \to (\mathbb{P}(\Gamma), \subseteq)$ poiché $\forall\ X, Y \in \mathbb{P}(\Gamma)\ X \subseteq Y \Rightarrow f(X) \subseteq f(Y)$ visto che $X \cap A \subseteq Y \cap A$.

Questa proprietà si chiama **isotonia** di $\subseteq$. Anche l'unione ha questa proprietà: $g : (\mathbb{P}(\Gamma), \subseteq) \to (\mathbb{P}(\Gamma), \subseteq)$ con $g(X) = A \cup X$

Esempio :

Sia Γ un insieme finito, definisco una funzione su $\mathbb{P}(\Gamma)$ e $(\mathbb{N}, \leq)$ $f : \mathbb{P}(\Gamma) \to \mathbb{N}$ come $\forall\ X \in \mathbb{P}(\Gamma)\ f(X) = |X|$. Anche questa è una funzione monotona.

1.5.2 Morfismi di reticoli

$(L, \leq)$ è un reticolo se $\forall\ x, y \in L\ \exists\ \inf(x, y)$ e $\exists\ \sup(x, y)$. Ogni reticolo individua una struttura algebrica con due operazioni, $(L, \wedge, \vee)$, e inoltre dalla struttura algebrica posso definire il reticolo.

Definizione 1.5.2 (*Morfismo di reticoli*)

Dati due reticoli $(L_1, \leq_1)$ e $(L_2, \leq_2)$, un morfismo di reticoli è una funzione $f : L_1 \to L_2$ che verifica le seguenti proprietà:

M1 $\forall\ x, y \in L_1\ f(\inf(x, y)) = \inf(f(x), f(y))$, *e analogamente* $\forall\ x, y \in L_1\ f(\sup(x, y)) = \sup(f(x), f(y))$.

M2 *Deve rispettare l'ordine.* $\forall\ x, y \in L_1$ *con* $x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$.

Esempio :

Riprendendo l'esempio precedente, $P_1 = P_2 = \mathbb{P}(\Gamma)$ e la relazione $(\mathbb{P}(\Gamma), \subseteq)$, definisco $f : \mathbb{P}(\Gamma) \to \mathbb{P}(\Gamma)$ come, fissato A sottoinsieme finito di Γ, $\forall\ X \in \mathbb{P}(\Gamma)\ f(X) = A \cap X$.

In questo reticolo, $\inf(X, Y) = X \cap Y$, quindi $f(\inf(X, Y)) = f(X \cap Y) = (X \cap Y) \cap A$. Per verificare M1, $(X \cap Y) \cap A = \inf(f(X, Y)) = \inf(X \cap A, Y \cap A) = (X \cap A) \cap (Y \cap A)$, vero per la proprietà commutativa, la proprietà associativa e l'idempotenza degli insiemi.

$$(X \cap A) \cap (Y \cap A) = (X \cap A) \cap (A \cap Y) = X \cap (A \cap A) \cap Y = X \cap A \cap Y$$

Esempio :

Sia Γ un insieme finito, definisco una funzione su $\mathbb{P}(\Gamma)$ e $(\mathbb{N}, \leq)$ $f : \mathbb{P}(\Gamma) \to \mathbb{N}$ come $\forall\ X \in \mathbb{P}(\Gamma) f(X) = |X|$.

Devo verificare M1, ossia che $f(\inf(X, Y)) = \inf(f(X), f(Y))$. $f(X \cap Y) = |X \cap Y|$, mentre $\inf(f(X), f(Y)) = \inf(|X|, |Y|)$, ossia il minore fra i due numeri. Non è vero in generale, quindi questa funzione non è un morfismo di reticoli.

In realtà M1 implica M2, a differenza di quanto visto nelle relazioni di equivalenza e di ordine.

Proposizione 1.5.1 (*Morfismo di reticoli 2*)

$(L, \leq_1)$ e $(L, \leq_2)$ due reticoli. Sia $f : L_1 \to L_2$ tale che $\forall\ x, y \in L_1\ f(\inf(x, y)) =$

$\inf(f(x), f(y))$ e $\forall\ x, y \in L_1\ f(\sup(x, y)) = \sup(f(x), f(y))$, *allora* f *è una funzione monotona, e quindi è un morfismo di reticoli.*

Dimostrazione: Bisogna dimostrare che conserva l'ordine, ossia che se $x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$. Per l'ipotesi, $\inf(x, y) = x$ e $\sup(x, y) = y$. Quindi $f(\inf(x, y)) = f(x)$. Per M1 $f(\inf(x, y)) = \inf(f(x), f(y))$, quindi $f(x) = \inf(f(x), f(y)) \Rightarrow f(x) \leq_2 f(y)$. ■

Stessa dimostrazione vale per il sup. Abbiamo dimostrato già che il contrario non vale, nell'esempio 1.5.2.

1.5.3 Isomorfismi

Un isomorfismo è un morfismo biunivoco.

Dato l'insieme delle parti di Γ, $(\mathbb{P}(\Gamma), \subseteq)$, e l'insieme $2 = \{0, 1\}$, 2^Γ è l'insieme delle funzioni $\Gamma \to \{0, 1\}$. Date due funzioni $f, g \in 2^\Gamma$, $f \leq g \Leftrightarrow\ \forall\ x \in \Gamma$ ho che $f(x) \leq g(x)$ (come da definizione 1.2.3).

$(2^\Gamma, \leq)$ è un reticolo. Infatti $\inf(f, g) : \Gamma \to 2$ è:

$$\inf(f, g)(x) = \begin{cases} f(x) & \text{se } f(x) \leq g(y) \\ g(x) & \text{altrimenti} \end{cases}$$

Analogamente, $\sup(f, g)(x) : \Gamma \to 2$ è:

$$\sup(f, g)(x) = \begin{cases} g(x) & \text{se } f(x) \leq g(y) \\ f(x) & \text{altrimenti} \end{cases}$$

Un esempio di isomorfismo è quindi $F : \mathbb{P}(\Gamma) \to 2^\Gamma$. Prendo un sottoinsieme $A \subseteq \Gamma$ (ossia un elemento $A \in \mathbb{P}(\Gamma)$) e definisco la "funzione caratteristica di A" che indicherò con $\varphi_A : \Gamma \to 2$ che dice se un elemento di Γ è o non è in Γ, ossia:

$$\forall\ x \in \Gamma\ \varphi_A(x) = \begin{cases} 0 \text{ se } x \notin A \\ 1 \text{ se } x \in A \end{cases}$$

F è biunivoca. Dimostriamo che è iniettiva e suriettiva.

Proposizione 1.5.2

Se $A, B \in \mathbb{P}(\Gamma)$ *e* $\varphi_A = \varphi_B \Rightarrow A = B$, *ossia per doppia inclusione* $A \leq B$ *e* $B \leq A$.

Dimostrazione: Per definizione di funzione caratteristica, $\forall\ x \in A \Rightarrow \varphi_A(x) = 1 = \varphi_B(x) \Rightarrow x \in B$. ■

Proposizione 1.5.3

$\forall\ f \in 2^\Gamma\ \exists\ A \in \mathbb{P}(\Gamma)$ *t.c.* $\varphi_A = f$.

Dimostrazione: Prendo $\Gamma = \{1, 2, 3, 4, 5, 6, 7\}$, e rappresento f dal punto di vista dell'occupazione.

1	2	3	4	5	6	7
0	0	1	1	0	1	0

Quindi $A = \{3, 4, 6\} = f^{-1}(1)$, ossia la controimmagine di φ_A. ■

Poiché F è un isomorfismo, $A \subseteq B \Rightarrow F(A) \leq F(B) = \varphi(A) \leq \varphi(B)$, infatti $\forall\, x \in \Gamma$:

$$\varphi_A(x) = \begin{cases} 0 \text{ se } x \notin A \Rightarrow \varphi_A(x) \leq \varphi_B(x) \\ 1 \text{ se } x \in A \Rightarrow \text{ poiché } A \subseteq B,\ \varphi_B(x) = 1 \Rightarrow \varphi_A(x) \leq \varphi_B(X) \end{cases}$$

Dimostriamo che si tratta di un morfismo di reticoli.

Proposizione 1.5.4

$F(\inf(A,B)) = \inf(F(A),F(B))$, ossia $F(\inf(A,B)) = F(A \cap B) = \varphi_{(A\cap B)}$ e $\inf(F(A),F(B)) = \inf(\varphi_A,\varphi_B)$.
Quindi $\inf(\varphi_A,\varphi_B) = \varphi_{(A\cap B)}$.

Dimostrazione: Per le proprietà dei reticoli:

- $\varphi_{A\cap B} \leq \varphi_A, \varphi_B$

$$\forall\, x \in \Gamma \varphi_{A\cap B}(x) = \begin{cases} 0 \text{ se } x \notin (A \cap B) \\ 1 \text{ altrimenti} \end{cases}$$

$$\varphi_{A\cap B}(x) = \begin{cases} 0 \leq \varphi_A \\ 1 \Rightarrow x \in (A \cap B) \subseteq A \Rightarrow \varphi_A(x) = 1 \Rightarrow \varphi_{A\cap B}(x) \leq \varphi_A(x) \end{cases}$$

- $f \leq \varphi_A, \varphi_B \Rightarrow f \leq \varphi_{A\cap B}$

$$f \in 2^{\Gamma}$$

$$f \leq \varphi_A, \varphi_B \Rightarrow\ \forall\, x \in \Gamma\ f(x) \leq \varphi_A(x) \text{ e } \varphi_B(x)$$

$$f(x) = \begin{cases} 0 \leq \varphi_{A\cap B}(x) \\ 1 \Rightarrow \varphi_A(x) = \varphi_B(x) = 1 \Rightarrow x \in (A \cap B) \Rightarrow \varphi_{A\cap B}(x) = 1 \end{cases}$$

■

L'insieme delle parti di un insieme Γ è in corrispondenza biunivoca con l'insieme delle funzioni da Γ in 2, quindi hanno la stessa cardinalità.

Considerazioni generali sugli isomorfismi

1. Sia $F : (P, \leq) \to (Q, \leq)$ un isomorfismo da P in Q, posso prendere la sua inversa $G : (Q, \leq) \to (P, \leq)$ che è a sua volta un isomorfismo da Q in P.
2. Se prendo tre strutture P, G, R e due isomorfismi $F : (P, \leq) \to (Q, \leq)$ e $G : (Q, \leq) \to (R, \leq)$, $G \circ F : (P, \leq) \to (R, \leq)$.
3. Le relazioni di equivalenza sono una generalizzazione dell'uguaglianza. La relazione di uguaglianza è la più piccola relazione di equivalenza, in cui tutte le classi sono costituite da un solo elemento.
4. Se prendo tutte le possibili strutture d'ordine $(P, \leq)$, posso creare una relazione di equivalenza per cui due strutture sono equivalenti se c'è un isomorfismo.

   Ossia, prendo due strutture $(P, \leq)$ e $(Q, \leq)$, e dico che $(P, \leq)$ è equivalente a $(Q, \leq)$ se esiste un isomorfismo da P a Q. Lo indico con $(P, \leq) \cong (Q, \leq)$.
5. Se due strutture sono isomorfe (come in figura 1.7), posso studiare una sola struttura e le proprietà di quella struttura valgono su tutte le strutture isomorfe.

Esercizio 11

Trovare tutti i reticoli (a meno di isomorfismi) con 4 elementi.

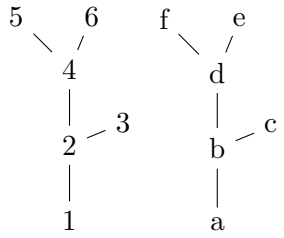

Figura 1.7: Esempio di strutture isomorfe

1.6 Numeri Naturali

$\mathbb{N}$ è l'insieme dei numeri naturali. Seguiamo la definizione di Peano.

Definizione 1.6.1 (*Numeri naturali*)

L'insieme dei numeri naturali è un insieme non vuoto tale che:
N1 *Esiste una funzione $\sigma : \mathbb{N} \to \mathbb{N}$ (una endofunzione) iniettiva detta "successore";*
N2 *Esiste un elemento di $\mathbb{N}$ chiamato "zero" ed indicato con 0 tale che $0 \notin Im_\sigma$, ossia che non è il successore di nessun numero naturale;*
N3 *Principio di induzione: se $U \subseteq \mathbb{N}$ tale che:*
- *$0 \in U$;*
- *$n \in U \Rightarrow \sigma(n) \in U$;*

allora $U = \mathbb{N}$.

Dire che un insieme è finito vuol dire che ogni iniezione sull'insieme è pure una suriezione. Quindi da N1 e N2 segue che $\mathbb{N}$ è infinito, poiché esiste una funzione iniettiva che non è suriettiva.

Proposizione 1.6.1

L'immagine di σ è tutto $\mathbb{N}$ escluso lo 0. $Im_\sigma = \mathbb{N} \setminus \{0\}$

Dimostrazione: Sia $U = Im_\sigma \cup 0$. U coincide con $\mathbb{N}$ per N3. Infatti:
- $0 \in U$ per definizione di U;
- $\forall\, n \in U,\ \sigma(n) \in U$.

■

L'elemento $\sigma(0)$ si indica con 1.

1.6.1 Iterazioni

Dato un insieme $A \neq \emptyset$ ed una funzione $f : A \to A$, con $\circ : A^A \times A^A \to A^A$ a indicare la composizione, $(A^A, \circ)$ è un monoide. Infatti $f \circ id_A = f = id_A \circ f$ è l'identità.

Definizione 1.6.2 (*Iterazioni*)

Le iterazioni di $f : A \to A$ sono definite da:
- *$f^0 = id_A$;*
- *$\forall\, n \in \mathbb{N}$ definisco $f^{\sigma(n)} = f \circ f^n$.*

Proposizione 1.6.2

f^n è ben definita per ogni $n \in \mathbb{N}$.

Dimostrazione: Sia $U = \{n \in \mathbb{N} : f^n \text{ è ben definita }\}$. $0 \in U$ per definizione. Se $n \in U f^n$ è definita, quindi è definita anche $f^{\sigma(n)} = f \circ f^n$, essendo f data. Quindi $U = \mathbb{N}$. ■

Iterazioni di σ

Definizione 1.6.3

Definiamo le iterazioni di σ come segue:
- $\sigma^0 = id_{\mathbb{N}}$;
- $\sigma^{\sigma(n)} = \sigma \circ \sigma^n \ \forall\ n \in \mathbb{N}$.

Proposizione 1.6.3

$\sigma^n(0) = n$

Dimostrazione: Si dimostra per induzione. $U = \{n \in \mathbb{N} : \sigma^n(0) = n\}$.

Lo 0 è già $\in U$, poiché $\sigma^0(0) = id_{\mathbb{N}}(0) = 0$.

$\sigma(n) \in U \Rightarrow \sigma^{\sigma(n)}(0) = \sigma(n)$. Per definizione delle iterazioni su σ, $\sigma^{\sigma(n)}(0) = \sigma \circ \sigma^n(0) = \sigma(n)$ poiché $\sigma(n) \in U$ per ipotesi. ■

Definizione 1.6.4 (*Potenze*)

Ho un monoide $(M, \cdot)$. $\cdot : M \times M \to M$ associativa e con unità 1_M. $a \in M$ $a \cdot 1_M = a = 1_M \cdot a$
- $a^0 = 1_M$
- $a^{\sigma(n)} = a \cdot a^n$

Sinceramente non ho capito che c'entra col resto e perché sta qui.

Proposizione 1.6.4

$\forall\ n \in \mathbb{N} \setminus \{0\}$, $0 \notin Im_{\sigma^n}$, ossia lo 0 non è nell'immagine di nessuna iterazione di σ, ossia comunque itero σ non ottengo mai lo 0.

Dimostrazione: Lo dimostriamo per assurdo. Supponiamo che $\exists\ n \in \mathbb{N}$ t.c. $0 \in Im_{\sigma^n} \Rightarrow \exists\ x \in \mathbb{N}$ t.c. $\sigma^n(x) = 0$. Poiché $n \neq 0 \Rightarrow n \in Im_\sigma = \mathbb{N} \setminus \{0\} \Rightarrow n = \sigma(t)$. Quindi $0 = \sigma^n(x) = \sigma^{\sigma(t)}(x) = (\sigma \circ \sigma^t)(x) = \sigma(\sigma^t(x)) \Rightarrow 0 \in Im_\sigma$. Ho ottenuto l'assurdo con N2. ■

Attraverso le tre proprietà che definiscono $\mathbb{N}$ si possono ritrovare tutte le altre proprietà di $\mathbb{N}$.

1.6.2 Operazioni su $\mathbb{N}$

Possiamo definire il monoide $(\mathbb{N}, +)$. L'operazione di somma $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ è definita così:

$$m + n = \sigma^n(m)$$

Esercizio 12

Dimostare che è commutativa, e che quindi $\sigma^n(m) = \sigma^m(n)$.

L'elemento neutro è lo 0, infatti: $m + 0 = \sigma^0(m) = id_{\mathbb{N}}(m) = m$ e $0 + m = \sigma^m(0) = m$ per la proposizione 1.6.3.

Osservazione 1

$n + 1 = n + \sigma(0) = \sigma(n)$

L'operazione + è associativa, oltre che commutativa.

La somma in $\mathbb{N}$ ha la "regola di cancellazione". $\forall\, m, n, k \in \mathbb{N}$, se $m + k = n + k \Rightarrow m = n$. In realtà in $\mathbb{N}$ non esiste l'inverso, quindi questa regola ha poco a che vedere con la "cancellazione".

Tutte le proprietà sono più facili da dimostare con il seguente lemma.

Lemma 1.6.5

$$m + \sigma(n) = \sigma(m + n)$$

Dimostrazione:

$$m + \sigma(n) = \sigma^{\sigma(n)}(m) = (\sigma \circ \sigma^n)(m) = \sigma(\sigma^n(m)) = \sigma(m + n)$$

■

Definizione 1.6.5 (*Prodotto su* $\mathbb{N}$)

$(\mathbb{N}, \cdot)$ *è un'operazione* $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *tale che* $\forall\, (m, n) \in \mathbb{N} \times \mathbb{N}$, $m \cdot n = (\sigma^m)^n(0)$.

Il prodotto è un'operazione associativa e distributiva.

Proposizione 1.6.6

$\sigma(0) = 1$ *è l'elemento neutro.*

Dimostrazione: $m \cdot \sigma(0) = (\sigma^m)^{\sigma(0)}(0) = \sigma^m(0) = m$
$\sigma(0) \cdot m = (\sigma^{\sigma(0)})^m(0) = \sigma^m(0) = m$ ■

Definizione 1.6.6 (*Legge di annullamento del prodotto*)

$m \cdot n = 0 \Leftrightarrow m = 0$ *oppure* $n = 0$.

Sul prodotto e sulla somma valgono le leggi distributive: $k \cdot (m + n) = k \cdot m + k \cdot n$ e, per commutatività, $(m + n) \cdot k = m \cdot k + n \cdot k$.

Lemma 1.6.7

$m \cdot \sigma(n) = m \cdot n + m$

Dimostrazione: $m \cdot \sigma(n)$ per definizione del prodotto è $(\sigma^m)^{\sigma(n)}(0)$ che per definizione di iterazione è $(\sigma^m \circ (\sigma^m)^n)(0) = \sigma^m((\sigma^m)^n(0)) = \sigma^m(m \cdot n) = m \cdot n + m$ ■

Usando i due lemmi (lemma 1.6.5 e lemma 1.6.7) si ottengono tutte le proprietà delle operazioni su $\mathbb{N}$.

1.6.3 Ordine naturale su $\mathbb{N}$

Possiamo definire una relazione d'ordine totale (e naturale) su $\mathbb{N}$ usando le due operazioni.

Definizione 1.6.7 (*Ordine naturale*)

$m \leq n \Leftrightarrow \exists\, k \in \mathbb{N} : m + k = n$

È una relazione d'ordine totale (ossia l'insieme $\mathbb{N}$ è linearmente ordinato), ossia $\forall\, m, n \in \mathbb{N}$ si ha che $m \leq n$ oppure $n \leq m$.

L'ordine naturale su $\mathbb{N}$ è un "ordine buono", ossia $(\mathbb{N}, \leq)$ si dice "bene ordinato". Il "buon ordinamento" è equivalente all'assioma della scelta. Vuol dire che ogni suo sottoinsieme non vuoto ha un primo elemento. $\mathbb{R}$, ad esempio, non è bene ordinato.

Dimostrazione del buon ordinamento: Dimostriamolo per assurdo. Suppongo esista un sottoinsieme $V \neq \emptyset$ che non ha un primo elemento. Ossia, $\forall\, v \in V\ \exists\, w \in V$ t.c. $w \leq v$.

Consideriamo la proposizione P_n: "$\forall\, n \in \mathbb{N} \wedge\ \forall\, v \in V,\ n \leq v$" e dimostriamo che è vera $\forall\, n \in \mathbb{N}$.

È vero con 0: $\forall\, v \in V 0 \leq v$.

Supponiamo sia vero per un $n \in \mathbb{N}$, e dimostriamo che è vero per $\sigma(n)$ che $\forall\, v \in V \sigma(n) \leq v$.

Per ipotesi di induzione so che $\forall\, v \in V,\ n \leq v \Rightarrow\ \exists\, x \in \mathbb{N}$ t.c. $n + x = v$, per la definizione di $\leq$. x non può essere 0, altrimenti n sarebbe il primo elemento di V. Quindi $x \neq 0 \Rightarrow x = \sigma(y) = y + 1$, e quindi $n + y + 1 = v$ ma per la proprietà commutativa $n + 1 + y = v \Rightarrow \sigma(n) + y = v \Rightarrow \sigma(n) \leq v$.

Siamo giunti all'assurdo. Se prendo $n = v + 1$ avrei che $v + 1 \leq v$. ■

1.6.4 Altre forme del principio di induzione

Se $n_0 \in U$ (base dell'induzione) e $n_0 \leq n \in U \Rightarrow n+1 = \sigma(n) \in U$, quindi $U = \{n \in \mathbb{N}, n_0 \leq n\}$.

$\mathbb{Z} \simeq \mathbb{N} \times \mathbb{N}/\rho$ con $(m, n)\rho(p, q) \Leftrightarrow m + q = n + p$. Le classi di equivalenza sono $[(0, 0)], [(m, 0)]$ e $[(0, m)]$. Posso chiamarle anche 0, m e $-m$

1.7 Principi del calcolo combinatorio

Enumerare corrisponde a mettere in fila una serie di elementi. Contare significa saper stabilire una corrispondenza biunivoca fra due insiemi, ossia saper dire che gli elementi di A sono quanti gli elementi di B, e saper poi dire che l'insieme A ha n elementi, ossia ha tanti elementi quanti sono i primi n numeri naturali, ossia tanti quanti gli elementi di $[n] = \{1, 2, \ldots n\}$.

Dati due insiemi A e B, se dico $A\rho B \Leftrightarrow$ esiste una corrispondenza biunivoca da A a B, verifico che ρ è:

- riflessiva;
- simmetrica;
- transitiva.

Quindi ρ è una relazione di equivalenza nell'insieme degli insiemi finiti. $A\rho B \Leftrightarrow |A| = |B| \Leftrightarrow A \leftrightarrow B \Leftrightarrow$ la cardinalità di A è uguale alla cardinalità di B.

1.7.1 Principio della somma

Proposizione 1.7.1 (*Principio della somma*)

Dati A, B tali che $A \cap B = \emptyset$, segue che $|A \cup B| = |A| + |B|$.

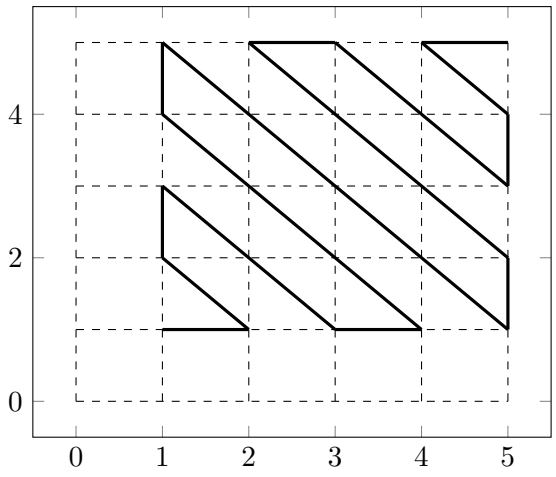

Figura 1.8: Metodo della diagonale

Dimostrazione: $|A| = m$, $|B| = n$. Devo quindi poter realizzare una corrispondenza biunivoca F fra $|A \cup B|$ e $[m+n]$. Ossia, dati $A = \{a_1, a_2, \dots a_m\}$ e $B = \{b_1, b_2 \dots b_n\}$, ho che $F(a_i) = i$ e $F(b_i) = m+i$. ■

È possibile generalizzare la regola della somma.

Proposizione 1.7.2 (*Principio della somma 2*)

Dati t insiemi $A_1, \dots A_t$ tali che $A_i \cap A_j = \emptyset$ se $i \neq j$, ho che:

$$\left| \bigcup_{i=1}^{t} A_i \right| = \sum_{i=1}^{t} |A_i|$$

1.7.2 Principio del prodotto

Proposizione 1.7.3 (*Principio del prodotto*)

Dati A, B, ho che $|A \times B| = |A| \cdot |B|$.

Dimostrazione: C'è una corrispondenza biunivoca $F : (A \times B) \to [m \cdot n]$. Quanto vale $F(a_i, b_j)$? In generale, contando con il metodo della diagonale (figura 1.8), ho che sulla diagonale k-esima trovo tutte le coppie tali per cui $i + j = k + 1$. ■

È possibile generalizzare la regola del prodotto.

Proposizione 1.7.4 (*Principio del prodotto 2*)

Se prendo un insieme finito di insiemi $\{A_1, \dots A_t\}$, ho che:

$$|A_1 \times \dots \times A_t| = |A_1| \cdot \dots \cdot |A_t|$$

Dimostrazione: Si dimostra per induzione su t. ■

Definizione 1.7.1 (*Principio del prodotto 3*)

Dato un sottoinsieme S del prodotto cartesiano X^n, $S \subseteq X^n$, ossia un insieme di n-uple, se verifico che:
- *al primo posto di una n-upla in S ci sono i_1 elementi;*
- *$\forall\, j = 2 \dots n-1$ ci sono i_j n-uple che hanno le prime $j-1$ coordinate uguali;*

allora $|S| = i_1 \cdot i_2 \cdot \dots i_n$.

1.7.3 Dimostrazioni biettive

Se voglio dimostrare che $a = b$, posso trovare due insiemi A e B tali che $|A| = a$ e $|B| = b$, e dimostrare che sono in biezione. Si indica solitamente con $A \leftrightarrow B$.

Due insiemi con intersezione disgiunta possono essere i due blocchi di una partizione con due soli blocchi.

Proposizione 1.7.5

Dato l'insieme delle funzioni da A in R $R^A = \{f : A \to R\}$, se $|A| = n$ e $|R| = r$, allora $\left|R^A\right| = r^n = |R^n|$. Quindi esiste una biezione fra R^A e R^n. R^n è il prodotto di R con sé stesso n volte. Quindi le funzioni da A in R sono quante le R-uple di n elementi.

Dimostrazione: Data una funzione $f : A \to R$, definisco $F : R^A \to R^n$ tale che $(f, A = \{a_1, \dots a_n\}) \mapsto (f(a_1), \dots f(a_n))$, che dal punto di vista dell'occupazione è:

$$\begin{matrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{matrix}$$

Ossia, ad ogni funzione $f : A \to R$ associo la n-upla dei valori di f ordinata seguendo un ordine lineare degli elementi di A. ■

Proposizione 1.7.6

Dati A, B disgiunti, $R^A \times R^B$ ha cardinalità $\left|R^A \times R^B\right| = \left|R^{A \cup B}\right|$, dato che $\left|R^A\right| = r^n$ e $\left|R^B\right| = r^m$ e che quindi $r^n \cdot r^m = r^{n+m}$.
Quindi $\left|R^A \times R^B\right|$ e $\left|R^{A \cup B}\right|$ sono in corrispondenza biunivoca.

Dimostrazione: Esiste una biezione $F : R^A \times R^B \to R^{A \cup B}$. Questa funzione prende una coppia di funzioni e ne restituisce una terza $(f : A \to R, g : B \to R) \mapsto h : (A \cup B) \to R$ definita come, $\forall\, x \in A \cup B$:

$$h(x) = \begin{cases} f(x) \text{ se } x \in A \\ g(x) \text{ se } x \in B \end{cases}$$

■

Dati due insiemi R, S ed un insieme A:

$$\left|R^A \times S^A\right| = \left|(R \times S)^A\right|$$

$$\left|(R^A)^B\right| = \left|R^{A \cdot B}\right|$$

Esercizio 13

Definire la biezione che dimostra le due proprietà precedenti.

La maggior parte dei numeri positivi che compaiono in combinatoria hanno un'interpretazione in teoria degli insiemi.

1.7.4 Fattoriale decrescente

Definizione 1.7.2

Il fattoriale decrescente è una successione:

$$\{[r]_n\}_{n\in\mathbb{N}} : \begin{cases} [r]_0 = 1 \\ [r]_{n+1} = [r]_n \cdot (r-n) \end{cases} \tag{1.1}$$

È evidente che:

$$[r]_n = \frac{r!}{(r-n)!}$$

Osservazione 2

$[r]_n = 0$ se $r < n$. Inoltre, $[r]_n = n!$ se $r = n$.

Proposizione 1.7.7

Dato $In(A,R)$, l'insieme delle funzioni iniettive da A in R, se $|A| = n$ e $|R| = r$, allora $|In(A,R)| = [r]_n$.
In altre parole, il fattoriale decrescente $[r]_n$ corrisponde all'insieme delle funzioni iniettive da A in R $In(A,R)$.

$$|In(A,R)| = |In(A - \{x\}, R)| \cdot |R - Im_f|$$

Dimostrazione: Ricordiamo la definizione di iniettività: $\forall\ x, y \in A$ se $f(x) = f(y) \Rightarrow x = y$, f è iniettiva.

Dimostriamo ora la proposizione per induzione. Se $A = \emptyset$, $|In(\emptyset, R)| = 1$.

Supponendo di aver calcolato il numero di funzioni inettive da un insieme con n elementi ad un insieme con r elementi (ossia $[r]_n$), dobbiamo determinare $[r]_{n+1}$.

Se $|A| = (n+1)$, sapendo che tutti gli elementi di A sono distinti, prendo $x \in A$.

Data una funzione $f : A \to R$, questa individua una coppia $(f(x), f^- : A \setminus \{x\} \to R)$ dove f^- è definita come f ossia $f^-(a) = f(a)$.

In quanti modi si può scegliere $f(x)$? In $\left|R \setminus Im_{f^-}\right|$ modi (ossia, $r-n$). Le funzioni iniettive da $A \setminus \{x\}$ in R sono $[r]_n$ per definizione, quindi per il principio del prodotto il numero di coppie che posso creare sono $[r]_{n+1} = [r]_n \cdot (r-n)$. ■

Proposizione 1.7.8

Sappiamo che $|\mathbb{P}(A)| = \left|2^A\right| = 2^n$ con $|A| = n$. Quanti sono i sottoinsiemi pari di A, ossia $S \subseteq A$ t.c. $|S| = 2k$?
Gli insiemi di cardinalità pari sono tanti quanti quelli di cardinalità dispari, quindi sono 2^{n-1}.

Dimostrazione: So che $2^{n-1} = |\mathbb{P}(A \setminus \{x\})|$, quindi l'insieme dei sottoinsiemi pari di A è in biezione con l'insieme delle parti di A a cui ho tolto un elemento. Indicando con P l'insieme dei sottoinsiemi pari di A, ho una biezione $F : \mathbb{P}(A \setminus \{x\}) \to P$:

$$F(S) = \begin{cases} S \text{ se } S \text{ è pari} \\ S \cup \{x\} \text{ se } S \text{ è dispari} \end{cases}$$

■

1.7.5 Coefficienti binomiali

Indichiamo con $\binom{n}{k}$ il numero di sottoinsiemi con k elementi di un insieme con n elementi. Vediamo subito che $\binom{n}{k}$ per $k > n$ è 0. $\binom{n}{0} = 1$, $\binom{n}{1} = n$. Inoltre $\binom{n}{k} = \binom{n}{n-k}$, ossia il numero di sottoinsiemi con k elementi è uguale al numero dei loro insiemi complementari.

Proposizione 1.7.9 (*Definizione ricorsiva di Pascal dei coefficienti binomiali*)

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \tag{1.2}$$

$\binom{n}{k}$ è il numero di sottoinsiemi con k elementi, indicato con $\mathbb{P}_k(A)$. Lo divido in due sottoinsiemi disgiunti, con cardinalità rispettivamente $\binom{n-1}{k}$ e $\binom{n-1}{k-1}$.
Fissato un $x \in A$, $\binom{n-1}{k}$ è l'insieme di tutti i sottoinsiemi con k elementi di $A \setminus \{x\}$, $\binom{n-1}{k-1}$ è l'insieme di tutti i sottoinsiemi con $k-1$ elementi di $A \setminus \{x\}$.

Dimostrazione: $\forall\ S \subseteq A$ con $|S| = k$ e $x \in A$ ho due casi: $x \in S$ o $x \notin S$. Definisco la biezione $F : \mathbb{P}_k(A) \to \mathbb{P}_k(A \setminus \{x\}) \cup \mathbb{P}_{k-1}(A \setminus \{x\})$ come:

$$F(S) = \begin{cases} S \text{ se } x \notin S \\ S \setminus \{x\} \text{ se } x \in S \end{cases}$$

Ho quindi che $\mathbb{P}_k(A) = X \cup Y$ con $X = \{S \subseteq A : |S| = k \wedge x \in S\}$ e $Y = \{S \subseteq A : |S| = k \wedge x \notin S\}$. Se tolgo x da A, le cardinalità dei due insiemi diventano $|X| = \binom{n-1}{k-1}$ e $|Y| = \binom{n-1}{k}$. ■

Proposizione 1.7.10

Quanto valgono i coefficienti binomiali? Diciamo questo:

$$[r]_n = n! \cdot \binom{r}{n}$$

da cui segue che:

$$\binom{r}{n} = \frac{[r]_n}{n!} = \frac{r!}{n! \cdot r - n!}$$

Stiamo dicendo quindi che $[r]_n$ (il numero di funzioni iniettive da A in R con $|A| = n$ e $|R| = r$) è uguale alla cardinalità di un insieme di coppie $|E|$. $n!$ è il numero di elementi al secondo posto della coppia, $\binom{r}{n}$ è il numero di elementi al primo posto.

Dimostrazione: $\binom{r}{n}$ è il numero di sottoinsiemi con n elementi di un insieme con r elementi.

$$E = \{(S, ?) \text{ con } |S| = n \wedge S \subseteq R\}$$

Abbiamo visto che ogni funzione $f : A \to R$ individua un'insieme immagine $Im_f \subseteq R$ e una partizione $\ker f \in \Pi(A)$, e che questi due insiemi sono in corrispondenza biunivoca $|Im_f| = |\ker f|$.

Se prendo una funzione iniettiva, il nucleo della funzione è la partizione più piccola, avendo per elementi le classi rappresentate dai singoli elementi del dominio. Quante sono le iniezioni $In(A, S)$ con $S = Im_f$? $[n]_n = n!$

Quindi, $E = \{(S, \bar{f} : A \to S)$, con $|S| = n \wedge S \subseteq R$ e $\bar{f} : A \to S$ insieme delle biezioni da A in $S\ \}$ ■

1.7.6 Teorema binomiale

Proposizione 1.7.11 (*Teorema binomiale*)

$$\forall\ n \in \mathbb{N}\ con\ n > 0\ (x+y)^n = \sum_{k=0}^{n} \binom{n}{k}\ x^k y^{n-k}$$

Si possono dimostrare anche identità polinomiali con le biezioni. Quando sono uguali due polinomi? Quando nel loro sviluppo hanno tutti i coefficienti uguali.

Teorema 1.7.12 (*Identità polinomiale*)

Dati due polinomi in n variabili $p(x_1,\ \dots\ x_n)$ e $q(x_1,\ \dots\ x_n)$, sono uguali se coincidono su insiemi infiniti, ossia se $\forall\ (a_1,\ \dots\ a_n) \in I^n$ con $I \subseteq \mathbb{R}$ e $|I| = \infty$, $p(a_1,\ \dots\ a_n) = q(a_1,\ \dots\ a_n)$, ossia i due polinomi coincidono ($p = q$).

Al posto di x e di y posso quindi mettere due interi $r, s \in \mathbb{N}$, e dimostrare che $(r+s)^n = \sum_{k=0}^{n} \binom{n}{k} r^k s^{n-k}$.

Dimostrazione: Il membro sinistro della proposizione equivalente alla definizione 1.7.11, $(r+s)^n$, è la cardinalità dell'insieme di funzioni da un insieme con n elementi ad uno con cardinalità $r+s$, ossia all'unione disgiunta di due insiemi con cardinalità rispettivamente r e s. Dicendo quindi che gli insiemi A, R e S hanno cardinalità $|A| = n$, $|R| = r$ e $|S| = s$, e che $T = R \cup S$, ho che $(r+s)^n = \left|T^A\right|$.
Il membro destro della proposizione è una somma, quindi corrisponde all'unione disgiunta di n insiemi.

$$\left|\bigsqcup_{k=0}^{n} E_k\right| = \sum_{k=0}^{n} |E_k|\ \text{ con }\ |E_k| = \binom{n}{k}\ r^k s^{n-k}$$

Devo definire l'insieme E_k. Per il principio del prodotto, è una terna:

$$\left(X,\ f_k : X \to R,\ g_{(n-k)} : (A \setminus X) \to S\right)$$

con $X \subseteq A$ tale che $|X| = k$, f_k appartenente all'insieme delle funzioni da X in R, e $g_{(n-k)}$ appartenente all'insieme delle funzioni da $A \setminus X$ (ossia il complementare di X) in S.
Dobbiamo mostrare ora che $T^A \leftrightarrow \bigsqcup E_k$, ossia che c'è una biezione. La funzione biettiva F associa ad una funzione $f : A \to T$ una terna:

$$\left(f^{-1}(R),\ f_k : X \to R,\ g_{(n-k)} : (A \setminus X) \to S\right) \in E_k$$

con $f^{-1}(R) = X$ a indicare la controimmagine di R e $\left|f^{-1}(R)\right| = k$. ■

1.7.7 Coefficienti multinomiali

Il coefficiente multinomiale, indicato con:

$$\binom{n}{k_1 \dots k_t}$$

è il numero delle t-scomposizioni di un insieme A con n elementi nella forma $(E_1, \dots, E_t)$ tali che $|E_1| = k_1, \dots |E_t| = k_t$.

Definizione 1.7.3 (*t-scomposizioni*)

Sia A un insieme con n elementi, una t-scomposizione di A è una t-upla $(E_1, \dots E_t)$ tale che:

1S $\bigsqcup_{i=1}^{t} E_i = A$
2S $E_i \cap E_j = \emptyset$ *se* $i \neq j$
E_i *è detto blocco.*

Ci sono due differenze fra una t-scomposizione e una partizione.

- Un blocco di una scomposizione può anche essere vuoto, un blocco di una partizione è necessariamente $\neq \emptyset$.
- Considero un insieme $A = \{a, b, c, d, e, f, g\}$. Posso avere una partizione:

  $$\pi = \{\{a\}, \{b, g, f\}, \{c, d\}, \{e\}\}$$

  e due 4-scomposizioni distinte:

  $$(\{a\}, \{b, g, f\}, \{c, d\}, \{e\}) \neq (\{a\}, \{c, d\}, \{b, g, f\}, \{e\})$$

  poiché le t-scomposizioni sono ordinate.

Il coefficiente multinomiale è una generalizzazione del coefficiente binomiale.

$$\binom{n}{k} = \binom{n}{k, n-k}$$

Partendo da questa uguaglianza, so che:

$$\binom{n}{k} = \binom{n}{k, n-k} = \frac{n!}{k!\ (n-k)!} \Rightarrow \binom{n}{k_1, \dots k_t} = \frac{n!}{k_1!\ \dots\ k_t!}$$

Proposizione 1.7.13

Il numero delle t-scomposizioni di A $(E_1, \dots E_t)$ *di* A *(indicato anche con* $E_1 + \dots + E_t = A$*) tali che* $|E_1| = k_1, \dots |E_t| = k_t$ *è:*

$$\binom{n}{k_1, \dots k_t} = \frac{n!}{k_1!\ \dots\ k_t!} \tag{1.3}$$

Dimostrazione: Per $t = 2$ è vero. Supponiamo sia vero per $t > 2$. Prendiamo una $(t+1)$-scomposizione $(E_1, \dots, E_t, E_{t+1})$ di A. Ogni scomposizione individua una coppia:

$$(E_{t+1}, (E_1, \dots E_t))$$

in cui $E_{t+1} \subseteq A$ e $(E_1, \dots E_t)$ è una t-scomposizione di $A \setminus E_{t+1}$, poiché $E_1 + \dots + E_t + E_{t+1} = A$.
In quanti modi posso scegliere un sottoinsieme $|E_{t+1}| = k_{t+1}$? In $\binom{n}{k_{t+1}}$ modi. Quindi quante coppie $(E_{t+1}, (E_1, \dots E_t))$ ho? È un prodotto, e per il principio del prodotto:

$$\binom{n}{k_{t+1}} \cdot \frac{(n - k_{t+1})!}{k_1! \dots k_t!}$$

Semplificando, si ottiene la tesi. ■

1.7.8 Teorema multinomiale

Proposizione 1.7.14

$$(x_1 + \cdots + x_t)^n = \sum_{(k_1,\ldots k_t):k_1+\ldots k_t=n} \binom{n}{k_1,\ldots,k_t} x_1^{k_1} \ldots x_t^{k_t} \tag{1.4}$$

Dove la sommatoria indica la somma di tutte le t-uple $(k_1, \ldots k_t)$ tali che $k_1 + \cdots + k_t = n$.

Dimostrazione: Si dimostra di nuovo per biezione. Prendo $x_i = r_i \in \mathbb{N}$. Quindi:

$$(r_1 + \cdots + r_t)^n = \sum_{(k_1,\ldots k_t):k_1+\ldots k_t=n} \binom{n}{k_1,\ldots,k_t} r_1^{k_1} \ldots r_t^{k_t}$$

Il membro sinistro è uguale alla cardinalità dell'insieme delle funzioni da A in T tali che $T = R_1 \cup \cdots \cup R_t$, in cui R_i con $i \in [1, t]$ sono insiemi a due a due disgiunti tali che $|R_i| = r_i$.

Ogni funzione individua una scomposizione di A in t-blocchi, in cui ogni blocco è dato dalla controimmagine $f^{-1}(R_i)$ ed ha cardinalità k_i.

Il membro destro è dato quindi dall'unione disgiunta di una serie di insiemi di $(t+1)$-tuple. Ciascuna $(t+1)$-upla ha al primo posto una t-scomposizione di A, e all'$(i+1)$-esimo posto una funzione dal blocco K_i nell'insieme R_i. Per il principio del prodotto, il numero di queste $(t+1)$-uple, per ogni possibile t-scomposizione, è proprio:

$$\binom{n}{k_1,\ldots,k_t} r_1^{k_1} \ldots r_t^{k_t}$$

Come nel caso del teorema binomiale, per dimostrare la biezione basta definire la funzione biettiva $F : T^A \to$ l'insieme di queste $(t+1)$-uple, che a ciascuna funzione $f : A \to T$ associa la t-scomposizione di A in cui ogni blocco è definito dalla controimmagine $f^{-1}(R_i)$ e tutte t funzioni che da un blocco K_i vanno in R_i. ■

Corollario 1.7.15 (*Corollario del teorema multinomiale*)

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

Dimostrazione:

$$(x-1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k x^{n-k}$$

Ponendo $x = 1$, per il teorema binomiale, ho la tesi. ■

1.7.9 Principio dei cassetti

R^A è l'insieme delle funzioni da A in R. $\left|R^A\right| = r^n$. Una funzione $f : A \to R \in R^A$ la posso interpretare in due modi:

Punto di vista dell'occupazione A viene interpretato come un insieme di oggetti. Il codominio R viene interpretato come un insieme di cassetti. Quindi una funzione da A in R è un modo di disporre gli oggetti di A nei cassetti di R.

Punto di vista della distribuzione Rappresento l'insieme A come un insieme di posti, e l'insieme R come un insieme di lettere (ossia come un alfabeto). Una funzione $f : A \to R$ mi dà una parola, ossia un modo di disporre le lettere di R nei posti di A.

Proposizione 1.7.16 (*Principio dei cassetti*)

Se $|A| > |R|$ non esistono funzioni iniettive da A in R.

Dal punto di vista dell'occupazione, se si mettono $|A| = n$ oggetti in $|R| = r$ cassetti con $n > r$, allora almeno un cassetto conterrà più di un oggetto.

Dal punto di vista della distribuzione, ogni parola di lunghezza n con lettere in un alfabeto di cardinalità r, con $n > r$, contiene almeno una lettera ripetuta.

I due punti di vista hanno una formalizzazione matematica distinta.

Proposizione 1.7.17

Dato un triangolo equilatero di lato 1, e dati 5 punti interni, almeno 2 di essi hanno distanza minore di $\frac{1}{2}$.

Dimostrazione: Si può partizionare il triangolo in 4 blocchi come in figura 1.9, in modo che dati due punti qualsiasi in uno stesso blocco questi siano a meno di $\frac{1}{2}$ di distanza.

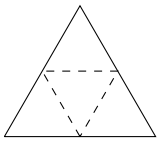

Figura 1.9: Le quattro partizioni possibili

Proposizione 1.7.18

Se si colorano i punti del piano con due colori (R,B) esister un rettangolo con tutti i vertici dello stesso colore.

Dimostrazione: Se prendo tre punti allineati, so che almeno due hanno lo stesso colore. Se prendo nove terne di punti allineati, a loro volta allineate in modo da poter formare un rettangolo con ciascuna coppia di terne, so che almeno due terne hanno la stessa combinazione di colori (figura 1.10).

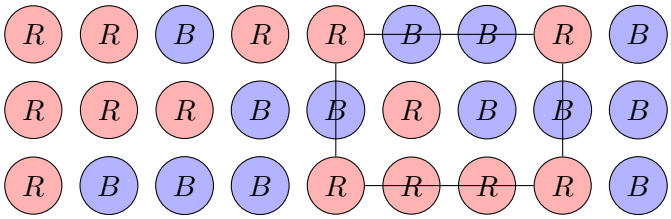

Figura 1.10: Il rettangolo realizzabile sul piano colorato

Esempio:

Prendo l'insieme $I = \{0, 1, 2\}$ e definisco $X = I \times I \times I$. Definisco la relazione di equivalenza ρ come:

$$(x, y, z)\ \rho\ (x', y', z') \Leftrightarrow \{x, y, z\} = \{x', y', z'\}$$

ρ divide X in classi di equivalenza. Quali sono gli elementi della classe $[(0,1,0)]$? Posso indicarla con $[\{0,1\}]$, ed è evidente che gli elementi della classe sono 6.

1.7.10 Principio di inclusione/esclusione

Proposizione 1.7.19

Sia Γ un insieme e siano $A_1, \ldots, A_t$ sottoinsiemi finiti di Γ.

$$|A_1 \cup A_2 \cup \ldots \cup A_t| = \sum_{\emptyset \neq I \subseteq \{1,\ldots,t\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| \tag{1.5}$$

Dimostrazione: Si può dimostrare per induzione, o si può fare una dimostrazione combinatoria. La dimostrazione combinatoria calcola il contributo alla somma di ogni elemento dell'unione.

Prendiamo $x \in A_1 \cup \cdots \cup A_t$ e siano $A_{j_1} \ldots A_{j_n}$ i sottoinsiemi che contengono x, ossia se $i \neq j_1, \ldots j_n$ allora $x \notin A_i$. Il contributo che x porta alla somma è evidentemente 1, perché la cardinalità dell'unione aumenta di uno.

Per $|I| = 1$ aggiungerò 1 per ogni sottoinsieme $A_{j_1} \ldots A_{j_n}$, ossia per ogni sottoinsieme contenente x poiché ogni altro A_i non aggiungerà niente alla somma. Per $k > 1$ il contributo alla somma sarà 1 solo per le intersezioni fra i sottoinsiemi $A_{j_1} \ldots A_{j_n}$, e 0 per ogni intersezione contenente un altro A_i. Quindi il contributo di x alla somma sarà:

$$\sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k}$$

So che, per il corollario 1.7.15:

$$\sum_{k=0}^{n} (-1)^{k} \binom{n}{k} = 0$$

Quindi:

$$1 + \sum_{k=1}^{n} (-1)^{k} \binom{n}{k} = 1 - \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} \Rightarrow \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} = 1$$

■

1.7.11 Numeri di Stirling di prima e seconda specie

Se indico con $S(n,k)$ (numero di Stirling di II specie) il numero delle partizioni in k-blocchi *non vuoti* di un insieme con n elementi, indicando con $Sur(A,R)$ l'insieme delle funzioni suriettive da A in R, posso esprimere il numero delle funzioni suriettive $|Sur(A,R)|$ come $S(n,r) \cdot r!$, con $|A| = n$ e $|R| = r$.

Ogni funzione suriettiva $f : A \to R$ individua biunivocamente una coppia (π, F) dove π è una partizione di A in $|R|$-blocchi, in cui ogni blocco (necessariamente non vuoto, o la funzione non sarebbe suriettiva) è individuato dalla controimmagine $f^{-1}(r)$ $\forall\ r \in R$, ed F è una biezione da $\pi \to R$. Quindi se voglio costruire una funzione suriettiva da A in R, partiziono A in r blocchi *non vuoti* e creo una biezione dai blocchi individuati in A ad R.

Ora troviamo $|Sur(A,R)|$ usando il principio di inclusione/esclusione.

Possiamo trovare il numero delle funzioni suriettive dall'insieme di tutte le funzioni R^A togliendo le funzioni non suriettive.

Supponiamo per semplicità che $R = \{1, \ldots, r\} = [r]$. f non è suriettiva $\Leftrightarrow$ $\exists\ i = 1, \ldots, r$ tale che $i \notin Im_f$. Se indico con $A_i = \{f : A \to R : i \notin Im_f\}$, l'unione $A_1 \cup \ldots \cup A_r$ è l'insieme delle funzioni non suriettive.

$$Sur(A, R) = \left|R^A\right| - |A_1 \cup \cdots \cup A_r|$$

Calcoliamo $|A_1 \cup \ldots \cup A_r|$ con il principio di inclusione/esclusione.

$$|A_1 \cup \ldots \cup A_r| = \sum_{\emptyset \neq I \subseteq \{1,\ldots,r\}} (-1)^{|I|-1} \left|\bigcap_{i \in I} A_i\right|$$

Se prendo I costituito da un solo elemento, $|A_1| = \left|(R \setminus \{1\})^A\right| = (r-1)^n$, quindi la cardinalità del generico $A_i = (r-1)^n$.

Con $|I| = 2$, la cardinalità dell'intersezione $|A_1 \cap A_2| = (r-2)^n$. In generale $|A_{i_1} \cap \cdots \cap A_{i_r}| = (r-k)^n$.

Quindi generalizzando:

$$(-1)^0 \cdot \binom{r}{1} \cdot (r-1)^n + (-1)^1 \cdot \binom{r}{2} \cdot (r-2)^n \cdots = \sum_{k=1}^{n} (-1)^{k-1} \binom{r}{k} (r-k)^n$$

Sapendo che r^n è $(-1)^0\binom{r}{0}\ (r-0)^n$:

$$\begin{aligned} |Sur(A, R)| = r^n - \sum_{k=1}^{n} (-1)^{k-1} \binom{r}{k} (r-k)^n = \\ r^n + \sum_{k=1}^{n} (-1)^{k} \binom{r}{k} (r-k)^n = \\ \sum_{k=0}^{n} (-1)^{k} \binom{r}{k} (r-k)^n \end{aligned}$$

Quindi il numero di Stirling di II specie è:

$$S(n, r) = \frac{|Sur(A, R)|}{r!} = \frac{1}{r!} \sum_{k=0}^{n} (-1)^k \binom{r}{k} (r-k)^n \tag{1.6}$$

Per il teorema di omomorfismo, data una funzione $f : A \to R$, ho che $|\ker f| = |Im_f|$. Consideriamo la funzione $F : \ker f \to Im_f$ che ad ogni blocco associa l'immagine degli elementi del dominio nel bocco ($F[x] = f(x)$), e definiamo la funzione $\bar{F} : \ker f \to R$ costruita a partire da F tale che $\bar{F}[x] = f(x)$ in genere non è biunivoca, a meno che la funzione f sia suriettiva. Di norma è solo iniettiva.

Diciamo questo:

$$f : A \to R \leftrightarrow (\ker f, \bar{F} : \ker f \to R \text{ iniettiva}) \tag{1.7}$$

L'insieme delle funzioni da A in R è in corrispondenza biunivoca con l'insieme di coppie con al primo posto una partizione di A ed al secondo posto una funzione $\bar{F}$ che a ciascun blocco di A associa elementi distinti di R (ossia, $\bar{F}$ è iniettiva).

Quindi:

$$r^n = \sum_{k=1}^{r} S(n, k) \cdot [r]_k$$

Si può scrivere anche come polinomio:

$$x^n = \sum_{k=1}^{r} S(n,k) \cdot [x]_k$$

Dall'algebra lineare si impara che la successione delle potenze e la successione dei fattoriali decrescenti si possono esprimere l'uno in funzione dell'altra, ed i coefficienti di cui sopra si possono invertire. Non lo dimostriamo qui.

$$[x]_n = \sum_{k=1}^{r} s(n,k) x^k$$

Il coefficiente $s(n,k)$ indica il numero di Stirling di prima specie.

1.7.12 Anagrammi

Esempio :

---

1. determinare il numero degli "anagrammi" (anche privi di senso) di MATEMATICA;
2. determinare il numero degli anagrammi che contengono almeno una di queste sequenze:
   - MATE;
   - ATI;
   - MAC.

Dal punto di vista della distribuzione, il dominio è un insieme di posti P di cardinalità 10, mentre il codominio è l'insieme delle lettere $L = \{\text{A, C, E, I, M, T}\}$. La parola MATEMATICA è una funzione $f : P \to L$ che associa ad ogni posto del dominio una lettera del codominio. Gli anagrammi di MATEMATICA sono tutte quelle funzioni tali per cui le cardinalità delle controimmagini delle lettere A, M e T sono:

$$\left|f^{-1}(A)\right| = 3$$
$$\left|f^{-1}(M)\right| = 2$$
$$\left|f^{-1}(T)\right| = 2$$

Sappiamo che ogni funzione individua un nucleo, ossia, in questo caso, una 6-scomposizione $E_1, \dots E_6$ dell'insieme dei posti. Quale 6-scomposizione dell'insieme dei posti è individuata dal nucleo della funzione che individua la parola "MATEMATICA"? Quindi per trovare gli

A	C	E	I	M	T
E_1	E_2	E_3	E_4	E_5	E_6
$\{2,6,10\}$	$\{9\}$	$\{4\}$	$\{8\}$	$\{1,5\}$	$\{3,7\}$

anagrammi devo trovare le 6-scomposizioni tali che $|E_1| = 3$, $|E_2| = 1$, $|E_3| = 1$, $|E_4| = 1$, $|E_5| = 2$, $|E_6| = 2$. La scomposizione $(\{7,1,2\},\{10\},\{3\},\{6\},\{4,5\},\{8,9\})$, ad esempio, individua l'anagramma AAEMMIATTC. Per la proposizione 1.7.13 è:

$$\frac{10!}{3!\ 2!\ 2!}$$

Adesso dobbiamo trovare il numero di anagrammi contenenti le sequenze richieste:

- A_1 = insieme degli anagrammi che contengono la sequenza MATE.
- A_2 = insieme degli anagrammi che contengono la sequenza ATI.
- A_3 = insieme degli anagrammi che contengono la sequenza MAC.

$|A_1 \cup A_2 \cup A_3|$ è la risposta al secondo punto, e posso calcolarlo con il principio di inclusione ed esclusione, secondo il quale:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

Consideriamo ciascuna sequenza come un'unica lettera.

Con A_1 il codominio è {(MATE), A, C, I, M, T}, con la A ripetuta due volte ($|E_{\mathrm{A}}| = 2$), e il dominio ha 7 posti. Quindi:

$$|A_1| = \frac{7!}{2!}$$

Con A_2 il codominio è {(ATI), A, C, E, M, T}, con la A e la M ripetute due volte ciascuna ($|E_{\mathrm{A}}| = 2$ e $|E_{\mathrm{M}}| = 2$), e il dominio ha 8 posti.

$$|A_1| = \frac{8!}{2!\ 2!}$$

Con A_3 il codominio è {(MAC), A, E, I, M, T}, con la A e la T ripetute due volte ciascuna ($|E_{\mathrm{A}}| = 2$ e $|E_{\mathrm{T}}| = 2$), e il dominio ha 8 posti.

$$|A_1| = \frac{8!}{2!\ 2!}$$

Ora devo trovare le cardinalità delle intersezioni $|A_1 \cap A_2|$, $|A_1 \cap A_3|$ e $|A_2 \cap A_3|$.

Con $A_1 \cap A_2$ il codominio è {(MATE), (ATI), A, C, M}, e il dominio ha 5 posti.

$$|A_1 \cap A_2| = 5!$$

Con $A_1 \cap A_3$ il codominio è {(MATE), (MAC), A, I, T}, e il dominio ha 5 posti.

$$|A_1 \cap A_3| = 5!$$

Con $A_2 \cap A_3$ il codominio è {(ATI), (MAC), A, E, M, T}, e il dominio ha 6 posti.

$$|A_2 \cap A_3| = 6!$$

Ora devo trovare la cardinalità dell'intersezione $|A_1 \cap A_2 \cap A_3|$. Il codominio è {(MATE), (MAC), (ATI)}, e il dominio ha 3 posti.

$$|A_1 \cap A_2 \cap A_3| = 3!$$

Adesso possiamo applicare il principio di inclusione/esclusione.

$$|A_1 \cup A_2 \cup A_3| = \frac{7!}{2!} + 2 \cdot \frac{8!}{2!\ 2!} - 2 \cdot 5! - 6! + 3!$$

Esempio :

---

1. determinare il numero degli "anagrammi" (anche privi di senso) di TRATTARE;
2. determinare il numero degli anagrammi che contengono almeno una di queste sequenze:
   - TRA;
   - ATTA;
   - ARE.

Abbiamo 8 posti. Il codominio è {A, E, R, T}. Il numero di anagrammi è:

$$\frac{8!}{2!\ 2!\ 3!}$$

- A_1 = insieme degli anagrammi che contengono TRA.
- A_2 = insieme degli anagrammi che contengono ATTA.
- A_3 = insieme degli anagrammi che contengono ARE.

Con A_1 il codominio è {(TRA), A, E, R, T}, ed ho 6 posti. $|E_{\mathrm{T}}| = 2$. Ma posso ottenere l'anagramma TRATRAET in due modi: ((TRA), T, R, A, E, T) e (T, R, A, (TRA), E, T). Quindi devo togliere il numero di parole formate da {(TRA), E, T} con $|E_{\mathrm{TRA}}| = 2$.

$$|A_1| = \frac{6!}{2!} - \frac{4!}{2!}$$

Con A_2 il codominio è {(ATTA), E, R, T}, ed ho 5 posti. $|E_{\mathrm{R}}| = 2$.

$$|A_2| = \frac{5!}{2!}$$

Con A_3 il codominio è {(ARE), A, R, T}, ed ho 6 posti. $|E_{\mathrm{T}}| = 3$.

$$|A_3| = \frac{6!}{3!}$$

Adesso dobbiamo procedere con le intersezioni.

Nel caso dell'intersezione $A_1 \cap A_2$, non posso avere la sequenza TRA e la sequenza ATTA separate, avendo solo due A nella parola TRATTARE. Quindi devo considerare TRATTA come una sola sequenza. Il codominio quindi è {(TRATTA), E, R}. Ho 3 posti.

$$|A_1 \cap A_2| = 3!$$

Per $A_1 \cap A_3$, il codominio è {(TRA), (ARE), T}, con $|E_{\mathrm{T}}| = 2$. Ho 4 posti. Ma posso anche avere la A in comune fra le due sequenze, e quindi avrei 4 posti ed un codominio {(TRARE), A, T} sempre con $|E_{\mathrm{T}}| = 2$. Quindi:

$$|A_1 \cap A_3| = \frac{4!}{2!} + \frac{4!}{2!} = 4!$$

Per $A_2 \cap A_3$, come con $A_1 \cap A_2$, ATTA e ARE devono essere considerate come una sequenza sola. Il codominio è {(ATTARE), T, R}, con 3 posti. Quindi:

$$|A_2 \cap A_3| = 3!$$

L'unico modo per intersecare tutte e tre le sequenze è la sequenza TRATTARE. Quindi $|A_1 \cap A_2 \cap A_3| = 1$.

Dato un insieme E ed una partizione tale per cui ogni classe ha lo stesso numero di elementi:

$$\frac{|E|}{\#\text{ classi}} = \#\text{ elementi di ciascuna classe}$$

Viceversa:

$$\frac{|E|}{\#\text{ elementi di ciascuna classe}} = \#\text{ classi}$$

Quindi ogni divisione può essere interpretata come una divisione fra la cardinalità di un insieme e o il numero delle classi di equivalenza, o il numero degli elementi di ciascuna classe. Sappiamo che il numero degli anagrammi di una parola di n lettere, con ciascuna lettera ripetuta k_i volte, è:

$$\frac{n!}{k_1! \dots k_t!}$$

Come possiamo interpretare questa divisione? S_n è l'insieme delle permutazioni di E con $|E| = n$, ed ha cardinalità $|S_n| = n!$. Negli anagrammi n è il numero di posti, quindi $n!$ è la cardinalità dell'insieme delle permutazioni dei posti.

Ad ogni permutazione di posti corrisponde un anagramma, ma la relazione non è biunivoca: a permutazioni distinte può corrispondere lo stesso anagramma. Dobbiamo prima definire una relazione di equivalenza sull'insieme delle permutazioni dei posti:

Definizione 1.7.4

Definisco una relazione di equivalenza ρ sull'insieme delle permutazioni e dico che, date le permutazioni σ e τ, $\sigma \ \rho \ \tau \Leftrightarrow \sigma$ e τ individuano lo stesso anagramma.

Quindi $k_1! \dots k_t!$ si può interpretare come il numero di elementi in ogni classe di equivalenza, e quindi c'è una relazione biunivoca fra l'insieme delle classi di equivalenza sulle permutazioni e l'insieme degli anagrammi:

$$\frac{n!}{k_1! \dots k_t!} = \frac{\#\text{ di permutazioni}}{\#\text{ di permutazioni equivalenti}} = \#\text{ di anagrammi}$$

Permutazioni senza punti fissi

d_n = numero delle permutazioni di E ($|E| = n$) senza punti fissi, ossia $\forall\ x \in E\ f(x) \neq x$. Supponiamo $E = \{1, 2, \dots n\} = [n]$.

Diciamo che A_i è l'insieme delle permutazioni che fissano i ($f(i) = i$). Quindi $A_1 \cup \dots \cup A_n$ è l'insieme delle permutazioni con almeno un punto fisso.

Quindi $d_n = |S_n| - |A_1 \cup \dots \cup A_n|$.

La cardinalità di ogni A_i è $(n-1)!$. La cardinalità di $A_i \cap A_j$ è $(n-2)!$. In generale, la cardinalità dell'intersezione di k insiemi distinti $|A_{i_1} \cap \dots \cap A_{i_k}| = (n-k)!$.

Sostituiamo nella formula del principio di inclusione/esclusione:

$$\sum_{\emptyset \neq I \subseteq \{1,\dots n\}} (-1)^{|I|-1} \binom{n}{|I|} \cdot (n - |I|)! = \binom{n}{1} \cdot (n-1)! - \binom{n}{2} \cdot (n-2)! \dots$$

Capitolo 2

Strutture algebriche

Gruppi, anelli, campi. In particolare, anello degli interi modulo m intero, anello dei polinomi.

2.1 Strutture algebriche con un'operazione

Una struttura algebrica è una coppia $(A, \cdot)$ dove A è un'insieme e $\cdot$ ("per") è un'operazione $\cdot : A \times A \to A$. Ad esempio $(\mathbb{N}, +)$ è una struttura algebrica.

Le operazioni sono funzioni definite su prodotti cartesiani a valori in un insieme. Un'operazione binaria è definita sul prodotto cartesiano fra due insiemi.

Riprendendo la composizione, dati tre insiemi A, B, C, B^A è l'insieme delle funzioni da A in B, C^B è l'insieme delle funzioni da B in C. La composizione $\circ$ è un'operazione definita sul prodotto cartesiano degli insiemi $B^A \times C^B$ in C^A ($\circ : B^A \times C^B \to C^A$).

Posso rappresentare un'operazione come funzione ($\circ\,(f, g)$) o inserendo l'operatore fra i due operandi ($g \circ f$).

Esempio :

$$f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \qquad f(x, y) = \sqrt{2} \cdot x + y$$

$$g : \mathbb{R} \to \mathbb{R} \times \mathbb{R} \qquad g(z) = (0, z)$$

$$g \circ f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R} \qquad (x, y) \xrightarrow{f} \sqrt{2} \cdot x + y = z \xrightarrow{g} \left(0, \sqrt{2}x + y\right)$$

$$f \circ g : \mathbb{R} \to \mathbb{R} \qquad z \xrightarrow{g} (0, z) \xrightarrow{f} \sqrt{2} \cdot 0 + z = z$$

Una struttura algebrica è un'insieme su cui è definita un'operazione che prende due elementi di quell'insieme e gliene associa un terzo.

Le strutture vengono classificate in base alle loro proprietà:

Proprietà associativa $\forall\ a, b, c \in A : a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Elemento neutro Esistenza di un'elemento neutro, o elemento identità. $1 \in A : \ \forall\ a \in A$, $a \cdot 1 = a = 1 \cdot a$

Proprietà commutativa $\forall\ a, b \in A$, $a \cdot b = b \cdot a$. In una struttura algebrica commutativa in genere l'identità si indica con 0.

Inverso Esistenza dell'inverso. $\forall\ a \in A\ \exists\ b \in A$ t.c. $a \cdot b = 1 = b \cdot a$.

2.1.1 Classificazione delle strutture algebriche con una operazione

Per essere studiabile, una struttura algebrica deve essere quantomeno associativa.

Semigruppo struttura algebrica associativa.

Monoide struttura algebrica associativa con elemento identità.

Gruppo struttura algebrica associativa con elemento identità e con inverso (ossia, monoide con inverso).

Gruppo abeliano struttura algebrica che presenta tutte e quattro le proprietà: associativa, elemento neutro, commutativa, inverso.

La struttura algebrica $(\mathbb{N}, +)$ è un monoide commutativo. Anche $(\mathbb{N}, \cdot)$ è un monoide commutativo. $(\mathbb{Z}, +)$ è un gruppo perchè esiste l'inverso. $(\mathbb{Z}, \cdot)$ invece è un monoide, perché non ha l'inverso per ogni elemento.

2.1.2 Gruppo simmetrico

Definizione 2.1.1 (*Gruppo simmetrico*)

Il prototipo di tutti i gruppi è il gruppo simmetrico su n elementi, il cui insieme è indicato con S_n. Prendiamo un insieme $E = \{e_1, \ldots, e_n\}$.

$$S_n = \{f : E \to E \text{ t.c. } f \text{ è biunivoca}\}$$

Quindi S_n è l'insieme di tutte le permutazioni degli elementi di E. Il gruppo simmetrico è definito sull'insieme S_n e l'operazione è la composizione: $(S_n, \circ)$. Verifica tutte le proprietà dei gruppi:

1. *$f \circ (g \circ h) = (f \circ g) \circ h$, ossia è associativo.*
2. *L'unità è la funzione identica (o identità) $i_E : E \to E$ tale che $\forall\ e \in E$, $i_E(e) = e$*

$$f \circ i_E = f = i_E \circ f$$

3. *Una funzione biunivoca f ha una funzione inversa g.*

$$g : E \to E \text{ t.c. } g\,(f(e)) = e$$

Una funzione $f : E \to E$ iniettiva su un insieme finito E è necessariamente suriettiva e quindi biunivoca. Un insieme è finito se non può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.

2.2 Monoidi

Un monoide $(M, \cdot)$ è una struttura algebrica con un'operazione $\cdot : M \times M \to M$ tale che:

1M L'operazione $\cdot$ è associativa;

2M $\exists\ 1_M$ t.c. $\forall\ a \in M,\ 1_M \cdot a = a = a \cdot 1_M$, ossia esiste l'elemento identità.

Un sottomonoide $(S, \cdot)$ con $S \subseteq M$ è un monoide in cui esiste l'operazione $\cdot : S \times S \to S$, ossia S è chiuso rispetto all'operazione $\cdot$, cioè $\forall\ s, s' \in S,\ s \cdot s' \in S$ e $1_M \in S$.

Ad esempio, considerando $(\mathbb{N}, +)$, il monoide $(P, +)$ con $P = \{m \in \mathbb{N} :\ \exists\ k \text{ t.c. } m = 2k\}$ è un suo sottomonoide, perchè la somma di due pari è pari e lo 0 appartiene ai pari. I dispari con il $+$ non sono un sottomonoide.

$k\mathbb{N} = \{m \in \mathbb{N} :\ \exists\ t \in \mathbb{N} \text{ t.c. } m = kt\}$ è la "versione generale" dell'insieme dei numeri pari.

Considerando $(\mathbb{N}, \cdot)$ e l'elemento neutro 1, i pari non sono un sottomonoide perché non hanno l'elemento neutro, ma i dispari sì.

2.2.1 Morfismi di monoidi

Definizione 2.2.1 (*Morfismo di monoidi*)

Dati i monoidi $(M, \cdot)$ e $(A, *)$, un morfismo di monoidi è un'applicazione $f : M \to A$ che conserva le strutture, ossia tale che $\forall\ x, y \in M$ ho che:

$$f(x \cdot y) = f(x) * f(y)$$

Inoltre, $f(1_M) = 1_A$.

2.2.2 Teorema di omomorfismo per i monoidi

Proposizione 2.2.1

Sia $f : (M, \cdot) \to (A, *)$ un morfismo di monoidi, f definisce una relazione di equivalenza ε_f tale che $\ker f = M/\varepsilon_f \cong Im_f$, ossia il quoziente è isomorfo all'immagine. Inoltre il quoziente ha una struttura di monoide:

$$(M/\varepsilon_f, \cdot) \cong (Im_f, *)$$

con $(Im_f, *)$ sottomonoide di $(A, *)$.

Dimostrazione: Ogni morfismo di monoidi $f : (M, \cdot) \to (A, *)$ individua un sottomonoide di $(A, *)$, che è $(Im_f, *)$.

Essendo f un morfismo di monoidi, $\forall\ f(x), f(y) \in Im_f,\ f(x) * f(y) = f(x \cdot y) \in Im_f$, quindi Im_f è chiuso rispetto a $*$. Devo poi verificare che $1_A \in Im_f \Leftarrow f(1_M) = 1_A$.

Anche $(\ker f, \cdot)$ è un monoide. Dobbiamo dimostrare l'esistenza dell'isomorfismo con Im_f.

$\ker f$ è l'insieme delle classi di equivalenza $[x] = \{y \in M : x\ \varepsilon_f\ y \Leftrightarrow f(x) = f(y)\} \in \ker f$.

Definiamo l'operazione di prodotto fra classi come la classe del prodotto di due rappresentanti $[x] \cdot [z] = [x \cdot z]$ qualsiasi rappresentante scelgo della classe. Bisogna verificare che questa definizione sia indipendente dai rappresentanti! Lo faremo nella sezione 2.2.4, in particolare nella dimostrazione 2.2.4.

L'operazione fra classi è associativa, perché è associativa l'operazione fra rappresentanti. Inoltre ho l'unità $[1_M]$ in $\ker f$.

L'isomorfismo fra $(Im_f, *)$ e $(\ker f, \cdot)$ segue naturalmente dal fatto che $\ker f$ e Im_f sono in biezione. Inoltre, essendo entrambi dei monoidi, la funzione f è un isomorfismo di monoidi. ■

2.2.3 Potenze (iterazioni sui monoidi)

Definizione 2.2.2 (*Potenze*)

A partire dal monoide $(M, \cdot)$ possiamo definire le iterazioni dell'operazione $\cdot$, ossia le potenze. Sia $a \in M$, si definisce:

1. $a^0 = 1_M$
2. $a^{n+1} = a \cdot a^n$

Proposizione 2.2.2 (*Commutatività della potenza*)

$\forall\, n \in \mathbb{N}$, $a \cdot a^n = a^n \cdot a$, ossia la potenza è commutativa.

Dimostrazione: Si dimostra per induzione. Si vede subito che con $n = 0$, per definizione $a \cdot a^0 = a = a^0 \cdot a$.

Per definizione di potenza $a \cdot a^{n+1} = a \cdot a \cdot a^n$, per ipotesi induttiva $a \cdot a^n \cdot a$ che di nuovo per definizione di potenza è $a^{n+1} \cdot a$. ■

Proposizione 2.2.3

Valgono tutte le proprietà tipiche delle potenze:

$$a^{m+n} = a^m \cdot a^n$$

Dimostrazione: Si dimostra anche questo per induzione su n. Con $n = 0$, $a^{m+0} = a^m = a^m \cdot 1_M = a^m \cdot a^0$.

Passo induttivo: $a^{m+n+1} = a \cdot a^{m+n}$ per definizione di potenze. Applicando l'ipotesi induttiva, $a \cdot a^{m+n} = a \cdot a^m \cdot a^n$. Per commutatività $a \cdot a^m \cdot a^n = a^m \cdot a \cdot a^n = a^m \cdot a^{n+1}$. ■

Teorema 2.2.4

Dato un monoide $(M, \cdot)$ ed un elemento $a \in M$, esiste un solo morfismo di monoidi $f : (\mathbb{N}, +) \to (M, \cdot)$ tale che $f(1) = a$, ed è $f(n) = a^n$.

Dimostrazione: f è un morfismo di monoidi, quindi deve verificare che $f(m + n) = f(m) \cdot f(n)$ e che $f(0) = 1_M$.

Per le proprietà delle potenze dimostrate precedentemente, $f(m + n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$, e $f(0) = a^0 = 1_M$ per la definizione delle potenze.

Inoltre verifica la condizione $f(1) = a$, infatti $f(1) = a^1 = a \cdot a^0 = a \cdot 1_M = a$.

Dobbiamo dimostrare l'unicità di f. Sia $g : (\mathbb{N}, +) \to (M, \cdot)$ un morfismo tale che $g(1) = a$, dimostriamo che $\forall\, n \in \mathbb{N}$, $g(n) = f(n) = a^n$.

Dimostriamolo per induzione su n. Per definizione di morfismo di monoidi, $g(0) = 1_M = f(0) = a^0$.

Supponiamo che $g(n) = f(n)$, per definizione di morfismo di monoidi $g(n + 1) = g(1) \cdot g(n) = a \cdot g(n) = a \cdot f(n) = a \cdot a^n = a^{n+1}$. ■

Esempio :

Sia Γ un insieme, la struttura algebrica $(\mathbb{P}(\Gamma), \cup)$ è in particolare un monoide. L'unione è associativa ($(A \cup B) \cup C = A \cup (B \cup C)$), ed esiste l'elemento neutro $\emptyset$.

Anche $(\mathbb{P}(\Gamma), \cap)$ è un monoide, con Γ come elemento neutro, poiché $\forall\ A, \Gamma \cap A = A$. Abbiamo quindi due esempi di monoidi commutativi.

Fissato un insieme $S \subseteq \Gamma$ diverso da $\emptyset$, possiamo considerare il suo insieme delle parti $\mathbb{P}(S)$ e definire l'applicazione $f : \mathbb{P}(\Gamma) \to \mathbb{P}(S)$ tale che $f(A) = A \cap S$.

Verifichiamo che questa applicazione è un morfismo di monoidi rispetto a $(\mathbb{P}(\Gamma), \cup)$ e $(\mathbb{P}(S), \cup)$. Dobbiamo dimostrare che $f(A \cup B) = f(A) \cup f(B)$. Infatti $f(A \cup B) = (A \cup B) \cap S = (A \cap S) \cup (B \cap S)$ per la proprietà distributiva, che è proprio $f(A) \cup f(B)$.

Inoltre l'applicazione conserva l'elemento neutro, poiché $f(\emptyset) = \emptyset \cap S = \emptyset$.

Verifichiamo che è un morfismo di monoidi anche rispetto $(\mathbb{P}(\Gamma), \cap)$ e $(\mathbb{P}(S), \cap)$. $f(A \cap B) = f(A) \cap f(B)$, infatti $(A \cap B) \cap S = (A \cap S) \cap (B \cap S)$ sempre per la proprietà distributiva. E anche in questo caso l'applicazione conserva l'elemento neutro, poiché $f(\Gamma) = \Gamma \cap S = S$, ed S è proprio l'elemento neutro di $(\mathbb{P}(S), \cap)$.

Esempio :

Sia $f : \mathbb{P}(\Gamma) \to \mathbb{P}(\Gamma)$ un'applicazione tale che $f(A) = \bar{A} = \{x \in \Gamma : x \notin A\}$, ossia che associa ad A il suo complementare $\bar{A}$. L'applicazione $f : (\mathbb{P}(\Gamma), \cup) \to (\mathbb{P}(\Gamma), \cap)$ è un morfismo di monoidi visto che verifica $f(A \cup B) = f(A) \cap f(B)$ per le leggi di De Morgan ($\overline{A \cup B} = \bar{A} \cap \bar{B}$) e $f(\emptyset) = \bar{\emptyset} = \Gamma$.

Possiamo considerare la stessa applicazione come un morfismo di monoidi da $f : (\mathbb{P}(\Gamma), \cap) \to (\mathbb{P}(\Gamma), \cup)$. Infatti $f(A \cap B) = \overline{A \cap B} = \bar{A} \cup \bar{B} = f(A) \cup f(B)$ e $f(\Gamma) = \bar{\Gamma} = \emptyset$.

2.2.4 Congruenze

Definizione 2.2.3

Le congruenze sono relazioni d'equivalenza definite sulle strutture algebriche. Sia ε una relazione d'equivalenza su A, con $(A, \cdot)$ monoide, si dice che ε è una congruenza rispetto all'operazione $\cdot$ se, dati $a\ \varepsilon\ b$ e $c\ \varepsilon\ d$, ho che $a \cdot c\ \varepsilon\ b \cdot d$.

Vuol dire che, dati $a \in [a]$ e $c \in [c]$, se $a \cdot c \in [a \cdot c]$ e ho una congruenza, allora $b \in [a]$ e $d \in [c]$ sono tali che $b \cdot d \in [a \cdot c]$. La congruenza fa sì che io possa definire operazioni sulle classi.

Proposizione 2.2.5

Riprendendo il teorema 2.2.2, abbiamo che considerato un morfismo di monoidi $f : (M, \cdot) \to (A, *)$, se definisco la relazione di equivalenza ε_f tale che $x, y \in M$ sono $x\ \varepsilon_f\ y \Leftrightarrow f(x) = f(y)$, questa relazione di equivalenza è una congruenza.

Dimostrazione : $x\ \varepsilon_f\ y,\ z\ \varepsilon_f\ w \Rightarrow (x \cdot z)\ \varepsilon_f\ (y \cdot w)$.
Infatti $f(x \cdot z) = f(x) * f(z)$ e $f(y \cdot w) = f(y) * f(w)$.

Avevamo definito ρ su $\mathbb{N} \times \mathbb{N}$, come $(a,b)\ \rho\ (c,d) \Leftrightarrow a+d=b+c$. Quindi a partire da $(M,\cdot)$ possiamo creare altri monoidi $(M^n,\cdot)$, ad esempio su $M^2 = M \times M$ in cui $(x,y)\cdot(z,t) = (x\cdot z, y\cdot t)$.

Ad esempio $(\mathbb{N},+) \to (\mathbb{N}\times\mathbb{N},+)$ in cui $(m,n)+(a,b) = (m+a, n+b)$ con l'elemento neutro $(0,0)$.

ρ è una congruenza rispetto a $+$ in $\mathbb{N}\times\mathbb{N}$. Inoltre, avendo visto che $\mathbb{N}\times\mathbb{N}/\rho = \mathbb{Z}$, abbiamo che $(\mathbb{Z},+)$ è un monoide.

2.3 Gruppi

Definizione 2.3.1

$(G,\cdot)$ è un gruppo se:
1G *$(G,\cdot)$ è un monoide*
2G *$\forall\ a \in G,\ \exists\ b \in G$ tale che $a\cdot b = 1_G$, con b comunemente indicato come a^{-1} e detto inverso di a.*

Possiamo definire un morfismo di gruppi. Un morfismo conserva strutture e proprietà, deve quindi essere un morfismo di monoidi che manda l'inverso nell'inverso.

Definizione 2.3.2 (*Morfismo di gruppi*)

Quindi $f : (G,\cdot) \to (G',*)$ è un morfismo di gruppi se:
1. *è un morfismo di monoidi*
2. *$\forall\ a \in G f(a^{-1}) = (f(a))^{-1}$*

Proposizione 2.3.1

Queste due proprietà sono la conseguenza di una sola, ossia che il morfismo conserva le operazioni. Infatti se $f(a\cdot b) = f(a) * f(b)$ allora sono vere tutte le proprietà.

Dimostrazione: Un morfismo che conserva le operazioni manda le unità nelle unità: $f(1_G) = f(1_G \cdot 1_G) = f(1_G) * f(1_G)$. Essendo entrambi gruppi hanno l'inverso, quindi moltiplicando entrambi i lati per l'inverso di $f(1_G)$ abbiamo $(f(1_G))^{-1} * f(1_G) = (f(1_G))^{-1} * f(1_G) * f(1_G) \Rightarrow 1_{G'} = f(1_G)$.
Inoltre, se il morfismo conserva le operazioni manda gli inversi negli inversi, ossia $f(a^{-1}) = (f(a))^{-1}$. Infatti $f(a) * f(a^{-1}) = f(a\cdot a^{-1}) = f(1_G) = 1_{G'} = f(a) * (f(a))^{-1}$. ■

2.3.1 Sottogruppi

Definizione 2.3.3 (*Sottogruppo*)

Partendo da $(G,\cdot)$ e scegliendo $S \subseteq G$ diverso da $\emptyset$, un sottogruppo $(S,\cdot)$ deve essere:
- *Chiuso: $\forall\ s,s' \in S,\ s\cdot s' \in S$*
- *Deve contenere l'unità: $1_G \in S$ (quindi S è un sottomonoide di G)*
- *Per essere anche un sottogruppo, S deve essere chiuso rispetto agli inversi: $s \in S \Rightarrow s^{-1} \in S$.*

Proposizione 2.3.2

Condizione necessaria e sufficiente affinché $(S,\cdot)$ con $S \neq \emptyset$ sia un sottogruppo del gruppo

$(G, \cdot)$ è:

$$a, b \in S \Rightarrow a^{-1} \cdot b \in S$$

Dimostrazione: Dimostrare che è condizione necessaria è banale. Per definizione di sottogruppo a^{-1} è in S, ed essendo chiuso $a^{-1} \cdot b \in S$.

Dobbiamo dimostrare che è sufficiente. $S \neq \emptyset$, quindi ha almeno un elemento $a \in S$. Prendiamo $b = a$, per la proprietà indicata sopra $a \cdot a^{-1} \in S \Rightarrow 1_G \in S$. Quindi S contiene almeno l'elemento neutro.

Contiene l'inverso: $\forall\ x \in S$, $x^{-1} \in S$ sempre per la proprietà sopra. Infatti prendendo $a = x$ e $b = 1_G$, $a^{-1} \cdot b \in S$ ossia $x^{-1} \cdot 1_G \in S \Rightarrow x^{-1} \in S$.

È chiuso: $\forall\ s, s' \in S \Rightarrow s \cdot s' \in S$. Abbiamo appena visto che $s \in S \Rightarrow s^{-1} \in S$, quindi per la solita proprietà ho che $(s^{-1})^{-1} \cdot s' \in S \Rightarrow s \cdot s' \in S$. ■

I sottogruppi di $(\mathbb{Z}, +)$ sono tutti e solo i gruppi $(k\mathbb{Z}, +)$. $(\mathbb{Z}, \cdot)$ non è un gruppo perché non ha l'inverso per ogni elemento.

Inverso di un prodotto

Dati $a, b \in G$, voglio conoscere l'inverso del prodotto $a \cdot b$, ossia $(a \cdot b)^{-1}$. Solitamente un gruppo $(G, \cdot)$ non è commutativo. Solo se il gruppo è commutativo ho che $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

Consideriamo il gruppo simmetrico (sezione 2.1.2) $(S_n, \circ)$, definito sull'insieme delle funzioni iniettive da un insieme con n elementi in sé stesso con l'operazione di composizione. Non è un gruppo commutativo.

Prendiamo le due funzioni σ e τ dal punto di vista dell'occupazione in figura 2.1. Se voglio trovare l'inverso π di $\sigma \circ \tau$ tale che $(\sigma \circ \tau) \circ \pi = i$ (l'identità) devo usare $\pi = (\tau^{-1} \circ \sigma^{-1})$.

σ			
1	2	3	4
2	3	1	4

τ			
1	2	3	4
1	2	4	3

$\sigma \circ \tau$			
1	2	3	4
1	2	4	3
2	3	4	1

$\tau \circ \sigma$			
1	2	3	4
2	3	1	4
2	4	1	3

Tabella 2.1: Il gruppo simmetrico non è commutativo

Quindi, l'inverso del prodotto è il prodotto degli inversi scambiati di posto:

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot 1_G \cdot a^{-1} = 1_G$$

2.3.2 Morfismi di gruppi

Un'applicazione $f : G \to G'$ è un morfismo di gruppi se $\forall\ a, b \in G$ ho che $f(a \cdot b) = f(a) * f(b) \Rightarrow f(1_G) = 1_{G'}$ e $f(a^{-1}) = (f(a))^{-1}$.

Esempio:

La funzione $\log : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ è un morfismo di gruppi, perché $\log(a \cdot b) = \log(a) + \log(b)$.

Anche la funzione $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ è un morfismo di gruppi, infatti $\exp(a+b) = \exp(a) \cdot \exp(b)$.

Anche l'iterazione della somma è un morfismo di gruppi. $f_n : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, infatti $\forall\, z \in \mathbb{Z}$, $f_n(z) = n \cdot z$

2.3.3 Nucleo di un morfismo di gruppi

Ogni morfismo di gruppi f individua due sottogruppi:

1. $Im_f \subseteq G'$
2. $\ker f \subseteq G$. Diversamente dalle definizioni già viste, in questo caso il nucleo $\ker f = \{u \in G : f(u) = 1_{G'}\}$ è una classe, ossia $\ker f \in G/\varepsilon_f$

Con i monoidi avevamo una struttura associativa $(M, \cdot)$ contenente l'unità 1_M. Il $\ker f$ l'abbiamo chiamato "quoziente", ossia:

$$\ker f = M/\varepsilon_f$$

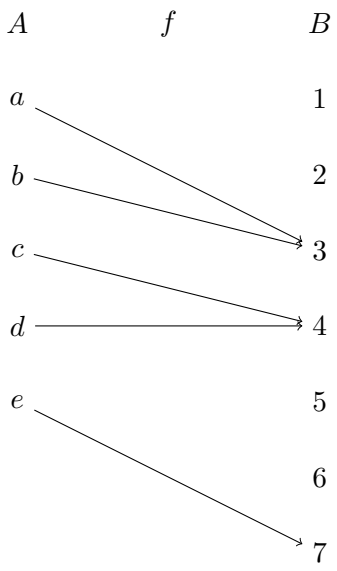

Figura 2.1: $\ker f = \{\{a, b\}, \{c, d\}, \{e\}\}$

Nel caso in figura 2.1 $\ker f = \{\{a, b\}, \{c, d\}, \{e\}\}$. *Devo* sapere quali classi ci sono per ricostruire la funzione. Per conoscere la f devo sapere tutti i blocchi della partizione, non posso ricostruire gli altri blocchi da un blocco solo.

Con i gruppi non è così. Mi basta la classe degli elementi che vanno nell'unità. Se conosco questa classe le conosco tutte. Infatti fissato il $\ker f$ conosco tutti gli elementi che hanno la stessa immagine di a, ossia $a \cdot \ker f = [a]$.

Abbiamo un morfismo di gruppi $f : (G, \cdot) \to (G', *)$. Dimostriamo intanto che il nucleo è un sottogruppo (o sottospazio).

Dimostrazione: Ho il nucleo $\ker f = [1_G]$, quindi conosco tutti gli elementi che finiscono nell'unità di G'

Condizione necessaria e sufficiente affinché un sottoinsieme sia un sottogruppo è che dati $a, b \in S \Rightarrow a^{-1} \cdot b \in S$.

Prendiamo $u, v \in \ker f$. Dobbiamo verificare che $u^{-1} \cdot v \in \ker f$, ossia che $f(u^{-1} \cdot v) = 1_{G'}$.

$$f(u^{-1} \cdot v) = f(u^{-1}) * f(v) = f(u)^{-1} * f(v)$$

Ma $f(u)^{-1} = 1_{G'}$, quindi ho:

$$f(u)^{-1} * f(v) = 1_{G'} * 1_{G'} = 1_{G'}$$

■

Vediamo ora come ogni elemento $b \in [a]$ si può esprimere come prodotto $a \cdot \ker f$, e viceversa.

Dimostrazione: Considero $b \in [a] \Rightarrow f(a) = f(b)$, ossia per definizione hanno la stessa immagine tramite il morfismo.

Quindi moltiplico entrambi i membri per $f(a)^{-1}$:

$$f(a)^{-1} * f(b) = 1_{G'} \Rightarrow 1_{G'} = f(a)^{-1} * f(b) = f(a^{-1} \cdot b)$$

Quindi $u = (a^{-1} \cdot b) \in \ker f$ e $b = a \cdot u = a \cdot (a^{-1} \cdot b)$. Quindi ogni elemento in $[a]$ si può esprimere come $a \cdot \ker f$.

Viceversa, dobbiamo prendere $b \in a \cdot \ker f \Rightarrow b = a \cdot u$. Ha per forza la stessa immagine di a, infatti $f(b) = f(a \cdot u) = f(a) * f(u) = f(a) * 1_G = f(a)$. Segue che b è nella classe di a ($b \in [a]$). ■

2.3.4 Teorema di omomorfismo per i gruppi

Teorema 2.3.3 (*Teorema di omomorfismo per i gruppi*)

Dato un morfismo $f : (G, \cdot) \to (G', *)$, allora

1. *La relazione di equivalenza ε_f individuata da f, tale che $x \; \varepsilon_f \; y \Leftrightarrow f(x) = f(y)$, è una congruenza.*
2. *Il gruppo $(G/\varepsilon_f, \cdot)$ è isomorfo al sottogruppo $(Im_f, *)$ di $(G', *)$, ossia esiste la biezione F:*

$$F : (G/\varepsilon_f, \cdot) \to (Im_f, *)$$

Questa proprietà vale per ogni struttura algebrica.

Ogni elemento $[a] \in G/\varepsilon_f$ è del tipo $a \cdot \ker f$.

$$\forall \; [a] \in G/\varepsilon_f, \; [a] = a \cdot \ker f$$

Non essendo il gruppo commutativo, ho che $b = a \cdot u = v \cdot a$, ma non che $u = v$. Posso quindi vedere b sia in $a \cdot \ker f$, sia in $\ker f \cdot a$. La prima è la classe laterale sinistra, la seconda è la classe laterale destra. Le due classi sono uguali:

$$\forall \; a \in G, \; a \cdot \ker f = \ker f \cdot a$$

Esempio:

Prendiamo la seguente funzione (o "proiezione"):

$$p_1 : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$
$$p_1(x, y) = x$$

È anche un morfismo di gruppi:

$$p_1 : (\mathbb{R} \times \mathbb{R}, +) \to (\mathbb{R}, +)$$

Qual è l'immagine Im_{p_1} della proiezione?

$$Im_{p_1} = \{r \in \mathbb{R} : \ \exists \ (x, y) \text{ t.c. } p_1(x, y) = r\}$$

In questo caso l'immagine è tutto $\mathbb{R}$. Infatti $\forall\ r \in \mathbb{R}$, $p_1(r, 0) = r$.

Troviamo il nucleo della proiezione.

$$\ker p_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} : p_1(x, y) = 0\} = \{(0, y) : y \in \mathbb{R}\}$$

L'elemento neutro del gruppo $\mathbb{R} \times \mathbb{R}$, ossia $1_{\mathbb{R}\times\mathbb{R}} = (0, 0)$, è nel $\ker p_1$. L'elemento neutro di $(\mathbb{R}, +)$ è 0.

Troviamo la classe di $(2, 3)$:

$$(2, 3) \in \mathbb{R} \times \mathbb{R}, p_1(2, 3) = 2$$
$$[(2, 3)] = \{(x, y) \in \mathbb{R} \times \mathbb{R} : f(x, y) = 2\}$$

Applicando il teorema di omomorfismo visto prima vediamo subito che è:

$$[(2, 3)] = (2, 3) + \ker p_1 = \{(2, 3) + (0, y) = (2, y + 3)\}$$

Esempi con i polinomi

Consideriamo $\mathbb{R}[x]$, l'insieme dei polinomi in una indeterminata x.

Definizione 2.3.4 (*Polinomio*)

Un polinomio è una espressione formale del tipo:

$$a_0 + a_1 x + \cdots + a_n x^n \text{ dove } a_n \neq 0$$

n si dice grado del polinomio.

C'è una differenza fra x come indeterminata e x come variabile. L'indeterminata indica che ci troviamo nei polinomi, e vuol dire che x è un simbolo. Variabile vuol dire che x è un elemento di un insieme, ossia $x \in E$. In genere si confonde indeterminata con variabile, perché quando si parla di polinomi la x è sì indeterminata, ma ogni polinomio individua una funzione polinomiale $p : \mathbb{R} \to \mathbb{R}$ tale che $a \mapsto p(a)$. Quindi il polinomio:

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

individua la funzione polinomiale $p : \mathbb{R} \to \mathbb{R}$ che $\forall\ a \in \mathbb{R}$ associa $1 + 2 \cdot a = p(a)$. Nel caso dei numeri reali, questa funzione è una biezione. Non è vero se prendo altri insiemi.

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Tabella 2.2: Somma e prodotto in $\mathbb{Z}_2$

Definizione 2.3.5 (*Uguaglianza fra polinomi in* $\mathbb{R}$)

Se due polinomi hanno la stessa funzione polinomiale, allora sono lo stesso polinomio.

Per creare i polinomi bisogna avere un campo.

Prendiamo $\mathbb{Z}_2 = \{0, 1\}$, ossia i resti della divisione per 2, costruiti partendo dalla congruenza modulo 2 ($\mathbb{Z}/\equiv_2$). Possiamo definire due operazioni, di somma e di prodotto.

Un campo è un gruppo rispetto a + e un gruppo rispetto a · togliendo l'elemento neutro (lo 0). $\mathbb{Z}_2$ è quindi un campo.

Possiamo creare dei polinomi a coefficienti in $\mathbb{Z}_2$, ossia $\mathbb{Z}_2[x]$, ad esempio $1 + x$. La funzione polinomiale rispetto a questo polinomio è:

- per $x = 0 \to p(0) = 1$
- per $x = 1 \to p(1) = 0$

Prendiamo il polinomio $1 + x^2$. La sua funzione polinomiale è:

- per $x = 0 \to p(0) = 1$
- per $x = 1 \to p(1) = 0$

Sono quindi due polinomi diversi che hanno la stessa funzione polinomiale.

Definizione 2.3.6 (*Uguaglianza fra polinomi*)

Due polinomi sono uguali se hanno tutti i coefficienti uguali.

Torniamo all'insieme dei polinomi reali. $(\mathbb{R}[x], +)$ è un gruppo commutativo. Come funziona l'operazione di +? Sommando i coefficienti.

L'elemento neutro è il polinomio nullo, ossia il polinomio con tutti i coefficienti uguali a 0. Si indica con $\underline{0}$. Il polinomio nullo ha grado -1.

Possiamo definire un morfismo di gruppi su tutta sta merda.

- Prendiamo tutti i polinomi di grado minore o uguale a due, indicati con $\mathbb{R}_2[x]$.
- Prendiamo l'applicazione $f : (\mathbb{R}_2[x], +) \to \left(\mathbb{R}^2, +\right)$ definito come segue:

$$f\left(a_0 + a_1x + a_2x^2\right) = (a_2, a_1 + a_2)$$

  Quindi $1 + 2x \mapsto (0, 2)$. L'applicazione f è un morfismo di gruppi.

Qual è l'immagine di questa f?

$$Im_f = \{(r, s) \in \mathbb{R}^2 : \exists\ p(x) \text{ t.c. } f\left(p(x)\right) = (r, s)\} = \mathbb{R}^2$$

Una data coppia (r, s) è immagine, ad esempio, di:

$$(r, s) = f(0 + (s - r)x + rx^2)$$

Troviamo il nucleo del morfismo.

$$\ker f = \{p(x) \in \mathbb{R}^2[x] : f\left(p(x)\right) = (0,0)\}$$

Quindi sono tutti i polinomi di grado 0 più il polinomio nullo, dovendo avere $a_2 = 0$ e $a_1 = 0$.

Tutti i polinomi nella classe $[p(x)] = a_0 + a_1x + a_2x^2$ devono potersi scrivere come $p(x) + \ker f$. L'immagine di $p(x)$ è:

$$f\left(p(x)\right) = (a_2, a_1 + a_2)$$

Quindi se voglio scrivere i polinomi $q(x) \in [p(x)]$ come $p(x) + \ker f$:

$$q(x) \in [p(x)] \Rightarrow q(x) = p(x) + a_0$$

con $a_0 \in \ker f$.

Monomorfismi ed epimorfismi

Consideriamo due gruppi, $(G, \cdot)$ e $(G', *)$, e il morfismo $f : (G, \cdot) \to (G', *)$. I due gruppi $\ker f \leq G$ e $Im_f \leq G'$ caratterizzano il morfismo.

1. f è un morfismo iniettivo (monomorfismo) $\Leftrightarrow \ker f = \{1_G\}$.
2. f è un morfismo suriettivo (epimorfismo) $\Leftrightarrow Im_f = G'$.

Il caso 1 è evidente: il $\ker f$ ha solo un elemento quindi la classe degli elementi con la stessa immagine $[a] = a \cdot \ker f$ ha un solo elemento, ossia a. Si può anche dimostrare direttamente.

Dimostrazione: Per ipotesi, f è iniettiva. La tesi è che il nucleo è costituito da un solo elemento, ossia $\ker f = \{1_G\}$, ossia $f(1_G) = 1_{G'}$, verificato essendo f un morfismo.
Viceversa, per ipotesi il nucleo ha un solo elemento:

$$\begin{aligned}\ker f = \{1_G\} &\Rightarrow f(a) = f(b) \Rightarrow \\ &\Rightarrow f(a) * f(b)^{-1} = 1_{G'} \Rightarrow \\ &\Rightarrow f(a \cdot b^{-1}) = 1_{G'} \Rightarrow \\ &\Rightarrow a \cdot b^{-1} = 1_G \Rightarrow a = b\end{aligned}$$

■

2.3.5 Classi laterali

Abbiamo detto che f individua due sottogruppi, $\ker f = \{u \in G : f(u) = 1_{G'}\} \leq G$ e $Im_f = \{x' \in G' : \ \exists\ x \in G,\ f(x) = x'\} \leq G'$. Il nucleo è una classe, e le altre classi si costruiscono a partire dal nucleo:

$$\forall\ a \in G,\ [a] = a \cdot \ker f = \ker f \cdot a$$

Proposizione 2.3.4 (*Cardinalità delle classi laterali*)

Tutte le classi hanno la stessa cardinalità.

$$|[a]| = |a \cdot \ker f| = |\ker f|$$

Dimostrazione: Bisogna far vedere che esiste una corrispondenza biunivoca:

$$\forall\ a \in G,\ \varphi_a : \ker f \to a \cdot \ker f$$
$$\forall\ u \in \ker f,\ \varphi_a(u) = a \cdot u \in a \cdot \ker f$$

φ_a è biunivoca.
φ_a è iniettiva, infatti $\forall\ u, v \in \ker f$ tali che $\varphi_a(u) = \varphi_a(v)$, ho che $a \cdot u = a \cdot v \Rightarrow$ essendo in un gruppo a ha l'inverso, quindi $a^{-1} \cdot a \cdot u = a^{-1} \cdot a \cdot v \Rightarrow u = v$. ■

Sia $(S, \cdot) \leq (G, \cdot)$ un sottogruppo qualunque di $(G, \cdot)$. Vediamo come si comportano le sue classi laterali. Prendiamo $a \in G$ e moltiplico tutti gli elementi di S per a, ossia creiamo le classi laterali $a \cdot S$ e $S \cdot a$.

- $a \cdot S = \{x \in G : x = a \cdot s \text{ con } s \in S\}$ è la classe laterale sinistra di S
- $S \cdot a = \{x \in G : x = s \cdot a \text{ con } s \in S\}$ è la classe laterale destra di S

Per la proposizione 2.3.4 tutte le classi laterali hanno la stessa cardinalità di S.

$$|a \cdot S| = |S| = |S \cdot a|\ \ \forall\ a \in G$$

Prendiamo l'insieme dei sottoinsiemi sinistri:

$$\{a \cdot S\}_{a \in G} \text{ con } a \cdot S \subseteq G$$

$a \cdot S$ non è un sottogruppo perché non contiene l'unità, ma è un sottoinsieme. L'insieme dei sottoinsiemi sinistri è una partizione di G. Infatti:

1. $\bigcup_{a \in G} a \cdot S = G$
2. $a \cdot S \neq \emptyset$, infatti necessariamente $a \in a \cdot S$, essendo $a = a \cdot 1_G$ e $1_G \in S$
3. $a \cdot S \cap b \cdot S \neq \emptyset \Rightarrow a \cdot S = b \cdot S$

Dimostriamo il punto 3.

Dimostrazione: Il punto 3 dice che:

$$(a \cdot S) \cap (b \cdot S) \neq \emptyset \Rightarrow a \cdot S = b \cdot S$$

Prendiamo un elemento c nell'intersezione non vuota:

$$c \in (a \cdot S) \cap (b \cdot S)$$
$$c = a \cdot s = b \cdot v, \text{ con } s, v \in S$$

è l'ipotesi.
Prendiamo un qualunque $x \in a \cdot S \Rightarrow x = a \cdot u$ con $u \in S$. Per ipotesi abbiamo che $a = c \cdot s^{-1} \Rightarrow$ sostituendo $x = c \cdot s^{-1} \cdot u$, ma sempre per ipotesi abbiamo che $x = b \cdot v \cdot s^{-1} \cdot u$. Quindi $x \in b \cdot S$, avendo che $(v \cdot s^{-1} \cdot u) \in S$. ■

Sapendo $\{a \cdot S\}_{a \in G}$ è una partizione di G, possiamo definire una relazione di equivalenza in G che indichiamo con ${}_S\sim$ (con il simbolo a sinistra perché S è una classe laterale sinistra).

Diciamo che due elementi sono equivalenti se sono nello stesso blocco. Ossia, dati $x, y \in G$, diciamo $x {}_S\sim y \Leftrightarrow\ \exists\ a \in G$ t.c. $x, y \in a \cdot S \Leftrightarrow x = a \cdot s$ e $y = a \cdot v$ con $s, v \in S$. Si può semplificare ulteriormente questa definizione, perché se un elemento x è nella classe posso prendere x come

rappresentante, e quindi dire che $x \in y \cdot S$ o che $y \in x \cdot S$ o che $x \cdot S = y \cdot S$. Tutte queste sono definizioni equivalenti.

Quindi posso scrivere $x \in y \cdot S$ come $x = y \cdot s$ con $s \in S$.

$$s = y^{-1} \cdot x \in S$$

C'è una differenza fra il nucleo di un morfismo e le semplici classi laterali: nel nucleo le classi laterali coincidono, in generale no. Le classi laterali hanno la stessa cardinalità ma non sono identiche.

Le due relazioni di equivalenza destra e sinistra ${}_S\sim$ e $\sim_S$ non sono uguali, e non sono congruenze.

$$a \cdot S \neq S \cdot a$$

Nel caso del nucleo invece abbiamo che $a \cdot \ker f = \ker f \cdot a$, e la relazione di equivalenza destra e sinistra è una sola, ossia ε_f, ed è una congruenza.

Definizione 2.3.7 (*Sottogruppo delle potenze di un elemento*)

Dato un gruppo $(G, \cdot)$ e un elemento $a \in G$, indichiamo con $<a>$ il sottogruppo generato da $a \in G$ costituito da tutte le potenze di a. Per le proprietà delle potenze è un sottogruppo, infatti contiene $1_G = a^0$.

$$<a>= \{a^z : z \in \mathbb{Z}\}$$

Contiene anche l'inverso di a^n, ossia a^{-n}.

Esempio :

Consideriamo il gruppo simmetrico S_4 e una permutazione $\sigma \in S_4$. Prendiamo il sottogruppo generato da questa permutazione, ossia tutte le potenze generate da σ. $\sigma^0 = id$, ossia è l'identità. $\sigma^1 = \sigma$. σ^2 cosa è? Si trova componendo σ con sé stessa, come fatto di seguito. In questo caso, facendo σ^3 riotteniamo l'identità.

σ			
1	2	3	4
2	3	1	4

σ^2			
1	2	3	4
2	3	1	4
3	1	2	4

σ^3			
1	2	3	4
2	3	1	4
3	1	2	4
1	2	3	4

Quindi il gruppo H delle potenze di σ è $<\sigma>= \{1, \sigma, \sigma^2\}$. L'inversa di σ è σ^2. H è un gruppo finito di ordine 3 (per il significato di ordine, vedere il teorema 2.3.5).

Vediamo la relazione di equivalenza e la classe laterale definite da H.

Dati due elementi μ e τ, questi sono equivalenti $\Leftrightarrow \mu \circ \tau^{-1} \in H$. Quindi $\mu \circ \tau^{-1} = \rho \in H$, ossia una qualche permutazione in H, quindi o l'identità, o σ, o σ^2.

Se ad esempio consideriamo due permutazioni τ e μ tali che $\mu \circ \tau^{-1} = \sigma$, segue che $\mu \circ \tau^{-1} \circ \tau = \sigma \circ \tau \Rightarrow \mu = \sigma \circ \tau$, come si vede nella tabella di seguito. Attenzione: il gruppo S_4 non è commutativo!

τ			
1	2	3	4
2	1	4	3

$\sigma \circ \tau$			
1	2	3	4
2	1	4	3
3	2	4	1

$\Rightarrow$

μ			
1	2	3	4
3	2	4	1

Prendiamo poi una permutazione τ', e componiamola con σ come nella tabella di seguito: otteniamo una permutazione μ' equivalente a τ'.

τ'			
1	2	3	4
4	3	2	1

$\sigma \circ \tau'$			
1	2	3	4
4	3	2	1
4	1	3	2

$\Rightarrow$

μ'			
1	2	3	4
4	1	3	2

Siamo nella classe destra, avendo composto $\sigma \circ \tau$.

Avere una congruenza mi dà modo di definire il prodotto fra classi. Ossia, dati a, b nella classe 1 e dati a', b' nella classe 2, con classi definite sulla struttura $(A, \cdot)$, vogliamo definire il prodotto fra classi, ossia un'operazione $[1] \cdot [2] = [3]$. La congruenza fa in modo che comunque io prenda i rappresentanti, i prodotti vadano sempre nella stessa classe. Quindi $a \cdot a'$ e $b \cdot b' \in [3]$.

È possibile vedere (ma non qui) che $\tau \circ \tau'$ e $\mu \circ \mu'$ *non* vanno nella stessa classe.

Teorema 2.3.5 (*Teorema di Lagrange*)

Sia $(G, \cdot)$ un gruppo finito, la cardinalità di G si dice ordine.
Se H è un sottogruppo di G, l'ordine di G è diviso dall'ordine di H. Ossia $\frac{|G|}{|H|}$ è un intero, ed è detto "indice di H".

Osservazione 3

Un gruppo di ordine un numero primo ha due sottogruppi.

Abbiamo visto che $\{a \cdot H\}_{a \in G}$ è una partizione di G, e che $|a \cdot H| = |H|$. Quindi:

$$|G/_{H} \sim| = \frac{|G|}{|H|}$$

Definizione 2.3.8 (*Sottogruppi normali*)

Un sottogruppo N di G si dice normale se, $\forall\, a \in G$, $a \cdot N = N \cdot a$, ossia ogni classe laterale destra è uguale alla classe laterale sinistra. Tutti i nuclei di morfismi sono sottogruppi normali.

Condizione necessaria e sufficiente affinché N sia normale è che $\forall\, a \in G$ e $\forall\, u \in N$, $a \cdot u \cdot a^{-1} \in G$. Deriva banalmente da $a \cdot N = N \cdot a$

Condizione necessaria e sufficiente affinché N sia normale è che la relazione d'equivalenza $\sim_N$ (o la relazione d'equivalenza ${}_N\sim$) sia una congruenza.

2.3.6 Permutazioni come cicli

Ogni permutazione è una biezione che può essere indicata sia dal punto di vista dell'occupazione sia dal punto di vista della distribuzione (ossia, come parola).

Consideriamo una permutazione $\sigma \in S_8$. Possiamo vederla dal punto di vista dell'occupazione, come nella tabella 2.3, o come parola:

17465238

Possiamo anche rappresentare le permutazioni come composte di cicli:

σ							
1	2	3	4	5	6	7	8
1	7	4	6	5	2	3	8

Tabella 2.3: σ dal punto di vista dell'occupazione

$$\sigma = (1)(27346)(5)(8)$$

(27346) significa che il 2 va nel 7, il 7 nel 3, il 3 nel 4, il 4 nel 6, e il 6 torna nel 2.

$\mu = (31)(542)(876)$ è un prodotto di cicli. Corrisponde alla permutazione nella tabella 2.4.

μ							
1	2	3	4	5	6	7	8
3	5	1	2	4	8	6	7

Tabella 2.4: μ dal punto di vista dell'occupazione

Le permutazioni vengono rappresentate come prodotti di cicli. I cicli di lunghezza 1 non vengono scritti, visto che ogni elemento va a finire in sé stesso. Quindi $\sigma = (1)(27346)(5)(8)$ posso scriverla come $\sigma = (27346)$.

Data una permutazione $\sigma \in S_n$ definita su $[n] = \{1 \dots n\}$, possiamo definire la relazione di equivalenza sui cicli $x \equiv_\sigma y \Leftrightarrow \exists\, n \in \mathbb{N}$ t.c. $y = \sigma^n(x)$. Questa è una relazione di equivalenza che divide $[n]$ in classi di equivalenza: le classi sono i cicli.

Ad esempio, nel caso del σ di prima, $7 = \sigma(2)$, $3 = \sigma^2(2)$, $4 = \sigma^3(2)$, $6 = \sigma^4(2)$.

Un $x \in \mathbb{N}$ è equivalente a tutti gli elementi $\sigma(x), \sigma^2(x), \dots \sigma^t(x)$ fino alla t-esima permutazione che torna in x (deve esistere, e t deve essere finito, altrimenti il ciclo sarebbe infinito).

Consideriamo la funzione $\mu_x : [n] \to [n]$, definita come:

$$\mu_x(y) = \begin{cases} y \text{ se } y \notin [x] \\ \mu(y) \text{ se } y \in [x] \end{cases}$$

Quindi μ_x è una permutazione, e si comporta come μ nella classe individuata da x, lasciando fissi tutti gli altri elementi.

Tornando alla permutazione μ nella tabella 2.4, possiamo trovare $\mu_3 = \mu_1$, $\mu_5 = \mu_4 = \mu_2$, e $\mu_6 = \mu_7 = \mu_8$, nella tabella 2.5.

μ_3							
1	2	3	4	5	6	7	8
3	2	1	4	5	6	7	8

μ_5							
1	2	3	4	5	6	7	8
1	5	3	2	4	6	7	8

μ_6							
1	2	3	4	5	6	7	8
1	2	3	4	5	8	6	7

Tabella 2.5: Le tre permutazioni μ_3, μ_5 e μ_6 individuate da μ

Possiamo trovare μ come composizione di μ_3, μ_5 e μ_6, come nella tabella 2.6. Questa composizione si chiama "rappresentazione di una permutazione come cicli disgiunti".

$\mu = \mu_3 \circ \mu_5 \circ \mu_6$								
1	2	3	4	5	6	7	8	
3	2	1	4	5	6	7	8	μ_3
3	5	1	2	4	6	7	8	μ_5
3	5	1	2	4	8	6	7	μ_6

Tabella 2.6: Composizione di $\mu_3 \circ \mu_5 \circ \mu_6$

Rappresentazione canonica (o standard) di una permutazione di $[n]$

Nel rappresentare una permutazione come cicli (disgiunti e non), non si possono omettere le parentesi, o si avrebbe una parola. Ma se le permutazioni sono in $\mathbb{N}$ possiamo trovare una rappresentazione standard (o canonica) dei cicli, senza parentesi.

Consideriamo la permutazione individuata dai cicli disgiunti (312)(5)(78)(46). Per trovare la rappresentazione canonica dobbiamo:

1. descrivere i cicli partendo dall'elemento maggiore:

$$(312)(5)(87)(64)$$

2. ordinare in maniera crescente in base al primo elemento:

$$(312)(5)(64)(87)$$

3. togliere le parentesi, perché sappiamo che i cicli finiscono al primo elemento non decrescente:

$$31256487$$

2.3.7 Trasposizioni

Le trasposizioni sono permutazioni che scambiano solo due elementi. Quindi hanno un solo ciclo di lunghezza 2 e tutti gli altri di lunghezza 1.

Teorema 2.3.6 (*Permutazioni come prodotto di trasposizioni*)

Ogni permutazione si può scrivere come un prodotto di trasposizioni. Il numero di trasposizioni varia.

Se una permutazione σ si esprime come un prodotto di un numero pari di trasposizioni, allora ogni altro prodotto di trasposizioni che individua σ ha un numero pari di trasposizioni. Stesso discorso vale se la permutazione si esprime come prodotto di un numero dispari di trasposizioni.

Definizione 2.3.9 (*Trasposizioni pari e dispari*)

Una permutazione è pari se si esprime come prodotto di un numero pari di trasposizioni, dispari se si esprime come prodotto di un numero dispari di trasposizioni.

Consideriamo A_n, l'insieme delle permutazioni pari. Ovviamente $A_n \subseteq S_n$. Ma è anche un sottogruppo di $(S_n, \circ)$?

– $1 \in A_n$, contiene l'unità.

– Deve essere chiuso. Si verifica subito, date $\sigma, \mu \in A_n$ quindi entrambe prodotto di un numero pari di trasposizioni, che $(\sigma \circ \mu) \in A_n$, ossia anche la loro composizione ha un numero pari di trasposizioni.

– Allo stesso modo deve essere che $\sigma^{-1} \in A_n$. Ma come si ottiene σ^{-1}?

  Sia $\sigma = \tau_1 \dots \tau_n$ con $n = 2t$ e τ_i una trasposizione. L'inverso di una trasposizione è se stessa, ossia $\tau^{-1} = \tau$, quindi:

$$\sigma^{-1} = \tau_n \dots \tau_1$$

$(A_n, \circ)$ è quindi un sottogruppo di $(S_n, \circ)$ e si chiama "gruppo alterno di ordine n".

L'insieme delle permutazioni dispari non è un sottogruppo di S_n perché il prodotto di due permutazioni dispari è una permutazione pari.

Proposizione 2.3.7

Il numero delle permutazioni dispari è uguale al numero delle permutazioni pari.

Dimostrazione: Dobbiamo trovare la corrispondenza biunivoca fra le permutazioni pari e le permutazioni dispari. Ossia, trovare $F : A_n \to P_n$ e $F^{-1} : D_n \to A_n$, con D_n ad indicare l'insieme delle permutazioni dispari.
Prendiamo $[n] = \{1 \dots n\}$ sui primi n numeri naturali. σ è una permutazione pari sui primi n numeri naturali. Per rendere σ dispari, la compongo con un'altra trasposizione.

$$F(\sigma) = (12) \circ \sigma \in D_n$$

F è biunivoca. Infatti esiste $F^{-1} : D_n \to A_n$, che per una trasposizione $\delta \in D_n$ è:

$$F^{-1}(\delta) = (12) \circ \delta \in A_n$$

Poiché l'inverso di una trasposizione è la trasposizione stessa:

$$(FF^{-1})(\delta) = F((12) \circ \delta) = (12) \circ (12) \circ \delta = \delta$$
$$(F^{-1}F)(\sigma) = F^{-1}((12) \circ \sigma) = (12) \circ (12) \circ \sigma = \sigma$$

■

Osservazione 4 (*Ordine del gruppo alterno*)

Come conseguenza della proposizione 2.3.7, siccome la cardinalità dell'insieme delle permutazioni è $n!$, la cardinalità di A_n è $\frac{n!}{2}$

Osservazione 5 (*Indice del gruppo alterno*)

L'indice di A_n quindi è:

$$\frac{|S_n|}{|A_n|} = 2$$

Quindi A_n è un sottogruppo normale, poiché se l'indice del sottogruppo H del gruppo finito G è il più piccolo fattore dell'ordine di G, allora H è un sottogruppo normale di G.

Osservazione 6

A_n è il nucleo del morfismo $f : (S_n, \circ) \to (\mathbb{Z}_2, +)$ definito come segue:

$$f(\sigma) = \begin{cases} 0 \text{ se } \sigma \text{ è pari} \\ 1 \text{ se } \sigma \text{ è dispari} \end{cases}$$

È un morfismo perché 1 per 1 va in 0 e 0 per 0 va in 0, ossia una permutazione pari per una pari va in una pari, e una permutazione dispari per una dispari va in una pari.

Proposizione 2.3.8

Ogni permutazione si esprime come prodotto di trasposizioni.

Prendiamo una permutazione σ. Abbiamo dimostrato che le permutazioni si possono esprimere come prodotto di cicli.

$$\sigma = \mu_1 \circ \mu_2 \circ \ldots \circ \mu_t$$

σ è il prodotto di t permutazioni. Ciascuna μ_i è una permutazione k_i-ciclica, ossia μ_i ha un solo ciclo di lunghezza k_i e tutti gli altri cicli sono di lunghezza 1.

$\sigma = \mu_1 \circ \mu_2$						
1	2	3	4	5	6	7
2	4	1	3	6	5	7

$$(1243)(56) = \mu_1 \circ \mu_2 \text{ con } \mu_1 = (1243) \text{ e } \mu_2 = (56)$$

Basta dimostrare che ogni permutazione k-ciclica si può esprimere come un prodotto di trasposizioni.

Per scrivere una permutazione k-ciclica come prodotto di trasposizioni, accoppio gli elementi a due a due.

$$(1243) = (12)(24)(43)$$

L'ordine è l'ordine di composizione delle funzioni.

(12)(24)(43)							
1	2	3	4	5	6	7	
1	2	4	3	5	6	7	(43)
1	4	2	3	5	6	7	(24)
2	4	1	3	5	6	7	(12)

(1243)						
1	2	3	4	5	6	7
2	4	1	3	5	6	7

Quindi, dato un ciclo $\mu_i = (a_1 a_2 \ldots a_{t-1} a_t)$, lo scrivo come prodotto di trasposizioni nel seguente modo:

$$\mu_i = (a_1 a_2)(a_2 a_3) \ldots (a_{t-1} a_t)$$

Ogni permutazione k_i-ciclica ha parità uguale alla parità di $k_i - 1$.

La parità di $\sigma = \mu_1 \circ \mu_2 \circ \ldots \circ \mu_t$ è:

$$\sum_{i=1}^{t} (k_i - 1) = t + \sum_{i=1}^{t} k_i$$

L'ordine di una permutazione σ è la cardinalità del sottogruppo generato da σ ($<\sigma>$) ossia tutte le potenze di σ. Se prendo una permutazione μ k-ciclica, l'ordine di μ è k.

Una trasposizione ha ordine 2. Ad esempio, $<(56)>= \{1, (56)\}$.

Il sottogruppo generato da $<(1243)>$ è $\{1, (1243), (14)(23), (1342)\}$.

$(1243)^2$			
1	2	3	4
2	4	1	3
4	3	2	1

$(1243)^3$			
1	2	3	4
2	4	1	3
4	3	2	1
3	1	4	2

Con una permutazione, l'ordine è l'inf di $\{t : \sigma^t = 1 \text{ con } t \neq 0\}$, ossia è il più piccolo intero t diverso da 0 per cui σ^t è l'identità. Se in generale σ è il prodotto di $\mu_1 \dots \mu_t$ cicli disgiunti, l'ordine di σ è il mcm dell'ordine dei suoi cicli.

$$\sigma^j = \mu_1^j \dots \mu_t^j = 1$$
$$<\sigma>= \{\sigma^0, \sigma^1 \dots \sigma^j\}$$

j deve essere il mcm delle lunghezze di ciascun sottogruppo $<\mu_i>$.

Esempio :

$H = \{\sigma \in S_4 \text{ t.c. } \sigma = 1 \text{ oppure } \sigma \text{ è il prodotto di trasposizioni disgiunte}\}$. H è un sottogruppo di S_4?

$$H = \{1, (12)(34), (13)(24), (14)(23)\}$$

H contiene l'unità, quindi verifica una delle proprietà. Verifichiamo subito che, data una permutazione σ, H contiene σ^{-1}: l'inverso di un elemento è l'elemento stesso.

In generale l'inverso di un prodotto in un gruppo non commutativo è il prodotto al contrario degli inversi. Ma in questo caso sono commutativi i singoli elementi, essendo trasposizioni disgiunte, e l'inverso di un elemento è l'elemento stesso, quindi:

$$\sigma^{-1} = ((12)(34))^{-1} = (34)^{-1}(12)^{-1} = (43)(21) = (12)(34)$$

Questa bella proprietà si chiama idempotenza.

$$\sigma_1 \circ \sigma_2 = \sigma_3 = \sigma_2 \circ \sigma_1$$
$$\sigma_1 \circ \sigma_3 = \sigma_1 = \sigma_3 \circ \sigma_1$$
$$\sigma_2 \circ \sigma_3 = \sigma_2 = \sigma_3 \circ \sigma_2$$

Vediamolo con $\sigma_1 \circ \sigma_2$:

$\sigma_1 \circ \sigma_2$			
1	2	3	4
3	4	1	2
4	3	2	1

$$\sigma_1 \circ \sigma_2 = (14)(23) = \sigma_3$$

Quindi H è un sottogruppo commutativo di un gruppo non commutativo.

L'ordine di H è 4. L'ordine di S_4 è 4!, e ricordiamo che S_4 può avere sottogruppi di ordine che divide l'ordine di S_4.

I sottogruppi di H (diversi da H e dall'unità) devono avere ordine 2. I sottogruppi di ordine 2 sono 3: $<\sigma_1>= \{1, \sigma_1\}$, $<\sigma_2>= \{1, \sigma_2\}$, $<\sigma_3>= \{1, \sigma_3\}$.

Osservazione 7

Se esprimo una permutazione come prodotto di cicli, il prodotto dei cicli è commutativo perché i cicli sono disgiunti. Non si possono commutare i cicli di una permutazione espressa come prodotto di cicli congiunti.

Esercizio 14

Determinare un elemento x di S_8 tale che $a \circ x \circ a = a \circ c \circ b \circ a \circ b$
Dove $a = (123)(234)(456)$ (occhio: non è un prodotto di cicli disgiunti). b è rappresentata dal punto di vista dell'occupazione nella tabella 2.7, e $c = (28)$ è una trasposizione.
Determinare l'ordine di x, la sua parità e una decomposizione in cicli disgiunti.
Un suggerimento:

$$a^{-1} \circ a \circ x \circ a \circ a^{-1} = a^{-1} \circ a \circ c \circ b \circ a \circ b \circ a^{-1} \Rightarrow x = c \circ b \circ a \circ b \circ a^{-1}$$

1	2	3	4	5	6	7	8
2	1	5	4	3	7	6	8

Tabella 2.7: La permutazione b

2.4 Strutture algebriche con due operazioni

Anelli Un anello è una struttura algebrica $(A, +, \cdot)$ t.c.

1. La prima operazione $(A, +)$ è un gruppo abeliano.
2. La seconda operazione considerata sull'insieme escluso l'elemento neutro, $(A \setminus \{0\}, \cdot)$ è un semigruppo.
3. $\forall\ a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c$
4. $\forall\ a, b, c \in A,\ (a + b) \cdot c = a \cdot c + b \cdot c$

Campi Un campo è un anello in cui $(A \setminus \{0\}, \cdot)$ è un gruppo abeliano.

Gli interi sono un anello: $(\mathbb{Z}, +, \cdot)$.

I razionali sono un campo: $(\mathbb{Q}, +, \cdot)$. Anche $\mathbb{R}$ e $\mathbb{C}$ sono un campo.

2.4.1 Anelli

Un anello è una struttura algebrica con 2 operazioni $(A, +, \cdot)$ tale che:

1A $(A, +)$ è un gruppo abeliano (ossia un gruppo commutativo)

2A $(A, \cdot)$ è un semigruppo, ossia una struttura algebrica associativa

3A valgono le proprietà distributive (devo scriverle entrambe perché non è detto che le operazioni siano commutative)

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

Definizione 2.4.1 (*Anello unitario*)

Se $(A, \cdot)$ è un monoide, ossia se ha l'unità, l'anello si dice "anello unitario".

Definizione 2.4.2 (*Anello commutativo*)

Se $(A, \cdot)$ è una struttura commutativa, l'anello si dice "anello commutativo".

Definizione 2.4.3 (*Anello primo di divisori dello zero*)

Se, dati $a, b \in A$ tali che $a \cdot b = 0$, si ha che $a = 0$ oppure $b = 0$ (oppure non esclusivo), allora l'anello si dice "privo di divisori dello zero", con 0 a indicare l'unità di $(A, +)$.

L'anello degli interi $(\mathbb{Z}, +, \cdot)$ è un anello commutativo unitario privo di divisori dello 0.

Esempio di anello con divisori dello 0 :

Prendiamo tutte le funzioni $\mathbb{R}^{\mathbb{R}}$ rispetto a $+$ e a $\cdot$, ossia $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$.

La somma di funzioni $(f + g) : \mathbb{R} \to \mathbb{R}$ è definita come $(f + g)(x) = f(x) + g(x)$.

Il prodotto di funzioni $(f \cdot g) : \mathbb{R} \to \mathbb{R}$ è definito, anche questo in modo naturale, come $(f \cdot g)(x) = f(x) \cdot g(x)$.

$(\mathbb{R}^{\mathbb{R}}, +, \cdot)$ è un anello. L'elemento neutro dell'anello rispetto a $(\mathbb{R}^{\mathbb{R}}, +)$ è una funzione $\underline{0} : \mathbb{R} \to \mathbb{R}$ con $\underline{0} + f = f = f + \underline{0}$. Quindi:

$$\underline{0}(x) = 0$$

L'unità dell'anello rispetto a $(\mathbb{R}^{\mathbb{R}}, \cdot)$ è la funzione $1 : \mathbb{R} \to \mathbb{R}$ definita come:

$$1(x) = 1$$

L'anello ha divisori dello 0. Ne facciamo un esempio, trovarne altri per esercizio. Consideriamo due funzioni $f, g \neq \underline{0}$. $f : \mathbb{R} \to \mathbb{R}$ è definita così:

$$f(x) = \begin{cases} x \text{ se } x = 2n \\ 0 \text{ altrimenti} \end{cases}$$

$g : \mathbb{R} \to \mathbb{R}$ è definita così:

$$g(x) = \begin{cases} x \text{ se } x = 2n + 1 \\ 0 \text{ altrimenti} \end{cases}$$

Il prodotto $(f \cdot g)(x) = 0 \ \forall \ x \in \mathbb{R}$, quindi $f \cdot g = \underline{0}$. Abbiamo trovato due elementi del gruppo $(\mathbb{R}^{\mathbb{R}}, \cdot)$ il cui prodotto dà $\underline{0}$ anche se sono entrambi diversi da $\underline{0}$. Quindi f e g sono due divisori dello 0.

2.4.2 Teorema di divisione

Teorema 2.4.1 (*Teorema di divisione per $\mathbb{Z}$*)

Dato $a \in \mathbb{Z}$ e un $n \in \mathbb{N}$ tale che $n > 0$, allora esistono due numeri $q, r \in \mathbb{Z}$ tali che
1D $a = n \cdot q + r$
2D $0 \leq r < n$

Inoltre, la coppia q, r è unica. Ossia se la coppia (q', r') soddisfa 1D e 2D, allora $q = q'$ e $r = r'$.

Dimostrazione: Lo dimostriamo usando il principio del buon ordinamento di $\mathbb{N}$: tutti i sottoinsiemi di $\mathbb{N}$ diversi dal vuoto hanno un primo elemento.

Sia $n > 2$. Definiamo l'insieme $M = \{m \in \mathbb{N} : m = a - n \cdot q \text{con} q \in \mathbb{Z}\}$. Il resto r è uno degli elementi di M, in particolare il più piccolo.

$M \neq \emptyset$, perché se $a > 0 \Rightarrow a \in M$ con $q = 0$. Se invece $a \leq 0$, basta porre $q = a \Rightarrow a - n \cdot a > 0 \Rightarrow a - n \cdot a \in M$.

Siccome M è diverso dal vuoto e è sottoinsieme di $\mathbb{N}$, segue per il principio del buon ordinamento che M ha un primo elemento r (il più piccolo). Quindi $r = a - n \cdot q \Rightarrow a = n \cdot q + r$.

Dobbiamo dimostrare la seconda proprietà, ossia che $0 \leq r < n$

Supponiamo per assurdo che $n \leq r \Rightarrow r = n + x$ con $x \leq r$. Siccome $a = n \cdot q + r$, $a = n \cdot q + (n + x) = n(q + 1) + x \Rightarrow x \in M$, e x minore di r, quindi ho l'assurdo: è r il più piccolo elemento di M. ■

Possiamo enunciare il teorema generale di divisione:

Teorema 2.4.2 (*Teorema di divisione generale*)

Dati $a, b \in \mathbb{Z}$, con $b \neq 0$, $\exists\, q, r \in \mathbb{Z}$ tali che $a = q \cdot b + r$ e $0 \leq r < |b|$. La coppia q, r è unica anche in questo caso. Segue come conseguenza dal teorema precedente.

2.4.3 Minimo comune multiplo e massimo comun divisore

Definizione 2.4.4 (*Minimo comune multiplo*)

Il $\text{mcm}(a, b)$ *è un* $m \in \mathbb{N}$ *tale che:*

1. $m \geq 0$
2. $m = k \cdot a$ *e* $m = h \cdot b$
3. m *è il* $\sup(a, b)$ *nel reticolo della divisibilità, ossia se* $z = k'a$ *e* $z = h'b$, *allora* $m \leq z$.

Definizione 2.4.5 (*Massimo comun divisore*)

Il $\text{MCD}(a, b)$ *è un* $d \in \mathbb{N}$ *tale che:*

1. $d \geq 0$
2. $d \mid a$ *e* $d \mid b$
3. d *è l'*$\inf(a, b)$ *nel reticolo della divisibilità, ossia se* $d' \mid a$ *e* $d' \mid b$, *allora* $d' \leq d$.

Esistenza del minimo comune multiplo e del massimo comun divisore

Dimostrazione: Il minimo comune multiplo esiste per il principio del buon ordinamento.

Definiamo l'insieme $M = \{t \in \mathbb{N} : t = k \cdot a \text{ e } t = h \cdot b\}$, M è non vuoto, infatti $a \cdot b \in M$. Ha un primo elemento, quindi $\text{mcm}(a, b)$ è il più piccolo elemento di M. ■

La dimostrazione per il MCD è più lunga.

Consideriamo $a, b \in \mathbb{Z}$ con $b \neq 0$, $\text{MCD}(a, b) = \text{MCD}(|a|, |b|)$. Supponiamo $a, b > 0$.

Indichiamo con $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ l'insieme degli interi positivi escluso lo 0. Consideriamo quindi l'insieme $S_{a,b} = \{n \in \mathbb{N}^* : n = a \cdot x + b \cdot y \text{ con } x, y \in \mathbb{Z}\}$, ossia l'insieme degli interi positivi n che sono combinazione lineare di a e di b. x ed y sono detti "coefficienti della combinazione".

$S_{a,b} \neq \emptyset$, infatti $a + b$, a, b sono tutti elementi di $S_{a,b}$.

$S_{a,b}$ ha un minimo d, che è proprio il $\text{MCD}(a, b)$. Bisogna dimostrare che:

1. $d \mid a$ e $d \mid b$
2. $z \mid a$ e $z \mid b \Rightarrow z \mid d$, ossia d è il $\sup(a, b)$ nel reticolo $(\mathbb{N}, \mid)$

Dimostrazione del punto 1 : Per ipotesi, d è il minimo di $S_{a,b}$ e $d = s \cdot a + t \cdot b$. Dobbiamo dimostrare che $d \mid a$, quindi che $a = q \cdot d + r$ con $r = 0$.

$$\begin{aligned} r &= a - q \cdot d \Rightarrow \\ r &= a - q \cdot (s \cdot a + t \cdot b) = \\ &= a - q \cdot s \cdot a - q \cdot t \cdot b = \\ &= a \cdot (1 - q \cdot s) + b \cdot (-q \cdot t) \end{aligned}$$

r è una combinazione lineare di a e b, quindi dovremmo avere che $r \in S_{a,b}$, se r fosse diverso da 0. Ma per il teorema di divisione su $\mathbb{Z}$ sappiamo che $0 \leq r < d$. Essendo d il minimo di $S_{a,b}$, r non può appartenere a $S_{a,b}$, quindi è necessariamente 0. ■

Dimostrazione del punto 2 : Per ipotesi, $z \mid a$ e $z \mid b$. Dobbiamo dimostrare che se $z < d$ allora $z \mid d$. Sappiamo che $a = z \cdot k$ e $b = z \cdot h$. Sapendo che $d = s \cdot a + b \cdot t$, possiamo sostituire e ottenere $d = s \cdot z \cdot k + t \cdot z \cdot h$, quindi $d = z \cdot (s \cdot k + t \cdot h)$, quindi d è un multiplo di z. ■

2.4.4 Algoritmo di Euclide per il calcolo del MCD

Il MCD si calcola con l'algoritmo di Euclide delle divisioni successive, basato sul lemma 2.4.3.

Lemma 2.4.3

Siano $a > b > 0$, posto $d = \text{MCD}(a, b)$ e $d' = \text{MCD}(b, r)$ dove $a = q \cdot b + r$, allora $d = d'$.

Dimostrazione : Dobbiamo dimostrare che $d \mid d'$ e $d' \mid d$, e che quindi sono uguali.
$d \mid a$, $d \mid b \Rightarrow d \mid (b \cdot q + r)$, ma siccome $d \mid b$, se divide la somma e uno degli addendi, divide anche l'altro addendo, quindi $d \mid r$. Da $d \mid r$e $d \mid b \Rightarrow d \mid d'$, e quindi $d < d'$. È necessariamente più piccolo del $\text{MCD}(b, r)$, poiché divide entrambi.
Ma $d' \mid b$ e $d' \mid r \Rightarrow d' \mid a = q \cdot b + r$. Quindi, visto che $d' \mid a$ e $d' \mid b \Rightarrow d' \mid d$. ■

Algoritmo di Euclide delle divisioni successive

Poniamo $a > b > 0$.

1. Usando il teorema di divisione su $\mathbb{Z}$, scriviamo a come $b \cdot q_1 + r_1$ con $0 \leq r_1 < b$. Se $r_1 = 0$ abbiamo trovato il $\text{MCD}(a, b) = b$, altrimenti continuiamo.
2. Sempre per il teorema di divisione, scriviamo $b = r_1 \cdot q_2 + r_2$ con $0 \leq r_2 < r_1$. Se $r_2 = 0$ abbiamo trovato il $\text{MCD}(a, b) = r_1$, ossia l'ultimo resto non nullo, altrimenti continuiamo.
3. Continuiamo a scrivere $r_1 = r_2 \cdot q_3 + r_3$. Il $\text{MCD}(a, b)$ sarà l'ultimo resto non nullo.

Poiché $0 \leq r_{(i+1)} < r_i$, $\exists\, n > 0$ tale che $r_n \neq 0$ e $r_{(n+1)} = 0$. Quindi al passo n-esimo avremo:

$$\begin{aligned} n.\ r_{(n-2)} &= r(n-1) \cdot q_n + r_n \\ (n+1).\ r_{(n+1)} &= q_{(n+1)} \cdot r_n + 0 \end{aligned}$$

Per il lemma 2.4.3 segue che $\text{MCD}(a, b) = \text{MCD}\left(r_{(n-1)}, r_n\right) = r_n$.

Identità di Bézout

Dall'algoritmo di Euclide possiamo ricavere l'identità di Bézout.

Dati $a, b \in \mathbb{Z}$ con $a, b > 0$, riprendiamo la definizione dell'insieme $S_{a,b}$:

$$S_{a,b} = \{m \in \mathbb{N}^+ : ax + by = m \text{ con } x, y \in \mathbb{Z}\}$$

Questo insieme ha un minimo $d = \inf S_{a,b} = \text{MCD}(a, b)$. d, essendo un elemento di $S_{a,b}$ si può scrivere come combinazione lineare di a e b, ossia $d = a \cdot s + b \cdot t$ con $s, t \in \mathbb{Z}$. Si chiama identità di Bézout. Le coppie s, t sono infinite (e quindi anche le identità di Bézout lo sono). L'insieme $D_{a,b}$ contiene tutte queste coppie:

$$D_{a,b} = \{(s, t) \in \mathbb{Z} \times \mathbb{Z} : d = a \cdot s + b \cdot t\}$$

Data una coppia (s, t), posso trovare ogni altra coppia $(s + k \cdot b, t - k \cdot a) \in D_{a,b}$ al variare di $k \in \mathbb{Z}$. Infatti andando a sostituire ho che:

$$a \cdot (s + k \cdot b) + b \cdot (t - k \cdot a) = a \cdot s + k \cdot a \cdot b + b \cdot t - k \cdot b \cdot a = a \cdot s + b \cdot t$$

Per calcolare una identità di Bézout si usa l'algoritmo di Euclide delle divisioni successive.

Proposizione 2.4.4

$S_{a,b}$ è l'insieme di tutti i multipli di $d = \text{MCD}(a, b)$.

$$S_{a,b} = \{k \cdot d : k \in \mathbb{N}^+ \text{ con } d = \text{MCD}(a, b)\}$$

Dimostrazione: Se $m = k \cdot d \Rightarrow m \in S_{a,b}$.
$m = k \cdot d = k \cdot (a \cdot s + b \cdot t) = a \cdot (k \cdot s) + b \cdot (k \cdot t) \Rightarrow m \in S_{a,b}$ perché possiamo prendere $x = k \cdot s$ e $y = k \cdot t$ e avere $m = a \cdot x + b \cdot t$.
Viceversa se $m \in S_{a,b} \Rightarrow m = k \cdot d$.
$m = a \cdot x + b \cdot y$. Essendo $d = \text{MCD}(a, b)$, ho che $a = h \cdot d$ e $b = h' \cdot d$. Quindi $m = h \cdot d \cdot x + h' \cdot d \cdot y = (h \cdot x + h' \cdot y) \cdot d \Rightarrow m$ è multiplo di d. ■

Esempio:

Troviamo il $\text{MCD}(159, 42) = d$, scrivendo ogni volta il resto r come combinazione di a e b, dopodiché scriviamo d come identità di Bézout.

Come si vede dalla tabella 2.8, il $\text{MCD}(159, 42)$ è 3.

Dobbiamo trovare l'identità di Bézout per 3. Possiamo iniziare scrivendo $3 = 9 - 6$, per poi sostituire i resti.

$$\begin{aligned}
3 &= 9 - 6 = \\
&= 9 - 33 + 9 \cdot 3 = 9 \cdot 4 - 33 = \\
&= 42 \cdot 4 - 33 \cdot 4 - 33 = 42 \cdot 4 - 33 \cdot 5 = \\
&= 42 \cdot 4 - 159 \cdot 5 + 42 \cdot 15 = \\
&= 42 \cdot 19 - 159 \cdot 5
\end{aligned}$$

$$159 > 42$$

1	$159 = 42 \cdot (3) + 33$	$33 = 159 - 42 \cdot (3)$
2	$42 = 33 \cdot (1) + 9$	$9 = 42 - 33$
3	$33 = 9 \cdot (3) + 6$	$6 = 33 - 9 \cdot (3)$
4	$9 = 6 + 3$	$3 = 9 - 6$
5	$6 = 3 \cdot (2)$	

Tabella 2.8: L'algoritmo di Euclide per trovare il MCD$(159, 42)$, con il resto di ogni passaggio scritto come identità di Bézout

2.4.5 Anello degli interi

Definizione 2.4.6 (*Numeri coprimi*)

Dati $a, b \in \mathbb{Z}$, a e b si dicono coprimi tra loro se $\text{MCD}(a, b) = 1$.

Definizione 2.4.7 (*Numero primo*)

$p \in \mathbb{N}$ si dice primo se $p \neq 1$ e è divisibile solo per 1 e per p.

Ripasso. $(\mathbb{Z}, +, \cdot)$ è un anello commutativo unitario privo di divisori dello zero.

Per costruire l'insieme $\mathbb{Z}$ abbiamo preso $\mathbb{N}$, costruito $\mathbb{N} \times \mathbb{N}$, abbiamo considerato il monoide $(\mathbb{N}, +)$ e creato il monoide $(\mathbb{N} \times \mathbb{N}, +)$. Sappiamo che prendendo una struttura algebrica e facendo il prodotto cartesiano della struttura per sé stessa si ottiene una struttura algebrica che mantiene le stesse operazioni e le stesse proprietà.

Abbiamo definito $+ : (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{N} \times \mathbb{N}$, dati $(a, b), (c, d)$, come $(a, b) + (c, d) \mapsto (a + c, b + d)$

Per ottenere l'insieme $\mathbb{Z}$ abbiamo definito una relazione di equivalenza su $\mathbb{N} \times \mathbb{N}$, ρ, che è una congruenza rispetto a $+$. $(\mathbb{N} \times \mathbb{N}/\rho, +)$ quindi è un monoide *perché ρ è una congruenza.*

Abbiamo detto che dati due elementi $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$, sono in relazione $(a, b)\ \rho\ (c, d) \Leftrightarrow a + d = b + c$, ossia se $a - b = c - d$.

Esercizio 15

Dimostrare che ρ è una congruenza.

Nota a margine: $\mathbb{N} \times \mathbb{N} \cong \mathbb{R}$, ossia è in corrispondenza biunivoca con i reali.

Abbiamo visto che le classi individuate da ρ sono di tre tipi, e che a ogni classe corrisponde un intero in $\mathbb{Z}$.

$$[(m, n)] = \begin{cases} [(m, 0)] = +m \\ [(0, 0)] = \underline{0} \\ [(0, m)] = -m \end{cases}$$

Quindi $(\mathbb{N} \times \mathbb{N}/\rho, +)$ non è solo un monoide: è un gruppo, perché ha l'inverso! Infatti:

$$[(m, 0)] + [(0, m)] = [(m, m)] = [(0, 0)]$$

L'anello degli interi $(\mathbb{Z}, +, \cdot)$ ha un'altra operazione, $\cdot$, che si potrebbe pensare dipendere da $(\mathbb{N}, \cdot)$, ma ρ non è una congruenza rispetto a $(\mathbb{N} \times \mathbb{N}, \cdot)$, se definiamo $\cdot$ naturalmente.

Consideriamo $\cdot : (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{N} \times \mathbb{N}$ tale che $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$. Con questa operazione, ρ *non* è una congruenza. Dobbiamo scegliere un'altra operazione $\cdot$ su $\mathbb{N} \times \mathbb{N}$.

Vediamo intanto che ρ non è una congruenza rispetto a $\cdot$.

Basta un controesempio: $(3,0)\cdot(2,0)=(6,0)$. Prendiamo ora un elemento nella classe $[(3,0)]$, ad esempio $(6,3)$, ed un elemento nella classe $[(2,0)]$, ad esempio $(4,2)$. Il loro prodotto $(6,3)\cdot(4,2)=(24,6)\in[(18,0)]\neq[(6,0)]$.

Per ottenere quindi una congruenza serve un'operazione di moltiplicazione differente in $\mathbb{N}\times\mathbb{N}$.

Se definiamo la congruenza come $(m,n)\ \rho\ (p,q)\Leftrightarrow m\cdot q=n\cdot p$, abbiamo che:

$$\begin{aligned}(m-n)(p-q)=\\ mp-np+nq-mq=\\ mp+nq-(np+mq)\end{aligned}$$

Se voglio esprimere questo intero $mp+nq-(np+mq)\in\mathbb{N}\times\mathbb{N}$, come dobbiamo esprimerlo? Che coppia deve darmi?

$$(m,n)\cdot(p,q)\in[((mp+nq),(np+mq))]$$

Questa parte non mi è assolutamente chiara.

2.4.6 Anello degli interi modulo n intero

Fissato un interno $n\geq 2$, abbiamo definito la congruenza $\equiv_n$ (congruenza modulo n) come:

$$a,b\in\mathbb{Z},\ a\equiv_n b\Leftrightarrow n\mid(a-b)$$

È una congruenza rispetto a entrambe le operazioni, $+$ e $\cdot$.

$(\mathbb{Z}/\equiv_n,+,\cdot)$ è un anello commutativo e unitario. Non è privo di divisori dello zero.

$$\mathbb{Z}/\equiv_2=\{[0],[1]\}$$

Ogni classe $[a]\in\mathbb{Z}/\equiv_n$ può essere rappresentato con il suo resto, ossia $[a]=[r]$ dove r è il resto nella divisione di a per n.

Possiamo considerare $\mathbb{Z}_n$ come l'insieme dei resti delle possibili divisioni per n.

$$\mathbb{Z}_n=\{0,1\ldots(n-1)\}$$

Esiste l'isomorfismo $\varphi_n:\mathbb{Z}/\equiv_n\to\mathbb{Z}_n$ che associa ad ogni classe il resto della divisione per n, ossia $\varphi_n[a]=r$

$(\mathbb{Z}_n,+,\cdot)$ è un anello.

$$\mathbb{Z}/\equiv_3=\{[0],[1],[2]\}\leftrightarrow\mathbb{Z}_3=\{0,1,2\}$$

Se il gruppo è finito possiamo scrivere le tavole di composizione rispetto alle operazioni.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Tabella 2.9: Tavole di composizione di $+$ e $\cdot$ in $\mathbb{Z}_3$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabella 2.10: Tavole di composizione di $+$ e $\cdot$ in $\mathbb{Z}_4$

Quando l'operazione è commutativa, la tavola è uguale (è simmetrica) rispetto alla diagonale.

$(\mathbb{Z}_3, +, \cdot)$ è sempre un anello commutativo unitario. Ha l'unità rispetto al $\cdot$, ossia 1.

Sia $(A, +, \cdot)$ un anello unitario (ossia monoide associativo rispetto a $\cdot$), indichiamo con $U(A)$ è il gruppo degli elementi invertibili di A rispetto a $\cdot$. Alcuni esempi:

$$\begin{aligned} U(\mathbb{Z}) &= \{-1, 1\} \\ U(\mathbb{Z}_2) &= \{1\} \\ U(\mathbb{Z}_3) &= \{1, 2\} \\ U(\mathbb{Z}_4) &= \{1, 3\} \end{aligned}$$

Vogliamo capire come è fatto in generale il gruppo degli elementi invertibili in $\mathbb{Z}_n$.

Proposizione 2.4.5

$[a] \in U(\mathbb{Z}/\equiv_n) \Leftrightarrow a, n$ *sono coprimi, ossia* $\text{MCD}(a, n) = 1$.

Corollario 2.4.6

$$U(\mathbb{Z}_n) = \{x \in \mathbb{N} : 0 < x < n \ e \ \text{MCD}(n, x) = 1\}$$

Osservazione 8

Considerando $\mathbb{Z}_p$ con p primo, il gruppo dei suoi elementi invertibili è $U(\mathbb{Z}_p) = \{1 \dots (p-1)\}$, ossia contiene tutti gli interi minori di p.

Dimostrazione: Per ipotesi, la classe $[a]$ è invertibile in $\mathbb{Z}/\equiv_n \Rightarrow \ \exists\, [b]$ t.c. $[a] \cdot [b] = [1]$.

Quindi per definizione di prodotto tra classi $[a] \cdot [b] = [a \cdot b] = [1]$. Quindi a e b nella divisione per n hanno lo stesso resto, ossia 1, quindi $a \cdot b = n \cdot q + 1$, e per il teorema di Bézout $a \cdot b - n \cdot q = 1$, ossia $1 \in S_{a,n} \Leftrightarrow 1$ è combinazione lineare di a e n. Quindi il $\text{MCD}(a, n)$ è 1, e a e n sono coprimi.

Dobbiamo dimostrare il viceversa, ossia che $\text{MCD}(a, n) = 1 \Rightarrow [a]$ è invertibile in $\mathbb{Z}/\equiv_n$.

Quindi 1 è combinazione lineare di a e n, ossia $1 = a \cdot s + n \cdot t$. Quindi passando alle classi, $[1] = [a \cdot s + n \cdot t] = [a \cdot s] + [n \cdot t] = [a] \cdot [s] + [0] = [a] \cdot [s]$, quindi la classe rappresentata da s è l'inverso della classe rappresentata da a, perché $[a] \cdot [s] = [1]$. ■

Grazie all'identità di Bézout possiamo trovare l'inverso di una classe.

$$[s] = [a]^{-1}$$

Se prendiamo $\mathbb{Z}_p$ con p primo, $U(\mathbb{Z}_p) = \mathbb{Z}_p - \{0\}$, ed è un gruppo, quindi $(\mathbb{Z}_p, +, \cdot)$ è un campo, ossia è una struttura algebrica con due operazioni su un insieme K tale che:

1. $(K, +, \cdot)$ è un anello commutativo unitario,
2. $(K \setminus \{0\}, \cdot)$ è un gruppo commutativo,

3. valgono le leggi distributive.

I campi non hanno divisori dello zero, ma gli anelli $(\mathbb{Z}_n, +, \cdot)$ hanno divisori dello zero. Infatti, siccome n non è primo, possiamo scrivere $n = a \cdot b$, quindi la classe $[0] = [a \cdot b] = [a] \cdot [b]$ entrambi diversi da 0.

Il campo $(\mathbb{Z}_p, +, \cdot)$ non ha divisori dello 0. Sia $a \cdot b = 0$ con $a \neq 0$ e $b \neq 0$, avendo l'inverso per ogni elemento diverso da 0 dovrei avere che $a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 \Rightarrow b = 0$ ma sarebbe un assurdo.

Teorema 2.4.7

La classe $[a] \in \mathbb{Z}/\equiv_n$ è invertibile $\Leftrightarrow \text{MCD}(a, n) = 1$, ossia se a e n sono coprimi.

Da questo teorema possiamo dedurre due corollari.

Corollario 2.4.8

$\mathbb{Z}_p = \{0, 1 \dots (p-1)\}$, ossia l'anello dei resti modulo p, è un campo $\Leftrightarrow$ p è un numero primo, ossia p è maggiore di 1 ed è divisibile solamente per 1 e per p.
Essere un campo significa che $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ è un gruppo abeliano.

Corollario 2.4.9

Sia p un numero primo, $p \mid a \cdot b \Rightarrow p \mid a$ oppure $p \mid b$.

Dimostrazione: Consideriamo il campo $(\mathbb{Z}_p, +, \cdot)$. Se $p \mid a \cdot b$, significa che $[p] = [0] = [a \cdot b] = [a] \cdot [b]$. Siamo in un campo, che non ha divisori dello zero. Quindi $[a] = [0]$ oppure $[b] = [0]$. ■

Proposizione 2.4.10

Ogni numero naturale $n \in \mathbb{N}$ maggiore di 1, o è primo o è prodotto di primi.

Dimostrazione: Si dimostra per induzione su n. Per $n = 2$ è vero.

L'ipotesi di induzione è che $P(m)$ è vera $\forall\ m \geq 2$ con $m < n$.

Dobbiamo dimostrare che $P(n)$ è vera. O n è primo, e ho verificato $P(n)$, oppure n non è primo, ossia $n = a \cdot b$ con $a < n$ e $b < n$. Per ipotesi di induzione $P(a)$ e $P(b)$ sono vere, quindi a è prodotto di primi o è primo, b è prodotto di primi o è primo, quindi n è prodotto di primi. ■

Teorema 2.4.11 (*Teorema fondamentale dell'aritmetica*)

Ogni numero naturale $n \geq 2$ si esprime in un unico modo come prodotto di potenze di numeri primi, ossia n ha una sola fattorizzazione.

$$n = p_1^{h_1} \cdot \ldots \cdot p_k^{h_k} = q_1^{t_1} \cdot \ldots \cdot q_s^{t_s} \Rightarrow k = s \ e\ \ \forall\ i \in [1, k]\ \exists\ j\ \ t.c.\ \ p_i^{h_i} = q_j^{t_j}$$

Dimostrazione: Si dimostra per induzione. Per $n = 2$ è vero.

Supponiamo come ipotesi induttiva che $P(m)$ sia vero per ogni m tale che $2 \leq m < n$. Per induzione dimostriamo che $P(n)$ è vera. Sappiamo che n si esprime come prodotto di primi:

$$n = p_1^{h_1} \cdot \ldots \cdot p_k^{h_k} = q_1^{t_1} \cdot \ldots \cdot q_s^{t_s}$$

p_1 divide n, quindi divide anche $q_1^{t_1} \cdot \ldots \cdot q_s^{t_s}$.

$$p_1 \mid n = q_1^{t_1} \cdot \ldots \cdot q_s^{t_s}$$

Per il corollario 2.4.9 $\exists\ j = 1 \dots s$ tale che $p_1 \mid q_j$. Ma posso ripetere lo stesso discorso per q_j: per il corollario 2.4.8 q_j divide n, quindi $q_j \mid n = p_1^{h_1} \cdot \ldots \cdot p_k^{h_k}$. Di nuovo, per il corollaro 2.4.9, deve esistere un indice i_j tale che $q_j \mid p_{i_j}$.
$p_1 \mid q_j \mid p_{i_j} \Rightarrow p_1 = q_j = p_{i_j}$, essendo tutti primi devono essere uguali.
Essendo p_1 e q_j uguali, se divido n per p_1 ottengo due scomposizioni:

$$\frac{n}{p_1} = p_1^{h_1 - 1} \cdot \ldots \cdot p_k^{h_k} = q_1^{t_1} \cdot \ldots \cdot q_j^{t_j - 1} \cdot \ldots \cdot q_s^{t_s}$$

Sia $m = \frac{n}{p_1} < n \Rightarrow P\left(\frac{n}{p_1}\right)$ è vera per ipotesi $\Rightarrow P(n)$ è vera.

Infatti per $P\left(\frac{n}{p_1}\right)$, $k = s$ e $\ \forall\ i = 1 \dots k\ \exists\ r$ tale che $p_i^{h_i} = q_r^{t_r}$. ■

Da questo segue:

Teorema 2.4.12

I numeri primi sono infiniti.

Dimostrazione: Supponiamo per assurdo che i numeri primi siano finiti. Abbiamo la lista di numeri primi $p_1 \dots p_N$. Consideriamo $n = (p_1 \dots p_N) + 1$. Non può essere un numero primo, perché non è nella lista. Per il teorema fondamentale deve essere il prodotto di numeri primi.
Sia p_i un intero tale che $p_i \mid n = (p_1 \dots p_i \dots p_N) + 1 \Rightarrow p_i \mid (p_1 \dots p_i \dots p_N)$ e $p_i \mid 1$, che è l'assurdo. ■

2.4.7 Funzione di Eulero

Abbiamo visto che $(\mathbb{Z}_n, +, \cdot)$ è un anello. Se n è primo, è un campo, quindi non ha divisori dello zero. Se invece $n = a \cdot b$ con $a < n$ e $b < n$, allora $(\mathbb{Z}_n, +, \cdot)$ è un anello con divisori dello zero.

Abbiamo chiamato $U(A)$ il gruppo degli elementi invertibili rispetto a $\cdot$ dell'anello $(A, +, \cdot)$. Considerando il campo $(\mathbb{Z}_p, +, \cdot)$ il gruppo degli invertibili $U(\mathbb{Z}_p) = \{1, \dots, p-1\}$, quindi la cardinalità $|U(\mathbb{Z}_p)| = p - 1$. Troviamo la cardinalità di $U(\mathbb{Z}_n)$ nel caso generale.

Consideriamo la funzione $\Phi : \mathbb{N}^+ \to \mathbb{N}^+$ definita come:

$$\Phi(n) = \text{ numero degli interi minori di } n \text{ e primi con } n$$

È verificato subito che $|U(\mathbb{Z}_n)| = \Phi(n)$. Infatti avevamo definito $U(\mathbb{Z}_n)$ come:

$$U(\mathbb{Z}_n) = \{m \in \mathbb{Z}_n : \mathrm{MCD}(m, n) = 1\}$$

Calcoliamo questa funzione (detta funzione di Eulero).

Sia $n = p_1^{h_1} \dots p_k^{h_k}$, se voglio conoscere $\Phi(n)$, so che sono n meno tutti i numeri che dividono n. Chiamo D l'insieme dei numeri $m < n$ che dividono n.

$$\Phi(n) = n - D$$

D si calcola con il principio di inclusione ed esclusione.

Sia p_i un fattore di n, indicando con A_{p_i} l'insieme dei multipli di p_i minori di n, abbiamo che:

$$A_{p_i} = \{m \in [n] : p_i \mid m\} \Rightarrow D = \bigcup_{i=1}^{k} A_{p_i}$$

Quindi:

$$\begin{aligned}\left|\bigcup_{i=1}^{k} A_{p_i}\right| = &\sum_{1\le i\le k} |A_{p_i}| \\ &- \sum_{1\le i<j\le k} \left|A_{p_i} \cap A_{p_j}\right| \\ &+ \sum_{1\le i<j<h\le h} \left|A_{p_i} \cap A_{p_j} \cap A_{p_h}\right| + \dots \\ &+ (-1)^{k-1} \left|A_{p_i} \cap \dots \cap A_{p_k}\right|\end{aligned}$$

Sappiamo che la cardinalità $|A_{p_i}| = \frac{n}{p_i}$. Infatti da $n = k \cdot p_i \Rightarrow k = \frac{n}{p_i}$, abbiamo che k è la cardinalità dell'insieme dei numeri multipli di p_i e non coprimi con n.

Se prendiamo l'intersezione di due insiemi? La cardinalità $\left|A_{p_i} \cap A_{p_j}\right|$ con $i \neq j$ è:

$$\left|A_{p_i} \cap A_{p_j}\right| = \frac{n}{p_i \cdot p_j}$$

L'ultima intersezione ha cardinalità 1. Mettendo in evidenza si ha:

$$\Phi(n) = n - |D| = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$$

Teorema 2.4.13 (*Teorema di Fermat*)

Se prendo $a \in \mathbb{Z}$ e $n \geq 2$ tali che $\mathrm{MCD}(a, n) = 1$, *allora* $a^{\Phi(n)} \equiv_n 1$.

Dimostrazione: L'insieme degli elementi invertibili di $\mathbb{Z}_n$ è l'insieme di tutti gli $h \in \mathbb{Z}_n$ tali che $\mathrm{MCD}(h, n) = 1$.

$$\begin{aligned}U(\mathbb{Z}_n) &= \{h \in \mathbb{Z}_n : \mathrm{MCD}(h, n) = 1\} \\ |U(\mathbb{Z}_n)| &= \Phi(n).\end{aligned}$$

Il prodotto $\prod_{h\in U(\mathbb{Z}_n)}[h \cdot a]$ per definizione del prodotto fra classi è:

$$\begin{aligned}&\prod_{h\in U(\mathbb{Z}_n)} [h \cdot a] = \\ &\prod_{h\in U(\mathbb{Z}_n)} [h] \cdot [a] = \qquad\qquad \text{e mettendo in evidenza } a \\ &[a]^{\Phi(n)} \cdot \prod_{h\in U(\mathbb{Z}_n)} [h]\end{aligned}$$

Siccome il $\mathrm{MCD}(h, n) = 1$ e il $\mathrm{MCD}(a, n) = 1$, allora il $\mathrm{MCD}(a \cdot h, n) = 1$. Quindi:

$$\begin{aligned}&\prod_{h\in U(\mathbb{Z}_n)} [h \cdot a] = \\ &\prod_{h\in U(\mathbb{Z}_n)} [h]\end{aligned}$$

Deve quindi essere che $[a]^{\Phi(n)} = 1$, e quindi che $a^{\Phi(n)} \equiv_n 1$. ■

Corollario 2.4.14 (*Piccolo teorema di Fermat*)

Dato p primo segue che $a^{p-1} \equiv_p 1$.

Esempio :

Calcolare le ultime 2 cifre di 81^{82}. Le ultime due cifre sono il resto modulo 100, quindi passando alle classi dobbiamo calcolare $r < 100$ tale che $81^{82} \equiv_{100} r$, ossia il rappresentante della classe.

Usiamo il teorema di Fermat. Per i teorema di Fermat sappiamo che $81^{\Phi(100)} \equiv_{100} 1$. Essendo $\Phi(100) = 40$, possiamo quindi dire che $81^{40} \equiv_{100} 1$.Quindi:

$$81^{82} = 81^{80+2} = 81^{80} \cdot 81^2$$
$$81^{80} \cdot 81^2 \equiv_{100} 1 \cdot 81^2 \Rightarrow 6561 \equiv_{100} 61$$

Proposizione 2.4.15

Il teorema di Fermat:

$$\text{MCD}(a, n) = 1 \Rightarrow a^{\Phi(n)} \equiv 1 \pmod{n}$$

è un corollario del teorema di Lagrange.

Dimostrazione : Il teorema di Lagrange dice che dato un gruppo finito, l'ordine di ogni suo sottogruppo divide l'ordine del gruppo. Quindi, dato un gruppo G finito e S sottogruppo di G, $|S| \mid |G|$ (ossia la cardinalità di S divide la cardinalità di G).

$\Phi(n) = |U(\mathbb{Z}_n)|$, ossia è la cardinalità del gruppo degli elementi invertibili rispetto a $\cdot$ dell'anello $(\mathbb{Z}_n, +, \cdot)$.

Consideriamo quindi $G = U(\mathbb{Z}_n)$, e $S = <a>$, il sottogruppo generato da a, ossia tutte le potenze di a.

$<a> = \{a^0, \dots a^t\}$. Ha $t + 1$ elementi. Quindi $a^{t+1} = 1$.

Consideriamo $(\mathbb{Z}_{12}, +, \cdot)$, con $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

$$U(\mathbb{Z}_{12}) = \{a : \text{MCD}(a, 12) = 1\} = \{1, 5, 7, 11\}$$

L'inverso di 5 è 5, perché $5 \cdot 5 = 25 \equiv_{12} 1$. L'inverso di 7 è 7, l'inverso di 11 è 11. L'ordine di $U(\mathbb{Z}_{12})$ è 4. Abbiamo tre sottogruppi non banali di ordine 2.

Prendiamo il sottogruppo $S = <5> = \{1, 5\}$. Attenzione: dire che $\text{MCD}(a, n) = 1$ in questo caso significa che $a \in U(\mathbb{Z}_n)$.

L'ordine di $<5>$ è il più piccolo intero positivo che mi dà 1. Quindi $5^2 = 1$, essendo l'ordine di $S = \{1, 5\}$ pari a 2.

Siccome l'ordine $|<a>| = o \mid \Phi(n)$, $\Phi(n) = k \cdot o$. Quindi $a^{\Phi(n)} = a^{o \cdot k} = 1^k = 1$. ■

2.4.8 Equazioni di primo grado in $\mathbb{Z}_n$

Come è fatta un'equazione di primo grado in $\mathbb{Z}_n$?

1. se la vedo in $\mathbb{Z}_n$, ho:

$$a \cdot x = b \text{ con } a, b, x \in \mathbb{Z}_n$$

2. se la vedo nell'insieme quoziente $\mathbb{Z}/\equiv_n$, ho:

$$[a] \cdot [x] = [b] \text{ in } \mathbb{Z}/\equiv_n$$

3. se la vedo in $\mathbb{Z}$, ho:

$$a \cdot x \equiv_n b \text{ con } a, b, x \in \mathbb{Z}$$

Osservazione 9

Le soluzioni di 3, se esistono, sono infinite, perché se $s \in \mathbb{Z}$ è una soluzione, $a \cdot s \equiv_n b$. Quindi ogni altro $s' \in [s]$ è tale che $a \cdot s' \equiv_n b$.
Passando alle classi si legge come $[a \cdot s] = [b] \Rightarrow [a] \cdot [s] = [b]$, e prendendo un altre rappresentante $s' \in [s]$, $[s'] = [s]$ e quindi anche $[a] \cdot [s'] = [b]$

In generale si distinguono due casi per la risoluzione delle equazioni:

1. $$\text{MCD}(a, n) = 1$$

   $[a]$ è invertibilie in $\mathbb{Z}/\equiv_n$, ossia se $a < n \Rightarrow a$ è invertibile in $\mathbb{Z}_n$. Quante soluzioni ci sono?

   - Nel caso 1 $a \cdot x = b$ in Z_n, $x = a^{-1} \cdot b$. La soluzione è unica.
   - Nel caso 2 $[a] \cdot [x] = [b]$, allora la soluzione $[x] = [a]^{-1} \cdot [b]$. La soluzione è unica.
   - Nel caso 3 le soluzioni sono infinite e sono tutte congruenti a x modulo n.

   Sappiamo che $x = a^{-1} \cdot b$. Come si trova a^{-1}? Con l'identità di Bézout. Siccome $\text{MCD}(a, n) = 1$, possiamo scrivere l'identità di Bézout per a, n.

   $$1 = a \cdot s + n \cdot t$$

   Passiamo alle classi modulo $[n]$.

   $$[1] = [a \cdot s] + [n \cdot t] = [a \cdot s] + [0] = [a] \cdot [s] \Rightarrow [a^{-1}] = [s]$$

   Quindi $[a^{-1}] = [s]$, ma potendo scrivere s come $n \cdot q + r$, abbiamo che $a^{-1} = r$.

2. $$\text{MCD}(a, n) = d > 1$$

   Proposizione 2.4.16

   L'equazione $a \cdot x = b$ ha soluzione in $\mathbb{Z}_n$ con $\text{MCD}(a, n) = d > 1 \Leftrightarrow d \mid b$, altrimenti è incompatibile (non ha soluzioni).

   Dimostrazione: Dimostriamo che è condizione necessaria.

   Se $a \cdot x = b$ è compatibile (ammette soluzioni) in $\mathbb{Z}_n$, ossia $\exists\ s \in \mathbb{Z}_n$ t.c. $a \cdot s = b$, allora $a \cdot s - b = q \cdot n$, ossia è un multiplo di n. Quindi $b = a \cdot s - q \cdot n$, ossia $b \in S_{a,n}$. $S_{a,n}$ sono tutti i multipli del $\text{MCD}(a, n) = d \Rightarrow b = k \cdot d$.

   Dimostrare che la condizione è sufficiente segue il percorso inverso. ■

   Come troviamo le soluzioni?

Osservazione 10

$$\mathrm{MCD}(a,n) = d \Leftrightarrow \mathrm{MCD}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$$

Da questa osservazione segue che se prendiamo:

$$\frac{a}{d} \cdot x = \frac{b}{d} \text{ in } \mathbb{Z}_{\frac{n}{d}}$$

questa equazione ricade nel caso 1, e quindi ha una sola soluzione s.

Proposizione 2.4.17

s è soluzione di $\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ $\Leftrightarrow$ s è soluzione di $a \cdot x \equiv b \pmod{n}$.

Dimostrazione: Se s è soluzione di $\frac{a}{d} \cdot x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$, allora $\frac{a}{d} \cdot s - \frac{b}{d} = q \cdot \frac{n}{d} \Rightarrow a \cdot s - b = q \cdot n \Rightarrow$ s è soluzione di $a \cdot x \equiv b \pmod{n}$.

Viceversa basta seguire l'ordine inverso. ■

$[s]_{\frac{n}{d}}$ è l'unica soluzione di $\left[\frac{a}{d}\right]_{\frac{n}{d}} [x]_{\frac{n}{d}} = \left[\frac{b}{d}\right]_{\frac{n}{d}}$, perché il $\mathrm{MCD}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, e quindi siamo nel caso 1.

Le soluzioni di $a \cdot x = b \pmod{n}$ si ripartiscono in classi di equivalenza modulo n, e precisamente in:

$$[s]_{\frac{n}{d}} = [s]_n \cup \left[s + \frac{n}{d}\right]_n \cup \ldots \cup \left[s + \frac{n}{d}(d-1)\right]_n$$

Ciò significa che le soluzioni di $[a] \cdot [x] = [b]$ in $\mathbb{Z}/\equiv_n$ sono d, e sono le d-classi di equivalenza in cui si ripartisce l'unica soluzione $[s]_{\frac{n}{d}}$ di $[\frac{a}{d}]x = [\frac{b}{d}]$ in $\mathbb{Z}/\equiv_{\frac{n}{d}}$.

Dimostrazione: Dimostriamo che:

$$[s]_{\frac{n}{d}} = [s]_n \cup \left[s + \frac{n}{d}\right]_n \cup \ldots \cup \left[s + \frac{n}{d}(d-1)\right]_n$$

Sappiamo che:

$$t \in [s]_{\frac{n}{d}} \Leftrightarrow t - s = k \cdot \frac{n}{d}$$

Quindi: $t = s + k \cdot \frac{n}{d}$

Bisogna solo dimostrare che $k < d$. Dividiamo per d:

$$k = n \cdot d + r$$

Quindi $t = s + (n \cdot d + r)\frac{n}{d}$, e quindi $t = s + r\frac{n}{d}$, perché $n \cdot d \equiv 0 \pmod{n}$.

Quindi $t \in \left[s + r\frac{n}{d}\right]$ con $r < d$.

Viceversa si segue l'ordine inverso.

Dobbiamo mostrare che le classi sono disgiunte. $t \in \left[s + r\frac{n}{d}\right]_n$, dove $r < d$ è il resto della divisione di k per d. Non possono esserci due resti distinti, quindi $\left[s + r_1\frac{n}{d}\right] \cap \left[s + r_2\frac{n}{d}\right] = \emptyset$, perché $r_1 \neq r_2$ ed entrambi $r_1, r_2 < d$. ■

Esempio del primo caso :

$$3 \cdot x \equiv 11 \pmod{25}$$

$\text{MCD}(3, 25) = 1 \Rightarrow$ l'equazione ha una sola soluzione.

Scrivo l'identità di Bézout:

$$1 = 3 \cdot (-8) + 25 \cdot (1)$$

Moltiplico entrambi i lati per 11:

$$11 = 3 \cdot (-8) \cdot (11) + 25 \cdot (11)$$

Passo alle classi:

$$[11] = [3] \cdot [-8 \cdot 11] = [3] \cdot [17] \cdot [11] \Rightarrow [x] = [17] \cdot [11] = [11 \cdot 17] = [12]$$

In $\mathbb{Z}$ ha infinite soluzioni, tutti gli interi nella classe $[12]$.

L'unica soluzione in $\mathbb{Z}_{25}$ è $x = 12$.

Vedendola come classi, $[a] \cdot [x] = [b]$ in $\mathbb{Z}/\equiv_{25}$. L'unica soluzione è la classe $[12] = [x]$.

Esempio del secondo caso :

$$200 \cdot x \equiv 62 \pmod{22}$$

Dobbiamo anzitutto verificare la compatibilità dell'equazione.

$$\text{MCD}(200, 22) = 2$$

Ha soluzioni, poiché $2 \mid 62$.

Consideriamo l'equazione ottenuta dividendo tutto per 2.

$$\frac{200}{2} \cdot x \equiv \frac{62}{2} \pmod{22} \Rightarrow 100 \cdot x \equiv 31 \pmod{11}$$

$100 \cdot x \equiv 31 \pmod{11}$ ha un'unica soluzione, essendo che $\text{MCD}(100, 11) = 1$. Troviamo l'identità di Bézout:

$$1 = 100 \cdot (s) + 11 \cdot (t) \Rightarrow 1 = 100 \cdot (1) + 11 \cdot (-9)$$

La soluzione è la classe $[1]_{11}$. Va ripartita in 2 classi modulo 22.

$$[1]_{22} \text{ e } \left[1 + \frac{n}{d}\right]_{22} = \left[1 + \frac{22}{2}\right]_{22} = [1 + 11]_{22} = [12]_{22}$$

Esempio :

$$12x \equiv 44 \pmod{100} \tag{2.1}$$

Deteminare le soluzioni dell'equazione in $\mathbb{Z}$. L'insieme di queste soluzioni si esprime come unione di classi di equivalenza modulo n.

L'equazione 2.1 è compatibile $\Leftrightarrow \text{MCD}(12, 100) \mid 44$. È verificato che $\text{MCD}(12, 100) = 4$ e che $4 \mid 44$, quindi l'equazione 2.1 è compatibile.

Per calcolare le soluzoni, per il teorema precedente, $12 \cdot x \equiv 44 \pmod{100}$ è equivalente a:

$$\frac{12}{4} \cdot x \equiv \frac{44}{4} \pmod{\frac{100}{4}}$$

Essendo il MCD $\left(\frac{12}{4}, \frac{100}{4}\right) = 1$, $3 \cdot x \equiv 11 \pmod{25}$ ammette una sola soluzione modulo 25.

Quindi $x = 3^{-1} \cdot 11$ in $\mathbb{Z}_{25}$. Per trovare l'inverso di 3 dobbiamo usare l'identità di Bézout con 3 e 25:

$$1 = 3 \cdot s + 25 \cdot t \Rightarrow 1 = 3 \cdot (-8) + 25 \cdot (1) \Rightarrow 1 = 3 \cdot (-8) \pmod{25}.$$

Quindi $3^{-1} = -8 = 17 \pmod{25}$.

Quindi $x = [17 \cdot 11]_{25} = [187]_{25} = [12]_{25}$.

$[12]_{25}$ è l'unica soluzione di $[3]_{25} \cdot [x]_{25} = [11]_{25}$. Equivale a dire che tutte le (infinite) soluzioni di $3 \cdot x \equiv 11 \pmod{25}$ sono gli interi di questa classe.

Le soluzioni intere di $12 \cdot x \equiv 44 \pmod{100}$ sono gli interi di $[12]_{25}$.

L'equazione 2.1 possiamo vederla come $[12]_{100}x = [44]_{100}$. In $\mathbb{Z}/\equiv_{100}$ l'equazione ha 4 soluzioni date dalle classi di equivalenza in cui si ripartisce la soluzione $[12]_{25}$:

$$[12]_{100} + [12 + 25]_{100} + [12 + 50]_{100} + [12 + 75]_{100}$$

$$[12]_{25} = \bigsqcup_{r=0}^{3} [12 + 25 \cdot r]_{100}$$

2.4.9 Equazioni diofantee

Definizione 2.4.8

Un'equazione diofantea è un'equazione lineare in due incognite a coefficienti in $\mathbb{N}^+$. È quindi un'equazione del tipo:

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

Dove $a, b, c \in \mathbb{N}^+$. Di quest'equazione si cercano le soluzioni intere $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

c è combinazione lineare di a e b. Quindi c deve essere nell'insieme $S_{a,b} = \{m \in \mathbb{N}^+ : m = a \cdot x + b \cdot y \text{ con } x, y \in \mathbb{Z}\}$.

Sappiamo che $d = \text{MCD}(a, b) = \inf S_{a,b}$, e che quindi $S_{a,b}$ è interpretabile come l'insieme dei multipli di d.

$$S_{a,b} = \{k \cdot d : k \in \mathbb{N}^+\}$$

Quindi l'equazione diofantea $a \cdot x + b \cdot y = c$ è compatibile $\Leftrightarrow c \in S_{a,b} \Leftrightarrow \text{MCD}(a, b) \mid c$.

Esempio :

$$33 = 28 \cdot x + 24 \cdot y$$

$\text{MCD}(28, 24) = 4$ non divide $33 \Rightarrow$ è incompatibile

$$6 = 15 \cdot x + 21 \cdot y$$

$\text{MCD}(21, 15) = 3 \mid 6 \Rightarrow$ è compatibile.

Troviamo l'identità di Bézout per 15, 21.

$$3 = 15 \cdot (3) + 21 \cdot (-2)$$

Per trovare la soluzione moltiplichiamo per 2:

$$2 \cdot 3 = 6 = 15 \cdot (3 \cdot 2) + 21 \cdot (-2 \cdot 2)$$

Quindi una soluzione dell'equazione diofantea è $(6, -4)$.

Come sono fatte tutte le altre?

L'insieme S delle soluzioni dell'equazione diofantea è:

$$S = \{(6 + k \cdot 21, -4 - k \cdot 15) : k \in \mathbb{Z}\}$$

Proposizione 2.4.18

Data l'equazione diofantea $a \cdot x + b \cdot y = c$ compatibile, l'insieme delle soluzioni S è dato da:

$$S = \{(s + k \cdot b, t - k \cdot a) : k \in \mathbb{Z}\}$$

dove (s, t) è una soluzione, che si determina dall'identità di Bézout.

Dimostrazione :

$$c = h \cdot d = h(a \cdot s' + b \cdot t') \Rightarrow s = h \cdot s' \text{ e } t = h \cdot t'$$

$(s + k \cdot b, t - k \cdot a)$ è soluzione.

$$c = s \cdot a + t \cdot b = a \cdot (s + k \cdot b) + (t - k \cdot a) \cdot b = a \cdot s + k \cdot a \cdot b + t \cdot b - k \cdot a \cdot b = a \cdot s + t \cdot b = c$$

Abbiamo dimostrato che tutte le coppie in questa forma sono soluzioni.

Ora facciamo vedere che tutte le soluzioni hanno questa forma, quindi che ogni soluzione dell'equazione diofantea (s', t') è tale che $s' = s + k \cdot b$ e $t' = t - k \cdot a$.

Per ipotesi abbiamo che:

$$\begin{cases} c = a \cdot s + b \cdot t \\ c = a \cdot s' + b \cdot t' \end{cases}$$

Quindi $a \cdot s + b \cdot t - a \cdot s' - b \cdot t' = 0 \Rightarrow a \cdot s - a \cdot s' = b \cdot t' - b \cdot t \Rightarrow a \cdot (s - s') = (t' - t) \cdot b \Rightarrow (s - s') = k \cdot b$, e quindi $a \cdot k \cdot b = (t - t') \cdot b \Rightarrow (t - t') = k \cdot a$.

Non mi è molto chiara questa dimostrazione. ■

2.4.10 Strutture algebriche e reticoli

Le strutture algebriche offrono esempi di reticoli.

Consideriamo un gruppo $(G, \cdot)$ e l'insieme $\mathscr{S}(G)$ dei sottogruppi di G. $(\mathscr{S}(G), \subseteq)$ con la relazione di "essere sottogruppo di" è un insieme parzialmente ordinato, ed è anche un reticolo.

Dati due sottogruppi $S, H \in \mathscr{S}(G)$, $S \wedge H = S \cap H$. L'intersezione di due sottogruppi è sempre un sottogruppo. Vediamo che è non vuoto: $1_G \in S \cap H$. Inoltre è chiuso:

$$\left.\begin{array}{l} a, b \in S \Rightarrow a^{-1} \cdot b \in S \\ c, d \in H \Rightarrow c^{-1} \cdot d \in H \end{array}\right\} \Rightarrow a, b \in S \cap H \Rightarrow \begin{cases} a^{-1} \cdot b \in S \\ a^{-1} \cdot b \in H \end{cases} \Rightarrow a^{-1} \cdot b \in S \cap H$$

L'unione, invece, in genere non è un sottogruppo.

$(n\mathbb{Z}, +)$ è un sottogruppo di $(\mathbb{Z}, +)$. $3\mathbb{Z} \cup 2\mathbb{Z}$ non genera un sottogruppo, infatti non è chiuso rispetto alla somma: $3 + 2 = 5 \notin 3\mathbb{Z} \cup 2\mathbb{Z}$.

Il sup di due sottogruppi non è quindi l'unione.

$S \vee H = < S \cup H >$, ossia è il sottogruppo generato dall'unione. È il più piccolo dei sottogruppi che contengono sia S che H. Quindi possiamo scrivere equivalentemente:

$$< S \cup H > = \bigcap T \text{ tali che } S, H \subseteq T$$

Sottogruppi di $(\mathbb{Z}, +)$

Quali sono i sottogruppi di $\mathbb{Z}$?

Proposizione 2.4.19

I sottogruppi di $(\mathbb{Z}, +)$ *sono tutti del tipo* $m \cdot \mathbb{Z}$. *I sottogruppi propri si ottengono con* $m \neq 0, 1$.

Dimostrazione: Dimostriamo anzitutto che $m \cdot \mathbb{Z}$ è un sottogruppo di $(\mathbb{Z}, +)$.

$\forall$ S sottogruppo di $(\mathbb{Z}, +) \Rightarrow S = m \cdot \mathbb{Z}$.

Dato un sottogruppo S, devo trovare un m. m è il più piccolo intero positivo, ossia l'$\inf(S \cap \mathbb{N}^+)$. $S \cap \mathbb{N}^+ \neq \emptyset$, visto che $S \neq \{0\}$. Quindi, per il principio del buon ordinamento, m è il primo elemento positivo.

Sia $m = \inf(S \cap \mathbb{N}^+)$. Dobbiamo dimostrare che $m\mathbb{Z} \subseteq S$ e $S \subseteq m\mathbb{Z}$.

$m\mathbb{Z}$ è il gruppo delle potenze rispetto all'addizione. Quindi $m\mathbb{Z} \subseteq S$ è banale, visto che deve contenere tutte le potenze di m.

$S \subseteq m\mathbb{Z}$. Prendiamo $h \in S$, dimostriamo che $h \in m\mathbb{Z}$, ossia $h = km$.

Applichiamo il teorema di divisione: $h = km + r$, con $0 \leq r < m$.

r è necessariamente 0. Infatti $r = h - km$. Sia h che $km \in S$, visto che $m \in S$ tutti i suoi multipli sono in S. Quindi anche $r \in S$, e necessariamente $r = 0$, essendo m il più piccolo intero positivo di S. ■

Prendiamo tutti i sottogruppi di $(\mathbb{Z}, +)$, $\mathscr{S}((\mathbb{Z}, +))$

$$(m\mathbb{Z}) \wedge (n\mathbb{Z}) = \text{mcm}(m, n)\mathbb{Z}$$

$$(m\mathbb{Z}) \vee (n\mathbb{Z}) = \text{MCD}(m, n)\mathbb{Z}$$

I sottogruppi di $(\mathbb{Z}, +)$ sono tutti del tipo $m \cdot \mathbb{Z}$. Allo stesso modo, i sottogruppi di $(\mathbb{Z}_n, +)$ sono tutti del tipo $k \cdot \mathbb{Z}_n$ dove k è un divisore di n, e $|k \cdot \mathbb{Z}_n| = h$ con $k \cdot h = n$.

Quindi, per ogni divisore h di n esiste un sottogruppo di $\mathbb{Z}_n$ di ordine h che è $k \cdot \mathbb{Z}_n$ dove $k \cdot h = n$.

Dimostrazione: $k \cdot \mathbb{Z}_n$ è un sottogruppo di $\mathbb{Z}_n$ per lo stesso motivo per cui $k \cdot \mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$. $k \cdot \mathbb{Z}_n = \{0, k \ldots, (h-1) \cdot k\}$. L'ultimo elemento è $(h-1) \cdot k$ perché $h \cdot k = n$, ossia $h \cdot k \equiv 0 \pmod{n}$. h è l'ordine del gruppo: il minimo intero positivo per cui k elevato all'ordine fa l'elemento neutro.

$$h = o(k \cdot \mathbb{Z}_n) = o(k) = \inf\{t : t \cdot k = 0 \text{ con } t \neq 0\}$$

Viceversa dobbiamo dimostrare che un sottogruppo qualunque S di $\mathbb{Z}_n$ è del tipo $k \cdot \mathbb{Z}_n$. k è il primo elemento positivo di S.

$$k = \inf(S \setminus \{0\})$$

Quindi, essendo $k \in S$, $k \cdot \mathbb{Z}_n \subseteq S$. Inoltre, dato $a \in S$, dividiamo a per k, quindi $a = k \cdot q + r$, dove $0 \leq r < k$. Quindi $r = a - q \cdot k \Rightarrow a \in S$ e $q \cdot k \in S$, quindi $r \in S \Rightarrow r = 0$, poiché k è l'$\inf(S \setminus \{0\})$.
Quindi $S = k \cdot \mathbb{Z}_n$. ■

$|S| = h = |k \cdot \mathbb{Z}_n|$. h è l'elemento tale che $h \cdot k = n$.

Per ogni divisore h di n esiste un sottogruppo di ordine h che è $k \cdot \mathbb{Z}_n$, con $h \cdot k = n$.

Per $\mathbb{Z}_n$ è vero che per ogni divisore di n esiste un sottogruppo che ha quell'ordine. Prima sapevamo solo che l'ordine di un sottogruppo deve dividere n, con $\mathbb{Z}_n$ vale anche il contrario.

Per ogni divisore h di n esiste un sottogruppo di $(\mathbb{Z}_n, +)$ di ordine h che è $k\mathbb{Z}_n$ dove $kh = n$.

Esempio:

Prendiamo $(\mathbb{Z}_6, +)$. I divisori di 6 sono 2 e 3.

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Il sottogruppo di ordine 2 è $3 \cdot \mathbb{Z}_6$

$$3 \cdot \mathbb{Z}_6 = \{0, 3\} \cong \mathbb{Z}_2$$

$3 \cdot \mathbb{Z}_6$ è isomorfo a $\mathbb{Z}_2$.

$+$	0	3
0	0	3
3	3	0

$+$	0	1
0	0	1
1	1	0

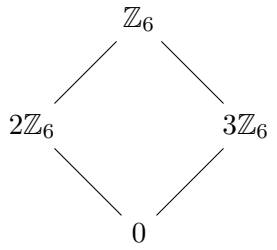

Figura 2.2: Reticolo dei sottogruppi di $\mathbb{Z}_6$

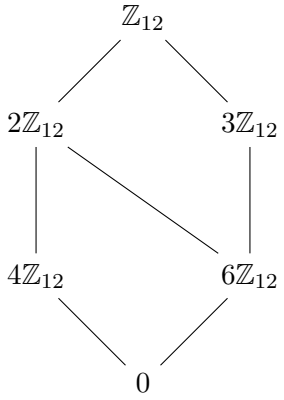

Figura 2.3: Reticolo dei sottogruppi di $\mathbb{Z}_{12}$

$2 \cdot \mathbb{Z}_6 = \{0, 2, 4\} \cong \mathbb{Z}_3, 2 \cdot \mathbb{Z}_6$ è isomorfo a $\mathbb{Z}_3$

Come è fatto il reticolo dei sottogruppi in $\mathbb{Z}_6$? Lo vediamo in figura 2.2. In generale, il reticolo dei sottogruppi di $\mathbb{Z}_n$ si indica con $(\mathscr{S}(\mathbb{Z}_n), \subseteq)$.

Osservazione 11

Se prendo $k \cdot \mathbb{Z}_n$, ha ordine h ed è isomorfo a $\mathbb{Z}_h$, dove $h \cdot k = n$.
L'isomorfismo è proprio: $\phi : \mathbb{Z}_h \to k \cdot \mathbb{Z}_n$ definito da, dato $t \in \mathbb{Z}_h$, $\phi(t) = t \cdot k$.

Facciamo un altro reticolo dei sottogruppi con $\mathbb{Z}_{12}$. Il risultato è in figura 2.3.

I divisori di 12 sono 2, 3, 4 e 6. Abbiamo 4 sottogruppi non banali.

Abbiamo un sottogruppo di ordine $2, 6 \cdot \mathbb{Z}_{12} = \{0, 6\} \cong \mathbb{Z}_2$. L'ordine di 6 è 2, perché $6 + 6 \equiv 0 \pmod{12}$.

Abbiamo un sottogruppo di ordine 3, $4 \cdot \mathbb{Z}_{12} = \{0, 4, 8\} \cong \mathbb{Z}_3$.

Abbiamo un sottogruppo di ordine 4, $3 \cdot \mathbb{Z}_{12} = \{0, 3, 6, 9\} \cong \mathbb{Z}_4$.

Abbiamo un sottogruppo di ordine 6, $2 \cdot \mathbb{Z}_{12} = \{0, 2, 4, 6, 8, 10\} \cong \mathbb{Z}_6$.

Esercizio 16

Creare il reticolo dei sottogruppi di $\mathbb{Z}_{16}$.

2.4.11 Gruppi ciclici

Definizione 2.4.9

Un gruppo $(G, \cdot)$ si dice ciclico, se $G =< a >$, ossia $G = \{a^t : t \in \mathbb{Z}\}$, ossia G è generato da un elemento $a \in G$ detto generatore.
L'ordine di G è l'ordine di a, ossia il minimo intero tale per cui a elevato all'ordine fa 1_G, ossia $\inf\{t : t > 0 \text{ e } a^t = 1_G\}$

$(\mathbb{Z}, +)$ è ciclico, generato da $<1>$. Anche $(\mathbb{Z}_n, +)$ è generato da $\{1\}$.

Teorema 2.4.20

Sia $(G, \cdot)$ un gruppo ciclico generato da $a \in G$, allora ci sono due casi:
1. *$|G| = \infty$*
2. *$|G| = n$, ossia la sua cardinalità è finita*

Nel caso 1 $(G, \cdot)$ è isomorfo a $(\mathbb{Z}, +)$. Nel caso 2, $(G, \cdot)$ è isomorfo a $(\mathbb{Z}_n, +)$.

Dimostrazione dei due casi: Caso 1. Troviamo $f : (\mathbb{Z}, +) \to (G, \cdot)$. $G =< a >$. L'isomorfismo è l'unico che esiste tale per cui $f(1) = a$. Ossia $f(t) = a^t$.

$$f(-t) = a^{-t} = (a^t)^{-1}$$

È un morfismo per la proprietà delle potenze. Inoltre f è suriettivo.
Bisogna dimostrare che è un isomorfismo, ossia che f è iniettivo.

$$f(t) = f(s) \Rightarrow f(t) = a^t = a^s = f(s) \Rightarrow a^t \cdot a^{-s} = 1_G \Rightarrow a^{t-s} = 1_G$$

Siamo nel caso in cui $|G| = \infty$, quindi $a^t \neq 0 \ \forall \ t \neq 0$. Quindi

$$t - s = 0 \Rightarrow t = s$$

Caso 2. $|G| = n, G = \{a^t : t \in \mathbb{Z}\} =< a >$
Dobbiamo trovare il morfismo $f : (\mathbb{Z}_n, +) \to (G, \cdot)$, l'unico per cui $f(1) = a$ e $f(t) = a^t$ con $t \in \mathbb{Z}_n$.
È suriettivo perché $\mathbb{Z}_n$ contiene tutte le potenze. Bisogna dimostrare che è iniettivo.
$f(t) = f(s)$, con $t, s \in \mathbb{Z}_n$. Quindi $a^t = a^s$, quindi $a^{t-s} = 1_G$. Sappiamo che:

$$a^n = 1_G$$

Se considero $t - s = q \cdot n + r, a^{t-s} = a^{qn} \cdot a^r = 1_G \Rightarrow 1_G \cdot a^r \Rightarrow a^r = a^0$
Quindi deve essere che $(t - s) \equiv 0 \pmod{n}$.
$f(t) = f(s) \Rightarrow a^t = a^s \Rightarrow a^{t-s} = 1_G \Rightarrow a^{t-s} = a^{qn+r} = 1_G$. Ho che $0 \leq r < n$. Quindi$1_G = a^{qn} \cdot a^r$, ma $a^{qn} = 1_G$, quindi $1_G = 1_G \cdot a^r \Rightarrow a^r = a^0$, essendo $r < n$.
Quindi essendo $r = 0, (t - s) = qn$, quindi $t - s \equiv 0 \pmod{n}$, ossia che $t - s = 0$ in $\mathbb{Z}_n$. ■

Esempio:

Scrivere le tavole moltiplicative dei tre gruppi $U(\mathbb{Z}_5)$, $U(\mathbb{Z}_8)$ e $U(\mathbb{Z}_{10})$. Calcolare la cardinalità dei suddetti gruppi, e di $U(\mathbb{Z}_{12})$.

Determinare quali sono isomorfi, esplicitando l'isomorfismo.

$$U(\mathbb{Z}_5) = \{1, 2, 3, 4\}$$

$$U(\mathbb{Z}_5) \qquad\qquad U(\mathbb{Z}_{10})$$

$$\begin{aligned}
&\overset{f}{\longrightarrow}\\
1 = 2^0 &\longrightarrow 1 = 3^0\\
2 = 2^1 &\longrightarrow 3 = 3^1\\
3 = 2^3 &\longrightarrow 7 = 3^3\\
4 = 2^2 &\longrightarrow 9 = 3^2
\end{aligned}$$

Figura 2.4: L'isomorfismo tra $U(\mathbb{Z}_5)$ e $U(\mathbb{Z}_{10})$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$$o(2) = 4 \Leftrightarrow 2^4 = 16 \equiv 1 \pmod 5$$
$$o(3) = 2 \Leftrightarrow 3^2 = 6 \equiv 1 \pmod 5$$
$$o(4) = 2 \Leftrightarrow 4^2 = 16 \equiv 1 \pmod 5$$

$$U(\mathbb{Z}_5) = <2> \cong \mathbb{Z}_4$$

$$U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$$U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$$

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$$U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$$

$$o(3) = 4 \Leftrightarrow 3^4 = 81 \equiv 1 \pmod{10}$$

$$U(\mathbb{Z}_{10}) = <3> \cong \mathbb{Z}_4$$

C'è un isomorfismo fra $U(\mathbb{Z}_5)$ e $U(\mathbb{Z}_{10})$. Il generatore deve andare nel generatore, il quadrato del generatore nel quadrato del generatore, etc.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$$o(5) = 2 \Leftrightarrow 5^2 = 25 \equiv 1 \pmod{12}$$
$$o(7) = 2 \Leftrightarrow 7^2 = 49 \equiv 1 \pmod{12}$$
$$o(11) = 2 \Leftrightarrow 11^2 = 121 \equiv 1 \pmod{12}$$

Quindi $U(\mathbb{Z}_{12})$ non è un gruppo ciclico. Vediamo se è isomorfo a $\mathbb{Z}_8$.

$\mathbb{Z}_8$ deve avere tre elementi di ordine 2.

$$o(3) = 2 \Leftrightarrow 3^2 = 9 \equiv 1 \pmod{8}$$
$$o(5) = 2 \Leftrightarrow 5^2 = 25 \equiv 1 \pmod{8}$$
$$o(7) = 2 \Leftrightarrow 7^2 = 49 \equiv 1 \pmod{8}$$

Quindi $\mathbb{Z}_8$ e $\mathbb{Z}_{12}$ sono isomorfi.

Esercizio 17

Risolvere la congruenza:

$$511 \cdot x \equiv 111 \pmod{842}$$

Scrivere le soluzioni modulo 842.

Esercizio 18

Calcolare $2^{2^{341}} \pmod{37}$.

2.4.12 Morfismo di anelli

Un morfismo di anelli è un'applicazione $f : A \to A'$ tale che conserva la struttura di anello. Deve essere un morfismo di gruppi abeliani per il $+$, e deve mantenere l'operazione $\cdot$. Quindi $f : (A, +) \to (A', +)$ è un morfismo di gruppi, e f mantiene l'operazione $\cdot$, ossia $f(a \cdot b) = f(a) \cdot f(b)$.

2.4.13 Morfismo di campi

Un morfismo di campi è un morfismo di gruppi rispetto al $+$, e un morfismo di gruppi rispetto al $\cdot$.

$f : G \to G'$ è un morfismo di gruppi $f : (G, \cdot) \to (G', *) \Leftrightarrow f(a \cdot b) = f(a) * f(b)$, ossia se conserva le operazioni.

Quindi:

$f : A \to A'$ è un morfismo di campi se $f(a + b) = f(a) + f(b)$ (quindi è un morfismo rispetto al più) e $f(a \cdot b) = f(a) \cdot f(b)$.

Se A e A' sono anelli unitari, un morfismo di anelli unitari $f : A \to A'$ deve mandare $f(1_A) = 1_{A'}$.

2.4.14 Teorema di omomorfismo per gli anelli

Abbiamo due anelli, $(A, +, \cdot)$ e $(A', +, \cdot)$.

$f : (A, +, \cdot) \to (A', +, \cdot)$ è un morfismo di anelli.

1. L'immagine di f, Im_f è un sottoanello di A'.
2. $A/\varepsilon_f = A/\ker f$ (inteso come morfismo di gruppi) è un anello isomorfo all'immagine Im_f. L'isomorfismo $F : A/\ker f \to Im_f$ è quello che manda una classe nell'immagine di tutti gli elementi della classe ($[a]$ è la classe di tutti gli elementi che hanno immagine $f(a)$ uguale).
$$F[a] = f(a) \ \forall \ [a] \in A/\ker f$$
3. $\ker f$ è un sottogruppo normale di $(A, +)$. Rispetto alla struttura di anello, $\ker f$ è un ideale di $(A, +, \cdot)$.

Definizione 2.4.10 (*Ideale di un anello*)

$I \subseteq A$ è un ideale se:
1. *$(I, +)$ è un sottogruppo di $(A, +)$*
2. *$\forall\ a \in A$ e $\forall\ u \in I \Rightarrow a \cdot u \in I$ e $u \cdot a \in I$, ossia comunque prendo un elemento nell'anello e un elemento nell'ideale, il loro prodotto è nell'ideale.*

Proposizione 2.4.21

Il nucleo di un morfismo di anelli è un ideale del dominio.

Dimostrazione: Siano $a \in A$, $u \in \ker f$, dobbiamo far vedere che $a \cdot u \in \ker f$. Sia $0_{A'}$ l'elemento neutro rispetto a $+$ di A':
$$\ker f = \{u \in A : f(u) = 0_{A'}\}$$
$$f(a \cdot u) = f(a) \cdot f(u) = f(a) \cdot 0_{A'} = 0_{A'} \Rightarrow f(a \cdot u) \in \ker f$$
Analogamente commutando si ha che $f(u \cdot a) = 0_{A'}$. ■

Alcuni esempi di anelli:

- $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Z}_n, +, \cdot)$. Se n è primo, $(\mathbb{Z}_n, +, \cdot)$ è un campo.
- Sia $\mathbb{K}$ un campo generico, con $(\mathbb{K}[x], +, \cdot)$ è l'anello dei polinomi a coefficienti in $\mathbb{K}$.
- anello delle matrici quadrate di ordine n, indicato così:
$$(\mathfrak{M}_n(\mathbb{K}), +, \cdot)$$

2.4.15 Anello dei polinomi

Un polinomio $p(x)$ è una espressione formale del tipo $a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n$, con $a_n \neq 0$. Diciamo che il grado di $p(x)$ indicato con $\delta(p(x))$ è n. x è l'indeterminata. x è un puro simbolo, non varia da nessuna parte.

Il polinomio nullo $\underline{0}$ tale che $\forall\ n \in \mathbb{N} a_n = 0$, ha grado -1.

La somma $p(x) + q(x)$ è definita coefficiente per coefficiente. Consideriamo i seguenti due polinomi:

$$\begin{aligned} p(x) &= a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n \\ q(x) &= b_0 + b_1 \cdot x + \cdots + b_m \cdot x^m \\ p(x) + q(x) &= a_0 + b_0 + (a_1 + b_1) \cdot x + \cdots + (a_n + b_n) \cdot x^n \end{aligned}$$

Il grado $\delta(p(x) + q(x)) = \sup(\delta(p(x)), \delta(q(x)))$.

$(\mathbb{K}[x], +)$ è un gruppo abeliano. L'elemento neutro è $\underline{0}$.

Per fare un anello, dobbiamo definire una moltiplicazione $\cdot : \mathbb{K}[x] \times \mathbb{K}[x] \to \mathbb{K}[x]$.

$$p(x) \cdot q(x) \stackrel{\text{def}}{=} c(x) = c_0 + c_1 \cdot x + \ldots$$

dove:

$$c_n = \sum_{i=0}^{n} a_i \cdot b_{n-i}$$

è il termine n-esimo.

Il grado del prodotto $\delta(p(x) \cdot q(x)) = \delta(p(x)) + \delta(q(x))$.

$(\mathbb{K}[x], +, \cdot)$ è un anello commutativo unitario privo di divisori dello 0. L'unità è la costante 1. Non è un campo: non tutti i polinomi sono invertibili.

$p(x)$ è invertibile $\Leftrightarrow$ $\exists\ p(x)$ tale che $p(x) \cdot q(x) = 1 \Leftrightarrow \delta(p(x)) = 0 \Leftrightarrow p(x)$ è una costante non nulla. Sono tutti e soli i polinomi invertibili.

Dimostrazione: $p(x) \cdot q(x) = 1$, e supponiamo che il grado $\delta(p(x)) = n > 0$. Il grado $\delta(p(x) \cdot q(x))$ dovrebbe essere 0, ma sapendo che è $n+m$, per essere vero dovrebbe essere che $m = -n$, che è l'assurdo. ■

È privo di divisori dello zero.

Dimostrazione: $p(x) \cdot q(x) = 0$, supponendo che $p(x)$ ha grado $n \geq 0$ e $q(x)$ ha grado $m \geq 0$, dovrei avere che la somma dei gradi $m + n = -1$, il grado del polinomio nullo. Assurdo. ■

2.4.16 Teorema di divisione in $\mathbb{K}[x]$

Nell'anello dei polinomi c'è il teorema di divisione, come in $\mathbb{Z}$. Gli anelli con il teorema di divisione si chiamano anelli Euclidei.

Siano $f(x)$ e $g(x)$ polinomi con $f(x) \neq 0$. Esistono allora due polinomi $q(x)$ e $r(x)$ tali che:

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

La coppia $(q(x), r(x))$ che soddisfa le due proprietà è unica.

Un elemento $r \in \mathbb{K}$ si dice "radice del polinomio $p(x)$" se sostituendo r a x, ossia facendo $p(r) = a_0 + a_1 \cdot r + \ldots a_n \cdot r^n$, ho che $p(r) = 0$.

Corollario 2.4.22 (*Primo corollario del teorema di divisione*)

r è radice di $p(x) \Leftrightarrow p(x) = q(x) \cdot (x - r)$.
Occhio: $(x - r)$ è un polinomio.

Dimostrazione: Condizione sufficiente: se prendo $p(x) = q(x) \cdot (x - r) \Rightarrow r$ è radice di $p(x)$.

Condizione necessaria: r è radice di $p(x) \Leftrightarrow p(r) = 0$. Per il teorema di divisione abbiamo che $p(x) = q(x) \cdot (x - r) + r(x)$, con $\delta(r(x)) \leq 0$, essendo minore del grado di $(x - r)$ (che è pari a 1).

Abbiamo che $p(r) = q(r)(0) + r(r) = 0$, quindi il grado di r non può essere 0, ossia non può essere una costante (le costanti non si annullano per nessun x), quindi $r(r) = 0$. ■

Corollario 2.4.23 (*Secondo corollario del teorema di divisione*)

Ogni polinomio a coefficienti in $\mathbb{K}$ ($p(x) \in \mathbb{K}[x]$) di grado $n \geq 0$ ha al più n radici.
L'unico polinomio con infinite radici è il polinomio nullo.

Dimostrazione: Per il corollario 2.4.22, se $r_1 \dots r_{n+1}$ fossero le radici, si potrebbe scrivere $p(x)$ come:

$$p(x) = \prod (x - r_i) \Rightarrow \delta(p(x)) = n + 1$$

■

Teorema 2.4.24

$p(x), q(x) \in \mathbb{R}[x]$ (o un qualsiasi altro campo infinito).

$$\forall\ n \in \mathbb{N},\ p(n) = q(n) \Rightarrow p(x) = q(x)$$

Dimostrazione: $\forall\ n \in \mathbb{N},\ p(n) - q(n) = 0 \Rightarrow\ \forall\ n$, n è radice, quindi $p(x) = q(x)$. ■

2.5 Matrici

2.5.1 Gruppo delle matrici m per n

Definizione 2.5.1 (*Matrice con m righe e n colonne*)

Una matrice M di m righe e n colonne, a valori ad esempio in $\mathbb{R}$, è una applicazione:

$$M : [m] \times [n] \to \mathbb{R}$$

Ossia associa ad una coppia (i, j) il valore $a_{i,j}$:

$$M(i, j) = a_{i,j}$$

Le matrici si possono rappresentare con una tabella.

L'insieme delle matrici con m righe e n colonne si indica con il simbolo $\mathfrak{M}_{m,n}(\mathbb{R})$.

Date due matrici M e N, la loro somma è:

$$(M + N)(i, j) = M(i, j) + N(i, j)$$

Possiamo indicare una matrice anche come $M = a_{i,j}$. Quindi:

$$M + N = (a_{i,j}) + (b_{i,j}) \stackrel{\text{def}}{=} (a_{i,j} + b_{i,j})$$

$(\mathfrak{M}_{m,n}(\mathbb{R}), +)$ è un gruppo abeliano. L'elemento neutro è la matrice contenente tutti 0, ossia l'applicazione costante con solo 0.

2.5.2 Anello delle matrici quadrate

Per fare il campo, ossia per poter definire un'operazione di moltiplicazione su tutti gli elementi del campo, dobbiamo avere matrici con uguale numero di righe e colonne. Si vede da come è definito il prodotto fra matrici.

Per capire cosa è il prodotto fra matrici, partiamo dai sistemi di equazioni lineari. Consideriamo un'equazione lineare in n incognite:

$$a_1 \cdot x_1 + \cdots + a_n \cdot x_n = b$$

Possiamo costruire un sistema di m equazioni lineari in n incognite:

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = b_m \end{cases}$$

Vogliamo rappresentarlo come matrice.

Scriviamo la matrice dei coefficienti:

$$A = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix}$$

Poi scriviamo la matrice delle incognite (è una matrice colonna):

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Poi scriviamo la matrice dei termini noti (anche questa è una matrice colonna):

$$B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

Abbiamo poi la matrice completa associata al sistema. Scrivo la matrice dei coefficienti e alla fine aggiungo, come ultima colonna, la matrice dei termini noti. È la matrice dei coefficienti con aggiunta la colonna dei termini noti.

$$A|B = \left(\begin{array}{ccc|c} a_{1,1} & \dots & a_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & \dots & a_{m,n} & b_n \end{array}\right)$$

Consideriamo il seguente sistema lineare con 4 incognite e 3 equazioni.

$$\begin{cases} 2x_1 + 3x_2 - x_4 = 1 \\ 3x_1 - x_3 + 2x_4 = -2 \\ x_1 + x_2 = 0 \end{cases}$$

Le sue matrici sono:

$$A = \begin{pmatrix} 2 & 3 & 0 & -1 \\ 3 & 0 & -1 & 2 \\ 1 & 1 & 0 & 0 \end{pmatrix} \qquad X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \qquad B = \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix}$$

Possiamo scrivere il sistema come:

$$A \cdot X = B$$

Come deve essere fatto il prodotto in modo che $A \cdot X$ sia proprio B?

Facciamo il caso più semplice in cui abbiamo una sola riga.

$$a_{1,1} \cdot x_1 + \ldots a_{1,n} \cdot x_n = b_1$$

Anche la matrice associata al sistema ha una sola riga:

$$A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \end{pmatrix}$$

La matrice delle incognite è una matrice colonna, e la matrice dei termini noti è una matrice 1 per 1.

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad B = \begin{pmatrix} b_1 \end{pmatrix}$$

Dobbiamo avere che $A \times X = B$. Quindi se moltiplichiamo una riga per una colonna otteniamo b_1.

$$\begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \end{pmatrix} \times \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \end{pmatrix} = a_{1,1} \cdot x_1 + \ldots + a_{1,n} \cdot x_n$$

In generale deve valere la stessa cosa. Prendiamo una matrice con 1 riga e m colonne, la possiamo moltiplicare per un'altra matrice con m righe e 1 colonna. Il prodotto mi dà una matrice con un solo elemento b.

$$M_{1,n} \times N_{n,1} = b$$

Quindi:

$$M_{1,n} = \begin{pmatrix} a_1 & \ldots & a_n \end{pmatrix} \qquad N_{n,1} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

$$M_{1,n} \times N_{n,1} = \begin{pmatrix} b \end{pmatrix} = a_1 \cdot c_1 + \ldots + a_n \cdot c_n$$

Posso moltiplicare una matrice con un certo numero di colonne per una matrice con lo stesso numero di righe. L'ordine è importante: n righe la prima e n colonne la seconda!

$$\begin{pmatrix} 1 & 2 & 5 & 6 \end{pmatrix} \times \begin{pmatrix} -1 \\ 0 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 15 \end{pmatrix}$$

In generale una matrice con m righe e n colonne $M_{m,n}$ si può moltiplicare per una matrice $N_{n,t}$ con n righe e t colonne. Il risultato è una matrice $C_{m,t}$ con m righe e t colonne.

$$C_{m,t} = \begin{pmatrix} M_1 \times N^1 & \dots & M_1 \times N^t \\ \vdots & \ddots & \vdots \\ M_m \times N^1 & \dots & M_m \times N^t \end{pmatrix}$$

Prendiamo la prima riga di M e la moltiplichiamo per la prima colonna di N.

M_1 o $M_{1,n}$ indica la prima riga di M, N^1 o $N_{n,1}$ indica la prima colonna di N.

$$C_{i,j} = M_i \times N^j = M_{i,n} \times N_{n,j}$$

i e j sono i numeri di riga o di colonna, e sono quindi fissati, mentre n rappresenta la larghezza o l'altezza della matrice.

Esempio :

$$\begin{pmatrix} 3 & 2 & 1 & 0 \\ -1 & -1 & 1 & 2 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Ha 3 righe e 4 colonne. Possiamo moltiplicarla per una matrice con 4 righe. Ad esempio, per una matrice con 4 righe e 2 colonne.

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \\ -1 & 0 \\ 1 & 1 \end{pmatrix}$$

Avremo una matrice con 3 righe e 2 colonne:

$$\begin{pmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \\ c_{3,1} & c_{3,2} \end{pmatrix}$$

Famo i calcoli:

$$c_{1,1} = M_{1,n} \times N_{n,1} = M_1 \times N^1 = \begin{pmatrix} 3 & 2 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix} = 3 + 0 - 1 + 0 = 2$$

$$c_{1,2} = M_{1,n} \times N_{n,2} = M_1 \times N^2 = \begin{pmatrix} 3 & 2 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 6 + 2 + 0 + 0 = 8$$

$$c_{2,1} = M_{2,n} \times N_{n,1} = M_2 \times N^1 = \begin{pmatrix} -1 & -1 & 1 & 2 \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix} = -1 + 0 - 1 + 2 = 0$$

$$c_{2,2} = M_{2,n} \times N_{n,2} = M_2 \times N^2 = \begin{pmatrix} -1 & -1 & 1 & 2 \end{pmatrix} \times \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix} = -2 - 1 + 0 + 2 = -1$$

$$c_{3,1} = M_{3,n} \times N_{n,1} = M_3 \times N^1 = \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix} = 0 + 0 + 0 + 1 = 1$$

$$c_{3,2} = M_{3,n} \times N_{n,2} = M_3 \times N^2 = \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 0 + 1 + 0 + 1 = 2$$

Il risultato quindi è:

$$\begin{pmatrix} 2 & 8 \\ 0 & -1 \\ 1 & 2 \end{pmatrix}$$

Ora, il prodotto si può definire su un insieme di matrici solo se le matrici sono quadrate. $\mathfrak{M}_n(\mathbb{R})$ è l'insieme delle matrici quadrate con n righe e con coefficienti in $\mathbb{R}$, e $(\mathfrak{M}_n(\mathbb{R}), +, \cdot)$ è un anello non commutativo (il prodotto non commuta) unitario.

L'unità rispetto al prodotto è la matrice con tutti 1 sulla diagonale, e 0 altrimenti. Si indica con I o con δ. Il termine $\delta_{i,j}$ è:

$$\delta_{i,j} = \begin{cases} 0 \text{ se } i \neq j \\ 1 \text{ se } i = j \end{cases}$$

L'anello ha divisori dello zero. Prendiamo ad esempio le matrici:

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

il loro prodotto è 0.

Esempio :

Prendiamo l'anello delle matrici quadrate di ordine 2, $(\mathfrak{M}_2(\mathbb{R}), +, \times)$.

$$S = \{ \left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) : x, y \in \mathbb{R} \}$$

S è un sottoanello di $(\mathfrak{M}_2(\mathbb{R}), +, \times)$?

Vediamo se è un sottogruppo. Prese due matrici in S, la differenza deve rimanere in S.

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} z & t \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x-z & y-t \\ 0 & 0 \end{pmatrix} \in S$$

Quindi $(S, +)$ è un sottogruppo.

Deve conservare il prodotto e l'unità.

$$\begin{pmatrix} x \cdot z & y \cdot t \\ 0 & 0 \end{pmatrix}$$

Conserva il prodotto, ma S non ha l'unità! L'unità è:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin S$$

S non contiene l'unità dell'anello, ma ha un'unità? No. Non è un anello unitario.

Consideriamo l'applicazione $f : S \to \mathbb{R}$ definita come segue:

$$f\left(\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)\right) = x$$

f è un morfismo? Deve conservare le operazioni, e mandare l'unità di S nell'unità di $\mathbb{R}$.

$$f\left(\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} z & t \\ 0 & 0 \end{smallmatrix}\right)\right) = f\left(\left(\begin{smallmatrix} x+z & y+t \\ 0 & 0 \end{smallmatrix}\right)\right) = x + z = f\left(\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)\right) + f\left(\left(\begin{smallmatrix} z & t \\ 0 & 0 \end{smallmatrix}\right)\right)$$

È un morfismo rispetto alla somma, quindi è un morfismo di gruppi abeliani.

$$f\left(\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} z & t \\ 0 & 0 \end{smallmatrix}\right)\right) = f\left(\left(\begin{smallmatrix} x\cdot z & y\cdot t \\ 0 & 0 \end{smallmatrix}\right)\right) = x \cdot z = f\left(\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)\right) \cdot f\left(\left(\begin{smallmatrix} z & t \\ 0 & 0 \end{smallmatrix}\right)\right)$$

Troviamo nucleo e immagine di questo morfismo.

$$\ker f = \left\{\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) \in S : f\left(\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)\right) = 0\right\} = \left\{\left(\begin{smallmatrix} 0 & y \\ 0 & 0 \end{smallmatrix}\right) \in S : y \in \mathbb{R}\right\}$$

È un ideale: un qualunque elemento dell'anello moltiplicato per un elemento del ker f è ancora nel nucleo.

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & z \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & x \cdot z \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & z \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & y \cdot z \\ 0 & 0 \end{pmatrix}$$

Il prodotto non è commutativo!

L'immagine è tutto $\mathbb{R}$.

L'insieme quoziente è isomorfo a $\mathbb{R}$. Come è fatto il quoziente?

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} + \ker f$$

$$\left[\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}\right] = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & z \\ 0 & 0 \end{pmatrix}$$

Un rappresentante più intuitivo è:

$$\left[\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}\right]$$

Parte II

Algebra lineare

Capitolo 3

Spazi vettoriali

La loro teoria serve ad inquadrare la risoluzione dei sistemi di equazioni lineari.
Spazio vettoriale delle matrici, spazio vettoriale delle n-uple di numeri reali.

3.1 Spazi vettoriali su un campo $\mathbb{K}$

Uno spazio vettoriale è una struttura algebrica $(V, +, \cdot)$ su un campo $\mathbb{K}$ le cui operazioni sono $+ : V \times V \to V$ e l'operazione "esterna" $\cdot : \mathbb{K} \times V \to V$. Il $\cdot$ è detto "moltiplicazione esterna". Gli elementi di V si dicono *vettori*.

Uno spazio vettoriale gode delle seguenti proprietà:

1V $(V, +)$ è un gruppo abeliano

2V $\forall\ k \in \mathbb{K},\ \forall\ v, w \in V,\ k \cdot (v + w) = k \cdot v + k \cdot w$. Questa proprietà è detta distributiva rispetto all'addizione in V (ossia, rispetto all'addizione vettoriale).

3V $\mathbb{K}$ è un campo, quindi $\forall\ k, h \in \mathbb{K}$ e $\forall\ v \in V$, $(k + h) \cdot v = k \cdot v + h \cdot v$. Questa proprietà è detta distributiva rispetto all'addizione in $\mathbb{K}$

4V $\forall\ k, h \in \mathbb{K},\ \forall\ v \in V$, $(h \cdot k) \cdot v = h \cdot (k \cdot v) = k \cdot (h \cdot v)$. È una specie di proprietà associativa.

5V $\forall\ v \in V$, $1 \cdot v = v$

Un elemento $k \in \mathbb{K}$ viene detto "scalare".

Gli spazi vettoriali danno una veste teorica alla risoluzione dei sistemi lineari.

Esempi di spazi vettoriali

Il nome degli spazi vettoriali viene dagli spazi vettoriali geometrici. $(V_O, +, \cdot)$ è lo spazio vettoriale su $\mathbb{R}$ dei vettori dello spazio euclideo applicati in un punto O (detto "origine").

La somma fra vettori geometrici si effettua con la "regola del parallelogramma" (figura 3.1). Le forze possono essere rappresentate dai vettori del piano.

L'elemento neutro è il vettore nullo, i cui estremi coincidono in O, e si indica con $\underline{\underline{O}} = \overrightarrow{OO}$. L'inverso di un vettore v è chiamato $-v$, ha stessa direzione, stesso modulo e verso contrario.

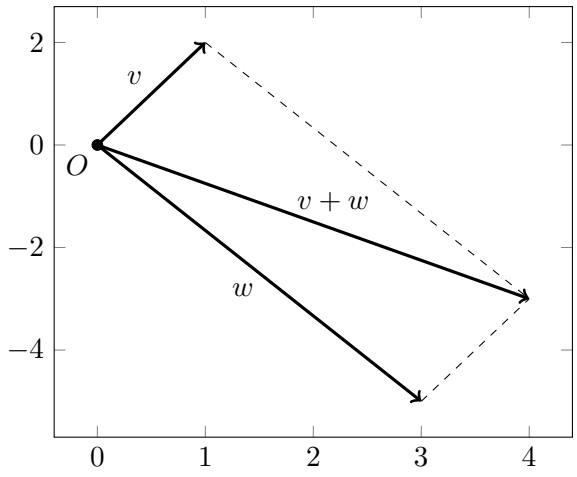

Figura 3.1: Metodo del parallelogramma

Per creare lo spazio vettoriale abbiamo bisogno infine dell'operazione esterna: il prodotto scalare $\cdot : \mathbb{R} \times V \to V$ (figura 3.2).

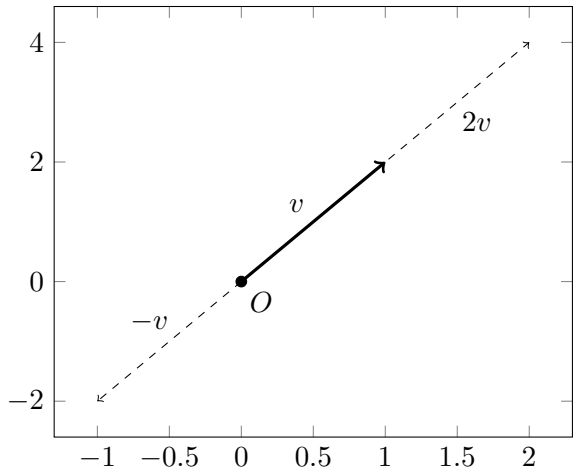

Figura 3.2: Prodotto scalare

Le n-uple degli elementi di un campo $\mathbb{K}$ sono uno spazio vettoriale, ossia $(\mathbb{K}^n, +, \cdot)$ è uno spazio vettoriale su $\mathbb{K}$. Se ad esempio il campo è $\mathbb{R}$ e $n = 3$, prendiamo le terne di numeri reali $(a, b, c) \in \mathbb{R}^3$. La somma di due terne è $(a, b, c) + (x, y, z) = (a + x, b + y, z + c)$. Moltiplicare una terna per un numero si chiama "moltiplicare per uno scalare", e $r \cdot (a, b, c) = (r \cdot a, r \cdot b, r \cdot c)$.

Anche i polinomi $(\mathbb{K}[x], +, \cdot)$ sono uno spazio vettoriale. Moltiplicare un polinomio per uno scalare (ossia per un elemento del campo) vuol dire moltiplicare tutti i coefficienti per lo scalare.

Abbiamo poi visto lo spazio vettoriale delle matrici. L'insieme delle matrici $(\mathfrak{M}_{m\times n}(\mathbb{K}), +, \cdot)$ è uno spazio vettoriale. Date due matrici $A = (a_{i,j})$ e $B = (b_{i,j})$, la loro somma è $A + B = (a_{i,j} + b_{i,j})$, mentre la moltiplicazione per uno scalare k è $k \cdot A = (k \cdot a_{i,j})$.

Dato un sottocampo di un campo $\mathbb{F} \subseteq \mathbb{K}$, ad esempio $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, possiamo vedere $\mathbb{K}$ come spazio vettoriale su $\mathbb{F}$ (o anche su $\mathbb{K}$). $(\mathbb{K}, +, \cdot)$ ha l'operazione $\cdot : \mathbb{F} \times \mathbb{K} \to \mathbb{K}$, che dati $h \in \mathbb{F}$ e $k \in \mathbb{K} \mapsto h \cdot k$.

3.1.1 Sottospazi vettoriali

Un sottoinsieme $W \subseteq V$, con $(V, +, \cdot)$ a indicare uno spazio vettoriale, si dice sottospazio di V se $(W, +, \cdot)$ è ancora uno spazio vettoriale. Le operazioni devono essere $+ : W \times W \to W$, e $\cdot : \mathbb{K} \cdot W \to W$.

Condizione necessaria e sufficiente affinché un insieme $W \subseteq V$ sia un sottospazio di $(V, +, \cdot)$ è che $W \neq \emptyset$, $\underline{0} \in W$, e che:

$$\forall\ v, w \in W \Rightarrow (v - w) \in W$$
$$\forall\ k \in \mathbb{K},\ \ \forall\ w \in W \Rightarrow k \cdot w \in W$$

Nello spazio dei vettori geometrici, quali sono i sottospazi? Deve contenere il vettore nullo. Quindi $W_0 = \{\underline{0}\}$ è un sottospazio banale. Se il sottospazio W_1 contiene un vettore $v \neq \underline{0}$, deve contenere anche:

- $0_{\mathbb{K}} \cdot v = \underline{0} \in W_1$. Infatti $0_{\mathbb{K}} \cdot v = (0_{\mathbb{K}} + 0_{\mathbb{K}}) \cdot v = 0_{\mathbb{K}} \cdot v + 0_{\mathbb{K}} \cdot v \Rightarrow 0_{\mathbb{K}} \cdot v = \underline{0}$
- $-1 \cdot v = -v$. Infatti $v + (-1) \cdot v = (1 - 1) \cdot v = 0_{\mathbb{K}} \cdot v = \underline{0}$. Se moltiplico un vettore per -1 ottengo il suo opposto.
- deve contenere tutti i multipli $k \cdot v$, con $k \in \mathbb{R}$.

Questo è un sottospazio, infatti verifica che $\forall\ v, w \in W_1 \Rightarrow v - w \in W_1$, e abbiamo visto che $\forall\ k \in \mathbb{R}$, $k \cdot v \in W_1$.

$$W_1 = \{k \cdot v \in V : k \in \mathbb{R}\}$$

Un sottospazio quindi è il sottospazio dei vettori che hanno la stessa direzione di v, ossia è il sottospazio dei multipli di un vettore. Un sottospazio che contiene un vettore deve per forza contenere tutti i suoi multipli.

Vediamo cosa succede se il sottospazio contiene un vettore $w \neq k \cdot v$ con $k \in \mathbb{R}$. Deve contenere anche tutti i multipli di w, per quanto appena visto. E deve quindi contenere le somme di tutti i vettori multipli di v e di tutti i vettori multipli di w.

$$W_2 = \{a \cdot v + b \cdot w : a, b \in \mathbb{R} \text{ e } v \neq k \cdot w\}$$

W_2 sono tutti i vettori sul piano individuato dai vettori v e w.

Se aggiungiamo un terzo vettore diverso da $k \cdot v$ e $h \cdot w$ con $h, k \in \mathbb{R}$, abbiamo che lo spazio vettoriale $W_3 \supseteq W_2$ è o $W_3 = W_2$ o $W_3 = V$. W_2 è detto "massimale".

Non esiste un sottospazio che lo contenga propriamente e che è diverso da tutto lo spazio.

Prendiamo l'insieme dei polinomi tali per cui il grado di $p(x) = n$.

$$W_1 = \{p(x) : \delta(p(x)) = n\}$$

Non è un sottospazio: non contiene il polinomio nullo, e la differenza fra due polinomi non sempre ha grado n.

$$W_2 = \{p(x) : \delta(p(x)) \leq n\}$$

Questo è invece un sottospazio.

$$W_3 = \{p(x) : \delta(p(x)) \leq 3 \text{ e } a_1 = a_2 = 0\}$$

Anche questo è un sottospazio. $\underline{0} \in W_3$. La differenza fra due polinomi $a_0+a_3\cdot x^3-b_0-b_3\cdot x^3 = a_0-b_0+(a_3-b_3)\cdot x^3$ è ancora dentro W_3, quindi è un sottogruppo. Inoltre $k\cdot(a_0+a_3\cdot x^3)$ è $k\cdot a_0+k\cdot a_3\cdot x^3$, che è sempre in W_3.

Consideriamo ora $(\mathbb{R}^4,+,\cdot)$, e il sottoinsieme:

$$W=\{(a_1,a_2,a_3,a_4) : a_1+a_2=0\}$$

Prendiamo due elementi (a_1,a_2,a_3,a_4) e (b_1,b_2,b_3,b_4) e facciamo la differenza, ossia $(a_1-b_1, a_2-b_2, a_3-b_3, a_4-b_4)$. Vediamo che $a_1-b_1+a_2-b_2$ è uguale a 0. Per verificare che è un sottospazio, dobbiamo verificare che una quaterna moltiplicata per k è ancora dentro W.

$$k\cdot(a_1,a_2,a_3,a_4)=(k\cdot a_1, k\cdot a_2, k\cdot a_3, k\cdot a_4)$$

È verificato, infatti $k\cdot a_1+k\cdot a_2=k\cdot(a_1+a_2)=k\cdot 0=0$.

È importante controllare sempre che il sottospazio sia vuoto, e che contenga il vettore nullo.

$$W_1=\{(a_1,a_2,a_3,a_4) : a_1=a_2^2\}$$

Questo non è un sottospazio, infatti non verifica che $k\cdot a_1=k\cdot a_2^2$, essendo $(k\cdot a_2)^2=k^2\cdot a_2^2\neq k\cdot a_2^2$.

Consideriamo lo spazio vettoriale delle matrici quadrate $(\mathfrak{M}_2(\mathbb{R}),+,\cdot)$.

$$W=\left\{\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) : a=0\right\}$$

È un sottospazio, infatti $\underline{0}=\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0\end{smallmatrix}\right)$ è dentro W. Inoltre:

$$k\cdot\begin{pmatrix} 0 & b \\ c & d\end{pmatrix}=\begin{pmatrix} 0 & k\cdot b \\ k\cdot c & k\cdot d\end{pmatrix}$$

Consideriamo l'insieme:

$$W_1=\left\{\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) : a=d-1\right\}$$

Non è un sottospazio, poiché $\underline{0}\notin W_1$.

Proposizione 3.1.1 (*Proposizione fondamentale per gli spazi vettoriali*)

Siano U,W sottospazi di $V \Rightarrow U\cap W$ è un sottospazio di V.

Questo vale per tutte le strutture algebriche.

Dimostrazione: Vediamo che $\underline{0}\in U\cap W$, essendo contenuto in entrambi.
Sia $v,w\in U\cap W \Rightarrow v-w\in U\cap W$, essendo $v-w\in U$ e $v-w\in W$.
Analogamente se $v\in U\cap W$ e $k\in\mathbb{K}\Rightarrow k\cdot v\in U\cap W$, essendo U e W sottospazi e quindi essendo ogni multiplo di v in entrambi. ■

3.1.2 Reticolo dei sottospazi vettoriali

Con i sottospazi vettoriali abbiamo un altro esempio di reticolo.

$\mathscr{S}(V)$ è l'insieme dei sottospazi dello spazio vettoriale $(V,+,\cdot)$. $(\mathscr{S}(V),\subseteq)$ è un reticolo, e $\subseteq$ indica la relazione di sottospazio. Siano $U,W\subseteq V$, l'inf di U e W è $U\cap W=U\wedge W$. Verifica le proprietà dell'inf, infatti se $T\subseteq U,W\Rightarrow T\subseteq U\cap W$.

Abbiamo già visto con i sottogruppi che l'unione di due sottogruppi in generale non è un sottogruppo. Anche qui, l'unione di due sottospazi non è, in generale, un sottospazio.

Abbiamo visto ad esempio che due sottospazi di $(V_O, +, \cdot)$ contenenti ciascuno i multipli di un solo vettore hanno un'unione che non è un sottospazio.

Il sup di U e W, $U \vee W$, deve contenere l'unione di U e W.

$$U \subseteq U \cup W \subseteq U \vee W$$

Inoltre sia T un sottospazio di V che contiene sia U che W, $U, W \leq T \Rightarrow U \vee W \leq T$.

Quindi il sup è il più piccolo dei sottospazi che contiene l'unione. Quindi è l'intersezione di tutti i sottospazi che contengono sia U che W.

$$U \vee W = \bigcap_{U,W \subseteq T} T$$

Vediamo come si caratterizza il sup.

Abbiamo il reticolo dei sottospazi di uno spazio vettoriale.

Prendiamo un sottoinsieme S dello spazio vettoriale V. Definiamo il sottospazio generato da da S. Lo indichiamo con $<S>$. È definito come il più piccolo dei sottospazi contenenti S. $U \vee W$ è il sottospazio generato da $<U \cup W>$.

Il sottospazio generato da S è quindi:

$$<S>= \bigcap_{S \subseteq T} T$$

Ossia l'intersezione di tutti i sottospazi contenenti S.

Prendendo $v \in V_O$, il sottospazio generato da v è:

$$<v>= \begin{cases} \underline{0} \text{ se } v = \underline{0} \\ \{k \cdot v : k \in \mathbb{K}\} \text{ se } v \neq \underline{0} \end{cases}$$

3.1.3 Combinazioni lineari e indipendenza lineare

Negli spazi vettoriali ci sono due concetti fondamentali da capire se si vuole capire qualcosa. Fissateli bene a mente, coglione.

Combinazione lineare Dati n vettori $v_1, \dots v_n$ vettori di V, e n scalari $k_1, \dots k_2 \in \mathbb{K}$, la combinazione lineare dei vettori $v_1 \dots v_n$ è un vettore:

$$v = k_1 \cdot v_1 + \dots + k_n \cdot v_n$$

Le combinazioni lineari di un solo vettore v sono tutti i multipli del vettore v.

Indipendenza lineare Si dice che un vettore v dipende dai vettori $v_1, \dots v_t$ se $v \in <\{v_1 \dots v_t\}>$, ossia se v appartiene allo spazio generato da questi vettori, ossia v si può scrivere come combinazione lineare dei vettori.

$$v = a_1 \cdot v_1 + \dots + a_t \cdot v_t$$

In caso contrario si dice che il vettore è indipendente linearmente, ossia non appartiene allo spazio generato.

3.1.4 Esempi di combinazioni lineari

Se prendiamo lo spazio vettoriale $(\mathbb{R}^2, +, \cdot)$, un vettore qualunque (a, b) possiamo scriverlo come combinazione lineare dei vettori $(1, 0)$ e $(0, 1)$.

$$(a, b) = a \cdot (1, 0) + b \cdot (0, 1)$$

Un vettore di $\mathbb{R}^3$ è formato da tutte le combinazioni lineari dei vettori $(1, 0, 0)$, $(0, 1, 0)$ e $(0, 0, 1)$.

In generale, un vettore di $\mathbb{R}^n$ è formato dalla combinazione lineare di tutti i vettori $e_1 \dots e_n$ dove:

$$e_i = \begin{cases} 1 \text{ al posto } i \\ 0 \text{ altrimenti} \end{cases}$$

Nello spazio dei polinomi $\mathbb{R}[x]$, un polinomio $p(x)$ è combinazione lineare dei polinomi $\{1, x, x^2, \dots x^n, \dots\}$, ossia combinazione lineare dei polinomi $\{x^i : i \in \mathbb{N}\}$.

Consideriamo le matrici quadrate di ordine 2, $\mathfrak{M}_2(\mathbb{R})$. Ogni matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ è una combinazione lineare del tipo:

$$a \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Tutte le matrici nello spazio delle matrici quadrate di ordine 2 sono combinazione lineare delle matrici $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

In generale, tutte le matrici $\mathfrak{M}_{m \times n}(\mathbb{R})$ sono combinazioni delle matrici $E_{h,k}(a_{i,j})$ dove:

$$a_{i,j} = \begin{cases} 1 \text{ se } i = h \text{ e } j = k \\ 0 \text{ altrimenti} \end{cases}$$

Nel caso di prima delle matrici quadrate di ordine 2, le matrici sono $E_{1,1}, E_{1,2}, E_{2,1}, E_{2,2}$.

Ritroviamo le combinazioni lineari negli spazi generati da sottoinsiemi di uno spazio vettoriale. S è sottoinsieme dello spazio $(V, +, \cdot)$. $\Sigma(S)$ è insieme delle combinazioni lineari dei vettori di S. Quindi ogni $v \in \Sigma(S)$ è una combinazione lineare del tipo $v = a_1 s_1 + \dots + a_n s_n$ con $s_i \in S$.

Proposizione 3.1.2

$< S >$, ossia lo spazio generato da S, è proprio $\Sigma(S)$.
S è un sistema di generaotri di $\Sigma(S)$.

Dimostrazione: Si dimostra per doppia inclusione. Banalmente $S \subseteq \Sigma(S)$, e $\Sigma(S)$ è un sottospazio di V. Infatti la differenza di due combinazioni lineari è in $\Sigma(S)$, così come il prodotto scalare di una combinazione lineare. Quindi $< S > \subseteq \Sigma(S)$.
Dobbiamo far vedere che ogni combinazione lineare è contenuta in $< S >$.

$$v \in \Sigma(S) \Rightarrow v = a_1 \cdot s_1 + \dots a_n \cdot s_n \text{ con } s_i \in S$$

S è sottoinsieme di T, con T sottospazio di V. $s_i \in T \ \forall \ i$, $a_i \cdot s_i \in T \ \forall \ i \Rightarrow v \in T$. $\Sigma(S) \subseteq T \ \forall \ T$ tale che $S \subseteq T$. ∎

Abbiamo quindi un'altra definizione del sup di due sottospazi.

$$U \vee W = < U \cup W > = \Sigma(U \cup W) = \bigcap_{U \cup W \subseteq T} T$$

Proposizione 3.1.3

$$(U \vee W) = U + W$$

$U + W$ è l'insieme di tutti i vettori che posso scrivere come somma di $u + w$ con $u \in U$ e $w \in W$.

$$U + W = \{u + w : u \in U \text{ e } w \in W\}$$

Dimostrazione: Banalmente $U+W \subseteq \Sigma(U \cup W)$, ossia $U+W$ sono combinazioni lineari degli elementi di U e W in cui i coefficienti delle combinazioni lineari sono sempre 1.

Abbiamo anche che U e $W \subseteq U + W$, che risulta essere un sottospazio.

Infatti prendendo gli elementi $(u + w)$ e $(u' + w')$, $(u + w) - (u' + w') = (u - u') + (w - w')$ è ancora in $U + W$. Poi $k \cdot (u + w) = k \cdot u + k \cdot w$ è dentro $U + W$.

Quindi se $U, W \subseteq U + W$, ed essendo $\Sigma(U \cup W)$ il più piccolo dei maggioranti di U e W, deve essere che $U + W = \Sigma(U \cup W)$. ■

Proposizione 3.1.4 (*Somma diretta fra spazi vettoriali*)

W e U hanno somma diretta, che si indica con $U \oplus W$, se $U \cap W = \{\underline{0}\}$. Le seguenti proposizioni sono equivalenti:

1. *U e W hanno somma diretta*
2. *ogni vettore di $U + W$ si può esprimere in un unico modo come $u + w$, con $u \in U$ e $w \in W$*

Dimostrazione: Il punto 1 implica il punto 2.

Sia $v \in U + W$ tale che $v = u + w = \bar{u} + \bar{w}$, allora $u = \bar{u}$ e $w = \bar{w}$.

Infatti $(u + w) - (\bar{u} + \bar{w}) = \underline{0}$. Da questo segue che possiamo scrivere $(u - \bar{u}) + (w - \bar{w}) = \underline{0}$. Quindi $u - \bar{u} = -(w - \bar{w})$. Questo vettore si può scrivere come somma di due elementi di U e come somma di due elementi di W, quindi è nell'intersezione. Quindi è il vettore nullo $\underline{0}$, e quindi $u = \bar{u}$ e $w = \bar{w}$.

Ora vediamo che il punto 2 implica il punto 1.

Dobbiamo dimostrare che l'intersezione contiene solo il vettore nullo. $U \cap W = \{\underline{0}\}$.

Consideriamo $v \in U \cap W$. Se $v \neq \underline{0}$, dobbiamo scriverlo come somma di due vettori in U e in W in due modi diversi, così andiamo in contraddizione con l'ipotesi del punto 2.

$v = \underline{0} + v$ con $v \in W$, e $v = v + \underline{0}$ con $v \in U$. Contraddizione. ■

Se $W \oplus U = V$, i sottospazi W e U sono detti sottospazi supplementari.

Consideriamo lo spazio vettoriale delle matrici quadrate di ordine n, $(\mathfrak{M}_n(\mathbb{K}), +, \cdot)$. A è simmetrica se $A = A^t$, ossia se la matrice A è uguale alla sua trasposta.

$$A = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 3 & 1 \\ 3 & - & 10 \end{pmatrix} \qquad A^t = \begin{pmatrix} 1 & 0 & 4 \\ -1 & 3 & -1 \\ 2 & 1 & 0 \end{pmatrix}$$

Se un elemento generico della matrice A lo indico con $a_{i,j}$, un elemento generico della matrice trasposta si indica con $a_{j,i}$.

Una matrice A si dice antisimmetrica se $A = -A^t$. Quindi l'elemento generico della matrice trasposta è $-a_{j,i}$, rispetto all'elemento generico della matrice antisimmetrica A indicato con $a_{i,j}$.

Se prendiamo l'insieme di tutte le matrici quadrate simmetriche, $\mathfrak{M}_s$, e l'insieme delle matrici quadrate antisimmetrice $\mathfrak{M}_a$, questi sono due sottospazi dello spazio vettoriale delle matrici quadrate di ordine n, $\mathfrak{M}_n$.

$$\mathfrak{M}_s, \mathfrak{M}_n \in \mathscr{S}\left((\mathfrak{M}_n(\mathbb{K}), +, \cdot)\right)$$

Inoltre hanno somma diretta, e sono sottospazi supplementari.

$$\mathfrak{M}_s \oplus \mathfrak{M}_a = \mathfrak{M}_n(\mathbb{K})$$

Hanno intersezione contenente solo il vettore nullo: $\mathfrak{M}_s \cap \mathfrak{M}_a = \{\underline{0}\}$.

Come possiamo scrivere una matrice qualsiasi come somma di una matrice simmetrica e di una antisimmetrica? $A \in \mathfrak{M}_n(\mathbb{K})$ si scrive come:

$$A = \frac{2A}{2} = \frac{2A - A^t + A^t}{2} = \frac{A + A^t}{2} - \frac{A - A^t}{2}$$

La prima è simmetrica, la seconda è antisimmetrica.

Studieremo solo gli spazi vettoriali finitamente generati, cioè quelli per cui esiste un sottoinsieme finito S tale che $<S>= V$, ossia lo spazio generato da S è uguale a tutto lo spazio vettoriale.

Ad esempio, lo spazio vettoriale di un campo $\mathbb{K}$ è generato da un solo elemento (l'unità).

$\mathbb{R}$ su $\mathbb{R}$, $\mathbb{C}$ su $\mathbb{C}$, sono generati da un solo elemento. $\mathbb{C}$ su $\mathbb{R}$ è generato da due elementi, un reale e un complesso. I due elementi sono 1 e i.

$$c = \{x + y \cdot i : x, y \in \mathbb{R}\} \in \mathbb{C}$$

Le n-uple di elementi di un campo sono generate da n vettori, ossia hanno un sistema di generatori di n elementi. $<\{e_1, \dots e_n\}>= \mathbb{K}^n$, dove:

$$e_i = (x_1, \dots x_n) : x_j = \begin{cases} 1 \text{ se } j = i \\ 0 \text{ se } j \neq i \end{cases}$$

Lo spazio dei polinomi a valori in un campo non è finitamente generato.

Lo spazio delle matrici $m \times n$, $\mathfrak{M}_{m\times n}(\mathbb{K})$, è finitamente generato. Abbiamo già visto come si scrivono i suoi elementi.

3.1.5 Indipendenza lineare

Definizione 3.1.1 (*Dipendenza dei sottospazi*)

> *Un sottoinsieme di uno spazio vettoriale è dipendente se* $\exists\, v \in S$ *t.c.* $v \in <S \setminus \{v\}>$. *Ossia lo spazio generato da* $S \setminus \{v\}$ *rimane uguale allo spazio generato da* S.
> *Quindi un sottoinsieme* S *è indipendente se* $\forall\, v \in S, v \notin < S \setminus \{v\} >$. *Ossia* $< S > \neq < S \setminus \{v\} >$.

$S = \{\underline{0}\}$ è un sottoinsieme dipendente. $< S \setminus \{\underline{0}\} >=< \emptyset >=< S >= \{\underline{0}\}$. In generale, ogni sottoinsieme contenente il vettore nullo è un sottoinsieme dipendente.

$S = \{v\}$ con $v \neq \underline{0}$ è sempre indipendente.

Se invece $S = \{v_1, v_2\}$, S è dipendente se $v_1 = a \cdot v_2$, ossia se $v_1 \in < v_2 >$, altrimenti S è indipendente.

La dipendenza dipende anche dal campo degli scalari.

Consideriamo lo spazio vettoriale di $\mathbb{C}$ su $\mathbb{C}$. $S = \{1, i\}$ è dipendente, perché $i \cdot 1 = i$.

In $\mathbb{C}$ su $\mathbb{R}$, invece, $S = \{1, i\}$ è indipendente (e genera pure tutto lo spazio).

Quindi lo stesso insieme di vettori, su spazi diversi, può avere una dipendeza o una indipendenza differente.

Consideriamo $(\mathbb{K}[x], +, \cdot)$ su $\mathbb{K}$, e l'insieme $S = \{(1-x), (1+x^2), (1+x-x^3)\}$.

Verifichiamo se $(1-x) \in <(1+x^2), (1+x-x^3)>$. Dobbiamo vedere se $(1-x)$ si può scrivere come:

$$a \cdot (1+x^2) + b \cdot (1+x+x^3) = ((a+b) + b \cdot x + a \cdot x^2 - b \cdot x^3) = (1-x)$$

Dovremmo risolvere il sistema in cui $a+b=1$, $b=-1$, $a=0$, $b=0$. Questo sistema non ha soluzioni. Un giorno impareremo a risolvere questi sistemi.

Si vede subito che $(1+x^2)$ non può essere dentro $<(1-x), (1+x+x^3)>$, siccome il coefficiente di secondo grado di questi polinomi sarà sempre 0. Anche $(1+x+x^3)$ non appartiene a $<(1-x), (1+x^2)>$. Quindi l'insieme S è indipendente.

Dobbiamo trovare un modo efficace ed efficiente per controllare se un insieme è dipendente o indipendente.

$$S = \{(1,1,1), (0,1,1), (5,-7,-7)\} \Rightarrow <S \setminus \{(5,-7,-7)\}> = \{(a, a+b, a+b) : a, b \in \mathbb{R}\}$$

Possiamo ritrovare $(5,-7,-7)$ in questo spazio? Sì. Dobbiamo avere $a=5$ e $a+b=-7$, quindi $b = -7-5 = -12$. Questo sottoinsieme è dipendente.

3.1.6 Caratterizzazione degli insiemi indipendenti

S è indipendente $\Leftrightarrow$ $\forall\, s_1, \ldots, s_t \in S$, $a_1 \cdot s_1 + \cdots + a_t \cdot s_t = \underline{0} \Rightarrow a_1 = \cdots = a_t = 0$, ossia l'unica combinazione lineare di vettori di S uguale al vettore nullo è quella banale.

S è dipendente $\Leftrightarrow$ $\exists\, s_1, \ldots s_t \in S$ tali che $a_1 \cdot s_1 + \cdots + a_t \cdot s_t = \underline{0}$ e $a_i \neq 0$ per qualche i, ossia esiste una combinazione lineare non banale di vettori di S uguale al vettore nullo.

Dimostrazione: Vediamo che è condizione necessaria. Se S è dipendente, $\exists\, v \in S$ tale che $v \in < S \setminus \{v\} >$. Quindi $v = a_1 s_1 + \cdots + a_t s_t$ dove $s_i \neq v$, essendo $s_i \in S \setminus \{v\}$. Quale combinazione lineare di vettori di S è uguale al vettore nullo?

$$a_1 s_1 + \cdots + a_t s_t - v = \underline{0}$$

Vediamo che è condizione sufficiente, ossia se esiste una combinazione lineare non banale uguale al vettore nullo, allora S è dipendente.

$$\exists\, a_1 s_1 + \cdots + a_t s_t = \underline{0}$$

Essendo non banale, possiamo supporre $a_1 \neq 0$. Prendiamo $v = a_1 s_1 = -(a_2 s_2 + \cdots + a_t s_t)$. Quindi:

$$v \in < S \setminus \{v\} >$$

Ossia, S è dipendente. ■

$$S = \{(1,2,2),(1,-2,-1),(0,4,3)\}$$

Per vedere se S è dipendente, usiamo la caratterizzazione vista. Facciamo una combinazione lineare dei suoi elementi e vediamo se è uguale al vettore nullo.

$$a\cdot(1,2,2)+b\cdot(1,-2,-1)+c\cdot(0,4,3)=\underline{0}\Rightarrow(a+b,2a-2b+4c,2a-b+3c)=\underline{0}$$

Dobbiamo risolvere il seguente sistema lineare:

$$\begin{cases} a+b=0 \\ 2a-2b+4c=0 \\ 2a-b+3c=0 \end{cases}$$

Risolvendo il sistema lineare abbiamo che le soluzioni sono $(a,-a,-a)\ \forall\ a\in\mathbb{R}$. Quindi il sistema è dipendente.

Fatto 1 (*Fatto fondamentale*)

Sia S un insieme indipendente, e v un vettore non in S. Possiamo avere due casi:
- *$S\cup\{v\}$ è dipendente $\Leftrightarrow v\in<S>$*
- *$S\cup\{v\}$ è indipendente $\Leftrightarrow v\notin<S>$*

Questa osservazione permette di costruire insieme indipendenti.

Costruiamo un insieme S indipendente in $\mathbb{R}^3$. Partiamo da un insieme indipendente, contenente quindi un vettore diverso dal vettore nullo.

$$v_1=(1,-1,2)\Rightarrow<v_1>=\{(a,-a,2a):a\in\mathbb{R}\}$$

Dobbiamo prendere $v_2\notin<v_1>$. Per farlo, assegnamo un valore ad a e cambiamo una coordinata. Prendiamo, fissando $a=2$, il vettore $(2,-2,4)$. Sicuramente il vettore $(2,-2,0)$ non è nello spazio generato da v_1.

$$v_2=(2,-2,0)$$

Quindi $S=\{v_1,v_2\}$ è ancora indipendente. Il suo spazio generato è:

$$<v_1,v_2>=\{a\cdot v_1+b\cdot v_2:a,b\in\mathbb{R}\}=\{(a+2b,-a-2b,2a):a,b\in\mathbb{R}\}$$

Possiamo trovare un vettore non in questo spazio, dando dei valori ad a e b. Ad esempio $a=1$ e $b=-1$, abbiamo il vettore $(-1,-3,2)$. Il vettore $(-1,-3,1)$ non è nell'insieme S. Quindi $S=\{(1,-1,2),(2,-2,0),(-1,-3,1)\}$ è ancora indipendente.

Lo spazio generato da S adesso è tutto $\mathbb{R}^3$. Possiamo infatti vedere che ogni vettore generico (a,b,c) si può scrivere come combinazione lineare dei tre vettori di S.

$$<S>=\{(a+2b-c,-a-2b-3c,2a+c):a,b,c\in\mathbb{R}\}$$

S è un sistema di generatori minimale. Minimale vuol dire che non esiste un sistema di generatori più piccolo di S, ossia un $G\subseteq S$, tale che $<G>=\mathbb{R}^3$.

3.1.7 Base di uno spazio vettoriale

Il concetto di base di uno spazio vettoriale $(V,+,\cdot)$ su uno spazio $\mathbb{K}$ unisce i concetti di combinazione e indipendenza lineare.

Definizione 3.1.2

Una base dello spazio vettoriale $(V, +, \cdot)$ è un sottoinsieme B di V tale che:
B è indipendente
$< B >= V$, ossia B è un sistema di generatori di V

Teorema 3.1.5

Ogni spazio vettoriale $(V, +, \cdot)$ su un campo $\mathbb{K}$ ha (almeno) una base B, e tutte le basi hanno la stessa cardinalità.

Se $|B| = \infty$, si dice che V ha dimensione infinita. Se invece $|B| = n$, si dice che V ha dimensione n. Si indica tipicamente con $\dim V = n$.

Esempio :

$(\mathbb{R}[x], +, \cdot)$ ha dimensione infinita. Infatti la base $B = \{x^i : i \in \mathbb{N}\}$ ha cardinalità infinita. Ogni polinomio $p(x)$ si scrive come combinazione lineare degli elementi di B, ossia:

$$p(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n \text{ con } n = \delta(p(x))$$

Gli elementi di B sono indipendenti, infatti l'unica combinazione lineare degli elementi di B che mi dà il vettore nullo $\underline{0}$ è quella banale, ossia $\sum_{i=0}^{\infty} a_i x^i = \underline{0} \Leftrightarrow a_i = 0 \ \forall \ i$.

Consideriamo $\mathbb{C}$ su $\mathbb{C}$, o in generale lo spazio vettoriale di $\mathbb{K}$ su $\mathbb{K}$, abbiamo che $\dim_{\mathbb{K}} \mathbb{K} = 1$. Se invece consideriamo $\mathbb{C}$ su $\mathbb{R}$, $\dim_{\mathbb{R}} \mathbb{C} = 2$, infatti la sua base è $B = \{1, i\}$.

Considerando le matrici $m \times n$, $(\mathfrak{M}_{m \times n}(\mathbb{R}), +, \cdot)$, la sua dimensione è $\dim \mathfrak{M}_{m \times n}(\mathbb{R}) = m \times n$. La sua base è $B = \{E_{i,j} : (i, j) \in [m] \times [n]\}$, dove la matrice generica è:

$$E_{i,j} = (e_{h,k}) = \begin{cases} 1 \text{ se } (h, k) = (i, j) \\ 0 \text{ altrimenti} \end{cases}$$

I polinomi di grado minore o uguale a n, ossia $(\mathbb{R}_n[x], +, \cdot)$, hanno dimensione $\dim \mathbb{R}_n[x] = (n + 1)$.

Tutte le basi viste finora si chiamano **basi canoniche**.

3.1.8 Caratterizzazione delle basi

Le seguenti proposizioni sono equivalenti:

1. B è una base di $(V, +, \cdot)$, ossia $< B >= V$ e B è indipendente
2. B è un sistema di generazione minimale, ossia preso $S \subsetneq B \Rightarrow < S > \neq < B >= V$
3. B è un insieme indipendente massimale, ossia dato $S \supsetneq B \Rightarrow S$ è dipendente, ossia non posso trovare un insieme più grande di B che sia indipendente

Dimostrazione : Dimostriamo che 1 implica 2.
La tesi è che B è minimale. Prendiamo un $S \subsetneq B \Rightarrow \ \exists \ w \in B$ tale che $w \notin S$. Abbiamo quindi che:

$$< S > \subseteq < B \setminus \{w\} > \subsetneq < B >= V$$

Segue quindi che $< S > \neq V$. B è un sistema di generatori minimale (ossia ha il minimo numero di elementi).

Dimostriamo che 2 implica 3.

Partendo dal fatto che B è un sistema di generatori minimale, dobbiamo dimostrare che B è un insieme indipendente massimale. B è indipendente, perché $\forall\ w \in B, < B \setminus \{w\} > \neq V$ essendo B un sistema di generatori minimale.

Dobbiamo far vedere ora che dato un $S \supsetneq B \Rightarrow S$ è dipendente. Infatti $\exists\ w \in S$ tale che $w \notin B$. Quindi $< B > \subseteq < S \setminus \{w\} > \subseteq < S > = V$. S è dipendente.

Dimostriamo che 3 implica 1.

La tesi è che $< B > = V$. Prendiamo un vettore qualunque $v \in V$ tale che $v \notin B$. $B \cup \{v\}$ è dipendente, quindi esiste una combinazione lineare non banale di vettori di $B \cup \{v\}$ che dà il vettore nullo. In particolare, questa combinazione lineare ha il coefficiente di v diverso da 0. Quindi v si può scrivere come combinazione lineare di vettori di B.

$$a_1 v + a_2 v_2 + \cdots + a_n v_n = \underline{0} \Rightarrow v = -\frac{a_2 v_2 + \cdots + a_n v_n}{a_1}$$

■

Proposizione 3.1.6

Consideriamo lo spazio vettoriale $(V, +, \cdot)$ su $\mathbb{K}$. B è una base se e solo se ogni vettore v di V si esprime in un solo modo come combinazione lineare di vettori di B.

Dimostrazione: Vediamo che è condizione necessaria. L'ipotesi è che B è una base. Supponiamo per assurdo che un vettore $v \in V$ si possa esprimere in due modi come combinazione lineare di elementi $e_i \in B$:

$$v = a_1 \cdot e_1 + \cdots + a_n \cdot e_n = b_1 \cdot e_1 + \cdots + b_n \cdot e_n \Rightarrow \underline{0} = (a_1 - b_1) \cdot e_1 + \cdots + (a_n - b_n) \cdot e_n$$

Essendo B indipendente, abbiamo che l'unica combinazione lineare che dà il vettore nullo è quella banale, quindi deve essere che $a_i = b_i\ \forall\ i$.

Dimostrare che è condizione sufficiente è molto più veloce. Sappiamo che ogni vettore di V si esprime in un solo modo come combinazione lineare di elementi di B. Quindi banalmente $< B > = V$. Inoltre, il vettore nullo si esprime in un solo modo:

$$\underline{0} = 0 \cdot e_1 + \cdots + 0 \cdot e_n$$

■

Osservazione 12

Sia $(V, +, \cdot)$ uno spazio vettoriale sul campo $\mathbb{K}$ di dimensione $\dim_{\mathbb{K}} V = n$.

1. *n vettori indipendenti sono una base*
2. *n generatori di V costituiscono una base*
3. *$(n+1)$ vettori costituiscono sempre un insieme dipendente*

Teorema 3.1.7 (*Teorema del completamento*)

Uno spazio vettoriale $(V, +, \cdot)$ sul campo $\mathbb{K}$ di dimensione $\dim_{\mathbb{K}} V = n$ e un insieme S indipendente. Segue che $|S| = t \leq n$. Esistono $v_1 \dots v_h$ vettori (indipendenti) di V tali che $S \cup \{v_1 \dots v_k\}$ è una base, con $t + h = n$.

Dimostrazione: Se $< S > = V \Rightarrow t = n$. Altrimenti, se $< S > \neq V$, possiamo trovare un vettore $v_1 \notin < S >$ tale che $S \cup \{v_1\}$ è indipendente. Si può ripetere il procedimento fino ad ottenere tutto V.

Prendiamo una base B di V. Se $< S > \neq V = < B >$, allora $\exists\ v_1 \in B$ tale che $v_n \in < S >$. ■

Teorema 3.1.8 (*Teorema dell'estrazione*)

Consideriamo un sottoinsieme $G \subseteq V$ tale che $<G>= V$, ossia G è un sistema di generatori di V. Possiamo trovare un sistema $S \subseteq G$ con $S = \{v_1, \dots v_n\}$ tale che $G \setminus S$ è una base di V.

Dimostrazione: $<G>= V$, ma G non è una base. Quindi $\exists\ v_1 \in G$ tale che $<G \setminus \{v_1\}>= V$, ossia $G \setminus \{v_1\}$ è sempre un sistema di generatori di V. Si può ripetere il procedimento fino ad ottenere una base, ossia finché $G \setminus S$ è indipendente.

Se $|G| = t$, dobbiamo togliere h vettori con $h = t - n$ e $\dim V = n$.

Alternativamente, prendiamo un vettore $v_1 \neq \underline{0}$. $\{v_1\}$ è indipendente. Se $< v_1 >\neq V =< G >$, allora $\exists\ v_2 \in G$ tale che $v_2 \notin < v_1 >$. Si ripete il ragionamento fino a trovare la base. ■

Esempio:

Nello spazio vettoriale $\mathbb{R}^3$, prendiamo l'insieme $G = \{(1,0,2), (-1,1,0), (1,1,4), (0,1,1)\}$. Il teorema dice che $\exists\ S \subseteq G$ tale che $G \setminus S$ è una base. La dimensione di $\mathbb{R}^3$ è 3, quindi dobbiamo togliere un solo vettore.

$(1,0,2) \neq \underline{0}$. Quindi L'insieme $\{(1,0,2)\}$ è indipendente. $(-1,1,0)$ è indipendente da $(1,0,2)$, quindi anche l'insieme $\{(1,0,2), (-1,1,0)\}$ è indipendente. I vettori nell'insieme generato da questi due vettori sono tutti nella forma $(a-b, b, 2a)$. Poniamo $a = 2$ e $b = 1$, e vediamo che il vettore $(1,1,4)$ è nello spazio generato da questi due. L'altro vettore $(0,1,1)$ non è generato dai due presi prima, quindi lo spazio $S = \{(1,0,2), (-1,1,0), (0,1,1)\}$ è una base.

Consideriamo ora l'insieme $S = \{(2,1,1), (2,-1,1)\}$. Troviamo un vettore che aggiunto a S faccia una base. Lo spazio generato da S è:

$$<S>= \{a(2,1,1) + b(2,-1,1) : a, b \in \mathbb{R}\} = \{(2a+2b, a-b, a+b) : a, b \in \mathbb{R}\}$$

Prima e terza coordinata sono "dipendenti", infatti $2a + 2b = 2(a + b)$. Se fissiamo $a = 1$ e $b = 1$, ottenendo $(4,0,2)$, e cambiamo la seconda coordinata (che non è dipendente dalle altre due), otteniamo una $(4,1,2)$ che è nello spazio generato. L'equazione del nuovo vettore deve essere incompatibile.

La coordinata da cambiare quindi non va scelta a caso, ma fra quelle dipendenti (se ce ne sono).

Sia B una base dello spazio vettoriale $(V, +, \cdot)$, abbiamo visto che ogni vettore v di V si esprime in un unico modo come combinazione lineare di vettori di B.

$$v = a_1 \cdot v_1 + \dots + a_n \cdot v_n$$

Ogni vettore si esprime come n-upla delle coordinate di v rispetto a B, ossia $(a_1, \dots, a_n)$.

Capitolo 4

Applicazioni lineari

Rappresentazione con matrici, diagonalizzazione.

4.1 Applicazione lineari

Definizione 4.1.1 (*Applicazione lineare*)

Le applicazioni lineari sono morfismi tra spazi vettoriali sullo stesso campo $\mathbb{K}$. Un'applicazione $L : V \to V'$ è lineare se conserva tutte le proprietà degli spazi vettoriali. Deve quindi conservare le operazioni:

1. $L(v + w) = L(v) + L(w)$
2. $\forall\ a \in \mathbb{K}\ e\ \forall\ v \in V,\ L(a \cdot v) = a \cdot L(v)$

Equivalentemente possiamo dire che:

$$\forall\ a, b \in \mathbb{K},\ \forall\ v, w \in V,\ L(a \cdot v + b \cdot w) = a \cdot L(v) + b \cdot L(w)$$

Conserva la linearità: manda una combinazione lineare nella combinazione lineare delle immagini con gli stessi coefficienti.

Dimostrazione: Vediamolo da sinistra verso destra, $L(a \cdot v + b \cdot w) = L(a \cdot v) + L(b \cdot w) = a \cdot L(v) + b \cdot L(w)$, per le due proprietà delle applicazioni lineari.
Viceversa, $L(a \cdot v + 0 \cdot w) = L(a \cdot v) = a \cdot L(v)$, e $L(1 \cdot v + 1 \cdot w) = 1 \cdot L(v) + 1 \cdot L(w) = L(v) + L(w)$. ■

Un morfismo di strutture algebriche individua un nucleo e un'immagine. Un'applicazione lineare $L : V \to V'$ quindi individua due sottospazi:

1. $Im_L = \{v' \in V' :\ \exists\ v \in V \text{ t.c. } L(v) = v'\} \leq V'$
2. $\ker L = \{v \in V : L(v) = \underline{0}_{V'}\} \leq V$

4.1.1 Teorema di omomorfismo per gli spazi vettoriali

Teorema 4.1.1

Data un'applicazione lineare $L : (V, +, \cdot) \to (V', +, \cdot)$ sul campo $\mathbb{K}$, si ha che:

1. $\ker L \leq V$
2. $Im_L \leq V'$

3. $V/\ker L \cong Im_L$, ossia i due insiemi sono isomorfi

Alcune proprietà delle applicazioni lineari:

1. $L(\underline{0}_V) = \underline{0}_{V'}$
2. $L(-v) = -L(v)$
3. $L(a \cdot v + b \cdot w) = a \cdot L(v) + b \cdot L(w)$
4. $L^{-1}(v') = v + \ker L$, ossia tutti i vettori v tali per cui $L(v) = v'$ si ottengono sommando v con gli elementi del nucleo
5. L manda insiemi dipendenti in insiemi dipendenti. Ossia, dato $S \leq V$, se è dipendente in V, $L(S)$ è dipendente in V'

Dimostrazione della proprietà 5 : $S \leq V$ è dipendente, ossia $\underline{0}_V = a_1 \cdot s_1 + \cdots + a_n \cdot s_n$ dove $s_i \in S$ e almeno un $a_i \neq 0$. Quindi:

$$L(\underline{0}_V) = L(a_1 \cdot s_1 + \cdots + a_n \cdot s_n) = a_1 \cdot L(s_1) + \cdots + a_n \cdot L(s_n) = \underline{0}_{V'}$$

Quindi anche $L(S)$ è dipendente. ■

Prendendo un insieme indipendente, non sappiamo con certezza cosa succede, ma possiamo dire quanto segue:

Proposizione 4.1.2

Un'applicazione lineare iniettiva $L : V \to V'$, ossia tale che $\ker L = \{\underline{0}_V\}$, manda insiemi indipendenti in insiemi indipendenti, e viceversa un'applicazione che manda insiemi indipendenti in insiemi indipendenti è un'applicazione iniettiva.

Dimostrazione : Vediamo che è condizione necessaria. L'applicazione L è iniettiva. Prendiamo S indipendente, come tesi abbiamo che $L(S)$ è a sua volta indipendente. Prendiamo la combinazione lineare $\underline{0}_V = a_1 \cdot s_1 + \cdots + a_n \cdot s_n$, sappiamo che ogni $a_i = 0$, abbiamo che $L(\underline{0}_V) = \underline{0}_{V'} = L(a_1 \cdot s_1 + \cdots + a_n \cdot s_n) = a_1 \cdot L(s_1) + \cdots + a_n \cdot L(s_n)$, e tutti i coefficienti a_i sono uguali a 0.

Vediamo che è condizione sufficiente. Se S è indipendente, la sua immagine $L(S)$ è indipendente. Se prendiamo $v \in \ker L$ e supponiamo per assurdo che $v \neq \underline{0}_V$, ma che, essendo nel $\ker L$, $L(v) = \underline{0}_{V'}$, abbiamo che l'immagine dello spazio indipendente $S = \{v\}$ è $L(S) = \{\underline{0}_{V'}\}$ che non è indipendente. Quindi v deve essere il vettore nullo.

Possiamo anche vedere che $L(v) = L(w) \Rightarrow v = w$. Sempre sotto l'ipotesi che insiemi indipendenti vanno in insiemi indipendenti, $L(v - w) = \underline{0}_{V'}$, quindi il vettore $v - w$ è nel $\ker L$. $v - w$ deve essere uguale al vettore nullo, e quindi v deve essere uguale a w, per lo stesso motivo di sopra. ■

Esempio :

$L : \mathbb{R}^3 \to \mathbb{R}^2$, definita come $L(a, b, c) = (a + 1, b + c)$ non è un'applicazione lineare. Infatti il vettore nullo $(0, 0, 0)$ va in $(1, 0)$.

$L : \mathbb{R}^3 \to \mathbb{R}^2$ definita come $L(a, b, c) = (a + b, a + c)$. Vediamo se è un'applicazione lineare.

$$\begin{aligned} &L\left((a, b, c) + (a', b', c')\right) = (a + b, a + c) + (a' + b', a' + c') = \\ &= (a + a' + b + b', a + a' + c + c') = L\left(a + a', b + b', c + c'\right) \end{aligned}$$

Controlliamo se conserva anche il prodotto scalare. Prendiamo un $k \in \mathbb{R}$.

$$L\left(k \cdot (a,b,c)\right) = L\left(k \cdot a, k \cdot b, k \cdot c\right) = (k \cdot a + k \cdot b, k \cdot a + k \cdot c) = k \cdot (a+b, a+c) = k \cdot L(a,b,c)$$

Quindi questa è un'applicazione lineare. Qual è il nucleo?

$$\begin{aligned}\ker L &= \{(a,b,c) \in \mathbb{R}^3 : L(a,b,c) = (a+b, a+c) = (0,0)\} = \\ &= \{(a,b,c) \in \mathbb{R}^3 : a+b = 0 \text{ e } a+c = 0\} = \\ &= \{(a,b,c) \in \mathbb{R}^3 : a = -b = -c\} = \\ &= \{(a,-a,-a) \in \mathbb{R}^3 : a \in \mathbb{R}\}\end{aligned}$$

Il nucleo ha dimensione 1. Il nucleo infatti è isomorfo a $\mathbb{R}$, o equivalentemente è ottenuto da tutti i multipli di $(1,-1,-1)$. Quindi l'applicazione non è iniettiva.

Come è fatta l'immagine?

$$Im_L = \{(x,y) : L(a,b,c) = (x,y)\} = \mathbb{R}^2$$

Infatti posso prendere la terna $(0,x,y)$, ho che la sua immagine è (x,y). Quindi l'immagine ha dimensione 2.

Possiamo notare che $\dim \mathbb{R}^3 = \dim \ker L + \dim Im_L$. La dimensione del dominio è data dalla dimensione del nucleo più la dimensione dell'immagine.

L'applicazione $L(a,b,c) = (a^2, b+c)$ non è lineare. Si vede subito, perché c'è un quadrato che causa rogne.

a,b,c sono le coordinate del vettore rispetto alla base canonica $\{(1,0,0),(0,1,0),(0,0,1)\}$. Per avere un'applicazione lineare, le coordinate dell'immagine devono essere date da equazioni lineari.

Cambiamo dominio. $L : \mathfrak{M}_2(\mathbb{R}) \to \mathbb{R}^3$.

$$L\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) = (a+2b, d, a+d)$$

Il suo nucleo è:

$$\ker L = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : L\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) = (0,0,0)\right\}$$

Ossia tutte le matrici tali che $a+2b=0$, $d=0$, $a+d=0$. Quindi a,b,d sono tutti 0.

$$\ker L = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : d = a = b = 0\right\} = \left\{\left(\begin{smallmatrix} 0 & 0 \\ c & 0 \end{smallmatrix}\right) : c \in \mathbb{R}\right\}$$

Il $\ker L$ ha dimensione 1, essendo ottenuto interamente da $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. Quindi l'immagine è tutto $\mathbb{R}^3$, dovendo avere dimensione 3.

Consideriamo l'applicazione $L(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = (a+d, d, a+d)$, abbiamo che il nucleo è:

$$\ker L = \left\{\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) : b, c \in \mathbb{R}\right\}$$

In questo caso il nucleo ha dimensione 2, e si può ottenere a partire dai vettori $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ e $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. Ora l'immagine ha dimensione 2. Come è fatta l'immagine?

$$Im_L = \{(x,y,z) \in \mathbb{R}^3 : x = a+d, y = d, z = a+d\} = \{(x,y,x) \in \mathbb{R}^3 : x = a+d, y = d\}$$

L'immagine è generata dai vettori $(1,0,1)$ e $(0,1,0)$.

Proposizione 4.1.3

Dati $v'_1, \dots v'_n$ vettori di V' e una base $B = \{b_1, \dots b_n\}$ di V, esiste una sola applicazione lineare $L : V \to V'$ tale che $L(b_i) = v'_i$. Non sappiamo niente sulle dimensioni di V e di V', ossia non sono necessariamente uguali.

Dimostrazione: Consideriamo il vettore $v = a_1 \cdot b_1 + \ldots + a_n \cdot b_n$. La sua immagine è:

$$L(v) = L(a_1 \cdot b_1 + \ldots + a_n \cdot b_n) = a_1 \cdot v'_1 + \ldots + a_n \cdot v'_n$$

L è l'applicazione lineare cercata, ed è unica. Sia L' tale che $L'(b_i) = v'_i$, allora $L = L'$.

$$L(V) = a_1 \cdot v'_1 + \ldots + a_n \cdot v'_n = a_1 \cdot L'(b_1) + \ldots + a_n \cdot L'(b_n) = L'(a_1 \cdot b_1 + \ldots + a_n \cdot b_n)$$

Le applicazioni quindi sono uguali, perché assumono gli stessi valori su ogni vettore. ■

4.1.2 Basi e applicazioni lineari

Per definire un'applicazione lineare basta fornire i valori che l'applicazione fornisce per la base. Consideriamo ad esempio $L : \mathfrak{M}_2(\mathbb{R}) \to \mathbb{R}^5$.

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \to (2, 0, 0, 1, 0)$$
$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \to (0, 0, 0, 0, 0)$$
$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \to (1, 1, 1, 1, 1)$$
$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \to (0, 1, 0, 1, 0)$$

Come si trova l'immagine di un vettore qualsiasi?

$$\begin{aligned} L\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) &= L\left(a \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + b \cdot \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) + c \cdot \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) + d \cdot \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) = \\ &= a \cdot L\left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)\right) + b \cdot L\left(\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\right) + c \cdot L\left(\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\right) + d \cdot L\left(\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) = \\ &= a \cdot (2, 0, 0, 1, 0) + b \cdot (0, 0, 0, 0, 0) + c \cdot (1, 1, 1, 1, 1) + d \cdot (0, 1, 0, 1, 0) = \\ &= (2a + c, c + d, c, a + c + d, c) \end{aligned}$$

4.1.3 Isomorfismi fra spazi vettoriali

Un'applicazione lineare biunivoca si dice "isomorfismo". Gli spazi vettoriali si dicono isomorfi. Spazi vettoriali isomorfi hanno la stessa dimensione. Vuol dire che esiste un'applicazione lineare $L : V \to V'$ isomorfa fra i due spazi vettoriali, e che quindi ogni base di V ha per immagine una base di V'.

Teorema 4.1.4 (*Teorema di isomorfismo*)

V è uno spazio vettoriale su $\mathbb{K}$ con $\dim V = n$, allora V è isomorfo a $\mathbb{K}^n$, e viceversa, se V è isomorfo a $\mathbb{K}^n$, allora $\dim V = n$.

Dimostrazione: Per ipotesi, V è uno spazio vettoriale su $\mathbb{K}$ di dimensione $\dim V = n$. Qual è l'isomorfismo con $\mathbb{K}^n$?

$$L_B : \mathbb{K}^n \to V$$

Abbiamo tante applicazioni isomorfe L_B, a seconda della base B di V che fissiamo. Siccome $\dim V = n$, $|B| = n$. Sia B una base $\{e_1, \ldots, e_n\}$:

$$L_B(a_1, \ldots, a_n) = v = a_1 \cdot e_1 + \cdots + a_n \cdot e_n$$

L_B associa ad ogni n-upla $(a_1, \ldots, a_n)$ il vettore di coordinate $a_1, \ldots, a_n$ rispetto alla base B. Infatti:

$$\begin{aligned} L_B\left((a_1, \ldots, a_n) + (b_1, \ldots, b_n)\right) = \\ = L_B\left(a_1 + b_1, \ldots, a_n + b_n\right) = \\ = (a_1 + b_1) \cdot e_1 + \ldots + (a_n + b_n) \cdot e_n = \\ = (a_1 \cdot e_1 + \ldots + a_n \cdot e_n) + (b_1 \cdot e_1 + \ldots + b_n \cdot e_n) = \\ = L_B(a_1, \ldots, a_n) + L_B(b_1, \ldots, b_n) \end{aligned}$$

Banalmente conserva anche il prodotto per uno scalare

$$L_B(k \cdot (a_1, \ldots, a_n)) = k \cdot L_B(a_1, \ldots, a_n)$$

$\ker L_B = \{\underline{0}\}$, poiché se $L_B(a_1, \ldots, a_n) = \underline{0}$, allora $a_1 \cdot e_1 + \ldots + a_n \cdot e_n = \underline{0}$, ma essendo B una base l'unica combinazione lineare che dà il vettore nullo è quella banale, quindi $a_i = 0$. ■

Un esempio tipico sono i vettori geometrici del piano. Ad un vettore nel piano corrisponde una coppia di punti, che non sono altro che le coordinate del vettore rispetto alla base $B = \{i, j\}$ con $|i| = 1$ e $|j| = 1$.

Possiamo studiare solo le n-uple di elementi di un campo $\mathbb{K}$ come spazi vettoriali, e da quelle passare a tutti gli altri spazi.

Vediamo un'ultima proprietà delle applicazioni lineari. Sia $L : V \to V'$ un'applicazione lineare, e sia $\dim V = n$ (finito):

$$\dim V = \dim \ker L + \dim Im_L$$

Dimostrazione:

$$\ker L \begin{cases} = \{\underline{0}\} \Rightarrow L \text{ è iniettiva, e } \bar{L} : V \to Im_L \text{ è suriettiva} \Rightarrow \dim V = \dim Im_L \\ \neq \{\underline{0}\} \end{cases}$$

Nel secondo caso, $B_k = \{u_1, \ldots, u_t\}$ è una base del $\ker L$, quindi $\dim \ker L = t \Rightarrow$ per il teorema del complemento esiste H sottoinsieme di V, $H = \{w_{t+1}, \ldots, w_n\}$ tale che $B_k \cup H$ è una base di $V \Rightarrow L(H)$ è una base di Im_L, quindi $\dim Im_L = n - t$.

Bisogna dimostrare che $< L(H) >= Im_L$, e che $L(H)$ è indipendente.

Prendiamo un vettore $v' \in Im_L$ tale che $L(v) = v'$.

$$\begin{aligned} v' = L(v) = L(a_1 \cdot u_1 + \ldots + a_t \cdot u_t + a_{t+1} \cdot w_{t+1} + \ldots + a_n \cdot w_n) = \\ = \underbrace{a_1 \cdot L(u_1) + \ldots + a_t \cdot L(u_t)}_{\underline{0}} + a_{t+1} \cdot L(w_{t+1}) + \ldots + a_n \cdot L(w_n) \end{aligned}$$

Quindi qualsiasi elemento di Im_L si può scrivere come combinazione di vettori di $< L(H) >$. Vediamo ora che è indipendente. Prendiamo una combinazione lineare che dà il vettore nullo, e mostriamo che è banale:

$$\begin{aligned} \underline{0} = a_{t+1} \cdot L(w_{t+1}) + \ldots + a_n \cdot L(w_n) = \qquad \text{(essendo } L \text{ lineare)} \\ = L\left(a_{t+1} \cdot w_{t+1} + \ldots + a_n \cdot w_n\right) \end{aligned}$$

Quindi il vettore $v = a_{t+1} \cdot w_{t+1} + \ldots + a_n \cdot w_n \in \ker L$, quindi $v = b_1 \cdot u_1 + \ldots b_t \cdot u_t$. Quindi, ancora, $\underline{0} = a_{t+1} \cdot w_{t+1} + \ldots + a_n \cdot w_n - (b_1 \cdot u_1 + \ldots b_t \cdot u_t)$, ossia una combinazione lineare di vettori di $B_k \cup H$, che è una base di V, quindi tutti i coefficienti a_i sono uguali a 0. ■

4.1.4 Analogia tra cardinalità e dimensione

Sia Γ un insieme di cardinalità $|\Gamma| = n$, e sia V uno spazio vettoriale su $\mathbb{K}$ di dimensione $\dim V = n$. $(\mathbb{P}(\Gamma), \subseteq)$ è un reticolo. Anche $(\mathscr{S}(V), \subseteq)$ è un reticolo. L'inf nel primo è l'intersezione, il sup è l'unione.

Nel secondo caso l'inf di due sottospazio è $W \cap U = W \wedge U$, mentre il sup è $W + U = W \vee U$.

La cardinalità di un sottoinsieme $A \subseteq \Gamma$ è $|\emptyset| = 0 \leq |A| \leq n = |\Gamma|$.

Negli spazi vettoriali, $\dim\{\underline{0}\} = 0 \leq \dim W \leq n = \dim V$.

L'unico sottospazio di dimensione n è lo spazio stesso.

Un'applicazione qualunque, ossia un morfismo di insiemi, abbiamo la stessa analogia con gli spazi vettoriali. Consideriamo un altro insieme Γ' con cardinalità $|\Gamma| = |\Gamma'|$. Consideriamo l'applicazione $f : \Gamma \to \Gamma'$. In questo caso f è iniettiva $\Leftrightarrow$ f è suriettiva. Stessa cosa vale con le applicazioni lineari fra spazi vettoriali con la stessa dimensione, ossia $L : V \to V'$ con $\dim V = \dim V'$. L è iniettiva $\Leftrightarrow$ L è suriettiva, per la formula vista prima.

Nel primo caso $\dim V = \dim \ker L + \dim Im_L$, essendo iniettiva $\dim \ker L = 0$, quindi $\dim Im_L = \dim V = \dim V'$. Viceversa, se è suriettiva $\dim Im_L = \dim V' = n$, quindi $\dim \ker L$ necessariamente è 0.

Se $|\Gamma'| > |\Gamma|$, non esistono funzioni suriettive, e al contrario se $|\Gamma'| < |\Gamma|$ non esistono funzioni iniettive. Vale lo stesso con gli spazi vettoriali: se $\dim V < \dim V'$, non esistono applicazioni lineari iniettive $L : V \to V'$, e se invece $\dim V > \dim V'$ non esistono applicazioni lineari suriettive $L : V \to V'$.

Nel primo caso $n = \dim V < \dim \ker L + \dim Im_L$, con $\dim Im_L = m > n$. La dimensione è sempre un numero positivo. Nel secondo caso:

$$n = \dim V > \underbrace{\dim \ker L}_{0} + \dim Im_L, \text{ con } \dim Im_L = m < n$$

La cardinalità del sup di due insiemi è $|A \cup B| = |A| + |B| - |A \cap B|$, che vista dal punto di vista del reticolo è $|A \vee B| = |A| + |B| - |A \wedge B|$. Negli spazi vettoriali, invece vediamo che:

$$\dim(W + U) = \dim U + \dim W - \dim(U \cap W)$$

Questa sopra è detta formula di Grassmann.

L'applicazione che a un sottoinsieme A di Γ associa la sua cardinalità, $A \mapsto |A|$, è un'applicazione $\mathbb{P}(\Gamma) \to \mathbb{N}$, è analoga all'applicazione che a un sottospazio W di V associa la sua dimensione, $W \mapsto \dim W$, ossia $\mathscr{S}(V) \to \mathbb{N}$.

Nell'insieme delle parti, l'applicazione conta il numero di elementi massimale che va da $\emptyset$ a A diminuito di 1, ossia parte dall'insieme vuoto e aggiunge un elemento:

$$\emptyset \subset \{1\} \subset \{1, 2\} \subset \{1, 2, 3\} \subset A$$

Con $A = \{1, 2, 3, 4\}$.

Allo stesso modo si può costruire una catena massimale che aggiunge un vettore alla volta fino ad ottenere la base di un sottospazio.

$$\{\underline{0}\} \subset \{e_1\} \subset \cdots \subset \dim W$$

Questi sono reticoli dotati di funzioni "rango", che vanno dal reticolo in $\mathbb{N}$, e che contano le catene. Ossia associano a ogni elemento del reticolo la cardinalità della catena massimale diminuita di 1.

Dimostrazione della formula di Grassmann:

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

$U + W$ è definito come:

$$U + W = \sum(U \cup W) = \{v = u + w : u \in U, w \in W\}$$

Se $U \cap W = \underline{0} \Rightarrow (B_U \cup B_W)$ è una base di $U + W$.

Altrimenti, se $U \cap W \neq \underline{0}$, con $\dim U = h$ e $\dim W = k$, sia $B = \{e_1, \ldots, e_t\}$ una base di $U \cap W$. Prendiamo una base di U, $B_U \supset B$, $B_U = \{e_1, \ldots, e_t, u_{t+1}, \ldots, u_h\}$, e allo stesso modo prendiamo una base di W, $B_W \supset B$, $B_W = \{e_1, \ldots, e_t, w_{t+1}, \ldots, w_k\}$. Come è la base della somma? Deve avere dimensione $h + k - t$. Dimostriamo quindi che $B_U \cup \{w_{t+1}, \ldots, w_k\}$ è una base di $U + W$.

Che sia un sistema di generatori è banale: ogni vettore di U si scrive come combinazione lineare di vettori di B_U, e ogni vettore di W si scrive come combinazione lineare di vettori di $B_U \cup \{w_{t+1}, \ldots, w_k\}$, essendo gli elementi di B contenuti in B_U.

Vediamo che è proprio una base, quindi è indipendente.

$$\underline{0} = \underbrace{a_1 \cdot e_1 + \ldots + a_t \cdot e_t + a_{t+1} \cdot u_{t+1} + \ldots + a_h \cdot u_h}_{\in U} + \underbrace{b_{t+1} \cdot w_{t+1} + \ldots + b_k \cdot w_k}_{\in W}$$

Quindi:

$$v = a_1 \cdot e_1 + \ldots + a_t \cdot e_t + a_{t+1} \cdot u_{t+1} + \ldots a_h \cdot u_h = -(b_{t+1} \cdot w_{t+1} + \ldots + b_k \cdot w_k) \in U \cap W$$

Appartenendo all'intersezione, possiamo scriverlo come combinazione lineare di elementi della base dell'intersezione:

$$v = c_1 \cdot e_1 + \ldots + c_t \cdot e_t = -(b_{t+1} \cdot w_{t+1} + \ldots + b_k \cdot w_k)$$

Quindi:

$$\underline{0} = c_1 \cdot e_1 + \ldots + c_t \cdot e_t + b_{t+1} \cdot w_{t+1} + \ldots + b_k \cdot w_k$$

Tutti i coeficienti quindi sono 0 e tutti i vettori sono indipendenti. ■

4.2 Rappresentazione di applicazioni lineari (con matrici)

Consideriamo la matrice seguente.

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in \mathfrak{M}_{3,4}(\mathbb{R})$$

La matrice A individua un'applicazione lineare $L_A : \mathbb{R}^4 \to \mathbb{R}^3$.

$$L_A\left(\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}\right) = A \times \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}$$

Per il prodotto fra matrici, $A_{3,4} \times X_{4,1} = B_{3,1}$.

$$\begin{pmatrix} 1 & 0 & 2 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 1 \cdot x + 0 \cdot y + 2 \cdot z + 1 \cdot t \\ 1 \cdot x + 1 \cdot y + 0 \cdot z + 0 \cdot t \\ 0 \cdot x + 1 \cdot y + 1 \cdot z + 1 \cdot t \end{pmatrix}$$

Quindi, ad esempio:

$$L\left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$$

Si vede subito che questa applicazione è un'applicazione lineare, per le proprietà del prodotto tra matrici.

$$L_A(X + Y) = A \times (X + Y) = A \times X + A \times Y$$
$$L_A(k \cdot X) = A \times (k \cdot X) = k \cdot A \times X = k \cdot L_A(X)$$

Dove vanno a finire i vettori della base canonica?

$$L_A\left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = A^1 \qquad \text{(la prima colonna di } A\text{)}$$

$$L_A\left(\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = A^2 \qquad \text{(la seconda colonna di } A\text{)}$$

$$L_A\left(\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = A^3 \qquad \text{(la terza colonna di } A\text{)}$$

$$L_A\left(\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = A^4 \qquad \text{(la quarta colonna di } A\text{)}$$

In generale $L_A(e_n) = A^n$, ossia l'n-esimo vettore della base canonica mi dà la colonna n-esima. Quindi:

$$L_A(X) = A \times X = A^1 \cdot x + A^2 \cdot y + A^3 \cdot z + A^4 \cdot t$$

Se in generale moltiplico per una matrice colonna con n elementi $(x_1, \ldots, x_n)$:

$$L_A(X) = A \times X = A^1 \cdot x_1 + \cdots + A^n \cdot x_n$$

Funziona anche al contrario, ossia è possibile passare da un'applicazione lineare ad una matrice. Consideriamo la seguente applicazione lineare $L : \mathbb{R}^3 \to \mathbb{R}^2$:

$$L\left(\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right) = \begin{pmatrix} 2x + y \\ z \end{pmatrix}$$

Quest'applicazione è un'applicazione L_A individuata da una matrice:

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Le colonne sono i valori che la matrice assume nei vettori della base canonica.

$$L\left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$
$$L\left(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
$$L\left(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quindi ogni matrice $A_{m\times n} \in \mathfrak{M}_{m\times n}(\mathbb{K})$ individua un'applicazione lineare $L_A : \mathbb{K}^n \to \mathbb{K}^m$, definita come:

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad L_A(X) = A \times X = A^1 \cdot x_1 + \ldots + A^n \cdot x_n$$

E viceversa ogni applicazione lineare $L : \mathbb{K}^n \to \mathbb{K}^m$ individua una matrice A in cui l'i-esima colonna $A^i = L(e_i)$, con e_i l'i-esimo elemento della base canonica di $\mathbb{K}^n$.

Una matrice $A_{m\times n}$ individua m righe $A_1 \ldots A_m$, e ciascuna riga è un elemento di $\mathbb{K}^n$. Identicamente ciascuna delle n colonne $A^1 \ldots A^n$ è un elemento di $\mathbb{K}^m$.

Lo spazio generato dalle colonne, $< A^1 \ldots A^n >$ è un sottospazio di $\mathbb{K}^m$, mentre lo spazio generato dalle righe $< A_1 \ldots A_m >$ è un sottospazio di $\mathbb{K}^n$.

Lo spazio generato dalle colonne della matrice è l'immagine dell'applicazione L_A.

$$< A^1 \ldots A^n >= Im_{L_A}$$

Si può prendere anche una base qualunque B, non obbligatoriamente una base canonica.

Riprendiamo l'applicazione $L : \mathbb{R}^3 \to \mathbb{R}^2$ di prima.

$$L\left(\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right) = \begin{pmatrix} 2x + y \\ z \end{pmatrix}$$

La matrice associata alla base canonica è:

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Possiamo associarci un'altra matrice cambiando base. Ad esempio, prendiamo la base di $\mathbb{R}^3$ $B = \{(1,1,0),(0,0,1),(0,1,1)\}$. Possiamo calcolare L nei vettori della base, e ottenere una nuova matrice:

$$L\left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$$
$$L\left(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$L\left(\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$A_B = \begin{pmatrix} 3 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Esempio :

Consideriamo gli spazi vettoriali $V = \mathbb{R}_3[x]$ e $V' = \mathfrak{M}_2(\mathbb{R})$, e la base canonica $B_c = \{1, x, x^2, x^3\}$ di V. L'applicazione è definita come:

$$L(1) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$$
$$L(x) = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix}\right)$$
$$L(x^2) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$$
$$L(x^3) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$$

L'immagine di un generico polinomio $p(x)$ è:

$$\begin{aligned} L(p(x)) &= L(a_0 + a_1 \cdot x + a_2 \cdot x^2 + a_3 \cdot x^3) = \\ &= a_0 \cdot L(1) + a_1 \cdot L(x) + a_2 \cdot L(x^2) + a_3 \cdot L(x^3) = \\ &= a_0 \cdot \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right) + a_1 \cdot \left(\begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix}\right) + a_2 \cdot \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) + a^3 \cdot \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) = \\ &= \begin{pmatrix} a_0 + a_3 & a_0 + a_3 \\ a_1 + a_3 & a_1 + a_3 \end{pmatrix} \end{aligned}$$

Cambiamo base. Possiamo prendere un'altra base semplicemente cambiando l'ordine, ossia considerare $B = \{x, x^3, 1, x^2\}$. Le coordinate di un generico vettore rispetto alla base canonica sono (a_0, a_1, a_2, a_3). Rispetto alla nuova base, le coordinate sono (a_1, a_3, a_0, a_2). L'applicazione è identica, ma stavolta va scritta come:

$$L(a_1, a_3, a_0, a_2) = a_1 \cdot L(x) + a_3 \cdot L(x^3) + a_0 \cdot L(1) + a_2 \cdot L(x^2)$$

Le basi sono insiemi ordinati. Alle n coordinate $(x_1, \ldots, x_n)$ devo sapere quale elemento della base associare.

Ad una matrice $A_{m \times n} \in \mathfrak{M}_{m \times n}(\mathbb{K})$, con in genere $\mathbb{K} = \mathbb{R}$, possiamo associare un'applicazione lineare $L_A : \mathbb{K}^n \to \mathbb{K}^m$ tale che:

$$L_A(X) = A_{m \times n} \times X_{n \times 1} = B_{m \times 1} \in \mathbb{K}^n \text{ con } X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

L_A è lineare per le proprietà del prodotto tra matrici.

Abbiamo visto che:

$$L_A(X) = A \times X = A^1 \cdot x_1 + \ldots + A^n \cdot x_n$$

Data una base canonica $B_c = \{e_1, \ldots, e_n\}$, l'immagine dell'$i$-esimo elemento $L(e_i) = A^i$ è l'i-esima colonna.

Viceversa data un'applicazione lineare $L : \mathbb{K}^n \to \mathbb{K}^m$, esiste un'unica matrice A tale che $L = L_A$, ed è l'unica matrice le cui colonne sono le coordinate delle immagini dei vettori della base canonica di $\mathbb{K}^n$.

$$A^i = L(e_i)$$

Vediamo come funziona su campi $\mathbb{K}$ qualsiasi. Consideriamo un'applicazione lineare $L : V \to V'$, e due basi B e B', rispettivamente di V e di V'. $B = \{e_1, \ldots, e_n\} \Rightarrow \dim V = n$, e $B' = \{e'_1, \ldots, e'_m\} \Rightarrow \dim V' = m$. L'immagine di un generico $v \in V$ è:

$$L(v) = L(x_1 \cdot e_1 + \ldots + x_n \cdot e_n)$$

$(x_1, \ldots, x_n)$ è la n-upla delle coordinate rispetto a B. Il vettore v si può anche scrivere come prodotto $B \times X$:

$$v = \begin{pmatrix} e_1 & \ldots & e_n \end{pmatrix} \times \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 \cdot e_1 + \ldots + x_n \cdot e_n$$

Anche un vettore $v' \in V'$ si può scrivere come la sua base per le sue coordinate, ossia $v' = B' \times X'$.

Le immagini degli elementi della base canonica saranno:

$$\begin{aligned} L(e_1) &= a_{1,1} \cdot e'_1 + \ldots + a_{m,1} \cdot e'_m = B' \times A^1 \\ &\vdots \\ L(e_n) &= a_{1,n} \cdot e'_1 + \ldots + a_{m,n} \cdot e'_m = B' \times A^n \end{aligned}$$

La matrice associata a L è la matrice A che ha per colonne le coordinate delle immagini dei vettori della base B di V rispetto alla base B' di V'. Tornando all'esempio di prima:

$$\begin{aligned} L(v) &= x_1 \cdot L(e_1) + \ldots + x_n \cdot L(e_n) = \\ &= x_1 \cdot B' \times A^1 + \ldots + x_n \cdot B' \times a^n = \\ &= B' \times (x_1 \cdot A^1 + \ldots + x_n \cdot A^n) = \\ &= B' \times A \times X = B' \times X' \qquad (A \times X = X') \end{aligned}$$

Esempio :

$V = \mathbb{R}_2[x]$, $V' = \mathbb{R}^4$. Come base di $\mathbb{R}_2[x]$ prendiamo $B = \{1, 1-x, 1-x^2\}$, mentre come base di V' prendiamo la base canonica. Troviamo la matrice A associata ad un'applicazione lineare $L : V \to V'$ e alle basi B e B'_c.

$$A_{4\times 3} = M^B_{B'_c}(L) = (A^1 A^2 A^3)$$

Dove A^1 sono le coordinate di $L(1)$, A^2 sono le coordinate di $L(1-x)$, e A^3 sono le coordinate di $L(1-x^2)$.

$$\begin{aligned} L(1) &= (0, 1, 0, 0) \\ L(1-x) &= (0, 1, 0, -1) \\ L(1-x^2) &= (-1, 0, -1, -1) \end{aligned}$$

L'immagine di un polinomio generico rispetto alla base B scelta è:

$$L(a_0 + a_1 \cdot x + a_2 \cdot x^2) = (a_2, a_2 + a_0, a_2, a_2 + a_1)$$

La matrice associata all'applicazione quindi è:

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

L'immagine di un generico vettore $p(x)$ è:

$$L\left(p(x)\right) = B' \times A \times X$$

B' è la base di arrivo, X sono le coordinate del vettore rispetto alla base di partenza, e A è la matrice che esprime l'applicazione lineare. Bisogna esprimere il vettore $p(x)$ rispetto alla base scelta. Prendiamo il vettore $p(x) = 2 - 2x + x^2 = 1(1) + 2(1-x) - 1(1-x^2)$. Le sue coordinate sono quindi:

$$\begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}$$

E la sua immagine è:

$$L\left(\begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}\right) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 1 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & -1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ 1 \\ -1 \end{pmatrix}$$

Proviamo a cambiare anche la base di V'. $B' = \{(1,1,1,0), (1,1,0,0), (1,0,0,0), (0,0,0,1)\}$. Dobbiamo trovare la matrice associata a queste due basi, adesso.

$$\bar{A} = M^B_{B'}(L)$$

Sempre lo stesso discorso: le colonne della matrice sono le coordinate delle immagini dei vettori della base B rispetto ai vettori della base B'. Sappiamo le immagini degli elementi di B rispetto alla base canonica B'_c. Le immagini vanno ora espresse rispetto alla nuova base B'. Si vede a occhio che le immagini rispetto a B' sono le seguenti:

$$L(1) = (0,1,0,0) = B' \times \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$$

$$L(1-x) = (0,1,0,-1) = B' \times \begin{pmatrix} 0 \\ 1 \\ -1 \\ -1 \end{pmatrix}$$

$$L(1-x^2) = (-1,0,-1,-1) = B' \times \begin{pmatrix} -1 \\ 1 \\ -1 \\ -1 \end{pmatrix}$$

Quindi:

$$\bar{A} = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 1 & 1 \\ -1 & -1 & -1 \\ 0 & -1 & -1 \end{pmatrix}$$

Riprendiamo il polinomio $p(x) = 2 - 2x + x^2 = 1(1) + 2(1-x) - 1(1-x^2)$ e troviamo il suo trasformato. Le sue coordinate per la matrice $\bar{A}$ mi danno le coordinate del suo trasformato *rispetto alla nuova base di* V', non rispetto alla base canonica di V'.

$$\bar{A} \times \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ -2 \\ -1 \end{pmatrix}$$

Quindi l'immagine del nostro $p(x)$ è:

$$L(p(x)) = 1 \cdot (1,1,1,0) + 2 \cdot (1,1,0,0) - 2 \cdot (1,0,0,0) + 1 \cdot (0,0,0,1) = (1,3,1,-1)$$

Che è l'immagine di prima.

4.2.1 Spazio vettoriale delle applicazioni lineari

Indichiamo con $\hom(V, V')$ lo spazio vettoriale delle applicazioni lineari da V in V', descriviamo un'applicazione $\varphi^B_{B'} : \hom(V, V') \to \mathfrak{M}_{m\times n}(\mathbb{K})$ dallo spazio vettoriale delle applicazioni lineari allo spazio vettoriale delle matrici:

$$L : V \to V' \mapsto \varphi^B_{B'}(L) = M^B_{B'}$$

La dimensione $\dim \hom(V, V')$ è $m \times n$, dove le dimensioni degli spazi sono $\dim V = n$ e $\dim V' = m$.

Invece di fare calcoli con le n-uple facciamo calcoli con le matrici.

Il nucleo $\ker L$ è l'insieme dei vettori v tali che $L(v) = \underline{0}$, quindi:

$$\ker L = \{v = B \times X : A \times X = 0\}$$

Dato un vettore $v' \in Im_L$, per controllare se c'è abbiamo un X' tale per cui $v' = B' \times X'$, dobbiamo solo controllare se X' è uguale a $A \times X$.

φ è un isomorfismo. Il suo $\ker \varphi = \{\underline{0}\}$, e l'$Im_\varphi = \mathfrak{M}_{m\times n}(\mathbb{K})$ è tutto lo spazio delle matrici.

4.2.2 Altre proprietà delle applicazioni lineari come matrici

Data un'applicazione lineare $L : V \to V'$, la matrice associata all'applicazione L rispetto alle basi B e B' (rispettivamente di V e di V'), indicata con $M^B_{B'}(L)$, è la matrice A le cui colonne $A^1, \dots A^n$ sono le coordinate rispetto a B' di $L(e_1), \dots L(e_n)$, con $B = \{e_1, \dots, e_n\}$.

$$L(e_i) = B' \times A^i \ \forall \ i = 1, \dots n$$

L'immagine di un vettore è:

$$L(v) = B' \times (A \times X)$$

$A \times X$ è la colonna delle coordinate di $L(v)$ rispetto a B'.

Consideriamo ora le applicazioni lineari $L : V \to V'$ e $L' : V' \to V''$, e le basi B, B' e B'' degli spazi V, V' e V''. Creiamo l'applicazione lineare composta:

$$L' \circ L : V \to V''$$

La matrice associata alla composta è il prodotto delle matrici associate.

$$M^{B'}_{B''}(L') \times M^B_{B'}(L) = M^B_{B''}(L' \circ L)$$

Sia $L : V \to V'$ un isomorfismo, ossia L è iniettiva e $\dim V = \dim V'$, L ha un'inversa $L^{-1} : V' \to V$. Le loro matrici associate sono:

$$M^B_{B'}(L) \times M^{B'}_B(L^{-1}) = I = M^{B'}_B(L^{-1}) \times M^B_{B'}(L)$$

4.3 Cambiamento di base

Prendiamo uno spazio vettoriale V di dimensione $\dim V = n$, e due basi di V, B e B'. Un vettore $v \in V$ si può scrivere rispetto a entrambi le basi. $v = B \times X$, con X a indicare la colonna delle coordinate di v rispetto a B, e $v = B' \times X'$, con X' a indicare la colonna delle coordinate di v rispetto a B'.

Come si può esprimere X' in funzione di X? Ossia, ho le coordinate X rispetto a B, posso trovare le coordinate X' rispetto a B'? Viene molto facile usando le matrici associate alle applicazioni lineari.

Consideriamo l'applicazione identità, $id : V \to V$, tale per cui $id(v) = v$. Prendiamo due basi differenti B e B' di V. La matrice associata $M^B_{B'}(id)$ avrà per colonne le coordinate di $e_1, \dots e_n \in B$ rispetto a B'.

$$v = id(v) = B' \times M^B_{B'}(id) \times X$$

Quindi, sapendo che $v = B \times X = B' \times X'$, segue che $X' = M^B_{B'}(id) \times X$.

$X' = P \times X$, con $P = M^B_{B'}(id)$, e quindi $P^{-1} = M^{B'}_B(id)$.

Esempio :

Siamo in $\mathbb{R}^2$. Consideriamo le basi:

$$\begin{aligned} B &= \{(1,0),(0,1)\} \\ B' &= \{(1,1),(1,2)\} \\ v &= (x,y) \in \mathbb{R}^2 \\ v &= x \cdot e_1 + y \cdot e_2 = B \times \begin{pmatrix} x \\ y \end{pmatrix} = B' \times \begin{pmatrix} x' \\ y' \end{pmatrix} \end{aligned}$$

Bisogna trovare la matrice associata alla funzione identità $id : \mathbb{R}^2 \to \mathbb{R}^2$ rispetto alle basi B e B'.

$$A = M^B_{B'}(id) = A^1 A^2$$

Le colonne sono le coordinate dei vettori della base B rispetto alla base B'. La prima colonna è:

$$e_1 = (1,0) = a_{1,1} \cdot e'_1 + a_{2,1} \cdot e'_2 = 2 \cdot (1,1) - 1 \cdot (1,2) \Rightarrow A^1 = \begin{pmatrix} 2 \\ -1 \end{pmatrix}$$

Per la seconda colonna, sapendo che $e_2 = B' \times A^2$, vediamo che è:

$$e_2 = (0,1) = a_{1,1} \cdot e'_1 + a_{2,1} \cdot e'_2 = -1 \cdot (1,1) + 1 \cdot (1,2) \Rightarrow A^2 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

Quindi:

$$A = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$$

Se ora prendo un vettore $w = (3,2)$, per trovare le sue coordinate rispetto alla base B', bisogna moltiplicare la matrice A per la colonna delle coordinate di w.

$$\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \times \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 4 \\ -1 \end{pmatrix}$$

Infatti $(3,2) = 4(1,1) - 1(1,2) = (4,4) - (1,2)$.

Esempio :

Un esempio più complicato.

$\mathbb{R}_2[x]$ è lo spazio vettoriale dei polinomi di grado minore o uguale a 2. $\dim \mathbb{R}_2[x] = 3$. La base canonica è $B_c = \{1, x, x^2\}$. Cambiamo base, e passiamo a $B' = \{2 + x + x^2, -x + 2x^2, 2 + x\}$.

Un vettore qualunque $v = p(x) = a + bx + cx^2$, si scrive rispetto alla base canonica come:

$$p(x) = B_c \times \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

Dobbiamo trovare la matrice associata all'identità rispetto alle due basi. $M_{B'}^{B_c}(id) = A$. Le sue colonne sono A^1, A^2, A^3.

$$e_1 = B' \times A^1$$
$$e_2 = B' \times A^2$$
$$e_3 = B' \times A^3$$

Esprimiamo i vettori della base canonica rispetto alla nuova base:

$$1 = a' \cdot (2 + x + x^2) + b' \cdot (-x + 2x^2) + c' \cdot (2 + x) \to (-1, 1/2, 3/2)$$
$$x = a' \cdot (2 + x + x^2) + b' \cdot (-x + 2x^2) + c' \cdot (2 + x) \to (2, -1, -2)$$
$$x^2 = a' \cdot (2 + x + x^2) + b' \cdot (-x + 2x^2) + c' \cdot (2 + x) \to (1, 0, -1)$$

La matrice quindi è:

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

Se ora vogliamo conoscere le coordinate del vettore $v = 2 + x^2$ rispetto alla base nuova:

$$\begin{pmatrix} -1 & 2 & 1 \\ 1/2 & -1 & 0 \\ 3/2 & -2 & -1 \end{pmatrix} \times \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 2 \end{pmatrix}$$

Quindi:

$$2 + x^2 = -1 \cdot (2 + x + x^2) + (-x + 2x^2) + 2 \cdot (2 + x)$$

4.4 Diagonalizzazione

Sia $L : V \to V$ un endomorfismo. Di solito con gli endomorfismi si lavora con matrici associati a una sola base.

$$M_B(L)$$

Prendendo un'altra base B', si può associare un'altra matrice alla stessa applicazione lineare, ma rispetto alla nuova base.

$$M_{B'}(L)$$

Le colonne di $A = M_B(L)$ sono le coordinate delle immagini dei vettori di B rispetto alla stessa base B.

$$B \times A^i = L(e_i)$$
$$B' \times A'^i = L(e'_i)$$

Che relazione c'è tra A e A'? Sono due matrici associate allo stesso endomorfismo, ma rispetto a due basi diverse.

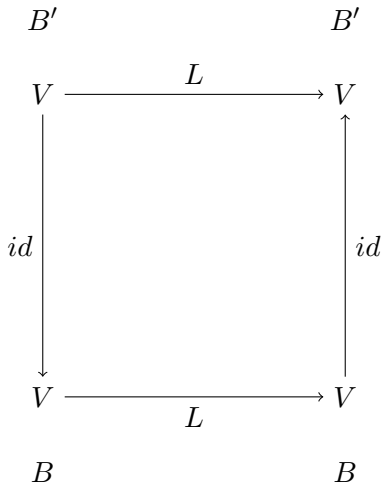

Figura 4.1: L rispetto a B' come composta di due cambi di base con L rispetto a B

$$L = id \circ L \circ id$$

Remember: la matrice associata alla composta è la composta delle matrici.

$$M_{B'}(L) = M^B_{B'}(id) \times M_B(L) \times M^{B'}_B(id)$$

Abbiamo visto che $M^{B'}_B(id)$ e $M^B_{B'}(id)$ sono l'una l'inversa dell'altra. Chiamiamo $P = M^{B'}_B(id)$. Segue che:

$$A' = P^{-1} \times A \times P$$

Questo è il legame tra le due matrici associate alla stessa applicazione lineare.

Definizione 4.4.1 (*Relazione di similitudine*)

Due matrici quadrate A e A' si dicono "simili" se soddisfano questa condizione, ossia se esiste una matrice invertibile P (quadrata e dello stesso ordine) tale che:

$$A' = P^{-1} \times A \times P$$

La relazione ρ per cui $A \rho A' \Leftrightarrow A$ è simile a A', è una relazione di equivalenza: è riflessiva (A è simile a sé stessa), è simmetrica ($A = P \times A' \times P^{-1}$), e banalmente è transitiva.
Vale anche il viceversa: se due matrici sono simili, rappresentano lo stesso endomorfismo rispetto a basi diverse.

Dimostrazione del viceversa: $L : V \to V$ è un endomorfismo, e A è la matrice associata a L rispetto a B. Prendiamo poi una matrice A' simile ad A. La tesi è che A' rappresenta lo stesso morfismo rispetto a un'altra base B'.
Essendo simile, $A' = P^{-1} \times A \times P$. Ma P è:

$$P = M_B^{B'}(id)$$

La nuova base B' è proprio $B' = B \times P$.

$$A' = M_{B'}^{B}(id) \times A \times M_B^{B'}(id)$$

A' è proprio la matrice A rispetto a una nuova base B'. ■

Ci sono due problemi equivalenti:

1. Data una matrice A, esiste una matrice diagonale D simile ad A?

   $$D = P^{-1} \times A \times P$$

   Una matrice diagonale D è una matrice $D = (d_{i,j})$ tale che $d_{i,j} = 0$ se $i \neq j$.

2. Dato un endomorfismo $L : V \to V$, esiste una base B di V per cui la matrice che rappresenta L rispetto a questa base B è una matrice D diagonale?

   $$M_B(L) = D$$

Sia $L : V \to V$ un'applicazione lineare. Se la matrice diagonale D rappresenta L rispetto a $B = \{e_1, \ldots, e_n\}$, possiamo dire che:

$$B \times D^1 = B \times \begin{pmatrix} d_{1,1} \\ 0 \\ 0 \\ \vdots \end{pmatrix} = L(e_1) = d_{1,1} \cdot e_1$$

In generale:

$$L(e_n) = d_{n,n} \cdot e_n$$

Definizione 4.4.2

Sia $L : V \to V$ un endomorfismo, un vettore $v \in V$ con $v \neq \underline{0}$ si dice autovettore *di L se $\exists\ \lambda \in \mathbb{K}$ tale che $L(v) = \lambda \cdot v$, ossia l'immagine di v è un suo multiplo.*

Se D è una matrice diagonale che rappresenta L rispetto alla base B, B è una base di autovettori. Viceversa, se esiste una base B di V formata da autovettori di L, allora la matrice associata a L rispetto a B è diagonale.

Sia v un autovettore di L, ossia tale per cui $L(v) = \lambda \cdot v$, λ si dice *autovalore* di L.

Un autovalore di L è uno scalare tale per cui esiste un vettore v la cui immagine è l'autovalore moltiplicato per il vettore v.

λ può essere 0: quando λ è 0, il vettore v va nel vettore nullo. Quindi L non è un'applicazione iniettiva.

$\lambda = 0$ è un autovalore di $L \Leftrightarrow \ker L \neq \{\underline{0}\} \Leftrightarrow L$ non è iniettiva.

Se L non è iniettiva, allora tutti i vettori $v \neq \underline{0}$ di $\ker L$ sono autovettori di autovalore 0.

Come si trovano gli autovalori e gli autovettori di un endomorfismo (e quindi della matrice associata all'endomorfismo)?

Consideriamo $L : V \to V$ e la base B. Abbiamo la matrice A associata a L rispetto a questa base, ossia $A = M_B(L)$.

$$\begin{aligned} L(v) &= \lambda \cdot v \Rightarrow \\ L(v) &= \lambda \cdot id(v) \Rightarrow \\ (L - \lambda \cdot id)(v) &= \underline{0} \Rightarrow \\ (A - \lambda \cdot I) &= M_B(L - \lambda \cdot id) \end{aligned}$$

Quindi, se $v = B \times X$, ossia X sono le coordinate di v rispetto alla base B, si ha che:

$$(A - \lambda \cdot I) \times X = \underline{0}$$

Se v esiste, allora X è soluzione non nulla di questo sistema. Se il $\det(A - \lambda \cdot I) \neq 0$, abbiamo che $X = \underline{0}$, quindi deve essere il determinante $\det(A - \lambda \cdot I) = 0$.

Gli autovalori di L sono gli zeri del polinomio $\det(A - \lambda \cdot I)$, detto anche polinomio caratteristico.

Una volta trovati gli autovalori, come si trovano gli autovettori? Risolvendo il sistema $(A - \lambda \cdot I) \times X = \underline{0}$.

Prendendo un'altra matrice A' associata a L rispetto a un'altra base, questa ha lo stesso polinomio caratteristico.

$$\det(A - \lambda \cdot I) = \det\left(A' - \lambda \cdot I\right)$$

Il polinomio caratteristico di L è un invariante di L, ossia se A' è un'altra matrice associata a L, si ha che $\det(A - \lambda \cdot I) = \det(A' - \lambda \cdot I)$.

Dimostrazione: A' rappresenta lo stesso endomorfismo L rappresentato da A. $A' = P^{-1} \times A \times P$.

$$\begin{aligned} \det(A' - \lambda \cdot I) &= \det\left(P^{-1} \times A \times P - \lambda \cdot I\right) = \\ &= \det\left(P^{-1} \times A \times P - \lambda \cdot P^{-1} \times P\right) = && \text{(si può mettere in evidenza)} \\ &= \det\left(P^{-1} \times (A - \lambda \cdot I) \times P\right) = && \text{(per Binet)} \\ &= \det\left(P^{-1}\right) \cdot \det(A - \lambda \cdot I) \cdot \det(P) = \\ &= \frac{1}{\det(P)} \cdot \det(A - \lambda \cdot I) \cdot \det(P) = \det(A - \lambda \cdot I) \end{aligned}$$

■

Data una matrice A, λ è autovalore di A se $A \times X = \lambda \cdot X$.

Il polinomio caratteristico di A è $\det(A - \lambda \cdot I)$. Matrici simili A e A', ossia $A \rho A'$, hanno gli stessi autovalori. *Non* hanno gli stessi autovettori: le coordinate cambiano.

L'applicazione $L : V \to V$ è diagonalizzabile, cioè esiste una matrice diagonale D che la rappresenta, se e solo se V ha una base di autovettori di L.

Autovettori relativi ad autovalori distinti sono indipendenti. Condizione sufficiente affinché $L : V \to V$ sia diagonalizzabile, è che L abbia $\dim V = n$ autovalori distinti, ossia n autovettori indipendenti.

$\det(A - \lambda \cdot I)$ è un polinomio di grado n, che quindi ammette al più n radici.

$$(A - \lambda \cdot I) = \begin{pmatrix} a_{1,1} - \lambda & \dots & a_{n,1} \\ \vdots & \ddots & \vdots \\ a_{1,n} & \dots & a_{n,n} - \lambda \end{pmatrix}$$

Quella sopra non è condizione necessaria: si possono avere meno autovalori distinti, ma avere comunque una base.

Dato un autovalore λ, con $E(\lambda)$ si indica l'insieme degli autovettori di autovalore λ, più il vettore nullo.

$$E(\lambda) = \{v \in V : L(v) = \lambda \cdot v\}$$

$E(\lambda)$ è un sottospazio di V, e si dice autospazio relativo all'autovalore λ.

Ciascun autovalore $\lambda_1, \dots \lambda_t$ avrà un suo autospazio $E(\lambda_i)$, e ciascun autospazio avrà una base B_i, con dimensione $\dim E(\lambda_i) = n_i$. Se la somma delle dimensioni fa n, ossia:

$$\dim E(\lambda_1) + \dots + \dim E(\lambda_t) = n$$

allora L è diagonalizzabile.

Abbiamo visto che, data un'applicazione lineare $L : V \to V$, con $\dim V = n$, e due basi di V, $B = \{e_1, \dots, e_n\}$ e $B' = \{e'_1, \dots e'_n\}$, abbiamo due matrici associate a L rispetto alle due basi, ossia $M_B(L)$ e $M_{B'}(L)$.

Sapendo che $L = id \circ L \circ id$, e che, data un'applicazione composta $G = L \circ F$, la matrice associata a G è il prodotto delle matrici associate a L e a F:

$$M^B_{B''}(G) = M^{B'}_{B''}(L) \times M^B_{B'}(F)$$

Sapendo questo, dicevamo, si vede che:

$$M_{B'}(L) = M^B_{B'}(id) \times M_B(L) \times M^{B'}_B(id)$$

Due matrici A, A' si dicono simili se esiste una matrice invertibili P per cui:

$$A' = P^{-1} \times A \times P$$

Proposizione 4.4.1

A e $A' \in \mathfrak{M}_n(\mathbb{K})$ sono simili $\Leftrightarrow$ rappresentano lo stesso endomorfismo rispetto a due basi diverse.

Da questa proposizione sorgono due problemi equivalenti:

1. Determinare, qualora esista, una matrice diagonale D simile a una matrice data A.
2. Determinare, qualora esista, una matrice D diagonale che rappresenta un endomorfismo L.

Dato un endomorfismo L (o una matrice A) si dice *autovettore* di L (o di A) un vettore $v \neq \underline{0}$ (nel caso della matrice, una n-upla diversa dalla n-upla nulla) tale che $\exists\ \lambda \in \mathbb{R}$ per cui $L(v) = \lambda \cdot v$. Nel caso della matrice, $A \times X = \lambda \cdot X$.

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = M_B(L)$$

$$B = \{v_1, v_2, v_3\}$$

$$\begin{aligned} L(v_1) &= 3 \cdot v_1 + 0 \cdot v_2 + 0 \cdot v_3 = 3 \cdot v_1 \\ L(v_2) &= v_2 \\ L(v_3) &= -v_3 \end{aligned}$$

Una matrice diagonale rappresenta L rispetto ad una base B se la base B è una base di autovettori.

Proposizione 4.4.2

Condizione necessaria e sufficiente affinché $L : V \to V$ sia diagonalizzabile è che V abbia una base di autovettori.
Con le matrici, condizione necessaria e sufficiente affinché una matrice $A \in \mathfrak{M}_n(\mathbb{R})$ sia diagonalizzabile è che in $\mathbb{R}^n$ ci sia una base composta da autovettori di A.

La matrice diagonale D ha sulla diagonale gli autovalori di L (rispettivamente di A).

Proposizione 4.4.3

Gli autovalori di L (rispettivamente della matrice A) sono gli zeri del polinomio caratteristico di L (rispettivamente di A), ossia del polinomio $\det(A - \lambda \cdot I)$.

Come si trovano gli autovettori, invece?

$$L(V) = \lambda \cdot v \Rightarrow L(V) - \lambda \cdot v = \underline{0} \Rightarrow (A \times X - \lambda \cdot X) = \underline{0} \Rightarrow (A - \lambda \cdot I) \times X = 0$$

Si risolve il sistema e si trovano gli autovettori.

4.4.1 Criterio di diagonalizzazione

Dobbiamo introdurre altre due proposizioni.

λ è un autovalore (con $\lambda \in \mathbb{R}$) $\Leftrightarrow \det(A - \lambda \cdot I) = 0$.

Quindi λ ha una molteplicità come radice del polinomio caratteristico, detta molteplicità algebrica di λ. Si indica con $m_a(\lambda)$.

Prendiamo tutti gli autovettori di autovalore λ.

$$E(\lambda) = \{v \in V : L(v) = \lambda \cdot v\}$$

$E(\lambda)$ contiene gli autovettori di L di autovalore λ, più il vettore nullo. $E(\lambda)$ è un sottospazio di V. Infatti, presi due elementi, contiene tutte le loro combinazioni lineari.

$$\begin{aligned} v, w &\in E(\lambda) \\ a \cdot v + b \cdot w &\in E(\lambda) \end{aligned}$$

Infatti $L(a \cdot v + b \cdot w) = a \cdot L(v) + b \cdot L(w) = a \cdot \lambda \cdot v + b \cdot \lambda \cdot w = \lambda \cdot (a \cdot v + b \cdot w)$.

Anche questo sottospazio, $E(\lambda)$, ha una sua dimensione, viene chiamata molteplicità geometrica, e viene solitamente indicata con $m_g(\lambda)$.

La molteplicità algebrica di λ è sempre minore o uguale di $n = \dim V$. Infatti $\det(A - \lambda \cdot I)$ ha grado n.

La molteplicità geometrica, invece, che è la dimensione $\dim E(\lambda)$, chiamato *autospazio relativo a* λ, è sempre minore o uguale della molteplicità algebrica. Quindi:

$$m_g(\lambda) \leq m_a(\lambda) \leq n$$

Infatti $\dim E(\lambda) = m_g(\lambda) = t$. La dimensione è la dimensione di una base di $E(\lambda)$, contenente t vettori. La base $B = \{v_1, \dots v_t\}$ contiene tutti vettori del tipo $L(v_i) = \lambda \cdot v_i$.

Ma $E(\lambda) \subseteq V$, ed essendo che $\dim V = n$, deve essere che $t \leq n$. Deve esserci una base $\bar{B}$ di V contenente la base B di $E(\lambda)$.

$$\bar{B} = \{v_1, \dots, v_t, w_{t+1}, \dots, w_n\}$$

La molteplicità algebrica è almeno t.

Proposizione 4.4.4

Se $v_1, \dots, v_t$ sono autovettori a due a due distinti relativi rispettivamente agli autovalori $\lambda_1, \dots, \lambda_t$ (con $\lambda_i \neq \lambda_j$ se $i \neq j$), costituiscono un insieme indipendente.

Dimostrazione: Per induzione sul numero t degli autovettori. Per $t = 1$ è vero, abbiamo un solo autovettore diverso dal vettore nullo (per definizione), che quindi costituisce un insieme indipendente.

Supponiamo il teorema vero per $t \geq 1$, e dimostriamo che è vero per $t+1$ vettori. Se fossero dipendenti, il vettore v_{t+1} apparterrebbe allo spazio generato $< v_1, \dots, v_t >$.

$$\underline{0} = a_1 \cdot v_1 + \dots + a_t \cdot v_t + a_{t+1} \cdot v_{t+1}$$

$$\begin{aligned} \underline{0} = L(\underline{0}) &= a_1 \cdot L(v_1) + \dots + a_t \cdot L(v_t) + a_{t+1} \cdot L(v_{t+1}) = \qquad \text{(essendo tutti autovettori)} \\ &= a_1 \cdot \lambda_1 \cdot v_1 + \dots + a_t \cdot \lambda_t \cdot v_t + a_{t+1} \cdot \lambda_{t+1} \cdot v_{t+1} \end{aligned}$$

Ogni λ_i, λ_j è una coppia di elementi a due a due distinti. Quindi al più un λ_i è pari a 0.

Sia v_j un vettore tale che $\lambda_j \neq 0$. Supponiamo v_j sia proprio v_{t+1}, quindi $\lambda_{t+1} \neq 0$.

Moltplicando per λ_{t+1}, si ottiene che:

$$\underline{0} = \lambda_{t+1} \cdot a_1 \cdot v_1 + \dots + \lambda_{t+1} \cdot a_{t+1} \cdot v_{t+1}$$

E inoltre ho sempre l'identità per cui:

$$\underline{0} = \lambda_1 \cdot a_1 \cdot v_1 + \dots + \lambda t + 1 \cdot a_{t+1} \cdot v_{t+1}$$

Sottraendo le due equazioni si ottiene che:

$$\underline{0} = a_1 \cdot (\lambda_{t+1} - \lambda_1) \cdot v_1 + \dots + a_t \cdot (\lambda_{t+1} - \lambda t) \cdot v_t$$

Essendo $v_1, \dots, v_t$ vettori indipendenti, e sapendo che ogni coppia λ_i, λ_j è formata da elementi distinti, e che:

$$a_1 \cdot (\lambda_{t+1} - \lambda_1) = \dots = a_t \cdot (\lambda_{t+1} - \lambda_t) = 0$$

Ogni $a_1, \dots, a_t$ deve essere a 0. λ_{t+1} si era detto essere diverso da zero, quindi anche a_{t+1} deve essere zero. ■

Proposizione 4.4.5

Le seguenti proposizioni sono equivalenti:

1. *L'applicazione lineare L è diagonalizzabile (o la matrice A è diagonalizzabile)*
2. *Esiste una base di V formata da autovettori dell'applicazione lineare L (rispettiva-*

mente della matrice A)

3. *V è somma diretta di autospazi, ossia $V = E(\lambda_1) \oplus \ldots \oplus E(\lambda_t)$, ossia ogni vettore $v \in V$ si esprime in un solo modo come somma di autovettori*
4. *Ogni autovalore di L ha molteplicità geometrica uguale a quella algebrica, e la somma delle molteplicità è:*

$$\sum_{\lambda} m_a(\lambda) = \sum_{\lambda} m_g(\lambda) = n$$

Dimostrazione: 1 implica 2 e 2 implica 1 lo abbiamo già visto.

3 implica che una base B di V si ottiene dall'intersezione $B_1 \cup \ldots \cup B_t$ dove B_i è una base di $E(\lambda_i)$. Autovettori relativi ad autovalori distinti sono indipendenti.

Le molteplicità geometriche sono le dimensioni delle basi, quindi viene subito anche la 4.

2 implica la 3, perché data una base di autovettori posso dividerli in base al loro autovalore. ■

Esempio:

Consideriamo l'applicazione lineare $T : \mathbb{R}^3 \to \mathbb{R}^3$. Si può definire un'applicazione lineare in tre modi:

1. dire quanto vale $T(x, y, z)$;
2. dire qual è la matrice A associata a T rispetto a una base B:

$$T(x, y, z) = A \times \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

   dove (x', y', z') sono le coordinate di (x, y, z) rispetto a B;
3. dire quali valori assume T sui valori di una base B, ad esempio $T(1, 1, 1)$, $T(1, 1, 0)$, $T(1, 0, 0)$.

Diciamo i valori che T assume sulla base:

$$T(1, 1, 1) = (3, 0, 6)$$
$$T(1, 1, 0) = (3, 1, 2)$$
$$T(1, 0, 0) = (2, 0, 0)$$

Si vede subito che $(1, 0, 0)$ è un autovettore di autovalore 2, infatti $T(1, 0, 0) = 2 \cdot (1, 0, 0)$.

Mettendo i valori per colonna si ha una matrice associata a T rispetto alla base B del dominio, e alla base canonica del codominio:

$$M_{B_c}^{B}(L) = A = \begin{pmatrix} 3 & 3 & 2 \\ 0 & 1 & 0 \\ 6 & 2 & 0 \end{pmatrix}$$

Bisogna trovare la matrice associata alla base B, ossia $M_B(L)$. La prima colonna di questa nuova matrice sarà la prima colonna della matrice A sopra, espressa rispetto ai vettori della base B.

$$(3, 0, 6) = a \cdot (1, 1, 1) + b \cdot (1, 1, 0) + c \cdot (1, 0, 0)$$

Se si vuole invece trovare la matrice $M_{B_c}(L)$, rispetto alla base canonica:

$$\begin{aligned}
&T(1,0,0) = (2,0,0)\\
&T(0,1,0) = T((1,1,0)-(1,0,0)) = T(1,1,0) - T(1,0,0) = (1,1,2)\\
&T(0,0,1) = (0,-1,4)
\end{aligned}$$

Quindi:

$$M_{B_c}(L) = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 2 & 4 \end{pmatrix}$$

Determiniamo gli autovalori di L.

$$\begin{aligned}
\det(A - \lambda \cdot I) &= \det\left(\begin{pmatrix} (2-\lambda) & 1 & 0 \\ 0 & (1-\lambda) & -1 \\ 0 & 2 & (4-\lambda) \end{pmatrix}\right) = \\
&= (2-\lambda)\cdot\left[\det\left(\begin{pmatrix} (1-\lambda) & -1 \\ 2 & (4-\lambda) \end{pmatrix}\right)\right] = \\
&= (2-\lambda)\cdot[(1-\lambda)\cdot(4-\lambda)+2] = (\lambda-2)^2\cdot(\lambda-3)
\end{aligned}$$

Quindi ha due autovalori: $\lambda_1 = 2$ e $\lambda_2 = 3$. Le molteplicità algebriche sono $m_a(2) = 2$, e $m_a(3) = 1$.

Troviamo gli autospazi.

$$E(3) = \{v \in \mathbb{R}^3 : T(v) = 3 \cdot v\}$$

Tutti i $v \in E(3)$ hanno coordinate X rispetto alla base canonica che risolvono il sistema $(A - 3 \cdot I) \times X = 0$.

$$\begin{pmatrix} -1 & 1 & 0 \\ 0 & -2 & -1 \\ 0 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

È equivalente al sistema:

$$\begin{cases} -x + y = 0 \\ 2y + z = 0 \end{cases}$$

Le soluzioni sono $z = -2\,y$ e $x = y$, ossia $(x, x, -2\,x)$.

$$E(3) = \{(x, x, -2\,x) \in \mathbb{R}^3 : x \in \mathbb{R}\}$$

La sua dimensione è $\dim E(3) = 1$, quindi $E(3)$ è isomorfo a $\mathbb{R}$, e l'isomorfismo è quello che associa a un certo $y \mapsto (y, y, -2\,y)$.

$$E(3) = <(1,1,-2)>$$

Troviamo gli autovettori di autovalore 2:

$$E(2) = \{v : T(v) = 2 \cdot v\}$$

Il sistema da risolvere è:

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & -1 \\ 0 & 2 & 2 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

Anche in questo caso la dimensione $\dim E(2) = 1$, quindi T non è diagonalizzabile. Infatti:

$$m_g(2) = 1 < m_a(2) = 2$$

Sapevamo già da prima che $E(2) =< (1, 0, 0) >$.

Capitolo 5

Risoluzione di sistemi lineari

5.1 Sistemi lineari

Un'equazione lineare è una combinazione lineare in n variabili.

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n = b$$

$a_1, \ldots, a_n, b \in \mathbb{R}$. $a_1, \ldots, a_n$ sono i coefficienti, b è il termine noto. $x_1, \ldots, x_n$ sono chiamate variabili.

$$3 \cdot x_1 - 2 \cdot x_2 + x_4 = 3$$

Questa è un'equazione lineare in 4 variabili. I coefficienti sono $(3, -2, 0, 1)$. Il termine noto è 3.

Un sistema lineare è un insieme di equazioni lineari nello stesso numero di variabili.

La soluzione di un'equazione in n variabili è una n-upla $(s_1, \ldots, s_n)$ con $s_1, \ldots, s_n \in \mathbb{R}$ tale che se sostituita al posto delle variabili rende l'equazione un'identitá:

$$a_1 \cdot s_1 + \ldots a_n \cdot s_n = b$$

Risolvere un sistema lineare vuol dire trovare tutte le n-uple che soddisfano le equazioni del sistema.

5.2 Matrici a scala

Definizione 5.2.1 (*Matrice a scala*)

Indichiamo con $p_{i,j}$ il primo elemento non nullo della i-esima riga della matrice, detto anche pivot. *Una matrice si dice "a scala" (per righe) se prendendo due pivot $p_{i,j}$ e $p_{h,k}$ con $i < h \Rightarrow j < k$. Ossia, il numero di zeri in ogni riga aumenta di riga in riga.*

Data una matrice $A_{m \times n}$, le sue m righe $A_1, \ldots, A_m$ si possono vedere come elementi di $\mathbb{K}^n$, e le sue n colonne $A^1, \ldots, A^n$ si possono vedere come elementi di $\mathbb{K}^m$.

Il rango per righe di A, $r_r(A)$ è la dimensione dello spazio generato dalle righe. Il rango per colonne $r_c(A)$ è la dimensione dello spazio generato dalle colonne.

$$r_r(A) = \dim < A_1, \ldots, A_m > \leq \mathbb{K}^n$$
$$r_c(A) = \dim < A^1, \ldots, A^n > \leq \mathbb{K}^m$$

Il rango per righe di una matrice a scala per righe è il numero di righe non nulle, perché le righe non nulle di una matrice a scala per righe sono indipendenti, quindi costituiscono una base dello spazio generato.

Proposizione 5.2.1

Data una matrice S a scala per righe, il rango per riga di S è il numero di righe non zero, ossia le righe non zero di S costituiscono un insieme indipendente.

Dimostrazione: Supponiamo per assurdo che esista una combinazione lineare non banale delle righe non nulle di S che dà il vettore nullo. Consideriamo il primo coefficiente diverso da zero, ossia un certo x_i. Tutti i coefficienti prima di i sono a zero, e il coefficiente con i è il pivot $p_{i,j}$ per x_i, quindi x_i deve essere zero. Assurdo. ■

Consideriamo un sistema $S \times X = B$. Il rango per righe $r_r(S)$ è sempre minore del rango per righe $r_r(S|B)$ della matrice completa del sistema. Se il rango per righe di una matrice è minore del rango per righe della matrice completa, il sistema non ha soluzione. Inoltre il sistema ha soluzione se la matrice dei termini noti appartiene allo spazio generato dalle colonne della matrice dei coefficienti. Ossia, il rango per colonne della matrice S è uguale al rango per colonna della matrice completa $S|B$. Equivalentemente, B appartiene all'immagine Im_{L_A}.

Per trovare le soluzioni, si parte dall'ultima riga non nulla.

Il numero delle incognite meno il rango per righe dei coefficienti mi dà il numero di parametri da cui dipende la soluzione.

Un sistema a scala si dice che ha ∞^{n-t} soluzioni, dove t è il rango per riga della matrice, e n è il numero di parametri. L'insieme delle soluzioni è in corrispondenza biunivoca con $\mathbb{R}^{n-t}$.

Le variabili che hanno per coefficiente i pivot si dicono legate, le altre si dicono libere. Un sistema con il rango per righe pari a t, ha $n - t$ variabili libere.

In un sistema omogeneo $S \times X = 0$, le soluzioni sono il $\ker L_S$. Inoltre la dimensione $\ker L_S = n - t = r_r(S)$. Siccome il rango per colonne $r_c(S) = \dim Im_{L_S}$, e sapendo che $L_S : \mathbb{R}^n \to \mathbb{R}^m$, sappiamo che $n = \dim Im_{L_S} - \dim \ker L_S$. $n - r_r(S) = \dim \ker L_S$. Quindi in definitiva il rango per righe e il rango per colonne sono uguali, in una matrice a scala.

$$S \times X = B \begin{cases} L_S(X) = S \times X, L_S : \mathbb{R}^n \to \mathbb{R}^m \\ B \in Im_{L_S} \Leftrightarrow \text{ il sistema ha soluzioni } \Leftrightarrow r_c(S) = r_c(S|B) \\ S \times X = 0 \Leftrightarrow \dim \ker L_S = n - r_r(S) \\ X \in \ker L_S \end{cases}$$

Il numero delle incognite $n = r_c(L_S) + \dim \ker L$, quindi $n = r_c(L_S) + n - r_r(S)$, quindi i due ranghi sono uguali.

5.3 Risoluzione dei sistemi lineari

Un sistema lineare $S \times X = C$ a scala, ossia in cui la matrice completa $S|C$ è a scala, è compatibile se e solo se $r(S) = r(S|C)$, ossia il rango della matrice S è uguale al rango della matrice completa, poiché solo in tal caso il sistema non contiene un'equazione impossibile del tipo $0 = b$ con $b \neq 0$.

Sia $\mathscr{S}$ l'insieme delle soluzioni di un sistema lineare compatibile. Le soluzioni si ottengono a partire dall'ultima equazione non nulla e risalendo via via. Il sistema ammette ∞^{n-t} soluzioni, dove $t = r(S) = r(S|C)$ è il rango della matrice completa. L'insieme delle soluzioni $\mathscr{S}$ è in corrispondenza biunivoca con $\mathbb{K}^{n-t}$, perché alla $(n-t)$-upla di variabili libere (che non hanno fra i coefficienti un pivot) corrisponde una sola soluzione, e viceversa una soluzione corrisponde a una $(n-t)$-upla di variabili libere.

Proposizione 5.3.1

In un sistema omogeneo $S \times X = 0$, l'insieme $\mathscr{S}$ è un sottospazio di $\mathbb{K}^n$.

Infatti:

$$S \times (X + Y) = S \times X + S \times Y = 0$$

E:

$$S \times k \cdot X = k \cdot S \times X = 0$$

5.4 Risoluzione con il metodo di Gauss

Definizione 5.4.1 (*Matrici equivalenti per righe*)

Date due matrici $A, A' \in \mathfrak{M}_{m\times n}(\mathbb{K})$ sono equivalenti per righe, indicato con $A \sim_R A' \Leftrightarrow <A_1, \ldots, A_m> = <A'_1, \ldots, A'_m> \subseteq \mathbb{K}^n$, ossia se hanno lo stesso spazio generato dalle righe.

Il rango per riga di una matrice A, indicato con $r_r(A)$, è la dimensione dello spazio generato dalle righe.

$$r_r(A) = \dim <A_1, \ldots, A_m>$$

Se due matrici sono equivalenti per righe, ossia $A \sim_R A'$, allora $r_r(A) = r_r(A')$.

5.4.1 Calcolo del rango per righe di A con il metodo di Gauss

Si applicano delle operazioni elementari a una matrice A in modo da ricavare una matrice a scala per righe S equivalente per righe alla matrice A. Il rango di A è uguale al rango di S, ossia è il numero di righe non nulle di S.

$$r_r(A) = r(S) = \text{ numero di righe non nulle di } S$$

Operazioni elementari

O1 Si moltiplica una riga per uno scalare $k \neq 0$.

$$A_i \to k \cdot A_i$$

O2 Scambio di righe. Al posto della riga i mettiamo la riga j, e viceversa.

$$A_i \leftrightarrow A_j$$

O3 Si sostituisce una riga con una combinazione lineare della riga con un'altra riga. Al posto della riga A_i sostituiamo una combinazione lineare $h \cdot A_i + k \cdot A_j$, con $i \neq j$ e $h \neq k$ e $k, h \neq 0$.

$$A_i \to h \cdot A_i + k \cdot A_j$$

Si possono combinare le operazioni elementari. Lo stesso metodo si applica anche alla risoluzione di sistemi lineari.

Esempio :

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

Dobbiamo trovare una matrice a scala equivalente alla matrice A. La prima riga ha il primo elemento diverso da 0, quindi va bene, e la lasciamo in pace. Dobbiamo fare in modo che tutte le altre righe abbiano 0 sulla prima colonna. Moltiplichiamo la prima riga per 2 e la sottraiamo alla seconda riga.

$$A_2 \to -2 \cdot A_1 + A_2$$

$$\begin{array}{cccc} -2 & -2 & -4 & 2 \\ 2 & -1 & 1 & 0 \\ \hline 0 & -3 & -3 & 2 \end{array}$$

Quindi la matrice ora è:

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

Stessa operazione per l'ultima riga. $A_3 \to A_3 + A_1$.

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

Non è ancora a scala. Sostituiamo alla terza riga la somma della seconda e della terza riga. $A_3 \to A_3 + A_2$

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

Il rango della matrice finale è 3, che è anche il rango della matrice iniziale. La combinazione lineare delle righe iniziali è uguale alla combinazione lineare delle righe della matrice finale.

Osservazione 13

Se E è una matrice ottenuta dalla matrice identità $I \in \mathfrak{M}_n\mathbb{K}$ applicando una operazione elementare, allora il prodotto $E \times A = A'$ è la matrice A' ottenuta dalla matrice A applicando la stessa operazione elementare.

L'algoritmo di Gauss è quindi il prodotto di un certo numero di matrici elementari fino ad ottenere una matrice a scala.

$$E_t \times \ldots \times E_1 \times A = S$$

Dato un sistema lineare $A \times X = B$, con il metodo di Gauss si ricava un sistema a scala $S \times X = B$ equivalente al sistema dato, ossia che ammette lo stesso insieme di soluzioni.

Si parte dalla matrice completa del sistema, $A|B$. Applicando l'algoritmo di Gauss alla matrice completa si ottiene una matrice a scala $S|C$.

Esempio :

$$\begin{cases} 4x + y - 3z + 2t = 1 \\ 3x - 2y - 2z + t = -5 \\ 5x + 4y - 4z + 3t = 7 \end{cases}$$

La matrice completa di questo sistema è:

$$A|B = \left(\begin{array}{cccc|c} 4 & 1 & -3 & 2 & 1 \\ 3 & -2 & -2 & 1 & -5 \\ 5 & 4 & -4 & 3 & 7 \end{array}\right)$$

Alle operazioni elementari sulle righe della matrice completa $A|B$, corrispondono operazioni elementari sulle equazioni, che sostituiscono alle equazioni delle altre equazioni equivalenti, che portano di fatto ad un sistema equivalente.

L'operazione elementare O1 corrisponde alla sostituzione dell'equazione E_i con un'equazione equivalente $k \cdot E_i$, con $k \neq 0$. L'operazione elementare O2 corrisponde a scambiare due equazioni. L'operazione elementare O3 corrisponde alla sostituzione di un'applicazione lineare con una combinazione lineare di quell'equazione con un'altra.

$$A_2 \to -3 \cdot A_1 + 4 \cdot A_2$$

-3(4)	-3	+9	-6	-3
4(3)	-8	-8	+4	-20
0	-11	1	-2	-23

$$A_3 \to -5 \cdot A_1 + 4 \cdot A_3$$

-5(4)	-5	+15	-10	-5
4(5)	16	-16	12	28
0	11	-1	2	23

$$A = \left(\begin{array}{cccc|c} 4 & 1 & -3 & 2 & 1 \\ 0 & -11 & 1 & -2 & -23 \\ 0 & 11 & -1 & 2 & 23 \end{array}\right)$$

Si vede ora che le ultime due righe sono uguali, quindi possiamo sostituire alla terza riga la terza più la seconda. $A_3 \to A_2 + A_3 = \underline{0}$.

$$A = \left(\begin{array}{cccc|c} 4 & 1 & -3 & 2 & 1 \\ 0 & -11 & 1 & -2 & -23 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Il sistema adesso è:

$$\begin{cases} 4x + y - 3z + 2t = 1 \\ -11y + z - 2t = -23 \end{cases}$$

Ora, a partire dall'ultima equazione, trovo la variabile legata in funzione delle altre variabili.

$$y = \frac{23 + z - 2t}{11}$$

Ora troviamo la x:

$$x = \frac{2t - 23 - z}{11} + 3z - 2t + 1$$

Il sistema ammette ∞^2 soluzioni, dipendenti dalle variabili libere (z e t). 2 è il numero delle incognite (4) meno il rango (2).

Vedendo la matrice come applicazione lineare L_A, abbiamo che l'immagine di una quaterna X che è soluzione del sistema, ossia $A \times X$, è proprio la quaterna dei termini noti B.

$$L_A(X) = A \times X = B$$

Ogni soluzione si può scrivere come una particolare soluzione aggiunta agli elementi del $\ker L_A$. La soluzione particolare è quella che si ottiene assegnando 0 alle variabili libere.

$$\ker L_A + X = \mathscr{S}$$

Y è soluzione di $A \times X = B$ se, presa una soluzione particolare H, ossia tale per cui $A \times H = B$, e un elemento $K \in \ker L_A$, si ha che $Y = K + H$. Infatti $A \times Y = A \times (K + H) = A \times K + A \times H = 0 + B = B$.

Viceversa, sapendo che $A \times Y = B$ e che $A \times H = B$, possiamo dire che $A \times Y - A \times H = \underline{0}$, e che quindi $A \times (Y - H) = 0$. Quindi $K = Y - H$ è nel $\ker L_A$, e quindi $Y = K + H$.

Il rango per righe di A è uguale al rango per colonne di A. La dimensione dello spazio generato dalle righe è uguale alla dimensione delo spazio generato dalle colonne, ma non sono lo stesso spazio. Identicamente, il numero di righe indipendenti è uguale al numero di colonne indipendenti.

Dimostrazione: Nel caso in cui $A \times X = 0$.

$$\dim < A_1 \dots A_m >= r_r(A) = n - t$$

$\ker L_A = \mathscr{S} = \{X : A \times X = 0\}$ è un sottospazio di $\mathbb{K}^n$ di dimensione $n - r_r(A)$.

$$n = \dim \mathbb{K}^n = \dim Im_{L_A} = \dim \ker L_A = r_c(A) + n - r_r(A) \Rightarrow r_c(A) = r_r(A)$$

L'immagine è combinazione lineare delle colonne.

$$A \times X = A^1 \cdot x_1 + \dots + A^n \cdot x_n = B$$

■

Teorema 5.4.1 (*Teorema di Rouché-Capelli*)

Un sistema ammette soluzione se il rango della matrice dei coefficienti è uguale al rango della matrice completa.

5.5 Matrici invertibili

$(\mathfrak{M}_n(\mathbb{K}), +, \times)$ è l'anello delle matrici quadrate sul campo $\mathbb{K}$. $(\mathfrak{M}_n(\mathbb{K}), +)$ è un gruppo abeliano. $(\mathfrak{M}_n(\mathbb{K}), \times)$ (con il prodotto righe per colonne) è una struttura algebrica associativa, distributiva, con unità, ma non commutativa. L'anello delle matrici quadrate ha un gruppo degli elementi invertibili.

$$U(\mathfrak{M}_n(\mathbb{K})) = \{A \in \mathfrak{M}_n(\mathbb{K}) : \exists\ B \text{ t.c. } A \times B = I\}$$

B solitamente si indica con A^{-1}. I è la matrice identità.

5.5.1 Caratterizzazione delle matrici invertibili

Si possono caratterizzare le matrici invertibili in diversi modi. Le seguenti sono tutte affermazioni equivalenti.

1. A è invertibile
2. Il sistema omogeneo $A \times X = 0$ ammette una sola soluzione, $X = 0$
3. L'endomorfismo $L_A : \mathbb{K}^n \to \mathbb{K}^n$ definito come $L_A(X) = A \times X$ è un isomorfismo di $\mathbb{K}^n$
4. Il rango di A è $r(A) = n$
5. Il sistema $A \times X = B$ ha una sola soluzione $\forall\ B \in \mathbb{K}^n$

Dimostrazione che 1 implica 2 : A è invertibile, ossia $\exists\ A^{-1}$ tale che $A \times A^{-1} = I = A^{-1} \times A$.

$$A \times X = 0 \Rightarrow A^{-1} \times A \times X = A^{-1} \times 0 \Rightarrow X = 0$$

■

Dimostrazione che 2 implica 3 : Grazie alle proprietà distributive si vede che L_A è un morfismo:

$$A \times X + A \times Y = A \times (X + Y)$$
$$(k \cdot A) \times X = A \times (k \cdot X)$$

È un morfismo iniettivo. Infatti il $\ker L_A$ contiene tutte le soluzioni del sistema omogeneo, e l'unica soluzione è il vettore nullo. Quindi $\ker L_A = \{\underline{0}\}$, quindi la funzione iniettiva.

Tutte le applicazioni lineari iniettive da uno spazio di dimensione n a uno spazio della stessa dimensione n, sono anche suriettive. Ogni endomorfismo iniettivo è anche suriettivo.

$$\underbrace{\dim \mathbb{K}^n}_{n} = \underbrace{\dim \ker L_A}_{0} + \underbrace{\dim Im_{L_A}}_{n}$$

■

Dimostrazione che 3 implica 4 : La tesi è che $r(A) = n$.

Il rango di una matrice si può definire in molti modi. Ad esempio, come la dimensione dello spazio generato dalle righe o dalle colonne.

$$r(A) = \dim < A_1, \ldots, A_n >= \dim < A^1, \ldots A^n >$$

$Im_{L_A} = \mathbb{K}^n$, essendo L_A iniettiva. Ma $Im_{L_A} =< A^1, \ldots, A^n >$, ossia l'immagine è lo spazio generato dalle colonne. Quindi il rango è la dimensione dell'immagine, cioè n. ■

Dimostrazione che 4 implica 5 : La tesi è che $A \times X = B$ ha una sola soluzione $\forall\ B \in \mathbb{K}^n$.

Possiamo scrivere $B = A \times X$ come:

$$B = A \times X = A^1 \cdot x_1 + \ldots + A^n \cdot x_n$$

Sappiamo che il rango di A è $r(A) = \dim < A^1, \ldots, A^n >= n$. Essendo lo spazio generato dalle colonne un sottospazio di $\mathbb{K}^n$, ed essendo questo sottospazio di dimensione n, lo spazio generato dalle colonne è proprio $\mathbb{K}^n$, e ne è anche una base. B quindi si scrive come combinazione lineare di $\{A^1, \ldots, A^n\}$.

L'insieme delle colonne è una base di $\mathbb{K}^n$, quindi $\forall\ B \in \mathbb{K}^n$, B si esprime in modo unico come combinazione lineare delle colonne di A. Quindi la n-upla delle coordinate di B è l'unica soluzione del sistema $A \times X = B$. ■

Dimostrazione che 5 implica 1 : Sappiamo che $A \times X = B$ ha una sola soluzione $\forall\ B \in \mathbb{K}^n$.

$$A \times X = I^1 \Rightarrow X = B^1$$

Con $B = A^{-1}$. Si può ripetere il procedimento per le colonne, ossia in generale $A \times X = I^n \Rightarrow X = B^n$. A^{-1} è la matrice che ha per colonne $B^1 \dots B^n$, poiché $A \times B = I$. ■

5.6 Determinante di una matrice

Definizione 5.6.1 (*Determinante*)

Il determinante è una funzione $\det : \mathfrak{M}_n(\mathbb{K}) \to \mathbb{K}$. *In particolare lavoreremo con matrici sui reali, quindi* $\det : \mathfrak{M}_n(\mathbb{R}) \to \mathbb{R}$. *La funzione determinante verifica le seguenti proprietà:*

1. *Se* A' *è la matrice ottenuta da* A *moltiplicando una riga per uno scalare* $k \neq 0$, *ossia applicando l'operazione elementare O1 dell'algoritmo di Gauss, allora* $\det(A') = k \cdot \det(A)$
2. *Se* A' *è la matrice ottenuta da* A *scambiando due righe, ossia applicando l'operazione elementare O2 dell'algoritmo di Gauss, allora* $\det(A') = -\det(A)$
3. *Se* A' *è la matrice ottenuta da* A *sostituendo alla riga* i*-esima* A_i *la combinazione lineare* $A_i + k \cdot A_j$, *con* $i \neq j$, *ossia applicando una versione particolare dell'operazione elementare O3 dell'algoritmo di Gauss, allora il determinante rimane uguale, ossia* $\det(A') = \det(A)$
4. $\det(I) = 1$, *ossia il determinante della matrice identità è 1*

Teorema 5.6.1

Esiste una sola funzione $\det : \mathfrak{M}_n(\mathbb{R}) \to \mathbb{R}$ *che soddisfa queste tre proprietà.*

5.6.1 Regola di Laplace per il calcolo del determinante

Il determinante si può calcolare o usando l'algoritmo di Gauss, o usando la regola di Laplace per il calcolo del determinante. La regola di Laplace riduce via via il calcolo del determinante al calcolo del determinante di una matrice 2×2.

Fatto 2

Data una matrice $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, *il suo determinate è* $\det(A) = a \cdot d - b \cdot c$.

Data una matrice $A \in \mathfrak{M}_n(\mathbb{R})$, definiamo:

Minore Si dice "minore" di $a_{i,j}$ il determinante della matrice $M_{i,j}$, che è la matrice ottenuta da A cancellando la i-esima riga e la j-esima colonna;

Complemento algebrico Si dice "complemento algebrico" di $a_{i,j}$, e si indica con $\mathcal{A}_{i,j}$, il minore di $a_{i,j}$, con segno positivo se la somma di riga e colonna è pari, negativo altrimenti. Ossia:

$$\mathcal{A}_{i,j} = (-1)^{i+j} \det(M_{i,j})$$

La regola di Laplace ci dice che il determinante di una matrice è la somma dei valori di una riga (o di una colonna) ciascuno moltiplicato per il suo complemento algebrico.

$$\det(A) = a_{i,1} \cdot \mathcal{A}_{i,1} + \dots + a_{i,n} \cdot \mathcal{A}_{i,n} = a_{1,j} \cdot \mathcal{A}_{1,j} + \dots + a_{n,j} \cdot \mathcal{A}_{n,j}$$

Esempio :

Troviamo il determinante di questa matrice:

$$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 1 & 2 & -1 & 1 \\ 0 & 1 & 1 & 1 \\ 2 & 0 & 0 & 1 \end{pmatrix}$$

Conviene partire dalla riga con più zeri.

$$\begin{aligned} \det\left(\begin{pmatrix} 1 & 0 & -1 & 0 \\ 1 & 2 & -1 & 1 \\ 0 & 1 & 1 & 1 \\ 2 & 0 & 0 & 1 \end{pmatrix}\right) &= 2 \cdot (-1) \cdot \mathcal{A}_{4,1} + 0 + 0 + 1 \cdot (1) \cdot \mathcal{A}_{4,4} = \\ &= -2 \cdot \det\left(\begin{pmatrix} 0 & -1 & 0 \\ 2 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix}\right) + 1 \cdot \det\left(\begin{pmatrix} 1 & 0 & -1 \\ 1 & 2 & -1 \\ 0 & 1 & 1 \end{pmatrix}\right) = \\ &= -2 \cdot 1 \cdot \det\left(\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\right) + \left(1 \cdot \det\left(\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}\right) - 1 \cdot \det\left(\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\right)\right) = \\ &= -2 \cdot (2-1) + 3 - 1 = -2 + 3 - 1 = 0 \end{aligned}$$

5.6.2 Proprietà del determinante

1. Se A è una matrice con due righe uguali, allora per le proprietà del determinante $\det(A) = -\det(A) \Rightarrow \det(A) = 0$
2. Se A è una matrice che ha una riga nulla, $\det(A) = k \cdot \det(A)$ con $k \neq 0 \Rightarrow \det(A) = 0$
3. Sia $D = (d_{i,j})$ una matrice diagonale, ossia tutti gli elementi non sulla diagonale sono uguali a 0, ossia $d_{i,j} = 0$ se $i \neq j$. Si può scrivere come:

   $$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} = \begin{matrix} a \\ b \\ c \end{matrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

   Quindi $\det(D) = d_{1,1} \cdot \ldots \cdot d_{n,n}$. Inoltre, una matrice diagonale con uno 0 sulla diagonale, ha come determinante 0.
4. A' è una matrice ottenuta da A tramite le operazioni elementari di scambio di righe e sostituzione di una riga A_i con una combinazione lineare $A_i + k \cdot A_j$, allora il $\det(A') = (-1)^s \det(A)$, dove s è il numero degli scambi di riga. Si può trovare il determinante trasformando la matrice in una matrice diagonale, o anche solo a scala, con l'algoritmo di Gauss.

Proposizione 5.6.2 (*Corollario della proprietà 4*)

$$\det(A) \neq 0 \Leftrightarrow r(A) = n$$

Il determinante $\det(A) = (-1)^s \cdot \det(D)$, dove $D \sim_R A$ con le operazioni dette nella proprietà 4. $\det(D) = d_{1,1} \cdot \ldots \cdot d_{n,n}$.

$\det(A) \neq 0 \Rightarrow \det(D) \neq 0 \Rightarrow d_{i,i} \neq 0 \ \forall \ i \Rightarrow r(D) = n$ essendo D una matrice a scala. Quindi, essendo A e D equivalenti per riga, $r(A) = r(D) = n$.

Abbiamo detto che $\det(A) \neq 0 \Leftrightarrow r(A) = n \Leftrightarrow A$ è invertibile $\Leftrightarrow A \times X = 0$ ha una sola soluzione $\Leftrightarrow A \times X = B \ \forall \ B \in \mathbb{R}^n$ ha una sola soluzione.

Teorema 5.6.3 (*Teorema di Binet*)

Il determinante del prodotto di due matrici è il prodotto dei determinanti delle singole matrici.

$$\det(A \times B) = \det(A) \cdot \det(B)$$

Corollario 5.6.4

$$\det\left(A^{-1}\right) = \frac{1}{\det(A)}$$

Dimostrazione:

$$A^{-1} \cdot A = I \Rightarrow \det\left(A^{-1} \times A\right) = \det(I) = 1 \Rightarrow \det\left(A^{-1}\right) \cdot \det(A) = 1 \Rightarrow \det\left(A^{-1}\right) = \frac{1}{\det(A)}$$

■

5.6.3 Calcolo della matrice inversa di una matrice A

1. Risolvendo n sistemi lineari:

$$\begin{aligned} A \times X^1 &= I^1 \\ &\vdots \\ A \times X^n &= I^n \end{aligned}$$

   Dove X^i è l'i-esima colonna della matrice inversa A^{-1}.

2. Usando il determinante e la cosiddetta "matrice aggiunta di A", indicata con $\mathrm{Agg}(A)$, ottenuta mettendo al posto di ogni elemento di A il complemento algebrico, e facendo poi la trasposta.

$$\mathrm{Agg}(A) = \begin{pmatrix} \mathcal{A}_{1,1} & \mathcal{A}_{1,2} & \ldots & \mathcal{A}_{1,n} \\ \mathcal{A}_{2,1} & \ddots & \ddots & \mathcal{A}_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ \mathcal{A}_{n,1} & \mathcal{A}_{n,2} & \ldots & \mathcal{A}_{n,n} \end{pmatrix}^t = \begin{pmatrix} \mathcal{A}_{1,1} & \mathcal{A}_{2,1} & \ldots & \mathcal{A}_{n,1} \\ \mathcal{A}_{1,2} & \ddots & \ddots & \mathcal{A}_{n,2} \\ \vdots & \ddots & \ddots & \vdots \\ \mathcal{A}_{1,n} & \mathcal{A}_{2,n} & \ldots & \mathcal{A}_{n,n} \end{pmatrix}$$

   Con questo secondo metodo, l'inversa di A si ottiene moltiplicando l'aggiunta di A per l'inverso del determinante.

$$A^{-1} = \frac{1}{\det(A)} \cdot \mathrm{Agg}(A)$$

Dimostrazione del metodo 2 : La matrice $\text{Agg}(A)$ si ottiene mettendo nel posto i, j il complemento algebrico dell'elemento $a_{j,i}$, ossia $\mathcal{A}_{j,i}$. Per dimostrare questo, si deve dimostrare che:

$$A \times \text{Agg}(A) = \det(A) \cdot I = \text{Agg}(A) \times A$$

Sia $c_{i,j}$ l'elemento generico di $A \times \text{Agg}(A)$. Deve essere che:

$$\begin{cases} c_{i,i} = \det(A) \\ c_{i,j} = 0 \text{ se } i \neq j \end{cases}$$

Calcoliamo $c_{i,j}$ con Laplace. L'elemento $c_{i,j}$ deve essere il prodotto dell'i-esima riga di A per la j-esima colonna di $\text{Agg}(A)$, ma la j-esima colonna di $\text{Agg}(A)$ è il complemento algebrico della j-esima riga di A.

$$c_{i,j} = A_i \times \text{Agg}(A)^j = a_{i,1} \cdot \mathcal{A}_{j,1} + \ldots + a_{i,n} \cdot \mathcal{A}_{j,n} = 0$$

Per Laplace, il determinante di A è $\det((\,)A) = a_{i,1} \cdot \mathcal{A}_{i,1} + \ldots + a_{i,n} \cdot \mathcal{A}_{i,n}$. Quindi sto facendo il determinante di una matrice che ha due righe, i e j, con $i \neq j$, che sono uguali. Quindi $c_{i,j}$ deve essere 0, mentre $c_{i,i}$ è proprio il determinante di A. ■

Esempio :

Troviamo l'inverso della seguente matrice usando il secondo metodo:

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

Il suo determinante è:

$$\det(A) = -1$$

La matrice inversa, secondo il secondo metodo, è:

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{Agg}(A)$$

La matrice aggiunta è:

$$\text{Agg}(A) = \begin{pmatrix} -1 & -1 & 1 \\ 2 & 3 & -3 \\ 2 & 1 & -2 \end{pmatrix}$$

Quindi la matrice inversa è:

$$A^{-1} = \begin{pmatrix} 1 & 1 & -1 \\ -2 & -3 & 3 \\ -2 & -1 & 2 \end{pmatrix}$$

Si potrebbe trovare la matrice inversa anche risolvendo i seguenti tre sistemi.

La prima colonna dell'inversa è la soluzione di:

$$\begin{pmatrix} 3 & 1 & 0 \\ 2 & 0 & 1 \\ 4 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

La seconda colonna dell'inversa è la soluzione di:

$$\begin{pmatrix} 3 & 1 & 0 \\ 2 & 0 & 1 \\ 4 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

La terza colonna dell'inversa è la soluzione di:

$$\begin{pmatrix} 3 & 1 & 0 \\ 2 & 0 & 1 \\ 4 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Si può usare il determinante per risolvere sistemi quadrati.

Teorema 5.6.5 (*Teorema di Cramer*)

Un sistema lineare $A \times X = B$ di n equazioni in n incognite ha una sola soluzione se e solo se il rango $r(A) = n$, ossia se e solo se $\det(A) \neq 0$. *Questo teorema ci dice come calcolare quest'unica soluzione.*
L'unica soluzione $(x_1, \ldots, x_n)$ del sistema di cui sopra è data da:

$$x_1 = \frac{\det(M_1)}{\det(A)}$$
$$\vdots$$
$$x_n = \frac{\det(M_n)}{\det(A)}$$

M_i è la matrice che si ottiene da A sostituendo la i-esima colonna con la colonna B dei termini noti.

Esempio :

Risolviamo il seguente sistema lineare. Ordiniamo prima le incognite e i termini noti:

$$\begin{cases} 2y + 2x = z + 1 \\ 3x + 2z = 8 - 5y \\ 3z - 1 = x - 2y \end{cases} = \begin{cases} 2x + 2y - z = 1 \\ 3x + 5y + 2z = 8 \\ x - 2y - 3z = -1 \end{cases}$$

Il determinante della matrice associata è:

$$\det(A) = 22 \neq 0$$

Quindi il sistema ha una sola soluzione.

$$x_1 = x = \frac{\det(M_1)}{\det(A)} = \det\left(\begin{pmatrix} 1 & 2 & -1 \\ 8 & 5 & 2 \\ -1 & -2 & -3 \end{pmatrix}\right) \cdot \frac{1}{22} = \frac{66}{33} = 3$$
$$x_2 = y = \frac{\det(M_2)}{\det(A)} = \det\left(\begin{pmatrix} 2 & 1 & -1 \\ 3 & 8 & 2 \\ 1 & -1 & -3 \end{pmatrix}\right) \cdot \frac{1}{22} = \frac{-22}{22} = -1$$
$$x_3 = z = \frac{\det(M_3)}{\det(A)} = \det\left(\begin{pmatrix} 2 & 2 & 1 \\ 3 & 5 & 8 \\ 1 & -2 & 1 \end{pmatrix}\right) \cdot \frac{1}{22} = \frac{44}{22} = 2$$

La soluzione quindi è $(3, -1, 2)$.

Capitolo 6

Esercizi ed esempi

Esempio :

Consideriamo l'applicazione lineare $F : \mathbb{R}^3 \to \mathbb{R}^3$ definita da:

$$F(x, y, z) = (x, 2x - 2y - 2z, 2x - 3y - z)$$

1. Trovare la matrice associata all'applicazione lineare rispetto alla base $B = \{(1, 1, 1), (1, 1, 0), (1, 0, 0)\}$.
2. Determinare, se possibile, una base di autovettori rispetto alla quale la matrice che rappresenta F è diagonale, trovare la matrice diagonale, e trovare la matrice P tale per cui la matrice A associata alla base canonica è:

$$A = P^{-1} \times D \times P$$

Le colonne della matrice associata a B sono le coordinate rispetto alla base B delle immagini dei vettori della base B.

$$\begin{aligned} F(e_1) = F((1, 1, 1)) &= (1, -2, -2) = -2(1, 1, 1) + 0(1, 1, 0) + 3(1, 0, 0) \\ F(e_2) = F((1, 1, 0)) &= (1, 0, -1) = -1(1, 1, 1) + 1(1, 1, 0) + 1(1, 0, 0) \\ F(e_3) = F((1, 0, 0)) &= (1, 2, 2) = 2(1, 1, 1) + 0(1, 1, 0) - 1(1, 0, 0) \end{aligned}$$

Quindi la matrice associata alla base B è:

$$M_B(F) = \begin{pmatrix} -2 & -1 & 2 \\ 0 & 1 & 0 \\ 3 & 1 & -1 \end{pmatrix}$$

Avremmo potuto trovare le coordinate delle immagini rispetto alla base B con il cambio di base. Per effettuare un cambio di base, bisogna trovare la matrice $M_B^{B_c}(id)$. La matrice $M_B^{B_c}(id)$ ha per colonne le coordinate della base canonica B_c rispetto alla base B.

$$M_B^{B_c}(id) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix}$$

Per la seconda domanda, bisogna trovare una base B_a di autovettori di F. Prima troviamo la matrice associata ad F rispetto alla base canonica:

$$A = M_B(F) = \begin{pmatrix} 1 & 0 & 0 \\ 2 & -2 & -2 \\ 2 & -3 & -1 \end{pmatrix}$$

Gli autovalori saranno le radici del determinante della matrice $A - \lambda \cdot I$.

$$A - \lambda \cdot I = \begin{pmatrix} 1-\lambda & 0 & 0 \\ 2 & -2-\lambda & -2 \\ 2 & -3 & -1-\lambda \end{pmatrix}$$

Il polinomio caratteristico è:

$$\begin{aligned} \det(A - \lambda \cdot I) &= (1-\lambda) \cdot [(-2-\lambda) \cdot (-1-\lambda) - 6] = \\ &= (1-\lambda) \cdot \left[2 + \lambda + 2\lambda + \lambda^2 - 6\right] = \\ &= (1-\lambda) \cdot \left[\lambda^2 + 3\lambda - 4\right] = \\ &= (1-\lambda) \cdot \left[\lambda^2 - \lambda + 4\lambda - 4\right] = \\ &= (1-\lambda)^2 \cdot (\lambda + 4) \end{aligned}$$

Gli autovalori quindi sono, con le rispettive molteplicità algebriche:

$$\begin{aligned} \lambda_1 = 1 \qquad & m_a(\lambda_1) = 2 \\ \lambda_2 = -4 \qquad & m_a(\lambda_2) = 1 \end{aligned}$$

Gli autovettori associati a 1 sono le soluzioni del sistema $(A - I) \times X = \underline{0}$, con $A - I$ pari a:

$$\begin{pmatrix} 0 & 0 & 0 \\ 2 & -3 & -2 \\ 2 & -3 & -2 \end{pmatrix}$$

Il sistema ha rango 1, quindi ha ∞^2 soluzioni, quindi $m_g(\lambda_1) = 2$. La molteplicità geometrica è il numero di incognite del sistema meno il rango della matrice associata al sistema (ossia, meno il numero di righe non nulle). Bisogna trovare una base di $E(1)$ (l'insieme degli autovettori di autovalore 1). Essendo la molteplicità geometrica di 1 pari a $m_g(1) = 2$, $E(1)$ avrà dimensione 2.

$$E(1) = \{(x, y, z) : 2x - 3y - 2z = 0\} = <(1, 0, 1), (0, 2, -3)>$$

Vediamo con $\lambda_2 = -4$.

$$\begin{pmatrix} 5 & 0 & 0 \\ 2 & 2 & -2 \\ 2 & -3 & 3 \end{pmatrix}$$

Applichiamo Gauss si ottiene:

$$\begin{pmatrix} 5 & 0 & 0 \\ 0 & 10 & -10 \\ 0 & 0 & 0 \end{pmatrix}$$

Da cui:

$$E(-4) = \{(x, y, z) : x = 0 \text{ e } y - z = 0\} = <(0, 1, 1)>$$

Abbiamo quindi la base di autovettori:

$$B_a = \{(1,0,1),(0,2,-3),(0,1,1)\}$$

La matrice diagonale rispetto a questa base è:

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -4 \end{pmatrix}$$

La matrice diagonale dipende dall'ordine che si dà ai vettori nella base di autovettori! Ora dobbiamo trovare P tale per cui la matrice associata alla base canonica è $A = P^{-1} \times D \times P$.

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 1 & -3 & 1 \end{pmatrix}$$

P^{-1} è la matrice che ha per colonne gli autovettori di B_a. P è l'inversa di P^{-1}.

$$\det\left(P^{-1}\right) = 2 - (-3) = 5$$

Quindi P è:

$$P = \frac{1}{5} \cdot \operatorname{Agg}\left(P^{-1}\right) = \frac{1}{5} \cdot \begin{pmatrix} 5 & 1 & -2 \\ 0 & 1 & 3 \\ 0 & -1 & -1 \end{pmatrix}^t = \frac{1}{5} \cdot \begin{pmatrix} 5 & 0 & 0 \\ 1 & 1 & -1 \\ -2 & 3 & -1 \end{pmatrix}$$

Esempio :

Consideriamo l'applicazione lineare $L : \mathbb{R}_2[x] \to \mathbb{R}_2[x]$ definita da:

$$\begin{aligned} L(a_0 + a_1 \cdot x + a_2 \cdot x^2) = {} & (a_0 - 3a_1 + 3a_2) \\ & + (3a_0 - 5a_1 + 3a_2) \cdot x \\ & + (6a_0 - 6a_1 + 4a_2) \cdot x^2 \end{aligned}$$

Trovare la matrice associata a L rispetto alla base canonica, trovare autovettori e autovalori ed eventualmente la matrice diagonale D che rappresenta L.

La base canonica è $B_c = \{1, x, x^2\}$. Le loro immagini sono:

$$\begin{aligned} L(1) &= 1 + 3 \cdot x + 6 \cdot x^2 \\ L(x) &= -3 - 5 \cdot x - 6 \cdot x^2 \\ L(x^2) &= 3 + 3 \cdot x + 4 \cdot x^2 \end{aligned}$$

Per trovare la matrice $M_{B_c}(L)$ bisogna mettere in colonna le coordinate di questi vettori rispetto alla base canonica.

$$A = M_{B_c}(L) = \begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix}$$

Facciamo il determinante del polinomio caratteristico per trovare gli autovalori.

$$\det(A - \lambda \cdot I) = \det\left(\begin{pmatrix} 1-\lambda & -3 & 3 \\ 3 & -5-\lambda & 3 \\ 6 & -6 & 4-\lambda \end{pmatrix}\right) = (\lambda+2)^2 \cdot (\lambda - 4)$$

Abbiamo due autovalori:

$$\begin{aligned} \lambda_1 = -2 \qquad & m_a(-2) = 2 \\ \lambda_2 = 4 \qquad & m_a(4) = 1 \end{aligned}$$

Bisogna trovare gli autospazi di questi autovalori.

$$E(-2) = \{p(x) \in \mathbb{R}_2[x] : (A + 2 \cdot I) \times X = 0 \text{ e } X \neq \underline{0}\}$$

X è la colonna delle coordiante di $p(x)$ rispetto alla base canonica. La matrice è:

$$\begin{pmatrix} 3 & -3 & 3 \\ 3 & -3 & 3 \\ 6 & -6 & 6 \end{pmatrix}$$

Il rango di questa matrice è 1, quindi i polinomi in $E(-2)$ sono tutti i polinomi per cui:

$$\begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \underline{0}$$

Avendo rango 1, la dimensione di $E(-2)$, ossia il numero delle incognite meno il rango della matrice $(A + 2 \cdot I)$ è 2.

$$E(-2) = \{a_0 + a_1 \cdot x + a_2 \cdot x^2 : a_0 - a_1 + a_2 = 0\} = <(1,1,0),(0,1,1)>$$

La base di $E(-2)$ è $\{(1,1,0),(0,1,1)\}$. Troviamo $E(4)$. La sua matrice è:

$$\begin{pmatrix} -3 & -3 & 3 \\ 3 & -9 & 3 \\ 6 & -6 & 0 \end{pmatrix}$$

Applicando Gauss viene:

$$\begin{pmatrix} -3 & -3 & 3 \\ 0 & 12 & -6 \\ 0 & 0 & 0 \end{pmatrix} \sim_R \begin{pmatrix} 1 & 1 & -1 \\ 0 & -2 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Il sistema diventa quindi:

$$\begin{cases} a_0 + a_1 - a_2 = 0 \\ -2a_1 + a_2 = 0 \end{cases} \Rightarrow \begin{cases} a_0 = a_1 \\ a_2 = 2a_1 \end{cases}$$

Quindi la soluzione è: $(1,1,2)$, ossia $1 + x + 2 \cdot x^2$.

La base di autovettori è: $\{1 + x + 2 \cdot x^2, 1 + x, x + x^2\}$. Rispetto a questa base, la matrice diagonale che rappresenta L è:

$$D = \begin{pmatrix} 4 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

Per trovare la matrice P tale per cui $M_{B_c}(L) = P^{-1} \times D \times P$, sapendo che P^{-1} è la matrice che ha per colonne le coordinate degli autovettori dell'autospazio, basta fare l'inversa di P^{-1}.

Se si vuole trovare il $\ker L$ e l'immagine Im_L?

L'immagine di L è generata dalle colonne della matrice associata a L. Quindi la dimensione dell'immagine è il rango della matrice associata A.

$$\dim <1+3\cdot x+6\cdot x^2, -3-5\cdot x-6\cdot x^2, 3+3\cdot x+4\cdot x^2>= r\left(M_{B_c}(L)\right) = \dim Im_L$$

Per trovare il $\ker L$, so che ne fanno parte i vettori $a_0 + a_1 \cdot x + a_2 \cdot x^2$ che risolvono questo sistema:

$$\begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix} \times \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = 0$$

Il rango della matrice associata è 3, quindi L è un'applicazione iniettiva (o meglio un isomorfismo) e il $\ker L$ contiene solo il vettore nullo (ha dimensione 0).

Problemi che si possono risolvere applicando il metodo di Gauss:

1. data un'applicazione lineare $L : V \to V'$, determinare Im_L e $\ker L$. Si trova la matrice A associata a L rispetto a una certa base, tipicamente quella canonica. La dimensione dell'immagine di L è il rango di A, ossia $\dim Im_L = r(A)$. L'immagine $Im_L =< L(e_1), \ldots, L(e_n) >$ è generata dalle immagini dei vettori della base, con la base $B = \{e_1, \ldots, e_n\}$. Faccio la trasposta di A, trovo una matrice a scala S simile ad A^t, e ho che le righe di S sono i vettori di una base di Im_L.

   Per il nucleo, $\ker L = \{v \in V : L(v) = 0\} = \{v \in V : A \times X = \underline{0}\}$. Basta risolvere il sistema e stai una Pasqua.

2. Dati un insieme G di generatori di V, con $|G| < \infty$, estrarre da G una base $B \subseteq G$. Si prende un vettore $v_1 \in G$ con $v_1 \neq \underline{0}$, $\{v_1\}$ è uno spazio indipendente. Si continuano ad aggiungere vettori $v_2, \ldots, v_n$ non appartenente allo spazio generato che si sta creando, fino a $n = \dim V$.

3. Dato un insieme di vettori indipendenti S con $|S| = t \leq n = \dim V$, determinare una base B di V che contiene S, ossia tale che $S \subseteq B$.

4. Se ho un certo numero di vettori e devo vedere quanti di questi sono dipendenti o indipendenti, li metto per righe o per colonne e applico Gauss. Il numero di righe non nulle è il numero di vettori indipendenti.

5. Dati due sottospazi U e W di V, determinare la somma e l'intersezione degli spazi, ossia $U + W$ e $U \cap W$. Se prendo una base B_U di U e una base B_W di W, ho che $< B_U \cup B_W >$ è un sistema di generatori di $U + W$, ma non è una base. Per avere una base applico Gauss.

Esempio :

Consideriamo $\mathbb{R}^4$, e un insieme $S = \{(1,1,1,1), (2,2,0,2)\}$ di vettori indipendenti.

Mettendo dei vettori per riga e applicando il metodo di Gauss si ha che lo spazio generato dalle righe resta uguale. Non vale lo stesso per le colonne, anche se la dimensione dello spazio generato dalle colonne resta uguale.

Si mettono per righe i vettori di S, la si trasforma eventualmente in una matrice a scala, e si completa la matrice fino ad averne una a scala.

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 0 & 2 \end{pmatrix} \sim_R \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix}$$

La base di $\mathbb{R}^4$ è:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Esempio :

$$U = \{(x, y, z, t) \in \mathbb{R}^4 : 2x + y - 3t = 0\}$$
$$W = <(1, 0, 1, 0), (-1, 1, 0, 1)>$$

Dati questi due sottospazi di $\mathbb{R}^4$, trovare una base della somma e una base dell'intersezione.

Una base di U è $B_U = \{(1, -2, 0, 0), (0, 0, 1, 0), (0, 3, 0, 1)\}$, quindi $\dim U = 3$. I vettori che generano W sono indipendenti, quindi loro sono una base di W, e $\dim W = 2$.

Se vogliamo trovare una base di $W + U = < B_U \cup B_W >$, si cerca la matrice equivalente per righe a quella che ha per righe i vettori delle due basi:

$$\begin{pmatrix} 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{pmatrix} \sim_R \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Quindi $\dim(U + W) = 4$. Sapendo che $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$, possiamo capire subito che $\dim U \cap W = 3 + 2 - 4 = 1$.

Per trovare il vettore che è base di $U \cap W$, si scrive il vettore v come combinazione lineare degli elementi di W.

$$v = (x, y, z, t) = a \cdot (1, 0, 1, 0) + b \cdot (-1, 1, 0, 1) = (a - b, b, a, b)$$

Si impone che questo v appartenga a U, ossia deve soddisfare l'equazione che abbiamo usato per definire U.

$$2 \cdot (a - b) + b - 3 \cdot b = 0$$

Da ciò viene che $a = 2b$, e che quindi il vettore dell'intersezione è $(b, b, 2b, b)$ per un generico b, o $(1, 1, 2, 1)$ per un esempio non generico.

Elenco delle tabelle

2.1 Il gruppo simmetrico non è commutativo 46
2.2 Somma e prodotto in $\mathbb{Z}_2$ 50
2.3 σ dal punto di vista dell'occupazione 55
2.4 μ dal punto di vista dell'occupazione 55
2.5 Le tre permutazioni μ_3, μ_5 e μ_6 individuate da μ 55
2.6 Composizione di $\mu_3 \circ \mu_5 \circ \mu_6$ 56
2.7 La permutazione b 60
2.8 L'algoritmo di Euclide per trovare il MCD$(159, 42)$, con il resto di ogni passaggio scritto come identità di Bézout 65
2.9 Tavole di composizione di $+$ e $\cdot$ in $\mathbb{Z}_3$ 66
2.10 Tavole di composizione di $+$ e $\cdot$ in $\mathbb{Z}_4$ 67

Elenco delle figure

1.1 Diagramma di Hasse della relazione $(\mathbb{P}(A), \subseteq)$ sull'insieme $A = \{1, 2, 3\}$ 8
1.2 Diagramma di Hasse della relazione $(A, |)$ sull'insieme $A = \{n \in \mathbb{N} : n \mid 24\} = \{1, 2, 3, 4, 6, 8, 12, 24\}$ 8
1.3 Reticolo modulare ma non distributivo 12
1.4 f come composizione di p e di $i \circ F$ 16
1.5 $f(x, y) = (x, x, 0)$ come composizione di una funzione suriettiva con una iniettiva 17
1.6 $\ker f = \{[1], [2], [5]\}$, $Im_f = \{a, b, d\}$ 17
1.7 Esempio di strutture isomorfe 22
1.8 Metodo della diagonale 26
1.9 Le quattro partizioni possibili 33
1.10 Il rettangolo realizzabile sul piano colorato 33

2.1 $\ker f = \{\{a, b\}, \{c, d\}, \{e\}\}$ 47
2.2 Reticolo dei sottogruppi di $\mathbb{Z}_6$ 79
2.3 Reticolo dei sottogruppi di $\mathbb{Z}_{12}$ 79
2.4 L'isomorfismo tra $U(\mathbb{Z}_5)$ e $U(\mathbb{Z}_{10})$ 81

3.1 Metodo del parallelogramma 93
3.2 Prodotto scalare 93

4.1 L rispetto a B' come composta di due cambi di base con L rispetto a B 120