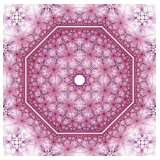
ALGORITMICA

COLLANA DI MATEMATICA E INFORMATICA

2

ALGORITMICA

COLLANA DI MATEMATICA E INFORMATICA



Sfortunatamente non si comprende come i libri scientifici più validi siano quelli in cui l'autore indica chiaramente cosa non sa; un autore fa infatti maggiormente del male ai suoi lettori quando nasconde le difficoltà.

Evariste Galois

È ben noto che competenze matematiche e informatiche sono ormai indispensabili in tutte le discipline scientifiche. Per soddisfare tale esigenza, la collana intende presentare testi didattici di base rivolti agli studenti universitari di area scientifica. Inoltre la collana ospita monografie centrate su aspetti avanzati delle discipline e raccolte di lezioni per corsi di dottorato, nonché atti di convegni scientifici di rilevanza internazionale.

Giovanni Vincenzi

Algebra per Informatica

www.aracneeditrice.it
info@aracneeditrice.it

via Quarto Negroni, 15
00040 Ariccia (RM)
(06) 93781065

ISBN 978-88-548-8225-6

I edizione: marzo 2015

Introduzione

Negli ultimi anni stiamo assistendo ad uno sviluppo intenso della tecnologia, dell' uso dei calcolatori e dei sistemi di controllo. Le competenze professionali si sono notevolmente evolute, e richiedono ormai una conoscenza delle discipline matematiche di base sempre più profonda. La Matematica Discreta, la Crittografia, la Teoria dei Codici, la Probabilità, lo studio dei Dati, lo studio degli Algoritmi e della Complessità computazionale sono solo alcuni esempi di discipline scientifiche in cui è necessario possedere adeguate conoscenze dell'Algebra affinché possano essere comprese.

Lo scopo di questo testo è quello di fornire il linguaggio e gli strumenti matematici di base che si usano tradizionalmente nei corsi di informatica della laurea magistrale e specialistica. Particolare attenzione è stata dedicata alla formalizzazione e all' interpretazione dei problemi teorici in modo tale da stimolare maggiori capacità di astrazione lasciando vivo l'aspetto intuitivo. Questo tipo di attitudini sono essenziali per comprendere a fondo le questioni tecnico-scientifiche e la loro possibilità di modellizzazione. Alcune dimostrazioni ritenute poco rilevanti per gli scopi del testo e facilmente reperibili in letteratura sono omesse.

Approfondimenti teorici e ulteriori spunti applicativi dell'algebra possono essere trovati nei testi indicati nella bibliografia.

INDICE

CAPITOLO 1

IL LINGUAGGIO MATEMATICO

1.1 RICHIAMI DI INSIEMISTICA

Lo studio dell'insiemistica sarà svolto in senso "ingenuo". In particolare riterremo noti i concetti di insieme, oggetto, appartenenza, proprietà, (tali concetti li diremo anche primitivi). Per denotare che un insieme A è costituito dagli oggetti "1", "3" e "a" useremo la scrittura: $A := \{1, 3, a\}$. Per evidenziare che l'oggetto "1" è un elemento di A useremo la scrittura: $1 \in A$ che si legge: "1 appartiene ad A". Siano A e B insiemi. Se ogni oggetto di A è oggetto di B e viceversa, ogni oggetto di B è oggetto di A, diremo che A e B sono *uguali* e scriveremo $A = B$.

Rileviamo che per descrivere un insieme non contano l'ordine e le ripetizioni. Quindi: $\{1, 3, a\} = \{a, 1, 3, a\} = \{1, 3, a, 3, a\}$.

Spesso le proprietà possono essere usate per descrive un insieme. Ad esempio se P_1 è la proprietà di "essere cittadino italiano", allora l'insieme $\{x : x \text{ verifica } P_1\}$ è costituito da tutti e soli i cittadini italiani;

Se P_2 è la proprietà di "essere numero intero positivo pari", allora l'insieme $2\mathbb{N} := \{x : x \text{ verifica } P_2\}$, è costituito da tutti e soli i numeri interi positivi pari.

Sia P_3 la proprietà di "essere numero intero positivo". Allora l'insieme $\{x : x \text{ verifica } P_3\}$ coincide con l'insieme dei numeri naturali positivi $\mathbb{N}$.

Se P è una proprietà, la sua negazione si denota col simbolo $\sim P$. Un insieme privo di elementi si dice *vuoto*, e si rappresenta col simbolo $\emptyset$. Osserviamo

che qualunque sia la proprietà P risulta: $\emptyset = \{x : \ x \text{ verifica P e } x \text{ verifica } \sim P\}$. Se S è un insieme, il numero degli elementi di S si dice anche *cardinalità* oppure *ordine* di S e si denota col simbolo $|S|$. Evidentemente $|\emptyset| = 0$, mentre $|\{\emptyset\}| = 1$.

Quesito: Che ordine ha l'insieme "$\{\{\emptyset\}\}$" ?

Siano S e T insiemi. Diremo che S è *incluso* in T (oppure che S è un *sottoinsieme* di T) e scriveremo $S \subseteq T$ se vale la seguente implicazione: $x \in S \Rightarrow x \in T$. Chiaramente $S = T \iff S \subseteq T$ e $T \subseteq S$.

Siano S e T insiemi. Diremo che S è *incluso propriamente* in T e scriveremo $S \subset T$ se $S \subseteq T$ e $S \neq T$.

Concludiamo questo paragrafo riportando alcuni esempi che evidenziano l'esatto utilizzo dei simboli che abbiamo richiamato.

Esempio 1.1.1

(1) "$1 \in \{1\}$" è corretta;

(2) $1 \in 1$ non è corretta perché un elemento deve necessariamente appartenere ad un insieme;

(3) "$\{1\} \in 1$" non è corretta perché un elemento deve appartenere ad un insieme e non ad un altro elemento;

(4) "$\{1\} \subseteq \{1\}$" è corretta;

(5) "$\{1\} \in \{1\}$" non è corretta perché il singleton di 1 non è elemento dell' insieme $\{1\}$;

(6) "$\{1\} \subseteq \{1, 2\}$" è corretta;

(7) "$\{1\} \in \{1, 2\}$ non è corretta perché il singleton di 1 non è un elemento dell' insieme $\{1, 2\}$;

(8) "$\emptyset \in \{\emptyset\}$" è corretta;

(9) "$\{\emptyset\} \in \emptyset$" non è corretta perché nessun elemento appartiene all'insieme vuoto;

(10) "$\emptyset \subseteq \{\emptyset\}$" è corretta;

(11) "$\{\emptyset\} = \emptyset$" non è corretta perché il singleton del vuoto ha un elemento mentre il vuoto è un insieme senza elementi;

(12) "$\{\emptyset\} \in \{1, 2\}$" non è corretta perché il singleton del vuoto non è un elemento del secondo insieme;

(13) "$\{1\} \in \{\{1\}, 2, \{2\}\}$" è corretta;

(14) "$\{\{1\}, \{1, 2\}\} = \{1, 2\}$" non è corretta perché i due insiemi sono costituiti da elementi diversi;

(15) "$\{\{1\},\{1,2\}\} = \{\{2\},\{1,2\}\}$" non è corretta perché gli elementi dei due insiemi differiscono;

(16) "$1 \in \{\{1\},2,\{2\}\}$" non è corretta perché l'elemento "1" non appartiene al secondo insieme.

1.2 RICHIAMI DI LOGICA

Una *proposizione* è una affermazione per la quale si può stabilire se sia vera o falsa, ma non può essere simultaneamente vera e falsa.

Generalmente una proposizione si indica con una lettera minuscola, come p, q, r...

A partire da una proposizione p si può definire la proposizione $\sim p$ (leggi "*non p*"), ottenuta negando l'affermazione espressa in p.

Ad esempio se p è la proposizione " Roma è in provincia di Napoli", allora $\sim p$ è la proposizione " Roma non è in provincia di Napoli".

Osserviamo che se p è vera allora $\sim p$ è falsa, e viceversa.

Le proposizioni possono essere più articolate. Ci sono infatti delle proposizioni che possono dipendere da una "variabile". Ad esempio:

" Ogni cittadino italiano è alto meno di due metri".

Per formalizzare questa proposizione, si denota con S l'insieme dei cittadini italiani e con $p(x)$ la proposizione " il cittadino x è alto meno di due metri". La proposizione precedente può essere formulata come segue:

$\forall x \in S$, $p(x)$. Questa scrittura si legge: *Per ogni* x *appartenente ad* S*, la proposizione* $p(x)$ *è verificata.*

Osserviamo che la negazione della proposizione precedente è:

" Esiste un cittadino italiano tale che la sua altezza è maggiore o uguale a due metri". Tale proposizione viene formulata come segue: $\exists x \in S$: $\sim p(x)$. Questa scrittura si legge: *"Esiste* x *appartenente ad* S*, tale che* $p(x)$ *non è verificata"*, oppure si può leggere *"esiste* x *appartenente ad* S*, tale che la proposizione* $\sim p(x)$ *è verificata"*.

Esercizio 1.2.1

(1) Negare la seguente proposizione: "Ogni studente iscritto a matematica nell' a.a. 2007/2008 ha superato l'esame di Algebra o di Analisi".

(2) Negare la seguente proposizione: "Ogni studente che nel 2008 ha superato l'esame di Algebra e di Analisi ha superato anche l'esame di Matematica di Base".

Se p e q sono proposizioni, allora possiamo considerare la proposizione "$p \vee q$". Tale proposizione è vera se almeno una delle affermazioni espresse da p oppure da q è vera, falsa se p e q sono entrambe false.

Se p e q sono proposizioni, allora possiamo considerare la proposizione "$p \wedge q$". Tale proposizione è vera se entrambe le affermazioni espresse sia dalla proposizione p che dalla proposizione q sono vere; falsa se p oppure q è falsa.

Se p e q sono proposizioni allora possiamo considerare la proposizione "$p \Rightarrow q$". Tale proposizione è falsa se p è vera e q è falsa, e quindi vera in tutti gli altri casi.

La proposizione $p \Rightarrow q$ si può leggere indifferentemente in uno dei seguenti modi:

i) "p *implica* q";
ii) "p *è condizione sufficiente affiché si verifichi* q";
iii)"q *è condizione necessaria affiché si verifichi* p";
iv) "p *solo se* q";
v) "q *se* p";
vi) "*se* p *allora* q".

Se accade simultaneamente che "p implica q" e "q implica p" si scrive semplicemente "$p \iff q$", e si dice "p *se solo se* q", "p *è condizione necessaria e sufficiente affiché si verifichi* q" oppure "p *è una caratterizzazione di* q".

Esercizio 1.2.2 Siano p e q proposizioni. Verificare che

(1) $\sim (p \vee q) \iff (\sim p) \wedge (\sim q)$;

(2) $\sim (p \wedge q) \iff (\sim p) \vee (\sim q)$.

(3) "p implica q" $\iff$ "$\sim$ q implica $\sim$ p "

Nella pratica per verificare che un'implicazione $p \Rightarrow q$ è vera, si suppone vera la proposizione p, e mediante una successione di implicazioni elementari che viene detta *dimostrazione* si prova che anche la proposizione q è vera.

Se una proposizione vera si presenta nella forma $p \Rightarrow q$, con p e q proposizioni, allora p e q si dicono rispettivamente *ipotesi* e *tesi* dell'implicazione $p \Rightarrow q$, e la stessa implicazione si dice *enunciato*. Con i termini *Teorema, Lemma, Corollario* e spesso anche col termine *Proposizione* intenderemo particolari proposizioni dimostrabili.

1.3 OPERAZIONI TRA INSIEMI

Siano S e T insiemi. Diremo *unione* dell'insieme S e dell'insieme T, l'insieme $S \cup T := \{x : x \in S \text{ oppure } x \in T\}$.

Siano S e T insiemi. Diremo *intersezione* dell'insieme S e dell'insiemeT l'insieme $S \cap T := \{x : x \in S \text{ e } x \in T\}$.

Osservazione 1.3.1 Siano S e T insiemi. Valgono le seguenti equivalenze (cfr esercizio 1.2.2):

(1) $x \notin S \cup T \iff x \notin S \text{ e } x \notin T$;

(2) $x \notin S \cap T \iff x \notin S \text{ o } x \notin T$.

Siano S e T insiemi. Diremo *differenza* dell'insieme S e dell'insieme T l'insieme $S \setminus T := \{x : x \in S \text{ e } x \notin T\}$.

Nelle notazioni che useremo $\mathbb{N}$ è l'insieme dei numeri interi positivi, quindi $0 \notin \mathbb{N}$, mentre $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. La scrittura $\mathbb{N} \cup 0$ (leggi "$\mathbb{N}$ unione 0") è scorretta perché l'unione può avvenire unicamente tra insiemi.

Sia S un insieme. Diremo *insieme delle parti di* S e scriveremo $\wp(S)$ l'insieme costituito da tutti i sottoinsiemi di S : $\wp(S) := \{X : X \subseteq S\}$.

Esempio 1.3.2 Sia $S = \{1, a, \{a\}\}$. Allora

$$\wp(S) = \{\emptyset, \{1\}, \{a\}, \{\{a\}\}, \{1, a\}, \{1, \{a\}\}, \{a, \{a\}\}, S\}.$$

Esercizio 1.3.3 Determinare l'insieme delle parti di $S = \{\emptyset, 1\}$.

Per le operazioni insiemistiche appena definite, valgono le seguenti proprietà:

Proposizione 1.3.4 *Per ogni* S, T, V *insiemi risulta:*

(1) $S \cap S = S$, $S \cup S = S$ *(proprietà iterativa dell'intersezione e dell'unione);*

(2) $S \cap T = T \cap S$, $S \cup T = T \cup S$ *(proprietà commutativa dell'intersezione e dell'unione);*

(3) $(S \cap T) \cap V = S \cap (T \cap V)$ *(proprietà associativa dell'intersezione);*

(4) $(S \cup T) \cup V = S \cup (T \cup V)$ *(proprietà associativa dell'unione);*

(5) $S \cap (T \cup V) = (S \cap T) \cup (S \cap V)$ *(proprietà distributiva dell'intersezione rispetto all'unione);*

(6) $S \cup (T \cap V) = (S \cup T) \cap (S \cup V)$ *(proprietà distributiva dell'unione rispetto l'intersezione).*

Dimostrazione – Le proprietà $(1) - (4)$ sono lasciate come esercizio.

5) Sia $x \in S \cap (T \cup V) \Rightarrow x \in S$ e $x \in (T \cup V) \Rightarrow x \in S$ e $(x \in T$ o $x \in V) \Rightarrow (x \in S$ e $x \in T)$ o $(x \in S$ e $x \in V) \Rightarrow x \in (S \cap T)$ o $x \in (S \cap V) \Rightarrow x \in (S \cap T) \cup (S \cap V)$.

Proviamo l'altra inclusione. Sia $x \in (S \cap T) \cup (S \cap V) \Rightarrow x \in (S \cap T)$ o $x \in (S \cap V) \Rightarrow (x \in S$ e $x \in T)$ o $(x \in S$ e $x \in V) \Rightarrow x \in S$ e $(x \in T$ o $x \in V) \Rightarrow x \in S$ e $x \in (T \cup V) \Rightarrow x \in S \cap (T \cup V)$.

6) Sia $x \in S \cup (T \cap V) \Rightarrow x \in S$ o $x \in (T \cap V) \Rightarrow x \in S$ o $(x \in T$ e $x \in V) \Rightarrow (x \in S$ o $x \in T)$ e$(x \in S$ o $x \in V) \Rightarrow x \in (S \cup T)$ e $x \in (S \cup V) \Rightarrow x \in (S \cup T) \cap (S \cup V)$.

Proviamo l'altra inclusione. Sia $x \in (S \cup T) \cap (S \cup V) \Rightarrow x \in (S \cup T)$ e $x \in (S \cup V) \Rightarrow (x \in S$ o $x \in T)$ e$(x \in S$ o $x \in V) \Rightarrow x \in S$ o $(x \in T$ e $x \in V) \Rightarrow x \in S$ o $x \in (T \cap V) \Rightarrow x \in S \cup (T \cap V)$. □

Osserviamo che non vale la proprietà commutativa della differenza insiemistica. Infatti in genere $S \setminus T \neq T \setminus S$, basti considerare due insiemi distinti (verificare con un esempio).

È opportuno osservare che una condizione necessaria e sufficiente affinché "$S \setminus T = T \setminus S$" è che "$S = T$".

Proposizione 1.3.5 *$S \setminus T = T \setminus S$ se e solo se $S = T$.*

Dimostrazione – Per verificare che la condizione è necessaria ($\Rightarrow$) proviamo la doppia inclusione. Se per assurdo S non è incluso in T allora esiste un elemento x tale che $x \in S$ e $x \notin T$, sicché $x \in S \setminus T$ e per ipotesi $x \in T \setminus S$, in particolare $x \in T$. Questa contraddizione prova che $S \subseteq T$. Analogamente si prova l'altra inclusione, e quindi $S \setminus T = T \setminus S$ solo se $S = T$. Viceversa se $S = T$ allora, banalmente, $S \setminus T = T \setminus S = \emptyset$. □

Osserviamo che la differenza insiemistica non è un' operazione associativa, ovvero se A, B, C, sono insiemi non è detto che $A \setminus (B \setminus C) = (A \setminus B) \setminus C$. Ad esempio consideriamo i seguenti insiemi.

$A := \{a, b, c, d, l, t\}$, $B := \{f, d, b, c\}$, $C := \{l, m, a, d\}$. Risulta:

$A \setminus (B \setminus C) = \{a, b, c, d, l, t\} \setminus (\{f, d, b, c\} \setminus \{l, m, a, d\}) = \{a, b, c, d, l, t\} \setminus \{f, b, c\} = \{a, d, l, t\}$.

$(A \setminus B) \setminus C = (\{a, b, c, d, l, t\} \setminus \{f, d, b, c\}) \setminus \{l, m, a, d\}) = \{a, l, t\} \setminus \{l, m, a, d\}) = \{t\}$.

Proposizione 1.3.6 *Siano S, T, V, insiemi allora:*

1) $(S \cap T) \setminus V = (S \setminus V) \cap (T \setminus V)$;

2) $(S \cup T) \setminus V = (S \setminus V) \cup (T \setminus V)$;

3) $S \setminus (T \cup V) = (S \setminus T) \cap (S \setminus V)$;

4) $S \setminus (T \cap V) = (S \setminus T) \cup (S \setminus V)$.

Dimostrazione – 1) Sia $x \in (S \cap T) \setminus V \Rightarrow x \in S \cap T$ e $x \notin V \Rightarrow (x \in S$ e $x \in T)$ e $x \notin V \Rightarrow (x \in S$ e $x \notin V)$ e $(x \in T$ e $x \notin V) \Rightarrow x \in (S \setminus V)$ e $x \in (T \setminus V) \Rightarrow x \in (S \setminus V) \cap (T \setminus V)$.

Sia $x \in (S \setminus V) \cap (T \setminus V) \Rightarrow x \in (S \setminus V)$ e $x \in (T \setminus V) \Rightarrow (x \in S$ e $x \notin V)$ e $(x \in T$ e $x \notin V) \Rightarrow (x \in S$ e $x \in T)$ e $x \notin V \Rightarrow x \in (S \cap T)$ e $x \notin V \Rightarrow x \in (S \cap T) \setminus V$.

2) Sia $x \in (S \cup T) \setminus V \Rightarrow x \in S \cup T$ e $x \notin V \Rightarrow (x \in S$ o $x \in T)$ e $x \notin V \Rightarrow (x \in S$ e $x \notin V)$ o $(x \in T$ e $x \notin V) \Rightarrow x \in (S \setminus V)$ o $x \in (T \setminus V) \Rightarrow x \in (S \setminus V) \cup (T \setminus V)$.

Sia $x \in (S \setminus V) \cup (T \setminus V) \Rightarrow x \in (S \setminus V)$ o $x \in (T \setminus V) \Rightarrow (x \in S$ e $x \notin V)$ o $(x \in T$ e $x \notin V) \Rightarrow (x \in S$ o $x \in T)$ e $x \notin V \Rightarrow x \in (S \cup T)$ e $x \notin V \Rightarrow x \in (S \cup T) \setminus V$.

3) Sia $x \in S \setminus (T \cup V) \Rightarrow x \in S$ e $x \notin (T \cup V) \Rightarrow x \in S$ e $(x \notin T$ e $x \notin V) \Rightarrow (x \in S$ e $x \notin T)$ e $(x \in S$ e $x \notin V) \Rightarrow x \in S \setminus T)$ e $x \in (S \setminus V) \Rightarrow x \in (S \setminus T) \cap (S \setminus V)$.

Sia $x \in (S \setminus T) \cap (S \setminus V) \Rightarrow x \in (S \setminus T)$ e $x \in (S \setminus V) \Rightarrow (x \in S$ e $x \notin T)$ e $(x \in S$ e $x \notin V) \Rightarrow x \in S$ e$(x \notin T$ e $x \notin V) \Rightarrow x \in S$ e $x \notin (T \cup V) \Rightarrow x \in S \setminus (T \cup V)$.

La verifica della 4) è lasciata come esercizio. □

Le relazioni 3 e 4 della proposizione precedente si chiamano *Formule di De Morgan*.

La nozione di intersezione e la nozione di unione può essere estesa in modo naturale a piu' di due insiemi. Eventualmente anche ad infiniti insiemi.

Esempio 1.3.7 Sia X_n un insieme numerico che dipende da un numero intero positivo "n". Ad esempio: $X_n = \{x \in \mathbb{N} : x \geqslant n\}$. Allora X_1 coincide con l'insieme dei numeri naturali positivi; $X_4 = \{x \in \mathbb{N} : x \geqslant 4\} = \{4, 5, 6, 7, 8, \ldots\}$. In questo modo l'insieme costituito da tutti gli X_n è infinito. Risulta:

$$\bigcap_{n \in \mathbb{N}} X_n = \emptyset.$$

Esempio 1.3.8 Sia ora I_n un altro insieme numerico che dipende da "n": $I_n = \{x \in \mathbb{N} : \ x \leqslant n\}$. Allora $I_6 = \{1, 2, 3, 4, 5, 6\}$ e evidentemente

$$\bigcup_{n \in \mathbb{N}} I_n = \mathbb{N}.$$

Siano S e T insiemi. Diremo *prodotto cartesiano di* S *e di* T l'insieme $S \times T := \{(s,t) : s \in S \text{ e } t \in T\}$, ovvero l'inseme costituito da tutte le coppie ordinate (s,t) di prima coordinata $s \in S$ e seconda coordinata $t \in T$.

Esempio 1.3.9 Siano $S = \{1,2,3\}$ e $T = \{1, a, \{1\}\}$. Allora $S \times T = \{(1,1),(1,a),(1,\{1\}),(2,1),(2,a),(2,\{1\}),(3,1),(3,a),(3,\{1\})\}$.

Osserviamo che $\emptyset \times T = \emptyset$ e $S \times \emptyset = \emptyset$.

Proposizione 1.3.10 *Siano* S *e* T *insiemi non vuoti allora* $S \times T = T \times S \iff S = T$.

Dimostrazione – "$\Leftarrow$" Ovvia.

"$\Rightarrow$" Sia $x \in S$. Sia y un elemento di T, allora $(x,y) \in S \times T$, e per ipotesi $(x,y) \in T \times S$. In particolare $x \in T$. Analogamente si prova che T è incluso in S. □

1.4 PARTIZIONE DI UN INSIEME

Sia S un insieme non vuoto e sia $\mathfrak{F}$ un insieme di parti di S. Si dice che $\mathfrak{F}$ è una *partizione* di S se valgono le seguenti condizioni:

(1) $\forall X \in \mathfrak{F}, X \neq \emptyset$;

(2) $\forall X, Y \in \mathfrak{F}, X \neq Y \Rightarrow X \cap Y = \emptyset$;

(3) $S = \bigcup_{X \in \mathfrak{F}} X$.

Esempio 1.4.1 Sia $S = \{a, b, c, 2, 3\}$.

$\mathfrak{F}_1 = \{\{a, b, 2\}, \{c, a\}, \{3\}\}$ non è una partizione.

$\mathfrak{F}_2 = \{\emptyset, \{a\}, \{b\}, \{c\}, \{2\}, \{3\}\}$ non è partizione perché non verifica la 1).

$\mathfrak{F}_3 = \{\{a, \}, e, \{2, b, 3\}\}$ non è partizione poiché "e" non è sottoinsieme di S (ma anche perché "c" non appartiene ad alcun sottoinsieme di $\mathfrak{F}_3$).

$\mathfrak{F}_4 = \{\{a, b, 2\}, \{c\}, \{3\}\}$ è una partizione di S.

Esempio 1.4.2 Sia S un insieme non vuoto, allora l'insieme $F = \{S\}$ è una partizione di S.

Chiaramente se $\mathfrak{F}$ è una partizione di S, allora la sua cardinalità coincide con la somma delle cardinalità di tutti gli elementi di F:

$$|S| = \sum_{X \in \mathfrak{F}} |X|.$$

Esempio 1.4.3 Nell'esempio 1.4.1 abbiamo $|S| = |\{a, b, 2\}| + |\{c\}| + |\{3\}| = 5$.

Esercizio 1.4.4 Sia $S = \{1, 2, 3, 4, 5, c, f, d\}$ Scrivere due esempi di partizioni di S. Scrivere due insiemi di parti di S che non sono partizione di S.

Esercizio 1.4.5 Siano A e B insiemi. Esprimere una condizione sufficiente affinché l'insieme $\{A \setminus B, B \setminus A, A \cap B\}$ sia una partizione di $A \cup B$.

Esempio 1.4.6 Ad una prova di Analisi matematica vengono assegnati due quesiti a e b, e tutti i 60 studenti svolgono correttamente almeno 1 quesito. Inoltre 5 studenti svolgono soltanto la prova a correttamente, e 20 studenti svolgono soltanto la prova b correttamente. Stabilire quanti studenti svolgono correttamente entrambe le prove. Porre:

$S := \{x : x$ è uno studente che ha sostenuto l' esame$\}$, $|S| = 60$;

$A := \{x \in S : x$ ha svolto correttamente la prova a$\}$;

$B := \{x \in S : x$ ha svolto correttamente la prova b$\}$;

$A \cap B := \{x \in S : x$ ha svolto correttamente entrambe le prove$\}$.

Allora le cardinalità degli insiemi $B \setminus A$ e $A \setminus B$ sono note.

Poiché l'insieme $\{A \setminus B, B \setminus A, A \cap B\}$ è una partizione di $A \cup B = S$, posto y la cardinaltà dell'insieme $A \cap B$ risulta:

$5 + 20 + y = 60$, per cui $y = 35$.

CAPITOLO 2

CORRISPONDENZE TRA INSIEMI

2.1 GENERALITÀ

Sia S l'insieme degli studenti della facoltà di Scienze, e sia T l'insieme dei docenti dell'Università di Salerno. Dal prodotto cartesiano $S \times T$ selezioniamo solo le coppie (s,t) tali che s sia studente di un corso tenuto dal docente t nell'a.a. 2009/2010, in questo modo individuiamo un sottoinsieme G di $S \times T$, ed abbiamo evidenziato una corrispondenza tra studenti e docenti.

In termini formali, se S e T sono insiemi non vuoti, diremo *corrispondenza tra S e T* una coppia $\mathfrak{R}=(S \times T, G)$ dove G è un sottoinsieme di $S \times T$. Il sottoinsieme G è detto *grafico della corrispondenza*, e considerati $x \in S$ e $y \in T$, diremo che x e y *si corrispondono* in $\mathfrak{R}$, se $(x,y) \in G$. In tal caso scriveremo $x\mathfrak{R}y$.

Esempio 2.1.1 $S = \{1,2,3\}$ $T = \{a,b,c\}$. Cosideriamo tre corrispondenze distinte tra S e T.

- $\mathfrak{R}_1 = (S \times T, G)$, dove $G = \{(1,b);(3,a)\}$. In questa corrispondenza abbiamo soltanto: $1\mathfrak{R}b$ e $3\mathfrak{R}a$.
- $\mathfrak{R}_2 = (S \times T, S \times T)$. Questa è la *corrispondenza totale.*
- $\mathfrak{R}_3 = (S \times T, \emptyset)$. Questa è la *corrispondenza vuota.*

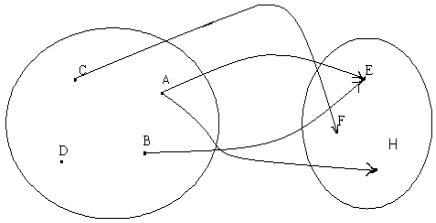
Esempio 2.1.2 $\mathfrak{R}=(\mathbb{N} \times \mathbb{Z}, G)$, dove $G = \{(x,y) \in \mathbb{N}^2 : x = y^2\}$. In questa corrispondenza abbiamo ad esempio

$$4\mathfrak{R}2, \quad 9\mathfrak{R}3, \quad 2 \not\mathfrak{R}3.$$

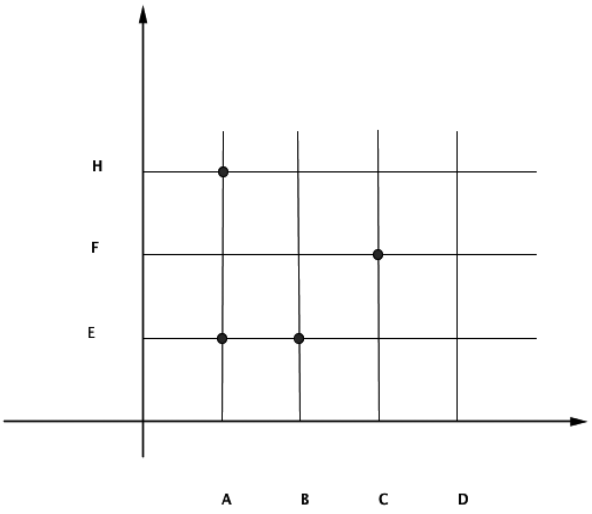
Esempio 2.1.3 La coppia $\mathfrak{R}_1$=($\mathbb{N}_0 \times \mathbb{N}_0, G_1$), con $G_1 = \{(x, y) \in \mathbb{Z} \times \mathbb{N}_0 : x^2 = y\}$ non è una corrispondenza. Infatti la coppia $(-2, 4) \in G_1$, ma $(-2, 4) \notin \mathbb{N}_0 \times \mathbb{N}_0$.

Esercizio 2.1.4 Trovare coppie di elementi che si corrispondono e coppie di elementi che non si corrispondono nella relazione $\mathfrak{R}_2$=($\mathbb{N}_0 \times \mathbb{N}_0, G_2$), dove $G_2 = \{(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0 : x^2 = y\}$.

Una corrispondenza tra S e T si può anche rappresentare graficamente, collegando gli elementi di S con gli elementi di T usando delle linee orientate. Tale rappresentazione di dice *sagittale*. Ad esempio se $S = \{A, B, C, D\}$ e $T = \{E, F, H\}$, ed $\mathfrak{R} = (S \times T, G)$, dove $G = \{(A, E), (A, H)(B, E), (C, F)\}$, allora la sua rappresentazione sagittale è:



Un'altro metodo grafico è la cosiddetta rappresentazione *cartesiana*, in cui si evidenziano su un riferimento cartesiano le coppie del grafico della corrispondenza tra S e T, dopo aver disposto gli elementi di S sull'asse delle ascisse, e gli elementi di T sull'asse delle ordinate. Ad esempio la rappresentazione cartesiana della corrispondenza precedente è:



In questo capitolo presenteremo due importanti tipi di corrispondenze: Le relazioni binarie e le applicazioni.

2.2 RELAZIONI BINARIE

Una corrispondenza di un insieme in se stesso si chiama *relazione binaria*. Quindi una relazione binaria in S è una coppia del tipo $\mathfrak{R}$=(S × S, G).

Diremo *diagonale di S*, l'insieme $\Delta_S := \{(x, y) \in S^2 : x = y\}$, e la relazione $\mathfrak{R}$=(S × S, Δ_S) la chiameremo *relazione identica*. Osserviamo che in tal caso $x \mathfrak{R} y \iff (x, y) \in \Delta_S \iff x = y$.

Sia S un insieme e sia $\mathfrak{R}$ una relazione binaria in S, diremo che:

(1) $\mathfrak{R}$ è *riflessiva* se $\forall x \in S$, $x \mathfrak{R} x$;

(2) $\mathfrak{R}$ è *simmetrica* se $\forall x, y \in S$, $x \mathfrak{R} y \Rightarrow y \mathfrak{R} x$;

(3) $\mathfrak{R}$ è *transitiva* se $\forall x, y, z \in S$, $x \mathfrak{R} y$ e $y \mathfrak{R} z \Rightarrow x \mathfrak{R} z$;

(4) $\mathfrak{R}$ è *asimmetrica* se $\forall x, y \in S$, $x \mathfrak{R} y$ e $y \mathfrak{R} x \Rightarrow x = y$;

(5) $\mathfrak{R}$ è *antiriflessiva* se $\forall x \in S, x \not\mathfrak{R} x$;

(6) $\mathfrak{R}$ è *antisimmetrica* se $\forall x, y \in S$, $x\mathfrak{R}y \Rightarrow y \not\mathfrak{R}x$.

Esempio 2.2.1 Nell'insieme S costituito dagli elementi $\{a, b, c, d\}$ possiamo definire una relazione simmetrica riflessiva ma non transitiva. A tal scopo consideriamo l'insieme

$$G = \{(a,a)(b,b)(c,c)(d,d)(a,b)(b,a)(b,c)(c,b)\}.$$

Allora la relazione $\mathfrak{R} = (S \times S, G)$ è simmetrica riflessiva ma non transitiva.

Esercizio 2.2.2 Individuare altre relazioni definite in S, che verificano certe proprietà e che non verificano altre.

Esercizio 2.2.3 È possibile definire in S una relazione antiriflessiva che non sia transitiva?

Per quanto detto, per definire una relazione binaria in un insieme S basta considerare x ed y elementi generici di S ed esprime quand'è che $x\mathfrak{R}y$.

Esempio 2.2.4 Sia Σ l'insieme costituito dalle rette del piano cartesiano, e sia $\mathfrak{R}$ la relazione binaria in Σ definita ponendo:
$r\mathfrak{R}s \iff$ r ed s hanno almeno un punto in comune. Allora $\mathfrak{R}$ non è transitiva.

Esercizio 2.2.5 Nell'insieme $\mathbb{Z}$ sia $\mathfrak{R}$ la relazione binaria definita ponendo:

$$r\mathfrak{R}s \iff r - s \text{ è un numero divisibile per } 10.$$

Quali proprietà verifica $\mathfrak{R}$?

Esercizio 2.2.6 Sia S un insieme e $\mathfrak{R}$ una relazione transitiva in S. Stabilire se la seguente equivalenza è verificata:
$\mathfrak{R}$ è antiriflessiva $\iff$ $\mathfrak{R}$ è antisimmetrica.

- **Relazioni di Equivalenza**

Una relazione binaria di S si dice *di equivalenza* se è riflessiva simmetrica e transitiva.

Esempio 2.2.7 Sia Σ l'insieme costituito dalle rette del piano cartesiano, e siano le relazioni binarie definite come segue:

- $r\mathfrak{R}_1 s$ se e solo se r ed s sono perpendicolari.

- $r\mathfrak{R}_2 s$ se e solo se r ed s sono parallele.
- $r\mathfrak{R}_3 s$ se e solo se r ed s sono incidenti.

Verificare che la relazione $\mathfrak{R}_2$ è di equivalenza. Cosa possiamo dire delle altre due relazioni?

Esercizio 2.2.8 Sia $G = \{(3,2),(2,5),(3,7),(9,9)\}$, e I_{10} l'insieme dei primi 10 numeri naturali positivi.

- È possibile completare l'insieme G in modo tale che $\mathfrak{R} = (I_{10} \times I_{10}, G)$ sia una relazione di equivalenza?
- È possibile completare l'insieme G in modo tale che $\mathfrak{R} = (I_{10} \times I_{10}, G)$ sia una relazione non transitiva?
- È possibile completare l'insieme G in modo tale che $\mathfrak{R} = (I_{10} \times I_{10}, G)$ sia una relazione antiriflessiva?

Siano x, y elementi di un insieme S in cui è definita una relazione di equivalenza $\mathfrak{R}$. Se $x\mathfrak{R}y$, diremo che x *ed* y *sono equivalenti modulo* $\mathfrak{R}$ e scriveremo $x \equiv y (\mathrm{mod}\ \mathfrak{R})$. Diremo *classe di equivalenza di* x *modulo* $\mathfrak{R}$ il sottoinsieme $[x]_{\mathfrak{R}} = \{y \in S : \ x \equiv y (\mathrm{mod}\ \mathfrak{R})\}$ costituito dagli elementi di S equivalenti ad x.

Concettualmente una relazione di equivalenza identifica gli elementi equivalenti di un insieme.

Esempio 2.2.9 In $\mathbb{Z}$ sia $\mathfrak{R}$ la relazion binaria definita ponendo: $x\mathfrak{R}y \iff 24$ divide $y - x$.

Tale relazione è di equivalenza. La classe $[6]_{\mathfrak{R}}$ è costituita da tutti i numeri del tipo $6 + 24k$. Nel linguaggio comune spesso facciamo uso delle classi di equivalenza senza rendercene conto. Infatti se diciamo "alle ore sei", intendiamo riferirci alle ore sei di tutti i giorni. Allora l'intera classe $[6]_{\mathfrak{R}}$ potrebbe rappresentare le ore 6 di tutti i giorni.

• Relazioni d' Ordine

Sia S un insieme non vuoto. Una relazione binaria in S la diremo *d'ordine largo* se è riflessiva asimmetrica e transitiva.

Esempio 2.2.10 In $\mathbb{N}$ sia $\mathfrak{R}$ la relazione binaria definita ponendo: $x\mathfrak{R}y \iff \exists z \in \mathbb{N}_0 : y = z + x$. Tale relazione è d'ordine largo. La chiameremo *relazione d'ordine usuale in* $\mathbb{N}$ e la denoteremo anche col simbolo $x \leqslant_u y$.

Esempio 2.2.11 Sia T un insieme, e sia $S = \wp(T)$. Gli elementi di S sono sottoinsiemi di T, e quindi si possono confrontare mediante l'inclusione. Sia quindi $\mathfrak{R}$ la relazione binaria definita ponendo: $X\mathfrak{R}Y \iff X \subseteq Y$. Tale relazione è d'ordine largo, e si chiama *relazione di inclusione in* S e verrà denotata col simbolo "$\subseteq$".

Esercizio 2.2.12 Sia $G = \{(3,2),(2,3),(2,5),(3,7),(9,9)\}$, e I_{10} l'insieme dei primi 10 numeri naturali positivi. È possibile completare l'insieme G in modo tale che $\mathfrak{R} = (I_{10} \times I_{10}, G)$ sia una relazione di ordine largo?

Sia S un insieme non vuoto. Una relazione binaria in S la diremo *d'ordine stretto* se è antiriflessiva e transitiva.

Esempio 2.2.13 In $\mathbb{N}$ sia $\mathfrak{R}$ la relazione binaria definita ponendo: $x\mathfrak{R}y \iff x < y$. Tale relazione è d'ordine stretto.

Esempio 2.2.14 Sia T un insieme, e sia $S = \wp(T)$. Gli elementi di S sono sottoinsiemi di T, e quindi si possono confrontare mediante l'inclusione. Sia quindi $\mathfrak{R}$ la relazione binaria definita in S, ponendo: $X\mathfrak{R}Y \iff X \subset Y$. Tale relazione è d'ordine stretto, e la diremo *relazione di inclusione stretta in* S, e verrà denotata col simbolo "$\subset$".

Una relazione binaria $\mathfrak{R}$ definita in S la diremo *d'ordine* se è d'ordine largo oppure d'ordine stretto.

Esercizio 2.2.15 Siano $a = p_1^{e_1}p_2^{e_2}\dots p_s^{e_s}$ e $b = q_1^{f_1}q_2^{f_2}\dots q_t^{f_t}$ interi positivi espressi come prodotti di potenze di numeri primi. In $\mathbb{N}$ siano le seguenti relazioni binarie definite ponendo:

$$a\mathfrak{R}_1 b \iff e_1 + e_2 + \dots + e_s \leqslant f_1 + f_2 + \dots + f_t$$

$$a\mathfrak{R}_2 b \iff e_1 + e_2 + \dots + e_s < f_1 + f_2 + \dots + f_t$$

Stabilire quali delle due relazioni suddette è d'ordine.

Sia $\mathfrak{R} = (S \times S, G)$ una relazione d'ordine largo definita in un insieme S. Consideriamo la relazione binaria in S definita ponendo: $x\mathfrak{R}^{\wedge}y \iff x\mathfrak{R}y$ e $x \neq y$. Si verifica facilmente che la relazione $\mathfrak{R}^{\wedge}$ è d'ordine stretto. La relazione $\mathfrak{R}^{\wedge}$ la diremo *associata* ad $\mathfrak{R}$.

Osserviamo che il grafico della relazione $\mathfrak{R}^{\wedge}$ coincide con $G \setminus \Delta_S$.

Esempio 2.2.16 Sia S un insieme. La relazione d'ordine stretta associata alla relazione di inclusione in S coincide con la relazione di inclusione stretta in S.

Dualmente se $\mathfrak{R} = (S \times S, G)$ una relazione d'ordine stretto definita in un insieme S, allora la relazione binaria definita ponendo: $x\mathfrak{R}^{\vee}y \iff x\mathfrak{R}y$ oppure $x = y$ è d'ordine largo. La relazione $\mathfrak{R}^{\vee}$ la diremo *associata* ad $\mathfrak{R}$.

Osserviamo che il grafico della relazione $\mathfrak{R}^{\vee}$ coincide con $G \cup \Delta_S$.

Pertanto qualunque sia il tipo di relazione d'ordine $\mathfrak{R}$, avremo che la relazione associata alla relazione associata ad $\mathfrak{R}$ coincide con $\mathfrak{R}$.

Se non vi è ambiguità una relazione d'ordine la denoteremo indifferentemente col simbolo "$<$", oppure col simbolo "$\leqslant$", a seconda se si vuole evidenziare l'ordine stretto oppure quello largo.

2.3 APPLICAZIONI TRA INSIEMI

Alcune corrispondenze $(S \times T, G)$ hanno la paricolarità che ogni elemento di S è in corrispondenza con un unico elemento di T. Tali corrispondenze le diremo *applicazioni*. La corrispondenza $i_S = (S \times S, \Delta_S)$, dove Δ_S è la diagonale di S è evidentemente un' applicazione, che chiameremo *applicazione identica su* S. L'esempio introduttivo del primo paragrafo non è un'applicazione, in quanto ci sono studenti ai quali corrispondono più di un docente. Anche le tre corrispondenze riportate nell' esempio 2.1.1 non sono applicazioni. Nell'esercizio 2.1.4 la corrispondenza considerata è in realtà un'applicazione. Più formalmente diremo che una corrispondenza $f=(S \times T, G)$ è un'*applicazione di dominio* S *e codominio* T se per ogni elemento $x \in S$ esiste un' unica coppia $(x, y) \in G$ di prima coordinata x. Quindi se $f=(S \times T, G)$ è un'applicazione, ogni elemento x del dominio individua un unico elemento del codominio. Tale elemento si denota con $f(x)$ e si chiama *immagine di* x *mediante* f. Per un'applicazione f di dominio S vale la seguente implicazione: $\forall x, y \in S, x = y \Rightarrow f(x) = f(y)$.

Esercizio 2.3.1 Stabilire se la corrispondenza $(\mathbb{N} \times \mathbb{Z}, G)$, dove $G = \{(x, y) \in \mathbb{N} \times \mathbb{Z} : x = y^2\}$ è un'applicazione.

Esercizio 2.3.2 Stabilire se la corrispondenza $(\mathbb{N} \times \mathbb{Z}, G)$, dove $G = \{(x, y) \in \mathbb{N} \times \mathbb{Z} : x^2 = y\}$ è un'applicazione.

Esercizio 2.3.3 Stabilire se la corrispondenza $(\mathbb{N} \times \mathbb{Z}, G)$, dove $G = \{(x, y) \in \mathbb{Z} \times \mathbb{N} : x = y^2\}$ è un'applicazione.

Per descrivere il grafico di un'applicazione basta definire le immagini del generico elemento del dominio. Per questo motivo usualmente le applicazioni si presentano nella forma:

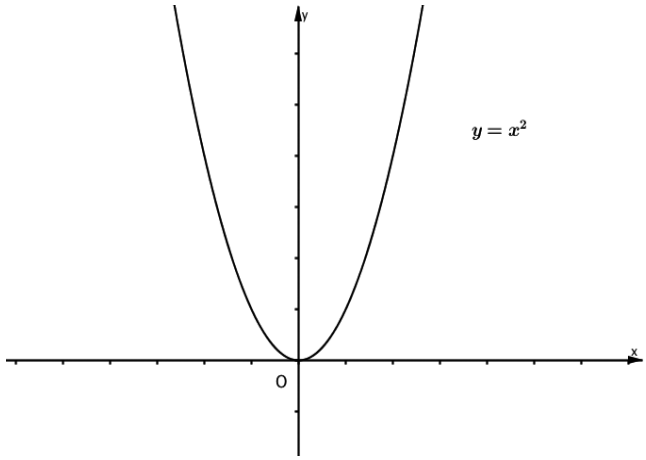
$$\begin{array}{l} f:\ S \to T \\ x \to f(x) \end{array}, \text{oppure equivalentemente } f:\ x \in S \to f(x) \in T.$$

Ad esempio la scrittura

$$\underset{x \to x^3,}{f:\ \mathbb{N} \to \mathbb{Z}}$$

rappresenta l'applicazione $f = (\mathbb{N} \times \mathbb{Z}, G)$, dove $G = \{(x, y) \in \mathbb{N} \times \mathbb{Z} : y = x^3\} = \{(x, x^3) : x \in \mathbb{N}\}$, e quindi $G = \{(x, f(x)) : x \in \mathbb{N}\}$.

Le funzioni reali elementari (studiate alle scuole superiori) sono esempi di applicazioni. Ciò che a suo tempo veniva detto "*grafico della funzione* f", coincide in base alle definizioni che abbiamo dato, con la rappresentazione cartesiana dell'applicazione f. Ad esempio il "grafico" della funzione $y = f(x) = x^2$, coincide con la rappresentazione cartesiana del grafico dell'applicazione di cui all'esercizio 2.3.2, ed è del tipo:



Se S e T sono insiemi non vuoti, la scrittura

$$f:\ S \to T$$

rappresenta una generica applicazione di dominio S e codominio T.

Sia f un'applicazione di dominio S e codominio T, e sia $X \subseteq S$. Diremo *immagine di* X *mediante* f, il sottoinsieme di T, denotato con $f(X)$, costituito dagli elementi del tipo $f(x)$ con $x \in X$. Formalmente $f(X) = \{f(x) : x \in X\}$

Esempio 2.3.4 *Sia* $f: x \in \mathbb{Z} \to 2x \in \mathbb{Z}$. Allora l'immagine di $\mathbb{N}$ mediante f è $f(\mathbb{N}) = \{f(x) : x \in \mathbb{N}\} = \{2x : x \in \mathbb{N}\}$, che coincide con l'insieme dei numeri pari positivi.

Sia f un'applicazione di dominio S e codominio T, e sia $Y \subseteq T$. Diremo *antiimmagine di* Y *mediante* f, il sottoinsieme di S, denotato con $f^{-1}(Y)$, costituito dagli elementi la cui immagine mediante f giace in Y. Formalmente $f^{-1}(Y) = \{x \in S : f(x) \in Y\}$

Esempio 2.3.5 *Sia* $f: x \in \mathbb{Z} \to x^2 \in \mathbb{Z}$. Allora l'antiimmagine di $\mathbb{N}$ mediante f è $f^{-1}(\mathbb{N}) = \{x \in \mathbb{Z} : f(x) \in \mathbb{N}\} = \{x \in \mathbb{Z} : x^2 \in \mathbb{N}\}$, che coincide con $\mathbb{Z} \setminus \{0\}$.

Sia f un'applicazione di dominio S e codominio T, diremo che f è *iniettiva* se elementi distinti di S hanno immagini distinte, ossia se vale l'implicazione: $\forall x, y \in S, x \neq y \Rightarrow f(x) \neq f(y)$. Dei due esempi precedenti il primo è di un' applicazione iniettiva, il secondo no.

Osserviamo che assegnata un' applicazione $f : S \to T$, ed un fissato elemento y di T, l'antiimmagine $f^{-1}(\{y\})$, può contenere più di un elemento. [1] Se f è iniettiva questo non accade, infatti dalla definizione di iniettività segue subito che esiste al più un elemento la cui immagine è y.

Sia f un'applicazione di dominio S e codominio T, diremo che f è *suriettiva* se ogni elemento del codominio T è immagine di almeno un elemento del dominio S. Nessuno dei due esempi precedenti è di un' applicazione suriettiva. Nel primo esempio i numeri dispari non sono immagine di alcun elemento del dominio; nel secondo esempio i numeri che non sono quadrati perfetti non sono immagine di alcun elemento del dominio. Un esempio di applicazione suriettiva è il seguente.

Osserviamo che assegnata un' applicazione $f : S \to T$, ed un fissato elemento y di T, l'antiimmagine $f^{-1}(\{y\})$ può essere l'insieme vuoto.[2] Se f è suriettiva questo non accade, infatti dalla definizione di suriettività segue subito che esiste almeno un elemento la cui immagine è y.

Esempio 2.3.6 $f: x \in \mathbb{Z} \to |x| \in \mathbb{N}_0$.

Sia f un'applicazione di dominio S e codominio T, diremo che f è *biettiva* se è sia iniettiva che suriettiva, ed una applicazione biettiva di un insieme in se stesso la diremo *permutazione*.

1 $f : x \in \mathbb{Z} \to x^2 \in \mathbb{N}_0$. Risulta $f^{-1}(\{4\}) = \{2, -2\}$
2 $f : x \in \mathbb{Z} \to x^2 \in \mathbb{N}_0$. Risulta $f^{-1}(\{5\}) = \emptyset$

Per quanto abbiamo già osservato se $f : S \to T$ è un' applicazione biettiva, l'antiimmagine $f^{-1}(\{y\})$, di un elemento y di T è costituita esattamente da un singolo elemento di S.

Esercizio 2.3.7 Quante permutazioni di I_3 ci sono?

Esercizio 2.3.8 Sia A l'insieme delle lettere dell'alfabeto.

- È possibile definire un'applicazione di iniettiva di dominio $\mathbb{N}$ e codominio A?
- È possibile definire un'applicazione di iniettiva di dominio A e codominio $\mathbb{N}$?

Esercizio 2.3.9 Sia

$$\begin{array}{rccc} f : \mathbb{Z} & \to & \mathbb{Z} \\ x \to & \begin{cases} x^3 \text{ se } x \notin \mathbb{N} \\ x^2 \text{ se } x \in \mathbb{N} \end{cases} & & \end{array}$$

(a) Stabilire se f è iniettiva.

(b) Stabilire se f è suriettiva.

(c) Determinare $f^{-1}(\{1\})$.

2.4 COMPOSIZIONE DI APPLICAZIONI

Siano S, T e V insiemi non vuoti, e siano f un'applicazione di dominio S e codominio T e g un'applicazione di dominio T e codominio V. Diremo *applicazione composta da* f *e da* g e la denoteremo col simbolo $g \circ f$ l'applicazione di dominio S codominio V e grafico $\{(x, g(f(x))) : x \in S\}$. Spesso un' applicazione composta si rappresenta con un disegno:

$$\begin{array}{ccc} S & \xrightarrow{g\circ f} & V \\ \downarrow f & g \nearrow & \\ T & & \end{array} .$$

Esempio 2.4.1 $f : x \in \mathbb{Z} \to x^2 \in \mathbb{N}_0$, e $g : x \in \mathbb{N}_0 \to \sqrt[3]{x} \in \mathbb{R}$. Allora $g \circ f : x \in \mathbb{Z} \to \sqrt[3]{x^2} \in \mathbb{R}$, infatti $g(f(x)) = g(x^2) = \sqrt[3]{x^2}$.

Osserviamo che qualunque sia l'applicazione $f : S \to T$, essa si può comporre a sinistra con i_T (l'applicazione identica su T) e a destra con i_S (l'applicazione identica su S). Entrambe le composte $i_T \circ f$ e $f \circ i_S$ coincidono chiaramente con l'applicazione f.

La seguente proposizione traduce la proprietà associativa della composizione.

Proposizione 2.4.2 *Siano* S, T, U *e* V *insiemi non vuoti, e siano* $f : S \to T$, $g : T \to U$ *e* $h : U \to V$ *applicazioni. Allora* $h \circ (g \circ f) = h \circ g) \circ f$

È da osservare che date due applicazioni f e g, talvolta si possono considerare entrambe le composte $g \circ f$ e $f \circ g$. Chiaramente non è detto che coincidono. Esprimeremo ciò dicendo che la composizione di applicazioni non è commtativa.

Esempio 2.4.3 $f : x \in \mathbb{Z} \to x^2 \in \mathbb{N}_0$ e $g : x \in \mathbb{N}_0 \to -x \in \mathbb{Z}$. Risulta $g \circ f \neq f \circ g$.

Proposizione 2.4.4 *Siano* S, T *e* V *insiemi non vuoti, e siano* $f : S \to T$ *e* $g : T \to V$ *applicazioni.*

(a) *Se* f *e* g *sono iniettive allora* $g \circ f$ *è iniettiva.*

(b) *Se* f *e* g *sono suriettive allora* $g \circ f$ *è suriettiva.*

(c) *Se* f *e* g *sono biettive allora* $g \circ f$ *è biettiva.*

Dimostrazione — 1) Siano x e y elementi del dominio di $g \circ f$, e supponiamo che $(g \circ f)(x)=(g \circ f)(y)$, allora $g(f(x)) = g(f(y))$. Poiché g è iniettiva risulta $f(x) = f(y)$, ma anche f è iniettiva quindi $x = y$.

2) Sia $v \in V$, e proviamo che esiste un elemento in S la cui immagine mediante $(g \circ f)$ è v. Per ipotesi g è suriettiva, allora esiste un elemento $t \in T$ tale che $g(t) = v$. D' altra parte anche f è suriettiva quindi esiste $s \in S$ tale che $f(s) = t$. L'elemento del dominio che cercavamo è proprio s. Infatti risulta: $(g \circ f)(s) = g(f(s)) = v$.

3) $g \circ f$ è iniettiva in quanto sia f che g sono iniettive; ma $g \circ f$ è anche suriettiva in quanto sia f che g sono suriettive; quindi $g \circ f$ risulta essere biettiva. □

Esercizio 2.4.5 Sia $f : x \in \mathbb{R} \to x^3 + 6x^2 + 12x + 89 \in \mathbb{R}$.

(a) Stabilire se f è iniettiva.

(b) Stabilire se f è suriettiva.

(c) Stabilire se f è biettiva.

Osserviamo che se la composta di due applicazioni f e g è biettiva non è detto che le due applicazioni f e g siano biettive.

Esempio 2.4.6 Siano $S = \{1, 2\}$ e $T = \{a, b, c\}$, e siano

$$\begin{array}{c} f : S \longrightarrow T \\ 1 \to c \\ 2 \to b \end{array} \qquad \text{e} \qquad \begin{array}{c} g : T \longrightarrow S \\ a \to 1 \\ b \to 2 \\ c \to 1 \end{array}$$

(In questo modo si vuole denotare il grafico dell'applicazione f, come l'insieme costituito dalle coppie $(1, c)$ e $(2, b)$; ed il grafico dell'applicazione g, come l'insieme costituto dalle coppie $(a, 1), (b, 2)$ e $(c, 3)$).

Appare evidente che in questo esempio le applicazioni f e g non sono biettive mentre l'applicazione composta $g \circ f$ è l'applicazione identica (i_S) su S, pertanto è biettiva. Osserviamo che in questo caso si puo' considerare anche l'applicazione composta $f \circ g$, la quale non è biettiva in quanto non è suriettiva (non è neanche iniettiva).

Proposizione 2.4.7 *Siano S, T e V insiemi non vuoti, e siano $f : S \to T$ e $g : T \to V$ applicazioni.*

(a) *Se $g \circ f$ è iniettiva allora f è iniettiva;*

(b) *Se $g \circ f$ è suriettiva allora g è suriettiva.*

Dimostrazione — (a) Siano x e y elementi di S tali che $f(x) = f(y)$ e proviamo che $x = y$. Allora $g(f(x)) = g(f(y))$, e per ipotesi $x = y$.

(b) Sia v un elemento di V , allora per ipotesi esiste un elemento s di S tale che $(g \circ f)(s) = v$. L'elemento $f(s)$ appartiene a T, e la sua immagine mediante g è v. Pertanto g è suriettiva. □

Sia $f : S \to T$ un'applicazione. Diremo che f è *invertibile* se esiste una applicazione $g : T \to S$ tale che

$$g \circ f = i_S \quad \text{e} \quad f \circ g = i_T.$$

Se una tale applicazione esiste essa è unica (vedi proposizione 2.4.8), si denota col simbolo "f^{-1}" e si chiama *inversa di* f.

Proposizione 2.4.8 *Sia $f : S \to T$ un' applicazione invertibile, allora esite un'unica applicazione $g : T \to S$ tale che $g \circ f = i_S$ e $f \circ g = i_T$.*

DIMOSTRAZIONE – Sia $g : T \to S$ e $g_1 : T \to S$ come nelle ipotesi, e proviamo che $g = g_1$. Risulta $g_1 = (g_1 \circ i_T) = g_1 \circ (f \circ g) = (g_1 \circ f) \circ g = i_S \circ g = g$. □

Teorema 2.4.9 (CARATTERIZZAZIONE DELLE APPLICAZIONI INVERTIBILI) *Sia* $f : S \to T$ *un'applicazione. Allora* f *è invertibile se e solo se* f *è biettiva.*

DIMOSTRAZIONE – Sia $f : S \to T$ un' applicazione invertibile, allora esiste $g : T \to S$ tale che $g \circ f = i_S$ e $f \circ g = i_T$. Per la (a) della Proposizione 2.4.7 si ha che f è iniettiva, e per la (b) della stessa Proposizione si ha che f è suriettiva.

Viceversa, se f è biettiva, allora per quanto osservato in precedenza esiste un unico elemento, $x \in S : f(x) = y$, ovvero $|\{y \in T : f^{-1}(\{y\})\}| = 1$. Consideriamo $g : T \to S$ l'applicazione il cui grafico è

$$G = \{(y, x) \in T \times S : \text{ “x è l'unico elemento di S: } f(x) = y\text{”}\}.$$

In particolare appartengono a G tutte le coppie del tipo $(f(x), x)$ con $x \in S$. Allora $(g \circ f)(x) = g(f(x) = x$ e $(f \circ g)(y) = f(g(y)) = y$. □

Proposizione 2.4.10 *Siano* $f : S \to T$ *e* $g : T \to V$ *applicazioni invertibili. Allora* $g \circ f$ *è invertibile e risulta* $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

DIMOSTRAZIONE – Per ipotesi f e g sono invertibili. Per il teorema di caratterizzazione sono entrambe biettive e quindi la loro composta è biettiva. Utilizzando nuovamente il suddetto teorema abbiamo che $g \circ f$ è invertibile. Componendo l' applicazione $g \circ f$ a destra con l'applicazione $f^{-1} \circ g^{-1}$ si ottiene l' applicazioni identica di V:

$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ f \circ f^{-1} \circ g^{-1} = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ i_T \circ g^{-1} = g \circ g^{-1} = i_V$.

Componendo a sinistra con $f^{-1} \circ g^{-1}$ si ottiene l'applicazione identica su S:

$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ g^{-1} \circ g \circ f = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ i_T \circ f = f^{-1} \circ f = i_S$. Pertanto l'applicazione $f^{-1} \circ g^{-1}$ è l' inversa di $g \circ f$. □

Assegnata un'applicazione invertibile $f = (S \times T, G)$, per determinare il grafico dell'applicazione inversa f^{-1}, basta scambiare le coordinate delle coppie di G. Nella pratica bisogna esprimere gli elementi di S in funzione degli elementi di T.

Esempio 2.4.11 Sia $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ definita ponendo:

$$f(x) = \frac{x+3}{2}\,.$$

Tale applicazione è biettiva, e quindi invertibile. Per esprimere l'inversa f^{-1}, bisogna esprimere il generico elemento $x \in S$ in funzione di un elemento generico di $y \in T$. In questo caso basta risolvere l'equazione $y = \frac{x+3}{2}$. Per cui $f^{-1}(y) = x = 2y - 3$.

Siano S e T insiemi non vuoti. Diremo che S è *equipotente a* T se esiste un'applicazione biettiva di S in T. Evidentemente ogni insieme non vuoto è equipotente a se stesso. Inoltre, in virtù della caratterizzazione delle applicazioni invertibili, se S è equipotente a T allora anche T è equipotente a S, e quindi senza ambiguità potremo dire che gli insiemi S e T sono *equipotenti*. Gli insiemi $\mathbb{N}$ e $\mathbb{Z}$ sono equipotenti. Un esempio di applicazione biettiva di dominio $\mathbb{N}$ e codominio $\mathbb{Z}$ è il seguente:

Esempio 2.4.12 Sia $f : \mathbb{N} \longrightarrow \mathbb{Z}$ definita ponendo:

$$f(x) = \begin{cases} \frac{x}{2} \text{ se } x \text{ è pari} \\ \frac{-(x+1)}{2} \text{se } x \text{ è dispari} \end{cases} .$$

Tale applicazione è biettiva, quindi $\mathbb{N}$ e $\mathbb{Z}$ sono equipotenti. Descrivere l'inversa di f.

Esercizio 2.4.13 Sia $f : S \to T$ un'applicazione iniettiva. Verificare che S è equipotente ad $f(S)$.

2.5 RELAZIONI DI EQUIVALENZA ED INSIEME QUOZIENTE

In questo paragrafo evidenzieremo il collegamento che sussiste tra i concetti di relazioni di equivalenza e partizione. Proveremo inoltre due teoremi fondamentali dell'insiemistica.

Lemma 2.5.1 *Siano* S *un insieme non vuoto e* $\mathfrak{R}$ *una relazione di equivalenza in* S. *Per ogni* x *ed* y *elementi di* S, *risulta* $x \equiv y (\mathrm{mod}\mathfrak{R}) \iff [x]_{\mathfrak{R}} = [y]_{\mathfrak{R}}$.

DIMOSTRAZIONE – "$\Rightarrow$" Sia $z \in [x]_{\mathfrak{R}}$, allora $x \equiv z(\mathrm{mod}\mathfrak{R})$, e per ipotesi si ha anche $y \equiv x(\mathrm{mod}\mathfrak{R})$. Per la transitività che $y \equiv z(\mathrm{mod}\mathfrak{R})$, sicché $z \in [y]_{\mathfrak{R}}$. L'arbitrarietà dell'elemento z assicura che $[x]_{\mathfrak{R}} \subseteq [y]_{\mathfrak{R}}$. L'altra inclusione si prova analogamente.

"$\Leftarrow$" La relazione $\mathfrak{R}$ in particolare è riflessiva, quindi $x \in [x]_{\mathfrak{R}}$, e $y \in [y]_{\mathfrak{R}}$. Per ipotesi $x \in [y]_{\mathfrak{R}}$, e quindi $y \equiv x(\mathrm{mod}\mathfrak{R})$. Poiché $\mathfrak{R}$ è simmetrica si ha $x \equiv y(\mathrm{mod}\mathfrak{R})$. □

In virtù del lemma precedente ogni elemento y di una classe di equivalenza $[x]_{\mathfrak{R}}$, individua l'intera classe di equivalenza. Per questo motivo diremo che y è un *rappresentante* di $[x]_{\mathfrak{R}}$.

Il seguente risultato prova che le classi di equivalenza sono a due a due disgiunte.

Lemma 2.5.2 *Siano S un insieme non vuoto e $\mathfrak{R}$ una relazione di equivalenza in S. Per ogni x ed y elementi di S, risulta* $[x]_{\mathfrak{R}} \neq [y]_{\mathfrak{R}} \iff [x]_{\mathfrak{R}} \cap [y]_{\mathfrak{R}} = \emptyset$.

Dimostrazione — "$\Leftarrow$" Se per assurdo le classi $[x]_{\mathfrak{R}}$, e $[y]_{\mathfrak{R}}$ coincidono, allora la loro intersezione sarebbe diversa dal vuoto. Questo contraddice le ipotesi.

"$\Rightarrow$" Per assurdo sia z un elemento di $[x]_{\mathfrak{R}} \cap [y]_{\mathfrak{R}}$. Allora $x \equiv z(\mathrm{mod}\mathfrak{R})$ e $y \equiv z(\mathrm{mod}\mathfrak{R})$. Per il lemma precedente le classi $[x]_{\mathfrak{R}}, [y]_{\mathfrak{R}}$ e $[z]_{\mathfrak{R}}$ coincidono. Questa contraddizione prova la tesi. □

Siano S un insieme non vuoto e $\mathfrak{R}$ una relazione di equivalenza in S. L'insieme delle classi di equivalenza di S modulo $\mathfrak{R}$ si denota col simbolo $S/\mathfrak{R}$ e si chiama *insieme quoziente di S rispetto ad $\mathfrak{R}$*. È importante osservare che $S/\mathfrak{R}$ è costituito da parti non vuote a due a due disgiunte e la cui unione è S. In altri termini l'insieme quoziente è una partizione di S.

Esempio 2.5.3 Sia S un insieme non vuoto, e sia i_S la relazione identica su S. Allora si ha $S/i_S = \{\{x\} : x \in S\}$ ovvero l'insieme costituito da tutti i singleton.

Esempio 2.5.4 Sia S un insieme non vuoto, e sia τ la relazione totale su S. Tale relazione determinerà un' unica classe di equivalenza, allora si ha $S/\tau = \{S\}$ ovvero il singleton di S.

Esempio 2.5.5 Ogni coppia di punti (A, B) dello spazio euclideo $\mathbb{E}^3$ individua un segmento orientato $\overline{AB}$. È ben noto dalla geometria elementare che la relazione $\equiv$ definita nell'insieme dei segmenti orientati $\mathbb{V}^3$ ponendo:

$$(A, B) \equiv (C, D) \iff (A, B) \text{ e } (C, D) \text{ sono equipollenti,}$$

è una relazione di equivalenza. Ogni oggetto dell'insieme quoziente $\mathbb{V}^3/\equiv$ si dice *vettore libero geometrico*, e usualmente di denota col simbolo $\overrightarrow{AB} = [(A, B)]_{\equiv}$. Osserviamo che $(A, B) \equiv (C, D) \iff \overrightarrow{AB} = \overrightarrow{CD}$, e che i segmenti (orientati) appartenenti ad una stessa classe hanno tutti la stessa lunghezza. Diremo *modulo del vettore* $\overrightarrow{AB}$, e lo denoteremo con $|\overrightarrow{AB}|$, la lunghezza del segmento $\overline{AB}$.

Prima abbiamo osservato che ogni relazione di equivalenza su S individua una partizione di S. Il seguente risultato prova che vale anche il viceversa:

Teorema 2.5.6 (Fondamentale sulle relazioni di equivalenza) *Siano S un insieme non vuoto e $\mathfrak{F}$ una partizione di S. Allora esiste un'unica relazione di equivalenza $\mathfrak{R}_{\mathfrak{F}}$ in S tale che $S/\mathfrak{R}_{\mathfrak{F}} = \mathfrak{F}$.*

Dimostrazione – Proviamo dapprima l'esistenza. Sia $\mathfrak{R}_{\mathfrak{F}}$ la relazione binaria in S definita ponendo:

$$x\mathfrak{R}_{\mathfrak{F}}y \iff \text{esiste} X \in \mathfrak{F} : x, y \in X.$$

In sostanza x ed y stanno in relazione se appartengono ad uno stesso elemento della partizione.

Ogni elemento di S giace in qualche $X \in \mathfrak{F}$, e quindi $\mathfrak{R}$ è riflessiva.

Se $x\mathfrak{R}_{\mathfrak{F}}y$, allora x ed y appartengono a qualche $X \in \mathfrak{F}$, sicché si ha anche $y\mathfrak{R}_{\mathfrak{F}}x$, e $\mathfrak{R}_{\mathfrak{F}}$ è simmetrica.

Siano x, y, z elementi di S tali che $x\mathfrak{R}_{\mathfrak{F}}y$ e $y\mathfrak{R}_{\mathfrak{F}}z$. Per definizione esistono X e Y tali che $x, y \in X$ e $y, z \in Y$. Allora l'intersezione $X \cap Y$ è non vuota, ed essendo $\mathfrak{F}$ una partizione deve essere necessariamente $X = Y$. Sicché x e z giacciono in X, e quindi $x\mathfrak{R}_{\mathfrak{F}}z$. In questo modo abbiamo provato che $\mathfrak{R}_{\mathfrak{F}}$ è di equivalenza.

Per provare che $S/\mathfrak{R}_{\mathfrak{F}} = \mathfrak{F}$ verifichiamo che ogni classe di equivalenza di $\mathfrak{R}_{\mathfrak{F}}$ coincide con qualche elemento della partizione e viceversa. Allora basta osservare che se x è un elemento di S, e X è un elemento della partizione che lo contiene, risulta:

$$[x]_{\mathfrak{R}_{\mathfrak{F}}} = \{y \in S : x \equiv y (\mathrm{mod} \mathfrak{R}_{\mathfrak{F}})\} = \{y \in S : \ x, y \in X\} = X.$$

Resta da provare l'unicità. A tal scopo sia $\mathfrak{R}$ una relazione di equivalenza tale che $S/\mathfrak{R} = \mathfrak{F}$, e proviamo che $\mathfrak{R} = \mathfrak{R}_{\mathfrak{F}}$. Ciò si verifica facilmente osservando che per ogni x ed y elmenti di S, si ha $x \equiv y (\mathrm{mod} \mathfrak{R})$ se e solo se $[x]_{\mathfrak{R}} = [y]_{\mathfrak{R}}$, ed essendo $S/\mathfrak{R} = \mathfrak{F}$ questo accade se e solo se x ed y appartengono ad uno stesso elemento di $\mathfrak{F}$ e quindi se e solo se $x \equiv y (\mathrm{mod} \mathfrak{R}_{\mathfrak{F}})$. □

Ad ogni applicazione $f : S \to T$ rimane associata una relazione di equivalenza $\mathfrak{R}_f$ in S definita ponendo:

$$x\mathfrak{R}_f y \iff f(x) = f(y).$$

La relazione $\mathfrak{R}_f$ la diremo *relazione di equivalenza determinata da* f.

Esercizio 2.5.7 Sia $f : x \in \mathbb{Z} \to |x| \in \mathbb{Z}$
Studiare la relazione $\mathfrak{R}_f$. In particolare descrivere l'insieme quoziente $\mathbb{Z}/\mathfrak{R}_f$.

Sia $\mathfrak{R}$ una relazione di equivalenza definita in S. L'applicazione $\pi : x \in S \to [x]_{\mathfrak{R}} \in S/\mathfrak{R}$, che ad ogni elemento di S associa la classe che esso stesso individua, la diremo *applicazione canonica di* S *su* $S/\mathfrak{R}$.

Esercizio 2.5.8 Sia $f : x \in \mathbb{Z} \to |x| \in \mathbb{Z}$. Scrivere l'applicazione canonica di $\mathbb{Z}$ su $\mathbb{Z}/\mathfrak{R}_f$.

Esercizio 2.5.9 Sia S un insieme con 8 elementi e T un insieme con 5 elementi. Usando la rappresentazione sagittale, definire un' applicazione f di S in T. Descrivere l'insieme quoziente $S/\mathfrak{R}_f$, e definire l'applicazione canonica di S su $S/\mathfrak{R}_f$.

La nozione di applicazione canonica ha un ruolo rilevante nel prossimo risultato.

Teorema 2.5.10 (DI DECOMPOSIZIONE DELLE APPLICAZIONI) *Siano* S *e* T *insiemi non vuoti, e sia* $f : S \to T$ *un'applicazione. Allora esiste un'unica applicazione* $\varphi : S/\mathfrak{R}_f \to T$ *tale che* $\varphi \circ \pi = f$. *Inoltre* φ *è inettiva e* $\varphi(S/\mathfrak{R}_f) = f(S)$.

DIMOSTRAZIONE — Lo scopo è quello di individuare un'applicazione φ in modo da ottenere un diagramma del tipo

$$\begin{array}{ccc} S & \xrightarrow{f} & T \\ \downarrow \pi & \varphi \nearrow & \\ S/\mathfrak{R}_f & & \end{array} .$$

Poniamo $\varphi = (S/\mathfrak{R}_f \times T, G)$ la corrispondenza di $S/\mathfrak{R}_f$ in T definita dal grafico $G = \{([x]_{\mathfrak{R}_f}, f(x)) : x \in S\}$.
Siano $[x]_{\mathfrak{R}_f}$ e $[y]_{\mathfrak{R}_f}$ elementi di $S/\mathfrak{R}_f$ e osserviamo che:

$$[x]_{\mathfrak{R}_f} = [y]_{\mathfrak{R}_f} \iff x\mathfrak{R}_f y \iff f(x) = f(y).$$

Da ciò segue che per ogni classe X di $S/\mathfrak{R}_f$ esiste un'unica coppia in G di prima coordinata X. In altre parole la corrispondenza φ è un'applicazione. Quanto osservato prova anche che se $\varphi([x]_{\mathfrak{R}_f}) = \varphi([y]_{\mathfrak{R}_f})$ allora $[x]_{\mathfrak{R}_f} = [y]_{\mathfrak{R}_f}$ cioè φ è iniettiva. Inoltre per ogni x elemento di S risulta: $(\varphi \circ \pi)(x) = \varphi(\pi(x)) = \varphi([x]_{\mathfrak{R}_f}) = f(x)$, e quindi $\varphi \circ \pi = f$ e l'immagine di $S/\mathfrak{R}_f$ mediante φ coincide con $f(S)$.

Per provare l'unicità consideriamo un'applicazione $\psi : S/\mathfrak{R}_f \to T$ tale che $\psi \circ \pi = f$, e verifichiamo che $\psi = \varphi$. Per ogni elemento $[x]_{\mathfrak{R}_f}$ del dominio $S/\mathfrak{R}_f$ si ha:

$$\psi([x]_{\mathfrak{R}_f}) = \psi(\pi(x)) = (\psi \circ \pi)(x) = f(x) = \varphi([x]_{\mathfrak{R}_f}). \qquad \square$$

Osserviamo che in virtù del teorema di decomposizione se $f : S \to T$ è un'applicazione, allora $S/\mathfrak{R}_f$ e $f(S)$ sono equipotenti.

2.6 INSIEMI ORDINATI

Sia S un insieme, e sia $\mathfrak{R}$ una relazione d'ordine (largo o stretto) in S. Si dice *insieme ordinato* la coppia $(S, \mathfrak{R})$. Se la relazione è d'ordine largo in luogo di $\mathfrak{R}$ si userà il simbolo "$\leqslant$" (leggi minore o uguale), ed in luogo della relazione associata $\mathfrak{R}^\wedge$ il simbolo "$<$" (leggi minore strettamente). In tal modo $x < y \iff x \leqslant y$ e $x \neq y$. Se invece $\mathfrak{R}$ è d'ordine stretto si userà il simbolo "$<$" in luogo di $\mathfrak{R}$, ed il simbolo "$<$" in luogo della relazione associata $\mathfrak{R}^\vee$.

Esempio 2.6.1 Sia $S = \{9, b, d, 7, 5\}$, e sia $\mathfrak{R} = (S \times S, G)$ una relazione binaria in S definita dal grafico $G = \{(9, d), (9, 5), (d, 5), (b, 5)\}$. Tale relazione è d'ordine stretto. Quindi $(S, <)$ è un insieme ordinato. Con tale ordinamento risulta $9 < 5$, $9 < d$, $d < 5$ e $b < 5$. Osserviamo anche che il grafico della relazione "$\leqslant$" è $G \cup \Delta$, dove Δ è la diagonale di S, e quindi $9 \leqslant 5$, $9 \leqslant d$, $d \leqslant 5, b \leqslant 5$, $9 \leqslant 9$, $b \leqslant b, d \leqslant d$, $7 \leqslant 7$, $5 \leqslant 5$.

Sia $(S, "<")$ un insieme ordinato.

(i) Si dice che un elemento M di S è *massimo* in S se "$\forall x \in S, x \leqslant M$".

(ii) Si dice che un elemento m di S è *minimo* in S se "$\forall x \in S, m \leqslant x$".

Osserviamo che nell'esempio precedente l'insieme ordinato $(S, "\leqslant")$ è sprovvisto sia di massimo che di minimo. Rileviamo che se un insieme ordinato S ha un massimo M, allora esso è unico. Infatti se M_1 è un elemento massimo in S allora risulta $M \leqslant M_1$, e $M_1 \leqslant M$. Per le proprietà asimmetrica della relazione "$\leqslant$ " risulta $M_1 = M$. L'eventuale elemento massimo di un insieme ordinato S si denota anche col simbolo $max_{\leqslant} S$, oppure col simbolo $max S$ se non vi è ambiguità.

Analogamente si prova che se esiste un elemento minimo allora esso è unico. L'eventuale elemento minimo di un insieme ordinato S si denota anche col simbolo $\min_{\leqslant} S$, oppure col simbolo $\min S$ se non vi è ambiguità.

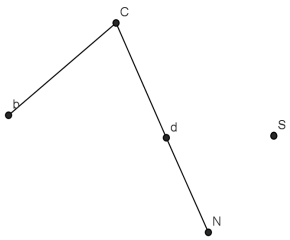
Sia $(S, \text{“} \leqslant \text{”})$ un insieme ordinato, e siano x, y e z elementi distinti di S. Diremo che z è *compreso tra* x *ed* y se $x < z < y$. Se x ed y non comprendono elementi, diremo che x ed y sono *consecutivi* .

Per rappresentare graficamente un insieme ordinato $(S, <)$ si può usare un disegno chiamato anche *Diagramma di Hasse*, che è costituito da vari segmenti i cui estremi rappresentano coppie di elementi consecutivi di S.

Nella pratica basta disegnare gli elementi di S come punti, avendo cura di collegare gli elementi consecutivi con un segmento che dal basso va verso l'alto.

Esempio 2.6.2 Sia $T = \{N, b, d, S, C\}$, e sia $\mathfrak{R} = (T \times T, G)$ una relazione binaria in S definita dal grafico $G = \{(N, d), (N, C), (d, C), (b, C)\}$

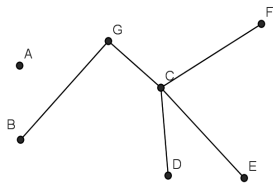
La Figura che segue è il diagramma di Hasse associato all'insieme ordinato $(T, <)$.



In questo diagramma di Hasse ci sono solo tre segmenti in quanto gli elementi N e C non sono consecutivi. È chiaro che se si costruisce il diagramma di Hasse a partire dalla relazione d'ordine (larga) associata a "$<$" si ottiene la stessa cosa, in quanto ai fini del disegno si considerano solo gli elementi consecutivi. È altrettanto chiaro che ogni diagramma ottenuto con poligonali

che vanno dal basso verso l'alto definisce un insieme di elementi e di coppie che individuano un insieme ordinato.

Esempio 2.6.3 Sia $S = \{A, B, C, D, E, , F, G\}$. La figura seguente può essere considerata il diagramma di hasse di una relazione d'ordine $\mathfrak{R}$ definita in S.



Il diagramma di Hasse rappresenta in modo efficace l'ordinamento in un insieme, senza dover distinguere se la relazione d'ordine che soggiace ad esso è stretta o larga. Nell'esempio in questione si capisce subito che l'insieme ordinato è privo di minimo e anche di massimo. Inoltre si nota che A è un punto *isolato* di S, ovvero che non è confrontabile con nessun elemento di S. Osserviamo inoltre che il grafico della relazione d'ordine stretto individuata dal diagramma della figura precedente, è $\Gamma = \{(B, G), (C, G), (D, C), (E, C), (C, F), (D, G), (E, G), (D, F), (E, F)\}$.
Per avere il grafico dell'ordinamento largo basta aggiungere la diagonale Δ.

Sia $(S, \mathfrak{R})$ un insieme ordinato, con $\mathfrak{R} = (S \times S, G)$, e sia X un sottoinsieme di S. È possibile definire una relazione in X. Basta considerare la coppia $\mathfrak{R}_X = (X \times X, G_X)$, dove $G_X = (X \times X) \cap G$. Se $\mathfrak{R}$ è d'ordine largo su S allora $\mathfrak{R}_X$ è d'ordine largo su X, Infatti:

- $\forall x \in X$ risulta $(x, x) \in (X \times X) \cap G = G_X$, quindi $x \mathfrak{R}_X x$;

- $\forall x, y \in X$ tali che $x\mathfrak{R}_X y$ e $y\mathfrak{R}_X x$, si ha che (x, y) e (y, x) giacciono in G. Essendo $\mathfrak{R}$ asimmetrica si ha $x = y$;
- $\forall x, y, z \in X$ tali che $x\mathfrak{R}_X y$ e $y\mathfrak{R}_X z$, le coppie $(x, y), (y, z)$ giacciono sia in $X \times X$ che in G. Per cui $(x, z) \in X \times X$, ed essendo $\mathfrak{R}$ transitiva si ha $(x, z) \in G$. Pertanto $(x, z) \in (X \times X) \cap G$, ossia $x\mathfrak{R}_X z$

Analogamente si prova che se $\mathfrak{R}$ è d'ordine stretto su S allora $\mathfrak{R}_X$ è d'ordine stretto su X. La relazione $\mathfrak{R}_X$ appena definita si chiama *relazione d'ordine indotta da* $\mathfrak{R}$ *su* X.

Esempio 2.6.4 Nell' insieme degli interi relativi $\mathbb{Z}$, la relazione d'ordine usuale "$\leqslant_u$" è d'ordine largo, e la sua relazione d'ordine stretto associata è "$<_u$". Le coppie $(\mathbb{Z},\leqslant_u)$ e $(\mathbb{Z},<_u)$ rappresentano quindi lo stesso insieme ordinato. Se consideriamo il sottoinsieme $\mathbb{N}$ di $\mathbb{Z}$, la relazione d'ordine indotta da $\leqslant_u$, (risp. da$<_u$) su $\mathbb{N}$ sarà semplicemente la relazione usuale larga (risp. stretta) in $\mathbb{N}$.

Esempio 2.6.5 Sia T un insieme, e sia $S = \wp(T)$. La relazione di inclusione "$\subseteq$" è d'ordine largo in S, e la sua relazione d'ordine stretto associata è "$\subset$". Le coppie $(S, \subseteq)$ e $(S, \subset)$ rappresentano quindi lo stesso insieme ordinato. Se X è un sottoinsieme S, la relazione d'ordine indotta da $\subseteq$, (risp. da $\subset$) su X sarà semplicemente la relazione di inclusione larga (risp. stretta) in X.

Sia $(S, <)$ un insieme ordinato, e sia X un sottoinsieme di S. Se non vi è ambiguità, la relazione $<_X$ indotta da "$<$" su X puo' essere ancora denotata col simbolo "$<$". Osserviamo, inoltre, che le proprietà dell'insieme ordinato $(X, <)$ non coincidono necessariamente con le proprietà dell'insieme ordinato $(S, <)$, come vedremo in seguito.

Esempio 2.6.6 Sia $T = \{1, a, r, 4\}$, e sia $S = \wp(T)$. L'insieme ordinato $(S, \subset)$ possiede massimo: $max_{\subset} S = T$. Sia $X = S \setminus \{T\}$. Appare chiaro invece che $(X, \subset)$ è privo di massimo (ad un tale elemento apparterrebbero tutti gli elementi di T).

Esercizio 2.6.7 Sia $T = \{1, a, r, 4\}$, e sia $S = \wp(T)$. Rappresentare con un diagramma di Hasse l'insieme ordinato $(S, \subset)$.

Esercizio 2.6.8 Sia $T = \{1, a, r, 4\}$, e sia $S = \wp(T)$. Determinare almeno due sottoinsiemi X ed Y di S, tali che $(X, \subset)$ e $(Y, \subset)$ siano privi di minimo.

Sia $(S, \leqslant)$ un insieme ordinato.

- Un elemento $a \in S$ si dice *minimale* se non esiste alcun elemento di S minore di a. (non esiste $b \in S$ tale che $b < a$).
- Un elemento $a \in S$ si dice *massimale* se non esiste alcun elemento di S maggiore di a (non esiste $b \in S$ tale che $a < b$).

Sia $(S, <)$ un insieme ordinato. Se S è dotato di massimo M (risp. minimo), tale elemento risulterà, chiaramente, anche elemento massimale (risp. minimale) in S.

Esempio 2.6.9 Sia $T = \{1, a, r, 4\}$, e sia $S = \wp(T)$. Sia $X = S \setminus \{T\}$. L'insieme $(X, \subset)$ è privo di massimo, però ciascun elemento $T \setminus \{1\}, T \setminus \{a\}, T \setminus \{r\}, T \setminus \{4\}$ è massimale in $(X, \subset)$.

Esercizio 2.6.10 Sia $(S, \leqslant)$ un insieme totalmente ordinato. Verificare che ogni elemento minimale è minimo.

Esercizio 2.6.11 Sia $(S, \leqslant)$ un insieme ordinato con un unico elemento minimale a. Stabilire se a è minimo di S.

Esercizio 2.6.12 Determinare gli eventuali elementi massimali o minimali, degli esempi di insiemi ordinati precedentemente esposti.

Sia $(S, \leqslant)$ un insieme ordinato, e sia $X \subseteq S$.

- Un elemento $a \in S$ si dice *minorante di* X se è minore o uguale di ogni altro elemento di X: $\forall x \in X, a \leqslant x$.
- Un elemento $a \in S$ si dice *maggiorante di* X se è maggiore o uguale di ogni altro elemento di X: $\forall x \in X, x \leqslant a$.

Esempio 2.6.13 Sia T l'insieme delle lettere dell'alfabeto, e sia $(S = \wp(T), \subset)$. Posto $X = \{\{a\}, \{z\}, \{s\}\}$, i seguenti elementi di S sono alcuni dei maggioranti di X:
$\{a, b, c, s, z\}$, $\{r, s, t, a, z, g, h\}$, $\{a, s, d, f, z...\}$. Il vuoto invece è l'unico minorante per X.

Sia $(S, \leqslant)$ un insieme ordinato, e sia $X \subseteq S$.

- Diremo che X è *superiormente limitato* se è dotato di qualche maggiorante.
- Diremo che X è *inferiormente limitato* se è dotato di qualche minorante.

Esempio 2.6.14 Sia T l'insieme delle lettere dell'alfabeto, e sia $(S = \wp(T), \subset)$. L'insieme $X = \{\{a\}, \{z\}, \{s\}\}$ è sia superiormente limitato che inferiormente limitato.

Esercizio 2.6.15 Sia S l'insieme dei numeri naturali maggiori o uguali a 2, e del tipo $2^\alpha 3^\beta$, con α e β elementi di $\mathbb{N}_0$: $S = \{2^\alpha 3^\beta \geqslant 2 : \ \alpha, \beta \in \mathbb{N}_0\}$. In S sia la relazione binaria definita ponendo: $\forall, x = 2^\alpha 3^\beta$ e $y = 2^\gamma 3^\delta$ elementi di S,

$$x \mathfrak{R} y \iff \alpha < \gamma \text{ e } \beta < \delta$$

.

(i) Stabilire se esistono sottoinsiemi infiniti di S superiormente limitati.

(ii) Stabilire se esistono sottoinsiemi infiniti di S non inferiormente limitati.

Ora diamo due definizioni:

- Sia $(S, \leqslant)$ un insieme ordinato, e sia X un sottoinsieme di S superiormente limitato. Diremo che X possiede *estremo superiore*, e lo denoteremo col simbolo $\sup_{\leqslant} X$, se l'insieme degli elementi di S che sono maggioranti di X possiede il minimo.
- Sia $(S, \leqslant)$ un insieme ordinato, e sia X un sottoinsieme di S inferiormente limitato. Diremo che X possiede *estremo inferiore*, e lo denoteremo col simbolo $\inf_{\leqslant} X$, se l'insieme degli elementi di S che sono minoranti di X possiede il massimo.

Esempio 2.6.16 Sia T l'insieme delle lettere dell'alfabeto, e consideriamo l'insieme ordinato $(\wp(T) \setminus \{\{a, z, s\}\}, \subset)$, dove T è l'insieme delle lettere dell'alfabeto. L'insieme $X = \{\{a\}, \{z\}, \{s\}\}$ è contenuto in $\wp(T) \setminus \{\{a, z, s\}\}$, ed è sia superiormente limitato che inferiormente limitato, d'altra parte l'insieme dei maggioranti non possiede minimo, e quindi X non possiede estremo superiore. Inoltre X possiede estremo inferiore e risulta $\inf_{\subset} X = \emptyset$.

Esercizio 2.6.17 Definire un insieme ordinato $(S, <)$, contenente un sottoinsieme X sia superiormente limitato che inferiormente limitato, dotato di estremo superiore e privo di estremo inferiore.

Osservazione 2.6.18 Sia $(\mathbb{Q}, <)$ l'insieme dei numeri razionali con l'ordinamento usuale. Sia X l'insieme dei razionali il cui quadrato è minore di 2: $X = \{x \in \mathbb{Q} : x^2 < 2\} = \{x \in \mathbb{Q} : x < \sqrt{2}\}$. Chiaramente X è superiormente limitato, d'altra parte ogni maggiorante deve essere maggiore di $\sqrt{2}$, per cui l'insieme dei maggioranti di X è privo di minimo (come è ben noto esistono infiniti razionali compresi tra un qualunque razionale e un qualunque numero irrazionale). Quindi X è privo di estremo superiore in $(\mathbb{Q}, <)$.

Esercizio 2.6.19 Sia $(\mathbb{R}, <)$ l'insieme dei numeri reali con l'ordinamento usuale quindi. Sia X l'insieme dei razionali il cui quadrato è minore di 2: $X = \{x \in \mathbb{Q} : x^2 < 2\} = \{x \in \mathbb{Q} : x < \sqrt{2}\}$. Possiamo affermare che X possiede l'estremo superiore in $(\mathbb{R}, <)$?

Sia $(S, \leqslant)$ un insieme ordinato.

- Diremo che S è *ben ordinato* se ogni parte non vuota di S è dotata di minimo: $\forall X \subset S, X \neq \emptyset \Rightarrow \exists min X$.
- Diremo che S è *totalmente ordinato* se ogni coppia di elementi di S è confrontabile: $\forall x, y \in S$, $x \leqslant y$ oppure $y \leqslant x$

Chiaramente un insieme totalmente ordinato $(S, <)$ induce su ogni suo sottoinsieme un ordinamento totale. Il diagramma di Hasse di un insieme totalmente ordinato finito èuna poligonale (verticale).

Rileviamo $(\mathbb{Z}, <)$ è totalmente ordinato, ma non è ben ordinato. In particolare non si inverte il seguente risultato:

Proposizione 2.6.20 *Sia $(S, \leqslant)$ un insieme ben ordinato. Allora $(S, \leqslant)$ è un insieme totalmente ordinato.*

Dimostrazione — Siano x, y elementi di S. Per ipotesi il sottoinsieme $X = \{x, y\}$ possiede minimo, e quindi risulta $x \leqslant y$ oppure $y \leqslant x$. □

La nozione che identifica gli insiemi ordinati è la "similitudine".

Siano $(S, <_1)$ e $(T, <_2)$ insiemi ordinati. Diremo che S e T sono *simili* se esiste una applicazione biettiva $f : S \to T$ tale che:

$$\forall x, y \in S, x <_1 y \Rightarrow f(x) <_2 f(y).$$

Una tale applicazione f si dice *similitudine* tra S e T.

Insiemi simili hanno (relativamente il loro ordinamento) le stesse proprietà, ed il loro studio si identifica a meno di una similitudine. Evidentemente due insiemi ordinati simili hanno lo stesso diagramma di Hasse.

Dalla teoria degli insiemi si prova poi l'esistenza di un insieme ben ordinato infinito $(S, \mathfrak{R})$ in cui ogni parte superiormente limitata è dotata di massimo. Si prova anche che ogni altro insieme ben ordinato infinito in cui ogni parte superiormente limitata sia dotata di massimo è simile a $(S, \mathfrak{R})$. In questo modo si perviene ad un modello dei numeri naturali (che finora abbiamo dati per noti), in cui lo zero 0 è il minimo di S, 1 è il il minimo di $S \setminus \{0\}$, e cosi' via.... Usando l'ordinamento si definiscono in S anche una somma e altre operazioni. L'insieme S si denota col simbolo $\mathbb{N}_0$, e l'ordinamento $\mathfrak{R}$ non è altro che quello usuale $(\leqslant_u)$. In particolare $(\mathbb{N}_0, \leqslant)$ è un insieme ben ordinato infinito.

Esercizio 2.6.21 Esiste un sottoinsieme proprio di $\mathbb{N}_0$ simile a $\mathbb{N}_0$?

CAPITOLO 3

L'INSIEME DEI NUMERI NATURALI

3.1 INTRODUZIONE

Nel paragrafo precedente abbiamo accennato a come si può pervenire ad un modello dei numeri naturali, e non è sembrato immediato trovare una definizione di numero naturale. Tuttavia per i nostri scopi possiamo ritenere che tale nozione sia del tutto acquisita, e che nell'operazione del contare si usano degli enti chiamati appunto *numeri naturali*. Il primo numero naturale positivo è il numero *uno*, e si denota col simbolo 1, mentre l'insieme di tutti i numeri naturali si denota col simbolo $\mathbb{N}$. Col simbolo $\mathbb{N}_0$ denoteremo l'unione di $\mathbb{N}$ e del singleton di 0, $\mathbb{N} \cup \{0\}$ (insieme dei numeri interi non negativi), mentre col simbolo $\mathbb{Z}$ denoteremo l'insieme dei numeri interi $\{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$. Ogni numero naturale n ha un successivo che si denota col simbolo $n+1$, mentre il precedente di un numero naturale maggiore di 0 si denota col simbolo $n-1$. Si assume che ogni numero n *è minore di* $n+1$, e si scrive $n < n+1$. Da ció consegue che nell'insieme $\mathbb{N}_0$ risulta definito un ordinamento naturale. Rispetto a tale ordinamento l'insieme $\mathbb{N}_0$ ha le seguenti proprietá:

(a) Ogni parte non vuota di $\mathbb{N}_0$ possiede minimo (buon ordinamento)

(b) Ogni parte non vuota di $\mathbb{N}_0$ superiormente limitata possiede massimo.

È opportuno ricordare che queste due proprietá sono caratterizzanti, nel senso che se $(S, \mathfrak{R})$ è un insieme ordinato non superiormente limitato che verifica sia la 1) che la 2), allora $(S, \mathfrak{R})$ è simile ad $\mathbb{N}_0$ con la relazione d'ordine usuale.

Sia ora X un sottoinsieme di $\mathbb{N}_0$. Ci poniamo il seguente quesito: Se in X giacciono i successivi di tutti i suoi elementi, e se anche $0 \in X$, possiamo concludere che $X = \mathbb{N}_0$? La risposta è affermativa, ed è contenuta nel *Principio di Induzione*.

3.2 IL PRINCIPIO DI INDUZIONE

Teorema 3.2.1 (PRIMA FORMA DEL PRINCIPIO DI INDUZIONE) *Sia X una parte non vuota di $\mathbb{N}_0$ e sia $0 = \min X$. Supponiamo inoltre che valga la proprietá:*

$$\mathfrak{P}) \quad \text{Sia } n > 0. \text{ Se } n-1 \in X \Rightarrow n \in X \ .$$

Allora $X = \mathbb{N}_0$.

DIMOSTRAZIONE – Per assurdo sia $\mathbb{N}_0 \neq X$. Il buon ordiamento di $\mathbb{N}_0$ assicura che la parte non vuota $A := \mathbb{N}_0 \setminus X$ possiede il minimo $m = \min A$. Chiaramente $0 \notin A$, quindi $m > 0$, inoltre $m-1$ non appartiene ad A in quanto m è il minimo di A, da cui necessariamente $m-1 \in X$. Per la proprietá $\mathfrak{P}$, anche il successivo di $m-1$ deve appartenere ad X, per cui $m \notin \mathbb{N}_0 \setminus X$. Questa è una contraddizione. □

Quindi il principio di induzione individua una condizione sufficiente affinché un sottoinsieme di $\mathbb{N}_0$ coincida con $\mathbb{N}_0$ stesso. Riportiamo di seguito alcune applicazioni del principio di induzione.

Esercizio 3.2.2 Provare che per ogni intero $n \geqslant 0$, $f(n) = 2n^3 - 3n^2 + n + 51 \geqslant 0$.

Sugg. Per $n = 0$ l'asserto è verificato. Per poter applicare il principio di induzione bisogna verificare il passo induttivo. A tal scopo sia $n > 0$, supponiamo che $f(n-1) \geqslant 0$, e proviamo che $f(n) \geqslant 0$. $f(n) = 2n^3 - 3n^2 + n + 51 = 2(n-1+1)^3 - 3(n-1+1)^2 + n + 51 = 2(n-1)^3 + 6(n-1)^2 + 6(n-1) + 2 - 3(n-1)^2 - 6(n-1) - 3 + n + 51$ riscrivendo si ottiene: $f(n) = 2(n-1)^3 - 3(n-1)^2 + n - 1 + 1 + 51 + 6(n-1)^2 - 3 + 2 = f(n-1) + 6(n-1)^2 \geqslant 0 + 6(n-1)^2 \geqslant 0$.

Se X è un sottoinsieme di $\mathbb{N}_0$ richiedere che $0 \in X$ equivale a richiedere che il minimo di X è 0. Sia ora X un sottoinsieme non vuoto di $\mathbb{N}_0$, e sia t il suo minimo. Se in X giacciono i successivi di tutti i suoi elementi, cosa possiamo concludere? Situazioni di questo genere si presentano spesso.

Consideriamo ad esempio la seguente disuguaglianza "$3^n < n!$". Si vede subito che non vale per i primi numeri $1, 2, 3$ e che vale per numeri abbastanza grandi (provare con n=9). Si prova facilmente che se un numero verifica quella disuguaglianza, allora anche il suo successivo la verifica. Per quali n sussiste la disuguaglianza considerata?

Sia $t > 0$, e denotiamo con $\mathbb{N}_t$ l'insieme dei numeri naturali ottenuto da $\mathbb{N}$ togliendo gli elementi $1, \ldots, t-1$ (in altre parole $\mathbb{N}_t = \mathbb{N} \setminus I_{t-1}$), è possibile riformulare la prima forma del principio di induzione in un modo più generale, modificando lievemente la dimostrazione.

Teorema 3.2.3 (Estensione della prima forma del principio di induzione) *Sia X una parte non vuota di $\mathbb{N}$, e sia $t = minX$ (Base di induzione). Supponiamo che inoltre valga la proprietà:*

$$\mathfrak{P}_1) \quad \text{Sia } n > t. \text{ Se } n-1 \in X \Rightarrow n \in X \ \ (\text{Passo induttivo}).$$

Allora $X = \mathbb{N}_t$.

Dimostrazione – Chiaramente $X \subseteq N_t$. Per assurdo sia X contenuto propriamente in N_t. Il buon ordiamento di $\mathbb{N}$ assicura che la parte non vuota $A := \mathbb{N}_t \setminus X$ possiede il minimo $m = minA$. Chiaramente $t \notin A$, quindi $m > t$, inoltre $m-1$ non appartiene ad A in quanto m è il minimo di A, da cui necessariamente $m-1 \in X$. Per la proprietà $\mathfrak{P}$, anche il successivo di $m-1$ deve appartenere ad X, per cui $m \notin \mathbb{N}_t \setminus X$. Questa è una contraddizione. □

Più in generale quindi possiamo asserire che il principio di induzione individua una condizione sufficiente affinché un sottoinsieme di $\mathbb{N}_0$ coincida con $\mathbb{N}_t$. Come abbiamo già accennato il pricipio di induzione si può anche applicare indirettamente per provare una una successione di disugaglianze. Più in generale, siano $P_1, P_2, \ldots, P_n, \ldots$ una successione di proposizioni, e sia X l'insieme degli indici per cui P_i è vera: $X = \{i \in \mathbb{N}_0 : P_i \text{ è verificata}\}$. Se X è non vuoto (quindi se qualche P_i è vera) e se verifica il passo induttivo, si può asserire che tutte le P_i sono verificate da un certo indice in poi.

Nell'esempio precedente poniamo P_n : "$3^n < n!$", e t il minimo degli interi n per cui P_n : è verificata. Utilizzando il principio di induzione possiamo asserire che la disuguaglianza $3^n < n!$ sussiste per ogni $n \geqslant t$. Il lettore verifichi che in questo caso la base di induzione è verificata per $t = 7$.

Esempio 3.2.4 P_n : "La somma dei primi n numeri coincide con $n(n+1)/2$".

Posto X l'insieme dei numeri positivi n per cui $1 + \ldots + n = n(n+1)/2$, si deve provare che $X = \mathbb{N}$.

Evidentemente $1 \in X$, in quanto la somma costituita dal solo addendo 1 coincide con $1(1+1)/2$.

Per provare il passo induttivo supponiamo che n sia un elemento di $\mathbb{N}_0$ maggiore di 0 tale che $n-1 \in X$, e proviamo che $n \in X$.

Se $n-1 \in X$ vuol dire che la somma dei primi $n-1$ numeri positivi coincide con $(n-1)n/2$, quindi $1+\ldots+n=1+\ldots+n-1+n=(n-1)n/2+n=n^2-n+2n/2 = n^2+n/2 = n(n+1)/2$. In definitiva si è provato che anche $n \in X$, e quindi anche il passo induttivo. Il principio di induzione assicura che $X = \mathbb{N}$.

Svolgere i seguenti esercizi usando dove è possibile il principio di induzione:

Esercizio 3.2.5 Siano a e b radici dell'equazione $x^2 - x - 1 = 0$. Provare che per ogni $n \in \mathbb{N}$ il numero $a^n + b^n$ è un intero.

Esercizio 3.2.6 Stabilire se il numero $2^{4(2n+1)} + 1$ è un numero primo per ogni $n \in \mathbb{N}_0$.

Esercizio 3.2.7 Per quali interi positivi n la somma dei primi n numeri dispari coincide con n^2?

Esercizio 3.2.8 Stabilire se il numero intero $n^2 + n + 41$ è un numero primo per ogni $n \in \mathbb{N}$.

Quando si applica il principio di induzione non si puó certo trascurare che sia verificata la base induttiva: l'insieme vuoto infatti è un sottoinsieme di $\mathbb{N}$ in cui giacciono i successivi di tutti i suoi elementi!

Esempio 3.2.9 Per quali $n \in \mathbb{N}$ il numero 7 divide $134^n + 1$? In questo caso il passo induttivo è immediatamente verificato: Supponiamo che 7 divida $134^n + 1$. Allora 7 divide $134(134^n + 1) - 133 = 134^{n+1} + 134 - 133 = 134^{n+1} + 1$, ed il passo induttivo è verificato. Se si trascura la verifica della base induttiva si potrebbe pensare di aver provato che $134^n + 1$ è un multiplo di 7 (qualunque sia n).

La scelta della base di induzione condiziona anche la verifica del passo induttivo, quindi non è sempre immediata. Provare a svolgere il seguente esercizio:

Esercizio 3.2.10 Stabilire per quali interi positivi, n, sussiste la seguente disuguaglianza: $n^3 < 3^n$.

Quando si applica il principio di induzione bisogna stare attenti a come si verifica il passo induttivo. Il seguente esempio mostra le possibili conseguenze che puó causare una verifica superficiale del passo induttivo:

Esempio 3.2.11 Siano $a, b \in \mathbb{N}_0$, e proviamo che $a = b$. Poniamo n il massimo tra a e b. Se $n = 0$ allora essendo a e b naturali saranno entrambi uguali ad 0 (base induttiva).

Sia ora $n > 1$, e procediamo per induzione. L'ipotesi indutttiva assicura che se il massimo tra due numeri naturali x ed y è $n-1$, allora $x = y$. Chiaramente il massimo tra $a-1$ e $b-1$ è proprio $n-1$, quindi per ipotesi induttiva $a-1 = b-1$. Da ció segue che $a = b$, e quindi il passo induttivo è provato. Dov'é l'errore?

Il principio di induzione sarà usato anche nella seguente forma:

Teorema 3.2.12 (Seconda forma del principio di induzione) *Sia* X *una parte non vuota di* $\mathbb{N}_0$*, e sia* $t = minX$ *(base di induzione). Supponiamo che inoltre valga la proprietà:*

$\mathfrak{P}_2$) Sia $n > t$. Se $i \in X$, per ogni $t \leqslant i < n \Rightarrow n \in X$ $(passo\ \ induttivo)$.

Allora $X = \mathbb{N}_t$.

Dimostrazione — Chiaramente $X \subseteq N_t$. Per assurdo sia X contenuto propriamente in N_t. Il buon ordiamento di $\mathbb{N}_0$ assicura che la parte non vuota $A := \mathbb{N}_t \setminus X$ possiede il minimo $m = minA$. Chiaramente $t \notin A$, quindi $m > t$, inoltre ogni numero i minore di m non appartiene ad A in quanto m è il minimo di A, per cui se $t \leqslant i < m$, necessariamente $i \in X$. Per la proprietá $\mathfrak{P}_2$, anche m deve appartenere ad X e questa è una contraddizione in quanto $m \in A$. □

Notiamo subito che la tesi della seconda forma coincide con la tesi della prima forma, mentre il passo induttivo $\mathfrak{P}_2$ sembra piú debole di $\mathfrak{P}_1$, essendo l'ipotesi (del passo induttivo $\mathfrak{P}_2$) piú forte dell'ipotesi espressa da $\mathfrak{P}_1$.

Vedremo in seguito che in molte applicazioni converrá usare la seconda forma del principio di induzione.

Teorema 3.2.13 (Algoritmo della divisione euclidea) *Siano* n *ed* m *interi non negativi, con* $m \neq 0$*. Allora esistono e sono unici* q *ed* r *numeri naturali tali che* $n = mq + r$ *e* $0 \leqslant r < m$.

DIMOSTRAZIONE – Proviamo dapprima l'esistenza di q ed r. Se $n = 0$ basta porre $q = 0$ e $r = 0$ per ottenere $n = mq + r$ e $0 \leqslant r < m$, sicché l'asserto è vero se $n = 0$. Procediamo per induzione (II forma), quindi possiamo supporre l'asserto vero per ogni numero maggiore o uguale a zero e minore di n, e provare che l'asserto è vero anche per n. Osserviamo che se $n < m$ allora basta porre $q = 0$ e $r = n$. Sicché possiamo supporre che $n \geqslant m$ per cui $0 \leqslant n - m < n$. Per ipotesi induttiva esistono q_1 e r_1 tali che $n - m = mq_1 + r_1$ e $0 \leqslant r_1 < m$ (osserviamo che in questa situazione la prima forma del principio di induzione non può essere applicata in quanto non è detto che $n - m$ sia esattamente $n - 1$). A questo punto basta isolare n, infatti: $n = m + mq_1 + r_1$. Se $m > 0$ allora basta porre $q = q_1 + 1$ e $r = r_1$. L'asserto quindi è vero per n, e per induzione è vero per ogni $n \geqslant 0$.

Per provare l'unicità supponiamo che $n = mq' + r'$ con $0 \leqslant r' < m$ e $n = mq + r$ con $0 \leqslant r < m$, e proviamo che $q = q'$ e $r = r'$. Per assurdo sia $r \neq r'$, e per fissare le idee supponiamo che $r > r'$. Sottraendo membro a membro si ottiene $0 = m(q - q') + r - r'$ da cui $0 < r - r' = m(q' - q) < r < m$. Essendo ogni multiplo positivo di m maggiore o uguale ad m, deve essere $q - q' = 0$ e quindi anche $r - r' = 0$. Da questa contraddizione segue che $r = r'$, e quindi necessariamente $0 = m(q - q')$, da cui anche $q = q'$.

Siano n ed m interi non negativi, con $m \neq 0$. Gli unici numeri naturali q ed r per cui "$n = mq + r$ e $0 \leqslant r < m$" si dicono rispettivamente *quoziente* e *resto* della divisione euclidea di n diviso m. Se r è 0, allora $n = mq$, e diremo che n è multiplo di m oppure che m è un divisore di n.

3.3 ELEMENTI DI COMBINATORICA

Sia n un intero non negativo. Induttivamente definiamo il fattoriale di n, che sarà denotato col simbolo "$n!$", mediante le posizioni:

$n! = 1$ se $n = 0$ e $n! = (n-1)!n$ se $n > 0$.

Ad esempio $1! = (1-1)!1 = 1 \cdot 1 = 1$. Analogamente risulta $5! = 4! \cdot 5 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$

Siano m ed n interi tali che $0 \leqslant m \leqslant n$. Si chiama *coefficiente binomiale di* n *rispetto ad* m il numero:

$$\binom{n}{m} = \frac{n!}{(n-m)!m!}.$$

Così ad esempio si ha:

$$\begin{pmatrix} 7 \\ 5 \end{pmatrix} = \frac{7!}{(7-5)!5!} = 21, \quad \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \frac{0!}{0!0!} = 1, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1!}{(1-1)!1!} = 1$$

Osserviamo che se $n = m$, risulta

$$\begin{pmatrix} n \\ m \end{pmatrix} = \frac{n!}{(n-n)!n!} = \frac{n!}{1 \cdot n!} = 1.$$

Chiaramente per ogni n e m interi tali che $0 \leqslant m \leqslant n$, risulta

$$\begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} n \\ n-m \end{pmatrix}.$$

Lemma 3.3.1 *Siano* a, b, c *numeri naturali. Se* a *divide sia* b *che* c, *allora* a *divide ogni combinazione lineare di* b *e* c. *In particolare* a *divide* $b + c$.

Dimostrazione — Sia $bh + ck$ una qualunque combinazione lineare di b e c (h e k interi). Per ipotesi $b = ax$ e $c = ay$, allora $bh + ck = axh + ayk = a(xh + yk)$, e quindi a divide $bh + ck$. □

Il seguente teorema prova che per ogni m ed n interi tali che $0 \leqslant m \leqslant n$ il coefficiente binomiale di n rispetto ad m è un numero naturale.

Teorema 3.3.2 *Siano* m *ed* n *interi tali che* $0 \leqslant m \leqslant n$. *Allora* $(n-m)! \cdot m!$ *divide* $n!$

Dimostrazione — Procediamo per induzione su n. Consideriamo la successione di proposizioni P_n:

"per ogni $0 \leqslant m \leqslant n \Rightarrow (n-m)!m!$ divide $n!$".

Se $n = 0$ l'unico intero m compreso tra 0 ed n è chiaramente 0, e quindi l'asserto è verificato. Anche se $n = m$ l'asserto è banalmente verificato, quindi possiamo supporre $0 \leqslant m < n$. Per ipotesi induttiva l'asserzione P_{n-1} è vera, quindi essendo $0 \leqslant m \leqslant n-1$ si ha che: $(n-1-m)! \cdot m!$ divide $(n-1)!$. Moltiplicando per $n-m$ si ha: $(n-m)!m!$ divide $(n-1)!(n-m)$; Se $m = 0$ l'asserto è banalmente verificato, quindi possiamo supporre $m > 1$, sicche' $0 \leqslant m-1 \leqslant n-1$. Ancora l'ipotesi induttiva assicura quindi che $(n-1-(m-1))!(m-1)!$ divide $(n-1)!$, e moltiplicando per m si ha che: $(n-m)!m!$ divide $(n-1)!m$. Da queste due informazioni e dal lemma precedente segue che $(n-m)!m!$ divide $(n-1)!(n-m) + (n-1)!m = (n-1)!(n-m+m) = n!$. □

Esercizio 3.3.3 Sia p un numero primo, e sia i un numero naturale compreso tra 0 e p. Provare che p divide $\binom{p}{i}$.

Il coefficiente binomiale si chiama cosi' perché viene usato nello sviluppo del binomio di Newton. Infatti si puo' provare che per ogni a, b interi e n intero non negativo risulta:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Esempio 3.3.4

$$(a+b)^4 = \binom{4}{0} a^4 b^0 + \binom{4}{1} a^3 b^1 + \binom{4}{2} a^2 b^2 + \binom{4}{3} a^1 b^3 + \binom{4}{4} a^0 b^4.$$

Esercizio 3.3.5 Calcolare la seguente somma:

$$\binom{7}{0} + \binom{7}{1} + \binom{7}{2} + \binom{7}{3} + \binom{7}{5} + \binom{7}{6}.$$

Esercizio 3.3.6 Calcolare la seguente somma:

$$\sum_{i=1}^{12} \binom{13}{i}.$$

Teorema 3.3.7 *Siano S e T insiemi finiti non vuoti di ordine n. Allora esistono $n!$ applicazioni biettive di S in T.*

Dimostrazione — Consideriamo la seguente successione di proposizioni P_n:

"Se $|S'| = |T'| = n$ allora esistono $n!$ applicazioni biettive di S' in T'".

Se $n = 1$ allora $S = \{x\}$ e $T = \{y\}$, per cui esiste un'unica applicazione di S in T, e l'asserto è verificato. Sia $n > 1$, e procediamo per induzione supponendo l'asserto vero per $n-1$. Sia x un elemento di S, e poniamo $T = \{y_1, y_2, \ldots, y_n\}$. Per ogni elemento y_r in T gli insiemi $S \setminus \{x\}$ e $T \setminus \{y_r\}$ hanno cardinalità $n-1$, e quindi per ipotesi induttiva l'insieme $\bar{\Phi}_r$ delle

applicazioni biettive di $S \setminus \{x\}$ in $T \setminus \{y_r\}$ sono $(n-1)!$. D'altra parte $\bar{\Phi}_r$ è equipotente all'insieme $\Phi_r = \{f : S \to T$, tale che f è biettiva e $f(x) = y_r\}$ costituito dalle applicazioni biettive di S in T che trasformano x in y_r. Allora Φ_r ha ordine $n-1!$. Se denotiamo con Φ l'insieme di tutte le applicazioni biettive di S in T si ha: $\Phi = \Phi_1 \cup \Phi_2 \ldots \cup \Phi_n$ e tale unione è disgiunta, in altri termini $\{\Phi_1, \Phi_2, \ldots \Phi_n\}$ è una partizione di Φ. Pertanto $|\Phi| = |\Phi_1| + |\Phi_2| + \ldots + |\Phi_n| = \underbrace{(n-1)! + \ldots + (n-1)!}_{n} = n!$, e la proposizione P_n è verificata.
□

Un'immediata conseguenza è il seguente risultato:

Corollario 3.3.8 *Sia S un insieme finito non vuoto di cardinalità n. Allora S possiede n! permutazioni.*

Esercizio 3.3.9 (Identità di Stiefel) Siano m ed n interi tali che $0 < m \leqslant n$. Verificare che $\binom{n-1}{m-1} + \binom{n-1}{m} = \binom{n}{m}$.

Sia un insieme finito S di cardinalità n, e sia $m \leqslant n$. Per stabilire quanti sono i sottoinsiemi di S che hanno cardinalità m, basta calcolare il coefficiente binomiale di n rispetto ad m. Infatti:

Teorema 3.3.10 *Sia S un insieme di cardinalità n, e sia $0 \leqslant m \leqslant n$. Allora il numero dei sottoinsiemi di S aventi cardinalità m è $\binom{n}{m}$.*

Dimostrazione – Osserviamo che S possiede un solo sottoinsieme di ordine n e $\binom{n}{n} = 1$, quindi l'asserto è verificato quando m coincide con n. L'asserto è ovviamente verificato anche quando $n = 0$ oppure quando $n = 1$. Chiaramente S possiede n sigleton e $\binom{n}{1} = n$, quindi l'asserto è verificato quando $m = 1$. Allora possiamo supporre che $1 < m < n$. Procediamo per induzione supponendo che l'asserto sia verificato per gli insiemi di ordine $n-1$.

Poniamo Φ l'insieme dei sottoinsiemi di S aventi ordine m. Per determinare l'ordine di Φ fissiamo un elemento a in S, e dividiamo Φ in due sottoinsiemi: Φ_1 costiutito da quelli che contengono a, e Φ_2 quelli che non contengono a. I sottoinsiemi di Φ_2 sono esattamente i sottoinsiemi di $S \setminus \{a\}$

aventi ordine m, ed essendo $0 \leqslant m \leqslant n-1$, per ipotesi induttiva abbiamo $|\Phi_2| = \begin{pmatrix} n-1 \\ m \end{pmatrix}$. D'altra parte posto Φ_1^* l'insieme costituito dai sottoinsiemi di $S \setminus \{a\}$ aventi ordine $m-1$ risulta che l'applicazione:

$$f : X \in \Phi_1 \to X \setminus \{a\} \in \Phi_1^*,$$

è biettiva. Essendo $0 \leqslant m-1 \leqslant n-1$ ancora per ipotesi induttiva si ha $|\Phi_1| = |\Phi_1^*| = \begin{pmatrix} n-1 \\ m-1 \end{pmatrix}$.

Sommando abbiamo $|\Phi| = |\Phi_1| + |\Phi_2| = \begin{pmatrix} n-1 \\ m-1 \end{pmatrix} + \begin{pmatrix} n-1 \\ m \end{pmatrix} = \begin{pmatrix} n \\ m \end{pmatrix}$.
□

Esempio 3.3.11 Se S è un insieme di 90 numeri, ci sono $\begin{pmatrix} 90 \\ 3 \end{pmatrix}$ terne possibili che possono essere estratte.

Esercizio 3.3.12 Giocando al tradizionale gioco del lotto, è più facile fare un ambo con una singola giocata oppure una quaterna con 780 giocate?

Corollario 3.3.13 *Sia S un insieme di ordine n. Allora l'insieme $\wp(S)$ ha ordine 2^n.*

Dimostrazione – In $\wp(S)$ sia $\sim$ la relazione binaria definita ponendo: $\forall X, Y \in \wp(S)$, $X \sim Y \iff X$ e Y sono equipotenti. Si verifica che $\sim$ è di equivalenza, e ciascuna classe di equivalenza è costituita da tutti e soli i sottoinsiemi di S aventi lo stesso ordine. Per il teorema precedente la classe dei sottoinsiemi aventi ordine 1, è costituita da $\begin{pmatrix} n \\ 1 \end{pmatrix}$ oggetti, e in generale la classe dei sottoinsiemi aventi ordine $i \leqslant n$, è costituita da $\begin{pmatrix} n \\ i \end{pmatrix}$ oggetti. Poiché $S/\sim$ è una partizione di S avremo:

$$|S| = \begin{pmatrix} n \\ 0 \end{pmatrix} + \begin{pmatrix} n \\ 1 \end{pmatrix} + \ldots + \begin{pmatrix} n \\ i \end{pmatrix} + \ldots + \begin{pmatrix} n \\ n \end{pmatrix} = (1+1)^n. \square$$

3.4 RAPPRESENTAZIONI POSIZIONALI

Anche se il concetto di numero è astratto, usando la proprità che ognuno di essi ha un successivo, si può pensare ad una loro rappresentazione mediante dei simboli, che per l'occorrenza si chiamano anche cifre. Come è noto nell' esercizio del contare usualmente si usano in successione i simboli (o cifre) $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Per denotare il successivo del numero 9, si usa la scrittura 10, dove l'1 che si trova a sinistra dello 0 sta a significare che si sono usate una sola volta tutte le dieci cifre a disposizione, mentre lo 0 serve per dare una posizione all' 1 in modo tale da poterlo leggerlo come una "decina". Quindi quando una cifra occupa la seconda posizione (da destra verso sinistra) essa riveste il ruolo di contatore delle decine. Ad esempio il numero 53 è quel numero composto da 5 decine e 3 unità. Una volta esaurite la disponibilità delle decine, si passa alle centinaia. Il numero successivo a 99 si denota col simbolo 100, e così via... Per questo motivo tale sistema di numerazione si dice *decimale posizionale*. Osserviamo che in tale sistema di numerazione per denotare i numeri $1, 10, 100, 1000$ etc... si usano i simboli $10^0, 10^1, 10^2, 10^3$, ed il numero 7602 si può scrivere $7602 = 7 \cdot 10^3 + 6 \cdot 10^2 + 0 \cdot 10^1 + 2 \cdot 10^0$.

Il discorso appena fatto si può rifare a partire da più o meno cifre. Ad esempio se usiamo soltanto i primi tre simboli $0, 1, 2$ il successivo di 2 sarà denotato col simbolo 10, dove l'1 che si trova sinistra dello 0 sta a significare che si sono usate una sola volta tutte le tre cifre a disposizione, mentre lo 0 serve per dare una posizione all' 1 in modo tale da poterlo leggerlo come una "terzina". Tale sistema di numerazione si dice *ternario posizionale* e tutti i numeri si rappresenteranno con le sole tre cifre $0, 1, 2$. Per evitare ambiguità per le rappresentazioni dei numeri in basi diverse da dieci, si usano le parentesi indicando la base a pedice.

Esempio 3.4.1 Il numero dodici nel sistema ternario si scriverà $(110)_3$ che esprime dodici come somma di tre terzine complete (ossia 3^2), più una terzina (3^1). In base dieci il numero dodici si denoterà semplicemente con 12.

Esempio 3.4.2 La scrittura $(1101101)_2$ è la rappresentazione del numero $1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 = 1 + 4 + 8 + 32 + 64 = 109$ (in base dieci).

Esercizio 3.4.3 Come si rappresenta il numero 271 in base 2?

Esercizio 3.4.4 Trasformare in base decimale il numero $(1110001101)_2$.

In generale abbiamo il seguente teorema:

Teorema 3.4.5 *Fissata una base* $a > 1$*, ogni intero positivi* n *si può rappresentare in base* a*.*

Dimostrazione — Per $n = 0$ e per $n = 1$ l'asserto è verificato in quanto esistono esattamente a simboli che rappresentano con un' unica cifra ogni numero minore di a. Allora la base induttiva è verificata e possiamo supporre $n \geqslant a$. Per la divisione euclidea esistono $q > 1$ ed r tali che $n = aq + r$ con $0 \leqslant r < a$. Chiaramente $q < n$, e per ipotesi induttiva si può rappresentare in base a: $q = (c_t \dots c_0)_a$, ossia $q = c_0 + c_1 a^1 + \dots + c_t a^t$. Allora $n = a \cdot (c_0 + c_1 a^1 + \dots + c_t a^t) + r = r + c_0 \cdot a + c_1 a^2 + \dots + c_t a^{t+1}$. In questo modo abbiamo ottenuto la rappresentazione di n in base a: $n = (c_t \dots c_0 r)_a$. □

La dimostrazione precedente fornisce un algoritmo per ottenere la rappresentazione di n in base a. Nella dimostrazione abbiamo già notato che il resto delle divisione euclidea tra n e a coincide con la cifra delle unità. Per ottenere la cifra delle "a-ine" basta considerare il resto r_1 della divisione tra q e ancora a: $q = aq_1 + r_1$ con $0 \leqslant r_1 < a$. Così procedendo fin quando non si ottiene un quoziente nullo si determina la rappresentazione di n in base a.

Esempio 3.4.6 Esprimere 124 in base 2.

$124 = 2 \cdot 62 + 0$
$62 = 2 \cdot 31 + 0$
$31 = 2 \cdot 15 + 1$
$15 = 2 \cdot 7 + 1$
$7 = 2 \cdot 3 + 1$
$3 = 2 \cdot 1 + 1$
$1 = 2 \cdot 0 + 1$
$(1111100)_2 = 124$

Esempio 3.4.7 Esprimere 137 in base 2.

$137 = 2 \cdot 68 + 1$
$68 = 2 \cdot 34 + 0$
$34 = 2 \cdot 17 + 0$
$17 = 2 \cdot 8 + 1$
$8 = 2 \cdot 4 + 0$
$4 = 2 \cdot 2 + 0$
$2 = 2 \cdot 1 + 0$
$1 = 2 \cdot 0 + 1$
$(10001001)_2 = 137$

Esempio 3.4.8 Esprimere 137 in base 3.

$137 = 3 \cdot 45 + 2$
$45 = 3 \cdot 15 + 0$
$15 = 3 \cdot 5 + 0$
$5 = 3 \cdot 1 + 2$
$1 = 3 \cdot 0 + 1$
$(12002)_3 = 137$

3.5 OPERAZIONI IN BASE a

Le usuali tecniche adottate per eseguire le quattro operazioni tra numeri rappresentati in base dieci, si possono estendere anche al caso in cui la base di rappresentazione scelta è diversa da dieci. Per la somma bisognerà prestare attenzione ai riporti; per la differenza bisogna fare attenzione ai vari "prestiti", che non sono necessariamente decine o centinaia...; per il prodotto e la divisione conviene tener presenti le tabelline fino a quella del $a-1$.

Esempio 3.5.1 Per sommare i numeri $(1220022)_3$ e $(12002)_3$ conviene incolonnarli:

$$\begin{array}{r} (1220022)_3 + \\ \underline{(0012002)_3 =} \\ (2002101)_3 \end{array}$$

Esempio 3.5.2 Calcoliamo la differenza dei due numeri precedenti.

$$\begin{array}{r} (1220022)_3 - \\ \underline{(0012002)_3 =} \\ (1201020)_3 \end{array}$$

Esempio 3.5.3 Calcoliamo ora il prodotto dei numeri $(122)_3$ e $(1002)_3$. Per comoditá nei riporti sottointenderemo che stiamo in base 3.

$$\begin{array}{r} (122)_3 \times \\ \underline{(1002)_3 =} \\ 1021 \\ \underline{122000} \\ 200021 \end{array}$$

I seguenti esempi mostrano che in base due la moltiplicazione e la divisione sono davvero semplici:

Esempio 3.5.4 Osserviamo che la moltiplicazione in base due si riduce difatto ad un'addizione. L'unica difficoltà sarà il riporto: bisognerà ricordare che $1+1=10, 1+1+1+1=100$, etc ....

$$
\begin{array}{rcccccccc}
 & (1 & 1 & 0 & 1 & 1 & 0)_2 & \times & \\
 & & & (1 & 0 & 1 & 1)_2 & = & \\
\hline
 & & & 1 & 1 & 0 & 1 & 1 & 0 & + \\
 & & 1 & 1 & 0 & 1 & 1 & 0 & & + \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & & & = \\
\hline
(1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0)_2.
\end{array}
$$

Esempio 3.5.5 Anche la per la divisione non c'è molta differenza, anzi il procedimento appare più veloce in quanto non bisogna fare le prove (moltiplicazioni) per individuare il multiplo massimo del divisore che sia minore del dividendo parziale. Infatti, in base due l'unico multiplo non nullo del divisore è il divisore stesso. Come esempio faremo la verifica della precedente moltiplicazione:

$$
\begin{array}{lcccccccccc}
(1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0)_2 & : & (1 & 0 & 1 & 1)_2 \\
- & 1 & 0 & 1 & 1 & & & & & = & (1 & 1 & 0 & 1 & 1 & 0)_2 \\
= & 0 & 1 & 1 & 1 & & & & & & & & & & & \\
 & 0 & 1 & 1 & 1 & 1 & & & & & & & & & & \\
- & & 1 & 0 & 1 & 1 & & & & & & & & & & \\
= & & 0 & 1 & 0 & 0 & & & & & & & & & & \\
 & & 0 & 1 & 0 & 0 & 0 & 0 & & & & & & & & \\
- & & & & 1 & 0 & 1 & 1 & & & & & & & & \\
= & & & & 0 & 1 & 0 & 1 & & & & & & & & \\
 & & & & 0 & 1 & 0 & 1 & 1 & & & & & & & \\
- & & & & 0 & 1 & 0 & 1 & 1 & & & & & & & \\
= & & & & 0 & 0 & 0 & 0 & 0 & & & & & & & \\
 & & & & 0 & 0 & 0 & 0 & 0 & 0 & & & & & &
\end{array}
$$

CAPITOLO 4

STRUTTURE ALGEBRICHE

4.1 OPERAZIONI IN UN INSIEME

Sia S un insieme non vuoto. Si dice *operazione binaria interna in* S una qualunque applicazione del tipo $\star : S \times S \to S$. La coppia $(S, \star)$ si dice struttura algebrica ad una operazione. L'immagine (x, y) mediante $\star$, che usualmente abbiamo denotato col simbolo $\star(x, y)$ si chiama *composto di* x *ed* y *mediante* $\star$, e in seguito sarà denotata col simbolo $x \star y$. Di chiaro significato è la nozione di *operazione n-aria interna in* S quando $n > 2$. Inoltre diremo *operazione unaria in* S una qualunque applicazione di S in S.

Spesso per denotare un'operazione si usano i simboli "$\cdot$"oppure "$+$". In tal caso avremo le strutture $(S, \cdot)$ oppure $(S, +)$ denotate moltiplicativamente oppure additivamente.

Esempio 4.1.1 Sia T un insieme, e poniamo $S = \wp(T)$. Utilizzando l'intersezione tra i sottinsiemi di T, possiamo definire la seguente operazione binaria in S:

$$\begin{array}{c} \cap\colon \wp(T) \times \wp(T) \to \wp(T) \\ (X, Y) \to X \cap Y \end{array}.$$

Analogamente possiamo definire le operazioni binarie di unione e differenza in S.

Esempio 4.1.2 Sia T un insieme, e poniamo $S = \wp(T)$. L'applicazione

$$\begin{array}{c} \diamond\colon \wp(T) \to \wp(T) \\ X \to T \setminus X \end{array}'$$

è un esempio di operazione unaria in S, anche chiamata *complemento in* T.

Esempio 4.1.3 L'usuale addizione è un'operazione binaria in $\mathbb{N}_0$:

$$\begin{array}{c} +\colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0 \\ (x,y) \to x+y \end{array}$$

Esempio 4.1.4 L'usuale addizione non è un'operazione binaria nell'insieme dei numeri dispari.

Sia $(S,\star)$ una struttura algebrica. Si dice che:

(a) $\star$ è *associativa* se $\forall x,y,z \in S, (x\star y)\star z = x\star(y\star z)$.

(b) $\star$ è *commutativa* se $\forall x,y \in S, x\star y = y\star x$.

(c) Un elemento $e \in S$ è *neutro* se $\forall x \in S, x\star e = e\star x = x$

Osserviamo che se una struttura algebrica possiede elemento neutro, questo è unico.

Esercizio 4.1.5 In $\mathbb{N}_0$ sia la seguente operazione: $\star : (x,y) \in \mathbb{N}_0 \times \mathbb{N}_0 \to x^2 + y^2 \in \mathbb{N}_0$. Stabilire:

(a) se la struttura $(\mathbb{N}_0,\star)$ possiede elemento neutro;

(b) se $\star$ è associativa;

(c) se $\star$ è commutativa.

Esempio 4.1.6 Sia

$$\begin{array}{c} \star : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0 \\ (x,y) \to x+y+1 \end{array}.$$

La struttura $(\mathbb{N}_0,\star)$ è associativa, ma non possiede elemento neutro.

Le operazioni di intersezione e unione in $S = \wp(T)$ di cui agli esempi precedenti, sono sia associative che commutative. La struttura $(S,\cap)$ possiede elemeto neutro, che coincide con T; anche la struttura $(S,\cup)$ possiede elemento neutro: $\forall X \in S, X\cup\emptyset = X$.

Sia $(S,\star)$ una struttura algebrica e sia X una parte non vuota di S, diremo che X è *una parte stabile* di S rispetto a $\star$ se $\forall x,y \in X, x\star y \in X$. Quando ciò accade è possibile definire un'applicazione:

$$\star_X\colon (x,y) \in X\times X \to x\star y \in X.$$

Rimane in questo modo definita una operazione binaria $\star_X$ in X che si che si chiama *operazione indotta da* $\star$ *su* X. Se non c'è ambiguità l'operazione indotta si continua a denotare con lo stesso simbolo dell'operazione di partenza.

Esempio 4.1.7 L'insieme $2\mathbb{N}_0$ dei numeri pari è una parte stabile di $\mathbb{N}_0$ rispetto all'addizione, e $(2\mathbb{N}_0, +)$ è associativa commutativa e possiede l'elemento neutro.

Esempio 4.1.8 L'insieme D dei numeri naturali dispari maggiori di 4 è una parte stabile di $\mathbb{N}_0$ rispetto alla moltiplicazione, ma non possiede l'elemento neutro.

Esempio 4.1.9 L'insieme D dei numeri naturali dispari non è una parte stabile di $\mathbb{N}_0$ rispetto all'addizione.

Sia $(S, \star)$ una struttura algebrica e sia X una parte di S. Si dice parte stabile generata da X, e si denota con $\langle X \rangle$, la più piccola parte stabile di S che contiene X. In particolare se X è una parte stabile di S, allora $X = \langle X \rangle$.

Esempio 4.1.10 Il singleton $\{4\}$ non è una parte stabile di $\mathbb{N}_0$. La parte stabile generata da $\{4\}$ è costituita da tutti i multipli positivi di 4: $\langle\{4\}\rangle = 4\mathbb{N}$. Osserviamo che la struttura $(4\mathbb{N}, +)$ è associativa commutativa, ma non possiede elemento neutro. Perché $4\mathbb{N}_0$ non è la parte stabile generata da 4?

Esercizio 4.1.11 Nella struttura $(\mathbb{N}_0, +)$, determinare la parte stabile generata dal sottoinsieme $\{6, 7\}$.

4.2 MONOIDI

Una struttura algebrica $(S, \star)$ si dice *monoide* se l'operazione $\star$ è associativa e se inoltre possiede l'elemento neutro. Nel paragrafo precedente abbiamo già rilevato che se S è un insieme di parti, allora $(S, \cap)$ e $(S, \cup)$ sono monoidi commutativi.

Esempio 4.2.1 Le strutture $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(2\mathbb{N}_0, +)$ sono monoidi

Esercizio 4.2.2 Sia

$$\begin{aligned} \star : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (x, y) &\to x + y + 1 \end{aligned}.$$

La struttura $(\mathbb{Z}, \star)$ è un monoide?

Sia $(S, \star)$ una struttura algebrica dotata di elemento neutro "e". Un elemento u di S si dice simmetrizzabile se $\exists u' \in S$ tale che $u \star u' = e = u' \star u$. In tal caso e l'elemento u' si dice *simmetrico* di u.

In un monoide gli elementi simmetrizzabili hanno un unico simmetrico. Infatti sia u un elemento simmetrizzabile di S, e supponiamo che esitano $u', u'' \in S$ tali che $u \star u' = e = u' \star u$ e inoltre $u \star u'' = e = u'' \star u$. Allora $u' = u' \star e = u' \star (u \star u'') = (u' \star u) \star u'' = e \star u'' = u''$.

Sia $(S, \star)$ un monoide, e sia u di S. Diremo che u è *regolare o cancellabile* se valgono le seguenti proprietà:

(i) $\forall a, b \in S,\ a \star u = b \star u \Rightarrow a = b$;

(ii) $\forall a, b \in S,\ u \star a = u \star b \Rightarrow a = b$.

Si verifica facilmente che ogni elemento simmetrizzabile di S è *regolare*.

In notazione moltiplicativa, se $(S, \cdot)$ è un monoide ed u è un elemento simmetrizzabile, allora il simmetrico di u si chiama *inverso* di u e si denota col simbolo u^{-1} . In tal caso quindi: $1 = u^{-1} \cdot u = u \cdot u^{-1} = 1$. In notazione additiva se $(S, +)$ è un monoide ed u è un elemento simmetrizzabile, allora il simmetrico di u si chiama *opposto* di u e si denota col simbolo $-u$. In tal caso quindi: $0 = (-u) + u = u + (-u) = 0$. Sia $(S, \star)$ un monoide. Diremo che $(S, \star)$ è un *gruppo* se ogni elemento di S possiede il simmetrico. Un gruppo si dice *abeliano* se l'operazione è commutativa. L'insieme $\mathbb{Q}$ dei razionali con l'usuale moltiplicazione non è un gruppo in quanto sebbene l'operazione è associativa e 1 è l'elemento neutro, lo zero non possiede inverso. Le strutture $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ e $(\mathbb{R} \setminus \{0\}, \cdot)$ sono esempi di gruppi. Un' altra importante classe di esempi è quella dei *gruppi di permutazioni*:

Sia X un insieme, e sia S_X l'insieme delle permutazioni su X. In S_X sia la seguente operazione binaria "$\cdot$", definita ponendo:

$$\cdot : (f, g) \in S_X \times S_X \to g \circ f \in S_X.$$

La struttura $(S_X, \cdot)$ è un gruppo, in cui $f \cdot g = g \circ f$. L'elemento neutro è l'applicazione identica su X, e l'inverso di ciascun elemento f è l'applicazione inversa di f.

Esempio 4.2.3 Denotiamo le 6 permutazioni di I_3 come segue:

$$\begin{array}{lccc} id: & I_3 & \longrightarrow & I_3 \\ & 1 & \to & 1 \\ & 2 & \to & 2 \\ & 3 & \to & 3 \end{array} \qquad \begin{array}{lccc} (12): & I_3 & \longrightarrow & I_3 \\ & 1 & \to & 2 \\ & 2 & \to & 1 \\ & 3 & \to & 3 \end{array}$$

$$
\begin{array}{lccc}
(23): & I_3 & \longrightarrow & I_3 \\
 & 1 & \to & 1 \\
 & 2 & \to & 3 \\
 & 3 & \to & 2
\end{array}
\qquad
\begin{array}{lccc}
(13): & I_3 & \longrightarrow & I_3 \\
 & 1 & \to & 3 \\
 & 2 & \to & 2 \\
 & 3 & \to & 1
\end{array}
$$

$$
\begin{array}{lccc}
(123): & I_3 & \longrightarrow & I_3 \\
 & 1 & \to & 2 \\
 & 2 & \to & 3 \\
 & 3 & \to & 1
\end{array}
\qquad
\begin{array}{lccc}
(132): & I_3 & \longrightarrow & I_3 \\
 & 1 & \to & 3 \\
 & 2 & \to & 1 \\
 & 3 & \to & 2
\end{array}
$$

Quindi $S_3 = \{id = 1, (12), (23), (13), (123), (132)\}$ L'operazione in S_3 la possiamo rappresentare con la *tavola di moltiplicazione*, cosrtruita moltiplicando ogni elemento della colonna a sinistra per ogni elemento della prima riga in alto.

$\cdot$	1	(12)	(23)	(13)	(123)	(132)
1	1	(12)	(23)	(13)	(123)	(132)
(12)	(12)	1	(132)	(123)	(13)	(23)
(23)	(23)	(231)	1	(132)	(12)	(13)
(13)	(13)	(132)	(123)	1	(23)	(12)
(123)	(123)	(23)	(13)	(12)	(132)	1
(132)	(132)	(13)	(12)	(23)	1	(123)

Osserviamo che l'operazione non è commutativa.

Sia $(S, \star)$ un monoide, e sia x un elemento di S. Poniamo $x^0 = 1$, e per ogni positivo n induttivamente, poniamo $x^n = x^{n-1}x$. Se inoltre x è un elemento invertibile è possibile definire x^n anche quando $n < 0$, ponendo $x^n = (x^{-1})^{-n}$. In particolare in un gruppo $(S, \star)$ è possibile definire per ogni intero n la potenza n-esima di ciascun elemento di S. Analoghe considerazioni si possono fare se il monoide S è assegnato additivamente. In tal caso si parlerà di multiplo n-esimo di ciascun elemento simmetrizzabile di S.

Esercizio 4.2.4 Sia $(S, \cdot)$ un monoide, e sia x un elemento di S. Provare per induzione che $\forall n, m \in \mathbb{N}_0$ risulta:

(1) $x^m x^n = x^{m+n}$

(2) $(x^m)^n = x^{mn}$.

Esercizio 4.2.5 Sia $(S, \cdot)$ un gruppo, e sia x un elemento di S. Provare che $\forall n, m \in \mathbb{Z}$ risulta:

(1) $x^m x^n = x^{m+n}$

(2) $(x^m)^n = x^{mn}$.

Sia $(S, \star)$ un monoide. Una parte stabile X di S si dice *sottomonoide* se la struttura $(X, \star_X)$ è un monoide; se inoltre la struttura $(X, \star_X)$ è un gruppo allora si dice che X è un *sottogruppo* di S.

Proposizione 4.2.6 *Sia $(S, \star)$ un monoide. L'insieme $U(S)$ degli elementi simmetrizzabili di S è una parte stabile. In particolare $(U(S), \star)$ è un sottomonoide di S.*

Dimostrazione — Siano x ed y elementi simmetrizzabili, e siano x' e y' i rispettivi simmetrici. Allora si verifica facilmente che $y' \star x'$ è l'elemento simmetrico di $x \star y$. □

Sia $(S, \cdot)$ è un monoide. Allora $U(S)$ è chiaramente un gruppo, e si chiama *gruppo degli elementi invertibili di* S.

Esempio 4.2.7 $U(\mathbb{Z}) = \{1, -1\}$.

Osservazione 4.2.8

Siano $(M_1, *_1)$ e $(M_2, *_2)$ monoidi. Nel prodotto cartesiano $M = M_1 \times M_2$ possiamo definire un' operazione componente per componente:

$$* : M \times M \to M$$
$$((x_1, y_1), (x_2, y_2)) \to (x_1 *_1 x_2, y_1 *_2 y_2)$$

Si verifica facilmente che la struttura $(M, *)$ è un monoide, che chiameremo *monoide prodotto*.

Esercizio 4.2.9 Siano $(M_1, *_1)$ e $(M_2, *_2)$ monoidi, e sia $M = M_1 \times M_2$ il monoide prodotto. Provare che il sottogruppo degli elementi invertibili $U(M)$ di M coincide col prodotto $U(M_1) \times U(M_2)$.

4.3 Esempi di strutture algebriche con due operazioni: anelli, reticoli e spazi vettoriali

• **Anelli**

Sia $(A, +, \cdot)$ una struttura algebrica con due operazioni. Diremo che A è un *anello* se valgono le seguenti condizioni:

(1) $(A, +)$ è un gruppo abeliano;

(2) L'operazione "$\cdot$" è associativa;

(3) L'operazione "$\cdot$" è distributiva rispetto all'operazione "$+$ ":$\forall a, b, c \in A, a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$.

Se $(A, +, \cdot)$ è un anello, le sue operazione si chiamano anche *addizione* e *moltiplicazione*. Un anello poi si dirà *commutativo* se l'operazione di moltiplicazione è commutativa. Se inoltre la struttura $(A, \cdot)$ è un monoide ossia se A possiede elemento neutro rispetto alla moltiplicazione, allora l'anello $(A, +, \cdot)$ si dice unitario.

L'insieme degli interi relativi, $\mathbb{Z}$ con le usuali operazioni di addizione e moltiplicazione, è un esempio di anello commutativo unitario.

Esempio 4.3.1 Sia $\mathbb{Z}[x]$ l'insieme costituito da tutti e soli i polinomi a coefficienti interi nell'indeterminata x. Le usuali operazioni di somma e prodotto tra due polinomi definiscono due operazioni interne a $\mathbb{Z}[x]$, e la struttura $(\mathbb{Z}[x], +, \cdot)$ è un anello commutativo unitario.

Esempio 4.3.2 Un esempio estremo di anello è quello costituito da un solo elemento $A = \{0\}$. In questo caso le due operazioni si banalizzano e coincidono. Tale anello si chiama anche *anello nullo.*

Altri esempi importanti di anelli che incontreremo in seguito è quello costituito dalle matrici dello stesso tipo.

Un anello non nullo $(A, +, \cdot)$ si dice *campo* se la struttura $(A \setminus \{0\}, \cdot)$ è un gruppo abeliano.

Osservazione 4.3.3 In un campo l'elemento neutro rispetto la moltiplicazione, 1, risulta diverso da 0.

L'insieme dei numeri razionali con le usuali operazioni di somma e prodotto è un campo: $(\mathbb{Q}, +, \cdot)$. Analogamente anche $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ sono campi. In seguito incontreremo anche esempi di campi finiti.

Le proprietà elementari in un anello sono le seguenti:

Proposizione 4.3.4 *Sia $(A, +, \cdot)$ un anello, e siano a, b, c elementi di A e n un numero intero relativo. Allora:*

(1) $a \cdot 0 = 0 \cdot a = 0$;

(2) $a(-b) = (-a)b = -ab$;

(3) $(na)b = a(nb) = n(ab)$;

(4) $a(b-c) = ab - ac$ *e* $(b-c)a = ba - ca$.

Gli elementi invertibili di un anello unitario $(A, +, \cdot)$ sono per definizione quelli del monoide moltiplicativo $(A, \cdot)$. Osserviamo anche che in un anello non vale sempre la legge di annullamento del prodotto, mentre in un campo si.

Esercizio 4.3.5 Siano $(A_1, +_1, \cdot_1)$ e $(A_2, +_2, \cdot_2)$ anelli unitari. In modo del tutto analogo a come fatto per i monoidi, definire *l' anello prodotto* e caratterizzare gli elementi invertibili.

Proposizione 4.3.6 *Sia $(A, +, \cdot)$ un campo, e siano a, b elementi di A. Se $ab = 0$, allora $a = 0$ oppure $b = 0$.*

Dimostrazione — Assumiamo che $a \neq 0$. Per ipotesi $ab = 0$ e a possiede elemento inverso a^{-1}. Moltiplicando a sinistra per a^{-1} abbiamo $a^{-1}ab = a^{-1}0$. Per le proprietà elementari sugli anelli abbiamo $b = 0$. □

•Reticoli

Sia $(S, \leqslant)$ un insieme ordinato. Diremo che S è un *reticolo* se per ogni x ed y in S esiste sia l'estremo superiore $\sup\{x, y\}$ che l'estremo inferiore $\inf\{x, y\}$. In tal caso si possono definire due operazioni interne: ï¿œ

$$\begin{array}{lll} \vee : S \times S \longrightarrow S & \text{e} & \wedge : S \times S \longrightarrow S \\ (x, y) \to \sup\{x, y\} & & (x, y) \to \inf\{x, y\}. \end{array}$$

Tali operazioni si dicono rispettivamente *unione* e *intersezione*, e la struttura $(S, \vee, \wedge)$ si dice *associata* al reticolo $(S, \leqslant)$.

Esempio 4.3.7 Sia T un insieme. L'insieme ordinato $(S = \wp(T), \subseteq)$ è un reticolo. In tal caso risulta per ogni X e Y elementi di S: $\sup\{X, Y\} = X \cup Y$ e $\inf\{X, Y\} = X \cap Y$, per cui nella struttura algebrca $(S; \vee, \wedge)$ si ha: $X \vee Y = X \cup Y$ e $X \wedge Y = X \cap Y$.

Sia $(S, \leqslant)$ un reticolo e sia $(S; \vee, \wedge)$ la struttura associata a $(S, \leqslant)$. Allora valgono le seguenti proprietà:

(1) Le operazioni $\vee$ e $\wedge$ sono associative;

(2) Le operazioni $\vee$ e $\wedge$ sono commutative;

(3) $a \vee (a \wedge b) = a = a \wedge (a \vee b)$ per ogni a e b in S.

Tali proprietà sono caratterizzanti. Infatti se $(S; \vee, \wedge)$ è una struttura algebrica con due operazioni interne che verificano le tre proprietà precedenti, allora è possibile definire una relazione d'ordine $\mathfrak{R}$ in S tale che $(S, \mathfrak{R})$ è un reticolo la cui struttura associata è proprio $(S; \vee, \wedge)$. Per fare ciò basta porre $a \mathfrak{R} b \iff a \wedge b = a$, e si verifica facilmente che $\mathfrak{R}$ è d'ordine largo, e che per ogni x ed y in S esiste sia l'estremo superiore $sup\{x, y\}$ che l'estremo inferiore $inf\{x, y\}$.

Esercizio 4.3.8 Esibire un esempio di insieme ordinato che non sia un reticolo.

Esercizio 4.3.9 Sia l'insieme ordinato $(\mathbb{N}, |)$, dove "$|$" rappresenta la relazione di divisibilità in $\mathbb{N}$. Verificare che $(\mathbb{N}, |)$ è un reticolo, ed esplicitare le operazioni $unione$ ed $intersezione$ della struttura associata ad $(\mathbb{N}, |$.)

Particolari esempi di reticoli sono le Algebre di Boole. Un reticolo con almeno due elementi è un'*algebra di Boole*, se è distributivo e complementato. Questo tipo di struttura algebrica fu studiata dal matematico G. Boole (1815-1864), il quale ne evidenziò il legame con le regole della logica proposizionale. Le algebre di Boole con soli due elementi $\{0, 1\}$ hanno notevoli applicazioni in informatica in quanto possono essere prese come modello per un' interpretazione dei circuiti elettrici che compongono un computer (per approfondimenti si rimanda a corsi più specifici).

Sia S un insieme, e sia Y un insieme. Diremo *operazione esterna a* S *con dominio di operatori* Y un'applicazione del tipo:

$$\cdot_{est} : Y \times S \to S.$$

Quando non vi è ambiguita' l'operazione "$\cdot_{est}$" sarà denotata semplicemente col simbolo "$\cdot$". Una parte T di S si dice *stabile rispetto l'operazione* $\cdot_{est}$ se

$$\forall \alpha \in Y e \, \forall t \in T \to \alpha \cdot_{est} t \in T.$$

• **Spazi Vettoriali**

Sia $(V, +, \cdot)$ una struttura algebrica con "$+$" operazione interna a V, e "$\cdot$" operazione esterna a V con dominio di operatori un campo $(K; +_K, \cdot_K)$:

$$+ : V \times V \to V \qquad e \qquad \cdot : K \times V \to V.$$

Diremo che V è un K-spazio vettoriale se sono verificate le seguenti condizioni:

(1) $(V, +)$ è un gruppo abeliano;

(2) $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v \qquad \forall \alpha \in K$ e $\forall u$ e $v \in V$;

(3) $(\alpha +_K \beta) \cdot u = \alpha \cdot u + \beta \cdot u \qquad \forall \alpha$ e $\beta \in K$ e $\forall u \in V$;

(4) $(\alpha \cdot_K \beta) \cdot u = \alpha \cdot (\beta \cdot u) \qquad \forall \alpha$ e $\beta \in K$ e $\forall u \in V$;

(5) $1_K \cdot u = u \qquad \forall u \in V$.

Gli elementi del campo (dominio degli operatori) vengono chiamati *scalari*, mentre gli elementi di V vengono detti *vettori*. L'elemento neutro del gruppo $(V, +)$, si chiama *vettore nullo*

Esercizio 4.3.10 Sia $(V, +, \cdot)$ un K-spazio vettoriale, e siano 0_K lo zero del campo K, e 0_V il vettore nullo di V.

(1) Provare che $0_K \cdot v = 0_V$ per ogni vettore v di V;

(2) Provare che $\alpha \cdot 0_V = 0_V$ per ogni scalare α di K.

Esempio 4.3.11 Poniamo $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. L'applicazione

$$\begin{aligned} + : \mathbb{R}^2 \times \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ ((a, b), (c, d)) &\to (a + c, b + d), \end{aligned}$$

definisce un operazione in $\mathbb{R}^2$ tale che $(\mathbb{R}^2, +)$ è un gruppo abeliano. Si puo' anche definire un'operazione esterna su $\mathbb{R}^2$, con dominio di operatori $\mathbb{R}$, basta considerare l'applicazione

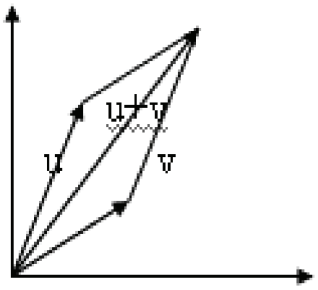
$$\begin{aligned} \cdot : \mathbb{R} \times \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (\alpha, (a, b)) &\to (\alpha \cdot a, \alpha \cdot b). \end{aligned}$$

Si verifica facilmente che la struttura $(\mathbb{R}^2, +, \cdot)$ è un $\mathbb{R}$-spazio vettoriale, in cui il generico vettore è una coppia. Tale struttura si chiama $\mathbb{R}$-*spazio vettoriale numerico di dimensione* 2.

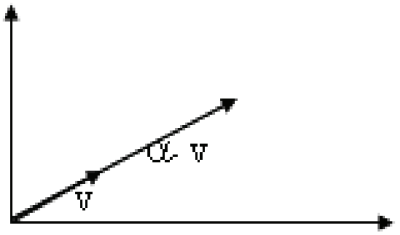
Per ogni intero positivo n e per ogni campo K, è possibile costruire (in modo analogo a come fatto nell'esempio precedente) il K-spazio vettoriale numerico di dimensione n. In questo caso il generico vettore sarà una n-pla.

Una rappresentazione grafica dell' $\mathbb{R}$-spazio vettoriale numerico di dimensione 2, può essere ottenuta considerando un riferimento cartesiano del piano reale, e ponendo V l'insieme costituito dai segmenti orientati con il primo estremo nell'origine. Questo equivale a considerare per ciascun vettore libero geometrico (ricordiamo che è una classe di equivalenza. Vedi

esempio 2.5.5), il rappresentante che ha come primo estremo l'origine. La somma interna tra due segmenti la si può definire con la regola del parallelogramma. In tal modo $(V, +)$ è un gruppo abeliano.



L'operazione esterna su V con dominio di operatori $\mathbb{R}$ si può definire ponendo $\alpha \cdot v$ il segmento di V avente lunghezza pari ad volte la lunghezza di v.



Si verifica facilmente che la struttura $(V, +, \cdot)$ è uno spazio vettoriale. Ogni vettore di v di V è individuato univocamente da un punto $P = P(v)$ del piano. Se denotiamo con $(x(v), y(v))$ le coordinate di $P(v)$, rimane definita un'applicazione $f : V \longrightarrow \mathbb{R}^2$ tra $\mathbb{R}$-spazi vettoriali, Tale applicazione è biettiva e inoltre.

(1) $f(v + w) = f(v) + f(w) \qquad \forall v, w \in V$;

(2) $f(\alpha \cdot v) = \alpha \cdot f(v)$.

Un'applicazione siffatta tra spazi vettoriali si dice *isomorfismo*. Gli spazi vettoriali $(V, +)$ e $(\mathbb{R}^2, +, \cdot)$ sono quindi *isomorfi*, e come strutture algebriche sono indistinguibili.

Esercizio 4.3.12 Nell' insieme quoziente $\mathbb{V}^2/\equiv$ dei vettori liberi del piano euclideo (vedi 2.5.5) definire un'operazione interna ed una esterna con dominio $\mathbb{R}$, in modo tale che $(\mathbb{V}^2/\equiv;+,\cdot)$ sia isomorfo a $(\mathbb{R}^2,+,\cdot)$.

4.4 CONGRUENZE E STRUTTURE QUOZIENTI

Sia $(S,\star)$ una struttura algebrica con un' operazione interna. Sia $\mathfrak{R}$ una relazione di equivalenza in S. Diremo che $\mathfrak{R}$ è una congruenza se:

$$\forall x,y,x',y' \in S,\ \ x\mathfrak{R}x' \text{ e } y\mathfrak{R}y' \Rightarrow x\star y\ \mathfrak{R}\ x'\star y'.$$

Esercizio 4.4.1 Definire in $(\mathbb{Z},+)$ una relazione di equivalenza che non sia una congruenza.

Esercizio 4.4.2 Definire in $(\mathbb{Z},+)$ una relazione di equivalenza che sia una congruenza.

L'importanza delle congruenze in una struttura algebrica $(S,\star)$ è che nell'insieme quoziente $S/\mathfrak{R}$, le classi di equivalenza si possono comporre. Infatti $([a]_{\mathfrak{R}},[b]_{\mathfrak{R}})=([a']_{\mathfrak{R}},[b']_{\mathfrak{R}}) \iff a\mathfrak{R}a'$ e $b\mathfrak{R}b'$, sicché per le congruenze si ha: $a\star b\ \mathfrak{R}\ a'\star b' \iff ([a\star b]_{\mathfrak{R}})=([a'\star b']_{\mathfrak{R}})$, ed è possibile definire la seguente *operazione quoziente*:

$$\begin{aligned}\star_{\mathfrak{R}} : S/\mathfrak{R}\times S/\mathfrak{R} &\to S/\mathfrak{R}\\ ([a]_{\mathfrak{R}},[b]_{\mathfrak{R}}) &\to ([a\star b]_{\mathfrak{R}}).\end{aligned}$$

Quando non c'è ambiguità l'operazione quoziente si denota ancora con $\star$. Se $\mathfrak{R}$ è una relazione di equivalenza in $(S,\star)$ che non non è una congruenza tale operazione non è definibile, come mostrano i seguenti esempi.

Esempio 4.4.3 Sia $\mathfrak{R}$ la relazione la relazione equivalenza in $(\mathbb{N},+)$ determinata dalla partizione $\{1,2,4\},\mathbb{N}\setminus\{1,2,4\}$. Evidentemente $[1]_{\mathfrak{R}}=[2]_{\mathfrak{R}}=[4]_{\mathfrak{R}}$, e $[3]_{\mathfrak{R}}=[5]_{\mathfrak{R}}=[6]_{\mathfrak{R}}=\ldots$; ma $[1+3]_{\mathfrak{R}}$ e $[2+3]_{\mathfrak{R}}$ sono classi distinte.

Esercizio 4.4.4 Sia $\mathfrak{R}$ la relazione la relazione equivalenza in $(\mathbb{N},+)$ determinata dalla partizione $\{1,2,3\},\mathbb{N}\setminus\{1,2,3\}$. Provare che $\mathfrak{R}$ non è una congruenza in $(\mathbb{N},+)$.

Esercizio 4.4.5 Sia $(M, \cdot)$ un monoide, e sia $(H, \cdot)$ un sottomonoide di M con $1_H = 1_M$. In M sia $\mathfrak{R}_H$ la relazione binaria definita ponendo:

$$a\mathfrak{R}_H b \iff \exists h \in U(H, \cdot) \text{tale che } b = ah.$$

Provare che $\mathfrak{R}_H$ è una congruenza.

Il comportamento dell'operazione quoziente in un monoide è descritto dalla seguente proposizione, la cui dimostrazione è lasciata per esercizio.

Proposizione 4.4.6 *Sia $(M, \cdot)$ un monoide, e sia $\mathfrak{R}$ una congruenza. Valgono ne seguenti proprietà:*
a) L'operazione quoziente è associativa;
b) $[1]_{\mathfrak{R}}$ è l'elemento neutro di $M/\mathfrak{R}$;
c) Se l'operazione "$\cdot$" è commutativa anche l'operazione quoziente "$\cdot_{\mathfrak{R}}$" lo è;
d) Se x è invertibile, allora anche $[x]_{\mathfrak{R}}$ è invertibile e si ha: $([x]_{\mathfrak{R}})^{-1} = ([x^{-1}]_{\mathfrak{R}})$.

4.5 OMOMORFISMI

Siano $(S, \sharp)$ e $(T, \star)$ strutture algebriche, e sia $f : S \to T$ un'applicazione. Si dice che f è un *omomorfismo* di S in T se $\forall x, y \in S,\ f(x \sharp y) = f(x) \star f(y)$. Un omomorfismo $f : S \to T$ che sia anche biettivo si dice *isomorfismo*. Un omomorfismo, quindi "conserva la composizione tra elementi", pertanto strutture isomorfe (anche se con elementi diversi) hanno le stesse proprietà rispetto la loro operazione.

Esempio 4.5.1 $(\mathbb{N}, +)$ e $(2\mathbb{N}, +)$ sono strutture isomorfe.

Esercizio 4.5.2 Sia $S = \{2^n : n \in \mathbb{N}\}$, verificare che S è una parte stabile di $(\mathbb{N}, \cdot)$, e che le strutture $(S, \cdot)$ e $(\mathbb{N}, +)$ sono isomorfe!

Esercizio 4.5.3 Sia $S = \{2^n : n \in \mathbb{Z}\}$, verificare che S è una parte stabile di $(\mathbb{R} \setminus \{0\}, \cdot)$. A quali delle seguenti strutture è isomorfa? $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Z} \setminus \{0\}, \cdot)$.

Proposizione 4.5.4 *Siano $(S, \star_1)$, $(T, \star_2)$ e $(V, \star_3)$ strutture algebriche, e siano $f : S \to T$ e $g : T \to V$ omomorfismi. Allora l'applicazione $g \circ f$ è un omomorfismo.*

DIMOSTRAZIONE — Siano x e y elementi di S, allora $g(f(x \star_1 y) = g(f(x) \star_2 f(y)) = g(f(x)) \star_3 g(f(y))$. □

Esercizio 4.5.5 iano $(S, \star_1)$, $(T, \star_2)$ strutture algebriche, e sia $f : S \to T$ un isomorfismo di S in T. Verificare che f^{-1} è un isomorfismo di T in S.

Esercizio 4.5.6 Siano $(S, \star_1)$, $(T, \star_2)$ strutture algebriche, e sia $f : S \to T$ un omomorfismo di S in T. Verificare che se X è una parte stabile di S allora $f(X)$ è una parte stabile di T.

Se $(S, \star)$ è una struttura algebrica e $\mathfrak{R}$ è una congruenza in S, l'applicazione canonica (vedi paragrafo 2.5) $\pi : x \in S \to [x]_{\mathfrak{R}} \in S/\mathfrak{R}$ è un omomorfismo (suriettivo) che si chiama anche *epimorfismo canonico.*

Il teorema di decomposizione delle applicazioni tra insiemi, ha come corrispondente il seguente:

Teorema 4.5.7 (DI OMOMORFISMO PER LE STRUTTURE ALGEBRICHE)
Siano $(S, \sharp)$ e $(T, \star)$ strutture algebriche, e sia $f : S \to T$ un omomorfismo. Allora $\mathfrak{R}_f$ è una congruenza in S, ed esiste un unico omomorfismo $\varphi : S/\mathfrak{R}_f \to T$ tale che $\varphi \circ \pi = f$. Inoltre φ è inettiva e $\varphi(S/\mathfrak{R}_f) = f(S)$.

DIMOSTRAZIONE — Per il teorema di decomposizione delle applicazioni, l'applicazione

$$\begin{aligned} \varphi : S/\mathfrak{R}_f &\to T \\ [x]_{\mathfrak{R}_f} &\to f(x), \end{aligned}$$

è l'unica applicazione tale che $\varphi \circ \pi = f$, inoltre φ è inettiva e $\varphi(S/\mathfrak{R}_f) = f(S)$. Per provare la tesi basta quindi verificare che $\mathfrak{R}_f$ è una congruenza e φ un omomorfismo.

Siano x, y, x', y' elementi di S tali che $x\mathfrak{R}_f y$ e $x'\mathfrak{R}_f y'$. Allora $f(x) = f(y)$ e $f(x') = f(y')$, e componendo in T risulta $f(x) \star f(x') = f(y) \star f(y')$. Essendo f un omomorfismo si ha $f(x\sharp x') = f(y\sharp y')$, sicché gli elementi $x\sharp x'$ e $y\sharp y'$ sono equivalenti modulo $\mathfrak{R}_f$, ovvero ($x\sharp x'$ $\mathfrak{R}_f$ $y\sharp y'$). Pertanto $\mathfrak{R}_f$ è una congruenza. Siano ora $[x]_{\mathfrak{R}_f}$ e $[y]_{\mathfrak{R}_f}$ elementi del dominio di φ. Risulta: $\varphi([x]_{\mathfrak{R}_f} \sharp [y]_{\mathfrak{R}_f}) = \varphi([x\sharp y]_{\mathfrak{R}_f}) = f(x\sharp y) = f(x) \star f(y) =$
$= \varphi([x]_{\mathfrak{R}_f}) \sharp \varphi([y]_{\mathfrak{R}_f})$. Pertanto φ è un omomorfismo. □

Il primo teorema di omomorfismo per le strutture algebriche può essere schematizzato così:

$$\begin{array}{ccc} S & \xrightarrow{f} & T \\ \downarrow \pi & \varphi \nearrow & \\ S/\mathfrak{R}_f & & \end{array} .$$

Esercizio 4.5.8 Siano $(S, <_1)$ e $(T, <_2)$ reticoli simili. Provare che le strutture algebriche associate$(S, \vee_1, \wedge_1)$ e $(T, \vee_2, \wedge_2)$ sono isomorfe.

CAPITOLO 5

L'ANELLO DEGLI INTERI

Abbiamo già osservato che $(\mathbb{Z}; +, \cdot)$ è un anello commutativo unitario, e che quindi valgono le proprietà espresse dalla proposizione 4.3.4. Questa sezione sarà dedicata allo studio approfondito sulla divisibilità in $\mathbb{Z}$, sulle congruenze e le loro applicazioni.

5.1 DIVISIBILITÀ IN $\mathbb{Z}$

Ricodiamo che se a e b sono due interi, si dice che a *divide* b se esiste un intero z tale che $b = az$. In particolare ogni numero intero divide 0, e l'elemento 0 divide soltanto lo 0. Per esprimere con una notazione che a divide b si scrive: $a \mid b$. Ricordiamo anche che il simbolo "$|a|$" denota il *valore assoluto* di a, ossia l'intero che coincide col massimo tra a e $-a$.

Dato un intero a gli elementi $1, -1, a, -a$ sono ovviamente dei divisori di a, per questo si dicono *divisori banali* di a. Ad esempio i divisori banali di -6 sono $1, -1, -6, 6$. Evidentemente il numero 7 possiede soltanto divisori banali.

Osserviamo che l'intero 1 ammette come divisori soltanto 1 e -1. Questi due elementi sono gli unici elementi invertibili di $\mathbb{Z}$.

Come è noto, in $\mathbb{Z}$ vale la legge di annullamento del prodotto:

$$\text{Se } ab = 0 \text{ allora } a = 0 \text{ oppure } b = 0.$$

Come conseguenza si ha che ogni elemento a non nullo è cancellabile, infatti per ogni b e c interi relattivi tali che $ac = ab$ si ha $a(c - b) = 0$, e quindi per la legge di annullamento del prodotto risulta $c = b$.

Lemma 5.1.1 *Se due interi si dividono mutuamente essi coincidono oppure sono l'uno l'opposto dell'altro.*

DIMOSTRAZIONE — Siano a e b interi e supponiamo che $a = cb$ e $b = da$, con c e d opportuni interi. Sostituendo si ha $a1 = cda$, e cancellando a si ottiene $1 = cd$ e quindi $c = d = \mp 1$. □

Diremo che un intero p è un numero *primo* se $p \neq \mp 1$ e i suoi divisori sono soltanto quelli banali. Chiaramente 0 non è primo.

Ricordiamo che assegnati due interi a e b una loro *combinazione lineare* è una somma del tipo $ah + bk$, dove $h, k \in \mathbb{Z}$ si dicono *coefficienti* della combinazione lineare. La somma e la differenza tra due interi sono esempi di particolari combinazioni lineari.

Siano a e b interi. Se $b = az$ per un opportuno $z \in \mathbb{Z}$, allora $b = (-a)(-z)$, quindi si ottiene che $-a$ divide b. In questo modo si può verificare che: $a \mid b \iff a \mid -b \iff -a \mid b \iff -a \mid -b \iff |a| \mid |b|$. Di conseguenza lo studio della divisibilità si può ricondurre da $\mathbb{Z}$ ad $\mathbb{N}$.

Proposizione 5.1.2 *Siano a, b e c numeri interi. Se c divide sia a che b allora c divide ogni loro combinazione lineare.*

Siano a e b interi non nulli, diremo che un intero d è un *massimo comune divisore* di a e di b se sono verificate le seguenti proprietà:

(1) d divide sia a che b;

(2) Ogni divisore comune di a e di b divide anche d.

Siano a e b interi non nulli, diremo che un intero c è un *minimo comune multiplo* di a e di b se sono verificate le seguenti proprietà:

(1) c è multiplo sia a che b;

(2) Ogni multiplo comune di a e di b è multiplo anche c.

Esempio 5.1.3 Gli interi 3 e -3 sono massimi comuni divisori di -6 e 15.

Per le osservazioni elementari fatte sulla divisibilità, è chiaro che se d è un massimo comun divisore di a e di b (non nulli), anche $-d$ lo è, e non ce ne sono altri. Infatti se d' fosse un massimo comun divisore di a e di b, gli

interi d e d' si dividerebbero mutuamente, e quindi $d' = \pm d$. Indicheremo con (a, b) il massimo comune divisore positivo tra a e b.

Se a e b sono due interi non nulli, allora il loro massimo comune divisore positivo coincide col massimo comune divisore positivo dei loro valori assoluti:

Proposizione 5.1.4 *Per ogni* a, *e* b *interi risulta:* $(a, b) = (|a|, |b|)$.

Quello che invece non appare evidente è che questa definizione di Massimo comune divisore coincide (come in seguito accenneremo) con quella che normalmente già si conosce, e che fa uso della nozione di numero primo.

Per determinare quindi il massimo comune divisore tra due interi non nulli possiamo supporre che questi siano positivi. Per individuare massimo comune divisore positivo tra due numeri è di fondamentale importanza la seguente proposizione.

Proposizione 5.1.5 *Siano* a *e* b *interi positivi. Se* $a = bq + r$ *con* $0 < r < b$. *Allora* $(a, b) = (b, r)$.

Dimostrazione — Per ipotesi $r = a - bq$. Per la proposizione 5.1.2 i divisori comuni di a e b sono tutti e soli i divisori comuni di b e di r. □

Se a è multiplo di b risulta ovviamente (a,b)=b. Se invece b non divide a, per la proposizione 5.1.5 $(a, b) = (b, r_1)$, con q_1 e r_1 interi tali che $a = bq_1 + r_1$, e $0 \leqslant r_1 < b$.

Se b è multiplo di r_1 risulta quindi r_1=(a, b), in caso contrario si ripete il ragionamento, ottenendo una sequenza $b > r_1 > r_2 \ldots$. Dopo un numero finito di passi necessariamente otterremo $r_s = 0$. Applicando ripetutamente la proposizione 5.1.5 si ottiene $(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{s-2}, r_{s-1}) = r_{s-1}$, e quindi r_{s-1} è il massimo comune divisore positivo tra a e b.

Il procedimeto esposto per determinare un massimo comune divisore tra due interi si chiama *Algoritmo delle divisioni successive*

Illustriamo con qualche esempio:

Esempio 5.1.6 a=306, b=135, allora (a,b)=9
306=135·2+36 $0 \leqslant 36 < 135$
135=36· 3+27 $0 \leqslant 27 < 36$
36=27·1 +9 $0 \leqslant 9 < 27$
27=9· 3.

Esempio 5.1.7 (13837,10201)=101
13837=10201· 1+3636
10201=3636· 2+2929
3636=2929· 1+707
2929=707·4+101
707=101· 7+0

Una conseguenza rilevante dell'algoritmo delle divisioni successive è che ogni resto si esprime come combinazione lineare di a e di b. Infatti dalle relazioni:
$a=b\cdot q_1+r_1$
$b=r_1\cdot q_2+r_2$
$r_1=r_2\cdot q_3+r_3$
$\vdots$
$r_{s-3}=r_{s-2}\cdot q_{s-1}+r_{s-1}$
si hanno le seguenti uguaglianze:
$a-b\cdot q_1=r_1$
$b-r_1\cdot q_2=r_2$
$r_1-r_2\cdot q_3=r_3$
$\vdots$
$r_{s-3}-r_{s-2}\cdot q_{s-1}=r_{s-1}$.
Il primo resto r_1 è combinazione lineare di a e di b. Sostituendo r_1 nella seconda equazione si ottiene r_2 espresso come combinazione lineare di a e di b. Sostituendo r_1 e r_2 nella terza equazione si ottiene l'espressione di r_3 come combinazione lineare di a e di b... e così via fino ad esprimere il $(a,b)=r_{s-1}$ come combinazione lineare di a e di b.

Esempio 5.1.8 Sia a=13837 e b=10201. Abbiamo visto che (a,b)=101= r_4. Per esprimere 101 come combinazione lineare di a e b bisogna sostituire progressivamente i resti delle divisioni successive espressi come combinazione linerare di a e b. Ponendo r_1 = 3636, r_2= 2929 e r_3=707 avremo:
r_1 = a - b
r_2 = b - 2 r_1
$r_3=r_1-r_2$
$r_4=r_2-4r_3$
Segue allora che
r_2=b - 2r_1= b - 2(a - b)=b - 2a+2b=3b-2a
$r_3=r_1-r_2$=(a - b) - (3b-2a)= a-b-3b + 2a=3a- 4b
$r_4=r_2-4r_3$=3b - 2a- 4(3a-4b)=3b-2a-12a +16b=-14a +19b
Da quest'ultima relazione si ha
101=13837ï¿œ(-14)+10201ï¿œ(19) e quindi u=-14 e v=19

Diremo che due interi non nulli sono *coprimi* se gli unici divisori in comune sono $\{1, -1\}$.

Teorema 5.1.9 (di Bezout) *Siano* a, b *numeri interi non nulli. Allora* a *e* b *sono coprimi se e solo se* 1 *è combinazione lineare di* a *e* b.

Dimostrazione — Supponiamo che a e b sono coprimi. Per l'algoritmo delle divisioni successive e le sue conseguenze il massimo comune divisore positivo di a e b è 1 e si esprime come combinazione lineare del tipo $au + bv$.

Viceversa, supponiamo che esistono u e v interi tali che $1 = au + bv$. Allora ogni divisore comune di a e b divide anche il numero 1, per la proposizione 5.1.2. Pertanto gli unici divisori comuni di a e di b sono 1 e -1. □

Corollario 5.1.10 *Siano* a, b *e* c *numeri interi tali che* c *divide* ab. *Se* c *è coprimo con* a *allora* c *divide* b.

Dimostrazione — Per il teorema di Bezout esistono $u, v \in \mathbb{Z}$ tali che $1 = cu + av$. Moltiplicando per b avremo: $b = bcu + bav$. Per ipotesi c divide ab, e quindi anche la combinazione $bcu + bav = b$. □

Lemma 5.1.11 *Siano* a, b *numeri interi, e sia* d *un massimo comune divisore di* a *e* b. *Allora* a' *e* b' *sono coprimi, dove* $a = a'd$ *e* $b = b'd$.

Dimostrazione — Sia c un divisore comune di a' e b', allora cd è divisore comune di a e di b. Quindi cd e d si dividono mutuamente, per cui $c = \pm 1$. □

Teorema 5.1.12 *Siano* a, b *numeri interi, e sia* d *un massimo comune divisore di* a *e* b. *Allora il quoziente* m *della divisione euclidea di* ab *per* d *è un minimo comune multiplo di* a *e* b.

Dimostrazione — Per ipotesi $ab = dm$, ed esistono a' e b' tali che $a = a'd$ e $b = b'd$. Allora $a'b'd = m$, ed m è un multiplo comune di a e b. Sia ora c un multiplo comune di a e b, e siano c' e c'' interi tali che $c = ac' = bc''$, in particolare $a'c' = b'c''$. Per il lemma 5.1.11, a' e b' sono coprimi, e per il lemma 5.1.10 a' divide c'', allora $a'c' = b'a'h$ per un opportuno intero h. Cancellando l'elemento a' abbiamo $c' = b'h$, e sostituendo risulta $c = ab'h = mh$. Abbiamo provato che c è multiplo di m. Pertanto m è un minimo comune multiplo di a e b. □

Assegnati a e b si come per i massimi comuni divisori, si verifica che se m è un minimo comune multiplo di a e b, anche $-m$ lo è, e non ce ne sono altri.

Esercizio 5.1.13 Calcolare un minimo comune multiplo positivo tra 10201 e 13837.

Esercizio 5.1.14 Sia z un intero multiplo di due interi coprimi a e b. Allora il prodotto ab divide z.

Ricordiamo che un intero non nullo e non invertibile, si dice *primo* se i suoi unici divisori sono quelli banali. Essi sono:

$$\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29, \dots$$

I numeri 1 e -1 non sono primi, in quanto sono invertibili; il numero 6 non è invertibile, ma non è primo, in quanto ammette divisori non banali.

Teorema 5.1.15 (DI CARATTERIZZAZIONE DEI NUMERI PRIMI) *Sia* p *un numero intero tale che* $|p| > 1$. *Allora* p *è primo se solo se vale la seguente proprietà:* $\forall a, b \in \mathbb{Z}, p|ab \Rightarrow p|a$ oppure $p|b$.

DIMOSTRAZIONE — Proviamo che la condizione è necessaria. A tal scopo siano a e b interi tali che $p|ab$. Per ipotesi i divisisori di p sono solo quelli banali, quindi se p non divide a i soli divisori comuni di questi ultimi sono 1 e -1, e per il lemma 5.1.10 segue che $p|b$.

Viceversa, sia c un divisore di p, allora esiste $z \in \mathbb{Z}$ tale che $p = cz$. Chiaramente p divide se stesso quindi $p|cz$, e per ipotesi $p|c$ oppure $p|z$. Nel primo caso p e c si dividono mutuamente e per il lemma 5.1.1 risulta $c = \mp p$. Se invece $p|z$, allora $z = px$ per un opportuno intero x, e quindi sostituendo $p = cxp$, da cui $1 = cx$. Anche in questo caso c è un divisore banale di p.

Proposizione 5.1.16 *Sia* p *un numero primo, e siano* $a_1, \dots a_n$ *interi relativi* $(n \geqslant 2)$. *Se* p *divide* $a_1 \cdots a_n$, *allora* p *divide qualche* a_j $(j \in I_n)$.

DIMOSTRAZIONE — Per $n = 2$ l'asserto segue dal teorema di carattrizzazione dei numeri primi. Sia $n > 2$ e procediamo per induzione. Il prodotto $b = a_1 \cdots a_{n-1}$ possiede almeno 2 fattori, e per ipotesi p divide ba_n. Per il teorema di caratterizzazione dei numeri primi p divide b oppure a_n. Se p divide b, per ipotesi induttiva esiste qualche $j \in I_{n-1}$ tale che p divide a_j. Il passo induttivo è provato.

Teorema 5.1.17 (FONDAMENTALE DELL'ARITMETICA) *Sia* n *un intero tale che* $|n| > 1$. *Allora* n *è primo oppure è prodotto di numeri primi.*

DIMOSTRAZIONE – Per provare l'asserto quando $n \geqslant 2$ procederemo per induzione.

Se $n = 2$ allora n è primo e l'asserto è provato. Sia $n > 2$ e supponiamo che l'asserto sia verificato per ogni numero maggiore o uguale a 2 e minore di n. Chiaramente possiamo supporre che n non sia primo, e quindi per definizione possiede un divisore non banale e positivo, a. Di conseguenza esiste $b \in \mathbb{Z}$ tale che $n = ab$ e $1 < a, b < n$. Per ipotesi induttiva a e b sono primi oppure prodotto di primi, e quindi n è prodotto di numeri primi.

Se $n \leqslant -2$ allora $-n \geqslant 2$, e per quanto già provato risulta:

$-n = p_1 \cdot p_2 \cdots p_r$, e quindi n si esprime come prodotto del tipo $(-p_1) \cdot p_2 \cdots p_r$. □

Il Teorema Fondamentale dell' Aritmetica assicura che ogni intero relativo diverso da 0, -1 e 1, si decompone nel prodotto di numeri primi. In realtà si può provare che tale decomposizione è unica a meno della posizione e del segno dei fattori primi. Ossia:

se $n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$, con $p_1, \ldots, p_r, q_1, \ldots, q_s$ numeri primi, allora si ha $r = s$, ed esiste una permutazione σ di I_r tale che $p_i = \pm q_{\sigma(i)}$ per ogni $i \in I_r$.

Ad esempio:

$$-30 = 5 \cdot 3 \cdot (-2) = 2 \cdot (-5) \cdot 3.$$

Come si può osservare i fattori sono gli stessi a meno della posizione e del segno.

Osserviamo che le nozioni di Massimo comune divisore e Minimo comune multiplo, coincidono con quelle che comunemente già si conoscono, e che fanno uso della nozione di numero primo.

Assegnati due interi a e b positivi, per il Teorema Fondamentale dell'Aritmetica, si possono individuare dei numeri primi distinti positivi, $p_1, \ldots, p_s$ tale che a e b si esprimono come potenze di tali primi:

$$a = p_1^{e_1} \cdots p_s^{e_s}, \quad b = p_1^{h_1} \cdots p_s^{h_s}, \text{con } e_1, \ldots e_s, h_1 \ldots h_s \text{ interi non negativi.}$$

Poniamo m_i il minimo tra gli esponenti e_i e h_i, e M_i il massimo tra gli esponenti e_i e h_i. Si verifica facilmente che il prodotto $d = p_1^{m_1} \cdots p_s^{m_s}$ è il massimo comune divisore positivo tra a e b, e il prodotto $m = p_1^{M_1} \cdots p_s^{M_s}$ è un minimo comune multiplo positivo tra a e b.

Teorema 5.1.18 (DI EUCLIDE) *Esistono infiniti numeri primi.*

DIMOSTRAZIONE — Per assurdo l'asserto sia falso, e supponiamo che l'insieme P dei numeri primi abbia un numero finito t di elementi, $P = \{p_1, \dots p_t\}$. Chiaramente l'intero $n = (p_1 \cdots p_t) + 1$ è in valore assoluto maggiore di 1, quiindi per il teorema fondamentale dell'aritmetica ammette un divisore primo, p_j con $j \in I_t$. D'altra parte p_j divide il prodotto $p_1 \cdots p_t$, e quindi anche $n - p_1 \cdots p_t = 1$. Questo è assurdo perché un numero primo non può dividere 1. □

5.2 LE CLASSI DEGLI INTERI MODULO m

Sia $m \in \mathbb{Z}$, e sia $m\mathbb{Z}$ la relazione binaria definita in $\mathbb{Z}$ ponendo $a\ m\mathbb{Z}\ b$ se e solo se a e b la differenza $a - b$ è multiplo di m, cioè $a\ m\mathbb{Z}\ b \iff m \mid a - b$. La relazione $m\mathbb{Z}$ è di equivalenza in $\mathbb{Z}$, e si chiama *congruenza modulo* m. Se a e b sono interi equivalenti modulo m si dicono anche *congruenti modulo* m, e si usa la notazione "$a \equiv b (\mathrm{mod} m)$".

In altre parole, possiamo dire che a è congruo a b modulo m se a e b differiscono per un multiplo di m, cioè:

$$a \equiv b(\mathrm{mod} m) \iff m|(a-b) \iff \exists k \in \mathbb{Z} : a = b + km.$$

Osserviamo che la relazione $0\mathbb{Z}$ è l'uguaglianza, infatti

$$a\ 0\mathbb{Z}\ b \iff 0|a-b \iff a - b = 0 \iff a = b.$$

Inoltre qualunque sia m, $\forall a, b \in \mathbb{Z}, a\ m\mathbb{Z}\ b \iff a\ (-m)\mathbb{Z}\ b$. Pertanto le relazioni $m\mathbb{Z}$ e $(-m)\mathbb{Z}$ coincidono. È opportuno osservare anche che la relazione $1\mathbb{Z}$ è la relazione totale. Queste considerazioni consentono di ricondurre lo studio delle congruenze in $\mathbb{Z}$ al caso in cui $m > 1$.

Sia m un intero. Per ogni $a \in \mathbb{Z}$ diremo *classe di congruenza di* a *modulo* m la classe di equivalenza di a modulo $m\mathbb{Z}$. Essa verrà denotata col simbolo $[a]_m$ anziché $[a]_{m\mathbb{Z}}$. Quindi:

$$[a]_m = \{x \in \mathbb{Z} : x \equiv a(\mathrm{mod} m)\} = \{a + km \in \mathbb{Z} : k \in \mathbb{Z}\}.$$

In particolare, la classe di 0 modulo m è costituita dai multipli interi di m: $[0]_m = \{km : k \in \mathbb{Z}\}$.

L'insieme quoziente $\mathbb{Z}/m\mathbb{Z}$ di $\mathbb{Z}$ rispetto alla relazione di equivalenza $m\mathbb{Z}$ si denota col simbolo $\mathbb{Z}_m$, e si chiama *insieme delle classi di interi modulo* m, o anche *insieme degli interi modulo* m. Osseviamo che se m divide a allora $[a]_m = [0]_m$. Più in generale si ha:

Lemma 5.2.1 *Sia* $m > 1$*e sia* $a \in \mathbb{Z}$*. Allora* $[a]_m = [r]_m$ *con* r *resto della divisione euclidea di* a *per* m*.*

Dimostrazione – Denotato con q il quoziente della divisione euclidea di a per m, si ha $a = mq + r$, e quindi m divide $a - r$, allora $a \equiv r(mod m)$ e le classi $[a]_m$ e $[r]_m$ coincidono. □

Teorema 5.2.2 . *Sia* $m > 1$*. Allora* $\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}$*, e la sua cardinalità è esattamente* m*.*

Dimostrazione – Sia $a \in \mathbb{Z}$, e sia r il resto della divisione euclidea di a per$m$, sicché $0 \leqslant r \leqslant m - 1$. Per il lemma precedente si ha $[a]_m = [r]_m$ e la prima parte del teorema è provata. Per completare la dimostrazione bisogna verificare che le classi $[0]_m, [1]_m, ..., [m-1]_m$ sono a due a due distinte. A tal scopo siano $0 \leqslant i < j \leqslant m - 1$ e proviamo che che $[i]_m \neq [j]_m$. Supponiamo per assurdo che $[i]_m = [j]_m$, allora $i \equiv j(mod m)$ e m divide $j - i$, per cui esiste $k \in \mathbb{N}_0$ tale che $j - i = mk$.

D'altra parte $0 \leqslant j - i \leqslant j \leqslant m - 1 < m$, sicché $0 \leqslant mk < m$. Allora $k = 0$, $j - i = 0$ e $i = j$. Pertanto le classi dei resti, $[0]_m, [1]_m, ..., [m-1]_m$ sono a due a due distinte, e l'insieme, $\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}$ è un insieme finito di ordine m. □

Esercizio 5.2.3 Determinare un intero c, compreso tra 300 e 370, che sia congruo a 13 modulo 72.

Esercizio 5.2.4 Quanti sono gli interi compresi tra 1000 e 1500 che sono congrui a a 13 modulo 72?

Esercizio 5.2.5 Esistono interi compresi tra 590 e 660, che sono congrui a 13 modulo 72?

Teorema 5.2.6 . *Sia* $m > 1$*. La relazione* $m\mathbb{Z}$ *è una congruenza nella struttura algebrica* $(\mathbb{Z}, +, \cdot)$*.*

Dimostrazione – Siano x, x', y, y' numeri interi tali che $x \; m\mathbb{Z} \; x'$ e $y \; m\mathbb{Z} \; y'$, allora esiste $h, k \in \mathbb{Z}$ tale che $x = mh + x'$ e $y = mk + y'$. Sommando i membri delle relazioni ottenute abbiamo:

$x + y = m(h + k) + (x' + y')$, da cui $x + y \; m\mathbb{Z} \; x' + y'$.

Moltiplicando avremo:

$xy = x'y' + m(x'k + y'h + hkm)$ da cui $xy \; m\mathbb{Z} \; x'y'$. □

Si può provare che non è possibile definire in $(\mathbb{Z}, +, \cdot)$ altre congruenze oltre alle relazioni del tipo $m\mathbb{Z}$.

Il precedente teorema permette di introdurre nell'insieme $\mathbb{Z}_m$ degli interi modulo m le operazioni di addizione e di moltiplicazione:

$$\begin{array}{rccc} +: & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m. \\ & ([a]_m, [b]_m) & \to & [a+b]_m \end{array} \qquad \text{In } \mathbb{Z}_m \quad [a]_m + [b]_m := [a+b]_m.$$

$$\begin{array}{rccc} \cdot: & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_m. \\ & ([a]_m, [b]_m) & \to & [a \cdot b]_m \end{array} \qquad \text{In } \mathbb{Z}_m \quad [a]_m \cdot [b]_m := [a \cdot b]_m.$$

La classe $[0]_m$ è l'elemento neutro rispetto alla somma e $[1]_m$ è l'elemento neutro rispetto la moltiplicazione. La struttura quoziente $(\mathbb{Z}_m, +, \cdot)$ risulta essere, al pari di $(\mathbb{Z}, +, \cdot)$, un anello commutativo unitario.

Esempio 5.2.7 $(\mathbb{Z}_4, \cdot)$ è un monoide ma non gruppo; $(\mathbb{Z}_4, +)$ è un gruppo abeliano; $(\mathbb{Z}_3, +, \cdot)$ è un campo finito di ordine 3.

Di seguito riportiamo come esempio la tavola di addizione e di moltiplicazione di $\mathbb{Z}_6$, dove per semplicità si sono denotate con $0, 1, 2, 3, 4, 5$ le classi $[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6$:

$+$	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

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Siano $m > 1$ e $a \in \mathbb{Z}$. Le considerazioni precedenti rivelano una relazione tra l'invertibilità della classe a e l'intero m. Si può osservare infatti che la classe $[3]_8$ è un elemento invertibile dell'anello $(\mathbb{Z}_8, +, \cdot)$, mentre la classe $[6]_8$ non lo è. Il seguente risultato caratterizza le classi invertibili modulo m.

Lemma 5.2.8 *Sia $m > 1$ un numero intero. Un elemento non nullo $[a]_m$ di $\mathbb{Z}_m$ è invertibile se e solo se a e m sono coprimi.*

DIMOSTRAZIONE – Se la classe $[a]_m$ è invertibile, esiste $[b]_m \in \mathbb{Z}_m$ tale che $[a]_m \cdot [b]_m = [ab]_m = [1]_m$ quindi m divide $ab-1$. Allora esiste $h \in \mathbb{Z}$ tale che $ab-1 = hm$, sicché $a(b)+m(-h) = 1$ e a e m sono coprimi.

Viceversa se a e m sono coprimi, esistono dei numeri interi u e v tali che $au+mv = 1$. Allora $[1]_m = [au+mv]_m = [a]_m[u]_m + [m]_m[v]_m = [a]_m[u]_m$. Pertanto la classe $[a]_m$ è invertibile, e risulta $[a]_m^{-1} = [u]_m$. □

Corollario 5.2.9 *Sia $m > 1$ un numero intero. L'anello $(\mathbb{Z}_m, +, \cdot)$ è un campo se e solo se m è un numero primo.*

DIMOSTRAZIONE – Sia $[a]_m$ un elemento non nullo dell'anello $(\mathbb{Z}_m, +, \cdot)$, e supponiamo che m sia primo. Allora m non divide a, d'altra parte m possiede solo divisori banali, perciò a ed m sono coprimi. Per il lemma precedente $[a]_m$ è invertibile.

Viceversa, supponiamo che $(\mathbb{Z}_m, +, \cdot)$ è un campo, e siano $a, b \in \mathbb{Z}$ tali che m divide ab, ossia $[0]_m = [ab]_m$. Se m non divide a, allora $(a, m) = 1$ e $[a]_m$ è invertibile, e moltiplicando a sinistra per $[a]_m^{-1}$ si ottiene $[0]_m = [a]_m^{-1}[ab]_m = [b]_m$. Pertanto m divide b. Abbiamo provato che se m divide un prodotto, allora divide uno dei fattori, e per il Teorema di caratterizzazione dei numeri primi, m è primo. □

(Rimarchiamo che il risultato precedente prova l'esistenza di infiniti esempi di campi finiti).

Un interessante risultato dell'aritmetica modulare è il seguente:

Teorema 5.2.10 (PICCOLO TEOREMA DI FERMAT) *Sia p un numero primo. Allora* $\forall a \in \mathbb{Z},\ a^p \equiv a \pmod{p}$.

DIMOSTRAZIONE – Bisogna provare che $[a]_p = [a^p]_p$. L'asserto è ovvio se $p = 2$. Allora possiamo supporre p dispari. Analizziamo dapprima il caso in cui $a \geqslant 0$. Se $a = 0$ l'asserto è verificato. Sia $a > 0$ e procediamo per induzione. L'elemento a si può scrivere come $(a-1)+1$, quindi possiamo riguardare a^p come potenza di un binomio:

$$((a-1)+1)^p = (a-1)^p + \sum_{i=1}^{p-1} \binom{p}{i} (a-1)^{p-i} + 1.$$

Per ogni i compreso tra 1 e $p-1$ il coefficiente binomiale $\binom{p}{i}$ è un multiplo di p, ne segue che $[a]_p^p = [(a-1)^p]_p + [1]_p$. Per ipotesi induttiva $[a-1]_p = [(a-1)^p]_p$, quindi $[a]_p^p = [a-1]_p + [1]_p = [a]_p$.

Se $a < 0$, essendo p dispari $a^p = -(-a)^p$. Per quanto già verificato nella prima parte della dimostrazione, $[(-a)^p] = [(-a)]$, per cui $[a]_p = [a^p]_p$. □

Concluderemo il paragrafo approfondendo lo studio del monoide moltiplicativo degli interi modulo m, $U(\mathbb{Z}_m, \cdot)$. Per ogni $m > 1$, per semplicità poniamo $U(\mathbb{Z}_m) = \mathbb{Z}_m^*$.

Essendo $(\mathbb{Z}_m, \cdot)$ un monoide commutativo unitario, $(\mathbb{Z}_m^*, \cdot)$ è un gruppo abeliano.

Esempio 5.2.11 $Z_{12}^* = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$.

Esercizio 5.2.12 Scrivere gli elementi e la tavola di moltiplicazione del gruppo $(Z_{15}^*, \cdot)$.

In sostanza per individuare Z_m^*, basta determinare l'insieme $\Phi(m) = \{x \in \mathbb{N} : x < m \text{ e } (x, m) = 1\}$.

Diremo *indicatore di Gauss-Eulero* la funzione

$$\begin{aligned} \varphi : \mathbb{N} &\longrightarrow \mathbb{N} \\ (m) &\to \varphi(m) := |\Phi(m)|. \end{aligned}$$

Esempio 5.2.13 $\Phi(8) = \{1, 3, 5, 7\} \subseteq \mathbb{N}$, e $\varphi(8) = 4$. $\Phi(12) = \{1, 5, 7, 11\}$, e $\varphi(12) = 4$. $\Phi(101) = I_{100}$, e $\varphi(101) = 100$.

Proposizione 5.2.14 *Sia m un numero intero positivo, allora il gruppo $U(\mathbb{Z}_m, \cdot)$ ha ordine $\varphi(m)$*

Dimostrazione – Basta osservare che $\Phi(m) = \{x \in \mathbb{N} : x < m \text{ e } (x, m) = 1\}$ e $U(\mathbb{Z}_m) = \{[x] \in \mathbb{Z}_m : x < m \text{ e } (x, m) = 1\}$. □

Un'applicazione f di $\mathbb{N}$ in $\mathbb{N}$ si dice anche *funzione aritmetica*, e si dice moltiplicativa se per ogni coppia (x, y) di numeri naturali coprimi si ha: $\varphi(xy) = \varphi(x)\varphi(y)$.

L' indicatore di Gauss-Eulero è una funzione aritmetica moltiplicativa.

Proposizione 5.2.15 *La funzione di Eulero è moltiplicativa.*

Dimostrazione – Sia $n = p^r q^s$, con p e q coprimi e osserviamo che $[a]_n = [b]_n$ se e solo se $[a]_{p^r} = [b]_{p^r}$ e $[a]_{q^s} = [b]_{q^s}$ (vedi Esercizio 5.1.14). Allora è possibile considerare l'applicazione

$$f : [a]_n \in \mathbb{Z}_{p^r q^s} \to ([a]_{p^r}, [a]_{q^s}) \in \mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}.$$

Per quanto già osservato tale applicazione è iniettiva, e quindi anche suriettiva essendo dominio e codominio equipotenti. Inoltre si verifica facilmente che f è un omomorfismo tra i monoidi $(\mathbb{Z}_{p^r q^s}, \cdot)$ e $(\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}, \cdot)$, sicché le due strutture sono isomorfe e hanno gli elementi invertibili che si corrispondono. D'altra parte per l'esercizio 4.2.9 il gruppo degli invertibili del codominio è il prodotto $U(\mathbb{Z}_{p^r}) \times U(\mathbb{Z}_{q^s})$, quindi anche nel dominio ci devono essere esattamente $\varphi(p^r)\varphi(q^s)$ elementi invertibili. Pertanto deve necessariamente essere $\varphi(p^r q^s) = \varphi(p^r)\varphi(q^s)$. □

Chiaramente se p è un numero primo, $\varphi(p) = p - 1$, e per ogni potenza p^n $(n > 0)$, $\varphi(p^n) = p^n - p^{n-1}$.

A questo punto in virtù della moltiplicatività, l'immagine $\varphi(m)$ si determina facilmente per ogni m.

Esempio 5.2.16 $\varphi(6125) = \varphi(7^2 5^3) = \varphi(7^2)\varphi(5^3) = (7^2 - 7)(5^3 - 5^2) = 420.$

Esercizio 5.2.17 Sia d un divisore di n, allora $\varphi(d)$ divide $\varphi(n)$. Basta fare la verifica quando d è una potenza di un primo.

Esercizio 5.2.18 Nel monoide $(\mathbb{Z}_{12}, \cdot)$, posto V il sottogruppo degli invertibili, verificare che nel quoziente $\mathbb{Z}_{12}/V$ l'unico elemento regolare è quello neutro (cfr. esercizio 4.4.5). Verificare inoltre che ogni elemento di $\mathbb{Z}_{12}/V$ coincide con l'insieme dei generatori di un sottogruppo di $(\mathbb{Z}_{12}, +)$, e viceversa.

5.3 EQUAZIONI CONGRUENZIALI

Dall'algebra elementare sappiamo che un'equazione del tipo $ax = b$ con coefficienti reali ammette una soluzione reale; d'altra parte se i coefficienti a e b sono interi relativi non è detto che la soluzione dell'equazione sia intera. In questo paragrafo tratteremo lo studio delle equazioni di primo grado $[a]_m x = [b]_m$ a coefficienti in un anello del tipo $(\mathbb{Z}_m, +, \cdot)$. Tali equazioni le diremo *equazioni congruenziali di termini* a b *ed* m. La ricerca delle soluzioni di un' equazione congruenziale, si riconduce alla ricerca di quei numeri interi c tali che $ac \equiv b (\mathrm{mod}\, m)$. Per questo motivo le equazioni congruenziali si denotano anche con la scrittura

$$ax \equiv b (\mathrm{mod}\ m),$$

e un intero c lo diremo *soluzione intera dell'equazione congruenziale di termini* a b *ed* m se $ac \equiv b (\mathrm{mod}\, m)$. Chiaramente in tal caso l'equazione $[a]_m x = [b]_m$ ammette come soluzione la classe $[c]_m$.

Teorema 5.3.1 *Siano* a, b *e* m *interi relativi, con* $m > 1$. *L'equazione congruenziale* $ax \equiv b (\mathrm{mod}\ m)$ *ammette soluzione se e solo se* $d = (a, m)$ *divide* b.

Dimostrazione — Se c è una soluzione dell'equazione allora esiste k tale che $ac - b = km$. Chiaramente d divide ogni combinazione lineare di a e di m, in particolare divide $ac - km = b$.

Viceversa, si supponga che d sia divisore di b, allora esiste h tale che $b = dh$. Essendo inoltre d un massimo comune divisore tra a ed m, esistono degli interi r ed s tali che $d = ra + sm$. Da ciò segue che $b = hd = h(ra + sm) = hra + hsm$, in particolare, $hra - b$ è multiplo di m e quindi $a(hr) \equiv b (\mathrm{mod} m)$. In questo modo abbiamo provato che hr è una soluzione dell'equazione congruenziale $ax \equiv b (\mathrm{mod}\ m)$. □

Esempio 5.3.2 L'equazione congruenziale $35x \equiv 21 (\mathrm{mod} 115)$ non ammette soluzioni. Infatti $(35, 115)$ non divide 21.

La dimosrazione del teorema precedente indica anche un algoritmo per calcolare una soluzione di un' equazione congruenziale quando questa ne ammette qualcuna. Ripercorriamo con un esempio:

Esempio 5.3.3 L'equazione congruenziale $10201x \equiv 707 (\mathrm{mod} 13837)$ ammette soluzione, infatti $(10201, 13837) = 101$ divide 707. I termini a ed m dell'equazione sono $a = 10201$ e $m = 13837$, e risulta $101 = 13837$ï¿œ$(-14) + 10201$ï¿œ(19) (vedi 5.1.8). Il coefficiente della combinazione lineare che moltiplica il primo termine dell'equazione congruenziale è 19 (nella dimostrazione $r = 19$); inoltre $707 = 101 \cdot 7$, quindi una soluzione è $19 \cdot 7 = 133$.

Conviene in generale fare una verifica: bisogna controllare se $10201 \cdot 133 - 707$ è multiplo di 13837.

Ora enunciamo due risultati che permettono un' ulteriore descrizione delle soluzioni intere di un'equazione congruenziale.

Teorema 5.3.4 *Siano* a, b *e* m *interi relativi, con* $m > 1$. *Se l'equazione congruenziale* $ax \equiv b (\mathrm{mod}\ m)$ *ammette una soluzione* c, *allora le soluzioni di tale equazione sono tutti e soli gli interi del tipo* $c + m_1 z$, *dove* z *è un qualunque intero e* m_1 *è il quoziente della divisione euclidea di* m *per* (a, m).

Abbiamo visto che un' equazione congruenziale può ammettere infinte soluzioni intere. D'altra parte assegnata un'equazione del tipo $[a]_m x = [b]_m$, questa possiede al più un numero finito di soluzioni distinte nell'anello $(\mathbb{Z}_m, +, \cdot)$. Il prossimo risultato prova che l'equazione $[a]_m x = [b]_m$ se non è priva di soluzioni in $(\mathbb{Z}_m, +, \cdot)$, allora possiede esattamente $d = (a, m)$ soluzioni.

Corollario 5.3.5 *Siano* a, b *e* m *interi relativi, con* $m > 1$. *Sia* d *il massimo comune divisore positivo di* a *e* m. *Se* d *divide* b *allora l'equazione congruenziale* $ax \equiv b \pmod{m}$ *ha esattamente* d *soluzioni a due a due incongrue modulo* m.

Esempio 5.3.6 Abbiamo verificato nell'esempio precedente che l'equazione congruenziale $10201x \equiv 707 \pmod{13837}$ ammette come soluzione il numero 133. In virtù dei teoremi precedenti ogni intero della forma $133 + 137 \cdot z$ con $z \in \mathbb{Z}$ è soluzione dell'equazione considerata. Inoltre ci sono 101 soluzioni non congrue modulo 13837: $133, 133 + 137, 133 + 2 \cdot 137, \ldots, 133 + 100 \cdot 137$.

Un insieme finito di t equazioni congruenziali si dice *sistema di equazioni congruenziali*, e si denota col simbolo

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \ldots \\ \ldots \\ a_t x \equiv b_t \pmod{m_t} \end{cases}.$$

Se un intero c è una soluzione intera di ogni equazione del sistema, allora si dice che c è *soluzione del sistema*. Chiaramente ciò accade se e solo se $[c]_{m_i}$ è soluzione di ogni equazione $[a]_{m_i} x = [b]_{m_i}$ nell'anello $(\mathbb{Z}_{m_i}, +, \cdot)$ per ogni $i \in I_t$.

Concluderemo il paragrafo con lo studio della risoluzione di particolari sistemi di equazioni congruenziali.

Teorema 5.3.7 Cinese del resto *Siano* $b_1, b_2, \ldots, b_t$ *interi relativi e* $m_1, m_2, \ldots, m_t$ *interi positivi a due a due coprimi. Allora il sistema*

$$\Sigma = \begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \ldots \\ \ldots \\ x \equiv b_t \pmod{m_t} \end{cases},$$

ammette una soluzione intera c, *ed ogni altra soluzione è congrua a* c *modulo* $m_1 \cdot m_2 \cdot \ldots \cdot m_t$.

DIMOSTRAZIONE — Per ogni $i \in I_t$ poniamo m'_i il prodotto $m_1 \cdot m_{i-1} \cdot m_{i+1} \ldots \cdot m_t$ in cui compaiono tutti i fattori tranne l'i-esimo. Allora gli interi m_i e m'_i risultano coprimi, e quindi $\forall i \in I_t$ l'equazione congruenziale $m'_i x \equiv 1 \bmod m_i$ ammette almeno una soluzione intera c_i. Verifichiamo che il numero intero $c = m'_1 c_1 b_1 + \ldots + m'_t c_t b_t$ è una soluzione del sistema. A tal scopo sia $i \in I_t$, e osserviamo che m_i divide ogni m'_j quando $i \neq j$ e per come stato scelto c_i abbiamo:

$$[c]_{m_i} = [m'_i c_i b_i]_{m_i} = [m'_i c_i]_{m_i}[b_i]_{m_i} = [b_i]_{m_i}.$$

Pertanto c è soluzione del sistema. Chiaramente per ogni intero del tipo $c + mz$, con $m = m_1 \cdot m_2 \cdot \ldots \cdot m_t$ e z un qualunque intero avremo ancora $[c + mz]_{m_i} = [c]_{m_i} = [b_i]_{m_i}$.

Sia ora u una soluzione del sitema Σ. Allora per ogni $i \in I_t$ avremo $c \equiv u (\bmod m_i)$, in particolare m_i divide $c - u$. Essendo $m_1, m_2, \ldots, m_t$ a due a due coprimi anche il prodotto $m_1 \cdot m_2 \cdot \ldots \cdot m_t$ divide $c - u$, sicché u giace nella classe di c modulo m. □

Osserviamo che Σ ammette un' unica soluzione intera minore del prodotto $m_1 \cdot m_2 \cdot \ldots \cdot m_t$.

Esempio 5.3.8 Risolviamo il seguente sistema di equazioni congruenziali:

$$\Sigma = \begin{cases} x \equiv 2 (\bmod 101) \\ x \equiv 4 (\bmod 137) \\ x \equiv 1 (\bmod 7) \end{cases} .$$

Poniamo $m_1 = 101, m_2 = 137, m_3 = 7$ e $b_1 = 2, b_2 = 4, b_3 = 1$. Allora $m'_1 = 137 \cdot 7 = 959$ $m'_2 = 101 \cdot 7 = 707$ $m'_3 = 137 \cdot 101$. Risolviamo singolarmente ciascuna delle seguenti equazioni:
i) $959x \equiv 1$ ($\bmod 101$). I numeri 959 e 101 sono coprimi, e dal teorema di Bezout possiamo esprimere 1 come loro combinazione lineare. $1 = 959(-2) + 101 \cdot 19$, quindi (-2) è soluzione della i.
ii) $707x \equiv 1$ ($\bmod 137$). Facendo i calcoli si ottiene: $1 = 289 \cdot 137 - 56 \cdot 707$ quindi -56 è soluzione della ii.
iii) $13837x \equiv 1$ ($\bmod 7$). Facendo i calcoli si ottiene: $1 = 13837 \cdot 3 - 7 \cdot 5930$, allora 3 è soluzione della iii.

Dalla dimostrazione del teorema cinese del resto si evince che l'intero $c = b_1 \cdot m'_1 \cdot (-2) + b_2 \cdot m'_2 \cdot (-56) + b_3 \cdot m'_3 \cdot 3 = 2 \cdot 259 \cdot (-2) + 4 \cdot 707 \cdot (-56) + 1 \cdot 13837 \cdot \cdot 3 = -120693$ è soluzione del sistema. Osserviamo che $-120693 \equiv 73025$ ($\bmod 101 \cdot 137 \cdot 7$).

Esercizio 5.3.9 Determinare un numero intero c minore di 100000, e multiplo di 46 37, e tale che $[c]_{17} = [2]_{17}$.

Il prossimo esempio è un'applicazione del teorema cinese del resto.

Esempio 5.3.10 Determinare un numero intero c compreso tra 100000 e 180000, tale che $[c]_{137} = [4]_{137}, [c]_{101} = [2]_{101}, [c]_7 = [1]_7$. Risolvendo questo problema si riesce a determinare il numero dei soldati di un esercito in cui si stima che ci siano circa 170000 unità. Si dispongono i militari prima in fila per 137, ed in coda si contano 4 soldati spaiati. Poi si dispongono i militari in fila per 101, ed in coda si contano 2 soldati spaiati. Infine si dispongono i militari in fila per 7, ed in coda si conta 1 solo soldato. Il sistema congruenziale che si deve risolvere è proprio quello riportato nell'esempio precedente. L'unico intero compreso tra 100000 e 180000 che risulta essere congruo a $-120693 \pmod{101 \cdot 137 \cdot 7}$ è 169884.

5.4 I CRITERI DI DIVISIBILITÀ

Essendo ben noti i criteri di divisibilità per 2 per 5, in questa sezione ci occuperemo dei criteri di divisibilità per gli altri numeri primi. Nei discorsi che seguono denoteremo con p un numero primo distinto da 2 e da 5, e con $a = a_n a_{n-1} \dots a_0$ un numero intero espresso in base 10 mediante le sue cifre. Chiaramente a si può esprimere come combinazione delle potenze di 10,

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0.$$

Per stabilire se a è divisibile per p, basta calcolare il resto della divisione euclidea di a per p. Chiaramente p divide a se e solo se $[a]_p = 0$.

$$[a]_p = [a_n]_p \cdot [10]_p^n + [a_{n-1}]_p [10]_p^{n-1} + \dots + [a_1]_p \cdot [10]_p + [a_0]_p.$$

Nello studio della divisibilità di a per il numero p assumono un ruolo significativo le potenza di 10 che risultano congrue ad 1 modulo p. Se infatti $10^s \equiv 1 \pmod{p}$ per qualche intero s, allora la relazione

$$[a]_p = [a_n]_p \cdot [10]_p^n + [a_{n-1}]_p [10]_p^{n-1} + \dots + [a_1]_p \cdot [10]_p + [a_0]_p.$$

può essere riscritta, utilizzando l'aritmetica modulare, con meno addendi, individuado difatto un numero b molto minore di a per il quale $[a]_p = [b]_p$. Il seguente esempio illustra il criterio di divisibilità per 11.

Esempio 5.4.1 se $p = 11$ $a = 213470351$. Poiché $10^2 \equiv 1(\mathrm{mod}11)$, possiamo esprimere a come combinazione delle potenze di $100 = 10^2$:

$$a = 51 \cdot 100^0 + 03 \cdot 100^1 + 47 \cdot 100^2 + 13 \cdot 100^3 + 02 \cdot 100^4,$$

passando alle classi e tenendo conto che $100^i \equiv 1(\mathrm{mod}11)$ per ogni i, si ha $[a]_{11} = [213470351]_{11} = [51]_{11} + [03]_{11} + [47]_{11} + [13]_{11} + [02]_{11} = [51 + 03 + 47 + 13 + 02]_{11} = [116]_{11}$.

Reiterando il procedimento avremo: $[116]_{11} = [16 + 1]_{11} = [6]_{11}$. Quindi il resto della divisione euclidea del numero 213470351 per 11 è 6.

In questo tipo di procedimento assume rilievo il minimo esponente $m = o(10, p)$, per cui $10^m \equiv 1(\mathrm{mod}p)$. Come conseguenza del piccolo teorema di Fermat si ha che per ogni primo p, sussiste la relazione:

$$10^{p-1} \equiv 1(\mathrm{mod}p),$$

ma come abbiamo visto nel caso $p = 11$, l'esponente $p - 1$ non è detto che sia il minimo per cui tale relazione sussiste.

Esempio 5.4.2 se $p = 11$ la minima potenza di 10 che risulta congrua ad 1 modulo p è $2 = o(10, 11)$.

Esempio 5.4.3 se $p = 3$ la minima potenza di 10 che risulta congrua ad 1 modulo p è $1 = o(10, 3)$.

Esempio 5.4.4 se $p = 37$ la minima potenza di 10 che risulta congrua ad 1 modulo p è $3 = o(10, 37)$.

Esempio 5.4.5 se $p = 7$ la minima potenza di 10 che risulta congrua ad 1 modulo p è $6 = o(10, 7)$.

In generale la classe dei resti modulo 11 di un numero naturale a coincide con la classe dei resti modulo 11 del numero ottenuto sommando a due a due, procedendo da destra verso sinistra, i numeri di due cifre individuati dalle cifre di a. Come conseguenza si ha subito che *un numero è divisibile per* 11 *se e solo se la somma delle cifre di posto pari e la somma delle cifre di posto dispari coincidono.*

Chiaramente è possibile ripercorrere il ragionamento precedente nel caso del numero primo 3, o anche del numero 9, tenendo conto che $10^i \equiv 1(\mathrm{mod}9)$ e anche $10^i \equiv 1(\mathrm{mod}3)$ per ogni i. In tal caso si ottiene che:

La classe dei resti modulo 9 (risp.3) di un numero naturale a *coincide con la classe dei resti modulo 9 (risp. 3) del numero ottenuto sommando le cifre di* a.

Queste considerazioni assumono un certo rilievo anche pratico quando si ha a che fare con numeri "grandi".

Esempio 5.4.6 Se si vuole stabilire se il numero $a = 17661412115589$ è divisibile per 7 si può tener conto che $10^6 \equiv 1 (\mathrm{mod} 7)$ e quindi raggruppando secondo le potenze di 10^6 abbiamo:

$a = 115589 \cdot (10^6)^0 + 661412 \cdot (10^6)^1 + 17(10^6)^2$, e quindi passando alle classi: $[a]_7 = [115589]_7 + [661412]_7 + [17]_7 = [777018]_7 = [777000]_7 + [18]_7 = [4]_7$.

In generale assegnato un qualunque numero a ed eseguendo la somma delle sue cifre raggruppate a sei alla volte da destra verso sinistra, lo studio della divisibilità per il numero 7 si riduce dopo "pochi passi" ad un numero che ha al più sei cifre.

Esercizio 5.4.7 $13^{13^{13}} + 1$ è divisibile per 7?

CAPITOLO 6

GRUPPI

In questo capitolo approfondiremo lo studio dei gruppi, già iniziato nel capitolo IV.

6.1 SOTTOGRUPPI E GRUPPI CICLICI

Osserviamo che dalle definizioni date, se G è un gruppo e H una parte non vuota di G, allora H è un sottogruppo di G se e solo se H è stabile, possiede elemento neutro ed ogni elemento di H è simmetrizzabile. Per denotare che H è un sottogruppo di G si scrive $H \leqslant G$. Quindi usando la notazione moltiplicativa avremo:

$$H \leqslant G \iff \begin{cases} \forall x, y \in H, x \cdot y \in H; \\ 1_G \in H; \\ \forall x \in H, x^{-1} \in H. \end{cases}$$

Esercizio 6.1.1 Scrivere l'equivalenza suddetta usando la notazione additiva.

Osserviamo che un gruppo può contenere parti stabili che non sono sottogruppi, ad esempio ogni insieme del tipo $\mathbb{N} \setminus I_t$ è una parte stabile del gruppo $(\mathbb{Z}, +)$.

Esercizio 6.1.2 Provare che per ogni $m \in \mathbb{Z}$, l'insieme $m \cdot \mathbb{Z} := \{mz : z \in \mathbb{Z}\}$ è un sottogruppo di $(\mathbb{Z}, +)$.

I sottogruppi di $(\mathbb{Z}, +)$ si possono caratterizzare.

Proposizione 6.1.3 *I sottogruppi di $(\mathbb{Z}, +)$ sono tutti e soli del tipo $m \cdot \mathbb{Z}$ con m intero.*

Dimostrazione — Abbiamo già osservato che ogni parte del tipo $m \cdot \mathbb{Z}$ è un sottogruppo di $(\mathbb{Z}, +)$. Sia ora H un sottogruppo di $(\mathbb{Z}, +)$, e proviamo che coincide con qualche $m \cdot \mathbb{Z}$. Se H è un sottogruppo banale di $(\mathbb{Z}, +)$ l'asserto è ovvio. Allora possiamo supporre che H contiene un elemento non nullo ed il suo opposto, sicché l'insieme $X := \{n \in H : n > 0\}$ è non vuoto. Poniamo $m := minX$. Poiché H è un sottogruppo di $(\mathbb{Z}, +)$, ogni multiplo di m giace in H, quindi $m \cdot \mathbb{Z} \subseteq H$. Sia $h \in H$, e siano q ed r il quoziente ed il resto della divisione euclidea di h per m:

$$h = mq + r, \quad 0 \leqslant r < m.$$

Per ipotesi l'elemento $r = h - mq$ giace in H, ed essendo minore di m non può appartenere ad X, allora deve coincidere con 0. Abbiamo provato che $h = mq$, quindi $H = m \cdot \mathbb{Z}$. □

Osserviamo inoltre che l'intersezione di una famiglia di sottogruppi di un gruppo G è ancora un sottogruppo. In particolare se X è un sottoinsieme di G, e donotiamo con $\mathfrak{F}_X$ la famiglia dei sottogruppi di G contenenti X, allora l'intersezione: $\langle X \rangle := \bigcap_{K \in \mathfrak{F}_X} K$ è un sottogruppo di G. Evidentemente $\langle X \rangle$ coincide col più piccolo sottogruppo di G contenete X, e si chiama *sottogruppo generato da* X. Nel caso in cui $X = \{x\}$ è un singleton denoteremo il sottogruppo generato da X semplicemente col simbolo $\langle x \rangle$.

Esercizio 6.1.4 Sia G un gruppo, e sia $x \in G$. Verificare che

$$\langle x \rangle = \{x^n : n \in \mathbb{Z}\}.$$

Esempio 6.1.5 Consideriamo il gruppo $(\mathbb{Z}, +)$. Il sottogruppo generato dal sottoinsieme $\{2\}$ di $\mathbb{Z}$ è $\langle 2 \rangle = 2\mathbb{Z}$.

Esercizio 6.1.6 Consideriamo il gruppo $(\mathbb{Z}, +)$. Determinare il sottogruppo generato dal sottoinsieme $\{5, 7\}$ di $\mathbb{Z}$.

Un gruppo G *si dice ciclico* se esiste $x \in G$ tale che $\langle x \rangle = G$. Un esempio di gruppo ciclico infinito è $(\mathbb{Z}, +)$, mentre ad esempio il gruppo S_3 non è ciclico.

Esercizio 6.1.7 Sia $G = \langle x \rangle$ un gruppo ciclico. Provare che G è finito se e solo se esiste un intero positivo n, tale che $x^n = 1$.

Il seguente risultato caratterizza l'ordine dei gruppi ciclici finiti.

Proposizione 6.1.8 *Sia $(G, \cdot)$ un gruppo ciclico finito, e sia x un suo generatore, allora $|G|$ coincide col minimo intero positivo m tale che $x^m = 1$.*

Dimostrazione — Per ipotesi $G = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$. Proviamo dapprima che per descrivere il gruppo G bastano le prime m potenze di x. Sia $n \in \mathbb{Z}$, allora $n = mq + r$ e $0 \leqslant r < m$ con q ed r opportuni. Allora $x^n = x^{mq}x^r = (x^m)^q x^r = 1^q x^r = x^r$. Pertanto $G = \{1 = x^0, x = x^1, \ldots, x^{m-1}\}$. Gli elementi $1 = x^0, x = x^1, \ldots, x^{m-1}$ sono a due a due distinti, altrimenti si individuerebbero due interi, i e j tali che $0 \leqslant i < j < m$ e $x^{j-i} = 1$, contraddicendo la minimalità di m. □

Sia G un gruppo ed x un suo elemento. Diremo che x è *periodico* se esiste un itero n tale che $x^n = 1$. Se x è un elemento periodico di G, si dice *periodo di x* il minimo intero positivo m tale che $x^m = 1$. In virù della proposizione precedente, se x è periodico, allora il suo periodo coincide con l'ordine del sottogruppo $\langle x \rangle$.

Proposizione 6.1.9 *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Dimostrazione — Per ipotesi $G = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ per un opportuno elemento x. Sia H un sottogruppo di G. Chiaramente possiamo supporre $H \neq 1$. Gli elementi di H sono delle potenze di x, e tra queste possiamo considerarne qualcuna positiva. Sia m la minima potenza positiva di x che giace in H. Verifichiamo che H è ciclico essendo x^m un suo generatore. Per la stabilità di H ogni potenza positiva di x^m giace ancora in H, e se n è negativo anche $(x^m)^n = (x^{-m})^{-n}$ giace in H. Rimane da provare che $H \subseteq \langle x^m \rangle = \{(x^m)^n : n \in \mathbb{Z}\}$. A tal scopo sia $h \in H \leqslant G$, allora $h = x^a$ per qualche intero a. Per l'algoritmo della divisione euclidea $a = mq + r$ dove $0 \leqslant r < m$. Le potenze x^a e x^{mq} appartengono ad H, allora anche x^r appartiene ad H. Pertanto r deve essere necessariamente nullo, e $h \in \langle x^m \rangle$. □

6.2 Classi laterali, teorema di Lagrange e di Eulero-Fermat

Sia H un sottogruppo di G e sia $\mathfrak{R}'_H$ la relazione binaria in G definita ponendo: $x\mathfrak{R}'_H y \iff x^{-1}y \in H$. Verifichiamo che $\mathfrak{R}'_H$ è di equivalenza:

i) $\mathfrak{R}'_H$ è riflessiva perché $x^{-1}x = 1$ e $1 \in H$;
ii) $\mathfrak{R}'_H$ è simmetrica perché se $x^{-1}y \in H$, allora $(x^{-1}y)^{-1} \in H$ per cui $y^{-1}x \in H$ e $y\mathfrak{R}'_H x$;
iii) La transitività della relazione $\mathfrak{R}'_H$ consegue dalla stabilità di H.

Analogamente si definisce $\mathfrak{R}''_H$ ponendo: $x\mathfrak{R}''_H y \iff xy^{-1} \in H$, e si verifica che $\mathfrak{R}''_H$ è una relazione d'equivalenza.

Le relazioni di equivalenza che abbiamo definito possono non essere congruenze, come mostra il seguente esempio:

Esempio 6.2.1 Sia $G = S_3$ e $H = \{1, (12)\}$. Chiaramente $H = \{1, (12)\}$ è un sottogruppo di G. Le relazioni $\mathfrak{R}'_H$ e $\mathfrak{R}''_H$ non sono congruenze . Infatti
$(23)\mathfrak{R}'_H(123)$
$(13)\mathfrak{R}'_H(132)$, ma componendo ordinatamente
$(23)\cdot(13) = (132)$ che non è in relazione con $(123)\cdot(132) = 1$, in quanto $(132)^{-1}\cdot 1 \notin H$. Un discorso analogo vale per la $\mathfrak{R}''_H$.

Qualunque sia l'elemento $x \in G$, risulta:
$[x]_{\mathfrak{R}'_H} = \{z \in G : x\mathfrak{R}'_H z\} = \{z \in G : x^{-1}z \in H\} = \{xh : h \in H\}$.
La classe d'equivalenza $[x]_{\mathfrak{R}'_H}$ si dice *laterale sinistro di H in G determinato da x*, e si denota con il simbolo xH. Allora l'insieme quoziente $G/\mathfrak{R}'_H = \{xH : x \in G\}$.

Analogamente, qualunque sia $x \in G$, risulta: $[x]_{\mathfrak{R}''_H} = \{hx : h \in H\}$. Tale classe d'equivalenza si dice *laterale destro di* H *in* G *determinato da x*, e si denota con il simbolo Hx, inoltre $G/\mathfrak{R}''_H = \{Hx : x \in G\}$.

Lemma 6.2.2 *Qualunque sia l'elemento* $x \in G$ *i laterali* xH*e* Hx *sono equipotenti ad* H.

Dimostrazione – L'applicazione $f : h \in H \to xh \in xH$ è biettiva. Analogamente si prova che H è equipotente ad Hx. □

Teorema 6.2.3 (di Lagrange) *Sia* G *un gruppo finito, e sia* H *un suo sottogruppo. Allora* $|H|$ *divide* $|G|$. *Inoltre* $|G| = |H||G/\mathfrak{R}'_H| = |H||G/\mathfrak{R}''_H|$.

Dimostrazione – . L'insieme $G/\mathfrak{R}'_H = \{xH : x \in G\}$ è una partizione di G, quindi posto $t = |G/\mathfrak{R}'_H|$ abbiamo

$$G = x_1H \cup \ldots \cup x_tH.$$

Per il lemma precedente tutti i laterali sono equipotenti ad H, quindi $|G| = \underbrace{|H| + \ldots + |H|}_{t} = |H| \cdot t$. In particolare $|H|$ divide $|G|$.

Analogamente posto $s = |G/\mathfrak{R}''_H|$ avremo $|G| = |H| \cdot s$, da cui $s = t$, e la dimostrazione è completa. □

Quanto abbiamo provato, assicura che in un gruppo finito G il numero dei laterali destri individuati da un sottogruppo H coincide col numero dei laterali sinistri. Tale invariante si chiama *indice di* H *in* G e si denota col simbolo $|G : H|$.

Corollario 6.2.4 *Sia* G *un gruppo finito di ordine* n*, e sia* x *un elemento di* G*. Allora il periodo di* x *divide* n*, ed in particolare* $x^n = 1$*.*

Dimostrazione — Per il teorema di Lagrange l'ordine m del sottogruppo ciclico $\langle x \rangle$ divide n, quindi $n = mq$ per un opportuno intero q. Per la proposizione 6.1.8, risulta $x^n = (x^m)^q = 1^q = 1$. □

Osservazione 6.2.5 Alla fine dell'esempio 5.4.1 abbiamo osservato che se p è un intero, per calcolare il resto di una classe modulo p assume rilievo il minimo esponente $m = o(10, p)$, per cui $10^m \equiv 1 (\mathrm{mod}\, p)$. Tale numero coincide evidentemente col periodo della classe di $[10]_p$ nel gruppo degli invertibili modulo p, ed in particolare m è un divisore di $p - 1$.

Il prossimo risultato è usato nel sistema RSA di crittografia a chiave pubblica.

Teorema 6.2.6 (di Eulero-Fermat) *Sia* m *un numero intero positivo. Per ogni* $a \in \mathbb{Z}$ *coprimo con* m*,* $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$*.*

Dimostrazione — Sia a un intero coprimo con m, allora $[a]_m$, per il lemma 5.2.8, appartiene al sottogruppo $U(\mathbb{Z}_m)$ degli elementi invertibili del monoide $(\mathbb{Z}_m, \cdot)$. Per la proposizione 5.2.14, il gruppo $U(\mathbb{Z}_m)$ ha ordine $\varphi(m)$, quindi per il corollario precedente $[a^{\varphi(m)}]_m = ([a]_m)^{\varphi(m)} = [1]_m$. Allora gli elementi $a^{\varphi(m)}$ e 1 sono equivalenti modulo m. □

6.3 CONGRUENZE E OMOMORFISMI

Nel paragrafo precedente abbiamo osservato che se G è un gruppo e H un sottogruppo di G, allora le relazioni $\mathfrak{R}'_H$ e $\mathfrak{R}''_H$ possono non essere una congruenza di G. D'altra parte in alcuni casi ciò accade:

Proposizione 6.3.1 *Sia* G *un gruppo, e sia* H *un sottogruppo di* G*. Se le relazioni* $\mathfrak{R}'_H$ *e* $\mathfrak{R}''_H$ *coincidono, allora individuano una congruenza di* G*.*

DIMOSTRAZIONE – Poniamo $\mathfrak{R}_H = \mathfrak{R}'_H = \mathfrak{R}''_H$. Siano x_1, x_2, y_1, y_2 elementi di G tali che $x_1 \mathfrak{R}_H x_2$ e $y_1 \mathfrak{R}_H y_2$. Segue che $x_1 x_2^{-1} = x_1 y_1 (x_2 y_1)^{-1}$ giace in H, allora $x_1 y_1 \mathfrak{R}_H x_2 y_1$, e analogamente $y_1^{-1} y_2 = (x_2 y_1)^{-1} x_2 y_2 \in H$, per cui $x_2 y_1 \mathfrak{R}_H x_2 y_2$. D'altra parte $\mathfrak{R}_H$ è una relazione transitiva, per cui $x_1 y_1 \mathfrak{R}_H x_2 y_2$. Abbiamo verificato che $\mathfrak{R}_H$ è una congruenza.

Esempio 6.3.2 Sia G il gruppo simmetrico su tre oggetti, e sia

$$H = \{1, (123), (132)\} = \langle (123) \rangle$$

il sottogruppo generato da una permutazione che sposta tutti gli elementi. È facile verificare che $\mathfrak{R}'_H = \mathfrak{R}''_H$.

Nei gruppi abeliani ogni sottogruppo individua una congruenza. Infatti se è G un gruppo abeliano e H un suo sottogruppo, per ogni $x \in G$ risulta chiaramente $xH = Hx$. Allora le relazioni $\mathfrak{R}'_H$ e $\mathfrak{R}''_H$ determinano le stesse classi di equivalenza, perciò $\mathfrak{R}'_H = \mathfrak{R}''_H$. Possiamo sintetizzare quanto detto con la seguente proposizione

Proposizione 6.3.3 *Sia* G *un gruppo abeliano, e sia* H *un sottogruppo di* G. *Allora* $\mathfrak{R}'_H$ *e* $\mathfrak{R}''_H$ *coincidono.*

Sia G un gruppo, e sia H un sottogruppo di G. Diremo che H è un sottogruppo *normale in* G se le relazioni $\mathfrak{R}'_H$ e $\mathfrak{R}''_H$ coincidono. In tal caso la congruenza determinata da H si denota semplicemente col simbolo $\mathfrak{R}_H$, ed inoltre la struttura quoziente $G/\mathfrak{R}_H$ si denota col simbolo G/H. Si può provare che le congruenze in un gruppo sono solo di questo tipo, infatti:

Teorema 6.3.4 *Sia* G *un gruppo e sia* $\mathfrak{R}$ *una congruenza in* G, *allora esiste un sottogruppo* H *normale in* G *tale che* $\mathfrak{R} = \mathfrak{R}_H$.

DIMOSTRAZIONE – Poniamo $H = [1]_{\mathfrak{R}}$. Si verifica facilmente che H è un sottogruppo di G. Inoltre per ogni x ed y in G risulta:

$$x \mathfrak{R}'_H y \iff x^{-1} y \in H \iff x^{-1} y \equiv 1 (\mathrm{mod} \mathfrak{R}),$$

d'altra parte $\mathfrak{R}$ è una congruenza in G, quindi:

$$x^{-1} y \equiv 1 (\mathrm{mod} \mathfrak{R}) \iff y \equiv x (\mathrm{mod} \mathfrak{R}).$$

Allora $x \mathfrak{R}'_H y \iff x \mathfrak{R} y$. Analogamente si verifica che le relazioni $\mathfrak{R}''_H$ e $\mathfrak{R}$ coincidono. Pertanto H è normale in G e $\mathfrak{R} = \mathfrak{R}_H$. □

Esercizio 6.3.5 Sia $(\mathbb{Z}, +)$ il gruppo additivo degli interi, e sia $m\mathbb{Z}$ un suo sottogruppo. Verificare che il quoziente $\mathbb{Z}/m\mathbb{Z}$ coincide con l'insieme $\mathbb{Z}_m$ costituito dalla classe dei resti modulo m.

Esercizio 6.3.6 Sia $(V, +)$ il gruppo additivo dei vettori orientati applicati nell'origine dello spazio euclideo. Si consideri il sottoinsieme V' di V, costituito dai vettori che giacciono nel piano α passante per l'origine. Verificare che V' è un sottogruppo di V. Descrivere la struttura $(V/V', +)$.

Esercizio 6.3.7 Sia G un gruppo, e siano H un sottogruppo normale di G, e X un sottogruppo di G. Provare che l'insieme $HX := \{hx : h \in H \text{ e } x \in X\}$ costituito da tutti i prodotti col promo fattore in H e il secondo in X è un sottogruppo di G. In particolare verificare che HX coincide col sottogruppo generato da H e da X. Inoltre si ha: $HX = \langle H, X\rangle = XH$.

Esercizio 6.3.8 Individuare un sottogruppo H di $(\mathbb{Z}_{36}, +)$ di ordine 3. Provare che il quoziente $\mathbb{Z}_{36}/H$ è ciclico, ed elencare i generatori.

In un gruppo quindi i sottogruppi normali caratterizzano le congruenze. Nella seconda parte di questo paragrafo evidenzieremo in che modo la nozione di congruenza in un gruppo è collegata a quella di omomorfismo tra gruppi.

Siano G_1 e G_2 gruppi, e sia $f : G_1 \to G_2$ un omomorfismo. Si dice *nucleo* di f e si denota col simbolo $\mathrm{Ker}(f)$, l'insieme degli elementi di G_1 la cui immagine mediante f coincide con l'elemento neutro di G_2:

$$\mathrm{Ker}(f) = \{x \in G_1 : f(x) = 1\}.$$

Esercizio 6.3.9 *Siano G_1 e G_2 gruppi, e sia $f : G_1 \to G_2$ un omomorfismo. Provare che:*
(i) $f(1) = 1$;
(ii) $\forall x \in G_1$, $f(x^{-1}) = (f(x))^{-1}$;
(iii) $\forall x \in G_1$ *e* $\forall n \in \mathbb{Z}$, $f(x^n) = (f(x))^n$.

Lemma 6.3.10 *Siano G_1 e G_2 gruppi, e sia $f : G_1 \to G_2$ un omomorfismo. Il nucleo di f è un sottogruppo normale di G_1*

DIMOSTRAZIONE – Siano $x, y \in \ker(f)$. Allora $f(x) = 1$ e $f(y) = 1$, quindi $f(xy) = f(x)f(y) = 1 \cdot 1 = 1$. Ciò prova che $\ker(f)$ è una parte stabile di G_1. Per la (i) dell'esercizio 6.3.9 si ha $f(1) = 1$, quindi $1 \in \ker(f)$. Sia $x \in \ker(f)$ e verifichiamo che $x^{-1} \in \ker(f)$. Per la (ii) dell'esercizio 6.3.9 si ha $f(x^{-1}) = (f(x))^{-1} = (1)^{-1} = 1$. Ne segue che $\ker((f)$ è un sottogruppo di G_1. Ora proviamo che $\ker(f)$ è normale in G_1. A tal scopo basta verificare che $\forall x \in G_1$ i laterali $x\ker(f)$ e $\ker(f)\, x$ coincidono. Un elemento del laterale $x\ker(f)$ è del tipo xz con $z \in \ker(f)$, per cui $f(xzx^{-1}) = f(x)f(z)f(x^{-1}) = 1$, sicché $k = xzx^{-1} \in \ker(f)$. Pertanto l'elemento $xz = xz(x^{-1}x) = (xzx^{-1})x = kx$ giace in $\ker(f)\, x$. Pertanto $x\ker(f) \subseteq \ker(f)\, x$. L'altra inclusione si prova analogamente. □

Sia $(G, \cdot)$ un gruppo. Per ogni sottogruppo normale N in G, è possibile definire l'applicazione $\pi : x \in G \to xN \in G/N$. Chiaramente π è un omomorfismo suriettivo, che si chiama *epimorfismo canonico di* G *su* G/N. Osserviamo che il nucleo di π è proprio N.

Per l'osservazione appena fatta e per il lemma precedente, abbiamo la seguente caratterizzazione dei sottogruppi normali:

Proposizione 6.3.11 *Sia* G *un gruppo. Un sottogruppo* H *di* G *è normale se e solo se coincide col nucleo di un omomorfismo di dominio* G.

Ora vediamo come si raffina il teorema di omomorfismo per le strutture algebriche nel caso dei gruppi.

Teorema 6.3.12 (PRIMO TEOREMA DI OMOMORFISMO) *Siano* G_1 *e* G_2 *gruppi e sia* $f : G_1 \to G_2$ *un un omomorfismo. Allora esiste un unico omomorfismo* $\varphi : G_1/\ker(f) \to G_2$ *tale che* $\varphi \circ \pi = f$ *, dove* $\pi : G_1 \to G_1/\ker(f)$ *è l'epimorfismo canonico. Inoltre è un monomorfismo, e i gruppi* $G_1/\ker(f)$ *e* $f(G_1)$ *sono isomorfi.*

DIMOSTRAZIONE – Proviamo dapprima che la relazione determinata dall'applicazione f coincide con la congruenza determinata dal nucleo di f. A tal scopo basta osservare che $\forall x, y \in G_1$, $x\mathfrak{R}_f y \iff f(x) = f(y) \iff f(x)(f(y))^{-1} = 1 \iff f(x)(f(y^{-1})) = 1 \iff xy^{-1} \in \mathrm{Ker}(f) \iff x\, \mathfrak{R}_{\mathrm{Ker}(f)}\, y$. Applicando il teorema di omomorfismo tra strutture algebriche si ha la tesi, con $\varphi : x\mathrm{Ker}(f) \in G_1/\ker(f) \to f(x) \in G_2$. □

Il primo teorema di omomorfismo può essere schematizzato col seguente diagramma:

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ \downarrow \pi & \varphi \nearrow & \\ G_1/\ker(f) & & \end{array} .$$

Corollario 6.3.13 *Ogni gruppo ciclico è isomorfo a qualche* $\mathbb{Z}_m$.

Dimostrazione — Sia $(G, \cdot)$ un gruppo ciclico, e sia x un suo generatore. L'applicazione $f : n \in \mathbb{Z} \to x^n \in G$ è un omomorfismo suriettivo tra il gruppo additivo degli interi e G. Il nucleo di f è un sottogruppo di $\mathbb{Z}$, quindi $Ker(f) = m\mathbb{Z}$ per un opportuno intero m. Per il primo Teorema di omomorfismo tra gruppi, il quoziente $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ è isomorfo a G. □

Di seguito riportiamo gli enunciati di altri due teoremi di isomorfismo per i gruppi.

Teorema 6.3.14 (Secondo Teorema di Omomorfismo) *Sia* G *un gruppo, e siano* N *e* H *sottogruppi di* G *con* N *normale in* $\langle N, H\rangle$. *Allora* $N \cap H$ *è normale in* H *e i quozienti* $\langle N, H\rangle/N$ *e* $H/N \cap H$*sono isomorfi.*

Teorema 6.3.15 (Terzo Teorema di Omomorfismo) *Sia* G *un gruppo, e siano* N *e* H *sottogruppi normali di* G, *con* $H \leqslant N$. *Allora il il quoziente* $\frac{G/H}{N/H}$ *è isomorfo a* G/N.

6.4 GRUPPI DI PERMUTAZIONI

Nei paragrafi precedenti abbiamo già visto che se X è un insieme, la struttura $(S_X, \cdot)$, il cui sostegno è costituito da tutte le permutazioni di X, è un gruppo, il *Gruppo delle Permutazioni su X*. L'operazione binaria è la seguente:

$$\cdot : (f, g) \in S_X \times S_X \to g \circ f \in S_X$$

L'elemento neutro è l'applicazione identica su X, e l'inverso di ciascun elemento $f \in S_X$ è l'applicazione inversa di f. La struttura $(S_X, \cdot)$ dipende dalla "quantità" (cardinalità), ma non dalla qualità degli elementi di X, come si evince anche dal seguente teorema:

Teorema 6.4.1 *Se* X *e* Y *sono insiemi equipotenti, allora i gruppi* $(S_X, \cdot)$ *e* $(S_Y, \cdot)$ *sono isomorfi.*

Dimostrazione — Per ipotesi esiste un'applicazione biettiva $\varphi : X \longrightarrow Y$. Per ogni $f \in S_X$ l'applicazione $\varphi \circ f \circ \varphi^{-1}$ è chiaramente una permutazione di Y, rimane quindi definita un applicazione del tipo

$$\Phi : f \in S_X \to \varphi \circ f \circ \varphi^{-1} \in S_Y.$$

Si verifica facilmente che Φ è un isomorfismo. □

In questo paragrafo approfondiremo lo studio dei gruppi di permutazioni, quando X è un insieme finito. Per il teorema precedente, se $|X| = n$, lo studio del gruppo S_X, equivale allo studio del gruppo delle permutazioni dell'insieme $I_n = \{1, 2, 3, \ldots, n\}$.

Poniamo S_n l'insieme costituito da tutte le permutazioni su I_n. Il gruppo $(S_n, \cdot)$ si chiama *gruppo delle permutazioni su* n *oggetti*, e per il Corollario 3.3.8 ha ordine $n!$. Sia f una permutazione, e $i \in I_n$. Diremo che la permutazione f *fissa* i se $f(i) = i$. In caso contrario diremo che f *sposta* i. La permutazione identica del gruppo $(S_n, \cdot)$ fissa ogni elemento di I_n. Due permutazioni f e g si dicono disgiunte se l'insieme degli elementi spostati da f e l'insieme degli elementi spostati da g sono disgiuti.

Ci sono più modi per rappresentare le permutazioni. Ad esempio se $f \in S_7$ è la permutazione definita ponendo:

$$\begin{array}{rccc} f: & I_7 & \longrightarrow & I_7 \\ & 1 & \to & 1 \\ & 2 & \to & 2 \\ & 3 & \to & 3 \\ & 4 & \to & 7 \\ & 5 & \to & 6 \\ & 6 & \to & 4 \\ & 7 & \to & 5 \end{array},$$

allora possimo semplicemente scrivere una tabella con due righe, in cui nella prima riga compaiono ordinatamente i numeri da 1 a 7, e in colonna, nella seconda riga compaiono le loro immagini:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 7 & 6 & 4 & 5 \end{pmatrix}.$$

Quando non c'è ambiguità, possiamo usare una notazione ancora più snella: $f = (4\ 7\ 5\ 6)$. Tale rappresentazione si ottiene considerando il primo elemento spostato, "4", seguito dalla sua immagine mediante f, "$f(4) = 7$", a sua volta seguito da "$f(7) = 5$", ... fino a ottenere nuovamente l'elemento "4" come immagine dell'elemento spostato "6"($f(6) = 4$).

Diremo che una permutazione f è un *ciclo di lunghezza* k (k numero positivo maggiore di 1), se esistono $i_1, \ldots, i_k \in I_n$ tali che

$$f(i_1) = i_2, f(i_2) = i_3, \ldots, f(i_{k-1}) = i_k, f(i_k) = i_1.$$

In tal caso useremo la notazione "$f = (i_1 \dots i_k)$".

Osservazione 6.4.2 In base alla definizione, non c'è differenza tra il ciclo $(i_1 \dots i_k)$, e un qualunque altro ciclo ottenuto da questo facendo slittare tutti gli i_j di un certo numero di posti. Ad esempio $(i_1 \dots i_k) = (i_2 i_3 \dots i_k i_1)$. Si evince che un ciclo di lunghezza k si può scrivere in k modi.

La permutazione dell'esempio precedente è un ciclo di lunghezza 4. Iterando il procedimento esposto otterremo un algoritmo che consente di decomporre ogni permutazione non identica nel prodotto di cicli a due a due disgiunti.

Vediamo dapprima con qualche esempio:

Esempio 6.4.3 Sia

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 7 & 6 & 4 & 5 & 10 & 9 & 8 \end{pmatrix}.$$

Allora

$f = (4\ 7\ 5\ 6)(8\ 10) = (8\ 10)(4\ 7\ 5\ 6)$

Nell'esempio precedente si è rilevato che la permutazione f è suscettibile di "due" rappresentazioni. Ciò dipende dal fatto che i cicli $(4\ 7\ 5\ 6)$ e $(8\ 10)$ sono permutabili. In generale abbiamo il seguente risultato:

Lemma 6.4.4 *Siano f e g permutazioni disgiunte in S_n. Allora f e g commutano.*

Dimostrazione — Consideriamo un generico elemento $i \in I_n$, e verifichiamo che $(f \cdot g)(i) = (g \cdot f)(i)$. Se i è fisssato da entrambe le permutazioni, risulta ovviamente $(f \cdot g)(i) = i = (g \cdot f)(i)$. Allora possiamo assumere che i sia spostato da almeno una delle due permutazioni considerate. Supponiamo che $f(i) \neq i$. Essendo f iniettiva $f(f(i)) \neq f(i)$, e per ipotesi i e $f(i)$ sono fissati da g. Allora

$(f \cdot g)(i) = (g \circ f)(i) = g(f(i) = f(i)$ e $(g \cdot f)(i) = (f \circ g)(i) = f(g(i) = f(i)$, come volevasi. In modo analogo si procede se i è spostato dalla permutazione g. □

Possiamo ora enunciare il teorema di decomposizione delle permutazioni.

Teorema 6.4.5 (di decomposizione in cicli delle permutazioni) *Sia f una permutazione non identica in S_n. Allora f è un ciclo, oppure si decompone nel prodotto di cicli a due a due disgiunti. Inoltre tale decomposizione è unica a meno dell'ordine dei fattori.*

Un ciclo di lunghezza 2 si chiama *trasposizione*.

Proposizione 6.4.6 *Sia* f *un ciclo di lunghezza* k*. Allora* f *si può esprimere come prodotto di* $k-1$ *trasposizioni.*

DIMOSTRAZIONE — Poniamo $f = (i_1 \dots i_k)$. È immediato verificare che: $f = (i_1 i_2)(i_1 i_3) \cdots (i_1 i_k)$. □

Sia f una permutazione di S_n. Per i risultati precedenti, f si esprime come prodotto di trasposizioni. Tale espressione non è detto che sia unica, d'altra parte si prova che la parità del numero di trasposizioni che intervengono non dipende dalla decomposizione considerata. Se tale numero è pari diremo che f è una permutazione *pari*, altrimenti diremo che f è una permutazione *dispari*

Esempio 6.4.7 Sia

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 3 & 7 & 6 & 4 & 5 & 10 & 9 & 8 \end{pmatrix}.$$

Allora
$f = (1\ 2)(4\ 7\ 5\ 6)(8\ 10) = (1\ 2)(4\ 7)(4\ 5)(4\ 6)(8\ 10)$ è una permutazione dispari.

Esercizio 6.4.8 S_{10} possiede sottogruppi di ordine 12?

Esercizio 6.4.9 S_{10} possiede sottogruppi di ordine 11?

Esercizio 6.4.10 Provare che l'insieme A_n delle permutazioni pari è un sottogruppo di S_n.

Esercizio 6.4.11 Sia $\Phi : S_n \to \{-1, 1\} = U(\mathbb{Z})$ definita ponendo:

$$\Phi(f) = \begin{cases} 1 & \text{se } f \text{ è pari} \\ -1 & \text{se } f \text{ è dispari} \end{cases}.$$

Verficare che Φ è un omomorfismo suriettivo e $S_n/A_n \simeq U(\mathbb{Z})$. In particolare $|S_n : A_n| = 2$.

CAPITOLO 7

SPAZI VETTORIALI

Nel capitolo 4 abbiamo già dato la definizione di Spazio Vettoriale su un campo, commentato le prime proprietà. Quando non c'è ambiguità parleremo semplicemente di spazi vettoriali, sottointendendo il campo degli scalari. In questo paragrafo approfondiremo lo studio di tale struttura.

7.1 SOTTOSPAZI E QUOZIENTI DI UNO SPAZIO VETTORIALE

Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K. Una parte V' si dice stabile se sono verificate le seguenti condizioni:

i) $\forall u, v \in V' \Rightarrow u + v \in V'$;

ii) $\forall \alpha \in K$ e $\forall v \in V' \Rightarrow \alpha \cdot v \in V'$.

Se la struttura $(V', +, \cdot)$ è un K-spazio vettoriale, allora V' si dice *sottospazio vettoriale di* V. Si ha la seguente proposizione:

Proposizione 7.1.1 *Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K. Un sottoinsieme V' di V è un sottospazio vettoriale di V se e solo se V' è stabile rispetto entrambe le operazioni:*

DIMOSTRAZIONE — Supponiamo che V' sia una parte stabile, e verifichiamo che la struttura $(V', +, \cdot)$ con le operazioni indotte, è un K-spazio vettoriale:

(1) Per provare che $(V', +)$ è un gruppo abeliano basta osservare che per la ii, $0 = 0v \in V'$ e inoltre per ogni $v \in V'$ anche l'elemento $(-1) \cdot v = -v \in V'$;

(2) $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v \qquad \forall \alpha \text{ e } \in K \text{ e } \forall u \text{ e } v \in V'$. Ovvia perché vale in V;

(3) $(\alpha +_K \beta) \cdot u = \alpha \cdot u + \beta \cdot u \qquad \forall \alpha \text{ e } \beta \in K \text{ e } \forall u \in V'$. Ovvia;

(4) $(\alpha \cdot_K \beta) \cdot u = \alpha \cdot (\beta \cdot u) \qquad \forall \alpha \text{ e } \beta \in K \text{ e } \forall u \in V'$. Ovvia;

(5) $1_K \cdot u = u \qquad \forall u \in V'$. Ovvia.

Viceversa: Se V' è un sottospazio di V, allora è anche parte stabile. □

Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K. Gli insiemi $\{0\}$ e V sono sottospazi di V i quali vengono chiamati *sottospazi banali*. Allora, ogni parte X di V contiene un sottospazio di V, ed è anche contenuta in un sottospazio di V. Osserviamo che l'intersezione di sottospazi di V è ancora un sottospazio di V. Diremo *sottospazio generato* da una parte X di V l'intersezione di tutti i sottospazi che contengono X. Tale sottospazio si denota così: $\langle X \rangle$. Se $X = \{v_1, v_2, \ldots, v_n\}$ è finito il sottospazio generato da X si denota anche col simbolo $\langle v_1, v_2, \ldots, v_n \rangle$.

Quando non c'è ambiguità un prodotto del tipo $\alpha \cdot v$ si denota semplicemente col simbolo $\alpha v'$. Una somma del tipo $\alpha_1 v_1 + \ldots + \alpha_n v_n$ si dice combinazione lineare dei vettori $v_1, v_2, \ldots, v_n$ secondo gli scalari $\alpha_1, \ldots \alpha_n$. Il sottospazio vettoriale generato da un numero finito di vettori è costituito da tutte le loro possibili combinazioni lineari. La verifica di ciò è lasciata come esercizio.

Esempio 7.1.2 Sia $(\mathbb{R}^2, +, \cdot)$ lo spazio vettoriale numerico su $\mathbb{R}$, e

$$A = \{(a, b) \in \mathbb{R}^2 : a \geqslant b\},$$
$$B = \{(a, b) \in \mathbb{R}^2 : a \cdot b \geqslant 0\},$$
$$C = \{(a, b) \in \mathbb{R}^2 : 2a - b = 0\}$$

sottoinsiemi di $\mathbb{R}^2$. Chiaramente C è un sottospazio, ma A e B non lo sono sono.

Esempio 7.1.3 Sia $(\mathbb{R}^3, +, \cdot)$ lo spazio vettoriale numerico su $\mathbb{R}$, e

$$A = \{(a, b, c) \in \mathbb{R}^3 : a^2 + b^2 + c^2 = 0\},$$
$$B = \{(a, b, c) \in \mathbb{R}^3 : a, b, c \geqslant 0\},$$
$$C = \{(a, b, c) \in \mathbb{R}^3 : a - b + 3c = 0\}$$

sottoinsiemi di $\mathbb{R}^3$. Chiaramente A e C sono sottospazi, ma B non lo è.

Esercizio 7.1.4 Verificare che l'insieme dei polinomi a coefficienti reali, $\mathbb{R}[x]$ è un $\mathbb{R}$-spazio vettoriale.

Quali dei seguenti sottoinsiemi è un sottospazio di $\mathbb{R}[x]$?

$$A = \{p \in \mathbb{R}[x] : \text{p=o oppure (p} \neq 0 \text{ e grado di p è maggiore di 5) }\},$$

$$B = \{p \in \mathbb{R}[x] : \text{p=o oppure (p} \neq 0 \text{ e grado di p è minore di 5)}\},$$

$$C = \{p \in \mathbb{R}[x] : \text{p=o oppure (p} \neq 0 \text{ e grado di p è 5)}\}.$$

Esercizio 7.1.5 Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K, e siano $v_1, v_2, \ldots, v_n$ elementi di V. Verificare che:

$$\langle v_1, v_2, \ldots, v_n \rangle = \{\sum_{i=1}^{n} \alpha_i v_i \in V : \alpha_i \in K\}.$$

Esempio 7.1.6 Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K. In virtù dell'esercizio precedente, avremo che il sottospazio generato da un singolo vettore $v \in V$ è costituito da tutti e soli i multipli di v:

$$\langle v \rangle = \{\alpha v \in V : \alpha \in K\}.$$

Esercizio 7.1.7 Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K, e siano V_1 e V_2 sottospazi di V. Verificare che:

$$\langle V_1, V_2 \rangle = \{v_1 + v_2 : \ v_1 \in V_1 \text{ e } v_2 \in V_2\}.$$

Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K, e siano V_1 e V_2 sottospazi di V. Il sottospazio generato da V_1 e V_2 si denota anche col simbolo $V_1 + V_2$, e si chiama *spazio somma*. Nel caso in cui $V_1 \cap V_2 = \{0\}$ lo spazio $V_1 + V_2$ si dice *somma diretta* e si denota col simbolo $V_1 \oplus V_2$.

Proposizione 7.1.8 *Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K, e siano V_1 e V_2 sottospazi di V. Allora V è somma diretta di V_1 e V_2 se e solo ogni vettore di V si esprime in unico modo come somma di un vettore di V_1 e un vettore di V_2.*

Dimostrazione — Supponiamo che $V = V_1 \oplus V_2$. Sia $v \in V$ e poniamo $v = v_1 + v_2 = u_1 + u_2$, con $u_1, v_1 \in V_1$ e $u_2, v_2 \in V_2$. Allora $v_1 - u_1 = u_2 - v_2 \in V_1 \cap V_2$, e per ipotesi $v_1 - u_1 = u_2 - v_1 = 0$. Ciò prova che $v_1 = u_1$ e $v_2 = u_2$. Viceversa, supponiamo che ogni vettore di V si esprime in unico modo come somma di un vettore di V_1 e un vettore di V_2. Sia v un vettore che giace in $V_1 \cap V_2$, allora risulta $v = 0 + v = v + 0$. Per l'unicita della scrittura segue che $v = 0$. □

Il teorema precedente consente di estendere agevolmente la nozione di somma diretta di più sottospazi. Siano $V_1, \dots V_t$ sottospazi di uno spazio vettoriale V. Diremo che lo spazio somma $V_1 + \dots + V_t$ è una *somma diretta* se ciascun vettore v di $V_1 + \dots + V_t$ si esprime in unico modo come somma del tipo $v = v_1 + \dots + v_t$ con ciascun $v_i \in V_i$. In tal caso scriveremo

$$V_1 \oplus \dots \oplus V_t.$$

Esempio 7.1.9 $\mathbb{R}^3 = V_1 \oplus V_2$, con $V_1 = \{(a, b, 0) : a, b \in \mathbb{R}\} \simeq \mathbb{R}^2$ e $V_2 = \{(0, 0, c) : c \in R\} \simeq \mathbb{R}$

Diremo che una relazione di equivalenza $\mathfrak{R}$ definita in un K-spazio vettoriale V è una *congruenza* in V, se è una congruenza rispetto alla struttura additiva $(V, +)$, e se inoltre vale la seguente proprietà:

$$(\star) : \forall u, v \in V, \forall \alpha \in K, u \,\mathfrak{R}\, v \iff \alpha \cdot u \,\mathfrak{R}\, \alpha \cdot v.$$

Se $\mathfrak{R}$ è una congruenza in V, nell'insieme quoziente $V/\mathfrak{R}$ è possibile definire le seguenti operazioni:

$$+ : ([u]_{\mathfrak{R}}, [v]_{\mathfrak{R}}) \in V/\mathfrak{R} \times V/\mathfrak{R} \to [u + v]_{\mathfrak{R}} \in V/\mathfrak{R}$$

$$\cdot_{est} : (\alpha, [v]_{\mathfrak{R}}) \in K \times V/\mathfrak{R} \to [\alpha \cdot v]_{\mathfrak{R}} \in V/\mathfrak{R}$$

La struttura $(V/\mathfrak{R}, +, \cdot_{est})$ è un K-spazio vettoriale.

Osservazione 7.1.10 Abbiamo visto che in un gruppo abeliano $(V, +)$ le congruenze sono tutte e sole del tipo $\mathfrak{R}_U$ con U sottogruppo di V. Tale proprietà si estende agli spazi vettoriali.

Teorema 7.1.11 *Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K. Allora le congruenze in V sono tutte e sole del tipo $\mathfrak{R}_U$, dove U è un sottospazio di V.*

Dimostrazione — Sia U un sottospazio di V. La relazione $\mathfrak{R}_U$ è una congruenza rispetto alla struttura additiva $(V, +)$, ogni classe di equivalenza è un laterale e $V/\mathfrak{R}_U = \{ v + U : v \in V\}$. D'altra parte

$$\forall u, v \in V, \forall \alpha \in K, \alpha \cdot u + U = \alpha \cdot v + U \iff u + U = v + U,$$

pertanto vale la proprietà $(\star)$, e $\mathfrak{R}_U$ è una congruenza in V.

Reciprocamente, se $\mathfrak{R}$ è una congruenza in V, in particolare $U = [0]_{\mathfrak{R}}$ è sottogruppo di $(V,+)$ tale che $\mathfrak{R} = \mathfrak{R}_U$ (vedi Teorema 6.3.4). Per concludere basta provare che U è un sottospazio di V. Siano $\alpha \in K$ e $u \in U$. Chiaramente

$$u \in U \iff u\mathfrak{R}_U 0 \iff u\mathfrak{R}0,$$

allora $\alpha \cdot u \,\mathfrak{R}_U\, \alpha \cdot 0 \iff \alpha \cdot u \in U$. Pertanto U è un sottospazio di V. □

In virtù di tale teorema, per ogni sottospazio U di V possiamo considerare lo spazio quoziente $V/U = \{ v + U : v \in V\}$.

7.2 DIPENDENZA LINEARE

Sia V uno spazio vettoriale su un campo K. Osserviamo che qualunque siano i vettori $v_1, v_2, \ldots, v_n \in V$ il vettore nullo si può esprimere come loro combinazione lineare mediante la *combinazione lineare nulla*, ossia ponendo gli scalari tutti uguali a zero: $0 = 0v_1 + \ldots + 0v_n$. Diremo che i vettori $v_1, v_2, \ldots, v_n$ *sono linearmente indipendenti* se il vettore nullo si esprime come loro combinazione lineare soltanto mediante la combinazione nulla. I vettori $v_1, v_2, \ldots, v_n$ li diremo *linearmente dipendenti* se non sono linearmente indipendenti. Se $v_1, v_2, \ldots, v_n$ sono linearmente indipendenti la parte $\{v_1, v_2, \ldots, v_n\}$ la diremo *libera*.

Esempio 7.2.1 I vettori $v_1, v_2, \ldots, v_n$ sono dipendenti se tra essi c'è quello nullo.

Esempio 7.2.2 Sia $(\mathbb{R}^2, +, \cdot)$ lo spazio vettoriale numerico $\mathbb{R}$, e siano i vettori $v_1 = (3,5)$ e $v_2 = (9,15)$. Allora v_1 e v_2 sono dipendenti. Infatti $0 = 3v_1 + (-1)v_2$

Esercizio 7.2.3 Provare che non esistono 3 vettori indipendenti in $\mathbb{R}^2$.

Esercizio 7.2.4 Sia $(\mathbb{R}^3, +, \cdot)$ lo spazio vettoriale numerico su $\mathbb{R}$, e siano i vettori $v_1 = (3,5,5)$, $v_2 = (9,15,4)$ e $v_3 = (1,-3,4)$. Per stabilire se v_1 e v_2 v_3 sono indipendenti bisogna risolvere un sistema lineare del tipo:

$$\Sigma = \begin{cases} 3\alpha_1 + 9\alpha_2 + \alpha_3 = 0 \\ 5\alpha_1 + 15\alpha_2 - 3\alpha_3 = 0 \\ 5\alpha_1 + 4\alpha_2 + 4\alpha_3 = 0 \end{cases},$$

di tre equazioni in tre incognite sul campo $\mathbb{R}$.

Esempio 7.2.5 I vettori $v_1, v_2, \ldots, v_n$ sono dipendenti se due di essi coincidono

Sia V uno spazio vettoriale su un campo K. Diremo che un vettore u *dipende linearmente da* $v_1, v_2, \ldots, v_n \in V$ se u si esprime come combinazione lineare di $v_1, v_2, \ldots, v_n$. Ciò equivale a dire che u appartiene allo spazio vettoriale generato da $v_1, v_2, \ldots, v_n$ (vedi esercizio 7.1.5).

Proposizione 7.2.6 *Se $v_1, v_2, \ldots, v_n$ sono linearmente dipendenti, allora uno di essi dipende dagli altri.*

Dimostrazione – Per ipotesi esistono $\alpha_1, \ldots, \alpha_n$ non tutti nulli tali che

$$\sum_{i=1}^{n} \alpha_i v_i = 0.$$

Supponiamo che $\alpha_j \neq 0$ per un certo indice j, allora abbiamo che il vettore v_j dipende dai rimanenti:

$$v_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} (-\alpha_i (\alpha_j)^{-1}) v_i.$$

□

Lemma 7.2.7 *Sia w un vettore che dipende da $v_1, v_2, \ldots, v_n, v$. Se v dipende da $v_1, v_2, \ldots, v_n$ allora anche w dipende da $v_1, v_2, \ldots, v_n$.*

Dimostrazione – Per ipotesi esistono degli scalari $\alpha_1, \ldots, \alpha_n, \alpha$ e $\beta_1, \ldots, \beta_n$ tali che

$$w = \sum_{i=1}^{n} \alpha_i v_i + \alpha v \text{ e } v = \sum_{i=1}^{n} \beta_i v_i. \quad \text{Allora} \qquad w = \sum_{i=1}^{n} (\alpha_i + \alpha\beta_i) v_i.$$

□

Esercizio 7.2.8 Sia $(V, +, \cdot)$ uno spazio vettoriale su un campo K, e siano v_1, v_2 e v_3 vettori distinti di V. Provare che se $v_1 - v_2 = \alpha(v_1 - v_3)$ per un opportuno scalare $\alpha \in K$, allora i vettori v_1, v_2 e v_3 sono dipendenti.

Proposizione 7.2.9 *Siano $v_1, v_2, \ldots, v_n$ vettori distinti. Essi sono indipendenti se e solo se nessuno di essi dipende dagli altri.*

Dimostrazione — Siano $v_1, v_2, \ldots, v_n$ vettori indipendenti, e per assurdo supponiamo che uno di essi dipendi dai rimanenti. Senza ledere le generalità supponiamo che v_1 dipenda da $v_2, \ldots, v_n$, allora per opportuni scalari $\alpha_2, \ldots \alpha_n$ abbiamo:

$$v_1 = \sum_{i=2}^{n} \alpha_i v_i, \text{e quindi} \quad 0 = -1v_1 + \sum_{i=2}^{n} \alpha_i v_i.$$

Questa è una contraddizione.

Per provare il viceversa ragioniamo per assurdo, e supponiamo che $v_1, v_2, \ldots, v_n$ siano vettori dipendenti. Allora per la proposizione 7.2.7 qualche vettore v_j dipende dai rimanenti, e ciò contraddice le ipotesi. □

Proposizione 7.2.10 *Siano $v_1, v_2, \ldots, v_n$ vettori indipendenti. Se $v \in V$ è un vettore che non dipende da $v_1, v_2, \ldots, v_n$, allora i vettori $v_1, v_2, \ldots, v_n, v$ sono indipendenti.*

Dimostrazione — Sia $\alpha, \alpha_1, \ldots \alpha_n$ scalari, e supponiamo che $\alpha v + \alpha_1 v_1 + \ldots + \alpha_n v_n = 0$. Se $\alpha \neq 0$, risulta

$$v = \sum_{i=1}^{n} -\alpha_i \alpha^{-1} v_i,$$

contro le ipotesi.

Assumiamo quindi che $\alpha = 0$. In tal caso abbiamo $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$, e per ipotesi ciascun α_i è nullo. □

Proposizione 7.2.11 *Siano $v_1, v_2, \ldots, v_n$ vettori indipendenti. Se $u = \alpha_2 v_2 + \ldots + \alpha_n v_n$ è una combinazione lineare di $v_2, \ldots, v_n$, allora i vettori $v_1 + u, v_2, \ldots, v_n$ sono indipendenti.*

Dimostrazione — Sia $0 = \beta_1(v_1 + u) + \beta_2 v_2 + \ldots + \beta_n v_n$. Allora $0 = \beta_1 v_1 + \beta_1(\alpha_2 v_2 + \ldots + \alpha_n v_n) + \beta_2 v_2 + \ldots + \beta_n v_n = \beta_1 v_1 + (\beta_1 \alpha_2 + \beta_2) v_2 + \ldots + (\beta_1 \alpha_n + \beta_n) v_n$. Per ipotesi $\beta_1 = 0, (\beta_1 \alpha_2 + \beta_2) = 0, \ldots (\beta_1 \alpha_n + \beta_n) = 0$, e quindi anche $\beta_2, \ldots \beta_n = 0$. □

Dalla proposizione precedente segue un risultato analogo per la dipendenza lineare.

Corollario 7.2.12 *Siano $v_1, v_2, \ldots, v_n$ vettori linearmente dipendenti. Se $u = \alpha_2 v_2 + \ldots + \alpha_n v_n$ è una combinazione lineare di $v_2, \ldots, v_n$, allora i vettori $v_1 + u, v_2, \ldots, v_n$ sono dipendenti.*

Sia X una parte di un K-spazio vettoriale. Se per ogni n-pla di vettori distinti $v_1, v_2, \ldots, v_n$ questi risultano indipendenti, allora la parte X si dice *libera*.

Una parte libera massimale, ovvero non contenuta propriamente in nessuna parte libera, si dice *base*.

Osservazione 7.2.13 Sia V uno spazio vettoriale. La proposizione 7.2.10, fornisce un metodo per individuare una base. Infatti a partire da una parte libera X di vettori indipendenti, se questa non è massimale, allora il sottospazio $\langle X \rangle$ è contenuto propriamente in V, sicché ad X possiamo aggiungere un ulteriore vettore v, in modo tale che $X \cup \{v\}$ ancora una parte indipendente.

In generale sussiste il seguente teorema.

Teorema 7.2.14 *Ogni* K*-spazio vettoriale possiede una base, e le basi sono tra loro equipotenti.*

Esercizio 7.2.15 Se $X = \{v_1, v_2, \ldots, v_n\}$ è una K-base, allora per ogni sottoinsieme Y di X si ha: $\langle X \rangle = \langle Y \rangle \oplus \langle X \setminus Y \rangle$.

Per il teorema precedente ha senso la seguente definizione. Sia V uno spazio vettoriale su un campo K. Diremo *dimensione* di V la cardinalità di una qualunque base di V. La dimensione di V la denoteremo col simbolo $\dim_K(V)$.

Chiaramente per individuare una base di uno spazio di dimensione finita n, basta prendere un qualunque vettore non nullo e applicare il Lemma 7.2.10 altre $n-1$ volte.

Esempio 7.2.16 La parte $X = \{(1,0,0), (0,1,0), (0,0,1)\}$ è un sistema di generatori minimale dello spazio vettoriale numerico $\mathbb{R}^3$, ed è anche una parte libera massimale, quindi è una base. Pertanto la dimensione di $\mathbb{R}^3$ è $3 = |X| = \dim_{\mathbb{R}} \mathbb{R}^3$.

Esempio 7.2.17 Sia $\mathbb{Q}[x]$ lo spazio vettoriale dei polinomi a coefficienti razionali. La parte $X = \{x^n : n \in \mathbb{N}_0\}$ è un una parte libera massimale, quindi è una base. Pertanto la dimensione di $\mathbb{Q}[x]$ è $|X| = \dim_{\mathbb{Q}} \mathbb{Q}[x] = |\mathbb{N}|$ (infinità numerabile).

Esercizio 7.2.18 La parte $X = \{(4,1,0), (0,1,1), (0,0,1)\}$ dello spazio vettoriale numerico $\mathbb{R}^3$, è una base?

Una base ordinata di un K-spazio vettoriale la diremo *riferimento*. Un riferimento si presenta quindi come una n-pla. Se K^n è lo spazio vettoriale numerico su K, La base ordinata

$$((1,0,\dots,0),(0,1,\dots,0),\dots(0,0,\dots,1))$$

si chiama *riferimento naturale* dello spazio K^n. Notiamo che K^n ha dimensione n.

Teorema 7.2.19 (DI CARATTERIZZAZIONE DELLE BASI) *Sia V un K-spazio vettoriale, e sia $X = \{v_1,\dots,v_n\}$ una parte finita costituita da n vettori. Sono equivalenti le seguenti condizioni:*

(a) *X è una base;*

(b) *X è una parte libera che genera V;*

(c) *X è un sistema di generatori minimale;*

(d) *Ogni vettore di V si esprime in un unico modo come combinazione lineare di vettori di X.*

DIMOSTRAZIONE — (a)⇒ (b) Per assurdo sia v un vettore di $V \setminus \langle X\rangle$. Per la proposizione 7.2.10 i vettori $v_1,\dots,v_n,v$ sono indipendenti, e questo contraddice la massimalità di X.

(b)⇒ (c) Per assurdo sia $Y \subset X$ un sistema di generatori di V, e sia $v_i \in X \setminus Y$. Allora v_i dipende da Y, e questo è assurdo per la proposizione 7.2.9

(c)⇒ (d) Sia

$$v = \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \beta_i v_i \Rightarrow 0 = \sum_{i=1}^{n} (\alpha_i - \beta_i) v_i.$$

Se fosse $\alpha_1 - \beta_1 \neq 0$, per la proposizione 7.2.9 il vettore v_1 dipenderebbe dai rimanenti, e per la proposizione 7.2.7 i vettori $v_2,\dots,v_n$ genererebbero V, contro l'ipotesi (c). Allora $\alpha_1 - \beta_1 = 0$ e quindi $\alpha_1 = \beta_1$. Analogamente per ogni $i = 1,\dots,n$ si prova che $\alpha_i = \beta_i$.

(d)⇒ (a) Sia $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$. Poiché $0v_1 + \dots + 0v_n = 0$, l'ipotesi (d) assicura che ciascun α_i è nullo, quindi $v_1,\dots,v_n$ sono indipendenti. Per l'ipotesi (d) ogni vettore dipende da $v_1,\dots,v_n$, quindi ogni parte contenente propriamente X non è libera. Pertanto X è una parte libera massimale. □

7.3 OMOMORFISMI TRA SPAZI VETTORIALI

Ricordiamo che assegnati V e W, spazi vettoriali su un campo K, un'applicazione $f: V \to W$ si dice omomorfismo, se per ogni scalare α, e ogni $u, v \in V$ risulta

$$f(u+v) = f(u) + f(v), \quad \text{e} \quad f(\alpha v) = \alpha f(v).$$

Un omomorfismo tra spazi vettoriali viene anche detto *applicazione lineare*.

Esempio 7.3.1 L'applicazione idendica $id_V : v \in V \to v \in V$ è un omomorfismo.

Esempio 7.3.2 L'applicazione nulla $0 : v \in V \to 0_V \in V$ è un omomorfismo (*omomorfismo nullo*).

Esempio 7.3.3 L'applicazione $f : (a, b) \in \mathbb{R}^2 \to (a, a+b, a+b) \in \mathbb{R}^3$ è un omomorfismo.

Esempio 7.3.4 L'applicazione $f : (a, b, c) \in \mathbb{R}^3 \to (a, b+1) \in \mathbb{R}^2$ non è un omomorfismo.

Proposizione 7.3.5 *Siano V e W spazi vettoriali su un campo K, e sia $f: V \to W$ un omomorfismo. Se $v_1, v_2, \ldots, v_n$ sono dipendenti, allora $f(v_1), f(v_2), \ldots, f(v_n)$ sono dipendenti.*

DIMOSTRAZIONE – Per ipotesi esistono $\alpha_1, \ldots, \alpha_n$ non tutti nulli tali che $0 = \alpha_1 v_1 + \ldots + \alpha_n v_n$. Allora $0 = f(0) = \alpha_1 f(v_1) + \ldots + \alpha_n f(v_n)$, e $f(v_1), f(v_2), \ldots, f(v_n)$ sono dipendenti. □

Osserviamo che un insieme di vettori indipendenti può essere trasformato mediante un omomorfismo in un insieme di vettori dipendenti, come ad esempio capita per l'omomorfismo nullo.

Esercizio 7.3.6 Verificare che l'applicazione $f : (a, b, c, d) \in \mathbb{R}^4 \to (a+c, b+c, 3a-2c+d) \in \mathbb{R}^3$ è un omomorfismo. Trovare due vettori indipendenti, le cui immagini sono dipendenti.

Ricordiamo che due spazi vettoriali V e W su un campo campo K si dicono isomorfi se esiste un isomorfismo $f: V \to W$ biettivo. In tal caso si verifica facilmente che anche l'applicazione inversa $f^{-1}: W \to V$ è un isomorfismo.

Proposizione 7.3.7 *Siano V e W spazi vettoriali su un campo K, e sia $f : V \to W$ un isomorfismo. Se $v_1, v_2, \dots, v_n$ sono indipendenti, allora $f(v_1), f(v_2), \dots, f(v_n)$ sono indipendenti.*

Dimostrazione — Per ipotesi f è un isomorfismo, quindi anche f^{-1} lo è. Per assurdo siano $f(v_1), f(v_2), \dots, f(v_n)$ dipendenti, allora per la Proposizione 7.3.5 anche $f^{-1}(f(v_1)) = v_1, f^{-1}(f(v_2)) = v_2, \dots, f^{-1}(f(v_n)) = v_n$ sono dipendenti e ciò contraddice le ipotesi. □

Osservazione 7.3.8 Sia V un K spazio vettoriale di dimensione n, e sia $\mathcal{B} = (v_1, \dots, v_n)$ una base ordinata di V. Allora ogni vettore di $v \in V$ si eprime in un unico modo come combinazione lineare dei vettori di X: $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$. Si verifica immediatamente che l'applicazione

$$\gamma_{\mathcal{B}} : v = \alpha_1 v_1 + \cdots + \alpha_n v_n \in V \to (\alpha_1, \dots, \alpha_n) \in K^n$$

è un isomorfismo, (detto *isomorfismo coordinato associato alla base ordinata $\mathcal{B}$).*

Osservazione 7.3.9 Siano V e W spazi vettoriali su un campo K, e sia $\mathcal{B} = (v_1, \dots, v_n)$ una base ordinata di V. Allora scelta una n-pla di vettori $(w_1, \dots, w_n)$ in W, è possibile definire un omomorfismo di dominio V e codominio W, tale che l'immagine di ciascun v_i sia w_i, per ogni $i \in I_n$. Per individuare tale omomorfismo, basta considerare l'applicazione

$$f : v = \alpha_1 v_1 + \cdots + \alpha_n v_n \in V \to f(v) = \alpha_1 w_1 + \cdots + \alpha_n w_n \in W.$$

Si verifica facilmente che tale applicazione è un omomorfismo (detto *ottenuto estendendo per linearità i valori assegnati alla base ordinata $\mathcal{B}$).*

Lemma 7.3.10 *Siano V e W spazi vettoriali su un campo K, di dimensione finita. Allora V e W sono isomorfi se e solo se hanno la stessa dimensione. In tal caso sono isomorfi allo spazio vettoriale numerico K^n.*

Dimostrazione — Chiaramente K^n ha dimensione n. Sia ora U uno spazio isomorfo a K^n, e sia $f : K^n \to U$ un isomorfismo. Posto $\mathcal{N} = (e_1, \dots, e_n)$ il riferimento naturale di K^n, dalla Proposizione 7.3.7 segue che i vettori $f(e_1), \dots, f(e_n)$ sono indipendenti. Sia ora $u \in U$. Il vettore $f^{-1}(u)$ giace in K^n, quindi si esprime come combinazione lineare del tipo $f^{-1}(u) = \alpha_1 e_1 + \dots + \alpha_n e_n$. Allora $u = f(\alpha_1 e_1 + \dots + \alpha_n e_n) = \alpha_1 f(e_1) + \dots + \alpha_n f(e_n)$. Pertanto i vettori $f(e_1), \dots, f(e_n)$ costituiscono una base di U, e U ha dimensione n.

Viceversa, abbiamo osservato precedentemente (Osservazione 7.3.8) che ogni K-spazio vettoriale di dimensione n è isomorfo allo spazio vettoriale numerico K^n. □

7.4 TEOREMI DI OMOMORFISMO TRA SPAZI VETTORIALI

Siano V e W spazi vettoriali su un campo K, e sia $f : V \to W$ un omomorfismo. Diremo *nucleo* di f l'insieme dei vettori

$$\mathrm{Ker}(f) = \{v \in V : f(v) = 0\}.$$

Diremo *immagine* di f l'insieme dei vettori

$$\mathrm{Imm}(f) = f(V).$$

Si verifica facilmente che sia $\mathrm{Ker}(f)$ che $\mathrm{Imm}(f)$ sono sottospazi rispettivamente di V e di W. Sia V uno spazio vettoriale su un campo K, e sia U un suo sottospazio. L'applicazione $\pi : v \in V \to v + U \in V/U$ è un omomorfismo suriettivo tra spazi vettoriali, che si chiama *epimorfismo canonico*.

Esercizio 7.4.1 *Siano V e W spazi vettoriali su un campo K, e sia $f : V \to W$ un omomorfismo. Provare le seguenti equivalenze:*

(a) *f è suriettiva se e solo se $\mathrm{Im}(f) = W$;*

(b) *f è iniettiva se e solo se $\mathrm{Ker}(f) = \{0\}$.*

I teoremi di omomorfismo tra gruppi si estendono agli spazi vettoriali. Di seguito riportiamo i tre enunciati:

Teorema 7.4.2 (PRIMO TEOREMA DI OMOMORFISMO PER GLI SPAZI VETTORIALI) *Siano V e W spazi vettoriali su un campo K, e sia $f : V \to W$ un omomorfismo. Allora esiste un unico omomorfismo $\varphi : V/\ker(f) \to W$ tale che $\varphi \circ \pi = f$, dove $\pi : V \to V/\ker(f)$ è l'epimorfismo canonico. Inoltre è un monomorfismo, e gli spazi vettoriali $V/\ker(f)$ e $f(V) = \mathrm{Imm}(f)$ sono isomorfi.*

Il primo teorema di omomorfismo per gli spazi vettoriali può essere schematizzato col seguente diagramma:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow \pi & \varphi \nearrow & \\ V/\ker(f) & & \end{array} .$$

Teorema 7.4.3 (Secondo Teorema di Omomorfismo per gli spazi vettoriali) *Sia* V *un* K*-spazio vettoriale, e siano* N *e* H *sottospazi di* V*. Allora gli spazi quozienti* $\langle N, H\rangle/N$ *e* $H/(N \cap H)$ *sono isomorfi.*

Teorema 7.4.4 (Terzo Teorema di Omomorfismo per gli spazi vettoriali) *Sia* V *un* K*-spazio vettoriale, e siano* N *e* H *sottospazi di* V*, con* H *sottospazio di* N*. Allora il il quoziente* $\frac{V/H}{N/H}$ *è isomorfo a* V/N*.*

Teorema 7.4.5 (Dimensione del quoziente) *Siano* V *uno spazio vettoriale su un campo* K*, di dimensione finita, e sia* W *un suo sottospazio. Allora* $\dim(V/W) = \dim(V) - \dim(W)$*.*

Dimostrazione — Sia U un sottospazio di V tale che $V = W \oplus U$. Allora $\dim(V) = \dim(W) + \dim(U)$, e ogni vettore di V si esprime in un unico modo come somma di un vettore di W e un vettore di U. Consideriamo la seguente applicazione:

$$f : v = w + u \in V = W \oplus U \to u \in U.$$

Chiaramente f è un omomorfismo, inoltre $\ker(f) = W$ e $U = \mathrm{Imm}(f)$. Per il primo teorema di omomorfismo abbiamo che $V/\ker(f)$ e $\mathrm{Imm}(f)$ sono isomorfi, e quindi hanno la stessa dimensione. Pertanto $\dim(V/W) = \dim(U) = \dim(V) - \dim(W)$. □

Teorema 7.4.6 *Siano* V *e* W *spazi vettoriali su un campo* K*, di dimensione finita, e sia* $f : V \to W$ *un omomorfismo. Allora* $\dim(V) = \dim(\ker(f)) + \dim(\mathrm{Imm}(f))$*.*

Dimostrazione — Per il primo teorema di omomorfismo abbiamo che $V/\ker(f)$ e $\mathrm{Imm}(f)$ sono isomorfi, sicché hanno la stessa dimensione. Quindi $\dim(\mathrm{Imm}(f)) = \dim(V/\ker(f))$, e per il teorema della dimensione del quoziente risulta $\dim(V/\ker(f)) = \dim(V) - \dim(\ker(f))$. Da ciò segue la tesi. □

Teorema 7.4.7 (Formula di Grassmann) *Sia* V *uno spazio vettoriale su un campo* K*, e siano* U *e* W *sottospazi vettoriali di* V *di dimensione finita. Allora* $\dim(U + W) - \dim(U \cap W) = \dim(U) + \dim(W)$*.*

Dimostrazione — Per il secondo teorema di omomorfismo si ha che gli spazi $(U + W)/U$ e $W/(W \cap U)$ sono isomorfi. Applicando il Teorema 7.4.6 si ha la tesi. □

Esercizio 7.4.8 Siano V e W spazi vettoriali su un campo K. Sia $\mathrm{Hom}(V,W)$ l'insieme costituito da tutti gli omomorfismi di V in W. Siano definite in $\mathrm{Hom}(V,W)$ le seguenti operazioni ponendo:

$\forall f, g \in \mathrm{Hom}(V,W)$, $\quad f+g : v \in V \to f(v)+g(v) \in W$, e

$\forall f \in \mathrm{Hom}(V,W)$ e $\alpha \in K$, $\quad \alpha \cdot f : v \in V \to \alpha f(v) \in W$.

Verificare che $((\mathrm{Hom}(V,W),+,\cdot)$ è un K-spazio vettoriale.

CAPITOLO 8

MATRICI E SISTEMI LINEARI

8.1 MATRICI SU UN ANELLO: DEFINIZIONI, NOTAZIONI E PROPRIETÁ

Sia K un anello, e sia I_m l'insieme dei primi m numeri positivi e I_n l'insieme dei primi n numeri positivi. Si dice *matrice con* m *righe ed* n *colonne* una qualunque applicazione A che ad ogni coppia di indici $(i,j) \in I_m \times I_n$ associa un elemento $a_{ij} = A(i,j)$ dell'anello K:

$$\begin{aligned} A : I_m \times I_n &\to K. \\ (i,j) &\to A(i,j) \end{aligned}$$

Una matrice A si denota anche col simbolo

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Talvolta una generica matrice A puó essere denotata anche col simbolo (a_{ij}). L'insieme delle matrici con m righe ed n colonne su un anello K si denota col simbolo $\mathfrak{M}_{mn}(K)$. Osserviamo che in alcuni casi può convenire separare il doppio indice a pedice (o all'apice) di un simbolo generico. Ad esempio se $i = 10$ e $j = 23$ conviene scrivere "$a_{10,23}$" , essendo la scrittura "a_{1023}" alquanto ambigua.

Siano $A \in \mathfrak{M}_{mn}(K)$, $I = \{i_1, i_2, \ldots, i_r\} \subseteq I_m$ e $J = \{j_1, j_2, \ldots, j_s\} \subseteq I_n$. L' applicazione ristretta $A/_{I\times J} : I \times J \to K$, si dice sottomatrice di A di righe $i_1, i_2, \ldots, i_r$ e di colonne $j_1, j_2, \ldots, j_s$. Essa verrà denotata col simbolo $A^{\{j_1,j_2,\ldots,j_s\}}_{\{i_1,i_2,\ldots,i_r\}}$, o più semplicemente con $A^{j_1,j_2,\ldots,j_s}_{i_1,i_2,\ldots,i_r}$.

Particolari sottomatrici di una matrice A sono le righe e le colonne. Sia $i \in I_m$. La riga i-esima di A è la sottomarice $A^{I_n}_{\{i\}} : \{i\} \times I_n \to K$, essa si denota semplicemente col simbolo A_i. Analogamente se $j \in I_n$, la colonna j-esima di A è la sottomarice $A^{\{j\}}_{I_m} : I_m \times \{j\} \to K$, che si denota semplicemente col simbolo A^j.

Esempio 8.1.1

$$A = \begin{pmatrix} 4 & \frac{1}{4} & 3 & 2 & \frac{1}{5} & \frac{1}{4} & \frac{-1}{2} \\ 3 & -2 & 4 & 8 & 2 & 3 & 5 \\ 0 & -2 & 4 & \frac{1}{5} & 2 & 7 & 5 \\ 1 & -6 & 4 & 7 & 2 & \frac{7}{4} & \frac{-1}{2} \\ -2 & -7 & 4 & \frac{1}{5} & 2 & 3 & 5 \end{pmatrix} \in \mathfrak{M}_{57}(\mathbb{Q}).$$

La sottomatrice di A di righe $1,4$ e di colonne $2,5,7$ è la matrice $A^{\{2,5,7\}}_{\{1,4\}} = \begin{pmatrix} \frac{1}{4} & \frac{1}{5} & \frac{-1}{2} \\ -6 & 2 & \frac{-1}{2} \end{pmatrix} \in \mathfrak{M}_{23}(\mathbb{Q})$.

La quarta colonna è $A^4 = \begin{pmatrix} 2 \\ 8 \\ \frac{1}{5} \\ 7 \\ \frac{1}{5} \end{pmatrix} \in \mathfrak{M}_{51}(\mathbb{Q})$, mentre ad esempio la seconda riga è la matrice $A_2 = \begin{pmatrix} 3 & -2 & 4 & 8 & 2 & 3 & 5 \end{pmatrix} \in \mathfrak{M}_{17}(\mathbb{Q})$.

Siano m ed n interi positivi, e sia K un anello. Nell'insieme $\mathfrak{M}_{mn}(K)$ è possibile definire un'operazione interna ed una esterna con dominio di operatori K. Utilizzando la somma interna dell' anello K possiamo definire la somma tra due matrici dello stesso tipo sommando semplicemente gli elementi che occupano la stessa posizione:

$$+ : \mathfrak{M}_{mn}(K) \times \mathfrak{M}_{mn}(K) \to \mathfrak{M}_{mn}(K)$$
$$(A=(a_{ij}),B=(b_{ij})) \to A+B=(a_{ij})+(b_{ij}) := (a_{ij}+b_{ij})$$

Esempio 8.1.2 Siano $A = \begin{pmatrix} \frac{1}{4} & \frac{-1}{2} & 3 \\ 2 & 3 & 5 \end{pmatrix}$ e $B = \begin{pmatrix} \frac{1}{4} & \frac{1}{2} & 6 \\ 2 & 0 & 5 \end{pmatrix} \in \mathfrak{M}_{23}(\mathbb{Q})$. Allora $A + B = \begin{pmatrix} \frac{1}{2} & 0 & 9 \\ 4 & 3 & 10 \end{pmatrix} \in \mathfrak{M}_{23}(\mathbb{Q})$.

Utilizzando il prodotto interno dell' anello K possiamo definire il prodotto tra un elemento di K ed una matrice su K, moltiplicando lo scalare α per ciascun elemento della matrice (a_{ij}). Talvolta il prodotto esterno verrà anche denotato col simbolo $\cdot_{est}$ (per distinguerlo dal prodotto interno $\cdot_{int}$ dell'anello K).

$$\begin{gathered} \cdot : K \times \mathfrak{M}_{mn}(K) \to \mathfrak{M}_{mn}(K) \\ (\alpha, A=(a_{ij})) \to \alpha \cdot A = \alpha \cdot (a_{ij}) := (\alpha \cdot a_{ij}) \end{gathered}$$

Esempio 8.1.3 Sia $A = \begin{pmatrix} \frac{1}{5} & \frac{-1}{3} & 3 \\ 1 & 0 & 5 \end{pmatrix} \in \mathfrak{M}_{23}(\mathbb{Q})$,

Allora $3 \cdot A = \begin{pmatrix} \frac{3}{5} & -1 & 9 \\ 3 & 0 & 15 \end{pmatrix} \in \mathfrak{M}_{23}(\mathbb{Q})$.

Esercizio 8.1.4 Sia K un campo, provare che $(\mathfrak{M}_{mn}(K); +, \cdot_{est})$ è uno spazio vettoriale su K.

Bisogna verificare per ogni A e $B \in \mathfrak{M}_{mn}(K)$ e per ogni α e $\beta \in K$ che:

1. $(\mathfrak{M}_{mn}(K); +)$ è un gruppo abeliano;
2. $\alpha \cdot (A + B) = \alpha \cdot A + \alpha \cdot B$;
3. $(\alpha + \beta) \cdot A = \alpha \cdot A + \beta \cdot A$;
4. $(\alpha \cdot_{int} \beta) \cdot_{est} A = \alpha \cdot_{est} (\beta \cdot_{est} A)$;
5. $1_K \cdot A = A$. (dove 1_K è l'unitá del campo K).

Siano $A = (a_{ij}) \in \mathfrak{M}_{mh}(K)$ e $B = (b_{ij}) \in \mathfrak{M}_{hn}(K)$. Osserviamo che la lunghezza di una riga di A coincide colla lunghezza di ciascuna colonna di B. In tal caso tra le due matrici si può eseguire il prodotto righe per colonne. Si pone:

$$A \cdot B = C = (c_{ij}), \text{dove } c_{ij} = \sum_{r=1}^{h} a_{ir} \cdot b_{rj} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + \ldots + a_{ih} \cdot b_{hj}.$$

Si osservi che $C \in \mathfrak{M}_{mn}(K)$, ed è quindi in generale di tipo diverso sia da A che da B, per cui il prodotto righe per colonne tra due matrici non sempre si può riguardare come operazione interna.

Esempio 8.1.5 Sia $A = \begin{pmatrix} 2 & 0 & 3 \\ 1 & 0 & 5 \end{pmatrix} \in \mathfrak{M}_{23}(\mathbb{Z}_7)$, e $B = \begin{pmatrix} 2 & 0 & 3 & 3 \\ 1 & 0 & 0 & 5 \\ -1 & 0 & 0 & 1 \end{pmatrix} \in$ $\mathfrak{M}_{34}(\mathbb{Z}_7)$. Risulta

$$A \cdot B = C = \begin{pmatrix} 1 & 0 & 6 & 2 \\ 4 & 0 & 3 & 1 \end{pmatrix} \in \mathfrak{M}_{24}(\mathbb{Z}_7).$$

Si osservi anche che se si puó eseguire il prodotto A per B non è detto che si possa eseguire il prodotto B per A. Se si considera peró l'insieme delle matrici $\mathfrak{M}_{mm}(K)$ (anche dette *quadrate di ordine m*), rimane definita una seconda operazione interna:

$$\begin{gathered} \cdot : \mathfrak{M}_{mm}(K) \times \mathfrak{M}_{mm}(K) \to \mathfrak{M}_{mm}(K) \\ (A, B) \to A \cdot B. \end{gathered}$$

La struttura $(\mathfrak{M}_{mm}(K), \cdot)$ è un monoide il cui elemento neutro è la matrice identica $\mathfrak{I}_m = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$.

Esercizio 8.1.6 provare con un esempio che in generale la struttura $(\mathfrak{M}_{mm}(K); \cdot)$ non è commutativa.

Proposizione 8.1.7 *Sia* $A \in \mathfrak{M}_{nn}(K)$. *Condizione sufficiente affinché le colonne* $A^1, \dots A^n$ *siano vettori indipendenti dello spazio* $\mathfrak{M}_{n1}(K)$ *è che* A *sia invertibile.*

Dimostrazione– Esprimiamo il vettore nullo come combinazione lineare dei vettori colonna: $c_1A^1 + \dots + c_nA^n = 0$. Posto $C = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$, risulta $AC = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Per ipotesi A invertibile quindi moltiplicando a sinistra per A^{-1} otteniamo $C = A^{-1}\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Da ciò segue che gli scalari $c_1, \dots, c_n$ sono tutti nulli. □

8.2 MATRICI EQUIVALENTI E MATRICI A SCALA

In questo paragrafo introdurremo l'algoritmo di riduzione a scala di una matrice, che permetterà di approfondire lo studio della dipendenza lineare delle righe e delle colonne di una matrice. Nel seguito, tutto ciò che sarà riferito alle righe di una matrice può essere riformulato per le colonne.

Sia $A \in \mathfrak{M}_{mn}(K)$. Un' *operazione elementare sulle righe di* A è una trasformazione di A ottenuta in uno dei seguenti modi:

(a) moltiplicando una riga A_i per uno scalare non nullo λ;

(b) scambiando di posto due righe A_i e A_j;

(c) sostituendo la riga A_i con $A_i + \lambda A_j$, dove $\lambda \in K; i \neq j$.

Osserviamo che iterando l'operazione elementare (c) si ottiene un' operazione del tipo $A_i \to A_i + \lambda_1 A_{j_1} + \ldots + \lambda_h A_{j_h}$. Questa operazione ha modificato la riga i-esima, aggiungendo ad essa una combinazione lineare di altre righe.

Proposizione 8.2.1 *Sia A una matrice le cui righe sono indipendenti. Allora anche le righe della matrice ottenuta da A mediante un' operazione elementare su una sua riga sono indipendenti.*

DIMOSTRAZIONE— L'asserto segue banalmente dalla Proposizione 7.2.11. □

Siano $A, B \in \mathfrak{M}_{mn}(K)$. Diremo che A e B sono *equivalenti* (e scriveremo $A \equiv B$) se B si ottiene da A mediante un numero finito di operazioni elementari. Si verifica facilmente che tale relazione è di equivalenza.

Esempio 8.2.2 Sia $A = \begin{pmatrix} 3 & -4 & 1 \\ 1 & -3 & 3 \end{pmatrix}$, e $B = \begin{pmatrix} 3 & -4 & 1 \\ 7 & -11 & 5 \end{pmatrix}$, $\in \mathfrak{M}_{23}(\mathbb{Z})$. Risulta $A \equiv B$

Esercizio 8.2.3 Sia $A = \begin{pmatrix} 3 & -4 & 1 \\ 1 & -3 & 3 \end{pmatrix} \in \mathfrak{M}_{23}(\mathbb{Z})$. Trovare una matrice che non è equivalente ad A.

Matrici del tipo

$$\begin{pmatrix} 3 & -4 & 1 & 1 \\ 0 & -3 & 3 & 2 \\ 0 & 0 & 8 & -1 \end{pmatrix} \in \mathfrak{M}_{34}(\mathbb{Z}) \text{ oppure } \begin{pmatrix} 3 & -4 & 1 & 1 \\ 0 & -2 & 6 & 2 \\ 0 & 0 & 7 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathfrak{M}_{64}(\mathbb{Z}),$$

si dicono a "scala". La caratteristica di queste matrici è che se una sua riga non è nulla, allora la riga successiva ha uno zero in più a sinistra. Formalmente, una matrice A si dice a *scala (secondo le righe)* se sono verificate le seguenti condizioni:

(a) se $A_i = 0$ allora $A_{i+1} = 0$;

(b) per ogni i, se $a_{i,j} \neq 0$ e $a_{i,h} = 0\ \forall h < j$, allora $a_{i+1,h} = 0\ \forall h \leqslant j$.

In ogni riga non banale il primo elemento non nullo prende il nome di *pivot*. Ad esempio il pivot della terza riga della seconda matrice dell'esempio precedente è il numero 7.

Sussiste il seguente teorema, la cui dimostrazione si basa su un metodo chiamato *algoritmo di Gauss per la riduzione a scala di una matrice*:

Teorema 8.2.4 *Ogni matrice è equivalente ad una a scala.*

Illustriamo con un esempio come si riduce a scala una matrice.

Esempio 8.2.5 Sia

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 0 & 1 & 0 \\ -1 & 0 & -1 & 3 \\ 1 & 0 & 1 & 3 \end{pmatrix} \in \mathfrak{M}_{44}(\mathbb{Z}).$$

Allora

$$A \underset{A_2 \to \frac{1}{3}A_2}{\equiv} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 0 & \frac{1}{3} & 0 \\ -1 & 0 & -1 & 3 \\ 1 & 0 & 1 & 3 \end{pmatrix} \underset{\substack{A_2 \to (A_1 - A_2) \\ A_3 \to (A_3 + A_1) \\ A_4 \to (A_1 - A_4)}}{\equiv} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & \frac{8}{3} & 4 \\ 0 & 2 & 2 & 7 \\ 0 & 2 & 2 & 1 \end{pmatrix}$$

$$\begin{array}{c} \equiv \\ \begin{array}{lcl} A_3 & \to & (A_2 - A_3) \\ A_4 & \to & (A_2 - A_4) \end{array} \end{array} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & \frac{8}{3} & 4 \\ 0 & 0 & \frac{2}{3} & -3 \\ 0 & 0 & \frac{2}{3} & 3 \end{pmatrix} \begin{array}{c} \equiv \\ A_4 \to (A_4 - A_3) \end{array} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & \frac{8}{3} & 4 \\ 0 & 0 & \frac{2}{3} & -3 \\ 0 & 0 & 0 & 6 \end{pmatrix}.$$

Appare chiaro che applicando l'algoritmo di Gauss ad una matrice si può pervenire a più matrici a scala.

Teorema 8.2.6 *Sia A una matrice quadrata. Allora le righe (risp. colonne) di A sono indipendenti, se e solo se una sua equivalente ridotta a scala possiede ancora righe (risp. colonne) indipendenti.*

Dimostrazione— Se la righe di A sono indipendenti, per la Proposizione 8.2.1 ogni matrice equivalente ad A ha le righe indipendenti, in particolare ogni sua ridotta a scala. Viceversa se una ridotta a scala di A ha le righe indipendenti, per la Proposizione 8.2.1 anche A ha le righe indipendenti. □

8.3 DETERMINANTE DI UNA MATRICE QUADRATA

In questo paragrafo considereremo matrici quadrate su di un anello unitario K.

Chiaramente particolari matrici quadrate sono quelle di ordine 1, ovvero quelle individuate da un singolo elemento di K. Tali matrici si presentano nella forma $(k) \in \mathfrak{M}_{11}(K)$. In tal caso l'elemento k si dirà anche *determinante* della matrice (k). Sia ora $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathfrak{M}_{22}(K)$, diremo *determinante* della matrice quadrata A lo scalare *det(A)*= $a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$.

Esempio 8.3.1 Sia $A = \begin{pmatrix} 3 & -4 \\ 1 & -3 \end{pmatrix} \in \mathfrak{M}_{22}(\mathbb{Z}_5)$. Risulta $\det(A) = 0$.

Esempio 8.3.2 Sia $A = \begin{pmatrix} 3 & -4 \\ 1 & -3 \end{pmatrix} \in \mathfrak{M}_{22}(\mathbb{Z}_7)$. Risulta $\det(A) = 2$.

Osserviamo che se denotiamo con g la permutazione non identica del gruppo simmetrico su due oggetti, e con $\sigma(g)$ la sua segnatura, risulta

$$\det\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathfrak{M}_{22}(K) = a_{1\,id(1)} \cdot a_{2\,id(2)} + (-1)^{\sigma(g)} a_{1\,g(1)} \cdot a_{2\,g(2)}\right.$$

Sia ora $m > 2$, e sia $A \in \mathfrak{M}_{mm}(K)$. Diremo determinante di A il seguente scalare:

$$\det(A) = \sum_{g \in S_m} (-1)^{\sigma(g)} a_{1g(1)} \dots a_{mg(m)}, \text{ dove } \begin{cases} \sigma(g) = 1 \text{ se } g \text{ è dispari} \\ \sigma(g) = 0 \text{ se } g \text{ è pari} \end{cases}.$$

Osserviamo che il determinante di una matrice quadrata di ordine n si esprime come somma di $n!$ addendi.

Esempio 8.3.3 Sia $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$. Allora $\det(A)$

$$= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

Da ciò segue la ben nota regola di Sarrius.

Assegnata una matrice $A = (a_{ij})$ diremo *trasposta* di A, e la denoteremo col simbolo A_t, la matrice ottenuta scambiando in A le righe con le colonne. Se $A = (a_{ij})$ avremo quindi $A_t = (a_{ji})$.

Esempio 8.3.4 Sia $A = \begin{pmatrix} 3 & -4 & -9 \\ 1 & -3 & 7 \\ 18 & 4 & 3 \end{pmatrix} \in \mathfrak{M}_{33}(\mathbb{R})$. Scambiando le righe con le colonne avremo $(A_t) = \begin{pmatrix} 3 & 1 & 18 \\ -4 & -3 & 4 \\ -9 & 7 & 3 \end{pmatrix}$.

Nell'esempio precedente si può verificare che i determinanti delle due matrici coincidono. Questo è un caso particolare del seguente teorema.

Teorema 8.3.5 (Determinante della trasposta) *Sia* $A \in \mathfrak{M}_{nn}(\mathbb{K})$. *Allora* $\det(A) = \det(A_t)$.

Dimostrazione – Sia $A = (a_{ij})$ e $A_t = (a'_{ij})$. Dalla definizione risulta

$$\det(A_t) = \sum_{g \in S_n} (-1)^{\sigma(g)} a'_{1g(1)} \dots a'_{ng(n)} = \sum_{g \in S_n} (-1)^{\sigma(g)} a_{g(1)1} \dots a_{g(n)n}.$$

Ovviamente una permutazione è pari se e solo se lo è la sua inversa, quindi $\sigma(g) = \sigma(g^{-1})$. Ora verifichiamo che per ciascun addendo si ha: $a_{g(1)1} \dots a_{g(n)n} = a_{1g^{-1}(1)} \dots a_{ng^{-1}(n)}$. A tal scopo poniamo:

$$\begin{array}{lcll} g(1) := i_1 & & 1 = g^{-1}(i_1) & & a_{g(1)1} = a_{i_1 g^{-1}(i_1)} \\ \vdots \quad , & \text{allora} & \vdots & \text{e quindi} & \vdots \quad . \\ g(n) := i_n & & n = g^{-1}(i_n) & & a_{g(n)n} = a_{i_n g^{-1}(i_n)} \end{array}$$

Moltiplicando termine a termine, e ordinando otteniamo $a_{g(1)1} \dots a_{g(n)n} = a_{1g^{-1}(1)} \dots a_{ng^{-1}(n)}$. D'altra parte

$$\sum_{g \in S_n} (-1)^{\sigma(g)} a_{1g(1)} \dots a_{ng(n)} = \sum_{g \in S_n} (-1)^{\sigma(g^{-1})} a_{1g^{-1}(1)} \dots a_{ng^{-1}(n)},$$

per cui $\det(A) = \det(A_t)$. □

Una matrice A con n colonne ed m righe può essere rappresentata anche col simbolo $\left(A^1 A^2 \dots A^n\right)$ oppure $\left(A^1, A^2, \dots A^n\right)$ in cui si evidenziano le colonne. Se si vogliono evidenziare le righe si usa il simbolo $\begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix}$.

Di seguito si riportano le principali proprietà del determinante di una matrice quadrata A.

Proposizione 8.3.6 (Proprietà dei determinanti)
Sia $A = \left(A^1 A^2 \dots A^n\right) \in \mathfrak{M}_{nn}(\mathbb{K})$.

1. $A^j = C + D$. *Allora* $\det\left(A^1 A^2 \dots A^j \dots A^n\right) = \det\left(A^1 A^2 \dots C \dots A^n\right)$ $+\det\left(A^1 A^2 \dots D \dots A^n\right)$;
2. $\det\left(A^1 A^2 \dots t \cdot A^j \dots A^n\right) = t \cdot \det\left(A^1 A^2 \dots A^j \dots A^n\right)$, *per ogni scalare* t *e indice* j;
3. *Se* A *possiede due colonne uguali allora* $\det(A) = 0$;
4. *Se si scambiano di posto due colonne, il determinante cambia di segno.*
   Analoghe proprietà valgono in relazione alle righe.

DIMOSTRAZIONE – Le proprietà 1, 2 si provano usando la definizione di determinante. La 3 discende dalla 1. Per provare la 4, senza ledere la generalità, proveremo che scambiando di posto le prime due colonne, il determinante cambia di segno. Osserviamo che $\det(A^1, A^2, \dots A^n) = \det(A^1 + A^2, A^2, \dots A^n) = -\det(A^1 + A^2, -A^2, \dots A^n) = -\det(A^1 + A^2, -A^2 + (A^1 + A^2), \dots A^n) = -\det(A^1 + A^2, A^1, \dots A^n) = \det(-A^1 - A^2, A^1, \dots A^n) = \det(-A^2, A^1, \dots A^n) = -\det(A^2, A^1, \dots A^n)$. □

Una matrice il cui determinante è nullo si dice *degenere*.

Teorema 8.3.7 *Due matrici equivalenti sono entrambe degeneri o non degeneri*

DIMOSTRAZIONE – Siano A e B matrici equivalenti. Se A è una matrice non degenere, per la 8.3.6, ogni operazione elementare sulle righe di A la trasforma in una matrice non degenere. Allora anche B è una matrice non degenere. □

Per il calcolo del determinante di una matrice si usa spesso la cosiddetta "regola di Laplace". Per mostrare tale metodo premettiamo una definizione. Assegnata una matrice $A \in \mathfrak{M}_{mm}(K)$ diremo *minore di posto (i,j)* e verrà denotato col simbolo A_{ij}, il determinante della sottomatrice di A ottenuta cancellando la riga i-esima e la colonna j-esima preso col proprio segno se $i+j$ è pari oppure col segno opposto se $i+j$ è dispari: $A_{ij} = (-1)^{i+j}\det(A^{I_m\setminus\{j\}}_{I_m\setminus\{i\}})$.

Teorema 8.3.8 (DI LAPLACE) *Sia A una matrice di ordine m. Per ogni coppia di indici* $(h,k) \in I_m \times I_m$ *il determinante di A coincide con una delle seguenti somme:*

$a_{h1} \cdot A_{h1} + a_{h2} \cdot A_{h2} + \cdots + a_{hm} \cdot A_{hm} = \sum_{r=1}^{m} a_{hr} \cdot A_{hr}$ (Tale somma viene anche detta *sviluppo secondo la riga h-esima*),

$a_{1k} \cdot A_{1k} + a_{2k} \cdot A_{2k} + \cdots + a_{mk} \cdot A_{mk} = \sum_{r=1}^{m} a_{rk} \cdot A_{rk}$ (Tale somma viene anche detta *sviluppo secondo la colonna k-esima*).

DIMOSTRAZIONE – Omessa.

Esempio 8.3.9 Sia $A = \begin{pmatrix} 1 & 3 & 4 \\ 7 & 0 & -2 \\ 4 & 1 & -1 \end{pmatrix} \in \mathfrak{M}_{33}(\mathbb{Z}_{11})$. Calcoliamo il determinante di A sviluppando secondo la seconda riga: $\det(A) = a_{21} \cdot A_{21} + a_{22} \cdot A_{22} + a_{23} \cdot A_{23} = -7 \cdot \det(\begin{pmatrix} 3 & 4 \\ 1 & -1 \end{pmatrix}) + 0 \cdot \det(\begin{pmatrix} 1 & 4 \\ 4 & -1 \end{pmatrix}) - (-2) \cdot \det(\begin{pmatrix} 1 & 3 \\ 4 & 1 \end{pmatrix}) = -7(-3-4) + 2(1-12) = 49 - 22 = 27 = 5$.

Chiaramente $\det(\mathfrak{I}_m) = 1$. Questo è un caso particolare di quanto contenuto nel seguente esercizo.

Esercizio 8.3.10 Usando la regola di Laplace, provare che il determinante di una matrice diagonale coincide col prodotto degli elementi che giacciono sulla diagonale principale.

Una matrice del tipo $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ & \ddots & \\ \mathbf{O} & & a_{nn} \end{pmatrix} \in \mathfrak{M}_{nn}(K)$, si dice *triangolare (superiore)*. Ad esempio $A = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 0 & 2 \\ 0 & 0 & 7 \end{pmatrix} \in \mathfrak{M}_{33}(K)$.

Esercizio 8.3.11 Usando la regola di Laplace, provare che il determinante di una matrice quadrata di tipo triangolare coincide col prodotto degli elementi che giacciono sulla diagonale principale.

Corollario 8.3.12 *Sia* $A = (a_{ij})$ *una matrice quadrata di ordine* m *su* K. *Siano* h *e* k *indici distinti di* I_m. *Allora:*

1. $a_{h1} \cdot A_{k1} + \cdots + a_{hm} \cdot A_{km} = 0$;
2. $a_{1h} \cdot A_{1k} + \cdots + a_{mh} \cdot A_{mk} = 0$.

Dimostrazione — Proveremo solo la 1). Sia $\tilde{A}$ la matrice ottenuta da A sostituendo la k-esima riga con la h-esima, quindi $\tilde{A} = \begin{pmatrix} A_1 \\ \vdots \\ A_h \\ \vdots \\ A_h \\ \vdots \\ A_m \end{pmatrix}$.

Poiché $\tilde{A}$ posssiede due righe uguali, il suo determinante è nullo. Osserviamo anche che A e $\tilde{A}$ differiscono solo per la k-esima riga. Sviluppando secondo la k-esima riga di $\tilde{A}$ si ha:

$0 = \tilde{a}_{k1} \cdot \tilde{A}_{k1} + \cdots + \tilde{a}_{km} \cdot \tilde{A}_{km} = a_{h1} \cdot A_{k1} + \cdots + a_{hm} \cdot A_{km}$.

Teorema 8.3.13 (Di Binet) *Siano* A *e* $B \in \mathfrak{M}_{mm}(K)$. *Allora* $\det(A \cdot B) = \det(A) \cdot \det(B)$.

Esercizio 8.3.14 Sia K un campo. Provare che l'applicazione $f : A \in \mathfrak{M}_{mm}(K) \to \det(A) \in (K; \cdot)$ è un omomorfismo. Stabilire se f è iniettiva o suriettiva.

Sia $A \in \mathfrak{M}_{mm}(K)$. Diremo che A è *invertibile* se esiste una matrice $B \in \mathfrak{M}_{mm}(K)$ tale che $A \cdot B = \mathfrak{I}_m = B \cdot A$

Assegnata una matrice quadrata, non sembra facile, almeno in prima istanza, stabilire se è invertibile, e soprattutto individuarne l'inversa. I seguenti risultati risolvono completamente questo tipo di problema.

Lemma 8.3.15 *Sia* $A \in \mathfrak{M}_{mm}(K)$. *Se* $\det(A) \neq 0$, *allora* A *è invertibile con inversa* $B = (b_{ij})$ *dove* $b_{ij} = A_{ji} \cdot \det(A)^{-1}$.

Dimostrazione — Sia $C = (c_{ij}) = A \cdot B$. Verifichiamo che $C = \mathfrak{I}_m$. Per ogni coppia di indici i e j risulta $c_{ij} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + \cdots + a_{im} \cdot b_{mj} = a_{i1} \cdot A_{j1} \cdot \det(A)^{-1} + a_{i2} \cdot A_{j2} \cdot \det(A)^{-1} + \cdots + a_{im} \cdot A_{jm} \cdot \det(A)^{-1}$
$= (a_{i1} \cdot A_{j1} \cdot + a_{i2} \cdot A_{j2} + \cdots + a_{im} \cdot A_{jm}) \cdot \det(A)^{-1}$. Se $i = j$, l'espressione tra parentesi è proprio il determinante di A, ed in tal caso $c_{ii} = 1$; se invece $i \neq j$ per il Corollario 8.3.12 tale espressione è nulla, ed in tal caso $c_{ij} = 0$. □

Esempio 8.3.16 Sia $A = \begin{pmatrix} 1 & 3 & 4 \\ 7 & 0 & -2 \\ 4 & 1 & -1 \end{pmatrix} \in \mathfrak{M}_{33}(Q)$. Abbiamo già visto che $\det(A) = 27$. Per individuare l'inversa di A puó essere utile il seguente schema:
$A^{-1} = \det(A)^{-1} \begin{pmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{pmatrix} = \frac{1}{27} \cdot \begin{pmatrix} 2 & 7 & -6 \\ -1 & -17 & 30 \\ 7 & 11 & -21 \end{pmatrix}$. Riguardando A come matrice sul campo $\mathbb{Z}_{11}$, risulterá
$A^{-1} = 9 \cdot \begin{pmatrix} 2 & 7 & -6 \\ -1 & -17 & 30 \\ 7 & 11 & -21 \end{pmatrix}$. Infatti in $\mathbb{Z}_{11}$ risulta $27^{-1} = 5^{-1} = 9$.

Lemma 8.3.17 *Sia* A *una matrice quadrata a scala. Se le sue righe (risp. colonne) sono indipendenti, allora* A *è una matrice non degenere.*

Dimostrazione — Sia A una matrice quadrata a scala con le righe indipendenti. Allora nessuna riga è nulla, e quindi nessun pivot può essere nullo. D'altra parte i pivot di ciascuna riga giacciono sulla diagonale principale, ed il loro prodotto coincide col determinante di A. □

Corollario 8.3.18 *Sia K un campo, e sia $A \in \mathfrak{M}_{mm}(K)$. Le colonne $A^1, \ldots, A^m$ sono indipendenti, se e solo se A è non degenere.*

Dimostrazione — Se A è non degenere, allora A è invertibile per il Lemma 8.3.15, e per la proposizione 8.1.7 le colonne $A^1, \ldots, A^m$ sono indipendenti. Viceversa, supponiamo che le colonne $A^1, \ldots, A^m$ siano indipendenti. Per la Proposizione 8.2.6 una matrice a scala associata ad A ha le colonne indipendenti e, per la proposizione 8.3.17, risulta non degenere. Pertanto per la proposizione 8.3.7 anche A è non degenere. □

Teorema 8.3.19 (Di caratterizzazione delle matrici invertibili) *Sia K un campo, e sia $A \in \mathfrak{M}_{mm}(K)$. Sono equivalenti:*

(a) *A è invertibile;*

(b) *Le colonne di A sono indipendenti;*

(c) *A è non degenere;*

(d) *Le righe di A sono indipendenti.*

Dimostrazione — $(a) \iff (c)$. Per il lemma 8.3.15 ogni matrice non degenere è invertibile. Viceversa se A è invertibile, allora esiste una matrice B tale che $A \cdot B = \mathfrak{I}_m$, sicché per il teorema di Binet risulta: $1 = \det(\mathfrak{I}_m) = \det(A \cdot B) = \det(A) \cdot \det(B)$, e quindi A è non degenere.

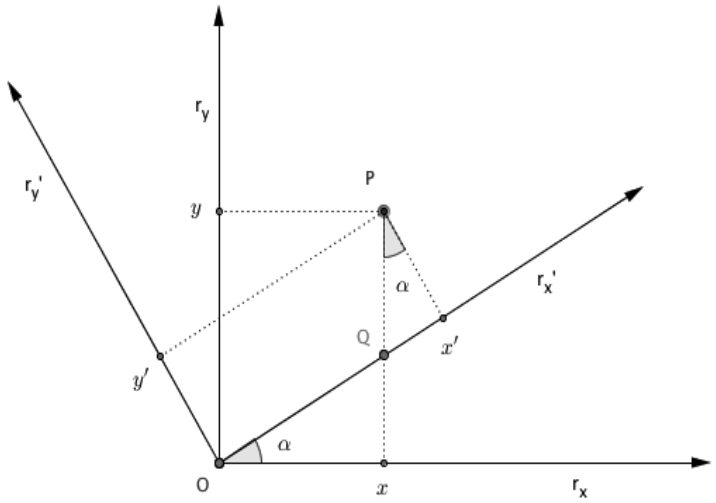
$(b) \iff (c)$. Segue dal corollario 8.3.18. Infine le righe di A coincidono con le colonne di A_t, e per il teorema 8.3.5 si ha $\det(A) = \det(A_t)$, quindi $(d) \iff (c)$. □

Osservazione Il gruppo degli elementi invertibili del monoide $(\mathfrak{M}_{n,n}(K), \cdot)$ si denota con $GL(n, K)$.

Esercizio 8.3.20 Sia $A_k = \begin{pmatrix} 1 & k & 1 \\ 7 & 0 & k \\ 0 & 1 & k \end{pmatrix} \in \mathfrak{M}_{33}(\mathbb{Q})$. Per quali valori del parametro k, la matrice A_k è non degenere?

8.4 ROTAZIONE DEGLI ASSI CARTESIANI: MATRICE DEL CAMBIAMENTO DI RIFERIMENTO

Siano $\mathfrak{R} = (O, r_x, r_y)$ e $\mathfrak{R}' = (O, r'_x, r'_y)$ due riferimenti cartesiani monometrici ortogonali, aventi la stessa origine, e tali che $\mathfrak{R}'$ sia ruotato di un angolo α rispetto ad $\mathfrak{R}$. Sia P un punto del piano, di coordinate $P \equiv_{\mathfrak{R}} (x, y)$ nel riferimento $\mathfrak{R}$ e $P \equiv_{\mathfrak{R}'} (x', y')$ nel riferimento $\mathfrak{R}'$.



Teorema 8.4.1 (CAMBIAMENTO DI COORDINATE) *La relazione che esprime il cambiamento delle coordinate di* P *nel passaggio dal riferimento* $\mathfrak{R}$ *al riferimento* $\mathfrak{R}'$ *è la seguente:*

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos(\alpha) & \operatorname{sen}(\alpha) \\ -\operatorname{sen}(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

DIMOSTRAZIONE — Poniamo $\rho = |\overline{OQ}|$ la lunghezza del segmento di estremi O, Q. Sussistono le seguenti relazioni:

$$x = \rho \cos(\alpha), \qquad y = |\overline{PQ}| + \rho \operatorname{sen}(\alpha),$$

$$x' = \rho + |\overline{PQ}| \operatorname{sen}(\alpha), \qquad y' = |\overline{PQ}| \cos(\alpha).$$

Esprimendo x' ed y' in funzione di x, y e α abbiamo:

$$x' = \rho + |\overline{PQ}|\ sen(\alpha) = \rho + (y - \rho\ sen(\alpha))sen(\alpha)$$
$$= \rho + y\ sen(\alpha) - \rho\ sen^2(\alpha) = \rho(1 - sen^2(\alpha)) + y\ sen(\alpha)$$
$$= \rho\ cos(\alpha)\ cos(\alpha) + y\ sen(\alpha) = x\ cos(\alpha) + y\ sen(\alpha).$$

Analogamente,

$$y' = |\overline{PQ}|\ cos(\alpha) = (y - \rho\ sen(\alpha))\ cos(\alpha)$$
$$= y\ cos(\alpha) - \rho\ sen(\alpha)\ cos(\alpha) = -x\ sen(\alpha) + y\ cos(\alpha).\square$$

La matrice

$$C = \begin{pmatrix} cos(\alpha) & sen(\alpha) \\ -sen(\alpha) & cos(\alpha) \end{pmatrix}$$

si chiama *matrice del cambiamento di riferimento*. Chiaramente ci si può chiedere quale sia l'espressione del cambiamento inverso di riferimento. A tal proposito osserviamo che la matrice C ha determinante 1 e la sua inversa è:

$$C^{-1} = \begin{pmatrix} cos(\alpha) & -sen(\alpha) \\ sen(\alpha) & cos(\alpha) \end{pmatrix}.$$

Pertanto

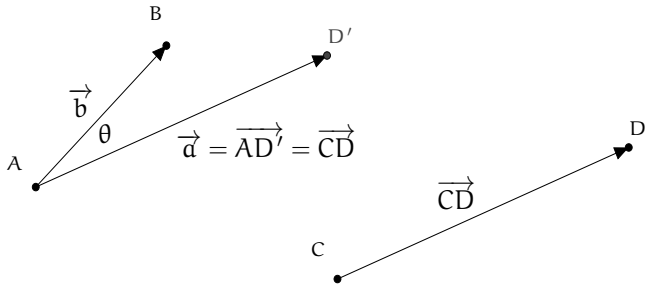
Corollario 8.4.2 *La relazione che esprime il cambiamento delle coordinate di* P *nel passaggio dal riferimento* $\mathfrak{R}'$ *al riferimento* $\mathfrak{R}$ *è la seguente:*

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} cos(\alpha) & -sen(\alpha) \\ sen(\alpha) & cos(\alpha) \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

8.5 PRODOTTI TRA VETTORI LIBERI

In questa sezione introdurremo dapprima la nozione di prodotto scalare tra vettori liberi dello spazio euclideo, e vedremo come questa nozione si estende ai vettori numerici di uno spazio K^n. Definiremo poi un'operazione interna tra i vettori liberi: Il prodotto vettoriale.

Siano $\overrightarrow{AB}$ e $\overrightarrow{CD}$ vettori liberi geometrici. Il segmento orientato $\overline{CD}$ è equipollente ad un segmento del tipo $\overline{AD'}$, sicché resta individuato un angolo Θ compreso tra $\overrightarrow{AB}$ e $\overrightarrow{AD'}$.

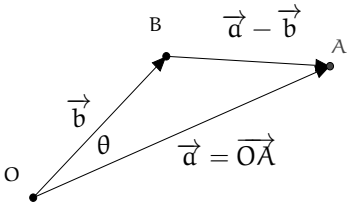


Diremo *prodotto scalare dei vettori* $\overrightarrow{AB}$ *e* $\overrightarrow{CD}$ il prodotto delle lunghezze dei segmenti $\overline{AB}$ e $\overline{CD}$ per il coseno dell'angolo Θ:

$$\overrightarrow{AB} \cdot \overrightarrow{CD} = |\overrightarrow{AB}| \cdot |\overrightarrow{CD}| \cdot \cos(\Theta).$$

Notiamo che due vettori ortogonali hanno prodotto scalare nullo, mentre per ogni vettore libero geometrico $\vec{v}$, risulta $\vec{v} \cdot \vec{v} = |\vec{v}|^2$.

Sia assegnato nello spazio euclideo $\mathbb{E}^3$ un riferimento monometrico ortogonale. Siano $\vec{a} = \overrightarrow{OA}$ e $\vec{b} = \overrightarrow{OB}$ vettori geometrici di componenti rispettivamente (a_1, a_2, a_3) e (b_1, b_2, b_3). I punti A, O, B sono i vertici di un triangolo i cui lati sono individuati dai vettori $\vec{a}$, $\vec{b}$, $\vec{a} - \vec{b}$.



Denotato con Θ l'angolo compreso tra $\vec{a}$ e $\vec{b}$, e applicando il teorema di Carnot abbiamo:

$$|\vec{a} - \vec{b}|^2 = |\vec{a}|^2 + |\vec{b}|^2 - 2|\vec{a}||\vec{b}|\cos(\Theta) = |\vec{a}|^2 + |\vec{b}|^2 - 2\vec{a} \cdot \vec{b}.$$

Da cui

$$\vec{a} \cdot \vec{b} = \frac{1}{2}(-|\vec{a} - \vec{b}|^2 + |\vec{a}|^2 + |\vec{b}|^2)$$

$$= \frac{1}{2}[a_1^2 + a_2^2 + a_3^2 + b_1^2 + b_2^2 + b_3^2 - (a_1 - b_1)^2 - (a_2 - b_2)^2 - (a_3 - b_3)^2]$$

$$= \frac{1}{2}(2a_1b_1 + 2a_2b_2 + 2a_3b_3) = a_1b_1 + a_2b_2 + a_3b_3.$$

Pertanto *il prodotto scalare tra due vettori geometrici, di cui si conoscono le componenti, si ottiene facendo la somma dei prodotti delle componenti omonime.*

In generale in uno spazio vettoriale numerico K^n, il *prodotto scalare standard* di due vettori $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$ è lo scalare:

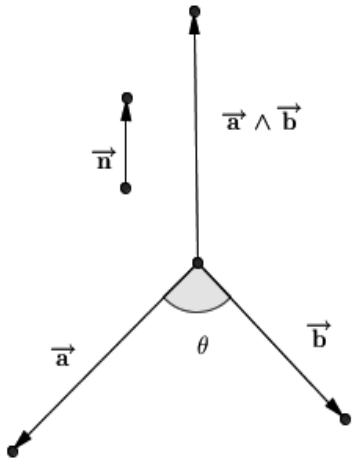
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = a_1b_1 + \ldots + a_nb_n.$$

Esercizio 8.5.1 Sia $A \equiv (1,7,5)$ e $B \equiv (5,1,7)$. Stabilire se l'angolo tra i vettori $\overrightarrow{OA}$ e $\overrightarrow{OB}$ è maggiore o minore di $\pi/3$.

Siano $\vec{a}$ e $\vec{b}$ vettori geometrici dello spazio euclideo. Diremo *prodotto vettoriale di* $\vec{a}$ *e* $\vec{b}$ il vettore nullo se uno dei due è il vettore nullo oppure se $\vec{a}$ e $\vec{b}$ sono paralleli, diversamente si pone:

$$\vec{a} \wedge \vec{b} = |\vec{a}||\vec{b}|sen(\theta) \cdot \vec{n},$$

dove θ è l'angolo compreso tra $\vec{a}$ e $\vec{b}$, e $\vec{n}$ è il versore (vettore di modulo unitario) perpendicolare al piano individuato da $\vec{a}$ e da $\vec{b}$, il cui verso è dato dalla regola della mano destra: *"disponendo le dita su* $\vec{a}$ *e il palmo su* $\vec{b}$ *allora il verso di* $\vec{n}$ *è dato dal pollice."*

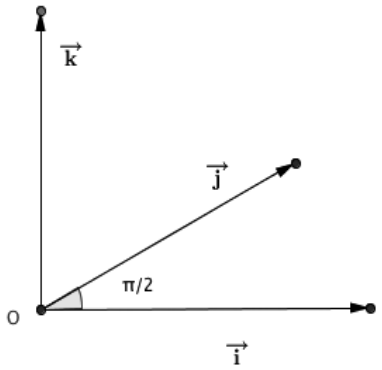


Esercizio 8.5.2 Siano $\vec{a}$ e $\vec{b}$ vettori geometrici dello spazio euclideo. Il prodotto $\vec{a} \wedge \vec{b}$ è sempre perpendicolare sia ad $\vec{a}$ che a $\vec{b}$?

Osservazione 8.5.3 Siano $\vec{a}$ e $\vec{b}$ vettori geometrici non nulli dello spazio euclideo. Allora $\vec{a}$ e $\vec{b}$ sono paralleli se e solo se $\vec{a} \wedge \vec{b} = \vec{0}$.

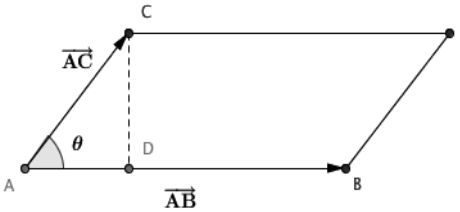
Osservazione 8.5.4 Siano $\vec{a}$ e $\vec{b}$ vettori geometrici dello spazio euclideo. Allora $\vec{a} \wedge \vec{b} = -(\vec{b} \wedge \vec{a})$.

Esercizio 8.5.5 Siano $\vec{i}$, $\vec{j}$ e $\vec{k}$ i vettori geometrici della base standard dello spazio euclideo, ovvero i vettori che individuano un riferimento monometrico ortogonale in $\mathbb{E}^3$, secondo la figura:



Allora $\vec{i} \wedge \vec{j} = \vec{k}$. Determinare tutti i possibili prodotti tra gli elementi $\vec{i}$, $\vec{j}$, $\vec{k}$,- $-\vec{i}, -\vec{j}, -\vec{k}$. L'insieme $L = \{\vec{0}, \vec{i}, \vec{j}, \vec{k}, -\vec{i}, -\vec{j} - \vec{k}\}$ col prodotto vettoriale è un monoide?

Osservazione 8.5.6 Sia $\mathfrak{P}$ un parallelogramma come in figura:



L'altezza di $\mathfrak{P}$ coincide con il modulo di $\overrightarrow{AC}$ per il seno dell'angolo θ.
Allora l'area di $\mathfrak{P}$ coincide con $|\overrightarrow{AC} \wedge \overrightarrow{AB}| = |\overrightarrow{AC}||\overrightarrow{AB}|sen(\theta)$.

Di facile vefirifica sono le seguenti proprietà:

Proposizione 8.5.7 (Proprietà del prodotto vettoriale) *Siano* $\vec{a}, \vec{b}, \vec{c}$ *vettori di* $\mathbb{E}^3$ *e* $\alpha \in \mathbb{R}$ *allora:*

(1) $\vec{a} \wedge \vec{b} = -\vec{b} \wedge \vec{a}$;

(2) $\alpha\vec{a} \wedge \vec{b} = \alpha(\vec{a} \wedge \vec{b}) = \vec{a} \wedge (\alpha\vec{b})$;

(3) $\vec{a} \wedge (\vec{b} + \vec{c}) = (\vec{a} \wedge \vec{b}) + (\vec{a} \wedge \vec{c})$;

(4) $(\vec{a} + \vec{b}) \wedge \vec{c} = (\vec{a} \wedge \vec{c}) + (\vec{b} \wedge \vec{c})$.

Proposizione 8.5.8 *Siano* (a_1, a_2, a_3) *e* (b_1, b_2, b_3) *le componenti di due vettori liberi* $\vec{a}$ *e* $\vec{b}$ *dello spazio euclideo espresse nel riferimento naturale* $\mathfrak{R} = (O; \vec{i}, \vec{j}, \vec{k})$. *Allora le componenti di* $\vec{a} \wedge \vec{b}$ *sono espresse dalla terna* $(a_2b_3 - a_3b_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1)$. *In particolare*

$$\vec{a} \wedge \vec{b} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}.$$

Dimostrazione – Utilizzando le definizioni e la proposizione 8.5.7 si ha: $\vec{a} = a_1\vec{i} + a_2\vec{j} + a_3\vec{k}$ e $\vec{b} = b_1\vec{i} + b_2\vec{j} + b_3\vec{k}$, e quindi

$$\begin{aligned} \vec{a} \wedge \vec{b} &= a_1b_1(\vec{i} \wedge \vec{i}) + a_1b_2(\vec{i} \wedge \vec{j}) + a_1b_3(\vec{i} \wedge \vec{k}) \\ &\quad + a_2b_1(\vec{j} \wedge \vec{i}) + a_2b_2(\vec{j} \wedge \vec{j}) + a_2b_3(\vec{j} \wedge \vec{k}) \\ &\quad + a_3b_1(\vec{k} \wedge \vec{i}) + a_3b_2(\vec{k} \wedge \vec{j}) + a_3b_3(\vec{k} \wedge \vec{k}) \\ &= a_1b_2\vec{k} + a_1b_3(-\vec{j}) + a_2b_1(-\vec{k}) + a_2b_3\vec{i} + a_3b_1\vec{j} + a_3b_2(-\vec{i}) \\ &= (a_2b_3 - a_3b_2)\vec{i} + (a_3b_1 - a_1b_3)\vec{j} + (a_1b_2 - a_2b_1)\vec{k}. \square \end{aligned}$$

Esempio 8.5.9 $\vec{a} \equiv (1,3,4)$ e $\vec{b} \equiv (2,7,-5)$ allora:

$$\vec{a} \wedge \vec{b} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ 1 & 3 & 4 \\ 2 & 7 & -5 \end{vmatrix} = \begin{vmatrix} 3 & 4 \\ 7 & -5 \end{vmatrix}\vec{i} - \begin{vmatrix} 1 & 4 \\ 2 & -5 \end{vmatrix}\vec{j} + \begin{vmatrix} 1 & 3 \\ 2 & 7 \end{vmatrix}\vec{k}$$

$$= -43\vec{i} + 13\vec{j} + \vec{k}.$$

Osservazione 8.5.10 Osserviamo che se $\vec{a}$ e $\vec{b}$ giacciono nel piano individuato dai versori $\vec{i}$ e $\vec{j}$, allora la loro terza componente è nulla, per cui

$$\vec{a} \wedge \vec{b} = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}\vec{k}.$$

In particolare l'area del parallelogramma che individuano $\vec{a}$ e $\vec{b}$ è il valore assoluto del determinante della matrice le cui righe sono le loro componenti:

$$\left|\det\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}\right|.$$

Proposizione 8.5.11 *Siano ora* $P_1 = (x_1, y_1)$ $P_2 = (x_2, y_2)$ $P_3 = (x_3, y_3)$ *punti del piano euclideo. Provare che l'area del triangolo di vertici* P_1, P_2 *e* P_3 *è*

$$1/2 \left| \det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} \right|.$$

Dimostrazione — Le componenti del vettore $\overrightarrow{P_1P_3}$ sono $(x_3 - x_1, y_3 - y_1)$ e le componenti del vettore $\overrightarrow{P_2P_3}$ sono $(x_3 - x_2, y_3 - y_2)$. L'area del parallelogramma che essi individuano è il doppio dell'area cercata, e coincide con il modulo del loro prodotto vettoriale.

$$|\overrightarrow{P_1P_3} \wedge \overrightarrow{P_2P_3}| = \left| \det \begin{pmatrix} x_3 - x_1 & y_3 - y_1 \\ x_3 - x_2 & y_3 - y_2 \end{pmatrix} \right|$$

$$= |-x_3y_2 + x_3y_1 + x_1y_2 - x_1y_1 + x_2y_3 - x_2y_1 - x_1y_3 + x_1y_1|.$$

D'altra parte

$$\det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} = \det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} - \det \begin{pmatrix} x_1 & y_1 \\ x_3 & y_3 \end{pmatrix} + \det \begin{pmatrix} x_2 & y_2 \\ x_3 & y_3 \end{pmatrix}$$

$$= x_1y_2 - x_2y_1 - x_1y_3 + x_3y_1 + x_2y_3 - x_3y_2,$$

il cui valore assoluto coincide con $|\overrightarrow{P_1P_3} \wedge \overrightarrow{P_2P_3}|$. □

8.6 SISTEMI LINEARI OMOGENEI

Un'equazione a coefficienti in K in n incognite si dice *lineare* se è di primo grado. L'equazione $x_1 + 7 + x_2 + x_1 \cdot x_2 = 0$ non è lineare, in quanto il monomio $x_1 \cdot x_2$ ha grado 2, e la stessa equazione risulta essere di secondo grado.

Un insieme Σ di m equazioni lineari su un campo K in n incognite si dice sistema lineare, e si rappresenta usualmente così:

$$\Sigma = \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \quad \vdots \qquad \vdots \qquad\qquad \vdots \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}.$$

La matrice $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \in \mathfrak{M}_{mn}(K)$ individuata dai coefficienti delle incognite si dice *matrice incompleta associata al sistema* Σ, e la matrice $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathfrak{M}_{m1}(K)$ si dice *colonna dei termini noti*, inoltre la matrice

$$\bar{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix} \in \mathfrak{M}_{m(n+1)}(K),$$ individuata dai coefficienti e dalla colonna dei termini noti si dice *matrice completa associata al sistema* Σ.

Talvolta il sistema Σ si rappresenta anche con la seguente identità vettoriale:

$$x_1 \cdot A^1 + \ldots + x_n \cdot A^n = B, \tag{1}$$

dove $A^1, \ldots, A^n$ sono le colonne di A.

Esempio 8.6.1 $\Sigma = \begin{cases} 3x_1 + 2x_2 + 5x_3 = 4 \\ -x_1 + x_2 - 6x_3 = -1 \\ x_1 + \quad +7x_3 = 0 \\ x_1 + x_2 + \quad = 1 \end{cases}$. Sistema di quattro equazioni in tre incognite sul campo $\mathbb{R}$, allora le matrici associate sono:

$$A = \begin{pmatrix} 3 & 2 & 5 \\ -1 & 1 & -6 \\ 1 & 0 & 7 \\ 1 & 1 & 0 \end{pmatrix} \in \mathfrak{M}_{43}(\mathbb{R}), \text{ e } \bar{\mathbf{A}} = \begin{pmatrix} 3 & 2 & 5 & 4 \\ -1 & 1 & -6 & -1 \\ 1 & 0 & 7 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{\mathbf{44}}(\mathbb{R}).$$

In virtù della 1, il sistema considerato in questo esempio si può rappresentare anche come segue:

$$x_1\begin{pmatrix}3\\-1\\1\\1\end{pmatrix}+x_2\begin{pmatrix}2\\1\\0\\1\end{pmatrix}+x_3\begin{pmatrix}5\\-6\\7\\0\end{pmatrix}=\begin{pmatrix}4\\-1\\0\\1\end{pmatrix}.$$

Sia Σ un sistema lineare di m equazioni in n incognite sul campo K, e sia A la matrice associata a Σ, B la colonna dei termini noti e $L := K[x_1, ...x_t]$.

Se denotiamo con $X = \begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix} \in \mathfrak{M}_{n1}(L)$, allora il prodotto della prima riga di A con la colonna X coincide con il primo membro della prima equazione di Σ: $A_1 \cdot X = a_{11} \cdot x_1 + a_{12} \cdot x_2 + \cdots + a_{1n} \cdot x_n$. Analogamente la i-esima equazione si può scrivere $A_i \cdot X = b_i$ e l'intero sistema $\Sigma = \begin{cases}A_1X = b_1\\A_2X = b_2\\\quad\vdots\\A_mX = b_m\end{cases}$ è completamente rappresentato dall'equazione matriciale $A \cdot X = B$. In tal caso una soluzione del sistema può essere rappresentata da una colonna $C = \begin{pmatrix}c_1\\c_2\\\vdots\\c_n\end{pmatrix}$ tale che $AC = B$.

Due sistemi si dicono *equivalenti* se ammettono le stesse soluzioni.

Esempio 8.6.2 I seguenti sistemi sono equivalenti:

$$\Sigma = \begin{cases}3x_1 + 2x_2 + 5x_3 = 4\\-x_1 + x_2 - 6x_3 = -1\end{cases} \quad \text{e} \quad \Sigma' = \begin{cases}3x_1 + 2x_2 + 5x_3 = 4\\-x_1 + x_2 - 6x_3 = -1\\19x_1 + 16x_2 + 23x_3 = 26\end{cases}.$$

Osserviamo che la terza equazione del secondo sistema si ottiene come combinazione lineare della prima equazione (per 7) e della seconda equazione (per 2).

Se C è una soluzione di Σ, allora $\Sigma = \begin{cases}A_1C = 4\\A_2C = -1\end{cases}$, e quindi $\begin{cases}7A_1C = 28\\2A_2C = -2\end{cases}$.

Sommando membro a membro otteniamo che C verifica anche la terza equazione del sistema Σ'

Più in generale abbiamo

Esercizio 8.6.3 Sia $\Sigma = \begin{cases} A_1X = b_1 \\ A_2X = b_2 \\ \quad \vdots \\ A_mX = b_m \end{cases}$, allora Σ è equivalente ad ogni sistema

$$\Sigma' = \begin{cases} A_1X = b_1 \\ A_2X = b_2 \\ \quad \vdots \\ A_mX = b_m \\ A_{m+1}X = b_{m+1} \end{cases},$$

ottenuto da Σ aggiungendo l'equazione $A_{m+1}X = b_{m+1}$, dove $A_{m+1} = \alpha_1A_1 + \ldots + \alpha_mA_m$ e $b_{m+1} = \alpha_1b_1 + \ldots + \alpha_mb_m$, per ogni scelta degli scalari $\alpha_1, \ldots \alpha_m$.

Esercizio 8.6.4 Scrivere un sistema Σ di tre equazioni in quattro incognite, e successivamente scrivere un sistema equivalente a Σ, ma con equazioni diverse.

Ai fini della risoluzione di un sistema non è rilevante se una sua soluzione si rappresenta come colonna o come riga. Pertanto spesso si identificherà il vettore $C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$ con il vettore $(c_1, c_2, \ldots, c_n)$, tenendo presente che gli spazi $\mathfrak{M}_{n1}(K)$ e $\mathfrak{M}_{1n}(K) = K^n$ sono isomorfi.

Un sistema del tipo $\Sigma = \begin{cases} A_1X = 0 \\ A_2X = 0 \\ \quad \vdots \\ A_mX = 0 \end{cases}$, dove la colonna dei termini noti è nulla si dice *omogeneo*.

Proposizione 8.6.5 *Sia* $A \in \mathfrak{M}_{mn}(K)$*, con* K *campo. I vettori colonna* $A^1, \ldots, A^n$ *sono indipendenti se e solo se il sistema omogeneo*

$$x_1 \cdot A^1 + \ldots + x_n \cdot A^n = 0$$

ammette solo la soluzione banale $x_1 = 0, \ldots, x_n = 0$*.*

Dimostrazione — I vettori $A^1, \ldots, A^n$ dello spazio vettoriale $\mathfrak{M}_{m1}(K)$ sono indipendenti se e solo se (per definizione) il vettore nullo $0 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ si esprime come combinazione lineare di $A^1, \ldots, A^n$ soltanto mediante scalari tutti nulli. □

Osserviamo anche che il sistema $AX = 0$ ammette sempre la soluzione nulla $\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

Più in generale proviamo che:

Teorema 8.6.6 *Sia* $A \in \mathfrak{M}_{mn}(K)$*, con* K *campo. L'insieme delle soluzioni del sistema omogeneo* $AX = 0$ *è un sottospazio dello spazio vettoriale* $\mathfrak{M}_{n1}(K)$*.*

Dimostrazione — Siano C e C' soluzioni del sistema $AX = 0$, e siano α e β elementi del campo K. Proveremo che $\alpha C + \beta C'$ è soluzione del sistema $AX = 0$. Per le proprietà delle operazioni tra matrici risulta:

$$A(\alpha C + \beta C') = A(\alpha C) + A(\beta C') = \alpha AC + \beta AC' = 0 + 0 = 0. \square$$

Esempio 8.6.7 L'insieme delle soluzioni di un sistema del tipo

$$\Sigma = \begin{cases} ax + by + cz = 0 \\ a'x + b'y + c'z = 0 \end{cases},$$

a coefficienti in K è un sottospazio di $\mathfrak{M}_{31}(K) \simeq K^3$. Nel caso in cui K è il campo dei reali, il sistema che abbiamo considerato rappresenta l'intersezione di due piani.

8.7 RANGO DI UNA MATRICE E TEOREMA DI ROUCHÈ CAPELLI

Sia $A \in \mathfrak{M}_{mn}(K)$. Si dice *rango* di A il seguente intero positivo:
$\rho(A) = \max\{n \in \mathbb{N}: n \text{ è l'ordine di una sottomatrice non degenere di} A\}$.

Chiaramente il rango di una matrice quadrata non degenere coincide col suo ordine.

Esempio 8.7.1 Sia $A = \begin{pmatrix} 1 & 6 & 3 & 5 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{34}(\mathbb{Q})$. Risulta $\rho(A) = 3$.

Sia A' una sottomatrice non degenere di una matrice A. Si dice che A' è una *sottomatrice fondamentale* di A se non è "contenuta" in nessun' altra sottomatrice non degenere di A. Evidentemente ogni sottomatrice non degenere o è fondamentale oppure è contenuta in una sottomatrice fondamentale.

Esempio 8.7.2 Sia $A = \begin{pmatrix} 1 & 0 & 3 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{34}(\mathbb{Z}_5)$. Risulta $\rho(A) = 2$.

Esempio 8.7.3 Sia $A = \begin{pmatrix} 1 & 1 & 3 & 0 \\ 2 & 1 & 1 & 1 \\ -1 & 1 & 7 & -2 \end{pmatrix} \in \mathfrak{M}_{34}(\mathbb{Q})$. Risulta $\rho(A) = 2$.

Se di una matrice A già si conosce il rango $\rho = \rho(A)$, e A' è una sottomatrice non degenere di ordine esattamente ρ, allora essa non è contenuta in nessun' altra sottomatrice non degenere, e quindi è necessariamente fondamentale.

Nelle applicazioni però il rango di una matrice si determina proprio individuando una sottomatrice fondamentale non degenere. Proveremo infatti che (vedi 8.7.9):

L'ordine di una qualunque sottomatrice fondamentale di A coincide col rango di A.

Esercizio 8.7.4 Sia $A = \begin{pmatrix} 1 & 0 & 3 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{34}(\mathbb{Z}_5)$. Determinare due sottomatrici fondamentali di A.

Esercizio 8.7.5 Sia $A = \begin{pmatrix} 1 & 1 & 3 & 0 \\ 2 & 1 & 1 & 1 \\ -1 & 1 & 7 & -2 \end{pmatrix} \in \mathfrak{M}_{34}(\mathbb{Q})$. Determinare due sottomatrici fondamentali di A.

Lemma 8.7.6 *Sia $A \in \mathfrak{M}_{mn}(K)$, con K campo. Se i vettori colonna $A^1, \dots, A^n$ sono indipendenti allora $m \geqslant n$. Inoltre se $A_{i_1}, \dots, A_{i_s}$ sono righe indipendenti di A, con $s \leqslant n$, allora esitono opportuni indici $i_1, \dots, i_n \in I_m$ tali che $\{i_1, \dots, i_s\} \subseteq \{i_1, \dots, i_n\}$ e la sottomatrice $A^{1,\dots,n}_{i_1,\dots,i_n}$ è non degenere.*

Dimostrazione — Per ipotesi i vettori $A^1, \dots, A^n$ dello spazio vettoriale $\mathfrak{M}_{m1}(K)$ sono indipendenti, quindi il loro numero non può superare la dimensione m dello spazio $\mathfrak{M}_{m1}(K)$. Ora completiamo la parte linearmente indipendente $A_{i_1}, \dots, A_{i_s}$ in un sistema minimale $A_{i_1}, \dots, A_{i_r}$ di generatori dello spazio $\langle A_1, \dots, A_m \rangle$, $(i_1, \dots, i_r \in I_m)$. Chiaramente $\langle A_{i_1}, \dots, A_{i_r} \rangle$ è un sottospazio di $\mathfrak{M}_{1n}(K)$, quindi $r \leqslant n$. Inoltre i sistemi

$$\Sigma = \begin{cases} A_1 X = 0 \\ A_2 X = 0 \\ \vdots \\ A_m X = 0 \end{cases} \quad \text{e} \quad \begin{cases} A_{i_1} X = 0 \\ A_{i_2} X = 0 \\ \vdots \\ A_{i_r} X = 0 \end{cases}$$

sono equivalenti. D'altra parte per la proposizione 8.6.5 il sistema Σ ammette solo la soluzione banale, allora ancora per la 8.6.5 le colonne della matrice $A^{1,\dots,n}_{i_1,\dots,i_r}$ sono indipendenti e appartengono $\mathfrak{M}_{r1}(K)$, per cui $n \leqslant r$. Abbiamo provato che $n = r$. Inoltre la matrice quadrata $A^{1,\dots,n}_{i_1,\dots,i_n}$ ha le righe e le colonne indipendenti, per cui è non degenere per il Teorema 8.3.19. □

Esempio 8.7.7 Sia $A = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 2 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \in \mathfrak{M}_{74}(\mathbb{Q})$. Una facile verifica prova che le colonne A^1, A^2, A^3, A^4 sono indipendenti. In virtù del lemma precedente, se consideriamo delle righe indipendenti, ad esempio $A_1 = A_{i_1}$ e $A_5 = A_{i_2}$, allora esistono altre due righe A_{i_3} e A_{i_4} in modo tale che la sottomatrice $A^{1,\dots,4}_{i_1,\dots,i_4}$ è non degenere. Osserviamo che la scelta delle righe A_{i_3} e A_{i_4} non è arbitraria nè univoca.

Il seguente risultato caratterizza il rango di una matrice come il numero massimo di righe (o colonne) linearmente indipendenti:

Lemma 8.7.8 *Sia* $A \in \mathfrak{M}_{mn}(K)$*, con* K *campo, e sia* $\bar{A} = A^{j_1,\dots,j_r}_{i_1,\dots,i_r}$ *una sottomatrice fondamentale di* A*. Allora i vettori* $A^{j_1},\dots,A^{j_r}$ *sono una base dello spazio* $\langle A^1,\dots,A^n\rangle$ *e* $A_{i_1},\dots,A_{i_r}$ *sono una base dello spazio* $\langle A_1,\dots,A_m\rangle$*. In particolare* $r = \dim(\langle A^1,\dots,A^n\rangle) = \dim(\langle A_1,\dots,A_m\rangle)$*.*

Dimostrazione — Poniamo $s = \dim(\langle A^1,\dots,A^n\rangle)$. Per ipotesi $\bar{A}$ è non degenere, allora per il Teorema 8.3.19 le sue colonne $\bar{A}^{j_1},\dots,\bar{A}^{j_r}$ sono vettori indipendenti dello spazio $\mathfrak{M}_{r1}(K)$. L'applicazione

$$\varphi : \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{pmatrix} \in \mathfrak{M}_{m1}(K) \to \begin{pmatrix} \alpha_{i_1} \\ \alpha_{i_2} \\ \vdots \\ \alpha_{i_r} \end{pmatrix} \mathfrak{M}_{r1}(K)$$

è un omomorfismo, e quindi comunque si considerano dei vettori $v_1 \in \varphi^{-1}(\{\bar{A}^{j_1}\}),\dots,v_r \in \varphi^{-1}(\{\bar{A}^{j_r}\})$, questi risultano essere indipendenti. In particolare $A^{j_1},\dots,A^{j_r}$ sono vettori indipendenti dello spazio $\langle A^1,\dots,A^n\rangle \subseteq \mathfrak{M}_{m1}(K)$, e $r \leqslant s$. Per assurdo $A^{j_1},\dots,A^{j_r}$ non sia una base di $\langle A^1,\dots,A^n\rangle$, allora esiste $j \in I_n \setminus \{j_1,\dots,j_r\}$ tale che $A^{j_1},\dots,A^{j_r},A^j$ sono vettori indipendenti di $\mathfrak{M}_{m1}(K)$. Chiaramente $r+1 \leqslant m$. Consideriamo la sottomatrice $\bar{\bar{A}} = A^{j_1,\dots,j_r,j}_{1,\dots,m}$.

L'applicazione

$$\psi : (\alpha_{j_1},\alpha_{j_2},\dots,\alpha_{j_r},\alpha_j) \in \mathfrak{M}_{1,r+1}(K) \to (\alpha_{j_1},\alpha_{j_2},\dots,\alpha_{j_r}) \in \mathfrak{M}_{1,r}(K)$$

è un omomorfismo. Allora le righe $\bar{\bar{A}}_{i_1} \in \psi^{-1}(\{\bar{A}_{i_1}\}),\dots,\bar{\bar{A}}_{i_r} \in \psi^{-1}(\{\bar{A}_{i_r}\})$ sono indipendenti e applicando il lemma precedente possiamo considerare un indice $i \in I_m \setminus \{i_1,\dots,i_r\}$ tale che la sottomatrice $A^{j_1,\dots,j_r,j}_{i_1,\dots,i_r,i}$ è non degenere, e contiene propriamente $\bar{A}$. Questa contraddizione prova che $r = s$, e quindi i vettori $A^{j_1},\dots,A^{j_r}$ sono una base dello spazio $\langle A^1,\dots,A^n\rangle$. Per provare che $A_{i_1},\dots,A_{i_r}$ sono una base dello spazio $\langle A_1,\dots,A_m\rangle$, osserviamo che la trasposta $\bar{A}_t$ è una sottomatrice fondamentale di A_t. La prima parte della dimostrazione prova che $r = s = \dim_K(\langle A^1_t,\dots,A^m_t\rangle) = \dim_K(\langle A_1,\dots,A_m\rangle)$. □

Teorema 8.7.9 (del rango) *Sia* $A \in \mathfrak{M}_{mn}(K)$*, e sia* $r = \rho(A)$ *il suo rango. Allora* r *coincide col massimo numero di colonne (o righe) linearmente indipendenti, nonché con l' ordine di una qualunque sottomatrice fondamentale di* A*.*

Dimostrazione — Per ipotesi A contiene una sottomatrice non degenere di ordine r, $\bar{A}$. Chiaramente $\bar{A}$ è una sottomatrice fondamentale, e per il lemma precedente ogni altra sottomatrice fondamentale di A ha ordine r. D'altra parte l'intero r coincide con la dimensione dello spazio generato dalle colonne (risp. righe) di A. Pertanto il massimo numero di colonne (risp. righe) linearmente indipendenti di A è esattamente r. □

Esercizio 8.7.10 Sia

$$A = \begin{pmatrix} 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 10 & 11 & 12 & 13 & 14 & 15 & 16 \end{pmatrix},$$

Utilizzando la dipendenza lineare delle righe provare che il rango di A è 2. Osservare che la matrice è equivalente ad una matrice con due righe uguali

Un sistema si dice *compatibile* se ammette soluzioni.

Teorema 8.7.11 (Rouchè-Capelli) *Siano le matrici $A \in \mathfrak{M}_{mn}(K)$ e $B \in \mathfrak{M}_{m1}(K)$, con campo K. Il sistema lineare $AX = B$ è compatibile se e solo se il rango della matrice completa coincide col rango della matrice incompleta.*

Dimostrazione — Siano $A = (A^1 \dots A^n)$ e $\bar{A} = (A^1 \dots A^n B)$ le matrici associate al sistema. Supponiamo che il sistema sia compatibile, allora esistono $c_1, \dots, c_n$ tali che $c_1 A^1 + \dots + c_n A^n = B$. Quindi il vettore $B \in \mathfrak{M}_{m1}(K)$ dipende linearmente dai vettori $A^1 \dots A^n$. Poniamo $r = \rho(A)$, e sia $A^{j_1,\dots,j_r}_{i_1,\dots,i_r}$ una sottomatrice fondamentale di A. Allora per il lemma 8.7.8, $\{A^{j_1}, \dots, A^{j_r}\}$ è una base di $\langle A^1, \dots, A^n \rangle$. Chiaramente B dipende linarmente dai vettori $\{A^{j_1}, \dots, A^{j_r}\}$, e quindi la dimensione di $\langle A^1, \dots, A^n, B \rangle$ coincide con r. Per il lemma 8.7.8 il rango della matrice completa è r.

Reciprocamente, supponiamo che $r := \rho(A) = \rho(\bar{A})$. Per il lemma 8.7.8 entrambi i sottospazi $\langle A^1, \dots, A^n \rangle$ e $\langle A^1, \dots, A^n, B \rangle$ hanno dimensione r. Allora per le proposizioni 7.2.10 e 7.2.7 il vettore B dipende da $A^1, \dots, A^n$. Pertanto il sistema $AX = B$ ammette soluzione. □

8.8 Risoluzione dei sistemi lineari

Sia $AX = B$ un sistema lineare. Osserviamo che se A è quadrata e non degenere, allora il suo rango coincide col rango della matrice completa, e quindi per il teorema di Rouche-Capelli il sistema è certamente compatibile.

In tal caso si riescono anche facilmente ad individuare le soluzioni del sistema infatti:

Teorema 8.8.1 (Primo teorema di unicità) *Sia* $A \in \mathfrak{M}_{mm}(K)$ *e sia* $AX = B$ *un sistema lineare con* $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$. *Se* A *è non degenere, allora* $A^{-1}B$ *è l'unica soluzione del sistema assegnato .*

Dimostrazione — Per ipotesi A è quadrata ed invertibile. Dall'equazione $A \cdot X = B$ moltiplicando a sinistra per A^{-1} si ha $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = A^{-1}B$, per cui $A^{-1}B$ è una soluzione del sistema. Se inoltre $C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix}$ è un' altra soluzione del sistema, allora $AC = B$, e quindi necesariamnete $C = A^{-1}B$. □

Nella pratica, per risolvere i sistemi lineari del tipo precedente si ricorre spesso alla regola di Cramer.

Teorema 8.8.2 (Regola di Cramer) *Siano* $A \in \mathfrak{M}_{mm}(K)$ *e* $B \in \mathfrak{M}_{m1}(K)$, *e sia* $AX = B$ *un sistema lineare. Supponiamo che* A *non è degenere, e sia* $C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix}$ *l'unica soluzione del sistema assegnato. Allora per ogni* $i \in I_m$ *si ha*

$$c_i = \det((A^1 \dots A^{i-1} B A^{i+1} \dots A^m)) \cdot \det(A)^{-1}.$$

Dimostrazione — Poniamo $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$. Per il Primo teorema di unicità l'unica soluzione del sistema $AX = B$ è il vettore $C = A^{-1}B$. Per cui

$$C = \det(A)^{-1} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{m1} \\ A_{12} & A_{22} & \dots & A_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1m} & A_{2m} & \dots & A_{mm} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

$$= \det(A)^{-1} \begin{pmatrix} b_1A_{11} + b_2A_{21} + \ldots + b_mA_{m1} \\ b_1A_{12} + b_2A_{22} + \ldots + b_mA_{m2} \\ \vdots \\ b_1A_{1m} + b_2A_{2m} + \ldots + b_mA_{mm} \end{pmatrix}$$

$$= \det(A)^{-1} \begin{pmatrix} \det(BA^2 \dots A^m) \\ \det(A^1B \dots A^m) \\ \vdots \\ \det(A^1A^2 \dots B) \end{pmatrix}.$$

Per cui, per ogni $i \in I_m$ abbiamo

$$c_i = \det(A)^{-1} \cdot \det((A^1 \dots A^{i-1}BA^{i+1} \dots A^m))\square$$

Il primo teorema di unicità si specializza nel caso dei sistemi omogenei:

Corollario 8.8.3 *Sia* $A \in \mathfrak{M}_{mm}(K)$ *e sia* $AX = 0$ *un sistema lineare omogeneo. Se* A *è non degenere allora l'unica soluzione del sistema è* $C = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

Esempio 8.8.4 Sia $A = \begin{pmatrix} 1 & 3 & 4 \\ 7 & 0 & -2 \\ 4 & 1 & -1 \end{pmatrix} \in \mathfrak{M}_{33}(\mathbb{Q})$, e $B = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \in \mathfrak{M}_{31}(\mathbb{Q})$, e sia Σ il sistema di tre equazioni in tre incognite $AX = B$.

Già abbiamo visto che $\det(A)$=27 e $A^{-1} = \frac{1}{27} \cdot \begin{pmatrix} 2 & 7 & -6 \\ -1 & -17 & 30 \\ 7 & 11 & -21 \end{pmatrix}$. Allora $X = A^{-1}B = \frac{1}{27} \cdot \begin{pmatrix} 2 & 7 & -6 \\ -1 & -17 & 30 \\ 7 & 11 & -21 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{27} \begin{pmatrix} -2 \\ 28 \\ -7 \end{pmatrix}$, per cui la soluzione del

sistema è la terna $x_1 = -\frac{2}{27},\ x_2 = \frac{28}{27},\ x_3 = -\frac{7}{27}$. Se applichiamo la regola di Cramer si ottengono gli stessi valori.

Chiaramente quando la matrice A (incompleta associata a Σ) non è quadrata oppure non è invertibile bisogna procedere in modo diverso. Facciamo un esempio.

Esempio 8.8.5 $\Sigma = \begin{cases} x+y+z=1 \\ x-y\ \ =0 \\ 2x+\ \ +z=1 \end{cases}$. Sistema di tre equazioni in tre incognite sul campo $\mathbb{R}$, allora le matrici associate sono:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \in \mathfrak{M}_{33}(\mathbb{R}), \text{ e } \bar{A} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} \in \mathfrak{M}_{34}(\mathbb{R}).$$

In questo caso $\det(A) = 0$, e il sistema $AX = B$ non può essere risolto moltiplicando ambo i membri per A^{-1}, dal momento che A non è invertibile. Tuttavia si verifica facilmente che $\rho(A) = \rho(\bar{\mathbf{A}}) = 2$, sicché per il Teorema di Rouchè-Capelli il sistema è compatibile. Per trovare le soluzioni di $AX = B$, considereremo un sistema le cui equazioni sono indicate da una sottomatrice fondamentale di A. Ad esempio $A^{\{1,3\}}_{\{1,2\}} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \mathfrak{M}_{22}(\mathbb{R})$, è una sottomatrice fondamentale di A, che è individuata dalle prime due righe di A e dalla prima e terza colonna di A.

Si proverà che il sistema assegnato è equivalente al sistema $\Sigma' = \begin{cases} x+y+z=1 \\ x-y\ \ =0 \end{cases}$ ottenuto selezionando solo le prime due equazioni. Essendo inoltre $A^{\{1,3\}}_{\{1,2\}}$ non degenere, ogni qualvolta si assegna un valore arbitrario $k \in \mathbb{R}$ alla seconda incognita si ottiene un sistema $\Sigma_k = \begin{cases} x+z=1-k \\ x\ \ =k \end{cases}$ che per il Primo teorema di unicità ammette soluzione. In questo caso quindi il sistema assegnato (Σ) ammette tante (terne) di soluzioni quanti sono gli elementi di $\mathbb{R}$.

Osserviamo che se il sistema precedente è riguardato su $\mathbb{Z}_7$, allora il sistema è ancora compatibile, e l'insieme delle soluzioni è: $\{(k, k, 1-2k) \quad \text{tale che} \quad k \in \mathbb{Z}_7\}$ che è costituito da 7 terne.

In generale dopo aver verificato la compatibilità di un sistema, si considera una sottomatrice fondamentale, di cui gli indici delle righe (per il teorema che tra poco enuncieremo) individuano le equazioni di un sistema equivalente, mentre gli indici delle colonne che non compaiono individuano le

incognite che devono essere parametrizzate. Il procedimento che abbiamo illustrato si estende chiaramente ad un qualunque sistema lineare con m equazioni in n incognite. Esattamente ciò è il contenuto del secondo teorema di unicità, di cui riportiamo solo l'enunciato:

Teorema 8.8.6 (Secondo teorema di unicità)
Sia $\Sigma = \begin{cases} A_1X = b_1 \\ A_2X = b_2 \\ \vdots \\ A_mX = b_m \end{cases}$ *un sistema compatibile di* m *equazioni in* n *incognite su un campo* K. *Posto* $\rho(A) = \rho(\bar{A}) = p$, *e* $A^{\{j_1,j_2,\dots,j_p\}}_{\{i_1,i_2,\dots,i_p\}}$ *una sottomatrice fondamentale di* $A = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{pmatrix}$, *si ha che il sistema assegnato è equivalente al sistema*

$\Sigma' = \begin{cases} A_{i_1}X = b_{i_1} \\ A_{i_2}X = b_{i_2} \\ \vdots \\ A_{i_p}X = b_{i_p} \end{cases}$. *Inoltre per ogni scelta dei parametri* $k_1, \dots k_{n-p}$ *sulle incognite individuate delle colonne distinte da* $\{j_1, j_2, \dots, j_p\}$ *rimane definito un sistema di* p *equazioni in* p *incognite che ammette un'unica soluzione.*

Dimostrazione — È sufficiente verficare che per ogni $i \neq i_1, \dots, i_p$ l'equazione $A_iX = b_i$ è combinazione lineare delle equazioni di Σ'. □

Corollario 8.8.7 *Sia* $A \in \mathfrak{M}_{mn}(K)$, *con* K *campo. L'insieme delle soluzioni del sistema omogeneo* $AX = 0$ *è un sottospazio dello spazio vettoriale* $\mathfrak{M}_{n1}(K)$ *di dimensione* $n - \rho(A)$.

Dimostrazione — Per il teorema 8.6.6 l'insieme V delle soluzioni è un sottospazio di $\mathfrak{M}_{n1}(K)$. Per calcolare la dimensione di V useremo il secondo

teorema di unicità. Riscriviamo il sistema $AX = 0$ come segue: Sia $\Sigma = \begin{cases} A_1X = 0 \\ A_2X = 0 \\ \vdots \\ A_mX = 0 \end{cases}$.

Chiaramente tale sistema è compatibile. Poniamo $p = \rho(A) = \rho(\bar{A})$. Senza ledere le generalità supponiamo che una sottomatrice fondamentale sia costituita dalle prime p righe e dalle prime p colonne: $A^{\{1,2,\ldots,p\}}_{\{1,2,\ldots,p\}}$ sottomatrice fondamentale di $A = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{pmatrix}$. Allora per il secondo teorema di unicità il sistema assegnato è equivalente al sistema $\Sigma' = \begin{cases} A_1X = 0 \\ A_2X = 0 \\ \vdots \\ A_pX = 0 \end{cases}$. Inoltre per ogni scelta dei parametri $k_1, \ldots k_{n-p}$ sulle incognite individuate dalle colonne $\{p+1, p+2, \ldots, n\}$ rimane definito un sistema di p equazioni in p incognite che ammette un'unica soluzione. Per le $(n-p)$-ple $(k_1, \ldots k_{n-p})$ consideriamo le seguenti $n-p$ scelte:

$$\begin{aligned} (k_1, \ldots, k_{n-p}) &= (1, 0, \ldots, 0) \\ (k_1, \ldots, k_{n-p}) &= (0, 1, \ldots, 0) \\ &\vdots \\ (k_1, \ldots, k_{n-p}) &= (0, 0, \ldots, 1) \end{aligned}.$$

In corrispondenza di tali scelte otterremo $n-p$ soluzioni del tipo:

$$v_1 = \begin{pmatrix} c_{1,1} \\ c_{1,2} \\ \vdots \\ c_{1,p} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} c_{2,1} \\ c_{2,2} \\ \vdots \\ c_{2,p} \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, v_{n-p} = \begin{pmatrix} c_{n-p,1} \\ c_{n-p,2} \\ \vdots \\ c_{n-p,p} \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Per ogni scelta $\alpha_1, \ldots, \alpha_{n-p}$ di scalari in K, il vettore $\sum_{i=1}^{n-p} \alpha_i \cdot v_i$ è del tipo $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_p \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-p} \end{pmatrix}$, dove $a_1, \ldots a_p$ sono opportuni scalari in K. In particolare se $\sum_{i=1}^{n-p} \alpha_i \cdot v_i = 0$ allora ciascun $\alpha_i = 0$, sicché i vettori $v_1, \ldots, v_{n-p}$ sono indipendenti. Sia ora $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_p \\ c_{p+1} \\ \vdots \\ c_n \end{pmatrix}$ una soluzione del sistema Σ.

Allora la combinazione lineare $\sum_{i=1}^{n-p} c_{p+i} \cdot v_i$ è del tipo $\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_p \\ c_{p+1} \\ \vdots \\ c_n \end{pmatrix}$, dove $d_1, \ldots, d_p$ sono opportuni scalari. D'altra parte $\sum_{i=1}^{n-p} c_{p+i} \cdot v_i$ è soluzione di Σ, e per il secondo teorema di unicità in corrispondenza della scelta dei valori $c_{p+1}, \ldots, c_n$ esiste un' unica soluzione di Σ, pertanto $d_1 = c_1, \ldots, d_p = c_p$. Questo prova che la generica soluzione di Σ è combinazione lineare dei vettori $v_1, \ldots, v_{n-p}$.

In questo modo abbiamo provato che lo spazio V delle soluzioni del sistema $AX = 0$ ha dimensione $n - p$. □

Nella dimostrazione precedente è stato utile rappresentare le soluzioni del sistema come colonne. Osserviamo invece che spesso esse si rappresentano come vettori numerici di K^n, anziché come vettori colonne dello spazio $\mathfrak{M}_{n1}(\mathbb{K})$.

Esempio 8.8.8 $\Sigma = \begin{cases} x_1 + x_2 + x_3 + x_4 = 1 \\ 2x_1 + \quad + x_4 = 1 \\ x_1 - x_2 - x_3 \quad = 0 \\ 3x_1 + 2x_2 + 2x_3 + 2x_4 = 2 \end{cases}$. Sistema di quattro equazioni in quattro incognite sul campo $\mathbb{R}$, allora le matrici associate sono:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 1 \\ 1 & -1 & -1 & 0 \\ 3 & 2 & 2 & 2 \end{pmatrix} \in \mathfrak{M}_{44}(\mathbb{R}), \text{ e } \bar{A} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 1 & 1 \\ 1 & -1 & -1 & 0 & 0 \\ 3 & 2 & 2 & 2 & 2 \end{pmatrix} \in \mathfrak{M}_{45}(\mathbb{R}).$$

Chiaramente A è degenere, e la sottomatrice $\bar{A}^{\{1,3,4,5\}}_{\{1,2,3,4\}}$ di $\bar{A}$ di ordine quattro che "contiene" $A^{\{1,3,4\}}_{\{1,2,4\}}$ è anch'essa degenere. Da ciò segue che che $A^{\{1,3,4\}}_{\{1,2,4\}}$ è una matrice fondamentale di A, e $\rho(A) = \rho(\bar{A}) = 3$. Pertanto il sistema è compatibile. Allora per il II teorema di Unicità

Σ è equivalente al sistema $\begin{cases} x_1 + x_2 + x_3 + x_4 = 1 \\ 2x_1 + \quad + x_4 = 1 \\ 3x_1 + 2x_2 + 2x_3 + 2x_4 = 2 \end{cases}$, e

$\forall k \in \mathbb{R}$ il sistema $\begin{cases} x_1 + x_3 + x_4 = 1 - k \\ 2x_1 + \quad + x_4 = 1 \\ 3x_1 + 2x_3 + 2x_4 = 2 - 2k \end{cases}$ ammette un'unica soluzione.

Risolvendo secondo la regola di Cramer si ha che l'insieme delle soluzioni è descritto dalle seguenti quaterne:

$$(\frac{\det\begin{pmatrix} 1-k & 1 & 1 \\ 1 & 0 & 1 \\ 2-2k & 2 & 2 \end{pmatrix}}{\det(A^{\{1,3,4\}}_{\{1,2,4\}})}, k, \frac{\det\begin{pmatrix} 1 & 1-k & 1 \\ 2 & 1 & 1 \\ 3 & 2-2k & 2 \end{pmatrix}}{\det(A^{\{1,3,4\}}_{\{1,2,4\}})}, \frac{\det\begin{pmatrix} 1 & 1 & 1-k \\ 2 & 0 & 1 \\ 3 & 2 & 2-2k \end{pmatrix}}{\det(A^{\{1,3,4\}}_{\{1,2,4\}})}).$$

Esempio 8.8.9 $\Sigma = \begin{cases} x_1 + x_2 + x_3 = 1 \\ 2x_1 + \quad + x_3 = 1 \\ 2x_1 + \quad + x_3 = 0 \\ 9x_1 + 2x_2 + 2x_3 = 1 \end{cases}$. Sistema di quattro equazioni in tre incognite sul campo $\mathbb{R}$, allora le matrici associate sono:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & 1 \\ 2 & 0 & 1 \\ 9 & 2 & 2 \end{pmatrix} \in \mathfrak{M}_{43}(\mathbb{R}), \text{ e } \bar{\mathbf{A}} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 1 \\ 2 & 0 & 1 & 0 \\ 9 & 2 & 2 & 1 \end{pmatrix} \in \mathfrak{M}_{44}(\mathbb{R}).$$

Si verifica che il determinante di $A^{\{1,2,3\}}_{\{1,2,4\}}$ è 7, e quindi tale sottomatrice è una matrice fondamentale di A. L'unica sottomatrice di $\bar{\mathbf{A}}$ di ordine quattro che "contiene" $A^{\{1,2,3\}}_{\{1,2,4\}}$ è $\bar{\mathbf{A}}$ che pero' non è degenere. Pertanto $\rho(A) \neq \rho(\bar{\mathbf{A}})$ ed il sistema non è compatibile.

Osserviamo che il sistema Σ dell'esempio precedente, anche riguardato come sistema su $\mathbb{Z}_7$ non è compatibile, dal momento che $\rho(A) = 2$ e $\rho(\bar{A}) = 3$

8.9 AUTOVALORI DI UNA MATRICE E RELATIVI AUTOSPAZI

Assegnata una matrice $A \in \mathfrak{M}_{nn}(K)$ il determinante della matrice $A - x\mathfrak{I}$ risulta essere un polinomio di grado n. Tale polinomio si chiama *polinomio caratteristico di A*, e si denota col simbolo $p_A(x)$.

Le radici in K del polinomio $p_A(x)$ si dicono *autovalori* di A. Per ciascun autovalore λ del polinomio $p_A(x)$ il sistema lineare omogeneo $(A - \lambda\mathfrak{I})X = 0$ ammette soluzioni non banali, e ciascuna di esse si dice *autovettore di* λ. L'insieme V_λ costituito dal vettore nullo e da tutti gli autovettori di λ si chiama *autospazio relativo a* λ, e si denota col simbolo V_λ. Dallo studio sui sistemi lineari, possiamo dire che V_λ è un sottospazio di K^n. La sua dimensione $g_\lambda = \dim V_\lambda$ si chiama *molteplicità geometrica* di λ, e per quanto già visto coincide con $n - \rho(A - \lambda\mathfrak{I})$. Per fissare meglio le definizioni appena date faremo un esempio:

Esempio 8.9.1 Sia $B = \begin{pmatrix} \frac{5}{2} & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{13}{2} & -15 \\ 2 & 2 & -5 \end{pmatrix} \in \mathfrak{M}_{33}(\mathbb{R})$.

Per determinare il polinomio caratteristico $p_B(x)$ di B bisogna considerare la matrice $B - x\mathfrak{I} = \begin{pmatrix} \frac{5}{2} - x & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{13}{2} - x & -15 \\ 2 & 2 & -5 - x \end{pmatrix}$, dove notiamo che tra i coefficienti compaiono anche polinomi. Eseguendo i calcoli si ha: $p_B(x) = \det(B - x\mathfrak{I}) =$

$= (\frac{5}{2} - x)[(\frac{13}{2} - x)(-5 - x) + 30] - \frac{1}{2}[\frac{9}{2}(-5 - x) + 30] - [9 - (13 - 2x)] =$

$= -\frac{65}{4}5 - \frac{65}{4}x + \frac{25}{2}x + \frac{5}{2}x^2 + \frac{65}{2}x + \frac{13}{2}x^2 - 5x^2 - x^3 + 75 - 30x + \frac{9}{4}5 + \frac{9}{4}x - 15 + 4 - 2x = -x^3 + 4x^2 - x - 6.$

Non è difficile verificare che il polinomio $p_B(x)$ ammette come radici gli elementi 2, -1 e 3, che per definizione sono gli autovalori di B.

1) Per determinare l'autospazio V_2 relativo all'autovalore 2 bisogna risolvere il sistema $(B - 2\mathfrak{I})X = 0$. Tenendo conto che

$$\begin{pmatrix} \frac{5}{2} & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{13}{2} & -15 \\ 2 & 2 & -5 \end{pmatrix} - \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{9}{2} & -15 \\ 2 & 2 & -7 \end{pmatrix},$$

si ha che il sistema da studiare è

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{9}{2} & -15 \\ 2 & 2 & -7 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

La sottomatrice $\begin{pmatrix} \frac{9}{2} & -15 \\ 2 & -7 \end{pmatrix}$ non è degenere, quindi risulta essere una sottomatrice fondamentale della matrice degenere $(B - 2\mathfrak{I}) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{9}{2} & -15 \\ 2 & 2 & -7 \end{pmatrix}$.

Allora il sistema da studiare è equivalente al sistema

$$\begin{cases} \frac{9}{2}x_1 + \frac{9}{2}x_2 - 15x_3 = 0 \\ 2x_1 + 2x_2 - 7x_3 = 0 \end{cases}.$$

Una soluzione è (1,-1,0), e l'autospazio relativo all'autovalore 2 è $\langle (1,-1,0) \rangle = \{(k,-k,0) : \ k \in \mathbb{R}\}$.

2) Per determinare l'autospazio V_{-1} relativo all'autovalore -1 bisogna risolvere il sistema $(B - (-1)\mathfrak{I})X = 0$. Quindi il sistema da considerare è:

$$\begin{pmatrix} \frac{7}{2} & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{15}{2} & -15 \\ 2 & 2 & -4 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

La sottomatrice $\begin{pmatrix} \frac{9}{2} & \frac{15}{2} \\ 2 & 2 \end{pmatrix}$ non è degenere, quindi risulta essere una sottomatrice fondamentale della matrice $B - (-1)\mathfrak{I}$,

Allora il sistema da studiare è equivalente al sistema

$$\begin{cases} \frac{9}{2}x_1 + \frac{15}{2}x_2 - 15x_3 = 0 \\ 2x_1 + 2x_2 - 4x_3 = 0 \end{cases}$$

Per come si è scelta la sottomatrice fondamentale, bisogna assegnare un parametro sulla terza incognita. Risolvendo si ottiene che la generica soluzione è del tipo $(0, 2k, k)$.

3) Per determinare l'autospazio V_3 relativo all'autovalore 3 bisogna risolvere il sistema $(B - 3\mathfrak{I})X = 0$. Quindi il sistema da considerare è:

$$\begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{7}{2} & -15 \\ 2 & 2 & -8 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$ Risolvendo si ottiene che l'autospazio relativo a 3 è: $\langle (k, 3k, k) \rangle = \{(k, 3k, k) : \ k \in \mathbb{R}\}$.

Osserviamo che nell'esempio precedente il numero degli autovalori di B coincide con l'ordine della matrice B, o ciò che è lo stesso le radici del polinomio caratteristico sono a due a due distinte.

Esercizio 8.9.2 Il termine noto del polinomio caratteristico di una matrice (quadrata) coincide col suo determinante.

Esercizio 8.9.3 Definire una matrice quadrata A di ordine 3 a coefficienti reali con due soli autovalori.

Esercizio 8.9.4 Siano λ_1 e λ_2 autovalori. Allora $V_{\lambda_1} \cap V_{\lambda_2} = \{0\}$.

Siano A e B matrici quadrate di ordine n a coefficienti in K. Diremo che A e B sono *coniugate* se $B = P^{-1}AP$ per un opportuna matrice non degenere $P \in \mathfrak{M}_{nn}(K)$.

Esercizio 8.9.5 Studiare la relazione di coniugio in $GL(n, K)$.

Proposizione 8.9.6 *Siano A e B matrici quadrate di ordine n a coefficienti in K. Se A e B sono coniugate allora hanno lo stesso polinomio caratteristico.*

Dimostrazione – Poniamo $B = P^{-1}AP$, con $P \in \mathfrak{M}_{nn}(K)$ e $\det(P) \neq 0$. Dalle definizioni abbiamo $p_B(x) = \det(B - x\mathfrak{I}) = \det(P^{-1}AP - x\mathfrak{I}) = \det(P^{-1}AP - P^{-1}x\mathfrak{I}P) = \det(P^{-1}(A - x\mathfrak{I})P)$. Per il teorema di Binet abbiamo $p_B(x) = \det(P^{-1}) \cdot \det(A - x\mathfrak{I}) \cdot \det(P) = (\det(P))^{-1}\det(A - x\mathfrak{I})\det(P) = \det(A - x\mathfrak{I}) = p_A(x)$. □

Ricordiamo che assegnati $V_1, \ldots V_t$ sottospazi di uno spazio vettoriale V, lo spazio somma $V_1 + \ldots + V_t$ è una *somma diretta* e si denota col simbolo $V_1 \oplus \ldots \oplus V_t$, se ciascun vettore v di $V_1 + \ldots + V_t$ si esprime in unico modo come somma del tipo $v = v_1 + \ldots + v_t$ con ciascun $v_i \in V_i$.

Teorema 8.9.7 *Sia K un campo e sia $A \in \mathfrak{M}_{nn}(K)$ una matrice quadrata di ordine n, e siano $\lambda_1, \ldots, \lambda_t$ gli autovalori di A. Allora $V_{\lambda_1} + \ldots + V_{\lambda_t} = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_t}$.*

Dimostrazione – Se $t = 1$ l'asserto è ovvio. Sia $t > 1$ e procediamo per induzione.

Sia C un vettore che giace nell'intersezione $V_{\lambda_1} \bigcap (V_{\lambda_2} + \ldots + V_{\lambda_t})$. Per provare la tesi è sufficiente provare che $C = 0$. Chiaramante C è soluzione del sistema $(A - \lambda_1\mathfrak{I})X = 0$, e si espime come somma del tipo $C = C_2 + \ldots + C_t$, con $C_i \in V_{\lambda_i}$, per ogni $i \geqslant 2$. Allora $AC = A(C_2 + \ldots + C_t) = AC_2 + \ldots + AC_t = \lambda_2\mathfrak{I}C_2 + \ldots + \lambda_t\mathfrak{I}C_t = \lambda_2C_2 + \ldots + \lambda_tC_t$. D'altra parte $AC = \lambda_1C = \lambda_1(C_2 + \ldots + C_t) = \lambda_1C_2 + \ldots + \lambda_1C_t$. Sottarendo riusciamo ad esprimere il vettore nullo come somma del tipo: $(\lambda_2 - \lambda_1)C_2 + \ldots + (\lambda_t - \lambda_1)C_t$. Per ipotesi induttiva $V_{\lambda_2} + \ldots + V_{\lambda_t} = V_{\lambda_2} \oplus \ldots \oplus V_{\lambda_t}$, quindi ciascun addendo $(\lambda_2 - \lambda_1)C_2, \ldots, (\lambda_t - \lambda_1)C_t$ coincide col vettore nullo, ed essendo gli autovalori $\lambda_1, \ldots, \lambda_t$ distinti, necessariamente gli autovettori $C_2, \ldots C_t$ devono essere tutti nulli. Allora anche $C = 0$. □

8.10 DIAGONALIZZAZIONE DI UNA MATRICE

Una matrice quadrata si dice *diagonale* se ogni elemento che non giace sulla diagonale principale è nullo. La matrice identica e la matrice nulla sono particolari esempi di matrici diagonali. Una matrice $A \in \mathfrak{M}_{nn}(K)$ si dice *diagonalizzabile* se esiste una matrice invertibile P tale che $P^{-1}AP$ è diagonale.

Ma come si fa a riconoscere se una matrice è diagonalizzabile?

Ad esempio non sembra immediato evincere la diagonalizzabilità della matrice $B = \begin{pmatrix} \frac{5}{2} & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{13}{2} & -15 \\ 2 & 2 & -5 \end{pmatrix} \in \mathfrak{M}_{33}(\mathbb{R})$, in quanto appare difficile individuare una matrice P invertibile tale che $P^{-1}BP$ sia diagonale. Il seguente teorema, di cui riportiamo solo l'enunciato, risolve completamente questo problema. In esso troviamo una caratterizzazione delle matrici diagonalizzabili:

Teorema 8.10.1 (DI CARATTERIZZAZIONE DELLE MATRICI DIAGONALIZZABILI) *Sia K un campo e sia $A \in \mathfrak{M}_{nn}(K)$ una matrice quadrata di ordine n, e siano $\lambda_1, \ldots, \lambda_t$ gli autovalori di A. Allora A è diagonalizzabile se e solo se $g_{\lambda_1} + \ldots + g_{\lambda_t} = n$.*

Per stabilire se una matrice A quadrata di ordine n è diagonalizzabile bisogna:

1)Determinare gli autovalori di A;

2)Risolvere i sistemi lineari che individuano gli autospazi.

Se la somma delle molteplicità geometriche relative agli autovalori di A è esattamente n allora la matrice A è diagonalizzabile.

In tal caso, per determinare una matrice P in modo tale che $P^{-1}AP$ sia diagonale bisogna semplicemente considerare una base in ciascun autospazio. Poiché la somma delle dimensioni degli autospazi è proprio n, si ottengono esattamente n vettori numerici di K^n. Disponendo in colonna tali vettori si ottiene una matrice P cercata. Vediamo con un esempio:

Esempio 8.10.2 Sia $B = \begin{pmatrix} \frac{5}{2} & \frac{1}{2} & -1 \\ \frac{9}{2} & \frac{13}{2} & -15 \\ 2 & 2 & -5 \end{pmatrix} \in \mathfrak{M}_{33}(\mathbb{R})$. Abbiamo visto nel paragrafo precedente che gli autovalori sono 2, -1, 3 e che gli autospazi relativi sono tutti unidimensionali, ossia $g_2 = g_{-1} = g_3 = 1$. Quindi la somma delle dimensioni

degli autospazi coincide con l'ordine della matrice B, e per il Teorema 8.10.1 B è diagonalizzabile.

Come abbiamo già verificato una base di V_2 è il vettore $(1,-1,0)$, mentre una base di V_{-1} è $(0,2,1)$ e una base di V_3 è $(1,3,1)$. Posta $P = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 3 \\ 0 & 1 & 1 \end{pmatrix} \in \mathfrak{M}_{33}(\mathbb{R})$ si ha che $P^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 1 \\ -\frac{1}{2} & -\frac{1}{2} & 2 \\ \frac{1}{2} & \frac{1}{2} & -1 \end{pmatrix}$ e si può verificare che $P^{-1}BP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$.

Dal procedimento esposto si evince che la matrice P si può individuare in più modi. Infatti oltre a non essere rilevante l'ordine con cui si scrivono gli autovalori di B, non c'è alcuna preferenza nella scelta dei vettori che descrivono una base di ciascun autospazio.

Inoltre rileviamo che sulla diagonale della matrice diagonalizzata troviamo proprio gli autovalori di B.

Se invece la somma delle molteplicità geometriche degli autovalori della matrice $A \in \mathfrak{M}_{nn}(K)$ è inferiore ad n, allora la matrice non è diagonalizzabile. Ciò accade se e solo se la molteplicità geometrica di almeno un autovalore di A è strettamente minore della sua molteplicità algebrica (come radice di $p_A(x)$).

Poiché un autospazio ha almeno dimensione uno, possiamo concludere affermando che le matrici di ordine n che posseggono n autovalori distinti sono sempre diagonalizzabili.

Esercizio 8.10.3 Determinare una matrice di ordine 3, che sia diagonalizzabile e con due soli autovalori.

Esercizio 8.10.4 È possibile trovare una matrice di ordine 3, con un autovalore nullo e che non risulti essere diagonalizzabile?

BIBLIOGRAFIA

[1] W. M. Baldoni, C. Ciliberto, G. M. Piacentini Cattaneo "Aritmetica, crittografia e codici", *Springer*, Milano, (2006).

[2] L. Childs, "Algebra", *ETS*, Pisa, (1989).

[3] J. H. Conway, R. K. Guy, "the book of numbers", *Springer-Verlag*, New York, (1996).

[4] M. Curzio, P. Longobardi, M. Maj, " Lezioni di Algebra", *Liguori*, Napoli, (1994).

[5] C. Delizia, P. Longobardi, M. Maj, C. Nicotera "Matematica Discreta", *Mc Graw-Hill*, (2009)

[6] D. Dikranjan, M.S. Lucido, "Aritmetica e Algebra", *Liguori*, Napoli, (2007).

[7] A. Facchini, "Algebra e Matematica Discreta", *Zanichelli*, Bologna, (2010).

[8] S. Franciosi, F. de Giovanni, "Elementi di Algebra", *Aracne*, Roma, (1992).

[9] G. M. Piacentini Cattaneo, "Matematica Discreta e applicazioni", *Zanichelli*, Bologna,(2008).

ALGORITMICA

COLLANA DI MATEMATICA E INFORMATICA

1. Francesco Catino, Francesco de Giovanni
Some Topics in the Theory of Groups with Finite Conjugacy Classes
isbn 978-88-548-8116-7, formato 17 × 24 cm, 120 pagine, 8 euro

2. Giovanni Vincenzi
Algebra per Informatica
isbn 978-88-548-8225-6, formato 17 × 24 cm, 172 pagine, 12 euro

Compilato il 11 febbraio 2015, ore 06:58
con il sistema tipografico LaTeX 2_ϵ

Finito di stampare nel mese di febbraio del 2015
dalla «Ermes. Servizi Editoriali Integrati S.r.l.»
00040 Ariccia (RM) – via Quarto Negroni, 15
per conto della «Aracne editrice int.le S.r.l.» di Ariccia (RM)