

INSIEMI E RELAZIONI

1. Insiemi e operazioni su di essi

Il concetto di *insieme* è primitivo ed è sinonimo di *classe*, *totalità*.

Sia A un insieme di elementi qualunque. Per indicare che a è un elemento di A scriveremo $a \in A$.

Se A, B sono insiemi, diremo che A è un *sottoinsieme* di B e scriveremo $A \subseteq B$ se ogni elemento di A è un elemento di B . Fra i sottoinsiemi di B ci sono in particolare B stesso e l' *insieme vuoto* che viene denotato con \emptyset .

Due insiemi A e B si dicono *uguali*, $A = B$, se hanno gli stessi elementi cioè se:

$$A \subseteq B \text{ e } B \subseteq A \Leftrightarrow A = B.$$

Diremo che un sottoinsieme A di B è *proprio*, se $A \neq B$ e scriveremo $A \subset B$;

Se A è un insieme, denoteremo con $P(A)$ l' insieme i cui elementi sono i sottoinsiemi di A ; $P(A)$ si dice l' *insieme delle parti* di A .

Se A, B sono insiemi, diremo *unione* di A e B l'insieme costituito dagli elementi che stanno in A oppure in B , $A \cup B = \{x : x \in A \text{ o } x \in B\}$, diremo *intersezione* di A e B l' insieme costituito dagli elementi comuni ad A e B , $A \cap B = \{x : x \in A \text{ e } x \in B\}$, mentre diremo *differenza* di A e B l'insieme degli elementi di A che non sono elementi di B , $A - B = A \setminus B = \{x : x \in A \mid x \notin B\}$.

Due insiemi si dicono *disgiunti* se la loro intersezione è l'insieme vuoto.

Se A è sottoinsieme di B diremo *complementare* (o *complemento*) di A in B l'insieme $B - A$ e lo denoteremo con $C_B A$.

Se B è l'*insieme ambiente* il complementare di A in B verrà semplicemente denotato con $C A$.

Se A, B sono insiemi, definiamo *prodotto cartesiano* di A e B e lo denoteremo con $A \times B$, l' insieme i cui elementi sono le coppie ordinate (a, b) con $a \in A$ e $b \in B$.

Proprietà:

- 1) $A \cap A = A, A \cup A = A$
- 2) $A \cap B = B \cap A, A \cup B = B \cup A$ (proprietà commutativa)
- 3) $A \cap \emptyset = \emptyset, A \cup \emptyset = A$
- 4) $(A \cap B) \cap C = A \cap (B \cap C), (A \cup B) \cup C = A \cup (B \cup C)$ (proprietà associativa)
- 5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (proprietà distributive dell'intersezione rispetto all'unione)
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (proprietà distributive dell'unione rispetto all'intersezione)
- 6) $C(A \cap B) = CA \cup CB; C(A \cup B) = CA \cap CB$ (Formule di De Morgan)

2. Applicazioni

Siano A, B insiemi. Si dice *applicazione* (o *funzione*) di A in B , e si denota con $f: A \rightarrow B$, una corrispondenza che associa ad ogni elemento $x \in A$ un elemento $f(x) \in B$.

Un' applicazione si dice:

iniettiva (od anche: 1-1) se ad elementi distinti di A corrispondono elementi distinti di B , cioè se

$$\forall x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \text{ o anche da } f(x_1) = f(x_2) \Rightarrow x_1 = x_2;$$

suriettiva (od anche: su tutto) se ogni elemento di B è il corrispondente di qualche elemento di A , cioè se $\forall y \in B, \exists x \in A : y = f(x)$;

biiettiva se è iniettiva e suriettiva; una applicazione biiettiva di A in B è detta pure una *corrispondenza biunivoca* fra A e B .

Sia $f: A \rightarrow B$ un' applicazione; dicesi *immagine* di f e si indica con Imf , il sottoinsieme di B costituito dagli elementi che sono corrispondenti di qualche elemento di A , cioè:

$$Imf = \{y \in B \mid \exists x \in A \text{ tale che } y = f(x)\}.$$

Chiaramente f è suriettiva se e solo se $Imf = B$.

Esempi:

- 1) $f: \mathbb{N} \rightarrow \mathbb{R}, n \rightarrow 1/n-1$ non è un' applicazione perché non esiste $f(1)$.
- 2) Sia $M = \{\text{esseri umani}\}$; $f: M \rightarrow M$, ad ogni essere umano \rightarrow un genitore. Non è una applicazione perché non è ben definito il corrispondente (padre o madre) di un elemento di M .

3) $f: \mathbb{Q} \rightarrow \mathbb{Z}$ $m/n \rightarrow m+n$; $\mathbb{Q} = \{m/n, m, n \in \mathbb{N}, n \neq 0 \text{ e la frazione è ridotta ai minimi termini}\}$ è un'applicazione.

E' iniettiva? No! $2/3 \neq 3/2 \Rightarrow f(2/3) \neq f(3/2)$.

E' suriettiva? No! Lo 0 non proviene da alcun elemento di \mathbb{Q} .

4) $i_A: A \rightarrow A \quad \forall x \in A \quad i(x) = x$ dicesi applicazione *identica* o *unità*, essa è iniettiva e suriettiva pertanto è biiettiva.

5) $f: \mathbb{N} \rightarrow \mathbb{N} \quad n \rightarrow n+1$ è un'applicazione iniettiva ma non suriettiva perché lo 0 non proviene da nessun elemento.

Prodotto di applicazioni. Siano $f: A \rightarrow B$, $g: B \rightarrow C$ applicazioni. Si definisce *prodotto* o *composizione* di f , g , l'applicazione di A in C ottenuta applicando successivamente prima f e poi g ; essa viene denotata con $g \circ f$ ed è definita da $(g \circ f)(x) = g(f(x)) \quad \forall x \in A$.

Il prodotto di applicazioni gode della *proprietà associativa* cioè per $f: A \rightarrow B$, $g: B \rightarrow C$, $h: C \rightarrow D$ si ha:

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Se l'applicazione $f: A \rightarrow B$ è biiettiva allora si può definire l'applicazione inversa $f^{-1}: B \rightarrow A$ come segue: $\forall y \in B$, $f^{-1}(y)$ è l'unico elemento $x \in A$ tale che $f(x) = y$.

Chiaramente è: 1) $f \circ f^{-1} = i_B$, 2) $f^{-1} \circ f = i_A$, 3) $(f^{-1})^{-1} = f$.

Sulla composizione di due applicazioni si hanno vari risultati, alcuni dei quali sono richiamati nelle seguenti due proposizioni.

Proposizione 1: Siano $f: A \rightarrow B$, $g: B \rightarrow C$ applicazioni. Allora

- (1) se f e g sono iniettive $\mathbf{P} \quad g \circ f$ è iniettiva,
- (2) se f e g sono suriettive $\mathbf{P} \quad g \circ f$ è suriettiva,
- (3) se f e g sono biettive $\mathbf{P} \quad g \circ f$ è biiettiva,
- (4) se $g \circ f$ è suriettiva $\mathbf{P} \quad g$ è suriettiva,
- (5) se $g \circ f$ è iniettiva $\mathbf{P} \quad f$ è iniettiva,
- (6) se $g \circ f$ è biettiva $\mathbf{P} \quad f$ è iniettiva e g è suriettiva.

Proposizione 2: Siano $f: A \rightarrow B$, $g: B \rightarrow A$ applicazioni, e inoltre $f \circ g = i_B$ e $g \circ f = i_A$ allora f e g sono entrambe biiettive e $g = f^{-1}$.

Dati due insiemi A e B possiamo considerare un nuovo insieme, denotato con B^A , costituito da tutte le applicazioni di A in B . Un caso particolarmente importante è il caso in cui $B = \{0,1\}$ è l'insieme costituito da due elementi $0,1$; denoteremo tale insieme con il simbolo $\underline{2}$.

Se $f \in \underline{2}^A$ cioè se $f: A \rightarrow \{0,1\}$ allora $\forall x \in A$ si ha $f(x) = 0$ oppure $f(x) = 1$

Se A è un insieme, per ogni suo sottoinsieme I , $I \subseteq A$, possiamo definire un'applicazione $f_I: A \rightarrow \{0,1\}$ che caratterizza gli elementi di I , detta *funzione caratteristica di I* nel seguente modo:

$$f_I: A \rightarrow \{0,1\} \quad f_I(x) = \begin{cases} 0 & \text{se } x \notin I \\ 1 & \text{se } x \in I \end{cases}$$

Chiaramente è: $f_A: A \rightarrow \{0,1\}$ $f_A(x) = 1 \forall x \in A$ e $f_\emptyset: A \rightarrow \{0,1\}$ $f_\emptyset(x) = 0 \forall x \in A$.

Teorema Sia A un insieme. Esiste una corrispondenza biunivoca fra gli insiemi $\underline{2}^A$ e $P(A)$.

Dimostrazione. Definiamo due applicazioni φ, ψ come segue. $\varphi: \underline{2}^A \rightarrow P(A)$ associa ad ogni applicazione $f: A \rightarrow \underline{2}$ il sottoinsieme di A costituito dagli elementi $x \in A$ tali che $f(x) = 1$.

$\psi: P(A) \rightarrow \underline{2}^A$ associa ad ogni sottoinsieme $B \subseteq A$ l'applicazione $f: A \rightarrow \underline{2}$ definita da

$$f(x) = \begin{cases} 0 & \text{se } x \notin B \\ 1 & \text{se } x \in B \end{cases}$$

È facile vedere che $\varphi \circ \psi = 1_{P(A)}$ e $\psi \circ \varphi = 1_{\underline{2}^A}$ e quindi basta applicare la proposizione 2.

Faremo uso del seguente assioma della teoria degli insiemi:

Assioma della scelta o di Zermelo: Sia A un insieme. Esiste allora una applicazione che ad ogni sottoinsieme non vuoto $B \subseteq A$ associa un elemento appartenente a B .

3. Potenza di un insieme

Si dice che due insiemi A e B hanno la stessa potenza o sono equipotenti se esiste una corrispondenza biunivoca fra A e B , e si scrive $|A| = |B|$.

Si dice che A ha potenza superiore di B e si scrive $|A| > |B|$ se B è equipotente ad un sottoinsieme di A ed A e B non sono equipotenti.

Un insieme si dice numerabile se ha la stessa potenza dell'insieme dei numeri naturali $\mathbf{N} = \{0, 1, 2, 3, \dots\}$.

Un insieme si dice avere la potenza del continuo se ha la stessa potenza dell'insieme \mathbf{R} dei numeri reali.

Proposizione: $\mathbf{N}, \mathbf{Z}, \mathbf{Q}$, hanno la stessa potenza.

Proposizione: La potenza di \mathbf{N} è minore di quella di \mathbf{R} , cioè $|\mathbf{R}| > |\mathbf{N}|$.

Dimostrazione. Osservato che $\mathbf{N} \subseteq \mathbf{R}$ basta provare che \mathbf{N} ed \mathbf{R} non sono equipotenti.

Supponiamo per assurdo che \exists la biiezione $f: \mathbf{N} \rightarrow \mathbf{R}$ così definita:

$$f(0) = \pm a_0, c_{01}c_{02}c_{03} \dots c_{0n} \dots$$

$$f(1) = \pm a_1, c_{11}c_{12}c_{13} \dots c_{1n} \dots$$

$$\dots \dots \dots$$

$$f(n) = \pm a_n, c_{n1}c_{n2}c_{n3} \dots c_{nn} \dots$$

Numeri reali in forma di numeri decimali illimitati non periodici di periodo 9

Considerato il numero $\alpha = 0, c_0 c_1 \dots c_n \dots$ con $c_0 \neq 9$ e $\neq c_{01}$, $c_1 \neq 9$ e $\neq c_{12}$, $c_2 \neq 9$ e $\neq c_{23}, \dots, c_n \neq 9$ e $\neq c_{nn} \dots$ si ha che $\forall n \in \mathbf{N} f(n) \neq \alpha$. Assurdo perché avevamo supposto $|\mathbf{N}| = |\mathbf{R}|$.

Proposizione: Per ogni insieme A è $|A| < |P(A)| = |2^A|$.

Dimostrazione. Anzitutto $P(A)$ contiene il sottoinsieme costituito dalle parti di A che possiedono un solo elemento e quindi otteniamo una applicazione iniettiva di A in questo sottoinsieme di $P(A)$. Proviamo adesso che non può esistere un' applicazione suriettiva di A in $P(A)$, e quindi A e $P(A)$ non sono equipotenti. Supponiamo per assurdo che esista una applicazione suriettiva $f: A \rightarrow P(A)$; per ogni elemento $a \in A$ consideriamo il sottoinsieme $f(a) \in P(A)$ e sia $B = \{a \in A \mid a \notin f(a)\}$; B è un sottoinsieme di A e quindi, per la suriettività di f esiste $b \in A$ tale che $f(b) = B$. Due casi sono possibili: $b \in f(b)$ allora per definizione deve essere $b \notin B$ oppure $b \notin f(b)$ allora per definizione $b \in B$; in entrambi i casi si ha l' assurdo.

Proposizione: Sia A un insieme numerabile. Allora $A \times A$ è pure numerabile.

Dimostrazione. Poiché A è numerabile possiamo numerare i suoi elementi $A = \{a_1, a_2, a_3, \dots\}$; disponiamo gli elementi di $A \times A$ nel quadro:

$(a_1, a_1), (a_1, a_2), (a_1, a_3), \dots$
 $(a_2, a_1), (a_2, a_2), (a_2, a_3), \dots$
 $(a_3, a_1), (a_3, a_2), (a_3, a_3), \dots$
 $\dots\dots\dots$

e stabiliamo la corrispondenza $f: \mathbf{N} \rightarrow A \times A$ come segue:

$$f(1) = (a_1, a_1), f(2) = (a_1, a_2), f(3) = (a_2, a_1), f(4) = (a_1, a_3), f(5) = (a_2, a_2), f(6) = (a_3, a_1), \dots$$

e così via secondo il cosiddetto metodo diagonale di Cantor.

Un insieme si dice finito se è vuoto oppure è equipotente all'insieme $\{1, 2, 3, \dots, n\}$ formato dai primi n numeri naturali, per qualche $n \in \mathbf{N}$. Un insieme non finito si dice infinito.

Proposizione: Sia A un insieme. Le seguenti condizioni sono equivalenti:

- (i) A è infinito.
- (ii) A possiede un sottoinsieme numerabile.
- (iii) A è equipotente ad un suo sottoinsieme proprio.

Dimostrazione. (i) \Rightarrow (ii) A non è vuoto; sia a_1 un elemento di A ; è $\{a_1\} \neq A$ perché A è infinito e sia $a_2 \neq a_1, a_2 \in A$; è $\{a_1, a_2\} \neq A$ e sia $a_3 \neq a_1, a_2, a_3 \in A$ e così via costruiamo un sottoinsieme numerabile $\{a_1, a_2, a_3, \dots\} \subseteq A$.

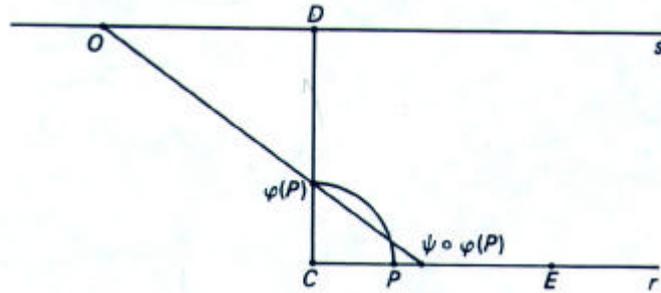
Osserviamo che in questa prova si è fatto uso dell'assioma di Zermelo.

(ii) \Rightarrow (iii) Sia $N \subseteq A$ un sottoinsieme numerabile; indichiamo con a_1, a_2, \dots gli elementi di N ; consideriamo il seguente sottoinsieme A' di A , $A' = (A - N) \cup \{a_2, a_4, a_6, \dots\}$.

Si ha $A' \neq A$ perché $a_1 \notin A'$ ed inoltre A' è equipotente ad A : basta infatti considerare l'applicazione $f: A' \rightarrow A$ definita da $f(x) = x$ se $x \in A - N$ ed $f(a_{2n}) = a_n$ per $n = 1, 2, \dots$

(iii) \Rightarrow (i) Un insieme finito non è equipotente ad un suo sottoinsieme proprio. Tale fatto, che sembra piuttosto evidente, può essere facilmente dimostrato mediante induzione.

Diamo un esempio di un insieme che si può mettere in corrispondenza biunivoca con un suo sottoinsieme proprio.



Siano: r una semiretta, CE un segmento su r , CD un segmento perpendicolare ad r e tale che $CD = CE$ ed s una retta parallela ad r e passante per D . Detti A l'insieme dei punti di CE diversi da E , e B l'insieme dei punti di CD diversi da D , per ogni punto $P \in A$, la circonferenza di centro C e raggio CP interseca CD in un punto $\varphi(P)$ e resta così definita un'applicazione $\varphi: A \rightarrow B$ biiettiva.

Proiettando da O i punti di CD diversi da D su r si ottiene una applicazione biiettiva ψ dall'insieme B nell'insieme dei punti di r ; dunque $\psi \circ \varphi$ risulta una applicazione biiettiva dall'insieme dei punti del segmento CE diversi da E nell'insieme dei punti di r .

Ipotesi del continuo: L'ipotesi del continuo afferma che se un insieme infinito A ha potenza minore della potenza del continuo, allora A è numerabile.

E' stato provato che sia l'ipotesi del continuo che la sua negazione sono entrambe compatibili con gli usuali assiomi della teoria degli insiemi.

4. Relazioni di equivalenza

Dicesi *relazione binaria* definita su un insieme A , un sottoinsieme $R \subseteq A \times A$. Se $(a, b) \in R$ scriviamo anche aRb e diciamo che a sta nella relazione R con b .

Esempi di relazioni binarie definite su A sono $A \times A$ stesso e la relazione identica I definita da aIb se e solo se $a = b$.

Si dice che una relazione binaria gode della proprietà :

riflessiva se aRa per ogni $a \in A$,

transitiva se da aRb e bRc segue aRc per $a, b, c \in A$,

antisimmetrica se da aRb e bRa segue $a = b$ per $a, b \in A$,

simmetrica se da aRb segue bRa per $a, b \in A$.

Una relazione binaria definita su un insieme A si chiama *relazione di equivalenza su A* se gode delle proprietà riflessiva, transitiva, simmetrica. Se E è una relazione di equivalenza, invece di aEb scriveremo $a \equiv b (E)$ e leggeremo “ a equivalente a b in E ” o, quando non c’è possibilità di equivoco, scriveremo semplicemente $a \equiv b$ e leggeremo “ a equivalente a b ”.

Dicesi *partizione* di A una famiglia di sottoinsiemi non vuoti di A tale che ogni elemento di A sta in uno ed uno solo dei sottoinsiemi della famiglia. I sottoinsiemi della famiglia si dicono le *classi della partizione*.

Una partizione di A definisce una relazione di equivalenza su A . Basta porre $a \equiv b (E)$ quando a e b stanno nella stessa classe della partizione: infatti si vede subito che E gode delle tre proprietà: riflessiva, transitiva, simmetrica.

Viceversa, una relazione di equivalenza su A definisce una partizione di A .

Infatti per ogni $a \in A$, consideriamo il sottoinsieme $C(a) \subseteq A$ costituito dagli elementi equivalenti ad a , cioè $C(a) = \{x \in A \mid x \equiv a\}$; si vede subito che la famiglia $\{C(a)\}_{a \in A}$ costituisce una partizione di A : infatti $a \in C(a)$ perché $a \equiv a$; inoltre se è pure $a \in C(b)$ si ha $a \equiv b$; se allora x è un elemento qualunque di $C(b)$ è $x \equiv b$ e per le proprietà simmetrica e transitiva $x \equiv a$ cioè $x \in C(a)$ da cui $C(b) \subseteq C(a)$; analogamente $C(a) \subseteq C(b)$. Ne segue che ogni elemento di A sta in una e una sola classe della famiglia $\{C(a)\}_{a \in A}$.

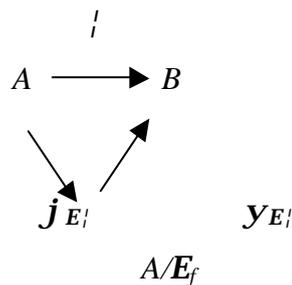
Sia ora E una relazione di equivalenza definita su A . Definiamo insieme *quoziente* di A rispetto ad E e lo denotiamo con A/E , l’insieme che ha come elementi le classi della partizione di A associata ad E , cioè $A/E = \{C(a) \mid a \in A\}$.

Se ad ogni $a \in A$ associamo la classe $C(a)$ cui esso appartiene, otteniamo una applicazione $\varphi_E: A \rightarrow A/E$ detta *applicazione canonica* associata ad E ; si vede subito che φ_E è suriettiva ed è iniettiva se e solo se $E = I$.

Siano dati ora due insiemi A, B ed una applicazione $f: A \rightarrow B$ tra essi, allora si può definire su A una relazione di equivalenza E_f ponendo $a \equiv b (E_f)$ se $f(a) = f(b)$; tale relazione si dice relazione di equivalenza *associata* ad f .

1° Teorema di omomorfismo: Sia $\iota: A \rightarrow B$ una applicazione ed E_f la relazione di equivalenza su A associata ad ι ; sia A/E_f l'insieme quoziente di A rispetto ad E_f e $\mathbf{j}_{E_f}: A \rightarrow A/E_f$ l'applicazione canonica associata ad E_f ; allora:

1) esiste una applicazione $\mathbf{y}_{E_f}: A/E_f \rightarrow B$ tale che il triangolo



commuta, cioè $\iota = \mathbf{y}_{E_f} \circ \mathbf{j}_{E_f}$;

2) l'applicazione $\mathbf{y}_{E_f}: A/E_f \rightarrow B$ è iniettiva;

3) $\text{Im } \iota = \text{Im } \mathbf{y}_{E_f}$; in particolare ι è suriettiva se e solo se \mathbf{y}_{E_f} è suriettiva.

Come conseguenza abbiamo che ogni applicazione f si può scrivere come prodotto di una applicazione suriettiva e di una iniettiva.

5. Relazioni di ordinamento parziale.

Una relazione binaria definita su un insieme A si chiama *relazione di ordinamento parziale* se gode delle proprietà *riflessiva, transitiva, antisimmetrica*. Un insieme A con una relazione R di ordinamento parziale definita su di esso, si chiama insieme *parzialmente ordinato*, brevemente p.o..

Se R è una relazione di ordinamento parziale definita su A , per $a, b \in A$ scriveremo $a \leq b$ invece che aRb e leggeremo “ a minore o uguale a b ”. Se è $a \leq b$ e $a \neq b$ allora scriveremo $a < b$ e leggeremo “ a strettamente minore di b ”.

Sia A un insieme p.o. e $a, b \in A$. Se $a \leq b$ oppure $b \leq a$ allora i due elementi a e b si dicono *confrontabili*. Un insieme p.o. in cui due qualunque elementi sono confrontabili, si dice un insieme *ordinato* o *linearmente ordinato* o *catena*. Un elemento $a \in A$ si dice *minimo* (assoluto) di A se $a \leq x$ per ogni $x \in A$. Il minimo, quando esiste, è unico.

Un elemento $a \in A$ si dice *minimale* o *minimo relativo* di A se non c' è nessun elemento minore o uguale ad a distinto da a stesso cioè se da $x \leq a$ segue $x = a$.

In modo del tutto analogo si danno le nozioni di *massimo* e di *massimo relativo*. Un insieme p.o. si dice *ben ordinato* quando ogni suo sottoinsieme ha il minimo. Un insieme ben ordinato è anche ordinato.

Minoranti e maggioranti; estremo inferiore ed estremo superiore: Sia A un insieme p.o. e B un suo sottoinsieme. Si chiama *minorante* di B in A un elemento $a \in A$ tale che $a \leq x$ per ogni $x \in B$.

Si chiama *estremo inferiore* di B in A il massimo dei minoranti. Notiamo che non è detto che esistano minoranti di B in A e se ne esistono può darsi che il loro insieme non abbia massimo; pertanto l'estremo inferiore non sempre esiste.

L'estremo inferiore a di B in A è caratterizzato dalle seguenti due proprietà:

- (i) $a \in A$ e $a \leq x$ per ogni $x \in B$
- (ii) se $b \in A$ è tale che $b \leq x$ per ogni $x \in B$ allora $b \leq a$.

Osserviamo che se l'estremo inferiore di B in A esiste ed è un elemento di B allora esso è il minimo di B ; viceversa il minimo di B , se esiste, è anche l'estremo inferiore di B in A .

In modo analogo si danno le definizioni di *maggioranti* e di *estremo superiore* di B in A .

Un insieme p.o. si dice *completo* quando ogni suo sottoinsieme ha estremo superiore e estremo inferiore. In particolare un insieme p.o. completo ha minimo e massimo.

Diagrammi di insiemi p.o. finiti: Assegnato un insieme p.o. finito $(A; \leq)$ è utile considerare il *diagramma* di A , ottenuto nel seguente modo. Si disegnano tanti punti quanti sono gli elementi dell'insieme, avendo l'accortezza di disegnare a più in basso di b se $a \leq b$; si congiungono poi due elementi a, b con un segmento se $a < b$ e non ci sono elementi maggiori di a e minori di b . Dal grafico che si ottiene si possono leggere con facilità tutte le proprietà dell'insieme p.o. A .

Condizioni equivalenti all'assioma di Zermelo: Le seguenti condizioni sono equivalenti all'assioma di Zermelo:

- (i) (Teorema di Zermelo). Ogni insieme può essere ben ordinato.
- (ii) (Lemma di Zorn). Se un insieme p.o. A gode della proprietà che ogni catena in esso contenuta ha un maggiorante allora A ha almeno un massimo relativo.

TEORIA DEI NUMERI

1. Numeri naturali, interi relativi e principi d'induzione

Le proprietà dell'insieme $N = \{0, 1, 2, \dots\}$ dei numeri naturali possono essere dedotte dai seguenti **assiomi di Peano**:

1. C'è un'applicazione iniettiva $f: N \rightarrow N$ che ad ogni numero naturale n fa corrispondere il numero naturale n^+ detto il successivo di n .
2. $N - \text{Im}f$ è costituito da un solo elemento denotato con 0.
3. (Assioma di induzione). Se $P \subseteq N$ è tale che $0 \in P$ ed inoltre da $n \in P$ segue $n^+ \in P$ allora $P = N$.

L'assioma 3 permette di dimostrare il **principio di dimostrazione per induzione I**: *Supponiamo che ad ogni numero naturale sia associata una proprietà $P(n)$. Se accade che:*

1. $P(0)$ è vera;
2. $P(n^+)$ è vera ogni qualvolta è vera $P(n)$;

allora $P(n)$ è vera per ogni $n \in N$.

Dimostrazione: Chiamiamo P l'insieme dei numeri n per cui $P(n)$ è vera. Allora per ipotesi abbiamo che $0 \in P$ e che se $n \in P$ allora $n^+ \in P$; per l'assioma 3, l'insieme P coincide con N .

Dall'assioma di induzione segue anche il Principio di definizione per induzione: si applica per definire funzioni $f: N \rightarrow M$, M un insieme qualunque. In base a questo principio la funzione f è perfettamente determinata quando è assegnato il valore $f(0)$ e una regola che permette di determinare $f(n^+)$ conoscendo $f(n)$; usiamo questo principio per definire somma e prodotto in N :

$$\text{Somma} \begin{cases} 0 + m = m \\ n^+ + m = (n + m)^+ \end{cases} \qquad \text{Prodotto} \begin{cases} 0 \cdot m = 0 \\ n^+ \cdot m = n \cdot m + m \end{cases}$$

Si dimostra che per tali operazioni valgono le proprietà associativa, commutativa, di cancellazione, nonché la proprietà distributiva del prodotto rispetto alla somma.

$\forall x, y, z \in \mathbb{N}$	$(x + y) + z = x + (y + z)$	$(xy)z = x(yz)$	<i>proprietà associativa</i>
$\forall x, y \in \mathbb{N}$	$x + y = y + x$	$xy = yx$	<i>proprietà commutativa</i>
$\forall x, y, z \in \mathbb{N}$	$x + y = z + y \Rightarrow x = z;$	$xy = zy \Rightarrow x = z, y \neq 0$	<i>legge di cancellazione</i>
$\forall x, y, z \in \mathbb{N}$	$x(y + z) = xy + xz$		<i>proprietà distributiva del prodotto risp. alla somma</i>

In \mathbb{N} si può definire un ordinamento parziale, detto *ordinamento aritmetico*:

$$a \leq b \text{ se esiste } x \in \mathbb{N} \text{ tale che } b = a + x$$

È immediato verificare le tre proprietà dell'ordinamento parziale.

Teorema: \mathbb{N} è ben ordinato con la relazione di ordinamento aritmetico.

Dimostrazione 1: Sia $S \subseteq \mathbb{N}$, S non vuoto e sia $M = \{m \mid m \leq s \text{ per ogni } s \in S\}$. Si ha $0 \in M$; inoltre se $s \in S$, $s^+ > s$ quindi $s^+ \notin M$. Ne segue che $M \neq \mathbb{N}$. Esiste allora per l'assioma 3, un numero $\bar{m} \in M$, tale che $\bar{m}^+ \notin M$. Allora $\bar{m} \leq s$ per ogni $s \in S$ e $\bar{m} \in S$ perché se fosse $\bar{m} \notin S$ sarebbe $\bar{m} < s$ per ogni $s \in S$ e quindi $\bar{m}^+ \leq s$ per ogni $s \in S$ cioè $\bar{m}^+ \in M$ contro l'ipotesi: \bar{m} è quindi il minimo di S .

Dimostrazione 2: Sia $S \subseteq \mathbb{N}$ un sottoinsieme privo di minimo; vogliamo dimostrare che è vuoto. Consideriamo la proprietà $P(n)$: "Tutti i naturali $\leq n$ non stanno in S "; evidentemente $P(0)$ è vera, altrimenti 0 sarebbe il minimo di S . Supponiamo vera $P(n)$ e dimostriamo $P(n+1)$: quindi tutti i naturali $\leq n$ non stanno in S , e se ci stesse $n+1$ allora esso sarebbe il minimo di S . Quindi è vera $P(n+1)$ e per il Principio d'induzione tutte le $P(n)$ sono vere: segue che S è vuoto.

Indicheremo con $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ l'insieme dei **numeri interi relativi**; si possono definire le operazioni di somma e prodotto tra numeri interi relativi in modo che valgano proprietà analoghe a quelle dei numeri naturali. Il prodotto di zero per un qualunque intero è uguale a zero; il prodotto di due interi relativi non nulli è uguale al prodotto dei loro valori assoluti (come numeri naturali) preso con il segno più o con il segno meno a seconda che abbiano lo stesso segno oppure no; in particolare il prodotto di due numeri diversi da zero è diverso da zero. Tale proprietà si esprime dicendo che in \mathbb{Z} vale la *legge di annullamento del prodotto*.

Osserviamo che l'insieme \mathbb{Z} si può rendere parzialmente ordinato usando la stessa definizione della relazione aritmetica su \mathbb{N} : si vede subito che ogni insieme del tipo $\{x \in \mathbb{Z} \mid a \leq x\}$, $a \in \mathbb{Z}$ fissato, è ancora ben ordinato.

Principio di dimostrazione per induzione II: Sia $\{P(n), n \in \mathbb{N}, n_0 \hat{=} 0\}$ una successione di proposizioni. Supponiamo che:

1. $P(n_0)$ è vera;
2. se $P(m)$ è vera per $n_0 \leq m < n$ allora $P(n)$ è vera;

allora tutte le proposizioni $P(n)$ sono vere per ogni $n \in \mathbb{N}$.

Teorema: Il Principio di induzione I è equivalente al principio d'induzione II.

2. Teorema di divisione, M.C.D e m.c.m

Teorema di divisione in \mathbb{N} : Siano $a, b \in \mathbb{N}$ con $b > 0$. Esiste un'unica coppia di interi q, r tali che $a = bq + r$ con $0 \leq r < b$

Dimostrazione 1: Procediamo per induzione sul numero a , precisamente useremo la forma II. Se $a < b$ allora risulta $a = 0b + a$ e il teorema è vero (almeno nel caso $a = 0 < b$). Supponiamo quindi $a \geq b$, e supponiamo il teorema vero per ogni a' tale che $0 \leq a' < a$. Consideriamo $a-b$: è un numero ≥ 0 e $< a$ perché $b > 0$. Per l'ipotesi induttiva si può scrivere $a-b = q_1b + r$ con $0 \leq r < b$; si ha allora $a = (q_1 + 1)b + r$. Per l'unicità supponiamo che si abbia $bq + r = bq_1 + r_1$ con q, q_1, r, r_1 soddisfacenti il teorema. Allora $b(q - q_1) = r_1 - r$; se fosse $r_1 > r$ si arriverebbe ad un assurdo perché $r_1 - r < b$ mentre essendo $b(q - q_1) > 0$ e $b > 0$ deve essere $(q - q_1) \geq 1$ e quindi $b(q - q_1) \geq b$. Segue allora $r_1 = r$ e da $b(q - q_1) = 0$ si ha $q - q_1 = 0$ per la legge di annullamento del prodotto. Se invece fosse $r_1 < r$ si avrebbe lo stesso risultato da $r - r_1 = b(q_1 - q)$.

Dimostrazione 2 Consideriamo l'insieme $S = \{a - bx \mid a - bx \geq 0, x \in \mathbb{N}\}$; S è non vuoto perché contiene $a - b \cdot 0 = a \in \mathbb{N}$ e quindi ha minimo, diciamo $r = a - bq$ per un certo $q \in \mathbb{N}$. Se fosse $r \geq b$ allora sarebbe $0 \leq r - b < r$ perché b è positivo e $r - b = a - b(q + 1)$, contro l'ipotesi che r è il minimo di S .

Teorema di divisione in \mathbb{Z} Siano a, b due interi relativi, $b \neq 0$. Esiste un'unica coppia di interi q, r tali che $a = bq + r$ con $0 \leq r < |b|$.

Massimo comune divisore e minimo comune multiplo. Siano $a, b \in \mathbb{Z}$, $a \neq 0, b \neq 0$. Diciamo che "a divide b" e scriviamo $a|b$ se esiste $c \in \mathbb{Z}$ tale che $b = ac$. Si chiama *massimo comune divisore (MCD) della coppia a, b* un numero $d \in \mathbb{Z}$ tale che:

1. $d|a$ e $d|b$
2. se $c|a$ e $c|b$ allora $c|d$

Si chiama *minimo comune multiplo (mcm) della coppia a, b* un numero $m \in \mathbb{Z}$ tale che:

1. $a|m$ e $b|m$
2. se $a|c$ e $b|c$ allora $m|c$

Supponiamo che d, d' siano entrambi massimo comune divisore di a, b ; dalla definizione segue $d | d'$ e $d' | d$ quindi $d = hd', d' = kd$ per certi $h, k \in \mathbb{Z}$. Sostituendo si ottiene $d = hkd$ e, per cancellazione, $hk = 1$; segue $h = k = 1$ oppure $h = k = -1$ e ci sono al più due massimi comuni divisori di a, b uno opposto dell'altro. Dimostriamo di seguito che il massimo comune divisore

esiste; quindi se d è massimo comune divisore lo è anche $-d$. Analogamente per il minimo comune multiplo.

Si suole indicare il massimo comune divisore positivo di a, b con $\text{MCD}(a,b)$ oppure solo (a, b) ; il minimo comune multiplo positivo viene indicato con $\text{mcm}(a, b)$ oppure $[a,b]$.

Teorema: Siano $a, b \in \mathbb{Z} - \{0\}$; allora esiste $\text{MCD}(a, b)$.

Dimostrazione 1: consideriamo l'insieme $S = \{ax + by \mid ax + by > 0, x, y \in \mathbb{Z}\}$; esso è non vuoto perché contiene, per esempio, $a^2 + b^2$. Quindi ha minimo, sia $d = a\bar{x} + b\bar{y}$. Verifichiamo che $d = \text{MCD}(a,b)$. Poiché è $d > 0$, per il teorema di divisione risulta $a = dq + r$ con $0 \leq r < d$; se fosse $r > 0$ allora $r = a - dq = a - (a\bar{x} + b\bar{y})q = a(1 - \bar{x}q) - b\bar{y}q \in S$ e questo è contro l'ipotesi che d è il minimo di A . Quindi $d|a$ ed analogamente si dimostra $d|b$. Se poi un intero c è tale che $c|a, c|b$ allora sarà $a = ch, b = ck$ e sostituendo: $d = ch\bar{x} + ck\bar{y} = c(h\bar{x} + k\bar{y})$ cioè $c|d$.

Dimostrazione 2 : (Algoritmo di Euclide delle divisioni successive). Possiamo supporre $a \geq b > 0$.

Applichiamo il teorema di divisione alla coppia a, b : $a = bq + r$ con $0 \leq r < b$; se $r = 0$ allora $b = \text{MCD}(a,b)$, come si verifica facilmente. Altrimenti possiamo dividere b per r , ottenendo: $b = r_1q_1 + r_2$ e ripetere il ragionamento di prima. Così continuando si arriva ad un termine poiché $b > r > r_1 > \dots \geq 0$; abbiamo così il seguente quadro:

$$\begin{aligned} a &= bq + r \\ b &= r_1q_1 + r_2 \\ r &= r_1q_2 + r_3 \\ &\dots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n \\ r_{n-1} &= r_nq_n \end{aligned}$$

Vogliamo dimostrare che r_n , l'ultimo resto non nullo, è il MCD di a,b . Usiamo l'induzione sul numero di divisioni; il primo passo lo abbiamo già visto. Consideriamo ora la coppia b, r : per l'ipotesi induttiva risulta r_n il MCD di b, r , perché il numero di divisioni effettuate è uno in meno. Dalla relazione $a = bq + r$ si vede che $r_n|a$ poiché $r_n|b$ e $r_n|r$; inoltre, se $c|a$ e $c|b$ allora $c|r$ perché $r = a - bq$ e quindi $c|r_n$ perché r_n è il MCD di b,r . Quindi $r_n = \text{MCD}(a,b)$.

Dalla dimostrazione del teorema precedente risulta che, dati due interi non nulli a,b il loro massimo comune divisore d si può scrivere $d = ax + by$ per certi interi relativi x,y . Ci riferiremo ad una tale relazione come all'**identità di Bézout**. Se $\text{MCD}(a,b) = 1$ allora a e b si diranno **primi tra loro o coprimi**.

3. Decomposizione in fattori primi

Un numero $p \in \mathbb{Z}$ si dice primo se è diverso da 0, ± 1 e i suoi unici divisori sono $\pm 1, \pm p$.

Si dimostra che

- 1) se p è un numero primo e $p \mid ab$ allora $p \mid a$ oppure $p \mid b$; più in generale: se p è un numero primo e $p \mid a_1 a_2 \dots a_r$ allora $p \mid a_i$ per qualche $i, 1 \leq i \leq r$.
- 2) se $a \mid bc$ e $(a,b) = 1$ allora $a \mid c$
- 3) Siano $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$. Allora un minimo comune multiplo di a, b è $[a, b] = (ab) / (a, b)$, cioè assegnati due interi diversi da zero a, b un loro minimo comune multiplo si ottiene dividendo il prodotto dei due numeri per il loro MCD

Teorema fondamentale dell'aritmetica: *Ogni numero naturale strettamente maggiore di uno si fattorizza nel prodotto di numeri primi positivi in maniera unica a meno dell'ordine dei fattori.*

Osserviamo che il teorema di decomposizione in fattori primi si estende facilmente a \mathbb{Z} ; infatti preso un numero minore di -1 , il suo opposto ha una fattorizzazione in fattori positivi. Basta allora cambiare di segno uno dei fattori; notiamo che in \mathbb{Z} l'unicità della decomposizione vale non solo a meno dell'ordine ma anche a meno del segno dei fattori primi.

Teorema di Euclide: *I numeri primi sono infiniti.*

Dimostrazione: Supponiamo per assurdo che tutti i numeri primi siano nell'insieme $P = \{p_1, p_2 \dots p_n\}$ e consideriamo il numero $1 + p_1 p_2 \dots p_n$. esso non è primo perché è maggiore di tutti gli elementi di P ; allora avrà un divisore primo q . Se q fosse un elemento di P allora q dividerebbe sia $p_1 p_2 \dots p_n$ che $1 + p_1 p_2 \dots p_n$ e quindi la loro differenza che fa 1: assurdo.

4. Sistemi di numerazione in base b

Quando scriviamo il numero $a = 3481$ intendiamo esprimere sinteticamente la somma:

$$a = 3 \cdot 10^3 + 4 \cdot 10^2 + 8 \cdot 10 + 1$$

che è la rappresentazione in base 10 del numero a . Tale rappresentazione dei numeri si dice posizionale perché il valore di una cifra dipende dalla sua posizione. La base 10 che si adopera usualmente è puramente convenzionale; più in generale si potrebbe *rappresentare lo stesso numero a in base b* , come precisato nel seguente teorema.

Teorema: *Per ogni intero $b > 1$ possiamo rappresentare un numero naturale $a > 0$ in maniera unica in base b :*

$$a = r_n b^n + r_{n-1} b^{n-1} + \dots + r_1 b + r_0$$

con $0 \leq r_i < b$ per ogni i e $r_n > 0$.

Usualmente si rappresentano le cifre, cioè i numeri tra 0 e $b - 1$, con un unico simbolo: ad esempio $\{0, 1\}$ per $b = 2$, $\{0, 1, \dots, 9, A, B, \dots, F\}$ per $b = 16$.

Dimostrazione: Procediamo per induzione su a . I numeri $0 < a < b$ si rappresentano con un'unica cifra, cioè abbiamo $n = 0$, $r_0 = a$. Se $a \geq b$ allora possiamo applicare il teorema di divisione: $a = bq + r_0$. Poiché $b > 1$ risulta $q < a$ e possiamo applicare l'ipotesi induttiva:

$$q = r_n b^{n-1} + r_{n-1} b^{n-2} + \dots + r_1.$$

Sostituendo si ha la tesi. Da notare che l'unicità della rappresentazione deriva dall'unicità di quoziente e resto nella divisione e dall'ipotesi induttiva.

La dimostrazione precedente fornisce anche un algoritmo per ottenere un numero in base b : si divide a per b e poi il quoziente ancora per b fino ad ottenere quoziente zero.

$$a = bq_0 + r_0$$

$$q_0 = bq_1 + r_1$$

...

$$q_{n-2} = bq_{n-1} + r_{n-1}$$

$$q_{n-1} = bq_n + r_n$$

La rappresentazione cercata è $a = (r_n r_{n-1} \dots r_1 r_0)_b$

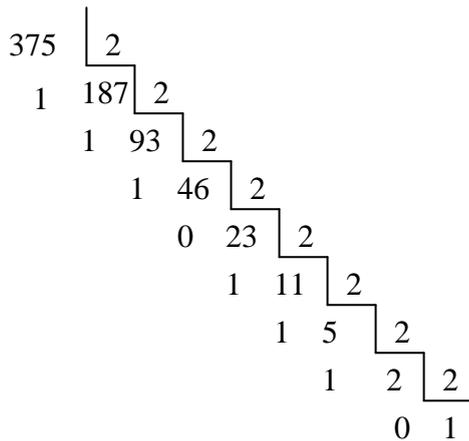
Si possono effettuare le quattro operazioni in qualunque base; l'unica novità è che bisogna usare la tavola pitagorica di base b .

Esempi:

$$5 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

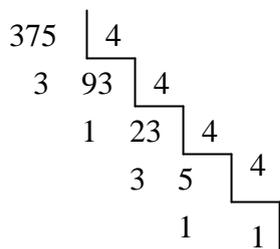
$$2749 = 2 \cdot 10^3 + 7 \cdot 10^2 + 4 \cdot 10^1 + 9 \cdot 10^0$$

Per scrivere un numero in base 2:



$$375 = (101110111)_2$$

Per scrivere un numero in base 4:



$$375 = (11313)_4$$

5. Congruenze

Fissato $n \in \mathbb{N}$ diciamo che $a \equiv b \pmod{n}$ se accade che $a - b = kn$ per qualche $k \in \mathbb{Z}$.

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$$

Ad esempio: $n=5$

$$7 \equiv 2 \pmod{5}$$

$$14 \equiv 4 \pmod{5}$$

Proposizione: Sono equivalenti:

- 1) $a \equiv b \pmod{n}$
- 2) $a = b + kn$ per qualche $k \in \mathbb{Z}$
- 3) a e b hanno lo stesso resto se divisi per n

Dimostrazione:

$1 \Rightarrow 2$: $n \mid a - b$ vuol dire che $a - b = kn$ per qualche intero $k \in \mathbb{Z}$.

$2 \Rightarrow 3$: Se $a = nq_1 + r_1$ e $b = nq_2 + r_2$, sostituendo in $a = b + kn$ si trova $nq_1 + r_1 = nq_2 + r_2 + kn$ cioè

$$r_1 - r_2 = n(q_2 - q_1 + k) \text{ e quindi } r_1 = r_2 \text{ per definizione di resto.}$$

$3 \Rightarrow 1$: Da $a = nq_1 + r$, $b = nq_2 + r$ si ottiene $a - b = n(q_1 - q_2)$.

Proprietà delle congruenze:

Dati $a \equiv b \pmod{n}$ e $a' \equiv b' \pmod{n}$ si ha che:

- 1) $a + a' \equiv b + b' \pmod{n}$
- 2) $aa' \equiv bb' \pmod{n}$
- 3) Se $a \equiv b \pmod{n}$ e d divide n ($n = dr$) allora $a \equiv b \pmod{d}$
- 4) Se $a \equiv b \pmod{r}$ e $a \equiv b \pmod{s}$ allora $a \equiv b \pmod{[r,s]}$
- 5) Se $r \neq 0$ e $ra \equiv rb \pmod{n}$ allora $a \equiv b \pmod{\frac{n}{(r,n)}}$

Avendosi per ipotesi $a - b = kn$ e $a' - b' = k_1n$ la 1) e la 2) seguono dal fatto che:

- sommando membro a membro, si ha:

$$a + a' - (b + b') = (k + k_1)n, \text{ cioè } a + a' \equiv b + b' \pmod{n};$$

- moltiplicando membro a membro si ottiene:

$$aa' = bb' + bk_1n + b'kn + kk_1n^2 = bb' + n(bk_1 + b'k + kk_1n) \text{ e quindi } aa' \equiv bb' \pmod{n}.$$

La 3) segue subito dalla proprietà transitiva della divisibilità. L'ipotesi di 4), per definizione, vuol dire che $a - b$ è multiplo comune di r, s e quindi la tesi segue dalla definizione di minimo comune multiplo. Per la 5), sia $d = (r, n)$ e quindi $r = r'd, n = n'd$ con $(r', n') = 1$; poiché $n \mid ra - rb = r(a - b)$, sostituendo si ottiene $r'd(a - b) = kdn'$ e quindi $r'(a - b) = kn'$ cioè $n' \mid r'(a - b)$.

Osserviamo che, nel caso che $(r, n) = 1$, la 5) è una proprietà di cancellazione delle congruenze.

Proposizione: *La congruenza in \mathbb{Z} fissato $n \in \mathbb{N}$ è una relazione di equivalenza.*

Infatti valgono le proprietà:

Riflessiva: $a \equiv a \pmod{n}$ $a - a = 0 = 0 \cdot n$

Transitiva: $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

$$a - b = k_1 n \quad \text{e} \quad b - c = k_2 n \quad \Rightarrow \quad a - c = (k_1 + k_2) n$$

Simmetrica: $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

$$a - b = kn \quad \Rightarrow \quad b - a = (-k)n$$

Le classi disgiunte in cui \mathbb{Z} viene ripartito dalla congruenza modulo n si sogliono denotare con $[0]_n, [1]_n, \dots, [n - 1]_n$, od anche senza indice se non c'è possibilità di confusione. L'insieme di tali classi, dette anche *classi di resto modulo n* , viene indicato con $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n - 1]_n\}$.

Notiamo che le proprietà 1) e 2) permettono definire operazioni di somma e prodotto in \mathbb{Z}_n :

$$[a] + [b] = [a + b] \quad [a][b] = [ab]$$

Tali operazioni sono ben definite, nel senso che il risultato non dipende dai rappresentanti scelti per le classi: se $a' \in [a]$ e $b' \in [b]$ allora $[a' + b'] = [a + b]$ per la 1) e $[a'b'] = [ab]$ per la 2).

Consideriamo le seguenti congruenze contenenti incognite:

$$1) \quad x + a \equiv b \pmod{n}$$

$$2) \quad ax \equiv b \pmod{n}$$

La 1) si risolve facilmente, infatti essendo $-a \equiv -a \pmod{n}$, sommando membro a membro si ottiene:

$$x = b - a \pmod{n}; \quad x + 2 \equiv 3 \pmod{5} \text{ da cui } x \equiv 3 - 2 \pmod{5} \text{ e quindi } x \equiv 1 + 5k$$

Per risolvere la 2) osserviamo che essa è equivalente all'equazione $ax + ny = b$ per qualche $y \in \mathbb{Z}$; pertanto risolvere la congruenza equivale dunque a risolvere quest'ultima equazione nelle incognite intere x, y . Posto $d = (a, n)$, e quindi $a = da', n = dn'$ con $(a', n') = 1$, si ottiene $da'x + dn'y = b$ da cui segue $d \mid b$. Perché la congruenza abbia soluzione è quindi necessario che $d \mid b$. In tal caso, posto $b = db'$ si ha, per l'identità di Bézout, $d = a\bar{x} + n\bar{y}$ e, moltiplicando per b' , $b = a\bar{x}b' + n\bar{y}b'$ e si trova che $x = \bar{x}b'$ è una soluzione della congruenza. Osserviamo che se x, x' sono soluzioni della congruenza si ha $ax + ny = b$ per qualche $y \in \mathbb{Z}$ e $ax' + ny' = b$ per qualche $y' \in \mathbb{Z}$; uguagliando

$ax + ny = ax' + ny'$ da cui $a(x - x') = n(y' - y)$ e quindi $a'(x - x') = n'(y' - y)$. Poiché $(a', n') = 1$ ne viene che a' divide $y' - y$, cioè si ha $y' - y = a'k$ per $k \in \mathbb{Z}$ e sostituendo $x - x' = n'k$. In definitiva abbiamo trovato che, se x, y è una soluzione, tutte le soluzioni si ottengono ponendo $x' = x - n'k$ e $y' = y + a'k$, col significato dei simboli sopra specificato.

6. Criteri di divisibilità

Supponiamo di avere un numero a e la sua rappresentazione in base dieci:

$$a = r_n 10^n + r_{n-1} 10^{n-1} + r_1 10 + r_0$$

Le proprietà 1) e 2) delle congruenze permettono di dimostrare alcuni criteri di divisibilità del numero a .

Criterio di divisibilità per 9: *Un numero a è divisibile per 9 se e solo se 9 divide la somma delle cifre.*

Dimostrazione: Poiché $10 \equiv 1 \pmod{9}$ per la 2) si ha $10^r \equiv 1 \pmod{9}$ per ogni $r \geq 0$, ed anche $r_s 10^r \equiv r_s \pmod{9}$ per la 1) e quindi $a = r_n 10^n + r_{n-1} 10^{n-1} + \dots + r_1 10 + r_0 \equiv r_n + r_{n-1} + \dots + r_1 + r_0 \pmod{9}$

Osserviamo che se risulta $a + b = c$, $ab = d$ per certi interi $a, b, c, d \in \mathbb{Z}$ allora è anche $[a]_n + [b]_n = [c]_n$, $[a]_n [b]_n = [d]_n$ per ogni $n \in \mathbb{N}$; questa proprietà può essere usata per controllare l'esattezza delle operazioni tra interi, anche se è solo una condizione necessaria. La ben nota *prova del nove* è basata sul precedente criterio: viene usato proprio il numero nove per la particolare facilità del calcolo del resto modulo nove.

Se un numero è divisibile per 9 allora lo è anche per 3

Criterio di divisibilità per 3: *Un numero a è divisibile per 3 se e solo se 3 divide la somma delle cifre.*

Criterio di divisibilità per 2 o per 5: *Un numero a è divisibile per 2 o per 5 se l'ultima cifra è rispettivamente divisibile per 2 o per 5 ($2 \mid r_0$ o $5 \mid r_0$).*

7. Teorema cinese del resto

Siano m_1, m_2, \dots, m_n numeri naturali > 1 due a due coprimi e a_1, a_2, \dots, a_n interi relativi. Allora il sistema di congruenze

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

ha soluzioni. Se \bar{x}, x' sono due soluzioni allora $\bar{x} \equiv x' \pmod{M}$, dove $M = m_1 m_2 \dots m_n$.

Dimostrazione: Fissato i supponiamo $a_i = 1, a_j = 0$ per $j \neq i$. Poniamo $k_i = m_1 m_2 \dots m_{i-1} m_{i+1} m_n$ ed osserviamo che $(m_i, k_i) = 1$: infatti un divisore primo di m_i che divide k_i dovrebbe dividere uno dei fattori m_j . Per l'identità di Bézout esistono interi r_i, s_i tali che $r_i k_i + s_i m_i = 1$; da questo si vede che $r_i k_i \equiv 0 \pmod{k_i}$ e $r_i k_i \equiv 1 \pmod{m_i}$. Se $r_i k_i \equiv 0 \pmod{k_i}$ allora anche $r_i k_i \equiv 0 \pmod{m_j}$ per $j \neq i$ poiché $m_j \mid k_i$ e dunque il numero $x_i = r_i k_i$ è soluzione del sistema nel caso particolare che stiamo studiando. In questa maniera abbiamo trovato n numeri x_1, x_2, \dots, x_n ; osserviamo che $a_i x_i \equiv a_i \pmod{m_i}$ e $a_j x_i \equiv 0 \pmod{m_j}$ per ogni $j \neq i$ ed inoltre $a_1 x_1 + a_2 x_2 + \dots + a_n x_n \equiv a_i \pmod{m_i}$ per ogni $i = 1, 2, \dots, n$. Pertanto $\bar{x} = a_1 x_1 + a_2 x_2 + \dots + a_n x_n$ è una soluzione del sistema. Se x' è un'altra soluzione allora si ha $\bar{x} - x' \equiv 0 \pmod{m_i}$ per ogni i ; per definizione questo significa $m_i \mid \bar{x} - x'$ e quindi $\bar{x} - x'$ è multiplo del minimo comune multiplo degli m_i . Poiché i numeri m_i sono coprimi tale minimo comune multiplo è il loro prodotto.

Osserviamo che la dimostrazione del teorema fornisce un algoritmo per trovare una soluzione del sistema, sempre che sia soddisfatta l'ipotesi, cioè che i moduli m_i siano coprimi. Osserviamo ancora che il teorema cinese dà solo una condizione sufficiente per la risolubilità del sistema: può effettivamente capitare che il sistema abbia soluzione anche se i moduli non sono a due a due coprimi.

Un procedimento alternativo a quello del teorema è di risolvere le congruenze due alla volta. Se $x \equiv a_1 \pmod{m_1}$ allora sarà $x = a_1 + m_1 u_1$ per ogni intero u_1 ; se è anche $x \equiv a_2 \pmod{m_2}$ allora dovrà essere $a_1 + m_1 u_1 = a_2 + m_2 u_2$ per opportuni interi u_1, u_2 . Quest'ultima equazione ammette soluzioni se $(m_1, m_2) \mid a_1 - a_2$; in tal caso si possono trovare soluzioni tramite l'identità di Bézout. Tali soluzioni saranno del tipo $\{\bar{x} + k[m_1, m_2], k \in \mathbb{Z}\}$; si dovranno poi ricercare tra questi i numeri che siano eventualmente soluzione della terza congruenza. Questo procedimento permette di trovare tutte le soluzioni del sistema, se esistono, e si può applicare anche nel caso in cui l'ipotesi del teorema cinese sia vera; in quest'ultimo caso si è sicuri a priori di trovare soluzioni.

Esempi:

Risolvere i seguenti sistemi di congruenze:

$$\text{a) } \begin{cases} x \equiv 2 \pmod{4} \\ 2x \equiv 3 \pmod{7} \end{cases} \quad \text{b) } \begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{3} \end{cases}$$

$$\text{a) } \begin{cases} x \equiv 2 \pmod{4} \\ 2x \equiv 3 \pmod{7} \end{cases} \Rightarrow \begin{cases} x = 2 + 4k \\ 2x = 3 + 7t \end{cases} \Rightarrow \begin{cases} x = 2 + 4k \\ 2(2 + 4k) = 3 + 7t \end{cases} \Rightarrow \begin{cases} x = 2 + 4k \\ 8k - 7t = -1 \end{cases}$$

si ha $k = -1 + 7m$ e $t = 1 + 8m$ e quindi $x = 2 + 4(-1 + 7m) = 2 - 4 + 28m = -2 + 28m$

b) Poiché i moduli $m_1 = 4$, $m_2 = 7$, $m_3 = 3$ sono a due a due coprimi allora il sistema, per il teorema cinese del resto, ammette soluzioni, che sono gli interi $x' = \bar{x} + kM$ dove $\bar{x} = 2x_1 + 5x_2 + 1x_3$ e $M = m_1 \cdot m_2 \cdot m_3 = 4 \cdot 7 \cdot 3$, $k \in \mathbb{Z}$.

I numeri x_1, x_2, x_3 sono ognuno una soluzione particolare rispettivamente dei seguenti tre sistemi:

$$\begin{aligned} 1) & \begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 0 \pmod{7} \\ x \equiv 0 \pmod{3} \end{cases} \\ 2) & \begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 1 \pmod{7} \\ x \equiv 0 \pmod{3} \end{cases} \\ 3) & \begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 0 \pmod{7} \\ x \equiv 1 \pmod{3} \end{cases} \end{aligned}$$

Osserviamo che :

- i due numeri $m_1 = 4$ e $k_1 = m_2 m_3 = 21$ sono coprimi per cui è $1 = r_1 k_1 + m_1 s_1$ ossia $1 = 21 r_1 + 4 s_1$, da cui segue che $x_1 = r_1 k_1 = 21 r_1$ è una soluzione del sistema 1).
Risulta $r_1 = 1$ e $s_1 = -5$ e quindi $x_1 = 21$.
- i due numeri $m_2 = 7$ e $k_2 = m_1 m_3 = 12$ sono coprimi per cui è $1 = r_2 k_2 + m_2 s_2$ ossia $1 = 12 r_2 + 7 s_2$ da cui segue che $x_2 = r_2 k_2 = 12 r_2$ è una soluzione del sistema 2).
Risulta $r_2 = 3$ e $s_2 = -5$ e quindi $x_2 = 36$.
- i due numeri $m_3 = 3$ e $k_3 = m_1 m_2 = 28$ sono coprimi per cui è $1 = r_3 k_3 + m_3 s_3$ ossia $1 = 28 r_3 + 3 s_3$ da cui segue che $x_3 = r_3 k_3 = 28 r_3$ è una soluzione del sistema 3).
Risulta $r_3 = 1$ e $s_3 = -7$ e quindi $x_3 = 28$.

In conclusione $\bar{x} = 2x_1 + 5x_2 + x_3 = 42 + 180 + 28 = 250$ e $x' = 250 - 84k$.

Proviamo a risolvere lo stesso sistema in un altro modo, uguagliando le congruenze due alla volta. Una volta trovate le soluzioni comuni a due congruenze si determinino tra queste quelle che soddisfano la terza congruenza.

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{3} \end{cases} \Rightarrow \begin{cases} x = 1 + 3a \\ x = 2 + 4b \\ x \equiv 5 \pmod{7} \end{cases} \Rightarrow \begin{cases} x = 1 + 3a \\ 1 + 3a = 2 + 4b \\ x \equiv 5 \pmod{7} \end{cases} \Rightarrow \begin{cases} x = 1 + 3a \\ 3a - 4b = 1 \\ x \equiv 5 \pmod{7} \end{cases} \quad \text{si ha} \quad \begin{cases} a = -1 + 4t \\ b = -1 + 3t \end{cases}$$

$$\text{e quindi} \begin{cases} x = 1 + 3(-1 + 4t) = 1 - 3 + 12t = -2 + 12t \\ x = 5 + 7c \end{cases} \Rightarrow \begin{cases} x = -2 + 12t \\ -2 + 12t = 5 + 7c \end{cases} \Rightarrow \begin{cases} x = -2 + 12t \\ 12t - 7c = 7 \end{cases}$$

$$\text{si ha} \quad \begin{cases} t = 21 + 7k \\ c = 35 + 12k \end{cases} \quad \text{da cui} \quad x = -2 + 12(21 + 7k) = -2 + 252 + 84k = 250 + 84k.$$

STRUTTURE ALGEBRICHE

1. Operazioni algebriche binarie

Dato un insieme $M \neq \emptyset$, chiamiamo *operazione algebrica binaria* definita su M una qualunque applicazione f che associa ad ogni coppia ordinata (a, b) di elementi distinti o no di M uno ed un solo elemento c appartenente ad M .

$$f: M \times M \rightarrow M \quad \forall (a, b) \in M \times M \quad f(a, b) = c \in M$$

L'operazione viene indicata con i simboli $: *, \circ, \hat{A}, \dots$ si ha $a * b = c$.

Esempi:

- 1) La somma e il prodotto introdotte in \mathbb{N} sono operazioni algebriche binarie, mentre la sottrazione e la divisione non lo sono.
- 2) Sia P l'insieme dei numeri pari e D quello dei numeri dispari, la somma è un'operazione algebrica binaria definita su P , mentre non lo è su D .
- 3) Sono esempi di operazioni algebriche binarie definite su \mathbb{N}^* ⁽¹⁾
 - l'applicazione f che associa alla coppia (a, b) , di elementi distinti o no, la potenza che ha per base il primo elemento e per esponente il secondo elemento: $f(a, b) \rightarrow a^b$ cioè $a * b = a^b$.
 - l'applicazione f che associa alla coppia (a, b) , di elementi distinti o no, il loro MCD: $a \circ b = \text{M.C.D.}(a, b)$.

Si dice che l'operazione $*$ definita su M gode della *proprietà commutativa* se:

$$\forall a, b \in M \text{ si verifica che: } a * b = b * a.$$

Le operazioni $+$ e \cdot su insiemi \mathbb{N} e \mathbb{Q} sono commutative; le operazioni $-$ e $:$ in \mathbb{Q} , come pure l'elevamento a potenza in \mathbb{N}^* non sono commutative.

L'operazione $*$ definita su M gode della *proprietà associativa* se:

$$\forall a, b, c \in M \text{ si verifica che: } (a * b) * c = a * (b * c).$$

Le operazioni $+$ e \cdot su \mathbb{N} , \mathbb{Q} e \mathbb{Z} sono associative.

⁽¹⁾ I simboli $\mathbb{N}^*, \mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*$ indicano gli insiemi dei numeri naturali interi, relativi, razionali e reali privati dello 0.

Non è associativa:

- l'elevamento a potenza in \mathbb{N}^* , (infatti ad esempio è: $(2*3)*4 \neq 2*(3*4)$, avendosi $(2*3)*4=2^3*4=(2^3)^4=2^{12}$ e $2*(3*4)=2*3^4=2^{81}$.)
- la sottrazione in \mathbb{Z} , (infatti ad esempio è: $8-(5-2) \neq (8-5)-2$, avendosi $8-(5-2)=8-3=5$ e $(8-5)-2=3-2=1$.)

Altri esempi:

1) Sia M un insieme non vuoto e $*$ l'operazione su di esso definita in modo tale che:

$\forall a, b \in M \quad a * b = b$. Tale operazione è associativa, (infatti è $(a*b)*c = a*(b*c)$, avendosi $(a*b)*c = b*c = c$ e $a*(b*c) = a*c = c$); ma non è chiaramente commutativa, a meno che l'insieme sia costituito da un unico elemento, cioè $|M| = 1$.

2) Sia E un insieme e $P(E)$ l'insieme delle sue parti, le operazioni di \cap e \cup su $P(E)$ sono commutative e associative.

Una *struttura algebrica* è un insieme non vuoto su cui sono definite una o più operazioni algebriche binarie.

Un *gruppoide* è una struttura algebrica con una operazione algebrica binaria definita su di esso, verrà denotato con $(M, *)$.

Un *semigrupp* è un gruppoide in cui l'operazione gode della proprietà associativa.

Un semigrupp si dice *abeliano* (o commutativo) se l'operazione in esso definita gode della proprietà commutativa.

Elemento neutro di un gruppoide $(M, *)$ è quell'elemento $e \in M$ tale che $\forall a \in M$ si ha:

$$a * e = e * a = a.$$

- \mathbb{N} , \mathbb{Z} , \mathbb{Q} , con l'operazione di addizione sono semigrupp abeliani ed hanno lo 0 elemento neutro.
- \mathbb{N} , \mathbb{Z} , \mathbb{Q} , con l'operazione di moltiplicazione sono semigrupp abeliani ed hanno 1 come elemento neutro ed è chiamato *elemento unità*.
- \mathbb{Q} con l'operazione di divisione non ha elemento neutro infatti $a:1 = a$ mentre $1:a \neq a$.

In un gruppoide $(M, *)$ con elemento neutro e dicesi *elemento simmetrico* di a un elemento a' tale che $a * a' = a' * a = e$.

Se $\exists a'$, si dice che a è simmetrizzabile.

-In \mathbb{N} nessun elemento tranne lo 0 è simmetrizzabile rispetto a +.

-In $(\mathbb{Z}, +)$ qualsiasi elemento è simmetrizzabile (il simmetrico di a è $-a$) così anche in (\mathbb{Q}^*, \cdot) (il simmetrico di a è $1/a$).

2. Gruppi

Un semigruppò con elemento unità nel quale ogni elemento è simmetrizzabile è detto gruppo.

Ciò equivale a dire che un gruppo è un insieme non vuoto M con una operazione algebrica binaria

$f: M \times M \rightarrow M: (a, b) \rightarrow a * b$ definita su esso la quale gode delle seguenti 3 proprietà:

- 1) $\forall a, b, c \in M : (a * b) * c = a * (b * c)$ ($*$ è associativa)
- 2) $\exists e \in M : a * e = e * a = a \quad \forall a \in M$ (e elemento neutro)
- 3) $\forall a \in M \exists a' \in M : a * a' = a' * a = e$ ($\forall a \in M$ è simmetrizzabile)

Teoremi

- In un gruppo l'elemento neutro è unico.

Supponiamo per assurdo che esistano due elementi neutri e ed e' . Per la proprietà dell'elemento neutro si ha:

$\forall a \in M \quad a * e = e * a = a$ dunque:

$e * e' = e' * e = e$ e anche $e' * e = e * e' = e'$ da cui $e = e'$.

- In un gruppo ogni elemento a ammette un solo simmetrico a' .

Supponiamo per assurdo che esistano $\forall a \in M$ due elementi simmetrici a'' ed a' . Consideriamo:

$$a'' * a * a' = \begin{cases} (a'' * a) * a' = e * a' = a' \\ a'' * (a * a') = a'' * e = a'' \end{cases}$$

da cui: $a'' = a'$.

Spesso l'operazione algebrica binaria del gruppo è indicata con \cdot (chiamata moltiplicazione) in tal caso l'elemento neutro verrà indicato con 1 ed è detto *unità*, mentre il simmetrico di a verrà indicato con a^{-1} , ed è detto il *reciproco* e il gruppo è detto *moltiplicativo*; usualmente in un gruppo moltiplicativo scriveremo ab invece di $a \cdot b$.

E' immediato verificare che: $(a^{-1})^{-1} = a$ e $(ab)^{-1} = b^{-1} a^{-1}$.

Talvolta, specialmente quando si tratta di gruppi abeliani, si usa la *notazione additiva* invece di quella moltiplicativa. Cioè: l'operazione del gruppo si chiama *addizione* (invece di moltiplicazione) e si scrive $a + b$ (invece di $a \cdot b$), l'elemento unità del gruppo si chiama *zero* e si indica con 0 (invece di 1); l'inverso di a si chiama *opposto* e si indica con $-a$ (invece di a^{-1}). Si pone inoltre $a + (-b) = a - b$.

Per semplicità di scrittura i teoremi che seguono saranno formulati nel caso di un gruppo moltiplicativo (G, \cdot) . Si noti che essi valgono anche nel caso generale di un gruppo $(G, *)$.

Teoremi

- 1) Se G è un gruppo, " $a, b \in G$ le due equazioni $ax=b$ e $ya=b$ ammettono una sola soluzione.
Infatti $x = a^{-1}b$ e $y = b a^{-1}$ sono soluzioni e sono uniche.
- 2) In un gruppo valgono le leggi di cancellazione a sinistra e a destra, cioè:
 $\forall a, b, c \in G$ da $ab = ac$ segue che $b = c$.
 $\forall a, b, c \in G$ da $ba = ca$ segue che $b = c$.

Altra definizione di gruppo. Un gruppo G è un semigruppò in cui le due equazioni $ax=b$ e $ya=b$ ammettono ciascuna una ed una sola soluzione per ogni $a, b \in G$.

$$\begin{array}{ccc}
 (G, \cdot) & & (G, \cdot) \\
 \left\{ \begin{array}{l} 1) \text{ Associativ a} \\ 2) \exists e \\ 3) \forall a \in G, \exists a^{-1} : a^{-1}a = aa^{-1} = e \end{array} \right. & \Leftrightarrow & \left\{ \begin{array}{l} 1) \text{ Associativ a} \\ 2) \forall a, b \in G, \text{ le equazioni } ax = b \text{ e } ya = b \\ \text{hanno una sola soluzione} \end{array} \right.
 \end{array}$$

Un gruppo si dice *abeliano* o *commutativo* se l'operazione gode della proprietà commutativa.

Chiamiamo *ordine di un gruppo finito* il numero dei suoi elementi.

Semigruppò e gruppo simmetrico. Sia M un insieme non vuoto. L'insieme delle applicazioni di M in M è un semigruppò rispetto al prodotto di applicazioni e si dice il *semigruppò simmetrico* su M .

L'insieme delle applicazioni biettive di M in M è un gruppo e si chiama il *gruppo simmetrico* su M . Se M è finito e ha n elementi, il gruppo simmetrico su M è finito ed ha $n! = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$ elementi. In quest'ultimo caso il gruppo simmetrico si suole chiamare *gruppo delle sostituzioni* su n elementi; se $M = \{1, 2, \dots, n\}$ allora un sostituzione viene spesso indicata con

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & & a_n \end{pmatrix}$$

dove $\{a_1, a_2, \dots, a_n\} = \{1, 2, \dots, n\}$.

3. Sottogruppi.

Sottosemigrosso di un semigrosso G è un sottoinsieme non vuoto A di G che risulta essere semigrosso rispetto alla stessa operazione definita in G.

Ciò accade se e solo se $\forall a, b \in A$ si ha che $ab \in A$ cioè

$$A \text{ sottosemigrosso di } G \iff " a, b \in A, ab \in A.$$

Sottogrosso di un gruppo G è un sottoinsieme A non vuoto di G che risulta essere un gruppo rispetto alla stessa operazione definita in G.

In ogni gruppo G esistono almeno due sottogrossi, i cosiddetti *sottogrossi banali o impropri*. Essi sono il gruppo stesso e il sottogrosso che ha come unico elemento l'elemento neutro di G; ogni altro sottogrosso è detto *proprio*.

Teorema: *Condizione necessaria e sufficiente affinché A (sottoinsieme non vuoto di G) sia un sottogrosso di G è che siano verificate le seguenti due condizioni:*

$$1) " a, b \in A \implies ab \in A$$

$$2) " a \in A \implies a^{-1} \in A$$

$$\text{In sintesi: } A \text{ è sottogrosso di } G \iff 1) " a, b \in A \implies ab \in A; \quad 2) " a \in A \implies a^{-1} \in A$$

Dimostrazione:

\Rightarrow Essendo A un sottogrosso di G, ossia un gruppo si ha che $\forall a, b \in A \quad ab \in A$ e $a^{-1} \in A$.

\Leftarrow Poiché da $a, b \in A \implies ab \in A$ segue che l'operazione definita in G è anche un'operazione definita in A.

Inoltre $\forall a, b, c \in A$ si ha $a(bc) = (ab)c$ perché la proprietà associativa che vale in tutto G, vale anche in A.

Poiché le condizioni 1) e 2) valgono $\forall a, b \in A$ per $b = a^{-1}$ si ha $a a^{-1} = e \in A$, cioè l'elemento neutro di G sta pure in A. Ed essendo anche che $\forall a \in A, a^{-1} \in A$ segue che: A è un gruppo, cioè un sottogrosso.

Le condizioni 1) e 2) equivalgono all'unica condizione $" a, b \in A \implies ab^{-1} \in A$.

Le condizioni del precedente teorema possono, in alcuni casi, essere alleggerite. E' il caso in cui A è un sottoinsieme finito di un gruppo G. Si ha infatti:

Teorema: *A sottoinsieme finito di un gruppo G è un sottogruppo di G \iff $a, b \in A \implies ab \in A$.*

Dimostrazione:

\implies Infatti essendo A un sottogruppo e quindi un gruppo, esso è chiuso rispetto all'operazione definita in G e quindi in A .

\Leftarrow Se $\forall a_i, a_j \in A \implies a_i a_j \in A$ si ha che A è un sottogruppo. Ci serviamo della seconda definizione di gruppo e cioè che le due equazioni $ax=b$ e $ya=b$ hanno una sola soluzione.

Nel nostro caso $\forall a_i, a_j$ facciamo vedere che le equazioni $a_i x = a_j$ e $y a_i = a_j$ hanno una sola soluzione. Consideriamo a tale scopo i prodotti $a_i a_1, a_i a_2, \dots, a_i a_n$ ciascuno di essi, per ipotesi $\in A$ e sono tutti, a due a due distinti (altrimenti per la legge di cancellazione da $a_i a_r = a_i a_s \implies a_r = a_s$) pertanto coincidono con gli n elementi di A , ed esattamente uno di essi sarà uguale ad a_j , cioè sarà $a_i a_r = a_j$ cioè l'elemento a_r è la soluzione in A dell'equazione $a_i x = a_j$.

Analogamente considerando i prodotti $a_1 a_i, a_2 a_i, \dots, a_n a_i$, si prova che l'equazione $y a_i = a_j$ ammette soluzione in A .

Osservazione: la finitezza di A è essenziale. Infatti:

$\mathbb{Q}^* = \mathbb{Q} - \{0\}$ con l'operazione di moltiplicazione è un gruppo.

$\mathbb{N}^* = \mathbb{N} - \{0\}$ con l'operazione di moltiplicazione non è un gruppo.

\mathbb{N}^* è un sottoinsieme di \mathbb{Q}^* e si ha che $\forall a, b \in \mathbb{N}^* \implies ab \in \mathbb{N}^*$ ma (\mathbb{N}^*, \cdot) non è un sottogruppo di (\mathbb{Q}^*, \cdot) .

Intersezione ed unione di sottogruppi.

Teorema: *Se S e H sono due sottogruppi di G $\implies S \cap H$ è un sottogruppo di G .*

Dimostrazione. Infatti:

- a) se $a \in S \cap H$, essendo S e H sottogruppi $\implies a^{-1} \in S$ e $a^{-1} \in H$ quindi $a^{-1} \in S \cap H$.
- b) se $a, b \in S \cap H$, essendo S e H sottogruppi $\implies ab \in S$, $ab \in H \implies ab \in S \cap H$.

Più in generale se $\{G_i\}_{i \in I}$ è un insieme di sottogruppi di G allora $G' = \bigcap G_i$ (formato dagli elementi comuni a tutti i sottogruppi G_i) è un sottogruppo di G .

Teorema: Se S e H sono due sottogruppi di G \mathbf{P} $S \dot{\cup} H$ non è sottogruppo di G , tranne nel caso in cui $H \dot{\cup} S$ oppure $S \dot{\cup} H$.

Dimostrazione. Sia $a \in S-H$ e $b \in H-S$, facciamo vedere che $ab \notin S \cup H$.

Supponiamo per assurdo che $ab \in S \cup H$, ad esempio $ab \in S$, avremo $ab=s$. Moltiplicando ambo i membri a sinistra per a^{-1} si avrebbe $a^{-1}ab = a^{-1}s \in S \Rightarrow b = a^{-1}s \in S$ ciò è assurdo perché $b \notin S$; analogamente se $ab \in H$ si perviene ad un assurdo.

4. Gruppi ciclici e generatori.

Se $a \in G$, si considerino tutti gli elementi “generati” da a usando l’operazione del gruppo. Nella notazione moltiplicativa poniamo:

$$a^0 = e^{(1)}, \quad a^1 = a, \quad a^m = a^{m-1} \times a \quad \text{per } m > 1.$$

$$a^{-1} = \text{inverso di } a \quad a^{-2} = (a^{-1})(a^{-1}) = (a^{-1})^2, \quad a^{-3} = (a^{-1})(a^{-1})(a^{-1}) = (a^{-1})^3, \quad \dots \dots$$

$$\text{cioè } a^{-m} = (a^{-1})^m.$$

E’ immediato provare che :

$$a^m a^n = a^{m+n} \quad (a^m)^n = a^{m \cdot n}$$

e da queste deriva che l’insieme $\{a^n \mid n \in \mathbb{Z}\}$ è un sottogruppo abeliano di G , che indicheremo con $G(a)$, si chiama *sottogruppo ciclico generato da a* .

Un gruppo G si dice *ciclico* quando coincide con un suo sottogruppo ciclico, cioè se esiste un suo elemento a tale che $G(a) = G$, l’elemento a è detto *generatore* di G .

Se l’operazione definita in G è l’addizione si hanno le seguenti posizioni:

$$0a = 0 \text{ (elemento neutro di } G) \quad 1a = a \quad ma = (m-1)a + a \quad (-1)a = -a \quad (-m)a = m(-a) \text{ e quindi:}$$

$$na + ma = (n+m)a \quad n(ma) = (nm)a$$

e gli elementi di $G(a)$ sono gli elementi del tipo ma , $m \in \mathbb{Z}$, cioè tutti i multipli di a secondo un intero relativo m .

Esempi:

- 1) $(\mathbb{Z}, +)$ è un gruppo ciclico, esso è generato dall’intero 1, e un altro generatore è -1 .
- 2) Dato un poligono regolare di $n \geq 3$ lati, il gruppo delle rotazioni attorno al centro del poligono che mutano in sé il poligono è un gruppo ciclico di ordine n .

⁽¹⁾ Pur usando la notazione moltiplicativa, per non creare confusione tipograficamente, continuiamo ad indicare con e l’elemento unità del gruppo.

Per il sottogruppo ciclico generato dall'elemento a si possono presentare due casi:

1) Le potenze di a sono a due a due distinte, cioè per $h \neq k$ è $a^h \neq a^k$ allora esiste una biiezione $\mathbb{Z} \leftrightarrow G(a)$, $n \rightarrow a^n$; tal caso $G(a)$ possiede infiniti elementi, e si dice che a è un elemento di *ordine o periodo infinito*.

Esempio:

$(\mathbb{Z}, +)$, l'elemento 1 ha ordine infinito, così come l'elemento -1 . $(\mathbb{Z}, +)$ può essere generato da 1 o da -1 .

2) Esistono due interi relativi $h \neq k$ tali che $a^h = a^k$, in tal caso supposto $k > h$ si ha

$a^k \times a^{-h} = a^h \times a^{-h} = e \Rightarrow a^{k-h} = e$ con $k-h > 0$, cioè esistono potenze di a ad esponente > 0 eguali ad e . Il più piccolo intero positivo n per cui $a^n = e$ dicesi *ordine o periodo* di a e si dice che a ha ordine finito n .

Se a ha ordine finito n , allora le potenze $a^0 = e, a^1 = a, a^2, \dots, a^{n-1}$ sono a due a due distinte, perché se fosse $a^{h'} = a^{k'}$, con $0 < h' < k' \leq n-1$ sarebbe $a^{k'-h'} = e$ con $0 < k'-h' \leq n-1$ e ciò è assurdo.

Inoltre ogni altra potenza $a^m \in G(a)$, con m intero relativo, è uguale ad una delle potenze a^r con $0 \leq r \leq n-1$, perché possiamo scrivere: $m = nq + r$ e quindi: $a^m = a^{nq+r} = a^{nq} \times a^r = (a^n)^q \times a^r$ ed essendo $a^n = e \Rightarrow a^m = a^r$

Pertanto se un elemento $a \in G$ ha ordine finito n , allora il sottogruppo $G(a)$ ha ordine n e i suoi elementi sono: $e, a, a^2, \dots, a^{n-1}$.

Generatori. Sia $G = G(a)$ un gruppo ciclico, vogliamo trovare i suoi generatori.

Chiaramente affinché un elemento di G , a^r , sia anch'esso un generatore è necessario e sufficiente che esista un qualche intero s tale che $(a^r)^s = a$ cioè, $a^{rs} = a$.

Distinguiamo i casi G ciclico infinito e G ciclico finito.

- Se G è ciclico infinito, l'uguaglianza $a^{rs} = a$ implica $rs=1$ e quindi r ed s sono entrambi 1 o entrambi -1 .

Ci sono allora solo due elementi che possono generare un gruppo ciclico infinito, a^1 e a^{-1} , l'uno inverso dell'altro.

- Se G è ciclico finito di ordine n , da $a^{rs} = a \Rightarrow a^{rs} \times a^{-1} = a \times a^{-1}$ cioè $a^{rs-1} = a^0 = e$ e quindi $rs-1$ deve essere un multiplo di n , $rs-1 = kn$, ossia $rs - kn = 1$ per qualche intero k , ciò significa (cfr. identità di Bezout) che $1 = \text{M.C.D.}(r, n)$, cioè r e n sono coprimi fra loro.

Quindi se a è generatore di un gruppo ciclico finito di ordine n allora tutte le potenze di a con esponente un numero r primo con n sono generatori di G .

Si prova che: *Ogni sottogruppo di un gruppo ciclico è un gruppo ciclico.*

Più esplicitamente: Ogni sottogruppo di un gruppo ciclico infinito diverso dal sottogruppo unità è un gruppo ciclico infinito, e ogni sottogruppo di un gruppo ciclico finito è un gruppo ciclico finito.

5. Teoremi di Lagrange, Fermat, Eulero.

Di notevole importanza nella teoria dei gruppi finiti è il seguente:

Teorema di Lagrange: *L'ordine di un sottogruppo G' di un gruppo finito G è un divisore dell'ordine del gruppo, cioè $|G'| \mid |G|$.*

Corollari:

1) *Se G' è un sottogruppo proprio di G allora $|G'| \leq |G|/2$.*

2) *Se G è un gruppo finito di ordine n ed $a \in G$ $a^n = e$.*

Infatti, detto m l'ordine di a , per il teorema di Lagrange, m è un divisore di n , cioè $n=km$ da cui $a^n = (a^m)^k = e^k = e$.

3) *Se G è un gruppo finito avente ordine un numero primo p , allora G è ciclico.*

Infatti sia $a \in G$ e $a \neq e$. Posto $H=G(a)$, l'ordine di H è maggiore di 1 e divide p , quindi necessariamente essendo p primo, coincide con p , cioè $H=G(a)=G$.

Si ha inoltre:

Teorema: *Un gruppo G è privo di sottogruppi propri $\hat{U} G$ è finito ed ha per ordine un numero primo p .*

Dimostrazione:

\Leftarrow G non può avere sottogruppi propri, perché l'ordine di un tale sottogruppo dovrebbe dividere l'ordine di G stesso ed essendo tale ordine un numero primo p , gli unici divisori sono se stesso e 1, che corrispondono ai due sottogruppi impropri.

\Rightarrow Sia $a \in G$ con $a \neq e$. Posto $H=G(a)$ dovrà necessariamente essere $G=H$, cioè G è ciclico ed è generato da a .

Dimostriamo che esso è finito; infatti se fosse ciclico infinito le potenze di a ad esponente pari formerebbero un sottogruppo proprio di G , assurdo. Quindi G è ciclico finito di ordine n .

Proviamo che n è primo; infatti se fosse $r \times s = n$ con $1 < r, s < n$, le potenze $e, a^r, (a^r)^2, \dots, (a^r)^{s-1}$ formerebbero un sottogruppo proprio di G di ordine s , e ciò è assurdo essendo G privo di sottogruppi propri. Quindi n è necessariamente primo.

Sull'esistenza di sottogruppi di un gruppo ciclico finito si ha il seguente

Teorema: *Se G è un gruppo ciclico finito di ordine n allora per ogni divisione r di n esiste un unico sottogruppo di ordine r .*

Come applicazione del teorema di Lagrange si può dimostrare il

Teorema di Fermat: Se p è un numero ed $a \in \mathbb{Z}$ è primo con p allora $a^{p-1} \equiv 1 \pmod{p}$.

La tesi equivale a dire che a^{p-1} e 1 divisi per p danno lo stesso resto, cioè la classe dei resti individuata da a^{p-1} è la stessa di quella individuata da 1, cioè $[a^{p-1}] = [1]$ in (\mathbb{Z}_p, \cdot) .

Per ogni numero $n \in \mathbb{N}$ indichiamo con $j(n)$ la cardinalità dell'insieme dei numeri naturali minori di n e primi con n . Essa è una funzione di \mathbb{N} in sè stesso nota come funzione di Eulero.

Si ha che $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ (cioè il prodotto Π è esteso a tutti i numeri primi p che dividono n , compreso sè stesso se n è primo).

Esempio: $\varphi(45) = 45 \times (1 - 1/3) \times (1 - 1/5)$, poiché i divisori primi di 45 sono 3 e 5.

$$\varphi(45) = 45 \times 2/3 \times 4/5 = 24.$$

Chiaramente se n è primo, $\varphi(p) = p - 1$, se n è composto, $\varphi(n) < n - 1$.

Una generalizzazione del precedente teorema di Fermat è il seguente:

Teorema di Eulero: Se $n \in \mathbb{N}$ ed $a \in \mathbb{Z}$ è primo con n \mathbf{P} $a^{j(n)} \equiv 1 \pmod{n}$.

Un numero x è una radice quadrata non banale di 1 se soddisfa l'equazione $x^2 \equiv 1 \pmod{n}$.

Esempio: 6 è una radice quadrata non banale di 1, mod 35.

Legato a quest'ultimo concetto e a quello di numero composto si ha il seguente:

Teorema: Se esiste una radice quadrata non banale di 1, diversa da 1 e -1 ($\equiv n-1$), mod n , allora n è composto.

6. Algebra modulare.

Si è visto che l'insieme delle classi di resto mod n viene indicato con $\mathbb{Z}_n = \{ [0], [1], \dots, [n-1] \}$ e che in esso sono state definite due operazioni, la somma e il prodotto mod n :

$$[a] + [b] = [a + b]$$

$$[a] \times [b] = [a \times b]$$

Tali operazioni sono *ben definite* nel senso che il risultato non dipende dai rappresentati scelti per le classi.

Infatti se $a' \in [a]$ e $b' \in [b]$ sarà $a-a'=kn$ e $b-b'=hn$ e

- sommando membro a membro si ha $(a+b) - (a'+b') = (k+h)n$ cioè $a'+b' \in [a+b]$
- moltiplicando la prima per b e la seconda per a' si ha $ab - a'b = bkn$ e $a'b - a'b' = a'hn$ e sommando membro a membro è $ab - a'b' = (kb + ha')n$ cioè $a'b' \in [ab]$.

Si verifica facilmente che tali operazioni sono associative e commutative pertanto $(\mathbb{Z}_n, +)$ e (\mathbb{Z}_n, \times) risultano essere dei *semigrupp* abeliani.

Rispetto alla somma c'è l'elemento neutro che è la classe $[0]$ ed ogni elemento $[a]$ ha il suo opposto $-[a]$ ossia $[n-a]$ poiché $[a]+[n-a]=[0]$, pertanto $(\mathbb{Z}_n, +)$ è un gruppo, detto *gruppo additivo mod n*, e la sua cardinalità è n .

Denotate le classi di equivalenza con i loro elementi rappresentativi, riportiamo la tabella dell'operazione del gruppo $(\mathbb{Z}_6, +)$.

$+_6$	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

Rispetto alla moltiplicazione, la classe $[1]$ è l'elemento neutro e non tutti gli elementi di \mathbb{Z}_n hanno inverso; solo quegli elementi che sono primi con n hanno inverso. Infatti affinché $[x] \in \mathbb{Z}_n$ sia l'inverso di $[a]$ dovrà aversi $[a][x]=[ax]=[1]$, ciò significa che ax e 1 devono stare nella stessa classe, cioè dovrà esistere un qualche $k \in \mathbb{Z}$ tale che $ax-1=kn$ ossia $ax-kn=1$; ciò non sempre è possibile, lo è solo se (cfr. Identità di Bezout) a ed n sono primi fra loro, cioè se $\text{M.C.D.}(a, n)=1$.

Pertanto posto $\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n \mid \text{M.C.D.}(a, n)=1\}$, (\mathbb{Z}_n^*, \cdot) è un gruppo, detto *gruppo moltiplicativo modulo n*, e la sua cardinalità è $\varphi(n)$.

Esempio:

1. se $n = 15$ denotate sempre le classi di equivalenza con i loro elementi rappresentativi, si ha:
 $\mathbb{Z}_{15} = \{0, 1, \dots, 13, 14\}$, $\varphi(15) = 15 \times (1 - 1/3) \times (1 - 1/5) = (15 \times 2 \times 4) / 15 = 8$.
 $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.
2. se $n = 7$ si ha $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.

7. Anelli, corpi, campi e relative sottostrutture

Si chiama anello un insieme non vuoto A con due operazioni algebriche binarie definite su di esso, una di addizione e una di moltiplicazione $(A, +, \times)$ tali che:

1) $(A, +)$ è un gruppo abeliano cioè:

$\forall a, b, c \in A$ si ha:

- $a + (b + c) = (a + b) + c.$
- $a + b = b + a.$
- $\forall a \in A \exists 0 \in A : a + 0 = 0 + a = a.$
- $\forall a \in A \exists -a \in A : a + (-a) = 0.$

2) (A, \times) è un semigrupp cioè:

$\forall a, b, c \in A$ è

- $a(b c) = (a b)c.$

3) valgono le proprietà distributive della moltiplicazione rispetto all'addizione sia a destra che a sinistra.

$\forall a, b, c \in A$

- $a(b + c) = a b + a c.$
- $(b + c)a = b a + c a.$

$(A, +)$ è detto gruppo additivo di A .

(A, \cdot) è detto semigrupp moltiplicativo di A .

Se la \times gode della proprietà commutativa, A è detto anello commutativo.

Se il semigrupp (A, \cdot) ha elemento unità diverso dallo zero, si indica con 1 e si chiama *identità* (o unità) dell'anello.

Un anello con elemento identità (o unità) ha almeno due elementi, l' 1 e lo 0 .

Proprietà dell'anello.

- 1) $\forall a \in A \exists 0 a = a 0 = 0$
- 2) $\forall a, b \in A \exists (-a) b = a(-b) = -a b$
- 3) $\forall a, b, c \in A \exists a(b-c) = a b - a c$ e $(b-c)a = b a - c a.$

Un elemento $a \neq 0 \in A$ si dice che è un *divisore dello zero* se esiste $b \neq 0 \in A$ tale che $ab=0$ oppure $ba=0$.

L'insieme delle matrici quadrate di ordine n è un esempio di anello con divisori dello zero.

Un anello commutativo privo di divisori dello zero dicesi *dominio d'integrità*.

Esempi di anelli commutativi con elemento identità, o unità, privi di divisori dello zero, sono:

$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$.

$(2\mathbb{Z}, +, \cdot)$ è un esempio di anello commutativo non unitario.

Anello di polinomi.

Sia R un anello commutativo. Con $R[x]$ denotiamo l'insieme dei polinomi nella indeterminata x a coefficienti in R .

Se $f(x) = a_0 + a_1 x + \dots + a_n x^n$ con $a_n \neq 0$, allora n si dice *grado* di $f(x)$ e a_n si chiama *coefficiente direttivo* o *primo coefficiente*.

Se R ha elemento unità 1 e $a_n = 1$, il polinomio $f(x)$ si dice *monico*.

$R[x]$ con l'usuale definizione di addizione e moltiplicazione risulta un anello commutativo, è *l'anello dei polinomi nell'indeterminata x* .

Si verifica che se R è privo di divisori dello zero lo è anche $R[x]$.

$R_n[x]$ indica *l'anello dei polinomi in x di grado $\leq n$* .

Dicesi **corpo** un anello A in cui gli elementi diversi da zero formano un gruppo rispetto alla moltiplicazione, tale gruppo si dice *gruppo moltiplicativo del corpo*.

Dicesi **campo** un corpo in cui la moltiplicazione è commutativa.

Sottostrutture.

Un sottoinsieme H non vuoto ($H \neq \emptyset$) di un anello [corpo , campo] A dicesi *sottoanello* [*sottocorpo* , *sottocampo*] di A se risulta essere un anello [corpo , campo] rispetto alle stesse due operazioni definite in A .

Condizioni caratteristiche.

- Sia A un anello e H un sottoinsieme non vuoto di A , $H \neq \emptyset$ e $H \subseteq A$, si verifica immediatamente:

$$H \text{ sottoanello di } A \Leftrightarrow 1) \forall a, b \in H \Rightarrow a \cdot b \in H \text{ e } 2) \forall a, b \in H \Rightarrow a - b \in H.$$

- Sia K un corpo e H un suo sottoinsieme con almeno due elementi, si ha:

$$H \text{ sottocorpo di } K \Leftrightarrow 1) \forall a, b \in H \Rightarrow a - b \in H \text{ e } 2) \forall a, b \in H, b \neq 0 \Rightarrow a \cdot b^{-1} \in H.$$

8. Omomorfismi fra strutture

Siano G e G' due gruppidi (oppure semigrupperi oppure gruppi).

Un'applicazione $f : G \rightarrow G'$ si dice un *omomorfismo* di G in G' quando, per ogni $a, b \in G$, è $f(ab) = f(a)f(b)$.

Un omomorfismo iniettivo si chiama pure *monomorfismo* od anche una *immersione* di G in G' .

Un omomorfismo suriettivo si chiama pure un *epimorfismo*.

Un omomorfismo biiettivo si dice un *isomorfismo* fra G e G' .

Proposizione: Sia $f : G \rightarrow G'$ un omomorfismo fra gruppi. Allora:

$$(i) \quad f(e) = e'$$

$$(ii) \quad f(a^{-1}) = (f(a))^{-1}$$

(iii) se H è un sottogruppo di G allora $f(H) = \{ a' \in G' \mid \exists a \in H \text{ tale che } f(a) = a' \}$ è un sottogruppo di G' .

(iv) se H' è un sottogruppo di G' allora $f^{-1}(H') = \{ a \in G \mid f(a) \in H' \}$ è un sottogruppo di G .

Dimostrazione:

(i) Da $f(a) = f(ae) = f(a)f(e) = f(a)$ dunque $f(e)$ è elemento neutro di G' .

(ii) Da $e' = f(e) = f(a a^{-1}) = f(a)f(a^{-1})$ segue che $f(a^{-1})$ è l'inverso di $f(a)$, cioè $f(a^{-1}) = (f(a))^{-1}$

(iii) Intanto $f(H)$ non è vuoto perché $e' = f(e) \in f(H)$. Inoltre se $a', b' \in f(H)$ significa che $a' = f(a)$ e $b' = f(b)$ con $a, b \in H$; allora $a'b'^{-1} = f(a)f(b^{-1}) = f(a b^{-1}) \in f(H)$ perché $a b^{-1} \in H$ essendo H un sottogruppo di G .

(iv) Intanto $f^{-1}(H')$ non è vuoto perché $e \in f^{-1}(H')$ in quanto $f(e) = e' \in H'$. Inoltre se $a, b \in f^{-1}(H')$ significa $f(a), f(b) \in H'$; allora $a b^{-1} \in f^{-1}(H')$ perché $f(a b^{-1}) = f(a)f(b)^{-1} \in H'$ essendo H' un sottogruppo di G' .

Nucleo ed immagine di un omomorfismo.

Sia $f : G \rightarrow G'$ un omomorfismo di gruppi. Definiamo *nucleo* di f e lo denotiamo con $\text{Ker } f$ il sottoinsieme di G : $\text{Ker } f = \{ a \in G \mid f(a) = e' \}$.

Definiamo *immagine* di f e la denotiamo con $\text{Im } f$, il sottoinsieme di G' :

$$\text{Im } f = \{ a' \in G' \mid \text{esiste } a \in G \text{ tale che } f(a) = a' \}.$$

Proposizione: Sia $f : G \rightarrow G'$ un omomorfismo di gruppi. Si ha:

- (i) $\text{Ker } f$ è un sottogruppo di G .
- (ii) $\text{Im } f$ è un sottogruppo di G' .
- (iii) f è iniettiva se e solo se $\text{Ker } f = \{e\}$.
- (iv) f è suriettiva se e solo se $\text{Im } f = G'$.

Dimostrazione:

- (i) È $\text{Ker } f = f^{-1}(\{e'\})$ e quindi basta applicare il punto (iv) della proposizione precedente.
- (ii) È $\text{Im } f = f(G)$ e quindi basta applicare il punto (iii) della proposizione precedente.
- (iii) Se f è iniettiva e $f(a) = e'$, essendo pure $f(e) = e'$ segue $a = e$ cioè $\text{Ker } f = \{e\}$. Viceversa sia $\text{Ker } f = \{e\}$ e siano $a, b \in G$ tali che $f(a) = f(b)$; da ciò segue $e' = f(a)f(b)^{-1} = f(ab^{-1})$ da cui $ab^{-1} \in \text{Ker } f$ quindi $ab^{-1} = e$ cioè $a = b$.

Siano R e R' due anelli (oppure corpi) un'applicazione $f : R \rightarrow R'$ è un omomorfismo di R in R' se $\forall a, b \in R$ risulta:

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

$$2) f(ab) = f(a) \cdot f(b)$$

Per gli omomorfismi tra anelli (o corpi) valgono teoremi analoghi a quelli per gli omomorfismi fra gruppi.

POLINOMI

1. Funzioni polinomiali e polinomi

Sono noti campi infiniti (es. il campo dei complessi \mathbb{C} , quello dei reali \mathbb{R} , quello dei razionali \mathbb{Q}) e campi finiti (es. \mathbb{Z}_p la classe dei resti mod p con p numero primo).

Nel seguito, ove non espressamente detto, indicheremo con K , un qualunque campo.

Dicesi *funzione polinomiale* (o funzione razionale intera) su K , una funzione p di K in se stesso, $p: K \rightarrow K$, tale che $\exists n \in \mathbb{N}$ ($n \geq 0$) e degli elementi $a_i \in K$ tali che $p(\alpha) = a_0 \alpha^0 + a_1 \alpha^1 + \dots + a_n \alpha^n$ $\forall \alpha \in K$.

Essa verrà indicata nel seguente modo:

$$x \rightarrow p(x) = a_0 x^0 + a_1 x^1 + \dots + a_n x^n \quad \forall x \in K$$

Detto F l'insieme di tutte le funzioni polinomiali di K in se stesso, è possibile definire in tale insieme la $+$ e il \cdot , tenendo conto della definizione di $+$ e \cdot nel campo K .

$$(p+q)(x) = p(x)+q(x) \qquad (p \cdot q)(x) = p(x) \cdot q(x) \qquad \forall x \in K$$

Due funzioni polinomiali sono uguali se assumono gli stessi valori in corrispondenza di ogni $x \in K$; cioè si "comportano" allo stesso modo.

F con queste due operazioni è un anello commutativo con elemento unità.

L'elemento neutro rispetto alla $+$, lo zero, è quella funzione polinomiale che associa $\forall x \in K$ l'elemento 0 di K .

La funzione opposta di p è la funzione $-p$ tale che $(-p)(x) = -p(x) \quad \forall x \in K$.

La funzione unità di F è la funzione polinomiale che associa $\forall x \in K$ l'elemento $1 \in K$, ossia la funzione costante uguale a 1 .

Un polinomio $p(x)$ a coefficienti nel campo K , è un'espressione del tipo:

$$p(x) = a_0 + a_1 x + a_1 x^2 + \dots + a_n x^n$$

con $a_i \in K$ e x un'indeterminata.

L'insieme dei polinomi in K si indica con il simbolo $K[x]$.

Due polinomi $p(x) = \sum a_i x^i$ e $q(x) = \sum b_i x^i$ sono uguali se e solo se $a_i = b_i \quad \forall i$, cioè hanno la stessa scrittura formale.

Da quanto detto si ha che le funzioni polinomiali e i polinomi vengono indicati allo stesso modo ma chiaramente si tratta di concetti diversi.

L' applicazione $\psi: K[x] \rightarrow F$ che ad ogni polinomio $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_n x^n \in K[x]$ associa la funzione $p(x)$ che manda ogni $c \in K$ in $p(c) = a_0 + a_1c + a_2c^2 + \dots + a_n c^n$ di K è suriettiva ma, in generale, non è iniettiva, infatti può accadere che due polinomi diversi danno luogo alla stessa funzione polinomiale.

Esempi:

1) Sia $K[x] = \mathbf{Z}_3[x]$; i due polinomi: $p(x) = x^2$ e $q(x) = x^3 + x^2 - x$ danno luogo alla stessa funzione polinomiale infatti:

$$\begin{array}{ll} p(0) = 0 & q(0) = 0 \\ p(1) = 1 & q(1) = 1 \\ p(2) = 1 & q(2) = 1 \end{array}$$

2) Sia $K[x] = \mathbf{Z}_2[x]$; i due polinomi: $p(x) = x - 1$ e $q(x) = x^3 - 1$ danno luogo alla stessa funzione polinomiale essendo: $p(0) = q(0) = 1$ e $p(1) = q(1) = 0$.

Ciò perchè $K = \mathbf{Z}_3, \mathbf{Z}_2$ sono finiti, se invece K fosse infinito, allora l' applicazione ψ sarebbe biunivoca e in tal caso due polinomi che definiscono la stessa funzione polinomiale sono uguali come polinomi.

$K[x]$ con le stesse operazioni definite in F è un anello commutativo con elemento 1; il polinomio nullo è quello i cui coefficienti sono tutti nulli, l' opposto del polinomio $p(x)$ è quel polinomio che ha come coefficienti gli opposti dei coefficienti di $p(x)$.

Per *grado* di un polinomio $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_n x^n$, $\text{deg}p(x)$, si intende l' intero n se $a_n \neq 0$, tale coefficiente è detto *coefficiente direttivo*.

Il grado di $p(x) = a_0$, cioè di una costante $\neq 0$ è zero, mentre al polinomio nullo (tutti i coefficienti nulli) non si attribuisce alcun grado (oppure si dà grado $-\infty$).

Si verifica facilmente che l'anello $K[x]$ è un dominio di integrità (cioè privo di divisori dello zero). Sono note le relazioni fra i gradi di due polinomi e quelli della loro somma e del loro prodotto.

$$\deg(p(x) + q(x)) \leq \max(\deg p(x), \deg q(x)) \quad \deg(p(x) \cdot q(x)) = \deg p(x) + \deg q(x)$$

2. Divisione, M.C.D., m.c.m. tra due polinomi

La struttura dei polinomi in un determinato campo, è simile a quella degli interi, nel senso che gran parte delle definizioni e proprietà degli interi (quali teorema della divisione, M.C.D., m.c.m., fattorizzazione,...) si danno in modo analogo per i polinomi.

Teorema della divisione. Sia K un campo e $K[x]$ l'anello dei polinomi nella indeterminata x a coefficienti in K . Siano $f(x)$ e $g(x)$ due polinomi $\in K[x]$ con $g(x) \neq 0$ (diverso dal polinomio nullo). Esiste una ed una sola coppia di polinomi $q(x), r(x) \in K[x]$ tali che

$$f(x) = g(x)q(x) + r(x) \text{ con } \deg q(x) = \deg f(x) - \deg g(x), r(x) = 0 \text{ (polinomio nullo) o } \deg r(x) < \deg g(x)$$

La dimostrazione si fa per induzione sul grado di $f(x)$, che si suppone maggiore di quello di $g(x)$, perché se $f(x) = 0$ si ha $0 = 0 \cdot g(x) + 0$ e se $\deg f(x) < \deg g(x)$ si ha $f(x) = g(x) \cdot 0 + f(x)$, inoltre essa dà una procedura per calcolare effettivamente il quoziente e il resto della divisione. Applicheremo tale procedura per determinare il MCD fra due polinomi mediante l'algoritmo di Euclide delle divisioni successive nel paragrafo 6 "Complementi ed esempi". Nel caso particolare che il divisore $g(x) = x - a$, per "ottenere" il quoziente e il resto della divisione si preferisce applicare la "regola di Ruffini".

Se $r(x) = 0$ allora si dice che $f(x)$ è divisibile per $g(x)$, oppure $g(x)$ divide $f(x)$ in $K[x]$.

M.C.D.

Siano $f(x), g(x) \in K[x]$. Un polinomio $d(x) \in K[x]$ è un M.C.D. fra $f(x)$ e $g(x)$

1. se $d(x)|f(x)$ e $d(x)|g(x)$
2. se $q(x)|f(x)$ e $q(x)|g(x)$ allora $q(x)|d(x)$

Come per i numeri, due polinomi hanno più di un M.C.D.: es. $x^2 - 1$ e $6x^2 - 12x + 6$ hanno come M.C.D. $(x - 1), (2x - 2), (3x - 3), \dots$, i quali si dividono l'uno l'altro.

L'algoritmo di Euclide, delle divisioni successive, che ci garantisce l'esistenza del M.C.D. fra interi, vale anche per i polinomi, per cui l'ultimo resto non nullo, nelle divisioni successive, fra due polinomi non entrambi nulli è un loro M.C.D.

Due polinomi $f(x)$ e $g(x)$ si dicono *associati* se esiste una costante non nulla a tale che $f(x) = a g(x)$.

Es. se $f(x) = 4x^2 + 12x - 4$ e $g(x) = x^2 + 3x - 1$ si ha $f(x) = 4 g(x)$.

“Essere associati” è una relazione di equivalenza e in ogni classe di polinomi c'è un polinomio il cui coefficiente direttivo è 1, esso è detto *monico*. Per convenzione il MCD di due polinomi è quel MCD monico.

Vale l'*identità di Bezout*: Se $d(x) = \text{M.C.D.}(f(x), g(x))$ allora esistono in $K[x]$ $h(x)$ ed $l(x)$ tali che

$$d(x) = f(x) \cdot h(x) + g(x) \cdot l(x)$$

Se $1 = \text{M.C.D.}(f(x), g(x))$ allora $f(x)$ e $g(x)$ sono detti coprime.

m.c.m.

Siano $f(x), g(x) \in K[x]$. Un polinomio $m(x) \in K[x]$ è un m.c.m. fra $f(x)$ e $g(x)$

3. se $f(x) | m(x)$ e $g(x) | m(x)$

4. se $f(x) | c(x)$ e $g(x) | c(x)$ allora $m(x) | c(x)$

3. Teorema di Ruffini e Radice multipla

Se $f(x) \in K[x]$, un elemento $a \in K$ si dice che è una radice o zero di $f(x)$ se risulta $f(a) = 0$.

Per il polinomio nullo, poiché tutti i coefficienti sono nulli, si ha che $\forall a \in K$ è una sua radice.

Teorema di Ruffini

Se $f(x) \in K[x]$ ed $a \in K$, a è una radice di $f(x)$ $\hat{U} (x - a) | f(x)$

Dimostrazione.

\Rightarrow Dividiamo $f(x)$ per $(x - a)$, si ha: $f(x) = (x - a)q(x) + r(x)$ con $\text{degr}(r) < 1$, facciamo vedere che è $r(x) = 0$; infatti essendo a radice è $f(a) = 0$ cioè $0 = f(a) = 0q(a) + r(a) = r(a)$

\Leftarrow Se è $(x - a) | f(x)$ si ha $f(x) = (x - a)q(x)$ è quindi per $x = a$ è $f(a) = 0$ cioè a è radice di $f(x)$.

Corollario. Un polinomio $f(x) \in K[x]$ di grado $n \neq 0$ ha al più n radici.

Dimostrazione. La dimostrazione viene fatta per induzione su n .

Se $n = 0 \Rightarrow f(x)$ è costante e non ha radici.

Se $n > 0 \Rightarrow f(x)$ o non ha radici e il teorema è vero, oppure ha una radice a e, per il teorema di Ruffini, si ha $f(x) = (x - a)q(x)$ in cui $q(x)$ ha grado $n - 1$. Poiché le radici di $f(x)$ sono a e le radici di q , che per ipotesi induttiva ha al più $n - 1$ radici, segue che $f(x)$ ha al più n radici.

Dal corollario segue che se $\alpha_1, \alpha_2, \dots, \alpha_r$, sono radici di $f(x)$ tutte distinte, allora $f(x)$ è divisibile per:

$$\left\{ \begin{array}{l} x - \alpha_1 \\ x - \alpha_2 \\ \dots \\ \dots \\ x - \alpha_r, \text{ con } r \leq n \end{array} \right. \Rightarrow f(x) \text{ è divisibile per } (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_r).$$

Se $f(x) \in \widehat{K}[x]$ e α è una radice di $f(x)$, diremo che α ha molteplicità s se s è il massimo intero tale che $(x - \alpha)^s \mid f(x)$.

Cioè α ha molteplicità s per $f(x)$ se $(x - \alpha)^s \mid f(x)$ e $(x - \alpha)^{s+1} \nmid f(x)$.

Si ricordi che la derivata prima di un polinomio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ è:

$$f'(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1$$

Si prova che $(f(x) + g(x))' = f'(x) + g'(x)$ e $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$

Teorema Se $f(x) \in \widehat{K}[x]$ e α è una sua radice, α è radice di molteplicità $\geq 2 \iff f'(\alpha) = 0$

Dimostrazione.

\Rightarrow Se α è radice multipla si ha $(x - \alpha)^2 \mid f(x)$ cioè $f(x) = (x - \alpha)^2 q(x)$ da cui derivando è:

$$f'(x) = 2(x - \alpha)q(x) + (x - \alpha)^2 q'(x) \text{ e posto } x = \alpha \Rightarrow f'(\alpha) = 0.$$

\Leftarrow Essendo α una radice, per il teorema di Ruffini è $(x - \alpha) \mid f(x)$ cioè $f(x) = (x - \alpha)q(x)$ da cui derivando si ha: $f'(x) = q(x) + (x - \alpha)q'(x)$ ed essendo $f'(\alpha) = 0$ segue che $q(\alpha) = 0$ ossia $(x - \alpha) \mid q(x)$ cioè $q(x) = (x - \alpha)q_1(x)$ da cui sostituendo è $f(x) = (x - \alpha)^2 q_1(x)$ cioè α ha molteplicità almeno 2.

Alla luce di questa definizione di molteplicità nel corollario di Ruffini, per cui ogni $f(x) \in K[x]$ di grado $n \geq 0$ ha al più n radici, va precisato che ognuna delle radici va "contata" con la sua molteplicità.

4. Riducibilità

Sia $f(x) \in K[x]$ un polinomio non nullo. Si dice che $f(x)$ è *riducibile* in $K[x]$ se esistono $g(x)$ e $h(x)$ non costanti (cioè di grado ≥ 1) tali che $f(x) = g(x) \cdot h(x)$.

Si dice che $f(x)$ è *irriducibile* in $K[x]$ se non è costante e non esistono $g(x)$ e $h(x) \in K[x]$ con $\deg g(x) \geq 1$ e $\deg h(x) \geq 1$ tale che $f(x) = g(x) \cdot h(x)$.

La riducibilità o meno di un polinomio, in un determinato campo K , dipende dal campo stesso.

Esempi:

$x + a$ è irriducibile in $K[x]$ qualunque sia K .

$x^2 + 1$ è irriducibile in $R[x]$ e in $Z_3[x]$, è riducibile in $C[x]$ ($x^2 + 1 = (x - 1)(x + 1)$)

e in $Z_2[x]$ ($x^2 + 1 = (x + 1)^2$)

$x^2 - 2$ è irriducibile in $Q[x]$, è riducibile in $R[x]$ ($x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$)

$x^2 + 2$ è riducibile in $C[x]$ e $Z_2[x]$, è irriducibile in $Q[x]$

Nella riducibilità dei polinomi, i polinomi irriducibili hanno lo stesso ruolo che hanno i numeri primi nella fattorizzazione degli interi, e come negli interi si dimostra che *ogni polinomio $f(x)$ di grado ≥ 1 si fattorizza in modo unico, a meno dell'ordine, nel prodotto di polinomi irriducibili.*

Determiniamo i polinomi irriducibili.

Nel campo complesso C , (come pure in R) la riducibilità o irriducibilità di un polinomio è conseguenza immediata del seguente:

Teorema Fondamentale dell'Algebra: *Ogni polinomio $f(x) \in C[x]$ di grado ≥ 1 ammette una radice in C .*

Corollario. *Ogni polinomio $f(x)$ di grado n ammette in C esattamente n radici.*

Dimostrazione. Se α_1 è una radice di $f(x)$, per il teorema di Ruffini, si ha $f(x) = (x - \alpha_1)q(x)$, con $q(x)$ di grado $n - 1$ e a coefficienti in C ; quindi per il teorema fondamentale dell'algebra $q(x)$ avrà la radice $\alpha_2 \in C$ pertanto proseguendo sarà $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$.

Quindi ogni polinomio di $C[x]$ si fattorizza in fattori lineari

In definitiva

i polinomi in $C[x]$ irriducibili in C , sono tutti e soli i polinomi di 1° grado.

Nel campo reale \mathbf{R} , osserviamo che: se $f(x)$ è a coefficienti reali e $\alpha \in \mathbf{C}$ è una radice di $f(x)$, anche α' (coniugato di α) è una radice di $f(x)$, e inoltre essendo $\alpha + \alpha'$, $\alpha \cdot \alpha'$ elemento di \mathbf{R} si ha che

$$(x - \alpha)(x - \alpha') = ax^2 + bx + c$$

con $a, b \in \mathbf{R}$. Si prova che

i polinomi in $\mathbf{R}[x]$ irriducibili su \mathbf{R} sono tutti e soli i polinomi di 1° grado e quelli di 2° grado con $\Delta \neq 0$.

Pertanto:

Ogni polinomio $f(x)$ di grado ≥ 3 è riducibile in \mathbf{R} .

Se $\deg f(x) = 3$ allora il polinomio avrà necessariamente una radice reale e le altre due saranno reali (distinte o no) oppure immaginarie e coniugate. Quindi ogni polinomio $f(x)$ di terzo grado è riducibile in tre fattori lineari (distinti o no) oppure in un fattore lineare e uno di secondo grado irriducibile.

Se $\deg f(x) > 3$ dispari allora il polinomio avrà sicuramente una radice reale per cui nella sua fattorizzazione ci sarà un fattore lineare.

Se $\deg f(x) > 3$ pari e il polinomio non ha radici reali allora può essere decomposto in fattori di 2° grado con radici immaginarie.

NOTA: Alla luce di quanto detto se $f(x)$ non ha radici in \mathbf{R} non vuol dire che esso è irriducibile.

Esempi:

I polinomi $x^4 + 3x^2 + 2$ e $x^4 + 1$ non hanno radici reali, ma sono riducibili, si ha infatti:

$$\begin{aligned} x^4 + 3x^2 + 2 &= (x^2 + 1)(x^2 + 2) \\ x^4 + 1 &= x^4 + 1 + 2x^2 - 2x^2 = (x^2 + 1)^2 - 2x^2 = (x^2 + 1 - \sqrt{2}x)(x^2 + 1 + \sqrt{2}x) \end{aligned}$$

Pertanto la mancanza di radici nel campo \mathbf{R} non assicura, in generale, l'irriducibilità, tranne nel caso in cui il grado di $f(x)$ è 2.

Nel campo dei razionali \mathbf{Q} , non siamo in grado di caratterizzare i polinomi irriducibili. Polinomi irriducibili in $\mathbf{Q}[x]$ ce ne sono di tutti i gradi. Esempio $x^n - 2$ in $\mathbf{Q}[x]$ è irriducibile qualunque sia n .

Ci limitiamo a far vedere come la irriducibilità in $\mathbf{Q}[x]$ è legata allo studio dei polinomi in $\mathbf{Z}[x]$.

Infatti se $f(x) = \frac{r_n}{s_n}x^n + \frac{r_{n-1}}{s_{n-1}}x^{n-1} + \dots + \frac{r_1}{s_1}x + \frac{r_0}{s_0}$ con $r_i, s_i \in \mathbf{Z}$ e $s_i \neq 0$,

possiamo ad esso associare un polinomio $g(x) \in \mathbf{Z}[x]$ moltiplicando $f(x)$ stesso per il m.c.m, s , dei suoi coefficienti $s_n, s_{n-1}, \dots, s_1, s_0$. Si ha infatti:

$$sf(x) = g(x) \in \mathbf{Z}[x] \quad \text{con} \quad g(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \text{con} \quad a_i \in \mathbf{Z}$$

Esempio:

$$f(x) = 3/8x^2 + 6/7x + 3/2 \quad \text{m.c.m.}(8, 7, 2) = 56$$

$$g(x) = 56 f(x) = 21x^2 + 48x + 84 = 3(7x^2 + 16x + 28)$$

Pertanto lo studio dei polinomi a coefficienti in \mathbf{Q} è ricondotto allo studio dei polinomi a coefficienti in \mathbf{Z} ; ed essendo $f(x)$ e $g(x)$ associati, ne viene che $g(x)$ sarà irriducibile in $\mathbf{Q}[x]$ se e solo se lo è $f(x)$.

Sia $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbf{Z}[x]$, $f(x)$ si dice *primitivo* se il $\text{MCD}(a_n, a_{n-1}, \dots, a_1, a_0) = 1$.

Chiaramente se uno dei coefficienti $a_i = 1$, il polinomio è primitivo.

Dato un polinomio $g(x) \in \mathbf{Z}[x]$, il polinomio primitivo ad esso associato è il polinomio $g(x)/d$ dove $d = \text{M.C.D.}$ dei coefficienti di $g(x)$.

Per quanto concerne la riducibilità in $\mathbf{Z}[x]$ e $\mathbf{Q}[x]$, si ha il seguente teorema, meglio noto come

Lemma di Gauss: *Sia $f(x) \in \mathbf{Z}[x]$ primitivo: $f(x)$ è decomponibile in $\mathbf{Q}[x]$ \Leftrightarrow $f(x)$ è decomponibile in $\mathbf{Z}[x]$.*

Nella dimostrazione si sfrutta il fatto che il prodotto di due polinomi primitivi è ancora un polinomio primitivo.

Esempi:

1) $f(x) = 2x^2 - 3x + 1 \in \mathbf{Z}[x]$, primitivo, esso è decomponibile in $\mathbf{Q}[x]$, $f(x) = 2(x-1)(x - \frac{1}{2})$, è

decomponibile pure in $\mathbf{Z}[x]$, si ha infatti $2x^2 - 3x + 1 = (x-1)(2x-1)$.

2) $x^4 + 10x^2 + 24 \in \mathbf{Z}[x]$, primitivo, è riducibile in $\mathbf{Q}[x]$, $f(x) = \left(\frac{2}{3}x^2 + \frac{16}{6}\right)\left(\frac{3}{2}x^2 + 9\right)$ è

decomponibile pure in $\mathbf{Z}[x]$, si ha infatti $x^4 + 10x^2 + 24 = (x^2 + 4)(x^2 + 6)$.

Dal lemma di Gauss segue che *un polinomio primitivo in $\mathbf{Z}[x]$ è irriducibile in $\mathbf{Q}[x]$ se e solo se lo è in $\mathbf{Z}[x]$.*

Il seguente teorema ci dà delle informazioni sulle radici razionali di un polinomio a coefficienti interi, pertanto permette di stabilire se esso è riducibile con fattori lineari in $\mathbf{Q}[x]$ (e quindi in $\mathbf{Z}[x]$).

Teorema. Se $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x]$ e $\mathbf{a} = r/s$ è sua radice razionale, con $M.C.D.(r, s) = 1$, allora r divide a_0 ed s divide a_n .

Dimostrazione. Infatti avendosi $a_n r^n/s^n + a_{n-1} r^{n-1}/s^{n-1} + \dots + a_1 r/s + a_0 = 0 \Rightarrow$

$$a_n r^n + a_{n-1} r^{n-1} s + \dots + a_1 r s^{n-1} + a_0 s^n = 0 \Rightarrow r(a_n r^{n-1} + a_{n-1} r^{n-2} s + \dots + a_1 s^{n-1}) = -a_0 s^n$$

ed essendo $M.C.D.(r, s) = 1 \Rightarrow r \mid a_0$

analogamente $-a_n r^n = s(a_{n-1} r^{n-1} + \dots + a_1 r s^{n-2} + a_0 s^{n-1})$ ed essendo $M.C.D.(r, s) = 1 \Rightarrow r \mid a_n$

Corollario. Se $f(x)$ è monico ($a_n = 1$) e \mathbf{a} è una sua radice razionale allora \mathbf{a} è intera e divide il termine noto.

Il suddetto teorema, conosciuto anche come “Criterio della radice” per la riducibilità di un polinomio a coefficienti interi in $\mathbb{Q}[x]$, in pratica ci permette di trovare le eventuali radici razionali di un polinomio a coefficienti interi; esse vanno cercate nell’insieme delle frazioni r/s dove r è un divisore del termine noto ed s è un divisore del coefficiente direttivo.

5. Criteri di Irreducibilità

Diamo ora due criteri che ci permettono di affermare se un polinomio a coefficienti interi è irriducibile in tale campo; essi danno delle condizioni sufficienti per l’irriducibilità, ma non necessarie.

1) **Criterio di Eisenstein**

Sia $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ un polinomio in $\mathbb{Z}[x]$ con $a_n \neq 0$, e supponiamo che esiste un numero primo p tale che:

1. $p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}, p \nmid a_n$

(p divide ogni coefficiente di $f(x)$ tranne quello di grado massimo)

2. $p^2 \nmid a_0$. (p^2 non divide il termine noto)

Allora il polinomio $f(x)$ è irriducibile in $\mathbb{Z}[x]$.

Dimostrazione. Supponiamo che $f(x)$ sia riducibile nel prodotto dei due fattori

$$b(x) = b_r x^r + b_{r-1} x^{r-1} + \dots + b_1 x + b_0 \quad \text{di grado } r$$

$$c(x) = c_s x^s + c_{s-1} x^{s-1} + \dots + c_1 x + c_0 \quad \text{di grado } s,$$

cioè si può scrivere:

$$f(x) = b(x)c(x) = (b_r x^r + b_{r-1} x^{r-1} + \dots + b_1 x + b_0)(c_s x^s + c_{s-1} x^{s-1} + \dots + c_1 x + c_0).$$

Confrontando i coefficienti si ha $a_0 = b_0 c_0$ e poiché $p \mid a_0$ e $p^2 \nmid a_0$ cioè $p \mid b_0 c_0$ e $p^2 \nmid b_0 c_0$ segue che p_0 divide uno solo dei coefficienti b_0, c_0 . Supponiamo che $p \mid b_0, p \nmid c_0$. Inoltre p non può dividere tutti gli b_i altrimenti dividerebbe tutti i coefficienti di $f(x)$, cioè gli a_i . Sia k il minimo intero tale che $p \nmid b_k$, cioè $p \mid b_0, p \mid b_1, \dots, p \mid b_{k-1}$ e $p \nmid b_k$. Ma $a_k = b_k c_0 + b_{k-1} c_1 + \dots + b_1 c_{k-1} + b_0 c_k$ è divisibile per p , da cui segue che $p \mid b_k c_0$ e ciò è assurdo perché p non divide né b_k né c_0 .

Poiché supporre $f(x)$ riducibile in $\mathbf{Z}[x]$ porta ad un assurdo, ne segue che $f(x)$ è irriducibile in $\mathbf{Z}[x]$.

Un altro criterio di irriducibilità è il criterio del Mod n .

Preliminarmente osserviamo che, fissato un intero positivo n , l'applicazione $\varphi: \mathbf{Z} \rightarrow \mathbf{Z}_n$, che associa ad ogni intero la classe resto modulo n a cui tale intero appartiene, è un omomorfismo.

L'applicazione $\bar{\varphi}: \mathbf{Z}[x] \rightarrow \mathbf{Z}_n[x]$, che associa ad ogni polinomio $f(x) \in \mathbf{Z}[x]$ il polinomio $\bar{f}(x) \in \mathbf{Z}_n[x]$ ottenuto da $f(x)$ riducendo i suoi coefficienti mod n , è ancora un omomorfismo.

Chiaramente se il grado di $f(x) \in \mathbf{Z}[x]$ è m allora il grado di $\bar{f}(x) \in \mathbf{Z}_n[x]$ è $\leq m$.

Se $n \nmid a_m$ sarà $\deg f(x) = \deg \bar{f}(x)$.

2) Criterio del Mod n

Siano:

$$\sim f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0 \in \mathbf{Z}[x] \text{ primitivo,}$$

$$\sim n \text{ un intero positivo che non divide il coefficiente direttivo di } f(x) \ a_m, \ n \nmid a_m$$

$$\sim \bar{f}(x) \text{ il polinomio ottenuto da } f(x) \text{ riducendo i suoi coefficienti mod } n \ (\bar{f}(x) \in \mathbf{Z}_n[x]).$$

Se $\bar{f}(x)$ è irriducibile in $\mathbf{Z}_n[x]$ \mathbf{P} $f(x)$ è irriducibile in $\mathbf{Q}[x]$ (e quindi in $\mathbf{Z}[x]$).

Questo criterio è molto utile perché i polinomi in $\mathbf{Z}_n[x]$ di grado $\leq m$ sono esattamente n^{m+1}

(tante sono le possibili scelte degli $m + 1$ coefficienti di un polinomio di grado $\leq m$ in $\mathbf{Z}_n[x]$) e pertanto è possibile stabilire se un polinomio di $\mathbf{Z}_n[x]$ sia riducibile o no in tale campo mediante un numero finito di prove.

Inoltre il suddetto criterio ci dà informazioni sulla irriducibilità o meno di polinomi per i quali non è possibile applicare il criterio di Eisenstein.

6. Complementi ed esempi

1. Ricordiamo il procedimento dell' algoritmo di Euclide delle divisioni successive:

Se $f(x)$ e $g(x)$ sono due polinomi operando con le divisioni successive si ha:

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

$$g(x) = r(x) q_1(x) + r_1(x)$$

$$r(x) = r_1(x) q_2(x) + r_2(x)$$

$$r_1(x) = r_2(x) q_3(x) + r_3(x)$$

..... e l'ultimo resto non nullo è un MCD fra $f(x)$ e $g(x)$

Esempi.

Trovare il MCD applicando l' algoritmo di Euclide fra

a) $f(x) = x^5 + x^4 + x + 1$ e $g(x) = x^3 - 3x - 2$ in $\mathbb{R}[x]$;

b) $f(x) = x^4 + 7x^2 + 3$ e $g(x) = x^2 + x + 2$ in $\mathbb{Z}_{11}[x]$

a) $f(x) = x^5 + x^4 + x + 1$ e $g(x) = x^3 - 3x - 2$

$$\begin{array}{r} x^5 + x^4 + 0x^3 + 0x^2 + x + 1 \quad \left| \begin{array}{l} x^3 + 0x^2 - 3x - 2 \\ \hline x^2 + x + 3 \end{array} \right. \\ \hline x^5 + 0 - 3x^3 - 2x^2 \\ \hline = x^4 + 3x^3 + 2x^2 + x + 1 \\ \hline x^4 + 0 - 3x^2 - 2x \\ \hline = 3x^3 + 5x^2 + 3x + 1 \\ \hline 3x^3 + 0 - 9x - 6 \\ \hline = 5x^2 + 12x + 7 \end{array}$$

$$q(x) = x^2 + x + 3$$

$$r(x) = 5x^2 + 12x + 7$$

$$\begin{array}{r} x^3 + 0x^2 - 3x - 2 \quad \left| \begin{array}{l} 5x^2 + 12x + 7 \\ \hline x/5 - 12/25 \end{array} \right. \\ \hline x^3 + 12/5x^2 + 7/5x \\ \hline = -12/5x^2 + 22/5x - 2 \\ \hline -12/5x^2 + 144/25x - 84/25 \\ \hline = 34/25x + 34/25 \end{array}$$

$$q_1(x) = \frac{x}{5} - \frac{12}{25} \quad r_1(x) = \frac{34}{25}x + \frac{34}{25}$$

$$\begin{array}{r} 5x^2 + 12x + 7 \\ \underline{5x^2 + 5x} \\ 7x + 7 \\ \underline{7x + 7} \\ 0 \end{array} \quad \begin{array}{l} \left| \frac{34}{25}x + \frac{34}{25} \right. \\ \hline \frac{125}{34}x + \frac{175}{34} \end{array}$$

$$q_2(x) = \frac{125}{34}x + \frac{175}{34} \quad r_2(x) = 0$$

L'ultimo resto non nullo è $\frac{34}{25}(x + 1)$, questo è un M.C.D.; per convenzione il MCD è fra tutti i MCD quello monico, cioè $x + 1$.

b) $f(x) = x^4 + 7x^2 + 3$ e $g(x) = x^2 + x + 2$ in $\mathbb{Z}_{11}[x]$

$$\begin{array}{r} x^4 + 0x^3 + 7x^2 + 0x + 3 \\ \underline{x^4 + x^3 + 2x^2} \\ -x^3 + 5x^2 + 0x + 3 \\ \underline{10x^3 + 5x^2 + 0x + 3} \\ 10x^3 + 10x^2 + 9x \\ \underline{6x^2 + 2x + 3} \\ 6x^2 + 6x + 1 \\ \underline{6x^2 + 6x + 1} \\ 0 \end{array} \quad \begin{array}{l} \left| x^2 + x + 2 \right. \\ \hline x^2 + 10x + 6 \end{array}$$

$$q(x) = x^2 + 10x + 6 \quad r(x) = 7x + 2$$

$$\begin{array}{r} x^2 + x + 2 \\ \underline{x^2 + 5x} \\ 7x + 2 \\ \underline{7x + 2} \\ 0 \end{array} \quad \begin{array}{l} \left| 7x + 2 \right. \\ \hline 8x + 1 \end{array} \quad (\text{l' inverso di } 7 \text{ in } \mathbb{Z}_{11} \text{ è } 8, \text{ cfr tabella moltiplicativa.})$$

$7x + 2$ è un M.C.D. di $f(x)$ e $g(x)$, quello monico si ottiene moltiplicando il M.C.D. trovato per 8,

$$56x + 16 = \boxed{x + 5}$$

Z_{11}	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Tabella moltiplicativa di Z_{11}

2. Determinare tutti i polinomi irriducibili di 2° e 3° grado in $Z_2[x]$ e in $Z_3[x]$.

I polinomi di grado $\leq m$ in Z_n sono tanti quante le disposizioni con ripetizione di n elementi su $m+1$ posti, cioè n^{m+1} .

I polinomi irriducibili di grado ≤ 2 in $Z_2[x]$ sono $2^3 = 8$, di cui quattro hanno il coefficiente direttivo nullo e quattro uguale a uno, pertanto i polinomi di 2° grado sono i seguenti quattro:

$$a x^2 + b x + c$$

1	0	0	x^2
1	0	1	$x^2 + 1 = (x + 1)^2$
1	1	0	$x^2 + x = x(x + 1)$
1	1	1	$x^2 + x + 1$ Irriducibile

I polinomi irriducibili di grado ≤ 3 in $Z_2[x]$ sono $2^4 = 16$. Di questi otto hanno il coefficiente direttivo nullo e otto uguale a uno, pertanto i polinomi di 3° grado sono i seguenti otto:

$$a x^3 + b x^2 + c x + d$$

1	0	0	0	x^3
1	1	0	0	$x^3 + x^2 = x^2(x + 1)$
1	0	1	0	$x^3 + x = x(x + 1)^2$
1	0	0	1	$x^3 + 1 = (x + 1)(x^2 + x + 1)$
1	1	1	0	$x^3 + x^2 + x = x(x^2 + x + 1)$
1	1	0	1	$x^3 + x^2 + 1$ Irriducibile
1	0	1	1	$x^3 + x + 1$ Irriducibile
1	1	1	1	$x^3 + x^2 + x + 1 = (x + 1)^3$

I polinomi di grado ≤ 2 in $Z_3[x]$ sono $3^3 = 27$. Di questi 9 hanno coefficiente direttivo zero, 9 sono monici (coefficiente direttivo uno), 9 sono non monici (coefficiente direttivo due).

$ax^2 + bx + c$				$ax^2 + bx + c$			
2	0	0	$2x^2$	1	0	0	x^2
2	1	1	$2x^2 + x + 1$	1	1	1	$x^2 + x + 1 = (x+2)^2$
2	2	2	$2x^2 + 2x + 2 = 2(x+2)^2$	1	2	2	$x^2 + 2x + 2$ Irriducibile
2	0	1	$2x^2 + 1 = 2(x+1)(x+2)$	1	0	1	$x^2 + 1$ Irriducibile
2	1	0	$2x^2 + x = x(2x+1)$	1	1	0	$x^2 + x = x(x+1)$
2	0	2	$2x^2 + 2$ Irriducibile	1	0	2	$x^2 + 2 = (x+2)(x+1)$
2	2	0	$2x^2 + 2x = 2x(x+1)$	1	2	0	$x^2 + 2x = x(x+2)$
2	1	2	$2x^2 + x + 2 = 2(x+1)^2$	1	1	2	$x^2 + x + 2$ Irriducibile
2	2	1	$2x^2 + 2x + 1$ Irriducibile	1	2	1	$x^2 + 2x + 1 = (x+1)^2$

I polinomi di grado ≤ 3 in $\mathbb{Z}_3[x]$ sono $3^4 = 81$ di cui 27 hanno coefficiente direttivo zero, 27 sono monici (coefficiente direttivo 1) e 27 hanno coefficiente direttivo 2.

Riportiamo i coefficienti dei 27 polinomi monici; da quest'ultimi è facile ottenere i coefficienti dei polinomi con coefficiente direttivo 2. Per determinare i polinomi irriducibili si procede caso per caso come prima.

$ax^3 + bx^2 + cx + d$				
1	1	0	0	$x^3 + x^2$
1	1	1	1	$x^3 + x^2 + x + 1$
1	1	2	2	$x^3 + x^2 + 2x + 2$
1	1	0	1	$x^3 + x^2 + 1$
1	1	1	0	$x^3 + x^2 + x$
1	1	0	2	$x^3 + x^2 + 2$
1	1	2	0	$x^3 + x^2 + 2x$
1	1	1	2	$x^3 + x^2 + x + 2$
1	1	2	1	$x^3 + x^2 + 2x + 1$
1	2	0	0	$x^3 + 2x^2$
1	2	1	1	$x^3 + 2x^2 + x + 1$
1	2	2	2	$x^3 + 2x^2 + 2x + 2$
1	2	0	1	$x^3 + 2x^2 + 1$
1	2	1	0	$x^3 + 2x^2 + x$
1	2	0	2	$x^3 + 2x^2 + 2$
1	2	2	0	$x^3 + 2x^2 + 2x$
1	2	1	2	$x^3 + 2x^2 + x + 2$
1	2	2	1	$x^3 + 2x^2 + 2x + 1$
1	0	0	0	x^3
1	0	1	1	$x^3 + x + 1$
1	0	2	2	$x^3 + 2x + 2$
1	0	0	1	$x^3 + 1$
1	0	1	0	$x^3 + x$
1	0	0	2	$x^3 + 2$
1	0	2	0	$x^3 + 2x$
1	0	1	2	$x^3 + x + 2$
1	0	2	1	$x^3 + 2x + 1$

SPAZI VETTORIALI

1. Spazi e sottospazi vettoriali

Definizione: Dato un insieme V non vuoto e un corpo K di sostegno si dice che V è un K -spazio vettoriale o uno spazio vettoriale su K se sono definite un'operazione di somma in V , $+$: $V \times V \rightarrow V$ ed un prodotto esterno, \times : $K \times V \rightarrow V$, per le quali valgono le seguenti otto proprietà:

Proprietà della somma:

1. $\forall \mathbf{v}, \mathbf{w}, \mathbf{z} \in V$ si ha: $(\mathbf{v} + \mathbf{w}) + \mathbf{z} = \mathbf{v} + (\mathbf{w} + \mathbf{z})$ (*proprietà associativa*);
2. $\forall \mathbf{v} \in V \exists \mathbf{0}_V \in V \mid \mathbf{v} + \mathbf{0}_V = \mathbf{v}$ (*esistenza di un elemento neutro*);
3. $\forall \mathbf{v} \in V \exists \mathbf{v}^1 \in V \mid \mathbf{v} + \mathbf{v}^1 = \mathbf{0}_V$ (*esistenza di un opposto*);
4. $\forall \mathbf{v}, \mathbf{w} \in V$ si ha: $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$ (*proprietà commutativa*).

Le proprietà 1 – 4 asseriscono che $(V, +)$ è un gruppo abeliano.

Proprietà del prodotto per un $a \in K$:

1. $\forall \mathbf{v} \in V$ e $\forall a, b \in K$ si ha: $a(b\mathbf{v}) = (ab)\mathbf{v}$;
2. $\forall \mathbf{v} \in V$ si ha: $1\mathbf{v} = \mathbf{v}$.

Proprietà distributive:

1. $\forall \mathbf{v} \in V$ e $\forall a, b \in K$ si ha: $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$;
2. $\forall \mathbf{v}, \mathbf{w} \in V$ e $\forall a \in K$ si ha: $a(\mathbf{v} + \mathbf{w}) = a\mathbf{v} + a\mathbf{w}$.

Dalla definizione di spazio vettoriale seguono:

- I. Il vettore nullo di V , che indicheremo con $\mathbf{0}_V$, è unico;
- II. Per ogni $\mathbf{v} \in V$ il suo opposto, che indicheremo con $-\mathbf{v}$, è unico e questo è uguale a $(-1)\mathbf{v}$. Si scrive: $\mathbf{v} + (-\mathbf{v}) = \mathbf{v} - \mathbf{v}$ e $\mathbf{w} + (-\mathbf{v}) = \mathbf{w} - \mathbf{v}$;
- III. $a\mathbf{v} = \mathbf{0}_V \Leftrightarrow a = \mathbf{0}_K$ oppure $\mathbf{v} = \mathbf{0}_V$;
- IV. Si ha $-(a\mathbf{v}) = a(-\mathbf{v}) = (-a)\mathbf{v} \quad \forall a \in K$ e $\forall \mathbf{v} \in V$.

Dati n vettori $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in V$ e n scalari $a_1, a_2, \dots, a_n \in K$ il vettore $\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n$ si chiama *combinazione lineare* di $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ con coefficienti a_1, a_2, \dots, a_n ed appartiene a V .

Sottospazio: Dato uno spazio vettoriale V su un campo K , si dice che S , con $S \hat{=} V$, è un sottospazio di V se S è uno spazio vettoriale su K rispetto alle operazioni di V .

Teorema: Sia $S \hat{=} V$. S è un sottospazio di V se e solo se " $a, b \hat{=} K$ e " $u, v \hat{=} S$, si ha $au + bv \hat{=} S$.

Dimostrazione: Se S è un sottospazio di V risulta che $au, bv \in S$ e quindi $au + bv \in S$.

Viceversa se $au + bv \in S$, risultano definite in S le stesse operazioni definite in V e quindi la somma è associativa e commutativa. Per $a = b = 1$ si ha $u + v \in S$, per $b = 0$ si ha $au \in S$, per $a = b = 0$ segue $0u = 0v \in S$. Le altre proprietà valgono in S in quanto valgono in V .

Dal teorema precedente segue che S è un sottospazio di V se e solo se:

- 1) $u, v \in S \Rightarrow u + v \in S$;
- 2) $a \in K$ e $u \in S \Rightarrow au \in S$;
- 3) $0v \in S$.

Osservazioni:

- 1) Ogni sottospazio di V deve necessariamente contenere il vettore nullo $0v$. Quindi se $0v \notin S \subset V$ allora S non è sottospazio di V .
- 2) Dalla definizione e dal teorema precedente segue che in ogni spazio vettoriale il vettore nullo costituisce da solo un sottospazio, detto *sottospazio nullo*. V stesso è un sottospazio. Questi due sottospazi $\{0v\}, V$ sono detti *sottospazi banali*.

Teorema di intersezione dei sottospazi: Se S e T sono sottospazi di V , allora $S \cap T$ è un sottospazio di V .

$S \hat{=} V, T \hat{=} V$, con S, T sottospazi $\Rightarrow S \cap T$ sottospazio di V .

Dimostrazione: Se $u, v \in S \cap T$ si ha $u, v \in S$ e $u, v \in T$; quindi poiché S e T sono sottospazi, $\forall a, b \in K$, segue $au + bv \in S$ e $au + bv \in T$. Questo implica che $au + bv \in S \cap T$.

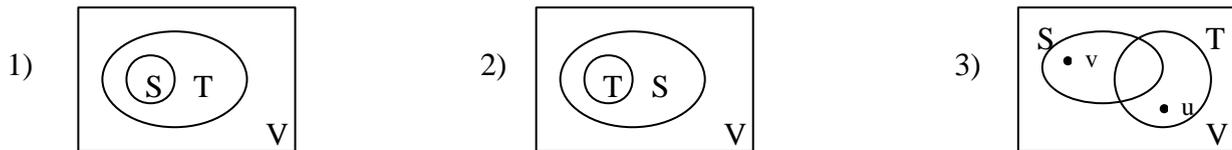
Dal precedente teorema segue:

Teorema: Se A_1, A_2, \dots, A_k sono sottospazi di V , allora $A_1 \cap A_2 \cap \dots \cap A_k = \bigcap_{i=1}^k A_i$ è un sottospazio di V .

Teorema di unione dei sottospazi: Siano S e T sottospazi di V . $S \cup T$ è sottospazio di V $\Leftrightarrow S \subseteq T$ oppure $T \subseteq S$.

Dimostrazione: Se $S \subseteq T$ [$T \subseteq S$] si ha $S \cup T = T$ [$S \cup T = S$] che è un sottospazio di V .

Viceversa se $S \cup T$ è sottospazio di V si possono presentare i seguenti casi:



Nei primi due casi il teorema è ovvio. Il terzo caso non si può presentare. Infatti se $v \in S$ e $v \notin T$, si ha $v \in S - T$ e analogamente se $u \in T - S$, si ha che $v \in S \cup T$ e $u \in S \cup T$ e quindi $u + v \in S \cup T$. Cioè $u + v$ è un elemento di S o di T .

Se $u + v \in S$ si avrebbe $v^1 = u + v$, $u = v^1 - v$ cioè u sarebbe elemento di S il che è assurdo.

Analogamente se $u + v \in T$ si avrebbe $u^1 = u + v$, $v = u^1 - v$ cioè v sarebbe elemento di T il che è assurdo.

Siano S e T due sottospazi di V . si chiama *somma* di S e T l'insieme $S + T = \{s + t \mid s \in S, t \in T\}$. L'insieme $S + T$ è formato da tutti i vettori di V che sono somma di (almeno) un vettore s di S e di un vettore t di T .

L'insieme $S + T$ è un sottospazio di V , in quanto se v_1 e $v_2 \in S + T$, $\forall a_1, a_2 \in K$ segue $a_1 v_1 + a_2 v_2 \in S + T$. Infatti da $v_1 = s_1 + t_1$ e da $v_2 = s_2 + t_2$ segue $a_1 v_1 + a_2 v_2 = a_1(s_1 + t_1) + a_2(s_2 + t_2) = (a_1 s_1 + a_2 s_2) + (a_1 t_1 + a_2 t_2) \in S + T$ poiché $a_1 s_1 + a_2 s_2 \in S$ e $a_1 t_1 + a_2 t_2 \in T$.

La somma $S + T$ di due sottospazi si dice *diretta* e si scrive $S \oplus T$ se ogni $v \in S + T$, si può scrivere in modo unico come somma di un vettore di S ed uno di T .

Teorema di caratterizzazione della somma diretta: $S + T = S \hat{A} T \hat{U} S \hat{C} T = \{0_v\}$

Dimostrazione: Se $S + T = S \oplus T$ (cioè ogni vettore di $S + T$ si può scrivere in modo univoco come somma di un vettore di S e uno di T) si ha che $S \cap T = \{0_v\}$. Infatti se esistesse $v \neq 0_v \in S \cap T$, potendosi scrivere $v = v + 0_v$ con $v \in S$ e $0_v \in T$ e $v = 0_v + v$ con $0_v \in S$ e $v \in T$, e cioè in modo non univoco, si ha un assurdo.

Se $S \cap T = \{0_v\}$, supponiamo che la somma $S + T$ non sia diretta. Allora esiste $v \in S + T$ tale che $v = s + t$ e $v = s_1 + t_1 \Rightarrow s + t = s_1 + t_1$. Allora $u = s - s_1 = t_1 - t$ con $s - s_1 \in S$ e $t_1 - t \in T$, quindi $u \in S \cap T$, e, per l'ipotesi, $u = \{0_v\}$. Allora $s - s_1 = 0_v$ e $t_1 - t = 0_v$ e quindi $s = s_1$ e $t = t_1$.

2. Generatori e vettori linearmente indipendenti

Fissati $v_1, v_2, \dots, v_n \in V$, l'insieme dei vettori di V che sono combinazioni lineari di v_1, v_2, \dots, v_n , cioè l'insieme dei vettori del tipo $a_1 v_1 + a_2 v_2 + \dots + a_n v_n$ con $a_i (i = 1 \dots n) \in K$ si suole indicare con $L(v_1, v_2, \dots, v_n) = \{ a_1 v_1 + a_2 v_2 + \dots + a_n v_n, a_i \in K \}$

Teorema:

1) $L(v_1, v_2, \dots, v_n)$ è un sottospazio di V .

Per dimostrare che $L(v_1, v_2, \dots, v_n)$ è un sottospazio di V bisogna verificare che se $u, v \in L(v_1, v_2, \dots, v_n)$ allora, per ogni $a, b \in K$, si ha $au + bv \in L(v_1, v_2, \dots, v_n)$.

Pertanto se $u = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$ e $v = b_1 v_1 + b_2 v_2 + \dots + b_n v_n$, si ha :

$$\begin{aligned} au + bv &= a(a_1 v_1 + a_2 v_2 + \dots + a_n v_n) + b(b_1 v_1 + b_2 v_2 + \dots + b_n v_n) = \\ &= aa_1 v_1 + aa_2 v_2 + \dots + aa_n v_n + bb_1 v_1 + bb_2 v_2 + \dots + bb_n v_n = \\ &= (aa_1 + bb_1) v_1 + (aa_2 + bb_2) v_2 + \dots + (aa_n + bb_n) v_n \in L(v_1, v_2, \dots, v_n) \quad \text{c.v.d.} \end{aligned}$$

2) $v_1, v_2, \dots, v_n \hat{I} L(v_1, v_2, \dots, v_n)$

Infatti:

$$\begin{aligned} v_1 &= 1v_1 + 0v_2 + \dots + 0v_n \\ v_2 &= 0v_1 + 1v_2 + \dots + 0v_n \\ &\dots \\ v_n &= 0v_1 + 0v_2 + \dots + 1v_n \end{aligned}$$

3) Se W è un sottospazio di V tale che $W \hat{E} \{v_1, v_2, \dots, v_n\}$ allora $W \hat{E} L(v_1, v_2, \dots, v_n)$

Infatti se $v \in L(v_1, v_2, \dots, v_n)$ allora $v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$. Essendo W un sottospazio esso contiene ogni combinazione lineare dei suoi elementi, e poiché fra questi vi sono v_1, v_2, \dots, v_n ne viene che $a_1 v_1 + a_2 v_2 + \dots + a_n v_n = v \in W$.

Il precedente teorema ci dice che $L(v_1, v_2, \dots, v_n)$ è un sottospazio di V , contiene v_1, v_2, \dots, v_n e fra tutti i sottospazi di V contenenti v_1, v_2, \dots, v_n , esso è il “minimo”, cioè quello che è contenuto in tutti gli altri.

Posto $S = L(v_1, v_2, \dots, v_n)$ si dice che S è “generato” da v_1, v_2, \dots, v_n , o che v_1, v_2, \dots, v_n “generano” S , o anche che $\{v_1, v_2, \dots, v_n\}$ è un sistema di generatori di S .

Se $L(v_1, v_2, \dots, v_n) = V$, si dice anche che V è “finitamente generato”.

Risulta:

V è generato da $v_1, v_2, \dots, v_n \iff$ 1) $v_1, v_2, \dots, v_n \in V$ e 2) $\forall v \in V$ è combinazione lineare di v_1, v_2, \dots, v_n .

Esempi

In \mathbb{R}^2 sono dati i vettori $v_1 = (1, 2)$, $v_2 = (2, 1)$, $v_3 = (1, -1)$. Risulta $\mathbb{R}^2 = L(v_1, v_2, v_3)$. Infatti dato un qualunque vettore (a, b) di \mathbb{R}^2 la relazione $xv_1 + yv_2 + zv_3 = v = (a, b)$ è verificata da infinite terne (x, y, z) in quanto si ha:

$$(a, b) = x(1, 2) + y(2, 1) + z(1, -1) = (x + 2y + z, 2x + y - z) \Rightarrow \begin{cases} x + 2y + z = a \\ 2x + y - z = b \end{cases} \quad \text{che ammette}$$

infinite soluzioni.

Risulta $\mathbb{R}^2 = L(v_1, v_2)$ in quanto si ha:

$$v = (a, b) = x(1, 2) + y(2, 1) = (x + 2y, 2x + y) \Rightarrow \begin{cases} x + 2y = a \\ 2x + y = b \end{cases} \quad \text{che ammette la soluzione}$$

$$\begin{cases} x = \frac{a - 2b}{-3} \\ y = \frac{b - 2a}{-3} \end{cases}$$

Osserviamo che $v_3 = \underline{x}v_1 + \underline{y}v_2$ infatti $(1, -1) = \underline{x}(1, 2) + \underline{y}(2, 1)$; per $\underline{x} = -1$, $\underline{y} = 1$;

$$(1, -1) = -1(1, 2) + 1(2, 1) = (1, -1).$$

Da questo esempio segue che:

- Se ad un insieme di generatori aggiungiamo altri vettori si ottiene sempre un sistema di generatori;
- Se da un sistema di generatori si “eliminano” alcuni vettori che sono combinazione lineare degli altri, si ottiene un insieme di generatori.

Non tutti gli spazi vettoriali sono generati da un numero finito di vettori (“finitamente generati”), cioè non sempre si ha che $V = L(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n)$.

Esempi

- 1) Lo spazio $K[x]$ non è finitamente generato.

Infatti se p_1, p_2, \dots, p_n sono n polinomi ed r è il loro massimo grado, si ha che $L(p_1, p_2, \dots, p_n)$ non contiene polinomi di grado $> r$ e poiché in $K[x]$ vi sono polinomi di grado $> r$ si ha che $K[x] \neq L(p_1, p_2, \dots, p_n)$. Ciò prova che nessun sottoinsieme finito di $K[x]$ genera $K[x]$, cioè $K[x]$ non è finitamente generato.

- 2) Lo spazio $K_r[x]$ è finitamente generato.

Infatti un suo qualsiasi vettore si può esprimere come combinazione lineare dei polinomi $1, x, x^2 \dots x^r$. Cioè $K_r[x] = L(1, x, x^2 \dots x^r)$.

- 3) Lo spazio K^n è finitamente generato da n vettori.

Infatti siano $\mathbf{e}_1 = (1, 0, \dots, 0)$, $\mathbf{e}_2 = (0, 1, 0, \dots, 0)$, ..., $\mathbf{e}_n = (0, 0, \dots, 1)$ si ha che $\mathbf{v} = (x_1, x_2, \dots, x_n) = (x_1, 0, \dots, 0) + (0, x_2, \dots, 0) + \dots + (0, \dots, x_n) = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \dots + x_n\mathbf{e}_n$.

- 4) Lo spazio $K^{m,n}$ è anch'esso finitamente generato.

Un insieme di generatori è costituito dalle $m \cdot n$ matrici aventi un solo elemento uguale a 1 e gli altri uguali a 0.

Per $m = n = 2$ si ha $K^{2,2}$ e un vettore di tale spazio è $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$

Le 4 matrici $E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, costituiranno un

sistema di generatori, infatti si ha:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}E_{11} + a_{12}E_{12} + a_{21}E_{21} + a_{22}E_{22}.$$

Vettori linearmente indipendenti

I vettori \mathbf{v}_i ($i = 1 \dots n$), si dicono *linearmente indipendenti* se la relazione $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n = \mathbf{0}_v$ è vera soltanto quando tutti gli $a_i = 0$.

In tal caso l'insieme $\{\mathbf{v}_i\}$ dicesi *libero*. In caso contrario i vettori si dicono linearmente dipendenti.

Osservazione. La nozione di vettori linearmente dipendenti e linearmente indipendenti non dipende dall'ordine dei vettori.

Proprietà

- 1) *Un insieme costituito da un solo elemento è linearmente indipendente se esso è diverso da $\mathbf{0}_v$ (infatti se $\mathbf{v} \neq \mathbf{0}_v$, $a\mathbf{v} = \mathbf{0}_v$ solo se $a = 0$), mentre è linearmente dipendente se esso è $\mathbf{0}_v$ (infatti $a\mathbf{0}_v = \mathbf{0}_v$ con $a \neq 0$).*
- 2) *L'insieme $\{0_v, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ non è l.i. : cioè un insieme contenente $\mathbf{0}_v$ è l.d.*
- 3) *Se $\mathbf{v} = \sum_{i=1}^n a_i \mathbf{v}_i$ allora $\{\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ non è libero (infatti avendosi $\mathbf{v} = a_1\mathbf{v}_1 + \dots + a_n\mathbf{v}_n$ si ha $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n - \mathbf{v} = \mathbf{0}_v$ e gli scalari non sono tutti nulli).*
- 4) *Se $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ sono linearmente dipendenti, allora uno di essi è combinazione lineare dei rimanenti. In particolare se due vettori \mathbf{v}_1 e \mathbf{v}_2 sono linearmente dipendenti, allora uno dei due è "multiplo" dell'altro. $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 = \mathbf{0}_v$; $a_1\mathbf{v}_1 = -a_2\mathbf{v}_2$; $\mathbf{v}_1 = -\frac{a_2}{a_1}\mathbf{v}_2$.*
- 5) *Se n vettori sono lin. ind. allora p di essi con $p < n$, sono lin. ind. Esempio: i vettori di \mathbb{R}^3 $\mathbf{v}_1 = (1, 0, 0)$, $\mathbf{v}_2 = (1, 1, 0)$, $\mathbf{v}_3 = (1, 1, 1)$ sono linearmente indipendenti (infatti $\mathbf{0}_{\mathbb{R}^3} = a\mathbf{v}_1 + b\mathbf{v}_2 + c\mathbf{v}_3 = a(1, 0, 0) + b(1, 1, 0) + c(1, 1, 1) = (a + b + c, b + c, c) \Rightarrow c = 0, b = 0, a = 0$). Anche i vettori $\mathbf{v}_1, \mathbf{v}_2$ oppure $\mathbf{v}_1, \mathbf{v}_3$ oppure $\mathbf{v}_2, \mathbf{v}_3$ (cioè due di essi) risultano linearmente indipendenti. Infatti $\mathbf{0}_{\mathbb{R}^3} = a\mathbf{v}_1 + b\mathbf{v}_2 = a(1, 0, 0) + b(1, 1, 0) = (a + b, b, 0) \Rightarrow a = 0, b = 0$.*
- 6) *Se r vettori sono linearmente dipendenti e si aggiungono ad essi altri vettori si ottiene un insieme di vettori sempre linearmente dipendenti. Esempio: i vettori di \mathbb{R}^3 $\mathbf{v}_1 = (1, 2, 0)$, $\mathbf{v}_2 = (0, 0, 1)$, $\mathbf{v}_3 = (2, 4, 3)$ sono linearmente dipendenti (infatti è $2\mathbf{v}_1 + 3\mathbf{v}_2 - \mathbf{v}_3 = \mathbf{0}_{\mathbb{R}^3}$ $2(1, 2, 0) + 3(0, 0, 1) - (2, 4, 3) = (0, 0, 0)$). Anche i vettori $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4 = (1, 2, 5)$, $\mathbf{v}_5 = (0, -1, 0)$ sono ancora linearmente dipendenti. Infatti si ha: $2\mathbf{v}_1 + 3\mathbf{v}_2 - \mathbf{v}_3 + 0\mathbf{v}_4 + 0\mathbf{v}_5 = \mathbf{0}_{\mathbb{R}^3}$.*

7) Se $\{v_i\}_{i=1 \dots n}$ sono linearmente indipendenti allora ogni loro combinazione lineare si scrive in un unico modo, e viceversa; $\hat{U} v = a_i v_i$ è unico.

Dimostrazione:

Se fosse $v = \sum_{i=1}^n a_i v_i$ e $v = \sum_{i=1}^n b_i v_i$ si avrebbe $(a_1 - b_1) v_1 + (a_2 - b_2) v_2 + \dots + (a_n - b_n) v_n = \mathbf{0}$

e, per l'indipendenza dei vettori v_1, v_2, \dots, v_n , è $a_1 - b_1 = 0 \quad a_2 - b_2 = 0 \quad \dots \quad a_n - b_n = 0$
cioè $a_1 = b_1, a_2 = b_2, a_n = b_n$

Viceversa se ogni combinazione lineare dei v_i è unica, da $\mathbf{0} = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$ essendo anche $\mathbf{0} = 0v_1 + 0v_2 + \dots + 0v_n$, segue $a_1 = a_2 = \dots = a_n = 0$.

3. Basi e dimensione

Definizione di base: Un insieme ordinato di vettori di V , (v_i) , si dice che è una *base* di V se i v_i sono linearmente indipendenti e se formano un sistema di generatori per V .

Teorema di caratterizzazione delle basi: $B = (v_i)_{i=1 \dots n}$ è una base di $V \iff v \in V$ si può scrivere in un solo modo nella forma $v = \sum a_i v_i$.

Dimostrazione: Se $B = (v_i)_{i=1 \dots n}$ è una base di V si ha che i v_i sono linearmente indipendenti e generano V . Allora un qualunque vettore $v \in V$ si può scrivere in maniera unica nella forma $v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$.

Viceversa se, qualunque sia $v \in V$, si ha $v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$ ne segue che (v_1, v_2, \dots, v_n) sono generatori di V e per l'unicità della rappresentazione risultano linearmente indipendenti.

Se $B = (v_i)$ è una base $\implies \exists$ una unica n -upla $(a_1, a_2, \dots, a_n) \in K^n$ tale che $v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$.

Gli scalari (a_1, a_2, \dots, a_n) sono detti *componenti del vettore v rispetto a B* . A volte si scrive ciò nel seguente modo: $v = (a_1, a_2, \dots, a_n)_B$.

Teorema: Se (v_1, v_2, \dots, v_n) è una base di V allora $\{v, v_1, v_2, \dots, v_n\}$ è un insieme di vettori linearmente dipendenti, $v \in V$.

Da questo teorema segue il seguente corollario.

Corollario: Se (v_1, v_2, \dots, v_n) è una base di V , allora non esistono in V più di n vettori lin. ind.

Segue che se V ha una base di n vettori allora ogni insieme di vettori lin. ind. è finito ed ha al più n elementi.

Teorema: Se $\{v_1, v_2, \dots, v_n\}$ è un insieme di generatori di V , esso contiene una base B di V .

$$V = L(v_1, v_2, \dots, v_n) \quad \text{E} \quad \exists B \subseteq \{v_1, v_2, \dots, v_n\}.$$

La dimostrazione si basa sul “metodo degli scarti successivi”.

Dal teorema segue che ogni spazio finitamente generato ha una base.

Teorema (completamento di un insieme libero a una base): Sia V uno spazio vettoriale finitamente generato, se v_1, v_2, \dots, v_n sono lin. ind. allora esiste una base B di V contenente tali vettori.

$$[v_1, v_2, \dots, v_n \text{ l. i.} \Rightarrow \exists B \mid \{v_1, v_2, \dots, v_n\} \subseteq B].$$

Dimostrazione: Infatti se $\{v_1, v_2, \dots, v_r\}$ sono linearmente indipendenti e $\{e_1, e_2, \dots, e_i\}$ è un insieme di generatori di V , allora $\{v_1, v_2, \dots, v_r, e_1, e_2, \dots, e_i\}$ generano V e quindi da essi si può estrarre una base con il metodo degli scarti successivi. Poiché v_1, v_2, \dots, v_r sono lin. ind. si scarteranno solo degli e_i ma non dei v_r , ottenendo una base in cui v_1, v_2, \dots, v_r sono i primi r elementi.

In relazione a questi ultimi due teoremi esiste un lemma dovuto a Steinitz che mette in relazione un insieme di vettori linearmente indipendenti (libero) qualsiasi di V e un insieme di generatori qualsiasi di V .

Lemma di Steinitz: Se $\{v_1, v_2, \dots, v_m\}$ è un insieme libero di V e $\{w_1, w_2, \dots, w_n\}$ è un insieme di generatori di V , allora $m \leq n$.

Il precedente lemma ci permette di dimostrare il seguente

Teorema di equicardinalità delle basi: Se $B = (v_1, v_2, \dots, v_n)$ è una base di V , allora tutte le basi di V hanno lo stesso numero n di vettori.

Dimostrazione: Siano $B = (v_1, v_2, \dots, v_m)$ e $C = (w_1, w_2, \dots, w_n)$ due basi di V . Per il lemma di Steinitz:

essendo B un insieme di generatori e C un insieme libero si ha che $m \leq n$
essendo B un insieme libero e C un insieme di generatori si ha che $n \leq m$ $\left. \vphantom{\begin{matrix} m \leq n \\ n \leq m \end{matrix}} \right\} \Rightarrow n = m$

Dicesi dimensione di uno spazio vettoriale V finitamente generato il numero n dei vettori di una sua qualsiasi base: si scrive $\dim V = n$.

Se V è uno spazio vettoriale di dimensione n le tre proposizioni risultano equivalenti.

- 1) $B = (v_1, v_2, \dots, v_n)$ è una base;
- 2) B è libero;
- 3) B è un insieme di generatori.

Esempi

- 1) $\dim \mathbb{R}^n = n$;
- 2) $\dim K^{n,m} = m \cdot n$;
- 3) $\dim K_r[x] = r + 1$.

Per convenzione la dimensione dello spazio nullo è zero. Base dello spazio vettoriale nullo è l'insieme vuoto.

Teoremi sulla dimensione dei sottospazi

1) **Teorema:** Sia V uno spazio vettoriale di dimensione n . Se W è un sottospazio di V , si ha:

- 1) $\dim W \leq n$;
- 2) $\dim W = n \iff W = V$.

Infatti

- 1) Essendo $\dim V = n$, segue che non esistono in V , e quindi in W , $n + 1$ vettori linearmente indipendenti. Allora $\dim W \leq n$
- 2) Se $\dim W = n$, esiste in W una base $B = (w_1, w_2, \dots, w_n)$. Poiché $W \subseteq V$, i vettori w_1, w_2, \dots, w_n sono n vettori di V lin. ind., dunque formano una base di V .
Segue $W = V$.

2) **Teorema:** $\dim (S + T) = \dim S + \dim T - \dim S \cap T$.

Nel caso particolare che $S + T$ è una somma diretta, si ha $\dim S \cap T = 0$ quindi $\dim S \oplus T = \dim S + \dim T$.

Se $V = S \oplus T$, allora una base di V si può ottenere come unione di una base B_1 di S e una base B_2 di T . Infatti qualunque $\mathbf{v} \in V$ si scrive in modo unico come somma di un vettore di S ed uno di T . Poiché ciascuno di questi due vettori si scrive in modo unico mediante i vettori rispettivamente di B_1 e di B_2 ne viene che un qualunque $\mathbf{v} \in V$ si scrive in modo unico come combinazione lineare dei vettori di B_1 e di B_2 .

CALCOLO COMBINATORIO

1. Disposizioni, permutazioni e combinazioni semplici.

Sia dato un insieme finito A di n elementi

$$(1) \quad A = \{a_1, a_2, a_3, \dots, a_n\}$$

Fissato un $k \in \mathbb{N}$, con $1 \leq k \leq n$, si chiamano *disposizioni semplici* degli n elementi di A a k a k (o di classe k) tutti i raggruppamenti ordinati formati con k elementi distinti di A .

Si osservi che due qualunque disposizioni di A della stessa classe differiscono o per qualche elemento oppure per l'ordine in cui si susseguono gli elementi.

1) Sia $A = \{a, b, c\}$; le disposizioni di classe 1 sono: a, b, c ; quelle di classe 2 sono: $(a, b), (a, c), (b, a), (b, c), (c, a), (c, b)$; quelle di classe 3 sono: $(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)$.

Teorema: Il numero delle disposizioni semplici di classe k degli n elementi di A è:

$$(2) \quad D_{n,k} = n \times (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1).$$

Si chiamano *permutazioni semplici* degli n elementi di A le disposizioni semplici di classe n .

Il numero delle permutazioni semplici di A si indica con P_n e, per la (2), si ha:

$$(3) \quad P_n = D_{n,n} = n \times (n-1) \times \dots \cdot 2 \cdot 1.$$

Dato un $n \in \mathbb{N}$, con $n > 1$, il numero

$$(4) \quad n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n$$

si chiama *n fattoriale* (o fattoriale di n).

Si pone per convenzione:

$$(5) \quad 1! = 1, \quad 0! = 1.$$

Si verifica facilmente che:

$$(6) \quad P_n = n! = n(n-1)! \quad D_{n,k} = \frac{n!}{(n-k)!}.$$

Se gli elementi di una permutazione sono disposti in maniera circolare, in modo che non sia possibile individuare il “primo” e l’ “ultimo” elemento, si parla di permutazione in *linea chiusa*; il loro numero si indica con $P_n^{(c)}$ e risulta:

$$(7) \quad P_n^{(c)} = (n - 1)!$$

Esempio:

2) In quanti modi diversi quattro persone possono sedersi attorno ad un tavolo? Tale numero è $P_4^{(c)} = 3! = 6$.

Infatti si ha:

$$\begin{array}{cccccc} d & d & b & c & b & c \\ a ? c ; & a ? b ; & a ? c ; & a ? d ; & a ? d ; & a ? b \\ b & c & d & b & c & d \end{array}$$

La permutazione (a_1, a_2, \dots, a_n) si chiama *permutazione fondamentale*.

Data una permutazione di A diversa dalla fondamentale, si dice che due suoi elementi formano una *inversione* se in essa si presentano in ordine inverso rispetto a quello in cui si presentano nella permutazione fondamentale.

Una permutazione si dice di *classe pari* o di *classe dispari* se i suoi elementi presentano rispettivamente un numero pari o dispari di inversioni. La permutazione fondamentale si considera di classe pari.

Esempio:

3) Calcolare il numero d’inversioni che presenta la permutazione $(5, 1, 3, 4, 2)$ rispetto alla permutazione fondamentale $(1, 2, 3, 4, 5)$.

Si ha:

$$\begin{array}{r} \underline{\quad\quad\quad 5\ 1\ 3\ 4\ 2} \\ 5 \quad .\ 1\ 1\ 1\ 1 \\ 1 \quad .\ .\ 0\ 0\ 0\ + \\ 3 \quad .\ .\ .\ 0\ 1 \\ 4 \quad .\ .\ .\ .\ 1 \\ \underline{\quad\quad\quad 2\ .\ .\ .\ .\ .} \\ 6 \end{array}$$

quindi la permutazione è di classe pari.

Teorema: Una permutazione cambia di classe se si scambiano di posto due elementi.

Se gli elementi sono consecutivi, il numero delle inversioni, dopo lo scambio, diminuisce o aumenta di un'unità e quindi la permutazione cambia classe.

Se tra i due elementi considerati ve ne sono altri p , occorrono $2p + 1$ scambi di posto di elementi consecutivi per ottenere lo scambio desiderato e quindi la permutazione cambia classe, essendo $2p + 1$ dispari.

Teorema: Delle $n!$ permutazioni di A , $n!/2$ sono di classe pari e $n!/2$ di classe dispari.

Per il teorema precedente, ad ogni permutazione di classe pari, scambiando due elementi, qualsiasi, corrisponde una permutazione di classe dispari e quindi, essendo $n!$ pari, il numero di permutazioni di classe pari è uguale al numero di permutazioni di classe dispari.

Si chiamano *combinazioni semplici* degli n elementi di A a k a k (o di classe k) tutti i raggruppamenti non ordinati formati con k elementi distinti di A .

Si osservi che due qualunque combinazioni di A della stessa classe differiscono almeno per un elemento.

Esempio:

4) Sia $A = \{a, b, c\}$; le combinazioni di classe 1 sono: a, b, c ; quelle di classe 2 sono: $(a, b), (a, c), (b, c)$; quella di classe 3 è: (a, b, c) .

Teorema: Il numero delle combinazioni di classe k degli n elementi di A è:

$$C_{n, k} = \frac{n(n-1)\dots(n-k+1)}{k!}$$

Da una qualsiasi combinazione di classe k di A si ottengono $k!$ disposizioni contenenti i medesimi elementi della combinazione considerata, per cui si ha:

$$C_{n, k} \cdot k! = D_{n, k}$$

ovvero:

$$(8) \quad C_{n, k} = \frac{D_{n, k}}{k!} = \frac{n(n-1)\dots(n-k+1)}{k!}$$

Si usa scrivere:

$$(9) \quad C_{n, k} = \binom{n}{k}$$

e si legge: « n su k » e si chiamano *coefficienti binomiali*.

Dalla (8) moltiplicando numeratore e denominatore per $(n-k)!$ E tenendo presente la (9) , si ha:

$$(10) \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

dalla quale risulta:

$$(11) \quad \binom{n}{k} = \binom{n}{n-k}$$

Affinché le (10) e (11) siano valide anche per $k=0$ si pone:

$$(12) \quad \binom{n}{0} = 1.$$

Teorema (FORMULA DI STIFEL):

$$(13) \quad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Le combinazioni $C_{n, k}$ possono contenere o meno un determinato $a \in A$; il numero di quelle che lo contengono è $\binom{n-1}{k-1}$ mentre il numero di quelle che non lo contengono è $\binom{n-1}{k}$ per cui vale la (13).

2. Disposizioni, permutazioni e combinazioni con ripetizione.

Dato l'insieme (1) e fissato un $k \in \mathbb{N}^*$, si chiamano *disposizioni con ripetizione* degli n elementi di A a k a k (o di classe k) tutti i raggruppamenti ordinati formati prendendo k elementi, eguali o distinti, tra gli n di A .

Esempio:

- 1) Sia $A = \{a, b\}$; le disposizioni con ripetizione di classe 1 sono: a, b ; quelle di classe 2 sono: $(a, a), (a, b), (b, a), (b, b)$; quelle di classe 3 sono: $(a, a, a), (a, a, b), (a, b, a), (a, b, b), (b, a, a), (b, a, b), (b, b, a), (b, b, b)$; ecc.

Teorema : Il numero delle disposizioni con ripetizione di classe k degli n elementi di A è:

$$(14) \quad D_{n,k}^{(r)} = n^k$$

Infatti, poichè ognuno dei k elementi di $D_{n,k}^{(r)}$ può essere uno qualsiasi degli n elementi di A , si ha:

$$D_{n,k}^{(r)} = n \times n \times \dots \times n = n^k$$

Si chiamano *permutazioni con ripetizione* degli n elementi di A tutti i raggruppamenti ordinati formati con tutti gli elementi di A presi rispettivamente r_1, r_2, \dots, r_n volte ($r_i \geq 1, i=1,2,\dots,n$).

Si osservi che due qualunque permutazioni con ripetizione differiscono tra loro soltanto per l'ordine in cui si susseguono gli elementi.

Esempio:

- 2) Sia $A = \{a, b\}$, $r_1 = 1$ e $r_2 = 3$. Si hanno le seguenti permutazioni con ripetizione: $(a, b, b, b), (b, a, b, b), (b, b, a, b), (b, b, b, a)$.

Teorema: Il numero delle permutazioni con ripetizione degli n elementi di A presi rispettivamente r_1, r_2, \dots, r_n volte ($r_i \geq 1, i=1,2,\dots,n$) è:

$$(15) \quad P_{(r_1, r_2, \dots, r_n)}^{(r)} = \frac{M!}{r_1! r_2! \dots r_n!} \quad \text{con } M = r_1 + r_2 + \dots + r_n.$$

Si osservi che la (15), per $n = 2$, diventa:

$$P_{(r_1, r_2)}^{(r)} = \frac{(r_1 + r_2)!}{r_1! r_2!} = \binom{r_1 + r_2}{r_1} = \binom{r_1 + r_2}{r_2}.$$

Si chiamano *combinazioni con ripetizione* degli n elementi di A a k a k (o di classe k) tutti i raggruppamenti non ordinati formati con k elementi, in cui ogni elemento può ripetersi sino a k volte.

Si osservi che due qualunque combinazioni con ripetizione di classe k differiscono o perchè contengono elementi diversi o per il numero di volte in cui un elemento è ripetuto.

Esempio:

3) Sia $A = \{a, b, c\}$; le combinazioni con ripetizioni di A di classe 1 sono: a, b, c ; quelle di classe 2 sono: $(a, a), (a, b), (a, c), (b, b), (b, c), (c, c)$; quelle di classe 3 sono: $(a, a, a), (a, a, b), (a, a, c), (a, b, c), (a, b, b), (a, c, c), (b, b, b), (b, b, c), (c, c, c), (c, c, b)$; ecc.

Teorema : Il numero delle combinazioni con ripetizione degli n elementi di A a k a k è:

$$(16) \quad C_{n,k}^{(r)} = \frac{n(n+1)\dots(n+k-1)}{k!} = \binom{n+k-1}{k}.$$

3. Complementi ed esempi

I problemi di calcolo combinatorio possono essere divisi in due grandi categorie a seconda della natura dei raggruppamenti considerati. In particolare si può distinguere tra raggruppamenti elementari (disposizioni, permutazioni, combinazioni semplici e con ripetizione), e raggruppamenti complessi, che derivano dalla giustapposizione di più raggruppamenti elementari.

a) Problemi elementari: classificazione dei raggruppamenti. Il problema fondamentale nelle applicazioni elementari del calcolo combinatorio è la classificazione, l'individuazione cioè del raggruppamento elementare considerato. Al riguardo può risultare utile il seguente schema:

- 1) determinare l'insieme A , $|A|=n$, degli oggetti considerati;
- 2) determinare la classe k , cioè il numero di oggetti che dovranno far parte di ogni raggruppamento;
- 3) verificare se l'ordine è rilevante: se l'ordine conta, si tratta di disposizioni o permutazioni; se l'ordine non conta, si tratta di combinazioni;
- 4) se l'ordine è rilevante, verificare se in ogni raggruppamento devono figurare tutti gli oggetti dell'insieme di partenza: in caso positivo si tratta di permutazioni, altrimenti di disposizioni;
- 5) verificare se sono possibili ripetizioni di oggetti: in caso positivo si tratta di disposizioni, combinazioni o permutazioni con ripetizione; viceversa si tratta di disposizioni, combinazioni o permutazioni semplici.
- 6) Controllare la presenza di eventuali vincoli o condizioni esplicitamente imposti.

I punti 2), 4) e 5) sono tra di loro collegati. Per esempio, se $k \geq n$ allora ci sarà almeno un raggruppamento in cui figurano tutti gli oggetti di A e se $k > n$ si avranno certamente dei raggruppamenti con ripetizione. Il punto 4), in particolare, verifica se tutti gli *oggetti* di A *devono* essere presenti in ciascun raggruppamento considerato. Così, tra le disposizioni e combinazioni con ripetizione se $k \geq n$ ci sarà almeno un raggruppamento (esattamente uno se nel caso di combinazione è $k=n$) in cui figureranno tutti gli elementi di A ; non è però vero che in ciascuno di tali raggruppamenti sono presenti tutti gli elementi di A .

Esempio 1. *Un' azienda vuole assumere 6 laureati provenienti da quattro facoltà universitarie, in quanti modi possibili può effettuare l'assunzione?*

- 1) l'insieme A degli *oggetti* considerati è costituito dalle quattro facoltà universitarie;
- 2) di ogni raggruppamento dovranno far parte 6 elementi;
- 3) l'ordine non conta: si tratta perciò di combinazioni;
- 4) non si tratta di permutazioni (ovvio);
- 5) le ripetizioni sono ammesse e anzi sicuramente in ogni raggruppamento ci sono ripetizioni ($k=6 > 4=n$).

In definitiva si ha $C_{4,6}^{(r)}$.

Esempio 2. *Al gioco del lotto, quante diverse cinquine possono farsi utilizzando il "temo" già assegnato (3, 13, 83)?*

- 1) Gli elementi considerati sono gli 87 numeri del lotto rimanenti, una volta estratti 3, 13 e 83;
- 2) ogni raggruppamento dovrà contenere due elementi, cioè i due numeri che completando il terno formano la cinquina;
- 3) l'ordine non conta e si tratta perciò di combinazioni;
- 4) non si tratta, ovviamente, di permutazioni;
- 5) non ci sono ripetizioni.

In definitiva si ha $C_{87, 2}$.

Esempio 3. *Nel sistema di numerazione decimale, quanti differenti numeri di quattro cifre possono scriversi sotto le condizioni $c_1 < c_2 < c_3 < c_4$, ove con c_j si indica la j -esima cifra (da sinistra)?*

- 1) Gli elementi considerati sono le nove cifre 1, ..., 9; lo zero non si considera perchè non potendo essere la prima cifra (significativa) non può essere nemmeno una delle cifre successive, che devono infatti essere tutte maggiori della prima;
- 2) ogni raggruppamento è formato da quattro elementi;
- 3) i raggruppamenti non differiscono tra di loro per l'ordine degli elementi, in quanto l'ordine è già stato prefissato: le cifre componenti il numero dovranno sempre presentarsi in ordine crescente;
- 4) non si tratta di permutazioni;
- 5) non ci sono ripetizioni.

In definitiva si ha $C_{9,4}$.

Esempio 4. *Quanti differenti orari scolastici di 5 ore ciascuno possono programarsi prevedendo 2 ore di Formazione Discreta, 2 ore di Formazione Analitica ed un'ora di Programmazione?*

- 1) Gli elementi sono le tre materie considerate: Italiano, Matematica e Storia;
- 2) ogni raggruppamento deve essere formato da cinque elementi corrispondenti alle cinque ore;
- 3) l'ordine è rilevante; anzi ogni raggruppamento differisce dall'altro solo per l'ordine;
- 4) tutti e tre gli elementi devono essere presenti in ogni raggruppamento: si tratta perciò di permutazioni;
- 5) in ogni raggruppamento ci sono ripetizioni, in particolare l'italiano e la matematica sono ripetute due volte ciascuno.

In definitiva si tratta di $P_{2,2,1}^{(r)}$.

b) Problemi complessi: scomposizione dei raggruppamenti in raggruppamenti elementari. I problemi più complicati di calcolo combinatorio si risolvono individuando dapprima le componenti elementari dei raggruppamenti complessi, poi considerando le relazioni che intercorrono tra essi. Questa scomposizione va condotta individuando una successione di operazioni che permette di ottenere i raggruppamenti semplici richiesti dal problema.

Esempio 5. *Si ha un mazzo di 40 carte (4 colori numerati da 1 a 10). Quante differenti "mani" di 8 carte ciascuna contengono esattamente due assi?*

Le operazioni per ottenere una mano che rispetti le indicazioni del problema sono:

- 1) scegliere tra i quattro assi i due assi che devono far parte della mano;
- 2) scegliere tra le altre 36 carte le sei carte che devono completare la mano.

L'operazione 1) può svolgersi in $C_{4,2}$ modi possibili: si tratta infatti di raggruppamenti di quattro elementi (i quattro assi), di classe due (i due assi da scegliere), l'ordine non conta e non sono ammesse ripetizioni (e perciò combinazioni semplici). L'operazione 2) può svolgersi in $C_{36,6}$ modi possibili: si tratta infatti di raggruppamenti di 36 elementi (le carte diverse dagli assi), di classe sei (il numero di carte per completare la mano), l'ordine non conta e non sono ammesse ripetizioni (e perciò si tratta di combinazioni semplici).

Dal momento che a ogni coppia di soluzioni ammissibili dell'operazione 1) e dell'operazione 2) corrisponde una differente mano di Otto carte tra quelle richieste dal problema, per ottenere il numero totale delle mani basta moltiplicare il numero di possibili

svolgimenti dell'operazione 1) per il numero di possibili svolgimenti dell'operazione 2). In definitiva, dunque, il numero delle mani richieste è: $C_{4,2}C_{36,6}$

Esempio 6 *Quanti differenti consigli di amministrazione di 7 membri è possibile formare disponendo di 10 candidati, dei quali però solo 3 possono assumerne la presidenza?*

Le operazioni per ottenere un possibile consiglio di amministrazione sono:

- 1) decidere dei tre candidati che possono prendere la presidenza quanti farne partecipare a qualunque titolo al consiglio di amministrazione: uno, due o tre;
- 2) stabilire quali dei candidati che possono assumere la presidenza inserire nel consiglio di amministrazione: questa operazione è banale nel caso che al punto 1) si decida di inserire tutti e tre i candidati;
- 3) individuare quali dei candidati che non possono assumerne la presidenza inserire nel consiglio di amministrazione.

L'operazione 1) dà tre risultati diversi: a) inserire uno dei candidati che possono assumere la presidenza; b) inserirne due; c) inserirli tutti e tre. L'operazione 2) ha un numero di possibili svolgimenti pari nel caso a) a $C_{3,1}$, nel caso b) a $C_{3,2}$, nel caso c) a $C_{3,3}$.

L'operazione 3) ha un numero di possibili svolgimenti pari nel caso a) a $C_{7,6}$, nel caso b) a $C_{7,5}$, nel caso c) a $C_{7,4}$.

Poiché a), b) e c) sono alternativi tra di loro, bisogna sommare il numero dei casi possibili nelle tre situazioni.

Complessivamente perciò i possibili consigli di amministrazione sono:

$$C_{3,1}C_{7,6} + C_{3,2}C_{7,5} + C_{3,3}C_{7,4}.$$

Si osservi che nei casi b) e c) si considera solamente l'effettiva composizione del consiglio di amministrazione, prescindendo da chi ne assuma effettivamente la presidenza.

Esempio 7. *Un'azienda ha un organico di 20 dirigenti tecnici e 10 amministrativi. In quante diverse maniere può costituirsi un comitato di 6 dirigenti, dei quali almeno 4 siano tecnici?*

Indichiamo con t i dirigenti tecnici e con a i dirigenti amministrativi. I comitati possibili saranno dei seguenti tre tipi:

1) $t t t t a a$

2) $t t t t t a$

3) $t t t t t t$

Nel caso 1) si hanno 4 dirigenti tecnici scelti in una rosa di venti e 2 dirigenti amministrativi scelti in una rosa di dieci: poichè l'ordine non conta, i casi possibili sono: $C_{20,4}C_{10,2}$.

Analogamente, per i casi 2) e 3) si ha rispettivamente $C_{20,5}C_{10,1}$ e $C_{20,6}$.

Essendo i casi 1), 2) e 3) alternativi tra loro, complessivamente i raggruppamenti possibili sono: $C_{20,4}C_{6,2} + C_{20,5}C_{6,1} + C_{20,6}$

Esempio 8. *Quanti sono nel sistema di numerazione decimale i numeri di cinque cifre che risultano uguali leggendo da sinistra a destra o viceversa (es. 35153)? E quanti sono quelli di sei cifre?*

- Se si può accettare b 0 come prima cifra, basta fissare le prime tre cifre a, b e c tra le 10 possibili, ottenendo $abcba$.

Quindi (ordine rilevante e ripetizioni possibili) $D^{(r)}_{10,3} = 10^3$. Anche per i numeri di sei cifre vale lo stesso risultato, essendo ancora sufficiente fissare le prime tre cifre a, b, c (da cui si ottiene $abccba$).

- Se lo 0 non si può accettare come cifra iniziale, allora si fisseranno sempre le prime tre cifre, ma la prima cifra si potrà scegliere tra 9 cifre; quindi: $9D_{10,2} = 9 \cdot 10^2$

Si ha lo stesso risultato anche per i numeri di 6 cifre.

4. Binomio di Newton

Teorema: Per ogni $a, b \in \mathbb{R}$ e $n \in \mathbb{N}^*$ si ha:

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

Si osservi che:

$$(a+b)^n = (a+b) \times (a+b) \dots (a+b) = A_0 a^n + A_1 a^{n-1} b + \dots + A_k a^{n-k} b^k + \dots + A_n b^n,$$

dove A_k ($k = 0, 1, \dots, n$) rappresenta il numero delle permutazioni con ripetizione degli elementi a e b presi rispettivamente $n-k$ e k volte, cioè si ha:

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

e quindi vale la (*).

La (*), per $a = b = 1$, diventa:

$$2^n = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n}$$

mentre, per $a=1$ e $b=-1$, si ha:

$$0 = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \dots + (-1)^k \binom{n}{k} + \dots - (-1)^n \binom{n}{n}.$$

Esempi.

1) $(2x + y)^5 =$

$$\begin{aligned} \sum_{k=0}^5 \binom{5}{k} (2x)^{5-k} b^k &= (2x)^5 + 5(2x)^4 y + 10(2x)^3 y^2 + 10(2x)^2 y^3 + 5(2x)y^4 + y^5 = \\ &= 32x^5 + 80x^4 y + 80x^3 y^2 + 40x^2 y^3 + 10xy^4 + y^5 \end{aligned}$$

2) $(a^2 - 2b^3)^4 = \sum_{k=0}^4 \binom{4}{k} (a^2)^{4-k} (-2b^3)^k = a^8 - 8a^6 b^3 + 24a^4 b^6 - 32a^2 b^9 + 16b^{12}$

5. Principio di inclusione ed esclusione

Sono dati un insieme A formato da N oggetti di natura qualsiasi ed n proprietà $\alpha_i, i = 1, 2, \dots, n$, riguardanti questi oggetti.

Definiamo:

- 1) $N(\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{ir})$ è il numero di oggetti di A che godono delle proprietà $\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{ir}$.
- 2) $N(\overline{a_{i1}}, \overline{a_{i2}}, \dots, \overline{a_{ir}})$ è il numero di oggetti di A che non godono delle proprietà $\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{ir}$.
- 3) $N(\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{ir}, \overline{a_{j1}}, \overline{a_{j2}}, \dots, \overline{a_{jt}})$ è il numero di oggetti di A che godono delle proprietà $\alpha_{i1}, \dots, \alpha_{ir}$ ma non godono delle $\alpha_{j1}, \dots, \alpha_{jt}$ (dove le α_i sono diverse dalle α_j).

Sussiste la seguente formula ("Principio di inclusione ed esclusione"):

$$N(\overline{a_1}, \overline{a_2}, \dots, \overline{a_n}) = N - \sum_{i=1}^n N(a_i) + \sum_{i,j \in \{C_{n,2}\}} N(a_i, a_j) - \sum_{i,j,k \in \{C_{n,3}\}} N(a_i, a_j, a_k) + (-1)^{n-1} \sum N(\alpha_{i1}, \dots, \alpha_{i,n-1}) + (-1)^n N(\alpha_{i1}, \dots, \alpha_{i,n})$$

Dimostrazione

Si procede per induzione su n . Trattiamo soltanto il passaggio da 3 a 4.

Casi particolari:

$$n = 1 \quad N(\overline{a_1}) = N - N(\alpha_1)$$

$$n = 2 \quad N(\overline{a_1}, \overline{a_2}) = N - N(\alpha_1) - N(\alpha_2) + N(\alpha_1, \alpha_2)$$

Passaggio da 3 a 4

Per l'ipotesi induttiva risulta:

$$N(\overline{a_1}, \overline{a_2}, \overline{a_3}, a_4) = N(\alpha_4) - N(\alpha_1, \alpha_4) - N(\alpha_2, \alpha_4) - N(\alpha_3, \alpha_4) + N(\alpha_1, \alpha_2, \alpha_4) + N(\alpha_1, \alpha_3, \alpha_4) + N(\alpha_2, \alpha_3, \alpha_4) - N(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

$$N(\overline{a_1}, \overline{a_2}, \overline{a_3}) = N - N(\alpha_1) - N(\alpha_2) - N(\alpha_3) + N(\alpha_1, \alpha_3) + N(\alpha_1, \alpha_2) + N(\alpha_2, \alpha_3) - N(\alpha_1, \alpha_2, \alpha_3)$$

Essendo

$$N(\overline{a_1}, \overline{a_2}, \overline{a_3}, \overline{a_4}) = N(\overline{a_1}, \overline{a_2}, \overline{a_3}) - N(\overline{a_1}, \overline{a_2}, \overline{a_3}, a_4) = N - \sum N(\alpha_i) + \sum N(\alpha_i, \alpha_j) - \sum N(\alpha_i, \alpha_j, \alpha_k) + N(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

Si ha la tesi.

Esempio

Sia S l'insieme dei soci di un club.

Consideriamo i seguenti sottoinsiemi di S :

- 1) $A = \{x : x \in S \text{ e giocano a tennis}\}$;
- 2) $B = \{x : x \in S \text{ e giocano a golf}\}$;
- 3) $C = \{x : x \in S \text{ e praticano altri sports}\}$.

Determinare il numero dei soci che non praticano nessuno sport nel caso in cui si conoscono

$|A|, |B|, |C|, |S|, |A \cap B|, |A \cap C|, |B \cap C|$ e $|A \cap B \cap C|$

Applicando il principio di inclusione ed esclusione si ha:

$$\bar{S} = |S| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|$$

6. Equazioni lineari diofantee

Vengono chiamate *equazioni diofantee*, in onore di Diofanto, matematico greco del III sec. d. C. che scrisse un libro su tali equazioni, quelle equazioni lineari indeterminate (in due o più incognite) delle quali si cercano le soluzioni intere, a volte con ulteriori restrizioni.

Molti problemi, anche semplici, della vita comune si risolvono mediante queste equazioni.

Ad esempio:

Problema 1. Determinare il numero delle soluzioni intere non negative ($x_i \geq 0$) dell'equazione

$$(1) \quad x_1 + x_2 + \dots + x_n = m$$

Il problema 1 è equivalente al seguente

Problema 2. In quanti modi si possono distribuire m palline in n scatole?

Il numero delle soluzioni della (1) è dato da

$$(*) \quad C_{n,m}^{(r)} = \binom{n+m-1}{m} = \binom{n+m-1}{n-1}.$$

Problema 3. Determinare il numero delle soluzioni intere della (1) tali che

$$(2) \begin{cases} x_1 + x_2 + \dots + x_n = m \\ x_i \geq r_i \in \mathbb{Z} \quad i = 1, 2, \dots, n \end{cases}$$

Posto nella (2) $z_i = x_i - r_i \geq 0$, la (1) diventa:

$$(3) z_1 + z_2 + \dots + z_n = m - r, \text{ con } z_i \geq 0 \text{ ed } r = \sum_{i=1}^n r_i$$

Per la (*), il numero delle soluzioni intere che soddisfano la (2) è dato da

$$C_{n, m-r}^{(r)} = \binom{n+m-r-1}{m-r} = \binom{n+m-r-1}{n-1}$$

Problema 4. Determinare il numero di soluzioni intere della (1) tali che

$$(3) \begin{cases} x_1 + x_2 + \dots + x_n = m \\ x_i > r_i \in \mathbb{Z} \quad i = 1, 2, \dots, t \end{cases}$$

Essendo $x_i \geq r_i + 1$, $i = 1, 2, \dots, t$, ponendo $\begin{cases} z_i = x_i & i = t+1, \dots, n \\ z_i = x_i - (r_i + 1) \geq 0 & i = 1, 2, \dots, t \end{cases}$ si ha:

$$z_1 + \dots + z_n = m - \sum_{i=1}^t (r_i + 1) = m - \bar{r} - t \quad \left(\bar{r} = \sum_{i=1}^t r_i \right)$$

e quindi il numero di soluzioni richieste è dato da

$$C_{n, m-\bar{r}-t}^{(r)} = \binom{n+m-\bar{r}-t-1}{m-\bar{r}-t} = \binom{n+m-\bar{r}-t-1}{n-1}$$

Problema 5. Determinare il numero delle soluzioni intere della (1) tale che

$$(4) \begin{cases} x_1 + x_2 + \dots + x_n = m \\ x_i \geq r_i \quad i = 1, 2, \dots, t \\ x_i > u_i \quad i = t + 1, \dots, n \end{cases}$$

Ponendo $z_i = \begin{cases} x_i - r_i & i = 1, 2, \dots, t \\ x_i - (u_i + 1) & i = t + 1, \dots, n \end{cases}$

La (1) diventa

$$z_1 + \dots + z_n = m - \sum_{i=1}^t r_i - \sum_{i=t+1}^n (u_i + 1) = m - r - (n - t) \quad \text{con } r = \sum_{i=1}^t r_i + \sum_{i=t+1}^n u_i$$

e quindi il numero di soluzioni richieste è dato da

$$\binom{n + m - r - n + t - 1}{m - r - n + t} = \binom{m - r + t - 1}{n - 1}$$

Problema 6. Determinare il numero delle soluzioni intere della (1) in cui alcune incognite sono soggette a limitazioni superiori.

Esempio 1. Determinare il numero di soluzioni soddisfacente le seguenti condizioni

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ x_i \geq 0 \quad i = 1, 2, 3, 4 \\ x_1 \leq 5, \quad x_2 < 7 \\ x_3 \leq 4 \end{cases}$$

Introduciamo le seguenti proprietà

$$\alpha_1 = \{x_1 \geq 6\} \quad \alpha_2 = \{x_2 < 7\} \quad \alpha_3 = \{x_3 \geq 5\}$$

Applicando il principio di inclusione ed esclusione si ha:

$$N(\bar{a}_1, \bar{a}_2, \bar{a}_3) = N - N(\alpha_1) - N(\alpha_2) - N(\alpha_3) + N(\alpha_1, \alpha_3) + N(\alpha_1, \alpha_2) + N(\alpha_2, \alpha_3) - N(\alpha_1, \alpha_2, \alpha_3)$$

Risulta

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ x_i \geq 0 \end{cases} \rightarrow N = \binom{4 + 20 - 1}{20}$$

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ x_i \geq 0 \quad i = 2, 3, 4 \\ x_1 \geq 6 \end{cases} \quad N(a_1) = \binom{14 + 4 - 1}{14}$$

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ x_i \geq 0 \quad i = 1, 3, 4 \\ x_2 \geq 7 \end{cases} \quad N(a_2) = \binom{13 + 4 - 1}{13}$$

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ x_i \geq 0 \quad i = 1, 2, 4 \\ x_3 \geq 5 \end{cases} \quad N(a_1) = \binom{15+4-1}{15}$$

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ x_1 \geq 6 \\ x_2 \geq 7 \\ x_3, x_4 \geq 0 \end{cases} \quad N(a_1, a_2) = \binom{7+4-1}{7}$$

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ x_1 \geq 6 \\ x_3 \geq 5 \\ x_2, x_4 \geq 0 \end{cases} \quad N(a_1, a_3) = \binom{9+4-1}{9}$$

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ x_2 \geq 7 \\ x_3 \geq 5 \\ x_1, x_4 \geq 0 \end{cases} \quad N(a_2, a_3) = \binom{8+4-1}{8}$$

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ x_1 \geq 0, \quad x_2 \geq 7, \quad x_3 \geq 5 \\ x_4 \geq 0 \end{cases} \quad N(a_1, a_2, a_3) = \binom{2+4-1}{2}$$

Allora il numero delle soluzioni richieste è

$$N(\bar{a}_1, \bar{a}_2, \bar{a}_3) = \binom{23}{20} - \binom{17}{3} - \binom{16}{3} - \binom{18}{3} + \binom{10}{3} + \binom{12}{3} + \binom{11}{3} - \binom{5}{3}$$

Esempio 2. Determinare il numero di soluzioni intere tale che

$$\begin{cases} x_1 + x_2 + x_3 = 9 \\ x_1 \geq 0, \quad x_2 > 2, \quad x_3 \geq 1 \end{cases} \Leftrightarrow \begin{cases} x_1 + x_2 + x_3 = 9 \\ x_1 \geq 0, \quad x_2 \geq 3, \quad x_3 \geq 1 \end{cases}$$

Ponendo $z_1 = x_1$, $z_2 = x_2 - 3$, $z_3 = x_3 - 1$ si ha

$$\begin{cases} z_1 + z_2 + z_3 = 5 \\ z_i \geq 0 \end{cases}$$

$$\text{Il numero richiesto è } \binom{5+4-1}{5}$$

Esempio 3. Trovare il numero di soluzioni intere tali che

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 15 \\ x_1 \geq -3, \quad x_2 > 0, \quad x_3 \geq 2 \\ x_4 > -1 \quad (x_4 \geq 0) \end{cases} \Leftrightarrow \begin{cases} x_1 + x_2 + x_3 + x_4 = 15 \\ z_1 \geq x_1 + 3, \quad z_2 = x_2 - 1, \\ z_3 = x_3 - 2, \quad z_4 = x_4 \end{cases} \Leftrightarrow \begin{cases} z_1 + z_2 + z_3 + z_4 = 15 \\ z_i \geq 0 \end{cases}$$

Il numero di soluzioni richieste è $\binom{4+15-1}{15}$

GRAFI

1. Definizioni, terminologia, esempi e applicazioni⁽¹⁾

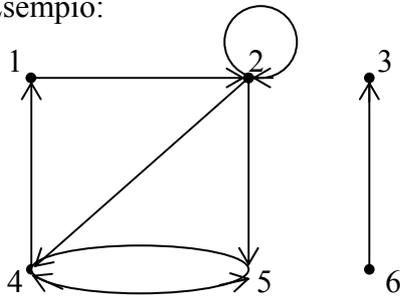
Un grafo orientato (o diretto o di-grafo) G è una coppia (V,E) dove V è un insieme non vuoto ed E una relazione binaria su V , $E \subseteq V \times V$, ossia un insieme di coppie ordinate di elementi di V .

Gli elementi di V sono chiamati *vertici* o *nodi*, gli elementi di E sono chiamati *spigoli* o *archi* (*edges*).

Se l'insieme V è finito, il grafo dicesi *finito*.

Se $(a,b) \in E$, a è il vertice iniziale e b il vertice finale; se il vertice finale coincide col vertice iniziale, cioè se $(a,a) \in E$, lo spigolo è detto *cappio* (*loop*).

Esempio:



$G = (V,E)$ orientato

$V = \{1, 2, 3, 4, 5, 6\}$

$E = \{(1, 2), (2, 2), (2,4), (2,5), (4,1), (4,5), (5,4), (6,3)\}$

fig.1

Un grafo non orientato, $G = (V,E)$, è una coppia (V,E) dove V è l'insieme dei vertici ed E è costituito da coppie non ordinate di vertici, cioè uno spigolo è un insieme $\{a,b\}$; tuttavia, per convenzione, per indicare il suddetto spigolo si usa la notazione (a,b) e inoltre le scritture (a,b) e (b,a) indicano lo stesso spigolo.

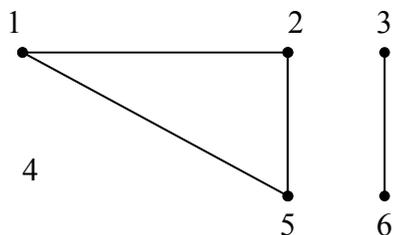
E' possibile avere spigoli del tipo (a,a) che vengono chiamati "selfloop".

(1) Si avvisa il lettore che certe definizioni che verranno date differiscono da quelle presenti in letteratura.

Nel seguito prenderemo in considerazione grafi in cui tutte le coppie di elementi di E sono distinti.

Un tale grafo si dirà *semplice*.

Esempio:



$G = (V, E)$ non orientato

$V = \{1, 2, 3, 4, 5, 6\}$

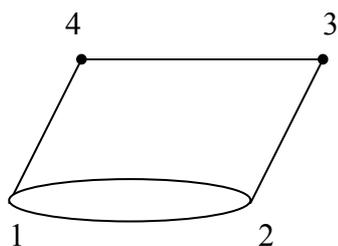
$E = \{(1, 2), (1, 5), (2, 5), (3, 6)\}$

4 è un vertice isolato.

fig.2

Un *multigrafo* è un grafo non orientato che ha archi multipli, cioè due vertici sono estremi di più spigoli.

Esempio:



$V = \{1, 2, 3, 4\}$

I vertici 1 e 2 sono estremi di due spigoli.

fig.3

Molte definizioni per i grafi orientati e non orientati coincidono, anche se certi termini hanno un significato leggermente diverso.

Se (a, b) è uno spigolo di un grafo orientato, si dice che (a, b) è incidente o *esce dal vertice a* ed è incidente o *entra nel vertice b*.

Esempio: nel grafo di fig.1 gli spigoli che escono dal vertice 2 sono $(2, 2)$, $(2, 4)$, $(2, 5)$, mentre gli spigoli che entrano nel vertice 2 sono $(1, 2)$ e $(2, 2)$.

Se (a, b) è uno spigolo di un grafo non orientato, si dice che (a, b) è incidente *sui vertici a e b*.

Esempio: nel grafo di fig.2, gli spigoli incidenti sul vertice 2 sono $(1, 2)$ e $(2, 5)$.

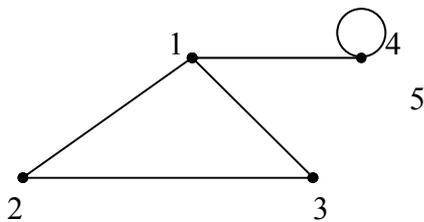
Se (a,b) è uno spigolo di un grafo, si dice che il vertice b è adiacente al vertice a .

Se il grafo è non orientato la relazione di adiacenza è simmetrica, mentre se il grafo è orientato la relazione di adiacenza non è necessariamente simmetrica.

Esempi nei grafi di fig.1 e fig.2, il vertice 2 è adiacente al vertice 1 perchè lo spigolo $(1,2)$ è presente in entrambi; nel grafo della fig.1, il vertice 1 non è adiacente al vertice 2, perchè l' arco $(2,1)$ non appartiene al grafo.

Grado di un vertice. Il grado di un vertice v in un grafo non orientato è il numero, $d(v)$, di spigoli incidenti con esso.

Se $d(v) = 0$, v si dice isolato; se $d(v) = 1$, v è detto vertice pendente. Un cappio relativo al vertice v si considera come uno spigolo incidente due volte su v .



$$d(1) = 3, \quad d(2) = d(3) = 2, \quad d(4) = 3, \quad d(5) = 0.$$

fig.4

Proposizione 1. In un grafo finito si ha:

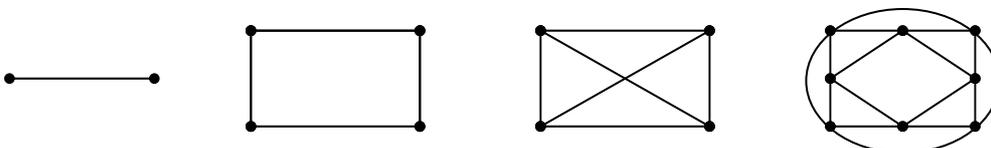
$$1) \quad 2|E| = \sum_{v \in V} d(v)$$

2) Il numero di vertici di grado dispari è pari.

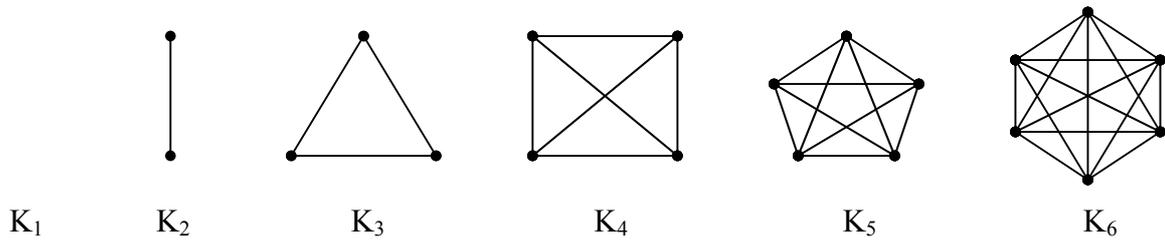
Un grafo non orientato i cui vertici hanno tutti lo stesso grado d si dice regolare di grado d .

Un grafo finito regolare di grado d con n vertici ha $\frac{1}{2} nd$ spigoli.

I seguenti grafi sono regolari di grado rispettivamente 1, 2, 3, 4.



Un grafo n.o. si dice completo se esso ha tutti gli spigoli possibili; un grafo completo con n vertici è regolare di grado $n-1$ e viene indicato con K_n .



Un grafo completo con n vertici ha esattamente $n(n-1)/2$ spigoli.

In un grafo orientato si chiama *grado uscente di un vertice v* , e si indica con $d^+(v)$, il numero di spigoli che escono da v , mentre si chiama *grado entrante di v* , e si indica con $d^-(v)$, il numero di spigoli entranti in v ; in tale computo i cappi contribuiscono in entrambi i casi.

Il grado di un vertice è dato dalla somma dei due gradi; chiaramente è:

$$\sum d^-(v) = \sum d^+(v) = |E|$$

In fig.1, per il vertice 2 è $d^-(2) = 2$, $d^+(2) = 3$, $d(2) = d^-(2) + d^+(2) = 5$

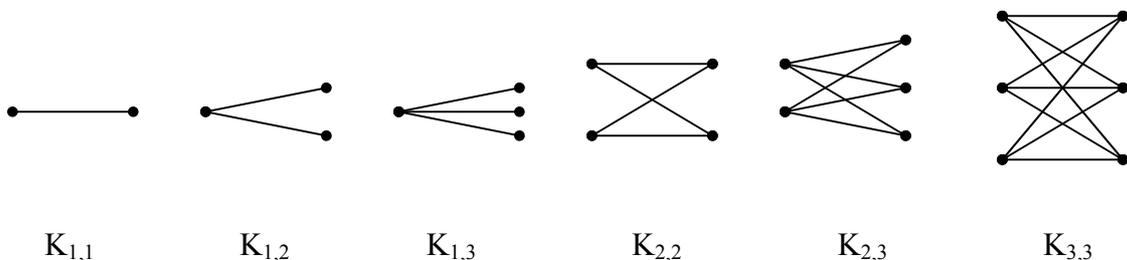
Un grafo si dice *bipartito* se l' insieme dei suoi vertici V può essere partizionato in due sottoinsiemi V_1 e V_2 , $V = V_1 \cup V_2$, tale che ogni spigolo unisce un vertice di V_1 con un vertice di V_2 .

Un grafo bipartito si dice *completo* se contiene tutti i possibili spigoli fra V_1 e V_2 .

In particolare se m, n sono interi positivi il grafo bipartito completo $K_{m,n}$ è il grafo tale che

$$V = \{a_1, \dots, a_m, b_1, \dots, b_n\}, E = \{s_{i,j} | i = 1, \dots, m, j = 1, \dots, n\}, \text{ con } s_{i,j} = \{a_i b_j\}.$$

Se $V_1 = \{a_1, \dots, a_m\}$ e $V_2 = \{b_1, \dots, b_n\}$ allora $K_{m,n}$ è il grafo con $m+n$ vertici, ogni vertice di V_1 è adiacente ad ogni vertice di V_2 ed ha $m \cdot n$ spigoli.



Si chiama *cammino (path) di lunghezza p di estremi a e b* in un grafo $G = (V, E)$ una sequenza di $p+1$ vertici (u_0, u_1, \dots, u_p) tale che $a = u_0$, $b = u_p$, e $(u_{i-1}, u_i) \in E$.

La lunghezza di un cammino è il numero dei suoi spigoli.

Il cammino contiene i vertici u_0, \dots, u_p e gli spigoli $(u_0, u_1), \dots, (u_{i-1}, u_i), \dots, (u_{p-1}, u_p)$.

Se esiste un cammino c da a a b si dice che b è raggiungibile da a tramite c .

Un cammino si dice *semplice* se tutti i suoi vertici sono distinti.

In fig.1 il cammino (1, 2, 5, 4) è un cammino semplice di lunghezza 3; il cammino (2, 5, 4, 5) non è semplice.

Per ogni vertice a c'è un unico cammino di lunghezza 0 da a allo stesso a .

Un cammino (u_0, \dots, u_n) si chiama *circuito o ciclo* se $u_0 = u_n$ e contiene almeno uno spigolo.

Il ciclo è semplice e i vertici u_0, \dots, u_n sono distinti.

Un *cappio* è un ciclo di lunghezza 1.

Un grafo senza cicli dicesi *aciclico*.

Un grafo $G = (V, E)$ si dice *connesso* se c'è almeno un cammino congiungente due suoi qualsiasi vertici.

Un grafo che non è connesso dicesi *sconnesso*.

Il grafo di fig.1 non è connesso.

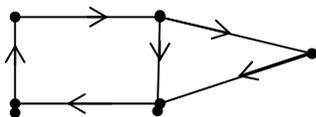
Se $a \in V$, si chiama *componente connessa* di a l'insieme C_a formato da tutti i vertici $x \in V$ per i quali esiste un cammino da a a x .

Sia \sim la relazione su V così definita: $\forall a, x \in V \quad a \sim x \Leftrightarrow$ esiste un cammino in G da a ad x .

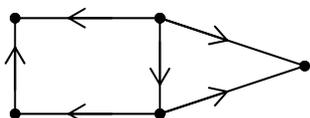
E' facile verificare che \sim è una relazione di equivalenza su V e per ogni $a \in V$ gli elementi ad esso equivalenti costituiscono la componente connessa di a . Ne segue che le varie componenti connesse formano una partizione dell'insieme V dei vertici, e ovviamente non c'è alcun spigolo che colleghi vertici appartenenti a componenti connesse distinte.

Si ha che G è connesso se e solo se G è costituito da una sola componente connessa.

Un grafo orientato si dice *fortemente connesso (strongly)* se per ogni $a, b \in V$ esiste un cammino orientato da a a b e da b ad a .

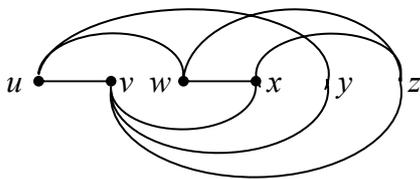
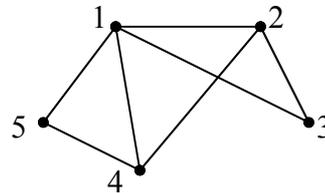
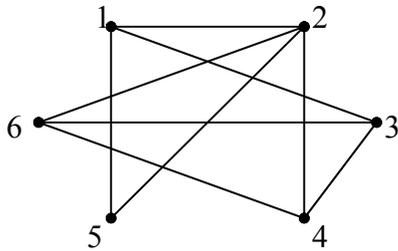


Un grafo orientato si dice *debolmente connesso (weakly)* se due qualsiasi vertici a, b sono uniti da un cammino non orientato.

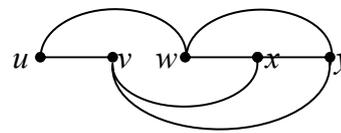


Due grafi $G = (V,E)$ e $G' = (V',E')$ si dicono isomorfi se esiste un' applicazione biunivoca $f: V \rightarrow V'$ tale che :

$$(a,b) \in E \Leftrightarrow (f(a),f(b)) \in E'.$$



(a)



(b)

(a) Coppia di grafi isomorfi, (b) coppia di grafi non isomorfi.

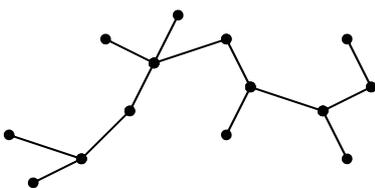
2. Alberi (Free Tree)

Una particolare classe di grafi sono gli *alberi* (il nome deriva, come vedremo più avanti, dalla somiglianza di questi grafi con gli alberi). Essi trovano applicazione in moltissimi problemi appartenenti a svariate discipline.

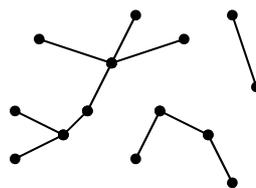
In molti problemi informatici i dati possono essere rappresentati mediante alberi, e questo fatto garantisce una risoluzione efficiente del problema che altrimenti sarebbe impossibile.

Una foresta è un grafo aciclico, un albero è un grafo connesso aciclico; gli alberi pertanto risultano essere le componenti connesse di una foresta.

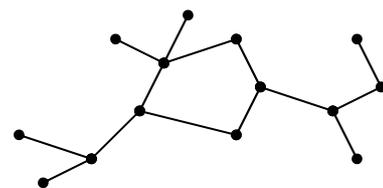
Esempi:



(a)



(b)



(c)

(a) Un albero libero. (b) Una foresta. (c) Un grafo che contiene un ciclo e non è perciò né un albero né una foresta.

Gli alberi possono essere caratterizzati in molti modi, si hanno infatti le seguenti due proposizioni:

Proposizione 1. *Sia $G = (V, E)$ un grafo (finito o infinito). Le seguenti affermazioni sono equivalenti:*

- a) G è un albero
- b) G è aciclico, ma se si aggiunge un qualsiasi spigolo si forma un ciclo
- c) Per ogni coppia di nodi a e b di G , esiste un unico cammino semplice da a a b .
- d) G è connesso, ma eliminando un arco qualsiasi di G si perde la connessione.

Dimostrazione. (a) \Rightarrow (b) Nell' ipotesi (a), G è aciclico. Inoltre, aggiungendo a G un arco $(u, v) \notin E$ si forma un ciclo dato da un cammino da v a u (esiste perché G è connesso) più l' arco (u, v) .

(b) \Rightarrow (c) Essendo G aciclico, ogni coppia di vertici può essere connessa da al più un cammino. Se vi fosse una coppia (u, v) non connessa da alcun cammino allora l' arco (u, v) potrebbe essere aggiunto senza perdere l' aciclicità.

(c) \Rightarrow (d) Dato che per ipotesi due vertici qualsiasi sono connessi esattamente da un unico cammino semplice, ovviamente G è connesso.

Sia $(u, v) \in E$. Supponiamo di rimuovere (u, v) da G . Se dopo tale eliminazione il grafo fosse ancora connesso, ci sarebbe in G' un cammino da u a v . Questo e l' arco (u, v) formano due diversi cammini in G da u a v .

(d) \Rightarrow (a) Supponendo (d) occorre solo verificare che G sia anche aciclico. Ma se G contenesse un ciclo, allora un qualsiasi arco su tale ciclo potrebbe essere eliminato senza perdere la proprietà di connessione.

Proposizione 2. *Sia $G = (V, E)$ un grafo finito e sia $|V| = n$. Allora le seguenti affermazioni sono equivalenti:*

- e) G è un albero
- f) G è aciclico e $|E| = |V| - 1$
- g) G è connesso e $|E| = |V| - 1$.

Dimostrazione. (e) \Rightarrow (f) se G è un albero, allora G è aciclico. Dimostriamo che $|E| = |V| - 1 = n - 1$ per induzione su n . Per $n = 1$ allora $|E| = \emptyset$ e quindi $|E| = |V| - 1$. Sia $n > 1$. Per la proprietà (d) della proposizione precedente, eliminando un arco da G si perde la connessione e si ottengono esattamente due componenti connesse. Queste componenti, di dimensione d_1 e d_2 rispettivamente, con $d_1 + d_2 = n$, sono alberi. Quindi, per l' ipotesi induttiva, ciascuna di esse ha $d_1 - 1$ e $d_2 - 1$ archi, rispettivamente. Questi, con l' arco inizialmente eliminato, danno in totale

$$|E| = (d_1 - 1) + (d_2 - 1) + 1 = d_1 + d_2 - 1 = n - 1.$$

(f) \Rightarrow (g) Supponiamo che G sia aciclico e che $|E| = |V| - 1$. Se G non fosse connesso, potremmo aggiungere a G degli archi sino ad ottenere la connessione e senza perdere l' aciclicità. Si otterrebbe un grafo $G' = (V, E')$ con $|E'| > |V| - 1$, connesso e aciclico (cioè un albero).

Ma allora $|E'| = |V| - 1$, contraddizione.

(g) \Rightarrow (e) Supponiamo adesso che G sia connesso e che $|E| = |V| - 1$. Se G fosse ciclico, allora potremmo eliminare da G alcuni archi sino a forzare l' aciclicità e senza perdere la connessione. Ne risulterebbe un albero $G' = (V, E')$ con $|E'| < |V| - 1$, contraddizione.

Alberi con radice

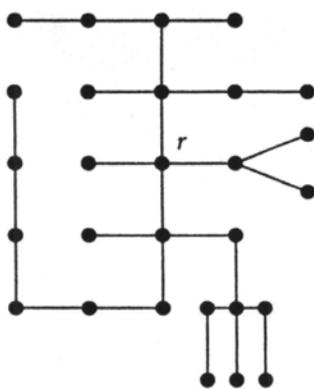
Un albero con radice è un albero con un vertice contraddistinto come radice.

Ricordiamo che in un albero, esiste un solo cammino fra due vertici qualsiasi u e v (prop.1, c); se l è la lunghezza di tale cammino diremo anche che l è la distanza fra u e v . Fissato arbitrariamente un vertice r come radice per ciascun nodo esiste uno ed un solo cammino che lo collega alla radice; tale cammino si chiama *cammino caratteristico del nodo*.

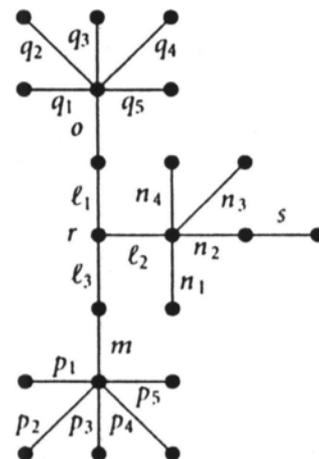
La lunghezza del cammino caratteristico di un nodo si chiama *livello del nodo*.

Ne deriva che un albero può essere disegnato disponendo i vertici su righe successive in relazione alla loro distanza dalla radice (cioè nel loro livello): nella prima riga viene fissato il vertice r , nella seconda riga tutti i vertici a livello 1 da r , nella terza riga i vertici a distanza 2 da r , ecc...

Esempio. I grafi delle figure (a) e (b) sono degli alberi perché ciascuno è connesso ed è privo di cicli.

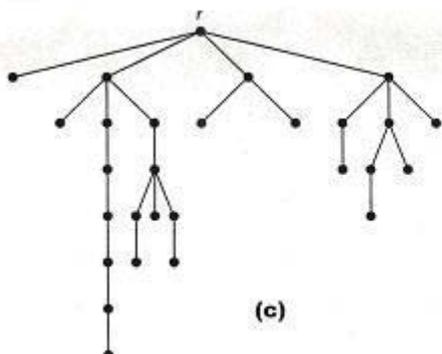


(a)

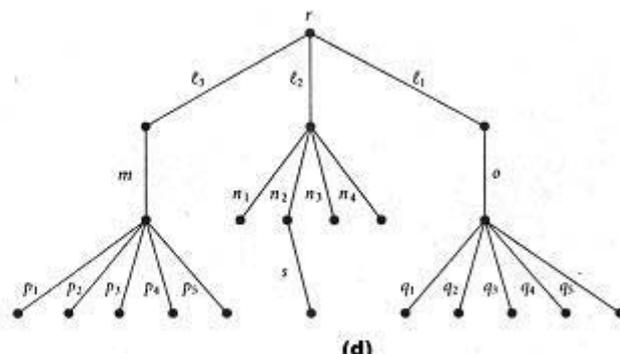


(b)

Fissando in ciascuno di essi come radice un vertice, ad esempio il vertice r , si ottiene un albero con radice e disponendo i vertici su righe successive in relazione alla loro distanza dalla radice si ottengono rispettivamente le figure (c) e (d).



(c)



(d)

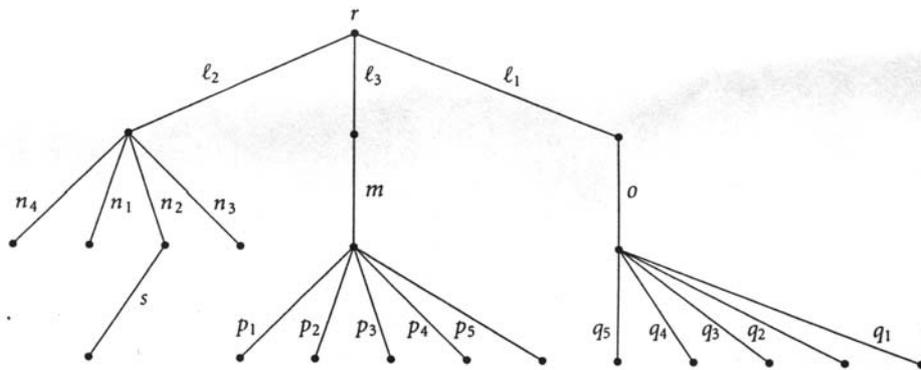
Se il cammino caratteristico di un nodo y contiene un nodo x , si dice che x è *antenato* di y e y è *discendente* di x .

Ogni nodo (eccetto la radice) è connesso tramite un ramo ad un altro nodo che ne è il *padre* e di cui rappresenta un *figlio*.

Un nodo senza figli si chiama *foglia*; un nodo con almeno una foglia si chiama *nodo interno*; il nodo interno senza padre è la radice; due o più nodi con lo stesso padre si chiamano *fratelli*.

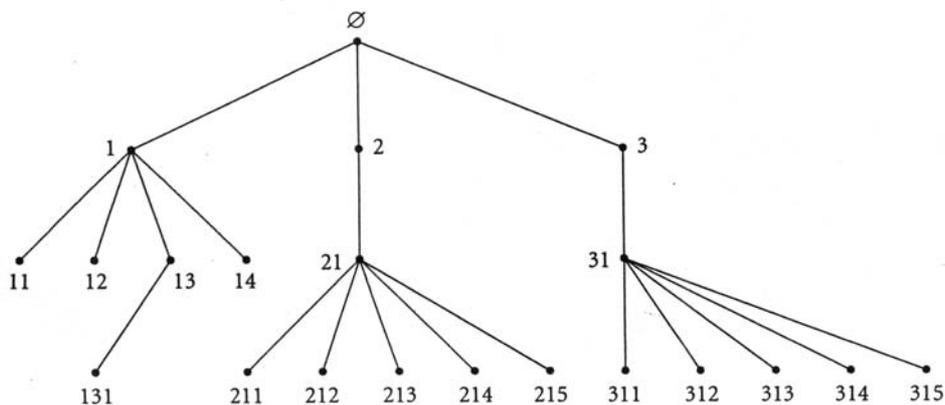
Un albero ordinato con radice è un albero con radice nel quale è imposto un ordine fra i nodi figli di ogni nodo.

Esempio. Se nell'albero con radice di cui alla fig.(d) fissiamo nei vari insiemi degli spigoli $\{l_1, l_2, l_3\}$, $\{m\}$, $\{n_1, n_2, n_3, n_4\}$, $\{o\}$, $\{p_1, p_2, p_3, p_4, p_5\}$, $\{q_1, q_2, q_3, q_4, q_5\}$, $\{s\}$ l'ordine come indicato nella figura seguente, si ottiene un albero ordinato con radice.



Osserviamo inoltre che è possibile ordinare un albero finito con radice dando in modo naturale ad ogni nodo un indice. In tal caso l'ordine imposto ai nodi è dato dalla successione finita di numeri naturali associata ad ogni nodo, la lunghezza della successione è uguale al livello del nodo; la successione associata alla radice è vuota.

Nella figura successiva nell'albero con radice precedentemente visto sono stati assegnati gli indici in modo naturale ai suoi nodi.



Dicesi *altezza di un nodo* v la lunghezza del più lungo cammino dal nodo v ad una foglia; tutte le foglie hanno altezza zero.

Dicesi *altezza di un albero* l' altezza della sua radice, o equivalentemente il massimo livello delle sue foglie.

Se T è un albero e x è un suo nodo, l' insieme dei nodi di T contenente x e tutti i suoi discendenti dicesi *sotto-albero di T e x* dicesi *radice* del sotto-albero.

Un albero si dice *binario* se ha al più due figli (detti rispettivamente figlio sinistro e figlio destro).

In un albero binario un nodo avente due figli si dice *pieno*.

Un albero binario di altezza h si dice *completo* se tutti i nodi di livello minore di h sono pieni.

Proposizione. Se T è un albero binario completo di altezza h ed n nodi, segue che:

$$n = 2^{h+1} - 1 \quad \text{ovvero} \quad h = \lg_2(n+1) - 1$$

Gli alberi ordinati con radice come rappresentazioni di espressioni algebriche.

Ad ogni espressione algebrica in cui compaiono addizioni, sottrazioni, moltiplicazioni, divisioni, estrazioni di radici, può essere associato un albero *ordinato* con radice grazie al fatto che ogni espressione algebrica può essere descritta per passi successivi mediante espressioni algebriche più semplici tra le quali bisogna eseguire una determinata operazione.

Esempio: l'espressione algebrica $c + \sqrt{(d - (a + bc)) / a}$ è ottenuta sommando le due espressioni algebriche c e $\sqrt{(d - (a + bc)) / a}$, quest'ultima è ottenuta applicando la radice quadrata all'espressione $(d - (a + bc)) / a$, la quale a sua volta è ottenuta dividendo tra loro le due espressioni $d - (a + bc)$ e a . L'espressione $d - (a + bc)$ si ottiene poi sottraendo le due espressioni d e $a + bc$; quest'ultima si ottiene sommando le due espressioni a e bc . Infine bc è ottenuta moltiplicando b e c . Questa descrizione dell'espressione algebrica considerata può essere rappresentata dall'albero *ordinato* con radice della figura 1, in cui le foglie rappresentano le variabili che compaiono nell'espressione, mentre tutti gli altri nodi rappresentano le operazioni presenti nell'espressione stessa.

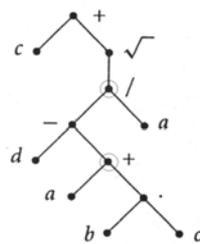


figura 1

È opportuno sottolineare il fatto che l'albero associato come prima descritto a un'espressione algebrica è *ordinato* con radice, per cui se si cambia l'ordine nell'insieme dei rami che escono da un nodo v , si ottiene ancora un albero ordinato con radice che rappresenta ancora un'espressione algebrica la quale però è diversa dalla precedente.

Esempio: l'albero *ordinato* con radice della figura 2, ottenuto dall'albero ordinato della figura 1 invertendo gli ordini sugli insiemi dei rami che escono dai nodo contrassegnati con \circ , è l'albero associato all'espressione $c + \sqrt{a/(d - (bc + a))}$, che è ben diversa da quella precedentemente considerata.

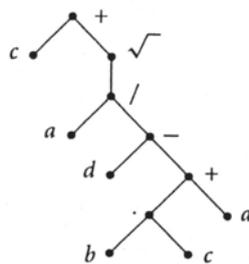


figura 2

La notazione infissa e la notazione polacca.

La notazione da noi usata per scrivere un'espressione algebrica è quella cosiddetta *a infisso*. Infatti nel denotare un'espressione ottenuta sommando, sottraendo, moltiplicando o dividendo due espressioni, il simbolo $+$, $-$, \cdot o $/$ viene scritto tra le due espressioni.

Esempio: scriviamo $a + bc$ e $a - bc$ per denotare le espressioni algebriche ottenute rispettivamente sommando e sottraendo le due espressioni a e bc ⁽¹⁾.

Le espressioni algebriche possono essere scritte, senza pericolo di ambiguità, anche ponendo il simbolo dell'operazione prima degli operandi. Tale notazione è detta *notazione polacca* (perché introdotta dal matematico polacco Lukasiewicz).

Ad esempio le espressioni algebriche da noi usualmente denotate $a + b$, $a \cdot b$, $c + \sqrt{(d - (a + bc))}/a$ e $c + \sqrt{a/(d - (bc + a))}$, in notazione polacca si scrivono $+ab$, $\cdot ab$, $+c\sqrt{/ - d + a \cdot bca}$ e $+c\sqrt{/ a - d + \cdot bca}$ rispettivamente.

Si noti che la notazione polacca permette di eliminare completamente l'uso delle parentesi, purché sia noto a priori a quanti operandi si applica ciascun simbolo (la cosiddetta *arietà* di un'operazione).

⁽¹⁾ Si ricordi che l'addizione, la sottrazione, la moltiplicazione e la divisione, sono operazioni *binarie*, mentre l'estrazione di radice quadrata è un'operazione *unaria*, ossia si applica ad un solo argomento.

3. Rappresentazioni di un grafo

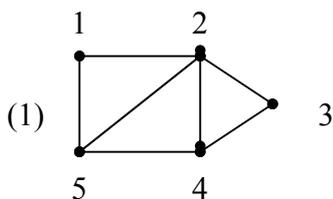
Ci sono diversi modi per rappresentare un grafo.

Tra i più importanti ricordiamo quelle matriciali e quella mediante liste di adiacenza.

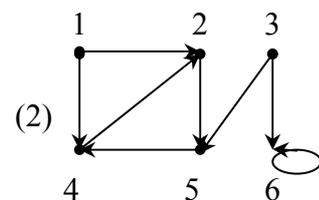
Dato un grafo (V,E) con $|V| = n$, la sua matrice di adiacenza è la matrice $n \times n$ il cui generico elemento $a_{i,j}$ è così definito:

$$a_{i,j} = \begin{cases} 1 & \text{se } (i,j) \in E \\ 0 & \text{altrimenti} \end{cases}$$

Esempi:



	1	2	3	4	5
1	0	1	0	0	1
2	1	0	1	1	1
3	0	1	0	1	0
4	0	1	1	0	1
5	1	1	0	1	0



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

Si osservi che la matrice di adiacenza di un grafo non orientato è simmetrica.

Lo spazio di memoria occupato da tale tipo di rappresentazione non dipende dal numero degli spigoli del grafo ma dal numero n dei vertici ed è uguale a n^2 .

La matrice d'incidenza di un grafo non orientato $G = (V,E)$ con $|V| = n$ e $|E| = m$ è la matrice $n \times m$ il cui generico elemento $b_{i,j}$ è così definito:

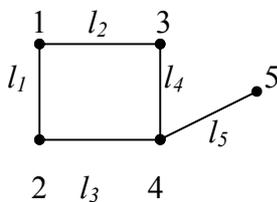
$$b_{i,j} = \begin{cases} 1 & \text{se } i \text{ è un nodo dello spigolo } l_j \\ 0 & \text{altrimenti} \end{cases}$$

Se il grafo $G = (V,E)$ è orientato è possibile definire la matrice d'incidenza solo se esso è semplice, cioè privo di cappi.

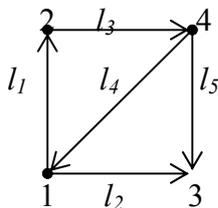
In queste ipotesi, poiché dobbiamo tenere conto se lo spigolo entra o esce da un nodo, il generico elemento $b_{i,j}$ è così definito:

$$b_{i,j} = \begin{cases} 1 & \text{se } i \text{ è il nodo iniziale dell' arco } l_j \\ -1 & \text{se } i \text{ è il nodo finale dell' arco } l_j \\ 0 & \text{altrimenti} \end{cases}$$

Riportiamo le matrici d'incidenza dei seguenti grafi:



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



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

Lo spazio di memoria occupato da tale tipo di rappresentazione è $n \times m$ è poiché $m \leq n(n-1)/2$ (si ha l'uguaglianza se il grafo è completo) risulta al più uguale a $n^2(n-1)/2$.

La rappresentazione con liste d'adiacenza di un grafo $G = (V,E)$ consiste in un vettore A_{d_j} di n liste, una per ogni vertice di V . Per ogni $a \in V$ la lista di adiacenza $A_{d_j}[a]$ contiene tutti i vertici b tale che esiste l'arco (a,b) ; pertanto $A_{d_j}[a]$ contiene tutti i vertici adiacenti ad a in G . In ogni lista di adiacenza i vertici vengono di solito memorizzati in un ordine arbitrario.

Riportiamo le due liste di adiacenza dei due grafi (1) e (2)

a	$A_{adj}[a]$
1	2, 5
2	1, 5, 3, 4
3	2, 4
4	2, 5, 3
5	4, 1, 2

a	$A_{adj}[a]$
1	2, 4
2	5
3	6, 5
4	2
5	4
6	6

Se G è orientato la somma di tutte le liste di adiacenza è $|E| = m$, se G non è orientato la somma delle lunghezze di tutte le liste di adiacenza è $2|E| = 2m$, perché se (a,b) è un arco non orientato allora b appare nella lista di a e viceversa.

In entrambi i casi lo spazio di memoria occupato da tale tipo di rappresentazione è $|V| + |E| = n + m$.

In relazione allo spazio di memoria da impegnare, una rappresentazione può essere più conveniente rispetto ad un'altra.

Chiaramente un "grafo sparso" (cioè se $m \ll n^2$) conviene rappresentarlo con la lista di adiacenza, mentre un "grafo denso" (cioè $|E| \sim |V|^2$) con la matrice di adiacenza.

APPLICAZIONI LINEARI

1. DEFINIZIONE DI APPLICAZIONE LINEARE.

Siano V e W due spazi vettoriali su un medesimo campo K . Sia $f:V \rightarrow W$ un'applicazione di V in W . Si dice che la f è **un'applicazione lineare di V in W** se sono verificate le seguenti proprietà:

$$\mathbf{a) } f(\mathbf{v}_1 + \mathbf{v}_2) = f(\mathbf{v}_1) + f(\mathbf{v}_2) \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V};$$

$$\mathbf{b) } f(\alpha \cdot \mathbf{v}) = \alpha \cdot f(\mathbf{v}) \quad \forall \alpha \in \mathbf{K}, \quad \forall \mathbf{v} \in \mathbf{V}.$$

TEOREMA

Sia $f:V \rightarrow W$ un'applicazione lineare. Allora:

$$(1) f(0_V) = 0_W;$$

$$(2) f(-v) = -f(v);$$

$$(3) f(a_1v_1 + a_2v_2 + \dots + a_rv_r) = a_1f(v_1) + a_2f(v_2) + \dots + a_rf(v_r)$$

DIMOSTRAZIONE

$$(1) f(0_V) = f(0 \cdot v) = 0 \cdot f(v) = 0_W;$$

$$(2) f(-v) = f((-1) \cdot v) = -1 \cdot f(v) = -f(v);$$

$$(3) \text{ Poich\`e } f(a_1v_1 + a_2v_2) = f(a_1v_1) + f(a_2v_2) = a_1f(v_1) + a_2f(v_2)$$

$$\text{facilmente } f(a_1v_1 + a_2v_2 + \dots + a_rv_r) = a_1f(v_1) + a_2f(v_2) + \dots + a_rf(v_r)$$

2. NUCLEO E IMMAGINE DI UN'APPLICAZIONE LINEARE.

Sia $f : V \rightarrow W$ un'applicazione lineare tra due spazi vettoriali V, W (su un campo K).

Si chiama **nucleo** dell'applicazione f l'insieme di vettori $v \in V$ tali che $f(v) = 0_W$. Il nucleo dell'applicazione f si indica con $\text{Ker } f$ ("KERNEL" dell'applicazione f):

$$\mathbf{Ker } f = \{ \mathbf{v} \in \mathbf{V} : f(\mathbf{v}) = \mathbf{0}_W \}.$$

Si chiama **immagine** dell'applicazione f l'insieme di vettori $w \in W$ che sono immagini di vettori di V . L'immagine dell'applicazione f si indica con $\text{Im } f$ o con $f(V)$:

$$\mathbf{Im } f = \{ \mathbf{w} \in \mathbf{W} : \exists \mathbf{v} \in \mathbf{V}, f(\mathbf{v}) = \mathbf{w} \}.$$

Poich\`e $f(0_V) = 0_W$, segue $0_V \in \text{Ker } f$, $0_W \in \text{Im } f$.

TEOREMA

Sia $f:V \rightarrow W$ un'applicazione lineare. Allora $\text{Ker } f$ \u00e9 un sottospazio di V .

DIMOSTRAZIONE

Dobbiamo dimostrare che:

$$1) 0_V \in \text{Ker } f;$$

$$2) \forall v_1, v_2 \in \text{Ker } f \Rightarrow v_1 + v_2 \in \text{Ker } f;$$

$$3) \forall \alpha \in K, \forall v \in \text{Ker } f \Rightarrow \alpha v \in \text{Ker } f.$$

$$1) 0_V \in \text{Ker } f \text{ poich\`e } f(0_V) = 0_W.$$

$$2) \text{ Siano } v_1, v_2 \in \text{Ker } f, \text{ allora: } f(v_1) = 0_W, f(v_2) = 0_W.$$

$$\text{Poich\`e } f(v_1 + v_2) = f(v_1) + f(v_2) = 0_W + 0_W = 0_W \Rightarrow v_1 + v_2 \in \text{Ker } f;$$

3) Sia $\alpha \in K$, $v \in \text{Ker } f$.

Poiché $f(\alpha \cdot v) = \alpha \cdot f(v) = \alpha \cdot 0_W = 0_W \Rightarrow \alpha v \in \text{Ker } f$.

TEOREMA (di caratterizzazione delle applicazioni lineari iniettive)

Sia $f: V \rightarrow W$ un'applicazione lineare.

f è iniettiva $\Leftrightarrow \text{Ker } f = \{0_V\}$.

DIMOSTRAZIONE

\Rightarrow Se f è iniettiva allora $\text{Ker } f = \{0_V\}$.

Infatti, se $v \in \text{Ker } f$, non può essere $v \neq 0_V$ poiché sarebbe $f(v) = f(0_V) = 0_W$ e la f non sarebbe iniettiva. Dunque $\text{Ker } f = \{0_V\}$.

\Leftarrow Se $\text{Ker } f = \{0_V\}$ allora f è iniettiva.

Siano $v_1, v_2 \in V$ con $v_1 \neq v_2 \stackrel{?}{\Rightarrow} f(v_1) \neq f(v_2)$.

Infatti, se fosse $f(v_1) = f(v_2)$ allora $f(v_1) - f(v_2) = 0_W$, dunque $f(v_1 - v_2) = 0_W \Rightarrow v_1 - v_2 \in \text{Ker } f$ essendo $\text{Ker } f = \{0_V\} \Rightarrow v_1 - v_2 = 0_V$ e quindi $v_1 = v_2$, contro l'ipotesi $v_1 \neq v_2$

TEOREMA

Sia $f: V \rightarrow W$ un'applicazione lineare. Allora $\text{Im } f$ è un sottospazio di W .

DIMOSTRAZIONE

Dobbiamo dimostrare che:

1) $0_W \in \text{Im } f$;

2) $\forall w_1, w_2 \in \text{Im } f \Rightarrow w_1 + w_2 \in \text{Im } f$;

3) $\forall \alpha \in K, \forall w \in \text{Im } f \Rightarrow \alpha w \in \text{Im } f$.

1) $0_W \in \text{Im } f$ poiché $f(0_V) = 0_W$.

2) Siano $w_1, w_2 \in \text{Im } f$, esistono allora $v_1, v_2 \in V$ tali che $f(v_1) = w_1, f(v_2) = w_2$. Consideriamo $v_1 + v_2$ in V . poiché $f(v_1 + v_2) = f(v_1) + f(v_2) = w_1 + w_2$, si ha $w_1 + w_2 \in \text{Im } f$

3) Sia $\alpha \in K, w \in \text{Im } f$. Essendo $w \in \text{Im } f$, esiste in V un v tale che $f(v) = w$. Consideriamo $\alpha \cdot v$. Poiché $f(\alpha \cdot v) = \alpha \cdot f(v) = \alpha \cdot w \Rightarrow \alpha \cdot w \in \text{Im } f$.

Sia $f: V \rightarrow W$ un'applicazione lineare. Se la f è *biunivoca*, allora essa è detta **isomorfismo** di V in W e i due spazi V, W sono detti *isomorfi*.

Evidentemente, se f è biunivoca essa è iniettiva e suriettiva ($f(V) = W$). In tal caso, tenendo conto dei teoremi precedenti, si ha:

TEOREMA

$f: V \rightarrow W$ è un isomorfismo se e solo se $\text{Ker } f = \{0_V\}$ e $\text{Im } f = W$.

($\dim V = \dim W \Leftrightarrow f$ è un isomorfismo)

3. PROPRIETA' RELATIVE A GENERATORI, INSIEMI LIBERI, BASI

Sia $f:V \rightarrow W$ un'applicazione lineare tra due spazi vettoriali V, W (su un campo K).

TEOREMA

- 1) Se v_1, v_2, \dots, v_r generano V allora $f(v_1), f(v_2), \dots, f(v_r)$ generano $f(V)$ (a generatori di V corrispondono generatori di $f(V)$): $V = \mathcal{L}(v_1, v_2, \dots, v_r) \Rightarrow f(V) = \mathcal{L}(f(v_1), f(v_2), \dots, f(v_r))$;
- 2) Se $f(v_1), f(v_2), \dots, f(v_r)$ sono linearmente indipendenti allora v_1, v_2, \dots, v_r sono linearmente indipendenti (vettori indipendenti di W provengono da vettori indipendenti di V) ((MA NON E' DETTO CHE A VETTORI INDIPENDENTI CORRISPONDANO VETTORI INDIPENDENTI)).

DIMOSTRAZIONE

1) Supponiamo che v_1, v_2, \dots, v_r siano dei generatori di V : dunque ogni vettore $v \in V$ è combinazione lineare di v_1, v_2, \dots, v_r . Dobbiamo dimostrare che $f(v_1), f(v_2), \dots, f(v_r)$ generano $f(V)$: dunque ogni vettore dell'immagine è combinazione lineare di $f(v_1), f(v_2), \dots, f(v_r)$.

Sia, quindi, $w \in f(V) \Rightarrow \exists v \in V: f(v) = w$

Ma: $v \in V \Rightarrow v = a_1v_1 + a_2v_2 + \dots + a_rv_r$

Dunque $f(v) = f(a_1v_1 + a_2v_2 + \dots + a_rv_r)$

$$w = a_1f(v_1) + a_2f(v_2) + \dots + a_rf(v_r)$$

2) Supponiamo $f(v_1), f(v_2), \dots, f(v_r)$ linearmente indipendenti. Dobbiamo dimostrare che v_1, v_2, \dots, v_r sono linearmente indipendenti.

Consideriamo l'equazione: $x_1v_1 + x_2v_2 + \dots + x_rv_r = 0_V$ e vediamo per quali valori degli scalari x_1, x_2, \dots, x_r essa è verificata.

Si ha:

$$x_1v_1 + x_2v_2 + \dots + x_rv_r = 0_V \Rightarrow f(x_1v_1 + x_2v_2 + \dots + x_rv_r) = f(0_V) = 0_W \Rightarrow x_1f(v_1) + x_2f(v_2) + \dots + x_rf(v_r) = 0_W$$

Da questa, essendo $f(v_1), f(v_2), \dots, f(v_r)$ linearmente indipendenti, segue $x_1 = 0, x_2 = 0, \dots, x_r = 0$.

Se la f è iniettiva le implicazioni del teorema precedente si possono invertire:

TEOREMA

Sia $f:V \rightarrow W$ iniettiva. Si ha:

- 1) Se $f(v_1), f(v_2), \dots, f(v_r)$ sono generatori di $f(V)$ allora v_1, v_2, \dots, v_r sono generatori di V ;
- 2) Se v_1, v_2, \dots, v_r sono linearmente indipendenti allora $f(v_1), f(v_2), \dots, f(v_r)$ sono anch'essi linearmente indipendenti.

DIMOSTRAZIONE

1) Supponiamo che $f(v_1), f(v_2), \dots, f(v_r)$ generano $f(V)$, dobbiamo dimostrare che $V = \mathcal{L}(v_1, v_2, \dots, v_r)$, ossia che ogni vettore di V è combinazione lineare di v_1, v_2, \dots, v_r .

Sia $v \in V$. Consideriamo $f(v)$. Si ha:

$$f(v) = a_1f(v_1) + a_2f(v_2) + \dots + a_rf(v_r) \Rightarrow f(v) = f(a_1v_1 + a_2v_2 + \dots + a_rv_r) \Rightarrow \text{(per l'iniettività della } f\text{)}^{(1)} \Rightarrow v = a_1v_1 + a_2v_2 + \dots + a_rv_r.$$

⁽¹⁾ Se f iniettiva: $f(v_1) = f(v_2) \Rightarrow v_1 = v_2$

2) Consideriamo l'equazione:

$$x_1 f(v_1) + x_2 f(v_2) + \dots + x_r f(v_r) = 0_W$$

e vediamo per quali valori degli scalari essa è verificata.

Si ha: $x_1 f(v_1) + x_2 f(v_2) + \dots + x_r f(v_r) = 0_W \Rightarrow f(x_1 v_1 + x_2 v_2 + \dots + x_r v_r) = 0_W \Rightarrow$ (per l'iniettività della f) $\Rightarrow x_1 v_1 + x_2 v_2 + \dots + x_r v_r = 0_V \Rightarrow$ (essendo v_1, v_2, \dots, v_r lin. ind.) $\Rightarrow x_1 = 0, x_2 = 0, \dots, x_r = 0$.

Abbiamo, dunque, la seguente situazione:

Sia $f: V \rightarrow W$ un'applicazione lineare

v_1, v_2, \dots, v_r sono generatori di V	\Rightarrow	$f(v_1), f(v_2), \dots, f(v_r)$ sono generatori di $f(V)$
	\Leftarrow se f è iniettiva	
$f(v_1), f(v_2), \dots, f(v_r)$ sono linearmente indipendenti	\Rightarrow	v_1, v_2, \dots, v_r sono linearmente indipendenti
	\Leftarrow se f è iniettiva	

Si ha, quindi, il seguente teorema:

TEOREMA

Sia $f: V \rightarrow W$ iniettiva. Allora:

- $\{v_1, v_2, \dots, v_r\}$ è una base di V se e solo se $f(v_1), f(v_2), \dots, f(v_r)$ è una base di $f(V) = \text{Im } f$;
- $\dim V = \dim \text{Im } f$.

DIMOSTRAZIONE

La 1) segue dai teoremi precedenti. La 2) segue dalla 1).

Più in particolare:

TEOREMA

Sia $f: V \rightarrow W$ un isomorfismo allora:

- (v_1, v_2, \dots, v_r) è una base di V se e solo se $f(v_1), f(v_2), \dots, f(v_r)$ è una base di W ;
- $\dim V = \dim W$.

4. RELAZIONE TRA $\dim V$, $\dim \text{Ker } f$, $\dim \text{Im } f$

Sia $f: V \rightarrow W$ un'applicazione lineare tra due spazi vettoriali V, W (su un campo K).

TEOREMA

Sia V finitamente generato. Allora:

$$\dim V = \dim \text{Ker } f + \dim \text{Im } f$$

5. ISOMORFISMO TRA GLI SPAZI V DI DIMENSIONE n E K^n

TEOREMA

Sia V uno spazio vettoriale di dimensione n. Esiste, allora, un isomorfismo fra V e K^n

Se $v \in V$ è un qualunque vettore di V e $B = \{v_1, v_2, \dots, v_n\}$ una base di V, allora $v = a_1v_1 + a_2v_2 + \dots + a_nv_n$ e tale modo di scomporre v, come combinazione lineare di v_1, v_2, \dots, v_n , è unico.

Considera l'applicazione $\varphi : V \rightarrow K^n$ tale che $\forall v \in V$ è $\varphi(v) = (a_1, a_2, \dots, a_n)$, si dimostra che tale applicazione φ è lineare e biunivoca, pertanto è un isomorfismo.

6. APPLICAZIONI LINEARI E MATRICI

Sia $f:V \rightarrow W$ un'applicazione lineare tra due spazi vettoriali V, W (su un campo K), con $\dim V = n$ e $\dim W = m$.

Sia $B = \{v_1, v_2, \dots, v_n\}$ una base di V, $C = \{w_1, w_2, \dots, w_m\}$ una base di W.

E' possibile definire una matrice $m \times n$, associata all'applicazione f, rispetto alle basi B, C, nel modo seguente:

per ogni vettore $v_i \in B$, determiniamo il corrispondente $f(v_i) \in W$. Essendo C una base di W, ognuno di questi vettori si può scrivere come combinazione lineare di w_1, w_2, \dots, w_m . Si ha, quindi:

$$v_1 \rightarrow f(v_1) = a_{11}w_1 + a_{21}w_2 + \dots + a_{m1}w_m = (a_{11}, a_{21}, \dots, a_{m1})$$

$$v_2 \rightarrow f(v_2) = a_{12}w_1 + a_{22}w_2 + \dots + a_{m2}w_m = (a_{12}, a_{22}, \dots, a_{m2})$$

⋮

$$v_n \rightarrow f(v_n) = a_{1n}w_1 + a_{2n}w_2 + \dots + a_{mn}w_m = (a_{1n}, a_{2n}, \dots, a_{mn})$$

La matrice:

$$M_f^{B,C} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \in K_{m,n}$$

si dice **matrice associata all'applicazione f rispetto alle basi B,C**.

Osserviamo che la prima colonna della matrice è formata dalle componenti del vettore $f(v_1)$ rispetto alla base C, la seconda colonna è formata dalle componenti del vettore $f(v_2)$ rispetto alla base C, ..., l'ultima colonna è formata dalle componenti del vettore $f(v_n)$ rispetto alla base C.

Sia M una matrice $m \times n$. Siano V e W due spazi vettoriali di dimensione rispettivamente, n ed m. Siano, infine, B, C due basi, l'una di V, l'altra di W. E' possibile associare ad M un'applicazione lineare $f : V \rightarrow W$, che si dirà associata ad M rispetto alle basi B, C, nel seguente modo:

sia $v \in V$ e siano x_1, x_2, \dots, x_n le componenti di v rispetto a B;

cioè: $v = x_1v_1 + x_2v_2 + \dots + x_nv_n \equiv (x_1, x_2, \dots, x_n)_B$.

Il vettore $f(v)$ è quel vettore di W le cui componenti $(y_1, y_2, \dots, y_m)_C$ sono determinate nel modo seguente:

$$y_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n$$

$$y_2 = a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n$$

⋮

$$y_m = a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n$$

essendo

$$M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Dunque, $v \equiv (x_1, x_2, \dots, x_n)_B \xrightarrow{f} (y_1, y_2, \dots, y_m)_C$ dove y_1, y_2, \dots, y_m sono determinate in modo che

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

L'applicazione così definita si indica con $f_M^{B,C}$.

7. APPLICAZIONI LINEARI MEDIANTE LE IMMAGINI DEI VETTORI DI UNA BASE

Sia $B = (v_1, v_2, \dots, v_n)$ una base di V . Supponiamo siano assegnati, secondo una certa legge f , i vettori $f(v_1), f(v_2), \dots, f(v_n)$. In tal caso è definita un'applicazione lineare $g : V \rightarrow W$, *estensione* della f a tutto V .

TEOREMA

Se $B = \{v_1, v_2, \dots, v_n\}$ è una base di V e w_1, w_2, \dots, w_n sono vettori di W , l'applicazione $f : B \rightarrow W$ tale che $f(v_1) = w_1, f(v_2) = w_2, \dots, f(v_n) = w_n$ definisce, in modo unico, un'applicazione lineare di V in W

DIMOSTRAZIONE

Sia $v \in V$, con $v = x_1v_1 + x_2v_2 + \dots + x_nv_n$.

Si può definire: $f(v) = f(x_1v_1 + x_2v_2 + \dots + x_nv_n) = x_1f(v_1) + x_2f(v_2) + \dots + x_nf(v_n)$.

Si verifica facilmente che tale applicazione di V in W è lineare ed è unica perché è la scomposizione di v come combinazione lineare di v_1, v_2, \dots, v_n .

8. STUDIO DI Ker f E Im f

Sia $f:V \rightarrow W$ un'applicazione lineare. Per definizione $\text{Ker } f = \{v \in V : f(v) = 0_W\}$.

Se B è una base di V , C una base di W , $M_f^{B,C}$ la matrice associata all'applicazione f , rispetto a B, C , posto $X = (x_1, x_2, \dots, x_n)_B$ allora $\text{Ker } f$ è l'insieme dei vettori X tali che $f(X) = 0_W$, ossia $f(x_1, x_2, \dots, x_n)_B = (0, 0, \dots, 0)$.

In modo equivalente, $\text{Ker } f$ è l'insieme dei vettori X tali che $M_f^{B,C} * X = 0$ ossia le cui componenti rispetto a B sono soluzioni del sistema omogeneo associato alle matrice $M_f^{B,C}$. Ricordiamo, inoltre, che $\dim V = \dim \text{Ker } f + \dim \text{Im } f$. Dunque: $\dim \text{Ker } f = \dim V - r$ essendo r il rango⁽²⁾ della matrice associata all'applicazione f , rispetto a B, C .

9. ENDOMORFISMO

Un'applicazione lineare di V in se stesso ($f: V \rightarrow V$) si dice *endomorfismo*.

Sia $f: V \rightarrow V$ un endomorfismo nello spazio vettoriale V su un campo K , diremo che $\lambda \in K$ è un *autovalore* di f se verifica questa proprietà:

$$\exists v \in V, v \neq 0_V : f(v) = \lambda v,$$

v si dice *autovettore* di f associato all'autovalore λ .

Allora: v autovettore di f associato all'autovalore λ $\stackrel{\text{def}}{\Leftrightarrow} f(v) = \lambda v \Leftrightarrow f_\lambda(v) = f(v) - \lambda v = 0 \Rightarrow$ l'insieme degli autovettori associati a λ è il nucleo di f_λ definito da $f_\lambda(v) = f(v) - \lambda v$ per cui è un sottospazio di V , chiamato *autospazio* di f associato all'autovalore λ e si denota con V_λ
 $\Rightarrow V_\lambda = \text{Ker } f_\lambda$.

10. ENDOMORFISMO SEMPLICE

Sia $f: V \rightarrow V$ un endomorfismo definito su V e sia, inoltre, $\dim V = n$.

Si dice che f è un **endomorfismo semplice** se ammette una base di autovettori:

f semplice (o diagonalizzabile) $\stackrel{\text{def}}{\Leftrightarrow} \exists B = \{v_1, v_2, \dots, v_n\}$ di autovettori, base di V .

Si dimostra che autovettori non nulli associati ad autovalori distinti sono linearmente indipendenti; da cui segue che, se il polinomio caratteristico⁽³⁾ ha n radici distinte in K , esiste una base di V formata da autovettori di f ed, in tal caso, f si dice che è semplice.

Sia $V = K^n$ e λ , autovalore di f , sia una radice di molteplicità r del polinomio caratteristico di f . Sappiamo che $\dim V_\lambda = n - \rho(M(f) - \lambda I)$.

Si dimostra che $\boxed{1 \leq \dim V_\lambda \leq r}$.

TEOREMA

Un endomorfismo $f: V \rightarrow V$ è semplice se e solo se esiste una base B di V tale che $M_f^{B,B}$ è diagonale.

⁽²⁾ Data una matrice $A(n \times m)$, il numero $r, 0 \leq r \leq \min(n, m)$, si dice rango di A se esiste almeno un minore di ordine r non nullo, e se tutti i minori di ordine maggiore di r sono nulli.

⁽³⁾ Si chiama polinomio caratteristico il determinante della matrice $M(f) - \lambda I$

DIMOSTRAZIONE

⇒ Se f è semplice, allora esiste una base $B = \{v_1, v_2, \dots, v_n\}$ di V di autovettori. Dunque:

$$f(v_1) = \lambda_1 v_1 \rightarrow \lambda_1 v_1 = \lambda_1 v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_n \cong (\lambda_1, 0, \dots, 0)_E$$

$$f(v_2) = \lambda_2 v_2 \rightarrow \lambda_2 v_2 = 0 \cdot v_1 + \lambda_2 v_2 + \dots + 0 \cdot v_n \cong (0, \lambda_2, 0, \dots, 0)_E$$

⋮

$$f(v_n) = \lambda_n v_n \rightarrow \lambda_n v_n = 0 \cdot v_1 + 0 \cdot v_2 + \dots + \lambda_n \cdot v_n \cong (0, 0, \dots, \lambda_n)_E$$

(dove $\lambda_1, \lambda_2, \dots, \lambda_n$ non sono tutti necessariamente distinti),

allora $M_f^{B,B} = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$ è una matrice diagonale (e sulla diagonale appaiono

gli autovalori della f)

⇐ Sia $f: V \rightarrow V$ e sia $B = \{v_1, v_2, \dots, v_n\}$ una base di V tale che $M_f^{B,B}$ è diagonale,

cioè: $M_f^{B,B} = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$.

Per definizione:

$$f(v_1) = \lambda_1 v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_n = \lambda_1 v_1$$

$$f(v_2) = 0 \cdot v_1 + \lambda_2 v_2 + \dots + 0 \cdot v_n = \lambda_2 v_2$$

⋮

$$f(v_n) = 0 \cdot v_1 + 0 \cdot v_2 + \dots + \lambda_n \cdot v_n = \lambda_n v_n$$

allora v_1, v_2, \dots, v_n sono tutti autovettori $\Rightarrow f$ è semplice.

Ricordiamo che una matrice quadrata $M \in K_{n,n}$ si dice *diagonalizzabile* se è simile ad una matrice diagonale.

In altre parole:

M è diagonalizzabile $\stackrel{\text{def}}{\Leftrightarrow} \exists P \in K_{n,n}, P$ invertibile: $P^{-1} \cdot M \cdot P = D$ (matrice diagonale).

TEOREMA

Sia $A \in K^{n,n}$ e sia $f: K^n \rightarrow K^n$ l'endomorfismo associato ad A . allora si ha:

A è diagonalizzabile se e solo se f è semplice.

DIMOSTRAZIONE

Infatti: se f è semplice sia $\{v_1, v_2, \dots, v_n\}$ una base di K^n formata da autovettori di f e sia P la matrice avente per colonne v_1, v_2, \dots, v_n (P è invertibile) allora $D = P^{-1}AP$ è diagonale e gli elementi di D sono gli autovalori di f , ripetuti ciascuno con la sua molteplicità ($PD = AP$). Viceversa se A è diagonale è ovvio che f è semplice.

TEOREMA

f è semplice \Leftrightarrow ^{teor} 1) tutte le radici del polinomio caratteristico di f sono in K ;
 2) $\dim V_\lambda = r_\lambda$ (la molteplicità di λ) (ovvero, $n - \rho(A - \lambda I) = r_\lambda$).

DIMOSTRAZIONE

Basta prendere come base formata da autovettori l'insieme F unione delle basi di ciascun autospazio $\Rightarrow M_f^{E,F}$ è una matrice diagonale, cioè:

$$\left\| \begin{array}{cccc} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & \lambda_m \end{array} \right\| \quad \begin{array}{l} \text{con } \lambda_1 \text{ ripetuto } r_1 \text{ volte} \\ \lambda_2 \text{ ripetuto } r_2 \text{ volte} \\ \dots \\ \lambda_m \text{ ripetuto } r_m \text{ volte} \\ \text{ed } r_1 + r_2 + \dots + r_m = n \end{array}$$

Sia V un K -spazio vettoriale e $f: V \rightarrow V$ un endomorfismo

$\lambda \in K$, λ un autovalore di $f \Leftrightarrow \exists v \in V, v \neq 0_V: f(v) = \lambda v \Rightarrow \lambda$ autovalore \Leftrightarrow
 $\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = \lambda x_1 \\ \dots \\ a_{n1}x_1 + \dots + a_{nn}x_n = \lambda x_n \end{cases}$ ha soluzioni non nulle;

ossia, se e solo se il determinante del sistema lineare omogeneo

$$\begin{cases} (a_{11} - \lambda)x_1 + \dots + a_{1n}x_n = 0 \\ \dots \\ a_{n1}x_1 + \dots + (a_{nn} - \lambda)x_n = 0 \end{cases}$$

è nullo $\Rightarrow \lambda$ autovalore di $f \Leftrightarrow \lambda$ è radice dell'equazione in T :

$$|A - T I| = \begin{vmatrix} a_{11} - T & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - T & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & \dots & \dots & a_{nn} - T \end{vmatrix} = 0 \quad \text{dove } A = M(f);$$

tale determinante si chiama *polinomio caratteristico* di A o di $f^{(4)}$ ed è di grado n .
 Per cui, gli autovalori di f sono le radici del polinomio caratteristico di f che appartengono a K .

⁽⁴⁾ Siano A e B le matrici associate a f rispetto alle basi F ed H rispettivamente. Si dimostra che A e B hanno lo stesso polinomio caratteristico.