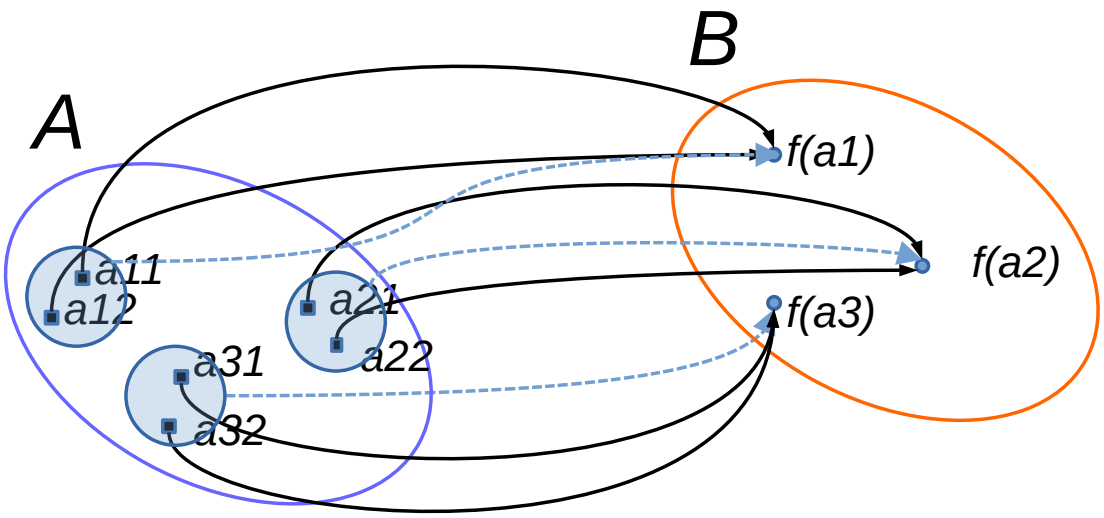


Algebra Generale

come l'ho capita io, ... e non è detto sia il modo giusto

luciano de falco alfano

ver. 0.7.1
2022-06-02

Indice

Presentazione **7**

Abbreviazioni **12**

Introduzione **14**

1 Operazioni tra insiemi **15**
1.1 nozioni . . . 15
1.2 operazioni tra insiemi . . . 18
1.3 prodotto cartesiano . . . 23
1.4 relazioni . . . 25
1.5 insieme quoziente . . . 27
1.6 applicazioni . . . 28
1.7 composizione di applicazioni . . . 33
1.8 insiemi equipotenti . . . 34
1.9 partizione di un insieme e applicazioni . . . 34
1.10 trasformazioni di un insieme . . . 36
1.11 leggi di composizione . . . 37
1.12 struttura algebrica . . . 39
1.13 omomorfismo, isomorfismo . . . 40
1.14 ripassando . . . 42

2 Gruppi, anelli, campi **46**
2.1 gruppi . . . 46
2.2 conseguenze algebriche della definizione di gruppo . . . 48
2.3 rappresentazione di gruppi finiti . . . 48
2.4 gruppo delle isometrie e delle simmetrie . . . 49
2.5 sottogruppi . . . 50
2.6 omomorfismi, isomorfismi, automorfismi di un gruppo . . . 52
2.7 traslazioni a destra e a sinistra, teorema di Cayley . . . 53
2.8 anelli . . . 54
2.9 campi . . . 55
2.10 ripassando . . . 56

3 Spazi vettoriali **59**
3.1 nozione di spazio vettoriale . . . 59
3.2 dipendenza e indipendenza lineare . . . 62
3.3 dimensione di uno spazio vettoriale . . . 64
3.4 relazioni tra le componenti del vettore somma di più vettori e le componenti dei vettori addendi . . . 64
3.5 sottospazi vettoriali . . . 65
3.6 sottospazi generati da r vettori indipendenti . . . 66
3.7 somme di due spazi vettoriali . . . 66
3.8 cambiamenti di base in E_n. legge di trasformazione delle componenti di un vettore . . . 68
3.9 ripassando . . . 69

4 Applicazioni lineari tra spazi vettoriali **72**
4.1 applicazioni lineari . . . 72
4.2 omomorfismi e isomorfismi tra spazi vettoriali . . . 73
4.3 immagine, rango, nucleo di una applicazione lineare . . . 74
4.4 spazio vettoriale quoziente . . . 76
4.5 spazio vettoriale delle applicazioni lineari di E in F . . . 78
4.6 relazioni tra applicazioni lineari e matrici . . . 79
4.7 endomorfismo e operatori lineari di E_n . . . 80
4.8 rappresentazione di un endomorfismo mediante matrice . . . 81
4.9 endomorfismo inverso . . . 82
4.10 rappresentazione di uno stesso operatore in basi diverse . . . 82
4.11 ripassando . . . 83

5 Autovalori e autovettori di un operatore lineare **86**
5.1 autovalori e autovettori di un operatore . . . 86
5.2 polinomio caratteristico di una matrice . . . 88
5.3 endomorfismi diagonalizzabili . . . 91
5.4 successione di sottospazi a bandiera indotta da A . . . 94
5.5 struttura di endomorfismi nilpotenti . . . 95
5.6 decomposizione di E_n in somma diretta di sottospazi invarianti per A . . . 97
5.7 autovettori generalizzati, forma canonica di Jordan . . . 97
5.8 polinomi di operatori e matrici . . . 98

Dizionario dei termini e dei sinonimi **100**

GNU Free Documentation License **103**
1. APPLICABILITY AND DEFINITIONS . . . 103
2. VERBATIM COPYING . . . 105
3. COPYING IN QUANTITY . . . 105
4. MODIFICATIONS . . . 106
5. COMBINING DOCUMENTS . . . 107

6. COLLECTIONS OF DOCUMENTS 108
7. AGGREGATION WITH INDEPENDENT WORKS 108
8. TRANSLATION 108
9. TERMINATION 109
10. FUTURE REVISIONS OF THIS LICENSE 109
11. RELICENSING 110

Bibliografia **111**

Indice analitico **112**

Elenco delle figure

1.1 Diagramma di Venn: rappresentazione di un insieme. 15
1.2 Operazione di unione 19
1.3 Operazione di intersezione 19
1.4 Operazione di partizione 20
1.5 Operazione di differenza tra insiemi 21
1.6 Operazione di ricomposizione da differenza e intersezione di insiemi 21
1.7 Complementare di un insieme 22
1.8 Legge di Morgan 23
1.9 Somma disgiunta 24
1.10 Relazione binaria 25
1.11 Applicazione: rappresentazione con diagrammi di Venn 28
1.12 Sx: Applicazione. Dx: Funzione binaria 29
1.13 Applicazione: terminologia 30
1.14 Applicazione biiettiva 31
1.15 Applicazione composta 33
1.16 Descrizione di un diagramma commutativo 34
1.17 Diagramma commutativo di applicazioni 35
1.18 Omomorfismo di una applicazione tra insiemi 41
1.19 Insiemi: relazioni tra le nozioni 42
1.20 Ripassando: Insiemi, relazioni tra le operazioni 43
1.21 Ripassando. Insiemi: relazioni, applicazioni, . . . isomorfismo 45

2.1 Rotazioni antiorarie di 60° e 120° di un esagono 50
2.2 Riflessione di un esagono rispetto l'asse H-K 51
2.3 Gruppi: dai gruppi ai campi 57

3.1 Ripassando: spazi vettoriali 71

4.1 Diagramma commutativo di applicazioni lineari con $E/Ker(L)$ 78
4.2 Ripassando: le applicazioni lineari 85

Elenco delle tabelle

versioni del documento 10
abbreviazioni 12

1.1 tabella di verità della implicazione logica 16
1.2 tabella di verità della coimplicazione 17

2.1 tabella moltiplicativa per un gruppo di ordine 1 48
2.2 tabella moltiplicativa per un gruppo di ordine 2 48
2.3 tabella moltiplicativa per un gruppo di ordine 3 48
2.4 tavola delle moltiplicazioni per le rotazioni di un esagono 50

Presentazione

Vi raccontiamo come è nato il progetto di scrivere queste righe.

In tenera età ci siamo iscritti alla Facoltà di Ingegneria dell'Università degli Studi di Roma. Avremmo voluto frequentare la Facoltà di Fisica, ma quel despota ☺ di nostro padre[1] ci pose di fronte alla scelta: o Ingegneria, o Medicina.

Risultato: per mettere dentro quanti più esami di fisica possibili ... Ingegneria Nucleare.

Solo che Ingegneria Nucleare includeva un esame semestrale intitolato: *Geometria II indirizzo algebra astratta*. Mai sentita nominare una tal materia! Così abbiamo acquistato il relativo testo e gli abbiamo dato un'occhiata ... per chiuderlo di corsa e precipitarci a compilare un piano di studi individuale che estromettesse *Algebra Astratta* e includesse *Calcolatori*, convinti che non saremmo mai riusciti a digerire concetti di tal fatta.

Ora, tanti anni dopo, ci è capitato di riprendere in mano alcuni dei vetusti testi del nostro corso di laurea. E, con sommo stupore, rileggendo con più calma il testo di *Algebra Astratta*, ci siamo resi conto che i concetti in questione non sono poi così incapibili.

Da qui l'idea di scrivere queste note. Nella speranza di aiutare qualcuno più giovane del sottoscritto a non essere altrettanto precipitoso nell'eliminare concetti che, se affrontati con calma, si dimostrano abbordabili e, perché no, interessanti.

Naturalmente lo sventurato lettore dovrà tenere conto del fatto che chi scrive è un banale ingegnere: quanto di più lontano possibile da un matematico[2]. Quindi non aspettatevi pletore di dimostrazioni. Per carità: le dimostrazioni in matematica sono fondamentali, ma per quelle esistono i testi scritti dai matematici. No. Molto semplicemente qui riporteremo a briglia sciolta quattro chiacchiere in base a quello che siamo riusciti a capire della materia. Senza avere la supponenza di essere esaustivi. Solo, per quanto riusciremo, vi assicuriamo che cercheremo di non scrivere svarioni. E, se qualcosa ci sarà sfuggito: pazienza, ... siamo umani.

[1] Che pensava costantemente cosa fosse meglio per i propri figli.

[2] La conoscete quella barzelletta che racconta di come un matematico, un fisico e un ingegnere si ritrovano a mensa ed osservando il pentolone della pasta a bollire sul fuoco, e si chiedono quanto gas sia necessario per cuocere la pasta?

Il matematico: "Basta risolvere l'integrale nel tempo del consumo istantaneo del combustibile, derivabile dalla quantità di calore necessaria per cuocere la pasta."

Il fisico: "Dato il calore specifico del gas e calcolato il volume dell'acqua con la pasta per conoscere il calore totale necessario alla cottura, basta una divisione per calcolare quanto gas si deve utilizzare."

L'ingegnere: "E se lo misurassimo?"

Un'ultima nota. Attenzione a non farvi fuorviare dall'affermazione che si tratta di una chiacchierata. L'*Algebra Generale*, per quanto capibile, è comunque impegnativa. Va affrontata con calma e riflettendo bene sui concetti esposti.

Se quanto vi abbiamo detto vi ha incuriosito, proseguite con la lettura. Altrimenti smettete di leggere e passate ad altro. Vi assicuriamo che Voi non ne morirete, e Noi ce ne faremo una ragione.

Un'ultima considerazione. Questo lavoro ha ereditato la struttura del manuale di algebra a suo tempo messo da parte. Stiamo parlando di [Gasparini 1977], scritto dalla professoressa Ida Cattaneo Gasparini, cui va tutta la nostra gratitudine.

struttura prevista

Visto che va di moda parlare di tecniche *Agile* per la gestione dei progetti, vediamo di applicarle alla pubblicazione di questo scritto: lo pubblicheremo facendolo via via crescere, un capitolo dopo l'altro. Questo perché ci vorrà parecchio tempo per completarlo. E contemporaneamente sappiamo che siete estremamente impazienti di leggerlo ☺. Quindi appena un nuovo pezzo sarà disponibile, lo pubblicheremo senza indugio.

Nel frattempo, qui di seguito indichiamo quello che, per ora, è l'elenco dei capitoli che dovrebbero essere inclusi nel testo[3]:

- ~~operazioni sugli insiemi~~
- ~~gruppi, anelli, campi~~
- ~~spazi vettoriali~~
- ~~applicazioni lineari tra spazi vettoriali~~
- ~~autovalori e autovettori di un operatore lineare~~, salvo il riassunto
- spazio duale
- spazi vettoriali euclidei e spazi unitari
- applicazioni multilineari e tensori

[3] In questo elenco, i capitoli cancellati con una linea orizzontale sovrascritta sono già stati redatti.

avvertenze

In questo documento usiamo le lettere maiuscole (ad es.: A, B, C) per indicare insiemi. E lettere minuscole, a volte numerate, per indicare elementi di un insieme (ad es.: $a, a1, a_1$ per indicare un elemento dell'insieme A). Mentre i concetti sono indicati per esteso (ad es.: *insieme*), a volte abbreviati (ad es. *ins.* per indicare *insieme*). Queste indicazione sono valide non solo per il testo, ma anche per i contenuti di diagrammi e mappe concettuali.

Vettori e matrici di solito sono indicati utilizzando il grassetto. Le seconde utilizzando lettere maiuscole. Ad es. il vettore $\mathbf{x}$. O la matrice di m righe per n colonne $\mathbf{A}_{m \times n}$.

Termini utilizzati, o definiti, per la prima volta sono scritti in grassetto. Se il termine in questione è riportato in *Indice analitico*, probabilmente il relativo numero di pagina punta ad un termine scritto in grassetto.

Per enfatizzare un aspetto da tenere in particolare considerazione, utilizziamo il corsivo o il sottolineato. Se si tratta di una parola o di poche frasi. Altrimenti tenete presente quanto segue.

Tutti i concetti esposti sono importanti. Ma alcuni sono decisamente pervasivi: ricompaiono in continuazione. In questi casi, per aumentare l'attenzione del lettore borderemo in rosso i paragrafi che li definiscono. Come abbiamo fatto con questo paragrafo.

Invece quando desideriamo fare una osservazione che scaturisce dal nostro pensiero (a volte, anche noi pensiamo ☺) useremo questo sfondo grigio per incasellare i relativi paragrafi.

Attenzione alle note a piè di pagina. Sono indicate da una numerazione crescente, in apice all'ultimo termine del testo cui fanno riferimento. Come ad esempio il seguente indicatore[4]. Nel caso di espressioni, questa notazione può suscitare confusione. Vi potreste chiedere se il numero è l'indicatore di una nota, o un esponente dell'espressione. Per non parlare di una nota che segue un esponente. Per questo motivo nelle espressioni l'indicatore di una nota è staccato di uno spazio. Come ad esempio in: x^2 [5].

storia del documento

La seguente tabella elenca le versioni di questo documento. Le sue colonne sono organizzare in questo modo:

ver. *versione* del documento;
del *data* del rilascio della versione; formato anno-mese-giorno;
pub. se il documento è stato *pubblicato*;

[4] Questa è una nota.
[5] Questa è una nota che segue un esponente di una espressione.

motivo sintetizza le principali modifiche del documento.

ver.	del	pub.	motivo
0.0	2022-03-09	no	1° cap.: op. tra insiemi
0.1	2022-03-27	si	chg 1° cap. + sez. omomorfismo in 1° cap. + prime 5 sezioni in 2° cap.: gruppi ...
0.2	2022-03-29	si	evidenziati i link chg Intro.→ Presentazione + cap.Intro. questo è il cap.1, gli altri cap. incrementano di 1 completato 3° cap.
0.3	2022-04-04	si	tolto il n.ro al cap. Intro. I capitoli *veri* ora ripartono da 1 Importata nel TOC la presentazione, senza num. Aggiunto un cap. di abbreviazioni, senza num. chg 1° cap. + 3° cap.: spazi vettoriali
0.4	2022-04-16	si	inserito un riassunto finale per ciascuno dei primi 3 capitoli
0.5	2022-05-02	si	resa omogenea la num. di teoremi, osservazioni, etc. + 6 sez. del cap. 4 (Applic. lin. tra spazi vet.)
0.6	2022-05-08	si	chg sezioni *riassumendo* → *ripassando* migliorata la formattazione delle img grandi finito il cap.4
0.7	2022-06-01	si	+ dizionario dei termini e dei sinonimi (embrionale) chg puntualizzato il prodotto per uno scalare chg estesa sez. 4.6 chg estesa sez. 4.10 chg estese le avvertenze + cap. 5 (Autovalori e autovettori di un op. lin.)
0.7.1	2022-06-02	si	chg estesa sez. 5.1

licenza

I termini completi sono riportati, in lingua inglese, in appendice a pag.103.

Per chi non conosce l'inglese, riportiamo qui di seguito la traduzione dei termini riassuntivi. Con l'avvertenza che il testo vincolante è quello in lingua inglese.

Abbreviazioni

voce	significato
|	Nel testo: *o*, *oppure*: in senso alternativo tra i termini a destra e a sinistra del simbolo. Nelle formule indica *tale che*.
Applic.	Applicazione
Cap.	Capitolo
Chg	Cambiamento (Change, in lingua inglese)
CNS | C.n.s.	Condizione Necessaria e Sufficiente
Comb.	Combinazione
Comp.	Componente | componenti
Compl.re	Complementare
Composiz.	Composizione
Def.	Definizione
Dim.	Dimensione
Distrib.	Distribuzione
El.	Elemento
Endom.	Endomorfismo
Equiv.	Equivalenza
Es.	Esempio
Img.	Immagine
Ins.	Insieme
Lin.	Lineare | Lineari
Num.	Numerazione
Op.	Operazione
Propr.	Proprietà
Pub.	Pubblicato
Rel.	Relazione
Risp.	Rispetto
S.gruppo	Sottogruppo
S.insieme	Sottoinsieme
S.spazio	Sottospazio
Sez.	Sezione

voce	**significato**
Sin.	Sinonimo
Sp.	Spazio
SVI	Sistema di Vettori Indipendenti
TOC	Tabella dei contenuti (Table of contents)
Ver.	Versione
Vet.	Vettoriale | Vettoriali
VI	Vettori Indipendenti

Introduzione

Cos'é l'algebra? Citando il relativo articolo su wikipedia l'algebra è una delle branche della matematica[6]: *... è lo studio dei simboli matematici e le regole per manipolarli ... Include di tutto, dalle soluzione delle equazioni elementari, allo studio delle astrazioni, come possono essere i gruppi, gli anelli, i campi. ...*

Quindi, come tutti i concetti di vasta portata, l'algebra è soggetta a diverse interpretazioni in diversi contesti. Parlando di matematica, si può suddividere l'algebra in due campi: l'algebra *elementare* e quella *generale*[7].

L'algebra elementare riguarda i concetti base della matematica: quali le variabili, le espressioni, le equazioni, ... Si comincia a studiare alle scuole superiori, e non si smette più: all'Università, come nella vita ☺.

Qui invece parliamo di algebra astratta. In questo ambito vedremo che è centrale il concetto di *struttura algebrica*, cui arriveremo gradualmente a partire dall'*insiemistica*.

La creazione del concetto di struttura algebrica e del *morfismo*, ad essa collegato, è stato fondamentale nella storia della matematica, perché ha permesso di classificare le entità e le operazioni su di esse in tipologie. E ha dimostrato che è possibile studiare le caratteristiche comuni ad un determinato tipo, cui appartengono più strutture algebriche simili tra loro, invece di perdersi nello studio dettagliato di ogni singola struttura algebrica.

[6] Oltre l'algebra, abbiamo la teoria dei numeri, la geometria e la analisi ... Giusto per citare alcuni dei campi di studio.

[7] O *astratta*.

Capitolo 1

Operazioni tra insiemi

In *algebra generale*, si comincia spesso parlando dei concetti di insiemistica. Questo perché l'uso di questi concetti permette di effettuare ragionamenti logici e di dimostrare teoremi, astraendo completamente dagli oggetti trattati.

1.1 nozioni

Iniziamo con alcune nozioni di base.

Un **elemento** di un insieme, è una nozione primitiva.

Per *elemento* si può intendere qualunque entità, considerata non suddivisibile. Una sorta di *atomo*. E con l'aggettivo *qualunque*, intendiamo proprio qualunque: concetti astratti o oggetti concreti. Ovvero ogni cosa vogliamo poter analizzare secondo le regole logiche che ci daremo nel seguito. Usualmente si indica un elemento con una singola lettera minuscola.

Anche il concetto di **insieme** è una nozione primitiva. È una collezione di *elementi distinti*. Usualmente si indica con una singola lettera maiuscola.

Possiamo identificare un insieme elencando i suoi elementi tra parentesi graffe, come ad es. in: $\{11, 13, 17, 19\}$.

Oppure si può identificare tramite una proprietà. Ad es., la formula: $S = \{x|P(x)\}$ indica che l'insieme S è composto da elementi x per i quali vale la proprietà $P(x)$.

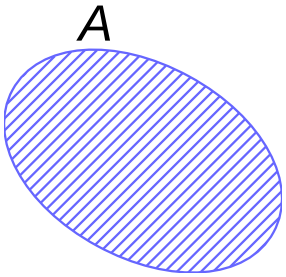


Figura 1.1: Diagramma di Venn: rappresentazione di un insieme.

Definizione 1.1.1. *La **cardinalità** di un insieme A composto da un numero finito si elementi è il numero dei suoi elementi. Si indica con $|A|$.*

Graficamente, spesso si rappresenta un insieme con un diagramma di Venn, ovvero un elissode che racchiude i suoi elementi. Ad esempio, come nella figura 1.1 che rappresenta l'insieme A con un diagramma di Venn.

Il concetto di **appartenenza** indica che un elemento appartiene a un insieme. L'appartenenza dell'elemento a all'insieme A si scrive $a \in A$.

I seguenti insiemi sono così **rilevanti** da essersi guadagnati dei nomi propri:

- i numeri interi *positivi*: P,
- i numeri naturali, ovvero interi *non negativi*: N,
- tutti i numeri interi: $\mathbb{Z}$,
- tutti i numeri razionali: Q,
- tutti i numeri reali: $\mathbb{R}$,
- tutti i numeri complessi: $\mathbb{C}$.

Un altro concetto molto utilizzato è quello di **implicazione** logica. La dizione *implica* indica che se uno o più fatti (*premesse*: p), sono[1] veri, hanno per conseguenza logica la verità di un altro fatto (*conclusione*: q).

La tabella di verità[2] della implicazione logica è indicata nella tabella 1.1.

Tabella 1.1: tabella di verità della implicazione logica

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Nelle formule la implicazione si indica con una freccia: $\Longrightarrow$. Mentre nel linguaggio parlato usiamo le congiunzioni *se ... allora ....* Ad esempio: *"*se *concluderò in tempo la riunione,* allora *parteciperò al seminario"*. In cui:

- la (singola) premessa è *"concluderò in tempo la riunione"*;
- e la conclusione è *"parteciperò al seminario"*.

Il concetto di implicazione

Personalmente non troviamo intuitivo il concetto di implicazione.

Lo ricordiamo pensando che è sempre vero, salvo quando è palesemente falso. E questo avviene quando le sue premesse sono vere e la conclusione invece non lo è.

Se le premesse, una o più, sono false, allora non vi è influenza alcuna riguardo la conclusione. La quale può essere sia vera che falsa. E quest'ultima affermazione ci mette in crisi!

[1] nel caso di più premesse: devono essere tutte vere

[2] Una tabella di verità evidenzia come cambia il valore *Vero* (V o T) e *Falso* (F) assunto da una funzione logica al variare dei valori V/F dei parametri in ingresso

Si può approfondire l'argomento leggendo Symbolic Logic di D. W. Agler [Agler 2013, capitoli: 1.2 Arguments e 5.5.6 Implication]

Se il concetto di implicazione *vale in entrambi i versi*, allora si parla di **coimplicazione** logica. In questo caso ognuno dei due fatti ha per conseguenza logica l'altro fatto. Di conseguenza i due fatti si *equivalgono logicamente*.

Nelle formule la coimplicazione si indica con la doppia freccia: $\iff$. Invece nel linguaggio parlato utilizziamo la frase *... se e solo se ....*

La sua tavola di verità è la tabella 1.2.

Tabella 1.2: tabella di verità della coimplicazione

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Questo concetto è più intuitivo. In questo caso la verità/falsità di una proposizione, afferma anche la verità/falsità dell'altra.

Avremo necessità di esprimere anche i seguenti concetti:

- *per qualunque valore di ...*, lo indichiamo con il simbolo $\forall \ldots$;
- *esiste un ...*, si indica con $\exists \ldots$;
- *... tale che ...*, si indica con $\ldots | \ldots$ (barra verticale).

Altro concetto importante: il *sottoinsieme*.

Definizione 1.1.2. *Si dice* ***sottoinsieme*** *un insieme A che è parte (o tutto) di un insieme B.*

In tal caso si dice che "*A è contenuto in B*", e si scrive $A \subseteq B$.

Definizione 1.1.3. *Nel caso particolare in cui B ha almeno un elemento in più di A, allora A è un* ***sottoinsieme proprio*** *di B.*

Un sottoinsieme proprio si indica con: $A \subset B$.

Vi è un legame tra il concetto di sottoinsieme e quello, che definiremo oltre, di *relazione*. Per ora osserviamo che per i sottoinsiemi valgono le seguenti *proprietà*[3].

$$A \subseteq A \qquad \text{riflessiva} \tag{1.1}$$

$$A \subseteq B \text{ e } B \subseteq C \Rightarrow A \subseteq C \qquad \text{transitiva} \tag{1.2}$$

Definizione 1.1.4. *Si definisce l'insieme* ***vuoto*** *un insieme che non ha elementi.*

[3] Anche il concetto di proprietà sarà approfondito nel prosieguo

Un insieme vuoto si indica con il simbolo $\varnothing$, e si considera sottoinsieme di qualunque insieme.

Consideriamo due insiemi A e B. Se osserviamo che ogni elemento di un insieme appartiene anche all'altro, e viceversa, allora diciamo che esiste una **relazione di uguaglianza** tra i due insiemi.

La relazione di uguaglianza si indica: $A = B$.

Definizione 1.1.5. *Consideriamo la possibilità che un insieme A sia contenuto in B e contemporaneamente B sia contenuto in A. Ciò è possibile se e solo se i due insiemi sono uguali.*

La definizione predetta è spesso usata per dimostrare che due insiemi sono uguali.

La relazione logica 1.3 esprime le affermazioni precedenti:

$$A = B \Leftrightarrow A \subseteq B \text{ e } B \subseteq A \tag{1.3}$$

Definizione 1.1.6. *Dato un insieme A, possiamo considerare l'insieme formato da tutti i suoi possibili sottoinsiemi, incluso lo stesso A e l'insieme vuoto. Tale insieme è detto* ***insieme delle parti****.*

Se A è l'insieme di riferimento, il suo insieme delle parti è indicato con $P(A)$.

Il concetto di *insieme delle parti* ci fa comprendere quanto l'insiemistica sia flessibile e generica. Infatti possiamo utilizzare le nozioni che stiamo definendo per ragionare sull'argomento che stiamo trattando. In altre parole: possiamo ragionare sulla insiemistica utilizzando i concetti di insiemistica.

1.2 operazioni tra insiemi

Dati due (o più) insiemi, è possibile definire delle operazioni tra loro.

Cominciamo con l'*unione* di insiemi.

Definizione 1.2.1. *Si dice* ***unione*** *di due insiemi, l'insieme ottenuto con gli elementi di entrambi*[4]*.*

La unione degli insiemi A e B si scrive $A \cup B$.

La figura 1.2 rappresenta graficamente l'operazione di unione tra i due insiemi A e B.

L'operazione di unione si può generalizzare per più di due insiemi.

[4] Ad esempio:

$A = \{1, 2, 3\}$
$B = \{3, 4, 5\}$
$A \cup B = \{1, 2, 3, 4, 5\}$

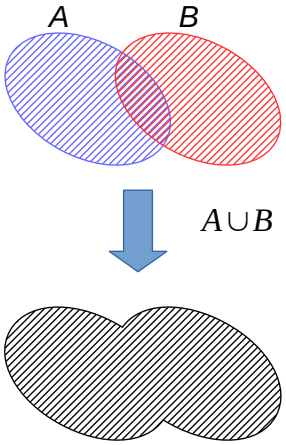


Figura 1.2: Operazione di unione

Definizione 1.2.2. *Si dice* ***intersezione*** *di due insiemi, l'insieme ottenuto con gli elementi* che appartengono ad entrambi[5].

La intersezione degli insiemi A e B si scrive $A \cap B$.

Una rappresentazione grafica della operazione di intersezione tra i due insiemi A e B è riportata in figura 1.3.

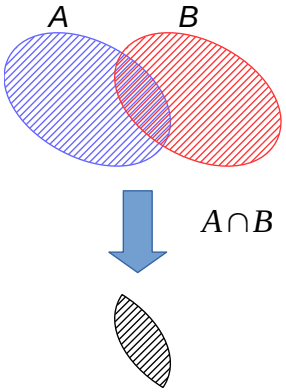


Figura 1.3: Operazione di intersezione

Anche l'intersezione si può generalizzare per più insiemi.

[5]Esempio di intersezione tra due insiemi:

$A = \{1, 2, 3\}$
$B = \{3, 4, 5\}$
$A \cap B = \{3\}$

Usando l'operazione di intersezione, è facile definire due insiemi *disgiunti*, ovvero che non hanno elementi in comune:

Definizione 1.2.3. *due insiemi sono* ***disgiunti*** *se la loro intersezione è l'*insieme vuoto.

Definizione 1.2.4. *Dato un insieme A, si chiama* ***partizione*** *la sua suddivisione in insiemi disgiunti, ovvero che non hanno elementi in comune.*

Dato un insieme A, è possibile effettuarne partizioni diverse. Ad esempio, data la popolazione dell'Italia, possiamo dividerla per anno di nascita. Questa è una sua partizione. Ma potremmo dividerla per sesso. Questa è un'altra possibile sua partizione.

Nell'immagine in figura 1.4, abbiamo partizionato l'insieme A nei sottoinsiemi disgiunti da $C1$ a $C4$.

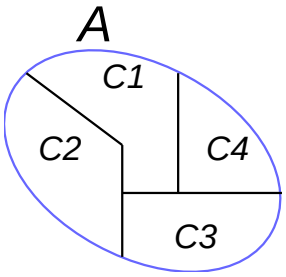


Figura 1.4: Operazione di partizione

Definizione 1.2.5. *Si dice* ***classe*** *un elemento di una partizione come definita in 1.2.4. Ovvero un sottoinsieme di A appartenente a una sua partizione.*

Indovinate un po' per quale motivo nell'immagine 1.4 i nomi dei sottoinsiemi iniziano con la lettera C? Già: ognuno è una classe di A.

Definizione 1.2.6. *Si dice* ***differenza*** *di due insiemi l'insieme ottenuto con gli elementi appartenenti ad A ma* non appartenenti *a B* [6].

La differenza di due insiemi A e B si scrive: $A - B$.

La figura 1.5 rappresenta graficamente l'operazione di differenza tra i due insiemi A e B.

Intuitivamente: unendo gli elementi che appartengono ad entrambi gli insiemi (intersezione), con quelli della differenza, riotteniamo l'insieme originale. Quindi vale sempre: $A = (A \cap B) \cup (A - B)$.

L'immagine 1.6 illustra efficacemente il precedente concetto.

[6] Esempio di differenza tra due insiemi:

$A = \{1, 2, 3\}$

$B = \{3, 4, 5\}$

$A - B = \{1, 2\}$

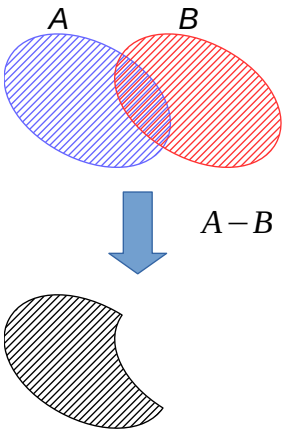


Figura 1.5: Operazione di differenza tra insiemi

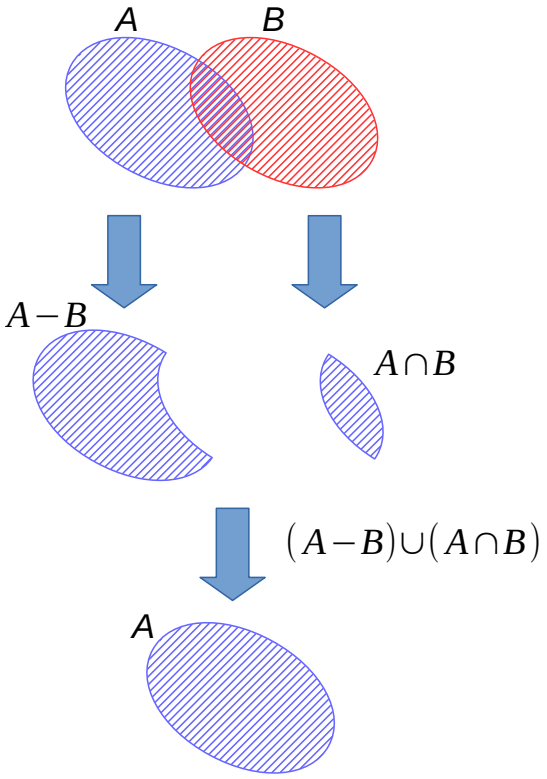


Figura 1.6: Operazione di ricomposizione da differenza e intersezione di insiemi

Nota: per l'operazione di differenza non vale la proprietà commutativa. Ovvero: $A - B \neq B - A$.

Se B è un sottoinsieme di A. *Gli elementi di A non appartenenti a B* formano l'insieme **complementare** di B rispetto A. Si indica con B' e vale $B' = A - B$

Graficamene avremo l'illustrazione 1.7.

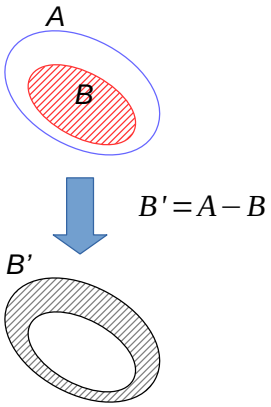


Figura 1.7: Complementare di un insieme

Una proprietà simpatica, consiste nell'osservare che se un insieme ha un complementare, vale anche il viceversa. Ovvero se: *B' è complementare di B* rispetto A, allora *B è complementare di B'* rispetto A.

Continuando a parlare di complementarietà. Se B è sottoinsieme di A, valgono queste proprietà:

- il complementare del complementare è il sottoinsieme iniziale (è l'osservazione precedente); ovvero
$$(B')' = B \tag{1.4}$$
- il complementare dell'insieme A è l'insieme vuoto; ovvero:
$$A' = \varnothing \tag{1.5}$$
- l'intersezione del sottoinsieme con il proprio complementare è l'insieme vuoto:
$$B \cap B' = \varnothing \tag{1.6}$$
- l'unione del sottoinsieme B con il proprio complementare B' è l'insieme A; cioè:
$$B \cup B' = A \tag{1.7}$$

È più complesso intuire le **leggi di Morgan**. Ovvero se B e C sono entrambi sottoinsiemi di A, valgono le seguenti:

$$(B \cap C)' = B' \cup C' \tag{1.8}$$
$$(B \cup C)' = B' \cap C' \tag{1.9}$$

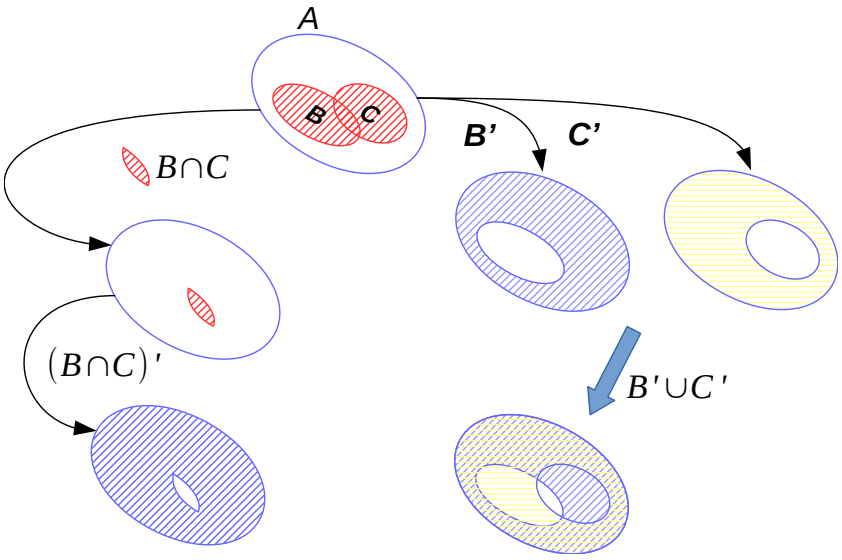


Figura 1.8: Legge di Morgan

La figura 1.8 rappresenta graficamente la uguaglianza 1.8.

A sinistra sono illustrati i due passi (intersezione di B con C, e poi il complemento rispetto A) che formano la parte sinistra dell'uguaglianza.

A destra abbiamo i tre passi della parte destra dell'uguaglianza, ovvero formare i complementi B' e C' e poi farne l'unione.

Confrontanto il risultato a sinistra, con quello a destra, si osserva che le campiture finali coprono le stesse regioni di A.

Come dicevano i prof. dell'università ai miei tempi? Ah, sì: "vi lascio come esercizio la dimostrazione grafica della uguaglianza 1.9 ... ☺".

Definizione 1.2.7. *Dati due insiemi si parla di* ***somma disgiunta***[7] *prendendo gli elementi che appartengono esclusivamente ad un insieme e non quelli che appartengono ad entrambi.*

La somma disgiunta si indica con il simbolo $+$[8].

La somma disgiunta di A e B vale: $A + B = A \cup B - (A \cap B) = (A - B) \cup (B - A)$

La somma disgiunta si può illustrare con la figura 1.9.

1.3 prodotto cartesiano

Il concetto di *prodotto cartesiano* è fondamentale. Permette di passare da una dimensione a più dimensioni.

[7] O **differenza simmetrica**: sono sinonimi.

[8] Oppure con il simbolo Δ.

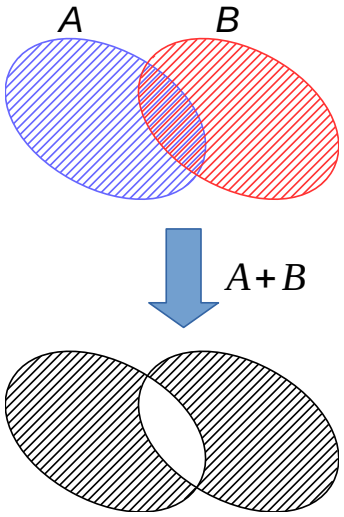


Figura 1.9: Somma disgiunta

Definizione 1.3.1. *Dati due insiemi, A e B. Formiamo le coppie ordinate usando gli elementi di questi insiemi. L'*insieme di queste coppie ordinate *è detto* ***prodotto cartesiano*** *di A per B, e si indica con $A \times B$.*

Questa espressione è così comune, che conviene accettarla e metterla nel nostro bagaglio di conoscenze spicciole.

Una coppia ordinata di elementi di A e B si indica con (a, b). Anche questa è una espressione che dobbiamo essere in grado di usare.

In pratica il prodotto cartesiano è:

$$A \times B = \{(a, b) | a \in A, b \in B\} \tag{1.10}$$

Esempio. Supponiamo di avere un insieme di tre maglie come segue: $A = \{rosso, bianco, verde\}$, e un insieme di modelli: $B = \{Mario, Luca, Fabio\}$. Il loro prodotto cartesiano è l'insieme $A \times B = \{(rosso, Mario), (rosso, Luca),$
$(rosso, Fabio), (bianco, Mario), ...(verde, Luca), (verde, Fabio)\}$, e rappresenta tutte le possibili combinazioni tra maglia e modello.

Facciamo un esempio più ortodosso. Dato l'insieme dei numeri reali: $\mathbb{R}$, il prodotto cartesiano $\mathbb{R} \times \mathbb{R}$ rappresenta le coordinate cartesiane dei punti di un piano rispetto ad una coppia di assi coordinati.

La definizione di prodotto cartesiano si può estendere ad n insiemi. Ad esempio:

$$\mathbb{R}^n = \overbrace{\mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}}^{\text{n-volte}}$$

1.4 relazioni

Affrontiamo ora il concetto di relazione, che ha diverse sfaccettature.

Usiamo il prodotto cartesiano, per indagare la *relazione binaria*.

Definizione 1.4.1. *Dati due insiemi, A e B, formiamo l'insieme delle coppie ordinate dei loro elementi. Si dice che esiste una* ***relazione binaria*** *tra i due insiemi, quando* esiste una proprietà (σ) che è vera per alcune delle coppie.

In pratica questa proprietà σ lega elementi di A con elementi di B. Di conseguenza, data una qualunque coppia (a, b), è possibile affermare una delle seguenti:

- a **é** in relazione con b;
- a **non è** in relazione con b.

Se indichiamo con $\mathcal{R}$ la relazione binaria, si dice che "*l'elemento a è riferito mediante $\mathcal{R}$ all'elemento b*".

È importante notare questo aspetto. Se si prendono tutte le coppie (a, b) per le quali vale "*a é in relazione con b*" otteniamo *sempre* un sottoinsieme S di $A \times B$. Viceversa, dato un qualunque sottoinsieme S del prodotto cartesiano $A \times B$, questo può sempre definire una relazione $\mathcal{R}$ tra gli elementi di A e B.

Definizione 1.4.2. *Per l'osservazione precedente, si definisce una relazione binaria: $\mathcal{R}$ tra A e B come un sottoinsieme S di $A \times B$.*

Una relazione binaria, se $S \subseteq A \times B$, si esprime con:

$$a\mathcal{R}b \Leftrightarrow (a, b) \in S \tag{1.11}$$

Vale la pena sottolineare il fatto che il concetto di relazione binaria è estremamente generale. La figura 1.10 rappresenta graficamente una relazione binaria tra gli insiemi A e B.

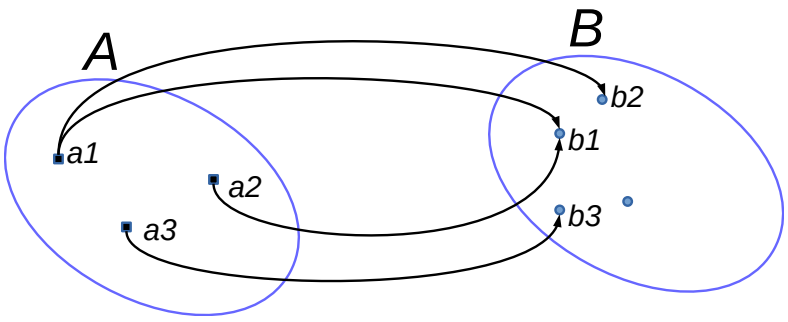


Figura 1.10: Relazione binaria

Le frecce in questa immagine rappresentano la relazione binaria tra gli elementi dei due insiemi. Vale:

$$\begin{aligned}\mathcal{R} = \{&(a1, b1),\\ &(a1, b2),\\ &(a2, b1),\\ &(a3, b3), \}\end{aligned}$$

Vogliamo vedere le capacità di metaragionamento che questi strumenti ci permettono?

Bene. Prendiamo un insieme I i cui elementi sono insiemi. Possiamo formare il prodotto cartesiano con se stesso: $I \times I$ che relaziona gli *insiemi elementi* a due a due.

Per ognuna di queste coppie, possiamo analizzare la rispondenza alla **relazione di inclusione**: se A è un sottoinsieme di B, rimane definita la relazione di inclusione *A è contenuto in B*. Non male, vero? Usare l'insiemistica per ragionare sull'insiemistica.

Definizione 1.4.3. *Ora restringiamo l'attenzione al caso di una relazione binaria tra A e se stesso, ovvero su $A \times A$.*
*In queste condizioni si parla di **relazione di equivalenza** se, per qualunque elemento di A, valgono le seguenti proprietà:*

- riflessiva*: un elemento equivale a se stesso;*
- simmetrica*: se un elemento a equivale a b, allora b equivale ad a;*
- transitiva*: se a equivale a b e b equivale a c allora a equivale a c.*

Una relazione di equivalenza si indica con $\sim$. Le precedenti, formalmente, si scrivono:

$$a \sim a \qquad \text{riflessiva} \tag{1.12}$$
$$a \sim b \implies b \sim a \qquad \text{simmetrica} \tag{1.13}$$
$$a \sim b, b \sim c \implies a \sim c \qquad \text{transitiva} \tag{1.14}$$

Esempio: supponiamo di avere l'insieme dei prodotti disponibili in un grande magazzino di vestiario. Una analisi dei prodotti per *tipologia* (ovvero: maglione, piuttosto che camicia, piuttosto che pantalone, ...) definisce una classe di equivalenza. Se cerco unicamente una camicia, senza preferenze di colore, taglia, ..., valgono le proprietà riflessiva (una camicia con serial number 12345678 equivale a se stessa), simmetrica (se la camicia con sn 12345678 equivale a quella con sn 12345679 vale anche il viceversa) e transitiva ...

Ed ora l'esempio ortodosso. Dato l'insieme delle rette in un piano, considerando parallele anche due rette coincidenti, la relazione di parallelismo è una relazione di equivalenza.

Ma non finisce qui. Tenetevi forte, perché possiamo definire

Definizione 1.4.4. *una **relazione d'ordine** sugli elementi di $A \times A$. È una relazione binaria per la quale valgono le proprietà:*

- *riflessiva, la conosciamo: a precede (in senso lato) se stesso;*
- antisimmetrica*, ovvero se a precede b e b precede a, deduciamo che a è uquale a b;*

- *transitiva, come per la relazione d'equivalenza.*

Formalmente, le proprietà predette si esprimono così:

$$a\mathcal{R}a \qquad \text{riflessiva} \tag{1.15}$$
$$a\mathcal{R}b, b\mathcal{R}a \Rightarrow a = b \qquad \text{antisimmetrica} \tag{1.16}$$
$$a\mathcal{R}b, b\mathcal{R}c \Rightarrow a\mathcal{R}c \qquad \text{transitiva} \tag{1.17}$$

Abbiamo già usato la terminologia *a precede b*, e si scrive: $a \prec b$.
Esiste anche la relazione inversa: $a \succ b$: *a segue b*.

Definizione 1.4.5. *Dato un insieme A, e una relazione di equivalenza in essa, possiamo prendere un suo elemento a e considerare tutti gli altri elementi presenti nell'insieme, per i quali vale la relazione di equivalenza predetta.*

L'insieme formato da a e dai sui equivalenti é la ***classe di equivalenza*** *dell'elemento a di A. La classe di equivalenza dell'elemento a si indica con* $[a]$.

Quindi vale: $[a] = \{x \in A | x \sim a\}$.
Nell'esempio del magazzino di vestiario, se consideriamo la relazione di equivalenza per *tipologia di vestiario*, tutte le camicie del magazzino formano la classe di equivalenza della camicia.
Nell'esempio delle rette parallele, data una retta, la sua classe di equivalenza individua una *direzione*.
Il concetto di classe di equivalenza è importante, perché può essere usato per decomporre un insieme in una partizione. A questo riguardo esiste un teorema[9] che afferma proprio questo concetto:

Teorema 1.4.6. *Le classi distinte di equivalenza individuate da una relazione di equivalenza definita in un insieme A vi determinano una partizione.*
Viceversa, data una partizione dell'insieme A, si può definire una relazione di equivalenza in A rispetto la quale gli elementi della partizione sono classi distinte di equivalenza.

Riprendendo l'esempio del magazzino. Se considero tutti i diversi tipi di vestiario (camicia, pantalone, gonna, giacca, ...), le relative classi di equivalenza mi suddividono il magazzino in sottoinsiemi disgiunti, che lo comprendono interamente: partizionano il magazzino.
Si noti che la seconda parte del teorema afferma anche l'inverso: data una partizione posso definire la relazione di equivalenza che la genera.

1.5 insieme quoziente

Definita la classe di equivalenza, è possibile concettualizzare l'*insieme quoziente*.

[9] per la dimostrazione, si veda ad es. [Gasparini 1977, sezione I.5]

Dato l'insieme A, e una relazione $\sim$ di equivalenza in esso, consideriamo l'insieme i cui elementi sono le classi di equivalenza definite dalla relazione predetta.

Questo insieme è detto **insieme quoziente** di A rispetto a $\sim$. E si indica con $A/\sim$.

Per quanto indicato dal teorema 1.4.6, l'insieme quoziente *è una partizione di* A; ovvero una sua suddivisione in sottoinsiemi disgiunti due a due.

Insieme quoziente

Perché parliamo di quoziente? Prendiamo la solita cassetta con 100 mele, e organizziamo le mele in classi equivalenti: le trentine con le trentine, le gialle con le gialle e le rosse con le rosse .... Supponiamo che ogni gruppo di mele sia formata da 5 elementi[a]: abbiamo diviso la cassetta 20 gruppi uguali di 5 mele (equivalenti) ciascuno. La cassetta è l'insieme A. Ogni gruppo di 5 mele è una diversa classe di equivalenza. I 20 gruppi sono il quoziente, ottenuto dividendo 100 per 5. Quindi abbiamo partizionato la cassetta in 20 insiemi tra loro disgiunti, formati ciascuno da 5 mele.

[a] Stiamo stiracchiando l'analogia, per poter applicare il concetto di divisione. Nella realtà non è detto che ogni classe sia formata esattamente da cinque elementi, ma concediamoci questa licenza poetica per amore della semplicità ... e per far tornare il discorso.

1.6 applicazioni

Chi conosce il concetto di funzione, qui si troverà a proprio agio. Infatti, *applicazione* e *funzione* sono sinonimi.

Per capire il loro uso nell'insiemistica consideriamo la seguente:

Definizione 1.6.1. *Dati due insiemi A e B. Una* ***applicazione*** *è una legge che ad un elemento di A associa un* unico *elemento di B.*

Come, ad esempio, la figura 1.11

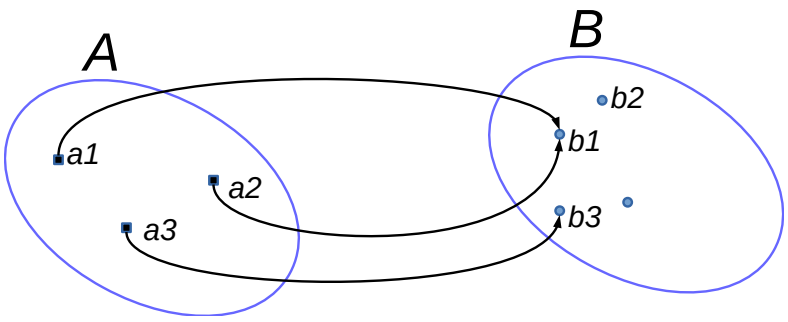


Figura 1.11: Applicazione: rappresentazione con diagrammi di Venn

Se questo concetto vi suona familiare, non stupitevi. Provate a fare un confronto con il concetto di relazione binaria. La differenza fondamentale è data dalle paroline "*unico elemento di B*". Nella relazione binaria non vi è questa limitazione.

Questo concetto è importante, ed è del tutto analogo a quello di funzione per i numeri reali, che possiamo osservare nell'esempio 1.12.

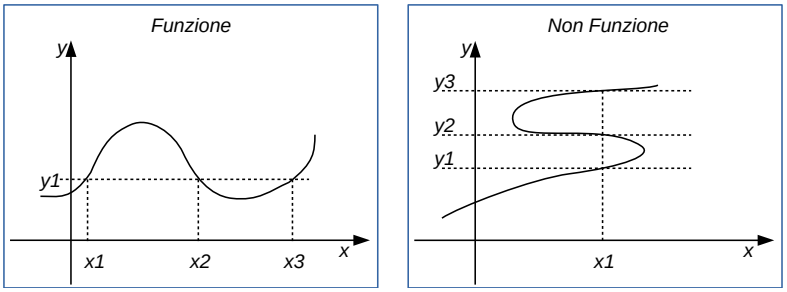


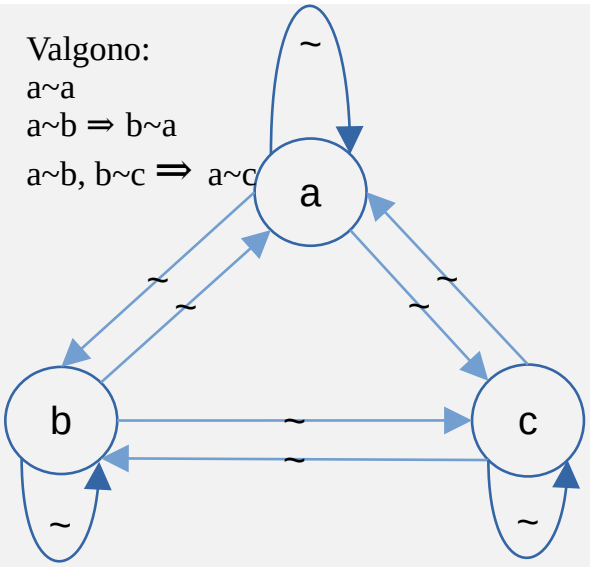
Figura 1.12: Sx: Applicazione. Dx: Funzione binaria

Nel riquadro a destra la curva traccia una relazione tra la variabile indipendente x e la variabile dipendente y. Ma *non è una funzione* perché vi sono valori di x cui corrispondono più valori di y. Ad esempio al valore $x1$ corrispondono tre valori di y: $y1$, $y2$ e $y3$.

Invece nel riquadro a sinistra, la curva è una funzione, in quanto ad un singolo valore di x corrisponde al più un valore di y.

Tanto per dissertare, osserviamo che la relazione di equivalenza *non è* una applicazione. Infatti in quel caso si richiede solo che valgano le proprietà riflessiva, simmetrica e transitiva. Non si richiede che l'elemento target sia unico per un dato elemento di partenza.

Ad esempio, consideriamo l'insieme rappresentato nella seguente figura.



Valgono le proprietà che definiscono la relazione di equivalenza. Ma non vi è unicità del target, perché, ad esempio, vale $a \sim b$, ma anche $a \sim c$.

Fatta la presentazione, qui vi è un po' di terminologia da tenere presente.

Per cominciare, l'insieme di partenza, è detto **dominio**, quello di arrivo è il **codominio**.

Se l'applicazione é f, e l'elemento di partenza é a, l'elemento di arrivo è detto ***valore*** *di* f *in* a, e si indica con $f(a)$.

Il grafico 1.13 indica i termini predetti

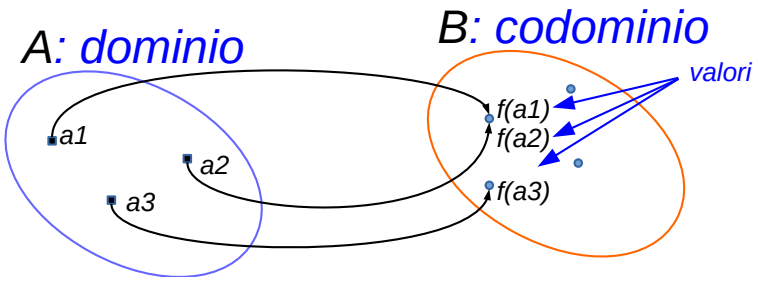


Figura 1.13: Applicazione: terminologia

Formalmente la funzione si indica come $f : A \to B$. O anche come segue per indicare la legge che lega a con b:

$$\begin{aligned} f \ &: A \to B \\ &a \mapsto b \end{aligned}$$

Ad esempio, da numero reale a numero reale, cambiare segno a un numero del dominio, è la funzione $\ldots (-1, 1) \ldots (1, -1) \ldots (1.5, -1.5) \ldots$; e si indica:

$$f : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto -x$$

Definizione 1.6.2. *L'insieme dei valori assunti da f al variare di $a \in A$ è detto* **immagine** di f.

L'immagine di f si indica con $Im(f)$, oppure $f(A)$. Si noti che nelle parentesi di f, qui indichiamo l'intero dominio, non il singolo elemento.

Nella figura 1.13, l'immagine della funzione è l'insieme
$Im(f) = \{f(a1), f(a2), f(a3)\}$.

Definizione 1.6.3. *Una applicazione è* ***suriettiva*** *se la funzione ricopre tutto il codominio. Ovvero se* ogni *elemento di B è immagine di* almeno *un elemento di A. In questo caso si dice che abbiamo* una applicazione f di A sopra B.

Nella figura 1.13 l'applicazione *non é* suriettiva perché vi sono due elementi di B che non sono in relazione con alcun elemento di A. Se B non avesse questi due elementi, allora l'applicazione illustrata sarebbe suriettiva.

Definizione 1.6.4. *Una applicazione è* ***iniettiva*** *se elementi distinti del dominio, hanno immagini distinte. Ovvero se un elemento b del codominio é riferito da* un solo *elemento A del dominio.*

Nella figura 1.13 l'applicazione *non é* iniettiva perché il valore $f(a1)$, oltre che da $a1$ è riferito anche dall'elemento $a2$. Se l'elemento $a2$ non facesse riferimento al valore $f(a1)$, allora l'applicazione sarebbe iniettiva.

Definizione 1.6.5. *Si parla di applicazione* ***biiettiva*** *se è sia suriettiva che iniettiva.*

In tal caso non solo vi è una relazione uno a uno tra un elemento a e il suo corrispondente b. Inoltre la funzione copre completamente il codominio.

Una applicazione biiettiva si indica come $f : A \leftrightarrow B$.

La figura 1.14 illustra un esempio di funzione biiettiva.

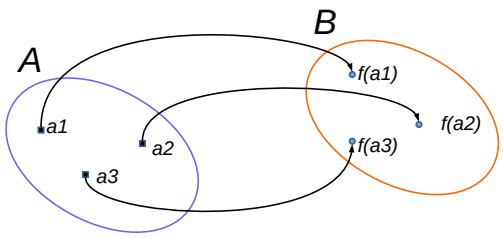


Figura 1.14: Applicazione biiettiva

E se volessimo invertire il concetto dell'applicazione, muovendoci dal codominio al dominio? Bene, facciamolo.

Definizione 1.6.6. *Data la funzione f da A a B, possiamo considerare l'elemento $b = f(a)$. Per l'elemento b possiamo avere la sua* immagine reciproca *considerando gli elementi a che lo riferiscono*[10] .

L'immagine reciproca di b si indica con $f^{-1}(b)$, e viene chiamata "***fibra** di f su b*".

Se l'applicazione é una applicazione suriettiva (definizione 1.6.3), tutti gli elementi del codominio sono raggiunti dall'applicazione. Quindi ogni elemento del codominio ha una sua fibra.

Se la funzione é una applicazione biiettiva (definizione 1.6.5), ogni elemento del codominio è raggiungibile dall'applicazione tramite un solo elemento del dominio. In questa condizione la fibra di ogni elemento del codominio è formata da un solo elemento del dominio.

Definizione 1.6.7. *Nel caso di una applicazione biiettiva (definizione 1.6.5) f tra dominio A e codominio B, comunque prendiamo un elemento $b \in B$, avremo sempre uno e un solo elemento a da cui raggiungerlo. Perciò possiamo definire una applicazione che leghi b con a. Questa è detta applicazione **inversa**.*

Una applicazione inversa si indica con f^{-1}, e si definisce:

$$\begin{aligned} f^{-1} : B &\to A \\ b &\mapsto a \end{aligned}$$

Teorema 1.6.8. *Si dimostra che l'immagine reciproca della unione di due insiemi è uguale alla unione delle loro immagini. Analogamente per l'operazione di intersezione.*

Formalmente, dati due insiemi M e N:

$$\begin{aligned} f^{-1}(M \cup N) &= f^{-1}(M) \cup f^{-1}(N) \\ f^{-1}(M \cap N) &= f^{-1}(M) \cap f^{-1}(N) \end{aligned}$$

Teorema 1.6.9. *Inoltre, si dimostra che l'immagine della unione di due insiemi è uguale alla unione delle loro immagini. Questa proprietà,* non vale *per l'operazione di intersezione.*

Formalmente, dati due insiemi M e N:

$$\begin{aligned} f(M \cup N) &= f(M) \cup f(N) \\ f(M \cap N) &\neq f(M) \cap f(N) \end{aligned}$$

Definizione 1.6.10. *È possibile definire una applicazione da A verso B, considerando l'insieme delle sue coppie ordinate (a, b), che formano un sottoinsieme M di $A \times B$, a patto che ad un valore di a corrisponda un unico valore di b. In tal caso M è il **grafico** della funzione, e tale grafico definisce la funzione stessa.*

[10] Attenzione al plurale. In generale è possibile che un elemento b sia riferito da più elementi di A.

1.7 composizione di applicazioni

Definizione 1.7.1. *Supponiamo di avere due applicazioni. La prima, f, dall'insieme A all'insieme B. E la seconda, g, dall'insieme B all'insieme C. Inoltre, supponiamo che il dominio di g in B contenga l'immagine di f. In queste condizioni, dato un elemento a, possiamo pensare di applicare in sequenza prima f, e sul relativo valore $f(a)$, applicare g ottenendo un valore finale $g(f(a))$ che sarà un elemento dell'insieme C. Ovvero:*

$$c = a \circ b \tag{1.18}$$

*Questo giochetto si chiama "*applicazione **composta** di f con g*". E nulla ci impedisce di immaginarla come una applicazione da A a C.*

Formalmente una applicazione composta di f con g si indica con: $g \circ f$ [11] .

La 1.18 nel linguaggio parlato si legge: "*c è il composto di a e b mediante* $\circ$". O, più semplicemente: "*c è il prodotto di a per b.* La dizione applicazione **prodotto** è un sinonimo di applicazione composta.

Vale:

$$\begin{aligned} g \circ f \ &: A \to C \\ &x \mapsto g(f(a)) \quad \forall a \in A \end{aligned}$$

Da un punto di vista grafico, una applicazione composta può essere rappresentata come in 1.15.

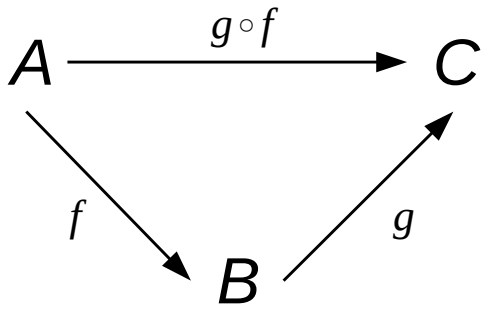


Figura 1.15: Applicazione composta

Per le applicazioni composte, date $f : A \to B$, $g : B \to C$, $h : A \to C$ si dimostrano le seguenti proprietà:

- associativa; ovvero $(h \circ g) \circ f = h \circ (g \circ f)$;
- esistono le applicazioni **identiche**[12] ; l'applicazione identica non modifica il valore di qualunque altra applicazione; ovvero:

[11] Notare la sequenza delle lettere. A differenza della locuzione nel linguaggio parlato, in cui l'ordine è invertito.

[12] Per applicazione identica si intende una applicazione che restituisce il suo elemento in ingresso: $I_A(a) = a$.

$f \circ I_A = I_B \circ f = f$; infatti $(f \circ I_A)(a) = f(I_A(a)) = f(a) \quad a \in A$; e $(I_B \circ f)(a) = I_B(f(a)) = f(a)$;

Inoltre si dimostra:

- l'applicazione composta di due applicazioni iniettive, è iniettiva;
- l'applicazione composta di due applicazioni suriettive, è suriettiva.

1.8 insiemi equipotenti

Definizione 1.8.1. *Due insiemi si dicono* ***equipotenti*** *se è possibile definire una applicazione biiettiva tra loro.*

Definizione 1.8.2. *Come caso particolare di equipotenza, se si può definire una applicazione biiettiva tra un insieme A e quello dei numeri naturali N, allora si dice che A è* ***numerabile****.*

1.9 partizione di un insieme e applicazioni

Esiste un rapporto tra il concetto di applicazioni e quello di partizione (teorema 1.4.6).

Prima di inoltrarci nel tecnicismo, parliamone in generale. E facciamolo con l'aiuto della figura 1.16.

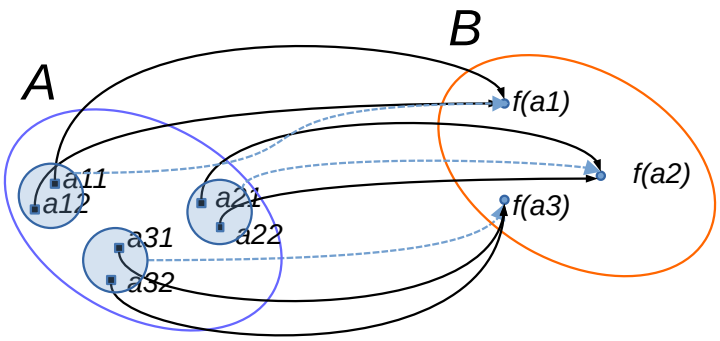


Figura 1.16: Descrizione di un diagramma commutativo

In questa figura, le frecce nere rappresentano una applicazione dal dominio A al codominio B. Vediamo che l'applicazione è suriettiva[13] ma *non* iniettiva[14].

In queste condizioni, raggruppiamo gli elementi del dominio che puntano allo stesso elemento del codominio. Ad esempio $C1 = \{a11, a12\}$ che puntano a $f(a1)$. Mentre $C2 = \{a21, a22\}$ perché puntano a $f(a2)$ e così via. Questo lo possiamo fare con una relazione di equivalenza: $a11 \sim a12$, $a21 \sim a22$ ....

[13] Tutti gli elementi del codominio vengono raggiunti.

[14] Più elementi dal dominio puntano ad uno stesso elemento del codominio.

A questo punto possiamo partire dalle classi di equivalenza $C1, C2, C3$ per arrivare agli elementi del codominio: $(C1, f(a1)), (C2, f(a2)), (C3, f(a3))$. Sono le frecce tratteggiate in figura 1.16: questa è una applicazione suriettiva e iniettiva. Partendo da una applicazione generica, usando un opportuno partizionamento del dominio, possiamo generare una applicazione suriettiva e iniettiva.

Vediamo qui di seguito quanto abbiamo detto con un maggiore dettaglio tecnico.

1. data una applicazione f di A in B;
2. definiamo equivalenti gli elementi del dominio di f che portano allo stesso elemento di codominio; indichiamo con $\sim$ questa equivalenza;
3. in questo modo abbiamo creato una partizione di A formata dalle classi di equivalenza definite al punto precedente, l'insieme di queste classi di equivalenza è un insieme quoziente (sezione 1.5); lo indichiamo con $A/\sim$; possiamo pensare di avere una applicazione (la indichiamo con π) che mette in relazione un qualsiasi elemento del dominio di f (ovvero A) con la classe di equivalenza (definizione 1.4.5) cui appartiene, e quindi il suo codominio è $A/\sim$;
   Formalmente, l'applicazione π si definisce con:

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

4. a questo punto possiamo chiudere il giro, e pensare di avere una applicazione di $A/\sim$ in B; ovvero legare una classe di equivalenza di A con il relativo elemento in B; indichiamo questa applicazione come $f/\sim$.

I punti predetti si sintetizzano con il diagramma commutativo di applicazioni 1.17.

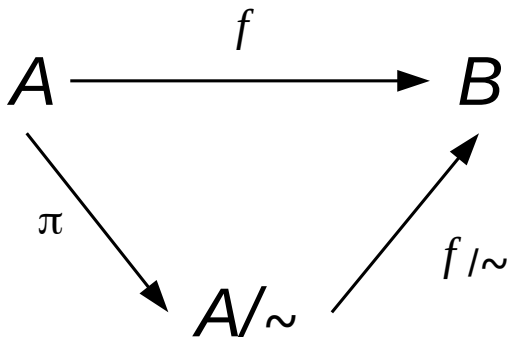


Figura 1.17: Diagramma commutativo di applicazioni

Nel diagramma 1.17 osserviamo: l'applicazione π che lega gli elementi del dominio di f agli elementi dell'insieme quoziente $A/\sim$, e l'applicazione $f/\sim$ che lega gli elementi dell'insieme quoziente al codominio di f.

Quindi l'uso opportuno della relazione di equivalenza $\sim$ permette la definizione di una funzione $f/\sim$ che è sicuramente iniettiva tra insieme quoziente $A/\sim$ e B.

Inoltre se f è suriettiva in B, allora $f/\sim$ è biiettiva.

Si può anche ragionare rispetto una equivalenza definita a priori. Se abbiamo una equivalenza (indicata con $\sim$) su un insieme A, possiamo dire che una applicazione $f : A \to B$ è **ben definita sullo spazio quoziente** se vale il diagramma commutativo precedentemente mostrato.

Formalmente, l'applicazione $f : A \to B$ è ben definita sullo spazio quoziente se:

$$a_1 \sim a_2 \in A/\sim \quad \Longrightarrow \quad f(a_1) = f(a_2)$$

Un'ultima osservazione. Il diagramma commutativo che abbiamo visto ci suggerisce un'altra possibile interpretazione: la funzione $f : A \to B$ può essere vista come una funzione composta di π con $f/\sim$.

Per chiudere questa sezione, facciamo un esempio di quelli seri.

Esempio 1.9.1. Prendiamo lo spazio euclideo in tre dimensioni e fissiamo in esso un piano bidimensionale (nominiamolo α).

Come applicazione prendiamo una proiezione dello spazio su α secondo una certa direzione non parallela al piano. Nominiamo π questa applicazione.

π è una applicazione suriettiva dello spazio euclideo su α (copre tutto il piano), ma non è iniettiva perché ogni punto dello spazio appartenente ad una retta secondo la direzione di proiezione individua lo stesso punto di proiezione sul piano.

Se nello spazio noi definiamo equivalenti due punti che danno la stessa proiezione su α, allora tramite π abbiamo definito una biiezione tra l'insieme quoziente e α.

1.10 trasformazioni di un insieme

Vediamo un esempio importante di uso dei concetti di insiemistica.

Definizione 1.10.1. *Chiamiamo* ***trasformazione*** *le* applicazioni biiettive *(definizione 1.6.5) di A in sè.*

In generale saranno possibili più trasformazioni di A. Ognuna di queste può essere considerata un elemento di un nuovo insieme. Tutte le possibili trasformazioni di A formeranno un insieme: l'insieme **delle trasformazioni di** A, che indichiamo con $T(A)$. Nel seguito con ρ, σ, τ indichiamo elementi di $T(A)$.

Queste trasformazioni sono applicazioni. Quindi esiste la possibilità di comporle formando una applicazione composta.

Si dimostra che esistono le seguenti proprietà:

- date due qualunque trasformazioni di A, la loro composizione è ancora una trasformazione di A ;
  Questa proprietà si esprime anche dicendo che l'insieme delle trasformazioni $T(A)$ è *chiuso* rispetto l'applicazione composta $\rho \circ \sigma$. Ovvero:

$$(\rho \circ \sigma) \in T(A) \quad \forall \rho, \sigma \in T(A) \tag{1.19}$$

- nel comporre le trasformazioni, vale la proprietà associativa; cioè:

$$(\rho \circ \sigma) \circ \tau = \rho \circ (\sigma \circ \tau) \quad \forall \rho, \sigma, \tau \in T(A) \tag{1.20}$$

- esiste una particolare trasformazione, detta *identità*, che può comporre una qualunque altra trasformazione senza alterarla; detta i la trasformazione identità, possiamo scrivere:

$$i \circ \rho = \rho \circ i = \rho \quad \forall \rho \in T(A) \tag{1.21}$$

- ogni trasformazione $\rho \in A$ ha una sua inversa ρ^{-1}; se si compone l'inversa con la trasformazione in analisi, si ottiene la trasformazione identità; abbiamo:

$$\rho^{-1} \circ \rho = \rho \circ \rho^{-1} = i \quad \forall \rho \in T(A) \tag{1.22}$$

Facciamo un paio di premesse che saranno approfondite in seguito.

Quando abbiamo un insieme e delle operazioni su di esso, diciamo di avere definito una **struttura algebrica** di un insieme.

Inoltre quando abbiamo una struttura algebrica con le proprietà su indicate, la nominiamo struttura di **gruppo**.

Quindi l'insieme $T(A)$ e la legge di composizione precedentemente vista è un esempio di struttura di gruppo.

1.11 leggi di composizione

Ora consideriamo diversi possibili modi di comporre applicazioni.

Facciamo un salto indietro, e dimentichiamo temporaneamente il concetto di applicazione.

Definizione 1.11.1. *Prendiamo un insieme A. Supponiamo sia possibile legare a delle coppie di elementi di A un terzo elemento, sempre appartenente ad A. In questo caso si dice di avere una* ***legge di composizione interna****.*

Se a, b e c sono i tre elementi predetti, si dice che "*c è il prodotto di a per b*".

Attenzione a non interpretare la precedente frase alla lettera. Una legge di composizione non deve essere necessariamente un *prodotto* in senso letterale. Piuttosto, è un concetto di operazione binaria del tutto generica.

Formalmente una legge di composizione si indica con il simbolo $\circ$, che rappresenta una operazione generica: $c = a \circ b$.

Essendo una operazione generica, spesso la legge di composizione è indicata con un simbolo più specifico, relativo alla particolare operazione considerata. O, addirittura, si può non indicare, dandolo per sottinteso.

L'insieme A, munito della legge di composizione, si indica con la coppia ordinata $(A, \circ)$. Come già indicato nella precedente sezione, questa è detta struttura algebrica.

Adesso ricordiamo la definizione di applicazione. Utilizzandola per analizzare il concetto di *legge di composizione*, possiamo anche dire che:

Definizione 1.11.2. *una* legge di composizione interna *è una applicazione definita su $A \times A$, o un suo sottinsieme, con valori in A.*

Esempio 1.11.3. L'operazione di *addizione* nell'insieme dei numeri naturali è una legge di composizione. Questa legge è definita per qualunque coppia di numeri naturali.

Esempio 1.11.4. Altro esempio: l'operazione di *sottrazione* nell'insieme dei numeri naturali, In questo caso l'operazione è definita solo se il minuendo è maggiore o uguale del sottraendo.

Quando si definisce una legge di composizione su un insieme A, varranno (o non varranno) determinate proprietà.

Le diverse strutture algebriche sono classificate secondo le proprietà soddisfatte dalla relativa legge di composizione.

Le proprietà da considerare sono le seguenti.

1. Proprietà **associativa**. Vale se, dati tre elementi composti tra loro, non è influente la precedenza con cui si esegue la prima composizione rispetto la seconda.

   Definizione 1.11.5. *Ovvero:*

   $$(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a, b, c \in A$$

   Un insieme non vuoto tra i cui elementi sia definita una legge di composizione che gode della proprietà associativa si dice **semigruppo**.
2. Proprietà **commutativa**. Vale se, dati due elementi, l'ordine di composizione è ininfluente.

   Definizione 1.11.6. *Ovvero:*

   $$a \circ b = b \circ a \quad \forall a, b \in A$$

   Di solito una legge di composizione commutativa si indica con il simbolo $+$.
3. Esistenza di un **elemento neutro**. Quando esiste un elemento che composto con qualunque altro elemento restituisce sempre l'altro elemento. In questo ambito deve valere la legge commutativa.

   Definizione 1.11.7. *Ovvero, detto e l'elemento neutro, vale:*

   $$e \circ a = a \circ e = a$$

   Ad esempio, lo *zero* è l'elemento neutro per l'operazione di addizione nell'insieme dei numeri naturali. Mentre l'*uno* è l'elemento neutro per la legge di composizione di moltiplicazione, sempre nell'insieme dei naturali.
   Si noti che non è detto che l'elemento neutro debba esistere. Ad esempio si prenda l'insieme dei numeri naturali pari. E come legge di composizione si consideri la moltiplicazione. In questo caso l'elemento neutro *non esiste*.
   Mentre si può dimostrare che se esiste un elemento neutro, questo è unico.

4. Esistenza di **elementi simmetrici**. Se esiste l'elemento neutro per una legge di composizione, dato un elemento a, si dice che ha un elemento simmetrico a' se la loro composizione rende l'elemento neutro.

   Definizione 1.11.8. *Cioè*
   $$a \circ a' = a' \circ a = e$$

   Se esiste il simmetrico di un elemento, non è detto sia unico. A meno che la legge di composizione sia associativa, in tal caso si dimostra l'univocità del simmetrico.

Quando su un insieme esistono più leggi di composizione, allora si possono avere dei rapporti tra queste leggi. Ad esempio si pensi alla *proprietà distributiva* della moltiplicazione rispetto l'addizione nell'insieme dei numeri reali.

Definizione 1.11.9. *Se si considerano due diversi insiemi A e B, è possibile considerare una legge di composizione tra elementi del prodotto cartesiano $B \times A$ verso un elemento di A. In questo caso si parla di* ***legge di composizione esterna****.*

Un esempio di composizione esterna è il prodotto di uno scalare k appartenente all'insieme dei numeri reali, per un vettore $\overrightarrow{v}$. Questo prodotto rende un nuovo vettore, che ha la stessa direzione di $\overrightarrow{v}$, un modulo pari a $|k|$ volte il modulo di $\overrightarrow{v}$, e un verso uguale a quello di $\overrightarrow{v}$ se $k > 0$, oppure opposto se $k < 0$

1.12 struttura algebrica

Come ci siamo detti: un insieme e una legge di composizione sui suoi elementi definisce quella che chiamiamo una *struttura algebrica*.

Uno stesso insieme può avere diverse strutture algebriche: dipende da quale (o quali: può essere più di una) legge di composizione stiamo considerando.

Ad esempio, prendiamo i numeri reali. Se la legge di composizione è l'addizione, allora avremo una struttura di *gruppo*. Se sullo stesso insieme consideriamo le leggi di moltiplicazione e addizione, allora abbiamo una struttura di *campo*.

Ora facciamo una considerazione interessante. Se abbiamo insiemi diversi, su cui sono definite leggi di composizione (ovvero: *operazioni*) con le stesse proprietà, allora "*tutti i teoremi basati su queste proprietà rimangono validi per ciascuno degli insiemi in questione*".

Ora consideriamo l'insieme U e quello delle sue parti $P(U)$ con le relative operazioni di unione, intersezione e complemento: $(P(U), \cup, \cap, ')$. Si dimostra che $\forall A, B, C \in P(U)$ valgono le seguenti proprietà:

$$A \cup B = B \cup A \tag{1.23}$$
$$A \cap B = B \cap A \tag{1.24}$$
$$A \cup \varnothing = A \tag{1.25}$$
$$A \cap U = A \tag{1.26}$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{1.27}$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{1.28}$$
$$A \cap A' = \varnothing \tag{1.29}$$
$$A \cup A' = U \tag{1.30}$$

Cioè le stesse proprietà delle operazioni su U. I teoremi per U valgono anche per $P(U)$.

Se si considera un nuovo insieme, formato da due elementi $I = \{0, 1\}$, e tre operazioni *or*, *and*, *not* definite come segue:

- *or*

$+$	0	1
0	0	1
1	1	1

- *and*

$\circ$	0	1
0	0	0
1	0	1

- *not*

$'$	
0	1
1	0

si dimostra che per questa struttura algebrica, detta **algebra di Boole**, valgono le stesse proprietà della struttura algebrica $(P(U), \cup, \cap, ')$.

La considerazione precedente è importante sia perchè, in base ad essa, basta dimostrare un teorema in un contesto per ritenerlo poi valido in tutti i contesti con la stessa struttura algebrica, ottenendo una notevole economia di pensiero. Sia perché può mettere in evidenza fatti essenziali da cui dipendono vari teoremi.

1.13 omomorfismo, isomorfismo

Affrontiamo ora un concetto più articolato: omomorfismo di una applicazione tra insiemi.

Definizione 1.13.1. *Dato l'insieme E dotato della legge di composizione $\circ$; e l'insieme E' dotato della legge di composizione $\square$; una applicazione Φ tra E ed E' è un* ***omomorfismo*** *relativamente alle leggi predette quando vale:*

$$\Phi(x \circ y) = \Phi(x) \square \Phi(y) \quad \forall x, y \in E \tag{1.31}$$

La figura 1.18 ci aiuta ad analizzare la definizione. L'insieme E (colore grigio-blu) ha la legge di composizione $\circ$ (freccia continua blu) che rende $z = x \circ y \quad \forall x, y \in E$. Mentre l'applicazione Φ (frecce tratteggiate) proietta gli elementi di E su E' (colore rosso).

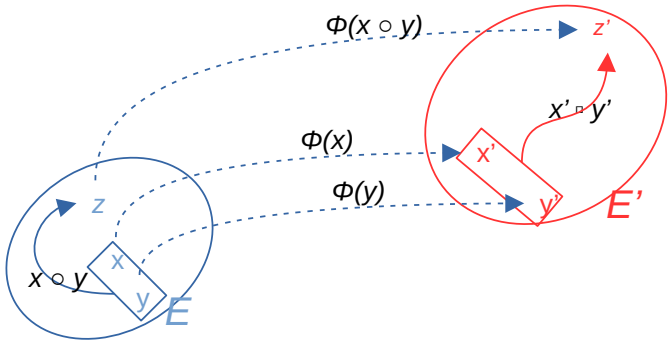


Figura 1.18: Omomorfismo di una applicazione tra insiemi

La figura permette di apprezzare l'equazione 1.31 che lega gli operatori di composizione dei due diversi insiemi affermando che possiamo arrivare all'elemento $z' \in E'$:

- sia usando l'applicazione Φ dall'elemento $z = x \circ y$;
- sia utilizzando l'operatore $\square$ di E' con $z' = x' \square y'$, dove x' e y' sono ottenuti utilizzando $x' = \Phi(x)$ e $y' = \Phi(y)$.

Notiamo che gli insiemi E ed E' possono coincidere. Ad esempio:

Esempio 1.13.2. con l'insieme dei numeri naturali N, legge di composizione la somma $(+)$ e $\Phi(n) = 3 \cdot n \quad \forall n \in N$, l'applicazione Φ è un omomorfismo perché:

$$\Phi(a + b) = 3 \cdot (a + b) = 3 \cdot a + 3 \cdot b = \Phi(a) + \Phi(b)$$

L'importanza del concetto di omomorfismo è dovuta al fatto che si dimostrano le seguenti.

Proposizione 1.13.3. Se Φ è un omomorfismo di $(E, \circ)$ in $(E', \square)$. Se esiste un elemento neutro e per la legge $\circ$, allora esiste un elemento neutro e' per gli elementi dell'immagine $\Phi(E)$ rispetto la legge $\square$, e vale $\Phi(e) = e'$.

Proposizione 1.13.4. Se Φ è un omomorfismo di $(E, \circ)$ in $(E', \square)$. Se esiste in E il simmetrico dell'elemento a, allora esiste in E' il simmetrico di $\Phi(a)$.

Questo vuol dire che le applicazioni omomorfe tra insiemi dotati di leggi di composizione preservano tutte le proprietà algebriche delle leggi in questione. Approfondiremo questo tema nel successivo capitolo 2.

Infine, definiamo il caso particolare del isomorfismo.

Definizione 1.13.5. *Si dice* ***isomorfismo*** *una applicazione omomorfa* Φ *tra due insiemi* E *e* E'*, se* Φ *è suriettiva e iniettiva.*

Se esiste un isomorfismo tra due insiemi, si dice che sono **isomorfi**.

1.14 ripassando

Nella sezione 1.1 abbiamo introdotto le nozioni e la nomenclatura di base dell'insiemistica. La figura 1.19 visualizza le principali relazioni tra di loro.

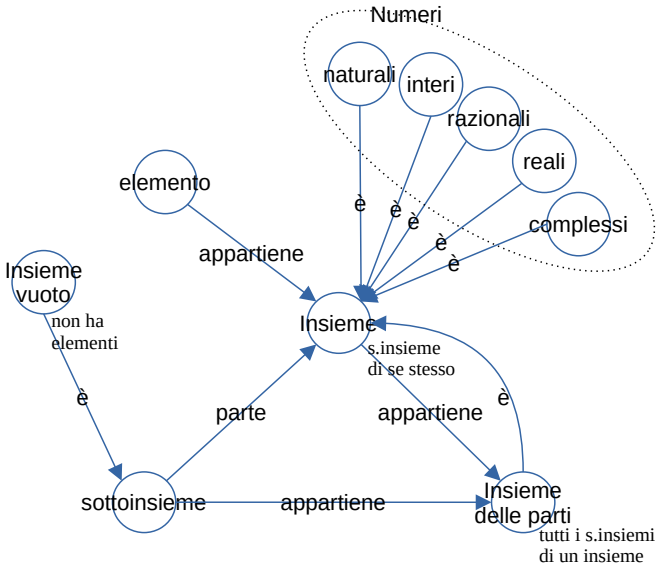


Figura 1.19: Insiemi: relazioni tra le nozioni

I concetti di *insieme* e di *elementi* che compongono l'insieme, sono centrali. I vari tipi di numeri cui ci hanno abituato gli insegnanti di *Algebra Elementare* (naturali, interi, ...) sono esempi di insiemi particolarmente significativi.

È possibile considerare insiemi che sono formati da *alcuni* degli elementi che formano l'insieme di riferimento: i *sottoinsiemi*.

Sono casi particolari di sottoinsiemi, l'*insieme vuoto* e lo stesso insieme di riferimeno.

Infine, possiamo vedere l'insieme di riferimento, quello vuoto, e tutti i suoi possibili sottoinsiemi, come elementi dell'*insieme delle parti*. Questo è un concetto duale: da un lato è un insieme, dall'altro l'insieme di riferimento è uno dei suoi elementi.

Invece la figura 1.20 ci introduce alle operazioni tra insiemi, che abbiamo visto nella sezione 1.2. Qui è rappresentata anche l'operazione di prodotto cartesiano (sezione 1.3).

A destra sono indicate le caratteristiche delle operazioni tra insiemi. Le operazioni principe sono *unione*, *intersezione* e *prodotto cartesiano*. Mentre *differenza* e *somma disgiunta* sono più esotiche.

Invece a sinistra, la differenza tra insieme di riferimento e sottoinsieme conduce al concetto di *insieme complementare*, con tutte le sue ricadute.

In basso, una suddivisione dell'insieme di riferimento in sottoinsiemi disgiunti crea un *insieme partizione*. I sottoinsiemi predetti sono i suoi elementi che vengono chiamati *classi*.

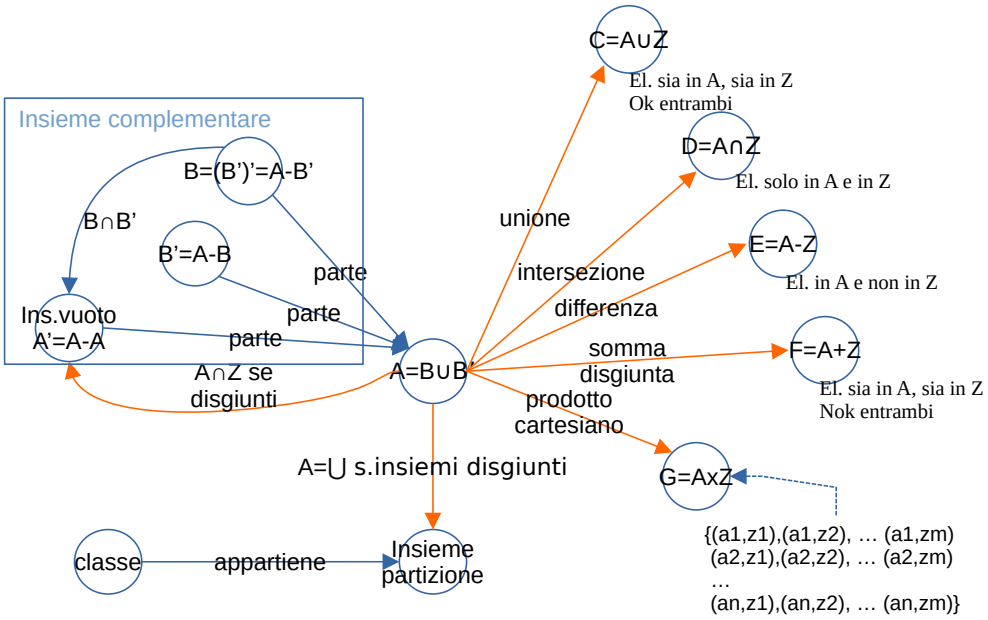


Figura 1.20: Ripassando: Insiemi, relazioni tra le operazioni

Infine, osserviamo con calma la figura 1.21 che riassume parecchi concetti correlati tra loro:

- le relazioni tra insiemi (sezione 1.4),
- l'insieme quoziente (sezione 1.5),
- l'applicazione (sezione 1.6),
- la loro composizione (sezione 1.7),
- la composizione interna ed esterna (sezione 1.11),
- la struttura algebrica (sezione 1.12),
- omomorfismo e isomorfismo (sezione 1.13),
- la partizione del dominio dell'applicazione 1.9.

Leggendola dall'alto in basso, da sinistra verso destra, ignorando per ora il box colorato in alto a sinistra, possiamo notare i seguenti elementi.

La *relazione binaria* è il concetto cardine, da cui derivano i successivi. È anche il più flessibile: lega genericamente elementi di due insiemi diversi. Da qui abbiamo tre archi che scendono in basso.

Il primo arco a sinistra è la sua specializzazione su un unico insieme, che, insieme alla imposizione della validità delle proprietà riflessiva, simmetrica e transitiva, deriva il concetto di *relazione di equivalenza*. Proseguendo da questa verso il basso osserviamo che una relazione di equivalenza definisce le *classi di equivalenza* che ci permettono di effettuare la *partizione* di un insieme. In particolare, considerando le diverse classi di equivalenza definite da una relazione di equivalenza otteniamo l'*insieme quoziente*, che è una partizione dell'insieme di partenza.

Ritorniamo in alto, alla relazione binaria, e seguiamo il secondo arco. Se specializziamo la relazione binaria, imponendo che all'elemento di partenza venga associato un solo elemento dell'insieme di arrivo, otteniamo il concetto di *applicazione*.

L'applicazione $f : A \to B$ è tale se un elemento del dominio A vede un solo elemento del codominio B. Ed è *suriettiva* se impegna tutti gli elementi del codominio. Per essere *iniettiva* è necessario che un elemento del codominio sia raggiunto ognuno da un solo elemento del dominio. Se queste due condizioni si verificano entrambe allora abbiamo una applicazione *biiettiva*.

E se una applicazione è biiettiva, allora possiamo definire la sua *inversa*, che mappa gli elementi del codominio verso quelli del dominio.

Torniamo di nuovo alla relazione binaria per seguire il terzo ramo. Abbiamo una applicazione *composta* se siamo in grado di effettuare in successione due applicazioni: $f : A \to B$ e poi dai relativi valori effettuare $g : B \to C$, avendo così il valore $g(f(a))$. In questi casi si dimostra che vale una ereditarietà delle caratteristiche delle applicazioni: se f e g sono entrambe suriettive, lo è anche la composta $f \circ g$; se sono entrambe iniettive, è iniettiva anche la composta.

Dalla composizione derivano i concetti di *composizione interna* e di *composizione esterna*.

Associando la composizione interna all'insieme A che genera il suo dominio ($A \times A$ o un suo sottoinsieme), abbiamo il concetto di *struttura algebrica*: $(A, \circ)$.

E da due strutture algebriche, arriviamo all'*omomorfismo* se abbiamo una applicazione tra le due strutture per la quale vale $\phi(x \circ y) = \phi(x) \square \phi(y)$. Se l'applicazione in questione è biiettiva, allora si parla di *isomorfismo*.

Il rettangolo colorato in alto a sinistra sintetizza il meccanismo che si può utilizzare per gestire applicazioni non iniettive. Utilizzando una relazione di equivalenza che raggruppa gli elementi del dominio che portano allo stesso elemento del codominio, creiamo l'insieme quoziente $A/\sim$ di A. Con l'applicazione $\pi : a \to [a]$ da qualunque elemento a otteniamo la sua classe di equivalenza $[a] \in A/\sim$. E da qui, con una apposita applicazione $f/\sim$, sicuramente iniettiva, possiamo arrivare sul codominio B.

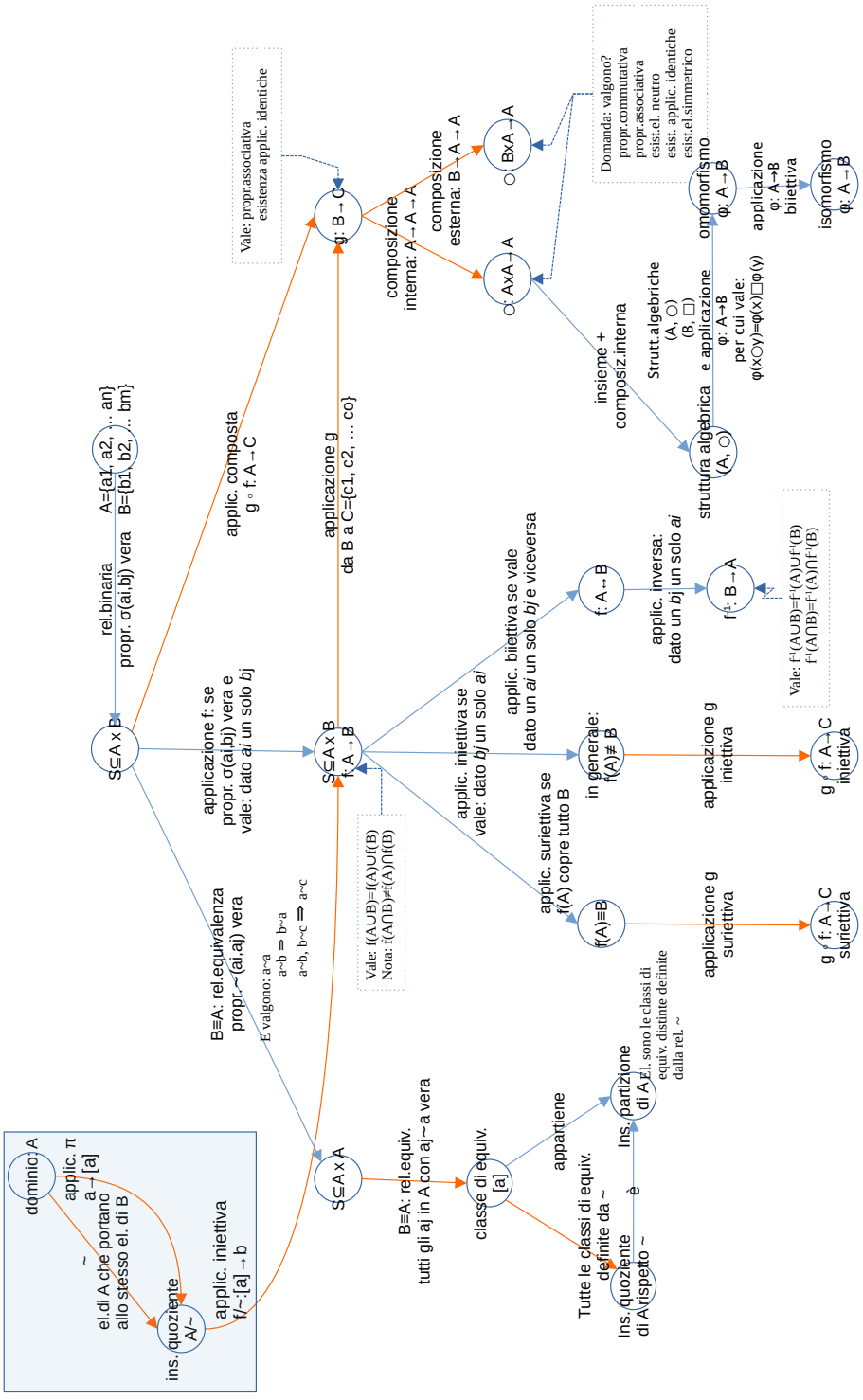


Figura 1.21: Ripassando. Insiemi: relazioni, applicazioni, . . . isomorfismo

Capitolo 2

Gruppi, anelli, campi

In questo capitolo approfondiamo il concetto di struttura algebrica. E, più in particolare, quello di *gruppo*.

Il termine è stato utilizzato per la prima volta da *Evariste Galois* nel 1830. Galois era un giovanissimo, matematico francese. Personaggio tanto geniale quanto irrequieto, morì nel 1832 a soli 21 anni a causa di un duello.

Il suo lavoro fu ignorato dalla maggior parte dei matematici francesi suoi contemporanei. Molti dei quali erano incapaci di comprenderlo perché troppo avanzato per la sua epoca.

Eppure i suoi appunti, anche se frammentari e in gran parte non dimostrati (furono aggregati frettolosamente dal Galois la notte precedente il duello) furono una pietra miliare nella storia della matematica. Lentamente riscoperti e ristudiati decenni dopo la sua morte, sono il seme che contribuì grandemente alla successva definizione dei concetti che illustreremo in questo capitolo, e nei successivi[1].

2.1 gruppi

Nel precedente capitolo abbiamo introdotto il concetto di gruppo. Definiamolo nuovamente.

[1] Ad esempio di veda l'articolo [Bottazzini 2006].

Definizione 2.1.1. *Un* ***gruppo*** *è un insieme G e una* legge di composizione interna[a] *(def. 1.11.1) $\circ$ tale che, dati gli elementi $a, b, c, e, a' \in G$, valgono le seguenti proprietà:*

$$a \circ b \in G \qquad \textit{chiusura/appartenenza} \tag{2.1}$$
$$(a \circ b) \circ c = a \circ (b \circ c) \qquad \textit{associativa} \tag{2.2}$$
$$e \circ a = a \circ e = a \qquad \textit{esistenza elemento neutro} \tag{2.3}$$
$$a \circ a' = a' \circ a = e \qquad \textit{esistenza elemento simmetrico} \tag{2.4}$$

Se, oltre le proprietà predette vale anche:

$$a \circ b = b \circ a \quad \textit{commutatività} \tag{2.5}$$

abbiamo un gruppo ***commutativo*** *o* ***abeliano****.*

[a] Ovvero una operazione binaria il cui dominio è $G \times G$ e il codominio è G.

Un gruppo si indica con la notazione $(G, \circ)$. La quale mette in evidenza che la struttura di gruppo è data dalla presenza dell'operazione definita sull'insieme G indicato.

Non sappiamo se l'avete notato. La proprietà 2.1 esprime il fatto che il risultato dell'operazione appartiene all'insieme G di partenza. E questo fa sì che si abbia il concetto di *chiusura*: se applico ripetutamente, in cascata, l'operazione, ottengo sempre elementi che appartengono a G. Non posso uscire da G applicando solo questa operazione ai suoi elementi.

In matematica è facile trovare esempi del concetto di gruppo.

Esempio 2.1.2. Consideriamo l'insieme dei numeri interi con l'operazione di addizione: $(\mathbb{Z}, +)$. Qui l'elemento neutro è lo zero, mentre gli elementi simmetrici sono i negativi dell'elemento considerato di volta in volta; ad es.: $(+2, -2)$, $(-3, +3)$ ...

Esempio 2.1.3. Oppure, prendiamo l'insieme dei numeri reali, *senza lo zero*, e l'operazione di moltiplicazione. In questo caso avremo il gruppo $(\mathbb{R}^*, \cdot)$. L'elemento neutro è l'uno. Mentre il simmetrico dell'elemento a è $\frac{1}{a}$.

Nel precedente esempio abbiamo indicato l'insieme dei numeri reali senza lo zero con il simbolo: $\mathbb{R}^*$. Ai matematici piace così ☺.

Gli esempi riportati sono minuzie. È possibile sbizzarrirsi con le varie tipologie di numeri[2], utilizzare le matrici o i vettori invece dei numeri, o forme di composizione meno usuali.

Per chi conosce qualcosa del calcolo matriciale, vale il seguente esempio:

Esempio 2.1.4. Data le matrici $m \times n$ di numeri reali, e l'operazione di somma di matrici, abbiamo il gruppo $(\mathcal{M}_{m \times n}(\mathbb{R}), +)$. L'elemento neutro è la matrice formata da tutti zeri. Mentre la matrice simmetrica è quella formata dagli elementi negati.

[2] Razionali, complessi ...

2.2 conseguenze algebriche della definizione di gruppo

Il fatto che $(G, \circ)$ sia un gruppo ha delle conseguenze. È possibile dimostrare le seguenti affermazioni:

1. l'elemento neutro di G è unico;
2. ogni elemento $g \in G$ ha un unico simmetrico;
3. vale la proprietà di *semplificazione*

$$a \circ b = a \circ c \Rightarrow b \circ c \quad a, b, c \in G$$

4. $(a^{-1})^{-1} = a \quad \forall a \in G$
5. $(a \circ b)^{-1} = a^{-1} \circ b^{-1} \quad \forall a, b \in G$
6. le equazioni $ax = b$ e $xa = b$ hanno l'unica soluzione $x = a^{-1}b$

2.3 rappresentazione di gruppi finiti

L'insieme G di un gruppo può essere finito o infinito. Se è finito, il numero dei suoi elementi è detto **ordine**.

Nel caso di insiemi finiti, visto che la *chiusura* dell'operazione del gruppo ci assicura che avremo a che fare sempre con elementi dell'insieme, è possibile rappresentare l'operazione con una tavola moltiplicativa.

Nel caso di ordine 1 avremo la tabella 2.1.

Tabella 2.1: tabella moltiplicativa per un gruppo di ordine 1

$\circ$	e
e	e

Più interessante il caso di due elementi in G. Qui avremo la tabella moltiplicativa 2.2.

Tabella 2.2: tabella moltiplicativa per un gruppo di ordine 2

$\circ$	e	a
e	e	a
a	a	e

Con tre elementi abbiamo la tabella moltiplicativa 2.3.

Tabella 2.3: tabella moltiplicativa per un gruppo di ordine 3

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Con l'ordine quattro, abbiamo due diversi tipi di tabelle moltiplicative. E con ordini superiori le tipologie aumentano.

Un esempio importante è quello relativo alle trasformazioni di un insieme A.

Esempio 2.3.1. L'insieme $T(A)$ delle applicazioni biiettive di A in sè (vedi 1.10) è un gruppo. Infatti le sue proprietà 1.19, 1.20, 1.21, 1.22 sono esattamente le proprietà che definiscono un gruppo.

2.4 gruppo delle isometrie e delle simmetrie

Facciamo una premessa.

Se consideriamo come insieme in analisi il piano euclideo ($\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$), vi è un tipo di trasformazioni biiettive particolarmente interessanti: quelle isometriche.

Definizione 2.4.1. *Una trasformazione di un piano, è una* ***isometria*** *se mantiene la distanza di due punti qualsiasi.*

Su un piano è sempre possibile definire la *trasformazione identica*, ovvero quella che trasforma un qualunque punto del piano in se stesso. La trasformazione identica è una isometria: non altera le distanze tra i punti.

Ora, consideriamo l'insieme S delle possibili isometrie del piano[3].

Ebbene abbiamo le seguenti affermazioni dimostrabili:

1. Se φ_1 e φ_2 sono isometrie allora la loro composizione[4] $\varphi_1 \circ \varphi_2$ è una isometria.
2. Vale l'associatività della composizione delle isometrie.
3. La trasformazione identica è l'elemento neutro.
4. Data l'isometria φ esiste la sua inversa φ^{-1} ed è una isometria.

Le proprietà precedenti sono quelle che definiscono un gruppo: $(S, \circ)$. Le isometrie nel piano, con la loro composizione, sono un gruppo.

Possiamo ragionare anche sulle *simmetrie* di una figura. Per simmetrie intendiamo quelle operazioni che trasformano una figura senza cambiarne l'aspetto.

Nello spazio le simmetrie sono studiabili tramite tre tipi di trasformazioni:

1. traslazioni;
2. rotazioni attorno ad un asse;
3. riflessioni rispetto un piano.

Nel piano le simmetrie possibili sono:

1. traslazioni[5];
2. rotazioni attorno ad un punto;
3. riflessioni rispetto una retta.

Ad esempio, prendiamo un esagono. Se lo facciamo ruotare di 60° in senso antiorario, rispetto il suo centro, otterremo una figura uguale a quella di partenza, con i vertici ruotati di una posizione. La figura 2.1 illustra due rotazioni di un esagono rispetto il suo centro.

[3] Per la considerazione precedente, l'insieme S non è vuoto: esiste almeno la trasformazione identica.

[4] Ovvero applicarle in sequenza, una dopo l'altra.

[5] Queste nel piano sono valide solo per figure di dimensioni illimitate. Perciò qui non le consideriamo.

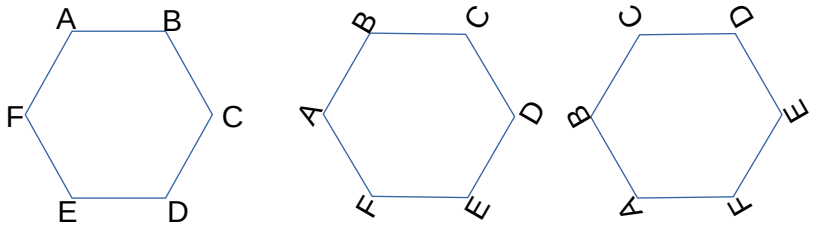


Figura 2.1: Rotazioni antiorarie di 60° e 120° di un esagono

Da sinistra verso destra, abbiamo una rotazione antioraria di 60°, ed una, sempre antioraria, di 120°. Le lettere ai vertici del poligono ci aiutano a visualizzare il movimento effettuato.

In generale, per un poligono regolare con n lati, le rotazioni saranno multipli interi di $\frac{2\pi}{n}$.

Indicando una rotazione con il simbolo R_n^k dove k è il multiplo intero e n è il numero di lati del poligono, la tabella 2.4 è la tavola delle moltiplicazioni per le rotazioni di un esagono.

Tabella 2.4: tavola delle moltiplicazioni per le rotazioni di un esagono

	R_6^0	R_6^1	R_6^2	R_6^3	R_6^4	R_6^5
R_6^0	R_6^0	R_6^1	R_6^2	R_6^3	R_6^4	R_6^5
R_6^1	R_6^1	R_6^2	R_6^3	R_6^4	R_6^5	R_6^0
R_6^2	R_6^2	R_6^3	R_6^4	R_6^5	R_6^0	R_6^1
R_6^3	R_6^3	R_6^4	R_6^5	R_6^0	R_6^1	R_6^2
R_6^4	R_6^4	R_6^5	R_6^0	R_6^1	R_6^2	R_6^3
R_6^5	R_6^5	R_6^0	R_6^1	R_6^2	R_6^3	R_6^4

Considerando l'insieme G formato dagli esagoni uguali, ruotati di $R^0, R^1, R^2, R^3, R^4, R^5$, vi possiamo associare la moltiplicazione come rotazine definita nei paragrafi precedenti. In queste condizioni, usando la tavola 2.4 possiamo verificare la validità delle proprietà che definiscono un gruppo.

Discorso analogo si può fare per le riflessioni. In questo caso illustriamo con la figura 2.2 un esempio di riflessione di un esagono rispetto l'asse H-K

Anche in questo caso le lettere ci aiutano a capire il movimento dei vertici attuato dall'operazione. Notiamo che in figura sono indicati solo tre assi di simmetria. In realtà gli assi possibili sono sei. Anche in questo caso possiamo costruire la relativa tabella delle moltiplicazioni, e verificare che abbiamo a che fare con un gruppo.

2.5 sottogruppi

Se abbiamo un gruppo $(G, \circ)$, possiamo considerare la presenza di sottoinsiemi $H \subseteq G$ che mantengono la struttura algebrica predetta.

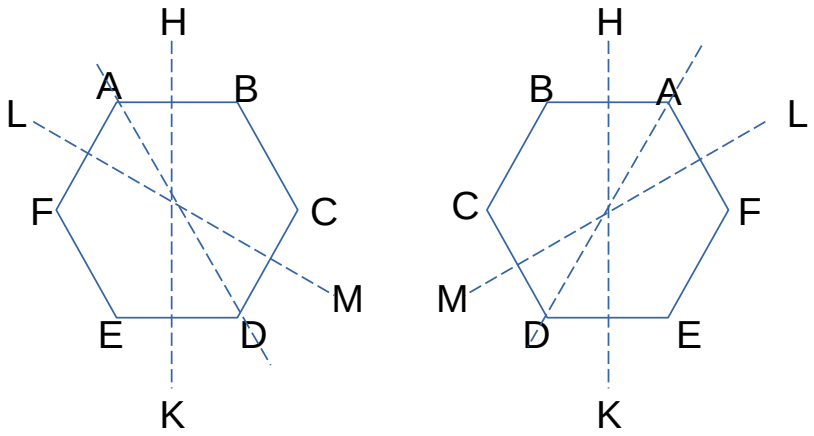


Figura 2.2: Riflessione di un esagono rispetto l'asse H-K

Definizione 2.5.1. *Un sottoinsieme non vuoto H è un* ***sottogruppo*** *di G se, rispetto il suo prodotto mantiene la stessa struttura algebrica.*

Si dimostra che vale la seguente affermazione.

Proposizione 2.5.2. Un sottoinsieme non vuoto H di G è un suo sottogruppo *se e solo se* valgono:

1. $a, b \in H \Rightarrow a \circ b \in H$
2. $a \in H \Rightarrow a^{-1} \in H$

Un semplice esempio di sottogruppo è il seguente.

Esempio 2.5.3. Consideriamo il gruppo $(\mathbb{Z}, +)$ degli interi con segno. Prendiamo per H il sottoinsieme dei numeri pari, incluso lo zero. Vale $(H, +)$, ed è un sottogruppo del precedente.

Se consideriamo il sottoinsieme dei numeri dispari, questo non è un sottogruppo di $(\mathbb{Z}, +)$ perchè la somma di due dispari rende un numero pari, uscendo dal sottoinsieme di partenza.

Ricordiamo che un insieme può essere considerato sottoinsieme di se stesso. Quindi $(G, \circ)$ può essere considerato un sottogruppo di se stesso.

Inoltre se consideriamo il sottoinsieme formato dal solo elemento neutro $e \in G$, anche $(\{e\}, \circ)$ è un sottogruppo di G.

Definizione 2.5.4. *Un sottogruppo H di G si dice* ***sottogruppo proprio*** *se $H \notin G$ e $H \notin \{e\}$.*

Vogliamo vedere un esempio più esotico di sottogruppo? Consideriamo il seguente.

Esempio 2.5.5. Dato l'insieme $T(\mathbb{R}^2)$ delle trasformazioni nel piano cartesiano (vedi 1.10 e 2.3.1). Le isometrie $S \in (R)^2$ (vedi 2.4.1) sono un sottogruppo di $T(\mathbb{R}^2)$.

2.6 omomorfismi, isomorfismi, automorfismi di un gruppo

Nella sezione 1.13.1 abbiamo visto la definizione di omomorfismo per applicazioni tra due insiemi dotati di leggi di composizione. Possiamo estendere quella definizione ai gruppi come segue.

Definizione 2.6.1. *Dati i due gruppi* $(G, \circ)$ *e* $(G', \square)$ *una applicazione* $\phi : G \to G'$ *è un* ***omomorfismo*** *se preserva le moltiplicazioni:*

$$\phi(x \circ y) = \phi(x) \square \phi(y) \tag{2.6}$$

Se esiste un omomorfismo tra due gruppi, allora i gruppi stessi si dicono *omomorfi*.
Si dimostra la seguente:

Proposizione 2.6.2. Se ϕ è un omomorfismo tra le strutture algebriche $(G, \circ)$ e $(G', \square)$, e se $(G, \circ)$ è un gruppo, allora lo è anche l'immagine $\phi(G) \subseteq G'$.

Riprendendo le considerazioni generali dell'introduzione abbiamo detto che il concetto di *morfismo* associato alla *struttura algebrica* permette la loro classificazione. Bene, l'omomorfismo è la base di partenza che in 2.6.8 ci porterà a questa conclusione.
Ed ora un concetto che intrigherà gli informatici. Il *Kernel* di un omomorfismo:

Definizione 2.6.3. *Si chiama* ***Kernel*** *dell'omomorfismo* $\phi : G \to G'$ *l'insieme degli elementi di* G *che hanno come immagine l'elemento neutro* $e' \in G'$.

Il *Kernel* si indica con *Ker* ϕ. E vale *Ker* $\phi = \{x \in G | \phi(x) = e'\}$.
Possiamo estendere anche il concetto di isomorfismo tra insiemi:

Definizione 2.6.4. *una applicazione* $\phi : G \to G'$ *omomorfa è un* ***isomorfismo*** se è biiettiva.

Si dicono *isomorfi* due gruppi $(G, \circ)$ e $(G', \square)$ se esiste un isomorfismo ϕ tra loro.

Esempio 2.6.5. Se i nostri ricordi del liceo ci assistono, vale:
$\log(x_1 \cdot x_2) = \log(x_1) + \log(x_2)$. Quindi se consideriamo la funzione log tra $(R^+, \cdot)$ e $(R, +)$, osserviamo che è sia suriettiva che iniettiva[6]. Quindi è un isomorfismo.

Osserviamo che se $\phi : G \to G'$ è un isomorfismo, vale *Ker* $\phi = \{e\}$. Perché il *Kernel* è formato da tutti gli elementi di G che puntano ad $e' \in G'$. Tra questi vi è sicuramente l'elemento neutro $e \in G$ (per il teorema 1.13.3). Ma non vi possono essere altri elementi perché ϕ è iniettiva.
Inoltre si dimostra la seguente:

Proposizione 2.6.6. Se $\phi : G \to G'$ è un isomorfismo, anche $\phi^{-1} : G' \to G$ è un isomorfismo.

[6] Ricordiamo che R^+ è l'insieme dei *numeri reali positivi*. E la funzione $y = \log(x)$ vale $-\infty < y < +\infty$ per $0 < x < +\infty$.

Consideriamo ora un insieme i cui elementi sono tutti i possibili gruppi. La relazione di isomorfismo è una relazione di equivalenze nell'insieme predetto.

Osservazione 2.6.7. Quindi, per le considerazioni fatte nella sezione 1.4[a] gli *isomorfismi definiscono una partizione dell'insieme dei possibili gruppi.*

Di conseguenza abbiamo la seguente:

Osservazione 2.6.8. Una classe di equivalenza di un isomorfismo definisce un *gruppo astratto.*

[a] Con particolare riferimento alla definizione di relazione di equivalenza (vedasi 1.4.3), alla definizione di classe di equivalenza (1.4.5) e al teorema di partizione (1.4.6).

Studiare i gruppi astratti permette di focalizzarsi sulle proprietà comuni a tutti i gruppi appartenenti ad una classe di equivalenza definita da un isomorfismo. Senza dover studiare i singoli gruppi uno ad uno.

Un caso particolarmente importante, è lo studio di applicazioni di un gruppo verso se stesso. Per questo motivo sono stati coniati dei termini ad hoc per questa casistica. Abbiamo:

Definizione 2.6.9. *Si chiama* ***endomorfismo*** *un* omomorfismo $\phi : G \to G$

Definizione 2.6.10. *Si chiama* ***automorfismo*** *un* isomorfismo $\phi : G \to G$

Quindi un automorfismo è una biiezione del gruppo G su G che preserva la sua struttura algebrica.

2.7 traslazioni a destra e a sinistra, teorema di Cayley

Sappiamo tutti cosa sia una traslazione. Quando spingo una carriola lungo una strada, ne sto effettuando la sua traslazione. L'algebra generale astrae questo concetto in questo modo:

Definizione 2.7.1. *Dato un elemento a appartenente al gruppo G, si chiama* ***traslazione a sinistra*** *la seguente applicazione:*

$$S_a : G \times G \to G \qquad \forall x \in G$$
$$(a, x) \mapsto a \circ x$$

Esiste il concetto di **traslazione a destra**:

$$D_a : G \times G \to G \qquad \forall x \in G$$
$$(a, x) \mapsto x \circ a$$

Si dimostra che le traslazioni predette sono applicazioni biiettive di G in sè. Inoltre abbiamo:

Proposizione 2.7.2. Dato un gruppo $(G, \circ)$, l'insieme delle traslazioni a sinistra $H = \{S_a | a \in G\}$ è a sua volta un gruppo.

E si dimostra il seguente *teorema di Cayley*:

Teorema 2.7.3. *Il gruppo H della traslazione a sinistra di un gruppo G è isomorfo.*

Quindi H è una immagine isomorfa di G tramite l'applicazione

$$\begin{aligned} \phi : G &\to H \\ a &\mapsto S_a \end{aligned}$$

2.8 anelli

Riprendiamo a parlare di gruppi pensando agli anelli. Quando parliamo di anelli, noi persone normali pensiamo agli ornamenti per le dita. Invece i matematici pensano a come costruirne uno nello spazio: con due operazioni. Una per definire la circonferenza principale: quella che identifica il foro dell'anello. E una per definire la circonferenza che identifica lo spessore dell'anello, facendola viaggiare lungo la circonferenza principale.

Quindi quando abbiamo due composizioni disponibili, ecco che i matematici pensano agli anelli:

Definizione 2.8.1. *un anello è un insieme A non vuoto con due leggi di composizione interne, indicate $(+)$ e $(\circ)$ per le quali valgono:*

$$(A, +) \quad \text{è un gruppo abeliano} \tag{2.7}$$

$$(\circ) \quad \text{è associativa} \tag{2.8}$$

$$\left.\begin{aligned} a \circ (b + c) &= a \circ b + a \circ c \\ (b + c) \circ a &= b \circ a + c \circ a \end{aligned}\right\} \quad \begin{aligned} &\forall a, b, c \in A \text{ vale la legge} \\ &\text{distributiva di } \circ \text{ rispetto } + \end{aligned} \tag{2.9}$$

Inoltre:

Definizione 2.8.2. *se la seconda legge $(\circ)$ di un anello A è commutativa, si dice che A è un* ***anello commutativo****.*

Le proprietà 2.7, 2.8, 2.9, quando sviluppate esplicitamente danno luogo alle seguenti

proposizioni:

$$a+b \in A \quad \forall a,b \in A \tag{2.10}$$
$$a+b = b+a \tag{2.11}$$
$$(a+b)+c = a+(b+c) \tag{2.12}$$
$$\exists\, 0 \,\text{rispetto}\, + \,|\, a+0=0 \quad \forall a \in A \tag{2.13}$$
$$\exists\, -a \,|\, a+(-a)=0 \tag{2.14}$$
$$a \circ b \in A \tag{2.15}$$
$$a \circ (b \circ c) = (a \circ b) \circ c \tag{2.16}$$
$$a \circ (b+c) = a \circ b + a \circ c \tag{2.17}$$
$$\begin{aligned} a \circ (b+c) &= a \circ b + a \circ c \\ (b+c) \circ a &= b \circ a + c \circ a \end{aligned} \tag{2.18}$$

Ancora:

Definizione 2.8.3. *se la seconda legge ($\circ$) di un anello A possiede un elemento neutro, si dice che A è un* ***anello unitario****.*

Esempio 2.8.4. Dato l'insieme $\mathbb{Z}$ dei numeri interi con segno, con le operazioni di somma ($+$) e di moltiplicazione ($\circ$) è un anello commutativo unitario. L'unità per la somma è l'elemento 0, mentre per la moltiplicazione è l'elemento 1.

Esempio 2.8.5. Date le matrici quadrate con elementi in $\mathbb{R}$ con le operazioni di addizione e moltiplicazione matriciali, abbiamo un anello. Infatti si verifica la validità delle proprietà 2.7, 2.8, 2.9.

Notiamo che questo anello non è commutativo. Ad esempio:
$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) \circ \left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2\\0&2\end{smallmatrix}\right)$, mentre abbiamo: $\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right) \circ \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&1\\0&2\end{smallmatrix}\right)$.

Osservazione 2.8.6. In un anello può capitare che valga $a \circ b = 0$ con $a \neq 0$ e $b \neq 0$.

Si può vedere riprendendo l'esempio dell'anello delle matrici quadrate (esempio 2.8.5) e considerando il fatto che la matrice nulla è quella con tutti zeri. Se calcoliamo: $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) \circ \left(\begin{smallmatrix}0&0\\0&2\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$, si vede che otteniamo lo zero a partire da elementi non nulli.

Definizione 2.8.7. *Si dicono* ***divisori dello zero*** *gli elementi di un anello, diversi da zero, il cui prodotto è zero.*

Siccome gli anelli sono casi particolari di gruppi, i concetti di omomorfismo (vedi 2.6.1), isomorfismo (vedi 2.6.4), kernel (vedi 2.6.3), endomorfismo (vedi 2.6.9) e automorfismo (vedi 2.6.10), si applicano anche a loro.

2.9 campi

I *campi* sono casi particolari degli anelli.

Definizione 2.9.1. *Se K è un anello, lo 0 è l'elemento neutro rispetto la prima legge di composizione*[7] *e indichiamo con $K^* = \{K - \{0\}\}$ l'insieme degli elementi di K diversi da 0. Se la seconda legge di composizione, definita su K, è una legge di gruppo per K^*, allora diciamo che K è un* ***corpo****.*

Definizione 2.9.2. *Se K è un corpo in cui* la seconda legge di composizione è commutativa*, allora lo diciamo* ***campo****.*

Esempio 2.9.3. L'insieme dei razionali con le leggi di addizione e moltiplicazione $(Q, +, \circ)$ è un campo, detto *campo dei razionali.*

Analogamente

Esempio 2.9.4. $(\mathbb{R}, +, \circ)$ è il *campo dei reali.*

Notiamo la seguente:

Osservazione 2.9.5. In un *corpo*[8] non vi sono divisori dello zero. Perché la seconda legge di composizione è chiusa su K^* [9] ma non può valere 0 perché questo non è compreso in K^*.

2.10 ripassando

Per sintetizzare quanto abbiamo letto in questo capitolo, possiamo fare riferimento alla figura 2.3.

[7] Cioè quella abeliana.
[8] E quindi anche in un campo.
[9] Ovvero: $\forall a, b \in K^*$ vale $a \circ b \ \in K^*$.

Figura 2.3: Gruppi: dai gruppi ai campi

Gli ingredienti di partenza per avere un gruppo $(G, \circ)$ sono in alto nella figura: un insieme G e una legge di composizione interna $\circ : G \times G \to G$.

Dopo di che possiamo considerare i concetti di gruppo abeliano e di sottogruppo.

La cosa si complica per l'*omomorfismo*. Qui ci servono due gruppi G e G', e una applicazione dal primo al secondo: $\phi : G \to G'$ per la quale valga: $\phi(x \circ y) = \phi(x)(y)$. Se tutto ciò è valido, ϕ è un omomorfismo, e gli insiemi G e G' sono omomorfi.

Sempre per l'omomorfismo: se $G \equiv G'$ allora abbiamo un *endomorfismo*. Se ϕ è biiettiva abbiamo un *isomorfismo*. E se per l'isomorfismo vale $G \equiv G'$, si parla di *automorfismo*.

Un isomorfismo definisce una relazione di equivalenza tra i possibili gruppi, e quindi una classe di equivalenza. Questa è detta *gruppo astratto*, in quanto sintetizza i comportamenti algebrici fondamentali di tutti i gruppi appartenenti alla classe. I gruppi astratti partizionano tutti i possibili gruppi.

Se risaliamo in alto e ci spostiamo a sinistra, sul gruppo abeliano, possiamo considerare la presenza di una seconda legge di composizione interna. Se per la seconda legge valgono la proprietà associativa e quella distributiva rispetto la prima legge, allora diciamo di avere un *anello*.

Un anello può essere commutativo o unitario. Ma, sopratutto la seconda legge può definire un gruppo sull'insieme $K^* = \{K - \{0\}\}$, e se è anche commutativa, allora abbiamo a che fare con un *campo*: $(K, +, \circ)$.

Capitolo 3

Spazi vettoriali

Come abbiamo visto nei capitoli precedenti, i matematici sono molto attenti ad evitare di duplicare lo studio di aree che hanno principi di base simili. Questo è uno dei principali motivi che hanno portato alla nascita dei concetti di *gruppo, morfismo, omomorfismo,* ...

Analogamente, l'analisi di analogie scaturite durante lo studio di aree diverse della matematica, hanno portato alla creazione del concetto di *spazio vettoriale*.

In particolare, è possibile osservare come le operazioni su vettori nello spazio tridimensionale $\mathbb{R}^3$ presentano proprietà analoghe a quelle delle operazioni su soluzioni di insiemi di equazioni lineari omogenee in n incognite con coefficienti $a_{ij} \in \mathbb{R}$. Quindi: gli ambiti sono completamente diversi, ma le proprietà algebriche sono simili. Come evitare di duplicare lo sforzo per studiarli? Forti di quanto letto nei capitoli precedenti, fondando il concetto di spazio vettoriale.

3.1 nozione di spazio vettoriale

Concetto che si sviluppa astraendo le caratteristiche delle operazioni dei vettori nello spazio tridimesionale. Ricordando che alla base delle operazioni vettoriali vi sono il concetto di somma tra vettori e quello di moltiplicazione per uno scalare, possiamo ricordare più facilmente questa definizione:

Definizione 3.1.1. *Dato un insieme non vuoto E* [a]*, diciamo* ***spazio vettoriale*** *su un campo K* [b]*, se tra i suoi elementi sono definite due operazioni di composizione:*

1. *una operazione $(+)$ di composizione* interna *$(E \times E \to E)$ che associa ad ogni coppia ordinata di vettori uno ed un solo vettore somma $\mathbf{z} = \mathbf{u} + \mathbf{v}$, e che ha le seguenti proprietà* [c]*:*

$$\left.\begin{array}{ll} \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u} & \textit{commutativa} \\ (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w}) & \textit{associativa} \\ \mathbf{u} + \mathbf{0} = \mathbf{0} + \mathbf{u} = \mathbf{u} & \textit{esistenza dell'elemento neutro} \\ \mathbf{u} + (-\mathbf{u}) = \mathbf{0} & \textit{esistenza dell'elemento opposto} \end{array}\right\} \tag{3.1}$$

2. *una operazione $(\circ)$ di composizione* esterna *$(K \times E \to E)$ che associa ad ogni coppia ordinata di elementi $(a, \mathbf{u})$* [d] *uno ed un solo vettore $\mathbf{v} = a \circ \mathbf{u}$ ed ha le seguenti proprietà:*

$$\left.\begin{array}{ll} a \circ (\mathbf{u} + \mathbf{v}) = a \circ \mathbf{u} + a \circ \mathbf{u} & \textit{distributiva rispetto la somma vettoriale} \\ (a + b) \circ \mathbf{u} = a \circ \mathbf{u} + b \circ \mathbf{u} & \textit{distributiva rispetto la somma in } K \\ a \circ (b \circ \mathbf{u}) = (a \circ b) \circ \mathbf{u} & \textit{associativa} \\ \mathbf{u} \circ 1 = 1 \circ \mathbf{u} = \mathbf{u} & \textit{neutralità per l'unità moltiplicativa del campo } K \end{array}\right\} \tag{3.2}$$

[a] I cui elementi sono detti **vettori**. I vettori nelle equazioni si indicano con lettere minuscole in grassetto. Ad es. $\mathbf{u}, \mathbf{v} \ldots$.

[b] I cui elementi sono detti **scalari**. In particolare K potrà essere il campo dei reali o dei complessi

[c] $\forall \mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{0} \in E$

[d] Con $a \in K$ e $\mathbf{u}, \mathbf{v} \in E$.

Attenzione a come interpretiamo le operazioni di somma $(+)$ nelle proprietà 3.2. Quando scriviamo $a + b$ facciamo riferimento alla somma tra scalari: in K. Mentre $a \circ \mathbf{u} + b \circ \mathbf{u}$ è una somma *tra vettori*, ovvero in E.

Ancora: è mandatario specificare il campo K. Un insieme E potrebbe essere uno spazio vettoriale su un dato campo K e non su un altro.

Osservazione 3.1.2. Inoltre attenzione a non farci influenzare troppo dai vettori nello spazio tridimensionale. Nella definizione precedente, *non abbiamo indicato esplicitamente* come effettuare le operazioni per avere il risultato delle due leggi di composizione volute. Vanno bene qualunque tipo di operazioni, purché soddisfino le proprietà 3.1 e 3.2.

Osservazione 3.1.3. Notiamo che le proprietà 3.1 definiscono $(E, +)$ come gruppo abeliano.

Osservazione 3.1.4. Considerando la composizione esterna $a \circ \mathbf{u}$. La possiamo pensare come una applicazione $E \to E$ per la quale vale $a \circ (\mathbf{u} + \mathbf{v}) = a \circ \mathbf{u} + a \circ \mathbf{u}$. E questa

è la definizione di omomorfismo (si veda 2.6.1). Quindi *fissato* $a \in K$ abbiamo un omomorfismo di E in E.

Osservazione 3.1.5. Riguardo l'esistenza dello zero, la sua definizione in 3.1 assicura la sua unicità, in quanto se ve ne fossero due, diciamoli $\mathbf{0}$ e $\mathbf{0}'$, varrebbe $\mathbf{0}' = \mathbf{0}' + \mathbf{0} = \mathbf{0}$.

Le seguenti conseguenze della definizione 3.1.1 si dimostrano facilmente. Valgono:

$$a\mathbf{0} = \mathbf{0} \qquad \forall a \in K \tag{3.3}$$

$$0\mathbf{v} = \mathbf{0} \qquad \forall \mathbf{v} \in E \tag{3.4}$$

$$(-a)\mathbf{v} = -(a\mathbf{v}) \qquad \forall a \in K, \mathbf{v} \in E \tag{3.5}$$

$$\text{se } a\mathbf{v} = \mathbf{0} \,\text{con}\, (v) \neq \mathbf{0} \Rightarrow a = 0 \tag{3.6}$$

Esempio 3.1.6. Il prodotto cartesiano dei reali per se stesso n volte, ovvero $\mathbb{R}^n$, che si può rappresentare come le n-ple ordinate di numeri reali, è uno spazio vettoriale sui reali se si definiscono:

- come somma l'operazione:

$$(x_1, x_2, \dots x_n) + (y_1, y_2, \dots y_n) = (x_1 + y_1, x_2 + y_2, \dots x_n + y_n)$$

- come prodotto per uno scalare[1] l'operazione:

$$a \circ (x_1, x_2, \dots x_n) = (ax_1, ax_2, \dots ax_n)$$

prendendo come elemento neutro $\mathbf{0} \in \mathbb{R}^n$ la n-pla formata da tutti zeri: $(0, 0, \dots 0)$

Esempio 3.1.7. Se ci si limita alle operazioni canoniche di somma tra vettori nel piano e nello spazio, e al prodotto per uno scalare, i vettori nel piano e quelli nello spazio sono spazi vettoriali.

Esempio 3.1.8. Consideriamo l'insieme delle matrici $m \times n$ con elementi in $\mathbb{R}$. Se si definisce l'operazione di somma tra due matrici A e B la matrice in cui ogni elemento è ottenuto sommando gli elementi di A e B con gli stessi indici. E se si definisce il prodotto dello scalare $\lambda \in \mathbb{R}$ per la matrice A come la matrice in cui ogni elemento è ottenuto moltiplicado λ per l'elemento di A con gli stessi indici.

In queste condizioni l'insieme predetto con le due operazioni in questione è uno spazio vettoriale.

Fin qui esempi abbastanza scontati. Ma quello che segue ci piace particolarmente.

Esempio 3.1.9. Chiamiamo $C(a, b)$ l'insieme di tutte le funzioni continue a valori reali $y = f(x)$ con $x \in \mathbb{R}$ e $a \leq x \leq b$ con $a, b \in \mathbb{R}$.

[1] Attenzione alla terminologia: *prodotto* ***per uno*** *scalare*. Non *prodotto scalare*. Questa ulteriore operazione la incontreremo più in là. Un prodotto scalare è un prodotto tra due vettori, che rende uno scalare. Invece in questo contesto abbiamo un prodotto tra uno scalare e un vettore, che rende un vettore.

$C(a,b)$ costituisce uno spazio vettoriale su $\mathbb{R}$ se si definisce la somma come somma di due funzioni $f, g \in C(a,b)$, e il prodotto per un reale $a \in \mathbb{R}$.

In particolare:

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) && x \in [a,b] \\ (af)(x) &= a(f(x)) && \forall x \in \mathbb{R} \end{aligned}$$

L'elemento neutro è la funzione nulla: $0 = f(x)\, \forall x \in [a,b]$.

3.2 dipendenza e indipendenza lineare

Definizione 3.2.1. *Dati $\mathbf{v}_1, \mathbf{v}_2, \dots \mathbf{v}_r$ vettori dello spazio vettoriale E sul campo K.*

*Ogni vettore $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots a_r\mathbf{v}_r$ con $a_1, a_2, \dots a_r \in K$ si chiama **combinazione lineare su** K dei vettori $\mathbf{v}_1, \mathbf{v}_2, \dots \mathbf{v}_r$.*

Definizione 3.2.2. *Dati $\mathbf{v}_1, \mathbf{v}_2, \dots \mathbf{v}_r$ vettori dello spazio vettoriale E sul campo K, si dicono **linearmente dipendenti** su K se esistono r scalari $a_1, a_2, \dots a_r$* non tutti nulli*, tali che valga:*

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots a_r\mathbf{v}_r = \mathbf{0} \tag{3.7}$$

Se non esistono r scalari $a_1, a_2, \dots a_r$ non tutti nulli, tali che valga l'equazione 3.7, i vettori in questione si dicono **linearmente indipendenti**. In questo caso:

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots a_r\mathbf{v}_r \neq \mathbf{0} \quad \text{per coefficienti non tutti nulli} \tag{3.8}$$

Definizione 3.2.3. *Un insieme di vettori linearmente indipendenti è detto **sistema indipendente**. Nelle equazioni usualmente si indica con R.*

Osservazione 3.2.4. Se dei vettori sono linearmente indipendenti, nessuno di essi può essere nullo.

Infatti, supponiamo $\mathbf{v}_1 = \mathbf{0}$. In tal caso potremmo utilizzare
$a_1 \neq 0, a_2 = 0, \dots a_r = 0$ per ottenere la validità della equazione 3.7, in contrasto con la nostra affermazione.

Notiamo che la dipendenza, o l'indipendenza, lineare dipendono dal campo K. Per convincercene, consideriamo il campo dei complessi $\mathbb{C}$. Questo è un spazio vettoriale sia sui reali che sui complessi. Se prendiamo i due vettori $\mathbf{u}_1 = 1, \mathbf{u}_2 = i$, questi nel campo dei reali sono indipendenti[2]. Ma nel campo dei complessi sono dipendenti. Infatti vale $i\mathbf{1} + (-1)\mathbf{i} = \mathbf{0}$.

Ora, dato lo spazio vettoriale E, consideriamo un suo insieme R di vettori indipendenti. Tale insieme avrà un numero di elementi (i vettori che lo compongono), indichiamolo con $r(R)$. Al variare di tutti i possibili gruppi di vettori indipendenti, avremo di volta in

[2] Non esiste una coppia di coefficienti reali che possa annullare la loro combinazione lineare: $a_1\mathbf{1} + a_2\mathbf{i} = \mathbf{0}$

volta diversi numeri di elementi per ciascuno di essi. L'insieme degli $r(R)$ predetti può essere:

- limitato superiormente; in tal caso ha un massimo finito; diciamolo n (3.9)
- non limitato superiormente; in tal caso il massimo tende ad infinito (3.10)

Se $n = max(r(R))$, consideriamo un qualunque insieme R_0 formato da n vettori linearmente indipendenti; ovvero $n = r(R_0)$ [3]. Ora prendiamo un qualunque vettore $\mathbf{v} \in E$ e consideriamo gli $n+1$ vettori $\{\mathbf{v}, R_0\}$: questo insieme è formato da vettori linearmente dipendenti. E si dimostra il seguente teorema:

Teorema 3.2.5. *Se uno spazio vettoriale E su K ammette un sistema di vettori indipendenti di ordine massimo n, indicato con R_0,* ogni *vettore $\mathbf{v} \in E$ si può esprimere* in uno e un sol modo *come combinazione lineare a coefficienti in K dei vettori R_0.*

Questo significa che, se $R_0 = \{\mathbf{e}_1, \mathbf{e}_2, \dots \mathbf{e}_n\}$ possiamo sempre scrivere:

$$\mathbf{v} = v^1\mathbf{e}_1 + v^2\mathbf{e}_2 + \cdots + v^n\mathbf{e}_n \quad v^1, v^2, \dots, v^n \in K \text{ non tutti nulli} \tag{3.11}$$

E il teorema 3.2.5 non solo afferma che vale l'equazione 3.11, oltretutto questa equazione *è unica.*

Si dimostra anche il teorema inverso del 3.2.5:

Teorema 3.2.6. *Se in uno spazio vettoriale E su K ogni vettore $\mathbf{v} \in E$ può essere espresso in modo univoco come combinazione lineare dei vettori $\{\mathbf{e}_1, \mathbf{e}_2, \dots \mathbf{e}_n\}$, i vettori $\{\mathbf{e}_i\}$ sono indipendenti.*

I teoremi esposti ci indicano che un sistema indipendente di ordine massimo R_0 genera per combinazione lineare e in modo univoco tutto lo spazio vettoriale E.

Definizione 3.2.7. *Si chiama **base** di E ogni sistema indipendente capace di generare tutto E.*

Definizione 3.2.8. *Si chiamano **componenti** di (v) nella base $\{\mathbf{e}_i\}$ i coefficenti della combinazione lineare che esprime (v).*

I componenti di un vettore usualmente si indicano con l'indice in apice, e vale l'equazione 3.11, che può essere espressa anche come:

$$\mathbf{v} = \sum_{i=1}^{n} v^i\mathbf{e}_i \tag{3.12}$$

Esempio classico di composizione sono i vettori dello spazio $\mathbb{R}^3$ dove il massimo numero di vettori indipendenti è tre. E ogni vettore nello spazio si può esprimere come:

$$\mathbf{v} = v^1\mathbf{e}_1 + v^2\mathbf{e}_2 + v^3\mathbf{e}_3$$

[3] R_0 è un **sistema indipendente di ordine massimo**.

3.3 dimensione di uno spazio vettoriale

Sintetizzando: la dimensione di uno spazio vettoriale è $n = r(R_0)$. A questa conclusione si arriva dimostrando che tutti i sistemi di vettori indipendenti di uno spazio vettoriale E capaci di generarlo hanno lo stesso numero di elementi, e che tale numero è il numero massimo di vettori indipendenti.

A questa conclusione si arriva utilizzando il seguente **teorema della base**:

Teorema 3.3.1. *Se* $\{\mathbf{e}_1, \mathbf{e}_2, \dots \mathbf{e}_r\}$ *con* $r \leq n$ *è un sistema di vettori indipendenti capace di generare* E*, ogni altro sistema di vettori indipendenti dello stesso ordine* r *a sua volta è capace di generare* E*. L'ordine* r *allora è l'ordine massimo dei sistemi di vettori indipendenti.*

Considerando il teorema 3.2.5 e il precedente teorema della base si arriva alla conclusione che:

Osservazione 3.3.2. un sistema di vettori $\{\mathbf{u}_i\}$ è una **base** se e solo se è un sistema di vettori indipendenti di ordine massimo.

Definizione 3.3.3. *Il numero di elementi di una base di* E *si chiama* ***dimensione dello spazio vettoriale*** E*.*

La dimensione di uno spazio vettoriale E su K si può indicare con $dim_k E$, oppure con $dim E$. Uno spazio vettoriale di dimensione n si può indicare con E_n.

Quando uno spazio vettoriale E su K è dotato di un insieme $r(R)$ non limitato superiormente (si veda 3.10), viene detto di *dimensione non finita*.

3.4 relazioni tra le componenti del vettore somma di più vettori e le componenti dei vettori addendi

Il concetto di base di uno spazio vettoriale è importante. Infatti permette di esprimere un qualunque vettore come somma di componenti. Ciò permette di esprimere le operazioni tra vettori come operazioni aritmetiche sulle loro componenti. Infatti si dimostra in modo immediato la seguente:

Proposizione 3.4.1. dato uno spazio vettoriale E_n,

- le componenti della somma di s vettori si ottengono sommando i corrispondenti componenti degli addendi; ovvero

$$\sum_{\alpha=1}^{s} \mathbf{v}_\alpha = \sum_{\alpha=1}^{s} \sum_{i=1}^{n} v_\alpha^i \mathbf{e}_i = (v_1^1 + v_2^2 + \dots)\mathbf{e}_1 + \dots + (v_1^n + v_2^n + \dots)\mathbf{e}_n$$

- le componenti di un prodotto di un vettore per uno scalare λ si ottiene moltiplicando le componenti del vettore per λ; ovvero

$$\lambda \mathbf{v} = \lambda \left(\sum_{i=1}^{n} v^i \mathbf{e}_i \right) = \lambda(v^1 \mathbf{e}_1) + \dots + \lambda(v^n \mathbf{e}_n)$$

A causa delle proprietà predette, le componenti di un vettore combinazione lineare di s vettori sono le combinazioni lineari delle analoghe componenti degli s vettori. In tal modo è possibile esprimere la dipendenza, o indipendenza, lineare in base a quella delle componenti.

Teorema 3.4.2. *Dato uno spazio vettoriale E_n di dimensione n, condizione necessaria e sufficiente affinché i vettori $\mathbf{v}_1, \mathbf{v}_2, \dots \mathbf{v}_r$, siano linearmente indipendenti (con $r \leq n$ perché per $r > n$ i vettori sono di certo dipendenti) è che sia r il rango della matrice*[4] *formata con le componenti dei vettori di una base:*

$$\begin{vmatrix} v_1^1 & v_2^1 & \dots & v_r^1 \\ v_1^2 & v_2^2 & \dots & v_r^2 \\ \vdots & \vdots & \vdots & \vdots \\ v_1^n & v_2^n & \dots & v_r^n \end{vmatrix}$$

3.5 sottospazi vettoriali

È interessante osservare che si possono considerare sottoinsiemi di uno spazio vettoriale, che si comportano in modo analogo ad esso rispetto le operazioni che lo definiscono. Perciò abbiamo la seguente:

Definizione 3.5.1. *Un sottoinsieme W non vuoto di uno spazio vettoriale E su K, si dice* ***sottospazio vettoriale*** *di E, se a sua volta è uno spazio vettoriale su K rispetto le operazioni che definiscono E come spazio vettoriale.*

E si dimostra la seguente:

Proposizione 3.5.2. Condizione necessaria e sufficiente affinché W sia un sottospazio vettoriale di E è che:

$$\mathbf{u}, \mathbf{v} \in W \Rightarrow a\mathbf{u} + b\mathbf{v} \in W \qquad \forall a, b \in K \tag{3.13}$$

Notiamo che se E è uno spazio vettoriale, il sottoinsieme formato dal vettore nullo $\{\mathbf{0}\}$ è un suo sottospazio vettoriale. Analogamente, possiamo considerare E come sottospazio di se stesso.

Altro:

Esempio 3.5.3. dato un qualunque vettore $\mathbf{x} \neq \mathbf{0}$ di uno spazio vettoriale E, l'insieme $\{\lambda\mathbf{x} \text{ con } \lambda \in K\}$ [5] è un sottospazio vettoriale di E.

E si può dimostrare anche la seguente:

Proposizione 3.5.4. se W_1 e W_2 sono sottospazi di E, lo è anche $W_1 \cap W_2$.

La proposizione precedente si può estendere a più di due sottospazi vettoriali.

[4] Ricordiamo che il rango di una matrice è il massimo numero di righe (o colonne) linearmente indipendenti.

[5] Ovvero l'insieme di tutti i vettori prodotti di $\mathbf{x}$ per uno scalare.

3.6 sottospazi generati da r vettori indipendenti

Il concetto di sottospazio vettoriale si applica in particolare quando si ha a che fare con sistemi di vettori indipendenti. Si dimostra la seguente:

Proposizione 3.6.1. Se $\mathbf{v}_1, \mathbf{v}_2, \dots \mathbf{v}_r$, con $r \leq n$, è un *sistema di vettori indipendenti* di E, allora l'insieme generato come combinazione lineare dei vettori $\{\mathbf{v}_i\}(i = 1, 2, \dots r)$ è un sottospazio vettoriale di E, di dimensione r.

In questo caso i vettori $\{\mathbf{v}_i\}$ sono una base del sottospazio S generato. Questo per definizione di S visto che è una combinazione lineare dei $\{\mathbf{v}_i\}$ e che questi sono linearmente indipendenti.

Osservazione 3.6.2. Lo spazio vettoriale S generato dai $\{\mathbf{v}_i\}$ è il più piccolo sottospazio che li contiene e viene detto **inviluppo lineare** generato dal sistema dei $\{\mathbf{v}_i\}$.
Si può indicare con: $[\mathbf{v}_1, \mathbf{v}_2, \dots \mathbf{v}_r]$.

Quanto detto sulla possibilità di utilizzare un sistema di vettori indipendenti per generare un sottospazio vettoriale, conduce alla dimostrazione del seguente **teorema del completamento della base**:

Teorema 3.6.3. *Dato E_n spazio vettoriale di dimensione n e $\{\boldsymbol{v}_i\}$ r vettori di E_n linearmente indipendenti. Allora esistono $n-r$ vettori $\boldsymbol{v}_{r+1}, \boldsymbol{v}_{r+2}, \dots \boldsymbol{v}_n$ tali che il sistema di vettori $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_r, \boldsymbol{v}_{r+1}, \dots \boldsymbol{v}_n\}$ sia una base di E_n.*

3.7 somme di due spazi vettoriali

Consideriamo ora due sottospazi di E. Diciamoli V e W. Possiamo definire la loro *somma* come segue:

Definizione 3.7.1. *La **somma di due sottospazi vettoriali** V e W, è il sottospazio $V + W$ di E ottenuto tramite tutte le possibili somme* $\mathbf{v} + \mathbf{w} \quad \forall \mathbf{v} \in V \quad \forall \mathbf{w} \in W$.

Si dimostra facilmente che una somma come quella definita in 3.7.1 è effettivamente un sottospazio vettoriale di E.
Inoltre è intuitivo il fatto che $V + W$ è il sottospazio vettoriale di E più piccolo che contiene sia V che W.
Ancora: la somma di sottospazi definita in 3.7.1 è commutativa e associativa.

Si definisce *somma diretta* una somma con le seguenti proprietà:

Definizione 3.7.2. *U si dice **somma diretta** dei sottospazi vettoriali V e W di E se valgono:*

$$V + W = U$$
$$V \cap W = \{\mathbf{0}\}$$

Usualmente si scrive: $U = V \oplus W$.

Esiste il seguente:

Teorema 3.7.3. *Sia U un sottospazio somma dei sottospazi V e W. Ogni elemento $\mathbf{u} \in U$ si decompone* in modo univoco *nella somma $\mathbf{u} = \mathbf{v}+\mathbf{w}$* se e solo se *vale $U = V \oplus W$*

Se la somma diretta di due sottospazi rende lo spazio d'origine, allora abbiamo la definizione di *sottospazi supplementari*:

Definizione 3.7.4. *Due sottospazi V e W di E si dicono **supplementari** in E se E è la loro somma diretta: $E = V \oplus W$.*

E, nella migliore tradizione, un (o più) sottospazio supplementare non si nega a nessuno! Si dimostra:

Teorema 3.7.5. *Ogni sottospazio vettoriale U di E, possiede in E uno spazio vettoriale supplementare W, generalmente non univocamente determinato. Vale:*

$$dim(W) = dim(E) - dim(U) \tag{3.14}$$

E, continuando a parlare di dimensioni, abbiamo:

Teorema 3.7.6. *Dato lo spazio vettoriale E, con V e W suoi sottospazi di dimensioni finite, vale: $dim(V + W) = dim(V) + dim(W) - dim(V \cap W)$* [6].

Volendoci allargare, possiamo considerare la possibilità di avere più spazi vettoriali $V_1, V_2, \ldots V_m$ tutti definiti sullo stesso campo K.

Facciamo il prodotto cartesiano di questi vettori: $V = V_1 \times V_2 \times \ldots V_m$ e diamo una struttura a V definendo

- la somma di elementi come:

$$(a_1, \ldots a_m) + (b_1, \ldots b_m) = a_1 + b_1, \ldots a_m + b_m \text{ dove } a_1, b_1 \in V_1, \ldots a_m, b_m \in V_m$$

- il prodotto per uno scalare come:

$$k(a_1, \ldots a_m) = ka_1, \ldots ka_m \text{ dove } a_1 \in V_1, \ldots a_m \in V_m,\ k \in K$$

[6] Intuitivamente: quando sommo le dimensioni dei due sottospazi, la dimensione della loro intersezione conta due volte: ne devo sottrarre una. Attenzione: questa non è una dimostrazione.

In queste condizioni si dimostra che esistono sottospazi di V isomorfi ai $\{V_i\}$, arrivando così a giustificare l'equazione:

$$V = V_1 \oplus V_2 \oplus \dots V_m$$

In pratica è possibile strutturare il prodotto cartesiano di spazi vettoriali diversi, facendo sì che a sua volta sia uno spazio vettoriale, purché i diversi spazi abbiano in comune il campo K.

3.8 cambiamenti di base in E_n. legge di trasformazione delle componenti di un vettore

È possibile definire basi diverse in relazione allo stesso spazio vettoriale E_n di dimensione n. Ad esempio possiamo utilizzare due diversi sistemi linearmente indipendenti: $\{\mathbf{e}_i\}$ ed $\{\mathbf{e'}_i\}$.

Sappiamo che qualunque vettore $\mathbf{v} \in E$ può essere rappresentato come combinazione lineare di ciascuna delle basi:

$$\mathbf{v} = a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + \dots a_n\mathbf{e}_n \tag{3.15}$$

$$\mathbf{v} = b_1\mathbf{e'}_1 + b_2\mathbf{e'}_2 + \dots b_n\mathbf{e'}_n \tag{3.16}$$

Ci possiamo chiedere che relazione vi sia tra le componenti delle combinazioni lineari precedenti. E se sia possibile, fissate le due basi, calcolare un gruppo di componenti per una base obiettivo a partire da quelle di una base d'origine. Ad esempio, conosciute le a_i, calcolare le b_i.

Le risposte a queste domande esistono: è possibile relazionare le basi in questione tramite matrici, dette **matrici di cambiamento di base**.

Si dimostra che le due matrici per passare da una base all'altra sono l'una l'inverso dell'altra. E utilizzando il calcolo matriciale è possibile esprimere il passaggio da una base all'altra tramite equazioni semplici.

In particolare se esprimiamo le componenti del vettore $\mathbf{v}$ in base $\{\mathbf{e}_i\}$ come matrice colonna $X = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$, mentre se le sue componenti in base $\{\mathbf{e'}_i\}$ sono espresse come $X' = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$, allora abbiamo:

$$X = A_{n\times n} \cdot X' \tag{3.17}$$

dove la matrice $A_{n\times n}$ è la matrice di passaggio tra basi, e l'operatore $(\cdot)$ è il prodotto riga per colonna tra matrici.

Se noi conosciamo le componenti b_i che formano la colonna X', la matrice $A_{n\times n}$ ci permette di calcolare i valori della colonna X, ovvero le componenti di $\mathbf{v}$ secondo la base $\{\mathbf{e}_i\}$.

Esiste l'equazione inversa della 3.17:

$$X' = A^{-1}_{n\times n} \cdot X \tag{3.18}$$

Per evitare di perdere una congrua quantità dello scarso numero di lettori di questo testo, ci fermiamo qui, evitando di addentrarci nel calcolo matriciale che permette di dimostrare le equazioni 3.17 e 3.18.

Chi è interessato all'argomento, anche per capire come si calcolano le matrici di cambiamento di base, può leggere la spiegazione presentata sul sito web YouMath [Youmath 2022].

3.9 ripassando

La figura 3.1 ci introduce alla sintesi di questo capitolo.

In alto a sinistra abbiamo gli *ingredienti di base* per costruire uno spazio vettoriale: un gruppo abeliano E e un campo K. Associandovi una legge di composizione esterna da $K \times E$ ad E con la contemporanea validità delle proprietà distributive rispetto le somme di entrambi i gruppi, la proprietà associativa e la neutralità rispetto l'unità del prodotto del campo, possiamo dire di avere uno spazio vettoriale E su K. In questo ambito, gli elementi di E si chiamano *vettori*, e, usualmente si indicano con una lettera minuscola in grassetto. Ad es. $\mathbf{v}$.

Dopo di che, a sinistra, scendendo di un livello, incontriamo i fondamentali concetti di (in)dipendenza lineare. Cioè, presi n vettori $\mathbf{v}_i$ possiamo trovare, oppure no, altrettanti elementi in K per i quali valga $\sum_{i=1}^{n} a_i\mathbf{v}_i = 0$. Se esistono degli a_i in grado di soddisfare la precedente equazione, diciamo che i vettori $\mathbf{v}_i$ sono *linearmente dipendenti*. In caso contrario sono *linearmente indipendenti*. Un insieme di vettori linearmente indipendenti è detto *sistema indipendente* e di solito si indica con R.

Perché la (in)dipendenza è importante? Perché studiando gli R [7] possiamo capire se esiste, oppure no, un n finito di grandezza massima. In caso affermativo abbiamo dei sistemi indipendenti R_0 di ordine massimo[8]. Li diciamo *base di* E perché si dimostra che per il loro tramite è possibile rappresentare un qualunque vettore di E come una *unica*[9] combinazione lineare. Chiamiamo *componenti di* $\mathbf{v}$ *nella base* R_0 i coefficienti di una tale combinazione lineare.

È interessante il fatto che se possiamo esprimere dei vettori $\mathbf{v}_i$ come combinazioni lineari di R_0, allora possiamo calcolare la loro somma facendo la somma delle loro componenti. Analogamente per il prodotto per uno scalare, lo possiamo calcolare facendo il prodotto delle loro componenti.

Inoltre, consideriamo due diverse basi, allora possiamo calcolare una matrice di cambiamento di base $A_{n\times n}$, che, tramite un prodotto matriciale riga per colonna, ci permette

[7] Ce ne saranno più di uno, con n diversi.

[8] Se non dovesse esistere un tale n finito, diciamo che la dimensione dello spazio vettoriale E non è finita. Questo è un caso di studio che abbiamo ignorato.

[9] Unica, nel senso che un vettore $\mathbf{v}$ ha un solo modo di essere rappresentato rispetto una base R_0 fissata. Se cambia la base, cambia la rappresentazione di $\mathbf{v}$.

di ottenere le componenti $X = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}$ di un vettore in una base, quando conosciamo le componenti $X' = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}$ nell'altra base.

Tornando in cima al nostro diagramma, dopo i concetti di (in)dipendenza lineare, possiamo considerare un sottoinsieme di E. Se questo, rispetto le stesse operazioni che definiscono lo spazio vettoriale E, mostra le stesse proprietà, allora possiamo parlare di un sottospazio vettoriale di E.

Se E ammette due sottospazi vettoriali, possiamo definire la loro somma e dimostrare che è a sua volta un sottospazio vettoriale di E.

Se i due sottospazi vettoriali sono disgiunti, la loro somma si dice *somma diretta*. E se la somma diretta è lo spazio d'origine, allora i due sottospazi sono *supplementari*.

Torniamo in cima al grafo un'ultima volta, per considerare la possibilità di fare il prodotto cartesiano di più spazi vettoriali. Otterremo un ulteriore spazio vettoriale.

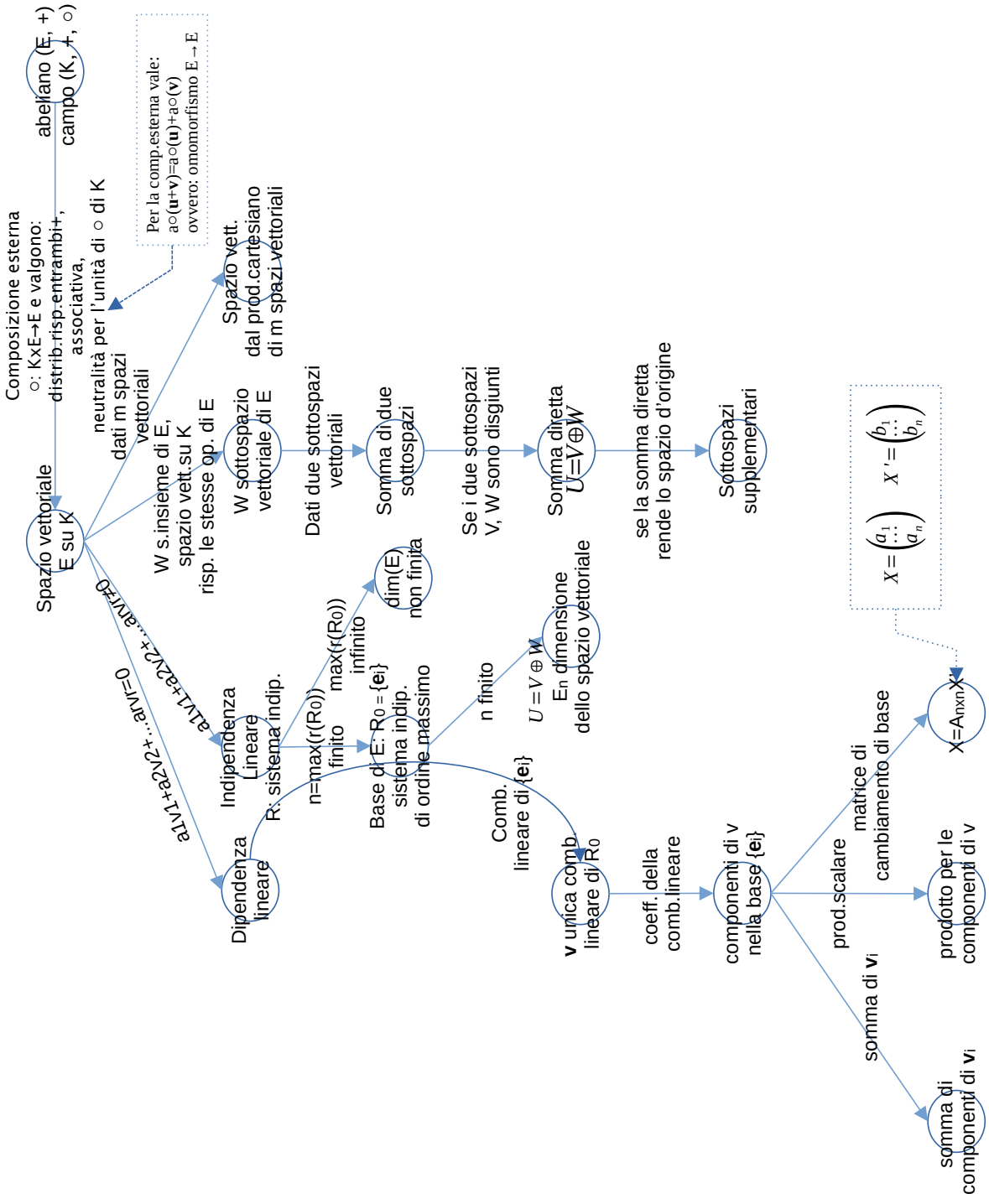


Figura 3.1: Ripassando: spazi vettoriali

Capitolo 4

Applicazioni lineari tra spazi vettoriali

Quindi ora sappiamo che uno spazio vettoriale è un gruppo abeliano E e un campo K, cui aggiungiamo una composizione esterna $K \times E \to E$ che soddisfa la manciata di proprietà 3.2.

Se prendiamo due di questi spazi, diciamo E ed F, sullo stesso campo K, possiamo considerare una applicazione da E ad F.

4.1 applicazioni lineari

Tra le possibili applicazioni sono particolarmente interessanti le applicazioni lineari.

Definizione 4.1.1. *Se E ed F sono due spazi vettoriali sullo stesso campo K, una* ***applicazione lineare*** *$L : E \to F$ è tale se $\forall \mathbf{x}, \mathbf{y} \in E, a \in K$ valgono:*

$$L(\mathbf{x} + \mathbf{y}) = L(\mathbf{x}) + L(\mathbf{y}) \qquad \textit{additività} \tag{4.1}$$

$$L(a\mathbf{x}) = aL(\mathbf{x}) \qquad \textit{omogeneità} \tag{4.2}$$

Le equazioni della precedente definizione si possono sintetizzare con la seguente equazione equivalente:

$$L(a\mathbf{x} + b\mathbf{y}) = aL(\mathbf{x}) + bL(\mathbf{y}) \quad \text{(propr. di sovrapposizione)} \tag{4.3}$$

Inoltre possiamo considerare una applicazione $L : E \to E$. In tal caso si dice che l'applicazione è una *trasformazione*[1].

Esempi elementari di applicazioni lineari possono essere i seguenti.

Esempio 4.1.2. L'operatore *nullo* O che associa il vettore nullo ad ogni vettore di E: $O(\mathbf{v}) = \mathbf{0} \quad \forall \mathbf{v} \in E$.

[1] O anche un *operatore*. Sono sinonimi.

Infatti: $O(a\mathbf{x}+b\mathbf{y}) = aO(\mathbf{x}) + bO(\mathbf{y}) = a\mathbf{0} + b\mathbf{0} = \mathbf{0}$

Esempio 4.1.3. L'operatore *identico* I che lascia inalterato il vettore cui viene applicato: $I(\mathbf{v}) = \mathbf{v} \quad \forall \mathbf{v} \in E$.

In questo caso: $I(a\mathbf{x}+b\mathbf{y}) = aI(\mathbf{x}) + bI(\mathbf{y}) = a\mathbf{x} + b\mathbf{y}$.

Premesso che l'insieme dei polinomi di grado $\leq n$ definisce uno spazio vettoriale ad es. sul campo dei numeri reali $\mathbb{R}$ [2]. Possiamo impostare un esempio più elaborato come segue.

Esempio 4.1.4. Detto $P(x)$ lo spazio vettoriale dei polinomi di grado $\leq n$, l'operatore di *derivazione* definisce una applicazione lineare.

Infatti per le proprietà di derivazione valgono le equazioni 4.1 e 4.2:

$$\frac{d}{dx}(P_1(x) + P_2(x)) = \frac{d}{dx}(P_1(x)) + \frac{d}{dx}(P_2(x))$$
$$\frac{d}{dx}(\lambda P(x)) = \lambda \frac{d}{dx}(P(x)) \quad \forall \lambda \in K$$

Data una applicazione lineare si dimostra la seguente.

Proposizione 4.1.5. Se $L : E \to F$ è una applicazione lineare valgono:

$$L(\mathbf{0}_E) = \mathbf{0}_F \tag{4.4}$$
$$L(-\mathbf{x}) = -L(\mathbf{x}) \tag{4.5}$$

4.2 omomorfismi e isomorfismi tra spazi vettoriali

Definizione 4.2.1. *Una applicazione lineare tra gli spazi vettoriali E e F è un* omomorfismo tra gli spazi vettoriali E e F.

Infatti una applicazione lineare come definita in 4.1.1 è compatibile con la definizione di omomorfismo 2.6.1 per i gruppi.

Definizione 4.2.2. *Definiamo **isomorfismo** tra gli spazi vettoriali E e F una applicazione lineare biiettiva.*

Possiamo vedere due spazi vettoriali isomorfi come realizzazioni diverse della stessa struttura algebrica. Infatti, quanto dimostrato per uno spazio vettoriale, vale anche per l'altro, a condizione che la dimostrazione utilizzi solo le nozioni basate sulle operazioni della struttura in analisi.

Un esempio semplice di isomorfismo è l'operazione di *omotetia*:

[2] Dove l'operatore somma è la somma tra polinomi, e il prodotto per uno scalare è il prodotto di un polinomio per un numero reale.

Esempio 4.2.3. Dato lo spazio vettoriale E e uno scalare fisso non nullo λ, la seguente applicazione è un isomorfismo:

$$\begin{aligned} L : E &\to E \\ \mathbf{v} &\mapsto \lambda\mathbf{v} \end{aligned}$$

Per un esempio più elaborato consideriamo lo spazio vettoriale $P(t)$ dei polinomi di grado $\leq n$ con coefficienti reali:

Esempio 4.2.4. l'applicazione che associa al generico polinomio $p(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0$ la tupla $(a_n, a_{n-1}, \ldots a_0)$, è un isomorfismo. Formalmente:

$$\begin{aligned} L : P_n[t] &\to R^{n+1} \\ p(t) &\mapsto (a_n, \ldots a_0) \end{aligned}$$

Quanto esemplificato in 4.2.4 può essere generalizzato nel seguente teorema:

Teorema 4.2.5. *Tutti gli spazi vettoriali su K con la stessa dimensione, sono isomorfismi tra loro.*

La dimostrazione del teorema 4.2.5 utilizza la combinazione lineare dei vettori in E e F (si veda l'equazione 3.11), definendo due basi, rispettivamente in E e in F. Da ciò si capisce che il teorema predetto è legato alla scelta delle basi in questione: si dice che *non è canonico*. Ovvero non è indipendente dalla scelta di un riferimento.

4.3 immagine, rango, nucleo di una applicazione lineare

Visto che le applicazioni lineari tra spazi vettoriali sono omomorfismi, valgono alcuni teoremi e definizioni già viste per gli omomorfismi tra gruppi.

Teorema 4.3.1. *Se $L : E \to F$ è una applicazione lineare tra gli spazi vettoriali indicati, entrambi sullo stesso campo K, allora l'immagine $L(E)$ è un sottospazio vettoriale di F.*

Definizione 4.3.2. *Si chiama **rango** di una applicazione lineare L, la dimensione della sua immagine $L(E)$.*

Definizione 4.3.3. *Data una applicazione lineare $L : E \to F$, l'insieme degli elementi $\mathbf{x} \in E | L(\mathbf{x}) = \mathbf{0}_F$ si chiama **kernel**[3] di L. E si indica $Ker(L)$.*

Si dimostra che:

Teorema 4.3.4. *Il kernel di una applicazione lineare $L : E \to F$ è un sottospazio vettoriale di E.*

E si definisce:

[3] O **nucleo**.

Definizione 4.3.5. *Si chiama* ***nullità*** *di una applicazione lineare* $L : E \to F$*, la dimensione del suo kernel. Si indica con* $N(L)$*.*

Si dimostra il seguente teorema:

Teorema 4.3.6. *Un omomorfismo suriettivo* $L : E \to F$ *è un isomorfismo* se e solo se *il suo kernel è composto dal solo zero di* E*:* $Ker(L) = \{\mathbf{0}_E\}$*.*

Il precedente teorema può essere utilizzato per dimostrare che due spazi vettoriali sono isomorfi. Basta definire un omomorfismo suriettivo $L : E \to F$ tra gli spazi vettoriali in analisi, per poi dimostrare che $Ker(L) = \{\mathbf{0}_E\}$.

Inoltre vale anche il seguente teorema, inverso del 4.2.5:

Teorema 4.3.7. *Due spazi vettoriali isomorfi hanno la stessa dimensione.*

I teoremi 4.2.5 e 4.3.7 si possono riunire nel seguente:

Teorema 4.3.8. *C.n.s. perché due spazi vettoriali siano isomorfi è che abbiano la stessa dimensione.*

Un esempio che dimostra la mancanza di isomorfismo è una proiezione che cambi il numero di dimensioni, come la seguente:

$$\begin{aligned} P : \mathbb{R}^2 &\to \mathbb{R} \\ (x, y) &\mapsto x \end{aligned}$$

Infatti il kernel di P è formato da tutti i vettori $(x, y) \mid x = 0, \forall y \in \mathbb{R}$ [4]. Visto che il kernel di L è diverso dal solo elemento $(0, 0)$ [5], per il teorema 4.3.6 possiamo affermare che in questo esempio non abbiamo un isomorfismo. Inoltre, per il teorema 4.3.8, deduciamo le dimensioni dei due spazi vettoriali sono diverse.

Il precedente teorema porta anche al seguente corollario:

Teorema 4.3.9. *Dato un isomorfismo* $L : E \to F$ *e un sottospazio vettoriale* U *di* E*, allora* L *è un isomorfismo tra* U *e* $L(U)$*.*

E si dimostra anche il seguente teorema:

Teorema 4.3.10 (dell'omomorfismo)**.** *Se* $L : E \to F$ *è un omomorfismo, lo spazio vettoriale immagine* $L(E)$ *è isomorfo rispetto ogni sottospazio vettoriale supplementare di* $Ker(L)$ *in* E*.*

Cosa vuol dire? Che, ad esempio, se sottraiamo a E il kernel di L, abbiamo un sottospazio vettoriale supplementare (si veda la definizione 3.7.4). Il sottospazio così ottenuto è isomorfo con $L(E)$.

Come conseguenza del teorema precedente abbiamo:

[4] Ovvero $x = 0$ e y qualunque numero reale.

[5] Che è lo zero di $\mathbb{R}^2$.

Teorema 4.3.11. *Se $dim(E) = n$, e abbiamo l'applicazione lineare $L : E \to F$, la somma delle dimensioni della sua immagine e di quella del suo kernel, uguagliano n:*

$$dim(E) = dim(L(E)) + dim(Ker(L)) \tag{4.6}$$

Infatti per il teorema 4.3.10 abbiamo $L(E)$ isomorfa con U supplementare di $Ker(L)$. Ma, se sono isomorfi hanno la stessa dimensione[6]. E siccome $dim(E) = dim(U) + dim(Ker(L))$ [7], allora abbiamo la 4.6.

Dobbiamo fare attenzione al fatto che, se l'applicazione lineare è un *operatore*, ovvero $E \equiv F$, non è detto che $L(E)$ sia uno spazio supplementare di $Ker(L)$. Ma in ogni caso la equazione 4.6 è valida.

4.4 spazio vettoriale quoziente

Ipotizziamo che lo spazio vettoriale E abbia un sottospazio vettoriale W. Definiamo il concetto di *congruenza* come segue:

Definizione 4.4.1. *dati due vettori $\mathbf{u}, \mathbf{v} \in E$, diciamo che sono* ***congruenti, modulo*** *W,* se e solo se *vale $\mathbf{u} - \mathbf{v} \in W$. Si scrive:*

$$\mathbf{u} \equiv \mathbf{v} \pmod{W}$$

Vettori congruenti modulo W

Questa definizione è una estensione dell'aritmetica modulo n agli elementi di uno spazio vettoriale.

Infatti nell'aritmetica modulo n (si veda il riferimento [Wikipedia 2022]) due numeri interi $n1, n2$ sono congruenti modulo n, se esiste un intero k tale che valga $n1 - n2 = k\ n$. Ovvero n è un divisore della loro differenza.

Persino noi riusciamo ad utilizzare questa definizione per *agganciare* quella di spazio vettoriale. Basta considerare l'insieme degli interi $\mathbb{Z}$. Fissato un $n > 1 \in N$, prendiamo il sottospazio $W = \{w | w = k\ n, \forall k \in \mathbb{Z}\}$. A questo punto, se $n1, n2 \in \mathbb{Z}$ e $n1 - n2 \in W$, possiamo dire che $n1$ e $n2$ sono congruenti.

La relazione di congruenza è una relazione di equivalenza, perché valgono le proprietà riflessiva, simmetrica e transitiva. Ovvero:

$$\mathbf{u} \equiv \mathbf{u}\ (mod\ W) \tag{4.7}$$

$$\mathbf{u} \equiv \mathbf{v}\ (mod\ W) \Rightarrow \mathbf{v} \equiv \mathbf{u}\ (mod\ W) \tag{4.8}$$

$$\mathbf{u} \equiv \mathbf{v}\ (mod\ W), \mathbf{v} \equiv \mathbf{z}\ (mod\ W) \Rightarrow \mathbf{u} \equiv \mathbf{z}\ (mod\ W) \tag{4.9}$$

[6] Teorema 4.3.7.

[7] Ricordiamo la equazione 3.14.

Congruenza come relazione di equivalenza

La proprietà riflessiva (equazione 4.7) si spiega con $\mathbf{u} - \mathbf{u} = \mathbf{0}$. Siccome W è uno spazio vettoriale, deve avere l'elemento neutro $\mathbf{0}$. Quindi $\mathbf{u} - \mathbf{u} \in W$.

La proprietà simmetrica (equazione 4.8) la ricaviamo dalla commutatività della somma tra vettori: $\mathbf{u} + (-\mathbf{v}) = (-\mathbf{v}) + \mathbf{u}$.

La proprietà transitiva (equazione 4.9) può essere spiegata considerando valide le seguenti: $\mathbf{u} - \mathbf{v} = \mathbf{w}_1$ con $\mathbf{w}_1 \in W$ e $\mathbf{v} - \mathbf{z} = \mathbf{w}_2$ con $\mathbf{w}_2 \in W$. Allora, sostituendo la $\mathbf{z} = \mathbf{v} - \mathbf{w}_2$, possiamo scrivere:
$\mathbf{u} - \mathbf{z} = \mathbf{u} - (\mathbf{v} - \mathbf{w}_2) = \mathbf{u} - \mathbf{v} + \mathbf{w}_2 = \mathbf{w}_1 + \mathbf{w}_2$. Ma abbiamo la chiusura dell'operazione di somma, quindi vale: $\mathbf{w}_1 + \mathbf{w}_2 \in W$.

Visto che la congruenza è una relazione di equivalenza, definisce una partizione dello spazio vettoriale E [8] in classi di equivalenza (teorema 1.4.6). Queste classi sono dette *classi laterali*.

Indicato un vettore $\mathbf{x}$, questo individuerà la classe di equivalenza cui appartiene: $[\mathbf{x}] = \{\mathbf{x} + \mathbf{w} | \mathbf{w} \in W\}$. Infatti al variare di $\mathbf{w}$ in W, l'espressione $\mathbf{w} - \mathbf{x}$ individua tutti gli elementi nella classe $[\mathbf{x}]$.

Ancora. Nella sezione 1.5 abbiamo visto che possiamo utilizzare le classi di equivalenza per ottenere un insieme quoziente. In questo caso indichiamo con E/W l'insieme quoziente di E rispetto la relazione di congruenza definita da W. Il seguente teorema ci dice che E/W può avere una struttura di spazio vettoriale:

Teorema 4.4.2. *Dato lo spazio vettoria E e il suo sottospazio W, il quoziente E/W è uno spazio vettoriale definendo le operazioni di somma e di prodotto per uno scalare come segue:*

$$[\mathbf{u}] + [\mathbf{v}] = [\mathbf{u} + \mathbf{v}] \quad \forall \mathbf{u}, \mathbf{x} \in E \tag{4.10}$$

$$\lambda[\mathbf{u}] = [\lambda \mathbf{u}] \quad \forall \lambda \in K, \mathbf{u} \in E \tag{4.11}$$

In più:

Teorema 4.4.3. *Se vale $E = U \oplus W$, lo spazio vettoriale E/W è isomorfo ad U.*

Data l'applicazione lineare L, assumendo $W \equiv Ker(L)$, il teorema 4.4.3 ci permette di enunciare in modo diverso, ma equivalente, il teorema 4.3.10:

Teorema 4.4.4 (dell'omomorfismo)**.** *Con L omomorfismo suriettivo dello spazio vettoriale E sullo spazio vettoriale F, allora F è isomorfo allo spazio vettoriale $E/Ker(L)$.*

La figura 4.1 illustra il diagramma commutativo che scaturisce dal teorema 4.4.4. Questo diagramma è analogo a quello illustrato dalla figura 1.17 per gli insiemi.

[8] Si noti. Gli elementi $\mathbf{u}$ e $\mathbf{v}$ appartengono ad E, oltre che al sottospazio W. Questo ci permette di parlare di equivalenza nello spazio vettoriale E, tramite il sottospazio W che definisce la relazione di nostro interesse: la congruenza.

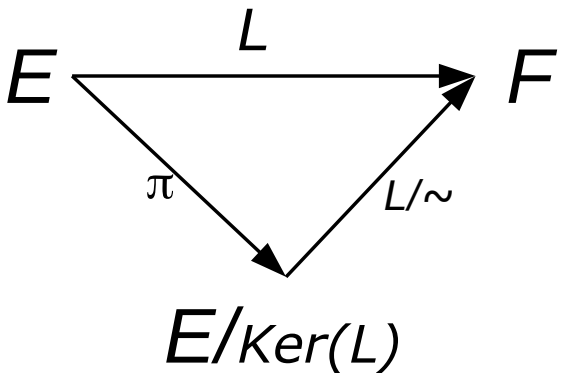


Figura 4.1: Diagramma commutativo di applicazioni lineari con $E/Ker(L)$

Per capire meglio. Si consideri un elemento $\mathbf{b} \in L(E)$. La variabile indipendente che lo genera sia $\mathbf{x} : L(\mathbf{x}) = \mathbf{b}$. Se abbiamo usato il sottospazio $Ker(L)$, la classa laterale di $\mathbf{x}$ è $\mathbf{x} + Ker(L)$. In questo caso vale: $L(\mathbf{x} + Ker(L)) = L(\mathbf{x}) + \mathbf{0}_F = \mathbf{b}$. Cioè tutti i valori di E che generano $\mathbf{b}$ sono nella classe laterale $[\mathbf{x}] = \mathbf{x} + Ker(L)$.

4.5 spazio vettoriale delle applicazioni lineari di E in F

Dati due spazi vettoriali E e F, entrambi su K. Possiamo considerare tutte le possibili applicazioni lineari tra i due spazi vettoriali in questione. Indichiamo questo insieme come $Hom(E, F)$ [9].

In $Hom(E, F)$ possiamo definire due operazioni: un somma interna e un prodotto per uno scalare esterno dando luogo ad una struttura vettoriale. In particolare:

1. Diciamo L_1, L_2 due applicazioni lineari, elementi di $Hom(E, F)$. La loro somma definita come segue è a sua volta un elemento di $Hom(E, F)$

$$(L_1 + L_2) : \mathbf{v} \mapsto L_1(\mathbf{v}) + L_2(\mathbf{v}) \quad \forall \mathbf{v} \in E \tag{4.12}$$

Infatti la somma 4.12 è un omomorfismo di E in F perché la definizione ci dà:

$$(L1_1 + L_2)(a\mathbf{v_1} + b\mathbf{v_2}) = L_1(a\mathbf{v_1} + b\mathbf{v_2}) + L_2(a\mathbf{v_1} + b\mathbf{v_2}) \tag{4.13}$$

che è la proprietà di sovrapposizione 4.3 delle applicazioni lineari.
Ma, essendo $L_1, L_2 \in Hom(E, F)$ possiamo riscriverla come segue:

$$\begin{aligned}
&(L_1 + L_2)(a\mathbf{v_1} + b\mathbf{v_2}) = \\
&L_1(a\mathbf{v_1} + b\mathbf{v_2}) + L_2(a\mathbf{v_1} + b\mathbf{v_2}) = \\
&aL_1(\mathbf{v_1}) + bL_1(\mathbf{v_2}) + aL_2(\mathbf{v_1}) + bL_2(\mathbf{v_2}) = \\
&a(L_1 + L_2)\mathbf{v_1} + b(L_1 + L_2)\mathbf{v_2} \qquad\qquad \forall \mathbf{v_1}, \mathbf{v_2} \in E \quad a, b \in K
\end{aligned}$$

[9] *Hom* è l'iniziale del termine inglese *homomorphism*.

che è la definizione di omomorfismo per l'applicazione $L_1 + L_2$.

2. La composizione esterna, lineare, la possiamo definire come segue:

$$(aL) : \mathbf{v} \mapsto aL(\mathbf{v}) \quad \forall \mathbf{v} \in E, a \in K \tag{4.14}$$

3. Per l'elemento neutro di $Hom(E, F)$, consideriamo l'applicazione (costante) che ad ogni $\mathbf{v}$ fa corrispondere lo zero: $\mathbf{0}_F \in F$.
4. Come applicazione opposta dell'applicazione L, quella che ad ogni $\mathbf{v} \in E$ associa il vettore opposto di $L(\mathbf{v}) \in F$

Con le definizioni predette, $Hom(E, F)$ è uno spazio vettoriale su K.

Le applicazioni lineari potrebbero avere lo spazio vettoriale E sia come dominio che come codominio. Ovvero $F \equiv E$. In tal caso le applicazioni L vengono nominate **operatori lineari**[10]. E il loro insieme è indicato con $End(E)$, invece di $Hom(E, E)$.

Un altro caso particolare lo abbiamo se $F \equiv K$. In questo caso $Hom(E, K)$ viene nominato **spazio duale di** E. Si indica con E^*. E le applicazioni si dicono **forme lineari**[11].

4.6 relazioni tra applicazioni lineari e matrici

Qui affrontiamo un argomento particolarmente rilevante. Infatti si dimostra il seguente:

Teorema 4.6.1. *Dati gli spazi vettoriali E_n e F_m sullo stesso campo K. Fissata una base $\{\mathbf{e}_i\}$ $i = 1, 2 \dots n$ di E_n, un omomorfismo $L : E_n \to F_m$ è determinato univocamente dalla trasformazione degli n elementi della base $\{\mathbf{e}_i\}$.*
Ancora. Fissata una base $\{\mathbf{f}_\alpha\}$ $\alpha = 1, 2 \dots m$ di F_m, l'omomorfismo L è rappresentato univocamente da una matrice $m \times n$ a coefficienti in K.
Viceversa. Una matrice $m \times n$, fissate le basi in E_n e F_m, individua un omomorfismo $L : E_n \to F_M$.

La dimostrazione della prima affermazione del teorema 4.6.1 è semplice. Basta osservare che un qualunque vettore $\mathbf{x} \in E_n$ si esprime come $\mathbf{x} = \sum_{i=1}^{n} x_i \mathbf{e}_i$. Siccome L è lineare, allora vale:

$$L(\mathbf{x}) = \sum_{i=1}^{n} x_i L(\mathbf{e}_i) \tag{4.15}$$

Quindi la trasformazione tramite L di un qualunque vettore di E_n dipende dalla trasformazione operata da L sugli elementi della base $\{\mathbf{e}_i\}$ di E_n.

Il prosieguo della dimostrazione è meno semplice. Ma cerchiamo di capirlo perché ci condurrà ad una conclusione fondamentale.

Nell'equazione 4.15 è centrale il termine $L(\mathbf{e}_i)$ che rappresenta la trasformazione della base i-esima. Consideriamo questi vettori di F:

$$\boldsymbol{\varepsilon}_i = L(\mathbf{e}_i) \quad i = 1, 2, \dots n \tag{4.16}$$

[10] O **endomorismi**, o **trasformazioni lineari**.
[11] O **forme funzionali**.

Se fissiamo una base in F, diciamo $(\mathbf{f}_1, \mathbf{f}_2, \ldots \mathbf{f}_m)$, i vettori di 4.16 si possono esprimere come loro combinazione lineare:

$$\boldsymbol{\varepsilon}_i = a_{1,i}\mathbf{f}_1 + a_{2,i}\mathbf{f}_2 + \ldots a_{m,i}\mathbf{f}_m \quad i = 1, 2, \ldots n \tag{4.17}$$

In forma matriciale la precedente diviene:

$$\boldsymbol{\varepsilon}_i = (\mathbf{f}_1, \mathbf{f}_2, \ldots \mathbf{f}_m) \begin{pmatrix} a_{1,i} \\ a_{2,i} \\ \ldots \\ a_{m,i} \end{pmatrix} \quad i = 1, 2, \ldots n \tag{4.18}$$

Possiamo affiancare le equazioni 4.18 al variare di i, ottenendo una notazione matriciale molto compatta:

$$(\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots \boldsymbol{\varepsilon}_n) = (\mathbf{f}_1, \mathbf{f}_2, \ldots \mathbf{f}_m) \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{pmatrix} \tag{4.19}$$

Indicheremo la matrice nell'equazione 4.19 come $\mathbf{A}_{m\times n}$.

Chi è interessato, nel sito web YouMath [Youmath 2022.05.06] troverà il calcolo per esteso di questa matrice e alcuni esempi.

Utilizzando vettori colonna per raggruppare le *componenti* del vettore $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix} = \mathbf{X}$ e del vettore $\mathbf{y} = L(\mathbf{x}) = \begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_m \end{pmatrix} = \mathbf{Y}$, dalla dimostrazione del teorema 4.6.1, con qualche calcolo, si arriva alla seguente basilare espressione:

$$\mathbf{Y} = \mathbf{A}_{m\times n}\mathbf{X} \tag{4.20}$$

Questa equazione è *fondamentale* perché ci permette di utilizzare il calcolo matriciale per analizzare il comportamento delle applicazioni lineari.

Infatti è possibile dimostrare anche il seguente:

Teorema 4.6.2. *Fissate le basi di E_n e F_m, esiste un isomorfismo tra lo spazio vettoriale $Hom(E, F)$* [12] *e lo spazio vettoriale $\mathcal{M}(m \times n, K)$ delle matrici $m \times n$ elementi in K* [13].

4.7 endomorfismo e operatori lineari di E_n

Considerando il caso in cui $F_m \equiv E_n$, ovvero le applicazioni lineari che legano elementi di uno spazio vettoriale ad elementi dello stesso spazio vettoriale. Le abbiamo chiamate *endomorfismi* e il loro spazio vettoriale è $Hom(E_n, E_n)$.

Su questo spazio possiamo introdurre una ulteriore operazione di *prodotto* definita come segue.

[12] Che contiene tutte le possibili applicazioni lineari tra E e F.

[13] Il quale contiene tutte le possibili matrici di $m \times n$ elementi in K.

Definizione 4.7.1. *Dati gli operatori A e B, endomorfismi sullo spazio vettoriale E_n, il loro* ***prodotto*** *è l'operatore C come segue:*

$$C(\mathbf{x}) = B(A(\mathbf{x})) \quad \forall \mathbf{x} \in E_n$$

Con qualche passaggio si dimostra che l'operatore *prodotto*, così definito, è un operatore lineare su E_n. E che valgono le proprietà associativa, e quella distributiva del prodotto rispetto la somma.

Quando si introduce una operazione di prodotto nell'ambito di una struttura di gruppo, si dice che si ha una struttura di *algebra*:

Definizione 4.7.2. *Uno spazio vettoriale su un campo K viene detto* ***algebra*** *se vi è definita una ulteriore legge di composizione interna associativa e distributiva rispetto la somma.*

Possiamo applicare l'operazione di prodotto a un qualunque endomorfismo A con la trasformazione identica I. In tal caso avremo:

$$AI = IA = A \quad \forall A \in Hom(E_n, E_n) \tag{4.21}$$

Possiamo replicare l'operazione prodotto dando luogo al concetto di *potenza*.

Definizione 4.7.3. *Il prodotto n volte dell'operatore A è detto* ***potenza****, e si scrive* $A^n = \underbrace{AA\ldots A}_{n \text{ volte}}$

Si pone $A^0 = I$. E vale: $A^{m+n} = A^m + A^n \quad$ con $m, n = 1, 2, \ldots$.

4.8 rappresentazione di un endomorfismo mediante matrice

Gli endomorfismi sono casi particolari degli omomorfismi. Perciò si applica il teorema 4.6.1 che origina il seguente caso particolare.

Teorema 4.8.1. *Data la base $\mathbf{e}_i$ dello spazio vettoriale E_n, ogni operatore lineare $A \in Hom(E_n, E_n)$ definisce univocamente una matrice $n \times n$.*

Viceversa, ogni matrice $n \times n$ identifica un unico endomorfismo lineare.

Notiamo che, siccome in questo caso $F \equiv E$, possiamo fissare una sola base $\mathbf{e}_i$. Non è necessario individuare una seconda base, come dovevamo fare con lo spazio vettoriale $F \neq E$.

Inoltre, gli spazi vettoriali $Hom(E, E)$ e $\mathcal{M}(n \times n, K)$ delle matrici $n \times n$ elementi in K sono isomorfi. E la dimensione di $Hom(E, E)$ è $n \times n$.

Diciamo che l'endomorfismo A è rappresentato dalla matrice $A_{n\times n}$, mentre B è rappresentato dalla matrice $B_{n\times n}$. Il loro *prodotto* $B \cdot A$, a sua volta è rappresentato dal prodotto delle righe di $A_{n\times n}$ per le colonne di $B_{n\times n}$

4.9 endomorfismo inverso

Un endomorfismo può non avere un inverso, salvo quando è biiettivo. In tal caso si indica il suo inverso con l'esponente *meno uno*. Ad esempio A^{-1}. E vale:

$$AA^{-1} = A^{-1}A = I$$

Definizione 4.9.1. *Gli endomorfismi biiettivi sono detti* ***automorfismi***

Gli automorfismi su E_n costituiscono un gruppo rispetto l'operazione prodotto. Tale gruppo è detto *gruppo lineare*.

Si dimostra il seguente:

Teorema 4.9.2. *Un endomorfismo ha un suo inverso* se e solo se *la sua matrice rappresentativa, in una qualunque base, ha determinante non nullo.*

Un operatore lineare che ammette un inverso, si dice *non singolare*.

Infine, si dimostra che il gruppo degli automorfismi di uno spazio vettoriale di dimensione n è isomorfo al gruppo delle matrici $n \times n$ non singolari[14]

4.10 rappresentazione di uno stesso operatore in basi diverse

Nella sezione 4.6 abbiamo visto che la matrice che rappresenta una applicazione lineare dipende dalle basi fissate. Nel caso di un operatore, ovvero $A \in Hom(E, E)$, possiamo fissare una sola base, visto che utilizziamo il solo spazio vettoriale E sia come domino che come codominio.

In ogni caso, variando la base, varia la rappresentazione dell'operatore, quindi la relativa matrice.

È possibile esprimere il rapporto tra le matrici dell'operatore rispetto due diverse basi, per il tramite della matrice che trasforma le basi scelte.

Se scegliamo due diverse basi $\{\mathbf{e}_i\}$ e $\{\mathbf{e}_{i'}\}$. Indichiamo con $A_{n\times n}$ la matrice che rappresenta A in $\{\mathbf{e}_i\}$, e $\tilde{A}_{n\times n}$ sia la matrice che rappresenta A in $\{\mathbf{e}_{i'}\}$.

Inoltre indichiamo con $C_{n\times n}$ la matrice invertibile che le lega le basi:

$$(\mathbf{e}_{1'}, \dots \mathbf{e}_{n'}) = (\mathbf{e}_1, \dots \mathbf{e}_n)C_{n\times n}$$

Si dimostra che valgono le seguenti equazioni:

$$\tilde{A}_{n\times n} = C^{-1}_{n\times n} A_{n\times n} C_{n\times n} \tag{4.22}$$

$$A_{n\times n} = C_{n\times n} \tilde{A}_{n\times n} C^{-1}_{n\times n} \tag{4.23}$$

Ricordiamo:

[14] Ricordiamo: una matrice è singolare se il suo determinante è nullo. Non è singolare se il suo determinante non è nullo. Una matrice ammette l'inversa se e solo se non è singolare.

Definizione 4.10.1. *che due matrici quadrate A e B si dicono simili se esiste una matrice P invertibile tale che valga $A = P^{-1}BP$* [15].

Quindi le equazioni precedenti per $\tilde{A}_{n\times n}$ e $A_{n\times n}$ ci dicono che due matrici corrispondenti allo stesso operatore, espresse in basi distinte, sono simili.

Osservazione 4.10.2. Nell'insieme delle matrici, la relazione di similitudine è una relazione di equivalenza. Una classe di equivalenza di matrici simili rappresenta uno stesso endomorfismo.

Infine, si dimostra:

Proposizione 4.10.3. Due matrici simili hanno lo stesso determinante.

4.11 ripassando

Osserviamo la figura 4.2 cominciando dalla parte destra, in alto. In questo capitolo abbiamo analizzato il comportamento di *applicazioni* tra due campi vettoriali E ed F. In particolare ci siamo focalizzati sulle *applicazioni lineari*, L, per le quali valgono le proprietà di additività e omogeneità.

Abbiamo visto che una applicazione lineare è, incondizionatamente un *omomorfismo*. Seguendo la prima freccia a sinistra del nodo dell'omomorfismo, abbiamo considerato il fatto che possiamo collezionare le applicazioni lineari come elementi di un insieme: l'insieme $Hom(E, F)$.

Continuando a scendere sul ramo sinistro, abbiamo definito gli elementi che ci permettono di vedere $Hom(E.F)$ come uno spazio vettoriale.

Tornando al nodo dell'omomorfismo. Il secondo ramo da sinistra, con la condizione di biiezione, ci porta al caso particolare di applicazioni isomorfe tra gli spazi vettoriali considerati. E, continuando a scendere, incappiamo nel teorema che indica come condizione necessaria e sufficiente affinché due spazi vettoriali E ed F siano isomorfi, il fatto che abbino la stessa dimensione.

Sempre con gli isomorfi: se prendimo un sottospazio vettoriale del dominio, U, allora l'applicazione L è un isomorfismo tra il sottospazio in questione e la sua immagine $L(U)$.

Tornando all'omomorfismo. Il terzo ramo ci ricorda che valgono incondizionatamente le proprietà relative allo zero e all'elemento opposto.

Invece il quarto ramo da sinistra ci ricorda che l'immagine dell'applicazione L è un sottospazio vettoriale del codominio F. E la dimensione di questo sottospazio è detto *rango* di L. Mentre a destra scivoliamo nel teorema dell'omomorfismo. Ovvero l'immagine di L è isomorfo con ogni spazio vettoriale supplementare del kernel di L in E.

Il quinto ramo da sinistra dell'omomorfismo considera l'insieme degli elementi di E tali che il relativo valore di L sia lo zero del codominio F. Questi elementi formano l'insieme kernel di L: $Ker(L)$.

[15] Per una trattazione più approfondita, si veda [Youmath 2022.05.10-2].

E qui abbiamo una osservazione interessante. L è un isomorfismo tra E ed F se e solo se il suo kernel è formato dal solo zero di E. Questo è il primo ramo di sinistra in uscita dal kernel di L.

Mentre il secondo ramo del kernel di L ci ricorda che è incondizionatamente un sottospazio vettoriale di E. E scendendo ricordiamo che ai matematici piace chiamare *nullità di* L la dimensione del kernel di L.

Torniamo all'omomorfismo per seguire il sesto ramo: quando il codominio F coincide con il dominio E. In questo caso particolare l'applicazione è un endomorfismo e prende il nome di *operatore*.

Dati due operatori, A e B, possiamo definire un'ulteriore operazione, detta *prodotto*, come composizione dei due operatori in questione (vedi la sezione 1.7).

Quando, oltre la somma e il prodotto per uno scalare, possiamo definire anche una legge di composizione interna associativa e distributiva rispetto la somma, allora parliamo di *algebra*.

Tornando un attimo indietro: possiamo applicare il prodotto in modo iterativo, ottenendo il concetto di potenza dell'operatore.

Risalendo all'endomorfismo. Se è biiettivo, allora esiste l'operatore inverso A^{-1}. Infine, anticipando l'ottavo ramo dell'ololomorfismo, se fissiamo una base $\{\mathbf{e}_i\}$ in E, allora possiamo rappresentare l'operatore L tramite una matrice $\mathbf{A}_{n\times n}$.

Il settimo ramo dell'omomorfismo, ci indica che vale l'equazione
$dim(E) = dim(L(E)) + dim(Ker(L))$. Ovvero: la dimensione del dominio è pari alla somma della dimensione dell'immagine dell'applicazione e di quella del suo kernel.

L'ottavo ramo dell'omomorfismo ci conduce all'interessantissima osservazione che è possibile rappresentare una qualunque applicazione lineare L tramite una matrice $\mathbf{A}_{m\times n}$ i cui elementi appartengono al campo K su cui insistono E e F.

Le successive osservazioni, che vale $\mathbf{Y} = \mathbf{AX}$, e che lo spazio delle applicazioni lineari e quello delle matrici $m \times n$ in K sono isomorfi, aprono le porte al fatto che l'analisi del comportamento delle applicazioni lineari è fattibile analizzando quello delle matrici $m \times n$.

La sezione 4.4 del capitolo ha riguardato l'individuazione di un metodo per partizionare il dominio E tramite una relazione di equivalenza: quella di congruenza.

E il relativo insieme quoziente E/W, può essere considerato uno spazio vettoriale definendo opportunamente le operazioni di somma e prodotto per uno scalare.

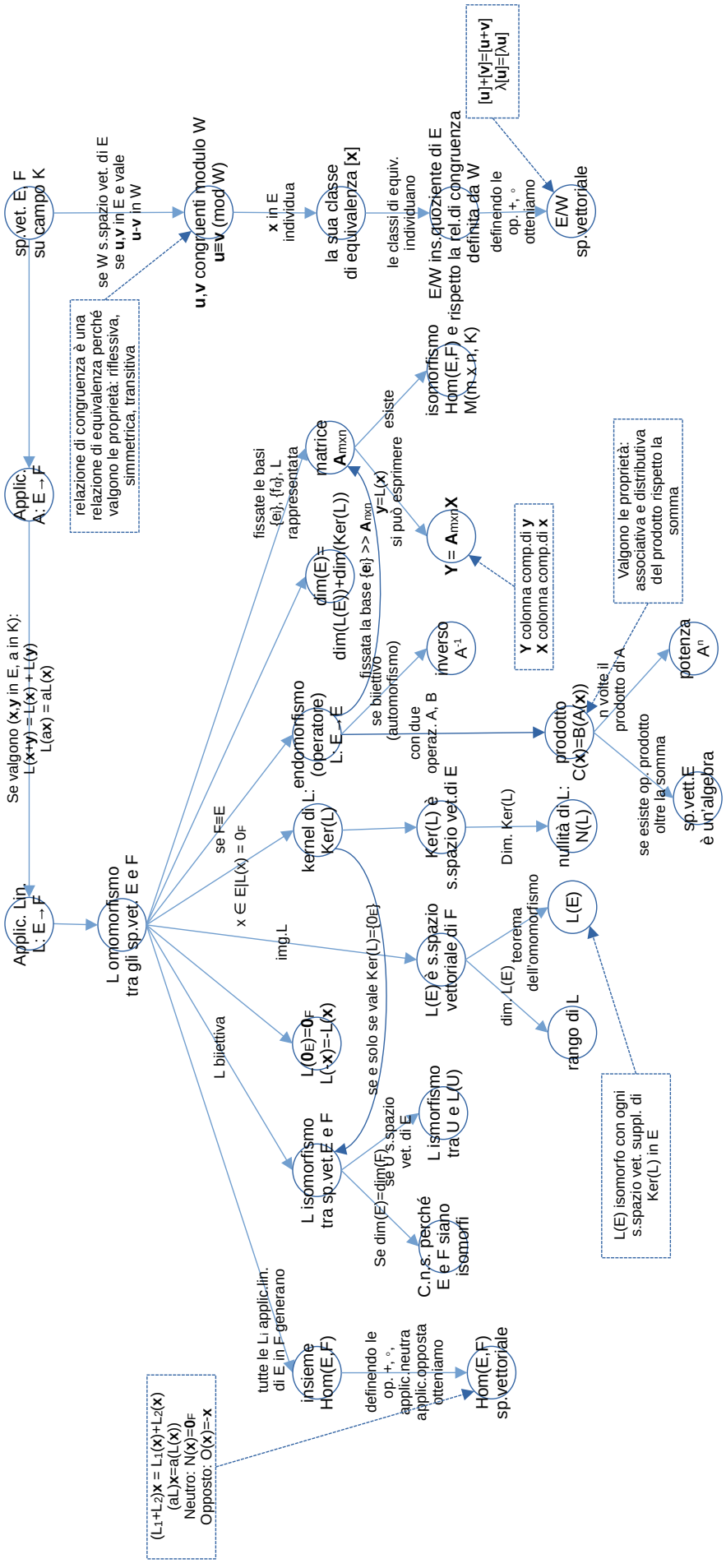


Figura 4.2: Ripassando: le applicazioni lineari

Capitolo 5

Autovalori e autovettori di un operatore lineare

In questo capitolo ci concentreremo sugli endomorfismi[1] su uno spazio vettoriale E.

5.1 autovalori e autovettori di un operatore

Qui vi è un primo concetto particolarmente importante da assimilare:

Definizione 5.1.1. *Dato A operatore sullo spazio vettoriale E_n, un sottospazio $U \subset E_n$ per il quale vale $A(U) \subseteq U$ si dice* ***sottospazio invariante*** *per A.*

Inoltre possiamo definire il concetto di *autovalore*:

Definizione 5.1.2. *Dato un operatore A, un elemento $\lambda \in K$ si chiama* ***autovalore*** *di A se esiste un vettore* non nullo $\mathbf{x}$ *tale che valga:*

$$A(\mathbf{x}) = \lambda \mathbf{x} \tag{5.1}$$

Il vettore $\mathbf{x}$ viene detto **autovettore** di A associato a λ.

Ricordi

La prima volta che abbiamo visto una equazione agli autovalori (ovvero la 5.1) è stato al corso di *Fisica del reattore nucleare*. Il testo di riferimento era [Zweifel 1973], ovviamente scritto in inglese[a].

Bene, a pagina 52 del testo citato, campeggiava l'equazione:

$$(\Sigma_a - v\Sigma_f - \nabla \cdot D\nabla)\phi(\mathbf{r}) = \frac{\Lambda}{\bar{v}}\phi(\mathbf{r})$$

[1] Anche detti *operatori*.

Senza entrare nel dettaglio del significato dei singoli simboli, se si organizza la precedente in questo modo:

$$A(\phi(\mathbf{r})) = \Lambda\phi(\mathbf{r})$$

dove $A(\phi(\mathbf{r})) \Rightarrow \bar{v}(\Sigma_a - v\Sigma_f - \nabla \cdot D\nabla)\phi(\mathbf{r})$, allora si nota la somiglianza con l'equazione 5.1.

Poi, in quel contesto, si indagava la condizione per $\Lambda = 0$. Vedremo tra poco, questo che conseguenze ha.

Già che ci siamo. Qualche pagina più in là (pag. 105), l'autore ci introduceva nel mondo degli operatori lineari (si veda il capitolo 4.7). Che poi avrebbe utilizzato per calcolare la reattività di un reattore nucleare.

Ci siamo dilungati nello scrivere questi ricordi della nostra infanzia per far capire ai nostri lettori che stiamo parlando di *Algebra astratta*, ma le ricadute di tutto ciò sono tremendamente reali.

[a] Un vero spasso per chi, come noi, aveva studiato l'inglese alle medie e al liceo. Dovevamo appuntare con la matita la traduzione di un termine del testo ogni 10 parole! E non ci riferiamo ai termini tecnici, ma al parlato corrente.

Possiamo scegliere $\lambda = \mathbf{0}_E$. In tal caso l'autovettore $\mathbf{x}$ appartiene al kernel di A.

Osservazioni riguardo gli autovettori

L'equazione 5.1 ha diversi aspetti interessanti.

Prima di tutto. Ci dice che l'operazione A sul vettore $\mathbf{x} \in E$ può essere trasformata in un prodotto del vettore per uno scalare: il suo autovalore. Il risultato di questo prodotto uguaglia il valore della $A(\mathbf{x})$.

Secondo aspetto. Qualunque vettore ottenuto come prodotto di $\mathbf{x}$ per uno scalare è un autovettore di λ. Infatti per la linearità di A possiamo scrivere:
$A(\alpha\mathbf{x}) = \alpha A(\mathbf{x}) \quad \forall \alpha \in K$. Quindi vale: $A(\alpha\mathbf{x}) = \alpha A(\mathbf{x}) = \alpha\lambda\mathbf{x} = \lambda(\alpha\mathbf{x})$, che è la definizione, per il vettore $\alpha\mathbf{x}$, di autovettore di A associato a λ.

Terzo aspetto.

Osservazione 5.1.3. La combinazione lineare di autovettori associati a λ è un autovettore associato a λ. Ad esempio, consideriamo la combinazione lineare $a\mathbf{x}_1 + b\mathbf{x}_2$. Per la linearità di A vale
$A(a\mathbf{x}_1 + b\mathbf{x}_2) = aA(\mathbf{x}_1) + bA(\mathbf{x}_2) = a\lambda\mathbf{x}_1 + b\lambda\mathbf{x}_2 = \lambda(a\mathbf{x}_1 + b\mathbf{x}_2)$. Questa è la definizione di autovettore per $a\mathbf{x}_1 + b\mathbf{x}_2$. Ed è generalizzabile per un qualunque numero di addendi.

Si dimostra la seguente affermazione:

Proposizione 5.1.4. Dato l'autovettore $\mathbf{x}$ dell'operatore A, il sottospazio X generato dal suo prodotto per uno scalare è un sottospazio invariante per A.

Questa dimostrazione non è complessa. Infatti se $X = \{\alpha\mathbf{x} | \alpha \in K\}$, possiamo scrivere: $A(\mathbf{x}) = \lambda\mathbf{x} \Rightarrow A(\alpha\mathbf{x}) = \lambda\alpha\mathbf{x}$. Il termine destro di questa equazione ci dice che: $A(X) \subseteq X$[2] che è la definizione 5.1.1.

Inoltre si dimostra:

Proposizione 5.1.5. Dato l'operatore A di E. Dato $\lambda \in K$ e sia $E(\lambda)$ l'insieme di tutti gli autovettori in E per λ. L'insieme $E(\lambda) \cup \mathbf{0}_E$ è un sottospazio vettoriale di E.

Anche questa affermazione si dimostra in modo abbastanza semplice. Prendiamo una manciata di autovettori appartenenti a E_λ. Chiamiamoli $\mathbf{x}_i \quad i = (1, 2, \dots h)$. Facciamone la combinazione lineare: $a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \dots a_h\mathbf{x}_h \quad a_i \in K$. Ma questa, per l'osservazione 5.1.3 è un autovettore, quindi è un vettore di E_λ. Ma per la condizione 3.13 questa è una c.n.s. per individuare uno spazio vettoriale.

Definizione 5.1.6. *Il sottospazio vettoriale $E(\lambda)$ viene detto* ***autospazio***[3] *di A relativamente all'autovalore λ.*

Ora consideriamo autovettori relativi ad autovalori distinti. Si dimostra:

Teorema 5.1.7. *Siano $\mathbf{x}_i \quad i = (1, 2, \dots n)$ autovettori dell'operatore A relativi agli autovalori* distinti *$\lambda_i \quad i = (1, 2, \dots n)$ $\lambda_i \in K$. I vettori $\mathbf{x}_i \quad i = (1, 2, \dots n)$ sono linearmente indipendenti.*

5.2 polinomio caratteristico di una matrice

Consideriamo come spazio vettoriale $E \equiv K^n$, e l'operatore $A : K^n \to K^n$ [4]. Sappiamo che A può essere espresso tramite una matrice di $n \times n$ elementi in K. I valori degli elementi di questa matrice, $\mathbf{A}_{n\times n}$, dipendono dalla base scelta per rappresentare i vettori di K^n [5].

[2] Si noti che $(\lambda \cdot \alpha) \in K$. Quindi vale $\lambda\alpha\mathbf{x} = X$

[3] O anche: **spazio caratteristico**.

[4] Attenzione: questa premessa sarà valida per tutta la sezione: Qui A è sempre un operatore su K^n.

[5] In queste condizioni usualmente si sceglie una base canonica $\mathbf{e}_1, \mathbf{e}_2, \dots \mathbf{e}_n$, dove

$$\begin{aligned} \mathbf{e}_1 &= \{1, 0, \dots, 0\} \\ \mathbf{e}_2 &= \{0, 1, \dots, 0\} \\ &\dots \\ \mathbf{e}_n &= \{0, 0, \dots, 1\} \end{aligned}$$

Gli 1 e 0 sono l'unità e lo zero in K. Per maggiori dettagli si veda [Youmath 2022.05.10] e [Wikipedia 2022.05.10].

Si dimostra la seguente:

Proposizione 5.2.1. Uno scalare $\lambda \in K$ è un autovalore dell'operatore A se e solo se vale

$$det(\mathbf{A}_{n\times n} - \lambda \mathbf{I}_{n\times n}) = 0 \tag{5.2}$$

dove $\mathbf{I}_{n\times n}$ è la matrice identica $n \times n$.

Lo sviluppo dell'espressione $det(\mathbf{A}_{n\times n} - \lambda \mathbf{I}_{n\times n})$ ci rende un polinomio di grado n, e quindi la 5.2 è una equazione di grado n in λ.

Definizione 5.2.2. *L'equazione 5.2 è detta* ***equazione caratteristica*** *della matrice* $\mathbf{A}_{n\times n}$.

Definizione 5.2.3. *Il polinomio al termine sinistro dell'equazione 5.2 è detto* ***polinomio caratteristico*** *della matrice* $\mathbf{A}_{n\times n}$.

Si dimostra:

Teorema 5.2.4. Matrici simili *(si veda la definizione 4.10.1) hanno lo stesso* polinomio caratteristico.

E, siccome matrici simili rappresentano lo stesso endomorfismo (si veda l'osservazione 4.10.2), allora possiamo dire:

Definizione 5.2.5. *Si chiama* polinomio caratteristico *dell'endomorfismo A il polinomio caratteristico della matrice $\mathbf{A}_{n\times n}$, dove quest'ultima è una matrice di A rispetto una qualunque base di E_n.*

Il polinomio caratteristico suddetto si indica con $P_A(\lambda)$.
Ed ha la forma:

$$P_A(\lambda) = c_0\lambda^n + c_1\lambda^{n-1} + c_2\lambda^{n-2} + \cdots + c_n \tag{5.3}$$

dove i coefficienti $c_i \;\; i = (0, 1, \ldots n)$ sono funzioni degli elementi che formano la matrice $A_{n\times n}$.

Per convincerci della validità dell'equazione precedente, ...

... sviluppiamo un semplice esempio. Sia $\mathbf{A}_{2\times 2} = \left(\begin{smallmatrix} 2 & 3 \\ 1 & 5 \end{smallmatrix}\right)$. In questo caso il polinomio caratteristico di A vale: $P_A(\lambda) = det(\mathbf{A}_{2\times 2} + \lambda \mathbf{I}_{2\times 2})$. Ovvero[a]:

$$\begin{aligned} P_A(\lambda) =& det\left(\begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \\ =& det\left(\begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) = \\ =& det\begin{pmatrix} 2-\lambda & 3 \\ 1 & 5-\lambda \end{pmatrix} = \\ =& (2-\lambda)(5-\lambda) - (3\cdot 1) = \\ =& 10 - 2\lambda - 5\lambda + \lambda^2 - 3 = \\ =& \lambda^2 - 7\lambda + 7 \end{aligned}$$

[a] Ricordiamo che il *determinante* di una matrice 2×2 vale: $det\begin{pmatrix} a11 & a12 \\ a21 & a22 \end{pmatrix} = (a11 \cdot a22) - (a12 \cdot a21)$. Per maggiori informazioni riguardo il calcolo del **determinante** di una matrice si può consultare [Youmath 2022.05.11].

Generalizzando l'esempio, si osserva che:

- il coefficiente di λ^n, c_0, vale sempre 1;
- il termine noto, c_n, vale sempre $det(\mathbf{A}_{n\times n})$;
- il coefficiente di λ^{n-1}, c_1, vale sempre la **traccia** di $\mathbf{A}_{n\times n}$[6].
  Da questa osservazione si deduce che la traccia di una matrice $\mathbf{A}_{n\times n}$ caratterizzante una operazione A non dipende dalla base scelta. Ovvero è invariante rispetto un cambiamento di base.

L'affermazione 5.2.1 ci dice che un autovalore esiste se l'equazione 5.3 ha uno o più zeri.

Se il campo K è il campo dei numeri complessi, l'espressione 5.2 ha sempre almeno una soluzione. Nell'ambito dei reali questo non è vero. Oltre i numeri complessi, però esistono dei campi nei quali l'equazione algebrica 5.2 ha sempe almeno una soluzione. Tali campi sono detti *campi algebricamente chiusi*:

Definizione 5.2.6. *Un campo K è algebricamente chiuso se ogni polinomio in K ha almeno una radice in K.*

Da questo momento diamo per assodato che lavoriamo con campi algebricamente chiusi. In questa condizione si dimostra:

Proposizione 5.2.7. Ogni operatore A di E_n, spazio vettoriale su un campo K algebricamente chiuso, possiede almeno un autovalore.

[6] Ricordiamo che la traccia di una matrice (quadrata) è la somma dei suoi elementi sulla diagonale principale: $tr(\mathbf{A}_{n\times n}) = \sum_{i=1}^{n} a_{i,i}$. Ad esempio si può consultare [Youmath 2022.05.11-2].

La dimostrazione della proposizione precedente è semplice. Per definizione, se K è algebricamente chiuso, allora il polinomio caratteristico $P_A(\lambda)$ ha almeno una soluzione. Che è a sua volta un autovalore di A.

5.3 endomorfismi diagonalizzabili

Riprendiamo il concetto che un operatore A dello spazio vettoriale E_n è rappresentabile tramite una matrice $\mathbf{A}_{n\times n}$ (si veda la sezione 4.6).

Non ci dispiacerebbe che la matrice in questione fosse in una forma particolarmente comoda da maneggiare. D'altro canto l'espressione 5.2 ci indica il fatto che vi è una relazione tra autovalori e matrice che esprime l'operatore. Quindi è possibile utilizzare autovalori e autovettori per cercare di individuare una matrice, espressione dell'operatore, che abbia una forma che ci faciliti il calcolo.

Se l'operatore A su E_n ha n autovettori linearmente indipendenti $\mathbf{v}_i \quad i = 1, \dots n$, allora vale $A(\mathbf{v}_i) = \lambda_i \mathbf{v}_i \quad i = 1, \dots n$. E si dimostra che, se si utilizzano gli autovettori in questione come base, rispetto questa base l'operatore A è rappresentabile con la matrice diagonale

$$\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & 0 \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} \tag{5.4}$$

Chi ha studiato un po' di calcolo matriciale, sa bene che le matrici diagonali sono particolarmente interessanti: il loro uso semplifica molto il prodotto righe per colonne.

Definizione 5.3.1. *Un operatore A si dice* ***diagonizzabile***[7] *se vi è una base di E che permette di rappresentarlo con una matrice diagonale.*

Si dimostra:

Proposizione 5.3.2. Un operatore A è diagonizzabile *se e solo se* ammette n autovettori linearmente indipendenti.

La dimostrazione della precedente è relativamente semplice. Prendiamo una base $\{\mathbf{e}_1, \mathbf{e}_2, \dots \mathbf{e}_n\}$ dello spazio vettoriale E_n, dove gli $\mathbf{e}_i$ sono autovettori dei rispettivi autovalori $\lambda_1, \dots \lambda_n$.

Dato un endomorfismo A, la trasformazione di questa base deve valere: $A(\mathbf{e}_i) = \lambda_i \mathbf{e}_i$.

Se rappresentiamo l'endomorfismo A con una matrice, l'espressione precedente è ottenibile solo con una matrice diagonale (ovvero la 5.4),

Infatti possiamo calcolare la trasformazione della base come segue:

$$\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & 0 \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} \cdot (\mathbf{e}_1, \mathbf{e}_2, \dots \mathbf{e}_n) \tag{5.5}$$

[7] Oppure **semplice**.

Ottenendo per la colonna i-esima: $A(\mathbf{e}_i) = 0\mathbf{e}_1 + 0\mathbf{e}_2 + \ldots \lambda_i\mathbf{e}_i + \ldots 0\mathbf{e}_n = \lambda_i\mathbf{e}_i$

La proposizione 5.3.2 ci dice che per rappresentare un endomorfismo utilizzando una matrice diagonale, possiamo metterci a cercare una base di E_n formata da autovettori.

Attenzione al fatto che la proposizione in questione *non afferma* che sia sempre possibile trovare una base formata da autovettori. Un semplice esempio è il seguente.

Consideriamo una trasformazione rappresentata da $\mathbf{A} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Gli autovalori si trovano risolvendo:

$$
\begin{aligned}
&det(\mathbf{A} - \lambda\mathbf{I}) = \\
&= det\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) = \\
&= det\left(\begin{pmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{pmatrix}\right) = \\
&= (1-\lambda)(1-\lambda) - 0 \cdot 1 = \\
&= (1-\lambda)^2
\end{aligned}
$$

Questa ha una sola soluzione: $\lambda = 1$. Per questo motivo abbiamo un solo autovettore, non due. Quindi non è possibile trovare una base per E_2 formata da due autovettori.

Invece è il caso di osservare che se un endomorfismo A ha autovalori distinti, allora il teorema 5.1.7 ci assicura che i suoi autovettori sono linearmente indipendenti. Di conseguenza possiamo affermare che A è diagonizzabile. Questa affermazione è sufficiente. Non è detto sia necessaria. Esistono endomorfismi diagonizzabili anche se non hanno tutti gli autovalori distinti.

Consideriamo una particolare caratteristica di un autovalore: la sua *molteplicità geometrica*.

Definizione 5.3.3. *Si chiama* ***molteplicità geometrica*** *di un autovalore λ di un endomorfismo A, la dimensione dell'autospazio $E(\lambda)$ di A relativo a λ.*

Ricordiamo (si veda la definizione 5.1.6) che un autospazio di A relativo all'autovalore λ è il sottospazio formato dai suoi autovettori in E, più $\{\mathbf{0}_E\}$. La dimensione di questo sottospazio è la molteplicità geometrica di λ.

Per definizione $E(\lambda) = \{\mathbf{x} \in E | A(\mathbf{x}) = \lambda\mathbf{x}\}$. L'equazione a destra, che definisce $E(\lambda)$, la possiamo scrivere: $A(\mathbf{x}) - \lambda\mathbf{x} = \mathbf{0}_E$. In forma matriciale questa diventa $(\mathbf{A} - \lambda\mathbf{I})\mathbf{x} = \mathbf{0}_E$, che è la definizione di kernel di una applicazione lineare (si veda 4.3.3): $\mathbf{x} \in E | L(\mathbf{x}) = \mathbf{0}$.

Se poniamo $L(\mathbf{x}) = (\mathbf{A} - \lambda\mathbf{I})\mathbf{x}$ capiamo che la dimensione di $E(\lambda)$ vale la dimensione del kernel $Ker(\mathbf{A} - \lambda\mathbf{I})$.

Invece la *molteplicità algebrica*:

Definizione 5.3.4. *La* ***molteplicità algebrica*** *dell'autovalore λ dell'endomorfismo A, è la sua molteplicità come radice dell'equazione caratteristica $P_A(\lambda) = 0$.*

A questo punto si può dimostrare il seguente:

Teorema 5.3.5. *Dato M sottospazio vettoriale invariante di E rispetto l'emdomorfismo A di E. L'azione di A su M sia l'endomorfismo A', allora il suo polinomio caratteristico $P_{A'}(\lambda)$ è un divisore del polinomio caratteristico di A: $P_A(\lambda)$*

La dimostrazione di questo teorema, che qui non sviluppiamo, si basa sul fatto che in queste condizioni è possibile scegliere delle basi tali che la matrice $\mathbf{A}$ per calcolare A, può essere espressa nella seguente forma *a blocchi*:

$$\mathbf{A} = \left(\begin{array}{c|c} \mathbf{A'} & \mathbf{T} \\ \hline \mathbf{0} & \mathbf{W} \end{array}\right) \tag{5.6}$$

dove $\mathbf{A'}$ è la matrice dell'endomorfismo A', e $\mathbf{0}$ è una matrice nulla. Per una matrice a blocchi di questo genere è possibile scrivere:

$$\begin{aligned} &det(\mathbf{A} - \lambda\mathbf{I}) = det(\mathbf{A'} - \lambda\mathbf{I})det(\mathbf{W} - \lambda\mathbf{I}) \\ &\quad \Rightarrow P_A(\lambda) = P_{A'}(\lambda)P_W(\lambda) \end{aligned}$$

che dimostra l'affermazione 5.3.5.

Dal precedente teorema, discende il seguente:

Teorema 5.3.6. *Dato l'endomorfismo A di E, con autovalore λ, vale la diseguaglianza:*

$$\textit{molteplicità geometrica di } \lambda \leq \textit{molteplicità algebrica di } \lambda$$

Il fatto che si possa esprimere un endomorfismo nella forma a blocchi 5.8 apre una ulteriore area d'indagine.

Se M è un sottospazio vettoriale invariante di E per l'endomorfismo A, possiamo scrivere

$$E = M \oplus N \tag{5.7}$$

dove N è il sottospazio vettoriale che complementa M rispetto E [8].

È possibile che N sia a sua volta invariante per l'endomorfismo A. Se questo è vero, possiamo scegliere delle basi per M e per N tali che la 5.8 diviene:

$$\mathbf{A} = \left(\begin{array}{c|c} \mathbf{A'} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{A''} \end{array}\right) \tag{5.8}$$

dove $\mathbf{A'}$ è la matrice per A', e $\mathbf{A''}$ è la matrice per A''. In tal caso definiamo:

Definizione 5.3.7. *Un endomorfismo A che ammette $E = M \oplus N$ con M ed N sottospazi invarianti per A, si dice* ***riducibile****.*

La definizione precedente vale per più (h) sottospazi invarianti per l'endomorfismo A, fino al caso limite in cui $h = n$. In quest'ultimo caso abbiamo un endomorfismo diagonizzabile.

Riprendendo quanto abbiamo detto finora, abbiamo il seguente:

Teorema 5.3.8. *Dato l'endomorfismo A di uno spazio vettoriale E_n sul un campo K algebricamente chiuso. C.n.s. affinché A sia diagonizzabile è che per ogni autovalore proprio λ_i, la sua molteplicità geometrica sia uguale alla sua molteplicità algebrica come radice del polinomio caratteristico $P_A(\lambda)$.*

[8] Ovvero formato da tutti i vettori di E non appartenenti a M. Più lo zero di E.

5.4 successione di sottospazi a bandiera indotta da A

Finora abbiamo indagato endomorfismi diagonizzabili o riducibili, che si traducono in matrici diagonali o con conformazione a blocchi sulla diagonale.

Proseguendo nella nostra ricerca di semplificazione della forma della matrice che rappresenta l'endomorfismo, possiamo interessarci alle matrici triangolari.

Queste sono più complesse delle matrici diagonali e a blocchi sulla diagonale, ma sono comunque più semplici da trattare di una matrice completa.

Le matrici triangolari sono definite come segue.

Definizione 5.4.1. *Una matrice quadrata $n \times n$ è **triangolare superiore** se per i suoi elementi vale: $a_{i,j} = 0 \quad \forall i > j$.*

ovvero se sono nulli tutti i suoi elementi al di sotto della diagonale.

Una matrice è **triangolare inferiore** se sono nulli tutti gli elementi al di sopra della diagonale: $a_{i,j} = 0 \quad \forall i < j$.

Si parla di matrici *strettamente triangolari*:

Definizione 5.4.2. *Una matrice quadrata $n \times n$ è **strettamente triangolare superiore** se per i suoi elementi vale: $a_{i,j} = 0 \quad \forall i \geq j$.*

cioè sono nulli, oltre gli elementi sotto la diagonale, anche quelli sulla diagonale.

Ovviamente vale anche la relativa definizione di matrice **strettamente triangolare inferiore**: $a_{i,j} = 0 \quad \forall i \leq j$.

Se in E_n riusciamo ad individuare una base rispetto la quale un endomorfismo A è rappresentato da una matrice triangolare, diciamo che A è **triangolarizzabile**.

Si dimostra il seguente teorema.

Teorema 5.4.3. *Dato l'endomorfismo A sullo spazio vettoriale E_n sul campo K* algebricamente chiuso*, esistono $n+1$ sottospazi $E_i \quad i = 0, 1, \ldots n$ tali che:*

1. *ogni E_i è invariante per A;*
2. *$dim(E_i) = i$;*
3. *$E_0 = \mathbf{0} \subset E_1 \subset E_2 \subset \ldots E_n$.*

Una successione di sottospazi del tipo $E_0 \subset E_1 \subset E_2 \subset \ldots E_n$ è detta **a bandiera**.

Che impatto ha il teorema precedente sulla rappresentazione di A in forma di matrice? Scegliendo opportunamente una base $\{\mathbf{e}_i\} \quad i = 1, 2, \ldots n$ [9], otteniamo la rappresentazione matriciale di A nella forma:

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \ldots & a_{1,n} \\ 0 & a_{2,2} & a_{2,3} & \ldots & a_{2,n} \\ 0 & 0 & a_{3,3} & \ldots & a_{3,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & a_{n,n} \end{pmatrix} \tag{5.9}$$

Inoltre si dimostra la seguente:

[9] Opportunamente significa scegliere $\mathbf{e}_1 \in E_1, \mathbf{e}_2 \in E_2, \ldots \mathbf{e}_n \in E_n$.

Proposizione 5.4.4. Se si rappresenta l'endomorfismo A su E_n sul campo K algebricamente chiuso nella forma 5.9, gli autovalori di A sono gli elementi della diagonale principale.

E questa affermazione ci permette di dare una seconda versione del teorema 5.4.3.

Teorema 5.4.5. *Dato un endomorfismo A di E_n sul campo K algebricamente chiuso, si può fissare una base $\{\mathbf{e}_i\}$ di E_n che permette di rappresentare A con una matrice triangolare.*

In pratica, data una generica matrice $\mathbf{A}$ che rappresenta l'omomorfismo A su E_n per una determinata base $\{\mathbf{e'}_i\}$, il teorema 5.4.5 afferma che possiamo sempre scegliere una diversa base $\{\mathbf{e}_i\}$ tale che la rappresentazione di A sia data da una matrice triangolare $\tilde{\mathbf{A}}$.

In queste condizioni vale l'equazione 4.22, che esprime il calcolo per uno stesso operatore di due diverse matrici ognuna nella propria base. Quindi, data una matrice $\mathbf{A}$ ad elementi nel campo K algebricamente chiuso, esiste una matrice $\mathbf{B}$ tale che valga:

$$\tilde{\mathbf{A}} = \mathbf{B}^{-1}\mathbf{A}\mathbf{B}$$

con $\tilde{\mathbf{A}}$ triangolare.

5.5 struttura di endomorfismi nilpotenti

Cominciamo con il definire il concetto di *nilpotenza*.

Definizione 5.5.1. *Diciamo che un endomorfismo A è **nilpotente** se esiste un numero intero $k > 0$ per il quale valga*

$$A^k = \mathbf{0} \tag{5.10}$$

Il più piccolo intero k per il quale valga la 5.10 è l'**indice di nilpotenza**[10].

Si dimostra il seguente

Teorema 5.5.2. *Se l'endomorfismo A sullo spazio vettoriale E ha indice di nilpotenza k, in E esiste una successione strettamente crescente di sottospazi:*

$$L_0 \subset L_1 \subset \dots L_k = E$$

tali che

$$A(L_{i+1}) \subset L_i \quad \forall i \geq 0 \tag{5.11}$$

Questo teorema ci dice che i sottospazi in questione ci assicurano una ampliamento graduale dei valori di A, fino alla convergenza su E.

Ora, dato un sottospazio L_i dell'endomorfismo A su E, consideriamo il suo sottospazio supplementare rispetto L_{i+1} [11], e chiamiamolo F_i. Si dimostra:

[10] O *grado* di nilpotenza.

[11] Ovvero quello formato da tutti gli elementi di L_{i+1} che non appartengono a L_i.

Teorema 5.5.3. *Se A è un endomorfismo su E con indice di nilpotenza k, si ha una successione di sottospazi F_i tali che:*

1. $L_{i+1} = F_{i+1} \oplus L_i \quad 1 \leq i \leq k-1$;
2. $A(F_{i+1}) \cap L_{i-1} = \{\mathbf{0}\}$;
3. $A(F_{i+1})$ *isomorfo a* F_{i+1};
4. $A(F_i) \subseteq F_{i-1}$.

Così come si dimostra la validita della seguente equazione:

$$E_n = F_1 \oplus F_2 \oplus \dots F_k \tag{5.12}$$

Inoltre si osserva che una base in E non si ottiene aggiungendo l'una all'altra le varie basi in F_i. È necessario trasformare via via una base nella successiva, più il relativo completamento. Qui non ci addentriamo nel descrivere in maggiore dettaglio questa procedura. Ci limitiamo ad osservare che è possibile costruire una base come segue:

$$\begin{aligned}
\mathbf{e}_1 &= A^{k-1}\mathbf{v}_1 = A\mathbf{e}_2 \\
\mathbf{e}_2 &= A^{k-2}\mathbf{v}_1 = A\mathbf{e}_3 \\
&\dots \\
\mathbf{e}_{k-2} &= A^2\mathbf{v}_1 = A\mathbf{e}_{k-1} \\
\mathbf{e}_{k-1} &= A\mathbf{v}_1 = A\mathbf{e}_k \\
\mathbf{e}_k &= \mathbf{v}_1
\end{aligned}$$

Lo spazio M_i generato dai vettori predetti è invariante. Questo ci permette di affermare che l'endomorfismo $A(M_i)$ [12] è rappresentato da:

$$\mathbf{A}_{M_i} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix} \tag{5.13}$$

Questa è una matrice triangolare superiore con tutti gli elementi a zero, salvo gli elementi $\mathbf{a}_{i,j+1} = 1$, ovvero quelli subito sopra la diagonale principale.

Visto che vale $E = M_1 \oplus M_2 \oplus \dots M_k$, per ottenere la matrice $\mathbf{A}$ che rappresenta A, possiamo comporre le diverse matrici $\mathbf{A}_{M_i} \quad i = 1, \dots k$ arrivando ad una matrice nella forma

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{M_1} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_{M_2} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{A}_{M_3} & \dots & \mathbf{0} \\ \dots & \dots & \dots & \dots & \dots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{A}_{M_k} \end{pmatrix} \tag{5.14}$$

[12] Ovvero l'endomorfismo A vincolato allo spazio M_i.

Dove le matrici $\mathbf{A}_{M_i}$ hanno la forma 5.13. Questa è detta **matrice di Jordan** relativa all'autovalore $\lambda = 0$. Ed è caratterizzata dall'avere tutti gli elementi uguali a zero, salvo quelli nella diagonale immediatamente superiore alla principale, che sono uguali a zero o ad uno.

5.6 decomposizione di E_n in somma diretta di sottospazi invarianti per A

I risultati ottenuti finora permettono di dimostrare che un operatore A sullo spazio vettoriale E definito su un campo algebricamente chiuso K, può essere rappresentato con una matrice con tutti gli elementi nulli salvo alcuni di quelli che compongono la diagonale principale e quella immediatamente superiore alla diagonale principale. Si dimostra:

Teorema 5.6.1. *Dato A endomorfismo sullo spazio vettoriale E_n, questo si decompone nella somma diretta di due sottospazi invariante di A: L_q e N_q tali che A/L_q è nilpotente con indice di nilpotenza q a A/N_q è invertibile.*

Il teorema 5.6.1 ci porta nella condizione descritta nella equazione 5.7. Quindi abbiamo a che fare con un endomorfismo riducibile. In tal caso la matrice rappresentativa può essere espressa nella forma 5.8, che riportiamo qui di seguito per comodità:

$$\mathbf{A} = \left(\begin{array}{c|c} \mathbf{A}' & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{A}'' \end{array}\right)$$

dove $\mathbf{A}'$ rappresenta A su L_q, mentre $\mathbf{A}''$ lo rappresenta su N_q.

Segue questo:

Teorema 5.6.2. *Dato A un endomorfismo sullo spazio vettoriale E_n, con p autovalori distinti $\lambda_1, \ldots, \lambda_p$ di molteplicità algebrica $r_1, \ldots r_p$ $(r_1 + r_2 + \ldots r_p = n)$. Allora lo spazio E_n è somma diretta di sottospazi $M_{r_1}, M_{r_2}, \ldots M_{r_p}$ [13] ognuno dei quali invariante per A e tale che $\mathbf{A} - \lambda_i \mathbf{I}$ è nilpotente su M_{r_i}*

5.7 autovettori generalizzati, forma canonica di Jordan

Definiamo:

Definizione 5.7.1. *é un **autovettore generalizzato** di rango q di un automorfismo A associato a un autovalore λ_i, un autovettore $\mathbf{x}$ per il quale valgono:*

$$(\mathbf{A} - \lambda_i \mathbf{I})^q \mathbf{x} = 0 \tag{5.15a}$$

$$(\mathbf{A} - \lambda_i \mathbf{I})^{q-1} \mathbf{x} \neq 0 \tag{5.15b}$$

[13] Si noti che qui l'indice r_i del sottospazio indica anche le sue dimensioni.

Nel caso $q = 1$ questa è la definizione di autovettore. Infatti la 5.1 si può riscrivere come: $(\mathbf{A} - \lambda_i \mathbf{I})\mathbf{x} = 0$

In questi casi si arriva a rappresentare A con una matrice di Jordan in cui gli elementi della diagonale principale valgono tutti λ_i, e la diagonale subito sopra la diagonale principale è formata da tutti 1.

Siamo nella condizione di applicare il teorema 5.6.2 alla dimostrazione del *teorema di Jordan*:

Teorema 5.7.2 (teorema di Jordan)**.** *dato l'endomorfismo A sullo spazio vettoriale E_n, con polinomio caratteristico $P_A(\lambda) = \prod_{i=1}^{r}(\lambda - \lambda_i)^{n_i}$, allora A è rappresentabile con una matrice tutta nulla salvo i valori $\lambda_i \quad i = 1, 2, \dots r$ sulla diagonale principale e 1 o zero sulla diagonale sopra la principale.*

Inoltre esiste un intero k_i che indica il numero di blocchi di Jordan; e k interi $p_{i_1} \geq p_{i_2} \geq \dots p_{i_{k_1}}$ che rappresentano l'ordine dei blocchi di Jordan relativi all'autovalore λ_i; e vale $p_{i_1} + p_{i_2} + \dots p_{i_{k_1}} = n_i$ dove n_i è la molteplicità algebrica della radice λ_i

I numeri $\lambda_i, k_i, p_{i_{k_i}}, n_i$ sono detti **numeri di Jordan**. E la matrice descritta in 5.7.2 è la **forma canonica di Jordan**

5.8 polinomi di operatori e matrici

Se $P(t)$ è un polinomio con coefficienti in K:

$$P(t) = a_0 t^n + a_1 t^{n-1} + \dots a_n \quad a_i \in K$$

e abbiamo l'operatore A su E_n. Definiamo[14]

$$P(A) = a_0 A^n + a_1 A^{n-1} + \dots a_n I \quad a_i \in K$$

In modo analogo se $\mathbf{A}$ è una matrice $n \times n$ in K [15], definiamo:

$$P(\mathbf{A}) = a_0 \mathbf{A}^n + a_1 \mathbf{A}^{n-1} + \dots a_n \mathbf{I} \quad a_i \in K \tag{5.16}$$

dove $\mathbf{I}$ è la matrice unitaria.

Ci possiamo chiedere se è possibile trovare una serie di coefficienti del polinomio $P(\mathbf{A})$ tali che valga $P(\mathbf{A}) = 0$. Polinomi siffatti si dicono **polinomi annullatori**.

Se lo spazio vettoriale E è finito, i polinomi annullatori sicuramente esistono, come stabilito dal seguente:

Teorema 5.8.1. *Per ogni matrice $\mathbf{A} \in \mathcal{M}(n \times n, K)$ esiste un polinomio, di grado non superiore a n^2 tale che $P(\mathbf{A}) = 0$.*

E si arriva al seguente:

[14] ricordiamo: I è l'operatore identico.

[15] Ricordiamo che una matrice siffatta rappresenta un operatore di K^n.

Teorema 5.8.2 (di Cayley - Hamilton)**.** *Ogni matrice* **A** *annulla il proprio polinomio caratteristico*[16] $P(\lambda)$.

Definiamo:

Definizione 5.8.3. *Il* ***polinomio minimo*** *di una matrice* **A***, è il polinomio* $m_A(\lambda)$ *che ha il minimo grado tra i polinomi annullatori di* **A***, e il coefficiente del termine di grado più alto pari ad* 1 [17].

Quindi il polinomio minimo di **A** ha tre proprietà che lo caratterizzano:
- $m(\lambda)$ ha il coefficiente del termine di grado più alto pari ad 1;
- vale $m(\lambda) = 0$, perchè è un polinomio annullatore;
- non esistono polinomi annullatori di **A** con grado inferiore a quello di $m(\lambda)$.

Abbiamo detto che le proprietà precedenti caratterizzano il polinomio minimo perché si dimostra:

Proposizione 5.8.4. il polinomio minimo della matrice **A** è unico.

Così come si dimostra:

Proposizione 5.8.5. matrici simili hanno lo stesso polinomio minimo.

Ricordando che matrici simili rappresentano lo stesso operatore (si veda l'osservazione 4.10.2), da quest'ultima affermazione possiamo estrapolare che il concetto di polinomio minimo *si applica anche ad un operatore* A, e non solo alle matrici che lo rappresentano.

Si dimostra anche:

Proposizione 5.8.6. se il polinomio $P(\lambda)$ è tale che $P(A) = 0$, allora $P(\lambda)$ è divisibile per il polinomio minimo $m_A(\lambda)$

Ed infine si dimostra:

Proposizione 5.8.7. polinomio caratteristico e polinomio minimo hanno le stessa radici, eventualmente con diversa molteplicità.

[16] Si veda la definizione 5.2.3.

[17] Ovvero l'unità di K Un polinomio con questa caratteristica si dice **monico**.

Dizionario dei termini e dei sinonimi

In questo capitolo riportiamo un semplice dizionario dei principali termini utilizzati.

Ne profittiamo per gestire anche l'inevitabile presenza di sinonimi.

L'uso di sinonimi nei linguaggi è del tutto normale. Però quando si ha a che fare con un testo che ci descrive qualcosa che dobbiamo assimilare, ci possono mettere in difficoltà. Per questo motivo in queste pagine abbiamo cercato di adottare una terminologia omogenea.

D'altro canto, per una nostra svista, o quando si legge di *Algebra generale* da altre fonti, può capitare di imbattersi in termini che riferiscono il nostro concetto con un vocabolo diverso: un sinonimo, appunto. Perciò abbiamo deciso di aggiungere un piccolo dizionario, che riporti anche i sinonimi che ci è capitato di osservare.

Attenzione al fatto che questo dizionario non deve essere considerato come un elenco esaustivo. Tutt'altro! Alla versione 0.7.1 del presente documento, questo capitolo è ancora embrionale.

Termine	**Definizione**
Algebra astratta	Sin. di Algebra generale: l'oggetto di questo documento.
Autospazio (di endom. per un autovalore)	Sottospazio vettoriale formato da tutti gli autovettori in E per l'autovalore λ dell'endomorfismo A.
Biiettiva (applicazione)	Applicazione suriettiva e iniettiva.
Cardinalità (insieme)	Numero di elementi che compongono un insieme finito.
Classe di una partizione	Elemento di una partizione di un insieme.
Differenza simmetrica	Sin. di somma disgiunta. Termine usato nell'ambito degli insiemi.
(insiemi) Disgiunti	Quando l'intersezione di due insiemi è l'insieme vuoto.
Codominio (di applicazione)	Insieme degli elementi possibili valori dell'applicazione.
Dominio (di applicazione)	Insieme degli elementi per i quali è definita l'applicazione.
Elemento	Una qualunque entità non divisibile; usualmente componente di un insieme.

Endomorfismo	Omomorfismo su uno stesso gruppo: $\phi : G \to G$. In questo caso $\phi(x \circ y) = \phi(x) \circ \phi(y)$.
Endomorfismo semplice	Sin. di endomorfismo diagonizzabile. Termine usato nell'ambito degli autovalori.
Forma funzionale	Sin. di forma lineare. Termine usato nell'ambito delle applicazioni lineari.
Funzione	Sin. di applicazione.
Immagine (di applicazione)	Insieme degli elementi del codominio dell'applicazione, che sono il valore di almeno un elemento del suo dominio.
Iniettiva (applicazione)	Applicazione per cui ogni elemento del dominio riferisce un solo elemento del codominio.
Insieme	Una collezione di elementi *distinti*.
Intersezione di insiemi	Insieme ottenuto con gli elementi in comune a tutti gli insiemi componenti.
Omomorfismo	Applicazione tra due gruppi $(G, \circ)$ e $(G', \square)$, o insiemi, ciascuno con una legge di composizione interna, che preserva i prodotti: $\phi(x \circ y) = \phi(x) \square \phi(y)$.
One-to-one (applicazione)	Sin. di iniettiva (applicazione). Utilizzato nella lingua inglese.
Onto (applicazione)	Sin. di suriettiva (applicazione). Utilizzato nella lingua inglese.
Operatore (lineare)	Sin. di endomorfismo. Termine usato nell'ambito delle applicazioni lineari.
Partizione di un insieme	Suddivisione di un insieme in insiemi disgiunti.
Prodotto cartesiano	Dati due insiemi, è l'insieme delle coppie ordinate dei loro elementi. Si indica con il simbolo $\times$.
Range (di applicazione)	Sin. di immagine dell'applicazione.
Somma diretta (di s.spazi vet.)	Dati due s.spazi vettoriali $\mathbf{V}, \mathbf{W}$, è la loro somma $\mathbf{V} \oplus \mathbf{W}$ purché valga $\mathbf{V} \cap \mathbf{W} = \{\mathbf{0}\}$.
Somma disgiunta	Insieme formato dagli elementi che appartengono esclusivamente ad uno degli insiemi dell'operazione e non a più di loro contemporaneamente. Si indica con il simbolo $+$.
Sottospazio invariante	Dato U sottospazio dello spazio vettoriale E. Quando il codominio di un operatore A è chiuso su U, si dice che U è un s.spazio invariante per A.

Sottospazio stabile	Sin. di sottospazio invariante. Termine usato nell'ambito degli autovalori.
Spazio caratteristico (di autovalore)	Sin. di autospazio dell'endomorfismo A relativamente all'autovalore λ.
Suriettiva (applicazione)	Applicazione che copre tutto il codomini.
Trasformazione (lineare)	Sin. di endomorfismo. Termine usato nell'ambito delle applicazioni lineari.
Unione di insiemi	Insieme ottenuto con tutti gli elementi degli insiemi componenti.

GNU Free Documentation License

Version 1.3, 3 November 2008

<https://fsf.org/>

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "**Document**", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "**you**". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "**Modified Version**" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "**Secondary Section**" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "**Invariant Sections**" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "**Cover Texts**" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "**Transparent**" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "**Opaque**".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "**Title Page**" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "**publisher**" means any person or entity that distributes copies of the Document to the public.

A section "**Entitled XYZ**" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "**Acknowledgements**", "**Dedications**", "**Endorsements**", or "**History**".) To "**Preserve the Title**" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which

the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents,

unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include

translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See `https://www.gnu.org/licenses/`.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions

of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

Bibliografia

[Agler 2013] "Symbolic Logic: syntax, semantics, and proof", David W. Agler, Rowman & Littlefield Publishers, inc. (2013)

[Bergman 2020] "An invitation to General Algebra and Universal Constructions", George M. Bergman, Dept. of Mathematics - University of California, Berkeley (2020)

[Bottazzini 2006] "La teoria delle equazioni algebriche", Umberto Bottazzini, in Storia della Scienza Vol.3, cap.VI, Gruppo editoriale L'Espresso (2006)

[Carrell 2005] "Fundamentals of Linear Algebra", James B. Carrel, Dept. of Mathematics - The University of British Columbia (2005)

[Gasparini 1977] "Strutture Algebriche, Operatori Lineari", Ida Cattaneo Gasparini, Libreria Eredi virgilio Veschi (1977)

[Lang 2005] "Undergraduate Algebra - Third Edition", Serge Lang, Springer (2005)

[Youmath 2022] "Matrice di cambiamento di base", consultato Aprile 2022

[Youmath 2022.05.06] "Matrice associata a una applicazione lineare", consultato 06 Maggio 2022

[Youmath 2022.05.10] "Base di uno spazio vettoriale/Basi canoniche", consultato 10 Maggio 2022

[Youmath 2022.05.10-2] "Matrici simili", consultato 10 Maggio 2022

[Youmath 2022.05.11] "Determinante di una matrice", consultato 11 Maggio 2022

[Youmath 2022.05.11-2] "Traccia di una matrice", consultato 11 Maggio 2022

[Wikipedia 2022] "Modular arithmetic", consultato Aprile 2022

[Wikipedia 2022.05.10] "Canonical basis", consultato 10 Maggio 2022

[Zweifel 1973] "Reactor Physics", Paul F. Zweifel, McGraw-Hill Kogakusha, Ltd. (1973); international student edition

Indice analitico

R^+, 52
R_0, 63
$T(A)$, 36
$\Leftrightarrow$, 17
$\Rightarrow$, 16
$\cap$, 19
$\circ$, 37
$\cup$, 18
$\exists \ldots$, 17
$\forall \ldots$, 17
$\in$, 16
$\mathbb{C}$, 16
$\mathbb{N}$, 16
$\mathbb{P}$, 16
$\mathbb{Q}$, 16
$\mathbb{R}$, 16
$\mathbb{Z}$, 16
$\oplus$, 67
$\subset$, 17
$\subseteq$, 17
$\varnothing$, 18
$\ldots | \ldots$, 17

algebra, 81
appartenenza (insieme), 16
applicazione, 28
    ben definita sullo spazio quoziente, 36
    biiettiva, 31
    composta, 33
    identica, 33
    iniettiva, 31
    inversa, 32
    isomorfismo, 42
    prodotto, 33
    suriettiva, 31
applicazioni lineari, 72
associativa, *vedi* proprietà associativa
automorfismo, 53
automorfismo (in applic. lin.), 82
autospazio (di endom. per un autovalore), 88
autovalore (def.), 86
autovettore (def.), 86
autovettori generalizzati, 97
autovettori lin. indipendenti, 88

bandiera (sottospazi a), 94
base, **63**
biiettiva, *vedi* applicazione biiettiva
Boole, *vedi* struttura algebrica di Boole

campi algebricamente chiusi, 90
chiusura, 47
classe (insieme), 20
classe di equivalenza, 27
classi laterali (applicazioni lineari), 77
codominio, 30
coimplicazione (logica), 17
commutativa, *vedi* proprietà commutativa
composizione esterna (legge), 39
composizione interna (legge), 37
congruenza (applicazioni lineari), 76

determinante (di matrice), 90
differenza (insieme), 20
differenza simmetrica (insieme), 23

dimensione dello spazio vettoriale, 64
divisori dello zero, 55
dominio, 30

elemento
    neutro, 38
    simmetrico, 39
elemento (insieme), **15**
endomorfismi (di spazi vet.), 79, 80
endomorfismo, 53
endomorfismo diagonizzabile, *vedi* operatore diagonizzabile
equazione caratteristica, 89
equipotenti, *vedi* insieme equipotenti

fibra (applicazione), 32
forme funzionali (di spazi vet.), 79
forme lineari (di spazi vet.), 79
funzione, 28

grafico della funzione (applicazione), 32
gruppo, 37, **47**
    $T(A)$, 49
    abeliano, 47
    anello, 54
    anello commutativo, 54
    anello unitario, 55
    astratto, 53
    campo, 56
    commutativo, 47
    corpo, 56

immagine reciproca (applicazione), 32
implicazione (logica), 16
indice di nilpotenza, 95
iniettiva, *vedi* applicazione iniettiva
insieme, **15**
    cardinalità, 16
    chiuso, 36
    complementare, 22
    delle parti, 18
    delle trasformazioni, 36
    disgiunti, 20
    equipotenti, 34
    immagine, 31
    isomorfi, 42
    numerabile, 34
    numeri reali positivi, 52
    vuoto, 17
intersezione (insieme), 19
inversa, *vedi* applicazione inversa
inviluppo lineare di un sistema di VI, 66
isometria, **49**
isomorfismo (gruppi), 52
isomorfismo (spazi vettoriali), 73

Jordan
    forma canonica di, 98
    matrice di, 97
    numeri di, 98
    teorema di, 98

kernel (applicazione lineare), 74

leggi di Morgan, 22

matrice strettamente triangolare inferiore, 94
matrice strettamente triangolare superiore, 94
matrice triangolare inferiore, 94
matrice triangolare superiore, 94
matrici di cambiamento di base, 68
matrici simili, *vedi* simili(matrici)
molteplicità algebrica (di autovalore), 92
molteplicità geometrica (di autovalore), 92

nilpotenza (endomorfismo), 95
non singolare (di operatore lin.), 82
nullità (applicazione lineare), 75
numerabile, *vedi* insieme numerabile

omomorfismo
    insiemi, 41
    kernel, 52
omomorfismo (gruppi), 52
omomorfismo (spazi vettoriali), 73

omomorfismo (teorema: applic. lin. di spazi vet.), **75**, 77
omotetia, 73
operatore, 72
operatore diagonizzabile, 91
operatore identico, 73
operatore nullo, 72
operatori lineari (di spazi vet.), 79
ordine (insieme finito), 48

partizione (insieme), 20
partizione dei gruppi, 53
polinomi annullatori, 98
polinomio caratteristico, 89
polinomio minimo, 99
polinomio monico, 99
prodotto (di endomorfismi), 81
prodotto cartesiano, 24
proprietà
    associativa, 38
    commutativa, 38
proprietà dei sottoinsiemi, 17

quoziente (insieme), 28

rango (applicazione lineare), 74
relazione
    binaria, 25
    d'ordine, 26
    di equivalenza, 26
    inclusione, 26
relazione di uguaglianza (insieme), 18
riducibile (endomorfismo), 93
rilevanti (insiemi), 16

scalare (elemento), 60
semigruppo, 38
simili (matrici), 83
simmetrie di una figura, 49
somma di sottospazi vettoriali, 66
    diretta, 67
somma disgiunta (insieme), 23
sottogruppo, 51
    proprio, 51
sottoinsieme, 17
    proprio, 17
sottospazi supplementari, 67
sottospazio invariante (def.), 86
sottospazio vettoriale, 65
    condizione, 65
spazio caratteristico (di autovalore), 88
spazio duale (di spazio vet.), 79
spazio vettoriale, 60
spazio vettoriale di dimensione non finita, 64
struttura algebrica, 37, 39
    di Boole, 40
suriettiva, *vedi* applicazione suriettica

teorema del completamento della base, 66
teorema della base, 64
teorema della combinazione in vettori indipendenti, 63
teorema della esistenza di vettori indipendenti, 63
teorema di Cayley, 54
teorema di Cayley - Hamilton, 99
teorema di esistenza del sottospazio supplementare, 67
traccia (di matrice), 90
trasformazione, 36, 72
    identica, 49
    isometrica, *vedi* isometria
trasformazioni lineari (di spazi vet.), 79
traslazione a sinistra, 53
traslazone a destra, 53
triangolarizzabile (endomorfismo), 94

unione (insieme), 18

vettore, 60
vettori
    base, *vedi* base, 64
    combinazione lineare, 62
    componenti, 63
    linearmente dipendenti, 62
    linearmente indipendenti, 62
    sistema indipendente, 62
    sistema indipendente di ordine massimo, 63