ALGEBRA LINEARE e GEOMETRIA

Lezioni ed Esercizi

VOLUME I

A. Basile - L. Stramaccia

Indice

1 INSIEMI **1**
- 1.1 Insiemi e Sottoinsiemi 1
- 1.2 Unione e Intersezione. 2
- 1.3 Differenza e prodotto cartesiano. 3
- 1.4 Applicazioni. 4
- 1.5 Composizione di applicazioni. 5
- 1.6 Esercizi svolti 7
- 1.7 Esercizi proposti. 14

2 RELAZIONI E OPERAZIONI **17**
- 2.1 Relazioni 17
- 2.2 Operazioni 19
- 2.3 Strutture algebriche 20
- 2.4 Permutazioni 23
- 2.5 Numeri complessi 27
- 2.6 Esercizi svolti 31
- 2.7 Esercizi proposti 39

3 SPAZI VETTORIALI **41**
- 3.1 Definizioni e prime proprietà 41
- 3.2 Dipendenza lineare. Basi. 44
- 3.3 Dimensione 47
- 3.4 Somme e somme dirette. 50
- 3.5 Esercizi svolti 53
- 3.6 Esercizi proposti 59

4 APPLICAZIONI LINEARI **63**
- 4.1 Applicazioni lineari 63
- 4.2 Nucleo e immagine di una applicazione lineare 66

4.3 Composizione di applicazioni lineari 69
4.4 Esercizi svolti 70
4.5 Esercizi proposti 79

5 MATRICI **81**
5.1 Lo spazio delle matrici 81
5.2 Moltiplicazione fra matrici. 83
5.3 Applicazioni lineari e matrici 86
5.4 Matrice di una applicazione lineare composta 90
5.5 Esercizi svolti. 92
5.6 Esercizi proposti 100

6 DETERMINANTI **103**
6.1 Esistenza 103
6.2 Proprietà dei determinanti. 105
6.3 Unicità 107
6.4 Determinante della trasposta e di un prodotto 109
6.5 Matrici invertibili 111
6.6 Esercizi svolti. 112
6.7 Esercizi proposti 119

7 SISTEMI LINEARI **121**
7.1 Sistemi di Cramer 121
7.2 Rango di una matrice 124
7.3 Sistemi lineari omogenei 128
7.4 Sistemi lineari non omogenei 130
7.5 Esercizi svolti 134
7.6 Esercizi proposti 145

8 POLINOMI **149**
8.1 Lo spazio dei polinomi 149
8.2 L'algoritmo Euclideo 152
8.3 Riducibilità 156
8.4 Massimo comun divisore 158
8.5 Esercizi svolti 159
8.6 Esercizi proposti 163

9 COORDINATE CARTESIANE **165**
9.1 Ascisse sulla retta e segmenti orientati 165
9.2 Coordinate cartesiane 166

9.3 Vettori geometrici 168
9.4 Vettori paralleli e complanari 171
9.5 Coordinate dei vettori 173
9.6 Traslazioni 176
9.7 Esercizi svolti 177
9.8 Esercizi proposti 183

10 SPAZIO AFFINE **187**
10.1 Allineamento e complanarità fra punti 187
10.2 Equazioni parametriche di rette e piani 188
10.3 Equazione cartesiana di un piano 191
10.4 Fasci di piani e di rette 196
10.5 Equazioni cartesiane di una retta. 198
10.6 Cambiamenti di riferimento affine 203
10.7 Esercizi svolti 208
10.8 Esercizi proposti 222

11 SPAZIO EUCLIDEO **227**
11.1 Nozioni angolari e modulo di un vettore 227
11.2 Prodotto scalare 230
11.3 Misure di distanze e di angoli 232
11.4 Cambiamenti di riferimento cartesiano 238
11.5 Prodotto vettoriale. 240
11.6 Esercizi svolti 242
11.7 Esercizi proposti 256

12 SPAZIO PROIETTIVO **259**
12.1 Elementi impropri 259
12.2 Coordinate omogenee 261
12.3 Uso delle coordinate omogenee 264
12.4 Esercizi svolti 268
12.5 Esercizi proposti 277

13 CURVE PIANE **281**
13.1 Generalità sulle curve piane 281
13.2 Complessificazione del piano reale 285
13.3 Curve algebriche 287
13.4 Ordine di una curva algebrica 289
13.5 Punti semplici e singolari di una curva 291
13.6 Condizioni analitiche per i punti singolari 295

13.7 Esercizi svolti 298
13.8 Esercizi proposti 307

14 LE CONICHE **309**
14.1 Generalità e classificazione 309
14.2 Fasci di coniche 313
14.3 Polarità definita da una conica 319
14.4 Diametri coniugati e assi 322
14.5 Esercizi svolti 327
14.6 Esercizi proposti 337

15 SUPERFICIE E CURVE SGHEMBE **341**
15.1 Generalità sulle superficie e curve sghembe 341
15.2 Complessificazione dello spazio reale 346
15.3 Superficie algebriche 348
15.4 Punti semplici e singolari di una superficie 350
15.5 Le Quadriche 352
15.6 Classificazione delle quadriche non degeneri 354
15.7 Esercizi svolti 357
15.8 Esercizi proposti 368

16 AUTOVETTORI E AUTOVALORI **373**
16.1 Autovettori e autovalori 373
16.2 Polinomio caratteristico 376
16.3 Diagonalizzazione 380
16.4 Triangolazione 384
16.5 Esercizi svolti 386
16.6 Esercizi proposti 404

17 PRODOTTI SCALARI **407**
17.1 Prodotti scalari 407
17.2 Prodotti scalari definiti positivi 409
17.3 Prodotti hermitiani 414
17.4 Applicazioni unitarie 418
17.5 Applicazioni simmetriche 423
17.6 Esercizi svolti 426
17.7 Esercizi proposti 439

18 FORME BILINEARI **443**
18.1 Forme lineari 443
18.2 Forme bilineari 446
18.3 Forme bilineari simmetriche 451
18.4 Forme quadratiche 453
18.5 Esercizi Svolti 456
18.6 Esercizi proposti 464

19 GRUPPI **467**
19.1 Definizioni e prime proprietà 467
19.2 Omomorfismi 471
19.3 Gruppi ciclici 474
19.4 Classi laterali 477
19.5 Sottogruppi normali. Gruppo quoziente 480
19.6 Esercizi svolti 483
19.7 Esercizi proposti 489

20 CAMPI FINITI **493**
20.1 Definizione ed esempi di anello 493
20.2 Divisori dello zero 495
20.3 Campi di Galois 497
20.4 Caratteristica di un campo finito 500
20.5 Alcune proprietà di un campo finito 502
20.6 Esercizi svolti 509
20.7 Esercizi proposti 523

Prefazione

L'algebra lineare, per alcuni suoi capitoli, costituisce da tempo la struttura fondamentale di ogni corso di geometria, è ad essa quindi che è dedicata buona parte della presente opera divisa in due volumi. Sono molti i testi che forniscono una trattazione completa ed esauriente della teoria, pertanto non è questo lo scopo che ci si prefigge, bensì quello di una semplice esposizione degli argomenti che gli autori usualmente sviluppano nell'ambito dei corsi di geometria per gli studenti di ingegneria.

La parte propriamente dedicata alla geometria occupa i capitoli 10-15 del primo volume. In essa il punto di vista è quello di una applicazione dei concetti più semplici sugli spazi vettoriali e sui sistemi lineari già sviluppati nei primi capitoli. Affidando talvolta la trattazione più alla semplice intuizione che al rigore formale e, in altri casi, omettendo alcune dimostrazioni, si è ottenuto di poter accennare a più argomenti senza per questo incorrere in un eccessivo appesantimento.

Il capitolo sui polinomi è inteso come propedeutico allo studio delle curve e superficie algebriche, nonchè ai problemi relativi agli autovalori ed alla diagonalizzazione con cui si apre il secondo volume.

La recente ristrutturazione degli studi di ingegneria ha rivelato un orientamento di interesse sempre maggiore nei confronti dell'algebra, specialmente nel caso del corso di laurea in ingegneria elettronica ed informatica. In linea con questa esigenza il secondo volume è dedicato alla parte più raffinata dell'algebra lineare, dalla diagonalizzazione e triangolazione sino alle forme quadratiche mentre gli ultimi due capitoli sono dedicati ai gruppi ed ai campi finiti. L'intento è quello di fornire le conoscenze di base essenziali per affrontare argomenti più complessi.

Ciascuno dei due volumi è corredato da numerosi problemi svolti e non che hanno lo scopo di rendere familiare il lettore con le tecniche di risoluzione che fanno parte del necessario corredo che i corsi di geometria devono fornire.

Lo sforzo degli autori è anche stato di rendere soddisfacente l'uso del testo pure in altri corsi di laurea scientifici quali matematica o fisica, dove ultimamente è stato talvolta richiesto.

La numerazione dei due volumi è progressiva per quanto riguarda le pagine ed i capitoli, pertanto il secondo volume prosegue il primo con il capitolo 16.
Un riferimento del tipo "Esempio 13.1.2" rimanda all' Esempio 2 *del paragrafo* 1 *del capitolo* 13. *Per comodità del lettore sia l'indice generale che l'indice analitico vengono riportati integralmente in entrambi i volumi*.

Capitolo 1

INSIEMI

1.1 Insiemi e Sottoinsiemi

Il concetto di *insieme* è un concetto primitivo. I sostantivi famiglia, collezione, aggregato, sono fra i più usati come sinonimi di insieme. Dati un insieme A ed un oggetto a sarà sempre possibile stabilire se a è o non è un elemento di A, o in altre parole se a appartiene o no ad A. Nel primo caso scriveremo $a \in A$, nel secondo $a \notin A$. Ogni insieme S i cui elementi appartengono tutti ad un dato insieme A si chiama un *sottoinsieme* di A. Per indicare che S e un sottoinsieme di A si scrive $S \subseteq A$. Se invece S non è un sottoinsieme di A, se esistono cioè elementi di S che non appartengono ad A, si scrive $S \nsubseteq A$. Due insiemi A e B si dicono *uguali* quando sono costituiti dagli stessi elementi, in tal caso si scrive $A = B$, si scrive invece $A \neq B$ nel caso contrario. Si ha quindi $A = B$ se e solo se $A \subseteq B$ e $B \subseteq A$. Si chiama *insieme vuoto* e si indica con $\emptyset$ l'insieme privo di elementi. L'insieme vuoto si considera sottoinsieme di ogni insieme. Un sottoinsieme S di A si dice un *sottoinsieme proprio* di A quando $S \neq A$. Si scrive in tal caso $S \subset A$. I simboli $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, sono generalmente usati per indicare rispettivamente l'insieme dei numeri naturali, l'insieme dei numeri interi, l'insieme dei numeri razionali, l'insieme dei numeri reali. Gli elementi che costituiscono un dato insieme vengono indicati fra parentesi in vari modi. Così per esempio, se A è l'insieme costituito dal solo elemento a, B l'insieme dei numeri naturali minori di 5, P l'insieme dei numeri naturali pari, si potrà scrivere:

$$A = \{a\}, \quad B = \{1, 2, 3, 4\} = \{x \in \mathbb{N} \mid x < 5\},$$

$$P = \{x \in \mathbb{N} \mid x \text{ è pari}\} = \{x \in \mathbb{N} \mid x = 2y, \text{ con } y \in \mathbb{N}\}.$$

Esempio 1.1.1.

$$\{1, a, b\} \subset \{1, 2, a, b, c\},$$

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$,

$\{x \in \mathbb{Z} \mid x^2 - 1 = 0\} = \{1, -1\}$,

$\{x \in \mathbb{Z} \mid 4x^2 = 1\} = \emptyset$.

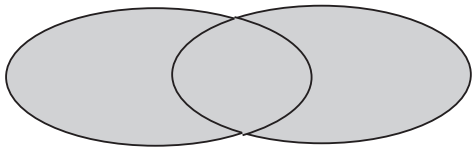
I sottoinsiemi propri dell'insieme $A = \{1, 2, a\}$ sono:

$$\emptyset, \{1\}, \{2\}, \{a\}, \{1, 2\}, \{1, a\}, \{2, a\}.$$

1.2 Unione e Intersezione.

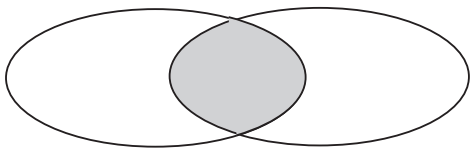
Dati due insiemi A e B, l'insieme costituito dagli elementi che appartengono ad A oppure a B si chiama *unione* di A e B e si denota con $A \cup B$:

(1) $$A \cup B = \{x \mid x \in A \text{ o } x \in B\}.$$



L'insieme costituito dagli elementi che appartengono ad A e a B si chiama *intersezione* di A e B e si denota con $A \cap B$

(2) $$A \cap B = \{x \mid x \in A \text{ e } x \in B\}.$$



Due insiemi A e B si dicono *disgiunti* se non hanno elementi in comune, cioè se $A \cap B = \emptyset$.

Esempio 1.2.1. Dati gli insiemi $A = \{1, 2, a, b\}$, $B = \{2, 3, a, c, d\}$, $C = \{3, d\}$, si ha:

$$A \cup B = \{1, 2, 3, a, b, c, d\},$$

$$A \cup C = \{1, 2, 3, a, b, d\},$$
$$B \cup C = \{2, 3, a, c, d\},$$
$$A \cap B = \{2, a\}, \quad A \cap C = \emptyset, \quad B \cap C = C.$$

Le precedenti definizioni si estendono ad una famiglia $\mathcal{F}$ di insiemi nel modo seguente:

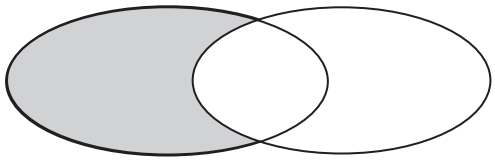
$$\bigcup_{A \in \mathcal{F}} A = \{x \mid x \in A \text{ per qualche } A \in \mathcal{F}\},$$

$$\bigcap_{A \in \mathcal{F}} A = \{x \mid x \in A \text{ per ogni } A \in \mathcal{F}\}.$$

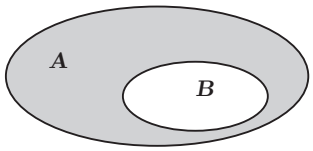
1.3 Differenza e prodotto cartesiano.

Si chiama *differenza* $A - B$ (in questo ordine) di due insiemi A e B, l'insieme degli elementi che appartengono ad A e non a B:

$$A - B = \{x \mid x \in A,\ x \notin B\}. \tag{3}$$



Nel caso che B sia un sottoinsieme di A, l'insieme $A - B$ prende il nome di *complementare* di B in A. Esso si potrà indicare con B_A^c o semplicemente con B^c quando l'insieme A possa essere sottointeso.



Si chiama *prodotto cartesiano* $A \times B$ degli insiemi A e B (in questo ordine), l'insieme costituito dalle coppie ordinate (a, b) di primo elemento in A e secondo in B:

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}. \tag{4}$$

Dati un insieme A ed un numero naturale n, l'insieme costituito dalle $n-$uple ordinate di elementi di A si indica con A^n:

$$A^n = \{(a_1, \ldots, a_n) \mid a_i \in A, \text{ per } i = 1, \ldots, n\}. \tag{5}$$

Esempio 1.3.1. Per $A = \{1, 2, 3, a, b\}$ e $B = \{2, 4, b, c\}$ si ha:

$$A - B = \{1, 3, a\}, \quad B - A = \{4, c\}.$$

Per $A = \{1, 2, a\}$ e $B = \{1, b\}$ si ha:

$$A \times B = \{(1,1), (1,b), (2,1), (2,b), (a,1), (a,b)\},$$

$$B \times A = \{(1,1), (1,2), (1,a), (b,1), (b,2), (b,a)\},$$

$$A^2 = \{(1,1), (1,2), (1,a), (2,1), (2,2), (2,a), (a,1), (a,2), (a,a)\}.$$

1.4 Applicazioni.

Siano dati due insiemi A e B. Una *applicazione* o *funzione* di A in B è una legge che associa a ciascun elemento di A un *unico* elemento di B. Se α è una applicazione di A in B scriveremo

$$\alpha : A \to B.$$

L'insieme A si chiama anche *il dominio* o *l'insieme di definizione* di α, mentre B si dice *il codominio* di α. L'elemento di B che l'applicazione α associa all'elemento x di A si indica con $\alpha(x)$ e si chiama *l'immagine* di x in α. Il sottoinsieme di B costituito dalle immagini di tutti gli elementi di A si indica con $\alpha(A)$ e si dice anche *l'insieme delle immagini*. Due applicazioni α e β di A in B si dicono *uguali* se

$$\alpha(x) = \beta(x) \quad \text{per ogni} \quad x \in A. \tag{6}$$

Scriveremo in tal caso $\alpha = \beta$.
Una applicazione α di A in B si dice *iniettiva* se elementi distinti di A hanno sempre immagini distinte in B. In altri termini α è iniettiva se e solo se vale la seguente proprietà:

$$\alpha(x) = \alpha(y) \quad \text{implica} \quad x = y, \quad \text{per ogni} \quad x, y \in A. \tag{7}$$

Si dice che α è *suriettiva* se $\alpha(A) = B$. Quindi α è suriettiva se e solo se per ogni elemento y di B esiste almeno un elemento x di A tale che si abbia $\alpha(x) = y$. Una applicazione che sia contemporaneamente iniettiva e suriettiva si chiama una applicazione *biiettiva* o anche una *biiezione*. Dato un insieme A, l'applicazione $id_A : A \to A$ definita da

$$id_A(x) = x \quad \text{per ogni} \quad x \in A$$

si chiama *l'applicazione identica* di A. Ovviamente id_A è una biiezione.

Esempio 1.4.1. Consideriamo le applicazioni:

$\alpha_1 : \mathbb{R} \to \mathbb{R}$ definita da $\alpha_1(x) = x^2 - 1$,

$\alpha_2 : \mathbb{N} \to \mathbb{N}$ definita da $\alpha_2(x) = 2x$,

$\alpha_3 : \mathbb{Q} \to \mathbb{Q}$ definita da $\alpha_3(x) = 2x + 1$.

L'applicazione α_1 non è iniettiva nè suriettiva, la α_2 è iniettiva ma non suriettiva, la α_3 è una biiezione.

Si dice che due insiemi A e B hanno lo stesso numero di elementi se esiste una biiezione di A in B. Un insieme A si chiama un *insieme finito* se, per qualche numero naturale n, esiste una biiezione di A nell'insieme $\{1, 2, ..., n\}$. In tal caso si dice che A ha n elementi. Un insieme A che non sia finito si chiama *infinito*.

1.5 Composizione di applicazioni.

Siano α una applicazione di A in B e β una applicazione di B in C. Si denota con $\beta \circ \alpha$ o semplicemente con $\beta\alpha$ l'applicazione di A in C definita come segue:

$$\beta\alpha(x) = \beta[\alpha(x)] \quad \text{per ogni} \quad x \in A. \tag{8}$$

L'applicazione $\beta\alpha$ si chiama *l'applicazione composta* di α e β (o anche *prodotto* di α e β). Si osservi che l'ordine in cui le applicazioni α e β vengono considerate è essenziale e che, anche quando gli insiemi A, B, C sono tali che si possa definire tanto l'applicazione $\beta\alpha$ quanto l'applicazione $\alpha\beta$, esse in generale non sono uguali.
Date le applicazioni $\alpha : A \to B$, $\beta : B \to C$, $\gamma : C \to D$, come immediata conseguenza della definizione di applicazione composta, si ottiene la seguente proprietà associativa:

$$\gamma(\beta\alpha) = (\gamma\beta)\alpha. \tag{9}$$

Una applicazione $\alpha : A \to B$ si dice *invertibile* se esiste una applicazione $\alpha^{-1} : B \to A$ tale che

$$\alpha^{-1}\alpha = id_A \quad \text{e} \quad \alpha\alpha^{-1} = id_B.$$

Se α è invertibile l'applicazione α^{-1} è unica. Se infatti β_1 e β_2 sono applicazioni di B in A tali che $\beta_1\alpha = \beta_2\alpha = id_A$ e $\alpha\beta_1 = \alpha\beta_2 = id_B$, si ha subito

$$\beta_1 = id_A\beta_1 = (\beta_2\alpha)\beta_1 = \beta_2(\alpha\beta_1) = \beta_2 id_B = \beta_2.$$

L'applicazione α^{-1} si chiama *l'inversa di* α.

Teorema 1.5.1. *L'applicazione $\alpha : A \to B$ è invertibile se e solo se è biiettiva.*

Dim. Se α è biiettiva, per ogni elemento $y \in B$ esiste uno ed un solo elemento $x \in A$ tale che $\alpha(x) = y$. Definiamo l'applicazione $\alpha^{-1} : B \to A$ ponendo $\alpha^{-1}(y) = x$ se e solo se $\alpha(x) = y$. Per ogni elemento $x \in A$, posto $\alpha(x) = y$, si ha

$$\alpha^{-1}\alpha(x) = \alpha^{-1}(y) = x = id_A(x).$$

D'altra parte, per ogni elemento $y \in B$, posto $y = \alpha(x)$, si ha

$$\alpha\alpha^{-1}(y) = \alpha(x) = y = id_B(y).$$

Ne segue $\alpha\alpha^{-1} = id_A$ e $\alpha^{-1}\alpha = id_B$. Viceversa sia α invertibile. Dato un qualsiasi elemento $y \in B$, si consideri $\alpha^{-1}(y)$. Da

$$\alpha[\alpha^{-1}(y)] = \alpha\alpha^{-1}(y) = y$$

segue allora che $y \in \alpha(A)$ e che quindi α è suriettiva. Se poi x_1 e x_2 sono elementi di A tali che $\alpha(x_1) = \alpha(x_2)$, da $\alpha^{-1}\alpha(x_1) = \alpha^{-1}\alpha(x_2)$ segue $x_1 = x_2$ e quindi α è iniettiva. □

Siano date due applicazioni $\alpha : A \to B$ e $\beta : B \to C$ invertibili. L'applicazione composta $\beta\alpha$ è ovviamente anch'essa biiettiva cioè invertibile, si ha inoltre

$$(\beta\alpha)(\alpha^{-1}\beta^{-1}) = \beta(\alpha\alpha^{-1})\beta^{-1} = \beta\beta^{-1} = id_C$$

e

$$(\alpha^{-1}\beta^{-1})(\beta\alpha) = \alpha^{-1}(\beta^{-1}\beta)\alpha = \alpha^{-1}\alpha = id_A,$$

pertanto l'inversa dell'applicazione $\beta\alpha$ è la seguente

$$(\beta\alpha)^{-1} = \alpha^{-1}\beta^{-1}. \tag{10}$$

1.6 Esercizi svolti

Nel corso degli esercizi faremo uso di alcuni connettivi logici come ad esempio quello di implicazione "$\Rightarrow$" e di doppia implicazione "$\Leftrightarrow$". Scriveremo pertanto $\mathcal{A} \Rightarrow \mathcal{B}$ per affermare che la proposizione $\mathcal{A}$ implica la proposizione $\mathcal{B}$ e $\mathcal{A} \Leftrightarrow \mathcal{B}$ per affermare che le proposizioni $\mathcal{A}$ e $\mathcal{B}$ sono equivalenti nel senso che $\mathcal{A}$ implica $\mathcal{B}$, ma anche $\mathcal{B}$ implica $\mathcal{A}$.

1.6.1. *(Leggi distributive)* Siano $A, B, C \subset X$. Valgono le seguenti uguaglianze :

(1) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

(2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

$$(1)\ x \in A \cup (B \cap C) \Leftrightarrow x \in A \text{ oppure } x \in (B \cap C) \Leftrightarrow$$

$$\Leftrightarrow x \in A \text{ oppure } (x \in B \text{ e } x \in C) \Leftrightarrow$$

$$\Leftrightarrow (x \in A \text{ oppure } x \in B) \text{ e } (x \in A \text{ oppure } x \in C) \Leftrightarrow$$

$$\Leftrightarrow x \in A \cup B \text{ e } x \in A \cup C \Leftrightarrow x \in (A \cup B) \cap (A \cup C).$$

Si noti che tutte le implicazioni logiche che compaiono nell'argomentazione esposta, sono invertibili ("se e solo se"), ovvero essa può essere letta anche al contrario. Ciò significa che abbiamo provato contemporaneamente la validità delle due proposizioni

$$x \in A \cup (B \cap C) \Rightarrow x \in (A \cup B) \cap (A \cup C),$$

$$x \in (A \cup B) \cap (A \cup C) \Rightarrow x \in A \cup (B \cap C).$$

Allora $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$ ed anche $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$, da cui l'uguaglianza.

$$(2)\ x \in A \cap (B \cup C) \Leftrightarrow x \in A \text{ e } x \in (B \cup C) \Leftrightarrow$$

$$\Leftrightarrow x \in A \text{ e } (x \in B \text{ oppure } x \in C) \Leftrightarrow$$

$$\Leftrightarrow (x \in A \text{ e } x \in B) \text{ oppure } (x \in A \text{ e } x \in C) \Leftrightarrow$$

$$\Leftrightarrow x \in A \cap B \text{ oppure } x \in A \cap C \Leftrightarrow x \in (A \cap B) \cup (A \cap C).$$

1.6.2. Siano $A, B \subset X$. Provare che

$$A - B = A \cap B^c.$$

Si noti che i due membri l'ugualianza sopra rappresentano modi diversi di scrivere l'insieme di tutti gi elementi x che sono in A e non in B.

1.6.3. Siano $A, B \subset X$. Mostrare che si ha :

$$(A \cup B)^c = A^c \cap B^c \quad \text{e} \quad (A \cap B)^c = A^c \cup B^c.$$

Per la prima:

$$x \in (A \cup B)^c \Leftrightarrow x \in X - (A \cup B) \Leftrightarrow x \in X \text{ e } x \notin (A \cup B) \Leftrightarrow$$

$$\Leftrightarrow x \in X \text{ e } (x \notin A \text{ e } x \notin B) \Leftrightarrow (x \in X \text{ e } x \notin A) \text{ e } (x \in X \text{ e } x \notin B) \Leftrightarrow$$

$$\Leftrightarrow x \in X - A \text{ e } x \in X - B \Leftrightarrow x \in A^c \text{ e } x \in B^c \Leftrightarrow x \in A^c \cap B^c.$$

Per la seconda:

$$x \in (A \cap B)^c \Leftrightarrow x \in X - (A \cap B) \Leftrightarrow x \in X \text{ e } x \notin (A \cap B) \Leftrightarrow$$

$$\Leftrightarrow x \in X \text{ e } (x \notin A \text{ oppure } x \notin B) \Leftrightarrow$$

$$\Leftrightarrow (x \in X \text{ e} x \notin A) \text{ oppure } (x \in X \text{ e } x \notin B) \Leftrightarrow$$

$$\Leftrightarrow x \in X - A \text{ oppure } x \in X - B \Leftrightarrow$$

$$x \in A^c \text{ oppure } x \in B^c \Leftrightarrow x \in A^c \cup B^c.$$

L'esercizio precedente fornisce le cosiddette *Leggi di De Morgan*, nel caso di due sottinsiemi A e B di X. Tali leggi valgono più in generale, nel senso dell'esercizio che segue.

1.6.4. Sia $A_i \subset X$, per ogni $i \in I$. In altre parole $\{A_i \mid i \in I\}$ è una famiglia di sottinsiemi di X indiciati su un insieme di indici I. In tale situazione valgono le relazioni :

(1) $(\bigcap_{i \in I} A_i)^c = \bigcup_{i \in I} A_i^c$.

(2) $(\bigcup_{i \in I} A_i)^c = \bigcap_{i \in I} A_i^c$.

Proviamo la prima, l'altra si prova con la stessa tecnica.

$$x \in (\bigcap_{i\in I} A_i)^c \Leftrightarrow x \in X \text{ e } x \notin \bigcap_{i\in I} A_i \Leftrightarrow$$
$$\Leftrightarrow x \in X \text{ e } x \notin A_i \text{ , per qualche } i \in I \Leftrightarrow$$
$$\Leftrightarrow x \in X - A_i \text{ , per qualche } i \in I \Leftrightarrow x \in \bigcup_{i\in I} A_i^c.$$

1.6.5. Dati sottinsiemi A, B di X, si ha

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B).$$

$$x \in (A - B) \cup (B - A) \Leftrightarrow x \in A - B \text{ oppure } x \in B - A \Leftrightarrow$$
$$\Leftrightarrow (x \in A \text{ e } x \notin B) \text{ oppure } (x \in B \text{ e } x \notin A) \Leftrightarrow$$
$$\Leftrightarrow (x \in A \text{ oppure } x \in B) \text{ e } (x \notin A \text{ oppure } x \notin B) \Leftrightarrow$$
$$\Leftrightarrow x \in A \cup B \text{ e } x \notin A \cap B \Leftrightarrow x \in (A \cup B) - (A \cap B).$$

A questo punto lo studente si sarà reso conto del ruolo preciso che svolgono i connettivi logici "e" ed "oppure", ed avrà notato che per essi valgono delle regole del tutto analoghe alle leggi distributive per le operazioni di intersezione ed unione.

1.6.6. Siano A, B, C sottinsiemi di un insieme X. Si provi che valgono le seguenti relazioni

$$A \cap (B - C) = A \cap B - A \cap C.$$
$$A \cup (B - C) \neq A \cup B - A \cup C.$$

Per la prima relazione si ha

$$x \in A \cap (B - C) \Leftrightarrow x \in A \text{ e } (x \in B \text{ e } x \notin C) \Leftrightarrow$$

$$\Leftrightarrow (x \in A \text{ e } x \in B) \text{ e } (x \in A \text{ e } x \notin C) \Leftrightarrow x \in A \cap B \text{ e } x \notin A \cap C.$$

Per provare la seconda portiamo un controesempio, cioè esibiamo un caso particolare in cui i due membri della relazione sono effettivamente diversi. Sia $X = \mathbb{N}$ e siano

$$A = \{12, 13\},\ B = \{7, 8, 9, 10, 11, 12\},\ C = \{11, 12\}.$$

Allora, da

$$B - C = \{7, 8, 9, 10\},\ A \cup B = \{7, 8, 9, 10, 11, 12, 13\},\ A \cup C = \{11, 12, 13\},$$

si ottiene

$$A \cup (B - C) = \{7, 8, 9, 10, 12, 13\} \quad \text{e} \quad (A \cup B) - (A \cup C) = \{7, 8, 9, 10\}.$$

1.6.7. Provare che, per insiemi A, B, C, valgono :

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(2) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(3) $A \times (B - C) = (A \times B) - (A \times C)$.

$$(1)\ (x, y) \in A \times (B \cup C) \Leftrightarrow x \in A \text{ e } y \in (B \cup C) \Leftrightarrow$$
$$\Leftrightarrow x \in A \text{ e } (y \in A \,\text{oppure}\, y \in B) \Leftrightarrow (x \in A \text{ e } y \in B) \,\text{oppure}\, (x \in A \text{ e } y \in C) \Leftrightarrow$$
$$\Leftrightarrow x \in A \times B \,\text{oppure}\, x \in A \times C \Leftrightarrow x \in (A \times B) \cup (A \times C).$$

Sostituendo, nella dimostrazione precedente, "oppure" con "e", si ottiene la dimostrazione della (2).

$$(3)\ (x, y) \in A \times (B - C) \Leftrightarrow x \in A \text{ e } y \in (B - C) \Leftrightarrow$$
$$\Leftrightarrow x \in A \text{ e } (y \in B \text{ e } y \notin C) \Leftrightarrow (x \in A \text{ e } y \in B) \,\text{e}\, (x \in A \text{ e } y \notin C) \Leftrightarrow$$
$$\Leftrightarrow (x, y) \in (A \times B) \text{ e } (x, y) \notin (A \times C) \Leftrightarrow (x, y) \in (A \times B) - (A \times C).$$

1.6.8. Sia $\mathbb{R}$ l'insieme dei numeri reali. Considerate le applicazioni

$\alpha : \mathbb{R} \to \mathbb{R}, \quad \alpha(x) = 2x,$

$\beta : \mathbb{R} \to \mathbb{R}, \quad \beta(x) = x^2 - 1,$

$\gamma : \mathbb{R} \to \mathbb{R}, \quad \gamma(x) = x + 2,$

si dica quali tra $\alpha, \beta, \gamma, \alpha\beta, \beta\alpha, \alpha\beta\gamma, \gamma\beta\alpha$, sono iniettive, suriettive, biiettive.

L'applicazione α è biiettiva, infatti
- è iniettiva, poichè da $\alpha(x) = \alpha(x')$ segue $2x = 2x'$ e quindi $x = x'$.
- è suriettiva. Comunque preso $y \in \mathbb{R}$, si ha infatti che $y = \alpha(x)$, essendo $x = \frac{y}{2}$.

Alla stessa conclusione si giunge più rapidamente osservando che, per ogni fissato $y \in \mathbb{R}$, il problema espresso dall'equazione lineare $y = 2x$, ammette l'unica soluzione $x = \frac{y}{2}$. Tale ragionamento permette di individuare immediatamente l'applicazione inversa di α che sarà data da

$$\alpha^{-1} : \mathbb{R} \to \mathbb{R}, \quad \alpha^{-1}(x) = \frac{x}{2}.$$

Allora α, inquanto applicazione invertibile risulta biiettiva.
L'applicazione β non è iniettiva. Si nota infatti subito che risulta, ad es., $\beta(-1) = \beta(1) = 0$. β non è neppure suriettiva. Si osservi che, posto $y = x^2 - 1$, si ottiene $x = \pm\sqrt{y+1}$. Quest'ultima espressione ha senso (in $\mathbb{R}$) soltanto se $y \geq -1$. Allora, un qualunque numero reale y minore di -1 non potrà scriversi nella forma $\beta(x)$.
γ è biiettiva. Si può ragionare come sopra e concludere che γ ammette come inversa l'applicazione $\gamma^{-1} : \mathbb{R} \to \mathbb{R}$, definita da $\gamma^{-1}(x) = x - 2$.
Determiniamo le composizioni indicate:

$\alpha\beta : \mathbb{R} \to \mathbb{R}$ è definita da $\alpha\beta(x) = \alpha(\beta(x)) = \alpha(x^2 - 1) = 2(x^2 - 1)$.

$\beta\alpha : \mathbb{R} \to \mathbb{R}$ è definita da $\beta\alpha(x) = \beta(\alpha(x)) = \beta(2x) = 4x^2 - 1$.

$\alpha\beta\gamma : \mathbb{R} \to \mathbb{R}$ è definita da $\alpha\beta\gamma(x) = \alpha(\beta(\gamma(x))) = \alpha(\beta(x+2)) =$
$= \alpha((x+2)^2 - 1) = \alpha(x^2 + 4x + 3) = 2x^2 + 8x + 6.$

$\gamma\beta\alpha : \mathbb{R} \to \mathbb{R}$ è definita $\gamma\beta\alpha(x) = \gamma(\beta(\alpha(x))) = \gamma(\beta(2x)) =$
$= \gamma(4x^2 - 1) = 4x^2 + 1.$

Con ragionamenti analoghi a quelli precedenti, ci si rende conto facilmente che nessuna delle composizioni indicate è iniettiva oppure suriettiva. Occupiamoci, ad esempio, dell'applicazione $\alpha\beta\gamma$.
Per provare che essa non è suriettiva, sia $y \in \mathbb{R}$ e supponiamo che $y = 2x^2 + 8x + 6$. Risolvendo l'equazione di secondo grado in x, si ottiene $x = \frac{-2\pm\sqrt{2(2+y)}}{2}$. Allora, nel caso in cui sia $y < -2$, segue che y non può scriversi nella forma $\alpha\beta\gamma(x)$, per nessun numero reale x.
Supponiamo poi che $x_1, x_2 \in \mathbb{R}$ siano tali che $\alpha\beta\gamma(x_1) = \alpha\beta\gamma(x_2)$. Si ha allora:

$$x_1^2+4x_1 = x_2^2+4x_2 \Rightarrow x_1^2-x_2^2 = -4(x_1-x_2) \Rightarrow x_1+x_2 = 4 \Rightarrow x_2 = -x_1-4.$$

Per $x_1 = 1$ segue $x_2 = -5$ ed è facile verificare che $\alpha\beta\gamma(1) = 16 = \alpha\beta\gamma(-5)$, cosicchè $\alpha\beta\gamma$ non è iniettiva.
Alla stessa conclusione si poteva anche giungere osservando che la funzione $f(x) = 2x^2+8x+6$ è continua ed ammette come derivata prima la funzione $f'(x) = 2(2x + 4)$; allora, $f(x)$ è strettamente crescente quando $x > -2$ e strettamente decrescente per $x < -2$. Ne segue che devono esistere due valori delle ascisse $x_1 < -2 < x_2$, per i quali la funzione assume lo stesso valore.

1.6.9. Posto $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$, si considerino le applicazioni

$$\alpha : \mathbb{R} \to \mathbb{R}, \quad \alpha(x) = \sqrt[3]{x} + 1,$$

$$\beta : \mathbb{R} \to \mathbb{R}^+, \quad \beta(x) = 2e^x.$$

Mostrare che α, β sono invertibili e determinare $\alpha^{-1}, \beta^{-1}, (\beta\alpha)^{-1}$.

Per quanto riguarda α, si osservi che, per ogni $y \in \mathbb{R}$, si ha:

$$y = \sqrt[3]{x} + 1 \Rightarrow x = (y-1)^3,$$

allora α è invertibile e si ha $\alpha^{-1} : \mathbb{R} \to \mathbb{R}$, $\alpha^{-1}(x) = (x-1)^3$.
Anche β è invertibile, infatti per ogni $y \in \mathbb{R}$, si ha :

$$y = 2e^x \Rightarrow e^x = \frac{y}{2} \Rightarrow x = log\, e^x = log\, \frac{y}{2} = log\, y - log\, 2,$$

essendo *log* il logaritmo in base e (numero di Nepero). Segue che l'inversa $\beta^{-1} : \mathbb{R} \to \mathbb{R}$ è definita da $\beta^{-1}(x) = log\, x - log\, 2$.
L'applicazione $\beta\alpha : \mathbb{R} \to \mathbb{R}^+$ è definita da

$$\beta\alpha(x) = \beta(\alpha(x)) = \beta(\sqrt[3]{x} + 1) = 2e^{\sqrt[3]{x}+1}$$

ed è invertibile inquanto composizione di applicazioni invertibili.
Da $y = 2e^{\sqrt[3]{x}+1}$ si ottiene subito $x = (log\, y - log\, 2 - 1)^3$, allora risulta $(\beta\alpha)^{-1} : \mathbb{R}^+ \to \mathbb{R}$ definita da $(\beta\alpha)^{-1}(x) = (log\, x - log\, 2 - 1)^3$.

1.6.10. Provare che l'applicazione $f : \mathbb{N} \to \mathbb{Z}$, definita ponendo

$$f(n) = \begin{cases} \frac{n+1}{2} & \text{se } n \text{ è dispari,} \\ \\ -\frac{n}{2} & \text{se } n \text{ è pari oppure } n = 0. \end{cases}$$

è biiettiva.

Proviamo che f è iniettiva. Dati $m, n \in \mathbb{N}$, si devono distinguere i seguenti casi.

a) m ed n sono entrambi dispari. In tal caso $f(m) = f(n) \Rightarrow \frac{m+1}{2} = \frac{n+1}{2}$, da cui $m = n$.

b) m ed n sono entrambi pari. Allora $f(m) = f(n) \Rightarrow -\frac{m}{2} = -\frac{n}{2}$, quindi ancora $m = n$.

c) m è pari ed n è dispari (o viceversa). Si ha $f(m) = f(n) \Rightarrow \frac{m+1}{2} = -\frac{n}{2}$, da cui si ottiene $-n = m+1$. L'ultima relazione è evidentemente falsa, poichè m, n sono numeri naturali. Non può quindi accadere che $f(m)$ ed $f(n)$ abbiano lo stesso valore quando m ed n sono distinti.

Proviamo che f è suriettiva. Sia $z \in \mathbb{Z}$ un intero e sia $|z|$ il suo valore assoluto. Se z è negativo (oppure $z = 0$), si ha $z = -|z|$, con $|z| \in \mathbb{N}$. Risulta allora $z = -\frac{2|z|}{2} = f(2|z|)$.
Se invece z è positivo, risulta $z = \frac{n+1}{2} = f(n)$, ove si ponga $n = 2z - 1$. Si noti che $2z - 1 \in \mathbb{N}$ è dispari.

1.6.11. Date le applicazioni

$$f : \mathbb{R} \to \mathbb{R}^+, \quad f(x) = x^2, \quad g : \mathbb{R}^+ \to \mathbb{R}, \quad g(x) = \sqrt{x},$$

si determinino le composizioni gf ed fg e si verifichi che g è iniettiva, mentre f è suriettiva.

La composizione $gf : \mathbb{R} \to \mathbb{R}$ è definita da

$$gf(x) = g(f(x)) = g(x^2) = \sqrt{x^2} = |x|.$$

Ne segue che gf è l'applicazione valore assoluto $|-| : \mathbb{R} \to \mathbb{R}$.
La composizione $fg : \mathbb{R}^+ \to \mathbb{R}^+$ è definita da

$$fg(x) = f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x.$$

Segue che la composizione fg coincide con l'applicazione identica su $\mathbb{R}^+$. Siano ora $x_1, x_2 \in \mathbb{R}^+$; se $g(x_1) = g(x_2)$, allora anche $fg(x_1) = fg(x_2)$, quindi $x_1 = x_2$, cosicchè g è iniettiva.
Per la suriettività di f si osservi che, per ogni $y \in \mathbb{R}^+$, risulta $y = f(\sqrt{y})$.

1.7 Esercizi proposti.

1.7.1. Dati gli insiemi $A = \{1, 2, 3, a, b\}$, $B = \{2, q, m, p\}$, $C = \{1, 3, a, p\}$, determinare:

$$A \cup B, \quad A \cup C, \quad B \cup C, \quad A \cap B, \quad A \cap C, \quad B \cap C,$$

$$A \cup (B \cap C), \quad A \cap (B \cup C), \quad (A \cup) \cap (A \cup C).$$

1.7.2. Dati gli insiemi $A = \{1, 2, 3, a, b, c, d\}$, $\quad B = \{1, a, b\}$, $\quad C = \{2, a, d\}$, determinare:

$$B - C, \quad C - B, \quad B_A^c, \quad C_A^c, \quad (B \cup C)_A^c, \quad (B \cap C)_A^c.$$

1.7.3. Siano A, B, C insiemi. Dimostrare le seguenti uguaglianze :

$$A \cup (B \cup C) = (A \cup B) \cup C,$$

$$A \cap (B \cap C) = (A \cap B) \cap C,$$

$$A \cup B = B \cup A,$$

$$A \cap B = B \cap A.$$

1.7.4. Sia A un sottoinsieme di B. Mostrare che si ha:

$$(A^c)^c = A, \quad \emptyset^c = B, \quad B^c = \emptyset, \quad A - A = \emptyset, \quad A - \emptyset = A, \quad A \cup \emptyset = A,$$

$$A \cap \emptyset = \emptyset, \quad A \cup B = B, \quad A \cap B = A, \quad A \cup A = A, \quad A \cap A = A,$$

$$A \cup A^c = B, \quad A \cap A^c = \emptyset.$$

1.7.5. Dire quali delle seguenti applicazioni sono iniettive, suriettive, biiettive:

$\alpha : \mathbb{N} \to \mathbb{N}$ tale che $\alpha(x) = 2x + 1$,

$\beta : \mathbb{Q} \to \mathbb{Q}$ tale che $\beta(x) = 3x - 2$,

$\gamma : \mathbb{R} \to \mathbb{R}$ tale che $\gamma(x) = x^2 - 2x + 1$,

$\delta : \mathbb{R}^2 \to \mathbb{R}$ tale che $\delta(x_1, x_2) = x_2$.

1.7.6. Date le applicazioni α, β, γ di $\mathbb{R}$ in $\mathbb{R}$ definite da:

$$\alpha(x) = 3x + 2, \quad \beta(x) = 2x^2 - 1, \quad \gamma(x) = \frac{x - 2}{4},$$

determinare $\alpha\beta,\ \beta\alpha,\ \alpha\beta\gamma,\ \gamma\beta\alpha$.

Capitolo 2

RELAZIONI E OPERAZIONI

2.1 Relazioni

Una *relazione binaria* su un insieme A (o più semplicemente una relazione su A) è un sottoinsieme di $A \times A$. Data una relazione R su A, scriveremo aRb anzichè $(a, b) \in R$.

Esempio 2.1.1. Siano $A = \{2, 4, 5, 6\}$ e R definita da aRb se a divide b. Si ha allora $2R2$, $2R4$, $2R6$, $4R4$, $5R5$, $6R6$, che significa

$$R = \{(2,2), (2,4), (2,6).(4,4), (5,5).(6,6)\}.$$

Una relazione $\sim$ su un dato insieme A si dice una *relazione di equivalenza* se, per ogni $a, b, c \in A$, valgono le seguenti proprietà :

(i) $a \sim a$,

(ii) $a \sim b$ implica $b \sim a$,

(iii) $a \sim b$ e $b \sim c$ implica $a \sim c$.

La proprietà (i) si chiama proprietà *riflessiva*, la (ii) proprietà *simmetrica*, la (iii) proprietà *transitiva*.

Esempio 2.1.2. Sull'insieme $\mathbb{N}$ dei numeri naturali definiamo le relazioni:

aR_1b se a divide b,

aR_2b se $a > b$,

aR_3b se $b - a = 1$,

aR_4b se a e b sono entrambi pari o entrambi dispari.

La R_1 non gode della proprietà (ii), per la R_2 vale solo la proprietà (iii), la R_3 non verifica nessuna delle tre proprietà, la R_4 è una relazione di equivalenza.

Esempio 2.1.3. *Congruenze*.
Consideriamo l'insieme $\mathbb{Z}$ degli interi relativi, e sia n un numero naturale. Per ogni coppia di interi a e b, si dice che *a è congruo a b modulo n*, e si scrive

$$a \equiv b \,(\mathrm{mod}\, n)$$

se e solo se n divide $a - b$.
Dividendo a e b per n, ponendo cioè $a = \alpha n + r,\ b = \beta n + s$, con $\alpha, \beta, r, s \in \mathbb{Z}$ e con $0 \leq r < n,\ 0 \leq s < n$, si ha subito $a \equiv b \,(\mathrm{mod}\, n)$ se e solo se $r = s$.
È facile mostrare che la relazione così definita è di equivalenza. Infatti, risulta $a \equiv a \,(\mathrm{mod}\, n)$ poichè $a - a = 0n$. Se $a - b = an$ con $a \in \mathbb{Z}$, allora $b - a = (-a)n$, quindi da $a \equiv b \,(\mathrm{mod}\, n)$ segue $b = a \,(\mathrm{mod}\, n)$. Se poi $a - b = \alpha n$ e $b - c = \beta n$ con $\alpha, \beta \in \mathbb{Z}$, si ha $a - c = (\alpha + \beta)n$. Quindi $a \equiv b \,(\mathrm{mod}\, n)$ e $b = c \,(\mathrm{mod}\, n)$ implicano $a = c \,(\mathrm{mod}\, n)$.
Questa relazione, che qui è solo un esempio di relazione di equivalenza, sarà ripresa nell'ultimo capitolo, in quanto di fondamentale importanza per gli argomenti che vi sono svolti.

Una *partizione* di un insieme A è una famiglia di sottoinsiemi di A, ciascuno non vuoto, a due a due disgiunti e tali che la loro unione è A.

Teorema 2.1.1. *Una relazione di equivalenza sull'insieme A definisce una partizione di A e, viceversa, una partizione di A definisce una relazione di equivalenza su A.*

Dim. Sia $\sim$ una relazione di equivalenza su A. Per ciascun elemento a di A definiamo

$$[a] = \{x \in A \mid x \sim a\}.$$

L'insieme

$$\mathcal{P} = \{[a], [b], [c], ...\}$$

è una partizione di A. Infatti, osservando che $a \in [a] \subseteq A$ si ha subito

$$[a] \neq \emptyset \quad \text{per ogni} \quad a \in A \quad \text{e} \quad A = \bigcup_{a \in A} [a].$$

Se inoltre $[a]$ e $[b]$ non coincidono risulta $[a] \cap [b] = \emptyset$. Infatti se $x \in [a] \cap [b]$, si ha $x \sim a$ e $x \sim b$ cioè $a \sim b$. Ne segue, per ogni elemento y di $[a]$, $y \sim a \sim b$ e quindi $y \in [b]$. E analogamente, per ogni elemento y di, $[b]$, $y \sim b \sim a$ cioè

$y \in [a]$. Si ha allora $[a] = [b]$ che è assurdo.
Viceversa se $\mathcal{P}$ è una partizione di A, definendo $a \sim b$ se esiste un elemento H di $\mathcal{P}$ tale che $a, b \in H$, si ottiene una relazione di equivalenza su A. Infatti le proprietà (i) e (ii) seguono subito da

$$A = \bigcup_{H \in \mathcal{P}} H.$$

Per quanto riguarda la proprietà (iii), da $a \sim b$ e $b \sim c$ segue che esistono due elementi H e K di $\mathcal{P}$ tali che $a, b \in H$ e $b, c \in K$. Pertanto $H \cap K \neq \emptyset$, quindi $H = K$, da cui $a \sim c$. □

Dato un insieme A e data una relazione R di equivalenza su A, la partizione di A definita da R si indica con il simbolo A/R e i suoi elementi si chiamano *classi di equivalenza*. L'importanza della nozione di partizione indotta da una relazione di equivalenza sarà chiara fin dal successivo Esempio 2.3.3. Accadrà spesso, nel seguito, di dover operare con le classi di equivalenza di una partizione.

Esempio 2.1.4. *Classi di resto modulo n.*
La partizione di $\mathbb{Z}$ definita dalla relazione di equivalenza dell'esempio precedente si indica usualmente con $\mathbb{Z}/(n)$ e i suoi elementi $[a], [b], ...$, prendono il nome di *classi di resto modulo n*.
Si osservi che se a è un intero il cui resto della divisione per n è r, se cioè si ha $a = \alpha n + r$ con $\alpha \in \mathbb{Z}$, risulta $[a] = [r]$ e pertanto si mostra facilmente che gli elementi distinti di $\mathbb{Z}/(n)$ sono i seguenti:

$$\mathbb{Z}/(n) = \{[0], [1], ..., [n-1]\}.$$

2.2 Operazioni

Una *legge di composizione interna* (binaria) definita in un insieme A, o anche una *operazione interna* in A, è una applicazione di $A \times A$ in A. Quando l'operazione sia indicata ad esempio con il simbolo $\circ$, l'immagine dell'elemento (a, b) di $A \times A$ si denota con $a \circ b$. Una operazione interna $\circ$ definita in un insieme A ha un qualche rilievo se gode di alcune proprietà fondamentali. Si dice che l'operazione $\circ$ è *associativa* se gode della seguente proprietà:

$$(1) \qquad a \circ (b \circ c) = (a \circ b) \circ c \quad \text{per ogni} \quad a, b, c \in A.$$

Si dice che $\circ$ è *commutativa* se:

$$a \circ b = b \circ a \quad \text{per ogni} \quad a, b \in A. \tag{2}$$

Un elemento u di A si chiama *elemento neutro* rispetto all'operazione $\circ$ se:

$$a \circ \ u = u \circ a = a \quad \text{per ogni} \quad \in A. \tag{3}$$

Se esiste un elemento neutro esso è unico, se infatti u e u' sono sono elementi neutri rispetto a $\circ$, si ha subito

$$u' \circ u = u \circ u' = u = u'.$$

Quando l'operazione $\circ$ possiede l'elemento neutro u, si dice che un elemento a di A è *invertibile* se esiste un elemento $a' \in A$ tale che

$$a \circ a' = a' \circ a = u. \tag{4}$$

L'elemento a' si chiama *inverso di a* e, se l'operazione $\circ$ è associativa, esso è unico. Se infatti a' e a'' sono inversi di a si ottiene subito

$$a' = u \circ a' = (a'' \circ a) \circ a' = a'' \circ (a \circ a') = a'' \circ u = a''.$$

Esempio 2.2.1. Sia $\mathcal{P}(A)$ l'insieme dei sottoinsiemi di un dato insieme A. L'unione e l'intersezione sono operazioni interne in $\mathcal{P}(A)$. Entrambe sono associative e commutative. L'elemento neutro rispetto all'unione è $\emptyset$, l'elemento neutro rispetto all'intersezione è A.

2.3 Strutture algebriche

Un insieme A con una o piu operazioni $\circ, \times, ...$, si chiama una *struttura algebrica* e, quando sia conveniente, si indica con $(A, \circ, \times, ...)$.
Consideriamo due strutture algebriche $(A, \circ)$ e $(B, \times)$. Una applicazione $f : A \to B$ si dice un *omomorfismo* della struttura $(A, \circ)$ nella strutlura $(B, \times)$ se:

$$f(a \circ b) = f(a) \times f(b) \quad \text{per ogni} \quad a, b \in A. \tag{5}$$

Se inoltre f e biiettiva, prende il nome di *isomorfismo* e le strutture $(A, \circ)$ e $(B, \times)$ si dicono *isomorfe*. Un isomorfismo di una struttura algebrica in sè stessa si dice anche un *automorfismo*.

Esempio 2.3.1. Indichiamo con $\mathbb{R}^+$ l'insieme dei numeri reali positivi e sia a un numero reale positivo e diverso da 1. L'applicazione $x \mapsto a^x$ è biiettiva, inoltre $a^{x+y} = a^x \cdot a^y$ pertanto essa è un isomorfismo della struttura $(\mathbb{R}, +)$ sulla struttura $(\mathbb{R}^+, \cdot)$.

Teorema 2.3.1. *Sia f un isomorfismo della strullura algebrica $(A, \circ)$ sulla struttura algebrica $(B, \times)$.*
Se $\circ$ è associativa, allora $\times$ è associativa.
Se $\circ$ è commutativa, allora $\times$ è commutativa.
Se u è l'elememo neutro rispetto a $\circ$ allora $f(u)$ è l'elemento neutro rispetto a $\times$.
Se $a \in A$ è invertibile e a' è un suo suo inverso, allora $f(a)$ è invertibile e $f(a')$ è un suo inverso.

Dim. L'applicazione f è biiettiva, pertanto comunque si consideri un elemento b di B esiste ed è unico l'elemento a di A tale che $f(a) = b$.
Supponiamo $\circ$ associativa e siano b_1, b_2, b_3 elementi di B,

$$\begin{aligned} b_1 \times (b_2 \times b_3) &= f(a_1) \times [f(a_2) \times f(a_3)] = \\ &= f(a_1) \times f(a_2 \circ a_3) = f[a_1 \circ (a_2 \circ a_3)] = \\ &= f[(a_1 \circ a_2) \circ a_3] = f(a_1 \circ a_2) \times f(a_3) = \\ &= [f(a_1) \times f(a_2)] \times f(a_3) = (b_1 \times b_2) \times b_3 \end{aligned}$$

ne segue che anche l'operazione $\times$ è associativa.
Supponiamo ora che $\circ$ sia commutativa, per ogni b_1 e b_2 in B si ha

$$\begin{aligned} b_1 \times b_2 &= f(a_1) \times f(a_2) = f(a_1 \circ a_2) = \\ &= f(a_2 \circ a_1) = f(a_2) \times f(a_1) = b_2 \times b_1, \end{aligned}$$

quindi anche l'operazione $\times$ è commutativa. Sia $u \in A$ l'elemento neutro rispetto a $\circ$ e consideriamo un qualsiasi elemento b di B,

$$b \times f(u) = f(a) \times f(u) = f(a \circ u) = f(a) = b,$$

inoltre

$$f(u) \times b = f(u) \times f(a) = f(u \circ a) = f(a) = b,$$

pertanto $f(u)$ è l'elemento neutro rispetto a $\times$.
Se infine l'elemento $a \in A$ è invertibile e a' è un suo inverso, da

$$f(a) \times f(a') = f(a \circ a') = f(u),$$

e da

$$f(a') \times (a) = f(a' \circ a) = f(u),$$

segue che anche $f(a)$ è invertibile e $f(a')$ è un suo inverso. □

Sia G un insieme con una operazione interna $\circ$. Si dice che la struttura algebrica $(G, \circ)$ è un *gruppo*, oppure che G è un gruppo rispetto all'operazione $\circ$, se:

(g_1) l'operazione $\circ$ è associativa,

(g_2) esiste l'elemento neutro rispetto a $\circ$,

(g_3) ogni elemento di G è invertibile.

Se inoltre l'operazione $\circ$ è commutativa il gruppo $(G, \circ)$ si chiama *commutativo* o *abeliano*.
Dato un sottoinsieme non vuoto H di G, se per ogni $a, b \in H$ si ha $a \circ b \in H$, l'operazione $\circ$ è una operazione interna in H. In questo caso, se la struttura algebrica $(H, \circ)$ è a sua volta un gruppo, si dice che è un *sottogruppo* di $(G, \circ)$.

Esempio 2.3.2. Siano $+$ e $\cdot$ le operazioni di addizione e moltiplicazione fra numeri reali. Poniamo inoltre

$$\mathbb{R}^* = \mathbb{R} - \{0\}, \quad \mathbb{Q}^* = \mathbb{Q} - \{0\}, \quad \mathbb{Z}^* = \mathbb{Z} - \{0\}.$$

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sono gruppi commutativi con elemento neutro 0, l'inverso del numero a è $-a$. $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ sono gruppi commutativi con elemento neutro 1, l'inverso del numero a è $1/a$. $(\mathbb{Z}^*, \cdot)$ non è un gruppo.

Consideriamo un insieme K con due operazioni interne, una detta di *addizione* e indicata con $+$, l'altra detta di *moltiplicazione* e indicata con $\cdot$. Si dice che la struttura algebrica $(K, +, \cdot)$ è un *campo* se:

(c_1) la struttura algebrica $(K, +)$ è un gruppo commutativo,

(c_2) indicato con 0 l'elemento neutro rispetto all'operazione di addizione $+$ e posto $K^* = K - \{0\}$, la struttura algebrica $(K^*, \cdot)$ è un gruppo commutativo,

(c_2) vale la seguente proprietà *distributiva*:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{per ogni} \quad a, b, c \in K.$$

L'elemento neutro 0 della proprietà c_2 si chiama *lo zero* del campo, l'elemento neutro della moltiplicazione si indica invece con 1 e si chiama *l'unità* del campo. Dato un sottoinsieme non vuoto H di K, se le operazioni $+$ e $\cdot$ sono operazioni interne in H e la struttura algebrica $(H, +, \cdot)$ è a sua volta un campo, si dice che $(H, +, \cdot)$ è un *sottocampo* di $(K, +, \cdot)$.

La nozione di campo sarà ripresa nell'ultimo capitolo, nel seguito il lettore potrà fare riferimento al campo dei numeri reali $(\mathbb{R}, +, \cdot)$ o al suo sottocampo dei numeri razionali $(\mathbb{Q}, +, \cdot)$. Si osservi che $(\mathbb{Z}, +, \cdot)$ non è un campo.

Esempio 2.3.3. Dato un numero naturale n, consideriamo l'insieme delle classi di resto modulo n:

$$\mathbb{Z}/(n) = \{[0], [1], ..., [n-1]\}$$

e definiamo in esso le seguenti operazioni:

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

$$[a] \cdot [b] = [a \cdot b].$$

Si osservi che le operazioni che compaiono a destra delle uguaglianze sono l'addizione e la moltiplicazione fra numeri interi relativi, da non confondersi quindi con le operazioni a sinistra delle uguaglianze che sono quelle definite ora. Tali operazioni sono ben definite, nel senso che le classi di resto $[a + b]$ e $[a \cdot b]$ non dipendono dalla scelta degli elementi a e b. Più precisamente se $a' \in [a]$ e $b' \in [b]$, si ha $a' - a = \alpha n$ e $b' - b = \beta n$, con $\alpha, \beta \in \mathbb{Z}$, pertanto

$$(a' + b') - (a + b) = (\alpha + \beta)n$$

e

$$a' \cdot b' - a \cdot b = (\alpha \cdot b' + \beta \cdot a)n.$$

Ne segue

$$(a' + b') \in [a + b] \quad \text{e} \quad (a' \cdot b') \in [a \cdot b]$$

cioè

$$[a' + b'] = [a + b] \quad \text{e} \quad [a' \cdot b'] = [a \cdot b].$$

Si mostra facilmente che la struttura $(\mathbb{Z}/(n), +)$ è un gruppo commutativo, l'elemento neutro rispetto all'addizione è $[0]$, l'inverso di $[a]$ rispetto all'addizione è $-[a] = [-a]$. La struttura algebrica $(\mathbb{Z}/(n) - \{[0]\}, \cdot)$ non è in generale un gruppo, anche se l'operazione $\cdot$ è associativa e commutativa ed esiste l'elemento neutro che è $[1]$. Vale inoltre la proprietà distributiva:

$$[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a \cdot (b + c)] = [a \cdot b + a \cdot c] =$$

$$= [a \cdot b] + [a \cdot c] = [a] \cdot [b] + [a] \cdot [c].$$

2.4 Permutazioni

Un importante esempio di gruppo finito (il motivo della sua importanza sarà chiarito nel penultimo capitolo) è quello delle permutazioni su n oggetti. Dato un numero naturale n, sia S un insieme di n oggetti che rappresenteremo con i primi n numeri naturali:

$$S = \{1, 2, ..., n\}.$$

Una *permutazione su S* è una biiezione di S in S. L'insieme di tutte le permutazioni su S si denota con S_n. Il prodotto di due permutazioni su S, nel senso di composizione di applicazioni, è ancora una permutazione su S. Si ha così una operazione interna in S_n e, ricordando quanto detto nel Capitolo 1 sulle biiezioni, si mostra subito che S_n con questa operazione è un gruppo, non commutativo, con elemento neutro id_S. Esso è detto il *gruppo simmetrico* su n oggetti.
Data una permutazione α di S_n si scrive usualmente

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix},$$

anzichè $\alpha(1) = i_1$, $\alpha(2) = i_2$, $\cdots$, $\alpha(n) = i_n$.

Esempio 2.4.1. Sia $A = \{1, 2, 3, 4, 5, 6\}$. Se

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 2 & 5 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 3 & 6 \end{pmatrix},$$

allora

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 5 & 2 \end{pmatrix}, \quad \beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix},$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 2 & 1 & 4 \end{pmatrix}, \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 2 & 3 & 4 \end{pmatrix}.$$

Una permutazione α di S_n che scambia due elementi distinti di A e lascia fissi tutti gli altri si chiama una *trasposizione*. Usando la notazione precedente α è del tipo

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & h & \cdots & k & \cdots & n \\ 1 & 2 & \cdots & k & \cdots & h & \cdots & n \end{pmatrix},$$

e si potrà indicare semplicemente con $\alpha = (hk)$.

Teorema 2.4.1. *Ogni permutazione di S_n, $(n \geq 2)$ si può esprimere come prodotto di trasposizioni.*

Dim. Ogni permutazione α di S_n tale che $\alpha(n) = n$ può essere riguardata come una permutazione di S_{n-1} e viceversa, ogni permutazione di S_{n-1} si può considerare come una permutazione di S_n che fissa n. Ciò posto, procediamo per induzione su n. Per $n = 2$ il teorema è banalmente vero. Supponiamo vera l'affermazione per $n - 1$ e consideriamo una permutazione α di S_n. Se

$\alpha(n) = h$, sia τ la trasposizione di S_n definita da $\tau(n) = h$ e $\tau(h) = n$. Risulta allora $\tau\alpha(n) = n$ e pertanto esistono, in S_{n-1}, le trasposizioni $\tau_1, \cdots, \tau_r$, tali che $\tau\alpha = \tau_1 \cdots \tau_r,$. Si può allora scrivere in $S_n \quad \alpha = \tau^{-1}\tau_1 \cdots \tau_r$. □

Teorema 2.4.2. *Esiste una applicazione $\varepsilon : S_n \to \{1, -1\}$ con le seguenti proprietà:*

(p_1) *per ogni $\alpha, \beta \in S_n$ si ha $\varepsilon(\alpha\beta) = \varepsilon(\alpha)\varepsilon(\beta)$,*

(p_2) *per ogni trasposizione $\tau \in S_n$ si ha $\varepsilon(\tau) = -1$.*

Dim. Consideriamo una permutazione α e poniamo:

$$C = \{(i, j) \in S^2 \mid i < j\},$$
$$C' = \{(i, j) \in C \mid \alpha(i) < \alpha(j)\},$$
$$C'' = \{(i, j) \in C \mid \alpha(i) > \alpha(j)\}.$$

Si ha ovviamente $C = C' \cup C''$. Detto t il numero degli elementi di C'', definiamo $\varepsilon(\alpha) = (-1)^t$. Consideriamo ora il prodotto

$$\Gamma_\alpha = \prod_{(i,j)\in C} [\alpha(j) - \alpha(i)],$$

che può scriversi

$$\Gamma_\alpha = \prod_{(i,j)\in C'} [\alpha(j) - \alpha(i)] \prod_{(i,j)\in C''} [\alpha(j) - \alpha(i)].$$

I fattori del primo prodotto sono positivi mentre quelli del secondo prodotto sono negativi, pertanto si ha:

$$\Gamma_\alpha = \prod_{(i,j)\in C'} [\alpha(j) - \alpha(i)](-1)^t \prod_{(i,j)\in C''} [\alpha(j) - \alpha(i)],$$

L'applicazione $(i, j) \mapsto (\alpha(i), \alpha(j))$, per $(i, j) \in C'$, e $(i, j) \mapsto (\alpha(i), \alpha(j))$ per $(i, j) \in C''$, è come si verifica facilmente una biiezione di C in C, pertanto l'insieme costituito dalle coppie $(\alpha(i), \alpha(j))$ con $(i, j) \in C'$ e dalle coppie $(\alpha(i), \alpha(j))$ con $(i, j) \in C''$, è ancora C. Ne segue

$$\Gamma_\alpha = \varepsilon(\alpha) \prod_{(i,j)\in C} (j - i).$$

Se α e β sono due qualsiasi permutazioni di S_n si ha

$$\Gamma_{\alpha\beta} = \prod_{i<j}[\alpha\beta(j) - \alpha\beta(i)] = \varepsilon(\alpha\beta)\prod_{i<j}(j-i),$$

e d'altra parte

$$\Gamma_{\alpha\beta} = \prod_{i<j}[\alpha\beta(j) - \alpha\beta(i)] = \varepsilon(\alpha)\prod_{i<j}[\beta(j) - \beta(i)] = \varepsilon(\alpha)\varepsilon(\beta)\prod_{i<j}(j-i),$$

ne segue $\varepsilon(\alpha\beta) = \varepsilon(\alpha)\varepsilon(\beta)$. Sia ora τ una trasposizione:

$$\tau = (hk) = \begin{pmatrix} 1 & \cdots & h\cdots & k & \cdots & n \\ 1 & \cdots & k\cdots & h & \cdots & n \end{pmatrix}.$$

Gli elementi di C'' in questo caso sono le coppie (h,j) con $h < j < k$ e le coppie (i,k) con $h < i < k$. Le prime sono in numero pari a $k-h$ mentre le seconde sono $k-h-1$, dunque C'' contiene un numero dispari di coppie e quindi $\varepsilon(\tau) = -1$. □

Il teorema precedente permette alcune rilevanti osservazioni:

(a) Se una permutazione α di S_n si esprime in due modi diversi come prodotto di r trasposizioni e di s trasposizioni, allora gli interi positivi r e s sono entrambi pari o entrambi dispari. Basti osservare infatti che da

$$\alpha = \tau_1 \cdots \tau_r = \tau'_1 \cdots \tau'_s$$

segue

$$\varepsilon(\alpha) = \varepsilon(\tau_1)\cdots\varepsilon(\tau_r) = \varepsilon(\tau'_1)\cdots\varepsilon(\tau'_s).$$

Quindi r e s non possono essere uno pari e l'altro dispari, altrimenti il secondo e il terzo membro della precedente avrebbero segno discorde.

(b) Per ogni permutazione α di S_n si ha $\varepsilon(\alpha) = 1$ oppure $\varepsilon(\alpha) = -1$ se e solo se α si esprime, rispettivamente, come prodotto di un numero pari di trasposizioni o come prodotto di un numero dispari di trasposizioni. Si dice che α è una ***permutazione pari*** se $\varepsilon(\alpha) = 1$, se invece $\varepsilon(\alpha) = -1$ si dice che α è una ***permutazione dispari***, $\varepsilon(\alpha)$ si chiama il ***segno*** di α. Si osservi che risulta $\varepsilon(id) = 1$.

(c) Per ogni permutazione α di S_n si ha

$$\varepsilon(\alpha) = \varepsilon(\alpha^{-1}).$$

Infatti

$$\varepsilon(\alpha)\varepsilon(\alpha^{-1}) = \varepsilon(\alpha\alpha^{-1}) = \varepsilon(id) = 1,$$

quindi $\varepsilon(\alpha)$ e $\varepsilon(\alpha^{-1})$ sono entrambi 1 o entrambi -1.

Osservazione 2.4.3. *Cicli di una permutazione*.
Sia α una permutazione di S_n tale che

$$\alpha(i_1) = i_2,\ \alpha(i_2) = i_3,\ \cdots,\ \alpha(i_h) = i_1.$$

La permutazione

$$\overline{\alpha} = \begin{pmatrix} i_1 & i_2 & \cdots & i_h & i_{h+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i_{h+1} & \cdots & i_n \end{pmatrix},$$

si dice un *ciclo di* α e si indica brevemente con $\overline{\alpha} = (i_1 i_2 ... i_h)$. La scrittura di $\overline{\alpha}$ come prodotto di trasposizioni è semplice, in quanto:

$$\overline{\alpha} = (i_1 i_h)(i_1 i_{h-1}) \cdots (i_1 i_2).$$

Determinando i cicli di α si può allora scriverla come prodotto di trasposizioni. Ad esempio se α è la seguente permutazione di S_9 :

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 3 & 9 & 2 & 1 & 6 & 4 & 8 \end{pmatrix}.$$

i suoi cicli sono

$$\alpha_1 = (176), \quad \alpha_2 = (25), \quad \alpha_3 = (498).$$

Si verifica allora facilmente che si ha $\alpha = \alpha_1\alpha_2\alpha_3$. Ma

$$\alpha_1 = (16)(17), \quad \alpha_3 = (48)(49).$$

quindi

$$\alpha = (16)(17)(25)(48)(49).$$

2.5 Numeri complessi

II campo dei numeri complessi, che insieme con quello dei numeri reali ricorre in tutti i capitoli successivi, si ottiene a partire dall'insieme $\mathbb{R}^2$ delle coppie ordinate di numeri reali, definendo in $\mathbb{R}^2$ le seguenti operazioni di addizione e moltiplicazione:

$$(a,b)+(c,d)=(a+c,b+d), \tag{6}$$

$$(a,b)\cdot(c,d)=(ac-bd,ad+be), \tag{7}$$

per tutte le coppie $(a,b),(c,d)\in\mathbb{R}^2$.
La dimostrazione che le operazioni cosi definite soddisfano le condizioni $(c_1),(c_2),(c_3)$ è un semplice esercizio, pertanto la struttura algebrica $(\mathbb{R}^2,+,\cdot)$ è un campo, esso si denota con $\mathbb{C}$ e prende il nome di *campo dei numeri complessi*. L'elemento neutro dell'addizione è $(0,0)$, mentre quello della moltiplicazione è $(1,0)$. L'inverso additivo del numero complesso (a,b) è $-(a,b)=(-a,-b)$ e, quando $(a,b)\neq(0,0)$, il suo inverso moltiplicativo è

$$(a,b)^{-1}=(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}).$$

La nozione di omomorfismo (e quella di isomorfismo) fra strutture algebriche data nel Paragrafo 2.3, si estende come segue al caso specifico di due campi C_1 e C_2. Usando gli stessi simboli $+$ e $\cdot$ per indicare le due operazioni di C_1 e C_2, un *omomorfismo* del campo C_1 nel campo C_2 (nel caso biiettivo un *isomorfismo*) è una applicazione $f:C_1\to C_2$ tale che

$$f(x+y)=f(x)+f(y)$$

e

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

per ogni $x,y\in C_1$.
Ciò premesso, si consideri l'insieme di numeri complessi

$$C'=\{(a,b)\in\mathbb{C}\mid b=0\}.$$

è facilmente verificabile che C' è un sottocampo di $\mathbb{C}$ e che l'applicazione $a\mapsto(a,0)$ è un isomorfismo del campo $\mathbb{R}$ nel campo C'. In virtù di questo isomorfismo, che si chiama *immersione di* $\mathbb{R}$ *in* $\mathbb{C}$, si può identificare $\mathbb{R}$ con C' e si pone:

$$a=(a,0)\qquad\text{per ogni}\qquad a\in\mathbb{R}.$$

Il numero complesso $(0,1)$ si chiama *l'unita immaginaria* e si denota con i. Poichè

$$i^2=(0,1)\cdot(0,1)=(-1,0)=-1,$$

il numero i è una radice in $\mathbb{C}$ dell'equazione $x^2=-1$. Per ogni numero complesso (a,b) risulta

$$(a,b)=(a,0)+(0,1)\cdot(b,0).$$

Potremo quindi scrivere $(a, b) = a + ib$, ignorando deliberatamente il segno della moltiplicazione, in quanto l'utilità di questa rappresentazione risiede nel fatto di poter sommare e moltiplicare numeri complessi come se le operazioni fossero quelle fra numeri reali.

Esempio 2.5.1. Determiniamo la somma e il prodotto dei due numeri complessi $(-1, 3)$ e $(4, 2)$:

$$-1 + 3i + 4 + 2i = 3 + 5i = (3, 5),$$

$$(-1 + 3i)(4 + 2i) = -4 - 2i + 12i + 6i^2 = -10 + 10i = (-10, 10).$$

Si chiama *coniugato* del numero complesso $z = a+ib$ il numero complesso $\overline{z} = a - ib$. L'applicazione $z \mapsto \overline{z}$ è un automorfismo del campo $\mathbb{C}$ e prende il nome di *coniugio*. Si osservi che si ha $z = \overline{z}$ se e solo se z è un numero reale.

Esempio 2.5.2. Scrivere il numero complesso

$$\frac{-2i - 3(-i + 1)}{i + 2}$$

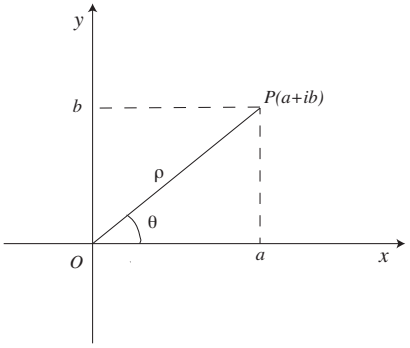
nella forma $a + ib$:

$$\frac{-2i - 3(-i + 1)}{i + 2} = \frac{i - 3}{i + 2} = \frac{(i - 3)(i - 2)}{(i + 2)(i - 2)} = \frac{-5i + 5}{-5} = -1 + i.$$

Determinare l'inverso moltiplicativo del numero complesso $2i - 1$:

$$\frac{1}{2i - 1} = \frac{2i + 1}{(2i - 1)(2i + 1)} = \frac{2i + 1}{-5} = -\frac{1}{5} - \frac{2}{5}i.$$

I numeri complessi si possono rappresentare con i punti del piano reale non appena si fissi un sistema di riferimento cartesiano come in figura. Il punto P di coordinate (a, b) rappresenta il numero complesso $z = a + ib$. I numeri reali sono rappresentati dai punti dell'asse x.



Indichiamo con ρ la distanza di P da O e con θ la misura (definita a meno di multipli di 2π) dell'angolo che il semiasse positivo x forma con la semiretta OP. I

numeri reali ρ e θ si chiamano rispettivamente *modulo* e *argomento* di z, il modulo di z si indica anche $|z|$. Si osservi che l'argomento di 0 è indeterminato. Da

$$a = \rho\cos\theta \quad \text{e} \quad b = \rho\sin\theta$$

segue

$$z = a + ib = \rho(\cos\theta + i\sin\theta), \tag{8}$$

che prende il nome di *rappresentazione trigonometrica* del numero complesso z.

Osservazione 2.5.1. Sono dati i numeri complessi

$$z = \rho(\cos\theta + i\sin\theta) \quad \text{e} \quad w = \nu(\cos\phi + i\sin\phi).$$

Si ha allora:

$$zw = \rho\nu[\cos(\theta+\phi) + i\sin(\theta+\phi)]$$

e (per $w \neq 0$)

$$\frac{z}{w} = \frac{\rho}{\nu}[\cos(\theta-\phi) + i\sin(\theta-\phi)].$$

Infatti

$$zw = \rho\nu[(\cos\theta\cos\phi - \sin\theta\sin\phi) + i(\sin\theta\cos\phi + \cos\theta\sin\phi)] =$$

$$= \rho\nu[\cos(\theta+\phi) + i\sin(\theta+\phi)].$$

$$\frac{z}{w} = \frac{\rho(\cos\theta + i\sin\theta)}{\nu(\cos\phi + \sin\phi)} = \frac{\rho(\cos\theta + i\sin\theta)(\cos\phi - i\sin\phi)}{\nu(\cos\phi + \sin\phi)(\cos\phi - i\sin\phi)} =$$

$$= \frac{\rho}{\nu}\frac{(\cos\theta\cos\phi + \sin\theta\sin\phi) + i(\sin\theta cos\phi - \cos\theta\sin\phi)}{cos^2\phi + \sin^2\phi} =$$

$$= \frac{\rho}{\nu}[\cos(\theta-\phi) + i\sin(\theta-\phi)].$$

Osservazione 2.5.2. *Radici n-esime di un numero complesso*.
Dati un numero complesso $z = \rho(\cos\theta + i\sin\theta)$ ed un numero intero positivo n, determinare le radici n-esime di z, ovvero le soluzioni dell'equazione

$$x^n = z.$$

Posto $x = r(\cos\phi + i\sin\phi)$, si ha

$$r^n = \rho \quad \text{e} \quad n\phi = \theta + 2k\pi \quad \text{con} \quad k \in \mathbb{Z}.$$

cioè

$$r = \sqrt[n]{\rho} \quad \text{e} \quad \phi = \frac{\theta + 2k\pi}{n} \quad \text{con} \quad k \in \mathbb{Z}.$$

Ma se k_1 e k_2 sono due interi relativi appartenenti alla stessa classe di resto modulo n (si veda l'Esempio 2.1.4), da

$$k_1 - k_2 = \alpha n \quad \text{con} \quad \alpha \in \mathbb{Z}$$

segue

$$\phi_1 - \phi_2 = \frac{\theta + 2k_1\pi}{n} - \frac{\theta + 2k_2\pi}{n} = 2\alpha\pi$$

e viceversa. Le radici n-esime di z sono quindi n e si ottengono per

$$k = 0, 1, \cdots, n-1.$$

Esempio 2.5.3. Determiniamo le radici quarte del numero complesso 1. Con la stessa notazione dell'esempio precedente, si ha in questo caso $\rho = 1$ e $\theta = 0$.
Ne segue

$$r = 1 \quad \text{e} \quad \phi = \frac{2k\pi}{4}$$

per $k = 0, 1, 2, 3$. Le quattro radici quarte di 1 (due di esse in $\mathbb{R}$) sono quindi:

$$x_0 = \cos 0 + i \sin 0 = 1,$$
$$x_1 = \cos \frac{\pi}{2} + i \sin \frac{\pi}{2} = i,$$
$$x_2 = \cos \pi + i \sin \pi = -1,$$
$$x_3 = \cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2} = -i.$$

2.6 Esercizi svolti

2.6.1. Nell'insieme $\mathcal{P}(S)$ dei sottinsiemi di S, si definiscano operazioni di somma e prodotto, come segue:

$$A + B = (A - B) \cup (B - A),$$

$$A \cdot B = A \cap B.$$

Si provi che $(\mathcal{P}(S), +)$ è un gruppo commutativo, mentre $(\mathcal{P}(S), \cdot)$ non è un gruppo. Si provi inoltre che vale la proprietà distributiva

$$A \cdot (B + C) = A \cdot B + A \cdot C.$$

L'operazione di somma in $\mathcal{P}(S)$

- è commutativa.

Infatti :

$$A + B = (A - B) \cup (B - A) = (B - A) \cup (A - B) = B + A.$$

- ammette $\emptyset$ come elemento neutro.

Infatti :

$$A + \emptyset = (A - \emptyset) \cup (\emptyset - A) = A, \quad \text{per ogni} \quad A \in \mathcal{P}(S).$$

- ammette inverso di ogni elemento.

Infatti:

$$A + A = (A - A) \cup (A - A) = \emptyset, \quad \text{per ogni} \quad A \in \mathcal{P}(S),$$

cosicchè ogni elemento di $\mathcal{P}(S)$ è invertibile, rispetto all'operazione di somma, ed è inverso di sè stesso.

- la proprietà associativa richiede più impegno per essere dimostrata.

Per raggiungere lo scopo conviene provare che entrambi gli insiemi $A + (B + C)$ e $(A + B) + C$ coincidono con l'insieme

$$(A \cap B \cap C) \cup (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cap (A^c \cap B^c \cap C).$$

Limitiamoci ad una delle due dimostrazioni.

$$A + (B + C) = [A - (B + C)] \cup [(B + C) - A] =$$

$$= \{A - [(B - C) \cap (C - B)]\} \cup \{[(B - C) \cap (C - B)] - A\} =$$

$$= \{A \cap [(B - C) \cap (C - B)]^c\} \cup \{[(B - C) \cap (C - B)] \cap A^c\} =$$

$$= \{A \cap [(B - C)^c \cap (C - B)^c]\} \cup \{[(B - C) \cap (C - B)] \cap A^c\} =$$

$$= \{A \cap [(B \cap C^c)^c \cap (C \cap B^c)^c]\} \cup \{[(B \cap C^c) \cap (C \cap B^c)] \cap A^c\} =$$

$$= \{A \cap [(B^c \cup C) \cap (C^c \cup B)]\} \cup \{[(B \cap C^c) \cap (C \cap B^c)] \cap A^c\} =$$

$$= \{A \cap [((B^c \cup C) \cap C^c) \cup [((B^c \cup C) \cap B)]\} \cup \{(A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C)\} =$$

$$= \{(A \cap B^c \cap C^c) \cup (A \cap B \cap C)\} \cup \{(A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C)\} =$$
$$= (A \cap B \cap C) \cup (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cap (A^c \cap B^c \cap C).$$

Si noti che nel corso della dimostrazione abbiamo largamente fatto uso delle Leggi di De Morgan e delle proprietà associativa e distributiva dell'unione e dell'intersezione.

Si noti che $(\mathcal{P}(S), \cdot)$ è una struttura commutativa e associativa, che ammette come elemento neutro l'insieme ambiente S. Essa non costituisce però un gruppo inquanto, dato un elemento $A \in \mathcal{P}(S)$, $A \neq S$, non esiste il suo inverso, rispetto all'operazione data.

Per quanto riguarda la proprietà distributiva, si ha:

$$A \cdot (B + C) = A \cap [(B - C) \cup (C - B)] =$$
$$= [(A \cap (B - C)) \cup (A \cap (C - B))] =$$
$$= ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B)) =$$
$$= (A \cap B) + (A \cap C) = A \cdot B + A \cdot C.$$

2.6.2. Sia $\mathbb{Z}/(n) = \{[0], [1], ..., [n-1]\}$ il gruppo additivo delle classi di resto modulo n. Esiste un omomorfismo ϕ, suriettivo ma non iniettivo, del gruppo additivo $\mathbb{Z}$ degli interi nel gruppo additivo $\mathbb{Z}/(n)$.

Si definisca $\phi : \mathbb{Z} \to \mathbb{Z}/(n)$, ponendo $\phi(a) = [a]$. Tale applicazione è un omomorfismo poichè, in base alla definizione di addizione in $\mathbb{Z}/(n)$, vedi Esempio 2.3.3, segue

$$\phi(a + b) = [a + b] = [a] + [b] = \phi(a) + \phi(b).$$

Per la suriettività, si osservi che, per ogni $[a] \in \mathbb{Z}/(n)$, si ha evidentemente $[a] = \phi(a)$. L'omorfismo ϕ non è iniettivo, inquanto per qualunque coppia di interi a, b, tali che $a - b = \alpha n$, per qualche $\alpha \in \mathbb{Z}$, si ha $[a] = [b]$ e quindi $\phi(a) = \phi(b)$.

2.6.3. Provare che $\mathbb{Z}/(5)$ e $\mathbb{Z}/(7)$ sono campi, mentre $\mathbb{Z}/(6)$ e $\mathbb{Z}/(9)$ non lo sono.

Sappiamo che $\mathbb{Z}/(n)$ non è in generale un campo, dipendendo questo dal fatto che non sempre i suoi elementi, diversi da $[0]$, ammettono inverso moltiplicativo.

Si ricordi che in $\mathbb{Z}/(n)$ si ha $[a] = [b]$, se e solo se a e b danno lo stesso resto rispetto alla divisione per n.

In $\mathbb{Z}/(5)$ si ha : $[1]\cdot[1] = [1],\ [2]\cdot[3] = [6] = [1],\ [3]\cdot[2] = [6] = [1],\ [4]\cdot[4] = [16] = [1]$.

In $\mathbb{Z}/(7)$ si ha : $[1]\cdot[1] = [1],\ [2]\cdot[4] = [8] = [1],\ [3]\cdot[5] = [15] = [1],\ [4]\cdot[2] = [8] = [1],\ [5]\cdot[3] = [15] = [1],\ [6]\cdot[6] = [36] = [1]$.

Allora tutti gli elementi non nulli di $\mathbb{Z}/(5)$ e di $\mathbb{Z}/(7)$ sono invertibili.

In $\mathbb{Z}/(6)$ l'elemento $[2]$ non ammette inverso moltiplicativo, infatti: $[2]\cdot[1] = [2],\quad [2]\cdot[2] = [4],\ [2]\cdot[3] = [6] = [0],\ [2]\cdot[4] = [8] = [2],\ [2]\cdot[5] = [10] = [4]$.

In $\mathbb{Z}/(9)$ l'elemento $[3]$ non ammette inverso moltiplicativo, infatti : $[3]\cdot[1] = [3],\quad [3]\cdot[2] = [6],\ [3]\cdot[3] = [9] = [0]\ [3]\cdot[4] = [12] = [3],\ [3]\cdot[5] = [15] = [6],\ [3]\cdot[6] = [18] = [0],\ [3]\cdot[7] = [21] = [3],\ [3]\cdot[8] = [24] = [6]$.

2.6.4. Nell'insieme $\mathbb{Z}\times\mathbb{Z}$ si definiscano le seguenti relazioni :

(1) $(r,s)\sim(u,v) \Leftrightarrow rv = su$,

(2) $(r,s)\sim(u,v) \Leftrightarrow r+u = s+v$.

Si provi che entrambe sono relazioni di equivalenza.

Proviamo soltanto la (1), l'altra si prova analogamente.
La relazione è simmetrica : da $rs = sr$ segue $(r,s)\sim(r,s)$.
La relazione è riflessiva : da $(r,s)\sim(u,v)$ si ottiene $rv = su$, quindi anche $su = rv$, da cui $(u,v)\sim(r,s)$.
La relazione è transitiva : da $(r,s)\sim(u,v)$ e da $(u,v)\sim(x,y)$ si ottiene $rv = su$ ed $ux = vy$. Allora, $ury = uyr = vxr = rvx = sux = usx$ da cui $ry = sx$, quindi $(r,s)\sim(x,y)$.

2.6.5. Nell'insieme delle rette (rispettivamente, dei piani) dello spazio Euclideo, il parallelismo è una relazione di equivalenza.

La nozione di parallelismo è quella usuale: due rette complanari sono parallele se coincidono oppure non hanno punti a comune. È immediato allora rendersi conto di quanto segue.
Ogni retta è parallela a se stessa (riflessività). Se una retta r è parallela ad una retta s, allora s è parallela ad r (simmetria). Se r è parallela ad s ed s è parallela a t, segue che r è parallela a t (transitività). Analogamente per i piani, intendendo che due piani sono paralleli se se coincidono oppure non hanno punti a comune.
Rispetto alla relazione di parallelismo, una classe di equivalenza di rette si chiama una *direzione*, mentre una classe di equivalenza di piani prende il nome di *giacitura*.

2.6.6. Provare che il gruppo simmetrico S_n ha $n! = 1 \cdot 2 \cdot ... \cdot n$ elementi.

Un elemento di S_n è una biiezione dell'insieme $\{1, 2, ..., n\}$ in sé. Definiamo un tale elemento α. Per assegnare il valore $\alpha(1)$ abbiamo a disposizione n scelte. Per il valore $\alpha(2)$, le scelte sono n, meno quella già impegnata, quindi $n-1$ scelte. Per il valore $\alpha(3)$ le scelte saranno $n-2$, e così via. In definitiva potremo definire α in $n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 1 = n!$ modi diversi.

2.6.7. Si considerino le permutazioni di S_6

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 2 & 3 \end{pmatrix} \quad .$$

Si calcolino $\alpha^{-1},\ \beta^{-1},\ \alpha\beta,\ \beta\alpha$.

α e β sono biiezioni, pertanto sono invertibili. Si noti che:

$$\alpha(1) = 2,\ \alpha(2) = 4,\ \alpha(3) = 1,\ \alpha(4) = 3,\ \alpha(5) = 6,\ \alpha(6) = 5$$

allora

$$\alpha^{-1}(1) = 3,\ \alpha^{-1}(2) = 1,\ \alpha^{-1}(3) = 4,\ \alpha^{-1}(4) = 2,\ \alpha^{-1}(5) = 6,\ \alpha^{-1}(6) = 5,$$

cosicchè si può scrivere

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 6 & 5 \end{pmatrix}.$$

Allo stesso modo si vede che

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 2 & 1 & 4 \end{pmatrix}.$$

Per quanto riguarda $\alpha\beta$, si ricordi che la composizione di permutazioni è definita come composizione di applicazioni, quindi

$$(\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(5) = 6,$$
$$(\alpha\beta)(2) = \alpha(\beta(2)) = \alpha(4) = 3,$$
$$(\alpha\beta)(3) = \alpha(\beta(3)) = \alpha(1) = 2,$$
$$(\alpha\beta)(4) = \alpha(\beta(4)) = \alpha(6) = 5,$$
$$(\alpha\beta)(5) = \alpha(\beta(5)) = \alpha(2) = 4,$$
$$(\alpha\beta)(6) = \alpha(\beta(6)) = \alpha(3) = 1,$$

che, riscrivendo in forma compatta, è

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 4 & 1 \end{pmatrix}.$$

Osserviamo che la composizione $\alpha\beta$ si può anche rappresentare come

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \\ 6 & 3 & 2 & 5 & 4 & 1 \end{pmatrix},$$

ove nella seconda riga sono riportate le immagini degli elementi della prima, e nella terza le immagini degli elementi della seconda.
Ragionando allo stesso modo per $\beta\alpha$, si ha :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

Ne segue che

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

2.6.8. Si scrivano come prodotto di trasposizioni le permutazioni

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 1 & 5 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 5 & 6 & 7 & 4 \end{pmatrix}.$$

α è una permutazione ciclica, cioè può essere scritta come

$$\alpha = (123465)$$

(si legga : "1 va in 2, 2 va in 3, 3 va in 4, 4 va in 6, 6 va in 5, 5 va in 1"). Allora

$$\alpha = (123465) = (15)(16)(14)(13)(12).$$

β è invece prodotto di due permutazioni cicliche disgiunte (cioè che non muovono contemporaneamente lo stesso elemento) :

$$\beta = (132)(4567).$$

In questo caso risulta

$$\beta = (12)(13)(47)(46)(45).$$

2.6.9. Determinare le radici cubiche del numero complesso $z = 1 + i\sqrt{3}$.

Conviene innanzitutto esprimere z in forma trigonometrica: $z = \rho(\cos\theta + i\sin\theta)$.
Si ha intanto : $\rho = |z| = \sqrt{(1)^2 + (\sqrt{3})^2} = 2$.
Poichè nel piano reale z è rappresentato dal punto P di coordinate $(1, \sqrt{3})$ e l'argomento θ è l'angolo che il segmento orientato OP (di lunghezza ρ) forma con il semiasse positivo delle ascisse (parte reale), si ottiene che

$$\sqrt{3} = \rho\sin\theta \Rightarrow \sin\theta = \frac{\sqrt{3}}{2} \Rightarrow \theta = \frac{\pi}{3}.$$

Segue allora

$$z = 2(\cos\frac{\pi}{3} + i\ \sin\ \frac{\pi}{3}).$$

Per calcolare le radici cubiche di z si deve risolvere, nel campo complesso, l'equazione

$$x^3 = z.$$

Ponendo $x = r(\cos\phi + i\sin\phi)$, deve risultare

$$r = \sqrt[3]{\rho} = \sqrt[3]{2},$$

ed anche

$$\phi = \frac{\pi/3 + 2k\pi}{3}, \qquad k = 0, 1, 2.$$

In corrispondenza a tali valori per k si ottengono gli argomenti :

$$\phi_0 = \frac{\pi}{9}, \quad \phi_1 = \frac{7}{9}\pi, \quad \phi_2 = \frac{13}{9}\pi.$$

Allora le radici cubiche di $z = 1 + i\sqrt{3}$ sono i tre numeri complessi :

$$x_0 = \sqrt[3]{2}(\cos\frac{\pi}{9} + i\sin\frac{\pi}{9}),$$

$$x_1 = \sqrt[3]{2}(\cos\frac{7}{9}\pi + i\sin\frac{7}{9}\pi),$$

$$x_2 = \sqrt[3]{2}(\cos\frac{13}{9}\pi + i\sin\frac{13}{9}\pi).$$

2.6.10. Determinare le radici quarte del numero complesso $z = -3$.

Posto ancora $z = \rho(\cos\theta + i\,\sin\theta)$, si ha $\rho = |z| = 3$. Facendo ricorso, come nell'esercizio precedente al grafico nel piano reale, si vede immediatamente che l'argomento di tale numero complesso è $\theta = \pi$.
Allora $-3 = 3(\cos\pi + i\sin\pi)$.
L'equazione da risolvere è ora

$$x^4 = -3 = 3(\cos\pi + i\sin\pi).$$

Segue che

$$r = \sqrt[4]{3} \quad \text{e} \quad \phi = \frac{\pi + 2k\pi}{4}, \qquad k = 0, 1, 2, 3.$$

Le radici quarte di -3 sono date pertanto da :

$$x_0 = \sqrt[4]{3}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}),$$

$$x_1 = \sqrt[4]{3}(\cos\frac{3}{4}\pi + i\sin\frac{3}{4}\pi),$$

$$x_2 = \sqrt[4]{3}(\cos\frac{5}{4}\pi + i\sin\frac{5}{4}\pi),$$

$$x_3 = \sqrt[4]{3}(\cos\frac{7}{4}\pi + i\sin\frac{7}{4}\pi).$$

2.7 Esercizi proposti

2.7.1. Dire quali delle seguenti relazioni sono riflessive, simmetriche, transitive.
Nell'insieme T dei triangoli del piano, aRb se a e b sono simili.
In $\mathbb{N}$, aRb se a è il quadrato di b.
In $\mathbb{N}$, aRb se a divide b.
Nell'insieme $\mathcal{P}(S)$ dei sottoinsiemi di S, ARB se $A \subseteq B$.
In $\mathbb{R}$, aRb se $a < b$.
In $\mathbb{R}$, aRb se $a \leq b$.
In $\mathbb{Z}$, aRb se $a - b$ è pari.

2.7.2. Sia $S = \{A, B, C, D\}$ essendo $A = \emptyset,\ B = \{1, 2\},\ C = \{1, 3\}$ e $D = \{1, 2, 3\}$. Mostrare che $\cup$ è una operazione interna in S mentre $\cap$ non lo è.

2.7.3. Sia P l'insieme dei numeri naturali pari. Mostrare che l'applicazione definita $n \mapsto 2n$ è un isomorfismo della struttura algebrica $(\mathbb{N}, +)$ nella struttura algebrica $(P, +)$.

2.7.4. Mostrare che i seguenti sottoinsiemi $\mathbb{Z}/(13)$:

$$S = \{[1], [12]\}, \quad T = \{[1], [5], [8], [12]\}$$

sono gruppi rispetto alla moltiplicazione definita in $\mathbb{Z}/(13)$ come nell'Esempio 2.3.3

2.7.5. Scrivere tutte le permutazioni del gruppo S_3. Per ogni $\alpha \in S_3$ determinare α^{-1} e per ogni $\alpha, \beta \in S_3$ determinare $\alpha\beta$.

2.7.6. Date le permutazioni di S_5:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix},$$

determinare α^{-1}, β^{-1}, $\alpha\beta$, $\beta\alpha$, $(\alpha\beta)^{-1}$, $(\beta\alpha)^{-1}$.

2.7.7. Procedendo come nell'Esempio 2.5.1, scrivere le seguenti permutazioni di S_8 come prodotto di trasposizioni :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 5 & 6 & 7 & 8 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 6 & 8 & 2 & 7 & 5 \end{pmatrix},$$

2.7.8. Siano z e w numeri complessi. Dimostrare che si ha:

$$\overline{z+w} = \overline{z} + \overline{w}, \qquad \overline{z \cdot w} = \overline{z} \cdot \overline{w}.$$

2.7.9. Sia z un numero complesso. Mostrare che $z + \overline{z}$ e $z \cdot \overline{z}$ sono numeri reali.

2.7.10. Scrivere i seguenti numeri complessi nella forma $a + ib$:

$$i(2i-1)(i+1), \quad (i+2)^2(i^2-2), \quad i\sqrt{2}(1+\sqrt{2}i),$$

$$\frac{1}{(i-1)(i+1)}, \quad \frac{2i-1}{i-2}, \quad \frac{(i-1)(i+1)}{(i-1)^2}, \frac{1}{2+3i)}, \quad \frac{1-i\sqrt{2}}{1+i}.$$

2.7.11. Esprimere i seguenti numeri complessi in forma trigonometrica :

$$3, \quad -2, \quad -3i, \quad \frac{1}{i}, \quad -\frac{1}{i+1}, \quad 4(1-i).$$

Determinare le radici cubiche dei seguenti numeri complessi:

$$8, \quad -8i, \quad 27i, \quad -4(\sqrt{3}+i).$$

2.7.12. Determinare le radici seste di 1 e mostrare che esse contengono le radici quadrate e le radici cubiche di 1.

Capitolo 3

SPAZI VETTORIALI

3.1 Definizioni e prime proprietà

Dati due insiemi K e V, una *legge di composizione esterna* (binaria) o anche una *operazione esterna* definita in V rispetto a K è una applicazione di $K \times V$ in V. L'immagine dell'elemento (α, v) di $K \times V$ sarà nel seguito indicata semplicemente con αv ed è bene osservare che, non essendo in generate (v, α) un elemento di $K \times V$, la scrittura $v\alpha$ è da ritenersi scorretta.
Consideriamo ora un campo K e un insieme V. Si dice che V è uno *spazio vettoriale su* K se è definita in V una operazione interna, detta *addizione* e indicata con $+$, in modo tale che la struttura algebrica $(V, +)$ sia un gruppo commutativo, cioè:

(g_1) $u + (v + w) = (u + v) + w$ per ogni $u, v, w \in V$,

(g_2) esiste l'elemento neutro $\overline{0} \in V$
tale che $v + \overline{0} = \overline{0} + v = v$ per ogni $v \in V$,

(g_3) per ogni elemento $v \in V$ esiste l'elemento $-v \in V$
tale che $v + (-v) = (-v) + v = \overline{0}$,

(g_4) $v + w = w + v$ per ogni $v, w \in V$.

È inoltre definita una operazione esterna in V rispetto a K in modo che le seguenti proprietà siano soddisfatte:

(p_1)) $\alpha(v + w) = \alpha v + \alpha w$ per ogni $\alpha \in K$ e $v, w \in V$,

(p_2)) $(\alpha + \beta)v = \alpha v + \beta v$ per ogni $\alpha, \beta \in K$ e $v \in V$,

(p_3)) $(\alpha\beta)v = \alpha(\beta v)$ per ogni $\alpha, \beta \in K$ e $v \in V$,

(p_4) per ogni $v \in V$ si ha $1v = v$,
dove 1 è l'unita del campo K.