Capitolo I
STRUTTURE ALGEBRICHE ELEMENTARI

In matematica, per semplificare la stesura di un testo, si fa ricorso ad un linguaggio specifico. In questo capitolo vengono fornite in maniera sintetica le nozioni di teoria degli insiemi, indispensabili alla comprensione del corso, nonché i concetti elementari di teoria dei gruppi, anelli e campi.

Assumeremo che il lettore conosca le nozioni di numeri naturali $\mathbb{N}$ (con lo zero $0 \in \mathbb{N}$), interi $\mathbb{Z}$, razionali $\mathbb{Q}$, reali $\mathbb{R}$, sebbene nel seguito richiameremo alcune delle loro proprietà.

1. Elementi di teoria degli insiemi

1.1. Definizione. Siano A e B due insiemi (finiti o infiniti). Si dice *prodotto cartesiano* di A per B, e si denota con $A \times B$, l'insieme delle coppie ordinate di elementi di A e di B, cioè

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

La relazione precedente si legge: "il prodotto cartesiano di A per B è uguale all'insieme delle coppie ordinate a, b tali che a appartiene ad A e b appartiene a B". L'insieme $A \times A$ si denota con A^2.

1.1.1. Esempio. Sia A l'insieme i cui elementi sono i simboli $\diamond, \star, \bullet$, cioè $A = \{\diamond, \star, \bullet\}$. Allora il prodotto cartesiano di A per se stesso è dato da:

$$A^2 = A \times A = \{(\diamond, \diamond), (\diamond, \star), (\diamond, \bullet), (\star, \diamond), (\star, \star), (\star, \bullet), (\bullet, \diamond), (\bullet, \star), (\bullet, \bullet)\}.$$

1.2. Definizione. Sia A un insieme. Una *relazione binaria* in A è un sottoinsieme qualunque del prodotto cartesiano $A \times A$. Se indichiamo con $\mathcal{R}$ tale sottoinsieme, diremo che due elementi a e b di A sono *in relazione* tra loro se $(a, b) \in \mathcal{R}$ e scriveremo $a\mathcal{R}b$.

1.2.1. Esempio. Sia $A = \mathbb{N}$, l'insieme dei numeri naturali, e sia $\mathcal{R}$ il sottoinsieme di $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ dei punti che si trovano sulla retta tratteggiata in figura.

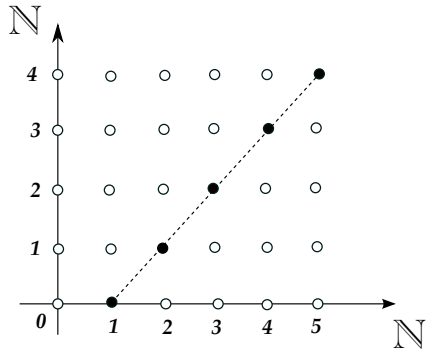

Figura 1

Allora $2\mathcal{R}1$, ma non vale $1\mathcal{R}1$. In effetti, $\mathcal{R}$ è dato dalla formula

$$n\mathcal{R}m \Leftrightarrow m = n - 1,$$

per ogni $(n, m) \in \mathbb{N}^2$.

1.3. Definizione. Una relazione binaria in un insieme A si dice *relazione di equivalenza* se valgono le seguenti proprietà:

- riflessiva, cioè $a\mathcal{R}a$, per ogni $a \in A$;
- simmetrica, cioè $a\mathcal{R}b \Rightarrow b\mathcal{R}a$, per ogni $a, b \in A$;
- transitiva, cioè $a\mathcal{R}b$ e $b\mathcal{R}c \Rightarrow a\mathcal{R}c$, per ogni $a, b, c \in A$.

1.3.1. Esempi. L'uguaglianza è una relazione d'equivalenza (in ogni insieme!).
Nell'insieme dei triangoli, la congruenza e la similitudine sono relazioni d'equivalenza.
La relazione dell'esempio 1.2.1 non è di equivalenza, in quanto non soddisfa la proprietà riflessiva.

1.4. Definizione. Sia A un insieme dotato di una relazione d'equivalenza $\mathcal{R}$. Per ogni $a \in A$, l'insieme $\{x \in A \mid x\mathcal{R}a\}$ si dice *classe d'equivalenza* di a e si denota con $[a]$. Ogni elemento x di $[a]$ si dice *rappresentante* della classe $[a]$ (ovviamente una classe ha tanti rappresentanti quanti sono i suoi elementi).

1.5. Proposizione. *Valgono le seguenti proprietà delle classi di equivalenza:*

1) Se $a\mathcal{R}b$, allora $[a] = [b]$.

2) Se $(a, b) \notin \mathcal{R}$, allora $[a] \cap [b] = \emptyset$.

3) $A = \cup_{a \in A}[a]$, e tale unione è disgiunta.

Dimostrazione. 1) Proviamo che $[a] \subseteq [b]$; sia $x \in [a]$, allora $x\mathcal{R}a$; d'altra parte, per ipotesi $a\mathcal{R}b$. Dunque, per la proprietà transitiva, $x\mathcal{R}b$, cioè $x \in [b]$. Analogamente si verifica l'altra inclusione $[a] \supseteq [b]$.
2) Supponiamo per assurdo che $x \in [a] \cap [b]$. Allora vale $x\mathcal{R}a$ e $x\mathcal{R}b$; per la proprietà simmetrica $a\mathcal{R}x$ e quindi, per la transitività, $a\mathcal{R}b$, contro l'ipotesi.
3) E' ovvio, usando la 2). □

1.6. Definizione. La decomposizione $A = \cup_{a \in A}[a]$ è detta *partizione* di A *associata alla relazione d'equivalenza* $\mathcal{R}$.

1.7. Definizione. L'insieme costituito dalle classi di un insieme A con la relazione di equivalenza $\mathcal{R}$ è detto *insieme quoziente di A modulo $\mathcal{R}$* e si indica con $A/\mathcal{R}$.
L'applicazione

$$\pi : \quad A \to A/\mathcal{R} \quad \text{definita da} \quad a \mapsto [a]$$

si dice *proiezione canonica sul quoziente.*

2. Gruppi

In prima approssimazione, una struttura algebrica è un insieme dotato di una o più operazioni. Nel caso in cui le operazioni siano più di una, esse dovranno essere compatibili.

2.1. Definizione. Si dice *operazione binaria* $*$ in un insieme G una applicazione

$$f : G \times G \longrightarrow G.$$

Il risultato $f((a,b))$ dell'operazione tra due elementi a e b si denota con $a * b$. In tal caso si dice che G è *chiuso* rispetto all'operazione $*$.

Notazione. Per indicare che si considera la struttura algebrica data dall'insieme G con l'operazione $*$, spesso si scrive $(G, *)$.

2.1.1. Esempi. E' ben noto che la somma ed il prodotto in $\mathbb{N}$ sono operazioni binarie. Costruiamo un esempio di insieme "non numerico" dotato di operazione binaria. Si consideri un triangolo equilatero ABC e sia R l'insieme delle sue rotazioni che portano a sovrapporre vertici a vertici. Usiamo la seguente notazione: per designare la rotazione che porta il vertice A in B, B in C e C in A, scriveremo:

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}.$$

Quindi gli elementi di R sono 3 ed esattamente:

$$e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \qquad x = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \qquad y = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}.$$

L'operazione che introduciamo in R è la composizione di rotazioni, che indicheremo con $\circ$; ad esempio $x \circ y$ è la rotazione che si ottiene operando prima y e poi x. Dunque $x \circ y = e$.
La seguente tabella indica i risultati delle operazioni:

$\circ$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

tabella 1

2.2. Osservazione. Le strutture $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ godono delle ben note proprietà:

$a + (b + c) = (a + b) + c$, per ogni $a, b, c \in \mathbb{N}$.

$a + b = b + a$, per ogni $a, b \in \mathbb{N}$.

Inoltre vi sono elementi dal comportamento speciale: 0 e 1; infatti

$0 + a = a$ e $1a = a$, per ogni $a \in \mathbb{N}$.

In generale diamo le seguenti definizioni in un insieme dotato di un'operazione binaria.

2.3. Definizione. Sia $(G, *)$ un insieme dotato di un'operazione binaria.

a) Diciamo che $*$ è *associativa* se

$$a * (b * c) = (a * b) * c, \quad \text{per ogni} \quad a, b, c \in G.$$

b) Diciamo che $*$ è *commutativa* se

$$a * b = b * a, \quad \text{per ogni} \quad a, b \in G.$$

c) Un elemento e di G è detto *elemento neutro* rispetto a $*$ (e scriveremo $(G, *, e)$) se

$$a * e = e * a = a, \quad \text{per ogni} \quad a \in G.$$

c) Sia $(G, *, e)$ come sopra e sia a un suo elemento. Un elemento $\overline{a} \in G$ tale che

$$a * \overline{a} = \overline{a} * a = e.$$

si dice, a seconda dell'operazione $*$, *inverso* di a e si indica con a^{-1} (ad esempio se $*$ è un prodotto); oppure *opposto* di a e si indica con $-a$ (ad esempio se $*$ è una somma).

2.3.1. Esempi. Negli esempi precedenti ogni insieme con operazione ammette un elemento neutro: $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$, $(R, \circ, e)$. Inoltre in R, y è l'inverso di x e x è l'inverso di y; mentre in $(\mathbb{N}, +, 0)$ e in $(\mathbb{N}, \cdot, 1)$ nessun elemento, eccetto quello neutro, ha opposto (risp. inverso).

Si può ampliare in modo naturale $(\mathbb{N}, +, 0)$ affinché ogni elemento abbia opposto; l'insieme così ottenuto è quello degli *interi relativi* che si denota con $\mathbb{Z}$ ed è definito da $\mathbb{Z} = \{\pm n \mid n \in \mathbb{N}\}$.

2.4. Definizione. Un insieme $(G, *)$ dotato di un'operazione binaria si dice *gruppo* se valgono le seguenti proprietà :

a) $*$ è associativa ;

b) esiste in G un elemento e che sia neutro rispetto a $*$;

c) ogni elemento di G ammette inverso (risp. opposto).

Se vale anche la proprietà commutativa :

d) $a * b = b * a$ per ogni $a, b \in G$,

allora $(G, *, e)$ si dice *gruppo commutativo* o *abeliano*.

2.5. Osservazione. $(\mathbb{Z}, +, 0)$, $(R, \circ, e)$ sono gruppi commutativi.

2.6. Proposizione. *Sia $(G, *, e)$ un gruppo. Allora:*

i) l'elemento neutro è unico;

ii) l'inverso di ogni elemento è unico.

Dimostrazione. *i*) Supponiamo che e ed e' siano due elementi neutri di G. Allora $e' * e = e$, poiché e' è elemento neutro; inoltre $e' * e = e'$, poiché e è elemento neutro. Dunque $e = e'$.
ii) Sia a un elemento di G che ammette due inversi b e c. Dunque $a * b = b * a = e$ e anche $a * c = c * a = e$. Per l'associatività dell'operazione in G si ha: $b * (a * c) = (b * a) * c$, cioè $b * e = e * c$, da cui $b = c$. □

3. Anelli e Campi

Vogliamo definire una nuova nozione per insiemi dotati di due operazioni che si comportano come la somma e il prodotto di $\mathbb{Z}$.

3.1. Definizione. Sia $(A, +, 0_A, \cdot, 1_A)$ un insieme dotato di due operazioni binarie, dette somma (denotata con $+$) e prodotto (denotato con $\cdot$), e di due elementi 0_A e 1_A, tali che :

a) $(A, +, 0_A)$ è un gruppo commutativo ;

b) il prodotto è associativo;

c) 1_A è elemento neutro rispetto al prodotto;

d) $a \cdot (b + c) = a \cdot b + a \cdot c$, per ogni $a, b, c \in A$.

In tal caso A si dice *anello*. Se inoltre il prodotto è commutativo, A si dice *anello commutativo*.

Notazione. Se A è un anello, con A^* si indica $A \setminus \{0_A\}$.

3.1.1. Esempio. $(\mathbb{Z}, +, 0, \cdot, 1)$ è ovviamente un anello commutativo.

Un altro esempio fondamentale di anello è dato dai polinomi a coefficienti interi.

Definizione 3.2. Con $\mathbb{Z}[X]$ si denota l'insieme dei *polinomi* in una *variabile* X a coefficienti in $\mathbb{Z}$, cioè l'insieme delle espressioni:

$$\mathbb{Z}[X] := \left\{ \sum_{i=0}^{n} a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \;\middle|\; n \in \mathbb{N}, a_i \in \mathbb{Z} \right\}.$$

Se $p(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$ diremo che $a_0, \ldots, a_n$ sono i *coefficienti* di $p(X)$, $a_i X^i$ si dice *monomio* e i è detto *grado* di tale monomio.
Infine diremo *grado* del polinomio $p(X)$ il massimo grado dei suoi monomi non nulli, cioè se $p(X)$ è come sopra, diremo che il grado di $p(X)$ è n, purché $a_n \neq 0$. Scriveremo $\deg(p(X)) = n$.

Ricordiamo le usuali operazioni in $\mathbb{Z}[X]$. Siano $p(X), q(X) \in \mathbb{Z}[X]$ due polinomi qualunque:

$$p(X) = \sum_{i=0}^{n} a_i X^i, \quad q(X) = \sum_{i=0}^{m} b_i X^i.$$

Supponendo $n \leq m$ si definisce:

$$p(X) + q(X) := \sum_{j=0}^{m} c_j X^j,$$

ove $c_j = a_j + b_j$ per $0 \leq j \leq n$ e $c_j = b_j$ per $n < j \leq m$; inoltre

$$p(X) \cdot q(X) = \sum_{h=0}^{m+n} d_h X^h$$

ove $d_h = \sum_{i+j=h} a_i b_j$.

3.3. Proposizione. *Con le precedenti operazioni $\mathbb{Z}[X]$ è un anello commutativo, detto anello dei polinomi a coefficienti interi.*

Dimostrazione. Siano $0_{\mathbb{Z}[X]}$ il polinomio nullo (cioè il polinomio costante uguale a $0_{\mathbb{Z}}$) e $1_{\mathbb{Z}[X]}$ il polinomio identico (cioè il polinomio costante uguale a $1_{\mathbb{Z}}$).
Ci limitiamo a provare che $(\mathbb{Z}[X], +, 0_{\mathbb{Z}[X]})$ è un gruppo commutativo.

- Associatività della somma. Comunque scelti tre polinomi in $\mathbb{Z}[X]$:

$$p(X) = \sum_{i=0}^{n} a_i X^i, \quad q(X) = \sum_{i=0}^{m} b_i X^i, \quad r(X) = \sum_{i=0}^{p} c_i X^i$$

proviamo che

$$\Big(p(X) + q(X)\Big) + r(X) = p(X) + \Big(q(X) + r(X)\Big).$$

Per semplicità supponiamo $n = m = p$ (il caso generale è analogo). Dalla definizione di somma segue:

$$I := \Big(p(X) + q(X)\Big) + r(X) = \sum_{i=0}^{n} (a_i + b_i)X^i + \sum_{i=0}^{n} c_i X^i = \sum_{i=0}^{n} [(a_i + b_i) + c_i]X^i.$$

D'altra parte

$$II := p(X) + \Big(q(X) + r(X)\Big) = \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} (b_i + c_i)X^i = \sum_{i=0}^{n} [a_i + (b_i + c_i)]X^i.$$

I coefficienti dei polinomi I e II sono, per ogni $i = 0, \ldots, n$ dati da

$$[(a_i + b_i) + c_i] \quad \text{e} \quad [a_i + (b_i + c_i)]$$

che risultano uguali in quanto la somma, in $\mathbb{Z}$, è associativa. Pertanto $I = II$, come volevamo.

- Il polinomio nullo $0_{\mathbb{Z}[X]}$ è elemento neutro rispetto alla somma: ovvio.

- Ogni polinomio $p(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ ammette opposto.
Infatti, sia $p'(X) = \sum_{i=0}^{n} (-a_i)X^i$, dove $-a_i$ è l'opposto in $\mathbb{Z}$ dell'intero a_i. Pertanto

$$p(X) + p'(X) = \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} (-a_i)X^i = \sum_{i=0}^{n} (a_i - a_i)X^i$$

dove l'ultima uguaglianza segue dalla definizione di somma tra polinomi. Ma $a_i - a_i = 0_{\mathbb{Z}}$ per ogni i, dunque $p(X) + p'(X) = 0_{\mathbb{Z}[X]}$. Pertanto $p'(X)$ è l'opposto di $p(X)$.

- Commutatività della somma. Si considerino due polinomi qualunque $p(X), q(X) \in \mathbb{Z}[X]$ come sopra (e ancora supponiamo $n = m$). Proviamo che

$$p(X) + q(X) = q(X) + p(X).$$

Per la definizione di somma:

$$I := p(X) + q(X) = \sum_{i=0}^{n} (a_i + b_i)X^i \quad \text{e} \quad II := q(X) + p(X) = \sum_{i=0}^{n} (b_i + a_i)X^i$$

I coefficienti dei polinomi I e II sono, per ogni $i = 0, \ldots, n$ dati da

$$a_i + b_i \quad \text{e} \quad b_i + a_i$$

che risultano uguali in quanto la somma, in $\mathbb{Z}$, è commutativa. Pertanto $I = II$, come volevamo.

Omettiamo le dimostrazioni delle proprietà $b), c), d)$ della definizione di anello. □

Ricordiamo le seguenti semplici proprietà dei polinomi:

3.4. Proposizione. *Siano $f(X), g(X) \in \mathbb{Z}[X]$; allora:*

i) $\deg(f(X) + g(X)) \leq \max\{\deg(f(X)), \deg(g(X))\}$;

ii) $\deg(f(X) \cdot g(X)) = \deg(f(X)) + \deg(g(X))$. □

Come per l'insieme dei numeri interi, anche $(\mathbb{Q}, +, 0, \cdot, 1)$ è un anello commutativo. Però $\mathbb{Q}$ rispetto a $\mathbb{Z}$ ha una struttura più ricca: ogni elemento non nullo è invertibile rispetto al prodotto. Infatti se $a/b \neq 0$, cioè $a \neq 0$, esiste $b/a \in \mathbb{Q}$ e $(a/b) \cdot (b/a) = 1$; quindi $b/a = (a/b)^{-1}$.

3.5. Definizione. Se K è un anello commutativo tale che ogni elemento non nullo ammette inverso moltiplicativo, allora K si dice *campo*.
Equivalentemente K è un campo se e solo se $(K, +, 0_K)$ e $(K^*, \cdot, 1_K)$ sono gruppi abeliani e il prodotto è distributivo rispetto alla somma.

3.5.1. Esempio. Da quanto visto prima, si deduce che $\mathbb{Q}$ è un campo, mentre $\mathbb{Z}$ non lo è.
Per questo corso, l'esempio fondamentale di campo è quello dell'insieme $\mathbb{R}$ dei numeri reali con le usuali operazioni di somma e prodotto.

In modo del tutto analogo a quanto visto per $\mathbb{Z}[X]$, si possono definire gli insiemi dei polinomi a coefficienti razionali o reali. Per entrambi vale l'analogo della 3.3 e precisamente:

3.6. Proposizione. *Con le usuali operazioni, gli insiemi $\mathbb{Q}[X]$ e $\mathbb{R}[X]$ sono due anelli commutativi, detti, rispettivamente, anello dei polinomi a coefficienti razionali e anello dei polinomi a coefficienti reali.* □

Per $\mathbb{Q}[X]$ e $\mathbb{R}[X]$ vale la stessa nozione di grado definita per $\mathbb{Z}[X]$ e le analoghe proprietà di 3.4.

4. Numeri complessi

Intuitivamente "aggiungiamo" a $\mathbb{R}$ una radice del polinomio a coefficienti reali X^2+1; denotiamo tale numero con i. Se consideriamo il più piccolo campo che contenga $\mathbb{R}$ ed i, esso deve sicuramente contenere tutte le possibili somme e prodotti di tali elementi. Diamo dunque la seguente

4.1. Definizione. Un *numero complesso* è un'espressione formale del tipo

$$z = a + ib\,, \quad \text{dove} \quad a, b \in \mathbb{R}.$$

Il numero reale a si dice *parte reale* e il numero reale b si dice *parte immaginaria* di z; in simboli:

$$a = Re(z), \quad b = Im(z).$$

Si dice *coniugato* di z il numero complesso $\overline{z} = a - ib$.
L'insieme di tutti i numeri complessi si denota con $\mathbb{C}$, cioè

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}.$$

Lasciamo al lettore la verifica del seguente risultato:

4.2. Proposizione. *Si definiscano in $\mathbb{C}$ le seguenti operazioni:*

$$(a+ib) + (c+id) := (a+c) + i(b+d)$$
$$(a+ib) \cdot (c+id) := (ac-bd) + i(bc+ad).$$

Rispetto a tali operazioni, $(\mathbb{C}, +, \cdot, 0_{\mathbb{C}}, 1_{\mathbb{C}})$ è un campo, dove $0_{\mathbb{C}} = 0_{\mathbb{R}} + i0_{\mathbb{R}}$ e $1_{\mathbb{C}} = 1_{\mathbb{R}} + i0_{\mathbb{R}}$. □

4.2.1. Esempio. Calcoliamo le seguenti operazioni in $\mathbb{C}$:

$$(2+3i) + (1-2i) = 3 + i; \quad (2+3i) \cdot (1-2i) = 8 - i.$$

Inoltre, nella dimostrazione di 4.2 si prova che ogni elemento non nullo $z = a + ib \in \mathbb{C}$ ammette inverso. Si cerca infatti un numero $x + iy \in \mathbb{C}$ tale che $(a+ib)(x+iy) = 1$. Vediamo i conti in un esempio numerico: calcoliamo $(2+3i)^{-1}$. Imponiamo

$$1 = (2+3i)(x+iy) = 2x + 2iy + 3ix - 3y = (2x-3y) + i(3x+2y) \quad \Longrightarrow \quad \begin{cases} 2x - 3y = 1 \\ 3x + 2y = 0 \end{cases}.$$

Si ottiene $x = 2/13$ e $y = -3/13$ e quindi $(2+3i)^{-1} = (2/13) - i(3/13)$. In generale, vale

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

4.3. Proposizione. *Per ogni numero complesso $z = a + ib$ valgono le seguenti proprietà:*

i) $\overline{\overline{z}} = z$;

ii) $\overline{z} = z$ *se e solo se* $z \in \mathbb{R}$;

iii) $z\overline{z} = a^2 + b^2$;

iv) $z + \overline{z} = 2Re(z)$. □

4.4. Osservazione. E' evidente che il polinomio $X^2 + 1 \in \mathbb{C}[X]$ si può scomporre in un prodotto di polinomi, in quanto i e $-i$ sono sue radici; dunque

$$X^2 + 1 = (X + i)(X - i).$$

Questo non sorprende, in quanto si è ampliato $\mathbb{R}$ ad un campo che contiene anche una radice di tale polinomio. Ma il fatto sorprendente è che questo nuovo campo dei numeri complessi contiene tutte le radici di *ogni* polinomio a coefficienti reali. Ricordiamo questo importante risultato:

4.5. Teorema fondamentale dell'algebra. *Sia $f(X)$ un polinomio a coefficienti reali. Allora f ammette almeno una radice complessa. Più precisamente, se $n = deg(f)$, allora esistono n radici di f in $\mathbb{C}$; quindi, poste $z_1, \ldots, z_n$ tali radici, il polinomio f si fattorizza completamente in $\mathbb{C}$:*

$$f(X) = a(X - z_1)(X - z_2) \cdots (X - z_n).$$

□

Un risultato ancora più generale dice che:

4.6. Teorema. *Sia $f(X) \in \mathbb{C}[X]$ un polinomio a coefficienti complessi di grado n. Allora esistono n radici di f in $\mathbb{C}$; cioè il polinomio f si fattorizza completamente in $\mathbb{C}$.* □

La proprietà suddetta si riassume dicendo che $\mathbb{C}$ è un campo *algebricamente chiuso*.

5. Omomorfismi di strutture algebriche

In questo paragrafo caratterizzeremo particolari applicazioni tra strutture algebriche.

Poiché si useranno coppie di strutture dello stesso tipo, converrà, per semplificare le notazioni, utilizzare lo stesso simbolo + per indicare ogni operazione di somma e analogamente il simbolo $\cdot$ sarà riferito ad ogni operazione di prodotto. Dal contesto risulterà chiaro in quale struttura tali operazioni verranno eseguite. Inoltre gli elementi neutri (della somma e del prodotto) verranno indicati con un indice relativo alla struttura alla quale appartengono.

Infine, per semplicità, per i gruppi verrà usata la sola notazione additiva.

5.1. Definizione. Un'applicazione tra due strutture algebriche dello stesso tipo si dice *omomorfismo* se preserva le operazioni definite nelle strutture medesime. Più precisamente:

i) se $(G, +, 0_G)$ e $(G', +, 0_{G'})$ sono due gruppi, un'applicazione $f : G \to G'$ è un *omomorfismo di gruppi* se

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

per ogni $x, y \in G$.

ii) se $(A, +, 0_A, \cdot, 1_A)$ e $(B, +, 0_B, \cdot, 1_B)$ sono due anelli, un'applicazione $f : A \to B$ è un *omomorfismo di anelli* se

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

per ogni $x, y \in A$.

5.1.1. Esempio. Le inclusioni canoniche $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{Z} \subset \mathbb{Z}[X]$ sono omomorfismi di anelli.

5.1.2. Esempio. L'applicazione $f : \mathbb{Z} \to \mathbb{Z}$ definita da $n \mapsto 2n$ è un omomorfismo di gruppi (additivi) ma non di anelli.

Proviamo le seguenti semplici proprietà degli omomorfismi di gruppi:

5.2. Proposizione. *Siano $(G, +, 0_G)$ e $(G', +, 0_{G'})$ due gruppi e sia $f : G \to G'$ un omomorfismo di gruppi. Allora:*

i) *$f(0_G) = 0_{G'}$, cioè l'immagine dell'elemento neutro di G è l'elemento neutro di G';*

ii) *per ogni $g \in G$ si ha $f(-g) = -f(g)$, cioè l'immagine dell'opposto di un elemento è l'opposto dell'immagine dell'elemento stesso.*

Dimostrazione.
i) Per definizione di elemento neutro si ha:

$$f(0_G) = f(0_G + 0_G) = f(0_G) + f(0_G)$$

dove l'ultima uguaglianza segue dal fatto che f è un omomorfismo di gruppi. Poiché $f(0_G)$ è un elemento di G', ammette opposto in G' e possiamo sommare tale opposto ad ambo i membri della precedente uguaglianza, ottenendo:

$$f(0_G) + [-f(0_G)] = f(0_G) + f(0_G) + [-f(0_G)].$$

Applicando a sinistra la definizione di opposto e a destra l'associatività della somma e la definizione di opposto si ha infine:

$$0_{G'} = f(0_G) + 0_{G'} \quad \Rightarrow \quad 0_{G'} = f(0_G).$$

ii) Poiché per 2.6, in un gruppo additivo, l'opposto di un elemento è unico, per provare che $f(-g)$ è l'opposto di $f(g)$ in G' basta provare la proprietà caratterizzante l'opposto, cioè che:

$$f(g) + f(-g) = 0_{G'}.$$

Ma per definizione di omomorfismo di gruppi additivi:

$$f(g) + f(-g) = f(g - g) = f(0_G) = 0_{G'}$$

dove l'ultima uguaglianza segue da *i*). □

Si può provare che, se $f : A \to B$ è un omomorfismo di anelli, allora valgono le precedenti proprietà relative alla somma ed anche le analoghe proprietà per il prodotto, cioè:

iii) $f(1_A) = 1_B$;

iv) per ogni $a \in A$ tale che esiste l'inverso a^{-1}, si ha $f(a^{-1}) = f(a)^{-1}$.

Infine, se A e B sono campi, un omomorfismo di anelli $f : A \to B$ si dice *omomorfismo di campi*.

5.3. Definizione. Un omomorfismo che è anche un'applicazione biunivoca si dice *isomorfismo*.