Università "Sapienza" di Roma

Facoltà di Informatica

Algebra

Appunti integrati con il libro "Geometria analitica con elementi di Algebra lineare", M. Abate, C. De Fabritiis

Author

Simone Bianco

18 ottobre 2022

Indice

Capitolo 0

Introduzione

Il seguente corso mira all'apprendimento dei principali elementi di Algebra Elementare, Algebra Lineare e Teoria dei Gruppi, incentrandosi principalmente su:

- **Insiemi**, partizioni, applicazioni, **relazioni** d'equivalenza e d'ordine, permutazioni. I numeri naturali e il **principio di induzione**. Il teorema binomiale.
- **Strutture algebriche**: Gruppi, anelli e campi, reticoli, sottostrutture, omomorfismi . Anelli di polinomi. L'algoritmo di Euclide. Classi resto modulo un intero. Congruenze ed equazioni in Z/n. Il teorema di Eulero-Fermat.
- **Sistemi di equazioni lineari**: algoritmo di Gauss, determinante di una matrice quadrata. Matrice inversa. Rango di una matrice: Il teorema di Cramer ed il teorema di Rouche-Capelli. Risoluzione di sistemi lineari omogenei.
- **Spazi vettoriali**: dipendenza e indipendenza lineare, basi. Matrici. Applicazioni lineari e loro rappresentazione: cambiamenti di base, diagonalizzazione di un operatore lineare. Polinomio caratteristico e relativa invarianza.
- **Elementi di teoria dei gruppi**: Gruppi ciclici, periodo di un elemento di un gruppo. Classificazione dei gruppi ciclici. Classi laterali modulo un sottogruppo. Il teorema di Lagrange e le sue conseguenze, sottogruppi normali. Il teorema fondamentale di omomorfismo tra gruppi.

Prima di approcciarsi al seguente corso, è consigliato avere una conoscenza di elementi di **teoria degli insiemi**, facilmente apprendibili attraverso il corso di ***Metodi Matematici per l'Informatica***

Capitolo 1

Algebra elementare

1.1 Richiami di insiemistica

Definiamo **insieme** una collezione di elementi su cui vengono svolte delle **operazioni algebriche**.

$$S : \{1, 2, 3, 4, ...\}$$

In questo corso tratteremo molto le proprietà e le operazioni applicabili sulle varie **strutture algebriche** rappresentate tramite insiemi, pertanto effettuiamo un breve ripasso di **teoria degli insiemi**:

- Dati due insiemi A, B, definiamo l'**insieme unione** $A \cup B$ come l'insieme dove

$$A \cup B : \{x \in A \vee x \in B\}$$

- Definiamo invece come **insieme intersezione** $A \cap B$ l'insieme dove

$$A \cap B : \{x \in A \wedge x \in B\}$$

- Considerato un insieme X, affermiamo che l'insieme A è **sottoinsieme** dell'insieme X (denotato come $A \subseteq X$) se si verifica che

$$A \subset S \iff x \in A \implies x \in X$$

- Considerato un insieme X e un insieme A tale che $A \subset X$, denotiamo l'**insieme complementare** di A su X come

$$X \setminus A = \{x \in X \mid x \notin A\}$$

- La **legge di De Morgan** afferma che

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$$

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$$

- Dato un insieme di partenza detto **dominio** ed un insieme di arrivo detto **codominio**, definiamo come **funzione** la relazione che associa ogni elemento del dominio ad un elemento del codominio

$$f : X \to Y : x \mapsto y$$

- Definiamo come **immagine della funzione** l'insieme di tutti gli elementi del codominio raggiungibili da un elemento del dominio

$$Im(f) = \{y \in Y, \exists x \in X \mid f(x) = y\}$$

- Una funzione viene detta **iniettiva** se <u>ogni</u> elemento del dominio è associato ad un elemento diverso del codominio

$$\texttt{Iniettività} : \forall x_1, x_2 \in X \mid x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

- Una funzione viene detta **suriettiva** se <u>ogni</u> elemento del codominio è raggiungibile da almeno un elemento del dominio

$$\texttt{Suriettività} : \forall y \in Y, \exists x \in X \mid f(x) = y$$

  In alternativa, potremmo affermare che una funzione è suriettiva se la sua immagine coincide con il suo codominio

$$\texttt{Suriettività} : Im(f) = Y$$

- Una funzione viene detta **biettiva** (o biunivoca) se è sia iniettiva sia suriettiva. Se esiste una funzione biettiva tra due insiemi X ed Y, allora tali insiemi possiedono la **stessa cardinalità**

$$\exists f : X \to Y \mid f \text{ è biettiva} \implies |X| = |Y|$$

- Definiamo come **prodotto cartesiano** di due insiemi X e Y l'insieme contenente tutte le coppie (x, y) dove $x \in X$ e $y \in Y$

$$X \times Y : \{(x, y) \mid x \in X, y \in Y\}$$

- Date due funzioni f, g, la loro **funzione composta** è una funzione che associa un elemento del dominio di f ad un elemento del codominio di g

$$f : X \to Y : x \mapsto f(x)$$
$$g : Y \to Z : x \mapsto g(x)$$
$$g \circ f : X \to Z : x \mapsto g(f(x)) : x \mapsto (g \circ f)(x)$$

- Definiamo come **insieme dei numeri naturali** l'insieme

$$\mathbb{N} : \{0, 1, 2, 3, ...\}$$

- Definiamo come **insieme dei numeri interi** l'insieme

$$\mathbb{Z} : \{..., -2, -1, 0, 1, 2, ...\}$$

- Definiamo come **insieme dei numeri razionali** l'insieme

$$\mathbb{Q} : \left\{\frac{m}{n} \,|\, m, n \in \mathbb{Z}, n \neq 0\right\}$$

- Definiamo come **insieme dei numeri irrazionali** l'insieme

$$\mathbb{I} : \left\{x \,|\, \nexists m, n \in \mathbb{Z} : x = \frac{m}{n}\right\}$$

- Definiamo come **insieme dei numeri reali** l'insieme

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$$

1.2 Assiomi e Strutture algebriche

Una particolare categoria di funzioni che studieremo durante il corso corrisponde alle **operazioni binarie**:

Definition 1. Operazione binaria

Dato un insieme S, definiamo **operazione binaria** una funzione che presi due elementi di S in input, restituisce un elemento di S in output

$$m : S \times S \to S : (x, y) \mapsto m(x, y)$$

Ad esempio, sull'insieme $\mathbb{R}$ possiamo considerare l'**operazione binaria additiva**, indicata come

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R} : (x, y) \mapsto x + y$$

e l'**operazione binaria moltiplicativa**, indicata come

$$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R} : (x, y) \mapsto xy$$

Inoltre, anche la composizione tra funzioni corrisponde ad un'operazione binaria:

$$\circ : X \times X \to X : (g, f) \to g \circ f$$

Tali operazioni binarie **possono** godere di alcune **proprietà algebriche**:

Definition 2. Associatività (Assioma 1)

Data un'operazione binaria $m : S \times S \to S$ e tre elementi $x, y, z \in S$, l'ordine di applicazione di tale operazione binaria non influenza il risultato

$$m(m(x, y), z) = m(x, m(y, z)) \quad \forall x, y, z \in S$$

Esempi:

- Operazione additiva: $(x + y) + z = x + (y + z) = x + y + z \quad \forall x, y, z \in S$
- Operazione moltiplicativa: $(xy)z = x(yz) = xyz \quad \forall x, y, z \in S$

Definition 3. Elemento neutro (Assioma 2)

Data un'operazione binaria $m : S \times S \to S$, esiste un elemento neutro e tale che

$$m(x, e) = x \quad \forall x \in S$$

Esempi:

- Operazione additiva: $x + 0 = x \quad \forall x \in S$
- Operazione moltiplicativa: $x \cdot 1 = x \quad \forall x \in S$

Definition 4. Elemento inverso (Assioma 3)

Data un'operazione binaria $m : S \times S \to S$, per ogni elemento $x \in S$, esiste un elemento inverso x^{-1} tale che

$$m(x, x^{-1}) = e$$

Tale assioma implica necessariamente l'esistenza dell'elemento neutro e

Esempi:

- Operazione additiva: $x + (-x) = 0 \quad \forall x \in S$
- Operazione moltiplicativa: $x \cdot \frac{1}{x} = 1 \quad \forall x \in S$

Definition 5. Commutatività (Assioma 4)

Data un'operazione binaria $m : S \times S \to S$, l'ordine elementi non influenza il risultato

$$m(x, y) = m(y, x) \quad \forall x \in S$$

Esempi:

- Operazione additiva: $x + y = y + x \quad \forall x \in S$
- Operazione moltiplicativa: $xy = yx \quad \forall x \in S$

Osservazioni

1. Se valgono gli assiomi di **elemento neutro** e di **commutatività**, allora può esistere **un solo elemento neutro**:

$$e_1 = m(e_1, e_2) = m(e_2, e_1) = e_2 \implies e_1 = e_2$$

2. Se vale l'assioma di **elemento inverso**, allora può esistere **un solo elemento inverso**:

$$m(x, x_1^{-1}) = 1 = m(x, x_2^{-1}) \implies m(x, x_1^{-1}) = m(x, x_2^{-1}) \implies x_1^{-1} = x_2^{-1}$$

Una volta definiti i quattro assiomi principali delle operazioni binarie, possiamo definire le seguenti quattro **strutture algebriche**:

Definition 6. Strutture algebriche semplici

Data la coppia (S, m) dove S è un **insieme** e m l'**operazione binaria** applicata su di esso, diciamo che tale coppia è:

- Un **semigruppo** se vale l'assioma di associatività (assioma 1)
- Un **monoide** se valgono gli assiomi di d'associatività e di elemento neutro (assiomi 1 e 2)
- Un **gruppo** se valgono gli assiomi di associatività, elemento neutro e elemento inverso (assiomi 1, 2 e 3)
- Un **gruppo abeliano** (o commutativo) se valgono gli assiomi di associatività, elemento neutro, elemento inverso e commutatività (assiomi 1, 2, 3 e 4)

Esempi:

- $(\mathbb{N} - \{0\}, +)$ è un **semigruppo** (assioma 1)
- $(\mathbb{N}, +)$ è un **monoide** commutativo (assiomi 1, 2 e 4)
- $(\mathbb{Z}, \div)$ è un **gruppo abeliano** (assiomi 1, 2, 3 e 4)
- $(\mathbb{Z}, \cdot)$ è un **monoide** commutativo (assiomi 1, 2 e 4)
- Dati due insiemi X, Y, denotiamo con Y^X l'insieme composto da tutte le funzioni da X in Y

$$Y^X : \{f : X \to Y\}$$

  Allora, la coppia $(X^X, \circ)$ è un monoide, poiché si ha:

$$f, g, h : X \to X \implies h \circ (g \circ f) = (h \circ g) \circ f \implies \texttt{Associatività}$$

$$f : X \to X : x \to f(x), \texttt{idt} : X \to X : x \to x \implies f \circ \texttt{idt} = f \implies \texttt{Elemento neutro}$$

  dove `idt` è la funzione identità, ossia $idt(x) = x$.

- Dato un insieme X, denotiamo con S_X il **gruppo simmetrico su X**, ossia l'insieme composto da tutte le funzioni biettive da X in se stesso.

$$S_X : \{f : X \to X \mid f \texttt{ è biettiva}\}$$

Allora, la coppia $(S_X, \circ)$ è un gruppo, poiché:

$$f, g, h : X \to X \implies h \circ (g \circ f) = (h \circ g) \circ f \implies \texttt{Associatività}$$
$$f : X \to X : x \to f(x), \texttt{idt} : X \to X : x \to x \implies f \circ \texttt{idt} = f \implies \texttt{Elemento neutro}$$
$$\exists f^{-1} : X \to X \mid f \circ f^{-1} = \texttt{idt} \implies \texttt{Elemento inverso}$$

Osservazione:

Una funzione f può essere invertibile se e solo se f è biettiva.

$$f \texttt{ è invertibile} \iff f \texttt{ è biettiva}$$

Dimostrazione:

Se f è invertibile, allora:

– f è suriettiva poiché:
$$x = f(f^{-1}(x)), \forall x \in X$$

– f è iniettiva poiché:
$$f(x) = f(y) \implies x = f^{-1}(f(x)) = f^{-1}(f(y)) = y$$

Se f è biettiva, allora
$$\forall x \in X, \exists! y \mid f(y) = x$$

Ponendo $y = f^{-1}(x)$, il vincolo biettivo è rispettato e inoltre otteniamo che
$$\forall f \in S_X, \exists f^{-1} \in S_X \mid f \circ f^{-1} = f^{-1} \circ f$$

Approfondimento sul gruppo simmetrico

Avendo introdotto il gruppo simmetrico su X come
$$S_X : \{f : X \to X \mid f \texttt{ è biettiva}\}$$

Tale insieme presenta alcune caratteristiche:

- Trattandosi di funzioni biettive, ogni elemento del gruppo simmetrico corrisponde ad una **permutazione** del dominio X
- Se X è finito, ossia possiede un numero finito di elementi (dunque $|X| = n$), allora denotiamo il suo **gruppo simmetrico di ordine** n come S_n
- Poiché tutte le permutazioni possibili di un insieme di n elementi corrispondono a $n!$, allora abbiamo che:
$$|X| = n \implies |S_n| = n!$$

1.3 Anelli e Campi

Consideriamo un insieme A e due operazioni binarie su di esso, definite come:

$$+ : A \times A \to A$$

$$\cdot : A \times A \to A$$

Se tale struttura algebrica risulta essere un **gruppo abeliano** nell'operazione somma, un **monoide** nell'operazione prodotto **relazione distributiva** tra le due operazioni, allora definiamo tale struttura algebrica come **anello**.

Definition 7. Anello

Definiamo una struttura algebrica del tipo $(A, +, \cdot)$ come **anello** se:

- $(A, +)$ è un **gruppo abeliano**
- $(A, \cdot)$ è un **monoide**
- Vale la **relazione distributiva**, definita come:

$$a(b + c) = ab + ac \quad \forall a, b, c \in A$$

Inoltre, definiamo tale struttura come **anello commutativo** se nella coppia $(A, \cdot)$ vale anche l'assioma **commutativo**:

$$ab = ba \quad \forall a, b \in A$$

Osservazione:

In un anello $(A, +, \cdot)$ applicare l'operazione prodotto tra un qualsiasi elemento $a \in A$ e l'elemento neutro 0 dell'operazione somma, restituirà l'elemento neutro stesso come risultato:

$$a \cdot 0 = 0 \quad \forall a \in A$$

Dimostrazione:

Riscriviamo l'elemento $a \in A$ come:

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

A questo punto, poniamo:

$$a = a \cdot 0 + a$$

$$a + (-a) = a \cdot 0 + a + (-a)$$

$$0 = a \cdot 0$$

Nel caso in cui si abbia un **anello commutativo** in cui viene rispettato l'assioma di **elemento inverso** nell'operazione prodotto, allora definiamo tale struttura algebrica come **campo**.

Definition 8. Campo

Definiamo una struttura algebrica del tipo $(A, +, \cdot)$ come **campo** se:

- $(A, +, \cdot)$ è un **anello commutativo**
- $(A, \cdot)$ ammette l'assioma di **elemento inverso**, ossia se:

$$\forall a \in A \setminus \{0\}, \exists a^{-1} \in A \,|\, a \cdot a^{-1} = 1$$

Dunque, in un campo si ha anche che $(A \setminus 0, +, \cdot)$ è un gruppo abeliano

Esempi:

- $(\mathbb{Z}, +, \cdot)$ è un **anello commutativo**
- $(\mathbb{Q}, +, \cdot)$ è un **campo**
- $(\mathbb{R}, +, \cdot)$ è un **campo**
- Sia A un **anello commutativo**. Definiamo l'**insieme dei polinomi** aventi come coefficienti elementi dell'anello A come:

  $A[x] : \{\texttt{polinomi a coefficienti in } A\} : \{a_0 + a_1 x + ... + a_n x^n \,|\, a_0, a_1, ..., a_n \in A\}$

  Dati due polinomi $p(x), q(x) \in A[x]$, dunque definiti come

$$p(x) = \sum_{i=0}^{n} a_i x^i \qquad q(x) = \sum_{i=0}^{n} b_i x^i$$

  abbiamo che:

  – L'**operazione somma** corrisponde a:

$$p(x) + q(x) = \sum_{i=0}^{+\infty} (a_i + b_i) x^i$$

  dove $a_i, b_i = 0$ per $i > n$

  – L'**operazione prodotto** corrisponde a:

$$p(x) \cdot q(x) = \sum_{i=0}^{n} \left(\sum_{j=0}^{n} a_i b_j x^{i+j} \right)$$

  – In $(A[x], +, \cdot)$ l'**elemento neutro** è il polinomio costante (ossia aventi solo grado zero), indicato col simbolo 1

– Poiché possiamo vedere ogni $a \in A$ come un **polinomio costante** in $A[x]$ (dunque un polinomio del tipo $p(x) = a_0 + a_1x^0 ... + a_nx^0 \in A[x] \,|\, a_0 \in A$), allora deduciamo che $A \subset A[x]$, implicando che $(A[x], +, \cdot)$ possa essere un anello commutativo se e solo se anche A lo è, fattore dato per vero come ipotesi iniziale.

– Tuttavia, l'anello commutativo $(A[x], +, \cdot)$ **non ammette elemento inverso nell'operazione prodotto**, poiché il grado dei polinomi è $0 \leq i \leq n$. Ad esempio, il polinomio $p(x) = x$ non ammette inversi, poiché $x^{-1} \notin A[x]$. Dunque, $(A, +, \cdot)$ **non è un campo**.

1.3.1 Numeri complessi

Introduciamo il simbolo i con cui indichiamo l'**unità immaginaria**, avente la seguente proprietà: $i^2 = -1$.

Definiamo l'insieme dei **numeri complessi** come

$$\mathbb{C} : \{a + ib \,|\, a, b \in \mathbb{R}\}$$

ossia l'insieme delle espressioni $z = a + ib$ composte dalla somma di una **parte reale**, indicata con $Re(z) = a$, ed una **parte immaginaria**, indicata con $Im(z) = b$.

Ovviamente, da tale definizione di insieme dei numeri complessi ne segue che $\mathbb{R} \subset \mathbb{C}$, poiché $\forall a \in \mathbb{R} \implies z \in \mathbb{C} \,|\, z = a + i \cdot 0$. Inoltre, definiamo un **numero immaginario puro** come un numero nella forma $z \in \mathbb{C} \,|\, z = 0 + i \cdot b$.

In questa sezione, vedremo le varie **proprietà dei numeri complessi**, arrivando fino al provare che essi corrispondano ad un **campo**.

Partiamo dal definire le operazioni di somma e prodotto. Dati due numeri $z, w \in \mathbb{C}$, definiti come $z = a + ib$ e $w = c + id$, abbiamo che:

$$z + w = a + ib + c + id = (a + c) + i(b + d) \implies z + w \in \mathbb{C}$$

$$zw = (a + ib)(c + id) = (ac - bd) + i(ad + bc) \implies zw \in \mathbb{C}$$

Verifichiamo facilmente che la struttura $(\mathbb{C}, +, \cdot)$ risulta essere un **anello commutativo**:

- **Associatività della somma**

$$(z + w) + q = z + (w + q) = z + w + q, \quad \forall z, w, q$$

- **Elemento neutro della somma**

$$\exists! 0 \in \mathbb{C} \,|\, z + 0 = z, \quad \forall z \in \mathbb{C}$$

- **Elemento inverso della somma**

$$\forall z \in \mathbb{C}, \exists! -z \in \mathbb{C} \,|\, z + (-z) = 0$$

- **Commutatività della somma**

$$\forall z, w \in \mathbb{C} \,|\, z + w = w + z$$

- **Associatività del prodotto**

$$(zw)q = z(wq) = zwq, \quad \forall z, w, q$$

- **Elemento neutro del prodotto**

$$\exists 1 \in \mathbb{C} \,|\, z \cdot 1 = z, \quad \forall z \in \mathbb{C}$$

- **Commutatività del prodotto**

$$\forall z, w \in \mathbb{C} \,|\, zw = wz$$

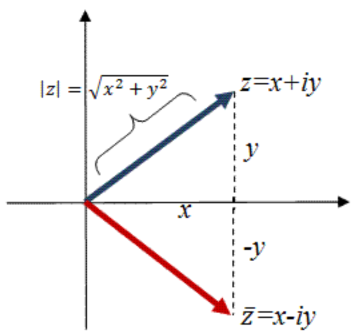
- **Relazione distributiva**

$$\forall z, w, q \in \mathbb{C} \,|\, z(w + q) = zw + zq$$

A questo punto, l'ultimo step da svolgere per poter definire $(\mathbb{C}, +, \cdot)$ come un **campo**, ossia provare l'ammissione dell'**assioma di elemento inverso del prodotto**.

Poiché un numero complesso è determinato da una **coppia di valori** $a, b \in \mathbb{R} \,|\, z \in \mathbb{C}, z = a + ib$, possiamo rappresentare tale numero graficamente attraverso il **piano di Gauss**, avente come ascisse la **parte reale** dei numeri complessi e come ordinate la **parte immaginaria**.

Ad esempio, il numero $z = -3 - 3i$ viene rappresentato come:



Per tale motivo, dato un elemento $z \in \mathbb{C}$, definiamo come suo **valore assoluto** il numero reale corrispondente alla distanza di z stesso dall'origine, facilmente ricavabile attraverso il **teorema di Pitagora**:

$$|z| = \sqrt{a^2 + b^2}$$

Inoltre, definiamo come **numero coniugato di** z ($\overline{z} \in \mathbb{C}$) il numero complesso avente come parte immaginaria il valore inverso della parte immaginaria di z:

$$z = a + ib \implies \overline{z} = a - ib \implies Im(\overline{z}) = -Im(z)$$

Osservazioni:

- Dati $z, w \in \mathbb{C} \,|\, z = a + ib, w = c + id$, la **somma dei loro coniugati** equivale al **coniugato della loro somma**

$$\overline{z} + \overline{w} = a - ib + c - id = (a - c) - i(b + d) = \overline{z + w}$$

- Dati $z, w \in \mathbb{C} \,|\, z = a + ib, w = c + id$, il **prodotto dei loro coniugati** equivale al **coniugato del loro prodotto**

$$\overline{z} \cdot \overline{w} = (a - ib)(c - id) = (ac - bd) - i(ad + bc) = \overline{zw}$$

- Dato $z \in \mathbb{C}$, il **prodotto** tra **esso** e il suo **coniugato** corrisponde al **quadrato del valore assoluto** di z

$$z \cdot \overline{z} = (a + ib)(a - ib) = a^2 - (ib)^2 = a^2 + b^2 = |z|^2$$

A questo punto, proviamo a definire l'elemento inverso del prodotto come:

$$\forall z \in \mathbb{C} \setminus \{0\}, \exists! z^{-1} = \frac{1}{z} = \frac{1}{a + ib} \,|\, z \cdot z^{-1} = 1$$

Tuttavia, il numero inverso $z^{-1} = \frac{1}{a+ib}$ non risulta apparire nella forma $c + id \,|\, c, d \in \mathbb{R}$ (poiché le parti reali e immaginarie dovrebbero essere al numeratore).

Decidiamo quindi di riscrivere z^{-1} come:

$$z = a + ib \implies z^{-1} = \frac{1}{z} = \frac{\overline{z}}{z \cdot \overline{z}} = \frac{\overline{z}}{|z|^2} = \frac{a - ib}{a^2 + b^2} = \frac{a}{a^2 + b^2} + i \cdot \frac{-b}{a^2 + b^2} \implies z^{-1} \in \mathbb{C}$$

A questo punto, ponendo $c = \frac{a}{a^2+b^2}$ e $d = \frac{-b}{a^2+b^2}$, otteniamo che $z^{-1} = c + id \implies z^{-1} \in \mathbb{C}$ è un numero complesso diverso da zero, rispettando il vincolo di dominio richiesto dalla condizione di validità dell'assioma di elemento inverso del prodotto.

Avendo provato quindi la validità dell'ultimo assioma richiesto, possiamo dichiarare i **numeri complessi** come un **campo**.

Approfondimento sui numeri complessi

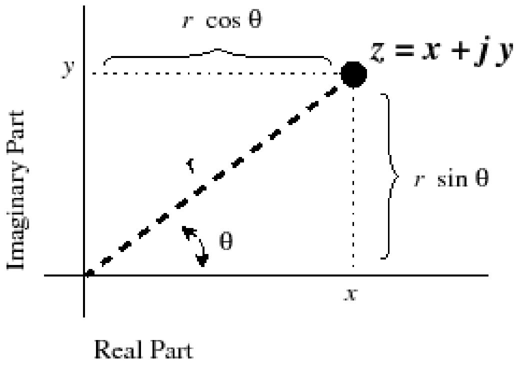
Abbiamo visto come un numero complesso possa essere espresso come un punto sul piano gaussiano tramite una **coppia di valori**, descrivendo la distanza di tale punto dall'origine del piano $(0, 0)$ come $|z|$.

Possiamo quindi descrivere una **circonferenza di raggio** $r = |z|$ rappresentante tutti i numeri complessi aventi la stessa distanza dall'origine, dove θ corrisponde all'**arco in radianti** descritto dal **vettore** costruito attraverso le due coordinate gaussiane rappresentate da z.

Dunque, se $r = |z|$, abbiamo che:

$$r = |z| \implies \begin{cases} a = r \cdot cos(\theta) \\ b = r \cdot sin(\theta) \end{cases} \implies \begin{cases} cos(\theta) = \frac{a}{r} = \frac{a}{|z|} \\ sin(\theta) = \frac{b}{r} = \frac{b}{|z|} \end{cases}$$

Graficamente, ciò corrisponde a dire che:



Tuttavia, ricordando le proprietà delle funzioni seno e coseno, notiamo come il sistema imposto ammetta **infinite soluzioni**, poiché se θ è una soluzione allora anche $\theta+2k\pi, k \in \mathbb{Z}$ è soluzione del sistema.

Per tale motivo, ogni soluzione valida viene detta **argomento di z** e, in particolare, esiste **un solo argomento principale** tale che $0 \leq \theta \leq 2\pi$. Definiamo quindi come $arg(z)$ l'insieme contenente tutti gli argomenti di z, mentre definiamo come $Arg(z)$ l'argomento principale di z.

Considerato il sistema imposto, dato un numero $z = a + ib \in \mathbb{C}$, possiamo riscrivere tale numero complesso nella sua **forma polare**, ossia:

$$z = a + ib = r \cdot cos(\theta) + r \cdot i \cdot sin(\theta) = r \cdot (cos(\theta) + i \cdot sin(\theta))$$

Introduciamo ora la seguente **notazione contratta**:

$$e^{i\theta} = cos(\theta) + i \cdot sin(\theta)$$

Riscriviamo quindi la forma polare di z come:

$$z = r \cdot (cos(\theta) + i \cdot sin(\theta)) = re^{i\theta}$$

Giustificazione:

Matematicamente, tramite le proprietà degli esponenti abbiamo che

$$e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$$

Svolgiamo ora tale calcolo tramite la notazione esplicita

$$(cos(\theta_1) + i \cdot sin(\theta_1)) \cdot (cos(\theta_2) + i \cdot sin(\theta_2)) =$$

$$[cos(\theta_1) \cdot cos(\theta_2) - sin(\theta_1) \cdot sin(\theta_2)] + i \cdot [cos(\theta_1) \cdot cos(\theta_2) + sin(\theta_1) \cdot sin(\theta_2)] =$$

Tramite le proprietà trigonometriche, riscriviamo tale espressione come:

$$cos(\theta_1 + \theta_2) + i \cdot sin(\theta_1 + \theta_2)$$

Riscrivendo il risultato nella forma contratta imposta, otteniamo che i due calcoli matematici risultano essere equivalenti tra di loro:

$$cos(\theta_1 + \theta_2) + i \cdot sin(\theta_1 + \theta_2) = e^{i(\theta_1+\theta_2)}$$

L'uso di tale notazione ci permette di svolgere in modo rapido operazioni tra numeri complessi, in particolare tramite la **formula di Moiuvre**:

$$z \in \mathbb{C}, z = re^{i\theta} \implies z^n = (re^{i\theta})^n = r^n e^{in\theta}$$

Esempi:

1. Dato $z = -i$, calcolare z^4.
   - Calcoliamo l'argomento principale di z: $|z| = \sqrt{0^2 + (-1)^2} = 1$

   $$\begin{cases} cos(\theta) = \frac{0}{1} = 0 \\ sin(\theta) = \frac{-1}{1} = -1 \end{cases} \implies Arg(z) = \frac{3}{2}\pi \implies arg(z) = Arg(z) + 2k\pi, k \in \mathbb{Z}$$

   - Quindi, riscriviamo z come

   $$z = re^{Arg(z)\cdot i} = e^{\frac{3}{2}\pi\cdot i}$$

   - A questo punto, z^4 corrisponderà a:

   $$z^4 = e^{4\cdot\frac{3}{2}\pi\cdot i} = e^{6\pi\cdot i} = e^{0\cdot i} = 1$$

2. Dato $z = 1 - i$, calcolare z^10.
   - Calcoliamo l'argomento principale di z: $|z| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$

   $$\begin{cases} cos(\theta) = \frac{1}{\sqrt{2}} \\ sin(\theta) = \frac{-1}{\sqrt{2}} \end{cases} \implies Arg(z) = \frac{7}{4}\pi \implies arg(z) = Arg(z) + 2k\pi, k \in \mathbb{Z}$$

   - Quindi, riscriviamo z come

   $$z = re^{Arg(z)\cdot i} = \sqrt{2}e^{\frac{7}{4}\pi\cdot i}$$

   - A questo punto, z^10 corrisponderà a:

   $$z^{10} = \sqrt{2}^1 0e^{10\cdot\frac{7}{4}\pi\cdot i} = 2^5 e^{\frac{35}{2}\pi\cdot i} = 2^5 e^{(16\pi + \frac{3}{2}\pi)\cdot i} = 2^5 e^{\frac{3}{2}\pi i}$$

   - Siccome abbiamo visto che $e^{\frac{3}{2}\pi i} = -i$, allora riscriviamo z^10 come:

   $$z^{10} 2^5 e^{\frac{3}{2}\pi i} = -2^5 i$$

Teorema fondamentale dell'algebra

Considerati due numeri z e n dove $z \in \mathbb{C}$ e $n \in \mathbb{N}, n \geq 2$, ci chiediamo quante siano le **soluzioni complesse dell'equazione** $x^n = z$.

Nel caso in cui $z = 0$, l'unica soluzione risulta essere $x = 0$. Nel caso in cui $z \neq 0$, invece, esistono n **distinte soluzioni**.

Utilizzando la formula di Moiuvre, possiamo riscrivere tale espressione come:

$$x^n = z$$

$$x = \sqrt[n]{z}$$

$$x = z^{\frac{1}{n}}$$

$$x = r^{\frac{1}{n}} e^{\frac{1}{n}\theta i}$$

Abbiamo quindi trovato **una soluzione valida** per l'equazione. Tuttavia, ricordando che un numero complesso z possiede **infiniti argomenti**, riscriviamo x come:

$$x = r^{\frac{1}{n}} e^{i(\frac{\theta}{n} + \frac{2k\pi}{n})}$$

A questo punto, al variare di $k = 0, 1, ..., n-1$ otteniamo le n **soluzioni all'equazione**. Difatti, quando $k = n$, riotteniamo la prima soluzione dell'equazione, mentre quando $k = n + 1$ otteniamo la seconda, e così via.

Esempio: Dato $z = i$, vogliamo sapere le soluzioni dell'equazione $x^3 = z$.

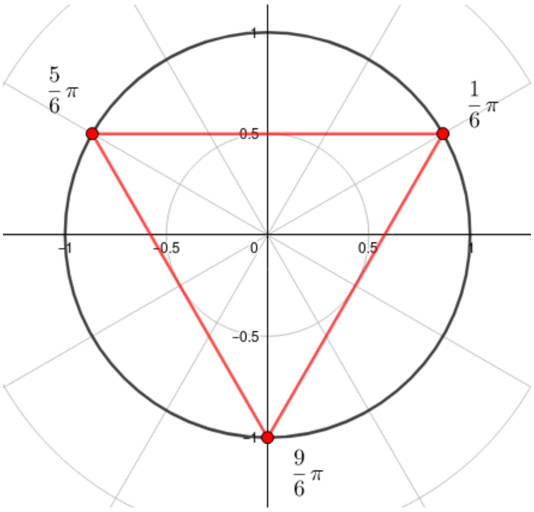
$$x^3 = i \implies x^3 = e^{\frac{1}{2}\pi i}$$

$$x = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{2k\pi}{3})}$$

- Se $k = 0$
$$x_1 = e^{i(\frac{1}{2 \cdot 3}\pi)} = e^{\frac{1}{6}\pi i}$$
- Se $k = 1$
$$x_2 = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{2\pi}{3})} = e^{\frac{5}{6}\pi i}$$
- Se $k = 2$
$$x_3 = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{4\pi}{3})} = e^{\frac{9}{6}\pi i} = e^{\frac{3}{2}\pi i}$$
- Se $k = 3$
$$x_4 = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{6\pi}{3})} = e^{i(\frac{1}{6}\pi + 2\pi)} = e^{\frac{1}{6}\pi i} \implies x_4 = x_1$$
- Se $k = 4$
$$x_5 = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{8\pi}{3})} = e^{i(\frac{1}{6}\pi + \frac{2\pi}{3} + 2\pi)} = e^{\frac{5}{6}\pi i} \implies x_5 = x_2$$
- ...

Notiamo quindi che nonostante esistano **infiniti argomenti di z**, le soluzioni risultano essere cicliche tra di loro, risultando in solo3 **soluzioni valide per l'equazione**.

Inoltre, graficando sul piano di Gauss le tre radici soluzioni dell'equazione, notiamo come ognuna di esse corrisponda al vertice di un triangolo equilatero iscritto in una circonferenza di raggio 1:



Osservazione:

Le n radici n-esime di un numero complesso sono i vertici di un poligono regolare di n lati inscritto in una circonferenza di raggio $|z|^{\frac{1}{n}}$.

Infine, concludiamo il nostro studio sui numeri complessi affermando il seguente **teorema fondamentale dell'algebra**

Definition 9. Teorema fondamentale dell'algebra

Data un'equazione del tipo:

$$(E) = a_0 + a_1 x + ... + a_n x^n$$

dove (E) indica una qualsiasi espressione e $a_i \in \mathbb{C}, n \geq 1, a_n \neq 0$, **esiste sempre almeno una soluzione complessa di** (E).

1.4 Relazioni

Dato un insieme S, definiamo come **relazione** R su S un **sottoinsieme del prodotto cartesiano** $S \times S$:

$$R \subseteq S \times S \implies R \subset \{(x, y) \,|\, x, y \in S\}$$

Data una coppia (x, y), se essa appartiene alla relazione R allora affermiamo ciò con la notazione xRy (oppure con $R(x, y)$), altrimenti affermiamo che essa non appartiene alla relazione con la notazione $x \not R\, y$ (oppure con $\not R\,(x, y)$).

$$xRy \implies (x, y) \in R$$
$$x \not R\, y \implies (x, y) \notin R$$

Tra le varie proprietà che possono essere soddisfatte da una relazione, in particolare evidenziamo:

- **Riflessività**:
$$xRx \quad \forall x \in S$$
- **Simmetria**:
$$xRy \implies yRx \quad \forall x, y \in S$$
- **Anti-simmetria**:
$$xRy \land yRx \implies x = y \quad \forall x, y \in S$$
- **Transitività**:
$$xRy \land yRz \implies xRz \quad \forall x, y, z \in S$$

Una relazione viene detta **relazione di equivalenza** se su di essa valgono le proprietà di riflessività, simmetria e transitività. L'esempio più banale tale relazione è la relazione di uguaglianza, indicata col simbolo $=$.

Una relazione viene detta **relazione d'ordine parziale** se su di essa valgono le proprietà di riflessività, anti-simmetria e transitività. L'esempio più banale tale relazione è la relazione di precedenza, indicata col simbolo $\prec$. Nel caso in cui tutti gli elementi di una relazione d'ordine parziale siano confrontabili tra di loro (ossia se $\forall x, y \in S$ vale $xRy \lor yRx$), definiamo tale relazione come **relazione d'ordine totale**.

Esempi:

- La relazione $\leq$ è un ordine totale
- Dato un insieme X, definiamo come $P(X)$ l'insieme contenente tutte le delle parti (ossia i sottoinsiemi) di X
$$P(X) = \{\texttt{tutti i sottoinsiemi di } X\}$$
La relazione $\subseteq$ su $P(X)$ risulta essere una relazione d'ordine parziale, poiché:
  - Ogni sottoinsieme A è sottoinsieme di se stesso (riflessività):
$$A \subseteq A \quad \forall A \in P(X)$$
  - Se un sottoinsieme A è sottoinsieme di B e B è sottoinsieme di A, allora ciò è possibile solo se A e B sono lo stesso sottoinsieme (anti-simmetria):
$$A \subseteq B \land B \subseteq A \implies A = B$$
  - Se un sottoinsieme A è sottoinsieme di B e B è sottoinsieme di C, allora anche A è sottoinsieme di C (transitività):
$$A \subseteq B \land B \subseteq C \implies A \subseteq C$$
  - Non tutti i sottoinsiemi sono confrontabili tra loro (ordine non totale), ad esempio $\{1\} \nsubseteq \{2\}$

- Dati due numeri naturali $m, n \in \mathbb{Z}$, affermiamo che m è divisore di n, indicato come $m \,|\, n$ (*Attenzione: non è il simbolo matematico "tale che"*), se esiste un elemento $p \in \mathbb{Z} \,|\, m \cdot p = n$:

$$| \, : \{(m,n) \,|\, m,n \in \mathbb{Z}, \exists p \in \mathbb{Z}, m \cdot p = n\}$$

Analizziamo le proprietà della relazione definita:

  – Soddisfa la **riflessività**:

$$m \,|\, m \quad \forall m \in \mathbb{Z} \implies m \cdot 1 = m$$

  – Soddisfa la **transitività**:

$$d \,|\, m \implies \exists p \in \mathbb{Z}, d \cdot p = m$$

$$m \,|\, n \implies \exists q \in \mathbb{Z}, m \cdot q = n$$

$$d \,|\, m \wedge m \,|\, n \implies n = m \cdot q = d \cdot p \cdot q = d \cdot (pq) \implies d \,|\, n$$

  – Non soddisfa l'**anti-simmetria**:

$$m \,|\, n \implies \exists p \in \mathbb{Z}, m \cdot p = n$$

$$n \,|\, m \implies \exists q \in \mathbb{Z}, n \cdot q = m$$

$$m \,|\, n \wedge n \,|\, m \implies m = n \cdot q = m \cdot p \cdot q$$

  a questo punto, si hanno due casi:

    * $m = 0 \implies n = p = q = 0$
    * $m \neq 0 \implies p \cdot q = 1 \implies p = q = \pm 1$
      · Se $p = q = 1 \implies m = n$
      · Se $p = q = -1 \implies m = -n$

  Dunque, deduciamo che non in tutti i casi la relazione $|$ risulta essere anti-simmetrica. Nel caso in cui la relazione venisse applicata su $\mathbb{N}$ invece che $\mathbb{Z}$, il caso in cui $p = q = -1$ verrebbe scartato, poiché $-1 \notin \mathbb{N}$, rendendo quindi la relazione anti-simmetrica e, di conseguenza, anche una relazione d'ordine parziale.

1.4.1 Relazione di congruenza

Un particolare esempio di relazione di equivalenza è la **relazione di congruenza**: dato $n \in \mathbb{N}, n \geq 2$ e dati $a, b \in \mathbb{Z}$ denotiamo con $a \equiv b (\bmod\ n)$ la relazione "a è congruente b modulo n se vale n è divisore di $b - a$ $(n \,|\, b - a)$.

Esempi:

- $7 \equiv 22 (\bmod\ 5) \implies b - a = 22 - 7 = 15\%5 = 0$
- $7 \equiv 13 (\bmod\ 5) \implies b - a = 13 - 7 = 6\%5 = 1$

La relazione definita risulta essere:

- **Riflessiva**:

$$0 = n \cdot 0 \implies n \,|\, 0 \implies n \,|\, a - a \implies a \equiv a (\texttt{mod}\ n) \quad \forall a \in \mathbb{Z}$$

- **Simmetrica**:

$$a \equiv b (\texttt{mod}\ n) \implies n \,|\, b - a \implies \exists p \in \mathbb{Z}, b - a = n \cdot p \implies$$
$$\implies a - b = n \cdot (-p) \implies n \,|\, a - b \implies b \equiv a (\texttt{mod}\ n)$$

- **Transitiva**:

  Siccome:

$$a \equiv b (\texttt{mod}\ n), b \equiv c (\texttt{mod n}) \implies b - a = n \cdot p, c - b = n \cdot q$$

  allora:

$$c - a = (c - b) + (b - a) = q \cdot n + p \cdot n = n(q + p) \implies n \,|\, c - a \implies a \equiv c (\texttt{mod}\ n)$$

1.4.2 Teorema della divisione con resto euclidea

Theorem 1. Teorema della divisione con resto euclidea

Dati due interi $m, n \in \mathbb{Z}$ dove $n > 0$, allora

$$\exists! q, r \in \mathbb{Z} \,|\, m = n \cdot q + r, 0 \leq r < n$$

dove q viene definito come **quoziente** e r come **resto** della divisione

Dimostrazione dell'unicità:

Supponiamo che q ed r non siano unici. Allora, ne segue che:

$$nq_1 + r_1 = m = nq_2 + r_2 \implies r_2 - r_1 = n(q_1 - q_2) \implies n \,|\, r_2 - r_1$$

Siccome $0 \leq r_1, r_2 < n \implies -n < r_2 - r_1 < n$ e siccome $n \,|\, r_2 - r_1$, ciò significa che $r_2 - r_1$ deve essere un multiplo di n compreso tra $-n$ ed n stesso. Poiché l'unico numero rispettante tali caratteristiche è 0, ne segue che:

$$r_2 - r_1 = 0 \implies r_2 = r_1$$

Quindi, otteniamo che:

$$nq_1 + r_1 = nq_2 + r_2 \implies nq_1 = nq_2 \implies q_1 = q_2$$

Dimostrazione dell'esistenza:

Sia $[m]$ la **classe di congruenza** di $m(\texttt{mod}\ n)$:

$$[m] : \{a \in \mathbb{Z} \,|\, a \equiv m(\texttt{mod} n)\}$$

Allora, abbiamo che:

$$n \,|\, m - a \implies m - a = n \cdot p \implies a = m - np$$

Sia r il minimo valore tra le $a \in [m]$, dove $a > 0$. Quindi, vale che

$$\exists r \in \mathbb{Z} \,|\, r = m - nq \implies m = nq - r$$

Verifichiamo ora che $0 \leq r < n$. Assumiamo per assurdo che $r \geq n$, allora ne segue che $r - n \geq 0$. Quindi abbiamo che:

$$r - n = (m - nq) - n = m - (q+1)n \implies m - (q+1)n \in [m] \implies r \text{ non è il minimo valore}$$

1.4.3 Classi di equivalenza

Data una relazione d'equivalenza generica $\sim$ definita su un insieme S, denotiamo con $[x]$ la sua **classe di equivalenza**, dove $[x] \subseteq S$ e $x \in S$.

$$[x] = \{y \in S \,|\, x \sim y\}$$

Ogni classe di equivalenza possiede **almeno un elemento**, poiché $x \sim x, \forall x \in S$ per riflessività della relazione d'equivalenza. Inoltre, per transitività abbiamo che:

- Avendo $x \sim y$, se $z \in [x] \implies z \sim x$ allora $z \sim y \implies z \in [y]$, dunque $[x] \subseteq [y]$. Effettuando il ragionamento opposto, ne traiamo che $[y] \subseteq [x]$ e dunque che

  $$x \sim y \implies [x] = [y]$$

- Supponiamo per assurdo che $zin[x] \cap [y]$. Ciò significa che $z \in [x] \land z \in [y] \implies z \sim x \land z \sim y$, dunque per transitività si verifica che $x \sim y$. Dunque, concludiamo che:

  $$x \nsim y \implies [x] \cap [y] = \emptyset$$

Definiamo come $S/\sim$ l'**insieme di tutte le classi di equivalenza** di una relazione d'equivalenza generica $\sim$.

Ad esempio, se $S = \mathbb{Z}$ e $\sim$ è la relazione di congruenza ($a \sim b \implies a \equiv b(\texttt{mod}\ n)$, allora denotiamo la classe di equivalenza di tale relazione come **insieme quoziente** Z_n. Per via del teorema della divisione con resto euclidea, Z_n risulta essere un insieme finito:

$$Z_n : \{[0], [1], ..., [n-1]\}$$

Dato un insieme X e un insieme I contenente degli indici, una **partizione di** X è un sottoinsieme di X disgiunto da tutte le altre partizioni di X:

$$X = \bigcup_{i \in I} X_i \text{ dove } i \neq j \implies X_i \cap X_j = \emptyset$$

Per comodità, denotiamo il partizionamento di un insieme X come

$$X = \coprod_{i \in I} X_i$$

In particolare, è opportuno puntualizzare come **applicare una relazione di equivalenza su un insieme equivale a partizionare tale insieme**, dove ogni classe di equivalenza corrisponde ad una partizione dell'insieme:

$$X = \coprod_{[x] \in S/\sim} [x]$$

Inoltre, dato un partizionamento di X, otteniamo una relazione di equivalenza $\sim$ su di esso:

- **Riflessività**:
$$\forall x \in X, \exists i \in I \,|\, x \in X_i \implies x \sim x$$

- **Simmetria**:
$$x \sim y, \exists i, j \in I \,|\, x, y \in X_i \implies x, y \in X_j \implies y \sim x$$

- **Transitività**:
$$x \sim y, y \sim z, \exists i, j \in I \,|\, x, y \in X_i, y, z \in X_j \implies y \in X_i \cap X_j$$

  Tuttavia, poiché le partizioni sono disgiunte tra loro, abbiamo che $i \neq j \implies X_i \cap X_j = \emptyset$, quindi si può verificare solo che $i = j \implies X_i = X_j$, dunque otteniamo che $x \sim z$.

Infine, affermiamo che applicare una relazione di equivalenza su un insieme equivale ad applicare una **funzione suriettiva** detta **"proiezione al quoziente"**:

$$p : X \to X/\sim : x \mapsto [x]$$