CAMPI E NUMERI COMPLESSI

ULTIMO AGGIORNAMENTO 10-2–2010

[Appunti] Appunti di Algebra Lineare

1. NUMERI

In questa sezione introdurremo la nozione di campo ponendo particolare attenzione al campo dei numeri complessi di cui daremo alcune proprietà.

In Matematica gli insiemi , e eventuali operazioni tra insiemi o tra elementi di un assegnato insieme debbono sempre essere definite. A volte trattando insiemi ben noti quali per esempio l' insieme $\mathbb{N}$ dei numeri naturali $0, 1, 2, \dots$, vengono date per conosciute sia la definizione che le operazioni tra gli elementi dell' insieme; nel caso specifico la somma e il prodotto. Per quanto riguarda i numeri naturali e l' insieme $\mathbb{Z}$ dei numeri interi $, \dots, -1, 0, 1, 2, \dots$ ci comporteremo in questo modo, poiché una trattazione assiomatica esula dai contenuti di questo corso. Ovviamente, anche in questi casi esiste una assiomatica precisa frutto di intenso lavoro sui fondamenti della Matematica. Proveremo a spiegarla dando un' idea delle problematiche coinvolte.

L' insieme $\mathbb{N}$ dei numeri naturali può essere descritto dai *Postulati di Peano* per i quali i numeri naturali sono un insieme $\mathbb{N}$ dotato di un elemento privilegiato (lo 0) e caratterizzati dal fatto che ogni elemento ha un successivo, ma 0 è l' unico elemento che non è successivo a nessun elemento. Da una rigorosa formulazione di questa definizione discendono facilmente tutte le proprietà dei numeri naturali , in particolare possono essere definite le operazioni di somma e prodotto che risultano essere associative e commutative.
Dati per conosciuti i numeri naturali possiamo introdurre senza tanta fatica l' insieme dei numeri interi $\mathbb{Z}$ e l' insieme dei numeri razionali $\mathbb{Q}$. Proveremo a spiegare come procedere.
Assegnati due numeri naturali n, m, non sempre l' equazione del tipo $n+x = m$ ha una soluzione in $\mathbb{N}$, infatti se $n > m$ sappiamo che la soluzione è un numero negativo. Allora $\mathbb{Z}$ è l'insieme dove la precedente equazione ha sempre un' unica soluzione.
Si può facilmente verificare che nel caso precedente x risulta essere soluzione di infinite equazioni, infatti abbiamo che le equazioni $3 + x = 1, \quad 6 + x = 4, \quad 1000 + x = 998$ hanno tutte la stessa soluzione -2. La notazione $-r$ viene introdotta considerandola come l' unica soluzione dell' equazione $r + x = 0$ con $r \geq 0$. quindi possiamo porre

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

Le operazioni di somma e prodotto e le loro proprietà si estendono a $\mathbb{Z}$.
La necessità di risolvere equazioni del tipo $nx = m$ con $n, m \in \mathbb{Z}$ comporta l' introduzione dell' insieme $\mathbb{Q}$ dei numeri razionali che di solito vengono rappresentati in forma frazionaria $\frac{m}{n}$. Si può facilmente verificare che nel caso precedente x risulta essere soluzione di infinite equazioni, infatti abbiamo che le equazioni

$$2x = 1, \quad 4x = 2, \quad 50x = 100$$

sono soddisfatte tutte dallo stesso valore di $x = \frac{1}{2} = \frac{2}{4} = \frac{50}{100}$. Osserviamo , però, che solo in un caso il numeratore e il denominatore sono privi di fattori in comune. Questo è un fatto generale e quindi poniamo

$$\mathbb{Q} = \{\frac{a}{b} \,\mathrm{con}\, b \neq 0,\ a, b \in \mathbb{Z}\,\mathrm{privi\,di\,fattori\,comuni}\}$$

Le operazioni di somma e prodotto e le loro proprietà si estendono a $\mathbb{Q}$.

Osservazione 1.1. Ricordiamo che sommando o moltiplicando due frazioni, secondo le ben note regole, possiamo ottenere una frazione con fattori in comune, infatti abbiamo

$$\frac{1}{3}+\frac{1}{6}=\frac{3}{6}=\frac{1}{2}$$
$$\frac{5}{2}\cdot\frac{4}{7}=\frac{20}{14}=\frac{10}{7}$$

Oltre ai numeri naturali, interi e razionali un insieme di numeri ritenuti ben noti sono i numeri reali. La costruzione dei numeri reali a partire dai numeri razionali richiede alcune conoscenze, come il concetto di successione di Cauchy oppure di estremo superiore, che saranno acquisite in seguito dallo studente. Possiamo però procedere nel modo seguente.

I numeri razionali possono essere rappresentati tramite il sistema numerico decimale, per esempio $\frac{1}{2}=0,5$ oppure $\frac{1}{3}=0,\overline{3}$. Questo ultimo esempio ci ricorda che lo sviluppo decimale dei numeri razionali ha la particolarità di essere periodico: nella sua scrittura esiste una sequenza finita di cifre (detta periodo) che si ripete all'infinito, da un certo punto in poi dopo la virgola. Ebbene diremo che l' insieme dei numeri reali , $\mathbb{R}$, è dato da tutti i numeri rappresentabili tramite il sistema numerico decimale.
Questo modo di rappresentare i numeri reali (e i numeri razionali) presenta alcune inconvenienze
Ci sono più rappresentazioni per lo stesso numero, infatti abbiamo che $1=0,\overline{9}$. Comunque è possibile verificare che l'espansione decimale di un numero reale unica a meno che il numero non sia razionale del tipo $q/10^m$, $q,m\in\mathbb{N}$.
Non è possibile sommare e moltiplicare numeri reali nel modo usuale perché potremmo avere infinite cifre dopo la virgola.
Un ultimo fatto che disturba molto da un punto di vista matematico , è che la rappresentazione ancorata alla scelta della base 10, ma si potrebbe scegliere una qualunque altra base, per esempio in informatica si usa base 2. Pertanto la rappresentazione non risulta essere *canonica* e a volte è disdegnata dai matematici.
Dal punto di vista intuitivo e del calcolo è utile sapere che i numeri reali possono essere messi in corrispondenza biunivoca con i punti di una retta, detta retta reale.
Usando la rappresentazione numerico decimale si può facilmente verificare che l ' insieme dei numeri reali contiene propriamente i numeri razionali infatti il numero

$$x=0,101001000100001\ldots$$

con ogni 1 separato da una sequenza di zeri di lunghezza crescente, non è razionale, perché, se fosse razionale, il suo periodo obbligherebbe una ricorsività delle sequenze di cifre.
I numeri reali che non sono razionali si dicono irrazionali. L' irrazionalità di alcuni numeri reali può essere dimostrata anche per via algebrica.

Esempio 1.2. Vediamo che $\sqrt{2}$ non è razionale. Supponiamo che lo sia. Possiamo scrivere

$$\sqrt{2}=\frac{a}{b}$$

con $b\neq 0$ e $a,b\in\mathbb{Z}$ privi di fattori comuni. Si ha

$$2=\frac{a^2}{b^2},\ \text{da cui}\ 2a^2=b^2.$$

Pertanto 2 divide b^2 e quindi b è pari; allora 4 divide b^2 e di conseguenza $2a^2$. Ragionando come in precedenza otteniamo che anche a è pari. Cos ì a e b hanno fattori in comune. Questa è in contraddizione con l' asserto iniziale, allora $\sqrt{2}$ non è razionale.

Osservazione 1.3. Un numero naturale n è un quadrato perfetto , se esiste un altro numero naturale m tale che $n=m^2$. La dimostrazione precedente può essere applicata a tutti i numeri naturali che non sono quadrati perfetti. In questo modo posssiamo produrre un numero infinito di numeri irrazionali

2. CAMPI E NUMERI COMPLESSI

Abbiamo appena visto che i numeri razionali (e i numeri reali) sono dotati di due operazioni , la somma + e il prodotto· che godono di notevoli proprietà:

(1) La somma è associativa, i.e. per ogni $x, y, z \in \mathbb{R}$ si ha
$$(x + y) + z = x + (y + z)$$
(2) La somma è commutativa, i.e. per ogni $x, y, \in \mathbb{R}$ si ha
$$x + y = y + x$$
(3) Esiste un elemento neutro, 0, per la somma i.e. per ogni $x, \in \mathbb{R}$ si ha
$$x + 0 = 0 + x = x$$
(4) Ogni elemento di $\mathbb{R}$ ha un opposto, i.e. per ogni $x, \in \mathbb{R}$ esiste $-x$tale che
$$x + (-x) = 0$$
(5) Il prodotto è associativo, i.e. per ogni $x, y, z \in \mathbb{R}$ si ha
$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$
(6) Il prodotto è commutativo, i.e. per ogni $x, y, \in \mathbb{R}$ si ha
$$x \cdot y = y \cdot x$$
(7) Esiste un elemento neutro, 1, per lil prodotto i.e. per ogni $x, \in \mathbb{R}$ si ha
$$x \cdot 1 = 1 \cdot x = x$$
(8) Ogni elemento non nullo di $\mathbb{R}$ ha un inverso, i.e. per ogni $x, \in \mathbb{R}$ esiste x^{-1} tale che
$$x \cdot x^{-1} = 1$$
(9) Il prodotto è distributivo rispetto alla somma, i.e. per ogni $x, y, z \in \mathbb{R}$ si ha
$$x \cdot (y + z) = x \cdot y + x \cdot z$$

Un insieme che gode di queste proprietà si dice *campo*. Per semplificare le notazioni, usualmente, il simbolo del prodotto viene omesso e si scrive xy per $x \cdot y$. Ovviamente $\mathbb{Q}$ e $\mathbb{R}$ sono campi. $\mathbb{N}$ e $\mathbb{Z}$ non sono campi: in entrambi i casi la proprietà (8) non è soddisfatta. Infatti l' inverso di 5, $\frac{1}{5}$, non è un numero intero e quindi naturale.

Vediamo ora alcuni esempi significativi di campi. Opportune estensioni dei numeri razionali sono un campo. Sia p un numero primo consideriamo l' insieme
$$\mathbb{Q}(\sqrt{p}) = \{x \in \mathbb{R}\,\text{tale che}\, x = a + \sqrt{p}b,\,\text{con}\, a, b \in \mathbb{Q}\}.$$
Si verifica rapidamente che $\mathbb{Q}(\sqrt{p})$ è chiuso rispetto alla somma e al prodotto, cioè, la somma e/o il prodotto di due elementi di $\mathbb{Q}(\sqrt{p})$ è ancora un elemento di $\mathbb{Q}(\sqrt{p})$.

Essendo $\mathbb{Q}(\sqrt{p})$ un sottinsieme di $\mathbb{R}$ le proprietà $(1), (2), (5), (6), (9)$ risultano essere verificate, ovviamente 0 e 1 appartengono a $\mathbb{Q}(\sqrt{p})$ e soddisfano le proprietà $(3)e(7)$, l'opposto di ogni elemento è in $\mathbb{Q}(\sqrt{p})$, quindi l' unica proprietà rimasta da verificare è l' esistenza dell' inversa. Sia $x = a + \sqrt{p}b$ con a e b non entrambi nulli, poniamo
$$x^{-1} = \frac{a - \sqrt{p}b}{a^2 - pb^2} = \frac{a}{a^2 - pb^2} + \frac{-\sqrt{p}b}{a^2 - pb^2}.$$
x^{-1} è l' inverso di x. Osserviamo che il fattore al denominatore della precedente espressione è sempre diverso da 0, perché p è un numero primo.

Un numero naturale n si dice privo di quadrati se la sua fattorizzazione in primi non contiene fattori ripetuti. Sia n un numero privo di quadrati, si può verificare in modo simile che
$$\mathbb{Q}(\sqrt{n}) = \{x \in \mathbb{R}\,\text{tale che}\, x = a + \sqrt{n}b,\,\text{con}\, a, b \in \mathbb{Q}\}$$
è un campo. Questi campi sono detti estensioni quadratiche di $\mathbb{Q}$, poiché l' elemento che è stato aggiunto, $\sqrt{n}$, è soluzione di un' equazione di secondo grado a coefficienti in $\mathbb{Q}$, i.e.$x^2 - n = 0$.

Possono essere costruiti anche campi con un numero finito di elementi. Rimandiamo al corso di Algebra per maggiori dettagli, osserviamo solamente che l' insieme $\mathbb{F}_2$ formato da due elementi, $\{0, 1\}$, con, oltre le usuali, l' ulteriore proprietà che $1 + 1 = 0$, è un campo.

Finora abbiamo dato numerosi esempi di campi che contengono i numeri razionali. Vogliamo ora introdurre un campo che contiene il campo dei numeri reali e che risulterà essere fondamentale sia dal punto di vista algebrico che geometrico. Questo è il campo dei numeri complessi che indicheremo con il simbolo $\mathbb{C}$. Alla base della definizione dei numeri complessi cè la definizione di un particolare numero complesso, denotato con i tale che $i^2 = -1$.
Ricordiamo che il prodotto cartesiano $A \times B$ tra due insiemi A e B è formato dall' insieme delle coppie (a, b), $a \in a, b \in B$. Scriveremo A^n per indicare il prodotto cartesiano tra n copie dell' insieme A.

Definizione 2.1. Ogni numero complesso z è individuato in modo univoco da una coppia di numeri reali $(x, y) \in \mathbb{R}^2$ e scriveremo $z = x \oplus iy$. x e y sono detti la parte reale e la parte immaginaria di z e vengono indicati con $Re\, z$ le $Im\, z$.

Definiamo la somma e il prodotto di due numeri complessi nel modo seguente

$$z_1 + z_2 = (x_1 + x_2) \oplus i(y_1 + y_2), \,\text{con}\, z_j = x_j \oplus iy_j,\ j = 1, 2$$

$$z_1 z_2 = x_1 x_2 - y_1 y_2 \oplus i(y_1 x_2 + x_1 y_2), \,\text{con}\, z_j = x_j \oplus iy_j,\ j = 1, 2$$

Osserviamo che i numeri reali possono essere considerati come il sottinsieme dei numeri complessi della forma $x \oplus i0$. In questo caso la somma e il prodotto di die tali numeri coincide con l' usuale prodotto di numeri reali. Inoltre l' operazione di somma riguarda separatamente le parti reali e le parti immaginarie e coinvolge solo numeri reali pertanto, d' ora in poi, per semplificare le notazioni scriveremo per un numero complesso $z = x + iy$ in quanto la notazione è consistente con le operazioni introdotte.

Proposizione 2.2. $\mathbb{C}$ *con le operazioni introdotte è un campo*

Dimostrazione: Si verifica facilmente che la somma verifica le proprietà $(1), (2), (3), (4)$ e che le proprietà $(6), (7), (9)$ sono soddisfatte. L'associatività del prodotto può essere verificata applicando le definizioni. Il calcolo risulta essere semplice, ma abbastanza lungo. In seguito, dopo aver dato una rappresentazione grafica dei numeri complessi, essa sarà facilmente verificabile. L' inverso di z risulta essere

$$z^{-1} = \frac{x - iy}{x^2 + y^2}$$

Un semplice conto dà $i^2 = -1$

Esempio 2.3. Si verifica immediatamente che
(a) $\frac{1}{2} - i\frac{\sqrt{3}}{2}$ è l' inverso di $\frac{1}{2} + i\frac{\sqrt{3}}{2}$
(b) $(2 + i)(3 - i) = 7 + i$

Osservazione 2.4. Notiamo un' analogia tra i numeri complessi e le estensioni quadratiche di $\mathbb{Q}$. Infatti anche in questo caso l' elemento i è soluzione dell equazione di secondo grado $x^2 + 1 = 0$. A differenza del caso razionale $\mathbb{C}$ è l' unica estensione quadratica di $\mathbb{R}$.
Osserviamo che anche

$$\mathbb{Q}(i) = \{x \in \mathbb{R} \,\text{tale che}\, x = a + ib, \,\text{con}\, a, b \in \mathbb{Q}\}$$

è un campo e in particolare è un' estensione quadratica di $\mathbb{Q}$.

3. Coordinate polari, potenze , radici

Poiché ogni numero complesso z è individuato in modo univoco da una coppia di numeri reali, possiamo identificare $\mathbb{C}$ con l' insieme $\mathbb{R}^2$. Tramite questa identificazione al numero complesso z corrisponde la coppia $(Re\, z, Im\, z)$. Quindi possiamo anche identificare i numeri complessi con l' insieme dei vettori aventi come punto iniziale l' origine e come punto finale il punto di coordinate $(Re\, z, Im\, z)$. Viceversa a un vettore v applicato nell' origine con punto finale (x, y) associamo il numero complesso $z = x + iy$. Un vettore v diverso dal vettore nullo è determinato anche dalla sua lunghezza (o modulo)

$$|v| = \sqrt{x^2 + y^2}$$

e dall' argomento $\theta \in [0, 2\pi)$ che indica l'angolo che il vettore v forma con l' asse delle ascisse. In questo caso abbiamo che

$$x = |v|cos\theta, \quad y = |v|sen\theta.$$

Osserviamo che nel caso in cui $x \neq 0$ si ha $\theta = arctg\, \frac{y}{x}$.. La coppia $(|v|, \theta)$ determina le coordinate polari del vettore v o del numero complesso z. è

Questa rappresentazione dei numeri complessi induce un' interpretazione geometrica della loro somma e del prodotto. Infatti alla somma di due numeri complessi z_1, z_2 corrisponde la somma dei vettori v_1, v_2 corrispondenti. Per il prodotto abbiamo la seguente rappresentazione

$$z_1z_2 = |v_1|(cos\theta_1 + isen\theta_1)|v_2|(cos\theta_2 + isen\theta_2) =$$

$$|v_1||v_2|[(cos\theta_1cos\theta_2 - isen\theta_1sen\theta_2) + i(cos\theta_1sen\theta_2 + cos\theta_2sen\theta_1)] =$$

$$|v_1||v_2|[cos(\theta_1 + \theta_2) + isen(\theta_1 + \theta_2)] \tag{3.1}$$

Quindi al prodotto z_1z_2 corrisponde il numero complesso associato al vettore v avente come lunghezza il prodotto della lunghezze e come argomento la somma degli argomenti, a meno di multipli di 2π. Usando questa rappresentazione risulta molto semplice verificare la propriet à associativa del prodotto di numeri complessi. la discussione precedente conduce alla seguente

Definizione 3.1. Il modulo di un numero complesso $z = x + iy$ è dato da

$$|z| = \sqrt{x^2 + y^2}.$$

Il coniugato di $z = x = iy$ è il numero complesso $\overline{z} = x - iy$

Quindi abbiamo

Proposizione 3.2. *Siano z, z_1, z_2 numeri compleesi*

(1) $|z| \geq 0$ *e l' uguaglianza vale* $\iff z = 0$
(2) $|z| = |\overline{z}|$
(3) $|z_1z_2| = |z_1||z_2|$
(4) $|z_1 + z_2| \leq |z_1| + |z_2|$
(5) $|Re\, z| \leq |z|, \quad |Im\, z| \leq |z|$

Dimostrazione Sono tutte verifiche semplici. La (4) segue dal fatto che la somma della lunghezza di 2 lati di un triangolo è maggiore della lunghezza del terzo lato.

Sono di immediata verifica anche le affermazioni della seguente

Proposizione 3.3. *Siano z, z_1, z_2 numeri compleesi*

(1) $\overline{\overline{z}} = z$
(2) $\overline{z}_1 + \overline{z}_2 = \overline{z_1 + z_2}$
(3) $\overline{z}_1\overline{z}_2 = \overline{z_1z_2}$
(4) $z = \overline{z} \iff z \in \mathbb{R}$
(5) $z = -\overline{z} \iff z \in i\mathbb{R}$
(6) $z + \overline{z} = 2Re\, z$
(7) $z - \overline{z} = i2Im\, z$
(8) $z\overline{z} = x^2 + y^2$

(9) $z^{-1} = \frac{\overline{z}}{x^2+y^2}$

La rappresentazione in coordinate polari del prodotto di numeri complessi trova la sua più fruttifera applicazione nella descrizione delle potenze e delle radici di un numero complesso.

Lemma 3.4. *(Formula di De Moivre) Sia* $z = |z|(cos\theta + isen\theta)$ *un numero complesso, per ogni intero* n *si ha*

$$z^n = |z|^n(cosn\theta + isenn\theta)$$

Dimostrazione E' sufficiente iterare la formula (3.1) nel caso specifico $z_1 = z_2 = z$.

Definizione 3.5. Sia z un numero complesso e n un numero naturale positivo, una radice $n-$esima di z , è un numero complesso w tale che $w^n = z$

Nel caso reale noi sappiamo che ogni numero reale x, differente da 0, ha una radice $n-$esima se n è dispari e due radici $n-$esime se n è pari ed x positivo, nel caso complesso invece la situazione è pi ù semplice, infatti si ha

Proposizione 3.6. *Sia* $z \neq 0$ *un numero complesso e* n *un numero naturale positivo, esistono esattamente* n *radici* $n-$*esime di* z

Dimostrazione Scriviamo $z = |z|(cos\theta + isen\theta)$ con $\theta \in [0, 2\pi)$. Consideriamo gli angoli

$$\theta_k = \frac{\theta + 2k\pi}{n}, \quad k = 0, 1, \dots, (n-1)$$

Ovviamente tutti i θ_k appartengono all' intervallo $[0, 2\pi)$; inoltre $\theta_k \neq \theta_j$ se $0 \leq j \neq k, \leq (n-1)$. Pertanto i numeri

$$w_k = |z|^{1/n}(cos\theta_k + isen\theta_k)$$

sono radici $n-$esime distinte di z.

Viceversa, sia $w = |w|(cos\phi + isen\phi)$ una radice $n-$esima di z, allora abbiamo $|w| = |z|^{1/n}$ e $\phi = \theta_k$ per un certo indice k in $0, 1, \dots, (n-1)$.

Esempio 3.7. I numeri complessi 1, i, -1, $-i$ sono radici quarte dell' unità. Essi hanno tutti modulo 1 e corrispondono ai valori 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ dell' angolo θ.

Osservazione 3.8. Nel caso in cui $|z| = 1$ abbiamo che anche le sue radici $n-$esime hanno lo stesso modulo. In particolare le radici $n-$esime di 1 sono della forma

$$u_k = (cos\frac{2k\pi}{n} + isen\frac{2k\pi}{n})$$

La proposizione precedente può essere riformulata nel modo seguente

Proposizione 3.9. *Sia* $a \neq 0$ *un numero complesso e* n *un numero naturale positivo, l' equazione*

$$Z^n = a \tag{3.2}$$

ha esattamente n *soluzioni distinte.*

Un' ulteriore riformulazione , apparentemente più debole, è che ogni equazione del tipo (3.2) ha sempre una soluzione , anche quando $a = 0$.

Questa affermazione è conseguenza di un teorema più generale che sicuramente è il teorema più importante relativo ai numeri complessi. Daremo solo l' enunciato di questo teorema, poiché le molteplici dimostrazioni date richiedono sempre delle conoscenze che saranno apprese in seguito. Daremo invece alcune definizioni che renderanno più comprensibile l'enunciato

Definizione 3.10. Un polinomio $p(X)$ di una variabile di grado $n \in \mathbb{N}$ a coefficienti in un campo $\mathbb{K}$ è un' espressione del tipo

$$P(X) := a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, \quad a_i \in \mathbb{K}, \text{, e} \, a_n \neq 0.$$

Il termine a_n viene detto coefficiente direttivo (del polinomio) e il termine a_0 termine noto. L' insieme dei polinomi a coefficienti in un campo $\mathbb{K}$ viene indicato con la notazione $\mathbb{K}[X]$.

Osservazione 3.11. Come nel caso dei campi, anche tra gli elementi di $\mathbb{K}[X]$ possono essere definite le operazioni di somma e prodotto. Inoltre tutte le proprietà dei campi, eccetto una, sono soddisfatte. Infatti nessun polinomio di grado $n \geq 1$ ha inverso. In questo caso si dir à che $\mathbb{K}[X]$ ha la struttura di anello commutativo.

Definizione 3.12. Sia $p(Z) \in \mathbb{C}[Z]$ un polinomio di grado n. Un numero complesso z_0 è una radice di $p(Z)$ se

$$P(z_0) = a_n z_0^n + a_{n-1} z_0^{n-1} + \cdots + a_1 z_0 + a_0 = 0$$

Lemma 3.13. *Sia $p(Z) \in \mathbb{C}[Z]$ un polinomio di grado n. $z_0 \in \mathbb{C}$ è una radice di $p(Z)$ se e solo se esiste un polinomio $q(Z) \in \mathbb{C}[Z]$ di grado $n-1$ tale che*

$$p(Z) = (Z - z_0)q(Z)$$

Dimostrazione Usando l 'algoritmo di Ruffini, possiamo dividere il polinomio $p(Z)$ per $(Z - z_0)$ ottenendo l' espressione

$$p(Z) = (Z - z_0)q(Z) + c_0 \quad \text{con } q(Z) \,\text{di grado } n-1.$$

Pertanto $P(z_0) = c_0$ e perció

$$P(z_0) = 0 \iff c_0 = 0$$

Siano ora in grado di enunciare il seguente

Teorema 3.14. Teorema Fondamentale dell' Algebra *Un polinomio di grado $n \geq 1$, $p(Z) \in \mathbb{C}[Z]$, ha sempre una radice complessa.*

Corollario 3.15. *Sia $p(Z) \in \mathbb{C}[Z]$ un polinomio di grado $n \geq 1$ e coefficiente direttivo a_n; esistono $z_1, z_2, \ldots, z_n \in \mathbb{C}$, non necessariamente distinti, tali che*

$$P(Z) = a_n(Z - z_1)(Z - z_2)\ldots(Z - z_n).$$

Osserviamo che nel caso reale, l' affermazione precedente è falsa, infatti il polinomio $X^2 + 1$ non ha radici reali. Comunque anche nel caso reale abbiamo una descrizione della fattorizzazione di un polinomio

Definizione 3.16. Un polinomio $aX^2 + bX + c \in \mathbb{R}[X]$ è irriducibile se $\Delta = b^2 - 4ac < 0$, i.e. non ha radici reali

I polinomi irriducibili di secondo grado e i polinomi di primo grado sono i termini che appaiono nella fattorizzazione dei polinomi $p(X) \in \mathbb{R}[X]$, infatti si ha

Teorema 3.17. *Sia $p(X) \in \mathbb{R}[X]$ un polinomio di grado $n \geq 1$ e coefficiente direttivo a_n; esistono $x_1, x_2, \ldots, x_k \in \mathbb{R}$ e polinomi irreducibili $p_1(X), p_2(X), \ldots, p_h(X)$ tali che $n = 2h + k$ e*

$$P(X) = (X - x_1)(X - x_2)\ldots(X - x_k)p_1(X)p_2(X)\ldots p_h(X).$$

4. Esercizi

(1) Verificare che

$$\mathbb{Q}(\sqrt{6}) = \{x \in \mathbb{R} \,\text{tale che}\, x = a + \sqrt{6}b, \,\text{con}\, a, b \in \mathbb{Q}\}.$$

è un campo

(2) Verificare che

$$\mathbb{Q}(i) = \{z \in \mathbb{C} \,\text{tale che}\, z = a + ib, \,\text{con}\, a, b, \in \mathbb{Q}\}.$$

è un campo

(3) Verificare che l' insieme $\mathbb{F}_3$ formato da tre elementi, $\{0,\ 1,\ -1\}$, con l' ulteriore proprietà che $1 + 1 = -1$, è un campo.

(4) Siano $u_0, u_1, \ldots, u_{n-1}$ le radici $n-$esime dell' unità Verificare che

$$\mathbb{Q}(1^{1/n}) = \{z \in \mathbb{C} \,\text{tale che}\, z = a_0u_0 + a_1u_1 + \ldots a_{n-1}u_{n-1}, \,\text{con}\, a_k \in \mathbb{Q}\}.$$

è un campo

(5) Calcolare $(2+i)(3-i)$ e l'inverso di $4-3i$
(6) Scrivere in coordinate polari i numeri $2+i2\sqrt{3}$ e $3(1+i)$
(7) Calcolare le radici terze dell' unità, i.e. tutti i numeri complessi z tali che $z^3=1$