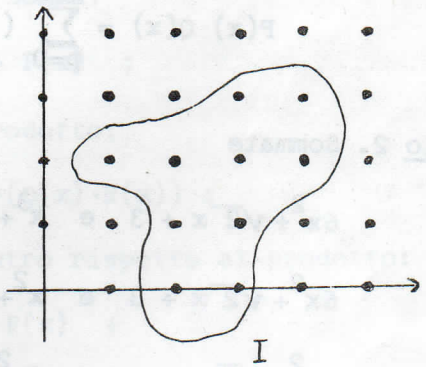
a) il prodotto di due monomi ax^m e bx^n è il monomio abx^{n+m}.

b) per moltiplicare due polinomi tra loro si moltiplicano a due a due i rispettivi monomi e poi si somma.

Se indichiamo con $P(x) = \sum_{j=0}^{n} a_j x^j$ e $Q(x) = \sum_{h=0}^{m} b_h x^h$, è utile avere una espressione del polinomio $P(x)\cdot Q(x)$. A questo scopo, consideriamo sommatorie a due indici (quelle a più indici si trattano in maniera analoga):

$$\sum_{(i,j)\in I} a_{ij} \quad \text{ove } I \text{ è un sottoinsieme di } \mathbb{N}\times\mathbb{N}.$$



Naturalmente la somma si può compiere in modi diversi: ad es., sommando prima fra loro i termini corrispondenti agli indici (i,j) con la stessa ascissa, e poi sommando tra loro le somme parziali così ottenute; oppure raggruppando prima i termini corrispondenti agli indici con la stessa ordinata.

Esercizio 1. Sia T il "triangolo" in $\mathbb{N}\times\mathbb{N}$ di "vertici" $(1,1)$, $(1,n)$, (n,n). Considerate $\sum_{(i,j)\in T} j$. Sommate in entrambi i modi sopra esposti, e, confrontandoli, ricavate la formula della somma dei primi n quadrati perfetti.

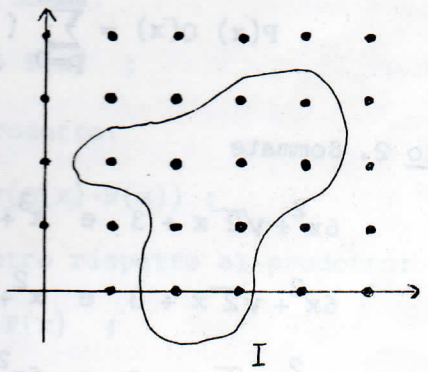
Per moltiplicare fra loro $P(x)$ e $Q(x)$ bisogna quindi moltiplicare ogni monomio $a_j x^j$ per ogni monomio $b_h x^h$ e poi sommare. Si ha quindi

a) il prodotto di due monomi ax^m e bx^n è il monomio abx^{n+m}.

b) per moltiplicare due polinomi tra loro si moltiplicano a due a due i rispettivi monomi e poi si somma.

Se indichiamo con $P(x) = \sum_{j=0}^{n} a_j x^j$ e $Q(x) = \sum_{h=0}^{m} b_h x^h$, è utile avere una espressione del polinomio $P(x)\cdot Q(x)$. A questo scopo, consideriamo sommatorie a due indici (quelle a più indici si trattano in maniera analoga):

$$\sum_{(i,j)\in I} a_{ij} \quad \text{ove } I \text{ è un sottoinsieme di } \mathbb{N}\times\mathbb{N}.$$



Naturalmente la somma si può compiere in modi diversi: ad es., sommando prima fra loro i termini corrispondenti agli indici (i,j) con la stessa ascissa, e poi sommando tra loro le somme parziali così ottenute; oppure raggruppando prima i termini corrispondenti agli indici con la stessa ordinata.

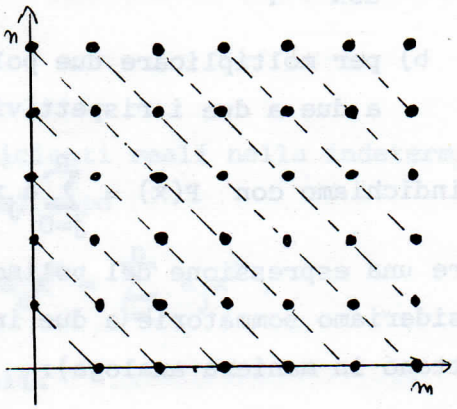
Esercizio 1. Sia T il "triangolo" in $\mathbb{N}\times\mathbb{N}$ di "vertici" $(1,1)$, $(1,n)$, (n,n). Considerate $\sum_{(i,j)\in T} j$. Sommate in entrambi i modi sopra esposti, e, confrontandoli, ricavate la formula della somma dei primi n quadrati perfetti.

Per moltiplicare fra loro $P(x)$ e $Q(x)$ bisogna quindi moltiplicare ogni monomio $a_j x^j$ per ogni monomio $b_h x^h$ e poi sommare. Si ha quindi

$$P(x)\,Q(x) = \sum_{(j,h)\in R} (a_j x^j)(b_h x^h) = \sum_{(j,h)\in R} a_j b_h x^{j+h}$$

dove R è il rettangolo $\left\{(j,h)\in \mathbb{N}\times\mathbb{N} \;\middle|\; 0\le j\le n,\ 0\le h\le m\right\}$.

Conviene in questo caso sommare lungo le diagonali indicate in figura, quelle cioè di equazione $j+h=p$, dove p è un numero naturale. Ogni somma parziale è del tipo



$$\left(\sum_{i+j=p} a_j b_h\right) x^p = \left(\sum_{j=0}^{p} a_j b_{p-j}\right) x^p$$

e quindi risulta

$$P(x)\,Q(x) = \sum_{p=0}^{m+n} \left(\sum_{j=0}^{p} a_j b_{p-j}\right) x^p \ .$$

Esercizio 2. Sommate

$$6x^2+\sqrt{2}\,x+3 \quad \text{e} \quad x^3+\frac{1}{2}x+2$$

$$6x^2+\sqrt{2}\,x+3 \quad \text{e} \quad x^2+\frac{1}{2}x+2$$

$$6x^2+\sqrt{2}\,x+3 \quad \text{e} \quad -6x^2+\frac{1}{2}x+2$$

e moltiplicate

$$6x^4+\sqrt{3}x^2+\pi x+2 \quad \text{per} \quad x^3-3x+8$$

$$4x^3+x \quad \text{per} \quad 8x^4+6x^2+1$$

$$x^5+x^4+x^3+x^2+x+1 \quad \text{per} \quad x-1$$

Proposizione: Nell' insieme dei polinomi a coefficienti reali le operazioni così definite soddisfano le seguenti proprietà:

1) Proprietà associativa della somma:

$$(P(x)+Q(x))+R(x) = P(x)+(Q(x)+R(x)) \ ;$$

2) esistenza dell'elemento neutro rispetto alla somma:

$$P(x) + 0 = 0 + P(x) = P(x) \ ;$$

3) esistenza dell'opposto:

per ogni $P(x)$ esiste $Q(x)$ tale che

$$P(x) + Q(x) = 0$$

(se $P(x) = \sum_{j=0}^{n} a_j x^j$, $Q(x)$, indicato con $-P(x)$ è dato da $Q(x) = \sum_{j=0}^{n} (-a_j) x^j$;

4) proprietà commutativa della somma:

$$P(x) + Q(x) = Q(x) + P(x) \ ;$$

5) proprietà associativa del prodotto:

$$(P(x) \cdot Q(x)) \cdot R(x) = P(x) \cdot (Q(x) \cdot R(x)) \ ;$$

6) esistenza dell'elemento neutro rispetto al prodotto:

$$P(x) \cdot 1 = 1 \cdot P(x) = P(x) \ ;$$

7) proprietà commutativa del prodotto:

$$P(x) \cdot Q(x) = Q(x) \cdot P(x) \ ;$$

8) proprietà distributiva del prodotto rispetto alla somma:

$$P(x) \cdot (Q(x) + R(x)) = P(x) \cdot Q(x) + P(x) \cdot R(x) \ .$$

Si può naturalmente definire il prodotto di un numero reale per un polinomio:

$$c \cdot \sum_{j=0}^{n} a_j x^j = \sum_{j=0}^{n} (c a_j) x^j \ .$$

A quali proprietà soddisfa tale operazione?

(Osservate che moltiplicare un polinomio per una costante è equivalente a moltiplicarlo per il polinomio di grado zero il cui unico termine è quello costante. Identificheremo pertanto le

costanti con i polinomi di grado 0).

Il grado è legato alle operazioni precedenti dalle seguenti proprietà:

$$gr(P(x) + Q(x)) \leq \max\{(gr(P(x)), gr(Q(x))\},$$
$$gr(P(x)\cdot Q(x)) = gr(P(x)) + gr(Q(x)).$$

(Perchè? Nel caso della somma potete dire qualcosa di più?).

Esercizio 3. Quali polinomi sono invertibili rispetto al prodotto?

Osservazione. Dall'ultima uguaglianza segue facilmente che il prodotto di due polinomi è nullo se e solo se almeno uno di essi è nullo. (Perchè?).

Abbiamo finora visto i polinomi come espressioni formali che si possono sommare e moltiplicare; essi sono però anche un modo di indicare funzioni (reali di variabile reale); è bene però mantenere distinti questi due aspetti e parlare nel secondo caso di funzioni polinomiali.
Ad esempio è chiaro che due polinomi, per come sono stati definiti, sono da intendersi uguali se e solo se hanno lo stesso grado e gli stessi coefficienti; non è però detto a priori che la stessa cosa valga per le funzioni polinomiali; si hanno però i fatti seguenti:

Esercizio 4. Dimostrare che due funzioni polinomiali di grado ≤ 3 coincidono se e solo se i rispettivi polinomi sono uguali (ovvero che se un polinomio di grado ≤ 3 è nullo come funzione polinomiale esso coincide con il polinomio nullo). Ad esempio, dato $P(x)=a_3x^3+a_2x^2+_1x+a_o$, da $P(0)=0$ si ha $a_o=0$, da $P(1)=0$ si ha..... .

Esercizio 5. Dimostrare la stessa cosa per due funzioni polinomiali di grado qualsiasi (ovvero che se $P(x)$ è un polinomio non nullo esiste $\xi \in \mathbb{R}$ tale che $P(\xi) \neq 0$). (traccia: si tratta di trovare un valore ξ abbastanza grande, per cui (se $a_n > 0$)

$$P(\xi) = a_n\xi^n + a_{n-1}\xi^{n-1} + \ldots + a_0 \geq a_n\xi^n - |a_{n-1}|\xi^{n-1} - \ldots - |a_0| \ldots$$

Avete visto per esercizio in precedenza che non tutti i polinomi sono invertibili (rispetto al prodotto); pertanto non sempre è definita la divisione fra polinomi. Questo fatto (unito naturalmente al volere delle proprietà 1),...,9)) richiama una analogia fra l'insieme degli interi e l'insieme dei polinomi: analogia ancora più profonda di quanto possa sembrare a prima vista. Infatti ad esempio vale anche per i polinomi una regola di divisione con resto.

Teorema. Dati due polinomi $P(x)$ e $D(x)$ (con $D(x) \neq 0$) esistono due polinomi $Q(x)$ e $R(x)$ tali che

$$P(x) = Q(x) \cdot D \cdot (x) + R(x) ,$$

ed inoltre

$$gr(R(x)) < gr(D(x)) .$$

I polinomi $Q(x)$ ed $R(x)$ che verificano queste condizioni sono unici, e si dicono rispettivamente quoziente e resto della divisione di $P(x)$ per $D(x)$.

Dimostrazione. Vediamo dapprima l'unicità: se $Q'(x)$ e $R'(x)$ fossero altri due polinomi con le stesse proprietà si avrebbe

$$Q(x)D(x) + R(x) = Q'(x)D^*(x) + R'(x) ,$$

cioè

$$(Q(x) - Q'(x))D(x) = R'(x) - R(x) .$$

Poichè il grado di $R'(x)-R(x)$ è minore di quello di $D(x)$, deve essere $Q(x)-Q'(x)=0$ e di conseguenza anche $R'(x)-R(x)=0$.

Vediamo ora l'esistenza di $Q(x)$ ed $R(x)$.

Sia $P(x) = \sum_{h=0}^{m} p_h x^h$, $D(x) = \sum_{k=0}^{n} d_k x^k$.

Se il grado m di $P(x)$ è minore del grado n di $D(x)$ si può porre $Q(x)=0$ ed $R(x)=P(x)$.

Supponiamo pertanto $m \geq n$ e poniamo

$$P^1(x) = \sum_{h=0}^{m_1} p_h^1 x^h = P(x) - \frac{p_m}{d_n} x^{m-n} \cdot D(x) .$$

$P^1(x)$ è un polinomio di grado $m_1 < m$; se $m_1 \geq n$ poniamo

$$P^2(x) = \sum_{h=0}^{m_2} p_h^2 x^h = P^1(x) - \frac{p^1_{m_1}}{d_n} x^{m_1-n} D(x) ,$$

e così via.

I gradi dei polinomi $P, P^1, P^2 \ldots$ decrescono $(m > m^1 > m^2 > \ldots)$; pertanto, dopo aver ripetuto per un numero finito di volte questo procedimento si ottiene un polinomio

$$P^k(x) = P^{k-1}(x) - \frac{p^{k-1}_{m_{k-1}}}{d_n} x^{m_{k-1}-n} D(x)$$

di grado minore di n .

Si ha pertanto

$$P(x) = \frac{p_m}{d_n} x^{m-n} D(x) + P^1(x) = \frac{p_m}{d_n} x^{m-n} D(x) +$$

$$+ \frac{p^1_{m_1}}{d_n} x^{m_1-n} D(x) + P^2(x) = \ldots =$$

$$= \frac{p_m}{d_n} x^{m-n} D(x) + \frac{p_{m_1}}{d_n} x^{m_1-n} D(x) + \ldots + \frac{p^{k-1}_{m_{k-1}}}{d_n} x^{m_{k-1}-n} D(x) + P^k(x) .$$

Basta pertanto assumere

$$Q(x)= \frac{1}{d_n} \left(P_m x^{m-n} + P^1_{m_1} x^{m_1-n} + \ldots + P^{k-1}_{m_{k-1}} x^{m_{k-1}-n}\right)$$

e

$$R(x) = P^{k}(x)$$

Q.E.D.

Vediamo ora un modo pratico di dividere i polinomi; supponiamo ad esempio di dover dividere

$$x^5+(\sqrt{2}+1)x^4-(2-\sqrt{2})x^3-(2\sqrt{2}+\tfrac{1}{2})x^2-\tfrac{3}{2}x+1$$

per

$$x^2+x-2 \ .$$

Scriviamo la seguente tabella:

$$x^5+(\sqrt{2}+1)x^4-(2-\sqrt{2})x^3-(2\sqrt{2}+\tfrac{1}{2})x^2-\tfrac{3}{2}x+1 \quad \Big| \quad x^2+x-2$$

x^5 diviso per x^2 dà x^3; scriviamo pertanto x^3 nella parte riservata al "quoto", come nella divisione ordinaria; scriviamo nella riga sotto al dividendo, mantenendo l'ordine, il prodotto di x^3 per il divisore; tiriamo una riga, e sottraiamo, ottenendo a questo punto

$$\begin{array}{l|l} x^5+(\sqrt{2}+1)x^4-(2-\sqrt{2})x^3-(2\sqrt{2}+\tfrac{1}{2})x^2-\tfrac{3}{2}x+1 & x^2+x-2 \\ \hline x^5+x^4-2x^3 & x^3 \\ \hline \sqrt{2}x^4+\sqrt{2}x^3-(2\sqrt{2}+\tfrac{1}{2})x^2-\tfrac{3}{2}x+1 & \end{array}$$

Ripetendo l'operazione precedente, poichè $\sqrt{2}x^4$ diviso per x^2 da $\sqrt{2}x^2$, si scrive $+\sqrt{2}x^2$ di fianco a x^3(quota) e si moltiplica $\sqrt{2}x^2$ per x^2+x-2, lo si scrive nella riga inferiore e si sottrae, ottenendo

$$
\begin{array}{l|l}
x^5+(\sqrt{2}+1)x^4-(2-\sqrt{2})x^3-(2\sqrt{2}+\frac{1}{2})x^2-\frac{3}{2}x+1 & x^2+x-2 \\
\hline
x^5+x^4-2x^3 & x^3+\sqrt{2}x^2 \\
\hline
\sqrt{2}x^4+\sqrt{2}x^3-(2\sqrt{2}+\frac{1}{2})x^2-\frac{3}{2}x+1 & \\
+\sqrt{2}x^4+\sqrt{2}x^3-2\sqrt{2}x^2 & \\
\hline
-\frac{1}{2}x^2-\frac{3}{2}x+1 &
\end{array}
$$

Così procedendo, si scrive ancora:

$$
\begin{array}{l|l}
x^5+(\sqrt{2}+1)x^4-(2-\sqrt{2})x^3-(2\sqrt{2}+\frac{1}{2})x^2-\frac{3}{2}x+1 & x^2+x-2 \\
\hline
x^5+x^4-2x^3 & x^3+\sqrt{2}x^2-\frac{1}{2} \\
\hline
\sqrt{2}x^4+\sqrt{2}x^3-(2\sqrt{2}+\frac{1}{2})x^2 & \\
\sqrt{2}x^4+\sqrt{2}x^3-2\sqrt{2}x^2 & \\
\hline
-\frac{1}{2}x^2-\frac{3}{2}x+1 & \\
-\frac{1}{2}x^2-\frac{1}{2}x+1 & \\
\hline
-x & 0
\end{array}
$$

Osserviamo ora che $-x$ ha grado inferiore a x^2+x-2. Abbiamo così finito, cioè: il quoziente della divisione è

$$x^3+\sqrt{2}x^2-\frac{1}{2}\ ,$$

ed il resto è $-x$.

Esercizio 6. Effettuate le seguenti divisioni:

x^2+2x+1	diviso	$x+1$
$x^2+2x-\sqrt{2}$	"	$x+1$
$x^7+x^5+85x^3+\sqrt{3}x^2+e$	"	$2x^3+x$
$x^5+\sqrt{3}x^4-\sqrt{5}x$	"	$x^6+6x^4+8311x^2$
x^7+a^7	"	$x+a$
x^7-a^7	"	$x-a$
x^7	"	$x-a$
x^5+a^5	"	$x+a$
x^6-a^6	"	x^2-a^2
x^5-a^5	"	$x^4+ax^3+a^2x^2+a^3x+a^4$

Definizione. Come per i numeri interi, diremo che il polinomio $P(x)$ è divisibile per il polinomio $D(x)$ se il resto della divisione di $P(x)$ per $D(x)$ è zero, ovverossia se esiste un polinomio $Q(x)$ tale che

$$P(x) = Q(x)\cdot D(x) \quad .$$

Osservazione. Se $P(x)$ e $D(x)$ sono a coefficienti razionali anche $Q(x)$ è tale. Perchè?

Esercizio 7. Provare le osservazioni seguenti:

a) Se $P(x)$ è divisibile per $Q(x)$ e $Q(x)$ è divisibile per $R(x)$, allora $P(x)$ è divisibile per $R(x)$.

b) Se $P(x)$ e $Q(x)$ sono divisibili per $R(x)$, anche che $P(x)+Q(x)$ è divisibile per $R(x)$.

c) Se $P(x)$ è divisibile per $Q(x)$, anche $P(x)\cdot R(x)$ è divisibile per $Q(x)$, quale che sia $R(x)$.

d) Se $P^1(x)$, $P^2(x),\ldots,P^k(x)$ sono divisibili per $Q(x)$, allora anche $P^1(x)R^1(x)+\ldots+P^k(x)R^k(x)$

è divisibile per $Q(x)$, quali che siano $R^1(x), R^2(x),\ldots,R^k(x)$.

e) Ogni polinomio è divisibile per un polinomio di grado nullo.

f) Se $P(x)$ è divisibile per $Q(x)$, allora $P(x)$ è anche divisibile per $cQ(x)$, con c costante moltiplicativa non nulla.

g) Ogni divisore di $P(x)$ dello stesso grado di $P(x)$ differisce da $P(x)$ per una costante moltiplicativa non nulla (è cioè della forma $cP(x)$, con $c\neq 0$).

h) Affinchè $P(x)$ e $Q(x)$ siano divisibili l'uno per l'altro occorre e basta che differiscano per una costante moltiplicativa non nulla.

i) Ogni divisore di $P(x)$ è anche un divisore di $cP(x)$, con c costante non nulla (e viceversa).

2. MASSIMO COMUN DIVISORE DI DUE POLINOMI.

Definizione. Sempre come per gli interi, dati due polinomi si dice loro divisore comune un polinomio che li divide entrambi; massimo comun divisore (abbreviando, M.C.D.) di due polinomi è un divisore comune divisibile per ogni altro divisore comune .

Ad es., $x+a$ è un divisore comune di x^3+a^3 e x^4-a^4.

Per quanto risulta dagli esercizi precedenti il M.C.D., se esiste, è unico a meno di una costante moltiplicativa non nulla. Vediamo ora l'esistenza del M.C.D. di due polinomi, per mezzo

dell'algoritmo delle divisioni successive, o algoritmo di Euclide.

Supponiamo dunque di avere due polinomi $P(x)$ e $D(x)$ di cui cerchiamo il M.C.D.; per la regola della divisione esistono due polinomi $Q^1(x)$ ed $R^1(x)$ tali che

$$P(x) = Q^1(x)\cdot D(x) + R^1(x) \ .$$

Se $R^1(x)\neq 0$, di nuovo esisteranno $Q^2(x)$, $R^2(x)$, $Q^3(x)$, $R^3(x)$,..., tali che

$$D(x) = Q^2(x)\cdot R^1(x) + R^2(x) \ ,$$
$$R^1(x) = Q^3(x)\cdot R^2(x) + R^3(x) \ ,$$
$$\ldots \qquad .$$

Osserviamo che, continuando di questo passo, il grado di $R^1(x)$, $R^2(x)$, $R^3(x)$,... decresce strettamente ($gr(R^1(x)) > gr(R^2(x)) > gr(R^3(x)) > \ldots$): esiste pertanto in definitiva un intero k tale che

$$P(x) = Q^1(x)\cdot D(x) + R^1(x) \ ,$$
$$D(x) = Q^2(x)\cdot R^1(x) + R^2(x) \ ,$$
$$R^1(x) = Q^3(x)\cdot R^2(x) + R^3(x) \ ,$$
$$\ldots\ldots$$
$$R^{k-3}(x) = Q^{k-1}(x)\cdot R^{k-2}(x) + R^{k-1}(x) \ ,$$
$$R^{k-2}(x) = Q^{k}(x)\cdot R^{k-1}(x) + R^{k}(x) \ ,$$
$$R^{k-1}(x) = Q^{k+1}(x)\cdot R^{k}(x) \ .$$

Dall'ultima uguaglianza si ricava che $R^k(x)$ divide $R^{k-1}(x)$ e pertanto da quella precedente si ricava che $R^k(x)$ divide $R^{k-2}(x)$. Così procedendo, si ottiene che $R^k(x)$ divide $R^{k-3}(x)$,... ed infine anche $D(x)$ e $P(x)$.
D'altra parte, è chiaro che ogni divisore di $P(x)$ e $D(x)$ è anche un divisore di $R^1(x)$, e quindi anche un divisore di $R^2(x)$ ed infine anche un divisore di $R^k(x)$.

Dunque $R^k(x)$ è un divisore comune di $P(x)$ e $D(x)$ che è divisibile per ogni altro divisore comune; è pertanto "il" M.C.D. di $P(x)$ e $D(x)$.

Troviamo ad es. il M.C.D. fra x^4-a^4 e x^3+a^3.

Dividendo x^4-a^4 per x^3+a^3 si ha quoto x e resto $-a^3x-a^4$.

Dividendo x^3+a^3 per $x+a$ (la costante moltiplicativa $-a^3$ "non conta") si ha quoto x^2-ax+a^2 e resto zero.

Pertanto $x+a$ è il M.C.D. cercato.

Esercizio 8. Trovare M.C.D. fra le seguenti coppie di polinomi

a) $x^4+\sqrt{2}x^3+(a^2+1)x^2+\sqrt{2}a^2x+1$
$x^7+3x^5+2\sqrt{2}x^4+2x^3-\sqrt{3}x^2-\sqrt{6}x-\sqrt{3}$

b) x^6-a^6
$x^4+2ax^3+2a^2x^2+a^3x$

c) $x^7+x^6+x^5+x^4+x^3+x^2+x+1$
$x^6+x^4+x^2+1$.

Osservazione. Se $P(x)$ e $D(x)$ sono a coefficienti razionali, cosa si può dire del loro M.C.D. E se sono a coefficienti interi?

Come definireste il minimo comune multiplo (abbreviato, m.c.m.) di due polinomi?

Che relazione intercorre tra m.c.m. e M.C.D?

Proposizione. Sia $M(x)$ il M.C.D. di $P(x)$ e $D(x)$. Esistono allora due polinomi $U(x)$ e $V(x)$ tali che

$$U(x)\,P(x) + V(x)\,D(x) = M(x) .$$

Inoltre, se i gradi di $P(x)$ e $D(x)$ sono positivi, si possono scegliere $U(x)$ e $V(x)$ di grado rispettivamente inferiore a quelli di $D(x)$ e $P(x)$.

Dimostrazione. Dalla penultima uguaglianza della costruzione precedente (ricordando che $M(x)=R^k(x)$) si ricava

$$M(x) = U^1(x)R^{k-2}(x) + V^1(x)\,R^{k-1}(x)\ ,$$

ove $U^1(x)=1$ e $V^1(x) = -Q^k(x)$.

Di nuovo dalla terzultima uguaglianza, si ricava

$$M(x) = U^2(x)R^{k-3}(x) + V^2(x)R^{k-2}(x)\ ,$$

ove $U^2(x)=V^1(x)$ e $V^2(x) = -Q^{k-1}(x)\,V^1(x) + U^1(x)$.

Così procedendo si ottiene la prima parte della tesi.

Per dimostrare la seconda parte supponiamo di conoscere già due polinomi $U(x)$ e $V(x)$ verificanti l'uguaglianza ma non la condizione successiva. Allora, dividendo $U(x)$ per $D(x)$ si ottiene?

$$U(x) = Q(x)D(x)+R(x)$$

e quindi

$$R(x)P(x) + (Q(x)P(x) + V(x))D(x) = M(x)\ .$$

$R(x)$ ha grado inferiore a quello di $D(x)$ per costruzione; se poi $Q(x)P(x)+V(x)$ avesse grado superiore o uguale a quello di $P(x)$, allora $M(x)$ avrebbe grado superiore o uguale a quello del prodotto $P(x)D(x)$, il che è assurdo, essendo $M(x)$ il M.C.D. Q.E.D.

Corollario. Due polinomi $P(x)$ e $Q(x)$ sono primi fra loro (cioè non hanno divisori comuni oltre le costanti non nulle) se e solo se esistono due polinomi $U(x)$ e $V(x)$ tali che

$$U(x)P(x) + V(x)Q(x) = 1\ .$$

Cerchiamo $U(x)$ e $V(x)$ come nel corollario, essendo $P(x)=x^2-a^2$, $Q(x)=x^2+2x+1$ ($|a|\neq 1$).

Basta cercare A,B,C,D tali che

$$(x^2- a^2)(Ax+B)+(x^2+ 2x+1)(Cx+D) = 1\ ,$$

cioè

$$(A+C)x^3+ (B+2C+D)x^2+ (-a^2A+2D+C)x + (-a^2B+D)=1 ,$$

cioè

$$\begin{cases} A+C=0 \\ B+2C+D=0 \\ -a^2A+2D+C=0 \\ -a^2B+D=0 \end{cases}$$

da cui..... .

Esercizio 9. Come prima, per $P(x)=x$, $Q(x)=x^3\sqrt{2}+ 6x+1$.

Corollario. Siano $P(x)$ e $Q(x)$ due polinomi primi tra loro. Supponiamo inoltre che $Q(x)$ divida $P(x)\cdot R(x)$. Allora $Q(x)$ divide $R(x)$.

Dimostrazione. Esistono $U(x)$ e $V(x)$ tali che

$$U(x)P(x) + V(x)Q(x) = 1$$

Moltiplicando entrambi i membri per $R(x)$ si ottiene

$$(P(x)R(x))\cdot U(x)+V(x)Q(x)R(x) = R(x)$$

Poichè $Q(x)$ divide entrambi i termini del primo membro, divide anche $R(x)$. Q.E.D.

3. SCOMPOSIZIONE DEI POLINOMI IN FATTORI IRRIDUCIBILI.

Definizione. Sia $P(x)$ un polinomio (a coefficienti reali) di grado ≥ 1. $P(x)$ si dice riducibile (in campo reale) se ammette divisori non banali (diversi cioè dalle costanti e da $c \cdot P(x)$, con $c \neq 0$). Se invece gli unici divisori di $P(x)$ sono banali, $P(x)$ si dice irriducibile (in campo reale).

Osservazione. Ogni polinomio di primo grado è irriducibile.

Esercizio 10. Esistono polinomi di secondo grado irriducibili in campo reale. Ad esempio? Sapreste determinarli?

Esercizio 11. Se il prodotto di due polinomi è divisibile per il polinomio irriducibile $P(x)$, almeno uno di essi lo è.

Se un polinomio $P(x)$ ha due scomposizioni in fattori irriducibili, se cioè si può scrivere

$$P(x) = P_1^1(x) \cdot P_o^2(x) \cdot \ldots \cdot P^h(x) = Q_1^1(x) \cdot Q^2(x) \cdot \ldots \cdot Q^k(x) \ ,$$

ove $P_j(x)$ e $Q_j(x)$ sono irriducibili, allora $h=k$ e, dopo un opportuno riordinamento degli indici, si ha

$$Q^j(x) = c_j P^j(x) \qquad j=1,2,\ldots,h \ ,$$

con c_j costante non nulla.

Per la dimostrazione si procede per induzione su h. Per $h=1$ la dimostrazione è ovvia. Supponiamo vera la tesi per $h-1$ e dimostriamola per h.

$P^1(x)$ divide $\prod_{j=1}^{k} Q^j(x)$; per l'esercizio precedente, $P^1(x) = c_j Q^j(x)$ per un opportuno indice j.

Si ottiene quindi

$$\prod_{l=2}^{h} P^l(x) = \frac{1}{c_j} \prod_{l \neq j} Q^l(x) .$$

Per l'ipotesi induttiva si ottiene la tesi.

Abbiamo così visto che la scomposizione di un polinomio di grado ≥ 1 in fattori irriducibili è essenzialmente unica (cioè, unica a meno di costanti moltiplicative non nulle). Vediamo ora che essa esiste.

Consideriamo le scomposizioni di $P(x)$ in fattori di grado ≥ 1 (non necessariamente irriducibili):

$$P(x) = P^1(x) \cdot P^2(x) \cdot \ldots \cdot P^h(x)$$

(chiameremo h la lunghezza di tale scomposizione).

Queste scomposizioni esistono (ad esempio $P(x)$ stesso; d'altra parte h è certamente sempre inferiore al grado di $P(x)$.

Non è difficile ora concludere che ogni scomposizione di lunghezza massima è composta di fattori irriducibili.

Abbiamo pertanto dimostrato il seguente teorema:

Teorema. Ogni polinomio $P(x)$ di grado ≥ 1 può essere scomposto in un prodotto di fattori irriducibili; inoltre, tale scomposizione è essenzialmente unica (nel senso visto in precedenza).

I teoremi e le proprietà dei polinomi dimostrati sino ad ora dipendono essenzialmente dall'aspetto algebrico dei polinomi; un legame tra l'aspetto algebrico e quello funzionale è dato dalla regola di Ruffini.

Teorema (Regola di Ruffini). Condizione necessaria e sufficiente affinchè un polinomio $P(x)$ sia divisibile per $(x-c)$ è che esso si annulli per $x=c$.

Dimostrazione. La necessità è ovvia.

Vediamo la sufficienza. Effettuiamo la divisione di $P(x)$ per $x-c$:

$$P(x) = Q(x)\,(x-c) + r$$

(con r costante eventualmente nulla).

Poichè $P(c)=0$, si ha $r=0$. Q.E.D.

Osservazione. Dato il polinomio $P(x)$, $P(c)$ è il resto della divisione di $P(x)$ per $(x-c)$.

Esercizio 12. Dimostrare (utilizzando questa volta la regola di Ruffini) che due funzioni polinomiali coincidono se e solo se i rispettivi polinomi sono uguali. Se infatti $P(x)$, polinomio non nullo, fosse divisibile per $x-a$ per ogni a reale, quanto sarebbe il suo grado?

4. NUMERI COMPLESSI.

Dato un polinomio $P(x)$ a coefficienti reali, di grado ≥ 1, il problema:

1) Esiste un numero reale α tale che $P(\alpha)=0$? (ovvero $P(x)$ ammette radici reali?)

è equivalente, in base al teorema di Ruffini, al problema:

2) Esiste un polinomio di primo grado 1 a coefficienti reali per cui $P(x)$ sia divisibile?

Supponiamo che per ogni polinomio $P(x)$ la risposta sia positiva. Questo vorrebbe dire che possiamo scrivere

$$P(x) = (x-\alpha)\,Q(x)\ ,$$

con $gr(Q(x)) = gr(P(x))-1$.

Se $gr(Q(x)) \geq 1$, allora anche $Q(x)$ avrebbe, per la nostra assunzione, una radice reale β, e quindi

$$Q(x) = (x-\beta)\, R(x) \ , \quad \text{etc.}$$

In definitiva si avrebbe la scomposizione di $P(x)$ come

$$P(x) = c(x-\alpha)(x-\beta)....$$

cioè come prodotto di un numero finito $(=gr(P(x)))$ di polinomi di primo grado.

Questo però non si verifica: esistono polinomi di coefficienti reali che non ammettono radici reali, come per esempio i polinomi di secondo grado con discriminante negativo, oppure i polinomi del tipo $x^{2n}+a$, con $a > 0$.

Osservazione. Ricordiamo la formula risolutiva dell'equazione di secondo grado $ax^2+bx+c=0$:

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

Tale formula è applicabile quando $\Delta = b^2-4ac \geq 0$, perchè solo allora si può estrarre la radice quadrata. Ma il caso $\Delta < 0$ è proprio quello in cui l'equazione non ammette radici; pertanto l'algoritmo risolutivo dato da questa formula non presenta inconvenienti.

Consideriamo ora un polinomio di terzo grado, che per semplicità supponiamo monico (cioè, il cui coefficiente del termine di grado massimo è 1):

$$P(x) = x^3+ax^2+bx+c \ .$$

Sia $K = \max\{|a|, |b|, |c|, 1\}$; allora

$$P(2K) = 8K^3+4aK^2+2bK+c \geq$$

$$\geq 8K^3-4K^3-2K^2-K \geq K^3 > 0 \ ,$$

mentre

$$P(-2K) = -8K^3 + 4aK^2 - 2bK + c \leq$$
$$\leq -8K^3 + 4K^3 + 2K^2 + K \leq -K^3 < 0 .$$

La funzione polinomiale $P(x)$ assume pertanto valori sia positivi che negativi. Per motivi di continuità, che qui non possiamo dimostrare, $P(x)$ deve necessariamente annullarsi per qualche valore compreso tra $-2k$ e $2k$ (un discorso del tutto analogo vale per un qualunque polinomio di grado dispari). Si ha quindi:

$$P(x) = (x-\alpha)Q(x) \quad , \quad \text{con} \quad gr(Q(x))=2 .$$

Si presentano pertanto le seguenti possibilità:

1) $P(x)$ ammette tre radici reali semplici;
2) $P(x)$ ammette due radici reali, di cui una di molteplicità 2;
3) $P(x)$ ammette una radice reale di molteplicità 3;
4) $P(x)$ ammette una sola radice reale semplice.

Il matematico Cardano trovò una formula risolutiva per l'equazione di terzo grado:
Cerchiamo le radici dell'equazione

$$x^3 + ax^2 + bx + c = 0 .$$

Con una traslazione $(x'=x+d)$ ci si riconduce ad una equazione del tipo

$$x^3 + px + q = 0$$

La soluzione x si può scrivere come somma

$$x = u+v$$

per cui:

$$u^3 + v^3 + (3uv + p)(u+v) + q=0 .$$

Scegliamo u e v in modo che:

$$uv = -\frac{p}{3} \quad \text{cioè} \quad 3uv + p = 0$$

Si ha allora

$$\begin{cases} u^3 \cdot v^3 = -\frac{p^3}{27} \\ u^3 + v^3 = -q \end{cases}$$

u^3 e v^3 sono allora le soluzioni dell'equazione

$$y^2 + qy - \frac{p^3}{27} = 0 \ ,$$

da cui formalmente

$$y = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \ ,$$

e quindi

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Applicando tale formula nel caso in cui $\frac{q^2}{4} + \frac{p^3}{27} < 0$ ci si trova di fronte a radici quadrate di numeri negativi e quindi essa perde significato. Se però, come vedremo, si estende il campo dei numeri reali in modo da attribuire un "opportuno" senso alla radice quadrata dei numeri negativi, la formula di Cardano dà tutte le radici dell'equazione.
Questa è solo la più antica delle ragioni che giustificano l'introduzione dei numeri complessi.

Consideriamo l'insieme $\mathbb{C}$ delle espressioni del tipo $a+ib$ (che diremo numeri complessi), al variare di a e b in $\mathbb{R}$, munito delle seguenti operazioni:

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

Le operazioni si compiono cioè considerando $a+ib$ come un polinomio in i, e sostituendo ad i^2, ogni volta che compare, -1.

E' immediato verificare le seguenti proprietà:

a) associatività e commutatività della somma,

b) associatività e commutatività del prodotto,

c) distribuitività della somma rispetto al prodotto,

d) $(0+i0) + (a+ib) = a+ib$,

e) $(1+i0)\cdot(a+ib) = a+ib$,

f) $(a+ib)+(-a+i(-b)) = 0+i0$,

g) $(a+ib)\cdot\left(\frac{a}{a^2+b^2} + i\left(\frac{-b}{a^2+b^2}\right)\right)=1+i0$ se $a+ib\neq 0+i0$.

Analogamente a quanto fatto con i polinomi, per semplicità di notazioni e convenienza di calcolo, scriveremo

$$a=a+i0 \quad , \quad ib=0+ib \quad , \quad 0=0+i0 \quad , \quad i(-b)=-ib \ .$$

Se $z=a+ib \in \mathbb{C}$, possiamo rileggere

d) $0+z = z$,

e) $1\cdot z = z$.

Per f) ha senso porre $-z=-a-ib$, e per g)

$$z^{-1} = \frac{1}{z} = \frac{a}{a^2+b^2} - i\,\frac{b}{a^2+b^2} \quad \text{se } z\neq 0 \ .$$

Le proprietà precedenti dicono che con i numeri complessi si possono compiere le quattro operazioni con le stesse regole formali che valgono per i numeri reali (o per i numeri razionali).

<u>Esercizio</u> 13. Calcolare $\frac{i^5-3i^2+4}{2i^3+1}$, $\frac{1-i}{1+i} + \frac{1+3i}{1-1}$, $\frac{3i^{30}-i^{19}}{2i-1}$

Se $z=a+ib$, a si dice la parte reale di z e si indica con $Re(z)$, mentre b si dice la parte immaginaria di z e si indica con $Im(z)$.

Possiamo identificare i numeri reali con quei numeri complessi la cui parte immaginaria è 0: infatti è di facile verifica che

i risultati delle operazioni tra di essi sono gli stessi sia considerandoli come numeri reali che come numeri complessi. I numeri complessi del tipo ib si diranno immaginari puri.

Osservazione. Si ha $(ib)^2=-b^2$, cioè i numeri reali negativi ammettono radici quadrate in campo complesso.

Se $z=a+ib$, il numero $a-ib$ si indica con $\bar{z}$ e si chiama il coniugato di z. le seguenti proprietà sono di verifica immediata:

1) $\overline{z_1+z_2}= \bar{z}_1+ \bar{z}_2$,

2) $\overline{z_1 \cdot z_2}= \bar{z}_1 \cdot \bar{z}_2$,

3) $\overline{(\bar{z})} = z$,

4) $\mathrm{Re}(z) = \frac{z+\bar{z}}{2}$,

5) $\mathrm{Im}(z) = \frac{z-\bar{z}}{2i}$,

6) $z \cdot \bar{z} = (\mathrm{Re}(z))^2 + (\mathrm{Im}(z))^2$.

Osservazione. Se z è reale, $\bar{z}=z$; se z è immaginario puro, $\bar{z}=-z$.

Da (6), si vede che il prodotto $z \cdot \bar{z}$ è un numero reale ≥ 0; inoltre

$$z \cdot \bar{z} = 0 \Leftrightarrow z=0 \quad .$$

Si indica con $|z|$, e si dice modulo di z, la radice quadrata aritmetica di $z \cdot \bar{z}$. Si hanno allora le seguenti proprietà:

1) $|z| \geq 0$, $|z| = 0 \Leftrightarrow z=0$,

2) $|z \cdot w| = |z| \cdot |w|$ (*) (e quindi $|z^n| = |z|^n$) ,

3) $|z|^2 = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2$

Se quindi $z \neq 0$, $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$, relazione che spiega come si ottiene la g).

Abbiamo dato una introduzione dei numeri complessi utile ai fini algoritmici, tale cioè da dare delle regole di calcolo abbastanza semplici, mentre ci siamo curati poco di definire bene in termini insiemistici cosa sia $\mathbb{C}$.
Questo, che risponde a necessità di rigore matematico, può essere fatto in diversi modi, naturalmente equivalenti fra loro, che si rilevano utili affrontando i vari problemi che si pongono.

A-I numeri complessi come resti della divisione dei polinomi per x^2+1.

Consideriamo l'insieme dei resti delle divisioni dei polinomi a coefficienti reali per x^2+1.
E' evidente che si tratta dell'insieme di tutti i polinomi a coefficienti reali di grado ≤ 1.
Osserviamo il seguente fatto: siano $P_1(x)$ e $P_2(x)$ due polinomi, e siano $R_1(x)$ e $R_2(x)$ i rispettivi resti della divisione per x^2+1. Allora il resto della divisione di $P_1(x)+P_2(x)$ per x^2+1 sarà $R_1(x)+R_2(x)$, cioè la somma di due polinomi qualunque aventi come vesti $R_1(x)$ e $R_2(x)$ è

(*) si deduce facilmente che:
$z \cdot w = 0 \Leftrightarrow z=0$ oppure $w=0$ (o entrambe).

un polinomio il cui resto è $R_1(x)+R_2(x)$.

Vediamo ora cosa succede per il prodotto $P_1(x)\cdot P_2(x)$.

Scriviamo

$$P_1(x)=Q_1(x)(x^2+1)+R_1(x) \quad , \quad P_2(x)=Q_2(x)(x^2+1)+R_2(x) \quad ,$$

quindi

$$P_1(x)P_2(x)=(Q_1(x)Q_2(x)(x^2+1)+Q_1(x)R_2(x)+R_1(x)Q_2(x))(x^2+1)+R_1(x)R_2(x).$$

Non è detto che $R_1(x)R_2(x)$ sia il resto della divisione di $P_1(x)P_2(x)$ per (x^2+1), perchè può essere $gr(R_1(x)\cdot R_2(x))=2$.

Poniamo $R_1(x) = a+bx$, $R_2(x)=c+dx$.

Allora

$$R_1(x)R_2(x) = bdx^2+ (ad+bc)x + ac \quad ,$$

e, dividendo per $x^2+ 1$:

$$R_1(x)R_2(x) = bd(x^2+1) + (ac-bd)+(ad+bc)x \ .$$

Ne segue che il resto della divisione di $P_1(x)P_2(x)$ per x^2+1 è

$$R(x)=(ac-bd)+(bc+ad)x \ .$$

Come si vede, l'espressione di $R(x)$ dipende da $R_1(x)$ e $R_2(x)$, per cui, comunque siano scelti due polinomi di resto $R_1(x)$ e $R_2(x)$ rispettivamente, il loro prodotto dà resto $R(x)$.

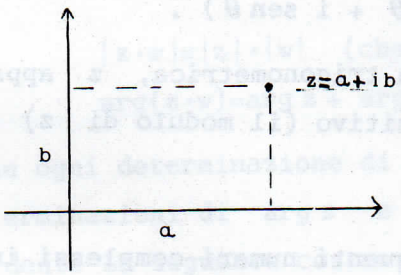
Abbiamo così introdotto una somma e un prodotto fra "resti"; se si chiama il resto $a+bx$ "numero complesso $a+ib$", si vede che le operazioni coincidono con quelle descritte in precedenza.

B-Il piano di Gauss.

In modo naturale, si può identificare $\mathbb{C}$ con il prodotto cartesiano $\mathbb{R}\times\mathbb{R}$, chiamando "numero complesso $a+ib$" la coppia di numeri reali (a,b), definendo formalmente in maniera opportuna le operazioni tra coppie di numeri reali, cioè

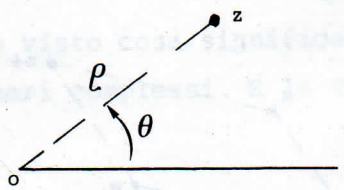
$$(a,b)+(c,d) = (a+c,b+d) \quad ;$$
$$(a,b)\cdot(c,d) = (ac-bd,ad+bc) \quad .$$

Questa rappresentazione di $\mathbb{C}$ ci permette una visualizzazione geometrica di $\mathbb{C}$ come "piano complesso", fissando nel piano un sistema di assi cartesiani ortogonali.



Su questo piano possiamo introdurre delle coordinate polari, fissando come semiasse polare il semiasse delle x positive, e considerando come coordinate di un punto del piano la sua distanza dall'origine e l'angolo che il raggio vettore dal punto all'origine forma con il semiasse polare (considerando come "verso" positivo quello antiorario).

Un numero complesso z viene allora identificato da due coordinate (ρ, θ), dove, se $\rho \neq 0$, θ è definito a meno di multipli di 2π, mentre, se $\rho = 0$, θ è arbitrario (ρ è sempre ≥ 0):



Per esempio, le coordinate polari di 1 sono $(1,0)$, quelle di i sono $(1,\pi/2)$, e quelle di -1 $(1,\pi)$.

Conoscendo le coordinate polari (ρ,θ) di z è facile ottenere

$$\mathrm{Re}\, z = \rho \cos\theta \quad , \quad \mathrm{Im}\, z = \rho \,\mathrm{sen}\,\theta \quad .$$

Viceversa, se $z=a+ib$,

a) $$\rho = \sqrt{a^2+b^2} = |z| \quad ,$$

b) $$\cos\theta = \frac{a}{|z|} \quad , \quad \mathrm{sen}\,\theta = \frac{b}{|z|} \quad .$$

Quindi ρ non è altro che il modulo di z ; le b) valgono naturalmente solo per $z \neq 0$, e definiscono θ a meno di multipli di 2π.

θ si chiama argomento di z , e si indica con argz (meglio, ogni valore di θ che soddisfi le b) si chiama una determinazione di arg z).

In definitiva, se $z \neq 0$ si può scrivere

$$z = \rho (\cos\theta + i \operatorname{sen}\theta) .$$

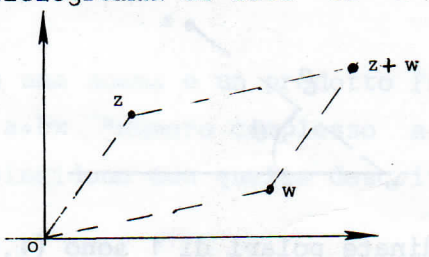
In questa forma, detta forma trigonometrica, z appare come prodotto di un numero reale positivo (il modulo di z) per un numero complesso di modulo 1.

Esercizio 14. Scrivere i seguenti numeri complessi in forma trigonometrica:

$$5 , \ -1 - \sqrt{3}i , \ -6 , \ -3 + \sqrt{3}i , \ 1/i , \ 4-4i , \ -3i ,$$
$$\sqrt{2} + \sqrt{2}i , \ {}^{-1}/_{1+i} .$$

Chiarita la rappresentazione nel piano dell'insieme $\mathbb{C}$, per renderla utile bisogna descrivere in questi termini le operazioni tra numeri complessi.

1-Somma. Vale la regola del parallelogramma": $z+w$ è il quarto vertice del parallelogramma di lati Oz e Ow:



2-Prodotto. Per descrivere il prodotto di due numeri complessi torna utile l'uso delle coordinate polari.

Siano $z = \rho(\cos\theta + i \operatorname{sen}\theta)$, $w = r(\cos t + i \operatorname{sen} t)$ due numeri complessi $\neq 0$. Allora

$z \cdot w = \rho r(\cos\theta + i \operatorname{sen}\theta)(\cos t + i \operatorname{sen} t) = \rho r(\cos\theta \cos t -$
$- \operatorname{sen}\theta \operatorname{sen} t + i(\cos\theta \operatorname{sen} t + \operatorname{sen}\theta \cos t)) =$
$= \rho r(\cos(\theta + t) + i \operatorname{sen}(\theta + t))$.

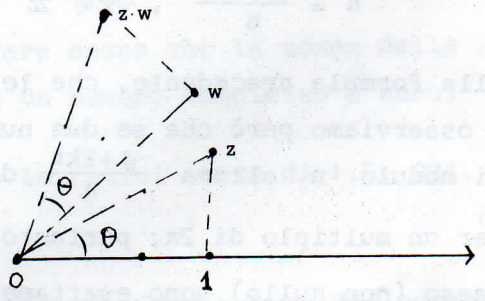
Abbiamo cioè ottenuto direttamente la forma trigonometrica di $z \cdot w$.

Si ha

$$|z \cdot w| = |z| \cdot |w| \quad \text{(che già sapevamo)}$$
$$\arg(z \cdot w) = \arg z + \arg w$$

(nel senso che ogni determinazione di $\arg(z \cdot w)$ si ottiene sommando due determinazioni di $\arg z$ e $\arg w$, e viceversa).

E' quindi evidente la seguente costruzione geometrica di $z \cdot w$:



Cioè, $z \cdot w$ è il terzo vertice del triangolo simile a $01z$ di lato $0w$ (corrispondente a 01).

Esercizio 15. Abbiamo visto cosa significa la moltiplicazione fra numeri complessi. E la divisione? E l'inversione?

Radici n-me di un numero complesso.

Supponiamo di dover cercare le radici n-me di un numero complesso $z = \rho(\cos\vartheta + i \operatorname{sen}\vartheta)$, di cercare cioè quei numeri w che risolvono l'equazione:

$$w^n = z \ .$$

Supponiamo che $w = r(\cos\alpha + i \operatorname{sen}\alpha)$ sia una soluzione.

Poichè

$$w^n = \left[r(\cos\alpha + i \operatorname{sen}\alpha)\right]^n = r^n(\cos n\alpha + i \operatorname{sen} n\alpha)$$

(questa è la formula di Moivre: risulta facilmente dalla regola del prodotto; dimostratela ad es. per induzione), affinchè w sia radice n-ma di z occorre e basta che $r^n = \varrho$, e che gli argomenti di w^n e z coincidano (naturalmente a meno di multipli di 2π), cioè che valga

$$n\alpha = \vartheta + 2k\pi \quad \text{per} \quad k \in \mathbb{Z} .$$

In definitiva $w = r(\cos\alpha + i \operatorname{sen}\alpha)$ è radice n-ma di $z = \varrho(\cos\vartheta + i \operatorname{sen}\vartheta)$ se e solo se

$$r = \sqrt[n]{\varrho} ,$$

$$\alpha = \frac{\vartheta + 2k\pi}{n} , \quad k \in \mathbb{Z} .$$

Sembrerebbe, dalla formula precedente, che le radici n-me di z siano infinite; osserviamo però che se due numeri interi k e k' sono congrui modulo n allora $\frac{\vartheta+2k\pi}{n}$ differisce da $\frac{\vartheta+2k'\pi}{n}$ solo per un multiplo di 2π; pertanto le radici n-me di un numero complesso (non nullo) sono esattamente n.
Ad esempio, sono determinate dalla formula per i valori $0,1,\ldots,n-1$ di k (verificatelo).
Come caso particolare osserviamo che le n radici n-me dell'unità (i numeri complessi w cioè tali che $w^n=1$) sono i numeri complessi di modulo unitario e di argomento $\frac{2k\pi}{n}$, con $k=0,1,2,\ldots,n-1$.
Graficamente essi sono determinati nel piano cartesiano come i vertici del poligono regolare di n lati inserito nel cerchio unitario di centro l'origine, e di cui un vertice coincide con il punto $(1,0)$.

Esercizio 16. Vedere che se w è un numero complesso tale che $w^n=z$, tutte e sole le radici n-me di z si ottengono moltiplicando w per le radici n-me dell'unità.

Esercizio 17. Non solo nel caso dell'unità, ma anche per un numero complesso qualsiasi le n radici n-me sono vertici di un poligono regolare. Trovare le posizioni di questi vertici.

Esercizio 18. Se ξ è una radice n-ma dell'unità, dimostrare che

$$\sum_{k=0}^{n-1} \xi^k = 0 \ .$$

Dimostrare anche che la somma delle n radici n-me di un numero complesso è zero.

Esercizio 19. Trovare le radici terze di $1, 8, 27i, -8i, -4\sqrt{3}-4i$.

Osservazione. La rappresentazione polare dei numeri complessi è molto utile per trovare o ricordare formule di trigonometria. Supponiamo ad esempio di dover sviluppare $\cos n\vartheta$; poichè evidentemente

$$(\cos\vartheta + i \operatorname{sen}\vartheta)^n = \cos n\vartheta + i \operatorname{sen} n\vartheta \ ,$$

per ottenere $\cos n\vartheta$ basterà esplicitare la parte reale del primo membro.
Analogo è il discorso per $\operatorname{sen} n\vartheta$.

Esercizio 20. Trovare $\operatorname{sen} 3\vartheta$, $\cos 3\vartheta$, $\operatorname{sen} 4\vartheta$, $\cos 4\vartheta$.

Esercizio 21. Descrivete geometricamente le applicazioni
$z \mapsto \bar{z}$, $z \mapsto zi$, $z \mapsto \bar{z}i$.

Esercizio 22. Risolvere

1) $z^4 - 2iz^2 + 3 = 0$

2) $\begin{cases} w^4 - z^2 = 0 \\ w^2 + 2z = 1 \end{cases}$

Esercizio 23. Spiegate l'errore: $-1 = \sqrt{-1}\cdot\sqrt{-1} = \sqrt{(-1)(-1)} = \sqrt{1} = 1$.

Teorema fondamentale dell'algebra.

Così come abbiamo parlato di polinomi a coefficienti reali possiamo anche parlare di polinomi a coefficienti complessi (e parlare nello stesso modo di grado, riducibilità, regola di divisione con resto, etc.).
Un teorema "importante" e "sorprendente" è il seguente:

Teorema (fondamentale dell'algebra o di D'Alembert).

Ogni polinomio a coefficienti complessi di grado ≥ 1 ammette radici in campo complesso (e quindi per la regola di Ruffini ne ammette esattamente tante quanto è il suo grado). Questo significa che ogni equazione complessa di grado n ha esattamente n radici (contate naturalmente con la loro molteplicità).

Se $P(x)$ è un polinomio a coefficienti reali (che è anche un polinomio a coefficienti complessi) e se α è un numero complesso si ha

$$P(\bar{\alpha}) = \overline{P(\alpha)} \quad .$$

Pertanto se α è una radice complessa di un polinomio a coefficienti reali anche $\bar{\alpha}$ lo è (con la stessa molteplicità).

Osserviamo ancora che $(x-\alpha)(x-\bar{\alpha})$ è un polinomio di secondo grado a coefficienti reali; da queste osservazioni e dal teorema fondamentale dell'algebra si deduce che ogni polinomio a coefficienti reali irriducibile in campo reale è un polinomio

di primo grado o un polinomio di secondo grado con discriminante negativo.

Si deduce anche che, come avevamo anticipato, tutti i polinomi a coefficienti reali di grado dispari ammettono almeno una radice reale.

Esercizio 24. E' facile verificare che (se $a > 0$)

$$x^n - a^n = (x-a)(x^{n-1} + ax^{n-2} + a^2x^{n-3} + \ldots + a^{n-2}x + a^{n-1})$$

per n quasiasi,

$$x^n + a^n = (x+a)(x^{n-1} - ax^{n-2} + a^2x^{n-3} - \ldots - a^{n-2}x + a^{n-1}),$$

per n dispari.

Come si può scomporre $x^n - a^n$ e $x^n + a^n$ in polinomi irriducibili in campo reale?

(Sfruttate la formula per trovare le radici n-me complesse, e raggruppate poi fra loro le radici coniugate).