IL TEOREMA FONDAMENTALE DELL'ALGEBRA.

Se

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \tag{1}$$

è un polinomio di grado n in x, i cui coefficienti a_0, a_1, ..., a_n sono numeri reali o complessi arbitrariamente assegnati $(a_0 \neq 0)$, si può domandare se esista qualche valore (reale o complesso) di x che annulli $f(x)$. In altri termini, si può chiedere se l'equazione $f(x) = 0$, ossia

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n x + a_n = 0,$$

ammette sempre *radici* (reali o complesse) qualunque sia il grado n di essa.

La risposta a questo problema è affermativa; si ha cioè il teorema seguente, che prende il nome di *teorema fondamentale dell'algebra*:

Ogni equazione algebrica (a coefficienti reali o complessi) ammette almeno una radice (reale o complessa).

Per il teorema fondamentale ora enunciato , l'equazione

$$(2) \qquad f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

ha almeno una radice x_1. Siccome il polinomio $f(x)$ si annulla per $x = x_1$, esso è divisibile per $x - x_1$ e il quoziente è un polinomio $\varphi_1(x)$ di grado n-1. Si ha cioè l'identità

$$f(x) = (x - x_1)\,\varphi_1(x).$$

Ma l'equazione (2), oltre alla radice x_1, ha per radici tutte e sole le radici della $\varphi_1(x) = 0$. E questa equazione, per il teorema fondamentale, ha almeno una radice x_2 (dove $x_2 \neq x_1$ oppure $x_2 = x_1$); indicando con $\varphi_2(x)$ il polinomio, di grado n-2, quoziente della divisione di $\varphi_1(x)$ per $x - x_2$, si ha l'identità

$$\varphi_1(x) = (x - x_2)\,\varphi_2(x),$$

da cui

$$f(x) = (x - x_1)(x - x_2)\,\varphi_2(x).$$

Così continuando, dopo n divisioni, si perviene all'identità

$$f(x) = (x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_n)\varphi_n ,$$

dove φ_n è una costante. Sviluppando il secondo membro appare che φ_n è il coefficiente di x^n e pertanto $\varphi_n = a_0$. Si conclude che sussiste l'identità

$$(3) \qquad f(x) = a_0(x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_n).$$

Se alla variabile x si sostituisce uno qualsiasi dei numeri $x_1, x_2, \ldots, x_n$ (che sono tra loro diversi oppure no), il secondo membro della (3), e quindi anche il primo, si annulla. Dunque, come del resto si era già detto, i numeri $x_1, x_2, \ldots, x_n$ sono radici della (2). È utile poi osservare che la (2) non ammette altre radici, all'infuori di queste, poiché ponendo nel secondo membro della (3) per x un numero $\neq$ da $x_1, x_2, \ldots, x_n$ si ottiene un numero $\neq 0$.

Come si è già detto, i numeri $x_1, x_2, \ldots, x_n$ possono essere tutti diversi oppure possono essere uguali a gruppi; con altre parole, i fattori lineari $x-x_1, x-x_2, \ldots, x-x_n$, in cui viene scomposto il polinomio $f(x)$, possono essere tutti diversi oppure no. In definitiva, si ha:

Un'equazione algebrica di grado n *(a coefficienti reali o complessi), possiede* n *radici (reali o complesse) (distinte o no) e non più.*

Dalla (3) si ha pure:

Un polinomio di grado n *in* x *(a coefficienti reali o complessi), si può scomporre nel prodotto di* n *fattori lineari in* x*, distinti o no, i quali sono determinati in modo unico.*

RADICI MULTIPLE DI UN'EQUAZIONE ALGEBRICA.

Se s (e non più di s) delle radici della (2) sono uguali ad α, ossia se s (e non più di s) dei fattori lineari in cui si scompone $f(x)$ coincidono con $x-\alpha$, si dice che α è *radice multipla secondo* s della (2), o più brevemente *radice* s^{upla} della (2); il numero (intero >0) s si chiama *ordine di multiplicità* della radice α. In particolare, se $s=1$ si dice che α è radice *semplice* della (2), se $s=2$ che è radice *doppia*, ecc..

La definizione può così porsi:

Un numero α (reale o complesso) si dice radice s^{upla} dell'equazione (2), quando il primo membro dell'equazione è divisibile per $(x-\alpha)^s$ e non per $(x-\alpha)^{s+1}$.

Se α è radice s^{upla} della (2), sussiste dunque l'identità

$$f(x) = (x-\alpha)^s \varphi(x),$$

dove $\varphi(x)$ è un polinomio di grado $n-s$ tale che $\varphi(\alpha) \neq 0$.

Pertanto, se la (2) possiede le radici $\alpha_1, \alpha_2, \ldots, \alpha_k$ rispettivamente di multiplicità $s_1, s_2, \ldots, s_k$, sussisterà l'identità

$$f(x) = a_0(x-\alpha_1)^{s_1} \cdot (x-\alpha_2)^{s_2} \cdot \ldots \cdot (x-\alpha_k)^{s_k},$$

dove $s_1 + s_2 + \ldots + s_k = n$.

Quando la (2) ammette radici multiple, il numero delle sue radici *distinte* è dunque $< n$, ma, convenendo di contare s volte ogni radice di multiplicità s, si può dire, in ogni caso, che il numero delle radici della (2) è n.

Si ha dunque il teorema:

Un'equazione algebrica di grado n *(a coefficienti reali o complessi) ammette radici (reali o complesse), la somma dei cui ordini di multiplicità è* n.

Si noti che, limitandosi al solo campo dei numeri reali, il precedente teorema diviene assai poco preciso! La grande precisione del teorema è derivata dalla estensione del campo numerico (da quello reale a quello complesso).

Condizione necessaria e sufficiente affinché un numero a *sia radice* s^{upla} *dell'equazione* $f(x) = 0$, *è che esso annulli* $f(x)$ *e le sue derivate* $f'(x), f''(x), \ldots, f^{s-1}(x)$, *ma non la* $f^{s}(x)$.

RISULTANTE DI DUE EQUAZIONI ALGEBRICHE. METODO DEL MASSIMO COMUN DIVISORE.

Si chiama *risultante* di due equazioni algebriche

$$(4) \qquad \begin{aligned} f(x) &= a_0 x^n + a_1 x^{n-1} + \dots + a_n = 0, \\ \varphi(x) &= b_0 x^m + b_1 x^{m-1} + \dots + b_m = 0, \end{aligned}$$

di gradi n e m $(n \geq m)$, un'espressione razionale intera nei coefficienti $a_0, a_1, \dots, a_n; b_0; b_1, \dots, b_m$ delle due equazioni, il cui annullarsi dà la condizione necessaria e sufficiente affinché le due equazioni abbiano una radice comune (almeno).

Il risultante R delle equazioni (4) si può ottenere applicando ai polinomi $f(x)$, $\varphi(x)$ il procedimento delle divisioni successive che porta al massimo comun divisore di $f(x)$ e $\varphi(x)$. Spingendo il procedimento fino ad ottenere un resto di grado zero in x, questo resto sarà una funzione intera dei coefficienti delle (4) il cui annullarsi dà la condizione necessaria e sufficiente affinché $f(x)$ e $\varphi(x)$ abbiano un massimo comun divisore di primo grado, ossia la condizione perché le (4) abbiano una radice comune. Tale resto sarà dunque il risultante R cercato

Uguagliando a zero il resto di 1° grado in x si ha l'equazione (di 1° grado) che porge la radice comune delle (4).

L'operazione mediante la quale dalle equazioni (4) si ottiene il loro risultante R si chiama *eliminazione di* x *fra le due equazioni*.

METODO DI EULERO.

Un altro metodo per determinare il risultante delle (4) è il seguente, dovuto ad EULERO (2).

Condizione necessaria e sufficiente affinché le (4) abbiano almeno una radice comune è che si annulli il determinante

$$
(5) \qquad \begin{vmatrix}
a_0 & a_1 & a_2 & \cdots & a_n & 0 & 0 & \cdots & 0 \\
0 & a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\
0 & 0 & a_0 & \cdots & a_{n-2} & a_{n-1} & a_n & \cdots & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & a_n \\
b_0 & b_1 & b_2 & \cdots & b_m & 0 & 0 & \cdots & 0 \\
0 & b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \\
0 & 0 & b_0 & \cdots & b_{m-2} & b_{m-1} & b_m & \cdots & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & b_m
\end{vmatrix}
$$

Il determinante (5) d'ordine $n+m$ è dunque il risultante R delle (4).

"APPLICAZIONE":

DISCRIMINANTE DI UN'EQUAZIONE ALGEBRICA.

Si chiama *discriminante* di un'equazione algebrica di grado n

$$(2) \qquad f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$$

una funzione razionale intera dei coefficienti dell'equazione, il cui annullarsi dà la condizione necessaria e sufficiente affinché l'equazione abbia una radice doppia (almeno).

Segue:

Il discriminante dell'equazione (2) è il risultante della (2) e dell'equazione derivata $f'(x) = 0$.

Infatti si è visto prima che le radici doppie (almeno) della (2) sono appunto tutte e sole quelle comuni alla (2) e all'equazione derivata $f'(x) = 0$.

Si ha pure:

Il discriminante dell'equazione (2) è il risultante dell'equazione $\varphi(x) = nf(x) - xf'(x) = 0$ *e dell'equazione* $f'(x) = 0$.

SISTEMA DI DUE EQUAZIONI ALGEBRICHE IN DUE INCOGNITE; TEOREMA DI BÉZOUT.

Sussiste il *teorema di* BÉZOUT:

Due equazioni algebriche in due incognite, di gradi n *e* m, *hanno in generale* nm *soluzioni comuni* (distinte o no).

ESTENSIONI A PIÙ EQUAZIONI ALGEBRICHE IN PIÙ INCOGNITE

La nozione di risultante di due equazioni algebriche in un'incognita si estende a $r+1$ equazioni algebriche in r incognite.

Consideriamo, ad esempio, il caso $r=2$, cioè il caso di tre equazioni algebriche in due incognite

$$(6) \qquad f(x, y) = 0, \qquad \varphi(x, y) = 0, \qquad \psi(x, y) = 0,$$

di gradi n, m, p nelle incognite x, y.

Si chiama *risultante* delle (6) un'espressione razionale intera nei coefficienti delle (6) il cui annullarsi dà la condizione necessaria e sufficiente affinché le tre equazioni abbiano una soluzione comune (almeno).

L'operazione mediante la quale dalle equazioni (6) si ottiene il loro risultante si chiama *eliminazione delle x, y fra le tre equazioni*.

Anche nel caso attuale, il risultante si calcola con sole operazioni razionali.

Considerando i coefficienti delle (6) come quantità indeterminate, il risultante è una funzione razionale intera omogenea, irriducibile, determinata in modo unico (a meno di un fattore numerico) dei coefficienti delle (6). E tale risultante è di grado mp nei coefficienti di f, di grado np in quelli di φ e di grado nm in quelli di ψ.

Anche il teorema di BÉZOUT si estende ad un numero qualunque di equazioni algebriche in altrettante incognite. Si ha:

Un sistema di r equazioni algebriche in r incognite, ammette in generale un numero finito di soluzioni dato dal prodotto dei gradi delle equazioni del sistema.