Capitolo 1

Relazioni simmetriche e moduli di Cauchy

1.1 Polinomi simmetrici e funzioni simmetriche elementari

Sia K un campo. Un polinomio $F(x_1, x_2, \ldots, x_n)$ in n variabili a coefficienti in K si dice *simmetrico* nelle x_i se

$$F(x_1, x_2, \ldots, x_n) = F(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}),$$

per ogni permutazione σ del gruppo simmetrico S^n. (Si noti che in un polinomio simmetrico in n variabili debbono comparire tutte le variabili.)

Tra i polinomi simmetrici nelle x_i hanno particolare importanza le *funzioni simmetriche elementari*:

$$\left\{ \begin{array}{lcl} \sigma_1 & = & -(x_1 + x_2 + \cdots + x_n), \\ \sigma_2 & = & x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \\ \sigma_3 & = & -(x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n) \\ & \vdots & \\ \sigma_n & = & (-1)^n x_1x_2\cdots x_n, \end{array} \right. \tag{1.1}$$

cioè la somma delle x_i (col segno meno), la somma dei prodotti a due a due,..., la somma dei prodotti a k a k (col segno $(-1)^k$). Per come sono costruite, è facile vedere come le σ_k in n variabili, che denoteremo con $\sigma_k^{(n)}$, si possano ottenere da quelle in $n-1$ variabili e da x_n. Ad esempio, per $n = 4$ abbiamo

$$\begin{array}{lcl} \sigma_1^{(4)} & = & -(x_1 + x_2 + x_3 + x_4) = \sigma_1^{(3)} - x_4, \\ \sigma_2^{(4)} & = & x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \end{array}$$

$$\begin{aligned}
&= x_1x_2 + x_1x_3 + x_2x_3 + (x_1 + x_2 + x_3)x_4 \\
&= \sigma_2^{(3)} - \sigma_1^{(3)}x_4 \\
\sigma_3^{(4)} &= -(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) \\
&= -x_1x_2x_3 - (x_1x_2 + x_1x_3 + x_2x_3)x_4 \\
&= \sigma_3^{(3)} - \sigma_2^{(3)}x_4, \\
\sigma_4^{(4)} &= x_1x_2x_3x_4 = (x_1x_2x_3)x_4 \\
&= -\sigma_3^{(3)}x_4,
\end{aligned}$$

e in generale,

$$\left\{\begin{array}{lcl}
\sigma_1^{(n)} &=& \sigma_1^{(n-1)} - x_n, \\
\sigma_2^{(n)} &=& \sigma_2^{(n-1)} - \sigma_1^{(n-1)}x_n, \\
\sigma_3^{(n)} &=& \sigma_3^{(n-1)} - \sigma_2^{(n-1)}x_n, \\
&\vdots& \\
\sigma_{n-1}^{(n)} &=& \sigma_{n-1}^{(n-1)} - \sigma_{n-2}^{(n-1)}x_n, \\
\sigma_n^{(n)} &=& 0 - \sigma_{n-1}^{(n-1)}x_n.
\end{array}\right. \tag{1.2}$$

In particolare si osservi che ponendo $x_n = 0$ nelle (1.1) si ottengono le σ_i per $n-1$ variabili.

Queste funzioni godono di un'importante proprietà:

Teorema 1.1. *Le funzioni simmetriche elementari di $x_1, x_2, \ldots, x_n$ sono algebricamente indipendenti su K. In altre parole, se $f(y_1, y_2, \ldots, y_n)$ è un polinomio a coefficienti in K e se*

$$f(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0,$$

allora f è il polinomio nullo.

Dim. Per induzione su n. Se $n = 1$, e $f(x_1) = 0$ per qualche f allora f è il polinomio nullo perchè x_1 è trascendente su K. Scriviamo come sopra $\sigma_i^{(n)}$ per le σ_i in n variabili, $i = 1, 2, \ldots, n$ e osserviamo che per le (1.2) un polinomio nelle $\sigma_i^{(n)}$ si può rappresentare come polinomio in x_n e nelle $\sigma_i^{(n-1)}$, $i = 1, 2, \ldots, n-1$; ne segue

$$\begin{aligned}
f(\sigma_1^{(n)}, \sigma_2^{(n)}, \ldots, \sigma_n^{(n)}) &= f_0(\sigma_1^{(n-1)}, \sigma_2^{(n-1)}, \ldots, \sigma_{(n-1)}^{n-1})x_n^k \\
&+ f_1(\sigma_1^{(n-1)}, \sigma_2^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)})x_n^{k-1} \\
&\vdots \\
&+ f_k(\sigma_1^{(n-1)}, \sigma_2^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)}) \\
&= 0.
\end{aligned}$$

Ma x_n è algebricamente indipendente su $K(x_1, x_2, \ldots, x_{n-1})$, e dunque a fortiori su $K(\sigma_1^{(n-1)}, \sigma_2^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)})$ che è contenuto nel precedente. Ne segue $f_i(\sigma_1^{(n-1)}, \sigma_2^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)}) = 0$, $i = 1, 2, \ldots, k$. Per induzione allora gli $f_i(y_1, y_2, \ldots, y_{n-1})$ sono nulli, e dunque anche $f(y_1, y_2, \ldots, y_n)$ lo è. $\diamondsuit$

1.2 Nota. Un altro modo per esprimere il contenuto del Teorema 1.1 è il seguente: *se $x_1, x_2, \ldots, x_n$ sono algebricamente indipendenti su un campo K, anche le loro funzioni simmetriche elementari $\sigma_1, \sigma_2, \ldots, \sigma_n$ lo sono.*

1.2 I moduli di Cauchy e il teorema fondamentale delle funzioni simmetriche

Il valore u di un polinomio in un punto α è dato dal resto della divisione del polinomio per $x - \alpha$. Questo fatto si generalizza come segue:

1.3 Lemma. *Se un polinomio assume uno stesso valore u su k punti (distinti) $\alpha_1, \alpha_2, \ldots, \alpha_k$, questo valore è il resto della divisione del polinomio per il prodotto $(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$.*

Dim. Dividendo si ottiene un resto di grado minore di k. Questo resto assume uno stesso valore u su k punti distinti e dunque è identicamente uguale a u. $\diamondsuit$

Le σ_i della (1.1) sono i coefficienti del polinomio:

$$F(x) = \prod_{i=1}^{n} (x - x_i) = x^n + \sigma_1 x^{n-1} + \cdots + \sigma_{n-1} x + \sigma_n. \tag{1.3}$$

Dividiamo ora $F(x)$ per $x - x_1$; otteniamo

$$\begin{aligned}
\frac{F(x)}{x - x_1} &= (x - x_2) \cdots (x - x_n) \\
&= x^{n-1} \\
&+ (x_1 + \sigma_1) x^{n-2} \\
&+ (x_1^2 + \sigma_1 x_1 + \sigma_2) x^{n-3} \\
&\vdots \\
&+ (x_1^{i-1} + \sigma_1 x_1^{i-2} + \cdots + \sigma_{i-2} x_1 + \sigma_{i-1}) x^{n-i} \\
&+ (x_1^i + \sigma_1 x_1^{i-1} + \cdots + \sigma_{i-1} x_1 + \sigma_i) x^{n-(i+1)} \\
&\vdots \\
&+ x_1^{n-1} + \sigma_1 x_1^{n-2} + \cdots + \sigma_{n-2} x_1 + \sigma_{n-1}.
\end{aligned}$$

Si vede da qui che le funzioni simmetriche elementari di $x_2, x_3, \ldots, x_n$ (cioè i coefficienti di $(x-x_2)\cdots(x-x_n)$) si esprimono in termini di x_1 e delle prime $n-1$ funzioni simmetriche elementari $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ di $x_1, x_2, \ldots, x_n$. Posto $a_i = x_1^i + \sigma_1 x_1^{i-1} + \cdots + \sigma_{i-1}x_1 + \sigma_i$, dividendo il quoziente

$$\frac{F(x)}{x-x_1} = x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-2}x + a_{n-1}$$

per $x - x_2$, abbiamo

$$\frac{F(x)}{(x-x_1)(x-x_2)} = x^{n-2} + b_1 x^{n-3} + \cdots + b_{n-3}x + b_{n-2}$$

dove

$$b_i = x_2^i + a_1 x_2^{i-1} + a_2 x_2^{i-2} + \cdots + a_{i-1}x_2 + a_i,$$

e poichè a_i dipende da $x_1, \sigma_1, \ldots, \sigma_i$, si ha che b_i dipende da $x_1, x_2, \sigma_1, \ldots, \sigma_i$. Ne segue che i coefficienti di $\frac{F(x)}{(x-x_1)(x-x_2)} = (x-x_3)\cdots(x-x_n)$ dipendono da $x_1, x_2, \sigma_1, \ldots, \sigma_{n-2}$.

I polinomi

$$\begin{aligned}
X_1 &= F(x) = (x-x_1)(x-x_2)\cdots(x-x_n),\\
X_2 &= \frac{X_1}{x-x_1} = (x-x_2)\cdots(x-x_n)\\
&\vdots\\
X_i &= \frac{X_{i-1}}{x-x_{i-1}} = (x-x_i)\cdots(x-x_n),\\
&\vdots\\
X_n &= \frac{X_{n-1}}{x-x_{n-1}} = x - x_n,
\end{aligned}$$

soni i *moduli di Cauchy del polinomio* $F(x)$ e sono di grado $n, n-1, \ldots, 1$, rispettivamente. Scriviamo esplicitamente l'ultimo modulo X_n, di primo grado:

$$X_n = x - x_n = x + x_1 + x_2 + \cdots + x_{n-1} + \sigma_1.$$

Se $f(x)$ è un polinomio a coefficienti in un campo, e $\alpha_1, \alpha_2, \ldots, \alpha_n$ sono le sue radici, i *moduli di Cauchy di* $f(x)$ si ottengono dagli X_i per $x_i = \alpha_i$.

1.4 Esempio. Per un polinomio di grado 3 i moduli di Cauchy sono:

$$\begin{aligned}
X_1(x) &= F(x) = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3,\\
X_2(x_1, x) &= (x-x_2)(x-x_3) = x^2 - (x_2+x_3)x + x_2x_3\\
&= x^2 + (x_1+\sigma_1)x + x_1^2 + \sigma_1 x_1 + \sigma_2\\
X_3(x_1, x_2, x) &= x - x_3 = x + x_1 + x_2 + \sigma_1,
\end{aligned}$$

e se $f(x) = x^3 + e_1x^2 + e_2x + e_3$ e ha le radici $\alpha_1, \alpha_2, \alpha_3$ i moduli di Cauchy di $f(x)$ sono:

$$\begin{aligned} X_1(x) &= f(x), \\ X_2(\alpha_1, x) &= (x-\alpha_2)(x-\alpha_3) = x^2 - (\alpha_2+\alpha_3)x + \alpha_2\alpha_3 \\ &= x^2 + (\alpha_1+e_1)x + \alpha_1^2 + e_1\alpha_1 + e_2 \\ X_3(\alpha_1, \alpha_2, x) &= x - \alpha_3 = x + \alpha_1 + \alpha_2 + e_1. \end{aligned}$$

Per un polinomio di grado 4:

$$\begin{aligned} X_1 &= F(x) = x^4 + \sigma_1x^3 + \sigma_2x^2 + \sigma_3x + \sigma_4, \\ X_2 &= x^3 + (x_1+\sigma_1)x^2 + (x_1^2 + \sigma_1x_1 + \sigma_2)x + x_1^3 + \sigma_1x_1^2 + \sigma_2x_1 + \sigma_3, \\ X_3 &= x^2 + (x_1+x_2+\sigma_1)x + x_1^2 + x_2^2 + x_1x_2 + \sigma_1(x_1+x_2) + \sigma_2, \\ X_4 &= x + x_1 + x_2 + x_3 + \sigma_1, \end{aligned}$$

e se $f(x) = x^4 + e_1x^3 + e_2x^2 + e_3x + e_4$ ed ha le radici $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, i moduli di Cauchy di $f(x)$ sono

$$\begin{aligned} X_1(x) &= f(x), \\ X_2(\alpha_1, x) &= x^3 + (\alpha_1+e_1)x^2 + (\alpha_1^2 + e_1\alpha_1 + e_2)x + \alpha_1^3 + e_1\alpha_1^2 + e_2\alpha_1 + e_3, \\ X_3(\alpha_1, \alpha_2, x) &= x^2 + (\alpha_1+\alpha_2+e_1)x + \alpha_1^2 + \alpha_2^2 + \alpha_1\alpha_2 + e_1(\alpha_1+\alpha_2) + e_2, \\ X_4(\alpha_1, \alpha_2, \alpha_3, x) &= x + \alpha_1 + \alpha_2 + \alpha_3 + e_1, \end{aligned}$$

(le e_i sono le σ_i calcolate nelle α_i).

Veniamo ora al *teorema fondamentale delle funzioni simmetriche.*

1.5 Teorema. *Sia $F = F(x_1, x_2, \ldots, x_n)$ un polinomio simmetrico. Allora F è un polinomio nelle funzioni simmetriche elementari delle x_i.*

Dim. Sia $u = F(x_1, x_2, \ldots, x_n)$; allora u è il valore del polinomio

$$F(x_1, x_2, \ldots, x_{n-1}, x)$$

nel punto x_n, e dunque è il resto della divisione di questo polinomio per $x - x_n = x + x_1 + x_2 + \cdots + x_{n-1} + \sigma_1 = X_n$. Poichè x_n non compare né nel dividendo né nel divisore, non può comparire nel resto che dunque è un polinomio F_1 che dipende dalle prime $n-1$ delle x_i e da σ_1. Abbiamo allora:

$$u = F(x_1, x_2, \ldots, x_{n-1}, x_n) = F_1(\sigma_1, x_1, x_2, \ldots, x_{n-1}) \tag{1.4}$$

e F_1, essendo uguale a F che è simmetrico, è anch'esso simmetrico. Scambiamo ora x_{n-1} e x_n; per la (1.4) si ha

$$F_1(\sigma_1, x_1, x_2, \ldots, x_{n-2}, x_n) = F_1(\sigma_1, x_1, x_2, \ldots, x_{n-2}, x_{n-1}) = u,$$

per cui il polinomio $F_1(\sigma_1, x_1, x_2, \ldots, x_{n-2}, x)$ assume lo stesso valore u su x_n e x_{n-1}, e perciò u è il resto di F_1 nella divisione per $(x - x_{n-1})(x - x_{n-2}) = X_{n-1}$ (Lemma 1.3.). Poichè X_{n-1} dipende da $x_1, \ldots, x_{n-2}, \sigma_1, \sigma_2$, si ha $F_1(\sigma_1, x_1, x_2, \ldots, x_{n-2}, x_{n-1}) = F_2(\sigma_1, \sigma_2, x_1, x_2, \ldots, x_{n-2})$.

Procedendo come sopra, scambiamo x_{n-2} e x_{n-1}; otteniamo:

$$u = F_2(\sigma_1, \sigma_2, x_1, x_2, \ldots, x_{n-3}, x_{n-1}),$$

e scambiando x_{n-2} con x_n:

$$u = F_2(\sigma_1, \sigma_2, x_1, x_2, \ldots, x_{n-3}, x_n).$$

Il polinomio $F_2(\sigma_1, \sigma_2, x_1, x_2, \ldots, x_{n-3}, x)$ ha dunque lo stesso valore u su x_n, x_{n-1} e x_{n-2}. I coefficienti di $X_{n-2} = (x - x_{n-2})(x - x_{n-1})(x - x_n)$ si determinano in funzione di $x_1, x_2, \ldots, x_{n-3}, \sigma_1, \sigma_2, \sigma_3$. Proseguendo in questo modo (o per induzione) si eliminano tutte le x_i e si resta con le sole σ_i:

$$u = F_n(\sigma_1, \sigma_2, \ldots, \sigma_n),$$

che fornisce u come polinomio nelle σ_i. Si osservi che questa dimostrazione contiene anche un algoritmo per il calcolo di u in termini delle σ_i. $\diamondsuit$

1.6 Esempio . Sia $u = F(x_1, x_2) = x_1^3 + x_2^3$. Il polinomio $F(x_1, x) = x^3 + x_1^3$ diviso per $X_2 = x + x_1 + \sigma_1$ fornisce il resto

$$F_1(\sigma_1, x_1) = -3\sigma_1 x_1^2 - 3\sigma_1^2 x_1 - \sigma_1^3,$$

e dividendo ora $F_1(\sigma_1, x)$ per $X_1 = x^2 + \sigma_1 x + \sigma_2$ otteniamo $F_2(\sigma_1, \sigma_2) = -\sigma_1^3 + 3\sigma_1\sigma_2$, che è il valore u di F cercato. Si osservi che questo risultato si può ottenere anche mediante il "completamento del cubo":

$$\begin{aligned} x_1^3 + x_2^3 &= (x_1 + x_2)^3 - 3x_1^2 x_2 - 3x_1 x_2^2 \\ &= (x_1 + x_2)^3 - 3(x_1 + x_2)x_1 x_2 \\ &= -\sigma_1^3 + 3\sigma_1\sigma_2. \end{aligned}$$

1.7 Nota. Come mostra questo esempio, il polinomio nelle σ_i che si ottiene non è in generale simmetrico nelle σ_i. D'altra parte è chiaro che se $f(\sigma_1, \sigma_2, \ldots, \sigma_n)$ è un qualunque polinomio nelle σ_i, sostituendo alle σ_i le loro espressioni nelle x_i si ottiene un polinomio che è simmetrico nelle x_i. Il Teor. 1.5 si può considerare come l'inverso di questo fatto.

1.8 Corollario. *Sia $f(x)$ un polinomio a coefficienti in un campo K e siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ le sue radici in un ampliamento di K. Sia poi*

$$u = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

il valore nelle α_i di un polinomio $F(x_1, x_2, \ldots, x_n)$ simmetrico e a coefficienti in K. Allora u appartiene a K.

Dim. Scriviamo F in funzione delle σ_i:

$$F(x_1, x_2, \ldots, x_n) = F_n(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Allora $u = F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F_n(e_1, e_2, \ldots, e_n)$, dove le e_i si ottengono dalle σ_i ponendo $x_i = \alpha_i$. Ma le e_i sono i coefficienti di $f(x)$, e dunque appartengono a K, e poiché F_n è un polinomio, ed è a coefficienti in K, u appartiene a K. $\diamondsuit$

Osserviamo poi che l'algoritmo visto nel teorema ci permette di esprimere il valore u di un polinomio simmetrico F nelle radici di un polinomio $f(x)$ a partire solo dai coefficienti di $f(x)$, e cioè senza conoscere queste radici.

1.9 Corollario. *Una funzione razionale simmetrica:*

$$W = \frac{f(x_1, x_2, \ldots, x_n)}{g(x_1, x_2, \ldots, x_n)},$$

si esprime in termini delle funzioni simmetriche elementari delle x_i.

Dim. Sia $\Pi = \prod_{\sigma \in S^n} g(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. Si tratta ovviamente di una funzione simmetrica. Poichè W è simmetrica per ipotesi, anche il prodotto $W\Pi$ lo è. Ma

$$W\Pi = f(x_1, x_2, \ldots, x_n) \prod_{1 \neq \sigma \in S^n} g(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}),$$

e il secondo membro, essendo uguale al primo, è simmetrico. Per il teorema, esso si esprime in termini delle funzioni simmetriche elementari delle x_i, e poichè ciò vale anche per Π, si ha il risultato. $\diamondsuit$

1.10 Teorema. *L'espressione di un polinomio simmetrico in termini delle funzioni simmetriche elementari è unica.*

Dim. Se

$$F(x_1, x_2, \ldots, x_n) = f_1(\sigma_1, \sigma_2, \ldots, \sigma_n) = f_2(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

con $f_1 \neq f_2$, allora la differenza $f_1 - f_2$ è un polinomio non nullo in n variabili che si annulla sui σ_i. Ma ciò contraddice il Teorema 1.1. $\diamondsuit$

1.3 Relazioni simmetriche

Ritorniamo ai moduli di Cauchy di un polinomio $f(x)$ le cui radici (distinte) siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ e consideriamo il secondo modulo $X_2(\alpha_1, x) = \frac{f(x)}{x - \alpha_1}$ come

un polinomio in due variabili α_1 e x; poniamo $\alpha_1 = x_1$. Scriviamo $X_2(x_1, x)$ per questo secondo modulo, che sarà perciò un polinomio nelle due variabili x e x_1 a coefficienti le funzioni simmetriche elementari delle α_i (v. Es. 1.1). Poniamo ora $x = x_2$ in $X_2(x_1, x)$, per cui $X_2(x_1, x_2) = \frac{f(x_2)}{x_2 - x_1}$. Per analogia, poniamo $x = x_1$ in $X_1(x) = f(x)$. Se α è una radice di $f(x)$ abbiamo $X_1(\alpha) = f(\alpha) = 0$, e lo stesso accade se sostituiamo α con una qualunque altra radice di $f(x)$:

$$X_1(\alpha_i) = 0,\ i = 1, 2, \ldots, n. \tag{1.5}$$

Se α_i e α_j sono due radici di $f(x)$, $i \neq j$, allora

$$X_2(\alpha_i, \alpha_j) = 0,\ i, j = 1, 2, \ldots, n,\ i \neq j, \tag{1.6}$$

in quanto $X_2(\alpha_i, \alpha_j) = \frac{f(\alpha_j)}{\alpha_j - \alpha_i}$, che è zero. Si vede analogamente che in generale, per $X_k(x_1, x_2, \ldots, x_k)$, si ha:

$$X_k(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}) = 0, \tag{1.7}$$

per qualunque scelta delle α_{i_s} distinte.

1.11 Definizione. Una *relazione* (algebrica) su un campo K tra le quantità $\alpha_1, \alpha_2, \ldots, \alpha_n$ è un'uguaglianza

$$\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0,$$

dove $\varphi(x_1, x_2, \ldots, x_n)$ è un polinomio a coefficienti in K.

Per quanto appena visto, i polinomi

$$X_1(x_1),\ X_2(x_1, x_2), \ldots, X_n(x_1, x_2, \ldots, x_n) \tag{1.8}$$

danno luogo a relazioni sostituendo alle x_i valori (distinti) presi tra le α_i. Queste relazioni sono però particolari: la prima sussiste qualunque sia α_i, la seconda qualunque sia la coppia α_i, α_j, ecc., come si vede dalle (1.5), (1.6) e (1.7). Chiamiamo *relazioni simmetriche tra le* α_i queste relazioni. Si osservi che in quanto polinomi nelle $x_1, x_2, \ldots, x_n$ i polinomi X_k non sono simmetrici (a parte X_n), perchè non vi compaiono tutte le variabili. I polinomi X_k, come polinomi nelle $x_1, x_2, \ldots, x_k$, sono invece simmetrici.

1.12 Esempio. Sia $f(x) = x^3 + 1$, e consideriamo il polinomio $\varphi(x_1, x_2) = x_1^3 - x_2^3$, che non è simmetrico nelle x_1, x_2, x_3 (non compare x_3). Per le tre radici α_i si ha $\alpha^3 = -1$, e dunque per ogni coppia di queste radici $\alpha_i^3 - \alpha_j^3 = 0$. $\varphi(x_1, x_2)$ è dunque un polinomio non simmetrico in x_1, x_2 e x_3, che però dà luogo ad una relazione simmetrica tra le tre radici di $f(x)$.

1.13 Teorema. *Siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ le radici di un polinomio (monico) $f(x)$, e sia $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_k)$ una relazione simmetrica tra le α_i a coefficienti in un campo K. Allora*

$$\begin{aligned}\varphi(x_1, x_2, \ldots, x_k) &= X_1(x_1)q_1(x_1, x_2, \ldots, x_k) \\ &+ X_2(x_1, x_2)q_2(x_1, x_2, \ldots, x_k) \\ &\vdots \\ &+ X_k(x_1, x_2, \ldots, x_k)q_k(x_1, x_2, \ldots, x_k),\end{aligned}$$

dove i $q_i(x_1, x_2, \ldots, x_k)$ sono polinomi nelle x_i a coefficienti in K.

Dim. Sia $k = 1$. Allora $\varphi(x_1)$ è tale che $\varphi(\alpha) = 0$ per $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$, e perciò è divisibile per $(x_1 - \alpha_1)(x_1 - \alpha_2)\ldots(x_1 - \alpha_n) = f(x_1) = X_1(x_1)$:

$$\varphi(x_1) = X_1(x_1)q_1(x_1).$$

Sia $k = 2$ e sia il grado di $\varphi(x_1, x_2)$ in x_2 minore di $n - 1$. Poichè $\varphi(\alpha_1, x_2)$ ha le $n - 1$ radici $\alpha_2, \ldots, \alpha_n$, esso non dipende da x_2, e quindi φ è un polinomio nella sola variabile x_1. Siamo allora nel caso precedente. Se invece il grado di $\varphi(x_1, x_2)$ in x_2 è maggiore o uguale a $n - 1$, dividiamo per $X_2(x_1, x_2)$ considerando φ eX_2 come polinomi in x_2:

$$\varphi(x_1, x_2) = X_2(x_1, x_2)q_1(x_1, x_2) + r(x_1, x_2),$$

con il grado di $r(x_1, x_2)$ in x_2 minore del grado $n - 1$ di $X_2(x_1, x_2)$ in x_2, per cui

$$\varphi(\alpha_1, x_2) = X_2(\alpha_1, x_2)q_1(\alpha_1, x_2) + r(\alpha_1, x_2).$$

Ma

$$\varphi(\alpha_1, \alpha_i) = X_2(\alpha_1, \alpha_i) = 0,$$

per $i = 2, 3, \ldots, n$, e dunque anche $r(\alpha_1, \alpha_i) = 0$. Ma allora $r(x_1, x_2)$ non dipende da x_2, e dunque dipende solo da x_1; inoltre, esso si annulla per ogni α_k, come si vede considerando $\varphi(\alpha_k, \alpha_i)$. Per il caso precedente r è uguale a $X_1(x_1)q_1(x_1)$, per un certo q_1. In definitiva,

$$\varphi(x_1, x_2) = X_2(x_1, x_2)q_1(x_1, x_2) + X_1(x_1)q_1(x_1). \tag{1.9}$$

Per induzione su k, sia ora il teorema vero per $k - 1$ e consideriamo il polinomio $\varphi(x_1, x_2, \ldots, x_k)$. Se il grado di φ in x_k è minore di $n - k + 1$, poichè $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, x_k)$ ammette le $n-k+1$ radici $\alpha_k, \ldots, \alpha_n$, abbiamo che φ dipende solo dalle $x_1, \ldots, x_{k-1}$, e per induzione si ha quanto si voleva. Altrimenti, dividiamo per $X_k(x_1, x_2, \ldots, x_k)$ rispetto a x_k, ottenendo

$$\varphi(x_1, x_2, \ldots, x_k) = X_k(x_1, x_2, \ldots, x_k)q_k(x_1, x_2, \ldots, x_k) + r(x_1, x_2, \ldots, x_k),$$

con il grado di r in x_k inferiore a quello di X_k, che è $n-k+1$. Poichè $r(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, x_k)$ si annulla per gli $n-k+1$ valori $\alpha_k, \alpha_{k+1}, \ldots, \alpha_n$, r non dipende da x_k, e poichè si annulla per ogni $(k-1)-$pla degli α_i, come si vede considerando $\varphi(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{k-1}}, \alpha_{i_k})$, esso ha per induzione la forma richiesta. Ne segue che anche φ ha la forma richiesta. $\diamondsuit$

I polinomi q_i in una, due,..., $k-1$ variabili determinati come quozienti nella dimostrazione del teorema, possono essere considerati come polinomi in k variabili, ma che dipendono solo dalla prima, dalle prime due,..., dalle prime $k-1$. Inoltre, è chiaro che se φ ha la forma del teorema, con i q_i polinomi qualunque in k variabili, allora si annulla per una qualunque $k-$pla degli α_i.

1.14 Esempio. Con f e φ come nell'Es. 1.12 , e φ considerata come funzione delle due variabili x_1 e x_2, si ha

$$X_2(x_1, x_2) = x_2^2 + x_1 x_2 + x_1^2;$$

dividendo φ per X_2 rispetto ad x_2 si ottiene

$$\varphi(x_1, x_2) = X_2(x_1, x_2)(x_1 - x_2),$$

che è della forma (1.9) con $q_2(x_1, x_2) = x_1 - x_2$ e $q_1(x_1) = 0$. Se consideriamo $\varphi(x_1, x_2) = -x_2^3 + x_1^4 + x_1 - 1$ abbiamo, nella forma (1.9),

$$\varphi(x_1, x_2) = X_2(x_1, x_2)(x_1 - x_2) + X_1(x_1)(x_1 - 1).$$

Nell'anello dei polinomi in al più n variabili, i polinomi in k variabili che si annullano per qualunque $k-$pla delle α_i, $k = 1, 2, \ldots, n$, formano un ideale, com'è subito visto. Ricordiamo che una *base* per un ideale I di un anello è un insieme $B \subseteq I$ tale che ogni elemento di I si scrive come combinazione $\sum a_i b_i$ di un numero finito di elementi $b_i \in B$ a coefficienti a_i nell'anello. Possiamo allora enunciare il Teor. 1.13 in questo modo:

1.13′ Teorema. *I moduli di Cauchy $X_1, X_2, \ldots, X_k$ di un polinomio $f(x)$ di grado n formano una base dell'ideale delle relazioni simmetriche in k variabili tra le radici di $f(x)$.*

1.15 Nota. Per costruzione, i monomi principali dei polinomi (1.8) sono rispettivamente

$$x_1^n, x_2^{n-1}, \ldots, x_{n-1}^2, x_n,$$

e sono pertanto primi a due a due. Si può dimostrare che questo fatto implica che i polinomi (1.8) sono una base standard (o di Gröbner) dell'ideale delle relazioni simmetriche dell'anello $K[x_1, x_2, \ldots, x_n]$.

1.16 Esempi. 1. Il discriminante $\Delta = \prod_{i<j}(x_i - x_j)^2$ del polinomio (1.3) è una funzione simmetrica. Applichiamo il Teor. 1.5 per esprimere Δ in termini delle funzioni simmetriche elementari per $n = 2$ e $n = 3$.

i) $n = 2$. $\Delta = (x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2$. Dividiamo Δ per $X_2 = x_2 + x_1 + \sigma_1$ come polinomi in x_2; otteniamo il resto $R_2 = 4x_1^2 + 4\sigma_1 x_1 + \sigma_1^2$. Dividendo R_2 per $X_1 = f = x_1^2 + \sigma_1 x_1 + \sigma_2$ si ottiene $\sigma_1^2 - 4\sigma_2$.

ii) $n = 3$, con $f = x^3 + px + q$ (si può ridurre un polinomio di terzo grado $f = y^3 + \sigma_1 y^2 + \sigma_2 y + \sigma_3$ a questa forma mediante la sostituzione $y = x - \frac{1}{3}\sigma_1$). Le divisioni successive danno un resto finale di $-4p^2 - 27q^3$.

2. La somma delle potenze $k-$esime delle x_i (nel nostro esempio, per $n = 4$):

$$\begin{aligned} V_1 &= x_1 + x_2 + x_3 + x_4 \\ V_2 &= x_1^2 + x_2^2 + x_3^2 + x_4^2 \\ V_3 &= x_1^3 + x_2^3 + x_3^3 + x_4^3 \\ V_4 &= x_1^4 + x_2^4 + x_3^4 + x_4^4 \end{aligned}$$

Dividiamo V_1 per X_1 e prendiamo il resto:

$$R = -\sigma_1,$$

che è l'espressione cercata. Dividiamo V_2 per X_3 e prendiamo il resto: $2x_1^2 + 2x_2^2 + 2x_1x_2 + 2\sigma_1 x_1 + 2\sigma_1 x_2 + \sigma_1^2$. Dividendo questo per X_2 otteniamo l'espressione cercata:

$$\sigma_1^2 - 2\sigma_2.$$

Per V_3 otteniamo un primo resto $-3x_2x_1^2 - 3\sigma_1 x_1^2 - 3x_2^2 x_1 - 6x_1 s_1 x_2 - 3x_1\sigma_1^2 - 3x_2^2\sigma_1 - 3\sigma_1^2 x_2 - s_1^3$, che diviso per X_2 dà resto $3\sigma_1 x_1^2 - \sigma_1^3 + 3x_1^3 + 3\sigma_2 x_1 + 3\sigma_2\sigma_1$. Dividendo questo per X_1 si ha l'espressione cercata:

$$-\sigma_1^3 + 3\sigma - 2\sigma_1 - 3\sigma_3.$$

Per V_4 si ottiene

$$\sigma_1^4 - 4\sigma_2\sigma_1^2 + 2\sigma_2^2 + 4\sigma_1\sigma_3.$$

Le formule di Newton permettono di dare un'espressione ricorsiva delle V_k in termini delle $V_{k-1}, V_{k-2}, \ldots, V_1$ e delle σ_i, $i = 1, 2, \ldots, k$:

$$V_n = -\sigma_1 V_{n-1} - \sigma_2 V_{n-2} - \cdots - n\sigma_n,$$

e per potenze $k-$esime con $k > n$

$$V_{n+k} = -\sigma_1 V_{n+k-1} - \sigma_2 V_{n+k-2} - \cdots - \sigma_n V_k.$$