UNIVERSITÀ DEGLI STUDI DI FIRENZE
FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
CORSO DI LAUREA IN MATEMATICA - A.A. 2009-2010

TITOLO DELLA TESI:

Polinomi Simmetrici

Candidato: Daniele Buratta
Relatore: Giorgio Maria Ottaviani

Indice

Introduzione

Nella prima parte sarà descritto l'ordinamento lessicografico *lex order* per i monomi in un polinomio e saranno introdotte le *funzioni simmetriche elementari*, strumenti utili per descrivere tutti quei polinomi che non cambiano forma quando si ha una permutazione delle variabili, detti appunto *polinomi simmetrici*.
Sarà quindi presentato il *Teorema Fondamentale dei polinomi simmetrici*, che rappresenta il cuore della Tesi e lega i polinomi simmetrici alle funzioni simmetriche elementari.
Dalla dimostrazione di quest'ultimo si ricaverà anche *un'algoritmo di scrittura* per i polinomi simmetrici in funzione delle funzioni simmetriche elementari.
Seguirà poi la definizione di *polinomio omogeneo* e lo studio dei polinomi simmetrici omogenei.

Nella seconda parte invece, saranno introdotte le *somme di potenze* e attraverso le *identità di Newton* si mostrerà che esiste una relazione lineare tra quest'ultime e le funzioni simmetriche elementari.
Si troverà quindi una relazione lineare anche tra i coefficienti di un polinomio monico e le funzioni simmetriche elementari.
Saranno infine introdotti il *Discriminante*, il quale osserveremo che lo si può scrivere in funzione dei coefficienti del polinomio, e la *funzione generatrice*, che applicata a P_k, che corrisponde al numero di funzioni simmetriche indipendenti di un certo grado k, ci aiuterà a stabilire il valore di un P_k arbitrario.

Capitolo 1

Polinomi simmetrici e funzioni simmetriche elementari

1.1 Lex Order

Notazione
Date $x_1, \dots, x_n$ variabili, un monomio sarà dato da $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$, dove $\alpha_i \in \mathbb{Z}_{\geq 0}$ e conseguentemente $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Definizione 1.1. *Un* **ordinamento lineare o totale** *è un ordinamento tale che, $\forall$ coppia di monomi x^α,x^β vale esattamente una delle seguenti affermazioni:*

- $x^\alpha > x^\beta$,
- $x^\alpha = x^\beta$,
- $x^\alpha < x^\beta$.

Definizione 1.2. *Un* **ordinamento monomiale** *su $k[x_1, \dots, x_n]$ è una qualunque relazione $>$ su $\mathbb{Z}^n_{\geq 0}$ o equivalentemente, una qualunque relazione su un insieme di monomi x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, soddisfacente:*

- *$>$ è una relazione d'ordine totale su $\mathbb{Z}^n_{\geq 0}$.*
- *Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$, allora $\alpha + \gamma > \beta + \gamma$.*
- *$>$ è ben-ordinata su $\mathbb{Z}^n_{\geq 0}$, ovvero ogni sottoinsieme non vuoto di $\mathbb{Z}^n_{\geq 0}$ ha elemento minimo secondo $>$.*

Per meglio comprendere il terzo punto della definizione precedente introduciamo il seguente lemma,

Lemma 1.1.1.
Una relazione d'ordine $>$ su $\mathbb{Z}^n_{\geq 0}$ è ben-ordinata se e solo se ogni sequenza strettamente decrescente in $\mathbb{Z}^n_{\geq 0}$

$$a(1) > a(2) > a(3) > \dots$$

ha un termine.

Definizione 1.3. Ordinamento Lessicografico (lex order)
Siano $\alpha = (\alpha_1, \dots, \alpha_n)$ e $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Diciamo $\alpha >_{lex} \beta$ se, nel vettore differenza $\alpha - \beta \in \mathbb{Z}^n$, il primo elemento diverso da zero più a sinistra è positivo.
Scriveremo $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.

Esempi:

- $(1, 2, 0) >_{lex} (0, 3, 4)$ dato che $(1, 2, 0) - (0, 3, 4) = (1, -1, -4)$
- $(3, 2, 4) >_{lex} (3, 2, 1)$ dato che $(3, 2, 4) - (3, 2, 1) = (0, 0, 3)$
- $(1, 0, \dots, 0) >_{lex} (0, 1, \dots, 0) >_{lex} (0, 0, 1, \dots, 0) >_{lex} \dots >_{lex} (0, \dots, 0, 1)$
- Struttura del dizionario: $a > b > \dots > z \Rightarrow$ arrow$>_{lex}$arson

Per completezza osservo che

Proposizione 1.1.2.
Lex order su $\mathbb{Z}^n_{\geq 0}$ è un ordinamento monomiale.

Osservazione 1. É importante notare che ci sono diversi lex order, dipendentemente da come sono ordinate le variabili.
Con il semplice lex order si intende $x_1 > x_2 > \dots > x_n$. Ma dato un qualsiasi ordine di variabili $x_1, \dots, x_n$ c'è un corrispondente lex order.

1.2 Leading Term

Definizione 1.4.
Sia $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio non nullo nel campo $k[x_1, \dots, x_n]$ e sia $>$ un ordine monomiale,

- *Il* **multidegree di** *f è*

$$multideg(f) = max\{\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0\}$$

(il max è calcolato in base alla scelta di $>$)

- *il* **leading coefficient di** f *è*

$$LC(f) = a_{multideg(f)} \in k$$

- *il* **leading monomial di** f *è*

$$LM(f) = x^{multideg(f)} \in k$$

- *il* **leading term di** f *è*

$$LT(f) = LC(f) \cdot LM(f) = a_{multideg(f)} x^{multideg(f)}$$

Esempio:
Prendiamo ora il polinomio $f = +4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$ e sia $>$ con lex order, allora:

$$\begin{aligned} multideg(f) &= (3,0,0), \\ LC(f) &= -5, \\ LM(f) &= x^3, \\ LT(f) &= -5x^3 \end{aligned}$$

Lemma 1.2.1.
Siano $f, g \in k[x_1, \ldots, x_n]$ polinomi non nulli. Allora valgono:

1. $multideg(fg) = multideg(f) + multideg(g)$
2. *Se* $f + g \neq 0 \Rightarrow multideg(f + g) \leq max\{multideg(f), multideg(g)\}$.
   Inoltre se $multideg(f) \neq multideg(g)$, *allora vale l'uguaglianza.*

1.3 Teorema Fondamentale dei polinomi simmetrici

Definizione 1.5. *Un polinomio* $f \in k[x_1, \ldots, x_n]$ *è* **simmetrico** *se*

$$f(x_{i_1}, \ldots, x_{i_n}) = f(x_1, \ldots, x_n)$$

per ogni possibile permutazione $x_{i_1}, \ldots, x_{i_n}$ *delle variabili* $x_1, \ldots, x_n$.

Definizione 1.6. *Date le variabili $x_1, \dots, x_n$, noi definiamo le* **funzioni simmetriche elementari** $\sigma_1, \dots, \sigma_n \in k[x_1, \dots, x_n]$ *nel modo seguente:*

$$\sigma_1 = x_1 + \ldots + x_n,$$

$$\vdots$$

$$\sigma_r = \sum_{i_1 < i_2 < \ldots < i_r} x_{i_1} x_{i_2} \cdots x_{i_r},$$

$$\vdots$$

$$\sigma_n = x_1 x_2 \cdots x_n.$$

Osservazione 2. Data $\sigma_i^{(n)}$, la i-esima funzione elementare nelle variabili $x_1, \dots, x_n$ (<u>nota</u>: l'apice di σ_i indica il numero di variabili e non è una potenza), se definisco anche $\sigma_0^{(n)} = 1$ e $\sigma_i^{(n)} = o$ se $i < 0$ o $i > n$, osservo che

$$\sigma_i^{(n)} = \sigma_i^{(n-1)} + x_n \sigma_{i-1}^{(n-1)} \qquad \forall n > 1 \ \forall i$$

Dimostrazione.

- $\boxed{i < 0 \text{ o } i > n}$ $\qquad 0 = \sigma_i^{(n)} = \sigma_i^{(n-1)} + x_n \sigma_{i-1}^{(n-1)} = 0 + 0.$
- $\boxed{i = 0}$ $\qquad 1 = \sigma_0^{(n)} = \sigma_0^{(n-1)} + x_n \sigma_{-1}^{(n-1)} = 1 + 0 = 1$
- $\boxed{0 < i \leq n}$

$$\begin{aligned}
\sigma_i^{(n)} &= x_1 x_2 \ldots x_i + x_1 x_3 \ldots x_i + \ldots + x_1 x_3 \ldots x_{i+1} + \ldots + x_1 \ldots x_n + x_2 \ldots x_n + x_{n-i} \ldots x_n = \\
&= (x_1 x_2 \ldots x_i + \ldots + x_1 \ldots x_{n-1}) + x_1 \ldots x_n + \ldots + x_{n-i} \ldots x_n = \\
&= \sigma_i^{(n-1)} + x_n (x_1 \ldots x_{n-1} + \ldots + x_{n-i} \ldots x_{n-1}) = \\
&= \sigma_i^{(n-1)} + x_n \sigma_{i-1}^{(n-1)}
\end{aligned}$$

□

Vediamo adesso il teorema centrale di tutto l'argomento,

Teorema 1.3.1 (TEOREMA FONDAMENTALE DEI POLINOMI SIMMETRICI).
Ogni polinomio simmetrico in $k[x_1, ..., x_n]$ può essere scritto, in modo unico, come un polinomio nelle funzioni simmetriche elementari $\sigma_1, \dots, \sigma_n$,
ovvero
$\forall f$ *simmetrico* $\exists\,!\ g$ *t.c.* $f(x_1, \dots, x_n) = g(\sigma_1, \dots, \sigma_n)$.

Dimostrazione. Useremo lex order con $x_1 > \ldots > x_n$. Dato un polinomio simmetrico non nullo $f \in k[x_1, ..., x_n]$ sia $LT(f) = ax^\alpha$.

Se $\alpha = (\alpha_1, \ldots, \alpha_n)$ per prima cosa mostriamo che $\alpha_1 \geq \ldots \geq \alpha_n$. Per assurdo supponiamo $\alpha_i < \alpha_{i+1}$ $\exists i$. Sia $\beta = (\alpha_1, \ldots, \alpha_{i+1}, \alpha_i, \ldots, \alpha_n)$ il vettore esponente ottenuto da α attraverso lo scambio tra α_i e α_{i+1}.
Dato che ax^α è termine di $f(x_1, \ldots, x_n)$, allora ax^β è termine di $f(x_1, \ldots, x_{i+1}, x_i, \ldots, x_n)$. Ma $f(x_1, \ldots, x_n) = f(x_1, \ldots, x_{i+1}, x_i, \ldots, x_n)$ dato che é simmetrico, quindi ax^β termine di f e ciò è impossibile dato che $\beta > \alpha$ in lex order e quindi ax^β diverrebbe $LT(f)$!

Sia ora $h = \sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3} \ldots \sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\sigma_n^{\alpha_n}$. Notiamo che $LT(\sigma_r) = x_1 \ldots x_r$ $1 \leq r \leq n$. Dunque

$$\begin{aligned}
LT(h) &= LT(\sigma_1^{\alpha_1-\alpha_2} \ldots \sigma_n^{\alpha_n}) = \\
&= LT(\sigma_1^{\alpha_1-\alpha_2}) \ldots LT(\sigma_n^{\alpha_n}) = \\
&= LT(\sigma_1)^{\alpha_1-\alpha_2} \ldots LT(\sigma_n)^{\alpha_n} = \\
&= x_1^{\alpha_1-\alpha_2}(x_1x_2)^{\alpha_2-\alpha_3} \ldots (x_1 \ldots x_n)^{\alpha_n} = \\
&= x_1^{\alpha_1}x_2^{\alpha_2} \ldots x_n^{\alpha_n} = x^\alpha
\end{aligned}$$

Dato che f e ah hanno lo stesso LT, utilizzando anche il lemma 1.2.1, segue

$$multideg(f - ah) < multideg(f)$$

ogni volta che $f - ah \neq 0$.

Definiamo ora $f_1 = f - ah$ e notiamo che f_1 è simmetrica dato che f e ah lo sono. Quindi se $f_1 \neq 0$ possiamo ripetere il processo precedente e formare $f_2 = f_1 - a_1h_1$, dove a_1 è costante e h_1 è prodotto di $\sigma_1 \ldots \sigma_n$. Inoltre, $LT(f_2) < LT(f_1)$ quando $f_2 \neq 0$. Continuando in questo modo possiamo ricavarci una sequenza di polinomi $f, f_1, \ldots$ con

$$multideg(f) > multideg(f_1) > \ldots$$

Ma dato che lex order è ben ordinato la sequenza deve terminare e succede esattamente per il primo valore di t per cui $f_{t+1} = 0$. Segue immediatamente che

$$f = ah + a_1h_1 + \ldots + a_th_t,$$

che mostra che f è polinomio nelle funzioni simmetriche elementari.

Infine proviamo l'unicità.

Suponiamo che f si possa scrivere in due differenti modi come combinazione delle funzioni simmetriche elementari

$$g_1(\sigma_1, \ldots, \sigma_n) = f = g_2(\sigma_1, \ldots, \sigma_n)$$

dove g_1 e g_2 sono polinomi in n variabili $y_1, \ldots, y_n$.
Dobbiamo ora provare che $g_1 = g_2$ in $k[y_1, \ldots, y_n]$.
Definiamo $g = g_1 - g_2$. Allora $g(\sigma_1, \ldots, \sigma_n) = 0$ in $k[x_1, \ldots, x_n]$. Supponiamo per assurdo $g \neq 0$ in $k[y_1, \ldots, y_n]$ e $g = \sum_{\beta=1}^{n} a_\beta y^\beta$. Allora $g(\sigma_1, \ldots, \sigma_n)$ è somma dei polinomi $g_\beta = a_\beta \sigma_1^{\beta_1} \ldots \sigma_n^{\beta_n}$, dove $\beta = (\beta_1, \ldots, \beta_n)$. Per quanto provato prima si ha

$$LT(g_\beta) = a_\beta x_1^{\beta_1+\ldots+\beta_n} x_2^{\beta_2+\ldots+\beta_n} \ldots x_n^{\beta_n}.$$

e dato che l'applicazione

$$(\beta_1, \ldots, \beta_n) \longmapsto (\beta_1 + \ldots + \beta_n, \beta_2 + \ldots + \beta_n, \ldots, \beta_n)$$

è iniettiva,
allora tutti i g_β hanno distinti LT. In particolare possiamo raccogliere $\beta = (\beta_1, \ldots, \beta_n)$ in modo tale che $LT(g_\beta) > LT(g_\gamma) \quad \forall\, \gamma \neq \beta$. Allora $LT(g_\beta)$ sará piú grande di tutti i termini dei g_γ.
Segue che non c'è nessun termine che può cancellare $LT(g_\beta)$ e quindi $g(\sigma_1, \ldots, \sigma_n)$ non può essere 0 in $k[x_1, \ldots, x_n]$, assurdo.

$\square$

Osservazione 3. **Cenni Storici**
La dimostrazione appena descritta è attribuita a Gauss, il quale aveva bisogno delle proprietà dei polinomi simmetrici per la sua seconda dimostrazione (datata 1816) del TEOREMA FONDAMENTALE DELL'ALGEBRA.

Gauss definiva il *lex order* nel modo seguente:
Dati 2 termini $Ma^\alpha b^\beta c^\gamma \ldots$ *e* $Ma^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$ *l'ordine superiore è attribuito al primo rispetto al secondo se,*

$$o \;\; \alpha > \alpha' \quad o \;\; \alpha = \alpha' \;\; e \;\; \beta > \beta' \quad o \;\; \alpha = \alpha', \beta = \beta' \;\; e \;\; \gamma > \gamma' \quad o \quad etc\ldots$$

ed è la definizione esplicita conosciuta più semplice del *lex order*.

Osservazione 4. **Algoritmo per la scrittura di un polinomio simmetrico in funzione di** $\sigma_1, \ldots, \sigma_n$.
Notiamo che la dimostrazione del teorema ci fornisce inoltre un algoritmo per la scrittura di un polinomio simmetrico in funzione di $\sigma_1, \ldots, \sigma_n$. E il teorema ci assicura anche che tale scrittura è unica.

Vediamo ora la <u>struttura dell'algoritmo</u>:

- $g := 0$.
- Sotto-algoritmo che calcola il $LT(f) := ax^\alpha$.
  Si può realizzare attraverso confronti tra gli esponenti dei monomi in accordo con la definizione di lex order e con la selezione del monomio il cui esponente corrisponde al $multideg(f)$.
- $g_1 := \prod_{i=1}^n \sigma_i^{\alpha_i-\alpha_{i+1}} = \sigma_n^{\alpha_n}\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\ldots\sigma_1^{\alpha_1-\alpha_2}$ con $\alpha_{n+1}=0$.
  Questo è costruito in modo t.c. $LT(f) = LT(g_1)$ e deriva dal calcolo visto nella dimostrazione del teorema.
- $f_1 := f - ag_1$.
- $g_2 := g + ag_1$.
- Se $f_1 \equiv 0 \rightarrow f := g_2$ e stampa f.
  altrimenti $\rightarrow f := f_1$, $g := g_2$ e ritorna al secondo passsaggio.

Vediamo adesso un'esempio di utilizzo dell'algoritmo:

$$\begin{aligned}
&f = x^3y + x^3z + xy^3 + xz^3 + y^3z + yz^3 \in k[x,y,z]\\
&g = 0
\end{aligned}$$

$$\Big\downarrow\ LT(f) = x^3y,\ g_1 = \sigma_1^2\sigma_2$$

$$\begin{aligned}
&f_1 = f - \sigma_1^2\sigma_2 = -2x^2y^2 - 5x^2yz - 2x^2z^2 - 5xy^2z - 5xyz^2 - 2y^2z^2 \not\equiv 0\\
&g_2 = g + g_1 = \sigma_1^2\sigma_2
\end{aligned}$$

$$\Big\downarrow\ f = f_1,\ g = g_2,\ LT(f) = -2x^2y^2,\ g_1 = \sigma_2^2$$

$$\begin{aligned}
&f_1 = f + 2\sigma_2^2 = -x^2yz - xy^2z - xyz^2 \not\equiv 0\\
&g_2 = g - 2g_1 = \sigma_1^2\sigma_2 - 2\sigma_2^2
\end{aligned}$$

$$\Big\downarrow\ f = f_1,\ g = g_2,\ LT(f) = -x^2yz,\ g_1 = \sigma_1\sigma_3$$

$$\begin{aligned}
&f_1 = f + \sigma_1\sigma_3 = 0\\
&g_2 = g - g_1 = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1\sigma_3
\end{aligned}$$

$$\Big\Downarrow$$

$$f = g_2 = \sigma_1^2\sigma_2 - 2\sigma_2^2 - \sigma_1\sigma_3$$

1.4 Polinomi omogenei

Definizione 1.7. *Un polinomio $f \in k[x_1, \dots, x_n]$ è* **omogeneo di grado totale k** *se ogni termine che appare in f ha grado totale k.*

Osservazione 5.

- La i-esima funzione simmetrica elementare σ_i è omogenea di grado totale i.
- Ogni polinomio può essere scritto (in modo unico) come somma di polinomi omogenei, ovvero
  dato $f \in k[x_1, \dots, x_n]$ sia f_k la somma di tutti i termini di f di ordine totale k. Allora ogni f_k è omogeneo e $f = \sum_k f_k$.
  Chiamiamo f_k il **k-esimo componente omogeneo di** f.

Proposizione 1.4.1.
Un polinomio f è simmetrico se e solo se tutti i suoi componenti omogenei sono simmetrici.

Dimostrazione.

$\Rightarrow$ Dato un polinomio simmetrico f, sia $x_{i_1}, \dots, x_{i_n}$ una permutazione delle variabili $x_1, \dots, x_n$. Questa permutazione porta un termine di f di grado totale k ad un altro dello stesso grado totale. Dato $f(x_{i_1}, \dots, x_{i_n}) = f(x_1, \dots, x_n)$ segue che anche il k-esimo componente omogeneo deve anch'esso essere simmetrico.

$\Leftarrow$ la dimostrazione è banale.

$\square$

Capitolo 2

Somme di potenze e applicazioni

2.1 Somme di potenze e identità di Newton

Consideriamo ora le seguenti somme di potenze:

$$s_k = x_1^k + x_2^k + \ldots + x_n^k.$$

Notiamo che s_k è simmetrico, vale allora:

Teorema 2.1.1.
Se k è un campo di caratteristica 0, allora tutti i polinomi simmetrici in $k[x_1, \ldots, x_n]$ possono essere scritti come un polinomio nelle somme di potenze $s_1, \ldots, s_n$.

Dimostrazione. Dato il teorema fondamentale dei polinomi simmetrici, ogni polinomio simmetrico è un polinomio nelle funzioni simmetriche elementari, allora è sufficiente provare che $\sigma_1, \ldots, \sigma_n$ sono polinomi in $s_1, \ldots, s_n$.
Useremo le identità di Newton [1]:

$$s_k - \sigma_1 s_{k-1} + \ldots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k \sigma_k k = 0 \qquad 1 \leq k \leq n \quad (2.1)$$

$$s_k - \sigma_1 s_{k-1} + \ldots + (-1)^{n-1}\sigma_{n-1}s_{k-n+1} + (-1)^n \sigma_n s_{k-n} = 0 \qquad k > n \quad (2.2)$$

Proviamo ora per induzione su k che σ_k è polinomio in $s_1, \ldots, s_n$.

[1] La struttura della dimostrazione delle id. di Newton è divisa in 2 parti:

1. Se definisco σ_0=1 e σ_i=0 per $i > n$ e $i < 0$ allora è immediato verificare che le equazioni (2.1) e (2.2) sono equivalenti $\forall k \geq 1$.
2. Si prova per ind. su k la (2.1). Per farlo basta utilizzare la relazione (dell'oss. 3) $\sigma_i^{(n)} = \sigma_i^{(n-1)} + x_n \sigma_{i-1}^{(n-1)}$ $\forall n > 1$ $\forall i$ e notare che $s_k^{(n)} = s_k^{(n-1)} + x_n^k$. (nota: gli apici di σ_i e s_j indicano il numero di variabili e non una potenza).

$\boxed{\textbf{Base}}$ $\sigma_1 = s_1$.

$\boxed{\textbf{Ipotesi Induttiva}}$ vera per $1, 2, \dots, k-1$, allora le id. di Newton indicano che :

$$\sigma_k = (-1)^{k-1}\frac{1}{k}(s_k - \sigma_1 s_{k-1} + \dots + (-1)^{k-1}\sigma_{k-1}s_1).$$

Allora la nostra assunzione induttiva è dimostrata, ovvero σ_k è polinomio in $s_1, \dots, s_n$.

$\square$

Osservazione 6. Dalle id. di Newton si evince che ogni funzione simmetrica elementare può essere scritta in termini di somme di potenze e viceversa.
infatti:
Dalle id. di Newton con $k = 2$ (dato che $s_1 = \sigma_1$):

$$s_2 = \sigma_1^2 - 2\sigma_2 \iff \sigma_2 = \frac{1}{2}(s_1^2 - s_2)$$

Dalle id. di Newton con $k = 3$:

$$s_3 - \sigma_1 s_2 + \sigma_2 s_1 - 3\sigma_3 = 0$$

$$\Big\downarrow \text{utilizzando quanto ottenuto prima e } s_1 = \sigma_1 \text{ ottengo}$$

$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \iff \sigma_3 = \frac{1}{6}(s_1^3 - 3s_1s_2 + 2s_3)$$

Iterando il procedimento si può ottenere il risultato $\forall k$ e applicando le trasformazioni per $s_1, s_2, \dots$ trovate ad un polinomio in $s_1, s_2, \dots, s_n$ lo trasformo in in polinomio in $\sigma_1, \sigma_2, \dots, \sigma_n$ e viceversa applicando le trasformazioni trovate per $\sigma_1, \sigma_2, \dots$ ad un polinomio in $\sigma_1, \sigma_2, \dots, \sigma_n$ lo trasformo in un polinomio in $s_1, s_2, \dots, s_n$.

2.2 Discriminante

Proposizione 2.2.1. *Dato un polinomio* $f(X) = X^n + a_1X^{n-1} + a_2X^{n-2} + \dots + a_n$ *monico* $\in k[X]$ *e* $x_1, \dots, x_n$ *le sue radici in* $\overline{k} \supseteq k$*, c'è una relazione lineare tra i suoi coefficienti* $a_1, \dots, a_n$ *e le funzioni simmetriche elementari* $\sigma_1, \dots, \sigma_n$*, più esattamente* $a_i = (-1)^i\sigma_i$ $\forall i$*, ovvero,*

$$f(X) = (X - x_1)(X - x_2)\dots(X - x_n) = \prod_{i=1}^{n}(X - x_i)$$

è equivalente a

$$f(X) = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \ldots + (-1)^n \sigma_n = \sum_{i=0}^{n} (-1)^i \sigma_i X^{n-i}$$

Dimostrazione. E' facile dimostrare l'enunciato procedendo per induzione su n. □

Definizione 2.1. *Il* **discriminante di** f *è così definito:*

$$D(f) = \prod_{i \neq j} (\alpha_i - \alpha_j) \qquad \textit{oppure} \qquad D(f) = \prod_{i<j} -1 \cdot (\alpha_i - \alpha_j)^2$$

dove α_i sono le radici di f.

Proposizione 2.2.2.
Dato un polinomio $f(X) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \ldots + a_n$ monico $\in k[X]$ e $x_1, \ldots, x_n$ le sue radici in $\overline{k} \supseteq k$, osserviamo che:

1. *Il polinomio ha radici multiple sse $D(f)$ è nullo.*
2. *$D(f)$ è polinomio in $a_1, \ldots, a_n$.*
3. *Sia nel caso di $n = 2$ che $n = 3$, $D(f)$ è proprio il discriminante delle equazioni di secondo e terzo grado.*

Dimostrazione.

1. La dimostrazione è banale.
2. Dato che $D(f)$ è simmetrico ed è in funzione di $x_1, \ldots, x_n$, allora per il teorema fondamentale dei polinomi simmetrici, lo posso scrivere nelle funzioni simmetriche elementari $\sigma_1, \ldots, \sigma_n$.
   Ma data la proposizione precedente, nel caso di un polinomio monico come f, c'è una relazione lineare tra i $\sigma_1, \ldots, \sigma_n$ e i coefficenti del polinomio $a_1, \ldots, a_n$, allora $D(f)$ lo si può scrivere in funzione di quest'ultimi.
3. - Nel caso $n = 2$ attraverso l'algoritmo derivato dal teorema fondamentale dei polinomi simmetrici e la sostituzione dei $\sigma_1, \ldots, \sigma_n$ con i $a_1, \ldots, a_n$, otteniamo

     $$D(f) = a_1^2 - 4a_2$$

     che è esattamente il discriminante dell'equazione di secondo grado.

- Nel caso $n = 3$ con lo stesso procedimento si ottiene

$$D(f) = 27a_3^2 - 18a_1a_2a_3 + 4a_2^3 + 4a_1^3a_3 - a_1^2a_2^2.$$

E se f attraverso una traslazione lo riportiamo nella forma $f(X) = X^3 + a_2X + a_3$, allora $D(f)$ rimane

$$D(f) = 27a_3^2 + 4a_2^3.$$

che è ciò che compare sotto radice (nella forma $\frac{a_3^2}{4} + \frac{a_2^3}{27}$) nelle formule di Cardano per la risoluzione dell'equazione di terzo grado.

$\square$

Proposizione 2.2.3.
Dato un polinomio f simmetrico omogeneo di grado totale k, osserviamo che:

1. *f può essere scritto come combinazione lineare dei polinomi della forma $\sigma_1^{i_1}\sigma_2^{i_2}\ldots\sigma_n^{i_n}$ dove $k = i_1 + 2i_2 + \ldots + ni_n$.*
2. *Sia m il massimo grado di x_1 che appare in f (per la simmetria m è il massimo grado in f di qualsiasi variabile). Se $\sigma_1^{i_1}\sigma_2^{i_2}\ldots\sigma_n^{i_n}$ appare nell'espressione di f allora si ha che $i_1 + i_2 + \ldots + i_n \leq m$*

Dimostrazione.

1. Dato f è simmetrico per teorema fondamentale dei polinomi simmetrici, lo posso scrivere in funzione di $\sigma_1, \ldots, \sigma_n$.
   Dato f è anche omogeneo di grado totale k, allora i termini che lo compongono devono essere tutti di grado k.
   Osservo infine che σ_i è di grado i, quindi $\sigma_j^{i_j}$ è di grado $j \cdot i_j$. Quindi $\sigma_1^{i_1}\sigma_2^{i_2}\ldots\sigma_n^{i_n}$ è di grado $1 \cdot i_1 + 2 \cdot i_2 + \ldots + n \cdot i_n = k$.
2. Consideriamo il monomio $\sigma_1^{j_1}\sigma_2^{j_2}\ldots\sigma_k^{j_k}$ che contiene il massimo grado di una qualunque variabile x_i. In σ_1 x_i ha esponente massimo esattamente j_1, in σ_2 ha esponente massimo esattamente j_2 e così via ,quindi in $\sigma_1^{j_1}\sigma_2^{j_2}\ldots\sigma_k^{j_k}$, x_i avrà esponente massimo $j_1 + j_2 + \ldots + j_k = m$.
   Quindi considerando un qualunque monomio $\sigma_1^{i_1}\sigma_2^{i_2}\ldots\sigma_n^{i_n}$ che compare in f e che non contenga necessariamente il massimo grado di x_i si avrà $i_1 + i_2 + \ldots + i_n \leq m$. $\square$

2.3 Funzione generatrice

Definizione 2.2.
Definisco P_k= # funzioni simmetriche indipendenti in $x_1, \dots, x_n$ variabili di grado k. E

$$P(t) = \sum_{i \geq 0} P_i t^i = P_0 + P_1 t + P_2 t^2 + \dots$$

la **funzione generatrice dei** P_k*, con t nuova variabile.*

Osservo allora che,

Osservazione 7.
Un polinomio simmetrico omogeneo in n variabili $x_1, \dots, x_n$ di grado 1, per la proposizione precedente, può essere scritto solo in funzione di $\sigma_1 \Rightarrow P_1 = 1$.
Se è di grado 2 in almeno 2 variabili $\Rightarrow$ può essere scritto in funzione di σ_1^2 e σ_2, infatti σ_1^2 è di grado $1 \cdot 2 = 2$ e σ_2 è di grado $2 \cdot 1 = 2 \Rightarrow P_2 = 2$.
Se è invece di grado 3 in almeno 3 variabili $\Rightarrow$ può essere scritto in funzione di σ_1^3, $\sigma_1\sigma_2$ e σ_3, infatti σ_1^3 è di grado $1 \cdot 3 = 3$, $\sigma_1\sigma_2$ è di grado $1 \cdot 1 + 2 \cdot 1 = 3$ e σ_3 è di grado $3 \cdot 1 = 3 \Rightarrow P_3 = 3$.

Vediamo ora il calcolo di P_k, e consideriamo per comodità, polinomi in infinite variabili:

Proposizione 2.3.1.

$$P(t) = \sum_{i \geq 0} P_i t^i = P_0 + P_1 t + P_2 t^2 + \dots = \prod_{i \geq 1} \frac{1}{1 - t^i}$$

Dimostrazione.
$\prod_{i \geq 1} \frac{1}{1 - t^i} = \frac{1}{1-t} \cdot \frac{1}{1-t^2} \cdot \frac{1}{1-t^3} \cdot \dots =$ per definizione di serie geometrica

$$= (\sum_i t^i)(\sum_j t^{2j})(\sum_k t^{3k}) \dots =$$
$$= (1 + t + t^2 + t^3 + \dots)(1 + t^{1 \cdot 2} + t^{2 \cdot 2} + t^{3 \cdot 2} + \dots)(1 + t^{1 \cdot 3} + t^{2 \cdot 3} + t^{3 \cdot 3} + \dots) \dots =$$
$$= 1 + t + (1+1)t^2 + (1+1+1))t^3 + (1+1+1+1+1)t^4 + \dots =$$
$$= 1 + t + 2t^2 + 3t^3 + 5t^4 + \dots$$

□

Osservazione 8. Osserviamo infine che la proposizione precedente ci permette di stabilire il valore di un P_k arbitrario, che rappresenta esattamente il numero di partizioni dell'intero k.

Bibliografia

[1] David Cox, John Little, Donald O'Shea, *IDEALS,VARIETIES, AND ALGORITHMS*, 3 ed., Springer, 2007.

[2] I.G.MacDonald, *SYMMETRIC FUNCTIONS AND HALL POLYNOMIALS*, Clarendon press · Oxford, 1979.

[3] Wikipedia -

W *http://it.wikipedia.org/wiki/Identità_di_Newton*

W *http://it.wikipedia.org/wiki/Equazione_cubica*