Lezione 8

Prerequisiti: Radici di polinomi. Campi di spezzamento. Lezione 5.

Risultanti e discriminanti.

In questa sezione studiamo criteri effettivi per stabilire quando due polinomi a coefficienti in un campo hanno radici comuni.

Sia F un campo.

Proposizione 8.1 I polinomi non nulli $f(x), g(x) \in F[x]$ hanno una radice comune in un'estensione algebricamente chiusa K di F se e solo se esistono polinomi non nulli $r(x), s(x) \in F[x]$ con $\deg r(x) < \deg g(x), \deg s(x) < \deg f(x)$ tali che

$$r(x)f(x) + s(x)g(x) = 0 \qquad (1)$$

Dimostrazione: Per il Teorema di Ruffini, $f(x), g(x)$ hanno una radice comune in K se e solo se $\mathrm{MCD}(f(x), g(x)) \neq 1$ in $K[x]$, ovvero, in base al Lemma 5.3, se e solo se $\mathrm{MCD}(f(x), g(x)) \neq 1$ in $F[x]$. Supponiamo che $f(x), g(x)$ abbiano una radice comune e sia

$$\mathrm{MCD}(f(x), g(x)) = h(x), \qquad h(x) \in F[x], \qquad h(x) \text{ non costante.}$$

Allora $r(x) = \dfrac{g(x)}{h(x)}$, $\quad s(x) = -\dfrac{f(x)}{h(x)}$ sono polinomi verificanti l'enunciato della proposizione. Viceversa, supponiamo che $f(x), g(x)$ non abbiano radici comuni. Allora $f(x), g(x)$ sono coprimi in $F[x]$. Se valesse la (1), per la proprietà di fattorizzazione unica in $F[x]$, necessariamente $g(x)$ dividerebbe $r(x)$, contro l'ipotesi sui gradi. □

Nelle ipotesi della Proposizione 8.1, sia $n = \deg f(x)$, $m = \deg g(x)$. Il primo membro della (1) è una combinazione lineare (evidentemente nulla) dei termini

$$f(x), xf(x), x^2 f(x), \ldots, x^{m-1} f(x), \quad g(x), xg(x), x^2 g(x), \ldots, x^{n-1} g(x), \qquad (2)$$

a coefficienti in F (evidentemente non tutti nulli). Quindi l'esistenza della (1) equivale alla lineare dipendenza di tali termini su F. Se

$$f(x) \quad = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1} + a_n x^n,$$

allora

$$
\begin{aligned}
xf(x) &= a_0x + a_1x^2 + a_2x^3 + \cdots + a_{n-2}x^{n-1} + a_{n-1}x^n + a_nx^{n+1} \\
x^2f(x) &= a_0x^2 + a_1x^3 + a_2x^4 + \cdots + a_{n-2}x^n + a_{n-1}x^{n+1} + a_nx^{n+2} \\
&\vdots \\
x^{m-1}f(x) &= a_0x^{m-1} + a_1x^m + a_2x^{m+1} + \cdots + a_{n-2}x^{n+m-3} + a_{n-1}x^{n+m-2} + a_nx^{n+m-1}
\end{aligned}
$$

Se

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{m-2}x^{m-2} + b_{m-1}x^{m-1} + b_mx^m,$$

allora

$$
\begin{aligned}
xg(x) &= b_0x + b_1x^2 + b_2x^3 + \cdots + b_{m-2}x^{m-1} + b_{m-1}x^m + b_mx^{m+1} \\
x^2g(x) &= b_0x^2 + b_1x^3 + b_2x^4 + \cdots + b_{m-2}x^m + b_{m-1}x^{m+1} + b_mx^{m+2} \\
&\vdots \\
x^{n-1}g(x) &= b_0x^{n-1} + b_1x^n + b_2x^{n+1} + \cdots + b_{m-2}x^{m+n-3} + b_{m-1}x^{m+n-2} + b_mx^{m+n-1}
\end{aligned}
$$

Questi sono tutti elementi dello spazio vettoriale dei polinomi a coefficienti in F aventi grado al più $n+m-1$, che è isomorfo a F^{n+m} mediante

$$u_0 + u_1x + \cdots + u_{n+m-1}x^{n+m-1} \mapsto (u_0, u_1, \ldots, u_{n+m-1})$$

Quindi la condizione di lineare dipendenza dei termini (2) equivale all'annullarsi del determinante della seguente matrice $(n+m)\times(n+m)$, detta *matrice di Sylvester:*

$$
S(f,g) = \begin{pmatrix}
a_0 & a_1 & a_2 & \cdots & \cdots & a_n & 0 & \cdots & \cdots & \cdots & 0 \\
0 & a_0 & a_1 & \cdots & \cdots & \cdots & a_n & 0 & \cdots & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & a_0 & \cdots & \cdots & \cdots & \cdots & a_n \\
\\
b_0 & b_1 & b_2 & \cdots & \cdots & \cdots & b_m & 0 & \cdots & \cdots & 0 \\
0 & b_0 & b_1 & \cdots & \cdots & \cdots & \cdots & b_m & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & 0 & b_0 & \cdots & \cdots & \cdots & b_m
\end{pmatrix}
\begin{matrix}
\left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} m \text{ righe} \\
\\
\left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} n \text{ righe}
\end{matrix}
$$

Per maggiore chiarezza, scriviamo la matrice nel caso particolare in cui n=2, m=3:

$$\begin{pmatrix} a_0 & a_1 & a_2 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 \end{pmatrix}$$

Definizione 8.2 Il determinante di $S(f,g)$ si dice *risultante di* $f(x), g(x)$. Lo si denota anche $R(f,g)$.

Dalle considerazioni appena effettuate, segue

Proposizione 8.3 I polinomi non nulli $f(x), g(x) \in F[x]$ hanno una radice comune in un'estensione algebricamente chiusa di F se e solo se $R(f,g) = 0$.

Per esempio, siano $f(x) = 3x^2 + x - 2$, $g(x) = x + 1$. Allora

$$R(f,g) = \det\begin{pmatrix} -2 & 1 & 3 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = -2-(1-3) = 0\,.$$

In effetti, $f(x), g(x)$ hanno in comune la radice -1.

Abbiamo definito il risultante in termini dei coefficienti dei polinomi. Ne diamo ora, senza dimostrazione, una rappresentazione in termini delle loro radici.

****Proposizione 8.4** Siano $f(x), g(x) \in F[x]$ non nulli, sia $\deg f(x) = n, \deg g(x) = m$, e siano a e b i coefficienti direttori di $f(x)$ e $g(x)$ rispettivamente. Siano, inoltre, $\alpha_1,\ldots,\alpha_n$ le radici di $f(x)$ e $\beta_1,\ldots,\beta_m$ le radici di $g(x)$ in un'estensione K algebricamente chiusa di F, contate con le rispettive molteplicità. Allora

$$R(f,g) = a^m b^n \prod_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} (\alpha_i - \beta_j)\,.$$

Dimostrazione: [G], Proposition 5.2.4.

Osservazione 8.5 Dalla Proposizione 8.4 segue che $R(f,g)$ è un'espressione polinomiale simmetrica di $\alpha_1,\ldots,\alpha_n$ a coefficienti in $F(\beta_1,\ldots,\beta_m)$; in base al Corollario 7.12 essa è quindi un'espressione polinomiale, a coefficienti in $F(\beta_1,\ldots,\beta_m)$, dei coefficienti di $f(x)$. Ma i coefficienti in $F(\beta_1,\ldots,\beta_m)$ sono a loro volta espressioni polinomiali simmetriche in $\beta_1,\ldots,\beta_m$ (a coefficienti in F) e quindi sono espressioni polinomiali dei coefficienti di $g(x)$. Complessivamente, $R(f,g)$ è un'espressione polinomiale, a coefficienti in F, dei coefficienti di $f(x)$ e $g(x)$.

Corollario 8.6 Nelle ipotesi della Proposizione 8.4,

$$R(f,g) = a^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b^n \prod_{j=1}^{m} f(\beta_j).$$

Definizione 8.7 Per ogni polinomio non nullo $f(x) \in F[x]$, di grado $n \geq 2$, e coefficiente direttore a, si dice *discriminante* di $f(x)$

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \frac{1}{a} R(f, f').$$

Dalle Proposizioni 5.4 e 8.3 segue

Proposizione 8.8 Un polinomio $f(x) \in F[x]$, di grado $n \geq 2$, ha, in un suo campo di spezzamento, una radice multipla se e solo se $\Delta(f) = 0$.

Corollario 8.9 Sia $f(x) \in F[x]$ un polinomio di grado $n \geq 2$ e coefficiente direttore a, e siano $\alpha_1, \ldots, \alpha_n$ le sue radici in suo campo di spezzamento su F. Allora, se $n \neq 0$ in F,

$$\Delta(f) = a^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Dimostrazione: Si ha

$$f(x) = a \prod_{i=1}^{n} (x - \alpha_i),$$

quindi

$$f'(x) = a \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} (x - \alpha_j).$$

Si noti che, per ogni i = 1, .., n, α_i annulla tutti gli addendi tranne uno, quello corrispondente all'indice i. Quindi

$$f'(\alpha_i) = a \prod_{\substack{j=1 \\ j \neq i}}^{n} (\alpha_i - \alpha_j)$$

In base al Corollario 8.6 si ha allora

$$R(f, f') = a^{n-1} \prod_{i=1}^{n} f'(\alpha_i) = a^{2n-1} \prod_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} (\alpha_i - \alpha_j)$$

I fattori sono complessivamente $n(n-1)$, la metà di essi sono del tipo $(\alpha_i - \alpha_j)$ con $i>j$. Immaginiamo di cambiare il segno a tutti questi ultimi. Ciò significa moltiplicare il prodotto per $(-1)^{\frac{n(n-1)}{2}}$. Nel prodotto, ogni fattore $(\alpha_k - \alpha_h)$ (con $k < h$) compare una volta per $i = k$, una volta per $i = h$, nella forma: $(\alpha_h - \alpha_k)$. Dopo il cambio di segno i due fattori saranno uguali. Dunque

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} a^{2n-1} \prod_{i=1}^{n} \prod_{i<j\leq n} (\alpha_i - \alpha_j)^2,$$

da cui la formula voluta. □

Esempi 8.10

a) Sia $f(x) = ax^2 + bx + c$ un polinomio di grado 2. Allora $f'(x) = 2ax + b$, e quindi

$$\Delta(f) = -\frac{1}{a}\det\begin{pmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{pmatrix} = -\frac{1}{a}(4a^2c - ab^2) = b^2 - 4ac$$

b) Sia $f(x) = x^3 + px + q$. Allora $f'(x) = 3x^2 + p$, e quindi

$$\Delta(f) = -\det\begin{pmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ 0 & p & 0 & 3 & 0 \\ 0 & 0 & p & 0 & 3 \end{pmatrix} = -4p^3 - 27q^2$$

Osservazione 8.11 Il ruolo del discriminante di un polinomio reale quadratico è ben noto: il suo segno determina il numero delle radici reali del polinomio. Vediamo ora come il discriminante svolga un ruolo analogo per i polinomi reali cubici.

Sia $f(x)$ un polinomio reale di grado 3, e siano $\alpha_1, \alpha_2, \alpha_3$ le sue radici complesse (sappiamo che una è reale, sia essa α_1). Supponiamo, per semplicità, che $f(x)$ sia monico. Allora esso ammette la decomposizione

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

ed il suo discriminante è

$$\Delta(f) = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_1 - \alpha_3)^2$$

Esso è prodotto di

$$\Delta_{12} = (\alpha_1 - \alpha_2)^2, \quad \Delta_{23} = (\alpha_2 - \alpha_3)^2, \quad \Delta_{13} = (\alpha_1 - \alpha_3)^2,$$

che sono i discriminanti dei suoi fattori monici di grado 2. Si hanno allora i seguenti casi:

1. Se $\Delta(f) = 0$, allora f ha una radice multipla. Questa è necessariamente reale. Dunque f ha una radice reale tripla, oppure una radice reale semplice ed una doppia.

2. Se $\Delta(f) < 0$, allora *f* ha una sola radice reale, e due radici non reali distinte.
3. Se $\Delta(f) > 0$, allora *f* ha due radici reali distinte, e nessuna radice doppia. Quindi *f* ha tre radici reali distinte.

L'espressione del discriminante data nel Corollario 8.9 può essere sostituita da una formula più agevole, basata sul calcolo di un determinante:

Proposizione 8.12 Sia $n \geq 2$, e siano $\alpha_1,...,\alpha_n \in F$. Allora

$$\prod_{\substack{i=1 \\ i>j}}^{n} (\alpha_i - \alpha_j) = \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

Questo determinante si chiama *determinante di Vandermonde* di $\alpha_1,...,\alpha_n$. Lo si denota con $\Delta(\alpha_1,...,\alpha_n)$.

Dimostrazione: Osserviamo preliminarmente che è sufficiente supporre che gli elementi α_i siano a due distinti; in tal caso il primo membro dell'uguaglianza da provare è non nullo. Procediamo per induzione su $n \geq 2$. Il caso $n = 2$ è ovvio. Sia allora $n > 2$, e supponiamo la tesi vera per $n - 1$. Sia

$$f(x) = \det \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} & x \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 & x^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \vdots & \alpha_{n-1}^{n-2} & x^{n-2} \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \vdots & \alpha_{n-1}^{n-1} & x^{n-1} \end{pmatrix}.$$

Allora $f(x)$ è un polinomio a coefficienti in *F*, di grado al più n-1, avente radici $\alpha_1,...,\alpha_{n-1}$: infatti sostituendo ciascuno di questi elementi ad x si ottiene una matrice avente due colonne uguali. Il coefficiente del termine di $f(x)$ avente grado n-1 è $C = \Delta(\alpha_1,...,\alpha_{n-1})$, che per l'ipotesi induttiva è non nullo. Si ha quindi

$$f(x) = C\prod_{j=1}^{n-1}(x - \alpha_j),$$

e, applicando ancora l'ipotesi induttiva:

$$\Delta(\alpha_1,...,\alpha_n) = f(\alpha_n) = \Delta(\alpha_1,...,\alpha_{n-1})\prod_{j=1}^{n-1}(\alpha_n - \alpha_j) = \prod_{\substack{i=1 \\ i>j}}^{n-1}(\alpha_i - \alpha_j)\prod_{j=1}^{n-1}(\alpha_n - \alpha_j),$$

da cui la tesi. □

Dal Corollario 8.9 e dalla Proposizione 8.12 segue subito:

Corollario 8.13 Sia $f(x) \in F[x]$ un polinomio non nullo di grado $n \geq 2$, e coefficiente direttore a, e siano $\alpha_1,...,\alpha_n$ le sue radici in suo campo di spezzamento su F. Allora, se $n \neq 0$ in F,

$$\Delta(f) = a^{2n-2}\Delta(\alpha_1,...,\alpha_n)^2 .$$

Osservazione 8.14 Si noti anzitutto che se il polinomio $f(x)$ è monico, la precedente uguaglianza è vera senza ipotesi aggiuntive sulla caratteristica. In tal caso il discriminante di $f(x)$ è una funzione delle sue radici. Per questo motivo ha senso parlare di *discriminante* di n elementi $\alpha_1,...,\alpha_n \in F$, che è

$$\Delta(\alpha_1,...,\alpha_n)^2$$

Si noti che questa definizione è indipendente dall'ordine in cui vengono considerati tali elementi (mentre $\Delta(\alpha_1,...,\alpha_n)$ è definito "a meno del segno"). Questa nozione sarà utile in seguito.