Il discriminante polinomiale e la formula di Cardano

di Gabriel Antonio Videtta

Nota. Per K, L ed F si intenderanno sempre dei campi. Se non espressamente detto, si sottintenderà anche che $K \subseteq L$, F, e che L ed F sono estensioni costruite su K. Per $[L : K]$ si intenderà $\dim_K L$, ossia la dimensione di L come K-spazio vettoriale. Per scopi didattici, si considerano solamente campi perfetti, e dunque estensioni che sono sempre separabili, purché non esplicitamente detto diversamente.

In questo documento si illustra il *discriminante polinomiale* e le sue principali applicazioni nella teoria di Galois.

Definizione (discriminante polinomiale)**.** Sia $p \in K[x]$. Se $\deg p = n$ e a_1, ..., $a_n \in \overline{K}$ sono le radici di p, si definisce il **discriminante polinomiale** $\operatorname{disc} p$ in modo tale che:

$$\operatorname{disc} p = \prod_{i<j} (a_i - a_j)^2 \in K[a_1, \ldots, a_n].$$

Osservazione (radici multiple di p e formule di Viète)**.** Si verifica facilmente che p ha radice multiple se e solo se $\operatorname{disc} p = 0$. Altrettanto semplicemente si verifica che $\operatorname{disc} p$ è un polinomio simmetrico in a_1, ..., a_n. Pertanto, per il Teorema fondamentale dei polinomi simmetrici, $\operatorname{disc} p$ può esprimersi[1] come elemento di $K[e_1, \ldots, e_n]$, dove $e_i := e_i(a_1, \ldots, a_n)$ è il polinomio simmetrico elementare negli a_i. Per le formule di Viète, i vari e_i possono esprimersi tramite i coefficienti c_i di $p(x)$ secondo la seguente relazione:

$$c_i = (-1)^{n-i} a e_{n-i},$$

dove si pone $e_0 := 1$. Inoltre, l'annullamento di $\operatorname{disc} p$ è indipendente dal coefficiente di testa del polinomio, dal momento che polinomi associati condividono le stesse radici.

Per esempio, per $n = 2$, se $p(x) = ax^2 + bx + c$ con $a \neq 0$, vale che:

$$\operatorname{disc} p(x) = \prod_{i<j} (a_i - a_j)^2 = a_1^2 + a_2^2 - 2a_i a_j = (a_1 + a_2)^2 - 4a_i a_j = e_1^2 - 4e_2,$$

[1] Un algoritmo per calcolare efficacemente un'espressione di $\operatorname{disc} p$ in questo senso è reperibile su `https://git.phc.dm.unipi.it/g.videtta/scritti/src/branch/main/Algebra/Notebook/1.%20Algoritmo%20di%20rappresentazione%20dei%20polinomi%20simmetrici`.

e dunque, poiché $b = c_1 = (-1)^{2-1}ae_{2-1} = -ae_1$ e $c = c_0 = (-1)^2 ae_2 = ae_2$, vale che[2]:

$$\operatorname{disc} p(x) = \left(-\frac{b}{a}\right)^2 - 4\frac{c}{a} = \frac{b^2}{a^2} - 4\frac{ac}{a^2} = \frac{b^2 - 4ac}{a^2} = \frac{\Delta}{a^2},$$

dove Δ è l'usuale discriminante delle equazioni di secondo grado. Pertanto, poiché[3] $a \neq 0$, p ha radici multiple se e solo se $\operatorname{disc} p = 0$, e quindi se e solo se $\Delta = 0$.

Osservazione (utilizzo della matrice di Vandermonde)**.** Un'espressione di $\operatorname{disc} p$ può anche essere calcolata attraverso le matrici di Vandermonde. Infatti, se M è la matrice di Vandermonde di a_1, ..., a_n radici di p, vale che:

$$M = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix},$$

e quindi:

$$\det(M) = \prod_{i<j}(a_i - a_j).$$

Pertanto vale che:

$$\det(M^2) = \det(MM^T) = \prod_{i<j}(a_i - a_j)^2 = \operatorname{disc} p(x).$$

Osservazione (invarianza di $\operatorname{disc} p$ e trasformazione di Tschirnhaus)**.** Si osserva facilmente che $\operatorname{disc} p$ è invariante per traslazioni. Infatti, se si considera $p(x + a)$ con $a \in K$ e a_1, ..., $a_n \in \overline{K}$ sono radici di $p(x)$, le radici di $p(x+a)$ sono $a_1 - a$, ..., $a_n - a$. Pertanto vale che:

$$\operatorname{disc} p(x + a) = \prod_{i<j}(a_1 - a - a_2 + a)^2 = \prod_{i<j}(a_1 - a_2)^2 = \operatorname{disc} p(x).$$

Sia ora $p(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$. Dalle formule di Viète, se a_1, ..., a_n sono le radici di $p(x)$, vale che:

$$c_{n-1} = -c_n(a_1 + \ldots + a_n) \implies \left(a_1 + \frac{c_{n-1}}{nc_n}\right) + \ldots + \left(a_n + \frac{c_{n-1}}{nc_n}\right) = 0.$$

Si può allora considerare la *trasformazione di Tschirnhaus* $\tau : K[x] \to K[x]$ tale per cui $p(x) \overset{\tau}{\mapsto} p(x + \frac{c_{n-1}}{nc_n})$, $\tau(p)$ ha come radici esattamente i vari $a_i + \frac{c_{n-1}}{nc_n}$, e quindi, sempre per

[2]In generale, compare sempre un termine a^{2n-2} al denominatore di $\operatorname{disc} p(x)$. Pertanto, in letteratura si definisce $\operatorname{disc} p(x)$ anche come il prodotto tra a^{2n-2} e il discriminante qui definito. In tal caso, il discriminante di un polinomio di secondo grado è esattamente Δ.

[3]Per quanto detto prima, a non svolge alcun ruolo nel determinare se p ha radici multiple.

le formule di Viète, è tale per cui il coefficiente di x^{n-1} è nullo. Dal momento che $\operatorname{disc} p$ è invariante per traslazione, calcolare $\operatorname{disc} \tau(p)$ può risultare più semplice e dunque più efficiente. In letteratura, applicare la trasformazione di Tschirnhaus su un polinomio si dice "deprimerlo", e un polinomio tale per cui $c_{n-1} = 0$ è detto *polinomio depresso*. Si osserva facilmente che deprimere un polinomio depresso non ha alcun effetto e la mappa restituisce il polinomio depresso di partenza. In particolare vale che $\tau^2 = \tau$.

Osservazione. Sia $p \in K[x]$ di grado n e siano $a_1, \ldots, a_n$ le sue radici. Se allora $\sigma \in S(\{a_1, \ldots, a_n\})$, vale che:

$$\prod_{i<j}(\sigma(a_i) - \sigma(a_j)) = \prod_{i<j} \frac{\sigma(a_i) - \sigma(a_j)}{a_i - a_j} \prod_{i<j}(a_i - a_j) = \operatorname{sgn}(\sigma) \prod_{i<j}(a_i - a_j),$$

dove si identifica tale segno come $\operatorname{sgn}(\varphi(\sigma))$, dove φ è l'azione di del gruppo di Galois di p sulle radici di p. Pertanto, se p è irriducibile e separabile, e $\sigma \in G := \operatorname{Gal}(L/K)$ dove $L = K(a_1, \ldots, a_n)$, vale che:

$$\sigma(\operatorname{disc} p) = \operatorname{disc} p,$$

e quindi $\operatorname{disc} p \in L^G = K$.

L'utilità del discriminante polinomiale per la teoria di Galois è sancita dalla seguente proposizione:

Proposizione. Sia p un polinomio irriducibile e separabile di grado n. Allora, se L è il suo campo di spezzamento su K, $\operatorname{Gal}\left(L/K\right) \hookrightarrow A_n$ se e solo se $\operatorname{disc} p$ è un quadrato[4] in K.

Dimostrazione. Sia $G := \operatorname{Gal}\left(L/K\right)$ e sia $\sigma \in G$. Allora $G \hookrightarrow A_n$ se e solo se $\operatorname{sgn}(\sigma) = 1$. Si consideri la seguente identità:

$$\sigma\left(\prod_{i<j}(a_i - a_j)\right) = \operatorname{sgn}(\sigma) \prod_{i<j}(a_i - a_j).$$

Poiché gli elementi fissati da tutte le $\sigma \in G$ sono esattamente gli elementi di K, se $G \hookrightarrow A_n$, $\operatorname{sgn}(\sigma)$ è 1, e quindi $\left(\prod_{i<j}(a_i - a_j)\right) \in K$. Pertanto, $\operatorname{disc} p$ è un quadrato in K, essendo $\left(\prod_{i<j}(a_i - a_j)\right)$ una sua radice quadrata. Analogamente, se $\operatorname{disc} p$ è un quadrato in K, $\left(\prod_{i<j}(a_i - a_j)\right) \in K$, e quindi $\operatorname{sgn}(\sigma) = 1$, da cui la tesi. □

Osservazione (discriminanti polinomiali per $n \leq 3$)**.** Si illustrano i discriminanti polinomiali per alcune specie di polinomio:

- se $p(x) = x - a$, $\operatorname{disc} p(x) = 1$, essendo il prodotto vuoto;

[4]Questa proposizione è ancora vera utilizzando il discriminante moltiplicato per a^{2n-2}, e quindi vale ancora per la definizione alternativa di discriminante.

- se $p(x) = ax^2 + bx + c$, $\operatorname{disc} p = \frac{\Delta}{a^2}$;
- se $p(x) = x^3 + px + q$, $\operatorname{disc} p = -4p^3 - 27q^2$.

Osservazione (classificazione dei gruppi di Galois per $\deg p = 3$)**.** Sia $p \in K[x]$ un polinomio di grado 3 irriducibile e separabile. Sia L il campo di spezzamento di p su K e $G := \operatorname{Gal}\left(L/K\right)$. Si osserva che 3 divide $|G|$ dal momento che, se α è una radice di p, $[K(\alpha) : K] = 3 \mid [L : K] = |G|$. Allora, se $\operatorname{disc} p$ è un quadrato in K, $G \hookrightarrow A_3$, e dunque, per cardinalità, $G \cong A_3$. Se invece $\operatorname{disc} p$ non è quadrato in K, G ha cardinalità 6, e dunque G è obbligatoriamente isomorfo a S_3 stesso.

Pertanto vale che:

$$\operatorname{Gal}\left(L/K\right) \cong \begin{cases} A_3 & \text{se } \operatorname{disc} p \text{ è quadrato in } K, \\ S_3 & \text{altrimenti.} \end{cases}$$

Si illustra adesso il metodo risolutivo delle equazioni di terzo grado, tramite la cosiddetta *formula di Cardano*. Innanzitutto, si assume che $p(x)$ sia un polinomio *depresso* di terzo grado della forma $x^3 + px + q$ (altrimenti è sufficiente applicare la trasformazione di Tschirnhaus a $p(x)$, ricavare le soluzioni e poi tornare indietro).

Sia $x = u + v$. Allora $p(u+v) = u^3 + v^3 + 3u^2v + 3uv^2 + p(u+v) + q = (u^3 + v^3 + q) + (3uv + p)(u + v)$. Si pone allora il seguente sistema di equazioni:

$$\begin{cases} u^3 + v^3 = -q, \\ uv = -\frac{p}{3} \implies u^3v^3 = -\frac{p^3}{27}. \end{cases}$$

Infatti, se il precedente sistema ammette soluzione, $p(x) = p(u+v)$ si annulla e $u + v$ è soluzione.

Dal momento che abbiamo sia la somma che il prodotto di u^3 e v^3, è possibile ricavare queste due quantità risolvendo l'equazione di secondo grado associata:

$$0 = y^2 - (u^3 + v^3)y + u^3v^3 = y^2 + qy - \frac{p^3}{27}.$$

Una volta ottenuti sia u^3 che v^3, prendendone la radice cubica, si otterrà dunque una radice di $p(x)$. In particolare varrà che:

$$y_{1,2} = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

e quindi:

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

Le altre due soluzioni di $p(x)$ si possono poi computare facilmente riducendosi a considerare il polinomio $p(x)/(x - \alpha)$, dove α è la soluzione ottenuta.