Capitolo 5

Monodromia

In questo capitolo consideriamo il gruppo di Galois di polinomi a un parametro:

$$f(w,z) = a_0(z)w^n + a_1(z)w^{n-1} + \cdots + a_n(z) \tag{5.1}$$

dove z è una indeterminata (parametro), e i coefficienti $a_i(z)$ sono funzioni razionali (polinomi) in z a coefficienti razionali. Il polinomio (5.1) è quindi un polinomio sul campo delle funzioni razionali $Q(z)$, e il suo gruppo di Galois G è il gruppo delle permutazioni delle radici $w_1, w_2, \ldots, w_n$ che mutano relazioni a coefficienti in $Q(z)$ tra queste radici ancora in relazioni. Se $C(z)$ è il campo delle funzioni razionali a coefficienti complessi, il gruppo di Galois di $f(w,z)$ su $C(z)$ è il gruppo delle permutazioni delle radici $w_1, w_2, \ldots, w_n$ che mutano relazioni a coefficienti in $C(z)$ tra queste radici ancora in relazioni. Quest'ultimo è allora un sottogruppo H di G, che prende il nome di *gruppo di monodromia* del polinomio (vedremo in seguito il motivo di questa denominazione).

Esempio. Il polinomio su $Q(z)$:

$$f(w,z) = w^2 - 2z^2,$$

ha due radici, $w_1 = \sqrt{2}z$, $w_2 = -\sqrt{2}z$, che non appartengono a $Q(z)$ (per la presenza di $\sqrt{2}$). Il gruppo di Galois G non è dunque il gruppo identico, e pertanto è di ordine 2. D'altra parte, le due radici appartengono a $C(z)$, e dunque il gruppo di monodromia H è l'identità.

5.1 Teorema. *Il gruppo di monodromia H di un polinomio è un sottogruppo normale del gruppo di Galois G.*

Dim. Sia $f(w,z)$ un polinomio come in (5.1), φ una funzione tale che $G_\varphi = H$. Allora $\varphi \in C(z)$, cioè φ è una funzione razionale delle radici w_i che è inoltre una funzione razionale di z (a coefficienti eventualmente irrazionali), che possiamo supporre polinomiale in z:

$$\varphi = \varphi(w_1, w_2, \ldots, w_n) = \alpha_0 z^m + \alpha_1 z^{m-1} + \cdots + \alpha_m. \tag{5.2}$$

φ è radice del polinomio:

$$\prod_{\sigma \in G/H} (w - \varphi^\sigma) = x^s + q_1(z) x^{s-1} + \cdots + q_s(z)$$

con $q_i(z) \in Q(z)$, e dunque:

$$\varphi^s + q_1(z)\varphi^{s-1} + \cdots + q_s(z) = 0.$$

Sostituendo in questa equazione l'espressione (5.2) di φ, otteniamo l'identità:

$$(\alpha_0 z^m + \alpha_1 z^{m-1} + \cdots)^s + q_1(z)(\alpha_0 z^m + \alpha_1 z^{m-1} + \cdots)^{s-1} + \cdots + q_s(z) = 0,$$

che deve valere per ogni valore di z. Sviluppando e ordinando secondo le potenze di z, e imponendo che i coefficienti di queste potenze (che sono polinomi nelle α_i) siano tutti nulli, otteniamo:

$$\begin{array}{lll}
b_0\alpha_0^p & +b_1\alpha_0^{p-1} & + \cdots + b_p = 0, \\
c_0\alpha_1^q & +c_1\alpha_1^{q-1} & + \cdots + c_q = 0, \\
\vdots & \vdots & \vdots \\
d_0\alpha_m^r & +d_1\alpha_1^{r-1} & + \cdots + d_r = 0.
\end{array}$$

Sia $g_0(w) = b_0 w^p + b_1 w^{p-1} + \cdots + b_p$ il polinomio che ammette la radice α_0, e siano $g_1(w), g_2(w), \ldots, g_m(w)$ i polinomi che ammettono rispettivamente le radici $\alpha_1, \alpha_2, \ldots, \alpha_m$. Aggiungendo a $Q(z)$ tutte le radici di questi polinomi $g_i(w)$ viene aggiunto in particolare φ (v. (5.2)), e dunque il gruppo di Galois su questo ampliamento è un sottogruppo K di $H = G_\varphi$. Inoltre, K è ottenuto aggiungendo tutte le radici di un polinomio (il polinomio $g(w) = \prod g_i(w)$), e dunque è un sottogruppo normale di G (Teor. 2.49, i)). E poiché già in $C(z)$ il gruppo di Galois di $f(w, z)$ è H, esso non può ridursi a un sottogruppo di H in un campo contenuto in $C(z)$. Dunque $H = K$. ♢

Se il gruppo H è transitivo, la (5.1) è irriducibile nel senso che non si può spezzare nel prodotto di due fattori $g(w, z)$ e $h(w, z)$ a coefficienti *complessi* (la transitività di G assicura soltanto che una tale decomposizione è impossibile se si richiede $g(w, z)$ e $h(w, z)$ abbiano coefficienti *razionali*).

Esempio. Il polinomio $f(w, z) = w^2 - 2z^2$ su $Q(z)$ dell'esempio precedente ha gruppo di Galois S_2, e dunque transitivo; il polinomio è quindi irriducibile su

$Q(z)$. Il gruppo di monodromia H è invece l'identità, e quindi non transitivo; il polinomio si spezza infatti su $C(z)$:

$$w^2 - 2z^2 = (w - \sqrt{2}z)(w + \sqrt{2}z).$$

Abbiamo definito il gruppo di monodromia in modo puramente algebrico. Tuttavia, il luogo naturale nel quale esso compare è quello della teoria delle funzioni algebriche di una variabile complessa z, cioè delle funzioni w soluzione di un'equazione algebrica $f(w, z) = 0$, dove f è un polinomio come (5.1) e il parametro z una variabile complessa. Le funzioni razionali di z sono le funzioni algebriche soluzioni delle equazioni di primo grado $a_0(z)w - a_1(z) = 0$.

Supponiamo d'ora in poi che $f(w, z)$ sia irriducibile su $Q(z)$ e che il primo coefficiente $a_0(z)$ non sia identicamente nullo. Per ogni fissato valore z_0 di z, $f(w, z_0)$ è un polinomio in w (di grado n, se $a_0(z_0) \neq 0$), che ha in generale n radici distinte e finite:

$$w_1 = w_1(z_0), w_2 = w_2(z_0), \ldots, w_n = w_n(z_0) \tag{5.3}$$

Fanno eccezione alcuni punti z_0, in numero finito, detti punti *critici* (o *singolari*), e sono i seguenti:

i) I punti z che annullano $a_0(z)$, per i quali uno o più radici della (5.1) diventano infinite. (Sostituendo w con $\frac{1}{w}$ si ottiene il polinomio $w^n f(\frac{1}{w}, z) = a_0(z) + a_1(z)w + \cdots + a_n(z)w^n$, il quale per $z = z_0$, e se $a_0(z_0) = 0$, ha la radice $w = 0$; diremo allora che $f(w, z)$ ha la radice $w = \infty$. Si avranno precisamente r radici infinite se $a_0(z_0) = a_1(z_0) = \ldots = a_{r-1}(z_0) = 0$ ma $a_r(z_0) \neq 0$.

ii) I punti z_0 che annullano il discriminante $D(z)$ di $f(w, z)$, e per i quali quindi due o più radici $w_i(z_0)$ coincidono (v. Nota seguente).

Estendiamo ora il piano di z aggiungendo il punto $z = \infty$. Il valore del polinomio in questo punto si definisce come segue. Operiamo la sostituzione $z = z_1^{-1}$; si ha:

$$f(w, z) = f(w, z_1^{-1}) = z_1^{-m} g(w, z_1),$$

dove m è il massimo grado dei polinomi $a_i(z)$. In ogni intorno del valore $z_1 = 0$ (escluso $z_1 = 0$), l'equazione $f(w, z) = 0$ è equivalente alla $g(w, z_1) = 0$. Diremo allora che il polinomio $g(w, 0)$ è ottenuto continuando $f(w, z)$ nel punto $z = \infty$, e che le radici w_i dell'equazione $g(w, 0) = 0$ sono le radici della $f(w, z) = 0$ corrispondenti al valore $z = \infty$.

I punti z_0 del piano di z, ampliato con il punto $z = \infty$, nei quali $f(w, z_0)$ ha meno di n radici distinte (dove, per il punto $z_0 = \infty$, $f(w, 0)$ è sostituito da $g(w, 0)$) sono punti *critici* (o *singolari*) del polinomio $f(w, z)$.

In conclusione, i punti critici (al finito) sono quelli nei quali si annulla il discriminante $D(z)$, mentre $z_0 = \infty$ è un punto critico se $D_1(0) = 0$, dove $D_1(z)$ è il discriminante del polinomio $g(w, z)$.

Nota 1. Ricordiamo che il discriminante di un polinomio è il *risultante* del polinomio e della sua derivata, diviso per il coefficiente del monomio di grado massimo n e con il segno $(-1)^{\frac{n(n-1)}{2}}$. Il risultante di due polinomi $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$ è il determinante R della *matrice di Sylvester* $(n+m)\times(n+m)$:

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & 0 & 0 \\ 0 & a_0 & a_1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_0 \dots & a_{n-1} & a_n \\ b_0 & b_1 & b_2 & \dots & 0 & 0 \\ 0 & b_0 & b_1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & b_0 \dots & b_{n-1} & b_n \end{pmatrix}$$

Il determinante R è un elemento del campo dei coefficienti di f e g. Nel caso di due polinomi $f(w,z)$ e $g(w,z)$ di $C(z)[w]$ il risultante è un polinomio $R(z)$ di $C(z)$. Inoltre $R(z) \equiv 0$ se e solo se f e g hanno un fattore non costante in comune. Ne segue che se $f(w,z)$ è irriducibile $R(z) = R(f,g)$ non può essere identicamente nullo; vi sono cioè solo un numero finito di valori $z = z_0$ per i quali $f(w,z_0)$ e $g(w,z_0)$ hanno una radice in comune $w \in C$. In particolare ciò accade con $g(w,z) = \frac{\partial f(w,z)}{\partial w}$. Se $f(w,z)$ è irriducibile, esso ha allora soltanto un numero finito di radici multiple, i punti critici del polinomio $f(w,z)$.

Esempi. 1. Il polinomio $f(w,z) = w^2 - z$ ha discriminante:

$$D(z) = \det(\begin{pmatrix} 1 & 0 & -z \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}) = -4z.$$

che si annulla per $z_0 = 0$. L'origine è dunque un punto singolare: il polinomio $f(w^2,0) = w^2$ ha le due radici coincidenti $w_1(0) = w_2(0) = 0$. Per tutti gli altri valori finiti z_0 di z le due radici $w_1(z) = \sqrt{z}$ e $w_2(z) = -\sqrt{z}$ sono distinte.

Consideriamo ora il punto $z_0 = \infty$. La sostituzione $z = z_1^{-1}$ porta al polinomio $g(w,z_1) = z_1w^2 - 1$, il cui discriminante :

$$D_1(z_1) = -1 \cdot \frac{1}{z} \cdot \det(\begin{pmatrix} z_1 & 0 & -1 \\ 2z_1 & 0 & 0 \\ 0 & 2z_1 & 0 \end{pmatrix}) = -1 \cdot \frac{1}{z}(-4z_1^2) = 4z_1$$

si annulla per $z_1 = 0$. Qundi $z_0 = \infty$ è un punto critico per $f(w,z)$.

2. Sia $f(w,z) = zw^2 - zw - 1$. Come nel caso precedente si tratta di un polinomio irriducibile su $C(z)$ (se si spezzasse, $f(w,z)$ avrebbe due radici in $C(z)$, ma le due radici di $f(w,z)$ non sono funzioni razionali di z). Si ha $f'(w,z) = \frac{\partial f(w,z)}{\partial w} = 2zw - z$, e $D(z) = z(z+4)$, che ha le radici $z = 0$ e $z = -4$.

Al finito $f(w,z)$ ha i punti singolari $z=0$ e $z=-4$; si verifica che $f(w,-4)$ e $f'(w,-4)$ hanno in comune la radice $\frac{1}{2}$. Con la sostituzione $z=z_1^{-1}$ abbiamo $g(w,z_1)=w^2-w-z_1$, $D'(z_1)=4z_1+1$, e dunque $D'(0)\neq 0$, per cui $z=\infty$ non è un punto critico.

3. Con $f(w,z)=(z-1)w^2-zw-1$, irriducibile, abbiamo $f'(w,z)=\frac{\partial f(w,z)}{\partial w}=2(z-1)w-z$. Il discriminante $D(z)=z^2+4z-4$ ha le radici $-2-2\sqrt{2},-2+2\sqrt{2}$. Al finito abbiamo i due punti singolari per $f(w,z)$: $-2-2\sqrt{2}$ e $-2+2\sqrt{2}$; si verifica che la radice $\frac{\sqrt{2}-1}{-3+2\sqrt{2}}$ di $f'(w,-2-\sqrt{2})$ è anche radice di $f(w,-2-\sqrt{2})$ (analogamente per $-2+2\sqrt{2}$).

Per quanto riguarda $z=\infty$, si ha $D'(z_1)=-4z_1^2+4z_1+1$, e dunque $D'(0)\neq 0$, per cui $z=\infty$ non è punto critico.

4. Riprendiamo l'esempio del polinomio w^2-z. Sia $z_0\neq 0$ un punto del piano complesso della variabile z. Sia z_0 di modulo ρ e anomalia θ: $z_0=\rho e^{i\theta}$. Se si fa percorrere alla variabile z un cammino chiuso comunque intrecciato intorno all'origine nel senso positivo (antiorario) che inizia e termina in z_0, z ritorna in z_0 ma con una diversa anomalia: $\theta+2\pi$. Ne segue che $w_1(z)$, che in z_0 ha il valore:

$$w_1(z_0)=\sqrt{z_0}=\rho^{\frac{1}{2}}e^{i\frac{\theta}{2}},$$

quando z ritorna in z_0 ha il valore:

$$\rho^{\frac{1}{2}}e^{i\frac{\theta+2\pi}{2}}=\rho^{\frac{1}{2}}e^{i\frac{\theta}{2}}e^{i\pi}=\rho^{\frac{1}{2}}e^{i\frac{\theta}{2}}(-1)=-\sqrt{z_0}=w_2(z_0).$$

In modo analogo si vede che $w_2(z)$, che in z_0 vale $-\sqrt{z_0}$, quando z ritorna in z_0 vale $\sqrt{z_0}=w_1(z_0)$. In altre parole, percorrendo un cammino chiuso intorno all'origine (che è un punto singolare del polinomio) di inizio e fine un punto $z_0\neq 0$, le radici del polinomio $f(w,z_0)=w^2-z_0$ si scambiano tra loro, e abbiamo il ciclo (w_1,w_2) di lunghezza 2.

Se invece il cammino chiuso non include l'origine, le due radici ritornano ognuna su se stessa, e si ha la permutazione identica $(w_1)(w_2)$. (Vedremo in seguito, e più in generale, il caso del punto critico).

Nota. Come si vede da questo esempio della funzione $\sqrt{z}$, e contrariamente al caso reale, il valore in un punto di una funzione di variabile complessa non dipende in generale solo dal punto, ma anche dal modo in cui questo viene raggiunto.

Una funzione $f(z)$ si dice *monodroma* (da *monos* (solo) e *dromos* (corso)) o *a un sol valore* in una parte S del piano di z se quando z si muove comunque dentro S la funzione riprende lo stesso valore ogni qualvolta z ritorni in uno stesso punto. Se non si specifica l'insieme S si intende che la funzione è monodroma in tutto il piano.

Ad esempio la funzione $\sqrt{z}$ è monodroma in ogni regione del piano che non contenga l'origine.

Sussiste in proposito il seguente teorema di teoria delle funzioni:

5.2 Teorema. *Una funzione algebrica è monodroma in tutto il piano se e solo se è una funzione razionale.* $\diamondsuit$

Ricordiamo brevemente altri risultati della teoria delle funzioni.

1. *Se per un valore finito z_0 il polinomio $f(w, z_0)$ ha p radici uguali a w_0, allora è possibile tracciare un cerchio C nel piano di z e un cerchio Γ nel piano di w, di centri rispettivamente z_0 e w_0, e raggi r e ρ abbastanza piccoli tali che a ogni punto interno a C corrispondono p radici interne a Γ.*

Nel seguito, quando parleremo di "punti vicini a un dato punto" intenderemo riferirci all'esistenza di cerchi C e Γ come sopra.

2. Si ha in particolare, dal risultato precedente, che *se per un valore finito z_0 il polinomio $f(w, z_0)$ ha una sola radice uguale a w_0, allora per un valore di z vicino a z_0 esso ammette una sola radice vicina a w_0.*

3. Consideriamo ora un punto z_0 e una curva L che parta da z_0 e che non passi per alcun punto singolare del polinomio. In z_0 il polinomio ha n valori distinti; scegliamone uno, $w_1(z_0)$. Per **2**, a ogni punto z di un opportuno cerchio C_0, di centro z_0, e in particolare ad ogni punto z della curva L interno a C_0, corrisponde un solo valore di w. Associamo questa serie continua di valori al valore iniziale $w_1(z_0)$. Muovendosi lungo la curva L, a ogni punto z_0' di C_0 corrisponde un ben determinato valore $w_1'(z_0')$. Prendendo la coppia (z_0', w_1') come nuovo punto di partenza, si arriva in un punto z_0'' e a un corrispondente ben determinato valore $w_1''(z_0'')$. I valori w definiscono in tal modo una funzione algebrica, che è uniforme e continua, e anzi analitica, nell'unione dei cerchi $C_0, C_0', \ldots$ aventi per centro i diversi punti della curva. L'operazione ora descritta prende il nome di *prolungamento analitico* della funzione (analitica) $w_1(z_0)$. In ogni punto z della curva i valori $w_1(z)$ sono quindi ben determinati e distinti.

4. *Sia A un'area piana semplicemente connessa limitata da una curva semplice e non contenente punti singolari di $f(w, z)$. Se si va da un punto z_0 a un altro punto z_1 seguendo due curve interamente contenute in A, e se si parte con lo stesso valore $w(z_0)$ si arriva allo stesso valore finale $w(z_1)$. Ovvero, ciò che è lo stesso, se z percorre una curva chiusa ($z_1 = z_0$), le funzioni $w_i(z)$ ritrovano il loro valore iniziale $w_i(z_0)$.*

Dim. Supponiamo che partendo con $w_1(z_0)$ e percorrendo un cammino chiuso $\gamma = ABCDA$ ($A = z_0$) si ritorni in A con un valore diverso. Lo stesso accade allora percorrendo una delle due regioni $\gamma_1 = ABDA$ e $\gamma_2 = BCDB$ dove BD è una curva semplice che unisce due punti di γ. Infatti, se percorrendo γ_1 e γ_2 si ritorna con lo stesso valore, lo stesso accade percorrendo prima γ_1 e poi γ_2, cioè percorrendo γ. Ragionando nello stesso modo su uno dei due cammini, si arriva a un'area abbastanza piccola da essere contenuta in un cerchio C come quello del teorema di **1**. Percorrendo la circonferenza di $\mathcal{C}$ la radice w_1 non ritorna al valore iniziale; all'interno di $\mathcal{C}$ vi sono dunque almeno due radici w_i contro il risultato **2.** $\diamondsuit$

5. Supponiamo che nel punto singolare z' il polinomio abbia p radici uguali a w_0. Per **1.**, in un punto vicino z_0 essa avrà p radici vicine a w_0. Vediamo cosa diventa una di queste, e sia $w_1(z)$ quando z, partendo da z_0, descrive (in senso positivo) una piccola curva circolare C di centro z' con punto iniziale e finale z_0. Il valore che $w_1(z)$

ha in z_0 dopo che z ha percorso la curva nel senso positivo (antiorario) ritornando in z_0 sarà, sempre per **1.** (in quanto la variazione potrà essere solo piccola) ancora una delle radici $w_i(z_0)$, che però potrà essere diversa da $w_1(z_0)$. Se è ancora $w_1(z_0)$, il punto z' non è singolare per la radice $w_1(z)$.

Altrimenti, sia w_2 la radice ottenuta (scriviamo w_i per $w_i(z_0)$). Descrivendo di nuovo la curva C nello stesso senso non è possibile che si ritrovi w_2 in quanto il percorso inverso deve restituire w_1. Si troverà quindi o w_1 oppure un'altra radice non ancora ottenuta. Se si ritrova w_1, le due radici w_1 e w_2 si scambiano quando si gira intorno a z'. Nell'altro caso sia w_3 la radice che si ottiene. Un nuovo giro attorno a z' con il valore iniziale w_3 non può portare né a w_2 né a w_3; si troverà pertanto w_1 o una nuova radice. Proseguendo in questo modo, se dopo q giri si ricade in w_1, girando intorno a z_0 q radici subiscono una permutazione circolare $(w_1, w_2, \ldots, w_q)$.

In conclusione, in z_0 il polinomio ha n radici, delle quali $n-p$ sono diverse da w_0. Se esse sono anche diverse tra loro, allora per queste radici z_0 è un punto ordinario (non singolare). Le n radici $w_i = w_i(z_0)$ vengono permutate secondo una permutazione che si spezza in cicli:

$$(w_1, w_2, \ldots, w_q)(w_{q+1}, w_{q+2}, \ldots, w_r) \cdots (w_{s+1}, w_{s+2}, \ldots, w_n).$$

Qualcuno dei cicli può essere di lunghezza 1: è il caso delle radici w_i per le quali z_0 non è un punto singolare; dopo un giro intorno a z_0 la radice w_i ritorna su se stessa.

Un cammino chiuso C nel piano di z dà luogo a una permutazione σ delle w_i, eventualmente identica. Se percorrendo un cammino intorno a un punto critico una w_i passa a un'altra w_j, il punto si dice *punto di diramazione*. È chiaro che lo stesso cammino percorso in senso inverso produce la permutazione inversa σ^{-1}, e che percorrendo due cammini, prima C_1 e poi C_2, si ottiene la permutazione prodotto $\sigma_1\sigma_2$.

L'insieme di queste permutazioni è quindi un gruppo, ed è precisamente il gruppo del Teor. 5.1 come ora vedremo (Teor. 5.3). Questo risultato si fonda sul seguente teorema:

5.3 Teorema (Hermite[1]). *Il gruppo Γ delle permutazioni indotte sulle radici $w_1, w_2, \ldots, w_n$ di $f(w,z)$ da tutti i cammini chiusi percorsi da z coincide con il gruppo H di monodromia.*

Dim. Occorre dimostrare che il gruppo in questione lascia invariate tutte e sole le funzioni razionali delle w_i, che sono funzioni razionali di z, cioè tutti gli elementi $\varphi \in C(z)(w_1, w_2, \ldots, w_n)$ che appartengono a $C(z)$. Sia

$$\varphi(w_1, w_2, \ldots, w_n, z) = f(z),$$

con f razionale, una tale funzione. Se z percorre un cammino C, la relazione precedente continua a valere lungo tutto C, e quando z ritorna al punto di

[1] *Sur les fonctions algébriques*, Compes Rendus Acad. Sci. Paris (32), 1851, 458-461.

partenza la $f(z)$ riprende il suo valore. Se $\sigma \in \Gamma$ è la permutazione delle w_i indotta dal cammino C, si ha allora:

$$\varphi(w_{\sigma(1)}, w_{\sigma(2)}, \ldots, w_{\sigma(n)}, z) = f(z);$$

ma $f(z) = \varphi(w_1, w_2, \ldots, w_n, z)$, e dunque:

$$\varphi(w_1, w_2, \ldots, w_n, z) = \varphi(w_{\sigma(1)}, w_{\sigma(2)}, \ldots, w_{\sigma(n)}, z).$$

Viceversa, se $\varphi = \varphi(w_{\sigma(1)}, w_{\sigma(2)}, \ldots, w_{\sigma(n)}, z)$ è una funzione razionale invariante per tutti gli elementi di Γ, sempre per il Teor. 5.2 essa è una funzione razionale di z. $\diamondsuit$

Esempi 1. Sia:

$$f(w, z) = w^4 - 2w^2 + 1 - z.$$

Posto $w^2 = t$ abbiamo $t = 1 \pm \sqrt{z}$, $w = \pm\sqrt{1 \pm \sqrt{z}}$, e dunque le quattro radici:

$$w_1 = \sqrt{1 + \sqrt{z}},\ w_2 = \sqrt{1 - \sqrt{z}},\ w_3 = -\sqrt{1 + \sqrt{z}},\ w_4 = -\sqrt{1 - \sqrt{z}}\ .$$

Il discriminante di questo polinomio è $D(z) = -256(z-1)z^2$, che ha le radici $z_0 = 0$ (doppia) e $z_1 = 1$.

Per $z_0 = 0$ abbiamo:

$$f(w, 0) = w^4 - 2w^2 + 1 = (w^2 - 1)^2,$$

e in $z_0 = 0$ $w_1(0)$ e $w_2(0)$ concidono (entrambi valgono 1). Analogamente coincidono $w_3(z_0)$ e $w_4(z_0)$, che in $z_0 = 0$ valgono -1. Il punto $z_0 = 0$ è di diramazione. Abbiamo visto che in un giro intorno all'origine $\sqrt{z}$ e $-\sqrt{z}$ si scambiano tra loro. Ne segue che lo stesso accade per w_1 e w_2. Analogamente per w_3 e w_4. In un giro di z intorno all'origine le radici della w subiscono la permutazione (1,2)(3,4).

Consideriamo ora il punto $z_1 = 1$. Quando z percorre una curva intorno al punto 1 (una curva che non circondi l'origine), $1 - \sqrt{z}$ compie un giro completo intorno all'origine. Posto $1 - \sqrt{z} = \rho e^{i\theta}$, dopo un giro si ha $1 - \sqrt{z} = \rho e^{i(\theta + 2\pi)}$, e dunque:

$$w_2 = \sqrt{1 - \sqrt{z}} = \rho^{\frac{1}{2}} e^{i\frac{\theta}{2}} \longrightarrow \rho^{\frac{1}{2}} e^{i(\frac{\theta}{2} + \pi)} = -\sqrt{1 - \sqrt{z}} = w_4\ .$$

Analogamente, $w_4 = -\sqrt{1 - \sqrt{z}} \longrightarrow \sqrt{1 - \sqrt{z}} = w_2$: w_2 e w_4 si scambiano tra loro.

In un giro intorno al punto $z_1 = 1$, $1 - \sqrt{z}$ non cambia invece anomalia (resta sempre con parte reale positiva) e dunque w_1 e w_3 tornano su se stessi:

$z_1 = 1$ non è di diramazione né per w_1 né per w_3. La permutazione dei w_i indotta da un giro di z intorno al punto $z_1 = 1$ è dunque la $\tau = (1)(3)(2,4)$.

Riguardo al punto $z = \infty$, la sostituzione $z = z_1^{-1}$ porta a $g(w, z_1)$ il cui discriminante $256(z_1 - 1)z_1^3$ ha la radice $z_1 = 0$; dunque $z = \infty$ è un punto critico.

Nota. I punti del piano complesso ampliato sono in corrispondenza biunivoca con i punti di una sfera mediante la proiezione stereografica. Il polo nord P della sfera si proietta nel punto all'infinito. Dato un numero finito di punti del piano, è sempre possibile tracciare sulla sfera una curva intorno a P cosí piccola che la curva corrispondente nel piano è cosí grande da racchiudere i punti dati. Se si percorre la curva sulla sfera in senso antiorario, nella curva proiezione il senso di percorrenza diventa quello orario: in tal modo percorrendo le due curve, il punto P sulla sfera e il punto all'infinito del piano vengono tenuti entrambi sulla sinistra. Se $z = \infty$ è un punto critico, per vedere quale permutazione si induce sui w_i percorrendo una curva intorno ad esso nel modo detto, si considerino le curve $\delta_1, \delta_2, \ldots, \delta_k$ percorse nel piano (in senso antiorario) a partire da un punto non singolare z_0. Siano $\sigma_1, \sigma_2, \ldots, \sigma_k$ le permutazioni corrispondenti. Si può dimostrare che ogni cammino chiuso da z_0 a z_0 è omotopo a un cammino ottenuto percorrendo le δ_i .

Torniamo al nostro polinomio. Riguardo al punto $z = \infty$, ruotando intorno ad esso si ottiene la permutazione $(\sigma\tau)^{-1} = (1,2,3,4)$. Non essendovi altri punti singolari, il gruppo di monodromia è il sottogruppo di S_4 generato da σ e τ. Si tratta di uno dei tre gruppi diedrali D_4, contenuti in S_4, e consta delle otto permutazioni:

$$I, (1,2)(3,4), (1)(3)(2,4), (1,4,3,2), (1,2,3,4), (1,3)(2,4), (1,4)(2,3), (1,3)(2,4).$$

Ad esempio, $\sigma\tau = (1,4,3,2)$, e ciò significa che a partire da un punto $z_0 \neq 0, 1$, un giro completo di z intorno a 0, seguito da uno intorno a 1, provoca sui w_i la permutazione ciclica $w_1 \to w_4 \to w_3 \to w_2 \to w_1$. Come altro esempio, un giro di z intorno al punto 1, seguito da un giro intorno a 0, e poi ancora da un giro intorno a 1 provoca sui w_i la permutazione $(w_1, w_4)(w_2, w_3)$; ecc.

In questo esempio, il gruppo di monodromia H coincide con il gruppo di Galois G. Se infatti fosse un sottogruppo proprio di G sarebbe un sottogruppo di S_4 che contiene D_4 propriamente, ma l'unico tale sottogruppo è lo stesso S_4. Ne segue che D_4 sarebbe normale in S_4, assurdo. Le funzioni monodrome delle w_i sono dunque funzioni razionali di z ma a coefficienti soltanto razionali.

Vediamo qualche esempio di funzione razionale dei w_i. Riguardo al punto $z = \infty$, ruotando intorno ad esso si ottiene la permutazione $(\sigma\tau)^{-1} = (1,2,3,4)$.

Sia $\varphi(w_1, w_2, z) = w_1^2 w_2^2$. Si ha $\varphi(w_1, w_2, z) = (1 + \sqrt{z})(1 - \sqrt{z}) = 1 - z \in Q(z)$. Sia $\gamma = (1,3)(2)(4)$ allora $\varphi(w_3, w_2, z) = w_3^2 w_2^2 = (1 + \sqrt{z})(1 - \sqrt{z}) = 1 - z$. Analogamente per gli altri elementi di D_4. Vi sono permutazioni di S_4

che non lasciano invariata φ. Ad esempio, la $(1)(4)(2,3) \notin D_4$: si ha infatti $\varphi(w_1, w_3, z) = w_1^2 w_3^2 = (1+\sqrt{z})^2 = 1 + z + 2\sqrt{z} \notin Q(z)$.

Le tre permutazioni $\sigma_1 = I, \sigma_2 = (1)(4)(2,3), \sigma_3 = (1,4)(2)(3)$ sono rappresentanti dei laterali di D_4 in S_4. Con $\gamma = w_1^2 w_2^2$ consideriamo $\prod(x - \gamma^{\sigma_i})$ (v. Cor. 2.33), e verifichiamo che è a coefficienti in $Q(z)$. Si ha infatti:

$$\begin{aligned}\prod(x-\gamma^{\sigma_i}) &= (x-(1-z))(x-(1+\sqrt{z})^2)(x-(1-\sqrt{z})^2) \\ &= x^3 + (z-3)x^2 + (3-2z-z^2)x - (z^3 - z^2 - z + 1).\end{aligned}$$

2. Analogamente si può vedere che il gruppo di monodromia di $f(w,z) = w^4 - zw - 1$ è il gruppo di Klein $H = \{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, mentre il gruppo di Galois è uno dei tre gruppi diedrali di S^4.

Vediamo ora alcune equazioni binomie.

3. Sia $f(w,z) = w^3 - z$, con le tre radici $w_1 = \sqrt[3]{z}, w_2 = \epsilon\sqrt[3]{z}, w_3 = \epsilon^2\sqrt[3]{z}$, dove ϵ è una radice terza dell'unità. Il discriminante è $-27z^2$, e $z = 0$ è un punto critico. Si ha $w_1 = \sqrt[3]{z} = \rho^{1/3}e^{i\frac{\theta}{3}}$, che dopo un giro intorno all'origine passa a $\rho^{1/3}e^{i\frac{\theta+2\pi}{3}} = \epsilon\sqrt[3]{z} = w_2$. Un altro giro, e w_2 passa a $\rho^{1/3}e^{i\frac{\theta+4\pi}{3}} = w_3$, e infine dopo un ulteriore giro w_3 passa a $\rho^{1/3}e^{i\frac{\theta+6\pi}{3}}$ che è uguale a w_1 in quanto $\cos\frac{1}{3}(\theta+6\pi)+\text{sen}\frac{1}{3}(\theta+6\pi) = \cos\frac{1}{3}\theta+\text{sen}\frac{1}{3}\theta$. Il gruppo di monodromia contiene dunque la permutazione $(1,2,3)$. La sostituzione $z = z_1^{-1}$ porta a $g = z_1 w^3 - 1$, che ha discriminante $-27z_1^2$ (uguale al precedente), e pertanto $z = \infty$ è un punto critico. Percorrendo in senso orario una curva che esclude l'origine si ha la permutazione inversa $(1,3,2)$. Pertanto, il gruppo di monodromia è ciclico di ordine 3: {I, (1,2,3),(1,3,2)}.

Che il gruppo di monodromia di $w^3 - z$ sia questo si può anche vedere come segue. Poiché il polinomio resta irriducibile in $C(z)$ (se si spezza, ha un fattore di primo grado, e dunque una radice in $C(z)$; ma se $\epsilon^k\sqrt[3]{z} \in C(z)$, anche $\sqrt[3]{z} \in C(z)$, assurdo) il gruppo di Galois su questo campo è il gruppo ciclico di ordine 3 (Teor. 3.10). Il gruppo di galois su $Q(z)$ è invece S^3.

4. $f(w,z) = w^4 - 2z^2$. Il discriminante è $-2048z^6$, dunque $z = 0$ è il solo punto critico al finito. Con la sostituzione $z = z_1^{-1}$ si ha lo stesso discriminante, e dunque $z = \infty$ è anch'esso critico. Ponendo:

$$w_1 = \sqrt[4]{2}\sqrt{z}, w_2 = i\sqrt[4]{2}\sqrt{z}, w_3 = -\sqrt[4]{2}\sqrt{z}, w_4 = -i\sqrt[4]{2}\sqrt{z},$$

si vede come sopra che il gruppo di monodromia è il gruppo $H = \{I, (1,3)(2,4)\}$ (che non è transitivo; il polinomio si riduce infatti su $C(z)$: $f(w,z) = (w^2 - \sqrt{2}z)(w^2 + \sqrt{2}z)$). Il gruppo di Galois G è il gruppo diedrale di ordine 8 (Teor. 3.3 e 3.6) che ha H normale, e quindi, essendo di ordine 2, centrale. Allora H è necessariamente il quadrato del ciclo (1,2,3,4), e dunque G è il diedrale dell'*Es.* 3.8.

5. Un classico esempio di applicazione del gruppo di monodromia è dato dalle equazioni per la divisione dell'argomento delle funzioni circolari, per esempio quella che a partire da:

$$z = cos\ \alpha$$

permette di determinare

$$w = cos \frac{\alpha}{n}.$$

La considerazione del gruppo di monodromia ci permetterà di dimostrare che queste equazioni sono *risolubili per radicali*, ovvero che $cos \frac{\alpha}{n}$ si esprime per radicali in termini di $cos(\alpha)$. Ad esempio, per $n = 2$, dalla nota formula $cos\ 2\alpha = 2cos^2\ \alpha - 1$ abbiamo $cos\ \alpha = 2cos^2\ \frac{\alpha}{2} - 1$ e l'espressione per radicali:

$$cos \frac{\alpha}{n} = \pm \sqrt{\frac{1 + cos\ \alpha}{2}}.$$

$cos \frac{\alpha}{2}$ è dunque radice dell'equazione:

$$2w^2 - 1 - z = 0.$$

Il polinomio $2w^2 - 1$ è un particolare polinomio di Tchebishev, il polinomio $T_2(w)$. I polinomi di Tchebishev sono definiti ricorsivamente come segue:

$$\begin{aligned} T_0(w) =&\ \ 1, \\ T_1(w) =&\ \ w, \\ T_n(w) =&\ \ 2wT_{n-1}(w) - T_{n-2}(w), \end{aligned}$$

ed è noto che

$$cos\ n\alpha = T_n(cos\ \alpha).$$

$cos \frac{\alpha}{n}$ si trova quindi in termini di $z = cos(\alpha)$ risolvendo l'equazione:

$$T_n(w) - z = 0, \tag{5.4}$$

e vedremo che questa equazione è risolubile per radicali.

Le n radici della (5.4) sono

$$w_0 = cos \frac{\alpha}{n}, w_1 = cos \frac{\alpha + 2\pi}{n}, \ldots, w_n = cos \frac{\alpha + 2(n-1)\pi}{n}.$$

Determiniamo ora il gruppo di monodromia; possiamo limitarci al caso $n = p$, primo. Affinché $z = cos\,\alpha$ descriva un cammino chiuso nel proprio piano complesso, è necessario e sufficiente che α si muti in $\pm\alpha + 2k\pi$, con k intero; viceversa, per ogni k, se α varia con continuità da α a $\pm\alpha + 2k\pi$, la z descrive nel piano complesso un cammino chiuso. La radice w_i si muta allora in w_j, dove j è definito dalla congruenza:

$$j \equiv \pm i + k \mod p \tag{5.5}$$

Il gruppo di monodromia H della (5.4) consta quindi delle $2p$ sostituzioni (5.5) che si ottengono al variare di k. Per determinare ora il gruppo di Galois G osserviamo che, essendo H normale in G, anche il sottogruppo di ordine p di H, che è caratteristico in H, sarà normale in G. Per il Teor. 3.29, G è allora un sottogruppo del gruppo lineare $\mathcal{L}_p$ che ha ordine $p(p-1)$ (si può dimostrare che G è tutto $\mathcal{L}_p$). In particolare, G è risolubile, e dunque l'equazione (5.4) è risolubile per radicali. Inoltre,

5.4 Lemma. *Aggiungendo $cos\frac{2\pi}{p}$ al campo $Q(z)$ il gruppo di Galois G su $Q(z)$ si abbassa al gruppo di monodromia H.*

Dim. Sia $j \equiv ai + k \mod p$ un elemento di $G = \mathcal{L}_p$, dopo l'aggiunta di $cos\frac{2\pi}{p}$, e consideriamo l'uguaglianza:

$$cos\frac{\alpha+2\pi}{p} + cos\frac{\alpha-2\pi}{p} = 2cos\frac{2\pi}{p}cos\frac{w}{p},$$

cioè la relazione:

$$w_1 + w_{-1} - 2cos\frac{2\pi}{p} \cdot w_0 = 0.$$

Questa relazione deve restare invariata per qualunqe permutazione del gruppo di Galois, ad esempio la $j \equiv ai \mod p$; ne segue:

$$w_a + w_{-a} - 2cos\frac{2\pi}{p} \cdot w_0 = 0.$$

D'altra parte,

$$w_a + w_{-a} = cos\frac{w+2a\pi}{p} + cos\frac{w-2\pi}{p} = 2cosa \cdot \frac{2\pi}{p} \cdot w_0,$$

e pertanto $a \equiv \pm 1 \mod p$. L'elemento $j \equiv ai + k \mod p$ di $G = \mathcal{L}_p$ appartiene dunque al gruppo di monodromia H. ◊

Osserviamo infine che l'aggiunta della quantità irrazionale $cos\frac{2\pi}{p}$ è necessaria se si vuole abbassare il gruppo di Galois G su $Q(z)$ al gruppo H. Infatti ad esempio la relazione

$$\frac{w_1 + w_{-1}}{2w_0} = cos\frac{2\pi}{p}$$

resta invariata per tutte le sostituzioni (5.4) di H.

Esempi. Vediamo ora gruppi di Galois e di monodromia di alcuni polinomi $T_n(x) - z$ così come sono stati determinati con il sistema di calcolo simbolico Maple©.

1. $f(x) = T_2(x) - z = 2x^2 - 1 - z$, $|G| = |H| = 2$.
2. $f(x) = T_3(x) - z = 4x^3 - 3x - z$, $|G| = |H| = 6$.
3. $f(x) = T_5(x) - z = 16x^5 - 20x^3 + 5x - z$, $|G| = 20$, $|H| = 10$.
4. $f(x) = T_7(x) - z = 64x^7 - 112x^5 + 56x^3 - 7x - z$, $|G| = 42$, $|H| = 14$.

Il gruppo G di 3. è il gruppo $\mathcal{L}_5$ delle trasformazioni lineari $x \to kx + t$, $(k, p) = 1$, $t = 0, 1, \ldots, p - 1 \bmod p$, di ordine $5(5 - 1) = 20$. Analogamente il gruppo G di 4. è il gruppo $\mathcal{L}_7$ di ordine $7(7 - 1) = 42$.