Capitolo 4

Equazioni di secondo, terzo e quarto grado

In questo capitolo ripercorriamo i tentativi di risoluzione per radicali dell'equazione generale di grado n qualunque, mettendo in luce gli elementi comuni alle soluzioni nei casi $n = 2, 3, 4$ e il motivo per il quale il procedimento che ha successo nei casi detti fallisce per $n \geq 5$. A priori potrebbero esistere altri procedimenti di risoluzione per radicali, ma sappiamo dalla teoria di Galois che ciò non è possibile per via del fatto che il gruppo simmetrico S_n per $n \geq 5$ non è risolubile (Teor. 3.25). In questo capitolo vedremo la dimostrazione diretta di questa impossibilità seguendo Ruffini e Abel (Teor. 4.5).

Sia $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$ un polinomio di grado n. Risolvere l'equazione $f(x) = 0$ significa determinare le radici α_i di $f(x)$ a partire dai coefficienti a_i, cioè dalle le funzioni simmetriche elementari delle α_i [1]. Poiché, al contrario delle a_i, ognuna delle α_i è una funzione completamente asimmetrica delle α_i stesse (una qualunque permutazione non identica porta una α_i in una $\alpha_j \neq \alpha_i$), risolvere l'equazione significa passare dalla situazione di completa simmetria delle a_i a quella di completa asimmetria delle α_i, ovvero da funzioni a un valore (simmetriche) alla funzione α_1 che assume n valori $\alpha_1, \alpha_2, \ldots, \alpha_n$. In particolare, la risoluzione per radicali richiede che questo passaggio avvenga mediante operazioni razionali ed estrazioni di radice.

L'idea di Lagrange e di altri per risolvere i casi $n = 2, 3$ e 4 è la seguente. Si cerca una funzione $z = z(\underline{\alpha})$ delle radici la quale, permutando comunque le α_i, assuma valori $z_1, z_2, \ldots, z_m$ in numero m inferiore al grado n del polinomio $f(x)$. Questi valori saranno radici del polinomio $g(z) = (z - z_1)(z - z_2) \cdots (z - z_m)$, di grado $m < n$ (o $m = n$ nel caso $n = 2$; ma allora $g(z)$ sarà del tipo $z^2 - c$ che si

[1] Come scrive Jacobi (Crelle J., 13, 1835, p. 340): *Resolutio aequationum algebraica poscit, ut, dato numero elementorum, singula elementa per functiones eorum symmetricas ope extractionis radicum exhibeantur.*

risolve con una estrazione di radice). Permutando le α_i le z_i vengono permutate, e quindi i coefficienti di $g(z)$, che sono le funzioni simmetriche elementari delle z_i, restano invariati. Essi sono allora funzioni simmetriche delle α_i e quindi (Teor. 1.5) polinomi nelle funzioni simmetriche elementari delle α_i, cioè nei coefficienti a_i del polinomio dato $f(x)$. Un'equazione come la $g(z) = 0$, le cui radici sono i valori distinti assunti da una funzione delle α_i quando le α_i vengono permutate dagli elementi di un gruppo di permutazioni, è una *risolvente* dell'equazione di partenza $f(x)$. Dalle radici di $g(z)$, espresse per radicali, si ottengono i valori di α_i costruendo un sistema di equazioni lineari una delle quali è la $\alpha_1 + \alpha_2 + \cdots + \alpha_n = -a_1$, e le altre hanno come termine noto un'espressione radicale delle z_i.

4.1 L'equazione di secondo grado

Sia $x^2 + px + q = 0$ l'equazione. Il valore della funzione $\alpha_1 + \alpha_2$ delle radici è noto, e pari a $-p$; cerchiamo allora un'altra funzione di α_1 e α_2, non simmetrica, e quindi in questo caso a due valori, e lineare. Questa funzione ha perciò la forma $a\alpha_1 + b\alpha_2$, con $a \neq b$ (altrimenti si ottiene solo un multiplo della somma $\alpha_1 + \alpha_2$, già nota). I due valori si trovano risolvendo un'equazione di secondo grado, che non deve essere del tipo della data, e quindi deve avere la forma $z^2 = c$: le due radici sono allora uguali e di segno contrario. Ne segue che a e b devono essere tali che scambiando tra loro α_1 e α_2 si ottengano valori uguali e opposti:

$$a\alpha_1 + b\alpha_2 = -a\alpha_2 - b\alpha_1,$$

da cui $a = -b$. Posto per semplicità $a = 1$, la funzione cercata è $\alpha_1 - \alpha_2$. L'equazione che dà i due valori $z_1 = \alpha_1 - \alpha_2$ e $z_2 = \alpha_2 - \alpha_1$ è:

$$(z - (\alpha_1 - \alpha_2))((z - (\alpha_2 - \alpha_1)) = 0,$$

cioè:

$$z^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = p^2 - 4q,$$

da cui:

$$z = \alpha_1 - \alpha_2 = \sqrt{p^2 - 4q}.$$

($\Delta = (\alpha_1 - \alpha_2)^2$ è il discriminante dell'equazione $f(x) = 0$). Assieme alla $\alpha_1 + \alpha_2 = -p$ abbiamo il sistema lineare:

$$\begin{cases} \alpha_1 + \alpha_2 &= -p, \\ \alpha_1 - \alpha_2 &= \sqrt{p^2 - 4q} \end{cases}$$

da cui si ottengono α_1 e α_2 nella nota forma[2]. Si osservi come dalle due funzioni simmetriche $\alpha_1 + \alpha_2$ e $(\alpha_1 - \alpha_2)^2 = p^2 - 4q$ si ottengano le due funzioni

[2]Per questa discussione e per il seguito si veda Laplace, *Oeuvres*, vol. XIV, p. 53-65.

asimmetriche α_1 e α_2 introducendo il radicale[3]. Nella terminologia del 3.2, con l'aggiunzione al campo dei coefficienti del radicale $\sqrt{p^2-4q}$ si ottiene l'intero campo di spezzamento di $f(x)$: $K(\sqrt{p^2-4q}) = K(\alpha_1, \alpha_2)$. Infine, scriviamo $\alpha_1 - \alpha_2$ come $\alpha_1 + w\alpha_2$, e $\alpha_1 + \alpha_2$ come $\alpha_1 + w^2\alpha_2$, con $w = -1$. Le due funzioni sono allora funzioni lineari delle radici α_1 e α_2 a coefficienti le radici seconde dell'unità -1 e 1. Scriviamo la formula risolutiva nel modo seguente:

$$\alpha_{1,2} = \frac{1}{2}[(\alpha_1 + \alpha_2) + \sqrt{(\alpha_1 - \alpha_2)^2}]. \tag{4.1}$$

Le due radici α_1 e α_2 si ottengono in corrispondenza ai due valori del radicale. Vedremo l'analogo della (4.1) per le equazioni di terzo e quarto grado con le radici terze e quarte dell'unità.

4.2 L'equazione di terzo grado

Consideriamo l'equazione di terzo grado nella forma ridotta:

$$f(x) = x^3 + px + q = 0$$

(ci si può sempre ridurre a questa forma sostituendo nell'equazione generale $y^3 + a_1y^2 + a_2y + a_3 = 0$ la y con $x - \frac{1}{3}a_1$). Come nel caso precedente abbiamo un'equazione lineare, data dalla somma delle tre radici $\alpha_1 + \alpha_2 + \alpha_3 = 0$. Ne cerchiamo allora altre due per avere un sistema di tre equazioni nelle tre incognite α_i. Se una funzione delle radici assume soltanto due valori permutando in tutti i modi le α_i, la somma e il prodotto di questi due valori sono funzioni razionali di p e q, coefficienti di un'equazione di secondo grado, che sappiamo risolvere per radicali, e della quale i due valori sono le radici. Proseguendo per analogia con il caso precedente, sia $a\alpha_1 + b\alpha_2 + c\alpha_3$ una funzione lineare. Permutando le α_i questa funzione assume sei valori; questi sono allora soluzioni di un'equazione di sesto grado. Per ridursi a un'equazione di secondo grado occorre che il cubo di questa funzione assuma solo due valori, ed è facile vedere che ciò si ottiene prendendo per a, b e c le radici terze dell'unità: $a = 1,\ b = w = -\frac{1}{2} + \frac{1}{2}i\sqrt{3},\ c = w^2 = -\frac{1}{2} - \frac{1}{2}i\sqrt{3}$. I due valori sono allora:

$$y_1 = (\alpha_1 + \alpha_2 w + \alpha_3 w^2)^3 \ \text{ e } \ y_2 = (\alpha_1 + \alpha_3 w + \alpha_2 w^2)^3,$$

radici dell'equazione $(y - y_1)(y - y_2)$. Si ottiene l'espressione dei coefficienti di questa equazione, che sono $-(y_1 + y_2)$ e y_1y_2, in termini di p e q dividendoli

[3]In generale, l'introduzione di un radicale di indice p moltiplica il numero dei valori della funzione per p e divide la simmetria per p, nel senso che l'ordine del gruppo delle permutazioni che lasciano invariata la funzione viene diviso per p. Si veda J. Stillwell, *Mathematics and its history*, Springer, New York, 2002, p.364–365.

successivamente per i moduli di Cauchy (Cap. 1):

$$X_3 = x + \alpha_1 + \alpha_2,\ X_2 = x^2 + \alpha_1 x + \alpha_1^2 + p,\ X_3 = f(x).$$

Si trova:

$$-(y_1 + y_2) = 27q,\ y_1 y_2 = -27p^3,$$

e dunque l'equazione:

$$y^2 + 27qy - 27p^3,$$

(*risolvente di Lagrange* della $f(x)$). Prendendo la funzione $\frac{1}{3}(\alpha_1 + w\alpha_2 + w\alpha_3)$ i calcoli sono più semplici, e la risolvente diventa:

$$y^2 + qy - \frac{1}{27}p^3.$$

Questa equazione ha le due radici:

$$y_1 = -\frac{1}{2}q + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},\quad y_2 = -\frac{1}{2}q - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \tag{4.2}$$

e dunque $\frac{1}{3}(\alpha_1 + w\alpha_2 + w^2\alpha_3) = \sqrt[3]{y_1}$ e $\frac{1}{3}(\alpha_1 + w^2\alpha_2 + w\alpha_3) = \sqrt[3]{y_2}$. Assieme alla $\alpha_1 + \alpha_2 + \alpha_3 = 0$ (si tratta del coefficiente di x^2 nella $f(x)$) abbiamo allora il sistema di tre equazioni lineari nelle tre incognite $\alpha_1, \alpha_2, \alpha_3$:

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 & = & 0 \\ \frac{1}{3}(\alpha_1 + w\alpha_2 + w^2\alpha_3) & = & \sqrt[3]{y_1} \\ \frac{1}{3}(\alpha_1 + w^2\alpha_2 + w\alpha_3) & = & \sqrt[3]{y_2} \end{cases}$$

Ciascun radicale cubico ha tre determinazioni; avendosi:

$$(\frac{1}{3}(\alpha_1 + w\alpha_2 + w^2\alpha_3)(\frac{1}{3}(\alpha_1 + w^2\alpha_2 + w\alpha_3) =$$
$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 = -\frac{p}{3},$$

una determinazione di $\sqrt[3]{y_1}$ e una di $\sqrt[3]{y_2}$ vanno scelte in modo che il prodotto valga $-\frac{p}{3}$. Risolvendo il sistema, si ottengono le tre radici dell'equazione data; se

$$\alpha_1 = \sqrt[3]{y_1} + \sqrt[3]{y_2}$$

è una di queste, con la determinazione dei radicali, le altre due sono:

$$\alpha_2 = w\sqrt[3]{y_1} + w^2\sqrt[3]{y_2},\ \alpha_3 = w^2\sqrt[3]{y_1} + w\sqrt[3]{y_2}$$

(*formule di Cardano*). Si osservi che i radicali che compaiono nelle formule sono funzioni razionali delle radici:

$$\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = \frac{\sqrt{-3}}{18}(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$$

e

$$\sqrt[3]{-\frac{q}{3}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}=\frac{\alpha_1}{2}+\frac{\sqrt{-3}}{6}(\alpha_2-\alpha_3).$$

Vedremo in seguito, quando parleremo delle equazioni di quinto grado, l'importanza di questa osservazione.

Esempi[4]. **1.** Sia data l'equazione $x^3-12x+16=0$. Si ha: $y_1=y_2=-8$. Scegliamo per i radicali la determinazione -2; abbiamo:

$$\begin{aligned}\alpha_1 &= \sqrt[3]{-8}+\sqrt[3]{-8}=-2+(-2)=-4,\\ \alpha_2 &= w\sqrt[3]{-8}+w^2\sqrt[3]{-8}=(w+w^2)\sqrt[3]{-8}=-1\cdot -2=2\\ \alpha_3 &= w^2\sqrt[3]{-8}+w\sqrt[3]{-8}=(w^2+w)\sqrt[3]{-8}=-1\cdot -2=2.\end{aligned}$$

2. L'equazione $x^3+x-2=0$ ha la radice 1. Applicando le formule abbiamo la somma:

$$\alpha=\sqrt[3]{1+\frac{2}{3}\sqrt{\frac{7}{3}}}+\sqrt[3]{1-\frac{2}{3}\sqrt{\frac{7}{3}}},$$

espressione che si può semplificare risolvendo in c e d l'equazione $\sqrt[3]{a+\sqrt{b}}=c+\sqrt{d}$. Si trova che i due radicali cubici sono uguali, nell'ordine, a $u=\frac{1}{2}+\frac{1}{2}\sqrt{\frac{7}{3}}$ e $v=\frac{1}{2}-\frac{1}{2}\sqrt{\frac{7}{3}}$. Ne segue:

$$\alpha_1=u+v=1,\ \alpha_2=wu+w^2v=-1+\frac{1}{2}i\sqrt{7},\ \alpha_3=w^2u+wv=-1-\frac{1}{2}i\sqrt{7}.$$

(Si osservi il risultato piuttosto sorprendente: $\sqrt[3]{1+\frac{2}{3}\sqrt{\frac{7}{3}}}+\sqrt[3]{1-\frac{2}{3}\sqrt{\frac{7}{3}}}=1$).

3. L'equazione $x^3-15x-4=0$ ha la soluzione $\alpha=4$. Dividendo per $x-4$ troviamo le altre due, $-2\pm\sqrt{3}$: le soluzioni sono tutte e tre reali. Se applichiamo Cardano troviamo l'espressione:

$$\sqrt[3]{2+\sqrt{-121}}+\sqrt[3]{2-\sqrt{-121}}$$

che fa intervenire la radice di un numero negativo, e quindi i numeri complessi. Riducendo come sopra si trova che i due radicali cubici valgono rispettivamente $2+\sqrt{-1}$ e $2-\sqrt{-1}$, e quindi la formula di Cardano dà effettivamente la radice 4.

Il caso, come questo, nel quale $\frac{q^2}{4}+\frac{p^3}{27}<0$, è il *casus irriducibilis* dell'equazione ("irriducibile" qui non ha niente a che vedere con l'irriducibilità dei

[4]Questi esempi sono tratti da J-P Tignol, *Galois' Theory of Algebraic Equations*, World Scientific, 2001.

polinomi; è un modo per dire che le soluzioni non si ottengono mediante radicali reali).

Consideriamo ora i due casi possibili per le radici. La radice quadrata del discriminante vale:

$$\sqrt{\Delta} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = -4p^3 - 27q^2 = -108(\frac{q^2}{4} + \frac{p^3}{27}).$$

1. L'equazione ha una radice reale $\alpha_1 = a$ e le altre due complesse coniugate, $\alpha_2 = b + ci$ e $\overline{\alpha_2} = b - ci$. Allora:

$$\sqrt{\Delta} = c((a - 2b)^2 + 2c^2)i$$

è puramente immaginario (essendo $c \neq 0$). Dunque $\Delta < 0$, cioè $\frac{q^2}{4} + \frac{p^3}{27} > 0$. Come $\sqrt[3]{y_1}$ in (4.2) possiamo prendere una radice cubica reale; allora anche $\sqrt[3]{y_2}$ sarà reale in quanto il prodotto $\sqrt[3]{y_1}\sqrt[3]{y_2} = -\frac{p}{3}$. Abbiamo quindi la radice reale $\alpha_1 = \sqrt[3]{y_1} + \sqrt[3]{y_2}$, ed essendo $w^2 = \overline{w}$, le altre due date dalle formule di Cardano sono complesse coniugate.

2*a*. L'equazione ha tre radici reali. In questo caso $\Delta \geq 0$. Se $\Delta = 0$, $y_1 = y_2 = -\frac{q}{2}$. Scelto per $\sqrt[3]{y_1}$ il valore reale, anche $\sqrt[3]{y_2}$ dovrà essere reale (il prodotto è $-\frac{p}{3}$) e quindi uguale a $\sqrt[3]{y_1}$. Ne segue $\alpha_1 = 2\sqrt[3]{y_1}$, $\alpha_2 = (w + w^2)\sqrt[3]{y_1} = -\alpha_1$, e $\alpha_3 = (w^2 + w)\sqrt[3]{y_1} = -\alpha_1$. Se dunque $\Delta = 0$, due delle tre radici reali sono coincidenti.

2*b*. Se $\Delta > 0$, $\sqrt{\Delta}$ è immaginario, e allora nella formula di Cardano occorre estrarre le radici cubiche di due numeri complessi coniugati. Sia $\alpha_1 = \sqrt[3]{y_1} + \sqrt[3]{y_2}$; i due addendi hanno somma reale α_1 e prodotto reale $-\frac{p}{3}$. Dunque sono radici di un'equazione di secondo grado a coefficienti reali, la $x^2 - \alpha_1 x - \frac{p}{3}$, e sono pertanto coniugati. Anche le coppie $w\sqrt[3]{y_1}$, $w^2\sqrt[3]{y_2}$ e $w^2\sqrt[3]{y_1}$, $w\sqrt[3]{y_2}$ sono coniugate, e dunque le somme che danno α_2 e α_3 sono reali. Inoltre, le tre radici sono distinte. Se infatti si avesse ad esempio $\alpha_1 = \alpha_2$, cioè $\sqrt[3]{y_1} + \sqrt[3]{y_2} = w\sqrt[3]{y_1}, w^2\sqrt[3]{y_2}$, allora

$$(1 - w)\sqrt[3]{y_1} = (w^2 - 1)\sqrt[3]{y_2}, \quad \frac{\sqrt[3]{y_1}}{\sqrt[3]{y_2}} = \frac{w^2 - 1}{1 - w} = -w - 1 = w^2,$$

e il rapporto tra i due numeri reali $\sqrt[3]{y_1}$ e $\sqrt[3]{y_2}$ sarebbe complesso.

Nota. Anche se le radici sono reali, le formule di Cardano richiedono dunque di estrarre radici di numeri complessi, che sappiamo fare solo scrivendo questi numeri in forma trigonometrica. Si può procedere come segue. Posto:

$$-\frac{q}{2} = \rho\cos\theta, \frac{q^2}{4} + \frac{p^3}{27} = -\rho^2\sin^2\theta,$$

la formula di Cardano diventa:

$$\alpha = \sqrt[3]{\rho(\cos\theta + i\sin\theta)} + \sqrt[3]{\rho(\cos\theta - i\sin\theta)}.$$

I valori dei due radicali sono, rispettivamente,

$$\rho^{\frac{1}{3}}(\cos\frac{\theta+2k\pi}{3} + i\sin\frac{\theta+2k\pi}{3}),\ \rho^{\frac{1}{3}}(\cos\frac{\theta+2k\pi}{3} - i\sin\frac{\theta+2k\pi}{3})$$

per $k = 0, 1, 2$. I valori vanno poi presi in modo che il loro prodotto sia reale, e per questo k deve avere lo stesso valore nelle due espressioni. Ne segue

$$\alpha = 2\rho^{\frac{1}{3}}\cos\frac{\theta+2k\pi}{3},$$

per cui le radici sono:

$$\alpha_1 = 2\rho^{\frac{1}{3}}\cos\frac{\theta+2k\pi}{3}, \alpha_2 = 2\rho^{\frac{1}{3}}\cos(\frac{\theta+2k\pi}{3} + 120^0), \alpha_3 = 2\rho^{\frac{1}{3}}\cos(\frac{\theta+2k\pi}{3} + 240^0),$$

valori che si possono calcolare noti ρ e θ. Ma per ipotesi $\rho = \sqrt{-\frac{p^3}{27}}$ e $\cos\theta = -\frac{q}{2\rho}$, e quindi ρ e θ si potranno calcolare usando per esempio i logaritmi.

L'estrazione di radici di numeri complessi non è un limite delle formule di Cardano: nel caso in cui tutte le soluzioni sono reali si può dimostrare infatti che non è possibile esprimerle in funzione dei coefficienti estraendo solo radici di numeri reali.

Raccogliendo quanto visto, l'analogo della (4.1) per le equazioni di terzo grado è:

$$\alpha_{1,2,3} = \frac{1}{3}[(\alpha_1+\alpha_2+\alpha_3) + \sqrt[3]{(\alpha_1+w\alpha_2+w^2\alpha_3)^3} + \sqrt[3]{(\alpha_1+w^2\alpha_2+w\alpha_3)^3}$$

da cui, per le considerazioni precedenti sulla scelta dei radicali,

$$\begin{aligned}
\alpha_1 &= \frac{1}{3}[(\alpha_1+\alpha_2+\alpha_3) + (\alpha_1+w\alpha_2+w^2\alpha_3) + (\alpha_1+w^2\alpha_2+w\alpha_3)] \\
\alpha_2 &= \frac{1}{3}[(\alpha_1+\alpha_2+\alpha_3) + w^2(\alpha_1+w\alpha_2+w^2\alpha_3) + w(\alpha_1+w^2\alpha_2+w\alpha_3)] \\
\alpha_3 &= \frac{1}{3}[(\alpha_1+\alpha_2+\alpha_3) + w(\alpha_1+w\alpha_2+w^2\alpha_3) + w^2(\alpha_1+w^2\alpha_2+w\alpha_3)]
\end{aligned}$$

4.3 L'equazione di quarto grado

Nella forma ridotta, alla quale ci si può ridurre, l'equazione è:

$$x^4 + px^2 + qx + r.$$

Come sopra abbiamo l'equazione lineare $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$. Per trovare le altre tre cerchiamo una funzione delle quattro radici che assuma solo tre

valori per le 4!=24 permutazioni. La funzione $z = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4$ è a sei valori, ma il quadrato $z_1 = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2$ ne ha tre: oltre a z_1 abbiamo $z_2 = (\alpha_1 - \alpha_2 + \alpha_3 - \alpha_4)^2$ e $z_3 = (\alpha_1 - \alpha_2 - \alpha_3 + \alpha_4)^2$. Esprimendo le funzioni simmetriche elementari delle z_i in termini dei coefficienti dell'equazione otteniamo la risolvente:

$$z^3 + 8pz^2 + 16(p^2 - 4r)z - 64q^2 = 0.$$

Le radici quadrate delle tre soluzioni z_1, z_2, z_3 di questa equazione permettono di scrivere:

$$\begin{aligned} \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4 &= \sqrt{z_1}, \\ \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 &= \sqrt{z_2}, \\ \alpha_1 - \alpha_2 - \alpha_3 + \alpha_4 &= \sqrt{z_3}, \end{aligned}$$

che assieme alla $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ danno un sistema di quattro equazioni in quattro incognite, che ha le soluzioni:

$$\begin{aligned} \alpha_1 &= \frac{1}{4}(\sqrt{z_1} + \sqrt{z_2} + \sqrt{z_3}), \quad \alpha_2 = \frac{1}{4}(\sqrt{z_1} - \sqrt{z_2} - \sqrt{z_3}), \\ \alpha_3 &= \frac{1}{4}(-\sqrt{z_1} + \sqrt{z_2} - \sqrt{z_3}), \quad \alpha_4 = \frac{1}{4}(-\sqrt{z_1} - \sqrt{z_2} + \sqrt{z_3}), \end{aligned}$$

(i segni dei radicali vanno scelti in modo che il prodotto $\sqrt{z_1}\sqrt{z_2}\sqrt{z_3}$ valga $-8q$).

Un'altra funzione a tre valori è $z_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, che assume gli altri due valori $z_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$ e $z_3 = \alpha_2\alpha_3 + \alpha_1\alpha_4$ (si tratta della funzione considerata da Lagrange). Un'altra è $z = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$. La funzione $z = \alpha_1\alpha_4 - \alpha_2\alpha_3$ è a sei valori, che però sono opposti a coppie, e dunque conduce a un'equazione di sesto grado che contiene l'incognita solo a potenze pari. La $z = \alpha_i + \alpha_j$ (considerata da Ampère) è a sei valori, e avendosi $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ questi valori sono opposti a coppie; si ottiene l'equazione $z^6 + 2pz^4 + (p^2 - 4r)z^2 - q^2 = 0$, e posto $z^2 = y$, la risolvente cubica $y^3 - 2py^2 + (p^2 - 4r)y + p^2$.

4.4 Teorema di Ruffini–Abel

Il successo dei metodi qui esposti per la risoluzione per radicali delle equazioni di grado al più 4 si deve in particolare al fatto che è possibile costruire funzioni delle radici a più valori una potenza delle quali sia a un valore (simmetrica) o a due valori (se i due valori sono uguali e di segno opposto la funzione si dice *alternante*). Per l'equazione di secondo grado abbiamo infatti considerato la funzione alternante $\alpha_1 - \alpha_2$ il cui quadrato è il discriminante Δ, che è simmetrico. Per l'equazione di terzo grado abbiamo utilizzato la funzione $\alpha_1 + w\alpha_2 + w^2\alpha_3$ che ha per cubo una funzione a due valori $\frac{1}{2}(q \pm 3\sqrt{-3\Delta})$, e

per l'equazione di quarto grado a partire dalla $z = \alpha_1\alpha_2 + \alpha_3\alpha_4$ si può ottenere una funzione il cui cubo è a due valori: $z_1 + wz_2 + w^2z_3$, dove gli z_i sono i tre valori della z.

Pe $n \geq 5$ non esistono funzioni di variabili algebricamente indipendenti a più di due valori che abbiano una potenza a uno o due valori. Sussistono in proposito i seguenti lemmi.

4.1 Lemma. *Le funzioni simmetriche e le alternanti di variabili algebricamente indipendenti sono le sole che possono avere potenze simmetriche.*

Dim. Sia $\varphi = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ una funzione non simmetrica, e sia φ^p simmetrica. Decomponendo p in fattori primi si può supporre p primo. Esiste almeno una trasposizione (α_i, α_j) che cambia un valore φ_1 della φ in un altro valore φ_2, mentre per ipotesi $\varphi_1^p = \varphi_2^p$. Se w è una radice primitiva $p-$esima dell'unità si ha allora $\varphi_2 = w\varphi_1$. Applicando di nuovo la trasposizione (α_i, α_j) da questa uguaglianza otteniamo la $\varphi_1 = w\varphi_2$, che sostituita nella precedente dà $\varphi_2 = w^2\varphi_2$ e quindi $w^2 = 1$, che assieme al fatto che p è primo implica $p = 2$ e perciò $w = -1$. Ne segue $\varphi_1 = -\varphi_2$, e quindi se φ non è alternante è simmetrica. ♢

4.2 Lemma. *Per $n \geq 5$, una funzione di n variabili algebricamente indipendenti che ha una potenza a due valori è essa stessa a due valori.*

Dim. Sia φ una funzione a più di due valori tale che φ^p sia a due valori (decomponendo p in fattori primi lo si può supporre primo). Poiché i tre cicli generano il gruppo di tutte le permutazioni pari, esiste un 3–ciclo che cambia il valore φ_1 in un altro valore φ_2, mentre lo stesso 3–ciclo lascia invariata la potenza φ^p, che è supposta a due valori. Avremo allora $\varphi_2 = w\varphi_1$; applicando il 3–ciclo a φ_2 otteniamo φ_3, e applicandolo a φ_3 otteniamo φ_1. Dunque $\varphi_1 = w^3\varphi_1$, da cui $w^3 = 1$ e $p = 3$. Analogamente, esiste un 5–ciclo che lascia invariata φ^p (anche i 5–cicli generano tutte le permutazioni pari, perché un 3–ciclo si ottiene come prodotto di due 5–cicli: (1,2,3)=(1,3,5,4,2)(1,3,2,4,5)) per cui si ottiene nello stesso modo $p = 5$, che contraddice $p = 3$. ♢

Ricordiamo che per "equazione generale di grado n sul campo K" si intende la particolare equazione $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + (-1)^n a_n = 0$ sul campo $K(a_1, a_2, \ldots, a_n)$, dove le a_i sono algebricamente indipendenti su K; le radici $\alpha_1, \alpha_2, \ldots, \alpha_n$ dell'equazione sono allora anch'esse indipendenti su K (Teor. 3.27). Data ora un'espressione per radicali di una radice α_i, si può sempre supporre che essa sia contenuta nel campo $K(\underline{\alpha}) = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, sia cioè una funzione razionale delle radici. Sussiste infatti il seguente *teorema delle irrazionalità naturali*, che diamo senza dimostrazione (ma si veda la Nota 1 qui sotto):

4.3 Teorema (ABEL) *Siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ le radici di un polinomio a coefficienti in un campo K. Se una radice α_i si esprime per radicali di elementi non appartenenti a $K(\underline{\alpha})$, allora si esprime anche per radicali di elementi appartenenti a $K(\underline{\alpha})$.*

Diciamo "irrazionalità naturale" dell'equazione $f(x) = 0$ un elemento di $K(\underline{\alpha})$, cioè una funzione razionale delle radici di $f(x)$, e "irrazionalità accessoria" un elemento algebrico su K che non appartiene a $K(\underline{\alpha})$.

4.4 Note. 1. Il Teor. 4.3 si dimostra facilmente se si considera il gruppo di Galois G di $f(x)$ su K. Infatti, se aggiungendo a K alcune irrazionalità accessorie di $f(x) = 0$ il gruppo G si riduce a un sottogruppo H, sia γ una irrazionalità naturale tale che $G_\gamma = H$. Allora il gruppo di Galois su $K(\gamma)$ è H. Pertanto, la riduzione del gruppo mediante l'aggiunzione di irrazionalità accessorie si ottiene anche mediante l'aggiunzione di una irrazionalità naturale.

2. Il Teor. 4.3 è quanto manca della dimostrazione data da Ruffini.

4.5 Teorema. (RUFFINI–ABEL) *Per $n \geq 5$ l'equazione generale di grado n non è risolubile per radicali.*

Dim. Sia x_1 una radice dell'equazione, e sia $y = \sqrt[p]{u}$ la prima radice che compare nell'espressione per radicali di x_1. La u è una funzione razionale dei coefficienti s_i, e dunque è simmetrica nelle x_i. Allora y, che possiamo supporre essere una funzione razionale delle x_i (Teor. 4.3), ha una potenza simmetrica, ma non è essa stessa simmetrica, altrimenti sarebbe una funzione razionale delle radici, e non un radicale di una funzione di queste (apparterrebbe cioè al campo). Dunque y è alternante (Lemma 4.2) e $p = 2$ (dimostrazione del Lemma 4.1)[5]. Operando razionalmente con y e con i coefficienti dell'equazione che sono funzioni simmetriche delle radici, otteniamo una funzione y_1 che è una funzione razionale di funzioni simmetriche e di una alternante, e dunque è a due valori. Di questa occorre ora estrarre una radice, diciamo $q-$esima: $y_2 = \sqrt[q]{y_1}$. Se ora y_2 ha più di due valori abbiamo una contraddizione: la sua potenza $q-$esima è y_1, che è a due valori, e ciò per $n \geq 5$ contraddice il Lemma 4.2. Ne segue che y_2 è a due valori, $q = 2$, e pertanto $y_2^2 = y_1$. Ma allora i due valori di y_2 sono $\pm\sqrt[q]{y_1}$, cioè hanno segno opposto, e perciò y_2 è alternante. Il suo quadrato y_1 è allora una funzione simmetrica, mentre abbiamo visto che è alternante. ♢

Nota. L'equazione di cui si parla nel teorema è l'equazione generale: i suoi coefficienti, che sono le funzioni simmetriche elementari delle radici x_i, sono quindi algebricamente indipendenti. Anche le x_i sono allora algebricamente indipendenti (Teor. 3.27), per cui si possono applicare i lemmi 4.1 e 4.2.

[5] Il primo radicale che si trova è quindi quadratico, come succede nei casi noti per $n \leq 4$.