Da "E. Giusti, Ipotesi sulla natura degli oggetti matematici"

Nota 2.
I numeri complessi.

Quelli che oggi chiamiamo numeri complessi traggono origine dalla soluzione delle equazioni algebriche; non come a volte si dice dalla volontà di dare soluzioni anche a equazioni, come ad esempio $x^2 + 1 = 0$, che non ne hanno,[1] ma per esprimere le soluzioni reali di equazioni di terzo grado. Come abbiamo visto, la soluzione dell'equazione

$$x^3 - 3px - 2q = 0$$

è data dalla formula di Cardano (o meglio di Del Ferro)

$$x = \sqrt[3]{q + \sqrt{q^2 - p^3}} + \sqrt[3]{q - \sqrt{q^2 - p^3}}.$$

A un esame di questa formula, salta subito agli occhi una difficoltà. Se $q^2 - p^3$ è maggiore o uguale a zero, essa permette di calcolare una soluzione dell'equazione mediante l'estrazione di radici, ma cosa succede se la quantità $q^2 - p^3$ sotto radice quadrata è negativa?

Questa situazione si verifica effettivamente. Ad esempio, se applichiamo la formula Cardano all'equazione

$$x^3 - 9x + 8 = 0$$

in cui $p = 3$ e $q = -4$, si trova

$$x = \sqrt[3]{-4 + \sqrt{16 - 27}} = \sqrt[3]{-4 - \sqrt{16 - 27}}$$

in cui compare la radice quadrata di un numero negativo. D'altra parte l'equazione si può risolvere esplicitamente, se si osserva che una radice è $x = 1$, e pertanto risulta

$$x^3 - 9x + 8 = (x - 1)(x^2 + x - 8).$$

[1]Secondo tale leggenda, si sarebbe introdotto a questo fine un numero i, con il quadrato uguale a -1. In questo modo, l'equazione $x^2 + 1 = 0$ ha soluzioni i e $-i$.

Le altre due radici si ottengono allora risolvendo l'equazione $x^2+x-8=0$, e sono

$$x = \frac{-1 \pm \sqrt{33}}{2}.$$

Abbiamo dunque una situazione paradossale: da una parte l'equazione ha tre radici reali, che nel nostro esempio si possono calcolare esplicitamente, dall'altra la formula risolutiva non è in grado di darcene nemmeno una, a meno che non si dia un senso alle radici dei numeri negativi. Siamo in presenza del *caso irriducibile* dell'equazione di terzo grado, chiamato così perché la sua soluzione non può essere ricondotta semplicemente al calcolo di radicali, che ha fatto discutere per più di due secoli.

Il primo che abbia tentato di dare un senso al caso irriducibile della formula di Cardano è stato un altro matematico bolognese, Raffaele Bombelli, nella sua *Algebra*, pubblicata nel 1572.[2] Oltre ai ben noti segni + e − e alle loro regole di moltiplicazione (+ per + fa +, + per − fa −, − per − fa +), Bombelli introduce due nuovi "segni", che chiama "più di meno" e "meno di meno", con le regole di moltiplicazione:

> Più via più di meno, fa più di meno.
> Meno via più di meno, fa meno di meno.
> Più via meno di meno, fa meno di meno.
> Meno via meno di meno, fa più di meno.
> Più di meno via più di meno, fa meno.
> Più di meno via men di meno, fa più.
> Meno di meno via più di meno, fa più.
> Meno di meno via men di meno, fa meno.

Ad esempio, per moltiplicare $4+\mathrm{di}-\sqrt{2}$ per $3+\mathrm{di}\sqrt{8}$ Bombelli dice:[3]

> Moltiplicaremo prima $+\mathrm{di}-\sqrt{2}$ via $+\mathrm{di}-\sqrt{8}$, fa -4, poi moltiplicaremo 3 via 4, fa 12, che gionto con -4 fa $+8$. Dipoi moltiplicaremo 3 via $+\mathrm{di}-\sqrt{2}$, farà $+\mathrm{di}-\sqrt{18}$, e dipoi 4 via $+\mathrm{di}-\sqrt{8}$, fa $+\mathrm{di}-\sqrt{128}$, che gionto con $+\mathrm{di}-\sqrt{18}$ fa $+\mathrm{di}-\sqrt{242}$, che gionto con $+8$ haveremo $8+\mathrm{di}-\sqrt{242}$ per produtto della moltiplicatione.

[2] Un'edizione moderna, a cura di U. Forti, è stata pubblicata da Feltrinelli, Milano 1966.

[3] La presenza delle radici deriva dal fatto che Bombelli applica i suoi risultati alla formula di Cardano, in cui le radici appaiono naturalmente. In effetti Bombelli moltiplica non i numeri che abbiamo riportato, ma le loro radici cubiche,

Si vede come si possono trovare le radici dei numeri negativi. Ad esempio, poiché per le regole dei segni più di meno 2 per più di meno 2 fa -4, una radice di -4 sarà più di meno 2 (e l'altra meno di meno 2).

Ritorniamo ora al nostro esempio. Avendo dato un senso alle radici di numeri negativi, la formula di Cardano si potrà scrivere

$$x = \sqrt[3]{-4 \text{più di meno} \sqrt{11}} + \sqrt[3]{-4 \text{meno di meno} \sqrt{11}}.$$

Per giungere alla soluzione, si devono ora calcolare le radici cubiche. Qui Bombelli non riesce a dare un metodo generale, e si limita a dire che per trovare la radice cubica di m più di meno n bisogna cercare "a tentoni" due numeri u e v tali che

$$u^2 + v^2 = \sqrt[3]{m^2 + n^2},$$
$$u^3 - 3uv^2 \quad = \quad m.$$

È immediato tradurre espressioni quali 3 più di meno 2" nella forma $3+2i$, e vedere nelle regole dei segni quelle della moltiplicazione tra numeri complessi. La realtà storica è però diversa: Bombelli non ha introdotto dei nuovi numeri, ma delle nuove "radici cubiche legate" $\sqrt[3]{a + \text{di} - b}$ e $\sqrt[3]{a - \text{di} - b}$, che si manipolano secondo le regole dei segni. I numeri che egli usa sono sempre gli stessi: i numeri reali positivi;[4] ma oltre ai segni usuali, $+$ e $-$, egli introduce due nuovi segni, più di meno" e meno di meno", con le relative regole di moltiplicazione. In questo modo, Bombelli riesce a dare un senso alle radici di numeri negativi, ma si arresta davanti alle radici cubiche delle nuove combinazioni numeriche, che non sa calcolare tranne che in alcuni casi costruiti ad hoc.

Salvo un apprezzamento di Leibniz, le idee di Bombelli non hanno seguito. I nuovi numeri $-$che non ci sono ancora$-$ si ripresentano però alcuni decenni più tardi in una forma diversa, ma sempre legati alle radici delle equazioni. Non si tratta più di dare senso alla formula di Cardano, ma di rispondere a un altro problema: quante radici ha un'equazione di grado n? In alcuni casi ce n'erano esattamente n; ad esempio l'equazione $x^2 - 1 = 0$ ha due soluzioni, 1 e -1. Altre volte invece ce ne potevano essere di meno: $x^2 + 1 = 0$ non ha soluzioni reali.

[4]In realtà, si dovrebbe parlare di un sistema numerico costituito dagli interi, dalle frazioni e dai *numeri surdi*, cioè i radicali; se abbiamo usato il termine "numeri reali" è stato solo per semplicità di espressione.

Davanti a questa situazione, Descartes enuncia il *teorema fondamentale dell'algebra*: ogni equazione ha tante soluzioni quant'è il suo grado, ma aggiunge che queste soluzioni

> non son sempre reali, ma talvolta soltanto immaginarie; cioè è sempre possibile immaginarne in ogni equazione tante quante ho detto, ma talvolta non v'è nessuna quantità che corrisponde a quelle che immaginiamo. Così, nonostante che nell'equazione $x^3 - 6x^2 + 13x - 10 = 0$ sia possibile immaginare tre radici, non ve n'è che una che sia reale, cioè 2.[5]

Descartes non ci dice cosa siano queste radici immaginarie, un termine che bisogna intendere alla lettera più che nel significato che ha assunto più tardi. C'erano però degli esempi provenienti dalle equazioni di secondo grado che ne suggerivano la forma. Ad esempio l'equazione $x^2 + 1 = 0$ ha formalmente le soluzioni $x = \pm\sqrt{-1}$,[6]; mentre l'equazione $x^2 - 2x + 5 = 0$ ha soluzioni $x = 1 \pm \sqrt{1-5} = 1 \pm 2\sqrt{-1}$. Le radici immaginarie delle equazioni di secondo grado sono dunque della forma $a + b\sqrt{-1}$.

In generale, si tenta di dimostrare che le radici immaginarie delle equazioni di ogni grado sono anch'esse della stessa forma. È questa l'interpretazione corrente del teorema fondamentale dell'algebra; un'interpretazione ambigua, perché si assume che ogni equazione abbia effettivamente tante radici quant'è il suo grado, e si cerca solo di dimostrare che queste radici non meglio precisate non possono essere che del tipo $a + b\sqrt{-1}$. Ad esempio, nel caso dell'equazione di terzo grado, si tratta di dimostrare che le radici date dalla formula cardanica nel caso irriducibile si possono scrivere nella forma $u + v\sqrt{-1}$, o in altre parole che la radice cubica di un numero complesso è sempre un numero complesso.

Di questo risultato vengono date dimostrazioni molto ingegnose, tra cui una da parte di Lagrange; tutte peraltro viziate dall'equivoco di fondo sulla formulazione del risultato da dimostrare. Nel frattempo, soprattutto ad opera di Eulero, i numeri complessi avevano mostrato singolari e inaspettate proprietà, tra cui la famosa *formula di Eulero* che collega le funzioni

[5] *Géométrie*, Leida 1637; *Oeuvres de Descartes*, a cura di C. Adam e P. Tannery, vol. VI, Vrin, Parigi 1982. Della *Géométrie* esiste una traduzione italiana in *Opere scientifiche di R. Descartes*, vol. II, a cura di E. Lojacono, UTET, Torino 1983, che indicheremo con *La Geometria*.

[6] Ricordiamo che il simbolo i per indicare la radice di -1 viene introdotto solo alla fine del Settecento.

trigonometriche con l'esponenziale:

$$e^{i\phi} = \cos\phi + i\sin\phi.$$

Formule come la precedente generarono non poche discussioni, segno se non altro dell'ambiguità che circondava ancora queste quantità immaginarie. Da segnalare in particolare la controversia sui logaritmi dei numeri negativi, che durante il Settecento coinvolse molti matematici. La questione venne sollevata incidentalmente da Leibniz, che in una lettera a Johann Bernoulli del marzo 1712 osservava i rapporti tra quantità negative e positive erano immaginari (ancora questo termine nel significato letterale!), dato che ad essi non corrispondeva nessun logaritmo. La replica di Bernoulli è immediata: dato che

$$d\log x = \frac{dx}{x} = \frac{d(-x)}{-x} = d\log(-x),$$

risulterà $\log x = \log(-x)$.

Comincia qui un nutrito scambio di lettere, nelle quali Leibniz tenta senza successo di convincere l'amico. Gli argomenti vengono presi sia dal calcolo differenziale, come quello appena visto, sia in manipolazioni algebriche; ad esempio Leibniz osserva che essendo $x^4 = (ix)^4$, si dovrebbe avere $4\log x = 4\log(ix)$, e dunque $\log x = \log(ix)$, con la conclusione assurda che quantità immaginarie come ix sarebbero dotate di logaritmi reali. È però anche vero che lo stesso argomento sembrerebbe dar ragione a Bernoulli, dato che da $x^2 = (-x)^2$ segue $\log x = \log(-x)$.

La soluzione dei paradossi, che viene data da Eulero in una magistrale memoria del 1749, è in un certo senso ancora più paradossale. Sulla base della sua formula, Eulero osserva che $e^{2ik\pi} = \cos 2k\pi + i\sin 2k\pi = 1$, e quindi se $e^y = x$ (cioè se $y = \log x$) si ha anche $e^{y+2ik\pi} = x$ per ogni intero k. In altre parole, ogni numero non ha un solo logaritmo, ma infiniti, che differiscono tra loro per multipli della quantità immaginaria $2i\pi$.

Non è difficile credere che la soluzione di Eulero non convinse tutti; la controversia continuò fino alla fine del secolo senza nuove argomentazioni, e coinvolse anche una discussione sulla natura dei numeri immaginari, che alcuni volevano totalmente separati dai reali, giungendo fino ad affermare che lo zero immaginario era altra cosa dallo zero reale.

La chiarificazione delle ambiguità viene all'inizio dell'Ottocento da due direzioni. Da una parte J. Robert Argand e con più efficacia C. F. Gauss introducono la rappresentazione geometrica dei numeri complessi $x + iy$ mediante i punti (x, y) del piano cartesiano, individuando i numeri reali nell'asse delle ascisse. In questo modo i numeri complessi perdevano il loro carattere "immaginario" e diventavano un'estensione a due dimensioni del continuo unidimensionale dei numeri reali.[7] In particolare, la moltiplicazione per i corrisponde alla rotazione di 90° in senso antiorario.

Dall'altra parte, nel suo *Cours d'analyse* Cauchy toglie ogni mistero alle equazioni tra quantità complesse, affermando che esse non sono altro che coppie di equazioni (una per la parte reale, l'altra per la parte immaginaria) tra quantità reali.

Una volta precisato il senso delle operazioni con i numeri complessi, lo stesso teorema fondamentale dell'algebra prende un aspetto differente: non si tratta più come prima di dimostrare che le soluzioni "immaginarie" si potevano sempre scrivere nella forma $a+ib$, ma di provare che ogni equazione aveva effettivamente un numero di soluzioni uguale al suo grado.

Si vede subito che è sufficiente dimostrare che ogni equazione algebrica ha una soluzione. Infatti se $P(x)$ è un polinomio di grado n, che ha una radice a, allora $P(x)$ è divisibile per $x-a$, e quindi $P(x) = (x-a)Q(x)$ con $Q(x)$ di grado $n-1$. D'altra parte anche $Q(x)$ avrà una radice b, e si scriverà nella forma $(x-b)R(x)$, con $R(x)$ di grado $n-2$, $R(x)$ avrà una radice c, e così via, fino a esaurire il grado n di $P(x)$.

Una volta enunciato correttamente, la dimostrazione del teorema fondamentale non è particolarmente difficile. Lo stesso Gauss ne dà tre dimostrazioni diverse, seguito poco dopo da Cauchy. Semmai, è proprio l'identificazione di un numero complesso con una coppia di numeri reali, e di conseguenza delle funzioni complesse come coppie di funzioni reali, che rende difficile l'emergere della teoria delle funzioni olomorfe, delle quali all'inizio si tarda a riconoscere le caratteristiche peculiari. Una volta che queste cominciano ad essere stabilite, prima fra tutte l'indipendenza dell'integrale dal cammino di integrazione, la teoria andrà prendendo forma, fino ad affermarsi come una delle grandi scoperte della matematica ottocentesca.

Nota 4.
Le equazioni di terzo e quarto grado.

Dopo una serie di tentativi infruttuosi che accompagnarono gran parte della matematica medievale, la formula risolutiva per le equazioni di terzo

[7] Più tardi, i quaternioni di Hamilton e gli "ottetti" di Cayley introducevano altri "numeri" di dimensione 4 e 8.

grado del tipo “cubo uguale a cose e numero”, ossia in formule:[8]

$$x^3 - 3px - 2q = 0 \tag{1}$$

venne trovata agli inizi del Cinquecento dal matematico bolognese Scipione del Ferro:

$$x = \sqrt[3]{q + \sqrt{q^2 - p^3}} + \sqrt[3]{q - \sqrt{q^2 - p^3}}. \tag{2}$$

In effetti, nei secoli precedenti la scoperta di Del Ferro molti matematici si erano cimentati con equazioni di terzo grado, e anche con equazioni di grado superiore,[9] senza però riuscire ad ottenere risultati decisivi.

Agli inizi si trattava di vere e proprie formule errate, in cui le equazioni di terzo grado venivano risolte adattando opportunamente le formule note per quelle di secondo grado. Ad esempio, nel *Libro di ragioni* del fiorentino Paolo Gherardi[10] troviamo regole di soluzione per l’equazione $x^3 - 2ax - bx - c = 0$ che si possono tradurre nella formula risolutiva

$$x = a + \sqrt{a^2 + (b + c)}.$$

Detto altrimenti, il Gherardi suggeriva di trattare l’equazione come se avesse cx al posto di c, nel qual caso diventa $x^3 - 2ax^2 - (b + c)x = 0$, e dividendo per x[11] si riduce effettivamente all’equazione di secondo grado $x^2 - 2ax - (b + c) = 0$, che ha la radice data del Gherardi.

Più tardi, le ricerche vertono su speciali equazioni di terzo grado, provenienti da problemi che si sapevano risolvere altrimenti, e dalla cui soluzione si sperava di ottenere lumi per il caso generale.[12] Un problema tipico era quello di trovare l’interesse conoscendo i capitali iniziale e finale e la durata del prestito; un problema la cui soluzione era nota fin da Leonardo Pisano, e che dà luogo a un’equazione di grado uguale al numero di anni di prestito.

---

[8] Sarà appena il caso di ricordare che né i matematici medievali, né quelli rinascimentali, avevano a disposizione notazioni algebriche, e che sia le equazioni sia le loro soluzioni venivano espresse a parole, queste ultime attraverso delle regole risolutive, ossia dei precetti per calcolare la soluzione.

[9] Nel *Trattato d’abaco* di Piero della Francesca (a cura di G. Arrighi, Domus Galilaeana, Pisa 1970) troviamo formule risolutive per equazioni fino al sesto grado incluso.

[10] A cura di G. Arrighi, Pacini Fazzi, Lucca 1987.

[11] Ricordiamo che usualmente la radice 0 e quelle negative non venivano prese in considerazione.

[12] Si veda a questo proposito il mio *L’algebra di Piero della Francesca: osservazioni e congetture*, Boll. Storia Sci. Mat. 1991.

È stato con ogni probabilità un tentativo simile a condurre alla soluzione dell'equazione (1). Come si sa, Scipione del Ferro non ha lasciato nessuno scritto da cui possiamo ricavare la genesi della formula risolutiva. Alcuni decenni fa, E. Bortolotti ne ha proposto una ricostruzione,[13] che tra l'altro ha il merito di condurre naturalmente a un'equazione priva del termine di secondo grado. Secondo Bortolotti, la formula di Del Ferro sarebbe scaturita dal tentativo di scrivere radicali cubici del tipo $\sqrt[3]{m \pm \sqrt{n}}$ nella forma $u \pm \sqrt{v}$; in altre parole di trovare u e v tali che

$$\begin{aligned} u + \sqrt{v} &= \sqrt[3]{m + \sqrt{n}} \\ u - \sqrt{v} &= \sqrt[3]{m - \sqrt{n}}. \end{aligned}$$

La soluzione di queste equazioni è immediata. Infatti, sommando membro a membro queste due equazioni si ottiene il valore di u:[14]

$$2u = \sqrt[3]{m + \sqrt{n}} + \sqrt[3]{m - \sqrt{n}}. \tag{3}$$

Abbiamo dunque un problema di cui si conosce la soluzione. Invece di fermarsi a questo punto, Scipione del Ferro continua a manipolare le due equazioni, fino ad ottenere un'equazione di terzo grado che ha la stessa u, o meglio $2u$, come soluzione.

Se si moltiplicano le due equazioni membro a membro, si ottiene

$$u^2 - v = \sqrt[3]{(m + \sqrt{n})(m - \sqrt{n})} = \sqrt[3]{m^2 - n},$$

e quindi

$$v = u^2 - \sqrt[3]{m^2 - n}.$$

Eleviamo ora al cubo la prima equazione; otterremo

$$m + \sqrt{n} = u^3 + 3uv + 3u^2\sqrt{v} + v\sqrt{v},$$

da cui, uguagliando separatamente le parti con le radici e quelle senza, avremo[15]

$$m = u^3 + 3uv.$$

[13] *L'algebra nella Scuola matematica bolognese del secolo XVI*, Periodico di Matem. 1925.

[14] Analogamente, il valore di v, che non è rilevante per quanto diremo, si può ricavare sottraendo le due equazioni.

[15] Come in precedenza, l'altra equazione $\sqrt{n} = (3u^2 + v)\sqrt{v}$ non ci interessa.

Sostituendo in quest'ultima il valore di v che avevamo trovato, si giunge all'equazione

$$u^3 + 3u^3 - 3u\sqrt[3]{m^2 - n} = m,$$

ossia, raccogliendo e moltiplicando per 2:

$$8u^3 - 6u\sqrt[3]{m^2 - n} - 2m = 0.$$

Questa equazione ha come soluzione il valore di u dato dalla (3). Se si pone allora $x = 2u$, l'equazione

$$x^3 - 3x\sqrt[3]{m^2 - n} - 2m = 0$$

ha soluzione

$$x = \sqrt[3]{m + \sqrt{n}} + \sqrt[3]{m - \sqrt{n}}.$$

Di qui segue subito la formula risolutiva dell'equazione $x^3 - 3px - 2q = 0$; basterà infatti prendere $m = q$ e scegliere n in modo che risulti $p = \sqrt[3]{m^2 - n} = \sqrt[3]{q^2 - n}$. Si vede subito che deve essere $n = q^2 - p^3$, e di qui si ricava la soluzione di Scipione del Ferro.

Fin qui la ricostruzione di Bortolotti; una proposta che da una parte conduce a un'equazione priva naturalmente del termine di secondo grado, e dall'altra inserisce il procedimento risolutivo in un filone di ricerca ben documentato in tutto il medioevo occidentale. Nonostante la mancanza del termine di secondo grado, la soluzione di Scipione del Ferro è generale, dato che ogni equazione di terzo grado

$$y^3 + 3ay^2 + by + c = 0 \tag{4}$$

si può ridurre alla forma (1) introducendo la nuova incognita $x = y + a$. Si ha infatti $y = x - a$, $y^2 = x^2 - 2ax + a^2$, $y^3 = x^3 - 3ax^2 + 3a^2x - a^3$, e con la sostituzione di questi valori l'equazione diventa

$$x^3 - 3ax^2 + 3a^2x - a^3 + 3a(x^2 - 2ax + a^2) + b(x - a) + c = 0,$$

e semplificando:

$$x^3 + (b - 3a^2)x + (2a^3 - ab + c) = 0.$$

Quest'ultima equazione non contiene il termine in x^2; una volta risolta, basterà sottrarre a alla soluzione, per ottenere quella dell'equazione (4).

Come abbiamo detto, la ricostruzione del metodo di Scipione del Ferro è totalmente congetturale. Più documentata è invece la soluzione di Nicolò Tartaglia, che come ci narra egli stesso la trovò dopo aver avuto notizia dell'avvenuta scoperta. L'idea di Tartaglia è di scomporre l'incognita x nella somma $y + z$. Ricordando che $(y+z)^3 = y^3 + z^3 + 3y^2z + 3yz^2 = y^3 + z^3 + 3yz(y+z)$, l'equazione (1) diventa

$$y^3 + z^3 + 3yz(y+z) - 3p(y+z) - 2q = 0.$$

Se ora si prende $z = \frac{p}{y}$, si ha $yz = p$, e dunque i due termini che contengono la somma $y + z$ si cancellano l'un l'altro, lasciando l'equazione

$$y^3 + \frac{p^3}{y^3} - 2q = 0$$

ossia moltiplicando per y^3:

$$y^6 - 2qy^3 + p^3 = 0.$$

Quest'ultima è solo apparentemente di sesto grado; in realtà è un'equazione di secondo grado nell'incognita y^3, e ha soluzione

$$y^3 = q \pm \sqrt{q^2 - p^3}.$$

Si può scegliere a piacere uno dei segni $+$ o $-$. Se si prende il primo, si ha

$$y = \sqrt[3]{q + \sqrt{q^2 - p^3}}$$

e dunque

$$z^3 = \frac{p^3}{y^3} = \frac{p^3}{q + \sqrt{q^2 - p^3}}.$$

Da questa, moltiplicando numeratore e denominatore per $q - \sqrt{q^2 - p^3}$ si ricava $z^3 = q - \sqrt{q^2 - p^3}$, e dunque

$$z = \sqrt[3]{q - \sqrt{q^2 - p^3}}$$

e in conclusione

$$x = y + z = \sqrt[3]{q + \sqrt{q^2 - p^3}} + \sqrt[3]{q - \sqrt{q^2 - p^3}},$$

cioè la formula di Del Ferro.

Come è noto, Tartaglia comunicò la sua soluzione a Gerolamo Cardano, mediante una poesiola tanto nota quanto brutta, che eviteremo di riportare per la centesima volta. Quest'ultimo, che aveva giurato di mantenere il segreto, una volta venuto a sapere che lo scopritore della formula risolutiva non era Tartaglia ma Del Ferro, si ritenne sciolto dal giuramento e pubblicò per primo nella sua *Ars magna*[16] la formula risolutiva (2), che da allora prese il nome di *formula di Cardano*. Ebbe così inizio una lunga controversia, tra accuse di furto, cartelli di sfida e risposte, tra Tartaglia da una parte, e Cardano e il suo discepolo Ludovico Ferrari dall'altra. I sei cartelli di sfida, sfida matematica, s'intende, lanciati da Tartaglia, e le sei risposte di Cardano e Ferrari, non ci apprendono nulla riguardo al tema che stiamo trattando; ma uno dei risultati, sebbene indiretti, della controversia, fu la soluzione da parte del Ferrari dell'equazione di quarto grado

$$x^4 + 2ax^3 + bx^2 + cx + d = 0. \tag{5}$$

Il metodo di Ferrari consiste nel portare a secondo membro i tre ultimi termini, e ad aggiungere ad ambo i membri la quantità a^2x^2. In questo modo si ottiene l'equazione

$$x^4 + 2ax^3 + a^2x^2 = (a^2 - b)x^2 - cx - d.$$

Il primo membro è un quadrato perfetto: $(x^2+ax)^2$, mentre in generale il secondo membro non lo è. Si aggiunge allora a sinistra e a destra la quantità $y^2+2y(x^2+ax)$. In questo modo il primo membro è il quadrato di x^2+ax+y, e l'equazione diventa

$$(x^2 + ax + y)^2 = (a^2 + 2y - b)x^2 + (2ay - c)x + y^2 - d.$$

A questo punto si sceglie y in modo che la quantità a secondo membro sia un quadrato perfetto: $(mx + n)^2$. Dovrà essere allora

$$m^2x^2 + 2mnx + n^2 = (a^2 + 2y - b)x^2 + (2ay - c)x + y^2 - d$$

e dunque

$$\begin{aligned} m &= \sqrt{a^2 + 2y - b} \\ n &= \sqrt{y^2 - d} \\ 2mn &= 2ay - c. \end{aligned}$$

[16] *Artis magnae, sive de regulis algebraicis, Liber unus*, Norimberga 1545.

Queste tre equazioni hanno una soluzione se $2ay - c$ è uguale al doppio prodotto delle prime due righe. Dovremo dunque avere $(2ay - c)^2 = 4(y^2 - d)(a^2 + 2y - b)$, e quindi y dovrà essere una soluzione dell'equazione ausiliaria di terzo grado

$$8y^3 - 4by^2 + (4ac - 8d)y + 4d(b - a^2) - c^2 = 0.$$

Se allora y è una soluzione di questa equazione, si potrà scrivere

$$(x^2 + ax + y)^2 = \left(x\sqrt{a^2 + 2y - b} + \sqrt{y^2 - d}\right)^2$$

e dunque l'equazione originale si spezzerà nelle due equazioni di secondo grado

$$x^2 + ax + y = x\sqrt{a^2 + 2y - b} + \sqrt{y^2 - d}$$

e

$$x^2 + ax + y = -x\sqrt{a^2 + 2y - b} - \sqrt{y^2 - d}.$$

La soluzione di queste ultime dà le quattro radici dell'equazione (5).

Nota 5.
La risolubilità per radicali delle equazioni algebriche.

Il teorema fondamentale dell'algebra, che abbiamo visto nella nota precedente, ci dice che ogni equazione di grado n a coefficienti complessi ha n radici complesse. Esso non ci dà però nessuna indicazione per trovare queste radici, meno che mai una formula risolutiva.

Naturalmente tali formule sono note per equazioni di grado basso. Ad esempio le soluzioni dell'equazione di secondo grado $x^2 + 2ax + b = 0$ sono date dalla formula

$$x = -a \pm \sqrt{a^2 - b}$$

e quelle dell'equazione di terzo grado $x^3 - 3px - 2q = 0$ dalla formula di Cardano

$$x = \sqrt[3]{q + \sqrt{q^2 - p^3}} + \sqrt[3]{q - \sqrt{q^2 - p^3}}.$$

Una formula dello stesso tipo, anche se molto più complicata, sussiste per le equazioni di quarto grado.

Una caratteristica comune di queste formule è che la soluzione delle equazioni in questione è data combinando i coefficienti delle equazioni mediante le operazioni aritmetiche: $+$, $-$, $\times$, $:$ e le estrazioni di radicali di vari gradi. In altre parole, le equazioni di grado minore di 5 sono *risolubili per radicali*.

Per quanto riguarda equazioni di grado superiore al quarto, le ricerche di formule risolutive simili alle precedenti non condussero a risultati positivi.

Alla fine del Settecento, J. L. Lagrange affronta il problema da un nuovo punto di vista. Invece di cercare una soluzione dell'equazione di quinto grado per mezzo di combinazioni dei suoi coefficienti, egli riesamina le soluzioni note delle equazioni di grado inferiore, nel tentativo di trovare, al di là della diversità delle formule risolutive e dei metodi impiegati per scoprirle, un sottofondo comune che facesse capire il motivo della loro risolubilità.

Data un'equazione di grado n

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

e dette x_1, x_2, …, x_n le sue radici, l'idea di Lagrange consiste nel cercare un'opportuna combinazione $f(x_1, x_2, \ldots, x_n)$ che prenda k valori diversi f_1, f_2, …, f_k quando si permutano le radici in tutti i modi possibili.

Questi valori della funzione f saranno allora soluzioni di un'equazione di grado k:

$$(y - f_1)(y - f_2)\cdots(y - f_k) = 0,$$

i cui coefficienti potranno essere espressi per mezzo di quelli dell'equazione originale a_0, a_1, …, a_{n-1}.

Se riusciamo a risolvere quest'ultima equazione, avremo trovato i valori di certe combinazioni delle radici, a partire dai quali potremo risalire alle radici stesse, e quindi potremo risolvere l'equazione di partenza.

Vediamo all'opera il metodo di Lagrange nel caso dell'equazione di quarto grado:

$$x^4 + mx^3 + nx^2 + px + q = 0.$$

Lagrange fa vedere che la funzione

$$f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$$

assume, quando si scambiano le radici, solo tre valori diversi:

$$\begin{aligned} y_1 &= x_1x_2 + x_3x_4 \\ y_2 &= x_1x_3 + x_2x_4 \\ y_3 &= x_1x_4 + x_2x_3, \end{aligned}$$ [17]

i quali saranno pertanto soluzioni dell'equazione di terzo grado

$$(y - y_1)(y - y_2)(y - y_3) = 0$$

che sviluppata diventa

$$y^3 - y^2(y_1 + y_2 + y_3) + y(y_1y_2 + y_1y_3 + y_2y_3) - y_1y_2y_3 = 0.$$

Introducendo ora al posto di y_1, y_2 e y_3 le loro espressioni in termini delle x_1, …, x_4, e usando le formule di Viète:

$$\begin{aligned}
&x_1 + x_2 + x_3 + x_4 = -m \\
&x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = n \\
&x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -p \\
&x_1x_2x_3x_4 = q
\end{aligned}$$

si trova

$$y^3 - ny^2 + (mp - 4q)y - q(m^2 - 4n) - p^2 = 0.$$

Risolta quest'ultima equazione, dai valori delle sue radici y_1, y_2 e y_3 potremo risalire a quelli delle radici dell'equazione di partenza. Posto infatti $z_1 = x_1x_2$, $z_2 = x_3x_4$, si ha

$$\begin{cases} z_1 + z_2 = y_1 \\ z_1z_2 = q \end{cases}$$

e dunque z_1 e z_2 sono soluzioni dell'equazione di secondo grado[18]

$$z^2 - y_1z + q = 0.$$

Risolta questa equazione, e trovate z_1 e z_2, dalle formule di Viète avremo:

$$\begin{aligned}
-p &= x_3x_4(x_1 + x_2) + x_1x_2(x_3 + x_4) = z_1(x_1 + x_2) + z_2(x_3 + x_4) \\
-m &= (x_1 + x_2) + (x_3 + x_4).
\end{aligned}$$

[17]Si vede subito che y_2 si ottiene da y_1 scambiando tra loro x_2 e x_3, mentre scambiando x_2 con x_4 si ottiene y_3. Tutte le altre permutazioni danno luogo a uno di questi tre valori; ad esempio se si porta x_1 in x_2, x_2 in x_4 e x_4 in x_1 lasciando inalterato x_3, y_1 diventa $x_2x_4 + x_3x_1 = y_2$.

[18]Che si ottiene ricavando una delle due incognite, ad esempio z_2, dalla prima equazione e sostituendo il valore così trovato nella seconda.

Questo è un sistema di due equazioni lineari nelle due incognite $x_1 + x_2$ e $x_3 + x_4$, che risolto dà:

$$x_1 + x_2 = \frac{p - mz_2}{z_2 - z_1}, \qquad x_3 + x_4 = \frac{mz_1 - p}{z_2 - z_1}.$$

Abbiamo così ottenuto i valori della somma $x_1 + x_2$ e del prodotto $x_1 x_2$:

$$\begin{aligned} &x_1 + x_2 = \frac{p - mz_2}{z_2 - z_1} \\ &x_1 x_2 = z_1. \end{aligned}$$

Di conseguenza x_1 e x_2 sono soluzioni dell'equazione di secondo grado

$$x^2 - \frac{p - mz_2}{z_2 - z_1} x + z_1 = 0$$

che risolta dà i valori delle prima due radici x_1 e x_2.

In maniera analoga, dalle relazioni

$$\begin{aligned} &x_3 + x_4 = \frac{mz_1 - p}{z_2 - z_1} \\ &x_3 x_4 = z_2 \end{aligned}$$

si ottengono le radici x_3 ed x_4.

L'equazione di quarto grado $x^4 + mx^3 + nx^2 + px + q = 0$ è così completamente risolta.[19]

Nota 6.
La teoria di Galois.

Quando Evariste Galois affronta la teoria delle equazioni, un certo numero di risultati erano già stati stabiliti. Scipione del Ferro e Ferrari avevano trovato delle formule risolutive per le equazioni di terzo e di quarto grado; Lagrange aveva legato la risolubilità per radicali al comportamento di opportune funzioni delle radici quando queste si scambiano tra loro. Infine,

[19] Da notare che la formula risolutiva esplicita è notevolmente complicata, dato che essa si ottiene risolvendo prima un'equazione di terzo grado, poi un'equazione di secondo grado nei cui coefficienti entra una soluzione dell'equazione precedente, e infine un'ulteriore equazione di secondo grado che contiene le radici della precedente.

Ruffini e Abel avevano dimostrato l'impossibilità della soluzione per radicali dell'equazione generale di grado superiore al quarto. Allo stesso tempo, Gauss aveva dimostrato la risolubilità per radicali dell'equazione ciclotomica $x^n = 1$, e Abel aveva esteso il risultato di Gauss a altre classi di equazioni.

Il problema che Galois si pone è quello di caratterizzare esattamente quali equazioni ammettano una soluzione per radicali. Prima di descrivere le linee fondamentali della sua opera, ricordiamo che si tratta di idee fortemente innovative, al punto che sono occorsi vari decenni prima che esse fossero pienamente comprese.

Un concetto essenziale per affrontare la teoria di Galois è quello di riducibilità di un polinomio. Per capire di che si tratta, consideriamo il polinomio a coefficienti razionali $x^3 - x^2 - 2x + 2$. Ricordando un po' di algebra elementare, vediamo subito che esso si può scrivere nella forma $(x-1)(x^2-2)$, ossia come prodotto di due polinomi di grado rispettivamente 1 e 2; si tratta di un polinomio *riducibile*.

Come è ovvio, Il polinomio $x-1$ non si può decomporre ulteriormente. Se restiamo nel campo dei numeri razionali, neanche il secondo polinomio si può decomporre in fattori; se invece ampliamo il campo dei numeri ammissibili, aggiungendo anche il numero $\sqrt{2}$ e tutti quelli che si ottengono da esso con le quattro operazioni, anch'esso si spezza nel prodotto $(x + \sqrt{2})(x - \sqrt{2})$.

Da questo esempio possiamo concludere due cose: primo, un polinomio può essere riducibile o meno a seconda del campo in cui si opera; secondo, l'ampliamento di un campo mediante un elemento fuori di esso può rendere riducibile un polinomio che non lo era. Ad esempio, nel campo dei numeri razionali l'equazione $x^4 - 5x^2 + 6 = 0$ si spezza nei fattori irriducibili $(x^2 - 2)(x^2 - 3) = 0$, se si aggiunge $\sqrt{2}$ i fattori diventano $(x+\sqrt{2})(x-\sqrt{2})(x^2-3)$, e infine se si aggiunge anche $\sqrt{3}$ si ha la fattorizzazione $(x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{3})(x - \sqrt{3})$. A questo punto, essendo tutti i fattori di primo grado, la fattorizzazione è completata.

In generale, supponiamo di avere un campo F,[20] e un'equazione

$$P(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

con coefficienti a_1, …, a_n in F. Se il polinomio $P(x)$ si spezza nel prodotto

[20] Grosso modo, un campo F è un insieme i cui elementi si possono sommare, sottrarre, moltiplicare e dividere (naturalmente se il divisore è diverso da 0) senza uscire da F. Ad esempio i numeri razionali formano un campo, come anche i numeri reali e i numeri complessi; non sono invece un campo i numeri interi, dato che il quoziente di due interi non è sempre un intero.

di due polinomi $Q(x)$ e $R(x)$, ambedue con coefficienti in F, si dice che il polinomio $P(x)$ (o l'equazione $P(x) = 0$) è riducibile in F, in caso contrario che è irriducibile.

Sia ora v un oggetto che non appartiene a F, che può essere un numero, come $\sqrt{2}$ nell'esempio precedente, o anche una variabile, e consideriamo l'insieme di tutte le *funzioni razionali* di v a coefficienti in F, cioè delle funzioni

$$f(v) = \frac{L(v)}{M(v)}$$

che si esprimono come quoziente di due polinomi $L(v)$ e $M(v)$ a coefficienti in F. Le funzioni razionali si possono sommare, sottrarre, moltiplicare e dividere tra loro, dando come risultato ancora delle funzioni razionali; esse formano dunque un campo, che contiene F, e che costituisce l'ampliamento di F con l'aggiunta di v.[21]

Ad esempio se si indica con $\mathbf{Q}$ il campo dei numeri razionali, il campo $\mathbf{Q}(\sqrt{2})$ è l'insieme delle funzioni razionali

$$f(\sqrt{2}) = \frac{L(\sqrt{2})}{M(\sqrt{2})}.$$[22]

Una volta chiarito questo punto, veniamo alla teoria di Galois. Data un'equazione di grado n:

$$P(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0 \qquad (6)$$

che come sappiamo ha n radici x_1, x_2, ..., x_n. si tratta di vedere se esse possono essere espresse mediante una formula nella quale entrano opportune radici di combinazioni di coefficienti; o più precisamente se esse si possono esprimere razionalmente in un campo opportunamente ampliato con l'aggiunta di alcuni radicali. Ad esempio, l'equazione di secondo grado

$$x^2 + 2bx + c = 0$$

[21] Usualmente questo campo si indica con $F(v)$.

[22] In questo caso, dato che $(\sqrt{2})^2$ è razionale, le potenze pari di $\sqrt{2}$ sono razionali, mentre le potenze dispari sono uguali a un numero razionale moltiplicato per $\sqrt{2}$. Di conseguenza, $\mathbf{Q}(\sqrt{2})$ è l'insieme delle funzioni della forma

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$$

con a, b, c e d razionali.

ha soluzioni

$$x = -b \pm \sqrt{b^2 - c}$$

e quindi si esprime razionalmente nel campo razionale ampliato con l'aggiunta di b e del radicale $\sqrt{b^2 - c}$.

Galois comincia coll'introdurre una funzione razionale delle radici della (6), $V(x_1, x_2, \ldots, x_n)$, che assume tanti valori diversi quanti sono i modi diversi di permutare tra loro le n radici. Come è noto, questi sono $n! = 1 \cdot 2 \cdots (n-1) \cdot n$. Galois dimostra che ogni radice della (6) si esprime come funzione razionale di V:[23]

$$x_1 = f_1(V), \;\; x_2 = f_2(V), \;\; \ldots \;\; x_n = f_n(V).$$

I valori diversi assunti da V quando si permutano le radici corrispondono alle diverse sostituzioni possibili su di esse. Se numeriamo queste ultime in un ordine qualsiasi:[24]

$$s_1 = e, \; s_2, \; \ldots, \; s_{n!},$$

avremo in corrispondenza i valori V_1, V_2, …, $V_{n!}$. La funzione V sarà allora soluzione dell'equazione

$$(V - V_1)(V - V_2) \cdots (V - V_{n!}) = 0.$$

Se il polinomio a primo membro è riducibile (nel campo ampliato aggiungendo i coefficienti, ma non le loro radici), Galois dimostra che essa si spezza in fattori irriducibili tutti dello stesso grado. Siccome la numerazione delle sostituzioni era arbitraria, possiamo supporre che un fattore irriducibile sia quello formato dai primi m fattori:

$$(V - V_1)(V - V_2) \cdots (V - V_{m_0}), \tag{7}$$

corrispondenti alle sostituzioni $s_1 = e$, s_2, …, s_m. Queste sostituzioni costituiscono il *gruppo di Galois* G_0 dell'equazione (6).

In un certo senso, il gruppo di Galois descrive il nostro grado di conoscenza (o di ignoranza) della V, e dunque delle radici dell'equazione di partenza. Se non sappiamo nulla −questo avviene ad esempio nel caso di un'equazione a coefficienti arbitrari− sarà il gruppo S_n di tutte le sostituzioni; via via che aumentano le nostre conoscenze, esso diviene più piccolo; se infine si riduce

[23]Più tardi, la funzione V ha ricevuto il nome di *risolvente di Galois*.

[24]Indichiamo con e la sostituzione identica, cioè quella che lascia tutto invariato.

alla sola sostituzione identica $s_1 = e$, la (7) diventa $V - V_1 = 0$, e quindi conosceremo la V e da essa tutte le radici della (6).

Vediamo ora cosa succede se ampliamo il campo con l'aggiunta delle radici di ordine p di una quantità A, cioè con le soluzioni dell'equazione $x^p = A$. Osserviamo innanzitutto che possiamo prendere p primo, dato che se $p = hk$, la radice $\sqrt[p]{A}$ si può scomporre in due radici successive di ordine h e k:

$$\sqrt[p]{A} = \sqrt[h]{\sqrt[k]{A}}.$$

Ciò premesso, Galois dimostra che possono succedere due cose: o il polinomio (7) resta irriducibile, e in questo caso il gruppo G_0 non cambia; o si spezza in p fattori, tutti dello stesso grado $m_1 = \frac{m_0}{p}$. Come sopra, potremo supporre che uno di questi sia

$$(V - V_1)(V - V_2) \cdots (V - V_{m_1}).$$

Le corrispondenti sostituzioni costituiscono un *sottogruppo* G_1 del gruppo di Galois G_0.

Quanto agli altri fattori, Galois fa vedere che le sostituzioni corrispondenti formano un insieme H che si può ottenere in maniera equivalente in due modi:

- sia applicando una stessa sostituzione del fattore a tutte le sostituzioni di G_1: $H = sG_1$,

- sia applicando le sostituzioni di G_1 a una sostituzione del fattore: $H = G_1 s$.

Si ha dunque $sG_1 = G_1 s$; in termini moderni G_1 è un sottogruppo *normale* di G_0. L'*indice* di G_1, cioè il rapporto tra il numero di elementi di G_0 e di G_1, è uguale all'ordine p della radice.

A questo punto, Galois si chiede: cosa succede quando un'equazione è risolubile per radicali? Come abbiamo visto, l'aggiunta di un radicale può o non può rendere riducibile il polinomio (7); d'altra parte prima o poi ciò dovrà avvenire, altrimenti l'equazione non sarebbe risolubile.

Se il polinomio si riduce per l'aggiunta delle radici $\sqrt[p]{A}$, il gruppo di Galois si ridurrà a un sottogruppo normale G_1 di indice p. Continuando in questo modo, si troverà una serie di gruppi

$$G_0 \supset G_1 \supset \cdots \supset G_k$$

ognuno normale e di ordine primo, in cui il primo gruppo è il gruppo di Galois G_0, e l'ultimo si riduce alla sola sostituzione identica $\{e\}$.

Galois dimostra che vale anche il viceversa: se il gruppo di Galois dell'equazione (6) è *risolubile*, cioè se si può inserire in una serie di sottogruppi di indice primo, che termina con $\{e\}$, allora l'equazione ammette una soluzione per radicali. Possiamo dunque dire che una condizione necessaria e sufficiente per la risolubilità per radicali di un'equazione è che il suo gruppo di Galois sia risolubile.

Vediamo come il risultato precedente si applica alle equazioni di terzo e quarto grado, che come abbiamo visto sono risolubili per radicali. Per questo dobbiamo studiare un po' più da vicino i gruppi di sostituzioni S_3 e S_4.

Un posto particolare tra le sostituzioni è occupato dagli scambi. Ad esempio, delle tre lettere $\{abc\}$ posso scambiare la prima con la terza, ottenendo $\{cba\}$. Una tale sostituzione si indica con (13); si ha allora

$$(13)\{abc\} = \{cba\}.$$

Analogamente

$$(23)\{abc\} = \{acb\} \text{ e } (12)\{cab\} = \{acb\}.$$

Tutte le sostituzioni si possono scrivere, anche in modi diversi, come prodotti di scambi; ad esempio la sostituzione s, che manda $\{abc\}$ in $\{bca\}$, non è uno scambio, in quanto tutte e tre le lettere cambiano di posto, ma si può scrivere come il prodotto (12)(13). Infatti si ha

$$(12)(13)\{abc\} = (12)\{cba\} = \{bca\}.$$

Si verifica facilmente che la stessa s si può scrivere anche nella forma (13)(23). Inoltre il prodotto di due scambi dipende dall'ordine dei fattori; ad esempio (12)(13) è diverso da (13)(12), dato che $(13)(12)\{abc\} = \{cab\}$.

Consideriamo ora la generica equazione di terzo grado. Come abbiamo detto, il suo gruppo di Galois è il gruppo S_3 di tutte le sostituzioni delle tre radici; esso ha $3! = 6$ elementi, e precisamente:

$$e,\ (12),\ (13),\ (23),\ (12)(13),\ (13)(12).$$[25]

[25]Le altre combinazioni di scambi danno luogo agli stessi elementi; ad esempio, come abbiamo visto, (13)(23) = (12)(13).

Questo gruppo ammette un sottogruppo A_3, formato da e e dalle sostituzioni *di ordine pari*, ossia che sono il prodotto di un numero pari di scambi:

$$A_3 = \{e,\ (12)(13),\ (13)(12)\}.$$

Si vede facilmente che A_3 è un sottogruppo normale; ad esempio si ha

$$(12)A_3 = \{(12),\ (13),\ (23)\} = A_3(12),$$

inoltre esso è di indice 2, che è primo. La serie

$$S_3 \supset A_3 \supset \{e\}$$

mostra che S_3 è risolubile, e quindi che l'equazione generale di terzo grado è risolubile per radicali. Di più, gli ordini dei due sottogruppi A_3 ed $\{e\}$ sono rispettivamente 2 e 3, e corrispondono rispettivamente all'aggiunta di una radice quadrata e di una radice cubica; precisamente alle radici quadrata e cubica che compaiono nella formula di Cardano.

Un calcolo simile, ma più complicato, mostra che anche l'equazione di quarto grado è risolubile per radicali. In questo caso, G_0 è il gruppo S_4 di tutte le sostituzioni delle quattro radici; G_1 è il gruppo A_4 di quelle formate da un numero pari di scambi, e cioè

$$\begin{gathered} e,\ (12)(13),\ (13)(12),\ (12)(14),\ (14)(12),\ (13)(14),\ (14)(13), \\ (23)(24),\ (24)(23),\ (12)(34),\ (13)(24),\ (14)(23). \end{gathered}$$

Come in precedenza, A_4 è un sottogruppo normale di S_4, di indice 2. Esso poi ammette il sottogruppo di indice 3:

$$G_2 = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\}$$

che a sua volta ha il sottogruppo normale

$$G_3 = \{e,\ (12)(34)\}$$

di indice 2. In conclusione, la serie

$$S_4 \supset A_4 \supset G_2 \supset G_3 \supset \{e\}$$

mostra la risolubilità per radicali dell'equazione generale di quarto grado. Gli indici dei vari sottogruppi sono 2, 3, 2 e 2; i primi due corrispondono alla soluzione dell'equazione ausiliaria di terzo grado, gli altri due alle soluzioni delle due equazioni di secondo grado che compaiono nel metodo di Ferrari.