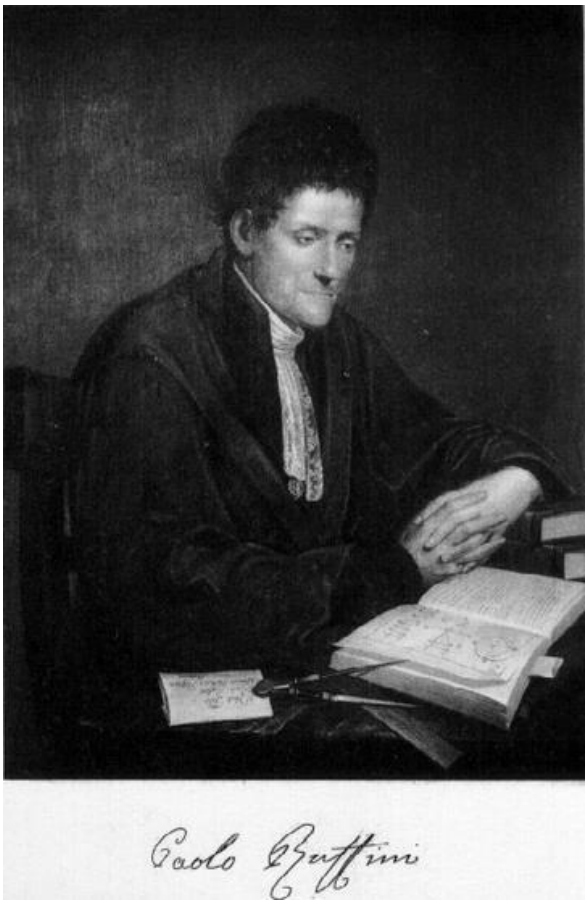
IL TEOREMA DI RUFFINI-ABEL
ovvero

IMPOSSIBILITA' DELLA SOLUZIONE DELLE EQUAZIONI DI QUINTO GRADO PER MEZZO DI RADICALI

(*Spiegazione di Crispin e Jakob per matematici ciclisti)*

I Edizione



Paolo Ruffini, (Valentano, 22 settembre 1765 – Modena, 10 maggio 1822)
Da https://es.wikipedia.org/wiki/Paolo_Ruffini#/media/File:Ruffini_paolo.jpg
Public Domain

1. Introduzione semi-biografica di Jakob.

Ricordo bene quando in quarta ginnasio il mio professore di matematica spiegò alla poco ricettiva classe in cui mi trovavo la formula risolutiva *generale* delle equazioni algebriche di secondo grado. Per risvegliare l'attenzione dell'uditorio, aggiunse che esistevano formule più complesse per le equazioni di terzo e di quarto grado, mentre non esistevano formule del genere per le equazioni di quinto grado e gradi

superiori. C'era a quanto pare un teorema (dal mio professore attribuito a "Paolo Ruffini ed altri") che dimostrava che, appunto, non esiste una formula risolutiva *generale* per le equazioni algebriche di quinto grado e gradi superiori, *per mezzo di radicali*.

Questa affermazione mi incuriosì. Da allora ho cercato di capire il perché di questa stranezza. Non che volessi dimostrare da solo un eventuale teorema: mi sarei più che accontentato di comprenderne la dimostrazione, o anche solo i capisaldi della medesima.

Sono passati moltissimi anni e al mio settantesimo compleanno non avevo ancora compreso il teorema di Ruffini-Abel -Galois (RAG). Da nessun libro di matematica divulgativa che ho avuto per le mani avevo mai recepito una seppur vaga idea di una dimostrazione. Intendiamoci, altro è saper ripetere una dimostrazione (ce ne sono alcune, soprattutto semplificazioni della dimostrazione di Galois, estremamente brevi), altro è capirne il meccanismo. Tutti i testi riferivano che Galois aveva scritto la sua memoria la sera prima di morire in duello scrivendo qua e là: "non ho il tempo di spiegare in dettaglio" o qualcosa del genere (o era lui quello del margine con troppo poco spazio? No, quest'altro doveva essere Fermat). D'altra parte Lagrange non aveva neppure degnato di una risposta Ruffini, il primo a concepire (a quanto pare) e dimostrare l'impossibilità di una formula generale per risolvere le equazioni di quinto grado per mezzo di radicali. In quanto a Abel, era morto tisico e in miseria a ventisei anni. Questi aneddoti - oltre a dimostrare che cercare di capire la soluzione delle equazioni di quinto grado porta scalogna - non mi avvicinavano di un passo a comprendere il senso e il metodo della dimostrazione. Lungi dall'interessarmi, mi irritavano profondamente. Nulla di tutto ciò, mi dicevo, ha alcunché a vedere con le mie domande. Qualche testo faceva un misterioso accenno ad un'intuizione di Lagrange che la solubilità per mezzo di radicali fosse legata alla simmetria delle permutazioni delle radici, nozione che nella mia ignoranza non capivo da dove venisse, né che significasse, né perché dovesse valere solo per le radici espresse per mezzo di radicali.

Neppure un grande divulgatore come W.W. Sawyer, a cui devo la mia comprensione di non banali concetti matematici, riuscì a darmi un'idea chiara. Direi che la parte sulla teoria di Galois è per me tra le meno soddisfacenti dei vari suoi libri che io ho avuto per le mani. Courant e Robbins, nel loro eccellente libro "Che cos'è la matematica", che sono solito citare ove necessario come C&R, non menzionano neppure Galois. L'Enciclopedia Feltrinelli (Matematica I, alla voce "Equazioni") dà una semplice dimostrazione, che si può seguire, ma è talmente

compatta da non poter rispondere alle poche domande che si sono venute sedimentando nella mia mente in sessant'anni.

Su Galois ho trovato il libro di un divulgatore ad alto livello, Harold Edwards, autore - tra le altre cose - di un saggio che mi ha aiutato a comprendere in modo per me soddisfacente il significato della Congettura di Riemann. Ahimé, il suo libro su Galois non mi è stato di altrettanto aiuto. Naturalmente, mentre per la Congettura di Riemann mi bastava capire il significato della congettura, qui chiedo di più, voglio addirittura comprendere almeno i capisaldi della dimostrazione di un teorema. Ma tant'è, neppure il bravo Edwards con me c'è riuscito.

RUFFINI E ABEL

Per poter dare la priorità della dimostrazione di questo teorema a Niels Abel, Paolo Ruffini fu accusato di aver dato una (anzi, più d'una) dimostrazione gravemente incompleta, o almeno, abbastanza incompleta da togliergli la gloria non solo di esser stato il primo a concepire l'esistenza del teorema (gloria che neppure Abel gli nega), ma anche di averlo dimostrato per primo.

Abel stesso non fu da meno. Nella sua prima dimostrazione (del 1823, Ruffini era morto da due anni) mancava molto alla completezza, e con sorpresa, cercando di avere lumi sulla sua ultima dimostrazione, ho trovato che ci sono due passi ancora abbastanza oscuri. In effetti, quando Abel pubblicò il suo risultato, diverse critiche furono sollevate contro la sua dimostrazione, che vengono risolte dicendo che la dimostrazione era oscura, ma l'intuizione era corretta. Bene, lo stesso si può dire di Ruffini, che, lavorando in isolamento e snobbato da Lagrange, probabilmente non si rese mai conto del fatto che la sua dimostrazione prendeva per ovvio un risultato che invece altri volevano dimostrato, mentre all'unico grande matematico che gli diede retta, Cauchy, andava bene così (rima non voluta). Vedremo se può andare bene anche ad altri. L'idea che Cauchy, come scrisse a Ruffini, avesse potuto trovare la dimostrazione soddisfacente e anzi, avesse pensato di utilizzarne dei concetti al Politecnico di Parigi, dove insegnava, in corsi che probabilmente anche Abel frequentò o di cui seppe nel 1826, mi ha spronato ulteriormente a cercare di capire la dimostrazione del teorema.

Trovai una dimostrazione finalmente chiara e completa di questo teorema, dovuta a Leopold Kronecker, che eventualmente metterò online in

seguito. Ma non ero del tutto soddisfatto, perché la dimostrazione di Kronecker seguiva un tragitto intellettuale del tutto diverso da quella di Ruffini, e non utilizzava se non molto da lontano la simmetria nelle permutazioni delle radici che, come sapevo fin da quando il teorema mi era stato reso noto nelle scuole medie, era alla base delle dimostrazioni classiche di Ruffini, Abel e infine Galois. Finalmente trovai una dimostrazione semplificata di un matematico francese, Pierre-Laurent Wantzel (1814-1848....morto anche lui giovane, come Abel e Galois - studiare l'equazione di quinto grado porta davvero male!), che prometteva di spiegarmi tutto quello che volevo.

Vediamo dunque se con l'aiuto di Wantzel possiamo capire qualcosa di più. Non utilizzerò solo il suo articolo originale, ma la presentazione data da Charles de Comberousse, nel suo Cours de Mathématiques, Tomo IV, parte II, pagine 598-619 (1890) e, infine e soprattutto, le presentazioni date da Joseph Serret e Joseph Carnoy nei loro rispettivi testi dallo stesso titolo: "Cours d'Algèbre supérieure", il primo del 1885, Tomo II, da pag.512, e il secondo, seconda edizione, del 1900, alle pagine 340 e seguenti.

Sorpresa! La presentazione di Carnoy occupa esattamente tre pagine e mezza. Quali ragionamenti, quali Lemmi, quali teoremi indispensabili sono assenti? Lo deciderà il lettore.

**

Fin qui l'introduzione semi-biografica di Jakob, il quale, comunque, non chiede di più di quanto il Carnoy dimostri. La dimostrazione non sarà rigorosa, ma dirà quanto meno quello che a lui basta.

Crispin invece è molto favorevole alla dimostrazione di Ruffini (l'ultima della serie) e pensa che sia più chiara di quella di Wantzel-Coumberousse-Carnoy, a cui è più vicina che quella di Abel. In effetti anche a me pare che chiarisca alcuni punti che i tre Francesi lasciano un poco in sospeso, per cui ho introdotto una parte della dimostrazione di Ruffini nella parte finale del mio saggio. Crispin ha dato un essenziale contributo a questa dimostrazione chiarendo (in parte grazie a Ruffini e in parte grazie al suo cervello non trascurabile) un certo numero di punti oscuri nella dimostrazione dei primi tre, e spero che il mio testo non gli dispiaccia.

DE

2. La dimostrazione (vista da Crispin e Jakob)

Normalmente si arriva alla meta se si sa dov'è la meta. Si sale sulla cima del Monte Bianco se, per incominciare, si sa dov'è il Monte Bianco.

L'idea che, penso, sbocciò nella testa di Ruffini, era la seguente: data l'equazione generale di quinto grado a coefficienti razionali della forma

$$f(x) = x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5 = 0 \qquad (1)$$

come possiamo scrivere una soluzione "algebrica" generale dell'equazione? Oppure, visti i tentativi falliti di innumeri matematici precedenti, come si può dimostrare che una tale soluzione non esiste per l'equazione di quinto grado?

Ma intanto, che vuol dire soluzione generale (vedremo più avanti che significa "algebrica")? Significa che al posto di tutti e cinque i coefficienti che compaiono nella (1) noi possiamo porre un numero razionale qualsiasi, zero incluso. In altre parole, la formula risolutiva deve contenere i cinque coefficienti in modo che, data un'equazione del tipo (1), ma nella quale i coefficienti assumano determinati valori, inserendo tali valori nella formula risolutiva dovremmo sempre ottenere la soluzione corretta. Il teorema nega che tale soluzione generale sia possibile, ma non nega che esistano soluzioni algebriche di particolari equazioni. Sarebbe negare l'ovvio, perché l'equazione

$$x^5 + a_5 = 0 \qquad (2)$$

ha le cinque soluzioni (algebriche, una reale e due coppie di complesse coniugate):

$$x_i = \alpha_i \sqrt[5]{a_5} \qquad (3)$$

in cui le α_i sono appunto le cinque radici quinte dell'unità.

Ma questa non può essere la soluzione generale, perché se, a_5 restando invariata, gli altri coefficienti non fossero nulli, ci verrebbero nondimeno proposte le stesse espressioni (3), questa volta evidentemente inutili.

> In realtà, qui c'è un primo punto che accetto senza dimostrazione: sappiamo che esistono trasformazioni dei coefficienti, attribuite a Tschirnhaus (1683), e continuatori (Bring, 1786; Jerrard, 1834), che in un'equazione di grado *n* possono rendere eguale a zero (al costo di risolvere equazioni di grado crescente) i coefficienti di grado *n-1, n-2, n-3,* cioè, nel caso dell'equazione "quintica", essa può essere ridotta alla forma:

$$x^5 + px + q = 0 \quad (1b)$$

È quel maledetto *px* che rovina tutto e non ci permette di passare alla forma (2). La necessaria trasformazione di Tschirnhaus che lo eliminerebbe, in linea di principio esiste, ma richiede la soluzione di un'equazione di grado superiore al quinto, e quindi non ci aiuta.

In realtà noi vogliamo, nel caso generale (basandoci sul teorema generale dell'algebra), cinque soluzioni della forma:

$$\begin{aligned} x_1 &= h_1(a_1, a_2, a_3, a_4, a_5) \\ x_2 &= h_2(a_1, a_2, a_3, a_4, a_5) \\ x_3 &= h_3(a_1, a_2, a_3, a_4, a_5) \\ x_4 &= h_4(a_1, a_2, a_3, a_4, a_5) \\ x_5 &= h_5(a_1, a_2, a_3, a_4, a_5) \end{aligned} \qquad (4)$$

I ragionamenti che seguiranno, basati sulle permutazioni delle radici, cadranno se alcuni coefficienti sono eguali, o hanno altre specifiche relazioni tra loro, o assumono determinati valori, come lo zero. Questi casi però sono esplicitamente esclusi dal fatto che noi cerchiamo una soluzione "generale".

A priori, non c'è nessun motivo per pensare che le funzioni h_i debbano avere qualche relazione fra loro. Si potrebbe pensare che le soluzioni siano date in qualche ordine, per esempio modulo e argomento crescente, che in qualche modo le distinguano l'una dall'altra. Ma, come è noto, i coefficienti della (1) sono esprimibili in termini delle stesse radici, grazie al fatto che la stessa equazione (1) può essere scritta nella forma (5):

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5) = 0 \qquad (5)$$

Svolgendo il prodotto, otteniamo:

$$\begin{aligned} & x^5 \\ & - (x_1 + x_2 + x_3 + + x_4 + x_5)\, x^4 + (\, x_1 x_2 + \, x_1\, x_3 + \, x_1 x_4 + \, \ldots) x^3 \\ & - \, (x_1 x_2\, x_3 + x_1\, x_2\, x_4 + x_1 x_2\, x_5 + x_2\, x_3\, x_4 + x_2\, x_3\, x_5 + \, \ldots) x^2 \\ & + (x_1 x_2\, x_3\, x_4 + \, x_1 x_2\, x_3\, x_5 + x_1\, x_2\, x_4\, x_5 + x_1\, x_3\, x_4\, x_5 \\ & + \, x_2\, x_3\, x_4\, x_5) x \, + (x_1 x_2\, x_3\, x_4 x_5) \\ & = 0 \end{aligned} \qquad (6)$$

da cui si vede come i coefficienti a_i si identifichino con le cosiddette "funzioni simmetriche elementari" delle radici o soluzioni. Qui si vede anche che le cinque radici sono trattate tutte allo stesso modo, e possono essere scambiate fra loro senza alcun effetto sull'equazione di partenza.

Il lettore inquisitivo può provare con le radici ($x_1 = 1,\ x_2 = 2,\ x_3 = 3,\ x_4 = 4, x_5 = 5$), se non ci crede, e vedrà che permutandole fra loro, cioè . per esempio - chiamando $x_1 = 4,\ x_2 = 5,\ x_3 = 1, etc.$ l'equazione resterà la stessa, cioè avrà gli stessi coefficienti, oltre ad avere per costruzione le stesse soluzioni in termini numerici, anche se con indici scambiati per le x_i.

In quanto poi all'ordine in cui si considerano le soluzioni, esso risulta ai nostri scopi irrilevante, perché nulla cambia nell'equazione.

Incidentalmente, il curioso lettore può provare a scrivere x_1 ovunque compare *x* nella (5), elevato agli esponenti indicati, e troverà l'identità 0 = 0, il che non dice molto, ma neanche troppo poco.

Ora supponiamo di sostituire nelle (4) i valori dei coefficienti in termini delle radici, ottenendo così cinque funzioni g_i .

$$\begin{aligned} x_1 - g_1(x_1, x_2, x_3, x_4, x_5) &= 0 \\ x_2 - g_2(x_1, x_2, x_3, x_4, x_5) &= 0 \\ x_3 - g_3(x_1, x_2, x_3, x_4, x_5) &= 0 \\ x_4 - g_4(x_1, x_2, x_3, x_4, x_5) &= 0 \\ x_5 - g_5(x_1, x_2, x_3, x_4, x_5) &= 0 \end{aligned} \qquad (7)$$

Nella prima equazione, scambiamo fra loro x_1 e x_2 . Otteniamo quindi:

$$x_2 = g_1(x_2, x_1, x_3, x_4, x_5) \qquad (8)$$

Ma poiché non possiamo avere due soluzioni diverse per x_2, ne segue che

$$g_1(x_2, x_1, x_3, x_4, x_5) = g_2(x_1, x_2, x_3, x_4, x_5) \qquad (7')$$

Cioè, g_1 e g_2 sono la stessa funzione con una permutazione delle radici. Supponendo di ripetere il gioco con le altre radici, ne discendono tre importanti conseguenze:

I. La soluzione generale in termini delle radici è data da

$$x_i = F(P_i(x_1, x_2, x_3, x_4, x_5))$$

In cui P_i è una opportuna permutazione delle radici.

II. La F conterrà più o meno complicate espressioni contenenti le radici x_i.
Tuttavia, è addirittura ovvio che queste espressioni si devono poter svolgere in modo da giungere sempre all'identità:

$$x_i = x_i \quad \text{(I)}$$

In altre parole, dalla formula per F sono banditi radicali la cui radice non possa essere estratta esattamente in termini delle radici dell'equazione. La formula deve contenere quindi solo funzioni razionali delle radici.

Si noti che questa osservazione (e non ipotesi), a parer mio (ma anche di Ruffini e di Cauchy) elementare, fu proprio ciò su cui si incentrò la critica di Abel, che sentì la necessità di dimostrarla come un teorema di diverse pagine, il che gli permise di dare il suo nome a questo teorema. Matematici, in genere americani (a cui piacciono le inutili iperboli), la ritengono un punto "cruciale" della dimostrazione. Mah! Abel fu un grandissimo matematico, e non aveva certo bisogno anche di questo riconoscimento.

Il contributo sarebbe però stato di fondamentale importanza se Ruffini avesse voluto dimostrare che esiste una formula risolutiva generale per le equazioni di quinto grado, e si fosse basato sull'ipotesi che le F contengono solo funzioni razionali delle radici. Invece, volendo dimostrare che tale formula generale non esiste, non si curò del caso in cui l'impossibilità della formula fosse già ovvia in partenza, come avverrebbe nel caso in cui la formula generale per F contenesse funzioni algebriche, e non razionali, delle radici dell'equazione.

Per completezza, notiamo che le funzioni più semplici considerate in questo contesto sono i *monomi* (che contengono solo prodotti di potenze di variabili diverse); combinando i monomi mediante le operazioni di addizione (e sottrazione), moltiplicazione (ed elevazione a potenza) otterremo le funzioni *intere*. Combinando le funzioni intere per mezzo delle due operazioni citate otterremo ancora funzioni intere, ma, introducendo la divisione, avremo le funzioni *razionali*. Infine, aggiungendo le estrazioni di radice avremo le funzioni *algebriche*.

Queste sono i soli tipi di funzioni che ci occorrono. Non è strano: il teorema di Ruffini fu dimostrato alla fine del '700, quando i prodigiosi sviluppi della teoria delle funzioni matematiche erano ancora lontani nel futuro e si era fermi alle cosiddette funzioni trascendenti elementari, cioè funzioni esponenziali e trigonometriche, e le loro inverse.

Quel che succede è apparente nelle equazioni di secondo grado:

Sia $x^2 + 2b\,x + c = 0$. Abbiamo,

$$x_1 = \left(-b + \sqrt{b^2 - c}\right) \text{ e } \quad x_2 = \left(-b - \sqrt{b^2 - c}\right) \qquad (13)$$

Ma, dalla (6), $2b = -(x_1 + x_2)$ e $c = x_1 x_2$, per cui,

$$x_1 = \frac{x_1 + x_2}{2} + \frac{1}{2}\sqrt{(x_1 - x_2)^2} \qquad (14)$$

A questo punto i coefficienti non c'entrano più, e gli indici delle radici dell'equazione sono completamente arbitrari. Ogni relazione tra le radici resta identica, e permutando x_1 e x_2 la relazione resta identica, cioè è simmetrica. Come ci aspettavamo, il radicale è calcolabile esattamente in termini delle radici dell'equazione, al costo di introdurre le radici quadrate dell'unità, che d'altra parte sono quelle che ci permettono di ottenere le due soluzioni dell'equazione dall'unica formula risolutiva. Calcolando il radicale, e scegliendo in modo arbitrario la radice +1 dell'unità, si ottiene

$$x_1 = \frac{x_1 + x_2}{2} + \frac{(x_1 - x_2)}{2} \qquad (15)$$

Il secondo membro è ora una funzione razionale, ma non è più simmetrica. Ne discende l'identità $x_1 = x_1$.

Permutiamo ora a sinistra e a destra x_1 con x_2 e troviamo, scegliendo sempre il segno + nel radicale, l'identità $x_2 = x_2$.
Il radicale del modulo è chiamato talora radicale aritmetico. Noi agiremo sempre su tale integrale e aggiungeremo le radici dell'unità a posteriori.

III. Considerando poi che le g discendono da funzioni dei coefficienti, che, essendo espressioni simmetriche delle radici, non cambiano variando l'ordine di queste ultime, ne segue l'importante risultato, in genere dato per scontato, che la soluzione generale dell'equazione di quinto grado è semplicemente:

$$x = A(a_1, a_2, a_3, a_4, a_5) \qquad (9)$$

in cui si potrà (fino ad un certo punto) fare a meno degli indici per le radici.

La funzione A in (9) dovrà contenere almeno un radicale; altrimenti l'equazione $x = A$ avrà un'unica soluzione, che andrà bene per un'equazione di primo grado, ma non potrà essere la soluzione generale di un'equazione di quinto grado. Ci sarà infatti una sola radice dell'unità, cioè 1, e non ci sarà modo di costruire altre soluzioni, (in questo caso) 5, come richiesto dal teorema fondamentale dell'algebra dimostrato proprio in quegli anni, all'inizio dell'Ottocento, da Gauss.

Ma Ruffini voleva dimostrare che una tale soluzione è impossibile, se vogliamo che A sia una funzione "algebrica", cioè una funzione che si basa unicamente sulle quattro operazioni e, al più, dei radicali di vario

indice razionale, che operano su funzioni razionali o, al più, a loro volta algebriche dei coefficienti a_i.
Avendo deciso di eseguire una dimostrazione per assurdo, Ruffini fece dunque l'ipotesi che A fosse una funzione algebrica, disponendosi a dimostrare che da questa ipotesi segue qualche impossibilità.

Una prima considerazione inevitabile è che, se la soluzione deve essere generale, qualcuno potrebbe non veder bene come da $x = A$ possano sortire le cinque radici, *A* restando invariata. Qui bisogna ammettere che la *A* non è precisamente invariata, ma è invariata a meno di opportune radici dell'unità. Prendiamo ad esempio la più semplice equazione di quinto grado, che abbiamo già vista ed è $x^5 = B$, dove *B* è una costante. La soluzione generale è allora:

$$x = \sqrt[5]{B} \qquad (10)$$

e la nostra domanda diventa: come otteniamo cinque soluzioni? Il fatto è che possiamo (anzi, dobbiamo) scrivere $B = B \cdot 1$, e $\sqrt[5]{B}\ \sqrt[5]{1}$ in luogo di $\sqrt[5]{B}$. Il pedone matematico non mancherà di stupirsi all'idea che 1 abbia cinque radici quinte, delle quali 1 è la sola radice reale. D'altronde, è ben noto che $\sqrt[2]{1}$ ha le due radici +1 e -1. Noi siamo però ciclisti matematici, e non possiamo far altro che consigliare al pedone di comprarsi una bicicletta come abbiamo fatto noi.

Poiché 5 è un numero primo, si può dimostrare (si veda l'Appendice) che le cinque radici dell'unità, cioè $\alpha_0 = 1$, α_1, α_2, α_3, α_4 sono potenze di una qualsiasi di esse, che chiameremo α, esclusa l'unità, che elevata a qualsiasi potenza può solo riprodurre sé stessa. Per cui avremo, senza perdita di generalità,

$$x_i = \alpha^i\ \sqrt[5]{B} \quad \text{, con } i = 1, 2, 3, 4, 5 \text{ ed } \alpha \neq \alpha_0 (= 1) \qquad (11)$$

"Senza perdita di generalità" è detto in senso assoluto, in quanto così facendo non prefissiamo un ordine delle radici dell'equazione secondo gli esponenti di α: scegliendo un'altra α di partenza scambiamo semplicemente fra loro le x_i.

> Il lettore inquisitivo potrà quindi esplorare che cosa succederebbe se, procedendo come logica comanda, scrivesse $x = \sqrt[5]{B}\ \sqrt[5]{1}\sqrt[5]{1}$ .... oppure $\sqrt[5]{B}\ \sqrt[5]{1}\sqrt[5]{1}\sqrt[5]{1}$ e via di seguito. La domanda, naturalmente, sarebbe: come si può essere sicuri che le radici diverse dell'equazione resterebbero cinque? L'Appendice dovrebbe illuminarlo.

Se nella nostra soluzione generale dell'equazione compariranno altri radicali, non di ordine cinque, allora compariranno altre radici dell'unità a

fattore di ogni radicale, di altro ordine. Di qui segue che il numero di soluzioni che può risultare combinando in tutti i modi possibili le varie radici dell'unità che moltiplicano i vari radicali è assai maggiore di cinque, ed il problema sembrerà essere piuttosto quelle di ridurle a cinque e solo cinque (in realtà non sarà così). *Ma il messaggio importante è che infine le radici dell'equazione sono diverse solo in grazia di come utilizziamo le varie radici dell'unità.*

Per quanto detto in precedenza, esprimendo la soluzione generale in termini delle radici anziché dei coefficienti dell'equazione, avremo:

$$x = F(x_1, x_2, x_3, x_4, x_5) \qquad (12)$$

Senza perdita di generalità, vista l'interscambiabilità delle radici, la soluzione per x_1 può essere scritta come:

$$[F(x_1, x_2, x_3, x_4, x_5) - x_1] = 0 \qquad (16)$$

in cui il membro di sinistra, $F - x_1$, dovrebbe essere una funzione totalmente simmetrica delle x_i, ovvero una funzione che, permutando le radici x_i, produrrebbe sempre un solo valore, zero.

Che succede permutando x_1 ed x_2?

L'equazione diventa:

$$F(x_2, x_1, x_3, x_4, x_5) - x_2 = 0 \qquad (17)$$

Otterremmo cioè la seconda radice. Ne segue che noi potremo dire di aver trovato la soluzione generale dell'equazione di quinto grado se riusciremo a trovare una funzione algebrica (anzi, razionale) F che assuma cinque valori, in generale differenti, permutando le radici. In effetti, le cinque radici possono essere permutate in vari modi, 5! = 120, per essere precisi.

L'obiettivo di Ruffini, a questo punto, è chiaro: occorre dimostrare che una tale funzione F non esiste, cioè non si può scrivere un'equazione del tipo dato in cui ogni radice dell'equazione è espressa mediante una singola funzione razionale nelle cinque radici, che abbia *almeno* cinque valori diversi permutando le radici.

Ora, questo lo si può provare, e questa impossibilità risiede proprio nel fatto che noi esigiamo che la nostra A nella formula (9) sia una funzione

algebrica dei coefficienti, cioè una funzione che includa al più radicali, e non funzioni trascendenti, ciò che risponderà a una delle mie domande a cui ho accennato.

Come abbiamo detto, i radicali presenti nella *F* risolutiva, una volta estratte le radici, devono essere funzioni razionali delle radici dell'equazione. Se non lo fossero, non potremmo giungere all'identità (I). Non possiamo però aspettarci che le funzioni risultanti siano anche funzioni simmetriche delle radici dell'equazione, perché, se lo fossero, sarebbero funzioni razionali dei coefficienti (i quali ultimi sono appunto le funzioni simmetriche elementari delle radici, e si può dimostrare che tutte le funzioni simmetriche non elementari possono essere costruite usando come mattoni le funzioni simmetriche elementari). In altre parole i radicali, espressi in termini dei coefficienti, sarebbero esattamente calcolabili, producendo funzioni razionali dei medesimi coefficienti, e scomparendo, come radicali, dalla formula generale per *x*.
In altre parole (come si è visto per l'equazione di secondo grado), in generale, i nostri radicali devono essere esattamente calcolabili in termini delle radici, ma non esattamente calcolabili in termini dei coefficienti, perché in tal caso scomparirebbero come radicali dalla formula risolutiva in termini dei coefficienti, ed avrebbero un unico valore.

Intanto abbiamo trovato una regola che è bene ricordare senza fare confusione:

"FUNZIONE SIMMETRICA DELLE RADICI = FUNZIONE RAZIONALE DEI COEFFICIENTI".

Ma che le funzioni risultanti dall'estrazione di radice non siano simmetriche in termini delle radici dell'equazione, non è una calamità. Anzi, è quello che vogliamo, altrimenti la nostra soluzione avrebbe un unico valore, perché "simmetrica" significa che il suo valore non muta permutando le radici.

Supponiamo ora che *la prima radice, la più interna in caso di radicali multipli*, da estrarre nella formula con cui si esprime esplicitamente la funzione *A* sia:

$$y = \sqrt[r]{P} \qquad (18)$$

Qui abbiamo usato la lettera *y* per indicare che stiamo lavorando soltanto su un elemento della nostra espressione per *x*; inoltre *r* non vale necessariamente 5 (ed effettivamente non vale 5). Tuttavia *r* deve essere primo. Se non lo fosse, dovremmo scomporlo nei suoi fattori primi e trattare, ad

esempio, il radicale $\sqrt[uv]{P}$ come un radicale della forma $\sqrt[u]{\sqrt[v]{P}}$, avendo posto $r = u\,v$, e $v < u$. A questo punto, riprenderemmo il lavoro sul radicale più interno, che di nuovo avrebbe un indice primo (v).

La P, per come procede il nostro studio, è una funzione delle radici dell'equazione. Non è neanche detto che le radici debbano necessariamente essere presenti tutte quante in ogni argomento di ogni radicale che troveremo nella formula completa della soluzione. Tuttavia, essendo questa la radice più interna, *P deve essere una funzione razionale, dei coefficienti dell'equazione (1)*, il che implica che sia una funzione simmetrica delle radici, cioè P deve essere invariante per qualsiasi scambio fra loro delle radici. E se P fosse una funzione algebrica, ma non razionale, dei coefficienti? Bene, "algebrica" vorrebbe solo dire che essa contiene ulteriori radicali, cioè non sarebbe il radicale più interno, ed invece che a P dovremmo applicare i ragionamenti che ora seguono ai radicali più interni che vi compaiono.

Si può notare che, nel caso generale di grado n, l'equazione

$$y = \sqrt[r]{P(x_1, x_2, x_3, \dots, x_n)} = \varphi(x_1, x_2, x_3, \dots, x_n) \qquad (19)$$

ammette r soluzioni distinte $y_1, y_2, y_3, \dots, y_r$, che differiscono soltanto per una radice dell'unità di indice r. D'altra parte le φ possibili, tutte soluzioni di questa equazione, sono $n!$, tante quante sono le possibili permutazioni delle x_i radici. Ciò ha due conseguenze:

a. r, che deve essere primo, deve essere uguale o minore di $n!$.

b. Alcune, anzi molte, φ ricavate da permutazioni differenti sono uguali tra loro, e forniscono la stessa radice y_i.

Ad esempio, nel caso dell'equazione di 5° grado, n=5, $n!$=120; queste 120 possibili φ (permutazioni) si devono distribuire uniformemente, per ragioni di simmetria, sulle r radici di P, per cui r, dovendo essere primo, è uguale o minore di 5 (deve essere primo e divisore di $120 = 2^3\ 3\ 5$). Infatti, se ad esempio r fosse uguale a 7, le 120 possibili permutazioni (e quindi le 120 possibili φ) non potrebbero distribuirsi in modo uniforme tra le r radici di P, poiché 7 non divide esattamente 120. In tal caso, ad una certa radice y_i corrisponderebbe un numero di permutazioni distinte diverso da quello che corrisponde ad un'altra y_j, e perderemmo la simmetria fra le radici, che è un poco la base del nostro discorso.

Noi siamo giunti a questo risultato per la sola ragione che le radici dell'equazione devono essere interscambiabili e quindi devono avere le stesse proprietà, tra cui quella di corrispondere a eguali porzioni delle 120 possibili permutazioni. In generale, tuttavia, va detto che abbiamo inconsciamente applicato uno dei primi teoremi della teoria dei gruppi, il Teorema di Lagrange, che Lagrange non credo abbia mai presentato come tale. Neanche a noi serve farlo.

Diversamente dalla *P*, come già notato in generale, per ipotesi la *y* non può essere simmetrica nelle radici dell'equazione, in quanto allora sarebbe una funzione razionale dei coefficienti dell'equazione (1), e la radice r-esima potrebbe essere estratta esattamente.

Ma che significa questa assenza di simmetria? Significa che se nell'equazione

$$y = \sqrt[r]{P(x_1, x_2, x_3, x_4, x_5)} = \varphi(x_1, x_2, x_3, x_4, x_5) \qquad (19)$$

noi permutiamo tra loro due radici, non sempre troviamo lo stesso valore, perché, come si è detto, $y = \varphi$ non può essere simmetrica. Ponendo dunque ai posti x_1, x_2 due radici dell'equazione che, permutate, cambino il valore del radicale φ, dobbiamo trovare due valori diversi per le due radici y_1 *e* y_2.

Qui si potrebbe osservare che magari il valore cambia solo se permutiamo fra loro tre o più radici dell'equazione. Ma l'obiezione non vale, perché qualsiasi permutazione di tre radici può essere scomposta in un prodotto di permutazioni di due radici, e quindi, se la permutazione di tre radici cambia il valore della funzione, ciò vuol dire che tra le varie permutazioni di due radici che la compongono, ce ne dovrebbe essere almeno una "malata", cioè che cambia il valore di y.

Ma come potranno essere diversi i due valori di $y = \varphi$, dal momento che $y^r = P$ e l'argomento *P* del radicale è funzione simmetrica delle due radici dell'equazione e quindi rimane invariato per la permutazione delle due radici, cioè - in questo caso - si comporta per noi come una costante? L'unica diversità che può comparire è una radice α dell'unità, diversa da 1.

> Ciò avviene per esempio per l'equazione di secondo grado, in cui possiamo avere valori diversi (in questo caso due) del radicale $\sqrt{b^2 - c}$ solo introducendo, come indicato in precedenza, due diverse radici quadrate dell'unità, una delle quali è uguale a 1.

Abbiamo quindi, senza perdita di generalità:

$$\varphi(x_2, x_1, x_3, x_4, x_5) = \alpha\, \varphi(x_1, x_2, x_3, x_4, x_5) \qquad (20)$$

Come si è detto, però, gli indici non hanno un significato assoluto e qualsiasi relazione fra radici deve restare invariata permutando fra loro le medesime. E quindi

$$\varphi(x_1, x_2, x_3, x_4, x_5) = \alpha\, \varphi(x_2, x_1, x_3, x_4, x_5) \qquad (21)$$

con la stessa α. Perché? Se non ci basta il concetto di interscambiabilità delle radici, possiamo procedere supponendo che invece sia

$$\varphi(x_1, x_2, x_3, x_4, x_5) = \beta\ \varphi(x_2, x_1, x_3, x_4, x_5) \qquad (22)$$

in cui β è una radice dell'unità differente da α. Sostituendo la

$$\varphi(x_2, x_1, x_3, x_4, x_5) = \alpha\ \varphi(x_1, x_2, x_3, x_4, x_5) \qquad (23)$$

otterremmo:

$$\varphi(x_1, x_2, x_3, x_4, x_5) = \alpha\beta\ \varphi(x_1, x_2, x_3, x_4, x_5) \qquad (24)$$

in cui, evidentemente, $\alpha\beta = 1$, ovvero, ponendo $\alpha = \gamma^A$ e $\beta = \gamma^B$, ciò che può sempre esser fatto, se γ è una radice r-esima dell'unità (Vedi Appendice), e ricordando che r è stato scelto come numero primo, otterremmo $\gamma^{A+B} = 1$. Ma se le due radici α, β dell'unità fossero diverse, come potrebbe la nostra espressione sceglierne una delle due? Come potrebbe sapere se le due radici che scambiamo sono da identificarsi con x_1, x_2 (nel qual caso si userebbe il coefficiente α) oppure con x_2, x_1(nel qual caso sarebbe richiesto il diverso coefficiente β)? Per queste ragioni non può essere altro che $\alpha = \beta$, e ciò varrebbe per qualsiasiasi coppia di radici permutassimo, che esse cambino oppure non cambino il valore della φ. Questo è, come si può osservare, solo un modo diverso di esprimere il concetto già enunciato che le radici sono fra loro interscambiabili.

A questo punto A dovrebbe essere eguale a B ma diverso da 0, e avremmo $\gamma^{2A} = 1$. Inoltre A dovrebbe essere eguale a 1, perché, in caso contrario, γ non sarebbe una radice di indice primo r dell'unità, perché c'è un solo valore di r, *primo*, che è anche pari ed è **r = 2**. Da cui A =B = 1. In conclusione $\alpha^2 = 1$, ovvero $\alpha = \pm 1$. Di qui un primo risultato notevole: *il radicale più interno che si trova nella soluzione generale di un'equazione polinomiale è invariabilmente una radice quadrata, se l'equazione è risolubile per via algebrica*. E questo lo si verifica non solo nel caso ovvio dell'equazione di secondo grado, ma anche in quelli, pure noti, delle equazioni di terzo e di quarto grado.

Per esempio, una prima soluzione di Tartaglia e Cardano dell'equazione cubica

$$t^3 + pt + q = 0 \qquad (25)$$

(forma a cui si può ridurre qualsiasi equazione di terzo grado ($x^3 + ax^2 + bx + c = 0$) mediante la sostituzione $t = x - a/3$) è data, con opportune notazioni, da:

$$t_1 = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \qquad (26)$$

Si potrebbe qui osservare anzitutto che l'equazione in *t* manca del coefficiente di secondo grado, e quindi, per quanto detto in precedenza, la formula risolutiva di Tartaglia-Cardano non sembra propriamente generale. Ma qualsiasi equazione di terzo grado può essere ridotta alla forma (23) per cui anche la soluzione (24) ha valore generale. Inoltre, il primo coefficiente ricompare subito nel suo pieno vigore usando la relazione $t = x - a/3$, con modifica opportuna degli altri coefficienti, con la sola conseguenza di complicare i calcoli che conducono alla soluzione.

In secondo luogo si potrebbe verificare che se fosse $p = 0$, le radici quadrate scomparirebbero, contrariamente a quanto dimostrato dalla teoria. Il caso di questo coefficiente è però diverso dal precedente. Anch'esso può esser fatto scomparire dall'equazione (trasformazione di Tschirnhaus), ma, per ottenerlo, ricomparirebbero le radici quadrate. Oppure lo si dovrebbe imporre eguale a zero, violando così la generalità della formula.

In generale, è ovvio che, in alcuni casi particolari di relazioni tra i coefficienti dell'equazione, l'argomento della radice quadrata può diventare 0, per cui la radice scompare. Ciò avviene ad esempio per le equazioni di secondo grado quando è 0 il discriminante dei coefficienti (l'equazione ammette due radici coincidenti), o per le equazioni di terzo grado quando vi sono tre radici coincidenti, ossia del tipo $x^3 - a = 0$.

La nostra prima *y* in generale ha dunque due valori eguali ed opposti, che si ottengono scambiando fra loro due date radici. Ma si può dimostrare che questo vale per qualsiasi coppia di radici. Infatti, se x_1 ed x_2 sono due radici che, permutate in *P*, fanno passare da φ_1 a φ_2, ed x_3 è un'altra radice, supponiamo per assurdo che permutando x_1 ed x_3 (la prima e la terza radice) si rimanga sulla stessa φ_1, mentre permutando x_1 ed x_2 (la prima e la seconda radice) si passa da φ_1 a φ_2.

Mettendo a primo membro la permutazione che viene considerata, abbiamo:

a) $x_1, x_2, x_3 \rightarrow \varphi_1$
b) $x_2, x_1, x_3 \rightarrow \varphi_2$ (permutazione di x_1 ed x_2 – φ cambia da φ_1 a φ_2)
c) $x_3, x_1, x_2 \rightarrow \varphi_2$ (permutazione della prima e della terza radice in (b) – φ_2 non cambia)
d) $x_1, x_3, x_2 \rightarrow \varphi_1$ (permutazione della prima e della seconda radice in (c)

– φ_2 cambia)
e) $x_3, x_1, x_2 \rightarrow \varphi_1$ (permutazione della prima e della terza radice in (d) – φ_1 non cambia)
f) $x_3, x_2, x_1 \rightarrow \varphi_2$ (permutazione della prima e della seconda radice in (e) – φ_1 cambia)

e si deduce che permutando ora x_1 ed x_3 (ossia la prima e la terza radice) in *P* si trova che $\varphi_1 = \varphi_2$. Il che è contro l'ipotesi.

Il ragionamento può essere ripetuto per qualsiasi coppia di radici x_i e x_j.

Sottoponendo la *y* a permutazioni, essa assumerà sempre o l'uno o l'altro valore. In particolare, non cambierà valore operando una permutazione **circolare** di tre radici (una permutazione in cui, ad esempio, x_1, x_2, x_3 diventano x_2, x_3, x_1 o x_3, x_1, x_2), in quanto una tale permutazione equivale al prodotto di due scambi di due radici, e quindi ad un doppio cambiamento di segno.

Abbiamo infatti in generale (abc) -> (cba) -> (cab) (permutazione circolare)

Ciò vale per tutte le permutazioni circolari di un numero dispari di radici, in particolare per un numero primo di radici (avendo già preso in considerazione l'unico numero primo che è pari, cioè 2).

Vediamo ora come appare la funzione $F(x_1, x_2, x_3, x_4, x_5)$. Vi compaiono delle funzioni razionali dei coefficienti, e con queste non abbiamo problemi. Vi compaiono radici quadrate di funzioni razionali dei coefficienti, come abbiamo appena visto, le quali tutte, per permutazione circolare di tre o cinque radici, non cambieranno valore. Se non vi comparissero radici cubiche o di ordine superiore di funzioni razionali dei coefficienti, la F non cambierebbe valore per la permutazione circolare di tre radici, perché non cambierebbe valore nessun elemento di essa. Ma questo è un guaio, perché la nostra soluzione generale:

$$[F(x_1, x_2, x_3, x_4, x_5) - x_1\ ] = 0 \qquad (27)$$

permutando circolarmente tre radici, ad esempio x_1, x_2, x_3, in modo che x_1 diventi x_2, porgerebbe:

$$[F(x_2, x_3, x_1, x_4, x_5) - x_2\ ] = 0 \qquad (28)$$

cioè, considerando che *F* rimane invariata per questo tipo di permutazione, si avrebbe in generale $x_1 = x_2$, che, invece, in generale non è vero. Naturalmente, se l'equazione fosse di secondo grado, e quindi con

due sole radici, il problema non si presenterebbe, perché una permutazione circolare di tre radici non esisterebbe; sarebbe solo possibile una trasposizione di due radici, con conseguente cambiamento di segno del valore del radicale.

Dunque, se esistono più di due radici, devono esserci altri radicali che non sono soggetti alla restrizione indicata. In particolare, nel caso dell'equazione cubica, dobbiamo trovare anzitutto una $z = \sqrt[r]{Q}$ che possa assumere **almeno tre valori.** Quanto vale r?

Il problema incontrato, che limitava il numero di radici diverse possibili, sorgeva dal fatto che la funzione *P* sotto radice era una funzione razionale dei coefficienti, e quindi era simmetrica nelle radici dell'equazione. Dunque, per risolvere il problema, la *Q* non potrà più essere simmetrica, e quindi non sarà più una funzione razionale dei coefficienti, ma una loro funzione algebrica, cioè conterrà dei radicali. Ma, siccome i più interni di questi radicali dovranno avere come radicandi delle funzioni razionali dei coefficienti, non potranno essere altro che radicali di indice 2, come abbiamo visto. Di conseguenza, ogni *Q* che conterrà radicali di indice 2 sarà invariabile per permutazioni circolari di tre, cinque, sette, etc., elementi.

Avremo quindi una *z* che, sottoponendo le radici dell'equazione ad una permutazione circolare di tre, cinque, sette elementi, dovrà poter assumere diversi valori, ma tale che sia sempre $z^r = Q$, con *Q* invariato, poiché tale resta per una permutazione circolare di tre, cinque, sette valori. Dovremo quindi ricorrere di nuovo alle radici dell'unità per avere valori differenti.

Designando con α una opportuna radice *r*-esima dell'unità si avrà dunque, per una permutazione circolare di tre elementi e con *r* numero primo,

$$\varphi(x_2, x_3, x_1, x_4, x_5) = \alpha\varphi(x_1, x_2, x_3, x_4, x_5) \qquad (29)$$

Questa relazione dovrà essere valida ogni volta che si permutano circolarmente le prime tre radici dell'equazione (questo ci garantisce che abbiamo sempre a che fare con la stessa α). Se ne dedurrà immediatamente, operando due nuove permutazioni circolari, riguardanti le prime tre radici dell'equazione:

$$\begin{aligned} \varphi(x_3, x_1, x_2, x_4, x_5) &= \alpha\varphi(x_2, x_3, x_1, x_4, x_5) \\ \varphi(x_1, x_2, x_3, x_4, x_5) &= \alpha\varphi(x_3, x_1, x_2, x_4, x_5) \end{aligned} \qquad (30)$$

Da cui:

$$\alpha^3 = 1 \text{ cioè } \mathbf{r = 3}$$

Se preferiamo, possiamo procedere come nel caso di secondo grado: possiamo per assurdo supporre che nelle (29) e (30), la prima $\alpha = \gamma^A$, la seconda sia $\beta = \gamma^B$, la terza sia $\zeta = \gamma^C$, e quindi $\gamma^{A+B+C} = 1$, con la solita ambiguità per la nuova φ di scegliere tra A, B, C, data l'indifferenza della funzione allo scambio degli indici delle radici. Di qui, A = B = C, e una sola α può essere usata.

Dunque il nuovo radicale incontrato, dopo quelli di indice 2, nel valore di x_1 dovrà essere di indice 3. Questo può di nuovo essere verificato sulle equazioni di terzo grado (per questo rimandiamo all'espressione scritta più sopra) ed anche in quelle di quarto grado.

Come la funzione *y* del caso precedente aveva due valori, rispettivamente *+y* e *-y*, la funzione *z* avrà quindi tre valori che chiameremo *z, αz, α^2z.*

Supponiamo ora che esistano più di quattro radici. In tal caso si possono anche operare nell'identità $z^3 = Q$ (si noti l'esponente 3) delle permutazioni circolari di cinque radici, che, come sappiamo, lasciano *Q* invariato. Per *z* (= *φ*), invece, sussistono solo due possibilità, pur permutando le cinque radici: o resta anch'esso invariato, nel qual caso il lavoro – come vedremo - è già fatto, o passa per i valori *αz, α^2z.*

In quest'ultimo caso, si può scrivere l'identità:

$$\varphi(x_2, x_3, x_4, x_5, x_1) = \alpha\varphi(x_1, x_2, x_3, x_4, x_5) \qquad (31)$$

relazione che deve rimanere valida ogni volta che si permutano ciclicamente tra loro le cinque radici dell'equazione. Si potrà quindi ripetere altre quattro volte la permutazione circolare delle cinque radici, e si avrà:

$$\begin{aligned}
\varphi(x_3, x_4, x_5, x_1, x_2) &= \alpha\varphi(x_2, x_3, x_4, x_5, x_1) \\
\varphi(x_4, x_5, x_1, x_2, x_3) &= \alpha\varphi(x_3, x_4, x_5, x_1, x_2) \\
\varphi(x_5, x_1, x_2, x_3, x_4) &= \alpha\varphi(x_4, x_5, x_1, x_2, x_3) \\
\varphi(x_1, x_2, x_3, x_4, x_5) &= \alpha\varphi(x_5, x_1, x_2, x_3, x_4)
\end{aligned} \qquad (32)$$

Da cui si ricava (in base al ragionamento già usato due volte):

$$\alpha^5 = 1 \qquad (33)$$

Il problema è che il radicale su cui stiamo lavorando è cubico e quindi *α* è una radice terza dell'unità, da cui:

$$\alpha^3 = 1 \qquad (34)$$

e quindi

$$\alpha^6 = 1, \qquad (35)$$

che, dividendo membro a membro la (35) per la (33), risulta possibile solo se

$$\alpha = 1,$$

cioè φ è invariabile per permutazioni circolari di cinque radici. Non solo, ma questa invariabilità si riflette anche sulle permutazioni di tre radici, perché abbiamo trovato appunto che $\alpha = 1$.

Intanto c'è una contraddizione, perché avevamo fatto l'ipotesi che il radicale cubico provvedesse tre valori, mentre vediamo che se ci sono più di quattro radici il radicale cubico provvede un solo valore. Dunque il radicale che segue quello quadratico sarà cubico e fornirà tre valori solo se l'equazione avrà al massimo quattro radici, cioè sarà di quarto grado. Altrimenti fornirà un solo valore. Questo, per il Carnoy, è un assurdo sufficiente a dimostrare che la dimostrazione è impossibile per l'equazione di quinto grado.

Inoltre, nel testo del Serret si nota che è inutile procedere oltre: poiché tutti i radicali racchiusi nell'espressione della radice di un'equazione generale di quinto grado sono eguali a funzioni razionali delle radici, che sono invariabili in seguito a una permutazione circolare di tre radici, la F che compare nella nostra equazione (16)

$$[F(x_1, x_2, x_3, x_4, x_5) - x_1\ ] = 0 \qquad (16)$$

gode della stessa particolarità, cioè anche la soluzione F è invariante per permutazioni circolari di tre radici. Ora, questo è assurdo, a meno che le tre radici non siano eguali tra loro, in quanto una prima permutazione circolare di tre radici della (16) darebbe:

$$F(x_2, x_3, x_1, x_4, x_5) - x_2 = 0$$

Ma $F(x_2, x_3, x_1, x_4, x_5) = F(x_1, x_2, x_3, x_4, x_5)$, che è già eguale a x_1.

Quindi (per il Serret) il caso è chiuso: la soluzione generale dell'equazione di quinto grado per mezzo di radicali è impossibile.

L'argomento può comunque essere esteso ad equazioni di grado superiore a 5, in quanto equazioni di grado superiore possono essere costruite introducendo radici note, nel modo seguente (ad esempio per l'ottavo

grado, con *a,b,c* noti, e anche nulli):

$$(x-a)(x-b)(x-c)P_5(x) = 0 \qquad (37)$$

Ma, divisa l'equazione per i monomi *(x-a)(x-b)(x-c)*, ciò che è sempre possibile fare, si tornerebbe al nocciolo dell'equazione di quinto grado,

$$P_5(x) = 0 \qquad (38)$$

per la quale la soluzione generale non esiste. Da cui segue che non può esistere neppure una soluzione generale per le equazioni di ordine superiore.

E con questo resta dimostrato il teorema di Ruffini (e anche di Abel).

Questa, ovviamente, non è intesa essere una dimostrazione rigorosa, ma vuol solo dare un'idea dei vari punti fermi della dimostrazione. Confesso però che questa dimostrazione mi lascia insoddisfatto, nel senso che c'è qualcosa di non definibile che ancora mi sfugge. Ad esempio se il radicale cubico produce un solo valore in un'equazione di quinto grado, potrebbero esserci radicali di quinto grado, con cinque radici, che non mi sembrano adeguatamente considerati. Il Comberousse se la cava dicendo che "applicando lo stesso ragionamento" ai radicali di ordine superiore, si giunge alla stessa conclusione (che non ci possano essere radicali di grado superiore al quinto lo abbiamo visto a pagina 13).

Per questo motivo invito il lettore a seguirmi in una dimostrazione assai più vicina a quella di Ruffini del 1813, in parte basata su quanto appreso fin qui dalla scuola francese derivata dal Wantzel e in parte ispirata alla dimostrazione del Maracchia ("*Storia dell'Algebra*", Liguori, Napoli, 2005).

La chiave della dimostrazione di Ruffini del 1813 resta l'esame di espressioni del tipo di (16), ma, per così dire capovolge la dimostrazione.

(i) $$y = \sqrt[r]{P(x_1,x_2,x_3,x_4,x_5)} = \varphi(x_1,x_2,x_3,x_4,x_5)$$

Ovvero: $$y^r = P$$

Si consideri ora una soluzione y_1, che potrà essere espressa come

(ii) $y_1 = \varphi(x_1,x_2,x_3,x_4,x_5) = \zeta\sqrt[r]{P(x_1,x_2,x_3,x_4,x_5)}$, con

$$\zeta^r = 1.$$

come abbiamo visto più sopra.

Ruffini ora dimostra quattro teoremi che in parte conosciamo. In quello che il Maracchia chiama Teorema I, effettua cinque permutazioni circolari che risultano in:

$$\begin{aligned} y_2 &= \varphi(x_2, x_3, x_4, x_5, x_1) \\ y_3 &= \varphi(x_3, x_4, x_5, x_1, x_2) \\ y_4 &= \varphi(x_4, x_5, x_1, x_2, x_3) \qquad (iii) \\ y_5 &= \varphi(x_5, x_1, x_2, x_3, x_4) \end{aligned}$$

Ma y_1^r = P, e come si è visto in precedenza, ciò vale per tutte le altre y_i. Come visto più sopra, se ne deduce che

$$\begin{aligned} y_2 &= \alpha\varphi(x_2, x_3, x_4, x_5, x_1) \\ y_3 &= \alpha\varphi(x_3, x_4, x_5, x_1, x_2) \\ y_4 &= \alpha\varphi(x_4, x_5, x_1, x_2, x_3) \qquad (iii) \\ y_5 &= \alpha\varphi(x_5, x_1, x_2, x_3, x_4) \end{aligned}$$

Dove però $\alpha^5 = 1$, ma non vale più $\alpha^3 = 1$, che nella dimostrazione precedente concludeva il discorso.

Qui interviene un secondo teorema di Ruffini (Teorema II): si supponga che $P\ (x_1, x_2, x_3, x_4, x_5\ )$ sia anche invariante rispetto alla permutazione circolare dei primi tre elementi, cioè

$$\begin{aligned} P(x_1, x_2, x_3, x_4, x_5\ ) &= P(x_2, x_3, x_1, x_4, x_5) \\ &= P(x_3, x_1, x_2, x_4, x_5) \end{aligned}$$

E chiamiamo:

$$\begin{aligned} y_1 &= \varphi(x_1, x_2, x_3, x_4, x_5\ ) \\ y_a &= \varphi(x_2, x_3, x_1, x_4, x_5) \\ y_{a+1} &= \varphi(x_3, x_1, x_2, x_4, x_5) \end{aligned}$$

Si tratta di mostrare che i tre valori di y_i sono eguali. Questo lo si è già fatto nel caso dell'equazione (29), ottenendo che si passa da una y_i alla successiva moltiplicandola per una radice dell'unità che per evitare confusioni chiameremo qui β, tale che $\beta^3 = 1$.

Eseguiamo ora una permutazione circolare del quinto ordine, su y_a, in modo da ottenere

$$y_b = \varphi(x_3, x_1, x_4, x_5, x_2)$$

Abbiamo cioè applicato "il prodotto" di una permutazione circolare di 3

elementi e quello di una permutazione circolare di cinque elementi per passare da y_1 a y_b. Ripetiamo cinque volte l'operazione, con i seguenti risultati (non è troppo difficile: si pensi prima a una permutazione circolare di tre elementi e poi a una di cinque):

$$y_{b+1} = \varphi(x_4, x_3, x_5, x_2, x_1)$$
$$y_{b+2} = \varphi(x_5, x_4, x_2, x_1, x_3)$$
$$y_{b+3} = \varphi(x_2, x_5, x_1, x_3, x_4)$$
$$y_{b+4} = \varphi(x_1, x_2, x_3, x_4, x_5) = y_1$$

Ora, y_b proviene da y_a mediante la stessa permutazione circolare del quinto ordine che fa passare da y_2 a y_1 (Teorema I), e quindi sappiamo che esiste una radice quinta α dell'unità che garantisce che

$$y_b = \alpha y_a$$

Da cui:

$$y_b = \alpha\, \beta y_1$$

Sfruttando lo stesso ragionamento dell'intercambiabilità delle radici già più volte usato, operando cinque volte con αβ, abbiamo che $(\alpha\beta)^5 = 1$.
Ma già sappiamo che $\alpha^5 = \beta^3 = 1$, e quindi si deve avere (per il ragionamento visto in precedenza, $\beta^6 = \alpha^5 = 1$) che $\beta = 1$ e quindi, $y_1 = y_a = y_{a+1}$.

In modo analogo si dimostra che sono eguali $y_1 = y_c = y_{c+1}$, operando con tre permutazioni circolari del terzo ordine sulle ultime tre variabili che compaiono nella $\varphi(x_1, x_2, x_3, x_4, x_5)$. Abbiamo cioè

$$y_1 = y_c = y_{c+1}$$

ovvero:
$\varphi(x_1, x_2, x_3, x_4, x_5) = \varphi(x_1, x_2, x_4, x_5, x_3) = \varphi(x_1, x_2, x_5, x_3, x_4)$.

Segue ora il Teorema IV, secondo il quale, se P è invariante rispetto a tutte le permutazioni considerate nei Teoremi I-III, allora sono anche eguali le funzioni considerate

$$y_1 = y_2 = y_3 = y_4 = y_5 = y_a = y_{a+1} = y_c = y_{c+1}$$

L'uguaglianza di

$$y_1 = y_a = y_{a+1} = y_c = y_{c+1}$$

deriva dai Teoremi II e III.

Ma applicando la permutazione circolare sulle tre ultime variabili (permutazione che crea y_c e y_{c+1}) a y_a (= y_1) si ottiene

$$(iv) \quad y_a = \varphi(x_2, x_3, x_1, x_4, x_5) \rightarrow \varphi(x_2, x_3, x_4, x_5, x_1) = y_2$$

E quindi $y_1 = y_2$. Ne segue che la radice α dell'unità che legava le permutazioni di y_1, y_2, y_3, y_4, y_5 vale 1, e l'uguaglianza di tutte le funzioni indicate è dimostrata.

L'argomento, però, non è conclusivo se n=4.
Si considerino le tre permutazioni, che, con notazione ovvia e tradizionale, possiamo indicare come

$$\tau = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_1 \end{pmatrix} \quad ; \quad \tau_a = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_1 & x_4 \end{pmatrix} \quad ; \quad \tau_c = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_3 & x_4 & x_2 \end{pmatrix}$$

rispetto alle quali l'invarianza di P può essere ancora dimostrata. Si ha che:

$$y_1 = \varphi(x_1, x_2, x_3, x_4) = y_a = \varphi(x_2, x_3, x_1, x_4) = y_{a+1} = \varphi(x_3, x_1, x_2, x_4) = y_c = \varphi(x_1, x_3, x_4, x_2) = y_{c+1} = \varphi(x_1, x_2, x_5, x_3, x_4)$$

Applicando ora la τ_c a y_a si ottiene $\varphi(x_2, x_1, x_4, x_3)$, che è diversa dalla

$$y_2 = \varphi(x_2, x_3, x_4, x_1)$$

A differenza di quanto avveniva nella (iv).
Ne segue che non si possono applicare le conseguenze del teorema IV, che "saldano" le due serie di funzioni eguali.
Così la dimostrazione di Ruffini non può garantire (e infatti non è vero) che le equazioni di quarto grado non abbiano soluzioni algebriche generali.

Il teorema di impossibilità può essere ora formulato negli stessi termini usati in precedenza dagli autori francesi. Se vogliamo che alla fine si possano avere le cinque identità differenti

$$x_i = x_i \text{ per } i = 1,2,3,4,5$$

due condizioni devono essere soddisfatte:

1) Non devono essere presenti radicali dei coefficienti che non sono risolubili con funzioni razionali delle radici;

2) Le funzioni razionali delle radici devono assumere cinque valori differenti, permutandole.

Poiché le funzioni che compaiono sono tutte invariabili per permutazioni delle radici, abbiamo che nella (16)

$$[F(x_1, x_2, x_3, x_4, x_5) - x_1] = 0$$

permutando le radici nella F, essa non varia, mentre varia la variabile isolata.

Il che dimostra il teorema di Ruffini.

So che Crispin preferiva la formulazione di Ruffini a quella di Wantzel e successori. Spero di averlo accontentato.

3. Commento generale.

A pensarci bene, non avrebbe dovuto essere considerato uno scandalo il fatto che un'equazione di grado superiore al quarto non fosse risolubile per mezzo di radicali.
Si pensi all'equazione di primo grado. In un mondo in cui non si sia ancora introdotta l'operazione della divisione, l'equazione (ridotta alla forma canonica)

$$a\,x + b = 0 \qquad (39)$$

sarebbe insolubile, a parte il caso banale $x + a = 0$.
Si introduce la divisione e si possono risolvere tutte le equazioni di primo grado.
Ora si cerchi di risolvere le equazioni di secondo grado. Di nuovo, se non introduciamo le radici quadrate, che non sono estensioni banali delle quattro operazioni note (sebbene non possano fare a meno di usarle), non possiamo risolvere l'equazione generale

$$a\,x^2 + bx + c = 0 \qquad (40)$$

ma solo qualche caso particolare, come

$$a^2\,x^2 - c^2 = 0 \qquad (41)$$

Che, senza estrazione di radici, porgerebbe

$$(ax + c)(ax - c) = 0 \quad \text{e quindi } x = \pm\frac{c}{a} \qquad (42)$$

Invece, l'introduzione dei radicali di secondo e terzo grado ci permette la soluzione delle equazioni di secondo, terzo e quarto grado (anche perché 4 non è un numero primo, e una radice quarta può essere calcolata per mezzo di due radici quadrate in successione). Ma, come abbiamo visto, un radicale, valido per le equazioni di secondo, terzo, quarto grado, è un'operazione concettualmente diversa da una divisione, che bastava per le equazioni di primo grado. Che si possano risolvere le equazioni di terzo e quarto grado per mezzo di radicali, funzioni introdotte per le equazioni di secondo grado, dovrebbe essere

considerato grasso che cola.

Perché dobbiamo aspettarci che le equazioni di quinto grado siano risolubili coi radicali, funzioni che andavano bene per i gradi inferiori? Infatti non è così. Ma non per questo non esistono soluzioni per le equazioni di quinto grado. Semplicemente, si tratta di funzioni più avanzate dei radicali. Il teorema ora detto di Abel-Ruffini (a torto, secondo me), e l'assai più estesa teoria di Galois, NON affermano che non esistono soluzioni, ma solo che non esistono soluzioni GENERALI per mezzo di radicali.
Grazie a sviluppi successivi, da un lato si studiò se a priori si potesse determinare se un'equazione di quinto grado fosse risolubile per mezzo di radicali (ne abbiamo vista una banalissima); dall'altro furono introdotte altre funzioni più avanzate di quelle algebriche, che provvedono soluzioni generali alle equazioni di grado superiore. Verso la metà del XIX secolo si diedero infatti soluzioni ad opera, inizialmente, di Betti [1] (1854; ignorato come sempre sono i precursori italiani) , Hermite (1858) , Brioschi (che diede anche la soluzione delle equazioni di sesto grado) , Kronecker, in termini di Funzioni Ellittiche modulari ed altre - tutte funzioni delle quali, ai tempi di Ruffini, non si parlava ancora. Secondo Wikipedia (2018) le soluzioni in forma chiusa pubblicate giungono al sesto grado.

L'unica impressione che ne ritraggo è che di fronte a fatti come questo è difficile pensare che la matematica abbia un'esistenza legata a come funziona il nostro cervello e non piuttosto indipendente, esistenza certo con caratteri assai diversi dalla nostra. A me pare che affermare che i risultati matematici sono una creazione del nostro cervello invece che una scoperta, equivalga a dire che chi cercava le sorgenti del Nilo in realtà le aveva messe lui dov'erano, sugli altipiani dell'Africa Centrale. E quando? E come? Mah!

([1]) Betti, in effetti, nel suo articolo del 1854 scrisse: “Cogli inversi degli integrali ultraellittici che si debbono al’Abel, io ho trovato la risoluzione analitica effettiva di qualunque equazione algebrica generale” (Annali di Science Matematiche e Fisiche , t.V, pp.10-17, Roma, 1854). Personalmente non so come sia valutata dai matematici moderni questa affermazione di Betti.

APPENDICE

Potenze delle radici *p*-esime dell'unità, con *p* primo.

Dimostriamo ora l'affermazione, che, data una *qualsiasi* radice *p*-esima α dell'unità, diversa da 1, le varie sue potenze, $\alpha, \alpha^2, \ldots, \alpha^{p-1}$ sono le *p*-1 *differenti* radici diverse da 1 dell'equazione $x^p - 1 = 0$, ma *solo se p è primo*.

Infatti, tra le varie radici *p*-esime dell'unità diverse da 1 (dove *p* può anche non essere primo), in generale ce ne sono alcune che, elevate ad un esponente *k* minore di *p*, già danno 1, cioè

$$\alpha^k = 1 \text{ per } k \leq p$$

Il più piccolo di questi valori *k* è definito *esponente* della radice α.

Teorema: L'esponente *k* di una radice non primitiva deve essere un divisore di *p*.

Dimostrazione: Sia d = MCD(k, p). Per il Teorema di Bézout, che ho già dimostrato in questo sito,

$$d = m\,k + n\,p, \text{ da cui}$$

$\alpha^d = \alpha^{mk+np} = \alpha^{mk}\alpha^{np} = (\alpha^k)^m\,(\alpha^p)^n = 1$, perché sappiamo che $\alpha^k = 1$ e $\alpha^p = 1$.

Ma *k* è l'*esponente* della radice α, e quindi è il più piccolo esponente per cui vale $\alpha^k = 1$. Di conseguenza deve essere $k \leq d$.

D'altronde *d* è un divisore di *k*, per cui $d \leq k$.

Ne segue che $d = k$.

Ma sappiamo che *d* è un divisore di *p*, per cui $k = d$ deve essere un divisore di *p*. **CDD.**

Una radice *p*-esima dell'unità diversa da 1 è definita *primitiva* se il suo esponente $k = p$.

Corollario: Se, nell'equazione $\alpha^p = 1$, p è un numero primo, tutte le radici dell'equazione sono primitive.

Dimostrazione: Una radice non primitiva ha per esponente un divisore di p, mentre una radice primitiva ha per esponente p stesso. Ora, se p è primo, esso non ha divisori, e quindi tutte le sue p-1 radici diverse da 1 (cioè tutte a parte 1) sono primitive. **CDD**

Ora, *tutte* le potenze *n*-esime di una radice ***primitiva*** α per $n \leq p$ sono *tutte* le diverse *p*-1 radici dell'unità (la *p*-esima essendo sempre =1). Ciò avviene perché se due *diverse* potenze *r*, *s* fossero eguali, il loro rapporto sarebbe 1, e quindi $\alpha^{r-s} = 1$, cioè, essendo *r* ed *s* minori di *p*, avremmo che α elevata ad un numero minore di *p* sarebbe eguale a 1, e quindi non sarebbe più ***primitiva***.