Capitolo 9

L'opera di Évariste Galois

9.1 Galois tra realtà e mito

Sulla vita di Évariste Galois (1811-1832) è stato scritto molto, forse per i risvolti la drammatici delle vicende che lo hanno visto coinvolto. Nell'immaginario collettivo di molti matematici Galois rappresenta il prototipo del genio incompreso da un sistema di valutazione ottuso che premia la mediocrità servile piuttosto che le idee brillanti che rompono gli schemi. Questa visione di un Galois solo contro tutto e contro tutti è stata diffusa soprattutto dal capitolo a lui dedicato nella monografia di E.T. Bell *Men of Mathematics* la cui attendibilità storica è stata impietosamente messa in discussione da Tony Rothman in un articolo [2] dove—con il ricorso alle fonti e senza una manipolazione finalizzata ad esaltare, esasperandoli, certi contrasti od incomprensioni che Galois certamente ebbe con le istituzioni scolastiche prima e con l'Accademia poi—ha ridimensionato o annullato del tutto la verosimiglianza di aneddoti su Galois che, senza aggiunere nulla alle sue indiscutibili doti matematiche, ne alterano i connotati. Mi sembra opportuno allontanarmi un poco in questo capitolo dall'impostazione seguita sinora per dedicare spazio ad alcuni aspetti della vita di Galois che aiutano a valutarlo meglio.

Bisogna dire che Galois non visse in un contesto storico facile: la Parigi della prima metà del XIX secolo era attraversata da profonde inquietudini. Una delle leggende su Galois è quella secondo cui egli non avrebbe mai trovato insegnanti che lo abbiano apprezzato o inoraggiato. Galois ebbe la sua formazione preuniversitaria a Parigi presso il Lycée Louis-le-Grand, che annovera altri studenti celebri come Maximilien Robespierre ed il romanziere Victor Hugo. Il suo rendimento scolastico non fu basso ma l'insegnante di matematica, Vernier, spronava Galois a lavorare in modo più sistematico: *intelligente, sensibili miglioramenti ma metodo insufficiente* è uno dei giudizi su Galois di Vernier. Galois, senza aver seguito classi preparatorie speciali ed un anno prima del consueto, tentò nel 1828 l'ammissione alla École Polytechnique, senza successo. Senza perdersi d'animo prese a seguire nello stesso anno le lezioni di un eccellente docente di

matematica, Louis-Paul-Émile Richard (1795-1849), che sarebbe stato insegnante di un altro grande matematico, Charles Hermite. Richard comprese subito l'enorme potenziale di Galois e lo incoraggiò molto. La fiducia riposta in lui agì da stimolo su Galois che proprio nel 1829 pubblicò sugli *Annales des Mathématiques* diretti da Joseph Diaz Gergonne il suo primo lavoro sulle frazioni continue periodiche. Nello stesso anno Galois stava già lavorando alla teoria delle equazioni algebriche ed alla fine di maggio sottopose al giudizio dell'*Académie* le sue prime ricerche sulla risolubilità delle equazioni di grado primo. Recensore del lavoro fu nominato Augustin-Louis Cauchy il cui comportamento è stato deformato da diverse ricostruzioni secondo le quali egli avrebbe perduto, dimenticato o addirittura deliberatamente distrutto i manoscritti di Galois, finendo per avere sulla coscienza la fine di un grandissimo matematico. Sul ruolo di Cauchy e su una sua *riabilitazione* a dispetto delle tradizioni consolidate si è pronunciato Rothman a partire da una lettera di Cauchy rinvenuta negli archivi della *Académie* da René Taton che dimostra come Cauchy non avesse perduto il lavoro di Galois ma che al contrario, si stava preparando a presentarlo all'Accademia unitamente ad alcune sue note nel gennaio 1830. Nel frattempo Galois aveva fallito per la seconda volta l'ammissione all'École Polytechnique nel luglio del 1829. L'episodio della mancata ammissione di Galois all'École Polytechnique, con tanto di lancio di cancellino in direzione di uno degli esaminatori, viene spesso utilizzato per avvalorare la tesi di Galois incompreso da insegnanti che non erano all'altezza. La tradizione della reazione stizzita di Galois, già riportata come non verificata da Dupuy in un primo lavoro del 1896 dedicato alla vita di Galois [3] nasconde invece una verità molto più amara, che avrebbe segnato il resto della breve vita di Galois. Il 2 luglio 1829, pochi giorni prima dell'esame di ammissione all'*École*, il padre di Évariste, Nicholas Gabriel, si suicidò nel suo appartamento parigino, a due passi dal liceo Louis-le-Grand. Non è certo difficile immaginare come Galois non fosse nelle migliori condizioni per affrontare una prova selettiva e questo tragico evento può certo spiegare meglio il suo comportamento. La mancata ammissione alla École Polytechique obbligò Galois a ripiegare sulla meno prestigiosa École Normale cui si iscrisse all'inizio del 1830. Fu allora, il 18 gennaio, che Cauchy scrisse la lettera cui alludevamo poc'anzi.

Proprio oggi avrei dovuto presentare all'Accademia prima un rapporto sul lavoro del giovane Galois e poi una mia memoria sulla determinazione analitica delle radici primitive nella quale dimostro come sia possibile ridurre tale determinazione alla risoluzione di equazioni numeriche dotate solo di radici intere e positive. Sono tuttavia a casa, indisposto. Sono dispiaciuto di non poter partecipare alla sessione odierna e vorrei pregarla di iscrivermi a parlare per la prossima sessione sui due argomenti indicati. La prego di accettare i miei omaggi... A.-L. Cauchy ([5], p.134, [2], p. 88)

Questa lettera dimostra che, sei mesi dopo aver ricevuto i manoscritti di Galois, Cauchy ne era ancora in possesso, li aveva letti e, probabilmente, si era reso conto della loro importanza. Tuttavia il 25 gennaio Cauchy presenta all'Accademia solo la sua memoria ma non il lavoro di Galois. Perché? Non sembrano esservi documenti in grado di spiegare il cambio di opinione di Cauchy

ma Taton [4, 5] ha ipotizzato che nella settimana tra il 18 ed il 25 gennaio Cauchy abbia convinto Galois a combinare i risultati delle sue ricerche in un'unica memoria con cui concorrere al premio di matematica indetto dall'Accademia, la cui scadenza era prevista per il 1 marzo. Benché non sia possibile provare che Cauchy abbia agito così, resta il fatto che Galois presentò a febbraio una memoria a Fourier, segretario perpetuo dell'Accademia. A suffragare la tesi di un Cauchy favorevolmente impressionato dal lavoro di Galois, Taton riporta un estratto del giornale *Le Globe* apparso il 15 giugno del 1831 ed in cui si chiedeva la liberazione di Galois che nel frattempo era stato arrestato, come vedremo fra poco. Qui leggiamo:

L'anno scorso, prima del 1 marzo, il Sig. Galois consegnò al Segretario dell'Istituto una memoria sulla risoluzione delle equazioni numeriche. Tale memoria avrebbe dovuto partecipare al Gran Premio di Matematica. Essa meritava il premio in quanto poté risolvere alcune difficoltà che Lagrange non era riuscito a superare. Il sig. Cauchy attribuiva sommi elogi all'autore per quanto seppe fare. E cosa è successo? La memoria è andata perduta ed il premio viene assegnato senza la partecipazione del giovane studioso. ([2], p. 89)

L'incidente cui si allude è la morte di Fourier, avvenuta nell'aprile del 1830: tra le carte di Fourier non si trovò traccia del lavoro di Galois, su cui peraltro Fourier non era l'unico a doversi pronunciare visto che la commissione era composta anche da Legendre, Lacroix, Poinsot e Poisson. Questa fatalità certo contribuì ad inasprire il carattere non facile di Galois che però riuscì a pubblicare tra aprile e giugno tre lavori sul *Bulletin des Sciences Mathématiques* edito da André d'Audebard, barone di Férussac e che aveva Christian Sturm (1803-1855) nel comitato di redazione: Sturm è un altro matematico che credette nelle doti di Galois. La parte principale del lavoro di Galois sulle equazioni (la teoria di Galois) si può considerare comunque pronta a metà del 1830 il che sfata un altro dei miti che circondano la figura di Galois, cioè che egli abbia gettato le basi della teoria nella febbrile veglia notturna precedente il duello in cui venne ucciso.

Le vicende del Galois matematico si intrecciano sempre più con il suo impegno politico. Le tendenze liberali ereditate dai genitori si erano esasperate dopo la tragica morte del padre avvenuta per lo scandalo suscitato da alcuni poemetti oltraggiosi circolati sotto il suo nome ma in realtà scritti da un sacerdote conservatore. Inutile dire che il legame tra gesuiti e Borboni, unito alla parte che ebbe lo sconsiderato uomo di chiesa nel suicidio del padre di Galois, contribuirono ad alimentare il suo odio verso la monarchia. Con la rivoluzione di luglio re Carlo X Borbone è costretto ad abbandonare la Francia ed al suo posto si insedia Luigi Filippo. Alla rivoluzione parteciparono anche gli studenti dell'*École Polytechnique* ma non quelli dell'*École Normale* che furono chiusi dentro la scuola dal direttore, Guigniault, contro cui Galois polemizzò a distanza rimediando l'espulsione dalla scuola. Galois cercò nel gennaio del 1831 di organizzare un corso privato di matematica ma il suo impegno politico impedì la continuazione di questo esperimento. Sul fronte matematico, Galois inviò una terza versione all'Accademia della sua famosa memoria, su invito di Poisson. Nel maggio del 1831 gli eventi precipitarono. Per festeggiare la liberazione di

diciannove repubblicani che si erano rifiutati di consegnare le armi quando la Guardia Nazionale, il corpo cui appartenevano, fu disarmata su ordine di Luigi Filippo il 31 dicembre 1830, Galois si ritrovò in un ristorante parigino il 9 maggio con circa duecento altri repubblicani. Ad un certo punto, tra un brindisi e l'altro, Galois ne propose uno "a Luigi Filippo!" brandendo un pugnale in una mano. Il gesto, forse mal compreso, costò un primo arresto a Galois: l'episodio fu anche riportato da Alexandre Dumas (padre), presente nel ristorante. Liberato dopo poco, fu arrestato nuovamente nel luglio 1831 perché il giorno della presa della Bastiglia fu sorpreso aggirarsi per le strade armato e vestito con un'uniforme della Guardia Nazionale vietata perché utilizzata dai repubblicani a scopi politici e ritenuta oltraggiosa verso il regime. Concluso il processo, il 23 ottobre Galois fu condannato a sei mesi di reclusione che scontò nel carcere di S. Pelagia, dove si trovava già dopo l'arresto. Galois in carcere tentò anche il suicidio ed ebbe l'ulteriore amarezza di ricevere dal segretario dell'Accademia, François Arago, il rapporto sulla sua memoria che veniva nuovamente respinta in questi termini:

Caro sig. Galois,

il vostro lavoro fu inviato al sig. Poisson per un parere. Egli lo ha restituito allegando un rapporto che qui cito:

"Abbiamo fatto ogni sforzo per capire le dimostrazioni del sig. Galois. I suoi argomenti non sono né abbastanza chiari né sufficientemente sviluppati per permetterci di giudicarne il rigore; non ci è stato nemmeno possibile farci un'idea sul lavoro.

L'autore afferma che le proposizioni contenute nel manoscritto sono parte di una teoria generale ricca di applicazioni. Spesso parti diverse di una teoria si chiariscono a vicenda e possono essere comprese più facilmente quando sono considerate insieme piuttosto che isolate una dall'altra. Per formarsi un'opinione bisogna quindi attendere che l'autore pubblichi un resoconto più completo di questo lavoro".

Per questo motivo, vi restituiamo il manoscritto con la speranza che possiate trovare utili per il lavoro futuro le osservazioni del sig. Poisson. ([2], p. 96)

A ben vedere il rapporto, negativo quanto all'esito, non è una stroncatura ma contiene un suggerimento migliorativo. Per apprezzare questo però occorreva che Galois fosse affiancato da una guida esperta che sapesse incoraggiarlo, togliendolo dallo scoramento che ogni bocciatura comunque comporta. Purtroppo Galois era nelle peggiori condizioni, trovandosi in prigione, completamente isolato dal mondo matematico. È facile comprendere che l'esito del rapporto su Galois fu quello di un ulteriore inasprimento verso il mondo accademico. Sylvestre Lacroix, un altro dei commissari incaricati di valutare il lavoro di Galois, nella sesta edizione dei *Compléments des Éléments d'Algèbre* ricorda l'impressione avuta dal lavoro di Galois:

Nel 1831 un giovane francese, Évariste Galois, morto l'anno seguente, aveva annunciato in una Memoria presentata all'Accademia delle Scienze che, affinché un'equazione irriducibile di grado primo fosse risolubile per radicali, era necessario e sufficiente che si potessero dedurre razionalmente tutte le radici, note che ne fossero due qualsiasi; tuttavia questa memoria sembrò praticamen-

te incomprensibile ai Commissari incaricati di esaminarla[1] (*cfr.* [7], p.382, in nota).

Trasferito da Santa Pelagia per un'epidemia di colera, Galois tornò libero il 29 aprile ma un mese più tardi, il 30 maggio, fu ferito gravemente allo stomaco, in un duello sulle cui motivazioni vi sono tre versioni difformi. Secondo alcuni [2] si sarebbe trattato di un duello per vendicare l'onore di una giovane, Stephanie-Félicie Poterin du Motel, con cui Galois aveva avuto una relazione. Secondo altri, l'uccisore di Galois (Pecheaux d'Herbinville) sarebbe stato un infiltrato che avrebbe avuto l'incarico di provocare Galois in un duello per eliminarlo. La ricostruzione più attendibile è quella presentata da Laura Toti-Rigatelli in [6]. All'inizio del maggio 1832, la duchessa di Berry, vedova del figlio di Carlo X, Carlo Ferdinando, assassinato il 14 febbraio 1820 con l'intento di sterminare la dinastia borbonica, era rientrata in Francia. Il figlio Enrico, conte di Chambord, partorito sette mesi dopo la tragica morte del marito e per questo detto *enfant du miracle*, era considerato dall'ala più reazionaria come sovrano legittimo al posto di Luigi Filippo e i repubblicani raccolti nella *Société des amis du peuple* intendevano sfruttare le difficoltà del sovrano per organizzare una insurrezione. Per questo scopo occorreva trovare un'occasione per radunare una folla considerevole ed un motivo per catalizzarne gli umori contro il sovrano. Qualcuno dei convenuti alla riunione della *Société* tenutasi il 7 maggio 1832 osservò che un cadavere eccellente, la cui morte potesse essere utilizzata come pretesto per sollevare la folla, avrebbe facilitato il compito. È a questo punto che Galois si sarebbe proposto come vittima sacrificale: la Francia era l'unico amore che gli restava, terminata la relazione con Stéphanie e perdute le speranze del riconoscimento accademico. Egli seppe convincere le resistenze degli astanti e fu convenuto che Galois si sarebbe lasciato uccidere in un duello. Per essere certo di morire, solo la pistola dello sfidante (L.D.) sarebbe stata carica. Alla *Société* restava il compito di organizzare un depistaggio, incolpando la polizia segreta di Luigi Filippo dell'assassinio di Galois. Egli, dal canto suo, per non scatenare le proteste del fratello, scrisse alcune lettere in cui si mostrava certo della morte imminente, attribuendola però alla fine di una relazione amorosa. Galois, trasportato all'ospedale dopo la ferita riportata nel duello vi morì il giorno successivo ed il 1 giugno furono fissati i funerali. Al momento però dell'inizio della cerimonia funebre si sparse la notizia della morte del generale Jean-Maximilien Lamarque che non solo era stato uno dei più importanti militari che avevano servito sotto Napoleone Bonaparte ma, terminata l'avventura napoleonica, era stato un esponente di spicco dell'opposizione parlamentare ai Borbone: un simbolo di valenza molto più grande del povero Galois. La ragion politica imponeva di ritardare la manifestazione antigovernativa ai funerali di Lamarque dove, era facile prevedere, sarebbe accorsa molta più gente. I funerali del generale, tenutisi il 3 giugno, sono ricordati come la più imponente manifestazione popolare

[1] En 1831, un jeune Français, Évariste Galois, mort l'année suivante, avait annoncé dans un Mémoire présenté à l'Académie des Sciences, que, pour qu'une équation, irréductible de degré premier soit soluble par radicaux, il faut et suffit que deux quelconques des racines étant connue, les autres s'en déduissent rationnellement; mais ce Mémoire parut à peu près inintelligible aux Commissaires chargés de l'examiner.

contro il regime di Luigi Filippo. *La morte di Galois era stata inutile* ([6], p. 132).

La notte del duello, Galois lasciò all'amico August Chevalier una lunga lettera in cui riassunse il contenuto delle sue ricerche e dove chiedeva di far pronunciare ufficialmente matematici famosi come Gauss e Jacobi sull'importanza dei teoremi che aveva dimostrato. Chevalier ed il fratello di Évariste, Alfred, ricopiarono i manoscritti e li inviarono a diversi celebri matematici ma fu solo nel 1843 che Joseph Liouville ne venne in possesso e dedicò il tempo necessario a comprenderne il contenuto per pubblicarli [7] nel 1846 sul *Journal de Mathématiques Pures et Appliquées* da lui diretto, essendosi convinto della loro importanza. Dunque, perché il lavoro di Galois cominciasse anche solo a circolare ufficialmente tra tutti i matematici, passarono più di dieci anni dalla sua morte. Nel presentare il lavoro di Galois, Liouville così si esprimeva a riguardo del suo stile:

La causa di questo fallimento fu uno smodato desiderio di concisione che occorre invece evitare sopratutto nel trattare gli argomenti astratti e misteriosi dell'algebra pura; La chiarezza è in effetti tanto più necessaria se si ha in animo di condurre il lettore più in là delle strade battute, nelle regioni più aride. "Quando si tratta di questioni trascendenti, occorre essere chiari in modo trascendente, diceva Descartes." Troppo spesso Galois ha trascurato questo precetto; e noi comprendiamo come degli illustri geometri abbiano ritenuto conveniente tentare di ricondure sulla retta via un esordiente ricco di talento ma inesperto, con la severità dei loro saggi consigli. Fosse stato, attivo ed ardente, l'autore davanti ai suoi censori, avrebbe potuto approfittare dei loro avvertimenti.[2] ([7], p. 382)

9.2 Opere minori di Galois

In questa sezione svolgiamo una panoramica sui lavori di Galois, escludendo la *Mémoire* che verrà esaminata in dettaglio nella prossima sezione. Galois pubblicò due lavori sugli *Annales des Sciences Mathématiques* editi da Gergonne. Il primo [10] si ricollega al lavoro di Lagrange sulla rappresentazione delle soluzioni di equazioni di secondo grado in frazioni continue *periodiche*. Lagrange (si veda il *Traité* [9]), considerò un numero reale x irrazionale rappresentato da una frazione continua periodica

$$x = p + \cfrac{1}{q + \cfrac{1}{p + \cfrac{1}{q + \cfrac{1}{p + \cfrac{1}{q + \cfrac{1}{p + \cfrac{1}{q + \ldots}}}}}}},$$

[2]Un desir exagéré de concision fut la cause de ce défaut que l'on doit surtout tâcher d'éviter en traitant les matières abstraites et mystérieuses de l'Algèbre pure. La clarté est, en effet, d'autant plus nécessaire, qu'on a dessein d'entraîner le lecteur plus loin des routes battues et dans des contrées plus arides. "Quand il s'agit de questions transcendantes, soyez, disait Descartes, transcendentalement clairs." Galois a trop souvent négligé ce précepte; et nous comprenons que d'illustres géomètres aient jugé convenable d'essayer de ramener au droit chemin, par la sévérité de leurs sages conseils, un débuttant plein de génie mais inexpérimentée. L'auter qu'ils censuraient était devant eux, ardent, actif, il pouvait profiter de leurs avis.

con p e q numeri naturali. Siccome da questo sviluppo segue che

$$x = p + \frac{1}{q + \frac{1}{x}}$$

si vede anche che

$$qx^2 - pqx - p = 0,$$

cioè che x risolve un'equazione di secondo grado a coefficienti razionali. Il risultato importante mostrato da Lagrange è l'inversione di questa osservazione e cioè che le soluzioni irrazionali di un'equazione di secondo grado a coefficienti razionali hanno uno sviluppo in frazione continua periodica. Le frazioni continue periodiche possono presentare o meno un antiperiodo, cioè un certo numero finito di cifre che non seguono la legge periodica che si instaura da un certo punto in poi. Quando l'antiperiodo è assente, la frazione continua era detta da Galois *immediatamente periodica*. Ora il teorema mostrato da Galois afferma che

Se una radice [reale] di un'equazione di grado qualsiasi è una frazione continua immediatamente periodica, allora l'equazione avrà anche un'altra soluzione ancora periodica che si ottiene dividendo l'unità negativa per la stessa frazione continua scritta nell'ordine inverso. ([7], p. 385)

In altre parole, limitandosi per semplicità come Galois ad un periodo composto da quattro cifre a, b, c e d, se

$$x_1 = a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \cfrac{1}{a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \dots}}}}}}}$$

è radice di un fattore quadratico di un'equazione di grado qualsiasi, allora anche

$$x_2 = -\cfrac{1}{d + \cfrac{1}{c + \cfrac{1}{b + \cfrac{1}{a + \cfrac{1}{d + \cfrac{1}{c + \cfrac{1}{b + \cfrac{1}{a \dots}}}}}}}}$$

è radice dello stesso fattore quadratico.

Il secondo lavoro di Galois pubblicato sugli *Annales* è in realtà composto da due brevissime note tra loro scorrelate. Nella seconda, dal titolo *Rayon de courbure des courbes dans l'éspace* egli fornì una interpretazione della curvatura per curve non piane ma è sulla prima parte—*Démonstration d'un théorème d'analyse*—che ora ci soffermeremo. Il teorema "dimostrato" da Galois ma che in realtà non è corretto viene così enunciato ([11], p. 392):

Assegnate due funzioni $F(x)$ ed $f(x)$ si avrà

$$\frac{F(x+h) - F(x)}{f(x+h) - f(x)} = \varphi(k)$$

per ogni valore di x ed h, con $k \in [x, x+h]$ e φ una funzione determinata.[3]

Una prima osservazione è che Galois assume tacitamente la *continuità* delle funzioni F ed f in tutto l'intervallo considerato. La sua dimostrazione erronea consta di pochi passaggi: posto

$$\frac{F(x+h) - F(x)}{f(x+h) - f(x)} = P$$

ne segue $F(x+h) - Pf(x+h) = F(x) - Pf(x)$ per cui, se si esclude il caso particolare in cui $F(x) - Pf(x)$ è costante, questa funzione avrà punti di massimo e di minimo che sono assunti in $[x, x+h]$. Detto $x = k$ uno dei punti in cui si ha un massimo od un minimo, *on aura évidentement* dice Galois,

$$k = \psi(P)$$

per una certa funzione ψ e *quindi* (*donc*) si avrà anche $P = \varphi(k)$ dove φ è un'altra funzione.

La dimostrazione suona un po' frettolosa, soprattutto quando Galois ne deduce un corollario sorprendente:

Da questo di può concludere, come corollario, che la quantità

$$\lim \frac{F(x+h) - F(x)}{h} = \varphi(x),$$

per $h = 0$, ciò che dimostra, a priori, l'esistenza delle funzioni derivate.[4] ([11], p. 393)

Inutile dire che la fama di Galois (il cui nome fu storpiato in Galais sulla rivista) non è legato a questo risultato che piuttosto illustra lo stato di confusione che ancora regnava nel comprendere il rapporto tra continuità e derivabilità di una funzione. D'altra parte, all'inizio del XIX secolo si riteneva come valida la dimostrazione di Ampère del "teorema" che deduceva la derivabilità dalla continuità *salvo* in un numero *finito* di punti. Ciò che sembrava inconcepibile era che una funzione continua potesse *non* essere monotòna in un intervallo di ampiezza sufficientemente piccola: non è un caso che fu grazie allo studio approfondito degli sviluppi in serie di Fourier e del modo di generare funzioni violentemente oscillanti che verranno trovati i primi esempi di funzioni continue

[3] Soient Fx et fx deux fonctions quelconques données; on aura, quels que soient x et h,

$$\frac{F(x+h) - F(x)}{f(x+h) - f(x)} = \varphi(k)$$

φ etant une fonction déterminée, et k une quantité intérmediaire entre x et $x+h$.

[4] *De là on peut conclure, comme corollaire, que la quantité*

$$\lim \frac{F(x+h) - F(x)}{h} = \varphi(x),$$

pour $h = 0$, est nécessairement une fonction de x, ce qui démontre, à priori, l'existence des fonctions dérivées.

in tutto un intervallo ma non derivabili in alcun punto. Il lavoro di Galois, ironia della sorte, non passò inosservato ma venne criticato da un altro matematico dall'ingegno penetrante che, come Galois, sarà apprezzato dopo la morte: il matematico boemo di origini italiane Bernhard Bolzano (1781-1848) che nel suo *Functionenlehre*, pubblicato solo nel 1930, così commentò il lavoro di Galois, riportato integralmente nel §136:

Questa dimostrazione non mi soddisfa. Senza dubbio l'equazione $\frac{F(x+h)-F(x)}{f(x+h)-f(x)} = P$ *richiede non solo che* P *venga considerato come un numero dipendente non solo da* x *e da* h*, ma anche dalla natura delle funzioni espresse attraverso i simboli* F *ed* f*. Ora, è vero che l'espressione* $Fx - P \cdot fx$ *non cambia valore quando* x *diventa* $x+h$*, da cui certamente segue (se si assume la continuità delle funzioni* Fx *ed* fx*) che l'espressione dovrà avere uno o più massimi o minimi tra* x *ed* $x + h$*. Ma non mi è affatto chiaro perché, se uno di questi venga indicato con* K*,* K *deve evidentemente essere una funzione di* P*. Cioè, così come nell'espressione* $Fx - P \cdot fx$ *compare non soltanto* P *ma anche i simboli* F *ed* f*, allo stesso modo potrebbe darsi, ed in effetti è così, che* K *non dipenda soltanto dal valore di* P*, ma anche dalla natura delle funzioni che noi indichiamo con* F *ed* f ([12], pp. 509-510)

Bolzano nel *Functionenelehre* fu il primo a proporre un esempio di funzione continua in un intervallo che non ammette derivata in un sottinsieme denso di questo intervallo.

Passando ai lavori apparsi sul *Bulletin des Sciences Mathématiques*, troviamo una breve nota [13] in cui Galois espone succintamente alcuni risultati ed idee che confluiranno nella *Mémoire*. Osserviamo solo che nel commentare i risultati ottenuti, Galois afferma che

Tutte queste proposizioni sono state ottenute ricorrendo alla teoria delle permutazioni.[5] ([13], p. 396)

Questo lavoro illustra in modo esauriente come Galois avesse già dimostrato o quanto meno intuito i risultati che confluiranno nella versione finale della *Mémoire* un paio d'anni prima di morire.

Sempre nel 1830, comparve un altro lavoro di Galois [14] dedicato alla risoluzione *numerica* delle equazioni algebriche. Il lavoro si ispira ad un metodo di risoluzione proposto da Adrien-Marie Legendre nell'ultimo dei tre *Suppléments* posti come appendice alla seconda edizione dell'*Essai sur la Théorie des Nombres* ([15]), cui anche Cauchy aveva dedicato spazio nella Nota III del primo volume del suo *Cours d'Analyse* del 1821 [16]. Il metodo di Legendre viene modificato soprattutto nella formulazione che, invece di basarsi su argomenti geometrici, è tradotta in termini puramente analitici [17], evitando il ricorso ad alcun tipo di grafico. Nella sostanza, Galois come Legendre riscrive un'equazione algebrica $F(x) = 0$, con F polinomio di grado n, nella forma

$$\varphi(x) = x$$

considerandola cioè come un problema di punto fisso e si pone il problema di trovare le radici reali più vicine ad un numero reale a fissato, una per difetto,

[5] Toutes ces propositions ont été déduites de la théorie des permutations.

l'altra per eccesso. Galois vuole eliminare il ricorso ad un'estrazione di radice n-esima che nel metodo esposto da Legendre occorre fare ad ogni passo. Per questo egli dapprima riscrive l'equazione proposta come

$$F(x) = X(x) - Y(x) = 0$$

dove X ed Y contengono rispettivamente i termini aventi coefficienti positivi e negativi. In seguito egli cerca un numero k tale che la funzione

$$x + \frac{F(x)}{kx^n}$$

sia monotòna crescente nell'intervallo $x > 1$, limitazione che non mina la generalità del metodo dal momento che le radici negative si possono ottenere studiando le radici positive dell'equazione $F(-x) = 0$ mentre quelle eventualmente presenti nell'intervallo $[0, 1]$ si riducono alle radici maggiori di 1 di $F(1/x) = 0$. Usando la scomposizione $F(x) = X(x) - Y(x)$, con calcoli diretti Galois conclude che la condizione sarà soddisfatta a patto che sia

$$1 - \frac{nX - xX'}{kx^{n+1}} + \frac{nY - xY'}{kx^{n+1}} > 0$$

e, siccome sia $nX - xX'$ come $nY - xY'$ sono positive, è sufficiente richiedere che

$$\frac{nX - xX'}{kx^{n+1}} < 1$$

quando $x > 1$, che si può verificare prendendo $k > nX(1) - X'(1)$. Similmente, Galois trova un altro numero h tale che

$$x - \frac{F(x)}{hx^n}$$

sia monotòna crescente sempre in $x > 1$, il che è possibile prendendo $h > nY(1) - Y'(1)$. Con queste scelte dei parametri k ed h, l'equazione $F(x) = 0$ può essere riscritta nella forma

$$x = x + \frac{F(x)}{kx^n} =: \varphi(x) \qquad \text{oppure} \qquad x = x - \frac{F(x)}{hx^n} =: \psi(x)$$

per cui la soluzione è vista come intersezione tra la retta $y = x$ ed una funzione monotòna crescente per $x > 1$. A questo punto si considera la successione di valori a, $\varphi(a)$, $\varphi(\varphi(a))$ (a, $\psi(a)$, $\psi(\psi(a))$) su cui vengono calcolati ambo i termini dell'equazione ricavando una successione di valori che convergono alla radice reale dell'equazione proposta più vicina ad a: per dettagli sul metodo, si veda [17].

L'ultima nota da esaminare è in effetti la più importante, quella che ebbe maggiore attenzione nella seconda metà dell'Ottocento. Si tratta di un lavoro di teoria dei numeri, pubblicato ancora nel 1830 e dedicato allo studio delle congruenze modulo un numero p primo [14], cui Gauss aveva dato un contributo

fondamentale nelle *Disquisitiones Arithmeticae*, pubblicate nel 1801. Galois considera una congruenza del tipo

$$F(x) = 0 \qquad \mod p \tag{9.1}$$

dove $F(x)$ è un polinomio di grado ν i cui coefficienti sono interi in $\mathbf{Z}_p$ con p numero *primo* assegnato. Un polinomio F a coefficienti in $\mathbf{Z}_p$, è irriducibile se *non* esistono altri polinomi φ e ψ e χ a coefficienti in $\mathbf{Z}_p$ tali che

$$F(x) = \varphi(x)\psi(x) + p\chi(x).$$

Ora, se F è irriducibile, una congurenza come (9.1) non ammette soluzione in $\mathbf{Z}_p$ e Galois si pone la domanda se sia possibile introdurre dei *simboli immaginari* (*symboles imaginaires*) per rappresentare le radici di (9.1) che svolgano un ruolo analogo di $\sqrt{-1}$ nell'algebra tradizionale. Un problema simile era stato affrontato pochi anni prima per una classe particolare di congruenze da Carl Gustav Jacob Jacobi (1804-1851) in un breve lavoro del 1827 [19] dove, considerando congruenze del tipo

$$x^{p+1} \equiv 1 \qquad \mod p$$

dove p è un numero primo della forma $6n-1$, egli aveva dimostrato che, oltre alle soluzioni $x = \pm 1$, ve ne erano altre $p-1$ della forma

$$x = a + b\sqrt{-3} \qquad \text{con} \qquad a^2 + 3b^2 \equiv 1 \mod p.$$

Le soluzioni di Jacobi rendono il numero di soluzioni distinte della congruenza pari al grado della conguenza stessa, $p+1$, fornendo un'analogia con il teorema fondamentale dell'algebra. Anche se Galois non sembra essere a conoscenza del lavoro di Jacobi egli nota espressamente che

Il vantaggio principale della nuova teoria appena esposta è di ricondurre le congruenze a soddisfare la proprietà (tanto utile per le equazioni ordinarie) di ammettere tante radici quante sono le unità nell'ordine del loro grado.[6]([18], p. 405)

Indicata dunque con ι una di queste soluzioni *immaginarie* di (9.1), si osserva che ι^ν e tutte le potenze di ι con esponente superiore a ν sono vincolate da (9.1). Si possono però formare quantità del tipo

$$\alpha := a_0 + a_1\iota + a_2\iota^2 + \cdots + a_{\nu-1}\iota^{\nu-1} \tag{9.2}$$

dove tutti i coefficienti a_i appartengono a $\mathbf{Z}_p$. Ora, le quantità distinte di questo tipo che si possono formare sono p^ν ed è possibile mostrare che nel loro insieme esse formano un *campo* necessariamente *finito*, noto oggi come *campo di Galois*. Proprio il fatto di essere in numero finito fa sì che, presa una qualsiasi quantità $\alpha \neq 0$ del tipo (9.2), esisterà un numero intero n tale $\alpha^n \equiv 1 \mod p$. Infatti, calcolando α^2, α^3, ecc., si può utilizzare il fatto che $F(\iota) \equiv 0$ per eliminare tutte

[6]Le principal avantage de la nouvelle théorie que nous venons d'exposer est de ramener les congruences à la propriété (si utile dans les équations ordinaires) d'admettre précisément autant des racines qu'il y a d'unités dans leur degré.

le potenze ι^m con $m \geq \nu$ per cui si torna sempre ad un'espressione del tipo (9.2). Inoltre le n quantità

$$\{1 \equiv \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

con $\alpha \neq 0$, non sono mai equivalenti e si possono incontrare due possibilità: o esse esauriscono la classe di espressioni (9.2), oppure ne esiste un'altra β non compresa tra queste per cui si possono formare nuove quantità

$$\{\beta, \beta\alpha, \beta\alpha^2, ..., \beta\alpha^{n-1}\}$$

non equivalenti tra loro. Se non sono state ancora esaurite le espressioni del tipo (9.2), si itera il procedimento che dovrà necessariamente avere un termine, essendo le $\alpha \neq 0$ in numero di $p^\nu - 1$. In definitiva, si dimostra in questo modo che

$$\alpha^{p^\nu - 1} \equiv 1 \qquad \text{mod } p,$$

generalizzando il classico teorema di Fermat. I campi di Galois saranno trattati da vari matematici nell'Ottocento e tra questi ricordiamo Jean-Alfred Serret che dedicherà agli immaginari di Galois parte delle sue ricerche, confluite nella terza edizione (1866) del suo *Traité d'Algèbre Supérieure* che sarà il testo di riferimento per generazioni di studenti in Francia.

9.3 Struttura della *Mémoire* di Galois

Il lavoro principale contenuto in [7] è la *Mémoire sur les conditions de résolubilité des équations par radicaux* [20] che rappresenta l'ultima versione inviata nel gennaio 1831 all'Accademia delle Scienze e bocciata dai recensori Poisson e Lacroix. La versione presente in [7] ha conservato una breve prefazione che funge anche da riassunto, benché Galois l'avesse poi espunta, forse dopo aver ricevuto il manoscritto non approvato. È commovente un passo in cui egli dice *Supplico i miei giudici almeno di leggere con attenzione queste poche pagine*[7] ([7], p. 417). Come riferito da Lacroix, Galois enuncia subito l'obiettivo del lavoro: trovare una condizione necessaria e sufficiente che deve essere soddisfatta da un'equazione algebrica affinché essa sia risolubile per radicali. Galois premette alcuni principî (*Principes*), quattro lemmi ed otto proposizioni, una delle quali manca del tutto di dimostrazione. Ricordiamo due tappe fondamentali nella storia dell'algebra dell'inizio XIX secolo. Nelle *Disquisitiones Arithmeticae* del 1801 Gauss era riuscito a dimostrare che tutte le equazioni ciclotomiche $x^p - 1 = 0$ sono risolubili per radicali, giustificando quanto era stato affermato da Vandermonde. Nel 1829 Abel pubblicò [21] poi un notevole risultato:

Teorema. Se P è un polinomio dotato di n radici $r_1, \cdots, r_n$ e se esistono funzioni razionali θ_i, con $i = 2, \cdots, n$ tali che

$$r_i = \theta_i(r_1), \quad i = 2, 3. \cdots n$$

[7] Je supplie mes juges de lire du moins avec attention ce peu de pages.

e se inoltre, $\forall i, j = 2, \cdots n$

$$\theta_i\theta_j(r_1) = \theta_j\theta_i(r_1),$$

allora l'equazione $P(x) = 0$ è risolubile per radicali. Abel stava dedicandosi a trovare condizioni necessarie e sufficienti perché un'equazione fosse risolubile per radicali ma non poté portare a termine gli studi perché stroncato nello stesso anno, il 1829, da tubercolosi. Proprio questo è il lavoro che intraprende Galois, portandolo a termine due anni dopo, nel 1831.

I principî posti da Galois alla base della teoria sono, in termini moderni, l'ampliamento di un campo con l'aggiunta di un elemento ed il concetto di gruppo, termine che compare per la prima volta in Galois. La prima definizione riguarda la riducibilità delle equazioni (oggi diremmo: dei polinomi).

Def. *Un'equazione è detta riducibile quando ammette divisori razionali, irriducibile in caso contrario.*[8] ([20], p. 418)

A parte qualche questione di nomenclatura, la definizione è quella che si trova ancor oggi. Galois attribuisce estrema importanza all'aggettivo *razionale*: se nelle equazioni numeriche, la riducibilità significa la scomposizione in fattori a coefficienti numerici e razionali, quando l'equazione è letterale la sua riducibilità consiste nell'avere essa un divisore i cui coefficienti si possono esprimere razionalmente in termini dei coefficienti dell'equazione di partenza. A questo punto Galois inserisce una importante novità:

C'è di più: si potrà convenire di ritenere razionale ogni funzione razionale di un certo numero di quantità determinate, date come note a priori. Per esempio, si potrebbe scegliere una certa radice di un numero intero e ritenere razionale ogni funzione razionale di questa radice.[9] ([20], p. 418)

Galois chiama *aggiunzione* (*adjunction*) questo processo di accrescimento del campo dei coefficienti di un'equazione data con l'aggiunta di un certo elemento. Questa nozione viene fissata *prima* che si parlasse di *campi*, benché sia chiaro che Galois concepisce questo nuovo oggetto come una sorta di estensione del campo $\mathbb{Q}$ dei coefficienti dell'equazione proposta. Galois è anche ben consapevole del fatto che l'aggiunzione di uno o più elementi in un campo ha un effetto cruciale sulla difficoltà della soluzione di una certa equazione:

Per esempio, l'aggiunta di una quantità può rendere riducibile un'equazione che non lo era prima[10] ([20], p. 418).

Arriviamo ora al concetto di gruppo, nome introdotto proprio da Galois. Ancora una volta si parla di gruppi di sostituzioni, cioè in termini attuali, di permutazioni mentre per Galois, come per Cauchy ed altri, le permutazioni

[8] Une équation est dite réductible quand elle admet des diviseurs rationnels; irréductible dans le cas contraire.

[9] Il y a plus: on pourra convenir de regarder comme rationelle toute fonction rationelle d'un certain nombre de quantités déterminées, supposées connues à priori. Par example, on pourra choisir une certaine racine d'un nombre entier, et regarder comme rationelle toute fontion rationnelle de ce radical.

[10] Par example, l'adjonction d'une quantité peut rendre réductible une équation irréductible.

erano gli arrangiamenti di un insieme di n oggetti. La definizione di sostituzione è sostanzialmente ripresa da una memoria di Cauchy del 1815 [22]. Se si spera di trovare in Galois una definizione assiomatica del concetto di gruppo, si resterà delusi. Ecco il passo in cui l'idea di gruppo è introdotta:

Quando vorremo raggruppare le sostituzioni, le faremo discendere tutte da una medesima permutazione.

Siccome si tratta sempre di problemi nei quali la disposizione iniziale delle lettere non influisce per nulla nei gruppi che considereremo, occorrerà avere le stesse sostituzioni, qualunque sia la permutazione da cui si è partiti. Pertanto, se in un gruppo siffatto vi sono le sostituzioni S e T, si è certi di avere anche la sostituzione ST.[11] ([20], p. 419).

L'idea di gruppo e la sua proprietà di chiusura rispetto al prodotto di composizione sono dunque modellate su un esempio preciso, quello delle sostituzioni e dunque si tratta di una formulazione lontana da quella moderna [23]. Nel seguito esporremo le idee di Galois seguendo l'approccio soprattutto di Camille Jordan (1838-1922), autore di un articolo [27] di commento alla teoria di Galois, nonché di un fondamentale *Traité des Substitutions* (1870).

Jordan fornisce all'inizio di [27] la definizione di gruppo:

Un sistema di sostituzioni forma un gruppo, se il prodotto di due sostituzioni qualsiasi appartenenti al sistema, appartiene ancora al sistema. ([27], p. 141).

Rilevante è la definizione di gruppo *transitivo*, già data in sostanza da Ruffini:

Un gruppo di sostituzioni tra le lettere α, β, γ,... è detto transitivo se le sue sostituzioni consentono di portare una qualsiasi di queste lettere nel posto occupato inizialmente da α. ([27], p. 141)

Centrale è la definizione di *trasformazione* di una sostituzione a da parte di un'altra sostituzione b, come la sostituzione[12] bab^{-1}.

Dato allora un gruppo $\{a, a_1, a_2, ...\}$, sottogruppo di un gruppo G, il suo *gruppo trasformato* da $b \in G$ è il *gruppo* formato dagli elementi $\{bab^{-1}, ba_1b^{-1}, ba_2b^{-1}, ...\}$ e se quest'ultimo gruppo coincide con quello di partenza, allora esso è detto commutabile (*permutable*) con b: si tratta della nozione di sottogruppo *normale* in G, che tanta importanza ha nelle conclusioni della *Mémoire*. Infine, Jordan introduce la distinzione tra gruppo G *composto* o *semplice* a seconda che esso contenga o meno un qualche sottogruppo le cui sostituzioni siano commutabili a G. Una distinzione importante introdotta nel *Commentaire* è quella tra gruppo *semplice* e gruppo *composto*:

[11] Quand nous voudrons grouper des substitutions, nous les ferons toutes provenir d'une méme permutation.

Comme il s'agit toujours de questions où la disposition primitive des lettres n'influe en rien dans les groupes que nous considérerons, on devra avoir lee mêmes substitutions, quelle que soit la permutation d'où l'on sera parti. Donc, si dans un pareil groupe on a les substitutions S et T, on est sûr d'avoir la substitution ST

[12] Avverto qui che seguo la convenzione in base al quale nel prodotto ab la sostituzione che agisce per prima è collocata più a destra: Jordan segue la convenzione opposta.

Un gruppo è semplice se non contiene alcun gruppo, eccettuato quello formato dalla sola identità, col quale le sue sostituzioni siano permutabili; in caso contrario il gruppo si dirà composto. ([27], p. 142)

Tornando alla *Mémoire*, Galois passa a discutere quattro lemmi.

Lemma I. *Un'equazione irriducibile non può avere alcuna radice in comune con un'equazione razionale, senza dividerla*[13] ([20], p. 419)

La dimostrazione è appena abbozzata, perché già stata presentata da altri. Per completezza, ne forniamo una in termini più moderni, sostanzialmente equivalente a quella data da Jordan. Si tratta di considerare due polinomi $p(x)$ e $q(x)$ a coefficienti in un campo F a caratteristica nulla: per non allontanarci troppo da Galois, assumiamo $F = \mathbb{Q}$. Sia p irriducibile e supponiamo che α sia una radice comune a p e q che dovrà appartenere ad un campo che include strettamente $\mathbb{Q}$. Se p non divide q, allora l'irriducibilità di p impone che p e q siano relativamente primi in $\mathbb{Q}$. Debbono allora esistere altri due polinomi u e v, sempre a coefficienti in $\mathbb{Q}$, tali che

$$u(x)p(x) + v(x)q(x) = 1.$$

Posto $x = \alpha$ si ha $p(\alpha) = q(\alpha) = 0$ che porta all'assurdo $0 = 1$, dimostrando il teorema. Senza soluzione di continuità si passa al Lemma II:

Lemma II. *Assegnata un'equazione qualsiasi priva di radici coincidenti, le cui radici sono $a, b, c, \ldots$ è sempre possibile formare una funzione V delle radici tale che due qualsiasi dei suoi valori, ottenuti permutando nella funzione le radici in tutti i modi possibili, non siano coincidenti.*[14] ([20], p.419)

Prima di dimostrare il Lemma, osserviamo che l'ipotesi di studiare una equazione a radici distinte non lede affatto la generalità della teoria di Galois. Infatti era ben noto un procedimento dovuto a Jan Hudde (1633-1704) e descritto in una lettera del 1657 che apparve nella edizione latina della *Géométrie* curata da van Schooten [24] grazie al quale era sempre possibile ridursi a questo caso. Precisamente, il risultato di Hudde si può formulare in questi termini [25]: sia a una radice di un polinomio $P \in \mathbb{Q}[x]$[15]. Allora a è una radice multipla di P se e solo se $P'(a) = 0$. Infatti, siccome a è radice di P possiamo scrivere

$$P(x) = (x - a)Q(x)$$

per cui, derivando, si ottiene

$$P'(x) = Q(x) + (x - a)Q'(x)$$

da cui si conclude che P' è divisibile per $(x - a)$ se e solo se Q lo è, cioè se e solo se $x = a$ è radice multipla di $P(x) = 0$.

[13] Une équation irréductible ne peut avoir aucune racine commune avec une équation rationnelle, sans la diviser.

[14] Étant donnée une équation quelconque, qui n'à pas racines égales,, dont les racines sont $a, b, c, \ldots$, on peut toujours former une fonction V des racines, telle qu'aucune des valeurs que l'on obtien en permutant dans cette fonction les racines de toutes manières, ne soient égales.

[15] Con $\mathbb{Q}[x]$ indico l'anello dei polinomi in una variabile, a coefficienti in $\mathbb{Q}$.

Fatta questa precisazione, mostriamo il Lemma II, osservando che Galois si limita a dire

Per esempio, basterà prendere

$$V = Aa + Bb + Cc + \cdots$$

A, B, C essendo numeri interi scelti opportunamente.[16] ([20], p. 419)

Dimostriamo questo asserto di Galois seguendo ancora Jordan [27]. Osserviamo che una dimostrazione di taglio diverso fu data qualche anno dopo da Georg Cantor in una breve nota del 1872 [26]. Per coerenza con quanto fatto altrove indicheremo con $r_1, r_2, \cdots, r_n$ le radici dell'equazione assegnata. Consideriamo una funzione del tipo suggerito da Galois

$$V = \sum_{i=1}^{n} m_i r_i$$

e consideriamo due permutazioni distinte σ e τ. Indichiamo con V_σ e V_τ i valori assunti da V quando sugli argomenti agiscono queste permutazioni, per cui

$$V_\sigma = \sum_{i=1}^{n} m_i r_{\sigma(i)} \qquad V_\tau = \sum_{i=1}^{n} m_i r_{\tau(i)} :$$

per verificare le richieste del Lemma occorre *escludere* tutti e soli quei valori di m_i che soddisfano alle equazioni

$$\sum_{i=1}^{n} m_i [r_{\sigma(i)} - r_{\tau(i)}] = 0 \tag{9.3}$$

qualunque sia la coppia di permutazioni σ e τ scelta. Come equazione nelle m_i, la (9.3) rappresenta l'equazione di un iperpiano e, poiché abbiamo n radici *distinte* dell'equazione proposta, è sufficiente evitare di prendere gli m_i che appartengono agli $\frac{1}{2}n!(n! - 1)$ iperpiani descritti da (9.3). La funzione V gioca un ruolo essenziale già a partire dal Lemma III che ne stabilisce la proprietà saliente:

Lemma III. *Data una funzione V come indicato nell'articolo precedente, essa godrà della proprietà che tutte le radici dell'equazione proposta si esprimeranno razionalmente in termini della V.*[17] ([20], p.420)

La dimostrazione di Galois è solo una traccia e proprio su questo punto Poisson, recensendo la memoria, annotò a margine del manoscritto come la dimostrazione

[16] Par example, on peut prendre

$$V = Aa + Bb + Cc + \cdots$$

A, B, C étant des nombres entiers convenablement choisis.

[17] La fonction V étant choisie comme il est indiqué dans l'article précedent, elle jouira de cette propriété, que toutes les racines de l'équation proposée s'exprimeront rationnellement en fonction de V.

fosse insufficiente benché la validità del teorema seguisse dalle *Réflexions* di Lagrange, §100, dove questi aveva studiato il numero di valori distinti assunti da funzioni delle radici di un'equazione algebrica, tra cui cadevano quelle del tipo proposte da Galois ([8], pp.374-379): questo dimostra che Poisson fece uno sforzo per comprendere il lavoro di Galois. Nella versione finale [20] della memoria, Galois annotò come questo lemma sia citato, senza dimostrazione, da Abel nella sua memoria postuma sulle funzioni ellittiche.

Per la dimostrazione del Lemma III seguo ancora il *Commentaire* di Jordan che viene anche riprodotto nella sostanza in [25].

Sia $V := V(r_1, r_2, \cdots, r_n)$ il valore della funzione V trovata nel Lemma II e calcolata sulle radici $\{r_1, r_2, \cdots, r_n\}$, in questo ordine, dell'equazione da risolvere

$$P(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots a_n = 0. \tag{9.4}$$

Formiamo il polinomio in n variabili $x_1, \cdots, x_n$

$$g(x_1, x_2, \cdots, x_n) := \prod_{\sigma} [V - V(x_1, \sigma(x_2), \sigma(x_3) \cdots, \sigma(x_n))] \tag{9.5}$$

dove il prodotto è fatto sulle permutazioni di $\{x_1, x_2, \cdots, x_n\}$ che lasciano x_1 inalterata. Per costruzione g è *simmetrica* nelle variabili $\{x_2, \cdots, x_n\}$ e dunque dipende solamente dai polinomi elementari simmetrici in $\{x_2, \cdots, x_n\}$, cioè a dire da

$$\begin{aligned} \overline{s}_1 &= x_2 + x_3 + \cdots + x_n \\ \overline{s}_2 &= x_2 x_3 + x_2 x_4 + \cdots \\ &\cdots\cdots \\ \overline{s}_{n-1} &= x_2 x_3 \cdots x_n. \end{aligned}$$

Ora, è possibile mostrare che le funzioni $\overline{s}_k$ si possono esprimere in termini di x_1 e dei polinomi simmetrici elementari s_k nelle variabili $\{x_1, x_2, \cdots, x_n\}$. Ad esempio,

$$\overline{s}_1 = s_1 - x_1 \quad \overline{s}_2 = s_2 - x_1 s_1 + x_1^2 ..., \text{ecc.}$$

dunque possiamo scrivere

$$g(x_1, x_2 \cdots x_n) = h(x_1, s_1, s_2, \cdots, s_{n-1}).$$

Quando al posto delle variabili $\{x_1, x_2, \cdots, x_n\}$ inseriamo gli n valori *distinti* $\{r_1, r_2, \cdots, r_n\}$ delle radici di $P(x) = 0$ avremo

$$g(r_1, r_2 \cdots, r_n) = h(r_1, a_1, a_2, \cdots, a_{n-1})$$

visto che i polinomi simmetrici elementari sono in questo caso i coefficienti di (9.4). D'altra parte, poiché l'identità compare tra le trasformazioni σ in (9.5) e visto il significato di V, possiamo concludere che $h(r_1, a_1, a_2, \cdots, a_{n-1}) = 0$. Non solo: siccome V è stata costruita in modo che non possa assumere due valori coincidenti quando si permutano tra loro le radici di (9.4), possiamo anche concludere che

$$g(r_i, r_1, r_2 \cdots r_{i-1}, r_{i+1}, \cdots r_n) \neq 0 \quad i \neq 1$$

dal momento che le permutazioni $(r_1, r_2 \cdots r_n) \mapsto (r_i, r_1, r_2 \cdots r_{i-1}, r_{i+1}, \cdots r_n)$ sono distinte dall'identità e, per definizione di V,

$$V(r_i, r_1, r_2 \cdots r_{i-1}, r_{i+1}, \cdots r_n) \neq V.$$

Dunque il polinomio $h(x, a_1, \cdots, a_{n-1}) \in \mathbb{Q}(V)[x]$[18] ha i coefficienti nel campo $\mathbb{Q}[V]$ ottenuto aggiungendo V al campo $\mathbb{Q}$ dei coefficienti di (9.4) ed ha in comune con $P(x)$ solo la radice $x = r_1$. Poiché ogni radice di $P(x)$ è semplice, il massimo comun divisore tra h e P è $x - r_1$ che appartiene anch'esso a $\mathbb{Q}(V)[x]$ dal momento che le operazioni coinvolte nella formazione del massimo comun divisore di due polinomi non fanno uscire dal campo $\mathbb{Q}(V)[x]$. Pertanto $r_1 \in \mathbb{Q}[V]$ e, ripetendo l'argomento per le altre radici di (9.4), si conclude che esistono n funzioni razionali $f_1, \cdots f_n$ tali che

$$r_i = f_i(V). \tag{9.6}$$

Il Lemma IV è la chiave per introdurre il gruppo di Galois dell'equazione (9.4) e consente di provare una proprietà di chiusura delle radici di (9.4) quando vengono operate delle opportune sostituzioni delle $\{r_i\}$.

Lemma IV. *Supponiamo di aver formato l'equazione in V e di aver preso uno dei suoi fattori irriducibili, in modo che V sia radice di un'equazione irriducibile. Siano V, V', V'',... le radici di quest'equazione irriducibile. Se $a = f(V)$ è una delle radici dell'equazione proposta, $f(V')$ sarà ancora una radice della proposta.*[19] ([20], pp. 420–421)

Quella che Galois chiama *equazione in V* è l'equazione in una variabile ausiliaria t che ammette come radici V e tutti i valori ottenuti da V permutando tra loro le r_i in tutti i modi possibili:

$$(t - V)(t - \sigma_2(V))(t - \sigma_3(V)) \cdots (t - \sigma_{n!}(V)) = \prod_{i=1}^{n!}(t - \sigma_i(V)) \tag{9.7}$$

dove il prodotto è fatto su tutte le permutazioni σ_i delle n radici $r_1, \cdots r_n$ di (9.4), $V_i := V(\sigma_i(x_1), \sigma_i(x_2), ..., \sigma_i(x_n))$ e $\sigma_1(V) = V$. Ora, l'equazione (9.7) è simmetrica nelle V_i e quindi, per definizione di $V \equiv V_1$, è simmetrica nei coefficienti di (9.4). Consideriamo il fattore irriducibile su $\mathbb{Q}$ della (9.7) cui appartiene V ed indichiamo con $V_2, ..., V_m$ le altre radici di questo fattore. Per procedere nella dimostrazione occorre ricordare un risultato che riguarda le funzioni razionali, cioè i quozienti di polinomi, avvertendo che tali risultati non furono utilizzati da esplicitamente Galois. Dimostro questo risultato ausiliario servendomi dell'esposizione della teoria di Galois fatta alla fine del XIX secolo dal matematico statunitense James Pierpont [28].

[18] Con $\mathbb{Q}(V)[x]$ indichiamo l'anello dei polinomi in x a coefficienti nel campo $F[V]$.

[19] Supposons que l'on ait formé l'équation en V, et que l'on ait pris l'un des ses facteurs irréductibles, en sorte que V soit racine d'une équation irreductible. Soient V, V', V''... les racines de cette équation irréductible. Si $a = f(V)$ est une des racines de la proposée, $f(V')$ de même sera une racine de la proposée.

Risultato ausiliario. *Assegnata l'equazione* $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$ *con coefficienti nel campo* F *e dette* r_1, r_2,...,r_n *le sue radici, ogni funzione razionale* $\psi(r_1)$ *di una di queste radici si può scrivere come*

$$\psi(r_1) = \beta_0 + \beta_1 r_1 + \cdots + \beta_{n-1} r_1^{n-1}$$

cioè come una funzione razionale intera (polinomio) di r_1.

Infatti, siccome r_1 risolve un'equazione di grado n, le sue potenze ad esponente superiore ad $n-1$ si esprimono come funzioni razionali intere delle potenze fino all'esponente $n-1$ compreso e dunque

$$\psi(r_1) = \frac{g(r_1)}{h(r_1)} = \frac{\alpha_0 + \alpha_1 r_1 + \cdots + \alpha_{n-1} r_1^{n-1}}{\beta_0 + \beta_1 r_1 + \cdots + \beta_{n-1} r_1^{n-1}}.$$

Se moltiplichiamo numeratore e denominatore di quest'espressione per $h(r_2) \cdot h(r_3) \cdots h(r_n)$, a denominatore otteniamo una funzione simmetrica delle r_i che dunque può esprimersi in termini dei coefficienti di $p(x)$ e appartiene per questo ad F. Il numeratore è invece simmetrico nelle radici r_2, r_3,...,r_n e quindi si può esprimere come polinomio di r_1 e dei coefficienti di $p(x)$, dimostrando il lemma. Passiamo a dimostrare il Lemma IV della *Mémoire*.

Dim. Da (9.6) sappiamo che $P(r_i) = P(f_i(V_1)) = 0$ $(i = 1, ..., n)$ e quindi la funzione razionale intera (cioè il polinomio) $P \circ f_i$ è annullata dalla radice V_1 di un polinomio irriducibile su F. Quindi, deve essere anche $P(f_i(V_j)) = 0$, per $j = 2, ..., m$ e questo significa che $f_i(V_j)$ è ancora una radice dell'equazione (9.4). Ora, possiamo anche escludere che $f_i(V_j) = f_k(V_j)$ quando $i \neq k$. Infatti, se così fosse avremmo

$$(f_i - f_k)(V_j) = 0$$

e dunque V_j annullerebbe il fattore irriducibile di (9.7) contenente V_1 ed il polinomio $f_i - f_k$. Ripetendo lo stesso argomento appena incontrato si otterrebbe anche che $(f_i - f_k)(V_1) = 0$ e dunque che $f_i(V_1) = f_k(V_1)$, cioè che $r_i = r_k$ per qualche coppia di indici i e k, contraddicendo il fatto che (9.4) debba avere tutte le radici distinte.

L'importanza di questo teorema sta nel fatto che le applicazioni

$$\sigma_j : r_i \mapsto f_i(V_j)$$

sono, $\forall j = 1, ..., m$, permutazioni delle radici della proposta. L'insieme di queste permutazioni forma un gruppo che (oggi) è detto gruppo di Galois associato all'equazione (9.4). A questo proposito vi sono due domande cui occorrerebbe rispondere: dapprima se il gruppo di Galois di un'equazione dipende dalla scelta di V e che il gruppo di Galois sia effettivamente un gruppo. Galois non si pone il primo problema e sembra dare per scontata la natura gruppale del sottoinsieme $\{\sigma_i\}$. Conformandoci ad un uso ormai radicato, indicherò con $\mathrm{Gal}(P/\mathbb{Q})$ il gruppo di Galois di P sul campo $\mathbb{Q}$. Terminati i lemmi, Galois passa a dimostrare le proposizioni principali della sua teoria. Osserviamo ancora che le permutazioni di $\mathrm{Gal}(P/\mathbb{Q})$ sono quelle che mandano V_1 in una qualunque delle

V_i, con $i = 1, ..., m$. Con la Proposizione I Galois caratterizza le permutazioni che appartengono a Gal$(P/\mathbb{Q})$.

Proposizione I. *Sia assegnata un'equazione con n radici $a, b, c, ...$ Esiste un gruppo di permutazioni delle lettere $a, b, c, ...$ che gode della seguente proprietà: 1°. che ogni funzione delle radici, invariante per le sostituzioni del gruppo, sia nota razionalmente;*

2° *Viceversa, che ogni funzione delle radici determinabile razionalmente, sia invariante sotto l'azione delle sostituzioni*[20] ([20], p. 421)

Siccome $V = V_1$ è funzione razionale delle $r_1, ..., r_n$ che a loro volta sono funzioni razionali di V, per il risultato ausiliario appena mostrato, ogni funzione razionale $\varphi(r_1, r_2, ..., r_n)$ si può scrivere come

$$\varphi(r_1, r_2, ..., r_n) = b_0 + b_1 V_1 + b_2 V_1^2 + \cdots + b_{m-1} V_1^{m-1} =: \psi(V_1) \tag{9.8}$$

dove m è il grado del fattore irriducibile contenente $V = V_1$. Mostriamo ora la prima implicazione contenuta nella Proposizione I. Applicando a (9.8) una delle sostituzioni $\sigma_1 = \text{id}$, σ_2,...,σ_m di Gal(P/F) otteniamo, per l'invarianza di φ

$$\varphi(r_1, r_2, ..., r_n) = \psi(V_1) = \psi(V_2) = \cdots = \psi(V_m)$$

per cui $\varphi(r_1, r_2, ..., r_n) = \frac{1}{m}[\psi(V_1) + \cdots + \psi(V_m)]$ e la funzione in parentesi è simmetrica nelle radici di un fattore irriducibile di un polinomio a coefficienti in $\mathbb{Q}$. Quindi i coefficienti di questo fattore irriducibile stanno in $\mathbb{Q}$ e ciò dimostra l'implicazione. Per l'implicazione opposta, si suppone che una funzione $\varphi(r_1, r_2, ..., r_n)$ sia razionalmente nota, cioè appartenga ad $\mathbb{Q}$, quale che sia l'ordine in cui compaiono i suoi argomenti. Allora l'equazione

$$b_{m-1} t^{m-1} + b_{m-2} t^{m-2} + \cdots + b_1 t + b_0 - \varphi = 0 \tag{9.9}$$

ha coefficienti in $\mathbb{Q}$ ed ammette come radice $t = V_1$, grazie a (9.8): siccome V_1 è anche radice di un'equazione irriducibile su $\mathbb{Q}$, allora (9.9) ammette anche tutte le V_2,...,V_m come sue radici per cui

$$\varphi = \psi(V_1) = \psi(V_2) = \cdots = \psi(V_m)$$

che mostra l'invarianza di φ.

La natura gruppale di Gal$(P/\mathbb{Q})$ discende dalle proprietà caratteristiche dell'insieme di sostituzioni $\{\sigma_1, \sigma_2, ...\sigma_m\}$. Infatti, siccome il fattore irriducibile $G(t)$ di cui V_1 è radice si può scrivere come

$$G(t) = (t - V_1)(t - V_{\sigma_2}) \cdots (t - V_{\sigma_m})$$

[20] Soit une équation donnée, dont a, b, c, ..., sont les m racines. Il y aura toujours un groupe de permutations des lettres a, b, c, ..., qui jouira de la propriété suivante: 1°. Que toute fonction des racines, invariable par les substitutions de ce groupe, soit rationnellement connue;

2° Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions.

ed ha coefficienti in $\mathbb{Q}$, allora esso deve restare invariato sotto l'azione delle sostituzioni σ_i per cui

$$G(t) = (t - V_{\sigma_i})(t - V_{\sigma_2\sigma_i}) \cdots (t - V_{\sigma_m\sigma_i})$$

che mostra come le $V_{\sigma_k\sigma_i}$ siano radici di $G(t)$: siccome $V_{\sigma_j} \neq V_{\sigma_k}$ quando $j \neq k$, concludiamo che le sostituzioni σ_i,...,$\sigma_j\sigma_i$,...,$\sigma_m\sigma_i$ non sono altro che quelle di partenza, al più disposte in ordine diverso.

L'oggetto da studiare dunque *non* è l'intero gruppo delle sostituzioni anche perché le funzioni delle radici di (9.4) che sono invarianti rispetto a tale gruppo, essendo funzioni simmetriche *non* consentono di discriminare tra una radice ed un'altra: ad esempio, conoscere la somma ed il prodotto (funzioni simmetriche) di due numeri x_1 ed x_2 non esime dal risolvere un'equazione di secondo grado completa per determinare i due numeri individualmente. Il gruppo $\mathrm{Gal}(P/\mathbb{Q})$ isola alcune permutazioni che lasciano invariate delle particolari relazioni tra le radici e l'obiettivo della teoria di Galois è proprio quello di cercare condizioni su questa struttura gruppale, verificate le quali si può essere certi della risolubilità di un'equazione algebrica. Dimostrata la Proposizione I Jordan stabilisce un corollario importante ([27], p. 147)

Corollario I. *Se due funzioni φ_1 e ψ_1 delle radici dell'equazione proposta sono numericamente uguali, la stessa uguaglianza sussisterà anche tra le funzioni φ_a e ψ_a ottenute effettuando su ciascuna di esse una qualsiasi delle sostituzioni di G*[21]

Infatti, poiché $\varphi_1 - \psi_1 = 0$ è nota razionalmente ($0 \in \mathbb{Q}$), per definizione delle sostituzioni $a \in G$, questa relazione resta valida per $\varphi_a - \psi_a = 0$.

Jordan fa seguire due teoremi che traspongono proprietà di un'equazione $F(x) = 0$ in proprietà del suo gruppo G.

Teorema II. *Ogni equazione irriducibile $F(x) = 0$ ha il suo gruppo transitivo, e viceversa.*

Infatti, se G non è transitivo, isolata una radice x_1 di $F(x) = 0$ si avrebbe che solo le radici $x_1, x_2, ..., x_m$ potrebbero essere scambiate con x_1 da una sostituzione di G, con $m < n = \deg F$. Le sostituzioni di G non possono che scambiare tra loro le radici dell'insieme $x_1, x_2, ..., x_m$: infatti, se una sostituzione a rimpiazza x_m con x_ϱ, poiché esiste una sostituzione b che manda $x_1 \mapsto x_m$, la sostituzione ab sostituisce x_1 con x_ϱ che dunque deve appartenere all'insieme $\{x_1, x_2, ..., x_m\}$. Grazie a questa osservazione Jordan conclude che le sostituzioni di G non possono modificare le funzioni simmetriche di $x_1, x_2, ..., x_m$ che pertanto sono razionali. Dunque l'equazione

$$(x - x_1)(x - x_2) \cdots (x - x_m) \tag{9.10}$$

è divisore *razionale* di $F(x)$ che è riducibile su $\mathbb{Q}$. Al contrario, se G è transitivo $F(x)$ non può ammettere alcun divisore razionale come (9.10) perché, se x_{m+1} è una radice di $F(x) = 0$ distinta da quelle di (9.10), dovendo esistere

[21] G indica il gruppo dell'equazione sul campo dei coefficienti dell'equazione proposta.

una trasformazione di G che manda x_1 in x_{m+1} per la ipotesi di transitività del gruppo, (9.10) si trasformerà sotto l'azione della stessa sostituzione in un prodotto distinto e pertanto, non essendo invariante sotto l'azione del gruppo G, è irrazionale.

Il teorema successivo dimostrato da Jordan ([27], pp. 147-148) fornisce la condizione sotto la quale il gruppo di un'equazione irriducibile ha ordine pari al grado dell'equazione stessa:

Teorema III. *L'ordine del gruppo di un'equazione irriducibile di grado ν, le cui radici sono funzioni razionali di una radice particolare x_1, è pari a ν.*

Infatti, la funzione $V_1(x_1, ..., x_\nu)$ che gode delle proprietà dei lemmi II e III mostrati da Galois è in effetti esprimibile come funzione della sola radice x_1: $V_1 = f(x_1)$. Essa è dunque radice dell'equazione di grado ν

$$[t - f(x_1)] \cdots [t - f(x_\nu)] = 0 \tag{9.11}$$

i cui coefficienti sono razionali, visto che sono simmetrici nelle quantità $x_1, ..., x_\nu$. Poiché l'ordine del gruppo G dell'equazione di partenza è il grado dell'equazione irriducibile di cui V_1 è radice, esso non può superare ν, in virtù del Lemma 1. Essendo però il gruppo G transitivo, esso deve contenere almeno ν sostituzioni: l'identità, e le $\nu - 1$ che debbono sostituire x_1 con una delle altre radici x_2,..., x_ν. Dunque G è composto esattamente da ν sostituzioni.

Fatte queste precisazioni, Jordan non espone le proposizioni II e III della *Mémoire* ma la Proposizione IV che Galois aveva enunciato in questi termini:

Proposizione IV. *Se si aggiunge ad un'equazione il valore numerico di una certa funzione delle sue radici, il gruppo dell'equazione si ridurrà in modo tale da non avere altre permutazioni se si eccettuano quelle che lasciano invariante la funzione.*[22] ([20], p.425)

Jordan rende la Proposizione IV in questo modo:

Teorema IV. *Sia G il gruppo di un'equazione $F(x) = 0$, φ_1 una funzione razionale qualsiasi delle sue radici: I. Le sostituzioni di G che non modificano il valore numerico di φ_1 formano un gruppo H_1: II L'aggiunta (adjonction) del valore di φ_1 ridurrà il gruppo dell'equazione precisamente ad H_1.*

La riduzione del gruppo può non esserci affatto: se φ_1 è una funzione che assume un *valore* razionale, il campo dei coefficienti non viene esteso affatto ed il gruppo non si riduce.
Per la dimostrazione del Teorema IV, Jordan considera due sostituzioni a ed a_1 di G che non alterino il valore di φ_1:

$$\varphi_a = \varphi_1 \qquad \varphi_{a_1} = \varphi_1$$

per cui, applicando $a_1 \in G$ alla prima relazione, grazie al Corollario I si ha anche

$$\varphi_{a_1 a} = \varphi_{a_1} = \varphi_1$$

[22] *Si l'on adjont à une équation la valeur numérique d'une certaine fonction des ses racines, le groupe de l'équation s'abaissera de manière à n'avoir plus d'autres que celles par lesquelles cette fonction est invariable.*

che mostra la chiusura delle sostituzioni che non alterano φ_1: indichiamo con H_1 il sottogruppo di G che lascia inalterata φ_1. Passando alla seconda parte del teorema, supponiamo di aver esteso il campo aggiungendo il valore di φ_1 a $\mathbb{Q}$. In questo modo, il valore di φ_1 diventa razionalmente *noto* in $\mathbb{Q}' := \mathbb{Q}[\varphi_1]$ e quindi il nuovo gruppo G' dell'equazione, riferito a $\mathbb{Q}'$, deve essere formato da sostituzioni che non alterano il valore di φ_1 sicché $G' \subseteq H_1$. Viceversa, se $a \in H_1$ e ψ_1 è una funzione delle radici r_1,..., r_n dell'equazione proposta che sia esprimibile razionalmente in $\mathbb{Q}'$, possiamo porre in evidenza la dipendenza razionale da φ_1 scrivendo $\psi_1 = \chi(\varphi_1)$, dove χ indica una funzione razionale. Poiché dunque $\psi_1 - \chi(\varphi_1) = 0$ è razionale, essendo nulla, quest'ultima relazione permane vera se si applica una qualunque sostituzione di G, in particolare vale per $a \in H_1$ e dunque concludiamo che

$$\psi_a - \chi(\varphi_a) = 0$$

e dunque, essendo $\varphi_a = \varphi_1$, si ottiene anche che $\psi_1 = \psi_a$, per cui a appartiene anche al gruppo ridotto G': $H_1 \subseteq G'$, che consente di ottenere $G' = H_1$, come occorreva dimostrare.

Il processo di riduzione si può continuare, immaginando di aggiungere a $\mathbb{Q}$ non solo il valore di φ_1 ma anche quello di altre funzioni φ_1', φ_1'',... razionali delle radici che ridurranno il gruppo dell'equazione al sottogruppo di G contenente le sostituzioni che non alterano il valore numerico di *tutte* le funzioni introdotte ([27], p. 149). Un'altra conseguenza del teorema IV posta in luce da Jordan è che, se φ_1 e ψ_1 sono due funzioni delle radici dell'equazione proposta che sono invarianti sotto l'azione dello stesso gruppo di sostituzioni in G, allora esse si esprimono razionalmente una tramite l'altra ([27], p. 149). Per chiarire come si modifichi la struttura gruppale di G dopo la sua riduzione ad H_1, Jordan dimostra il seguente

Teorema V. *Ferme restando le ipotesi come nel teorema precedente*[23]*, siano* a_0*,* a_1*,* a_2*,... le sostituzioni di* H_1*:*

$$a_0, a_1, a_2, ...; ba_0, ba_1, ba_2, ...; ca_0, ca_1, ca_2, ...; ...$$

quelle di G*: l'equazione*

$$(Y - \varphi_1)(Y - \varphi_b)(Y - \varphi_c) \cdots = 0 \tag{9.12}$$

il cui grado è pari al rapporto tra l'ordine di G *e quello di* H_1*, avrà coefficienti razionali e sarà irriducibile.* ([27], p. 149)

Prima di esaminare la dimostrazione, osserviamo che l'irriducibilità di (9.12) è riferita a $\mathbb{Q}$. Inoltre, con a_0 Jordan indica l'identità di G. Jordan, che svolge l'abbozzo di dimostrazione contenuto nella *Mémoire* di Galois, sta suddividendo le sostituzioni di G in un *quadro*

$$\begin{array}{ccccc} a_0 & a_1 & a_2 & \cdots & a_\nu \\ ba_0 & ba_1 & ba_2 & \cdots & ba_\nu \\ ca_0 & ca_1 & ca_2 & \cdots & ca_\nu \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array} \tag{9.13}$$

[23] Il teorema IV.

in cui la prima riga ospita le sostituzioni del *sottogruppo* H_1, con $a_i \neq a_j$ se $i \neq j$; la seconda riga ospita le sostituzioni ottenute applicando $b = ba_0 \subseteq H_1$ a tutte le sostituzioni di H_1 ottenendo permutazioni che non soltanto sono distinte tra loro ma sono anche distinte da tutte le sostituzioni di H_1: se così non fosse ma si avesse $ba_j = a_k$ per una coppia di indici j, k, allora avrebbe $b = a_k a_j^{-1} \in H_1$, contrariamente all'ipotesi. Similmente, se c non appartiene a nessuna delle sostituzioni precedenti, tutte le sostituzioni del tipo ca_j sono distinte tra loro e da tutte quelle contenute nelle righe precedenti. Procedendo, è chiaro che si esauriranno le sostituzioni di G in un numero di righe pari al rapporto tra il numero di elementi di G e quello degli elementi di H_1, cioè pari all'*indice* di H_1 in G: in effetti questo quadro è del tutto analogo a quello che si utilizza ancora oggi per dimostrare il teorema di Lagrange sull'ordine dei sottogruppi di un gruppo finito.

Per la dimostrazione del Teorema V, Jordan osserva che una sostituzione σ qualsiasi appartenente a G dovrà anche ricadere in una delle righe del quadro (9.13) e lo stesso deve accadere per le sostituzioni σb, σc,... .Ora, se b e c stanno su righe diverse dello schema (9.13), lo stesso deve succedere per σb e σc perché, se fosse $\sigma b = da_i$ e $\sigma c = da_j$, allora avremmo

$$\sigma^{-1} d = b a_i^{-1} = c a_j^{-1}$$

da cui si potrebbe concludere che $c = b a_i^{-1} a_j$, contrariamente all'ipotesi fatta. Osserviamo anche che la sostituzione $\sigma = ba_i$ manda φ_1 in φ_{ba_i}. Poiché la relazione $\varphi_1 = \varphi_{a_i}$ deve restare invariata sotto l'azione di una sostituzione di G come b, si ha $\varphi_\sigma = \varphi_b$ cosicché, in definitiva, σ trasforma φ_1 in φ_b. Allo stesso modo si dimostra che, se σb è della forma ca_j, allora σ trasforma φ_b in φ_c e, proseguendo, si vede che l'effetto di una qualsiasi sostituzione di G è quello di *permutare* tra loro i valori di φ_1, φ_b, φ_c,... . Osserviamo ora che i coefficienti dell'equazione (9.12) sono funzioni simmetriche di φ_1, φ_b, φ_c, ... e dunque una *qualunque* sostituzione $\sigma \in G$ li deve lasciare inalterati, per quanto appena dimostrato. Per la proprietà caratteristica delle sostituzioni di G (Proposizione I), i coefficienti di (9.12) sono razionali. Quanto all'irriducibilità di (9.12) osserviamo che, se ciò non fosse vero, allora potremmo isolare un fattore razionale come $(Y - \varphi_1)(Y - \varphi_b)$ i cui coefficienti, essendo razionali, dovrebbero restare inalterati sotto l'azione di una sostituzione $c \in G$. Poiché una tale sostituzione trasforma

$$(Y - \varphi_1)(Y - \varphi_b) \mapsto (Y - \varphi_c)(Y - \varphi_{cb})$$

occorrerebbe dunque che i fattori di questi due prodotti coincidessero, a meno dell'ordine. Ora, se fosse $\varphi_b = \varphi_c$ si avrebbe anche $\varphi_{b^{-1}c} = \varphi_1$ che mostrerebbe come $b^{-1}c \in H_1$ e dunque $c = ba_j$, contrariamente all'ipotesi. Che il grado dell'equazione sia quello indicato nel teorema segue dalla formazione dello schema (9.13).

Notiamo che, a parte la prima riga di (9.13) che, per definizione, è un sottogruppo di G, nessuna delle altre righe ha struttura gruppale, mancando ad esempio in ciascuna di esse, l'identità. È però possibile ottenere una ripartizione

di G in sottogruppi, lasciandosi guidare dalle proprietà di invarianza della funzione φ_1. Jordan osserva ([27], §14, p. 150) che le sostituzioni che non alterano φ_b sono quelle del tipo ba_jb^{-1}, con $a_j \in H_1$; quelle che non alterano φ_c sono del tipo ca_jc^{-1}, con $a_j \in H_1$, e così via. Infatti, se $\sigma \in G$ è tale che $\varphi_{\sigma b} = \varphi_b$, allora applicando $b^{-1} \in G$ deve essere anche $\varphi_{b^{-1}\sigma b} = \varphi_1$ per cui $b^{-1}\sigma b = a_j$ e quindi $\sigma = ba_jb^{-1}$. In modo analogo si ottiene l'implicazione opposta: se $\sigma = ba_jb^{-1}$ allora σ non altera il valore di φ_b. Con questa osservazione, Jordan passa al Teorema VI che precisa la riduzione di G quando si aggiungono *tutti* i valori φ_1, φ_b, φ_c che φ_1 può assumere sotto l'azione delle sostituzioni di G.

Teorema VI. *Ferme restando le ipotesi dei teoremi precedenti*[24]*, l'aggiunta simultanea dei valori di φ_1, φ_b, φ_c, ..., ridurrà il gruppo dell'equazione proposta ad I, essendo I il gruppo più generale, tra quelli contenuti in H_1, commutabili con le sostituzioni di G.* ([27], p. 150)

In altri termini, I è il sottogruppo normale di G, massimale tra quelli inclusi in H_1.

Lo schema della dimostrazione ricalca quelli già visti nei teoremi precedenti. Anzitutto si osserva che il gruppo ridotto I dell'equazione di partenza, a seguito dell'aggiunta di φ_1, φ_b, φ_c, ... deve essere formato da sostituzioni che stanno nel gruppo

$$J := H_1 \cap H_b \cap H_c \cdots$$

dove

$$H_b = bH_1b^{-1}, \qquad H_c = cH_1c^{-1}, ...$$

visto che le sostituzioni di I debbono lasciare inalterati *tutti* i valori assunti dalla funzione $\varphi_1(r_1, r_2, ..., r_n)$ sotto l'azione delle sostituzioni di G. Ora, presa $s \in J$ e $\sigma \in G$, la sostituzione $\sigma s\sigma^{-1}$ deve stare in

$$\sigma H_1\sigma^{-1} \cap \sigma H_b\sigma^{-1} \cap \sigma H_c\sigma^{-1} \cdots .$$

Poiché però $\sigma b = da_j$, per qualche sostituzione d e qualche $a_j \in H_1$, abbiamo che l'elemento generico di $\sigma H_b\sigma^{-1}$ è del tipo

$$\sigma ba_kb^{-1}\sigma^{-1} = da_ja_ka_j^{-1}d^{-1} \in H_d :$$

pertanto possiamo concludere che $\sigma s\sigma^{-1}$ appartiene ancora a J e quindi $J \subseteq I$. Viceversa, poiché $I \subseteq H_1$, le trasformazioni delle sue sostituzioni sotto l'azione di b, c, ..., appartengono ad H_b, H_c che, però, non fanno altro che riprodurre sostituzioni appartenenti ad I: ne concludiamo che tutte le sostituzioni di I sono comuni ad H_1, H_b, H_c,... e quindi $I \subseteq J$.

Emerge da questo teorema il ruolo giocato dai sottogruppi *normali* del gruppo G di un'equazione che diverrà cruciale nel decidere se un'equazione assegnata sia o meno risolubile algebricamente.

Jordan osserva ora che, se H_1 è normale in G, si avrà $H_1 = H_b = H_c = \cdots = I$ e φ_1, φ_b, φ_c, $\cdots$, essendo invarianti sotto l'azione delle medesime sostituzioni di

[24] I teoremi IV e V.

G, si esprimono razionalmente in funzione di una sola di esse. Viceversa, se φ_1, φ_b, $\varphi_c, \cdots$ si esprimono razionalmente in funzione di una sola di esse, saranno invarianti per lo stesso insieme di sostituzioni di G cosicché $H_1 = H_b = H_c = \cdots$ che risulterà un gruppo normale in G.

A questo punto Jordan ha gli elementi per aggiungere dettagli sul gruppo di Galois dell'equazione (9.12):

Teorema VII. *Sia N l'ordine di G, $N' = \frac{N}{\nu}$ l'ordine di I. L'ordine del gruppo G' dell'equazione* (9.12) *sarà ν.*

Dunque l'equazione (9.12) ha grado uguale all'ordine del suo gruppo di Galois. Per dimostrarlo, occorre ripercorrere il procedimento che ha portato ad ottenere il gruppo di Galois per l'equazione assegnata, a partire questa volta da (9.12). Infatti, Jordan considera la funzione

$$W := M_1\varphi_1(r_1, r_2, \cdots, r_n) + M_b\varphi_b(r_1, r_2, \cdots, r_n) + M_c\varphi_c(r_1, r_2, \cdots, r_n) + \cdots \tag{9.14}$$

dove i coefficienti M_i sono da scegliere in modo che W assuma sempre valori distinti, comunque si permutino tra loro le radici di (9.12). Per definizione, W è radice di un'equazione irriducibile su $\mathbb{Q}$, di grado pari all'ordine del gruppo G' dell'equazione (9.12). Possiamo però considerare W come funzione delle radici $r_1, r_2, \cdots, r_n$ dell'equazione assegnata $p(x) = 0$: in questo senso, W non è modificata dalle trasformazioni di I, mentre lo è da quelle di $G \setminus I$. Possiamo applicare a W le considerazioni fatte nel teorema V e concludere che essa dipende da un'equazione irriducibile di grado pari al rapporto tra gli ordini di G ed I.

Concludiamo questa analisi del *Commentaire* enunciando il Teorema IX che lega la presenza di una successione di sottogruppi normali di G, inclusi successivamente uno nell'altro, alla riduzione della risoluzione dell'equazione di partenza a quella di equazioni di gradi opportuni

Teorema IX. *Sia $F(x)$ un'equazione il cui gruppo G sia composto: G, I, I',...., una successione di gruppi tali che: I. Ciascuno di essi è contenuto in quello che lo precede e commutabile con le sostituzioni di quet'ultimo; II. Ciascuno di essi sia il più generale tra quelli che soddisfano alle due proprietà mensionate; Siano N, $\frac{N}{\nu}$, $\frac{N}{\nu\nu'}$,... gli ordini rispettivi di questi gruppi: la soluzione dell'equazione proposta dipenderà da quella di equazioni successive i cui gruppi saranno semplici e conterranno, rispettivamente ν, ν', ... sostituzioni.* ([27], p. 152)

Con questo teorema entra in scena la *serie di composizione* di G, cioè una successione di sottogruppi

$$G \equiv I_0 \supseteq I_1 \supseteq \cdots \supseteq I_n = \mathrm{id}$$

tali che I_i è il sottogruppo normale massimale contenuto in I_{i-1}. Ora, quando gli indici ν, ν',..., di ciascuno di questi sottogruppi in quello che lo precede nella serie di composizione sono tutti i numeri primi, allora l'equazione (9.12) corrispondente è *abeliana* e dunque risolubile *algebricamente*. L'approccio gruppale di Galois, perfezionato da Jordan, consiste dunque nel tradurre la richiesta di risolubilità algebrica di un'equazione in una richiesta sulla struttura del gruppo associato.

Come detto, Jordan non segue fedelmente l'ordine delle idee di Galois che, nella Proposizione II, aveva affrontato il problema del comportamento del gruppo di Galois di un'equazione quando al campo $\mathbb{Q}$ venga aggiunto un elemento, radice di un'equazione ausiliaria.

Proposizione II. *Se si aggiunge ad un'equazione la radice r si un'equazione ausiliaria irriducibile, 1° di queste due eventualità se ne presenterà una: o il gruppo dell'equazione non cambierà, oppure si dividerà in p gruppi ciascuno appartenente all'equazione proposta quando gli si aggiunga ciascuna delle radici dell'equazione ausiliaria; 2° questi gruppi godranno della proprietà notevole che è possibile passare da uno all'altro operando su tutte le permutazioni del primo con una medesima sostituzione di lettere*[25] ([20], pp. 423-424)

La dimostrazione di Galois è anche in questo caso estremamente concisa.

La successiva Proposizione III, priva di dimostrazione ma con l'aggiunta *On trouvera la démonstration*, tratta il caso in cui si aggiungano ad F tutte le radici dell'equazione (9.15).

Proposizione III *Se si aggiungono ad un'equazione <u>tutte</u> le radici di un'equazione ausiliaria, i gruppi oggetto del Teorema II godranno dell'ulteriore proprietà che le sostituzioni sono le stesse in ogni gruppo*[26]. ([20], p.425)

Osserviamo che se u_1 è una radice di un'equazione ausiliaria *irriducibile* su F

$$T(x) = 0 \tag{9.15}$$

e se $K := F[u_1] \supseteq F$ è il campo ottenuto aggiungendo u_1 ad F, il fattore irriducibile su F di (9.7) cui appartiene V può ancora essere irriducibile in K ed in questo caso $\mathrm{Gal}(P/K) = \mathrm{Gal}(P/F)$; in caso contrario, tale fattore irriducibile si spezza in fattori di grado minore (tutti dello stesso grado, come dimostra Galois) e dunque in questo caso $\mathrm{Gal}(P/K) \subseteq \mathrm{Gal}(P/F)$. Conseguenza non banale della fattorizzazione appena menzionata è che, se $t = \deg T$,

$$\frac{|\mathrm{Gal}(P/F)|}{|\mathrm{Gal}(P/K)|} \quad \text{divide } t. \tag{9.16}$$

Aggiungo un'osservazione sul testo di Galois. Egli afferma che si passa da un sottogruppo ad un altro operando su tutte le permutazioni del primo con una medesima sostituzione di lettere. Ora, se $\mathrm{Gal}(P/K) = \{\mathrm{id}, \sigma_2, \sigma_3, ..., \sigma_k\}$ e τ_1, τ_2,...,τ_ℓ sono permutazioni di $\mathrm{Gal}(P/F)$ che non stanno in $\mathrm{Gal}(P/K)$, allora le permutazioni ottenute seguendo superficialmente la prescrizione di Galois sono, utilizzando τ_1,

$$\{\tau_1, \sigma_2\tau_1, ..., \sigma_k\tau_1\} \qquad ... \qquad \{\tau_\ell, \sigma_2\tau_\ell, ..., \sigma_k\tau_\ell\} :$$

[25] Si l'on adjoint à une équation donnée la racine r d'une équation auxiliaire irréductible, 1° il arrivera de deux choses l'une: ou bien le groupe de l'équation ne sera pas changé, ou bien il se partagera en p groupes appartenant chacun à l'équation proposée respectivement quand on lui adjoint chacune des racines de l'équation auxiliaire; 2° ces groupes jouiront de la propriété remarquable, que l'on passera de l'un à l'autre en óperant dans toutes les permutations du premier une même substitutions des lettres

[26] Si l'on adjoint à une équation <u>toutes</u> les racines d'une équation auxiliaire, les groupes dont il est question dans le théoreme II jouiront de plus de cette propriété, que les substitutions sont les mêmes dans chaque groupe.

come visto in precedenza questi insiemi *non* sono gruppi, mancando dell'identità. Si può recuperare la struttura gruppale moltiplicando a sinistra per τ_i^{-1} ed ottenere gli insiemi

$$\{\mathrm{id}, \tau_1^{-1}\sigma_2\tau_1, ..., \tau_1^{-1}\sigma_k\tau_1\} \qquad ... \qquad \{\mathrm{id}, \tau_\ell^{-1}\sigma_2\tau_\ell, ..., \tau_\ell^{-1}\sigma_k\tau_\ell\}$$

che invece *sono* dei gruppi, tutti dello stesso ordine, come afferma Galois. La partizione del gruppo cui allude Galois si esprime dicendo che, aggiunte *tutte* le radici $u_1, u_2, ...u_t$ di (9.15) ad F, $\mathrm{Gal}(P/F[u_1, u_2, ..., u_t])$ è un sottogruppo normale di $\mathrm{Gal}(P/F)$, cioè a dire che, se $\sigma \in \mathrm{Gal}(P/F)$ e $\tau \in \mathrm{Gal}(P/F[u_1, u_2, ..., u_t])$, allora

$$\sigma \circ \tau \circ \sigma^{-1} \in \mathrm{Gal}(P/F[u_1, u_2, ..., u_t])$$

Con le rimanenti Proposizioni, Galois si dedica alla risposta che aveva animato tutta la sua ricerca, fornire una condizione sotto la quale un'equazione risulta risolubile per radicali. Invece di darne una dimostrazione, per la quale rimando a [25], Cap. 14, procediamo ad illustrare il metodo di Galois operando su un'equazione di quarto grado. La Proposizione V è posta sotto forma di problema:

Proposizione V *In quali casi un'equazione [algebrica] è risolubile per radicali semplici?*[27] ([20], p.426)

Galois non fornisce, al solito, una dimostrazione formale ma alcuni passi della proposizione sono importanti per chiarire lo scopo delle sue ricerche:

Osservo anzitutto che, per risolvere un'equazione, occorre ridurre successivamente il suo gruppo finché esso non contenga che una sola permutazione. Infatti, quando un'equazione è risolta, una qualunque funzione delle sue radici sarà nota, così come succede quando essa non è invariante sotto alcuna permutazione[28] ([20], p. 426).

Il gruppo di un'equazione misura il grado di indistinguibilità delle radici e finché esso è composto da permutazioni diverse da quella identica non si ha che una conoscenza imperfetta delle radici dell'equazione proposta, imperfezione che è massima quando il gruppo coincide con l'intero gruppo delle permutazioni agenti su n elementi e quindi sono note solo le funzioni simmetriche delle radici che non permettono di distinguere in alcun modo tra loro le radici. Precisato questo, Galois illustra la marcia da intraprendere per tentare la riduzione del gruppo dell'equazione, aggiungendo degli opportuni radicali. Il primo passo è l'aggiunta del primo radicale che viene estratto nel corso della soluzione. Se aggiungendo tale radicale al campo dei coefficienti dell'equazione proposta il gruppo può non ridursi, nel qual caso si è trattata di una semplice preparazione, oppure il gruppo si riduce. Affinché l'equazione sia risolubile occore che la riduzione del gruppo avvenga in un numero *finito* di passi. È possibile che

[27] *Dans quels cas une équation est-elle soluble par de simples radicaux?*

[28] J'observerai d'abord que, pour résoudre une équation, il faut succéssivement abaisser son groupe jusqu'à ne contenir pluse qu'une seule permutation. Car, quand une équation est résolue, une fonction quelconque de ses racines est connue, même quand elle n'est invariable par aucune permutation.

ad un certo punto la riduzione del gruppo sia operabile in modi diversi grazie ad estrazioni di radici. Galois considera il radicale di indice p più basso possibile, osservando che p è primo: se fosse un numero composto, una riduzione si dovrebbe operare attraverso l'aggiunta di una radice con indice pari ad uno dei suoi fattori primi. Galois chiama radicali semplici quelli con indice primo. Osserva ora Galois che, ai fini della determinazione del gruppo di un'equazione è sempre possibile supporre *nota* una radice p-esima α dell'unità in quanto essa si ottiene attraverso estrazioni di radice con indice *inferiore* a p e dunque, per l'ipotesi fatta su p, queste quantità radicali non possono ridurre il gruppo. Dunque, invocando le Proposizioni II e III, Galois conclude che il gruppo dell'equazione si spezza in p (sotto)gruppi le cui relazioni sono quelle ricordate nelle Proposizioni. Viceversa, Galois suppone che il gruppo $\mathrm{Gal}(P/F)$ si spezzi in p sottogruppi ciascuno dotato delle proprietà enunciate nella proposizione III ed intende dedurre da ci 'o che, aggiungendo una radice di indice p-esima il gruppo di partenza si riduce ad uno, diciamo G_p dei p sottogruppi. Per questo Galois costruisce una funzione $\theta(r_1, r_2, ..., r_n)$ invariante rispetto alle permutazioni contenute in G_p, ma variabile quando invece agiscono le permutazioni che nno appartengono a G_p. Senza avvertire la necessità di aggiungere qualche commento, Galois afferma che, operando successivamente con permutazioni che stanno in $\mathrm{Gal}(P/F)$ ma non in G_p, allora θ assumerà, oltre a θ, altri $p-1$ valori θ_1, θ_2, ..., θ_{p-1} distinti tra loro e da θ cosicché

$$(\theta + \alpha\theta_1 + \alpha^2\theta_2 + ... + \alpha^{p-1}\theta_{p-1})^p$$

risulterà invariante sotto l'azione di tutte le permutazioni in $\mathrm{Gal}(P/F)$ e quindi, per la caratterizzazione di $\mathrm{Gal}(P/F)$ contenuta nella Proposizione I, razionalmente nota. Se ora si aggiunge al campo F dei coefficienti dell'equazione di partenza, grazie alla Proposizione IV si conclude che il gruppo dell'equazione risultante da questa aggiunzione non conterrà altre permutazioni che quelle dei p sottogruppi, uno dei quali è G_p.

Il contenuto della Proposizione V si può riformulare, con una buona dose di *senno del poi*, come segue:

Sia $P(x)$ un polinomio a radici distinte. Allora $P(x) = 0$ è risolubile per radicali se e solo se $\mathrm{Gal}(P/F)$ *è un gruppo risolubile, cioè se esiste una catena di sottogruppi G_i, con $i = 1, ..., t = \mathrm{deg}T$, T essendo un polinomio ausiliario di cui sono note le radici, tali che*

- $\mathrm{Gal}(P/F) \equiv G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = \{\mathrm{id}\}$,
- *per tutti gli $i = 1, ..., t$, G_i è sottogruppo normale di G_{i-1} di indice primo.*

Dopo aver illustrato come il gruppo delle permutazioni agenti su 4 elementi ammetta la giusta struttura per giungere alla riduzione di $\mathrm{Gal}(P/F)$ all'identità, Galois applica la teoria generale alle equazioni irriducibili di grado pari ad un numero primo. Così, nella Proposizione VI, egli mostra il seguente lemma:

Lemma. *Un'equazione irriducibile di grado primo non può divenire riducibile con l'aggiunta di un radicale avente indice diverso dal grado dell'equazio-*

ne.[29]([20], p. 429)

Mentre nella Proposizione VII si pone la domanda

Proposizione VII. *Qual è il gruppo di un'equazione irriducibile di grado primo n, risolubile per radicali?*[30] ([20], p. 429)

Il lemma oggetto della Proposizione VI permette di asserire che il più piccolo gruppo ammissibile, dopo l'identità, deve essere formato da n elementi ed, operando tale gruppo su un insieme di n oggetti, non può che essere un gruppo ciclico. Iterando il ragionamento Galois conclude che condizione necessaria e sufficiente alla risolubilità per radicali di un'equazione irriducibile di grado primo è che ogni funzione invariante sotto le permutazioni $x_k \mapsto x_{ak+b}$, dove a e b sono costanti (intere) sia razionalmente nota. In alternativa, il risultato qui ottenuto viene così enunciato nella Proposizione VIII che chiude la *Mémoire*

Proposizione VIII. *Affinché un'equazione irriducibile di grado primo sia risolubile per radicali, occorre e basta che, note due qualsiasi delle sue radici, le altre si possano dedurre da queste solo con operazioni razionali.*[31] ([20], p. 432)

Nel corso della *Mémoire* Galois menziona il fatto che la risolubilità delle equazioni di quarto grado sia dovuta al fatto che è possibile trovare ridurre il gruppo dell'equazione generale, il gruppo simmetrico agente su 4 elementi, in modo conforme a quanto prescritto nella proposizione V. In generale, egli osserva che il gruppo di un'equazione generale (letterale) di grado n è il gruppo simmetrico su n elementi mentre per l'equazione ciclotomica

$$\frac{x^n - 1}{x - 1} = 0$$

il gruppo si riduce a quello ciclico su n lettere, la cui cardinalità coincide con il grado dell'equazione da risolvere.

Sarebbe interessante seguire la storia della diffusione della teoria di Galois ad opera di matematici come Enrico Betti o Camille Jordan e seguire i cambiamenti che tale teoria ha subito fino al fondamentale libro di Emil Artin *Foundations of Galois Theory*, pubblicato nel 1938. Mi riservo di presentare in forma più completa questi argomenti in una prossima edizione, limitandomi per ora a rinviare il lettore interessato all'articolo di Kiernan [29] o al libro di Toti-Rigatelli [30].

[29] Une équation irréductible du degré premierne peut devenir réductible par l'adjonction d'un radical dont l'indice sera autre que le degré même de l'equation.

[30] Quel est le groupe d'une équation irréductible d'un degré premier n, soluble par radicaux?

[31] Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il *faut* et il *suffit* que deux quelconques des racines étant connues, les autres s'en déduisent rationellement.

Bibliografia

[1] E.T. Bell: Men of Mathematics. Simon and Schuster, New York (USA), 1950. Trad. It. I grandi matematici. Sansoni, Firenze, 1990.

[2] T. Rothman: Genius and biographers: the fictionalization of Évariste Galois. *Amer. Math. Monthly*, **89**, 84–106, (1982).

[3] P. Dupuy: La vie d'Évariste Galois. *Ann. Scient. Éc. Norm. Super.*, **13** (S. III), 197-266, (1896).

[4] R. Taton: Les relations d'Évariste Galois avec les mathmaticiens de son temps. Revue d'Histoire des Sciences et de ses Applications **1**, 114-130, (1947).

[5] R. Taton: Sur les relations scientifiques d'Augustin Cauchy et d'Évariste Galois. Revue d'Histoire des Sciences **24**, 123-148, (1971).

[6] L. Toti Rigatelli: *Matematica sulle barricate. Vita di Évariste Galois.* Sansoni, Firenze, (1993).

[7] É. Galois: Œuvres mathématiques. *J. Math. Pures Appl.*, **11** (S. 1), 381—444, (1846).

[8] J.L. Lagrange: Réflexions sur la résolution algébrique des équations, *Nouveaux Mém. de l'Acad. des Sciences et Belles-Lettres de Berlin*, **1**, 134–215, (1770); **2**, 138-253, (1771). In *Œuvers Complètes*, vol. 3, J.A. Serret, Ed., Gauthier-Villars, Paris, (1869), 205-421.

[9] J.L. Lagrange: Traité de la résolution des équations numériques de tous les degrés, avec des notes sur pluiseurs points de la Théorie des équations algébriques, Courcier, Paris, (1808). In *Œuvers Complètes*, vol. 8, J.A. Serret, Ed., Gauthier-Villars, Paris, (1879), 11-370.

[10] È. Galois: Démonstration d'un théorème sur les fractions continues périodiques. *Annales des Sciences Mathématiques.* **19**, 294-301, (1828-1829). In [7], pp. 385-392.

[11] È. Galois: Notes sur quelques points d'Analyse. *Annales des Sciences Mathématiques.* **21**, 182-184, (1830-1831). In [7], pp. 392-394.

[12] B. Bolzano: *Functionenlehre.* In *The mathematical work of Bernard Bolzano*, a cura di S. Russ. Oxford University Press, Oxford (U.K.), (2004).

[13] É. Galois: Analyse d'un Mémoire sur la résolution algégbrique des équations. *Bull. Sci. math.*, **13**, 271- (1830).

[14] É. Galois: Note sur la résolution des équations numériques. *Bull. Sci. math.*, **13**, 413-414, (1830). In [7], pp. 397-398.

[15] A.-M. Legendre: *Essai sur la théorie des nombres.* Courcier, Paris, (1816).

[16] A.-L. Cauchy: *Cours d'analyse de l'École royale Polytechnique.* Vol. I *Analyse Algébrique*, (1821).

[17] M. Galuzzi: Galois' note on the approximative solution of numerical equations (1830). *Arch. Hist. Exact Sci.*, **56**, 29-37, (2001).

[18] É. Galois: Sur la théorie des nombres. *Bull. Sci. math.*, **13**, 428-, (1830). In [7], pp. 398-407.

[19] C.G.J. Jacobi: De residuis cubicis commentatio numerosa. *Journ. für die reine und angewandte Mathematik* (1827)

[20] É. Galois: Mémoire sur les conditions de résolubilité des équations par radicaux. In [7], pp. 417–433.

[21] N.H. Abel: Mémoire sur une classe particulière d'équations résolubles algébriquement. *J. für die reine und angew. Math. (Crelle)*, **4**, 131–156, (1829).

[22] A. Dahan: Les travaux de Cauchy sur les substitutions. Étude de son approche du concept de groupe. *Archive for History of Exact Sciences*, **23**, 279–319, (1980).

[23] I. Radloff: Évariste Galois: principles and applications. *Historia Mathematica*, **29**, 114–137, (2002).

[24] J. Hudde: *Epistola Prima de Reductione Æquationum.* In R. Des Cartes Geometria, a cura di F. van Schooten, Knoch (Frankfurt an Mein) (1695).

[25] J.-P. Tignol: *Galois' Theory of Algebraic Equations.* World Scientific, Singapore, (2001).

[26] G. Cantor: Algebraische Notiz. *Math. Annalen* **5**, 133-134, (1872)

[27] C. Jordan: Commentaire sur Galois. *Math. Annalen* **1**, 141–160, (1869)

[28] J. Pierpont: Galois' theory al algebraic equations. I. Rational resolvents. *Annals Math.* **1** (S. II), 113–143, (1899-1900).

[29] B.M. Kiernan: The development of Galois theory from Lagrange to Artin. *Archive for History of Exact Sciences*, **13**, (1971), 40–154.

[30] L. Toti-Rigatelli: *La mente algebrica: storia dello sviluppo della teoria di Galois nel XIX secolo.* Bramante, Busto Arsizio, (1989).