Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea Magistrale in Matematica

ALL'ORIGINE DELLA TEORIA DI GALOIS: GLI SVILUPPI DELL'ALGEBRA NELLA PRIMA METÁ DELL'OTTOCENTO

Tesi di Laurea in Storia della Matematica

Relatrice:
Chiar.ma Prof.ssa
Maria Giulia Lugaresi

Presentata da:
Giorgio Morodo

Anno Accademico 2023-2024

A Gaia.
In questo momento, nessun dovere è più urgente di quello di dirti:
Grazie di Cuore!

Indice

Elenco delle figure

1 Introduzione

Per affrontare la storia delle formule risolutive delle equazioni algebriche, dobbiamo partire dall'Italia del XVI secolo, in particolare dall'ambiente legato all'Università di Bologna. Infatti, è proprio qui che venne scoperta la formula risolutiva di una particolare tipologia di equazioni di terzo grado, ad opera di Scipione del Ferro (1465-1526).
Tale scoperta abbatteva un confine che pochi anni prima il matematico Luca Pacioli (1445-1514), autore del più famoso trattato di Algebra rinascimentale, *"Summa de arithmetica, geometria, proportioni et proportionalità"*, riteneva invalicabile. Questa fu la prima volta in cui la nuova civiltà europea riuscì a superare i risultati della scienza classica, guadagnando una coscienza nei propri mezzi che, non a caso, avrebbe originato l'intenso sviluppo della matematica nei secoli successivi.
Come o quando del Ferro sia giunto alla formula risolutiva non lo si sa con precisione, poichè egli non la pubblicò mai; approssimativamente, però, si colloca nel decennio tra il 1505 e il 1515. Tuttavia, prima di morire la rivelò ad un suo studente, Antonio Maria Fior, un mediocre matematico, che si creò una certa fama come esperto nella risoluzione di questo genere di problemi.

Il circolare della voce dell'esistenza di una formula risolutiva per l'equazione di terzo grado giunse anche a Brescia, in particolare arrivò alle orecchie di Niccolò Fontana (1499-1557), meglio noto come Tartaglia; ciò lo stimolò a trovare un proprio metodo per risolvere questo tipo di equazioni. Intorno al 1535 egli riuscì nella propria impresa e, per mettere alla prova l'efficacia della sua scoperta, venne organizzata una gara matematica tra lui e Fior.
La *"pubblica disputazione"* consisteva nella risoluzione di trenta problemi a testa, proposti dall'avversario in un tempo stabilito. Chi fosse riuscito a risolverne di più avrebbe vinto la sfida. La disputa si concluse con la vittoria schiacciante di Tartaglia che riuscì a risolvere tutti i quesiti, a differenza di Fior che non ne risolse alcuno.
La spiegazione dell'esito della sfida è relativamente semplice: i trenta problemi avanzati da Tartaglia erano di varia natura, mentre quelli proposti da Fior erano tutti riconducibili ad equazioni della forma $x^3 + px^2 = q$, convinto che nessuno sapesse risolvere equazioni del genere. Ma, Tartaglia, avendo studiato l'argomento a fondo, conosceva un metodo generale per ridurre queste equazioni a quelle del tipo $x^3 + px = q$, che erano in grado di risolvere sia lui che Fior.

La notizia della vittoria di Tartaglia ebbe larga diffusione e raggiunse anche Girolamo Cardano (1501-1576), professore sia all'Università di Bologna che a Milano, che nel frattempo stava preparando, con l'allievo Ludovico Ferrari (1522-1565), il materiale destinato a realizzare un'opera di ampio respiro sull'Algebra, l' *"Ars Magna"*. Dunque, Cardano, desideroso di scoprire la formula in possesso di Tartaglia, lo convinse a soggiornare a casa sua con la promessa di presentarlo ad un ricco mecenate, ben sapendo che Tartaglia era da sempre stato privo di una fonte concreta di sostentamento.
Qui, dopo giorni di attesa, Cardano riuscì a farsi confidare il metodo risolutivo, con la solenne promessa, però, di non divulgare la scoperta, poiché Tartaglia intendeva pubblicarla a coronamento del suo trattato sull'Algebra.
Tuttavia, quando Cardano scoprì a Bologna, che del Ferro, ben prima di Tartaglia, aveva già trovato tale formula risolutiva, si decise ad inserirla nell' *"Ars Magna"* (1545), scatenando l'ira di Tartaglia.
In difesa di Cardano intervenne Ferrari, che inviò al matematico bresciano diversi *"Cartelli di mate-*

matica disfida". Fino a giungere alla pubblica disputa tenutasi nel 1548, nella quale uscì vittorioso Ferrari.

Nell' *"Ars Magna"* viene esposta anche la formula risolutiva delle equazioni di quarto grado, la cui paternità appartiene a Ferrari. Infatti, va precisato, che Cardano nella sua opera ammette di non essere lo scopritore di nessuna delle due formule.

L'ultimo rappresentante in ordine cronologico della ricca scuola matematica bolognese del XVI secolo è Rafael Bombelli (1526-1573), che realizzò l' *"Algebra"*, una sorta di sintesi di quanto era stato scoperto fino a quel momento sulla teoria delle equazioni algebriche.
Il contributo maggiore di Bombelli fu l'introduzione delle quantità immaginarie *"più di meno"* e *"meno di meno"*, necessarie per trattare i casi irriducibili e rendere così sempre applicabili le formule risolutive trovate.

Dopo la pubblicazione dell' *"Ars Magna"* di Cardano, l'Algebra si era trasformata principalmente nella teoria delle equazioni algebriche, in quanto la ricerca di formule risolutive mediante radicali per equazioni generali di grado superiore al quarto era diventata il problema fondamentale.
Ciò lo si nota nella parte conclusiva dell'opera *"Réflexions"* di Lagrange, dove egli esprimeva la sua profonda convinzione nell'aver smascherato i principi originali che si nascondevano dietro i metodi di risoluzione delle equazioni algebriche, e che erano alla base del loro successo per equazioni di grado non superiore al quarto: *"il tutto si riduce, come si è visto, ad una sorta di calcolo di combinazioni, tramite il quale si trovano a priori i risultati che uno può aspettarsi."* ([21] pagina 403)
Tuttavia, si mostrava ugualmente consapevole che la risolubilità algebrica di equazioni di grado superiore al quarto, per tale via, fosse ancora lontana dall'essere ottenuta.
"Sarebbe opportuno farne l'applicazione ad equazioni di quinto grado e di gradi superiori la cui soluzione è ad oggi sconosciuta; tuttavia questa applicazione richiede un numero troppo grande di ricerche e di combinazioni, la cui riuscita è ancora molto dubbia perchè possa dedicarmi attualmente a questo lavoro". ([21] pagina 403)

Alla fine del XVIII secolo iniziò a farsi largo l'ipotesi, per certi aspetti sorprendente, dell'impossibilità di ottenere una formula risolutiva generale per equazioni di grado superiore al quarto. Tale tesi fu sostenuta anche da Gauss (1777-1855) che, nel 1799, affermò:
"Dopo tante fatiche di molti geometri rimane solo una minima speranza di poter pervenire un giorno alla risoluzione generale delle equazioni algebriche ed appare sempre più verosimile che una tale risoluzione sia impossibile e contraddittoria." ([22] pagina 17)

Nel stesso anno Paolo Ruffini (1765-1822), medico e matematico italiano attivo a Modena, pubblicò la dissertazione *"Teoria generale delle Equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto"*.
La dimostrazione del teorema fu bersagliata da critiche, alcune benevole, altre meno, cui Ruffini rispose con nuove versioni della stessa, tese a chiarirne e semplificarne l'impianto; l'ultima fu pubblicata nel 1813 nella memoria intitolata *"Riflessioni intorno alla soluzione delle equazioni algebriche generali"*.
Tuttavia, anche la dimostrazione finale presentava alcune lacune, che furono colmate nel 1826 dal matematico norvegese Niels-Henrik Abel (1802-1829); ciò portò al famoso *"teorema Abel-Ruffini"*, che afferma la non esistenza di una formula risolutiva esprimibile tramite radicali per le equazioni

di grado superiore al quarto.

Fallita la possibilità di trovare tali formule, era rimasto aperto il problema di caratterizzare le equazioni che, pur essendo di grado maggiore o uguale al quinto, sono tuttavia risolubili per radicali, il che equivale a trovare condizioni necessarie e sufficienti affinché un'equazione algebrica di grado n qualunque sia risolubile per radicali. La memoria presentata da Galois nel 1829 all'*Académie des sciences* di Parigi conteneva la risposta al problema.

L'importanza del lavoro non consisteva però semplicemente nell'aver trovato le condizioni cercate, ma nel modo in cui sono state ottenute.
Galois comprese che non bisognava studiare direttamente l'equazione in questione, ma associare ad essa un altro ente matematico le cui proprietà fossero traducibili in proprietà dell'equazione stessa e viceversa, ed analizzare quindi il nuovo ente.
Ad ogni equazione, dunque, il matematico francese associò quello che egli stesso definì, usando per la prima volta tale termine, un *"gruppo"* di sostituzioni sulle radici dell'equazione medesima, e che oggi viene chiamato *"gruppo di Galois"*.
Poi, servendosi di uno dei risultati chiave della teoria, ovvero l'esistenza di una corrispondenza biunivoca tra le estensioni del campo di partenza, in cui sono definiti i coefficienti del polinomio, e i gruppi di Galois associati a tali estensioni, fornì criteri per determinare quando un'equazione polinomiale potesse essere risolta tramite radicali.

In questa tesi, dopo aver fornito un quadro del contesto storico-scientifico in cui si colloca l'opera matematica di Évariste Galois, presenteremo una biografia scientifica dell'autore e una descrizione dei suoi scritti matematici. Il nucleo centrale della tesi riguarderà una presentazione della teoria di Galois, a partire dall'esame delle memorie del matematico francese.

2 Évariste Galois nel suo tempo

2.1 Vicende storiche del primo trentennio del XIX secolo in Francia

Agli inizi dell'800 l'ascesa di Napoleone non si era ancora conclusa, la fine dell'alleanza franco-russa avvenuta nel 1811, anno di nascita di Évariste Galois, era stata vista dall'imperatore stesso come un'opportunità per conquistare Mosca, così il 24 giugno 1812 la Grande Armata guidata da Napoleone diede inizio alla campagna di Russia, 4 mesi più tardi fu costretta alla ritirata.

La sconfitta subita minò la leadership napoleonica, e nel 1814 l'imperatore fu costretto ad abdicare, ottenendo la sovranità della sola Isola d'Elba; in Francia iniziò il periodo della Restaurazione con il ritorno della famiglia Borbone al comando. Il 3 maggio dello stesso anno Luigi XVIII fece ritorno a Parigi e la popolazione era ben consapevole che le conquiste ottenute con la Rivoluzione non si sarebbero salvate.

Dopo pochi mesi del nuovo regime si era già creato un forte malcontento e nel popolo stava rinascendo la passione rivoluzionaria. Napoleone dall'Isola d'Elba aspettava l'occasione giusta per riconquistare il potere perduto, e il 26 febbraio 1815 sulle note della Marsigliese, nel frattempo canto reso fuorilegge dal nuovo regime, e fra le acclamazioni di *"Vive l'Empereur"* si imbarcò con destinazione la Provenza.
Il sogno di Napoleone e dei suoi sostenitori durò solo cento giorni ed ebbe rovinosamente fine sul campo di battaglia di Waterloo il 18 giugno 1815.

L'8 luglio fece ritorno a Parigi, per la seconda volta, Luigi XVIII. In Francia ricominciava la Restaurazione borbonica in condizioni peggiori rispetto a 3 mesi prima.

Il Paese era spaccato in due opposti schieramenti, da una parte i sostenitori della Rivoluzione, dall'altra i sostenitori della monarchia. Questi ultimi avevano come rappresentante il conte d'Artois, fratello del re, ed erano desiderosi di punire a qualunque costo i responsabili dei *Cento Giorni.* Proprio questa sete di vendetta portò al *"Terrore Bianco"* e al massacro di centinaia di bonapartisti.

Nel frattempo il 15 ottobre 1815 Napoleone venne sbarcato prigioniero ed esiliato a Sant'Elena, una piccola isola nel mezzo dell'Oceano Atlantico, così remota e sperduta da rendere impossibile ogni tentativo di fuga. Morì il 5 maggio 1821 a causa di un tumore allo stomaco.

Il clima sempre più teso in Francia portò nel 1820 all'uccisione del figlio del conte d'Artois per mano di un operaio. Il regime reagì con una serie di riforme che andarono a limitare ulteriormente la partecipazione dei cittadini alla vita pubblica; venne ristabilita la censura e le scuole di Stato furono messe sotto particolare controllo, i docenti non allineati al regime furono licenziati e sostituiti da ecclesiastici. Tutto ciò accadde quando per Évariste Galois venne il momento di iscriversi al *Lycée Louis-le-Grand.*

Il 16 settembre 1824, dopo giorni di agonia, morì Luigi XVIII, gli succedette suo fratello, il conte d'Artois, capo del partito monarchico, con il nome di Carlo X.

Il 26 luglio del 1830, in risposta al voto popolare per la formazione del nuovo governo, Carlo X realizzò, tramite quattro ordinanze, un colpo di Stato.
Il popolo francese rispose immediatamente all'arroganza della corona con tre giornate di rivoluzione di piazza, che vennero ricordate come *"Le Trois Glorieuses"*, costringendo il re all'abdicazione. Al suo posto succedette al trono il duca d'Orléans, Luigi Filippo.

2.2 La Famiglia Galois

Évariste Galois nacque a Bourg-la-Reine, in Francia, il 25 ottobre del 1811. Il padre, Nicolas-Gabriel Galois, era proprietario di un istituto di istruzione per giovani, mentre, la madre, Adélaide-Marie Demante, era figlia di Thomas-François Demante, professore di Giurisprudenza all'Università della Sorbona e presidente del tribunale di Louviers.
Évariste era il secondo di tre figli, Nathalie-Théodore la maggiore e Alfred il minore.
Sia la famiglia Galois che la famiglia Demante godevano di una discreta agiatezza economica ed erano molto influenti nelle vicende cittadine.

La madre di Évariste aveva ricevuto da suo padre un'educazione di prim'ordine ed era una donna molto intelligente, vivace, generosa e dotata di un forte temperamento.
Il ramo paterno, invece, aderì fin da principio agli ideali rivoluzionari, lo zio di Évariste intraprese la carriera militare fino a diventare ufficiale della Guardia Imperiale, mentre il padre, più amante degli studi che del clamore dei campi di battaglia, assunse la direzione del collegio. Durante i Cento Giorni napoleonici, Nicolas-Gabriel divenne sindaco di Bourg-la-Reine, carica che mantenne fino al 1829, l'anno in cui si suicidò, non potendo più sopportare le calunnie sul suo conto alimentate dal parroco della cittadina e da diverse facoltose famiglie, sempre legate ai Borbone.

2.3 Gli anni al Lycée Louis-le-Grand

Nel 1823 Évariste, dodicenne, si trasferì a Parigi per frequentare il prestigioso *Lycée Louis-le-Grand*; fino a quel momento era stato compito di sua madre impartirgli un'adeguata educazione.
Nella scuola c'erano rappresentanze di tutte le fazioni politiche, ciò rendeva il clima molto vivace: gli animi si accendevano facilmente e sedare le liti non era una cosa da poco.
La facile tendenza dei collegiali alla ribellione era giustificata anche dalla rigida disciplina che imponeva l'istituto. La loro giornata iniziava prestissimo, alle 5.30 del mattino, in anguste camerate, poco capienti e sprovviste di qualsiasi tipo di riscaldamento per far fronte ai rigidi inverni.
Dopo aver provveduto a lavarsi e vestirsi in maniera celere, i ragazzi dovevano celebrare la preghiera comune e recarsi nelle aule, che non avevano banchi ma solo gradini sui quali gli studenti si sedevano usando le ginocchia per appoggiare i libri e i quaderni, l'illuminazione era scarsa (una candela ogni due), così come l'igiene, sul pavimento e sui gradini correvano frotte di topi e non era raro che qualcuno venisse morso.

Il silenzio doveva essere assoluto nei dormitori, nelle aule e nel refettorio. Le punizioni per i trasgressori erano tanto severe quanto frequenti, queste consistevano nell'essere mandati in celle di rigore a pane e acqua.

Contemporaneamente all'ingresso di Galois al *Louis-le-Grand* fu sostituito il direttore con Nicolas Berthot, una figura vicina ai Borbone.
Évariste, al tempo tutt'altro che un coraggioso combattente bensì timido scolaro, nonostante mal sopportasse le regole dell'istituto, non tardò a distinguersi come uno dei migliori studenti. Tuttavia, ciò non lo rendeva felice, egli soffriva in particolare la mancanza del padre, al quale era molto affezionato. Inoltre, i giorni nella cella di rigore, inevitabili anche per lui, lo mortificavano profondamente e lo facevano sentire ancora più solo e abbandonato.

Durante l'estate del 1826 cambiò nuovamente il direttore del liceo, a Berthot succedette Pierre-Laurent Laborie, uomo di mediocri capacità ma molto gradito al regime.
Laborie diede subito prova della sua ristrettezza di vedute comunicando il 21 agosto dello stesso anno, attraverso una lettera alla famiglia Galois, che Évariste dovesse ripetere il secondo anno perchè troppo giovane per accedere alla classe successiva, nonostante i suoi risultati scolastici fossero ottimi.
La famiglia Galois inizialmente si oppose, ma su fortissime insistenze del direttore dovette cedere. Per Évariste questa fu una pesante umiliazione.

Tuttavia, fu proprio questa insensata e ingiusta decisione a permettere un cambiamento di tendenza nei gusti intellettuali del ragazzo. Nei primi due anni la matematica non lo aveva interessato molto, ma il forzato ritorno in seconda e il cambio di libro di testo gli fecero nascere una passione a tratti ossessiva per la disciplina.
Il cambio in questione riguardò il manuale di geometria di Sylvestre-François Lacroix (1756-1843) che fu sostituito con quello di Adrien-Marie Legendre (1752-1833) e la leggenda narra che il volume di Legendre, previsto dall'autore per due anni di lavoro, fu letto da Galois in due giorni. La matematica divenne il suo rifugio al mondo triste del *Louis-le-Grand* che lo circondava.

Il suo nuovo insegnante di matematica fu Jean Hippolyte Véron, detto Vernier, docente dotato di poca fantasia che si atteneva rigidamente al libro di Legendre per le sue lezioni.
Tali lezioni non bastavano a Galois, che spesso trovava nuove e originali dimostrazioni ai teoremi che leggeva sul manuale. Vernier, resosi conto del talento del ragazzo, lo spronava a lavorare in modo più sistematico: *"zelo, progressi notevolissimi ma metodo insufficiente"* ([4] pagina 32) è stato uno dei suoi giudizi su Galois.

Ulteriori pareri dei suoi professori furono: *"Il furore della matematica lo domina, stimo perciò sarebbe meglio che i genitori permettessero ch'egli si dedicasse a quell'unico studio; qui egli perde tempo e non fa altro che tormentare gli insegnanti e farsi tempestare di punizioni."* ([4] pagina 33).
In quegli anni il giovane matematico si era prefissato un obiettivo ben preciso: essere ammesso all'*École Polytechnique.*

2.3.1 I libri di testo di Lacroix e Legendre per l'insegnamento della geometria

Nel XVIII secolo tornò alla ribalta la Geometria Analitica, che ritrovò il suo fascino dopo che per oltre un secolo era stata oscurata dal Calcolo Infinitesimale. Principale fautore di questo sovvertimento fu Gaspard Monge (1746-1818).
Monge fu un matematico originale e insegnante stimolante, docente presso illustri istituti, tra i quali l'*École Polytechnique*. L'unica dote pedagogica che gli mancava era quella di saper scrivere manuali in modo chiaro; tuttavia, questa sua lacuna fu abbondantemente colmata dai suoi studenti, che produssero una marea di manuali elementari di Geometria Analitica, tant'è che si può parlare di una vera e propria rivoluzione nell'insegnamento della matematica.

Tra il 1798 e il 1802 fu pubblicato il manuale elementare di Geometria di Lacroix, *"Elémens de Géométrie"*. Egli fu allievo, e poi anche collega, di Monge, ispirato dalle sue lezioni realizzò tale testo che ebbe un successo enorme, tanto da essere riedito per ben venticinque volte in novantanove anni.
Lacroix sosteneva che l'Algebra e la Geometria *"dovessero venire trattate separatamente e tenute distinte l'una dall'altra il più possibile; e che i risultati raggiunti in ciascuna di esse dovessero servire a chiarire quelli dell'altra, giacchè tra l'una e l'altra v'è la stessa corrispondenza che esiste, per così dire, tra il testo di un libro e la sua traduzione."* ([17] pagina 670).

Il contenuto del testo di Lacroix è molto simile ai manuali usati all'inizio del secolo scorso, esso si divide in due sezioni, la prima tratta i seguenti argomenti:

1. Le proprietà delle rette e curve
2. Le rette perpendicolari e oblique
3. La teoria delle rette parallele
4. I poligoni
5. La retta e il cerchio
6. I poligoni inscritti e circoscritti nella circonferenza
7. L'area dei poligoni e della circonferenza
8. I piani e le rette
9. I poliedri

Mentre la seconda sezione tratta:

1. I corpi tondi
2. La proporzione tra corpi tondi

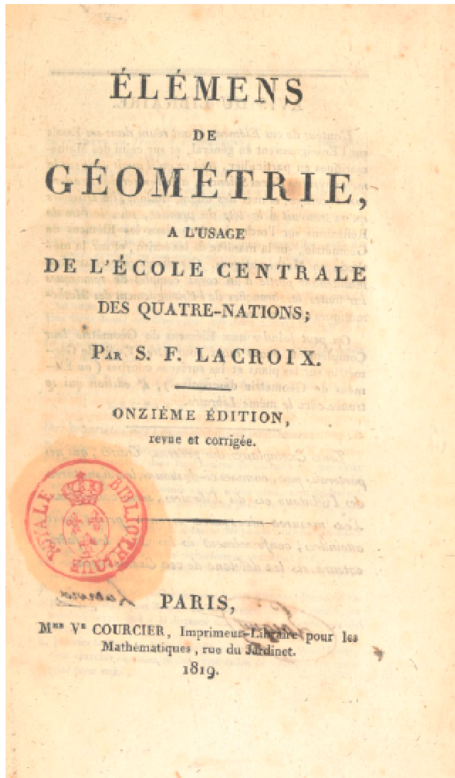

ÉLÉMENS
DE
GÉOMÉTRIE,
A L'USAGE
DE L'ÉCOLE CENTRALE
DES QUATRE-NATIONS;
PAR S. F. LACROIX.
ONZIÈME ÉDITION,
revue et corrigée.
PARIS,
Mme Ve COURCIER, Imprimeur-Libraire pour les Mathématiques, rue du Jardinet.
1819.

Figura 1: Frontespizio degli *Élémens de Géométrie* di Lacroix

Nonostante Legendre fosse uno studioso di Analisi Infinitesimale, pubblicò nel 1794, l'anno del Terrore, il manuale *"Éléments de Géométrie"*.
In prefazione l'autore stesso dichiarò che il suo obiettivo era di *"comporre una trattazione veramente rigorosa degli elementi [della geometria]"* ([17] pagina 679).
Tale manuale si inscrive, quindi, in un ritorno ai metodi geometrici, dai quali la matematica nel Settecento si era progressivamente allontanata nella convinzione che i metodi analitici fossero non solo più efficaci e generali, ma consentissero un'unificazione di tutto il sapere matematico.

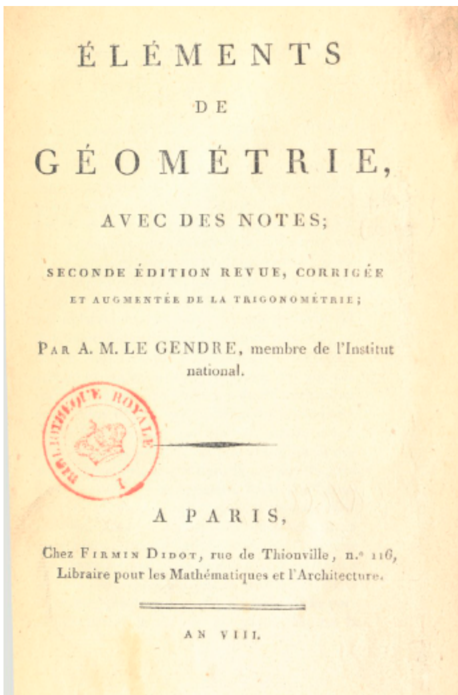
Gli *"Éléments de Géométrie"* di Legendre sono divisi in otto libri:

1. I principi
2. Seguito dei principi
3. Le proporzioni delle figure
4. I poligoni regolari, e la misura della circonferenza
5. I piani e gli angoli solidi

6. I Poliedri
7. La sfera
8. I corpi tondi

Come nella tradizione settecentesca, gli *"Éléments"* di Legendre non danno esplicitamente il quinto postulato e svolgono una teoria delle parallele che implicitamente lo ammette. L'uso dell'Algebra, che non è escluso dall'opera, rende molte dimostrazioni più spedite, mentre la teoria delle proporzioni le rende molto più semplici e permette di estendere gli argomenti trattati.

Anche tale manuale ebbe un grandissimo successo, tanto da essere ristampato per ben venti volte solo durante la vita di Legendre, e influenzò profondamente non solo i matematici europei, ma anche quelli d'oltreoceano. Infatti, in America si affermò come testo base per la disciplina.



ÉLÉMENTS
DE
GÉOMÉTRIE,
AVEC DES NOTES;

SECONDE ÉDITION REVUE, CORRIGÉE
ET AUGMENTÉE DE LA TRIGONOMÉTRIE;

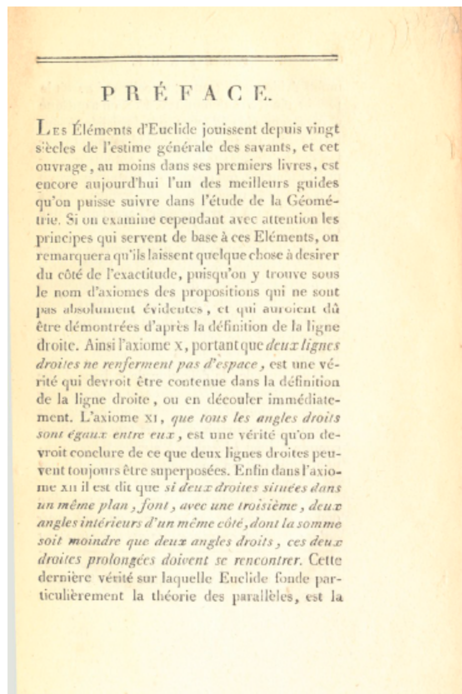
PAR A. M. LE GENDRE, membre de l'Institut national.

A PARIS,

Chez FIRMIN DIDOT, rue de Thionville, n.° 116,
Libraire pour les Mathématiques et l'Architecture.

AN VIII.

(a) Frontespizio degli *Éléments de Géométrie* di Legendre



PRÉFACE.

LES Éléments d'Euclide jouissent depuis vingt siècles de l'estime générale des savants, et cet ouvrage, au moins dans ses premiers livres, est encore aujourd'hui l'un des meilleurs guides qu'on puisse suivre dans l'étude de la Géométrie. Si on examine cependant avec attention les principes qui servent de base à ces Eléments, on remarquera qu'ils laissent quelque chose à desirer du côté de l'exactitude, puisqu'on y trouve sous le nom d'axiomes des propositions qui ne sont pas absolument évidentes, et qui auroient dû être démontrées d'après la définition de la ligne droite. Ainsi l'axiome X, portant que *deux lignes droites ne renferment pas d'espace*, est une vérité qui devroit être contenue dans la définition de la ligne droite, ou en découler immédiatement. L'axiome XI, *que tous les angles droits sont égaux entre eux*, est une vérité qu'on devroit conclure de ce que deux lignes droites peuvent toujours être superposées. Enfin dans l'axiome XII il est dit que *si deux droites situées dans un même plan, font, avec une troisième, deux angles intérieurs d'un même côté, dont la somme soit moindre que deux angles droits, ces deux droites prolongées doivent se rencontrer.* Cette dernière vérité sur laquelle Euclide fonde particulièrement la théorie des parallèles, est la

(b) Prima pagina estratta dalla prefazione agli *Éléments de Géométrie* di Legendre

Figura 2: Gli *Éléments de Géométrie* di Legendre

2.4 Tentativi falliti di accedere all'École Polytechnique

Nel 1794 era stata istituita una commissione incaricata di creare un istituto di alto livello per la preparazione degli ingegneri, nacque così l'illustre *École Polytechnique.* Tra le file dei suoi docenti compaiono nomi prestigiosi quali: Gaspard Monge, Joseph-Louis Lagrange (1736-1813), Pierre-Simon Laplace (1749-1827), Adrien-Marie Legendre, Sylvestre-François Lacroix e altri ancora.

L'istituto era molto selettivo, per l'ammissione bisognava superare un difficile esame, ed ogni candidato aveva a disposizione solo due tentativi.
Galois nel giugno del 1828, senza aver seguito classi preparatorie speciali ed un anno prima del consueto, tentò l'esame d'ammissione, ma non riuscì a superare la prova. Amareggiato ma non vinto, decise di ritentare l'anno successivo, così, nel frattempo, fece ritorno al *Louis-le-Grand.* Lo attendevano le lezioni di un eccellente docente di matematica, Louis-Paul-Emile Richard (1795-1849).

L'incontro con Richard fu uno dei più felici della vita di Évariste, che finalmente aveva trovato un interlocutore in grado di condividere i suoi entusiasmi e capire le sue ambizioni.
Richard comprese subito l'enorme potenziale di Galois, su di lui affermò: *"questo studente lavora solo nei regni più elevati della matematica"*, e lo incoraggiò molto, tanto che nel 1829, su sua intercessione, Évariste pubblicò sugli *Annales de Mathématiques pures et appliquées* un suo lavoro sulle frazioni continue periodiche, *Démonstration d'un théorème sur les fractions continues périodiques.*

Nello stesso anno, Galois stava già lavorando alla teoria delle equazioni algebriche con metodi originali, elaborando nuovi concetti che anch'egli comprendeva avrebbero rivoluzionato l'Algebra.
Anche per tale impresa l'entusiasmo di Évariste era sostenuto e alimentato da Richard.
Il risultato di questo periodo di esaltazione di Galois fu la stesura di due memorie, che secondo Richard dovevano essere giudicate con urgenza direttamente dall'*Académie des sciences*, quindi, anziché passare per vie burocratiche, il professore del *Louis-le-Grand* contattò direttamente Augustin-Louis Cauchy (1789-1857) affinché presentasse i lavori di Galois durante una seduta della commissione.

Non si sa bene che cosa successe alle memorie presentate da Galois, a riguardo esistono diverse ricostruzioni secondo le quali Cauchy avrebbe perduto, dimenticato o addirittura deliberatamente distrutto i manoscritti.

Una delle ricostruzioni riguardo tale vicenda vuole che Cauchy non le avesse più presentate all'*Académie* e che, resosi conto della loro importanza, avesse convinto Galois a condensare e chiarire i risultati delle sue ricerche in un'unica memoria da presentare al *Gran Prix de Mathèmatiques*, indetto dalla stessa *Académie* nel 1828.

Galois, infatti, partecipò a tale competizione; tuttavia la sfortuna volle che questa volta il suo manoscritto fosse preso, senza un valido motivo, da Jean-Baptiste-Joseph Fourier (1768 -1830), membro permanente dell'*Académie*, e portato a casa sua.
Dopo qualche settimana Fourier morì e la memoria di Évariste non fu mai ritrovata, così il suo nome venne depennato dalla competizione.

Nel frattempo, nel luglio del 1829, pochi giorni dopo il tragico evento del suicidio del padre, Évariste

fallì per la seconda volta l'esame d'ammissione all'*École Polytechnique*, esaurendo definitivamente tutti i tentativi che aveva a disposizione.
L'aneddoto del suo esame è diventato iconico: gli fu chiesto di esporre la teoria dei logaritmi, ma la sua presentazione essendo un lavoro originale, non seguiva la tradizionale linea argomentativa dei testi didattici del momento. Questo suscitò il disappunto degli esaminatori e ne nacque un diverbio acceso, tant'è che alla fine Galois, esasperato e convinto di avere ragione, tirò il cancellino della lavagna ad uno dei due docenti.

La mancata ammissione all'*École Polytechnique* l'obbligò a ripiegare sulla meno desiderata *École Préparatoire*, cui si iscrisse all'inizio del 1830.

2.4.1 Louis-Paul-Emile Richard

Louis-Paul-Emile Richard nacque il 31 marzo 1795 a Rennes, in Francia. Primogenito di un tenente colonnello che aveva combattuto con onore nelle armate della Repubblica e dell'Impero, egli non aveva potuto seguire le orme paterne a causa di un incidente, avvenuto quand'era solo ragazzo, che gli provocò una piccola infermità permanente.
Fu così costretto, con enorme vantaggio della scienza, a ripiegare verso l'altra sua grande passione, la matematica, diventando insegnante.

Iniziò la sua carriera nel 1814 come *maitre d'étude* presso il liceo imperiale di *Douai*, per poi passare l'anno dopo al collegio reale di *Pontivy*, dove nel 1816 divenne professore di *Mathématiques spéciales*. Dal 1820 si trasferì a Parigi, come insegnante di *Mathématiques élémentaires*, dapprima al collegio *Saint-Louis*, poi al *Louis-le-Grand*, dove riottenne la cattedra di *Mathématiques spéciales*.

Richard era un docente dotato di eccezionali capacità didattiche, molti giovani che entrarono all'*École Polytechnique* lo dovettero a lui.
Di natura era timido e schivo, ma disposto a qualunque sacrificio nell'interesse dei suoi allievi verso i quali era sempre molto generoso. Tra i suoi studenti, e non è un caso, si trovano nomi famosi: oltre a Galois fu docente di Urbain Le Verrier (1811-1877), Charles Hermite (1822-1901) e Joseph-Alfred Serret (1829-1885).
Per i suoi meriti nel campo dell'istruzione pubblica fu decorato nel gennaio del 1837.

Morì a Parigi l'11 marzo 1849, all'età di cinquantatre anni, e nonostante fosse stato solo un insegnante di liceo, la sua notorietà era tale che ricevette l'onore di un necrologio nei *Nouvelles Annales de Mathématiques*.

Sebbene fosse stato incoraggiato insistentemente dai suoi amici e colleghi a pubblicare manuali basati sui suoi insegnamenti, Richard si rifiutò sempre e non pubblicò mai nulla.

2.5 Gli anni all'École Normale

Nel 1794, alla stessa commissione che fu incaricata di realizzare l'*École Polytechnique*, fu dato anche il compito di fondare un'altra scuola, sempre di alto livello, per la preparazione degli insegnanti nei collegi. Nacque così il 30 ottobre dello stesso anno l'*École Normale*.

La scuola aveva lo scopo di rifondare il sistema educativo francese per garantire un insegnamento di base omogeneo per tutti. I corsi tenuti all'*École Normale* riguardavano l'insieme delle scienze e delle materie umanistiche. Per quanto riguarda le scienze molti corsi furono tenuti dagli stessi illustri docenti che prestavano servizio anche all'*École Polytechnique*.

Purtroppo già nel maggio del 1795 venne chiusa, per poi essere rifondata da Napoleone il 17 marzo del 1808; tuttavia anche questa seconda avventura ebbe termine, infatti l'8 settembre 1822 l'istituto fu chiuso perchè considerato un focolaio di idee repubblicane.
Il 9 marzo 1826 venne istituita l'*École Préparatorie* nei locali del Liceo *Louis-le-Grand*, questa era di stampo prettamente filo-monarchico e prevedeva due anni di corsi e consentiva di accedere all'insegnamento nei collegi.
In seguito alla Rivoluzione di luglio l'*École Préparatoire*, per decreto del nuovo re Luigi Filippo, prese il nome di *École Normale*, riallacciandosi all'esperienza del 1794.

La scelta di Galois di ripiegare sull'*École Préparatoire* fu dettata anche dal fatto che la sua frequentazione gli avrebbe garantito un sussidio. Infatti, dopo la morte del padre la situazione economica familiare non era affatto rosea.
Il 20 febbraio 1830 Évariste firmò il documento con il quale si impegnava a rimanere per 10 anni al servizio dell'istruzione pubblica.

All'*École Préparatoire* Galois fece la conoscenza di Auguste Chevalier, che ebbe su lui un'influenza rilevante, infatti attraverso le sue accalorate discussioni gli trasmise la passione per la politica.
Chevalier era un convinto seguace del *sansimonismo*, la teoria ispirata alle idee di Claude-Henry de Rouvroy Conte di Saint-Simon (1760-1825).
Tale dottrina venne esposta e sviluppata in un'opera collettiva apparsa nel 1830, *"Exposition de la doctrine de Saint-Simon"*, nella quale si può vedere come questa corrente politica contenesse il germe del socialismo che sarebbe nato pochi anni dopo.

Durante *"Le Trois Glorieuses"*, Galois e gli altri studenti dell'*École Normale* furono costretti a seguire gli avvenimenti segregati nell'istituto. Infatti, il direttore della scuola, Guigniault, aveva impedito ai ragazzi di lasciare la struttura, sbarrando tutte le porte che davano sulla strada, e ricordando loro che a seguito del contratto decennale firmato erano già dei funzionari dello Stato. Inoltre, se ciò non fosse bastato, avrebbe chiesto l'intervento della gendarmeria per evitare di mescolare i suoi studenti con i rivoltosi.
L'ipocrisia di Guigniault nei confronti del popolo francese non si limitò alle giornate di scontri; infatti, successivamente alla caduta di Carlo X, egli si dichiarò convinto sostenitore della rivolta e aggiunse che avrebbe messo a disposizione del Governo Provvisorio sia se stesso che i suoi studenti.

Tale atteggiamento fece indignare il giovane matematico, che si pose l'obiettivo di portare a galla la viltà e l'opportunismo di Guigniault.
Per questo nel dicembre dello stesso anno uscì una lettera su *"La Gazette des Écoles"*, nota rivista dedicata agli studenti, nella quale si dichiarava:

"[...] Ho pensato che avreste accolto con sollecitudine ogni mezzo per smascherare quest'uomo [Guigniault]. Ecco i fatti che possono essere attestati da 46 studenti. Il 28 luglio, al mattino, desiderando parecchi allievi dell'École Normale andare sulla linea del fuoco, il sign. Guigniault disse

loro, a due riprese, che avrebbe potuto chiamare la gendarmeria per ristabilire l'ordine nella scuola. La gendarmeria il 28 luglio! [...] Ecco l'uomo che l'indomani ombreggiò il suo cappello con una coccarda tricolore." ([4] pagine 76-77)

La rivista aggiunse in una nota che era stata una loro decisione togliere la firma dell'autore, nonostante esso non ne avesse fatto richiesta.

L'articolo suscitò l'ira di Guigniault, che interrogò riguardo l'accaduto tutti gli studenti dell'École Normale.
Tutti i compagni di Galois smentirono il loro coinvolgimento, mentre egli, nonostante non avesse affermato di essere l'autore, non lo negò nemmeno, infatti la sua risposta fu: *"Signor direttore, io non credo di poter rispondere a questa domanda, perchè sarebbe contribuire a denunciare uno dei nostri compagni."* ([4] pagina 80)
Pur non avendo nessuna prova concreta della colpevolezza di Galois, Guigniault colse l'occasione per sbarazzarsi della sua presenza tanto indesiderata.

Nel frattempo, la sua adesione alla causa repubblicana era cresciuta al punto che fosse solito affermare con amici e parenti: *"se sapessi che basta un corpo per incitare il popolo alla rivolta, offrirei il mio."* ([4] pagina 70)

In questi anni, Galois, ampliò anche il suo giro di amicizie con la frequentazione di giovani repubblicani ai quali si sentiva legato per la comunanza di ideali. Inoltre aderì alla *Société des Amis du Peuple*, gruppo che riuniva i più attivi e violenti sostenitori del partito repubblicano, definiti dalla stampa di regime come soggetti particolarmente pericolosi per l'incolumità dei cittadini.
Tale società possedeva anche un'organizzazione armata sotto la copertura dell'artiglieria della Guardia Nazionale.
Il primo gesto che fece dopo l'espulsione fu proprio quello di arruolarsi in tale battaglione.

Galois aveva anche un altro progetto per la testa: organizzare un corso di Algebra avanzata dove rendere pubblici i risultati delle sue memorie.
Egli non temeva, anzi non era proprio interessato, al fatto che qualcuno potesse "rubargli" le scoperte, infatti per Évariste la scienza era patrimonio di tutti.
Così scelse di pubblicare un annuncio su *La Gazette Des Écoles* per raggiungere quanti più interessati.

L'annuncio destò l'interesse di Siméon-Denis Poisson, che proprio in quei giorni chiese al giovane matematico un'ulteriore copia delle sue ricerche per presentarla, per la terza volta, all'*Académie des sciences*. Galois, inizialmente titubante, scrisse nuovamente la memoria e l'*Académie* incaricò Lacroix e Poisson stesso di esaminarla.

Il corso di Algebra avanzata non ebbe il successo da lui sperato: gli argomenti trattati risultarono incomprensibili ai suoi "alunni", così come i suoi metodi e le sue parole. In breve tempo più nessuno seguì le sue lezioni.

2.5.1 Sull'insegnamento della scienza

Il 2 gennaio 1831 Galois pubblicò, sempre, su *"La Gazette des Écoles"* una lettera relativa all'insegnamento della scienza in Francia.

Évariste denunciava le modalità poco chiare di assunzione dei docenti, scelti più in base alle loro simpatie e opinioni politiche che per merito: *"Anzitutto nelle scienze le opinioni contano per niente [...] Io mi chiedo se un professore è buono o scadente, e mi preoccupo molto poco del suo modo di pensare su argomenti estranei ai suoi studi scientifici. Non era dunque senza dolore e indignazione che, sotto il governo della Restaurazione, si vedevano i posti diventare preda dei migliori offerenti in fatto di idee monarchiche e religiose. Questo stato di cose non è cambiato; la mediocrità... è ancora privilegiata."* ([4] pagine 85-86)

La lettera continuava con critiche rivolte al metodo di insegnamento della matematica; in particolare, Galois era molto perplesso verso il limitare i ragazzi al solo ascolto e alla sola ripetizione dei concetti a discapito dell'imparare a ragionare, per Évariste "il ragionamento doveva diventare una seconda memoria".

"Fino a quando i poveri giovani saranno obbligati ad ascoltare o a ripetere tutto il giorno? Quando si lascerà il tempo per meditare su questo ammasso di conoscenze, per coordinare questa folla di proposizioni sconnesse, di calcoli senza nesso? Non ci sarebbe qualche vantaggio a esigere dagli studenti gli stessi metodi, gli stessi calcoli, le stesse forme di ragionamento, se fossero allo stesso tempo i più semplici e i più fecondi? Ma no, si insegnino minuziosamente teorie tronche e cariche di riflessioni inutili, mentre si tralasciano le proposizioni più semplici e più brillanti dell'algebra; invece... si dimostrano con grande fatica calcoli e ragionamenti sempre lunghi, qualche volta falsi, corollari la cui dimostrazione viene da sé." ([4] pagine 86)

Non mancavano accuse anche agli editori dei manuali: *"Da dove viene il male? [...] I librai vogliono grossi volumi: più cose ci sono nelle opere degli esaminatori, più sono sicuri di una vendita fruttuosa; ecco perché vediamo apparire ogni anno queste voluminose compilazioni dove si vedono i lavori travisati dei grandi maestri accanto a saggi dello scolaro."* ([4] pagine 86-87)

Infine, nella lettera sono anche presenti delle considerazioni riguardo il modo di esaminare i ragazzi, con particolare riferimento agli esami d'ammissione all'*École Polytechnique*: *"Perché gli esaminatori pongono le domande in maniera ingarbugliata? Sembrerebbe che temano di essere capiti da quelli che interrogano; da dove viene questa disgraziata abitudine di complicare le domande con difficoltà artificiose?"* ([4] pagina 87)

SUR L'ENSEIGNEMENT DES SCIENCES.

Des Professeurs. — Des Ouvrages. — Des Examinateurs.

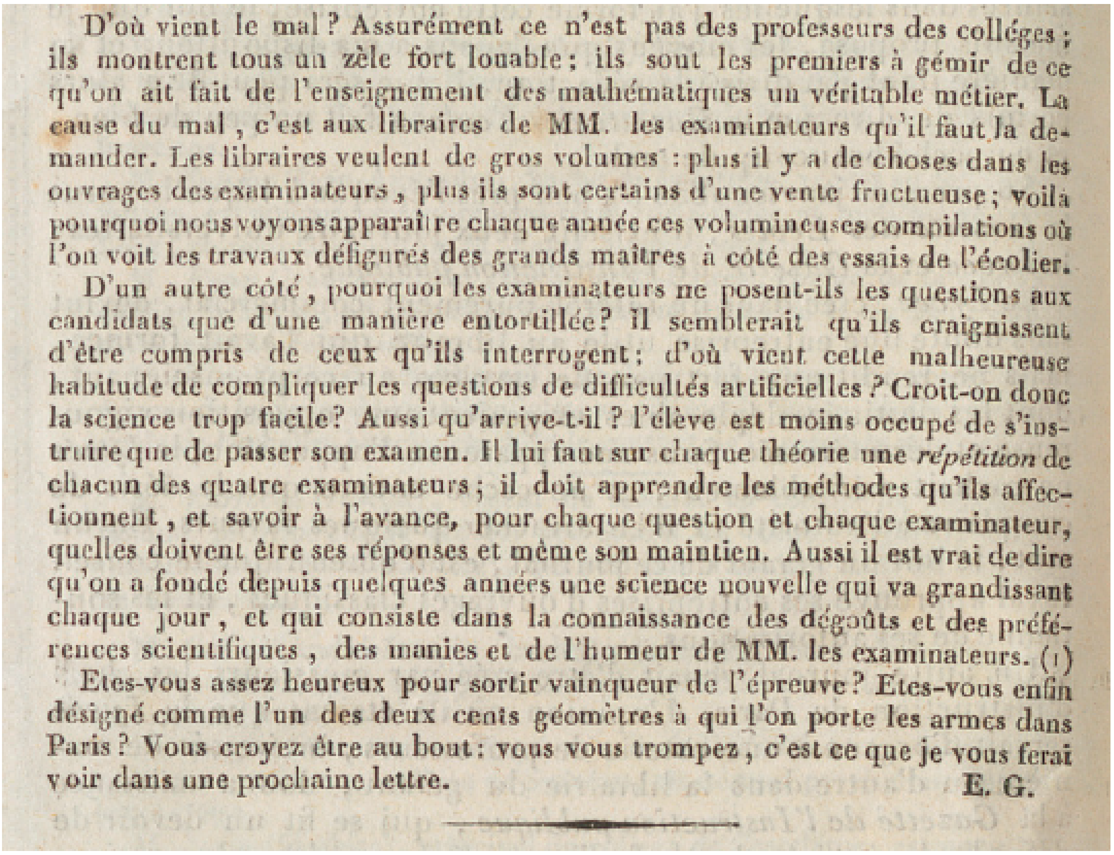
Monsieur le rédacteur,

Je vous serais obligé, si vous vouliez bien accueillir les réflexions suivantes, relatives à l'étude des mathématiques dans les colléges de Paris.

D'abord dans les sciences les opinions ne comptent pour rien; les places ne sauraient être la récompense de telle ou telle manière de voir en politique ou en religion. Je m'informe si un professeur est bon ou mauvais, et je m'inquiète fort peu de sa façon de penser dans des matières étrangères à ses études scientifiques. Ce n'était donc pas sans douleur et indignation que, sous le gouvernement de la restauration, on voyait les places devenir la proie des plus offrants en fait d'idées monarchiques et religieuses. Cet état de choses n'est pas changé; la médiocrité, qui fait preuve de sa répugnance pour le nouvel ordre de choses, est encore privilégiée; et cependant les opinions ne devraient pas être mises en ligne de compte, lorsqu'il s'agit d'apprécier le mérite scientifique des individus.

Commençons par les colléges; là les élèves de mathématiques se destinent pour la plupart à l'école polytechnique; que fait-on pour les mettre en état d'atteindre ce but? Cherche-t-on à leur faire concevoir le véritable esprit de la science par l'exposé des méthodes les plus simples? Fait-on en sorte que le raisonnement devienne pour eux une seconde mémoire? N'y aurait-il pas au contraire quelque ressemblance entre la manière dont ils *apprennent* les mathémathiques et la manière dont ils *apprennent* les leçons de français et de latin? Jadis un élève aurait appris d'un professeur tout ce qui lui est utile de savoir; maintenant il faut le supplément de un, de deux répétiteurs pour préparer un candidat à l'école polytechnique.

Jusques à quand les pauvres jeunes gens seront-ils obligés d'écouter ou de répéter toute la journée? Quand leur laissera-t-on du temps pour méditer sur cet amas de connaissances, pour coordonner cette foule de propositions sans suite, de calculs sans liaison? N'y aurait-il pas quelque avantage à exiger des élèves les mêmes méthodes, les mêmes calculs, les mêmes formes de raisonnement, s'ils étaient à la fois les plus simples et les plus féconds? Mais non, on enseigne minutieusement des théories tronquées et chargées de réflexions inutiles, tandis qu'on omet les propositions les plus simples et les plus brillantes de l'algèbre; au lieu de cela, on démontre à grands frais de calculs et de raisonnements toujours longs, quelquefois faux, des corollaires dont la démonstration se fait d'elle-même.



D'où vient le mal ? Assurément ce n'est pas des professeurs des colléges ; ils montrent tous un zèle fort louable ; ils sont les premiers à gémir de ce qu'on ait fait de l'enseignement des mathématiques un véritable métier. La cause du mal, c'est aux libraires de MM. les examinateurs qu'il faut la demander. Les libraires veulent de gros volumes : plus il y a de choses dans les ouvrages des examinateurs, plus ils sont certains d'une vente fructueuse ; voilà pourquoi nous voyons apparaître chaque année ces volumineuses compilations où l'on voit les travaux défigurés des grands maîtres à côté des essais de l'écolier.

D'un autre côté, pourquoi les examinateurs ne posent-ils les questions aux candidats que d'une manière entortillée ? Il semblerait qu'ils craignissent d'être compris de ceux qu'ils interrogent ; d'où vient cette malheureuse habitude de compliquer les questions de difficultés artificielles ? Croit-on donc la science trop facile ? Aussi qu'arrive-t-il ? l'élève est moins occupé de s'instruire que de passer son examen. Il lui faut sur chaque théorie une *répétition* de chacun des quatre examinateurs ; il doit apprendre les méthodes qu'ils affectionnent, et savoir à l'avance, pour chaque question et chaque examinateur, quelles doivent être ses réponses et même son maintien. Aussi il est vrai de dire qu'on a fondé depuis quelques années une science nouvelle qui va grandissant chaque jour, et qui consiste dans la connaissance des dégoûts et des préférences scientifiques, des manies et de l'humeur de MM. les examinateurs. (1)

Etes-vous assez heureux pour sortir vainqueur de l'épreuve ? Etes-vous enfin désigné comme l'un des deux cents géomètres à qui l'on porte les armes dans Paris ? Vous croyez être au bout : vous vous trompez, c'est ce que je vous ferai voir dans une prochaine lettre.

E. G.

Figura 3: Sull'insegnamento delle scienze, *La Gazette des Écoles*, 2 gennaio 1831

2.6 Guai con la giustizia

Il 31 dicembre 1830 Luigi Filippo decretò lo scioglimento della Guardia Nazionale. Le batterie di repubblicani rifiutarono di lasciarsi disarmare e diciannove di essi furono arrestati per questo gesto di ribellione.
In aprile ebbe inizio il loro processo, che fu seguito con grande interesse da un'enorme folla che li acclamava. La vicenda giudiziaria si concluse con l'assoluzione degli imputati, che vennero accolti come eroi all'uscita del tribunale.

Per festeggiare la sentenza la *Société des Amis du Peuple* organizzò un pranzo, che si tenne il 9 maggio, per gli artiglieri rilasciati.
Al fine di evitare le provocazioni della polizia erano stati preparati anticipatamente dei brindisi, ma con il procedere del banchetto divennero incontrollati.

Ad un tratto si alzò in piedi Galois, in una mano reggeva un bicchiere colmo di vino e nell'altra un coltello a serramanico, e brindò: *"A Luigi Filippo!"* ([4] pagina 93). La maggioranza dei presenti lo imitò, ma alcuni, spaventati dalle possibili conseguenze, scapparono. Il pranzo si concluse nel disordine.

Il giorno successivo la polizia lo arrestò con l'accusa di incitamento ad un attentato contro la vita del re; fu condotto al carcere di *Sainte-Pelagie*.
Al processo Évariste affermò che le parole del brindisi erano state travisate: *"Alzai quel coltello dicendo "A Luigi Filippo, se tradisce!". Queste parole sono state udite solo dai miei vicini, dati i fischi che aveva suscitato la prima parte della frase, perché si credeva che io brindassi alla salute di Luigi Filippo."* ([4] pagina 94).
I testimoni chiamati da Galois sostennero la sua versione; pertanto egli venne assolto.

Il 14 luglio 1831 la Francia celebrava la Presa della Bastiglia. I membri del partito repubblicano organizzarono una manifestazione patriottica; coloro che avevano fatto parte della Guardia Nazionale erano invitati a partecipare in uniforme, nonostante essa fosse stata resa illegale perchè ritenuta oltraggiosa verso il regime.
Il corteo fu interrotto dalla polizia che fece disperdere i manifestanti e ne arrestò alcuni, tra cui Galois.

Al momento dell'arresto, egli indossava l'uniforme della Guardia Nazionale, come da programma, e aveva con sé diverse armi, questo diede un buon pretesto per incriminarlo. Verso sera Évariste fu condotto nuovamente a *Sainte-Pélagie*.
Il nuovo processo ebbe inizio solo il 23 ottobre, l'accusa era di porto illegale di uniforme e di armi proibite. Galois fu condannato a 9 mesi.

In carcere, il giovane matematico, tentò anche il suicidio ed ebbe l'ulteriore amarezza di ricevere dal segretario dell'*Académie*, François Arago (1786-1853), 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." [5] pagina 96)

Nella primavera del 1832 scoppiò in Francia un'epidemia di colera. A *Sainte-Pélagie*, come in tutto il Paese, si presero misure per limitare il contagio e i morti; i detenuti più giovani e quelli più

deboli furono trasferiti.
Il 16 marzo 1832, Galois venne mandato in una casa di salute, in qualità di prigioniero sulla parola.

Il trasferimento nella clinica portò nella vita del giovane matematico una grande novità: conobbe Stéphanie, la figlia di uno dei medici, e se ne innamorò.
Cosa ci fu tra i due non è possibile ricostruirlo con precisione, ma da alcuni frammenti delle lettere che si scambiarono, si è ipotizzato che in un primo momento Galois avesse pensato che la ragazza ricambiasse i suoi sentimenti, oppure che la stessa Stéphanie avesse incoraggiato il suo amore.
Tuttavia, dopo che Évariste si dichiarò apertamente, la ragazza lo rifiutò.

Galois terminò la sua pena il 29 aprile del 1832.

2.6.1 Prefazione alle memorie

Durante il periodo di detenzione Galois approfondì le sue ricerche matematiche e nell'ottobre del 1831 scrisse per le sue memorie, *Sulle condizioni di risolubilità delle equazioni per radicali* e *Delle equazioni primitive che sono risolubili per radicali*, una prefazione, che conteneva una forte accusa contro la cultura scientifica del suo tempo.

"Innanzitutto, il secondo foglio di quest'opera non è ingombro dei cognomi, nomi, qualità, dignità ed elogi di qualche principe avaro. [...] Non ci si vede neanche, in caratteri grossi tre volte il testo, un omaggio rispettoso a qualche alta posizione nelle scienze, a uno scienziato protettore, cosa tuttavia indispensabile (stavo per dire inevitabile) per chiunque a vent'anni voglia scrivere. Non dico a nessuno che devo ai suoi consigli o ai suoi incoraggiamenti tutto ciò che c'è di buono nella mia opera. Non lo dico: perché sarebbe mentire. Se avessi da aggiungere qualcosa ai grandi del mondo o ai grandi della scienza (e coi tempi che corrono la distinzione è impercettibile tra queste due classi di persone), giuro che non sarebbero affatto ringraziamenti. Io devo agli uni di far comparire così tardi la mia prima delle due memorie, agli altri di aver scritto il tutto in prigione." ([4] pagine 113-114)

Galois riconobbe alcuni difetti nell'esposizione del suo lavoro ed era consapevole che la sua opera, almeno inizialmente, non sarebbe stata capita e avrebbe potuto suscitare risa e scherno:

"Tutto concorre dunque a farmi pensare che nel mondo scientifico l'opera che sottopongo al pubblico sarà ricevuta con il sorriso della compassione. [...] E' coscientemente che mi espongo allo scherno degli stolti." ([4] pagine 115-116)

Consapevole dell'incompletezza della sua teoria, Galois sperava che il proprio manoscritto potesse capitare in futuro tra le mani di chi fosse stato in grado di capirlo ed eventualmente completarlo.

"[...] nella speranza che queste ricerche potranno capitare nelle mani di persone a cui una boria stupida non ne impedirà la lettura, e dirigerle nella nuova via che deve, secondo me, seguire l'analisi dei suoi rami più alti." ([4] pagina 116)

2.7 La morte di Galois

Dopo un mese dal suo rilascio, il 30 maggio 1832, Galois fu ferito gravemente allo stomaco in un duello sulle cui motivazioni vi sono tre versioni differenti. Secondo alcuni si sarebbe trattato di un duello per vendicare l'onore di Stéphanie, con cui Galois avrebbe avuto una relazione; per altri l'uccisore di Évariste sarebbe stato un infiltrato del re, che avrebbe avuto l'incarico di provocarlo in un duello per eliminarlo. La ricostruzione, ad oggi più attendibile, è la seguente.

Durante i primi di maggio del 1832 era ritornata in Francia Marie-Caroline, duchessa di Berry, vedova del figlio di Carlo X, che al momento dell'uccisione del marito era, all'insaputa di tutti, incinta.
Tra i monarchici si creò una frattura tra chi vedeva il re Luigi Filippo come un usurpatore e chi invece lo sosteneva.

I repubblicani raccolti nella *Société des amis du Peuple* intendevano sfruttare le difficoltà del sovrano per organizzare un'insurrezione. Venne indetta un'assemblea per il 7 maggio, alla quale fu invitato anche Galois.
Per questo scopo occorreva trovare un'occasione per radunare una folla considerevole ed un motivo per catalizzarne gli umori contro il re. Qualcuno dei presenti osservò che un cadavere eccellente, la cui morte potesse essere utilizzata come pretesto per sollevare la folla, avrebbe facilitato il compito.
Fu a questo punto che Galois si sarebbe proposto come vittima sacrificale. Egli spiegò brevemente che la sua vita non aveva più senso di essere vissuta, era stato tradito dalle sue più grandi passioni: Stéphanie e la matematica; non gli restava che il suo amore per la Francia, libera dall'oppressione della monarchia. Il cadavere che cercavano sarebbe stato il suo.
Egli seppe convincere le resistenze dei presenti e fu stabilito che Galois si sarebbe lasciato uccidere in un duello. Per essere certo di morire, solo la pistola dello sfidante sarebbe stata carica.
Alla *Société* restava il compito di organizzare il depistaggio, incolpando la polizia segreta di Luigi Filippo dell'assassinio di Évariste.

Nelle ultime ore prima del duello, è molto probabile che Galois avesse avuto un profondo rimpianto per quello che non era stato tra lui e la matematica. Tante idee, alcune ancora non ben formulate gli ronzavano nella testa, così riassunse brevemente la memoria presentata all'*Académie* e vi aggiunse altri nuovi teoremi e congetture.
A conclusione dell'esposizione scrisse con rammarico: *"Mi manca il tempo e le mie idee non sono sufficientemente sviluppate su questo campo, che è immenso."* ([4] pagina 129)

Inviò il suo lavoro, insieme ad una lettera d'addio, all'amico fidato Chevalier. In quest'ultima lo supplicò: *"Chiedi pubblicamente a Jacobi e a Gauss di esprimere il loro parere non sulla verità, ma sull'importanza di questi teoremi."* ([4] pagina 129)

Il 30 maggio, come da programma, Galois si presentò nei pressi dello stagno Glacière per il duello. Fu ferito all'addome, ma non morì subito.
Non si sa chi trovò Évariste agonizzante, tuttavia verso le 9 del mattino fu trasportato all'ospedale Cochin, qui fu raggiunto da suo fratello Alfred, al quale Évariste disse che il suo feritore apparteneva alla polizia del re. Il 31 maggio morì a causa del sopravvento di una peritonite acuta.

I funerali furono fissati per il 2 giugno. Al momento dell'inizio della cerimonia, però, 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, ma, terminata l'avventura napoleonica, era stato un esponente di spicco dell'opposizione parlamentare ai Borbone. Dunque una figura molto più grande del povero Galois.

La ragione politica imponeva di ritardare la manifestazione antigovernativa rispetto ai funerali di Lamarque dove, era facile prevedere, sarebbe accorsa molta più gente.
L'estremo saluto al generale, avvenuto il 3 giugno, è ricordato come la più imponente manifestazione popolare contro il regime di Luigi Filippo. La morte di Galois era stata inutile.

La memoria che l'*Académie* aveva più volte respinto fu pubblicata 14 anni dopo la sua morte, grazie al lavoro del fratello Alfred e di Chevalier, che ricopiarono i manoscritti e li inviarono a diversi celebri matematici. Solo Joseph Liouville (1809-1882) nel 1846 ne comprese il valore; tuttavia nel presentare il lavoro di Galois, si espresse così a riguardo del suo stile:

"La causa di questo fallimento fu uno smodato desiderio di concisione che occorre invece evitare soprattutto 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. [...] noi comprendiamo come degli illustri geometri abbiano ritenuto conveniente tentare di ricondurre 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." ([3] pagina 381)

3 Scritti Matematici

Comprendere gli scritti di Galois è davvero una sfida non da poco, tant'è che per afferrare completamente il senso del solo *Mémoire sur les conditions de résolubilité des équations par radicaux*, il suo scritto più noto, è servito quasi un secolo di studio da parte dei massimi algebristi del XIX secolo.

Galois è ben consapevole che possa risultare poco chiaro, infatti in un passaggio del *Discours préliminaire* al *Mémoire* del 7 ottobre del 1830 afferma:

"Lo scopo che ci si è proposti è quello di determinare dei caratteri per la risolubilità delle equazioni per radicali. Possiamo affermare che non esiste nell'analisi pura una materia più oscura e forse più isolata da tutto il resto. La novità di questa materia ha reso necessari nuove denominazioni, nuovi caratteri. Non dubitiamo che questo inconveniente scoraggerà fin dai primi passi il lettore che perdona a malapena agli stessi autori che hanno tutto il possibile credito di parlargli un nuovo linguaggio, ma comunque siamo stati obbligati a conformarci alla necessità dell'argomento, la cui importanza richiede senza dubbio qualche attenzione." ([2] pagina 9)

Dal *Mèmoire* è nata la teoria di Galois, che ha portato con sè la creazione di nuovi concetti, tra i più importanti troviamo quello di *gruppo* e quello di *campo*. Questi nuovi strumenti sono stati chiariti e sviluppati attraverso il lavoro di diversi algebristi durante tutto il XIX e il XX secolo.
Questi due elementi hanno permesso di ampliare lo studio dell'algebra introducendo un nuovo punto di vista relativo allo studio di *strutture*, intese come schemi logici comuni che possono essere formati da elementi della più disparata natura.

Tali passaggi ci hanno condotto all'algebra *astratta* o *assiomatica*. Astratta perchè non ci interessa conoscere la natura degli oggetti con i quali operiamo, assiomatica perchè è costruita dagli assiomi posti a suo fondamento.

3.1 La ricezione della teoria di Galois nelle Università

Il primo studioso che si cimentò nella comprensione degli scritti di Galois fu Joseph Liouville (1809-1882), il quale curò la pubblicazione non solo del *Mèmoire* ma anche delle altre opere.

Fu l'italiano Enrico Betti (1832-1892) il primo a realizzare uno studio in qualche modo significativo sulla memoria di Évariste, nel 1851 pubblicò una nota *Sopra la risolubilità per radicali delle equazioni irriduttibili di grado primo* sulla rivista *Annali di Scienze matematiche e fisiche*; l'anno successivo, sempre sulla stessa rivista, presentò una lunga memoria dal titolo *Sulla risoluzione delle equazioni algebriche*, nella quale affermava di aver migliorato e sviluppato la teoria di Galois. In realtà i meriti di Betti sono stati sovrastimati, viste anche le diverse inesattezze presenti nel suo lavoro: egli utilizzava con troppa leggerezza il termine gruppo, con il quale indicava sia insiemi che gruppi veri e propri; tale ambiguità lo portò addirittura a confondere il concetto di classe laterale con quello di gruppo coniugato. Inoltre, non considerava la sostituzione identica come una vera sostituzione, concludendo che: *Affinché un'equazione sia risolta è necessario e sufficiente che il suo gruppo non contenga più nessuna sostituzione.* ([2] pagina 10)

Fu Richard Dedekind (1831-1918) ad organizzare il primo corso universitario sulla teoria di Galois, tenuto negli anni accademici 1856-57 e 1857-58 presso l'Università di Gottinga. Il testo delle sue lezioni riguardo i gruppi di sostituzioni rappresentava un'opera di eccezionale chiarezza. Dedekind definì che cosa fossero una sostituzione e il prodotto tra sostituzioni, e osservò che nell'insieme delle sostituzioni esisteva sempre *"quella con la quale nessun elemento viene cambiato"*, ovvero la sostituzione identità.
Passò poi a dimostrare la proprietà associativa del prodotto tra sostituzioni:

Proposizione 1. *Sia* $\theta \cdot \theta' = \phi$, $\theta' \cdot \theta'' = \psi$, *allora è* $\phi \cdot \theta'' = \theta \cdot \psi$ *o, più brevemente,* $(\theta \cdot \theta') \cdot \theta'' = \theta \cdot (\theta' \cdot \theta'')$

Segue un'altra proposizione:

Proposizione 2. *Comunque si scelga una coppia di equazioni delle tre* $\phi = \theta$, $\phi' = \theta'$, $\phi \cdot \phi' = \theta \cdot \theta'$, *segue sempre la terza*

Dedekind considerava queste due proposizioni fondamentali e affermò che tutti i risultati successivi dipendevano da queste e dalla finitezza del numero di sostituzioni; quindi arrivò ad afferrare, ma non formalizzò, il concetto di *gruppo finito*.

Purtroppo le lezioni di Dedekind rimasero incomplete proprio nella parte relativa alla finalità della teoria di Galois; infatti in queste non compariva la condizione di risolubilità per radicali di un'equazione di grado n.

Oltre a Dedekind anche il matematico norvegese Ludwig Sylow (1832-1918) tenne un corso universitario sulla teoria di Galois nell'anno accademico 1862-63 presso l'Università di Christiania, in Norvegia. Sylow, come Dedekind, interruppe le sue lezioni prima di introdurre le condizioni di risolubilità per radicali delle equazioni di grado n.
Per quanto riguarda l'Italia, il primo a portare tale teoria tra i banchi universitari fu Cesare Arzelà (1847-1912), nell'anno accademico 1866-67 presso l'Università di Bologna.

Alla fine del XIX secolo la teoria di Galois ebbe finalmente ampia diffusione negli ambienti accademici, con il proliferare di diversi trattati e corsi; tra questi uno di quelli che ebbe maggior fortuna fu quello tenuto da Felix Klein (1849-1925) all'Università di Gottinga nel 1886.

Tornando al nostro Paese, fu Alfredo Capelli (1855-1910) a riaccendere l'interesse sulla teoria dei gruppi con la pubblicazione di diverse memorie. Nell'anno accademico 1896-97 alla Scuola Normale Superiore di Pisa, Luigi Bianchi (1856-1928) tenne un corso sulla teoria di Galois che presentava diversi elementi originali. Anche in questo caso le sue dispense divennero un trattato dal titolo *Lezioni sulla teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo Galois*. Tale opera ha rappresentato e rappresenta, poichè ancora oggi viene citata, un vero e proprio punto di riferimento non solo per l'algebra italiana, ma anche per quella estera; la sua peculiarità sta nel fornire prove a tutte le congetture che ancora non erano state avvalorate.

Chi invece si avventurò con successo nel cercare di districare le riflessioni e le ispirazioni di Galois fu Camille Jordan (1838-1922). Jordan fu molto affascinato dagli scritti di Évariste e realizzò a partire da essi, oltre che la sua tesi di laurea, anche varie opere e commentari, tra i quali ricordiamo il *Commentaire sur Galois* e la sua opera più celebre *Traité des substitutions et des équations algébriques.*

La finalità della teoria di Galois sta nel dimostrare che un'equazione algebrica di grado n, a coefficienti reali o complessi, è risolubile per radicali se e solo se il gruppo ad essa associato è *risolubile.* Per giungere a tale risultato è necessario passare per la *Corrispondenza di Galois*, che, invece, rappresenta il cuore della teoria. Tale concetto è stato chiarito e migliorato nei primi decenni del XX secolo da vari algebristi, tra questi quelli che hanno dato i maggiori contributi furono David Hilbert (1862-1942), Oystein Ore (1889-1968) ed Emil Artin (1898-1962). Attualmente la *Corrispondenza di Galois* rappresenta il legame biunivoco che esiste tra le estensioni di campo e i gruppi di automorfismi.

3.2 Opere Minori

In questa sezione si daranno brevi cenni ai contributi matematici di Galois, pubblicati tra il 1828 ed il 1830 su due prestigiose riviste scientifiche francesi: gli *Annales de Mathématiques pures et appliquées* e il *Bulletin des Sciences mathématiques, astronomiques, physiques et chimiques.*

3.2.1 Dimostrazione di un teorema sulle frazioni continue periodiche

Questo lavoro venne pubblicato sugli *Annales de Mathématiques pures et appliquées*, tra il 1828-29. Galois riprende e sviluppa il lavoro di Joseph Louis Lagrange sulla rappresentazione delle soluzioni di equazioni di secondo grado a coefficienti interi in frazioni continue periodiche.
Pertanto, prima di passare ad analizzare il contributo di Galois, cerchiamo di inquadrare sinteticamente la questione.

Definizione (Frazione Continua)**.** Una frazione continua è un'espressione del tipo

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \dots}}}$$

dove i termini a_i e b_i, finiti o infiniti, possono essere numeri reali o complessi.

Quando $a_0 \in \mathbb{Z}$, tutti gli altri $a_i \in \mathbb{N}$ e per ogni i, $b_i = 1$, allora parliamo di *Frazioni Continue Aritmetiche.*

Una frazione continua aritmetica è *limitata* quando gli a_i sono in numero finito, altrimenti è *illimitata.*

Una frazione continua illimitata è detta *periodica* quando i suoi termini si ripetono da un certo punto in poi; è detta *immediatamente periodica* quando non ha antiperiodo.

Passiamo ora a descrivere il *Metodo di Lagrange*: consideriamo l'equazione

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

con $a_i \in \mathbb{N}$ per ogni i, Lagrange propone la sostituzione $x = \alpha + \frac{1}{y}$, con $\alpha \in \mathbb{N}$. Ora suppone che $P(\alpha) \cdot P(\alpha + 1) < 0$ e che nell'intervallo $]\alpha, \alpha + 1[$ ci sia una sola radice, affinchè il procedimento possa essere iterato ponendo $y = \beta + \frac{1}{z}$, $z = \gamma + \frac{1}{t}, \ldots$

In questo modo la radice cercata può essere espressa dalla frazione continua

$$\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \ldots}}$$

Tale sviluppo prende il nome di *Metodo di Lagrange*, esso ha termine se la radice cercata è razionale, altrimenti prosegue all'infinito.
Lagrange passa poi ad esaminare il suo metodo concentrandosi particolarmente sulle equazioni di secondo grado a coefficienti interi in una sola incognita.

Veniamo ora all'argomento di più nostro interesse: il teorema sulle frazioni continue che Galois formula, ancora diciassettenne, mentre frequentava il Collegio *Louis-Le-Grand* di Parigi:

Teorema. *Se una delle radici di un'equazione di grado qualunque è una frazione continua immediatamente periodica, questa equazione avrà necessariamente un'altra radice ugualmente periodica che si otterrà dividendo l'unità negativa per questa stessa frazione periodica, scritta nell'ordine inverso.* ([2] pagina 33)

Galois propone una dimostrazone pragmatica, che come vedremo è un suo tratto caratteristico, ovvero presenta un esempio ad hoc con una frazione continua immediatamente periodica.

Per fissare le idee, considera solo periodi di quattro termini, affermando che il procedimento uniforme del calcolo assicura che sarebbe lo stesso se ne ammettessimo un numero più grande.
Pertanto, sia una delle radici di grado qualunque espressa nel modo seguente:

$$x = a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \cfrac{1}{a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \ldots}}}}}}}$$

l'equazione di secondo grado cui appartiene questa radice è:

$$x = a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \cfrac{1}{x}}}}.$$

Ora da questa equazione, tramite operazioni algebriche, è possibile ottenere la radice correlata. Infatti, portando al primo membro gli elementi che formano il periodo e considerando il loro reciproco con segno cambiato troviamo la seguente scrittura

$$x = -\cfrac{1}{d + \cfrac{1}{c + \cfrac{1}{b + \cfrac{1}{a - x}}}} \; ,$$

Quindi, sostituendo alla x del secondo membro se stessa, otteniamo una nuova frazione continua:

$$x = -\cfrac{1}{d + \cfrac{1}{c + \cfrac{1}{b + \cfrac{1}{a + \cfrac{1}{d + \cfrac{1}{c + \cfrac{1}{b + \cfrac{1}{a + \ldots}}}}}}}} \; .$$

Ecco quindi la radice correlata che stavamo cercando; questa, come si vede, è uguale a -1 diviso la radice proposta.

Galois, poi, osserva che la radice di partenza è stata scelta maggiore dell'unità, ma ciò non intacca la generalità della dimostrazione; infatti egli la ripercorre una seconda volta considerando il reciproco di tale radice, e mostrando che il risultato ottenuto è in linea con la tesi.

La trattazione continua con l'analisi dei segni e dei valori delle due radici.

"Sia A una frazione continua immediatamente periodica qualunque e sia B la frazione continua che se ne deduce capovolgendo il periodo; si vede che se una delle radici di un'equazione è $x = A$, essa avrà necessariamente un'altra radice $x = -\frac{1}{B}$; ora, se A è un numero positivo maggiore dell'unità, $-\frac{1}{B}$ sarà negativo e compreso tra 0 e -1; e, viceversa, se A è un numero negativo compreso tra 0 e -1, $-\frac{1}{B}$ sarà un numero positivo maggiore dell'unità." ([2] pagina 37)

Galois dà anche un risultato reciproco che permette di restringere il teorema di Lagrange:

"Si può dimostrare che, reciprocamente, se una delle due radici di un'equazione di secondo grado è positiva e maggiore dell'unità e l'altra è compresa tra 0 e -1, queste radici saranno esprimibili in frazioni continue immediatamente periodiche."([2] pagina 37)

Anche in questo caso egli utilizza un esempio paradigmatico: sia $P(x) = ax^2 + bx + c = 0$ una generica equazione di secondo grado, sia A una frazione continua immediatamente periodica che rappresenta la componente periodica della frazione continua dello sviluppo, secondo Lagrange, della radice α di $P(x) = 0$, ossia

$$\alpha = p_1 + \cfrac{1}{p_2 + \cfrac{1}{\dots + \cfrac{1}{A}}}\,, \qquad A = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots + \cfrac{1}{a_n + \cfrac{1}{a_1 + \dots}}}}\,.$$

Galois suppone inizialmente che la prima delle radici dell'equazione proposta, $P(x) = 0$, abbia antiperiodo di lunghezza 1, ovvero $\alpha = p + \frac{1}{A}$.
Quindi l'equazione che si ottiene compiendo la sostituzione $x \to p + \frac{1}{x}$, resta sempre un'equazione di secondo grado, e ha come radice A.

Infatti, $P\left(p + \frac{1}{x}\right) = ap^2x^2 + a + 2pax + bpx^2 + bx + cx^2 = 0$

Dunque, per il risultato precedente la seconda radice dell'equazione originale, $P(x) = 0$, è della forma

$$\beta = a + \cfrac{1}{-\cfrac{1}{B}} = a - B\,; \quad con -1 < \beta < 0$$

pertanto ne segue che $a - B \in]0, 1[$, ma ciò è possibile solo se a è uguale alla parte intera di B, e la parte intera di B è a_n, quindi $a = a_n$. Allora

$$\alpha = a_n + \cfrac{1}{a_1 + \cfrac{1}{\dots + \cfrac{1}{a_n + \cfrac{1}{a_{1+\dots}}}}} = a_n + \cfrac{1}{a_1 + \cfrac{1}{\dots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n + \dots}}}}$$

Perciò anche α è immediatamente periodica.

Analogamente, Galois dimostra l'impossibilità di avere un antiperiodo di lunghezza 2, dopodichè non tratta ulteriori casi di antiperiodi con lunghezza superiore, ma ci assicura che potrebbero essere svolti in maniera analoga utilizzando il ragionamento appena visto.

Inoltre, osserva anche che: *"Se una delle radici di un'equazione di secondo grado è non solo immediatamente periodica ma anche simmetrica, cioè se i termini del periodo a uguale distanza degli estremi sono uguali, si avrà $B = A$; di modo che queste due radici saranno A e $-\frac{1}{A}$; l'equazione sarà dunque $Ax^2 - (A^2 - 1)x - A = 0$."* ([2] pagine 38-39)

L'osservazione prosegue con l'illustrazione della forma dell'equazione generica di secondo grado che ha come radici due frazioni continue immediatamente periodiche e simmetriche.

A conclusione di questo articolo, Galois mostra, svolgendo un esempio di una particolare equazione, parte dei risultati sopra esposti.

3.2.2 Note su alcuni punti d'analisi

Anche questo lavoro, come il precedente, fu pubblicato sugli *Annales de Mathématiques pures et appliquées* tra il 1830-31.
Esso è strutturato in due note tra loro scollegate: *Dimostrazione di un teorema di analisi* e *Raggio di curvatura delle curve nello spazio.*

Dimostrazione di un teorema di analisi

Il teorema che Galois vuole dimostrare è il seguente:

Teorema 3. *Siano date due funzioni qualunque $F(x)$ e $f(x)$; si avrà, quali che siano x ed h,*

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

dove φ è una funzione determinata, e k una quantità intermedia tra x e $x + h$.

Dimostrazione. Poniamo infatti

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

se ne dedurrà $F(x+h) - Pf(x+h) = F(x) - Pf(x)$ da dove si vede che la funzione $F(x) - Pf(x)$ non cambia cambiando in essa x con $x + h$; da cui segue che a meno che essa non resti costante entro questi limiti, e ciò non potrebbe verificarsi se non in casi particolari, questa funzione avrà, tra x e $x + h$, uno o più massimi e minimi[1].

[1]**Teorema di Weierstrass.** Sia $[a, b] \subset \mathbb{R}$ intervallo chiuso e limitato e non vuoto, sia $f : [a, b] \to \mathbb{R}$ una funzione continua. Allora f ammette almeno un punto di massimo e di minimo in $[a, b]$.

Sia k il valore di x corrispondente a uno di essi, si avrà evidentemente $k = \psi(P)$ dove ψ è una funzione determinata; dunque si deve avere anche $P = \varphi(k)$ essendo φ un'altra funzione ugualmente determinata; il che dimostra il teorema. $\square$

([2] pagine 42-43)

Ci accorgiamo immediatamente che Galois assume senza mai esplicitarlo, nè nelle ipotesi del teorema nè nella dimostrazione, che le funzioni F ed f sono continue in tutto l'intervallo considerato.

Questo lavoro di Galois, alquanto impreciso e non corretto, non sfuggì ai matematici dell'epoca; Bernard Placidus Johann Nepomuk Bolzano (1781-1848) lo contestò nella sua opera *Functionenlehre*:

"Questa dimostrazione non mi soddisfa. Senza dubbio l'equazione $\dfrac{F(x+h)-F(x)}{f(x+h)-f(x)} = P$ 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 perchè, 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." ([16] pagine 509-510)

Da questo risultato errato, Galois ne deduce anche un corollario altrettanto sbagliato:

Corollario. *La quantità $\lim \dfrac{F(x+h)-F(x)}{f(x+h)-f(x)} = \varphi(k)$ per $h = 0$, è necessariamente una funzione di x, il che dimostra, a priori, l'esistenza delle funzioni derivate.* ([2] pagina 43)

Questo lavoro mostra una certa confusione da parte di Galois relativa al rapporto tra continuità e derivabilità di una funzione.
Tuttavia, le sue responsabilità possono essere attenuate, in quanto all'inizio del XIX secolo sembrava assurdo che una funzione continua potesse non essere monotona in un intervallo sufficientemente piccolo; fu attraverso studi dettagliati degli sviluppi in serie di Fourier e del modo di generare funzioni violentemente oscillanti, che furono trovati i primi esempi di funzioni continue in tutto l'intervallo, ma non derivabili in alcun punto.

Uno dei primi risultati di questo tipo fu trovato da Karl Theodor Wilhelm Weierstrass (1815-1897) nel 1872 (quindi 40 anni dopo la morte di Galois). Weierstrass determinò una funzione reale di variabile reale che ha la proprietà di essere continua in ogni punto, ma di non essere derivabile in alcuno; tale funzione prende il nome di *funzione di Weierstrass*.
Anche altri matematici, come il già citato Bolzano, avevano lavorato su funzioni simili, senza però pubblicare nulla.

Raggio di curvatura delle curve nello spazio

In questa nota Galois fornisce un'interpretazione della curvatura per curve non piane.

3.2.3 Analisi di una memoria sulla risoluzione algebrica delle equazioni

Nell'aprile del 1830 Galois pubblica questa nota sul *Bulletin des Sciences mathématiques, astronomiques, physiques et chimiques*, in cui espone in modo conciso, e senza dimostrazioni, alcuni risultati ed idee che confluiranno nella prima memoria, *Mémoire*, e nella seconda.

Innanzitutto egli dà le definizioni di equazioni primitive e non primitive.
Per Galois un'equazione è detta primitiva se non può essere semplificata con il metodo di Gauss[2], altrimenti è detta non primitiva.

Un'equazione primitiva può essere risolubile per radicali, a riguardo Galois fornisce i seguenti risultati:

1. Un'equazione di grado primo è risolubile per radicali se e solo se note due qualunque delle sue radici le altre si deducono da esse razionalmente.[3]
2. Un'equazione primitiva di grado m è risolubile per radicali se $m = p^\nu$ con p numero primo.
3. Un'equazione primitiva di grado p^ν è risolubile per radicali se note due qualunque delle sue radici le altre si deducono da esse razionalmente.

É importante osservare come lo stesso Galois affermi: *"Tutte queste proposizioni sono state dedotte dalla teoria delle permutazioni."* ([2] pagina 46)
Dunque questo mostra come Évariste avesse già dimostrato, o quanto meno intuito, i risultati che confluiranno nella versione finale della *Mémoire.*

3.2.4 Nota sulla risoluzione delle equazioni numeriche

Due mesi dopo, nel giugno 1830, Galois pubblica due ulteriori lavori sul *Bulletin des Sciences mathématiques, astronomiques, physiques et chimiques*; quello che ora andremo ad analizzare è relativo alla risoluzione numerica delle equazioni algebriche.

Egli si riallaccia al lavoro di Adrien-Marie Legendre presente nell'ultimo dei tre *Suppléments* posti come appendice alla seconda edizione dell'*Essai sur la Théorie des Nombres.*

[2]**Lemma di Gauss.** Se un polinomio è irriducibile in $\mathbb{Z}[x]$, allora è irriducibile anche in $\mathbb{Q}[x]$.

[3]Galois tralascia di precisare che l'equazione deve essere irriducibile, ma probabilmente aveva intuito che questa è una condizione insindacabile.
Le equazioni irriducibili di grado primo sono l'esempio più semplice di equazioni primitive.

Galois propone una modifica al metodo di Legendre relativa all'eliminare il ricorso ad un'estrazione di radice n-esima, che è richiesto ad ogni passaggio.

Infatti, nel metodo di Legendre, presa un'equazione di grado n, $Fx = 0$, si vuole determinare la radice più vicina ad una certa ascissa assegnata a. Per far ciò si riscrive l'equazione Fx come $Fx = X - Y$ con X e Y a termini positivi. Ora Legendre si serve dei termini X e Y per ricavare due funzioni ausiliarie

$$x = \varphi x = \sqrt[n]{\frac{X}{\left(\frac{Y}{x^n}\right)}}\,, \qquad x = \psi x = \sqrt[n]{\frac{X}{\left(\frac{x^n}{Y}\right)}}\,. \tag{1}$$

Le curve $y = \varphi x$ e $y = \psi x$ si trovano una sopra e l'altra sotto la bisettrice del primo e terzo quadrante, $y = x$.

Per determinare la radice cercata di $Fx = 0$ si passa a studiare i punti fissi delle funzioni ausiliarie; ovvero a risolvere le equazioni $\varphi x = x$ e $\psi x = x$; questi rappresentano i punti di intersezione della bisettrice con le curve.

Per risolvere queste equazioni si considerano le successioni di valori a, φa, $\varphi\varphi a$, $\ldots$ e a, ψa, $\psi\psi a$, $\ldots$ su cui vengono calcolati entrambi i termini delle equazioni (1), ricavando una successione di valori che convergono alla radice reale dell'equazione proposta più vicina ad a.

Dunque il contributo di Galois risiede nel cercare due funzioni ausiliarie più comode.
Per ottenere la prima egli determina un valore k tale che $x + \frac{F(x)}{kx^n}$ sia monotona crescente per $x > 1$. Per trovare tale k si serve della scomposizione di $F(x)$ fatta nel metodo di Legendre, ossia $F(x) = X(x) - Y(x)$; poi con calcoli diretti conclude che la condizione è soddisfatta se

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

Dal momento che $nX - xX'$ e $nY - xY'$ sono positivi, è sufficiente richiedere che $\frac{nX - xX'}{kx^{n+1}} < 1$ per $x > 1$. Ciò si può verificare prendendo $nX(1) - X'(1) < k$.

In maniera analoga, per la seconda funzione, Galois determina un valore h tale che $x - \frac{F(x)}{hx^n}$ sia monotona crescente in $x > 1$, questa condizione è soddisfatta prendendo $h > nY(1) - Y'(1)$.

Pertanto le funzioni ausiliarie sono:

$$x = x + \frac{F(x)}{kx^n} = \varphi(x)\,, \qquad x = x - \frac{F(x)}{hx^n} = \psi(x)\,.$$

Chiariamo che chiedere la crescente monotonia solo per valori $x > 1$ implica cercare radici maggiori dell'unità; tuttavia, ciò non limita la validità del metodo, infatti le radici negative possono essere determinate studiando quelle positive dell'equazione $F(-x) = 0$, e quelle comprese nell'intervallo $[0, 1]$ le si ottengono cercando le radici maggiori di 1 dell'equazione $F\left(\frac{1}{x}\right) = 0$.

3.2.5 Sulla teoria dei numeri

Il secondo lavoro pubblicato nel giugno del 1830 da Galois sul *Bulletin des Sciences mathématiques, astronomiques, physiques et chimiques* riguarda la teoria dei numeri, nello specifico si concentra sullo studio delle congruenze modulo un numero p primo. Tale lavoro confluirà nella seconda memoria.

Galois considera una congruenza del tipo

$$F(x) \equiv 0 \qquad \mod p \tag{2}$$

dove $F(x)$ è un polinomio di grado ν i cui coefficienti appartengono a $\mathbb{Z}_p$ con p numero primo assegnato.
Inoltre egli assume che F sia irriducibile, quindi non è possibile trovare tre funzioni $\varphi(x)$, $\psi(x)$, $\chi(x)$ tali che $F(x) = \varphi(x) \cdot \psi(x) + p\chi(x)$.

Ne segue dunque che (2) non ha radici in $\mathbb{Z}_p$. Pertanto Galois ritiene necessario introdurre dei simboli immaginari, sulla scia dell'unità immaginaria, $i = \sqrt{-1}$, per poter rappresentare gli zeri della congruenza (2).
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 dal titolo *De residuis cubicis commentatio numerosa* dove, considerando congruenze del tipo

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

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

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

Tali soluzioni di Jacobi rendono il numero di radici distinte della congruenza pari al grado della conguenza stessa, $p + 1$, fornendo un'analogia con il teorema fondamentale dell'algebra[4].
Tuttavia Galois nel suo lavoro mostra di non essere per nulla a conoscenza delle scoperte di Jacobi;

[4]**Teorema fondamentale dell'algebra.** Ogni polinomio a coefficienti complessi in una variabile di grado $n \geq 1$ del tipo

$$a_n z^n + \ldots + a_1 z + a_0$$

ammette almeno una radice complessa.
Dal teorema segue che un polinomio a coefficienti complessi ammette esattamente n radici complesse contate con la giusta molteplicità, mentre un polinomio a coefficienti reali ammette al più n radici reali.

infatti nelle prime righe del suo scritto afferma: *"Essendo stato condotto da ricerche particolari a considerare le soluzioni incommensurabili, sono pervenuto ad alcuni risultati che credo nuovi."* ([2] pagina 50)

Ma anche in conclusione della nota egli scrive: *"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."* ([2] pagina 58)

Chiamiamo i una delle radici immaginarie della congruenza (2). Notiamo che tutte le potenze di i maggiori o uguali a ν sono vincolate da (2); dunque si possono formare quantità del tipo:

$$\alpha := a + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1} \tag{A}$$

dove gli $a_i \in \mathbb{Z}_p$.

Esistono p^ν modi di formare α, dovuti alle p scelte per ogni coefficiente; tutte queste quantità distinte nel loro insieme formano un campo finito, oggi noto come *campo di Galois*.
Il fatto che il campo sia finito fa si che presa una qualunque quantità $\alpha \neq 0$ del tipo (A) esista un intero n tale che $\alpha^n \equiv 1 \mod p$. Galois non dimostra questa affermazione, la tratta come una conseguenza imprescindibile.

La successione delle potenze di α; $\alpha^0 \equiv 1$, α, α^2, α^3, ... sono in numero illimitato, quindi deve esisterne almeno una che sia congrua modulo p a una potenza precedente. Dunque poniamo α^n come la prima quantità che si incontra nella sequenza $1,\ \alpha\,, \alpha^2,\ \alpha^3, \ldots$ che sia congrua (mod p) a una potenza precedente. Necessariamente dovrà essere $\alpha^n \equiv 1 \pmod p$. Infatti, se si avesse $\alpha^n \equiv \alpha^m \pmod p$ con $m \neq 0$ e $m < n$, ne risulterebbe $\alpha^n - \alpha^m \equiv 0 \pmod p$ da cui $\alpha^m(\alpha^{n-m} - 1) \equiv 0 \pmod p$. Quindi o $\alpha^m \equiv 0 \pmod p$ oppure $\alpha^{n-m} \equiv 1 \pmod p$ con $n - m \neq 0$ e $n - m < n$.

Se fosse $\alpha^m \equiv 0 \pmod p$ allora α^m non potrebbe essere una delle $p^\nu - 1$ espressioni di (A) a coefficienti non tutti nulli, poichè nessuna di queste è congrua a $0 \pmod p$.
Non può essere neanche $\alpha^{n-m} \equiv 1 \pmod p$ con $n - m \neq 0$ e $n - m < n$; siccome, per ipotesi α^n è la prima delle successive potenze di α che è congrua (mod p) a una delle potenze precedenti.
Pertanto ogni potenza di α successiva ad n è congrua (mod p) ad un elemento della sequenza $1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \ldots,\ \alpha^{n-1}$. Inoltre, affinchè due potenze di α siano congrue tra loro (mod p), è necessario e sufficiente che gli esponenti differiscano per multipli di n.

Adesso riguardo alle seguenti n quantità, $\{1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}$ con $\alpha \neq 0$, abbiamo due possibilità: o che queste coprano tutte le espressioni di (A), oppure ne esiste un'altra, β, non contemplata nell'insieme precedente.
Pertanto si possono formare nuove quantità non equivalenti tra loro

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

Si itera tale procedimento fino a che non si esauriscono le espressioni di (A).
Questa procedura ha necessariamente termine poichè le espressioni $\alpha \neq 0$ sono in numero finito, $p^\nu - 1$.
Da ciò segue che $\alpha^{p^\nu - 1} \equiv 1 \mod p$. Ovvero si dimostra il *Piccolo Teorema di Fermat*.

3.3 Memoria sulle condizioni di risolubilità delle equazioni per radicali

Il *Mémoire sur les conditions de résolubilité des équations par radicaux*, anche detto per brevità solo *Mémoire*, è l'opera principale realizzata da Galois riguardo la caratterizzazione delle equazioni che sono risolubili per radicali; la versione che è stata conservata rappresenta una sintesi dell'ultimo lavoro inviato, nel gennaio 1831, all'Académie des Sciences e bocciata dai recensori Siméon-Denis Poisson e Sylvestre-François Lacroix.
In questo resoconto è presente anche una breve prefazione, nella quale Galois mostra tutto il suo rammarico relativo al respingimento dell'opera, e implora i futuri matematici che si cimenteranno nell'analisi di essa a prestarle la giusta attenzione.

"Supplico i miei giudici di leggere con attenzione almeno queste poche pagine." ([2] pagina 69)

Tale preghiera, con anche un'ammissione riguardo la poca chiarezza espositiva dei suoi risultati, è presente anche nel congedo della lettera all'amico Chevalier, incaricato di conservare e divulgare le sue scoperte:

"Ma io non ho tempo, e le mie idee non sono ancora ben sviluppate su questo terreno che è immenso.
Farai stampare questa Lettera nella "Revue encyclopédique".
Mi sono spesso azzardato nella mia vita ad avanzare proposizioni delle quali non ero sicuro; ma tutto quello che ho scritto qui è da quasi un anno nella mia testa ed è troppo nel mio interesse non sbagliarmi perchè mi si sospetti di aver enunciato dei teoremi dei quali non avrei la dimostrazione completa.
Pregherai pubblicamente Jacobi e Gauss di dare il loro parere, non sulla verità, ma sull'importanza dei teoremi.
Dopo questo, ci sarà, qualcuno che troverà il suo profitto a decifrare tutto questo guazzabuglio." ([2] pagina 68)

Sempre in queste poche righe introduttive all'opera, Galois corre dritto al punto enunciando subito l'obiettivo del lavoro, ovvero trovare una condizione generale che permetta di stabilire quando un'equazione algebrica irriducibile di grado primo è risolubile per radicali:

"Perchè un'equazione di grado primo, che non ha divisori commensurabili, sia risolubile per radicali, è necessario e sufficiente che tutte le radici siano funzioni razionali di due qualunque tra esse." ([2] pagina 69)

Il *Mémoire* è suddiviso in alcuni principi, quattro lemmi e otto proposizioni; non tutti i risultati hanno dimostrazione e quelli che ne possiedono sono comunque prove molto concise e affrettate.

3.3.1 Principi

Galois inizia la sua trattazione dando la definizione di equazione riducibile ed equazione irriducibile:

Definizione. *Un'equazione è detta riducibile quando ammette divisori razionali, irriducibile in caso contrario.* ([2] pagina 70)

É giusto sottolineare come tale definizione è in sostanza quella che si utilizza ancora oggi.

Fatto ciò egli si sofferma sull'aggettivo *razionale*, al quale attribuisce molta importanza: 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 sempre nella scomposizione in fattori i quali però possono essere espressi razionalmente in termini dei coefficienti dell'equazione di partenza.

Galois passa poi a trattare le *aggiunzioni*; queste consistono nel processo di allargamento del campo dei coefficienti di un'equazione data tramite l'aggiunta di uno o più elementi.
"C'è di più: si potrà convenire di considerare come razionale ogni funzione razionale di un certo numero di quantità determinate, supposte note a priori. Per esempio, si potrà scegliere una certa radice di un numero intero e considerare come razionale ogni funzione razionale di questo radicale. Nel caso si convenga di considerare come note in questo senso alcune quantità, diremo che le aggiungiamo all'equazione che si deve risolvere. Diremo che queste quantità sono aggiunte all'equazione." ([2] pagina 70)

Sebbene al tempo non fosse stato ancora formalizzato il concetto di campo, è chiaro che Galois in questa nozione si riferisca alle *estensioni di campo*, in particolare all'estensione del campo $\mathbb{Q}$ dei coefficienti dell'equazione proposta.
Dunque, ogni quantità definita in funzione del campo $\mathbb{Q}$ e delle sue aggiunzioni è da considerarsi una quantità razionale.

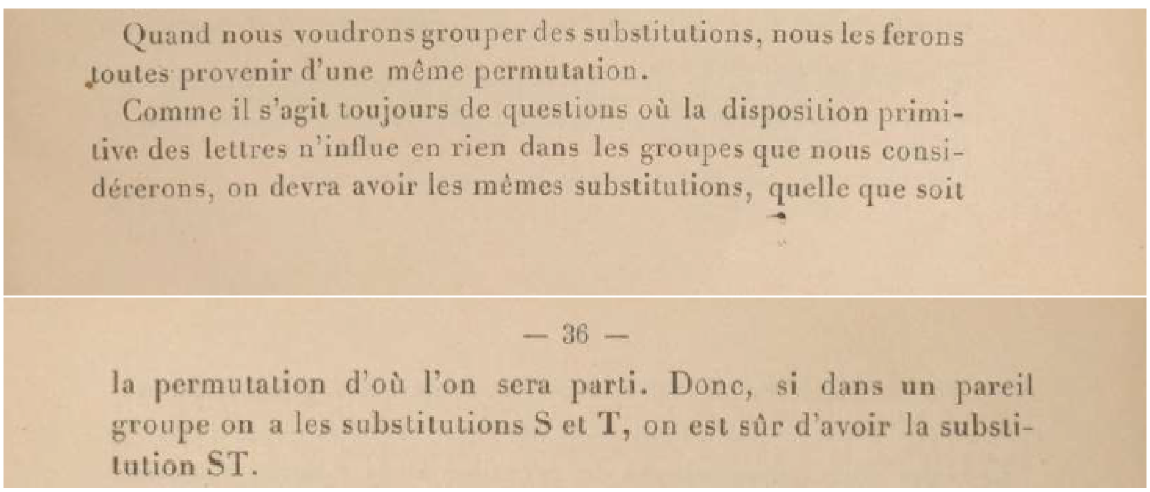
Egli nota anche che l'aggiunzione di uno o più elementi in un campo può rendere riducibile un'equazione che prima non lo era. Per chiarire questo concetto si serve di un esempio relativo allo studio delle equazioni ciclotomiche:
Considerata l'equazione $\dfrac{x^n - 1}{x - 1} = 0$ con n primo, se aggiungiamo a $\mathbb{Q}$ una delle radici delle equazioni ausiliarie di Gauss, l'equazione proposta diventa riducibile.

Conclusa la parentesi sulle aggiunzioni, Galois passa ad analizzare le nozioni di *permutazione* e di *sostituzione*.
Per *permutazione* egli intende la disposizione di n oggetti in tutti i modi possibili; mentre per *sostituzione* intende il passaggio da una permutazione ad un'altra; anche se poi nel corso di tutta la memoria è possibile riscontrare alcune incertezze nell'uso dei due vocaboli. Infatti, Galois spesso li usa come sinonimi.
Tuttavia, come sottolinea Laura Toti Rigatelli nella nota a pagina 74 di [2], "nel manoscritto sono presenti molte cancellature e aggiunte e nel margine di un foglio si legge, seppure cancellata, la frase: *"Mettere dappertutto al posto della parola permutazione la parola sostituzione"*."

Galois comprende anche che *"la permutazione dalla quale si parte per indicare le sostituzioni è del tutto arbitraria, quando si tratta di funzioni; giacché non c'è alcuna ragione perchè, in una funzione di più lettere, una lettera occupi un posto piuttosto che un altro."*([2] pagina 71)
Attraverso questi due concetti appena introdotti Galois arriva a formulare una nozione primitiva, e lontana da quella attuale[5], di *gruppo*, modellata sulle sostituzioni:

"Quando vorremo raggruppare le sostituzioni, le faremo tutte provenire da una stessa permutazione.
Poichè si tratta sempre di questioni nelle 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. Dunque, se in un gruppo siffatto vi sono le sostituzioni S e T, si è certi di avere anche la sostituzione ST." ([2] pagina 71)

Questa è la prima volta che il termine *gruppo* compare nella letteratura matematica con un significato diverso da quello di insieme.
Inoltre, in tale definizione compare anche la proprietà di *chiusura* dell'operazione di composizione, dalla quale deriva l'esistenza sia dell'elemento neutro che dell'elemento inverso per ogni permutazione.


Quand nous voudrons grouper des substitutions, nous les ferons toutes provenir d'une même 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 les mêmes substitutions, quelle que soit

— 36 —

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.

Figura 4: Definizione Gruppo

[5]**Definizione (Gruppo).** Un insieme A si dice *gruppo* se è dotato di un'operazione binaria $A \times A \to A,\ (a,b) \mapsto a * b$ tale che

- Esiste l'elemento neutro: esiste $u \in A$ tale che $a * u = u * a = a$ per ogni $a \in A$;
- Vale la proprietà associativa: per ogni a, b, $c \in A$ si ha $a * (b * c) = (a * b) * c$;
- Esiste l'elemento inverso: per ogni $a \in A$ esiste $\tilde{a} \in A$ tale che $a * \tilde{a} = \tilde{a} * a = u$.

3.3.2 Lemmi

In questo sottocapitolo, così come nel prossimo, presenteremo le idee di Galois servendoci spesso di dimostrazioni non sue; alcune di queste sono prese dal *Commentaire sur Galois* di Camille Jordan. Ciò è dovuto al fatto che egli è spesso sfuggevole e frettoloso nel mostrare i propri risultati.

Lemma I. *Un'equazione irriducibile non può avere alcuna radice comune con un'equazione razionale senza dividerla.* ([2] pagina 72)

La dimostrazione di Galois è appena abbozzata, ciò è dovuto al fatto che tale risultato era già noto ai matematici del XIX secolo.
Per completezza, mostriamo la prova del lemma attraverso una dimostrazione moderna che ricalca quella offerta da Jordan.

Dimostrazione. Presi due polinomi $P(x)$, $Q(x) \in \mathbb{Q}[x]$ a caratteristica nulla.[6] Sia P irriducibile e supponiamo che $\alpha \in \mathbb{Q}$ sia una radice in comune a P e Q. Se P non divide Q, allora l'irriducibilità di P implica che P e Q sono tra loro primi in $\mathbb{Q}[x]$.
Pertanto, per l'Identità di Bézout[7], devono esistere altri due polinomi $U(x)$, $V(x) \in \mathbb{Q}[x]$ tali che $U(x)P(x) + V(x)Q(x) = 1$.
Ora, posto $x = \alpha$ si ha $P(\alpha) = Q(\alpha) = 0$, da cui ne segue l'assurdo che $0 = 1$. Dunque P e Q non hanno alcuna radice in comune. $\square$

Lemma II. *Data un'equazione qualunque, che non abbia radici uguali, le cui radici siano a, b, c, ..., si può sempre formare una funzione V delle radici, tale che nessuno dei valori che si ottengono permutando in tutti i modi le radici in questa funzione sia uguale a un altro.* ([2] pagina 72)

L'ipotesi di studiare un'equazione a radici distinte non intacca la generalità del risultato. Infatti era ben noto un procedimento dovuto a Johannes Hudde (1628-1704), descritto in una lettera del 1657 che apparve nell'edizione latina della *Géométrie* di René Descartes (1596-1650), attraverso il quale era sempre possibile ridursi a questo caso.

Il metodo, in sostanza, è il seguente: sia α una radice del polinomio $P \in \mathbb{Q}[x]$, α è una radice multipla di P se e solo se $P'(\alpha) = 0$.
Infatti, P lo possiamo riscrivere come $P(x) = (x - \alpha)Q(x)$ e derivando otteniamo $P'(x) = Q(x) + (x - \alpha)Q'(x)$ da cui ne segue che P' è divisibile per $(x - \alpha)$ se e solo se Q lo è, cioè se α è radice multipla di $P(x)$.

Per capire a pieno questo risultato è utile specificare che cosa si intende per *polinomio simmetrico*, anche se utilizzando il linguaggio di Galois dovremmo riferirci ad equazioni simmetriche.

[6] La caratteristica di un anello è definita come il più piccolo numero naturale n diverso da zero tale che l'elemento $\underbrace{1 + 1 + ... + 1}_{n\ volte}$ sia uguale a zero. Se un tale n non esiste, allora la caratteristica è 0 per definizione.

[7] **Identità di Bézout.** Siano a e b due interi non entrambi nulli e sia d il loro massimo comune divisore, allora esistono due altri interi x e y tali che $ax + by = d$.

Definizione (Polinomio simmetrico)**.** Un polinomio si dice *simmetrico* se per ogni permutazione sull'ordine delle indeterminate il polinomio resta invariato, ovvero se $P(x_1, x_2, \ldots, x_n) = P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$ per ogni σ permutazione possibile; in altre parole, ogni permutazione manda il polinomio in se stesso.

Di fatto, la funzione V non è simmetrica rispetto alle permutazioni sull'ordine delle radici, quindi, ogni volta che ne cambiamo la disposizione, otteniamo un valore diverso di V. Ad esempio, $V(a, b, c, \ldots) \neq V(c, b, a, \ldots)$.
Dunque, la funzione V ci permette di distinguere tra tutte le possibili permutazioni delle radici perché produce valori unici per ciascuna permutazione.

Per il lemma II Galois si limita a dire:
"Per esempio, si può prendere

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

con A, B, C numeri interi convenientemente scelti." ([2] pagina 72)

Utilizzando questo suggerimento di Galois e la dimostrazione data da Jordan sul *Commentaire* forniamo una prova del lemma:

Dimostrazione. Siano $r_1, r_2, \ldots, r_n$ le radici dell'equazione assegnata; consideriamo la funzione

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

Prese due permutazioni distinte σ, τ chiamiamo V_σ, V_τ i valori che assume V quando agiscono sugli argomenti delle radici rispettivamente σ e τ:

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

Ora escludiamo tutti i valori di m_i che soddisfano la seguente equazione

$$\sum_{i=1}^{n} m_i [r_{\sigma(i)} - r_{\tau(i)}] = 0 \tag{3}$$

qualunque sia la coppia di permutazioni σ, τ scelta.

La (3) nelle variabili m_i rappresenta l'equazione di un iperpiano; dunque basterà evitare di prendere gli m_i che appartengono agli iperpiani descritti da (3) per soddisfare il lemma. □

Lemme II. — *Étant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont a, b, c, ..., on peut toujours former une fonction V des racines, telle qu'aucune des valeurs que l'on obtient en permutant dans cette fonction les racines de toutes manières, ne soit égale à une autre.*

Par exemple, on peut prendre

$$V = Aa + Bb + Cc + \ldots,$$

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

Figura 5: Lemma II

Lemma III. *Scelta la funzione V come è indicato al punto precedente, essa godrà di questa proprietà, che tutte le radici dell'equazione proposta si esprimano razionalmente in funzione di V.* ([2] pagina 72)

Poichè per il lemma II V è costruita in modo da essere unica per ogni configurazione delle radici, allora ogni radice si può esprimere come funzione razionale di V, cioè esiste una relazione diretta tra le radici e la funzione V. Pertanto, questo collegamento implica che possiamo studiare le radici dell'equazione tramite la funzione V stessa.

Anche in questo caso la dimostrazione di Galois si limita ad essere una traccia:

Dimostrazione. Sia $V = \varphi(a, b, c, d, \ldots)$ *o* $V - \varphi(a, b, c, d, \ldots) = 0$.
Moltiplichiamo tra di loro tutte le equazioni simili, che si ottengono permutando in queste tutte le lettere, lasciando fissa solo la prima; verrà un'espressione del tipo:

$$[V - \varphi(a, b, c, d, \ldots)][V - \varphi(a, c, b, d, \ldots)][V - \varphi(a, b, d, c, \ldots)] \cdots ,$$

simmetrica in $b, c, d, \ldots$, *la quale di conseguenza si potrà scrivere in funzione di* a. *Avremo dunque un'equazione della forma.*

$$F(V, a) = 0 .$$

Dico ora che da essa si può ottenere un valore di a. *É sufficiente perciò cercare la soluzione comune a questa equazione e alla proposta. Questa soluzione è l'unica comune, poichè non si può avere, per esempio,*

$$F(V, b) = 0$$

questa equazione avendo un fattore comune con l'equazione simile. Altrimenti una delle funzioni $\varphi(a, \ldots)$ *sarebbe uguale a una delle funzioni* $\varphi(b, \ldots)$*; il che è contro l'ipotesi.*
Segue da ciò che a *si esprime in funzione razionale di* V *ed è la stessa cosa per ogni altra radice.* ([2] pagine 72-73) □

Sul margine sinistro del manoscritto è riportata la seguente annotazione di Poisson: *"La dimostrazione di questo lemma non è sufficiente, ma esso è vero per il n.100 della memoria di Lagrange, Berlino 1775"*. ([2] pagina 72)
Poisson fa riferimento all'opera *Réflexions* di Lagrange, nella quale si studia il numero di valori distinti assunti da funzioni delle radici di un'equazione algebrica, tra queste rientrano anche le funzioni proposte da Galois.
Questa nota mostra come Poisson abbia effettivamente compiuto lo sforzo di tentare di comprendere il lavoro di Galois, ma senza successo.

A seguito della postilla Galois aggiunge di suo pugno: *"Abbiamo voluto trascrivere testualmente la dimostrazione che abbiamo dato di questo lemma in una memoria presentata nel 1830. Vi abbiamo aggiunto come documento storico la nota che il signor Poisson ha creduto di dovervi apporre. Si giudicherà."*([2] pagina 73 nota 3)
A riprova della forte delusione patita a seguito della bocciatura del suo lavoro.

A fine dimostrazione, Galois fa presente come questo lemma sia citato, pur manchevole di prova, da Abel nella sua memoria postuma sulle funzioni ellittiche.

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

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

e se inoltre, per ogni $i, j = 2, \ldots, n$

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

allora l'equazione $P(x) = 0$ è risolubile per radicali.

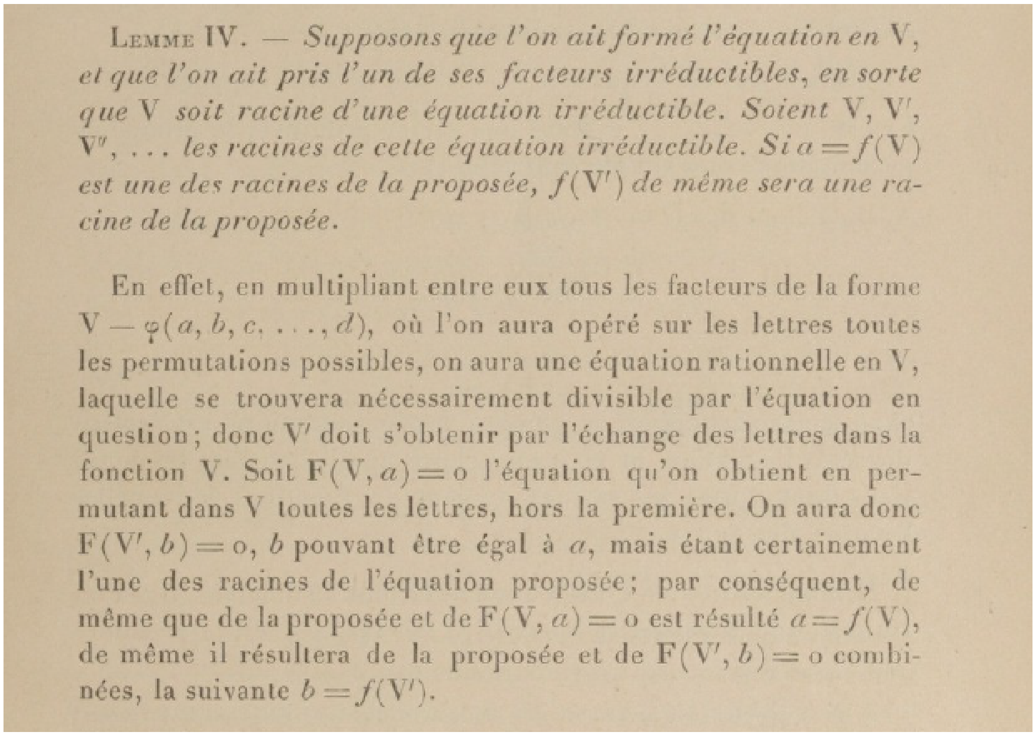
Galois commenta così tale risultato:

*"É notevole che da questa proposizione si possa concludere che ogni equazione dipende da un'equazione ausiliaria tale che tutte le radici di questa nuova equazione siano funzioni razionali le une delle altre; infatti l'equazione V rientra in questo caso.
D'altronde questa osservazione è una pura curiosità. Infatti, un'equazione che ha questa proprietà non è, in generale, più facile da risolvere di un'altra."* ([2] pagina 73)

Lemma IV. *Supponiamo che si sia formata l'equazione in V, e che si sia preso uno dei suoi fattori irriducibili, in modo tale che V sia radice di un'equazione irriducibile. Siano $V, V', V'', \ldots$ le radici di questa equazione irriducibile. Se $a = f(V)$ è una delle radici della proposta, analogamente $f(V')$ sarà una radice della proposta.*

*Dimostrazione. Infatti, moltiplicando tra di loro tutti i fattori della forma $V - \varphi(a, b, c, \ldots, d)$, dove si saranno operate sulle lettere tutte le permutazioni possibili, si avrà un'equazione razionale in V la quale risulterà divisibile per l'equazione in questione; dunque V' si deve ottenere mediante lo scambio delle lettere nella funzione V.
Sia $F(V, a) = 0$ l'equazione che si ottiene permutando in V tutte le lettere, esclusa la prima.*

Si avrà dunque $F(V', b) = 0$, b potendo essere uguale ad a[8]*, ma essendo certamente una delle radici dell'equazione proposta; di conseguenza, come dalla proposta e dalla $F(V, a) = 0$ è risultato $a = f(V)$, analogamente risulterà dalla proposta e da $F(V', b) = 0$ combinate la seguente $b = f(V')$.*
([2] pagina 73) □



Lemme IV. — *Supposons que l'on ait formé l'équation en V, et que l'on ait pris l'un de ses facteurs irréductibles, en sorte que V soit racine d'une équation irréductible. 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.*

En effet, en multipliant entre eux tous les facteurs de la forme $V - \varphi(a, b, c, \ldots, d)$, où l'on aura opéré sur les lettres toutes les permutations possibles, on aura une équation rationnelle en V, laquelle se trouvera nécessairement divisible par l'équation en question; donc V' doit s'obtenir par l'échange des lettres dans la fonction V. Soit $F(V, a) = o$ l'équation qu'on obtient en permutant dans V toutes les lettres, hors la première. On aura donc $F(V', b) = o$, b pouvant être égal à a, mais étant certainement l'une des racines de l'équation proposée; par conséquent, de même que de la proposée et de $F(V, a) = o$ est résulté $a = f(V)$, de même il résultera de la proposée et de $F(V', b) = o$ combinées, la suivante $b = f(V')$.

Figura 6: Lemma IV

L'importanza di questo lemma sta tutta nella seguente applicazione: rinominate le radici dell'equazione come $r_1, \ldots, r_n$ consideriamo $\sigma_j : r_i \to f_i(V_j)$, con σ_j che rappresentano le permutazioni delle radici dell'equazione. L'insieme di queste permutazioni con l'operazione di composizione forma un gruppo, oggi noto come *gruppo di Galois*.
Gli elementi di tale gruppo sono meglio caratterizzati nella Proposizione I.

Terminati i Lemmi egli passa a mostrare le Proposizioni principali della sua teoria.

[8] ovvero b viene fissato e tutte le altre lettere permutano tra loro.

3.3.3 Proposizioni

Come già detto all'inizio del sottocapitolo precedente, ci serviremo anche di altri risultati per le dimostrazioni delle proposizioni, viste le prove molto concise e a volte sfuggevoli di Galois.

PROPOSIZIONE I

Teorema. *Sia data un'equazione, della quale a, b, c, ... sono le m radici. Ci sarà sempre un gruppo di permutazioni delle lettere a, b, c, ... che godrà della seguente proprietà*

1. *Che ogni funzione delle radici, invariabile per le sostituzioni di questo gruppo, sia razionalmente nota*[9].
2. *Reciprocamente, che ogni funzione delle radici, determinabile razionalmente, sia invariabile per le sostituzioni.*

([2] pagina 74)

Dimostrazione. Rinominiamo le m radici come $r_1, \ldots, r_m$. Siccome $V = V_1$ è funzione razionale delle radici, che a loro volta sono funzioni razionali di V, si ha che ogni funzione razionale $\varphi(r_1, \ldots, r_m)$ può essere riscritta come:

$$\varphi(r_1, \ldots, r_m) = \alpha_0 + \alpha_1 V_1 + \alpha_2 V_1^2 + \ldots + \alpha_{n-1} V_1^{n-1} =: \psi(V_1) \tag{4}$$

n è il grado del fattore irriducibile contenente $V = V_1$.

Mostriamo la prima implicazione. Applichiamo a (4) una delle sostituzioni $\sigma_1 = id, \sigma_2, \ldots, \sigma_n$ del gruppo in questione, otteniamo, per l'invarianza di φ, che

$$\varphi(r_1, r_2, \ldots, r_m) = \frac{1}{n}[\psi(V_1) + \ldots + \psi(V_n)]$$

la funzione tra parentesi quadrate 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 $\mathbb{Q}$; ciò dimostra l'implicazione 1°.

Mostriamo la seconda implicazione. Per ipotesi $\varphi(r_1, r_2, \ldots, r_m) \in \mathbb{Q}$. Allora l'equazione

$$\alpha_{n-1} t^{n-1} + \alpha_{n-2} t^{n-2} + \ldots + \alpha_1 t + \alpha_0 - \varphi = 0 \tag{5}$$

ha coefficienti in $\mathbb{Q}$ e ammette come radice $t = V_1$. Ora poichè abbiamo appena mostrato che V_1 è radice di un'equazione irriducibile in $\mathbb{Q}$, ovvero (4), allora l'equazione (5) ammette tutti i valori $V_2, \ldots, V_n$ come sue radici; pertanto $\varphi = \psi(V_1) = \psi(V_2) = \ldots = \psi(V_n)$; ciò mostra l'invarianza di φ sotto l'azione delle sostituzioni. □

[9] Quando diciamo che una funzione è razionalmente nota, vogliamo dire che il suo valore numerico è esprimibile in funzione razionale dei coefficienti dell'equazione e delle quantità aggiunte. [Nota di Galois] ([2] pagina 74)

Galois a conclusione della dimostrazione nomina tale gruppo come *gruppo dell'equazione*.

Questa proposizione caratterizza le sostituzioni che appartengono al gruppo dell'equazione, o come diremo oggi al gruppo di Galois; infatti, il fattore irriducibile di cui V_1 è radice si può scrivere come

$$(t - V_1)(t - V_{\sigma_2}) \cdots (t - V_{\sigma_n})$$

che ha coefficienti in $\mathbb{Q}$; questo resta invariato sotto l'azione delle sostituzioni σ_i, pertanto

$$(t - V_{\sigma_i})(t - V_{\sigma_2\sigma_i}) \cdots (t - V_{\sigma_n\sigma_i})$$

ha come radice le $V_{\sigma_k\sigma_j}$. Siccome $V_{\sigma_k} \neq V_{\sigma_j}$ quando $j \neq k$, ne segue che le sostituzioni $\sigma_i, \ldots, \sigma_j\sigma_i, \ldots, \sigma_n\sigma_i$ sono quelle di partenza, al più disposte in ordine diverso.
Questo perchè come osserva Galois nel primo *scolio* alla proposizione *"la disposizione delle lettere non è assolutamente da considerare, ma solamente le sostituzioni di lettere per mezzo delle quali si passa da una permutazione all'altra. Così può essere data arbitrariamente una prima permutazione, purchè le altre permutazioni si deducano da essa sempre tramite le stesse sostituzioni di lettere. Il nuovo gruppo così formato godrà evidentemente delle stesse proprietà del primo, giacchè nel teorema precedente si tratta solo di sostituzioni che si possono fare nelle funzioni."* ([2] pagina 76)

Dunque il gruppo di Galois non studia l'intero gruppo delle sostituzioni sulle funzioni delle radici, ma solo alcune permutazioni che lasciano invariate delle particolari relazioni tra le radici.
L'obiettivo della teoria di Galois é proprio quello di cercare delle condizioni su questa struttura di gruppo, che se verificate ci diano la certezza che l'equazione algebrica sia risolubile.

Questo era l'originale punto di vista di Galois: usare i gruppi di permutazioni per descrivere come le varie radici di una data equazione sono collegate le une con le altre. Oggi il gruppo di Galois è definito come segue, poichè l'approccio moderno alla teoria comprende lo studio degli automorfismi delle estensioni di campi.

Definizione (Gruppo di Galois). Siano $F \subseteq E$ un'estensione di campo, chiamiamo *gruppo di Galois* di E su F il seguente insieme con l'operazione di composizione

$$Gal(E/F) = \{\sigma \in Aut(E)^{10} \mid \sigma(a) = a \ \forall a \in F\}.$$

Dunque è l'insieme dei $\sigma \in Aut(E)$ tale che $\sigma\big|_F = id\big|_F$.

PROPOSIZIONE II

Teorema. *Se si aggiunge a un'equazione data la radice r di un'equazione ausiliaria, 1° si otterrà di due cose l'una: o il gruppo dell'equazione non sarà cambiato, o si dividerà in p gruppi appartenenti ciascuno all'equazione proposta rispettivamente quando si aggiunge a essa ciascuna delle radici dell'equazione ausiliaria; 2° questi gruppi godranno della proprietà notevole, che si passerà dall'uno all'altro operando in tutte le permutazioni del primo una stessa sostituzione di lettere.*

[10] automorfismi di E.

([2] pagina 76-77)

La dimostrazione che dà Galois di questo risultato è molto concisa e sbrigativa; pertanto ne proponiamo un'altra, servendoci comunque di quella proposta da Galois.

Dimostrazione. Mostriamo il primo punto: consideriamo l'estensione di campo $\mathbb{Q} \subseteq \mathbb{Q}(r)$, se l'equazione ausiliaria in V

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

resta irriducibile in $\mathbb{Q}(r)$ allora il gruppo dell'equazione non cambia. Invece, se l'equazione in V si decompone in p fattori tutti dello stesso grado e forma:

$$\prod_{i=1}^{n!}(t-\sigma_i(V)) \quad \text{si spezza in} \quad f(V,r)f(V,r')f(V,r'')\cdots$$

con r, r', r'', ... altri valori di r. Allora il gruppo dell'equazione proposta si decompone anch'esso in p gruppi, tutti dello stesso ordine.

Mostriamo il secondo punto: per il lemma IV tutti i valori di V sono funzioni razionali gli uni degli altri. Supponiamo che V sia una radice dell'equazione $f(V,r)=0$ e che $\sigma(V)$ ne sia un'altra. Allo stesso modo se V' è una radice di $f(V',r')=0$, $\sigma(V')$ ne sarà un'altra.
Alla luce di ciò, operando dappertutto nel gruppo relativo ad r una certa sostituzione di lettere, si ottiene il gruppo relativo a r'.
Dunque per passare dalla permutazione $\sigma(V)$ alla permutazione $\sigma(V')$ è necessario eseguire la stessa sostituzione che occorre per passare dalla radice V alla radice V'. $\square$

PROPOSITION II.

Théorème (1). — *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 opérant dans toutes les permutations du premier une même substitution de lettres.*

1° Si, après l'adjonction de r, l'équation en V, dont il est question plus haut, reste irréductible, il est clair que le groupe de l'équation ne sera pas changé. Si, au contraire, elle se réduit, alors l'équation en V se décomposera en p facteurs, tous de même degré et de la forme

$$f(\mathrm{V}, r) \times f(\mathrm{V}, r') \times f(\mathrm{V}, r'') \times \ldots,$$

$r, r', r'', \ldots$ étant d'autres valeurs de r. Ainsi, le groupe de l'équation proposée se décomposera aussi en groupes chacun d'un même nombre de permutations, puisque à chaque valeur de V correspond une permutation. Ces groupes seront respecti-

— 41 —

vement ceux de l'équation proposée, quand on lui adjoindra successivement $r, r', r'', \ldots$.

2° Nous avons vu plus haut que toutes les valeurs de V étaient des fonctions rationnelles les unes des autres. D'après cela, supposons que, V étant une racine de $f(\mathrm{V}, r) = 0$, $\mathrm{F}(\mathrm{V})$ en soit une autre; il est clair que de même si V' est une racine de $f(\mathrm{V}, r') = 0$, $\mathrm{F}(\mathrm{V}')$ en sera une autre; car on aura

$$f[\mathrm{F}(\mathrm{V}), r] = \text{une fonction divisible par } f(\mathrm{V}, r).$$

Donc (*lemme* 1)

$$f[\mathrm{F}(\mathrm{V}'), r'] = \text{une fonction divisible par } f(\mathrm{V}', r').$$

Cela posé, je dis que l'on obtient le groupe relatif à r' en opérant partout dans le groupe relatif à r une même substitution de lettres.

En effet, si l'on a, par exemple,

$$\varphi_\mu \mathrm{F}(\mathrm{V}) = \varphi_\nu(\mathrm{V}),$$

on aura encore (*lemme* I),

$$\varphi_\mu \mathrm{F}(\mathrm{V}') = \varphi_\nu(\mathrm{V}').$$

Donc, pour passer de la permutation $[\mathrm{F}(\mathrm{V})]$ à la permutation $[\mathrm{F}(\mathrm{V}')]$, il faut faire la même substitution que pour passer de la permutation (V) à la permutation (V').

Le théorème est donc démontré.

Figura 7: Proposizione II

Il primo punto della proposizione ci introduce alla *Corrispondenza di Galois*, oggi definita nel seguente modo:

Definizione (Corrispondenza di Galois)**.** Sia $F \subseteq E$ estensione di campi, esiste una corrispondenza biunivoca tra $\{K \,\text{campi}\,|\, F \subseteq K \subseteq E\}$ e $\{H \,\text{gruppi}\,|\, H \leq Gal(E/F)\}$. Tale corrispondenza è così fatta:

- $K \to Gal(E/K) \leq Gal(E/F)$;
- $\{a \in E \,|\, \varphi(a) = a, \, \forall \varphi \in H\} \leftarrow H$, ossia H agisce su E, E^H, e i suoi punti fissi sono l'insieme in questione.

Il secondo punto, invece, fa riferimento a gruppi coniugati. Questi, attraverso la corrispondenza di Galois, ci offrono *campi coniugati*, che in algebra moderna sono così formulabili:

Definizione (Campi coniugati)**.** Sia $F \subseteq K \subseteq E$ estensione di campi, $\sigma \in Gal(E/F)$, allora definiamo il *campo coniugato di* K, $\sigma(K)$, come l'immagine dell'isomorfismo $\sigma : K \to \sigma(K)$.

Riguardo a questo secondo punto osserviamo anche che, presi due campi F e K tali che $F \subseteq K$, sia P un polinomio, allora se $Gal_K(P)$[11] $= \{id, \sigma_2, \sigma_3, \dots, \sigma_k\}$ e $\tau_1, \tau_2, \dots, \tau_l$ sono permutazioni del $Gal_F(P)$ che non stanno nel $Gal_K(P)$, allora le permutazioni ottenute seguendo le direttive di Galois sono:

$$\{\tau_1, \sigma_2\tau_1, \dots, \sigma_k\tau_1\} \quad \dots \quad \{\tau_l, \sigma_2\tau_l, \dots, \sigma_k\tau_l\}.$$

Questi insiemi non sono gruppi perchè privi dell'elemento neutro. Si può recuperare la struttura di gruppo moltiplicando a sinistra per τ_i^{-1} e si ottengono

$$\{id, \tau_1^{-1}\sigma_2\tau_1, \dots, \tau_1^{-1}\sigma_k\tau_1\} \quad \dots \quad \{id, \tau_l^{-1}\sigma_2\tau_l, \dots, \tau_l^{-1}\sigma_k\tau_l\}$$

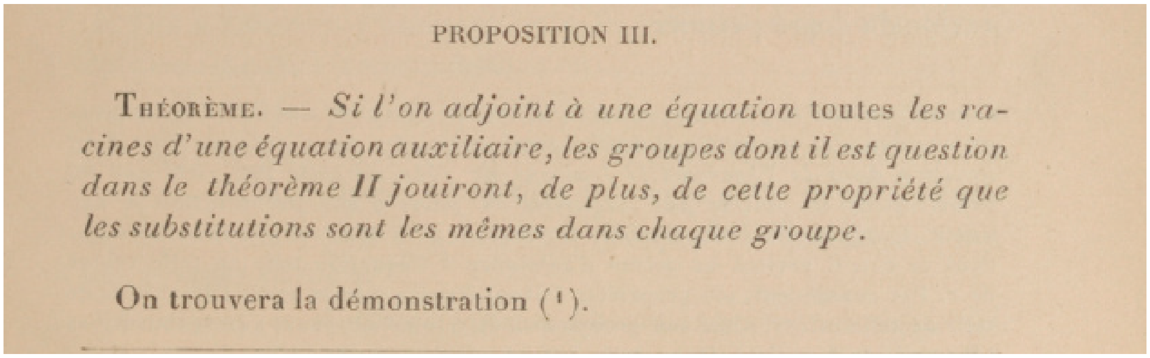
questi gruppi sono tutti dello stesso ordine, come dimostrato da Galois.

PROPOSIZIONE III

Teorema. *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.* ([2] pagina 78)

Questo teorema non è stato dimostrato da Galois, egli a riguardo scrive *"Si troverà la dimostrazione."*([2] pagina 78)

[11] Gruppo di Galois del polinomio P sul campo K.



PROPOSITION III.

THÉORÈME. — *Si l'on adjoint à une équation* toutes *les racines d'une équation auxiliaire, les groupes dont il est question dans le théorème II jouiront, de plus, de cette propriété que les substitutions sont les mêmes dans chaque groupe.*

On trouvera la démonstration (1).

Figura 8: Proposizione III

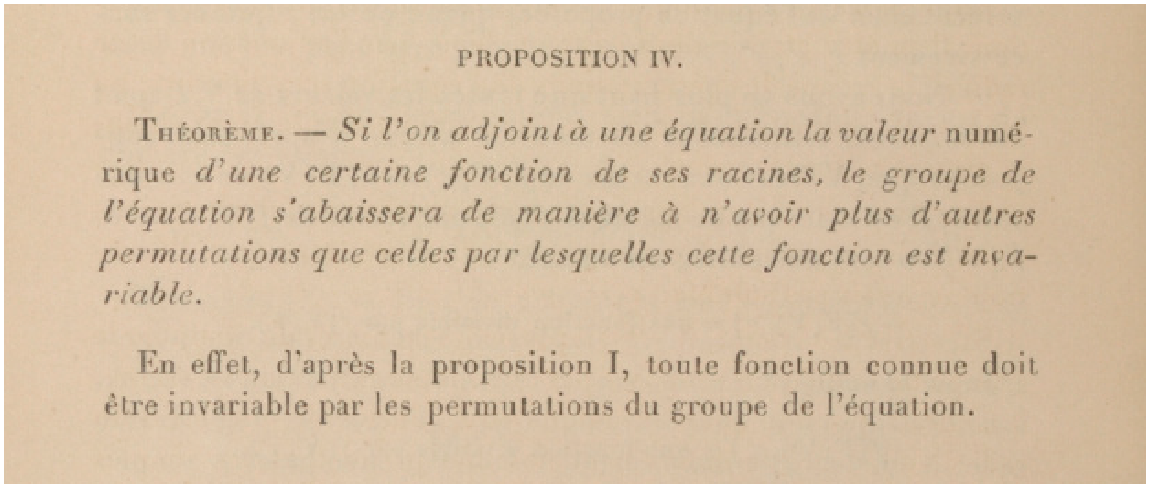
Tale risultato tratta il caso in cui si estende il campo di partenza aggiungendo ad esso tutte le radici di un'equazione ausiliaria.
Pertanto, il gruppo dell'equazione su questo campo esteso è un sottogruppo normale del gruppo dell'equazione sul campo originale, tale sottogruppo è chiamato da Galois *Decomposizione Propria.*

Definizione (Sottogruppo normale)**.** Sia G un gruppo, $H \leq G$ sottogruppo, diciamo che H è un *sottogruppo normale* di G, $H \lhd G$, se preso $h \in H$, per ogni $g \in G$, si ha che $ghg^{-1} \in H$, ovvero che $gH = Hg$, cioè che le classi laterali sinistre e destre di ogni elemento del gruppo H coincidano.

PROPOSIZIONE IV

Teorema. *Se si aggiunge a un'equazione il valore numerico di una certa funzione delle sue radici, il gruppo dell'equazione si abbasserà in maniera da non avere più altre permutazioni che quelle per le quali questa funzione è invariabile.* ([2] pagina 78)

Galois rimanda la validità di tale risultato alla Proposizione I:
"In effetti, secondo la Proposizione I, ogni funzione nota deve essere invariabile per le permutazioni del gruppo dell'equazione." ([2] pagina 78)



PROPOSITION IV.

Théorème. — *Si l'on adjoint à une équation la valeur* numérique *d'une certaine fonction de ses racines, le groupe de l'équation s'abaissera de manière à n'avoir plus d'autres permutations que celles par lesquelles cette fonction est invariable.*

En effet, d'après la proposition I, toute fonction connue doit être invariable par les permutations du groupe de l'équation.

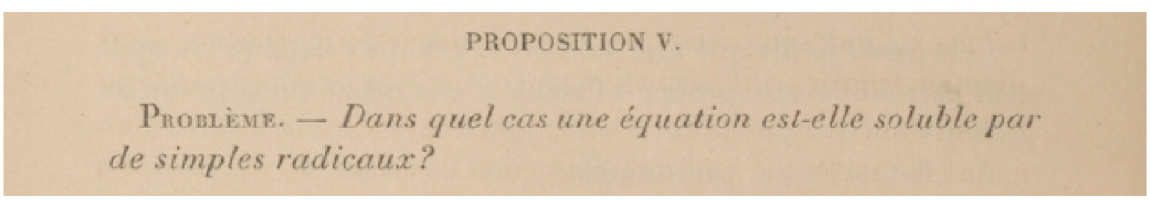
Figura 9: Proposizione IV

Il processo di riduzione del gruppo dell'equazione può essere iterato aggiungendo al campo non solo il valore di una certa funzione delle sue radici, φ_1, ma anche quello di altre funzioni delle sue radici, φ_1', φ_1'', ... Si ottiene, quindi, un sottogruppo che contiene solo sostituzioni che non alterano il valore numerico di tutte le funzioni aggiunte.

Un'ulteriore conseguenza di questo teorema è stata messa in luce da Jordan nella sua opera *Commentaire sur Galois*; siano φ_1 e ψ_1 due funzioni delle radici dell'equazione proposta, se entrambe sono invarianti sotto l'azione dello stesso gruppo di sostituzioni, allora esse si esprimono razionalmente una tramite l'altra. ([15] pagina 149)

PROPOSIZIONE V

Problema. *In quali casi un'equazione è risolvibile per semplici radicali?* ([2] pagina 79)



PROPOSITION V.

Problème. — *Dans quel cas une équation est-elle soluble par de simples radicaux?*

Figura 10: Proposizione V

Anche in questo caso Galois non fornisce una dimostrazione formale al problema, ma una sorta di spiegazione a grandi linee; ciononondimeno alcuni passi sono importanti per chiarire lo scopo delle sue ricerche.

Osserverò innanzitutto che, per risolvere un'equazione, è necessario abbassare successivamente il suo gruppo, fino a che non conterrà che una sola permutazione. Infatti, quando un'equazione è risolta, una funzione qualunque delle sue radici è nota anche quando essa non è invariabile per alcuna permutazione. ([2] pagina 79)

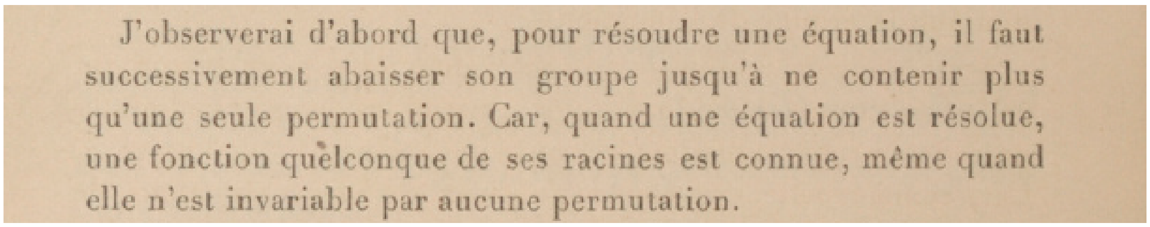

J'observerai d'abord que, pour résoudre une équation, il faut successivement abaisser son groupe jusqu'à ne contenir plus qu'une seule permutation. Car, quand une équation est résolue, une fonction quelconque de ses racines est connue, même quand elle n'est invariable par aucune permutation.

Figura 11: Incipit spiegazione proposizione V

Il gruppo di un'equazione misura il grado di indistinguibilità delle sue radici, finchè esso è composto da permutazioni diverse dalla sola identità si ha una conoscenza imperfetta di tali radici. L'imperfezione è massima quando il gruppo dell'equazione coincide con l'intero gruppo delle permutazioni su n elementi, S_n, e quindi sono note solo le funzioni simmetriche delle radici che non permettono di distinguerle in alcun modo tra loro.

Galois prosegue mostrando come estendere il campo di partenza per far si che il gruppo dell'equazione si riduca, dunque utilizza ancora implicitamente la *corrispondenza di Galois*.

Egli estende il campo iniziale attraverso l'aggiunta di una radice dell'equazione, dunque possiamo trovarci di fronte a due possibilità, o il gruppo dell'equazione non si riduce, e dunque tale estensione di campo è stata una semplice preparazione, oppure il gruppo dell'equazione si riduce. Affinchè l'equazione sia risolubile per radicali occorre che la riduzione del gruppo avvenga in un numero finito di passi. É anche possibile che la riduzione di tale gruppo possa essere realizzata in più modi, ovvero che esistano più di un'estensione di campo che, tramite sempre la corrispondenza di Galois, siano associate a gruppi dell'equazione ridotti. In questi casi, Galois, ci dice di considerare l'estensione di campo realizzata aggiungendo il radicale di indice p, primo, più basso possibile. Tali radicali li battezza come *radicali semplici.*

In seguito, osserva che per la determinazione del gruppo di un'equazione è sempre possibile aggiungere al campo una radice p-esima dell'unità, α, poichè questo radicale non riduce il gruppo.

Dunque, attraverso le proposizioni II e III, Galois conclude che il gruppo dell'equazione si spezza in p sottogruppi che godono delle seguenti proprietà:

1. si passa da un gruppo all'altro tramite una e una sola sostituzione;

2. tutti i gruppi contengono le stesse permutazioni.

Viceversa, Galois suppone che, se il gruppo dell'equazione si può dividere in p sottogruppi che godono delle due proprietà sopra citate, allora mediante un'estrazione di radice p-esima si può ridurre il gruppo dell'equazione ad uno di questi sottogruppi.
Per mostrare ciò egli costruisce una funzione delle radici, $\theta(r_1, r_2, \ldots, r_n)$, che sia invariabile per tutte le sostituzioni di uno dei p sottogruppi, ma che vari invece quando agiscono le altre permutazioni degli altri sottogruppi.
Operando su θ una sostituzione del gruppo totale, che non sia appartenente a quelle dei p sottogruppi, si ottiene un nuovo valore, diverso dal precedente, che chiameremo θ_1. Ora facendo agire su θ_1 la stessa sostituzione otterremo ancora un nuovo valore che chiameremo θ_2, e così via.
Poichè abbiamo che p è primo, questa sequenza sarà formata da $p-1$ valori tutti distinti, che indicheremo come θ_i con $i = 1, 2, \ldots, p-1$.
Se applicassimo $p+k$ volte la stessa sostituzione a θ otterremo il valore θ_k.

La funzione

$$(\theta + \alpha\theta_1 + \alpha^2\theta_2 + \ldots + \alpha^{p-1}\theta_{p-1})^p \tag{6}$$

è invariabile per tutte le permutazioni del gruppo totale dell'equazione, allora per la proposizione I si ha che tale funzione è razionalmente nota.
Ora, se si estrae la radice p-esima di questa funzione e con essa si estende il campo di partenza, per la proposizione IV, il gruppo dell'equazione si riduce alle permutazioni dei p sottogruppi.

Pertanto la condizione sopra esposta è necessaria e sufficiente affinchè un gruppo si possa ridurre.

Iterando il ragionamento sul nuovo gruppo dell'equazione, se questo si decompone nel modo indicato, allora otterremo un altro nuovo gruppo ridotto; e così via, fino a che non avremo un gruppo formato solo dall'elemento neutro.

É implicito nelle parole di Galois il concetto di *serie di composizione* introdotto da Jordan nel 1870.

Definizione (Serie di composizione)**.** Sia G un gruppo, una *serie di composizione* di G è una catena di gruppi, $id = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$, in cui, per ogni $i = 1, 2, \ldots, n$, valgono le seguenti condizioni:

- H_i è un sottogruppo normale massimale[12] di H_{i+1};
- il gruppo quoziente H_{i+1}/H_i è un gruppo semplice[13].

Dopo aver illustrato la proposizione V, Galois passa all'analisi delle equazioni irriducibili di grado primo.

[12] Un *sottogruppo massimale* è un sottogruppo proprio non contenuto in alcun altro sottogruppo.

[13] Un *gruppo semplice* è un gruppo non banale in cui gli unici sottogruppi normali sono il sottogruppo formato dall'elemento neutro e se stesso.

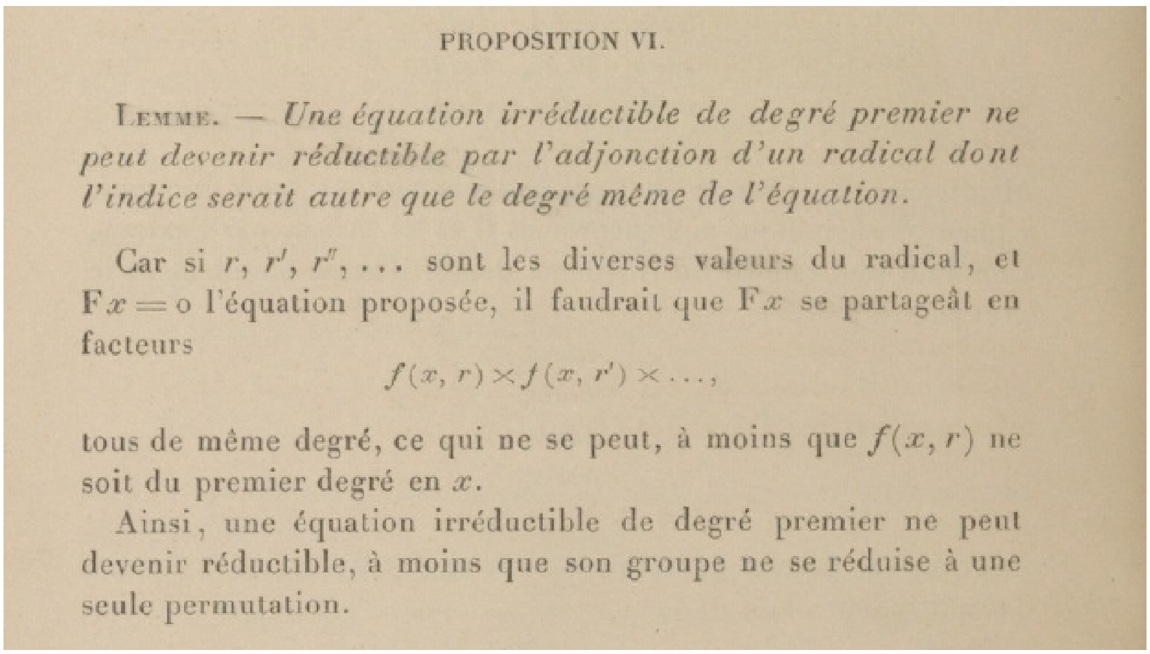
PROPOSIZIONE VI

Lemma. *Un'equazione irriducibile di grado primo non può diventare riducibile tramite l'aggiunzione di un radicale il cui indice sia diverso dal grado stesso dell'equazione.*

Dimostrazione. *"Infatti se* r*,* r'*,* r''*, … sono i diversi valori del radicale, e* $Fx = 0$ *l'equazione proposta, sarebbe necessario che* Fx *si dividesse in fattori*

$$f(x,r) \times f(x,r') \times \ldots$$

tutti dello stesso grado, il che non è possibile a meno che $f(x,r)$ *non sia di primo grado in* x*. Così un'equazione irriducibile di grado primo non può diventare riducibile, a meno che il suo gruppo non si riduca a una sola permutazione."* ([2] pagina 82) □



PROPOSITION VI.

Lemme. — *Une équation irréductible de degré premier ne peut devenir réductible par l'adjonction d'un radical dont l'indice serait autre que le degré même de l'équation.*

Car si r, r', r'', … sont les diverses valeurs du radical, et $Fx = 0$ l'équation proposée, il faudrait que Fx se partageât en facteurs

$$f(x,r) \times f(x,r') \times \ldots,$$

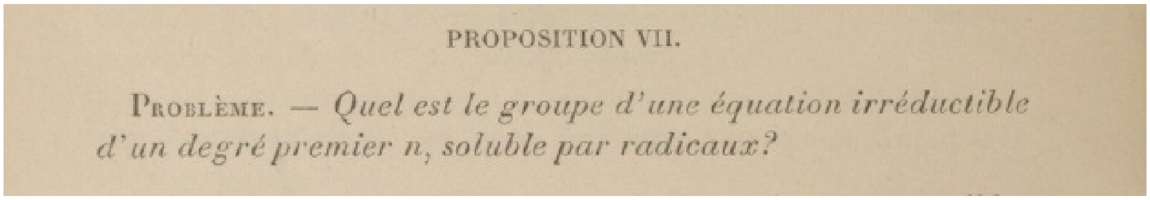
tous de même degré, ce qui ne se peut, à moins que $f(x,r)$ ne soit du premier degré en x.

Ainsi, une équation irréductible de degré premier ne peut devenir réductible, à moins que son groupe ne se réduise à une seule permutation.

Figura 12: Proposizione VI

PROPOSIZIONE VII

Problema. *Qual è il gruppo di un'equazione irriducibile di grado primo* n*, risolubile per radicali?* ([2] pagina 83)



PROPOSITION VII.

PROBLÈME. — *Quel est le groupe d'une équation irréductible d'un degré premier n, soluble par radicaux?*

Figura 13: Proposizione VII

Dalla proposizione VI si ha che il più piccolo gruppo ammissibile, dopo quello formato dalla sola identità, deve contenere n permutazioni. Operando tale gruppo su un insieme di n elementi, si ottiene 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 delle radici, invariante sotto le permutazioni $x_k \to x_{ak+b}$ con a e $b \in \mathbb{Z}$ costanti, sia razionalmente nota.

In alternativa, il risultato qui ottenuto viene enunciato in un altro modo nella proposizione VIII che conclude il *Mémoire*.

PROPOSIZIONE VIII

Teorema. *Perchè un'equazione irriducibile di grado primo sia risolubile per radicali, è necessario e sufficiente che, note due qualsiasi delle radici, le altre si deducano da esse razionalmente.*

Dimostrazione. Innanzitutto è necessario; poichè la sostituzione

$$x_k, \quad x_{ak+b}$$

non lascia mai due lettere allo stesso posto, è chiaro che, aggiungendo due radici all'equazione, per la proposizione IV il suo gruppo dovrà ridursi a una sola permutazione.
In secondo luogo, questo è sufficiente, perchè, in questo caso, nessuna sostituzione del gruppo lascerà due lettere allo stesso posto.
Di conseguenza, il gruppo conterrà al più $n(n-1)$ permutazioni. Dunque non conterrà che una sola sostituzione circolare (altrimenti ci sarebbero almeno n^2 permutazioni). Dunque ogni sostituzione del gruppo, x_k, x_{fk}, dovrà soddisfare alla condizione

$$f(k+c) = fk + C$$

Dunque ecc.
Il teorema è quindi dimostrato.
([2] pagina 86) □

PROPOSITION VIII.

Théorème. — *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 rationnellement.*

Premièrement, il le faut, car la substitution

$$x_k, \quad x_{ak+b}$$

ne laissant jamais deux lettres à la même place, il est clair qu'en adjoignant deux racines à l'équation, par la proposition IV, son groupe devra se réduire à une seule permutation.

En second lieu, cela suffit; car, dans ce cas, aucune substitution du groupe ne laissera deux lettres aux mêmes places. Par conséquent, le groupe contiendra tout au plus $n(n-1)$ permutations. Donc, il ne contiendra qu'une seule substitution circulaire (sans quoi il y aurait au moins n^2 permutations). Donc, toute substitution du groupe, x_k, x_{fk}, devra satisfaire à la condition

$$f(k+c) = f(k) + C.$$

Donc, etc.

Le théorème est donc démontré.

Figura 14: Proposizione VIII

3.4 Delle equazioni primitive che sono risolubili per radicali

Questo manoscritto incompiuto è il terzo e ultimo lavoro che forma la *Seconda Memoria* di Galois.

In essa, Galois considera due diverse questioni: la prima riguarda l'applicazione delle condizioni di risolubilità per radicali a una classe di equazioni che egli chiama "primitive", la seconda, invece, concerne l'applicazione della teoria delle equazioni algebriche alle equazioni modulari delle funzioni ellittiche.

Essa ha suscitato meno interesse rispetto alla prima, e dunque è stata scarsamente analizzata.

Gli altri due scritti che compongono questa *Seconda Memoria* sono, i già affrontati, *Analisi di una memoria sulla risoluzione algebrica delle equazioni* e *Sulla teoria dei numeri*, entrambi pubblicati nel 1830 nel *"Bulletin des Sciences mathématiques, astronomiques, physiques et chimiques"* di Ferussac.

Il manoscritto del frammento in questione non è datato; tuttavia, in esso Galois ricorre a risultati sulla risolubilità di un'equazione per radicali, che ci lasciano intendere che la sua stesura sia posteriore a quella dell'articolo del giugno 1830.

La lettura diretta è insufficientemente comprensibile rispetto alla prima memoria.

Per quanto ci è al momento noto, l'unico matematico che si è dedicato all'analisi di quest'ultimo manoscritto è Camille Jordan.
A tal proposito, anche Laura Toti Rigatelli, la più importante biografa di Évariste Galois, afferma che *"Dés équations primitives qui sont solubles par radicaux"* sia stato fino ad oggi approfondito in maniera proficua solo dal matematico sopra citato. Il suo *"Traitré des substitutions et des équations algébriques"* fa il punto sugli sviluppi dell'algebra nei cento anni che lo hanno preceduto, implementandone molti aspetti e risolvendone molte tralasciate lacune. Il suo è un contributo originale, che segna l'avvio dello sviluppo della moderna teoria sui gruppi astratti, ed è il punto di partenza per l'applicazione dell'algebra e delle teorie dei gruppi.

In quest'opera, Galois cerca di stabilire una condizione generale in cui un'equazione primitiva sia risolubile per radicali; a riguardo egli afferma:

"Ora possiamo qui di seguito stabilire un carattere generale fondato sul grado stesso di queste equazioni. Questo carattere è il seguente: perchè un'equazione primitiva sia risolubile per radicali, è necessario che il suo grado sia della forma p^ν, p essendo un numero primo. E da questo seguirà immediatamente che, quando si dovrà risolvere per radicali un'equazione irriducibile il cui grado ammetta dei fattori primi ineguali, non lo si potrà fare che mediante il metodo di decomposizione di Gauss[14]; se no l'equazione sarà irrisolubile." (pagina 88 [2])

[14]**Lemma di Gauss.** Sia $f \in \mathbb{Z}[x]$, se f si fattorizza in modo non banale su $\mathbb{Q}[x]$, allora f si fattorizza in $\mathbb{Z}[x]$.

DES ÉQUATIONS PRIMITIVES

QUI SONT SOLUBLES PAR RADICAUX ([1]).

(Fragment.)

Cherchons, en général, dans quel cas une équation primitive est soluble par radicaux. Or, nous pouvons de suite établir un caractère général fondé sur le degré même de ces équations. Ce caractère est celui-ci : *Pour qu'une équation primitive soit résoluble par radicaux, il faut que son degré soit de la forme p^ν, p étant premier*. Et de là suivra immédiatement que, lorsqu'on aura à résoudre par radicaux une équation irréductible dont le degré admettrait des facteurs premiers inégaux, on ne pourra le faire que par la méthode de décomposition due à M. Gauss; sinon l'équation sera insoluble.

Figura 15: Incipit "Delle equazioni primitive che sono risolubili per radicali"

4 Commento alla teoria di Galois

Marie Camille Ennemond Jordan è stato uno dei maggiori matematici francesi della fine dell'Ottocento; egli lavorò in un'ampia varietà di settori, contribuendo praticamente ad ogni argomento matematico studiato in quel periodo; ne sono una testimonianza la serie di teoremi ed enunciati che prendono il suo nome.
Jordan riuscì a cogliere la profondità del pensiero di Galois, e alla teoria di Galois dedicò pregevoli memorie e il monumentale *Traité des substitutions et des équations algébriques* (Trattato delle sostituzioni e delle equazioni algebriche, 1870). Si deve, dunque, a Jordan la prima esposizione sistematica della teoria di Galois.

Di seguito presenteremo le idee di Galois relative al *Mémoire* seguendo l'approccio del *Commentaire sur Galois*[15] di Jordan.

Nella parte preliminare Jordan delinea che cosa intende per *gruppo di sostituzioni*, *gruppo transitivo*, *trasformazione di una sostituzione*, *gruppo trasformato*, *gruppo semplice* e *gruppo composto.*

Definizione (Gruppo di sostituzioni)**.** *Un sistema di sostituzioni forma un gruppo, se il prodotto di due sostituzioni qualsiasi appartenenti al sistema, appartiene ancora al sistema.* (pagina 141 [15])

Definizione (Gruppo transitivo)**.** *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.* (pagina 141 [15])

Definizione (Trasformazione di una sostituzione)**.** Siano a, b due sostituzioni, la trasformazione di a da parte di b è la sostituzione bab^{-1}.

Definizione (Gruppo trasformato)**.** Dato un gruppo $\{a, a_1, a_2, \ldots\}$, sottogruppo di un gruppo G, il suo gruppo trasformato da $b \in G$ è il gruppo formato dagli elementi $\{bab^{-1}, ba_1b^{-1}, ba_2b^{-1}, \ldots\}$

Inoltre, Jordan osserva che se il gruppo trasformato coincide con quello di partenza, allora tale gruppo si dice *commutabile con b*. Questo non è altro che il concetto di sottogruppo normale in G.

Definizione (Gruppo semplice e gruppo composto)**.** *Un gruppo si dice semplice se non contiene alcun gruppo, eccetto quello formato dalla sola identità, col quale le sue sostituzioni siano permutabili; in caso contrario il gruppo si dirà composto.* ([15] pagina 142)

Nel capitolo successivo, *Théorie des irrationnelles algébrique* (Teoria degli irrazionali algebrici), Jordan introduce i primi tre lemmi di Galois, accompagnati da dimostrazioni accurate, per poi passare alle proposizioni; di queste solo la prima e in parte la quarta sono analoghe a quelle del *Mémoire*. Egli, infatti, percorre una strada alternativa nel tentativo di chiarire i risultati ottenuti da Galois.

[15] Questo lavoro è un commento alla teoria di Galois che è stato poi incluso e rivisto nell'opera magna *Traité des substitutions et des équations algébriques.*

Mostrata la prima proposizione, Jordan espone i seguenti risultati:

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*[16]. ([15] pagina 147)

Dimostrazione. Poichè $\varphi_1 - \psi_1 = 0 \in \mathbb{Q}$, allora presa la sostituzione $a \in G$ si ha che $\varphi_a - \psi_a = 0$. □

Teorema II. *Ogni equazione irriducibile $F(x) = 0$ ha il suo gruppo transitivo e viceversa.* ([15] pagina 147)

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.* ([15] pagina 147)

Dimostrazione. Consideriamo la funzione $V_1(x_1, \ldots, x_\nu)$ che gode delle proprietà dei lemmi II e III di Galois. V_1 è esprimibile in funzione della sola radice x_1, quindi $V_1 = f(x_1)$.
V_1 è soluzione della seguente equazione di grado ν

$$(t - f(x_1)) \cdots (t - f(x_\nu)) = 0\,,$$

dove i coefficienti di tale equazione sono razionali poichè sono simmetrici nelle quantità $x_1, \ldots, x_\nu$.

Poichè l'ordine del gruppo dell'equazione di partenza, G, è pari al grado dell'equazione irriducibile di cui V_1 è radice, per il lemma I esso non può essere maggiore di ν.

Ora, essendo il gruppo G transitivo, si ha che in esso devono esserci almeno ν elementi, l'identità e altre $\nu - 1$ sostituzioni, le quali portano le altre radici, $x_2, \ldots, x_\nu$, nel posto occupato da x_1.

Dunque G ha esattamente ν elementi. □

Questo teorema ci fornisce la condizione sotto la quale il gruppo di un'equazione irriducibile ha ordine pari al grado dell'equazione stessa.

Il teorema IV di Jordan è l'equivalente logico della proposizione IV di Galois, è stata solo riformulata in altri termini.

Teorema IV. *Sia G il gruppo di un'equazione $F(x) = 0$, φ_1 una funzione razionale qualsiasi delle sue radici: 1°. Le sostituzioni di G che non modificano il valore numerico di φ_1 formano un gruppo H_1: 2°. L'aggiunta del valore di φ_1 ridurrà il gruppo dell'equazione precisamente ad H_1.* ([15] pagina 148)

Tuttavia è doveroso osservare che se φ_1 fosse una funzione che assume un valore razionale, allora

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

aggiungendo questo valore al campo dei coefficienti non si avrebbe nessuna estensione di campo, pertanto, per la corrispondenza di Galois, il gruppo dell'equazione non si ridurrebbe.

Dimostrazione. 1) Prese due sostituzioni a, $a_1 \in G$ che non modificano il valore di φ_1, avremo

$$\varphi_a = \varphi_1, \quad \varphi_{a_1} = \varphi_1.$$

Applicando a_1 alla prima relazione, si ha per il corollario I che

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

ciò mostra la chiusura delle sostituzioni che non alterano φ_1.
Indichiamo con H_1 l'insieme delle sostituzioni che lasciano inalterato il valore numerico di φ_1, per la definizione di Jordan di gruppo di sostituzioni si ha che H_1 è un gruppo. Più precisamente H_1 è sottogruppo di G.

2) Estendiamo il campo dei coefficienti, $\mathbb{Q}$, aggiungendo il valore di φ_1, ottenendo quindi il campo $\mathbb{Q}(\varphi_1)$. Pertanto ora φ_1 è razionalmente noto in questo nuovo campo; quindi il nuovo gruppo dell'equazione, che chiameremo G', riferito a $\mathbb{Q}(\varphi_1)$ sarà formato da sostituzioni che lasciano inalterato il valore di φ_1. Ciò comporta che $G' \subseteq H_1$.

Viceversa, sia $a \in H_1$ e sia ψ_1 una funzione delle radici $r_1, \ldots, r_n$ dell'equazione proposta, inoltre supponiamo che ψ_1 sia esprimibile in $\mathbb{Q}(\varphi_1)$. Esiste una dipendenza razionale tra ψ_1 e φ_1, che possiamo rappresentare come $\psi_1 = \chi(\varphi_1)$, dove χ indica una funzione razionale.
Poichè $\psi_1 - \chi(\varphi_1) = 0$, per il corollario I, si ha che tale relazione resta valida anche se si applica una qualunque sostituzione di G, in particolare vale per $a \in H_1$

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

dal momento che $\varphi_a = \varphi_1$ si ottiene che $\psi_a = \psi_1$, per cui a appartiene anche al gruppo ridotto G'; ne segue che $H_1 \subseteq G'$.
Siccome $G' \subseteq H_1 \subseteq G'$ concludiamo che $G' = H_1$, ciò dimostra il teorema. □

Dimostrato il teorema Jordan fa seguire due corollari:

Corollario I. *Estendendo il campo $\mathbb{Q}$ aggiungendo oltre a φ_1 anche i valori di altre funzioni razionali delle radici, φ_1', φ_1'' ..., il gruppo G prosegue nel suo processo di restrizione, fino a combaciare con il gruppo che lascia inalterati tutti i valori delle funzioni introdotte.*

Corollario II. *Prese due funzioni delle radici dell'equazione proposta, φ_1 e ψ_1, invarianti sotto l'azione dello stesso gruppo di sostituzioni in G, allora esse si esprimono razionalmente una tramite l'altra.*

Teorema V. *Ferme restando le ipotesi come nel teorema precedente, siano $a_0, a_1, a_2, \ldots$ le sostituzioni di H_1:*

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

quelle di G: l'equazione

$$(Y-\varphi_1)(Y-\varphi_b)(Y-\varphi_c)\cdots=0 \tag{7}$$

il cui grado è pari al rapporto tra l'ordine di G e quello di H_1, avrà coefficienti razionali e sarà irriducibile[17]. ([15] pagina 149)

Jordan con a_0 indica l'identità di G.

Teorema VI. *Ferme restando le ipotesi dei teoremi precedenti, 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.* ([15] pagina 150)

In sostanza I è il sottogruppo normale di G, che è anche massimale tra tutti quelli contenuti in H_1.
Jordan osserva che, se $H_1 \lhd G$, allora $H_1 = H_b = H_c = \cdots = I$ e le funzioni φ_1, φ_b, φ_c, ..., essendo invarianti sotto l'azione delle medesime sostituzioni di G, si esprimono razionalmente in funzione di una sola di esse.
Viceversa, se φ_1, φ_b, φ_c, ... si esprimono razionalmente in funzione di una sola di esse, allora queste sono invarianti per lo stesso insieme di sostituzioni di G, pertanto $H_1 = H_b = H_c = \cdots = I$, con $I \lhd G$.

Teorema VII. *Sia N l'ordine di G, $N' = \dfrac{N}{\nu}$ l'ordine di I. L'ordine del gruppo G' dell'equazione* (7) *sarà ν.* ([15] pagina 151)

Quindi l'equazione (7) ha grado uguale all'ordine del suo gruppo di Galois.

Chiudiamo questa veloce esposizione del *Commentaire* con il seguente teorema, visto anche che i risultati successivi trattano questioni che il povero Galois non è riuscito ad affrontare, a causa del sopraggiungere del duello.

Teorema IX. *Sia $F(x)$ un'equazione il cui gruppo G sia composto: G, I, I', ... una successione di gruppi tali che: 1°. Ciascuno di essi è contenuto in quello che lo precede e commutabile con le sostituzioni di quest'ultimo; 2°. Ciascuno di essi sia il più generale tra quelli che soddisfano alle due proprietà menzionate; siano N, $\dfrac{N}{\nu}$, $\dfrac{N}{\nu\nu'}$, ... 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.* ([15] pagina 152)

Jordan sta introducendo la *serie di composizione* del gruppo G, cioè una successione di sottogruppi del tipo:

$$id = I_n \leq \cdots \leq I_1 \leq I_0 = G\,,$$

dove per ogni k, I_k è un sottogruppo normale massimale contenuto in I_{k-1}.
Quando gli indici di ciascuno di questi sottogruppi in quello che lo precede nella serie di composizione, ν, ν', ..., sono tutti numeri primi[18], allora l'equazione corrispondente (7) è risolubile per radicali.

[17] L'irriducibilità è riferita a $\mathbb{Q}$.
[18] Tale condizione implica che I_{k-1}/I_k è un gruppo commutativo.

L'approccio ai gruppi di Galois, perfezionato da Jordan, consiste nel tradurre la richiesta di risolubilità algebrica di un'equazione in una richiesta sulla struttura del gruppo associato.

5 Conclusioni

L'oggetto principale delle ricerche di Galois era stato quello di determinare in quali casi equazioni polinomiali del tipo $a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n = 0$ fossero risolvibili mediante radicali, ossia quando gli zeri di tale equazione sono esprimibili attraverso operazioni razionali ed estrazione di radici n-esime effettuate sui coefficienti. Il suo approccio al problema, oggi noto come *teoria di Galois*, rappresenta uno dei molti risultati altamente originali raggiunti dall'algebra nel XIX secolo.
Évariste cominciò le sue ricerche a partire da alcuni lavori di Lagrange sulle permutazioni delle radici di un'equazione polinomiale; poi, traendo ispirazione dalla dimostrazione di Abel dell'irrisolvibilità dell'equazione di quinto grado mediante radicali, scoprì che un'equazione algebrica irriducibile è risolvibile mediante radicali se e soltanto se il gruppo simmetrico delle sue soluzioni è risolvibile.
La teoria di Galois può fornire un algoritmo per trovare effettivamente le radici di un'equazione, quando queste siano esprimibili mediante radicali; ma nel suo approccio alla teoria delle equazioni l'accento è generalmente posto più sulla struttura algebrica che non sulla trattazione di casi specifici.

L'opera di Évariste fu importante non solo per avere introdotto come elemento fondamentale nella teoria delle equazioni la nozione di gruppo, ma anche per aver portato, attraverso i contributi di matematici a lui successivi, quali Dedekind e Kronecker, a quella che possiamo chiamare *aritmetizzazione dell'Algebra*. Ciò non significa un ritorno alla concezione dell'Algebra in vigore nel Medioevo e nel Rinascimento, ossia la ricerca di un algoritmo per trovare un numero ignoto. Significa, invece, lo sviluppo di un'accurata trattazione assiomatica di strutture algebriche in termini di campi numerici.

Il risultato cardine della teoria di Galois risiede nella Proposizione V del *Mémoire*, nella quale viene mostrato il legame tra i campi intermedi, ottenuti estendendo il campo di partenza con l'aggiunta di radici di equazioni ausiliarie, e i sottogruppi del gruppo dell'equazione, ovvero del gruppo di Galois. Tale legame oggi è noto come *Corrispondenza di Galois*.
Pertanto, questa proposizione è fondamentale perché mostra come la risolubilità di un'equazione dipenda dalla simmetria delle sue radici.

La comprensione della teoria di Galois è essenziale in molteplici ambiti, dalla crittografia alla fisica teorica, dove l'analisi delle simmetrie riveste un ruolo cruciale.
La sua breve e travagliata vita ha aggiunto un alone di tragedia al suo lavoro, ma anche un'aura di leggenda intorno alla sua figura.

Bibliografia

[1] Évariste Galois: *Oeuvres mathématiques d'Évariste Galois*. Gauthier-Villars et fils (Paris) (1897).

[2] Évariste Galois: *Scritti Matematici*, a cura di Laura Toti Rigatelli, Bollati Boringhieri, Mappano di Caselle (Torino) (2000).

[3] Évariste Galois: *OEuvres mathématiques*. J. Math. Pures Appl., 11 (S. 1), 381—444, (1846).

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

[5] Tony Rothman: *Genius and biographers: the fictionalization of Évariste Galois*. Amer. Math. Monthly

[6] Évariste Galois: *Démonstration d'un théorème sur les fractions continues périodiques.* Annales de mathématiques pures et appliquées. Tome 19, pp.294-301, (1828-1829).

[7] Évariste Galois: *Notes sur quelques points d'Analyse*. Annales de mathématiques pures et appliquées. 21, 182-184, pp. 392-394, (1830-1831).

[8] Évariste Galois: *Analyse d'un mémoire sur la résolution algébrique des équations*. Bulletin des sciences mathématiques, astronomiques, physiques et chimiques. Tomes 13, pp. 271-272 (1830).

[9] Évariste Galois: *Note sur la résolution des équations numériques*. Bulletin des sciences mathématiques, astronomiques, physiques et chimiques. Tomes 13, pp. 413-414 (1830).

[10] Évariste Galois: *Sur la théorie des nombres*. Bulletin des sciences mathématiques, astronomiques, physiques et chimiques. Tomes 13, pp. 428-444 (1830).

[11] Évariste Galois: *Mémoire sur les conditions de résolubilité des équations par radicaux.* Journal de mathématiques pures et appliquées ou Recueil mensuel de mémoires sur les diverses parties de mathématiques publié par Joseph Liouville. Tome XI, p. 417-433 (1846).

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

[13] Joseph-Louis Lagrange: *Réflexions sur la résolution algebrique des équations, Nouveaux Mémoire*. de l'Académie des sciences et Belles-Lettres de Berlin, **1**, 134–215, (1770); **2**, 138-253, (1771). In Œuvers Complétes, vol. 3, J.A. Serret, Ed., Gauthier-Villars, Paris, (1869), 205-421.

[14] Joseph-Louis 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.

[15] Camille Jordan: *Commentaire sur Galois*. Math. Annalen 1, Paris, 141–160, (1869).

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

[17] Carl B. Boyer: *Storia della Matematica*, traduzione di Adriano Carugo, Mondadori, prefazione di Lucio Lombardo Radice (2000).

[18] Morris Kline: *Storia del pensiero matematico, vol. II ("Dal Settecento ad oggi")*, Giulio Einaudi editore, Torino, (1991).

[19] Leopold Infield: *Évariste Galois: La breve vita di un genio della matematica*, Castelvecchi editore, (2015).

[20] Leopold Infield: *Tredici ore per l'immortalità. La vita del matematico Galois*, Feltrinelli, (1957).

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

[22] Carl Friedrich Gauss: *Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse*, in Gauss Werke, vol. 3, Göttingen, (1866), 1-30.

[23] Paolo Ruffini: *Teoria generale delle Equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto*, Bologna, Stamperia di San Tommaso d'Aquino, (1799). In Opere Matematiche di Paolo Ruffini a cura di E. Bortolotti, vol. 1, pp. 1–324, Cremonese, Roma, (1953).