# OPERE MATEMATICHE
## pubblicate sotto gli auspici della società matematica di Francia con una introduzione di M. Émile Picard

Evariste Galois

## Introduzione


Le Opere di Galois sono, come si sa, state pubblicate nel 1846 da Liouville, nel *Journal de Mathématiques*. Era spiacevole non poter possedere le Opere del grande matematico; così la Società matematica ha deciso di far ristampare le Memorie di Galois. Questa edizione è conforme alla precedente; si è solamente soppresso l'avvertimento posto da Liouville all'inizio della pubblicazione.

Un lavoro, che sembra definito, sul percorso di Galois fu pubblicato da M. Paul Dupuy, negli Annales de *l'École Normale supérieur* (1896). Come documenti anteriori relativi alla vita di Galois, bisogna citare l'Annuncio necrologico che gli dedicò l'amico Auguste Chevalier, nella *Revue encyclopédique* (settembre 1832) e un articolo apparso nel *Magasin pittoresque*, nel 1848. Evariste Galois è nato a Bourg-la-Reine, vicino Parigi, il 25 ottobre 1811; lasciò la casa paterna nel 1823, per entrare in quarta al collegio Louis-le-Grand. Dall'età di quindici anni, le sue straordinarie predisposizioni per le Scienze matematiche iniziano a manifestarsi; i libri elementari di Algebra non lo soddisfano ed è nelle Opere classiche di Lagrange che forma la sua educazione algebrica. Sembra che a diciassette anni Galois avesse già ottenuto risultati della massima importanza riguardanti la teoria delle equazioni algebriche. Si possono avanzare solo

delle congetture sul percorso delle sue idee, le due Memoria che egli presentò all'Accademia delle Scienze sono state perse; una cosa tuttavia è certa: era, all'inizio del 1830, in possesso dei suoi principi generali, come mostra l'analisi di una Memoria sulla risoluzione algebrica delle equazioni nel Bullettin de Férussac, dove sono enunciati una serie di risultati che sono chiaramente applicazioni di una teoria generale. Questo breve articolo è il più importante che sia stato pubblicato dallo stesso Galois, la Memoria fondamentale sull'Algebra ritrovata nei suoi quaderni e stampata solo nel 1846.

Si troveranno, nell'articolo di M. Dupuy, informazioni di grande interesse sulla vita di Galois. È poco probabile che ormai si possano aggiungere nuovi documenti a quelli che possediamo ora. Dopo due insiccessi all'École Polytechnique, Galois entrò all'École Normale nel 1829 e fu obbligato a lasciarla l'anno successivo. Nell'ultimo anno della sua vita, si dedico interamente alla politica, posso parecchi mesi dentro Sainte Pélagie e, ferito mortalmente in duello, morì il 31 maggio 1832. In presenza di una vita così breve e tormentata, l'ammirazione raddoppia per il genio prodigioso che ha lasciato nella Scienza una traccia così profonda; gli esempi di produzioni precoci non sono rari presso i grandi matematici, ma quello di Galois è notevole tra tutti. Sembra che il giovane sfortunato abbia tristemente pagato il riscatto del suo genio. Con lo svilupparsi delle sue brillanti capacità matematiche, si vede incupirsi il suo carattere, altrimenti gaio e aperto. e il sentimento della sua immensa superiorità sviluppa in lui un orgoglio eccessivo. Questa fu la causa delle delusioni che ebbero tanta influenza sulla sua carriera, e la prima delle quali fu lo smacco all'École Polytechnique. Il suo esame in questa École lasciò ricordi: senza correre troppo come vuole la leggenda, diciamo solo che Galois rifiutò di rispondere a una domanda, che giudicava ridicola, sulla teoria aritmetica dei logaritmi. Non ci possono essere dubbi quindi che si sia prestato a fornire sui suoi lavori le spiegazioni che gli richiedevano i matematici con i quali era in contatto, spiegazioni che rendeva necessariamente la produzione rapida delle sue Memorie; così si comprende facilmente che il merito non è stato riconosciuto dai suoi contemporanei. Fu con grande pazienza che Liouville riuscì a cogliere il legame delle idee di Galois, e furono necessari ancori numerosi commentatori per completare le lacune che rimanevano in più di una dimostrazione, e per riportare le teorie del grande matematico al grado di semplicità che rivestono oggi.

La teoria delle equazioni deve a Lagrangre, Gauss e Abel i progressi considerevoli, ma nessuno di essi giunse a mettere in evidenza l'elemento fondamentale da cui dipendono tutte le proprietà delle equazioni; questa gloria era riservata a Galois, che mostrò che a ogni equazione algebrica corrisponde un gruppo di sostituzioni nel quale si riflettono i caratteri essenziali dell'equazione. In Algebra, la teoria dei gruppi era stata prima l'oggetto di numerose ricerche dovute, per la maggior parte, a Cauchy, che aveva introdotto già alcuni elementi di classificazione; gli studi di Galois sulla Teoria delle equazioni gli mostrarono l'importanza della nozione di sotto-gruppo invariante di un gruppo dato, e fu così portato a dividere i gruppi in gruppi semplici e composti, distinzione fondamentale che supera di molto, in realtà, il campo dell'Algebra e si estende al concetto di gruppi di operazioni nella sua accezione più estesa.

Le teorie generali, per prendere nella Scienza diritto di menzione definitivo, hanno più spesso bisogno di illustrarsi mediante applicazioni particolari. In parecchi campi, queste non sono sempre facili da trovare, e si potrebbe citare, nei Matematici moderni, più di una teoria confinata, se oso dire, nella sua eccessiva generalità; dal punto di vista artistico, che gioca un ruolo capitale nelle Matematiche pure, nulla è più soddisfacente dello sviluppo di queste grandi teorie, tuttavia buone menti respingono questa tendenza, che ha forse i suoi pericoli. Non si può emettere, per Galois, un simile rammarico; la risoluzione algebrica delle equazioni gli ha fornito, dall'inizio, un campo particolare di applicazioni dove lo seguirono poi numerosi matematici, tra i quali si deve citare al primo posto M. Camille Jordan.

I lavori di Galois, sulle equazioni algebriche, hanno reso il suo nome celebre, ma sembra che egli abbia fatto, in Analisi, scoperte almeno molto importanti. Nella sua lettera a Auguste Chevalier, scritta la vigilia della sua morte, e che è una specie di testamento scientifico, Galois parla di una Memoria che si potrebbe comporre con le sue ricerche sugli integrali. Non conosciamo

di queste ricerche se non ciò che dice in questa lettera; numerosi punti rimangono oscuri in qualche enunciato di Galois, ma si può tuttavia farsi un'idea precisa di alcuni dei risultati ai quali era giunto nella teoria degli integrali di funzioni algebriche. Si acquista così la convinzione che era in possesso di risultati più essenziali sugli integrali abeliani che Riemann doveva ottenere venticinque anni più tardi. Non vediamo senza stupore Galois parlare dei periodi di un integrale abeliano relativo a una funzione algebrica qualunque; per gli integrali iperellittici, non abbiamo alcuna difficoltà a comprendere ciò che intende per *periodo*, ma non è così nel caso generale, e si è quasi tentati di supporre che Galois aveva prefigurato almeno certe nozioni sulle funzioni di una variabile complessa, che verranno sviluppate solo numerosi anni dopo la sua morte. Gli enunciati sono precisi; l'illustre autore fa la classificazione in tre specie degli integrali abeliani, e afferma che, se $n$ indica il numero degli integrali di prima specie linearmente indipendenti, i periodi saranno in numero di $2n$. Il teorema relativo all'inversione del parametro e dell'argomento negli integrali di terza specie è nettamente indicato, così come le relazioni tra i periodi degli integrali abeliani; Galois parla così di una generalizzazione dell'equazione classica di Legendre, dove figurano i periodi degli integrali ellittici, generalizzazione che l'aveva probabilmente portato alle importanti relazioni scoperte poi da Weirstrass e da M. Fuchs. Ne abbiamo parlato assai per mostrare l'estensione delle scoperte di Galois in Analisi; se qualche anno in più gli fossero stati dati per sviluppare le sue idee in questa direzione, sarebbe stato il glorioso continuatore di Abel e avrebbe edificato, nelle sue parti essenziali, la teoria delle funzioni algebriche di una variabile come la conosciamo oggi. Le riflessioni di Galois portarono ancora più lontano; egli concluse la sua lettera parlando dell'applicazione all'Analisi trascendente della teoria dell'ambiguità. Si ricava all'incirca ciò che intende per questa, e su questo terreno che, come dice, è immenso, rimane ancora oggi molto da scoprire e da fare.

Non è senza emozione che si termina la lettura del testamento scientifico di questo giovane di venti anni, scritto la vigilia del giorno in cui doveva scomparire in una oscura disputa. La sua morte fu per la Scienza una perdita immensa; l'influenza di Galois, se fosse vissuto, avrebbe grandemente modificato l'orientazione delle ricerche matematiche nel nostro paese. Non mi arrischierò in confronti pericolosi: Galois ha senza dubbio uguali tra i grandi matematici di questo secolo; nessuno lo supera per l'originalità e la profondità delle sue concezioni.

Émile Picard

Presidente della Società matematica di Francia.

# Opere Matematiche di Evariste Galois

# I. Articoli pubblicati da Galois

## Dimostrazione di un teorema sulle frazioni continue periodiche[1]

Sappiamo che se, con il metodo di Lagrange, sviluppiamo in frazione continua una delle radici di un'equazione di secondo grado, questa frazione continua sarà periodica, e sarà ancora anche per una delle radici di un'equazione di qualsiasi grado, se questa radice è radice di un fattore razionale di secondo grado di primo membro della proposta, nel qual caso questa equazione avrà, almeno, un'altra radice che sarà anch'essa periodica. In entrambi i casi, la frazione continua può anche essere immediatamente periodica o non esserlo immediatamente, ma, quando si verificherà quest'ultima circostanza, ci sarà almeno una delle trasformate di cui una delle radici sarà immediatamente periodica.

Ora, quando un'equazione ha due radici periodiche, rispondendo a uno stesso fattore razionale di secondo grado, e che uno di essi è immediatamente periodico, esiste tra queste due radici una relazione assai singolare che sembra non essere stata ancora notata, e che può essere espressa dal seguente teorema:

Teorema. *Se una delle radici di un'equazione di grado qualsiasi 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 continua periodica, scritta in ordine inverso.*

Dimostrazione. Per fissare le idee, prendiamo solo periodi di quattro termini; perché il cammino uniforme del calcolo dimostra che sarebbe lo stesso se ne ammettessimo di più. Sia una delle radici di un'equazione di grado qualsiasi espressa come segue: □

$$x=a+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}+\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}+\dots\dots;$$

l'equazione di secondo grado, alla quale apparterrà questa radice e che conterrà di conseguenza la sua correlativa, sarà

$$x=a+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}+\frac{1}{x};$$

ora si ricava da ciò successivamente

$$a-x=-\frac{1}{b}+\frac{1}{c}+\frac{1}{d}+\frac{1}{x}, \qquad \frac{1}{a-x}=-(b+\frac{1}{c}+\frac{1}{d}+\frac{1}{x})$$

$$b+\frac{1}{a-x}=-\frac{1}{c}+\frac{1}{d}+\frac{1}{x}; \qquad \frac{1}{b}+\frac{1}{a-x}=-(c+\frac{1}{d}+\frac{1}{x})$$

$$c+\frac{1}{b}+\frac{1}{a-x}=-\frac{1}{d}+\frac{1}{x}, \qquad \frac{1}{c}+\frac{1}{b}+\frac{1}{a-x}=-(d+\frac{1}{x})$$

$$d+\frac{1}{c}+\frac{1}{b}+\frac{1}{a-x}=-\frac{1}{x}, \qquad \frac{1}{d}+\frac{1}{c}+\frac{1}{b}+\frac{1}{a-x}=-x$$

cioè

$$x=-\frac{1}{d}+\frac{1}{c}+\frac{1}{b}+\frac{1}{a-x}$$

[1]Libro XIX degli *Annales de Mathématiques* di M. Gergonne, pag. 294. Galois era allora allievo al collegio Luois-le-Grand. (J. Liouville)

è quindi sempre quella l'equazione di secondo grado che dà le due radici di cui si tratta; ma mettendo continuamente per $x$, nel suo secondo membro, questo stesso secondo membro che ne è in effetti il valore, dà

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

quindi questo è l'altro valore di $x$, dato da questa equazione; valore che, come si vede, è uguale a $-1$ diviso per il primo.

In quanto sopra abbiamo assunto che la radice proposta era più grande dell'unità; ma, se si avesse

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

se ne concluderebbe, per uno dei valori di $\frac{1}{x}$,

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

l'altro valore di $\frac{1}{x}$ sarà quindi, per quanto detto

$$\frac{1}{x}=-\frac{1}{d}+\frac{1}{c}+\frac{1}{b}+\frac{1}{a}+\frac{1}{d}+\frac{1}{c}+\frac{1}{b}+\frac{1}{a}+\ldots,$$

da cui si concluderà, per l'altro valore di $x$,

$$x=-(d+\frac{1}{c}+\frac{1}{b}+\frac{1}{a}+\frac{1}{d}+\frac{1}{c}+\frac{1}{b}+\frac{1}{a}+\ldots$$

o

$$x=-\frac{1}{d+\frac{1}{c}+\frac{1}{b}+\frac{1}{a}+\frac{1}{d}+\frac{1}{c}+\frac{1}{b}+\frac{1}{a}}$$

ciò che rientra esattamente nel nostro teorema.

Sia $A$ una frazione continua qualunque, immediatamente periodica, e sia $B$ la frazione continua che se ne deduce invertendo 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 tra 0 e $-1$, $-\frac{1}{B}$ sarà un numero positivo maggiore dell'unità. Così, quando una delle radici di una equazione di secondo grado è una frazione continua immediatamente periodica, maggiore dell'unità, l'altra è necessariamente compresa tra 0 e $-1$, e reciprocamente se uno di esse è compresa tra 0 e $-1$, l'altra sarà necessariamente positiva e più grande dell'unità.

Si può dimostrare che, viceversa, se una delle due radici di un'equazione di secondo grado è positiva, è maggiore dell'unità, e che l'altra è compresa tra 0 e $-1$, queste radici saranno esprimibili in frazioni continue immediatamente periodiche. Infatti, sia sempre $A$ una frazione continua immediatamente periodico qualsiasi, positivo e maggiore dell'unità, e $B$ la frazione continua immediatamente periodica che se ne deduce, invertendo il periodo, la quale sarà anche, come essa, positiva e maggiore dell'unità. La prima delle radici della proposta non potrà essere della forma $x = p + \frac{1}{A}$, poiché allora, in virtù del nostro teorema, la seconda dovrà essere $x = a + \frac{1}{-\frac{1}{B}} = a - B$; ora $a - B$ non sarà compreso tra 0 e finché la parte intera di $B$ sarà uguale a $p$; in tale caso il primo valore sarà immediatamente periodico. Non si potrà avere di più, per il primo valore di $x$, $x = p + \frac{1}{q+\frac{1}{A}}$,poiché allora l'altro sarà $x = p + \frac{1}{1-B}$ o $x = p - \frac{1}{B-q}$; ora, affinché questo sia compreso tra 0 e $-1$, servirà dapprima che $\frac{1}{B-q}$ sia uguale a $p$ più una frazione; basterebbe quindi che $B - q$ sia più piccolo dell'unità, ciò che richiederà che $B$ sia uguale a $q$, più

una frazione; da cui si vede che $q$ e $p$ dovranno essere rispettivamente uguali ai due primi termini del periodo che corrisponde a $B$ o ai due ultimi termini del periodo che corrisponde ad $A$; di modo che, contrariamente all'ipotesi, il valore di $x = p + \frac{1}{q+\frac{1}{A}}$, sarà immediatamente periodico. Dimostreremo, con un ragionamento analogo, che i periodi non potranno essere preceduti da un maggiore numero di termini non inclusi in esso.

Quindi, quando si tratterà un'equazione numerica con il metodo de Lagrange, si sarà sicuri che non ci sono radici periodiche da sperare finché non si incontrerà una trasformazione avente almeno una radice positiva maggiore dell'unità e un'altra compresa tra 0 e $-1$; e se, infatti, la radice che si cerca deve essere periodica, al massimo sarà a questa trasformata che inizieranno i periodi.

Se una delle radici di un'equazione di secondo grado è non solo immediatamente periodica ma anche simmetrica, cioè, se i termini del periodo sono a uguale distanza dagli estremi, avremo $B = A$; in modo che queste due radici saranno $A$ e $-\frac{1}{A}$; l'equazione sarà quindi

$$Ax^2 - \left(A^2 - 1\right) x - A = 0$$

Reciprocamente, ogni equazione di secondo grado della forma

$$ax^2 - bx - a = 0$$

avrà le sue radici contemporaneamente immediatamente periodiche e simmetriche. Infatti, mettendo a turno per $x$ l'infinito e $-1$, si ottengono risultati positivi, mentre ponendo $x = 1$ e $x = 0$, si ottengono risultati negativi; da cui si vede che questa equazione ha una radice positiva maggiore dell'unità e una radice negativa compresa tra 0 e $-1$, e che queste radici sono immediatamente periodiche; inoltre, questa equazione non cambia cambiando $x$ in $-\frac{1}{x}$; da cui segue che se $A$ è una delle sue radici l'altra sarà $-\frac{1}{A}$ e che, in questa caso, $B = A$.

Applichiamo queste generalità all'equazione di secondo grado

$$3x^2 - 16x + 18 = 0$$

si trova dapprima una radice positiva compresa tra 3 e 4; ponendo

$$x = 3x + \frac{1}{y}$$

si ottiene la trasformata

$$3y^2 - 2y - 3 = 0$$

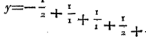
la cui forma ci indica che i valori di $y$ sono contemporaneamente periodiche e simmetriche; infatti, ponendo, a turno

$$y = 1 + \tfrac{1}{z} \quad z = 2 + \tfrac{1}{t} \quad t = 1 + \tfrac{1}{u}$$

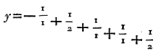
si ottengono le trasformate

$$2z^2 - 4z - 3 = 0$$
$$3t^2 - 4t - 2 = 0$$
$$3u^2 - 2u - 3 = 0$$

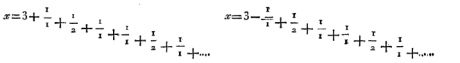
l'identità tra le equazioni in $u$ e in $y$ prova che il valore positivo di $y$ è



il suo valore negativo sarà quindi



i due valori di $x$ saranno quindi



di cui l'ultimo, in virtù della formula nota

$$p-\frac{1}{q}=p-1+\frac{1}{1}+\frac{1}{q-1},$$

diviene

$$x=1+\frac{1}{1}+\frac{1}{1}+\frac{1}{2}+\frac{1}{1}+\frac{1}{2}+\frac{1}{1}+\frac{1}{3}+\frac{1}{2}+\frac{1}{1}+\frac{1}{3}+\frac{1}{2}+\frac{1}{1}+\ldots\ldots$$

# Note su alcuni aspetti di Analisi

## § I. - Dimostrazione di un teorema di Analisi[3]

Teorema. *Siano $Fx$ e $fx$ due funzioni qualunque date; si avrà, qualunque siano $x$ e $h$*

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

*essendo $\varphi$ una funzione determinata, e $k$ una quantità intermedia tra $x$ e $x+h$.*

Dimostrazione. Poniamo, infatti,

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

se ne dedurrà

$$F(x+h)-Pf(x+h)=Fx-Pfx$$

da cui si vede che la funzione $Fx-Pfx$ non cambia quando si cambia $x$ in $x+h$; da cui segue che a meno che essa non rimanga costante tra questi limiti, ciò che potrebbe avvenire solo in casi particolari, questa funzione avrà, tra $x$e $x+h$, uno o più massimi e minimi. Sia $k$ il valore di $x$ corrispondente a uno di essi; si avrà evidentemente $k=\psi(P)$, essendo $\psi$ un'altra funzione determinata; pertanto si deve avere anche $P=\varphi(k)$, essendo $\varphi$ un'altra funzione pure determinata; ciò che dimostra il teorema. □

Da ciò si può concludere come corollario che la quantità

$$\lim\frac{F(x+h)-Fx}{f(x+h)-fx}=\varphi(x)$$

per $h=0$, è necessariamente una funzione di $x$, ciò che dimostra, *a priori*, l'esistenza delle funzioni derivate.

## II. Raggio di curvatura delle curve dello spazio

Il raggio di curvatura di una curva in uno qualunque dei suoi punti $M$ è la perpendicolare abbassata da questo punto sull'intersezione del piano normale al punto $M$ con il piano normale consecutivo, come è facile verificare con considerazioni geometriche.

Ciò posto, sia $(x,y,z)$ un punto della curva; si sa che il piano normale in questo punto avrà per equazione

$$(X-x)\frac{dx}{ds}+(Y-y)\frac{dy}{ds}+(Z-z)\frac{dz}{ds}=0 \tag{0.0.1}$$

essendo $X,Y,Z$ i simboli delle coordinate correnti. L'intersezione di questo piano normale con il piano normale consecutivo sarà dato dal sistema di questa equazione e della seguente

$$(X-x)\frac{d\left(\frac{dx}{ds}\right)}{ds}+(Y-y)\frac{d\left(\frac{dy}{ds}\right)}{ds}+(Z-z)\frac{d\left(\frac{dz}{ds}\right)}{ds}=1 \tag{0.0.2}$$

visto che

$$\left(\frac{dx}{ds}\right)^2+\left(\frac{dy}{ds}\right)^2+\left(\frac{dz}{ds}\right)^2=1$$

[3] *Annales de Mathématiques* di M. Gergonne, libro XXI, pag. 182 (1830-1831). È per una errata stampa che vi si legge: *Galais, élève à l'École normale*, in invece di *Galois*.

Se è facile vedere che il piano $I$ è perpendicolare al piano $N$, poiché si ha

$$\frac{dx}{ds}d\left(\frac{dx}{ds}\right)+\frac{dy}{ds}d\left(\frac{dy}{ds}\right)+\frac{dz}{ds}d\left(\frac{dz}{ds}\right)=0$$

pertanto la perpendicolare abbassata dal punto $(x, y, z)$ sull'intersezione dei due piano $N$ e $I$ non è altra cosa della perpendicolare abbassata dallo stesso punto sul piano $I$. Il raggio di curvatura è quindi la perpendicolare abbassata dal punto $(x, y, z)$ sul piano $I$. Questa considerazione dà, molto semplicemente, i teoremi noti sui raggi di curvatura delle curve nello spazio.

### Analisi di una Memoria sulla risoluzione algebrica delle equazioni[4]

Si chiamano equazioni non primitive le equazioni che, essendo, per esempio, di grado $mn$, si scompongono in $m$ fattori di grado $n$, per mezzo di una sola equazione di grado $m$. Queste sono le equazioni di M. Gauss. Le equazioni primitive sono quelle che non godono di una simile semplificazione. Io sono, riguardo alle equazioni primitive, giunti ai risultati seguenti:

1° Affinché un'equazione di primo grado sia risolvibile per radicali, è necessario e sufficiente che, note due qualunque delle sue radici, le altre si deducano razionalmente.

2° Affinché un'equazione primitiva di grado $m$ sia risolvibile per radicali, è necessario che $m = p^\nu$, essendo $p$ un numero primo.

3° A parte i casi menzionati qui sopra, affinché un'equazione primitiva di grado $p^\nu$ sia risolvibile per radicali, è necessario che, note due qualunque delle sue radici, le altre si deducano razionalmente.

Alla regola precedente sfuggono i casi molto particolari che seguono:

(1) Il caso di $m = p^\nu = 9, = 25$;

Il caso di $m = p^\nu = 4$ e in genere quello dove, essendo $a^\alpha$ un divisore di $\frac{p^\nu-1}{p-1}$, si avrà $a$ primo, e

$$\frac{p^\nu-1}{a^\alpha(p-1)}\nu = p \quad (mod.\, a^\alpha)$$

Questi casi si discostano tuttavia molto poco dalla regola generale.

Quando $m = 9, = 25$, l'equazione diverrà del genere di quelle che determinano la trisezione e la quadrisezione delle funzioni ellittiche.

Nel secondo caso, bisognerà sempre che, essendo note due delle radici, le altre si deducano, almeno per mezzo di un numero di radicali, di grado $p$, uguale al numero dei divisori $a^\alpha$di $\frac{p^\nu-1}{p-1}$, che sono tali che

$$\frac{p^\nu-1}{a^\alpha(p-1)}\nu = p \quad (mod.\, a^\alpha) \quad a\ primo$$

Tutte queste proposizioni sono state dedotte dalla teoria delle permutazioni.

Ecco altri risultati che derivano dalla mia teoria.

1° Sia $k$ il modulo di una funzione ellittica, $p$ un numero primo dato $> 3$; affinché l'equazione di grado $p + 1$, che dà i diversi moduli delle funzioni trasformate rispetto al numero $p$, sia risolvibile per radicali, *bisogna* che delle due cose l'una: o che una delle radici sia razionalmente nota, o che tutte siano funzioni razionali le une delle altre. Non si tratta qui, ben inteso, che di valori particolari di modulo $k$. È evidente che la cosa non avviene in generale. Questa regola non vale per $p = 5$.

2° È da notare che l'equazione modulare generale di sesto grado, corrispondente al numero 5, si può abbassare a una di quinto grado di cui è la ridotta. Al contrario, per gradi superiori, le equazioni modulari non si possono abbassare[5].

[4] *Bulletin des Sciences mathématiques* di M. Férussac, t. XIII, p. 271 (anno 1830, quaderno d'aprile)

[5] Questa affermazione non è del tutto esatta, come Galois notò nella sua lettera a M. Auguste Chevalier, che si trova più avanti. Dice in generale, sul tema dell'articolo qui riprodotto: "La condizione che ho indicato nel *Bullettin de Férusac*, per la risolvibilità mediante radicali, è troppo restrittiva; vi sono alcune eccezioni, ma così è." Quanto alle equazioni modulari in particolare, dichiara l'abbassamento del grado $p + 1$ al grado $p$ possibile, non solo per $p = 5$, ma ache per $p = 7$ e $p = 11$; ma ne mantiene l'impossibilità per $p > 11$.

## Nota sulla risoluzione delle equazioni numeriche[6]

M. Legendre ha per primo osservato che, quando un'equazione algebrica era messa sotto la forma

$$\varphi x = x$$

dove $\varphi x$ è una funzione di $x$ che cresce costantemente con $x$, era facile trovare la radice di questa equazione immediatamente più piccola di un numero dato $a$, se $\varphi a < a$, e la radice immediatamente maggiore di $a$, se $\varphi a > a$.

Per dimostrarlo, si costruisce la curva $y = \varphi x$ e la retta $y = x$. Sia presa un'ascissa $= a$, e supponiamo, per fissare le idee, $\varphi a > a$, dico che sarà facile ottenere la radice immediatamente superiore ad $a$. Infatti, le radici dell'equazione $\varphi x = x$ non sono che le ascisse dei punti di intersezione della retta e della curva, ed è chiaro che ci si avvicinerà al punto più vicino di intersezione sostituendo all'ascissa $a$ l'ascissa $\varphi a$. Si avrà un valore più vicino ancora prendendo $\varphi\varphi a$, poi $\varphi\varphi\varphi a$ e così di seguito.

Sia $Fx = 0$ un'equazione data di grado $n$, e $Fx = X - Y$, avendo $X$ e $Y$ solo termini positivi. Legendre mette successivamente l'equazione sotto queste due forme:

$$x = \varphi x = \sqrt[n]{\frac{X}{\left(\frac{Y}{x^n}\right)}} \quad x = \psi x = \sqrt[n]{\frac{X}{\left(\frac{x^n}{Y}\right)}}$$

le due funzioni $\varphi x$ e $\psi x$ sono sempre, come si vede, l'una più grande e l'altra più piccola di $x$. Così, con l'aiuto di queste due funzioni, si potrà avere le due radici dell'equazione più approssimate di un numero dato $a$, l'una in più e l'altra in meno.

Ma questo metodo presenta l'inconveniente di esigere, a ogni operazione, l'estrazione di una radice $n - esima$. Ecco due forme più comode. Cerchiamo un numero $k$ tale che la funzione

$$x + \frac{Fx}{kx^n}$$

cresca con $x$, quando $x > 1$, (Basta, infatti, saper trovare le radici di una equazione che sono più grandi dell'unità.)

Avremo, per la condizione proposta,

$$1 + \frac{d\frac{X-Y}{kx^n}}{dx} > 0 \quad oppure \quad 1 - \frac{nX - xX'}{kx^{n+1}} + \frac{nY - xY'}{kx^{n+1}} > 0$$

ora si ha identicamente

$$nX - xX' > 0 \quad nY - xY' > 0$$

basta quindi porre

$$\frac{nX - xX'}{kx^{n+1}} < 1 \quad per \quad x > 1$$

e basta, per questo, prendere per $k$ il valore della funzione $nX - xX'$, relativa a $x = 1$.

Si troverà lo stesso un numero $h$ tale che la funzione

$$x - \frac{Fx}{kx^n}$$

crescerà con $x$, quando $x$ sarà $> 1$, cambiando $Y$ in $X$.

Così, l'equazione data si potrà mettere sotto una delle forme

$$x = x + \frac{Fx}{kx^n} \quad x = x - \frac{Fx}{kx^n}$$

che sono tutte entrambe razionali e danno per la risoluzione un metodo semplice.

[6] *Bullettin des Sciences mathématiques* de M. Férussac, t. XIII, p. 413 (anno 1830, quaderno di giugno)

## Sulla Teoria dei Numeri[7]

Quando è opportuno considerare come nulle tutte le quantità che, nei calcoli algebrici, si trovano moltiplicate per un numero primo dato $p$, e si cercano, in questa convenzione, le soluzioni di una equazione algebrica $Fx = 0$, ciò che M. Gauss indica con la notazione $Fx \equiv 0$, si ha la consuetudine di considerare solo le soluzioni intere di questi tipi di problemi. Essendo stato portato da ricerche particolari a considerare le soluzioni incommensurabili, sono giunto a qualche risultato che credo nuovo.

Sia una simile equazione o congruenza, $Fx = 0$, e $p$ il modulo. Supponiamo dapprima, per maggiore semplicità, che la congruenza in questione non ammetta alcun fattore commensurabile, cioè che non si possano trovare tre funzioni $\varphi x, \psi x, \chi x$ tali che

$$\varphi x \cdot \psi x = Fx + p \cdot \chi x$$

In questo caso, la congruenza non ammetterà alcuna radice intera, nemmeno alcuna radice incommensurabile di grado inferiore. Bisogna quindi considerare le radici di questa congruenza come specie di simboli immaginari, poiché esse non soddisfano alle questioni dei numeri interi, simboli il cui impiego, nel calcolo, sarà spesso così utile come quello dell'immaginario $\sqrt{-1}$ nell'analisi comune.

È la classificazione di questi immaginari, e la loro riduzione al più piccolo numero possibile, che ci occuperà.

Chiamiamo $i$ una delle radici della congruenza $Fx = 0$, che supporremo di grado $\nu$.

Consideriamo l'espressione generale

$$a + a_1 i + a_2 i^2 + ... + a_{\nu-1} i^{\nu-1} \tag{0.0.3}$$

dove $a, a_1, a_2, ..., a_{\nu-1}$ rappresentano numeri interi. Dando a questi numeri tutti i valori, l'espressione (A) acquisisce $p^\nu$, che godono, così come voglio mostrare, delle stesse proprietà dei numeri naturali nella *teoria dei resti delle potenze.*

Prendiamo dalle espressioni (A) che i $p^\nu - 1$ valori di $a, a_1, a_2, ..., a_{\nu-1}$ non sono tutti nulli: sia $\alpha$ uno di queste espressioni.

Se si eleva successivamente $\alpha$ alle potenze $2^a, 3^a, ...$, si avrà una successione di quantità della stessa forma (poiché ogni funzione di $i$ si può ridurre al $(\nu-1)^{esimo}$ grado). Pertanto si dovrà avere $\alpha^n = 1$ , essendo $n$ un certo numero; sia $n$ il più piccolo numero tale che si abbia $a^n = 1$. Si avrà un insieme di $n$ espressioni, tutte diverse tra loro.

$$1, \alpha, \alpha^2, \alpha^3, ..., \alpha^{n-1}$$

Moltiplichiamo queste $n$ quantità per un'altra espressione $\mathscr{C}$ della stessa forma. Otterremo ancora un nuovo gruppo di quantità tutte diverse dalle prime e diverse tra loro. Se le quantità (A) non sono esaurite, si moltiplicheranno ancora le potenze di $\alpha$ per una nuova espressione $\gamma$, e così di seguito. Si vede pertanto che il numero $n$ dividerà successivamente il numero totale delle quantità (A). Essendo questo numero $p^n - 1$, si vede che $n$ divide $p^\nu - 1$. Da ciò segue ancora che si avrà

$$\alpha^{p^{\nu-1}} = 1 \quad oppure \quad \alpha^{p^\nu} = \alpha$$

Si dimostrerà poi, come nella teoria dei numeri, che vi sono radici primitive $\alpha$ per le quali si abbia precisamente $p^\nu - 1 = n$ e che riproducono, di conseguenza, per elevazione alle potenze, tutta la serie delle altre radici.

E una qualunque di queste radici primitive dipenderà solo da una congruenza di grado $\nu$, congruenza *irriducibile*, senza che l'equazione in $i - esimo$ lo sia, poiché le radici della congruenza in $i$ sono tutte delle potenze della radice primitiva.

---

[7] *Bullettin des Sciences mathématiques* de M. Férussac, t. XIII, p. 428 (anno 1830, quaderno di giugno); con la nota seguente: "Questa Memoria da parte delle ricerche di M. Galois sulla teoria delle permutazioni e delle equazioni algebriche. (J. Liouville)

Si vede qui questa conseguenza significativa che tutte le quantità algebriche che possono presentarsi nella teoria sono radici di equazioni della forma

$$x^{p^\nu} = x$$

Questa proposizione, enunciata algebricamente, è questa: Essendo data una funzione $Fx$ e un numero primo $p$, si può porre

$$fx \cdot Fx = x^{p^\nu} - x + p\varphi x$$

dove $fx$ e $\varphi x$ sono funzioni intere, tutte le volte che la congruenza $Fx \equiv 0 \ (mod.p)$ sarà irriducibile.

Se si vogliono avere tutte le radici di una simile congruenza per mezzo di una sola, basta osservare che si ha generalmente

$$(Fx)^{p^n} = F\left(x^{p^n}\right)$$

e che, di conseguenza, essendo $x$ una delle radici, le altre saranno[9]

$$x^p, x^{p^2}, ..., x^{p^{\nu-1}}$$

Si tratta ora di far vedere che, reciprocamente a quanto detto, le radici dell'equazione o della congruenza $x^{p^\nu} = x$ dipenderanno tutte da una sola congruenza di grado $\nu$.

Sia infatti $i$ una radice di una congruenza irriducibile e tale che tutte le radici della congruenza $x^{p^\nu} = x$ siano funzioni razionali di $i$ (È chiaro che qui, come nelle equazioni ordinarie, questa proprietà vale)[10].

È d'altra parte evidente che il grado $\mu$ della congruenza in $i$ non potrà essere che più piccolo di $\nu$, altrimenti la congruenza $(\nu)$

$$x^{p^{\nu-1}} - 1 = 0$$

avrebbe tutte le radici comuni con la congruenza

$$x^{p^{\mu-1}} - 1 = 0$$

ciò che è assurdo, poiché la congruenza $(\nu)$ non ha radici uguali, come si vede prendendo la derivata del primo membro. Dico ora che $\mu$ non può essere maggiore di $\nu$.

Infatti, se così fosse, tutte le radici della congruenza

$$x^{p^\mu} = x$$

dovrebbero dipendere razionalmente da quelle della congruenza

$$x^{p^\nu} = x$$

Ma è facile vedere che, se si ha

$$i^{p^\nu} = i$$

ogni funzione razionale $h = fi$ darà ancora

$$(fi)^{p^\nu} = f\left(i^{p^\nu}\right) \quad da\, cui \quad h^{p^\nu} = k$$

---

[9]Dal fatto che le radici della congruenza irriducibile di grado $\nu$ $Fx = 0$ sono espresse dalla serie $x, x^p, xp^2, ..., xp^{r-1}$ non si potrà concludere che queste radici siano sempre quantità esprimibili per radicali. Ecco un esempio del contrario:

$$x^2 + x + 1 = 0 \ \ (mod\, 2)$$

dà

$$x = \frac{-1 + \sqrt{-3}}{2}$$

che si riduce a

$$\frac{0}{0} \ \ (mod\, p)$$

formula che non ci insegna nulla.

[10]La proposizione generale qui trattata si può enunciare così: Data una equazione algebrica, si potrà trovare una funzione razionale $\theta$ di tutte le sue radici, in modo che, reciprocamente, ognuna delle radici si esprime razionalmente in $\theta$. Questo teorema era conosciuto come di Abel, così come si può vedere dalla prima parte della Memoria di questo celebre matematico relativa alle funzioni ellittiche.

Pertanto tutte le radici della congruenza $x^{p^\mu} = x$ saranno comuni con l'equazione $x^{p^\nu} = x$, ciò che è assurdo.

Sappiamo quindi infine che tutte le radici dell'equazione o congruenza $x^{p^\nu} = x$ dipendono necessariamente da una *sola* congruenza *irriducibile* di grado $\nu$.

Ora, per avere questa congruenza irriducibile da cui dipendono le radici della congruenza $x^{p^\nu} = x$, il metodo più generale sarà di liberare dapprima questa congruenza da tutti i fattori comuni che potrebbe avere con congruenze di grado inferiore e della forma

$$x^{p^\mu} = x$$

Si otterrà così una congruenza che dovrà dividersi in congruenze irriducibili di grado $\nu$. E, siccome si sa esprimere tutte le radici di ognuna di queste congruenze irriducibili per mezzo di una sola, sarà facile ottenerle tutte con il metodo di M. Gauss.

Più spesso, tuttavia, sarà facile trovare per tentativi una congruenza irriducibile di un grado dato $\nu$, e se ne deve dedurre tutte le altre.

Siano, per esempio, $p = 7$, $\nu = 3$. Cerchiamo le radici della congruenza

$$x^{7^3} = x \quad (mod\, 7) \tag{0.0.4}$$

Osservo che la congruenza

$$i^3 = 2 \quad (mod\, 7) \tag{0.0.5}$$

essendo irriducibile, e di grado 3, tutte le radici della congruenza (1) dipendono razionalmente da quelle della congruenza (2), di modo che tutte le radici della (1) sono della forma

$$a + a_1 i + a_2 i^2 \quad oppure \quad a + a_1 \sqrt[3]{2} + a_2 \sqrt[3]{4} \tag{0.0.6}$$

Bisogna ora trovare una radice primitiva, cioè una forma dell'espressione (3) che, elevata a tutte le potenze, dà tutte le radici della congruenza

$$x^{7^3-1} = 1 \quad cioè \quad x^{2^1 \cdot 3^2 \cdot 19} = 1 \quad (mod\, 7)$$

e abbiamo bisogno per questo solo di avere una radice primitiva di ogni congruenza

$$x^2 = 1 \quad x^{3^2} = 1 \quad x^{19} = 1$$

La radice primitiva della prima è $-1$; quelle di $x^{3^2} - 1 = 0$ sono date dalle equazioni

$$x^3 = 2 \quad x^3 = 4$$

di modo che $i$ è una radice primitiva di $x^{3^2} = 1$.

Rimane solo da trovare una radice di $x^{19} - 1 = 0$, o piuttosto di

$$\frac{x^{19} - 1}{x - 1} = 0$$

e provare per questo se si può soddisfare alla domanda ponendo semplicemente $x = a + a_1 i$, invece di $a + a_1 i + a_2 i^2$; dovremo avere

$$(a + a_1 i)^{19} = 1$$

ciò che, sviluppando con la formula di Newton, e riducendo le potenze di $a$, di $a_1$e di $i$, con le formule

$$a^{m(p-1)} = 1 \quad a_1^{m(p-1)} = 1 \quad i^3 = 2$$

si riduce a

$$3\left[a - a_4 a_1^2 + 3\left(a^5 a_1^2 + a^2 a_1^5\right) i^2\right] = 1$$

da cui, separando,

$$3a - 3a^4 a_1^3 = 1 \quad a^5 a_1^2 + a^2 + a_1^5 = 0$$

Queste ultime due equazioni sono soddisfatte ponendo $a = -1$, $a_1 = 1$. Pertanto

$$-1 + i$$

è una radice primitiva si $x^{19} = 1$. Abbiamo trovato prima, per radici primitive di $x^2 = 1$ e di $x^{3^2} = 1$, i valori $-1$ e $i$; rimane solo da moltiplicare tra loro le tre quantità

$$-1 \quad i \quad -1+i$$

e il prodotto $i - i^2$ sarà una radice primitiva della congruenza

$$x^{7^3-1} = 1$$

Pertanto l'espressione $i-i^2$ gode della proprietà che, elevando a tutte le potenze, si otterranno $7^3 - 1$ espressioni differenti della forma

$$a + a_1 i + a_2 i^2$$

Se vogliamo avere la congruenza di grado minore da cui dipende la nostra radice primitiva, bisogna eliminare $i$ tra le due equazioni

$$i^3 = 2 \quad \alpha = i - i^2$$

Si ottiene così

$$\alpha^3 - \alpha + 2 = 0$$

Sarà opportuno prendere per base degli immaginari e rappresentare con $i$ la radice di questa equazione, di modo che

$$I^3 - i + 2 = 0 \tag{0.0.7}$$

e si avranno tutti gli immaginari della forma

$$a + a_1 i + a_2 i^2$$

elevando $i$ a tutte le potenze e riducendo dall'equazione (i).

Il vantaggio principale della nuova teoria che esponiamo è di ridurre le congruenze alla proprietà (se utile nelle equazioni ordinarie), di ammettere precisamente tante radici quanti unità di sono nell'ordine del loro grado.

Il metodo per avere tutte queste radici sarà molto semplice. In primo luogo, si potrà sempre preparare la congruenza data $Fx = 0$ in modo che non abbia più radici uguali, o, in altre parole, che non abbia più fattore comune con $F'x = 0$, e il modo per farlo è evidentemente lo stesso per le equazioni ordinarie.

Poi, per avere le soluzioni intere, basterà, così come M. Libri sembra aver fatto per primo l'osservazione, cercare il più grande fattore comune a $Fx = 0$ e a $x^{p-1} = 1$.

Se ora si vogliono avere le soluzioni immaginarie di secondo grado, si cercherà il più grande fattore comune a $Fx = 0$ e a $x^{p^2-1} = 1$, e, in generale, le soluzioni dell'ordine $\nu$ saranno dato da più grande comune divisore a $Fx = 0$ e a $x^{p^\nu-1} = 1$.

È soprattutto nella teoria delle permutazioni, dove si ha sempre bisogno di variare la forma degli indici, che la considerazione delle radici immaginarie delle congruenze sembra indispensabile. Essa offre un metodo semplice e facile di riconoscere in quale caso una equazione primitiva è risolvibile per radicali, come provo a darne un'idea in due parole.

Sia un'equazione algebrica $fx = 0$, di grado $p^\nu$; supponiamo che le $p^\nu$ radici siano indicate con $x_k$, dando all'indice $k$ i $p^\nu$ valori determinati dalla congruenza $kp^\nu = k \ \ (mod\, p)$.

Prendiamo una qualunque funzione razionale $V$ delle $p^\nu$ radici $x_k$. Trasformiamo questa funzione sostituendo dappertutto all'indice $k$ l'indice $(ak + b)\, P^r$, essendo $a, b, r$ costanti arbitrarie che soddisfano alle condizioni di $ap^{\nu-1} = 1$, $bp^\nu = b \ \ (mod\, p)$ e di $r$ intero.

Assegnando alle costanti $a, b, r$ tutti i valori a loro possibili, si otterranno in tutto $p^\nu \left(p^\nu - 1\right)^\nu$ modi di permutare le radici tra loro con sostituzioni della forma $\left[x_k, x_{(ak+b)p^r}\right]$ ,e la funzione $V$ ammetterà in generale da queste sostituzioni $p^\nu \left(p^\nu - 1\right)^\nu$ forme differenti.

Ammettiamo ora che l'equazione proposta $fx = 0$ sia tale che ogni funzione delle radici, invariabile per le $p^\nu \left(p^\nu - 1\right)^\nu$ permutazioni costruite, abbia per ciò stesso un valore numerico razionale.

Si osserva che, in queste circostanze, l'equazione $fx = 0$ sarà risolvibile per radicali, e, per giungere a questa conseguenza, basta osservare che il valore sostituito a $k$, in ogni indice, si può mettere sotto le tre forme

$$(ak+b)^{p^r} = \left[a\left(k+b'\right)\right]^{p^r} = a'k^{p^r} + b" = a'\left(k+b'\right)^{p^r}$$

Le persone abituate alla teoria delle equazioni lo vedranno senza sforzo.

Questa osservazione avrebbe poca importanza se non avessi dimostrato che, reciprocamente, un'equazione primitiva non potrebbe essere risolvibile per radicali, a meno di soddisfare alle condizioni che ho enunciato. (Escludo le equazioni di non e venticinquesimo grado).

Così, per ogni numero della forma $p^\nu$, si potrà formare un gruppo di permutazioni tale che ogni funzione di radici invariabili per queste permutazioni dovrà ammettere un valore razionale quando l'equazione di grado $p^\nu$ sarà primitiva e risolvibile per radicali.

D'altra parte, vi sono solo le equazioni di un simile grado $p^\nu$ che siano contemporaneamente primitive e risolvibili per radicali.

Il teorema generale che ho enunciato precisa e sviluppa le condizioni che avevo dato nel Bullettin del mese di aprile. Indica il modo di formare una funzione di radici il cui valore sarà razionale, tutte le volte che l'equazione primitiva di grado $p^\nu$ sarà risolvibile per radicali, e porta, di conseguenza, alle caratteristiche di risolvibilità di queste equazioni, con calcoli se non praticabili, almeno possibili in teoria.

È da notare che, nel caso in cui $\nu = 1$, i diversi valori di $k$ non sono diversi dalla successione dei numeri interi. Le sostituzioni della forma $(x_k, x_{ak+b})$ saranno nel numero di $p\,(p-1)$.

La funzione che, nel caso di equazioni risolvibili per radicali, deve avere un valore razionale, dipenderà, in generale, da una equazione di grado $1 \cdot 2 \cdot 3 \ldots (p-2)$, alla quale bisognerà, di conseguenza, applicare il metodo delle radici razionali.

# Opere Postume

## Lettera a Auguste Chevalier[13]

Mio caro amico,

ho fatto nell'Analisi parecchie cose nuove.

Le une concernenti la teoria delle equazioni; le altre le funzioni integrali.

Nella teoria delle equazioni, ho ricercato in quali casi le equazioni fossero risolvibili per radicali, ciò che mi ha dato occasione di approfondire questa teoria e di descrivere tutte le trasformazioni possibili su un'equazione, anche quando essa non è risolvibile per radicali.

Si potranno fare con tutto ciò tra Memorie.

La prima è scritta, e malgrado ciò che ne dice Poisson, la mantengo, con le correzioni che vi ho fatto.

La seconda contiene applicazioni assai curiose della teoria delle equazioni. Ecco il riassunto delle più importanti:

1° Dalle proposizioni II e III della prima Memoria, si vede una grande differenza tra aggiungere ad un'equazione una delle radici di una equazione ausiliaria o aggiungerle tutte.

In entrambi i casi, il gruppo dell'equazione si divide per l'aggiunta in gruppi tali, che si passa da una all'altra con una stessa sostituzione; ma la condizione che questi gruppi abbiano le stesse sostituzioni vale certamente solo nel secondo caso. Ciò si chiama la *scomposizione propria*.

In altre parole, quando un gruppo $G$ ne contiene un altro $H$, il gruppo $G$ si può dividere in gruppi, che si ottengono ciascuno operando sulle permutazioni di $H$ in una stessa sostituzione; ne segue che

$$G = H + HS + HS' + ....$$

E così si può dividere in gruppi che hanno tutti le stesse sostituzioni, di modo che

$$G = H + TH + T'H + ...$$

Questi due tipi di scomposizioni non coincidono solitamente. Quando essi coincidono, la scomposizione è detta *propria*.

È facile vedere che, quando il gruppo di una equazione non può subire alcuna scomposizione propria, si potrà meglio trasformare questa equazione, i gruppi delle equazioni trasformate avranno sempre lo stesso numero di permutazioni.

Al contrario, quando il gruppo di un'equazione può avere una scomposizione propria, in modo da dividersi in $M$ gruppi di $N$ permutazioni, si potrà risolvere l'equazione data per mezzo di due equazioni: una avrà un gruppo di $M$ permutazioni, l'altra uno di $N$ permutazioni.

Quando quindi si avrà esaurito sul gruppo di una equazione tutto ciò che vi è di scomposizioni proprie possibili su questo gruppo, si arriverà a gruppi che si potranno trasformare, ma le cui permutazioni saranno sempre nello stesso numero.

Se questi gruppi hanno ciascuno un numero primo di permutazioni, l'equazione sarà risolvibile per radicali; altrimenti, no.

Il più piccolo numero di permutazioni che possa avere un gruppo non scomponibile, quando questo numero non è primo, è $5 \cdot 4 \cdot 3$.

2° Le scomposizioni più semplici sono quelle che avvengono con il metodo di M. Gauss.

[13]Scritta la vigilia della morte dell'autore. (Inserita nel 1832 nella *Revue encyclopédique*, numero di settembre, pag. 568)

Siccome queste scomposizioni sono evidenti, anche nella forma attuale del gruppo dell'equazione, è inutile soffermarsi a lungo su questo argomento.

Quelle scomposizioni sono praticabili su un'equazione che non si semplifica con il metodo di M. Gauss?

Ho chiamato *primitive* le equazioni che non si possono semplificare con il metodo di M. Gauss; non che queste equazioni siano realmente non scomponibili, poiché essere possono pure risolversi per radicali.

Come lemma alla teoria delle equazioni primitive risolvibili per radicali, ho esposto nel giugno 1830 nel *Bullettin de Férussac*, un'analisi sugli immaginari della teoria dei numeri.

Si troverà qui allegata[14] la dimostrazione dei teoremi seguenti:

1° Affinché un'equazione primitiva sia risolvibile per radicali essa deve essere di grado $p^\nu$, con $p$ numero primo.

2° Tutte le permutazioni di una simile equazione sono della forma

$$x_{k,l,m\ldots} \left| x_{ak+bl+cm+\ldots+k, a'k+b'l+c'm+\ldots+k', a'k+\ldots.} \right.$$

essendo $l, l, m \ldots \nu$ indici, che, prendendo ciascuno $p$ valori, indicano tutte le radici. Gli indici sono presi secondo il modulo $p$; cioè che la radice sarà la stessa quando si aggiungerà a uno degli indici un multiplo di $p$.

Il gruppo che si ottiene operando tutte le sostituzioni di questa forma lineare contiene, in tutto,

$$p^\nu \left(p^\nu - 1\right) \left(p^\nu - p\right) \ldots \left(p^\nu - p^{\nu-1}\right)$$

permutazioni.

Si ha che, in questa generalità, le equazioni che soddisfano siano risolvibili per radicali.

La condizione che ho indicato nel *Bullettin de Férussac* perché l'equazione sia risolvibile per radicali è molto restrittiva; vi sono poche eccezioni, ma ve ne sono.

L'ultima applicazione della teoria delle equazioni è relativa alle equazioni modulari di funzioni ellittiche.

Si sa che il gruppo dell'equazione che ha per radici i seni dell'ampiezza delle $p^2 - 1$ divisioni di un perioso è questo:

$$x_{k,l,\ \ x_{ak+bl,ck+dl}}$$

di conseguenza l'equazione modulare corrispondente avrà per gruppo

$$x_{\frac{k}{l}}, x_{\frac{ak+nl}{ck+dl}}$$

nel quale $\frac{k}{l}$ può avere i $p+1$ valori

$$\infty, 0, 1, 2, \ldots, p-1$$

Così, convenendo che $k$ può essere infinito, si può scrivere semplicemente

$$x_k, x_{\frac{ak+nl}{ck+dl}}$$

Dando ad $a, b, c, d$ tutti i valori, si ottiene

$$(p+1)(p-1)$$

permutazioni.

Ora questo gruppo si scompone *propriamente* in due gruppi, le cui sostituzioni sono

$$x_k, x_{\frac{ak+b}{ck+d}}$$

essendo $ad - bc$ un residuo quadratico di $p$.

Il gruppo così semplificato è di

$$(p+1)\, p \frac{p-1}{2}$$

permutazioni.

[14] Galois parla dei manoscritti, fino ad allora inediti, che sono qui pubblicati.

Ma è facile vedere che non è più scomponibile propriamente, a meno che $p = 2$ o $p = 3$.

Così, in qualsiasi modo si trasforma l'equazione, il suo gruppo avrà sempre lo stesso numero di permutazioni.

Ma è curioso sapere se il grado si può abbassare.

E dapprima non può divenire più piccolo di $p$, le cui radici $x_k$ si indicano dando a $k$ tutti i valori, ivi compreso l'infinito, e il cui gruppo ha per sostituzioni

$$x_k, x_{\frac{ak+b}{ck+d}}$$

essendo $ad - bc$ un quadrato, si può abbassare al grado $p$.

Ora serve per questo che il gruppo si scomponga (impropriamente, s'intende) in $p$ gruppi di $(p+1)\,\frac{p-1}{2}$ permutazioni ciascuno.

Siano 0 e $\infty$ due lettere congiunte in uno di questi gruppi. Le sostituzioni che non fanno cambiare 0 e $\infty$ di posto saranno della forma

$$x_k, x_{m^2k}$$

Pertanto se $M$ è la lettere congiunta a 1, la lettera congiunta a $m^2$ sarà $m^2M$. Quando $M$ è un quadrato, si avrà quindi $M^2 = 1$. Ma questa semplificazione può aver luogo solo per $p = 5$.

Per $p = 7$ si trova un gruppo di $(p+1)\,\frac{p-1}{2}$ permutazione, dove

$$\infty, 1, 2, 4$$

hanno rispettivamente per lettere congiunte

$$0, 3, 6, 5$$

Questo gruppo ha sei sostituzioni della forma

$$x_k, x_{a\frac{k-b}{k-c}}$$

essendo $b$ la lettera congiunta di $c$, e $a$ una lettera che è residuo o non residuo contemporaneamente a $c$.

Per $p = 11$, le stesse sostituzioni avranno luogo con le stesse notazioni

$$\infty, 1, 3, 5, 5, 9$$

aventi rispettivamente per congiunte

$$0, 2, 6, 8, 10, 7$$

Così per il caso di $p = 5, 7, 11$, l'equazione modulare si abbassa al grado $p$.

A rigore, questa equazione non è possibile nei casi più elevati.

La terza Memoria concerne gli integrali.

Si sa che una somma di termini di una stessa funzione ellittica si riduce sempre a un solo termine, più delle quantità algebriche o logaritmiche.

Non vi sono altre funzioni per le quali questa proprietà valga.

Ma proprietà assolutamente simili suppliscono in tutti gli integrali di funzioni algebriche.

Si trattano contemporaneamente tutti gli integrali il cui differenziale è una funzione della variabile e di una funzione irrazionale della variabile, che questa irrazionale sia o no un radicale, che essa si esprima o no per radicali.

Si trova che il numero dei periodi distinti dell'integrale più generale relativo a una irrazionale data è sempre un numero pari.

Sia $2n$ questo numero, si avrà il seguente teorema:

Una somma qualunque di termini si riduce a $n$ termini, più quantità algebriche e logaritmiche.

Le funzioni di prima specie sono quelle per le quali la parti algebrica e logaritmica è nulla.

Ve ne sono $n$ distinte.

Le funzioni di seconda specie sono quelle per le quali la parte complementare è puramente algebrica.

Ve ne sono $n$ distinte.

Si può supporre che i differenziali delle altra funzioni non siano mai infiniti se non una volta per $x = a$, e, inoltre, che la loro parte complementare si riduce a un solo logaritmo, $\log P$, essendo $P$ una quantità algebrica. Indicando con $\Pi(x, a)$ queste funzioni, si avrà il teorema

$$\Pi(x, a) - \Pi(a, x) = \sum \varphi a \cdot \psi x$$

essendo $\varphi a, \psi x$ funzioni di prima e seconda specie.

Se ne deduce, chiamando $\Pi(a)$ e $\psi$ i periodi di $\Pi(x, a)$ e $\psi x$ relativi a una stessa rivoluzione di $x$,

$$\Pi(a) = \sum \varphi a \times \psi x$$

Così i periodi delle funzioni di terza specie a integrali definiti, che è la più bella scoperta di M. Jacobi, non è praticabile, tranne il caso delle funzioni ellittiche.

La moltiplicazione delle funzioni integrali per un numero intero è sempre possibile, come l'addizione, per mezzo di un'equazione di grado $n$ le cui radici sono i valori da sostituire nell'integrale per avere i termini ridotti.

L'equazione che dà la divisione dei periodi in $p$ parti uguali è del grado $p^{2n} - 1$. Il suo gruppo ha in tutto

$$\left(p^{2n} - 1\right)\left(p^{2n} - p\right) ... \left(p^{2n} - p^{2n-1}\right)$$

permutazioni.

L'equazione che dà la divisione di una somma di $n$ termini in $p$ parti uguali è di grado $p^{2n}$. Essa è risolvibile per radicali.

*Sulla trasformazione.* - Si può dapprima, seguendo ragionamenti analoghi a quelli che Abel ha consegnato nella sua ultima Memoria, dimostrare che se, in una stessa relazione tra integrali, si hanno le due funzioni

$$f\Phi(x, X)\, dx \quad f\Psi(y, Y)\, dy$$

l'ultimo integrale avente $2n$ periodi, sarà consentito supporre che $y$ e $Y$ si esprimono mediante una sola equazione di grado $n$ in funzione di $x$ e di $X$.

Da ciò si può supporre che le trasformazioni abbiano luogo costantemente tra due soli integrali, poiché si avrà evidentemente, prendendo una funzione qualunque razionale di $y$ e $Y$

$$\sum \int f(y, Y)\, dy = \int F(x, X)\, dx$$

più una quantità algebrica e logaritmica.

Si avranno su questa equazione riduzioni evidenti nel caso in cui gli integrali dell'uno e dell'altro membro non avranno entrambi lo stesso numero di periodi.

Così dobbiamo solo confrontare degli integrali che abbiano entrambi lo stesso numero di periodi.

Si dimostrerà che il più piccolo grado di irrazionalità di due simili integrali non può essere maggiore per l'uno che per l'altro.

Si farà poi vedere che si può sempre trasformare un integrale dato in un altro nel quale un periodo del primo sia diviso per il numero primo $p$, rimanendo gli altri $2n - 1$ gli stessi.

Rimarrà quindi soltanto da confrontare che integrale dove i periodi saranno gli stessi da parte a parte, e tali, di conseguenza, che $n$ termini dell'uno si esprimano senza altre equazioni che una solo di grado $n$, per mezzo di quelle dell'altro, e reciprocamente. Qui non sappiamo nulla.

Tu sai, mio caro Augusto, che questi non sono i soli temi che ho esplorato. Le mie principali riflessioni, dopo qualche tempo, erano dirette all'applicazione dell'analisi trascendente della teoria dell'ambiguità Si trattava di vedere *a priori*, in una relazione tra quantità in funzioni trascendenti, quali scambi si potevano sostituire alle quantità date, senza che la relazione potesse cessare di valore. Ciò fa riconoscere l'impossibilità di molte espressioni che si potrebbero cercare. Ma non ho il tempo, e le mie idee non sono ancora ben sviluppate su questo terreno, che è immenso.

Tu farai stampare questa Lettera nella *Revue encyclopédique*.

Mi sono spesso azzardato nella mia vita ad avanzare proposizioni di cui non ero sicuro; ma tutto quanto ho scritto è da più di un anno nella mia testa, ed è troppo ed è troppo nel mio interesse non sbagliare perché mi preoccupi di enunciare teoremi di cui non avrei la dimostrazione completa.

Tu pregherai pubblicamente Jacobi o Gauss di esprimere il loro parere, non sulla verità, ma sull'importanza dei teoremi.

Dopo, vi saranno, spero, persone geniali che troveranno il loro profitto nel decifrare tutto questo disordine.

Ti abbraccio con affetto.

E. Galois

29 maggio 1832.

## Condizioni di risolvibilità delle equazioni per radicali

[16]La Memoria qui aggiunta[17] è estratta da un'Opera che ho avuto l'onore di presentare all'Accademia un anno fa. Quest'Opera non essendo stata compresa, essendo state messe in dubbio le proposizioni in essa contenute, ho dovuto accontentarmi di dare, in forma sintetica, i principi generali e una *sola* applicazione della mia teoria. Supplico i miei giudici di leggere almeno con attenzione queste poche pagine.

Si troverà qui una *condizione* generale che è *soddisfatta da ogni equazione risolvibile per radicali*, e che reciprocamente assicura la loro risolvibilità. Si fa una sola applicazione alle equazioni il cui grado è un numero primo. Ecco il teorema dato dalla nostra analisi:

*Affinché un'equazione di grado primo, che non ha divisori commensurabili, sua risolvibile per radicali, è necessario e sufficiente che tutte le radici siano funzioni razionali di due qualunque tra di esse.*

Le altre applicazioni della teoria sono esse stesse altrettante teorie particolari. Esse richiedono d'altra parte l'impiego della teoria dei numeri, e di un algoritmo particolare: le riserviamo per un'altra occasione. Esse sono in parte relative alle equazioni modulari della teoria delle funzioni ellittiche, che dimostriamo di non potersi risolvere mediante radicali.

16 gennaio 1831.

E. Galois

**Principi.** Inizierò con lo stabilire alcune definizioni e una serie di lemmi che sono tutti noti.

*Definizioni.* - Una equazione è detta *riducibile* quando ammette divisori razionali; *irriducibile* nel caso contrario.

Serve qui spiegare ciò che si deve intendere con il termine *razionale*, poiché si presenterà spesso.

---

[16]Questa Memoria e la seguente sono state ritrovate nelle carte di Galois e pubblicate per la prima volta nel 1846 da Liouville, che le aveva fatte precedere dalla nota seguente:

"Inserendo nella loro Raccolta questa lettera, gli editori della *Revue Encicopédique* annunciavano di voler pubblicare prossimamente i manoscritti lasciati da Galois. Ma questa promessa non è stata mantenuta. M. Auguste Chevalier aveva tuttavia preparato il lavoro. Ce lo ha rimesso e si troverà nei fogli che seguiranno:

1° Una Memoria intera sulle condizioni di risolvibilità delle equazioni per radicali, con l'applicazione alle equazioni di primo grado;

2° Un frammento di una seconda Memoria dove Galois tratta della teoria generale delle equazioni che egli chiama *primitive*.

Abbiamo conservato la maggior parte delle note che M. Auguste Chevalier aveva aggiunto alle Memorie indicate. Queste note sono tutte contrassegnate dalle iniziali A. Ch. Le altre note sono dello stesso Galois.

Completeremo questa pubblicazione con qualche altro pezzo estratto dai quaderni di Galois, e che, senza avere una grande importanza, potranno tuttavia ancora essere letti con interesse dai matematici."

Gli estratti di cui parla Liouville nell'ultima frase di questa nota non sono mai stati pubblicati.

[17]Ho giudicato opportuno porre all'inizio di questa Memoria la prefazione che leggete, benché l'abbia trovata cancellata nel manoscritto. (A. Ch.)

Quando l'equazione ha *tutti* i suoi coefficienti numerici e razionali, ciò vuol dire semplicemente che l'equazione si può scomporre in fattori che abbiano i loro coefficienti numerici e razionali.

Ma quando i coefficienti di un'equazione *non saranno tutti* numerici e razionali, allora bisognerà intendere per divisore razionale un divisore i cui coefficienti si esprimeranno in funzione razionale dei coefficienti della proposta.

Inoltre: si potrà convenire di considerare come razionale ogni funzione razionale di un certo numero di quantità determinate, supposto 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.

Quando converremo di considerare così come note certe quantità. diremo che le *aggiungiamo* all'equazione che si deve risolvere. Diremo che queste quantità sono *aggiunte* all'equazione.

Ciò posto, chiameremo *razionale* ogni quantità che si esprimerà in funzione razionale dei coefficienti dell'equazione e di un certo numero di quantità *aggiunte* all'equazione e convenute arbitrariamente.

Quando ci serviremo di equazioni ausiliarie, esse saranno razionali, se i loro coefficienti sono razionali nel nostro significato.

Si vede, inoltre, che le proprietà e le difficoltà di una equazione possono essere del tutto differenti secondo le quantità che le sono aggiunte. Per esempio, l'aggiunta di una quantità può rendere riducibile una equazione irriducibile.

Così, quando si aggiunge all'equazione

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

dove $n$ è un numero primo, una radice di una equazione ausiliaria di M. Gauss, questa equazione si scompone in fattori e diviene, di conseguenza, riducibile.

Le sostituzioni sono il passaggio da una permutazione all'altra.

La permutazione da cui si parte per indicare le sostituzioni è del tutto arbitraria, quando si tratta di funzione; poiché non vi è alcuna ragione affinché, in una funzione di più lettere, una lettera occupi un posto piuttosto che un altro.

Quando vorremo raggruppare sostituzioni, le faremo tutte provenire da una stessa permutazione.

Siccome si tratta sempre di questioni dove la disposizione iniziale delle lettere non influisce per nulla sui gruppi che considereremo, si dovranno avere le stesse sostituzioni, qualunque sia la permutazione dalla quale si sarà partiti. Pertanto, se in un simile gruppo si hanno le sostituzioni $S$ e $T$, si è certi di avere la sostituzione $ST$.

Queste sono le definizioni che abbiamo creduto di dover richiamare.

LEMMA 1. *Un'equazione irriducibile non può avere alcuna radice comune con un'equazione razionale, senza dividerla.*

Poiché il massimo comun divisore tra l'equazione irriducibile e l'altra equazione sarà ancora razionale; pertanto, ecc.

LEMMA 2. *Data un'equazione qualunque, che non ha radici uguali, le cui radici sono $a, b, c, ...$, si può sempre formare una funzione $V$ delle radici, tale che nessuno dei valori che si ottengono permutando in questa funzione le radici in tutti i modi, sia uguale a un'altra.*

Per esempio, si può prendere

$$V = Aa + Bb + Cc + ...$$

essendo $A, B, C$ numeri interi opportunamente scelti.

LEMMA 3. *La funzione $V$ essendo scelta come è indicato nell'articolo precedente, essa godrà di questa proprietà, che tutte le radici dell'equazione proposta si esprimeranno razionalmente in funzione di $V$.*

Infatti, sia

$$V = \varphi(a, b, c, d, ...)$$

oppure

$$V - \varphi(a, b, c, d, ...) = 0$$

Moltiplichiamo tra loro tutte le equazioni simili, che si ottengono permutando in queste tutte le lettere, mantenendo fissa solo la prima; verrà un'espressione seguente:

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

simmetrica in $b, c, d, ...$, la quale potrà, di conseguenza, essere scritta in funzione di $a$. Avremo quindi un'equazione della forma

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

Ora dico che da ciò si può ricavare il valore di $a$. Basta per questo cercare la soluzione comune a questa equazione e alla proposta. Questa soluzione è la sola comune, poiché non si può avere, per esempio

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

avendo questa equazione un fattore comune con l'equazione simile, senza che una delle funzioni $\varphi(a, ...)$ sia uguale a una delle funzioni $\varphi(b, ...)$; ciò che è contro l'ipotesi.

Basta da ciò che $a$ si esprima in funzione razionale di $V$, e così anche per le altre radici.

Questa proposizione[18] è citata nella dimostrazione da Abel, nella Memoria postuma sulle funzioni ellittiche.

Lemma 4. *Supponiamo che si sia formata l'equazione in $V$, e che si sia preso uno dei suoi fattori irriducibili, di modo che $V$ sia radice di un'equazione irriducibile. Siano $V, V', V$", ... le radici di questa equazione irriducibile. Se $a = f(V)$ è una delle radici della proposta, anche $f(V')$ sarà una radice della proposta.*

Infatti, moltiplicando tra loro tutti i fattori della forma $V - \varphi(a, b, c..., d)$, dove si avranno operato sulle lettere tutte le permutazioni possibili, si avrà un'equazione razionale in $V$, la quale si troverà necessariamente divisibile per l'equazione in questione; pertanto $V'$ si deve ottenere per lo scambio delle lettere nella funzione. Sia $F(V, a) = 0$ l'equazione che si ottiene permutando in $V$ tutte le lettere, salvo la prima. Si avrà quindi $F(V', b) = 0$, potendo $b$ essere uguale ad $a$, ma essendo certamente una delle radici dell'equazione proposta; di conseguenza, come anche della proposta e di $F(V, a) = 0$ è risultata $a = f(V)$, come risulterà della proposta e di $F(V', b) = 0$ combinate, la seguente $b = f(V')$.

## PROPOSIZIONE I

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

*1° Che ogni funzione delle radici, invariabile[19] per le sostituzioni di questo gruppo, sia razionalmente nota;*

*2° Reciprocamente, che ogni funzione delle radici, determinabile razionalmente, sia invariabile per le sostituzioni.*

---

[18] È notevole che da questa proposizione si possa concludere che ogni equazione dipende da una equazione ausiliare tale che tutte le radici di questa nuova equazione siano funzioni razionali le une delle altre; poiché l'equazione ausiliaria in $V$ è in questo caso. Inoltre, questa nota è puramente curiosa. Infatti, un'equazione che ha questa proprietà non è, in generale, più facile da risolvere di un'altra.

[19] Chiamiamo qui invariabile non solo una funzione la cui forma è invariabile per le sostituzioni delle radici tra loro, ma anche quella il cui valore numerico non varierà per queste sostituzioni. Per esempio, se $Fx = 0$ è una equazione, $Fx$ è una funzione delle radici che non varia per alcuna permutazione.

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.

(Nel caso delle equazioni algebriche, questo gruppo non è altra cosa dell'insieme delle $1 \cdot 2 \cdot 3...m$ permutazioni possibili sulle $m$ lettere, poiché, in questo caso, le funzioni simmetriche sono le sole determinabili razionalmente.)

(Nel caso dell'equazione $\frac{x^n-1}{x-1} = 0$, se si suppone $a = r, b = r^g, c = r^{z^2}...$, essendo $g$ una radice primitiva, il gruppo delle permutazioni sarà semplicemente questo:

$$\begin{array}{c} abcd....k \\ bcd....ka \\ cd....kab \\ ..... \\ kabc....i \end{array}$$

in questo caso particolare, il numero delle permutazioni è uguale al grado dell'equazione, e la stessa cosa si avrà nelle equazioni in cui tutte le radici saranno funzioni razionali le une delle altre.)

Dimostrazione. Qualunque sia l'equazione data, si potrà trovare una funzione razionale $V$ delle radici, tale che tutte le radici siano funzioni razionali di $V$. Ciò posto, consideriamo l'equazione irriducibile di cui $V$ è la radice (lemmi III e IV).

Siano $\varphi V, \varphi_1 V, \varphi_2 V, ...\varphi_{m-1} V$ le radici della proposta. Scriviamo le permutazioni seguenti delle radici:

$$\begin{array}{cccccc} (V) & \varphi V & \varphi_1 V & \varphi_2 V & .... & \varphi_{m-1} V \\ (V') & \varphi V' & \varphi_1 V' & \varphi_2 V' & .... & \varphi_{m-1} V' \\ (V") & \varphi V" & \varphi_1 V" & \varphi_2 V" & .... & \varphi_{m-1} V" \\ .... & .... & .... & .... & .... & .... \\ \left(V^{(n-1)}\right) & \varphi V^{(n-1)} & \varphi_1 V^{(n-1)} & \varphi_2 V^{(n-1)} & .... & \varphi_{m-1} V^{(n-1)} \end{array}$$

dico che questo gruppo di permutazioni gode della proprietà enunciata. Infatti:

1° Ogni funzione $F$ delle radici, invariabile per le sostituzioni di questo gruppo, potrà essere così descritta: $F = \psi V$, e si avrà

$$\psi V = \psi V' = \psi V" = ... = \psi V^{(n-1)}$$

Il valore di $F$ potrà quindi determinarsi razionalmente.

2° Reciprocamente, se una funzione $F$ è determinabile razionalmente, e si pone $F = \psi V$, si dovrà avere

$$\psi V = \psi V' = \psi V" = ... = \psi V^{(n-1)}$$

poiché l'equazione in $V$ non ha divisore commensurabile e che $V$ soddisfa all'equazione $F = \psi V$, essendo $F$ una quantità razionale. Pertanto la funzione $F$ sarà necessariamente invariabile per le sostituzioni del gruppo sopra descritto.

Così questo gruppo gode della doppia proprietà di cui si tratta nel teorema proposto. Il teorema è quindi dimostrato. □

*Scolio* I. È evidente che, nel gruppo delle permutazioni in questione, la disposizione delle lettere non è da considerare, ma solo le sostituzioni delle lettere per le quali si passa da una permutazione all'altra.

Così si può dare arbitrariamente una prima permutazione, purché le altre permutazioni si deducano sempre dalle stesse sostituzioni delle lettere. Il nuovo gruppo così formato godrà evidentemente delle stesse proprietà del primo, poiché nel teorema precedente, si tratta solo di sostituzioni che si possono fare nelle funzioni.

*Scolio* II. Le sostituzioni sono indipendenti anche dal numero delle radici.

PROPOSIZIONE II

Teorema. [20] *Se si aggiunge a un'equazione data la radice $r$ di una equazione ausiliaria irriducibile, 1° si avranno di due cose l'una: o il gruppo dell'equazione non sarà cambiato, oppure si dividerà in p gruppo appartenenti ciascuno all'equazione proposta rispettivamente quando le si unisce ognuna delle radici dell'equazione ausiliaria; 2° questi gruppi godranno della notevole proprietà, che si passerà da uno all'altro operando in tutte le permutazioni del primo una stessa sostituzione di lettere.*

1° Se, dopo l'aggiunta di $r$, l'equazione in $V$, di cui si è prima trattato, resta irriducibile, è chiaro che il gruppo dell'equazione non sarà cambiato. Se, al contrario, essa si riduce, allora l'equazione in $V$ si scomporrà in $p$ fattori, tutti dello stesso grado e della forma

$$f(Vr) \times f(Vr') \times f(Vr") \times ...$$

essendo $r, r', r", ...$ altri valori di $r$. Così, il gruppo dell'equazione proposta si scomporrà in gruppi ognuno di uno stesso numero di permutazioni, poiché a ogni valore di $V$ corrisponde una permutazione. Questi gruppi saranno rispettivamente quelli dell'equazione proposta, quando le si aggiungerà successivamente $r, r', r", ....$

2° Abbiamo visto in precedenza che tutti i valori di $V$ erano funzioni razionali le une delle altre. Da ciò, supponiamo che, essendo $V$ una radice di $f(Vr) = 0$, $F(V)$ ne sia un'altra; è chiaro che anche se $V'$ è una radice di $f(Vr') = 0$, $F(V')$ ne sarà un'altra; poiché si avrà

$$f[F(V, r)]$$

una funzione divisibile per $f(V, r)$.

Quindi (lemma I)

$$f[F(V', r')]$$

una funzione divisibile per $f(V', r')$.

Ciò posto, dico che si ottiene il gruppo relativo a $r'$ operando ovunque nel gruppo relativo a $r$ una stessa sostituzione delle lettere.

Infatti, se si ha, per esempio,

$$\varphi_\mu F(V) = \varphi_\nu(V)$$

si avrà ancora (lemma I)

$$\varphi_\mu F(V') = \varphi_\nu(V')$$

Pertanto, per passare dalla permutazione $[F(V)]$ alla permutazione $[F(V')]$, basta fare la stessa sostituzione per passare dalla permutazione $(V)$ alla permutazione $(V')$.

Il teorema è quindi dimostrato.

PROPOSIZIONE III

Teorema. *Se si aggiungono a una equazione tutte le radici di una equazione ausiliaria, i gruppi di cui si tratta nel teorema II godranno, inoltre, della proprietà che le sostituzioni sono le stesse in ogni gruppo.*

Si troverà la dimostrazione[21].

[20] Nell'enunciato del teorema, dopo queste parole: *la radice r di una equazione ausiliaria irriducibile*, Galois aveva messo dapprima queste: *di grado p primo*, che ha più tardi cancellato. Ancora, nella dimostrazione, invece di $r, r', r", ...$ *essendo altri valori di r*, la scrittura iniziale riportava: $r, r', r", ...$ *essendo i diversi valori di r*. Infine si trova a margine del manoscritto la nota seguente dell'autore:

"Vi sono alcune cose da completare in questa dimostrazione. Non ne ho il tempo."

Questa riga è stata tracciata con una grande rapidità sul foglio; circostanza che, unita alle parole: "Non ne ho il tempo", mi fa pensare che Galois ha riletto la sua Memoria per correggerla prima di andare sul posto. (A. Ch.)

[21] Nel manoscritto, l'enunciato del teorema si trova a margine e ne sostituisce un'altra che Galois aveva scritto con la sua dimostrazione sotto lo stesso titolo: *Proposizione III*. Ecco il testo originario: Teorema: *Se l'equazione in r è della forma $r^p = A$, e se le radici $p^{esime}$ dell'unità si trovano nel numero delle quantità precedentemente aggiunte, i p gruppi di cui si tratta nel teorema II godranno, inoltre, della proprietà che le sostituzioni delle lettere per le quale si passa da una permutazione a un'altra in ogni gruppo siano le stesse per tutti i gruppi*. Infatti, in questo caso, equivale ad aggiungere ugualmente all'equazione tale o talaltro valore di

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 modo da non avere più altre permutazioni se non quelle per le quali questa funzione è invariabile.*

Infatti, dalla proposizione I, ogni funzione nota deve essere invariabile per le permutazioni del gruppo dell'equazione.

PROPOSIZIONE V

Problema. In quale caso un'equazione è risolvibile per radicali semplici?

Osserverò dapprima che, per risolvere un'equazione, si deve abbassare successivamente il suo gruppo fino a contenere soltanto una sola permutazione. Poiché, quando un'equazione è risolta, una funzione qualunque delle sue radici è nota, anche quando essa non è invariabile per alcuna permutazione.

Ciò posto, cerchiamo a quale condizione deve soddisfare il gruppo di un'equazione, perché possa abbassarsi così per l'aggiunta di quantità radicali.

Seguiamo il percorso delle operazioni possibili in questa soluzione, considerando come operazioni distinte l'estrazione di ogni radice di grado primo.

Aggiungiamo all'equazione il primo radicale estratto nella soluzione. Si potranno avere due casi: o, per l'aggiunta di questo radicale, il gruppo delle permutazioni dell'equazione sarà diminuito; oppure, questa estrazione di radice essendo solo una semplice preparazione, il gruppo rimarrà lo stesso.

Sempre avverrà che dopo un certo numero *finito* di estrazioni di radici, il gruppo dovrà trovarsi diminuito, altrimenti l'equazione non sarà risolvibile.

Se, arrivato a questo punto, vi fossero numerosi modi di diminuire il gruppo dell'equazione proposta con una semplice estrazione di radice, basterebbe, per quanto detto, considerare soltanto un radicale del grado meno alto possibile tra tutte i radicali semplici, che sono tali che la conoscenza di ognuno di essi diminuisce il gruppo dell'equazione.

Sia quindi $p$ il numero primo che rappresenta questo grado minimo, di modo che con un'estrazione di radice di grado $p$, si diminuisce il gruppo dell'equazione.

Possiamo sempre supporre, almeno per ciò che è relativo al gruppo dell'equazione, che, tra le quantità aggiunte in precedenza all'equazione, si trova una radice $p^{esima}$ dell'unità, $\alpha$. Poiché, siccome questa espressione si ottiene da estrazioni di radici di grado inferiore a $p$, la sua conoscenza non altererà in nulla il gruppo dell'equazione.

Di conseguenza, dai teoremi II e III, il gruppo dell'equazione dovrà scomporsi in $p$ gruppi che godono gli uni rispetto agli altri di questa duplice proprietà: 1° che si passa da uno all'altro con una e una sola sostituzione; 2° che tutti contengono le stesse sostituzioni.

Dico reciprocamente che, se il gruppo dell'equazione si può suddividere in $p$ gruppi che godono di questa duplice proprietà, si potrà, con una semplice estrazione di radice $p^{esima}$, con l'aggiunta di questa radice $p^{esima}$, ridurre il gruppo dell'equazione a uno di questi gruppi parziali.

Prendiamo, infatti, una funzione delle radici che sia invariabile per tutte le sostituzioni di uno di questi gruppi parziali, e varia per ogni altra sostituzione. (Basta, per questo, scegliere una funzione simmetrica dei diversi valori che assume, per tutte le permutazioni di uno dei gruppi parziali, una funzione che non è invariabile per alcuna sostituzione).

Sia $\theta$ questa funzione delle radici.

Operiamo sulla funzione $\theta$ una delle sostituzioni del gruppo totale che non sono comuni con i gruppi parziali. Sia $\theta_1$ il risultato. Operiamo sulla funzione $\theta_1$ la stessa sostituzione, e sia $\theta_2$ il risultato, e così di seguito.

---

$r$. Di conseguenza, le sue proprietà devono essere le stesse dopo l'aggiunta di tale o talaltro valore. Così il suo gruppo deve essere lo stesso quanto alle sostituzioni (Proposizione I, scolio). Pertanto, ecc.

Tutto ciò è cancellato con cura; il nuovo enunciato porta la data del 1832 e mostra, per il modo in cui è scritto, che l'autore era estremamente frettoloso, ciò che conferma l'affermazione che ho avanzato nella Nota precedente. (A. Ch.)

Siccome $p$ è un numero primo, questa successione si potrà fermare al termine $\theta_{p-1}$; poi si avrà $\theta_p = \theta_1$, $\theta_{p+1} = \theta_1$ e così di seguito.

Ciò posto, è chiaro che la funzione

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

sarà invariabile per tutte le permutazioni del gruppo totale e, di conseguenza, sarà effettivamente nota.

Se si estrae la radice $p^{esima}$ di questa funzione, e la si aggiunge all'equazione, allora, per la proposizione IV, il gruppo dell'equazione non conterrà più altre sostituzioni oltre quelle dei gruppi parziali.

Così, affinché il gruppo di una equazione possa abbassarsi per una semplice estrazione di radice, la condizione sopra è necessaria e sufficiente.

Aggiungiamo all'equazione il radicale in questione; potremo ragionare ora sul nuovo gruppo come sul precedente, e basterà che si scomponga nel modo indicato, e così di seguito, fino a un certo gruppo che conterrà solo una sola permutazione.

*Scolio.* - È facile osservare questo percorso nella risoluzione nota delle equazioni generali di quarto grado. Infatti, queste equazioni si risolvono per mezzo di una equazione di terzo grado, che richiede l'estrazione di una radice quadrata. Nella successione naturale delle idee, è quindi con questa radice quadrata che si deve cominciare. Ora, aggiungendo all'equazione di quarto grado questa radice quadrata, il gruppo dell'equazione, che contiene in tutto ventiquattro sostituzioni, si scompone in due che ne contengono solo dodici. Indicando con $a, b, c, d$ le radici, ecco uno di questi gruppi

$$\begin{array}{ccc} abcd & acdb & adbc \\ badc & cabd & dacb \\ cdab & dbac & bcad \\ dcba & bdca & cbda \end{array}$$

Ora questo gruppo si divide in tre gruppi, come è indicato dai teoremi II e III. Così, mediante l'estrazione di un solo radicale di terzo grado, rimane semplicemente il gruppo

$$\begin{array}{c} abcd \\ badc \\ cdab \\ dcab \end{array}$$

questo gruppo si divide di nuovo in due gruppi:

$$\begin{array}{cc} abcd & cdab \\ badc & dcba \end{array}$$

Così, dopo una semplice estrazione di radice quadrata, resterà

$$\begin{array}{c} abcd \\ badc \end{array}$$

che si risolverà infine con una semplice estrazione di radice quadrata.

Si ottiene così, sia la soluzione di Descartes, sia quella di Euler; poiché, benché dopo la risoluzione dell'equazione ausiliaria di terzo grado quest'ultima estrae tre radici quadrate, si sa che ne bastano due, poiché la terza si deduce razionalmente.

Applicheremo ora questa condizione alle equazioni irriducibili il cui grado è primo.

Applicazione alle equazioni irriducibili di grado un numero primo.

PROPOSIZIONE VI.

Lemma. *Un'equazione irriducibile di grado un numero primo non può divenire riducibile per l'aggiunta di un radicale il cui indice sarà diverso dal grado stesso dell'equazione.*

Poiché se $r, r', r$", ... sono i diversi valori del radicale, e $Fx = 0$ l'equazione proposta, richiederebbe che $Fx$ si divida in fattori

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

tutti dello stesso grado, cosa non possibile, a meno che $f(x, r)$ non sia di primo grado in $x$.

Così, un'equazione irriducibile di grado un numero primo non può divenire riducibile, a meno che il suo gruppo non si riduca a una sola permutazione.

## PROPOSIZIONE VII.

Problema. Qual è il gruppo di una equazione irriducibile di grado un numero primo $n$, risolvibile per radicali^?

Dalla proposizione precedente, il più piccolo gruppo possibile, prima di quello che ha una sola permutazione, conterrà $n$ permutazioni. Ora, un gruppo di permutazioni di un numero primo $n$ di lettere non si può ridurre a $n$ permutazioni, a meno che una di queste permutazioni non si deduca dall'altra per una sostituzione circolare dell'ordine $n$. (Si veda la Memoria di M. Cauchy, *Journal de l'École Polytechnique*, XVII quaderno.) Così, il penultimo gruppo sarà

$$\left\{\begin{array}{cccccccc} x_0 & x_1 & x_2 & x_3 & ... & x_{n-3} & x_{n-2} & x_{n-1} \\ x_1 & x_2 & x_3 & x_4 & ... & x_{n-2} & x_{n-1} & x_0 \\ x_2 & x_3 & ... & ... & ... & x_{n-1} & x_0 & x_1 \\ ... & ... & ... & ... & ... & ... & ... & ... \\ x_{n-1} & x_0 & x_1 & ... & ... & x_{n-4} & x_{n-3} & x_{n-2} \end{array}\right.$$

essendo $x_0, x_1, x_2, ..., x_{n-1}$ le radici.

Ora, il gruppo che precederà immediatamente quello nell'ordine delle scomposizioni dovrà comporsi di un certo numero di gruppi aventi tutti le stesse sostituzioni di quello. Osservo che queste sostituzioni si possono esprimere così (poniamo, in generale, $x_n = x_0$, $x_{n+1} = x_1$, ...; è chiaro che ognuna delle sostituzioni del gruppo (G) si ottiene mettendo dappertutto al posto di $x_k, x_{k+c}$, essendo $c$ una costante).

Consideriamo uno qualunque dei gruppi simili al gruppo (G). Dal teorema II, si dovrà ottenere operando dappertutto in questo gruppo una stessa sostituzione; per esempio, mettendo dappertutto nel gruppo (G), al posto di $x_k, x_{f(k)}$, essendo $f$ una certa funzione.

Le sostituzioni di questi nuovi gruppi dovendo essere le stesse di quelle del gruppo (G), si dovrà avere

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

essendo $C$ indipendente da $k$.

Pertanto

$$f(k + 2c) = f(k) + 2C$$
$$.....$$
$$f(k + mc) = f(k) + mC$$

Se $c = 1$, $k = 0$, si troverà

$$f(m) = am + b$$

ossia

$$f(k) = ak + b$$

con $a, b$ costanti.

Pertanto, il gruppo che precede immediatamente il gruppo (G) dovrà contenere solo sostituzioni tali che

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

e non conterrà, di conseguenza, altra sostituzione circolare oltre a quella del gruppo (G).

Si ragionerà su questo gruppo come sul precedente, e ne seguirà che il primo gruppo nell'ordine di scomposizione, cioè il gruppo *effettivo* dell'equazione, può contenere solo sostituzioni della forma

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

Pertanto, *se un'equazione è irriducibile con grado un numero primo è risolvibile per radicali, il gruppo di questa equazione potrà contenere solo sostituzioni della forma*

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

*essendo a e b costanti.*

Reciprocamente, se questa condizione vale, dico che l'equazione sarà risolvibile per radicali. Consideriamo, infatti, le funzioni

$$\begin{array}{lcl} (x_0 + \alpha x_1 + \alpha^2 x_2 + .... + \alpha^{n-1} x_{n-1}) & = & X_1 \\ \left(x_0 + \alpha x_a + \alpha^2 x_{2a} + .... + \alpha^{n-1} x_{(n-1)a}\right) & = & X_a \\ \left(x_0 + \alpha x_{a^2} + \alpha^2 x_{2a^2} + .... + \alpha^{n-1} x_{(n-1)a^2}\right) & = & X_{a^2} \\ ..... & = & ..... \end{array}$$

essendo $\alpha$ una radice $n^{esima}$ dell'unità, $a$ una radice primitiva di $n$.

È chiaro che ogni funzione invariabile per sostituzioni circolari delle quantità $X_1, X_a, X_{a^2}, ...$ sarà, in questo caso, immediatamente nota. Pertanto, si potrà trovare $X_1, X_a, X_{a^2}, ...$ con il metodo di M. Gauss per le equazioni binomie. Pertanto, ecc.

Così, affinché un'equazione irriducibile di grado un numero primo sia risolvibile per radicali, è necessario e sufficiente che ogni funzione invariabile per le sostituzioni

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

sia razionalmente nota.

Così la funzione

$$(X_1 - X)(X_a - X)(X_{a^2} - X)...$$

dovrà, qualunque sia $X$, essere nota.

È quindi necessario e sufficiente che l'equazione che dà questa funzione delle radici ammetta, qualunque sia $X$, un valore razionale.

Se l'equazione proposta ha tutti i coefficienti razionali, l'equazione ausiliaria che dà questa funzione li avrà pure tutti e basterà riconoscere se questa equazione ausiliaria di grado $1.2.3...(n-2)$ ha oppure no una radice razionale, ciò che si sa fare.

Questo è il metodo che bisognerebbe impiegare nella pratica. Ma presentiamo il teorema sotto un'altra forma.

## PROPOSIZIONE VIII.

Teorema. *Perché un'equazione irriducibile di grado un numero primo sia risolvibile per radicali, è necessario e sufficiente che essendo note due qualunque delle radici, le altre si deducano razionalmente.*

In primo luogo, si deve, per la sostituzione

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

non lasciando 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, ciò basta; poiché, in questo caso, nessuna sostituzione del gruppo lascerà due lettere agli stessi posti. Di conseguenza, il gruppo conterrà al massimo $n(n-1)$ permutazioni. Pertanto, conterrà solo una sostituzione circolare (altrimenti vi sarebbero almeno $n^2$ permutazioni). Pertanto, ogni sostituzione del gruppo, $x_k, x_{fk}$, dovrà soddisfare alla condizione

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

Pertanto, ecc.

Il teorema è quindi dimostrato.

## ESEMPIO DEL TEOREMA VII.

Sia $n = 5$; il gruppo sarà il seguente:

$$\begin{array}{lllll} abcde & bcdea & cdeab & deabc & eabcd \\ acebd & cebda & ebdac & bdace & daceb \\ aedbc & edcba & dcbae & cbaed & baedc \\ adbec & dbeca & becad & acedb & cadbe \end{array}$$

## EQUAZIONI PRIMITIVE RISOLVIBILI PER RADICALI - (Frammenti)

Cerchiamo, in generale, in quale caso un'equazione primitiva è risolvibile per radicali. Ora, possiamo di seguito stabilire un carattere generale fondato sul grado stesso di queste equazioni. Questo carattere è: *Affinché un'equazione primitiva sia risolvibile per radicali, è necessario che il suo grado sia della forma $p^\nu$, essendo $p$ un numero primo.* E da ciò seguirà immediatamente che, quando si dovrà risolvere per radicali un'equazione irriducibile il cui grado ammetterà fattori primi diseguali, lo si potrà dare solo con il metodo di scomposizione dovuto a M. Gauss; altrimenti l'equazione sarà insolubile.

Per stabilire la proprietà generale che abbiamo enunciato relativamente alle equazioni primitive che si possono risolvere per radicali, possiamo supporre che l'equazione che si vuole risolvere sia primitiva, ma cessi di esserlo per l'aggiunta di un radicale semplice. In altri termini, possiamo supporre che, essendo $n$ primo, il gruppo dell'equazione si divida in $n$ gruppi irriducibili coniugati, ma non primitivi. Poiché, a meno che il grado dell'equazione sia primo, un simile gruppo si presenterà sempre nella successione delle scomposizioni.

Sia $N$ il grado dell'equazione, e supponiamo che dopo un'estrazione di radice di grado primo $n$, essa divenga non primitiva e si divida in $Q$ equazioni primitive di grado $P$, per mezzo di una sola equazione di grado $Q$.

Se chiamiamo $G$ il gruppo dell'equazione, questo gruppo dovrà dividersi in $n$ gruppi coniugati non primitivi, nei quali le lettere si distribuiranno in sistemi composti di $P$ lettere congiunte a ognuno. Vediamo in quanti modi si potrà fare.

Sia $H$ uno dei gruppi coniugati non primitivi. È facile vedere che, in questo gruppo, due lettere qualunque prese a piacere faranno parte di un certo sistema di $P$ lettere congiunte, e faranno parte di uno solo.

Poiché, in primo luogo, se vi fossero due lettere che non possono far parte di uno stesso sistema di $P$ lettere congiunte, il gruppo $G$, che è tale che una qualunque delle sue sostituzioni trasformi le une nelle altre tutte le sostituzioni del gruppo $H$, sarà non primitivo, ciò che è contrario all'ipotesi.

In secondo luogo, se due lettere facessero parte di numerosi sistemi differenti, ne seguirebbe che i gruppi che corrispondono ai diversi sistemi di $P$ lettere congiunte non sarebbero primitivi, ciò che è ancora contrario all'ipotesi.

Ciò posto, siano

$$\begin{array}{lllll} a_0 & a_1 & a_2 & \ldots & a_{p-1} \\ b_0 & b_1 & b_2 & \ldots & b_{p-1} \\ c_0 & c_1 & c_2 & \ldots & c_{p-1} \end{array}$$

le $N$ lettere: supponiamo che ogni linea orizzontale rappresenti un sistema di lettere congiunte. Siano

$$a_0 \quad a_{0,1} \quad a_{0,2} \quad \ldots \quad a_{0,p-1}$$

$P$ lettere congiunte tutte poste nella prima colonna verticale. ( È chiaro che possiamo fare che sia una qualunque, invertendo l'ordine delle linee orizzontali).

Siano, pure

$$a_{1,0} \quad a_{1,1} \quad a_{1,2} \quad a_{1,3} \quad \ldots \quad a_{1,p-1}$$

$P$ lettere congiunte tutte poste nella seconda colonna verticale di modo che

$$a_{1,0} \quad a_{1,1} \quad a_{1,2} \quad a_{1,3} \quad \ldots \quad a_{1,p-1}$$

appartengano rispettivamente alle stesse linee orizzontali di

$$a_0 \quad a_{0,1} \quad a_{0,2} \quad a_{0,3} \quad ... \quad a_{0,p-1}$$

siano, anche, i sistemi di lettere congiunte

$$\begin{array}{cccccc} a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} & ... & a_{2,p-1} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} & ... & a_{3,p-1} \\ ... & ... & ... & ... & ... & ... \end{array}$$

otterremo così, in tutto, $P^2$ lettere. Se il numero totale delle lettere non è esaurito, si prenderà un terzo indice, di modo che

$$a_{m,n,0} \quad a_{m,n,1} \quad a_{m,n,2} \quad a_{m,n,3} \quad ... \quad a_{m,n,p-1}$$

sia, in generale, un sistema di lettere congiunte; e si arriverà così a questa conclusione, che $N = P^\mu$, essendo $\mu$ un certo numero uguale a quello degli indici differenti di cui si avrà bisogno. La forma generale delle lettere sarà

$$a_{k,k_m,k_n,...k_\mu}$$

essendo $k_1, k_2, k_3, ..., k_\mu$ indici che possono assumere ciascuno i $P$ valori $0, 1, 2, 3, ..., P-1$.

Si vede così, dal modo in cui abbiamo proceduto, che, nel gruppo $H$, tutte le sostituzioni saranno della forma

$$\left[a_{k_1,k_0,k_2,...,k_\mu}, a_{\varphi(k_2),\psi(k)_2,\chi(k_2),...,\sigma(k_\mu)}\right]$$

poiché ogni indice corrisponde a un sistema di lettere congiunte.

Se $P$ non è un numero primo, si ragionerà sul gruppo di permutazioni di uno qualunque dei sistemi di lettere congiunte, come sul gruppo $G$, sostituendo ogni indice con un certo numero di nuovi indici, e si troverà $P = R^\alpha$, e così di seguito; da cui infine $N = p^\nu$,essendo $p$ un numero primo.

**Equazioni primitive di grado $p^2$.** Soffermiamoci un momento a trattare di seguito le equazioni primitive di un grado $p^2$, essendo $p$ un numero dispari. (Il caso di $p = 2$ è stato esaminato). Se un'equazione di grado $p^2$ è risolvibile per radicali, supponiamo dapprima tale che divenga non primitiva per un'estrazione di radicale.

Sia quindi $G$ un gruppo primitivo di $p^2$ lettere che si divide in $n$ gruppi non primitivi coniugati a $H$.

Le lettere dovranno necessariamente, nel gruppo $H$, distribuirsi così

$$\begin{array}{cccccc} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} & ... & a_{0,p-1} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} & ... & a_{1,p-1} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} & ... & a_{2,p-1} \\ ... & ... & ... & ... & ... & ... \\ a_{p-1,0} & a_{p-1,1} & a_{p-1,2} & a_{p-1,3} & ... & a_{p-1,p-1} \end{array}$$

essendo ogni linea orizzontale e verticale un sistema di lettere congiunte.

Se si permutano tra loro le linee orizzontali, il gruppo che si otterrà, essendo primitivo e di grado un numero primo, dovrà contenere solo sostituzioni della forma

$$(a_{k_1,k_2}, a_{mk_1+mk_2})$$

essendo gli indici presi rispetto al modulo $p$.

Sarà così per le linee che non potranno dare che sostituzioni della forma

$$(a_{k_1,k_2}, a_{k_1,qk_2+r})$$

Pertanto infine tutte le sostituzioni del gruppo $H$ saranno della forma

$$(a_{k_1,k_2}, a_{m_1k_1+n_1,m_2k_2+n_2})$$

Se un gruppo $G$ si divide in $n$ gruppi coniugati a quello descritto, tutte le sostituzioni del gruppo $G$ dovranno trasformare le une nelle altre le sostituzioni circolari del gruppo $H$, che sono tutte scritte come segue:

$$(a_{k_1,k_2}, ..., a_{k_1+\alpha_1,k_2+\alpha_2,...}) \tag{0.0.8}$$

Supponiamo quindi che una delle sostituzioni del gruppo $G$ si formi sostituendo rispettivamente

$$\begin{array}{ll} k_1 & con \quad \varphi_1(k_1,k_2) \\ k_2 & con \quad \varphi_2(k_1,k_2) \end{array}$$

Se, nelle funzioni $\varphi_1, \varphi_2$, si sostituiscono per $k_1$ e $k_2$ i valori $k_1+\alpha_1, k_2+\alpha_2$, si dovranno ottenere risultati della forma

$$\varphi_1 + \mathscr{C}_1 \quad \varphi_2 + \mathscr{C}_2$$

ed è facile concludere immediatamente che le sostituzioni del gruppo $G$ devono essere tutte comprese nella formula

$$(a_{k_1,k_2}, a_{m_1k_1+n_1k_2+\alpha_1 m_2k_1+n_2k_1+\alpha_2}) \tag{0.0.9}$$

Sappiamo, dal n°[22], che le sostituzioni del gruppo $G$ non possono abbracciare che $p^2-1$ o $p^2-p$ lettere. Non è $p^2-p$, poiché, in questo caso, il gruppo $G$ sarebbe primitivo. Se quindi, nel gruppo $G$, si considerano solo le permutazioni dove la lettera $a_{0,0}$, per esempio, conserva sempre lo stesso posto, si avranno solo sostituzioni dell'ordine di $p^2-1$ tra le $p^2-1$ altre lettere.

Ma ricordando qui che è semplicemente per la dimostrazione che abbiamo supposto che il gruppo primitivo $G$ si divideva in gruppi coniugati non primitivi. Siccome questa condizione non è per nulla necessaria, i gruppi saranno spesso molto più composti.

Si tratta quindi di riconoscere in quale caso questi gruppi potranno ammettere sostituzioni dove $p^2-p$ lettere soltanto varieranno, e questa ricerca richiede qualche tempo.

Sia quindi $G$ un gruppo che contiene qualche sostituzione dell'ordine $p^2-p$; dico dapprima che tutte le sostituzioni di questo gruppo saranno lineari, cioè della forma (A1).

La cosa è riconosciuta vera per le sostituzioni dell'ordine $p^2-1$; basta quindi dimostrarla per quelle dell'ordine $p^2-p$. Considereremo quindi un gruppo dove le sostituzioni sarebbero tutte $m$ dell'ordine $p^2$o dell'ordine $p^2-p$. (Si veda il luogo citato).

Allora le $p$ lettere che, in una sostituzione dell'ordine $p^2-p$, non varieranno, dovranno essere lettere congiunte.

Supponiamo che queste lettere congiunte siano

$$a_{0,0}, a_{0,1}, a_{0,2}, ..., a_{0,p-1}$$

Possiamo dedurre tutte le sostituzioni dove queste $p$ lettere non cambiando posto, possiamo dedurle da sostituzioni della forma

$$(a_{k_1,k_2}, a_{k_1,\varphi k_2})$$

e da sostituzioni dell'ordine $p^2-p$, il cui periodo sarà di $p$ termini. (Si veda ancora il luogo citato).

Le prime devono necessariamente, affinché il gruppo goda della proprietà voluta, ridursi alla forma

$$(a_{k_1,k_2}, a_{k_1,mk_2})$$

secondo quanto si è visto per le equazioni di grado $p$.

Quanto alle sostituzioni il cui periodo sarebbe di $p$ termini, siccome sono coniugate alle precedenti, possiamo supporre un gruppo che le contiene senza contenere queste: quindi esse dovranno trasformare le sostituzioni circolari (a) le une nelle altre; quindi saranno anche lineari.

Siamo quindi arrivati a questa conclusione, che il gruppo primitivo di permutazioni di $p^2$ lettere deve contenere solo sostituzioni della forma (A1).

[22]Questa Memoria fa seguito a un lavoro di Galois che non possiedo, mi è impossibile indicare la Memoria qui citata e in seguito.

Ora, prendiamo il gruppo totale che si ottiene operando sull'espressione

$$a_{k_1,k_2}$$

tutte le sostituzioni lineari possibili, e cerchiamo quali sono i divisori di questo gruppo che possono godere della proprietà voluta per la risolvibilità delle equazioni.

Quale è dapprima il numero totale delle sostituzioni lineari? In primo luogo, è chiaro che ogni trasformazione della forma

$$k_1k_2, m_1k_1 + n_1k_2 + 1\alpha_1 m_2k_1 + n_2k_2 + \alpha_2$$

non sarà per questo una sostituzione; poiché è necessario, in una sostituzione che a ogni lettera della prima permutazione corrisponda una sola lettera della seconda; e reciprocamente.

Se quindi si prende una lettera qualunque $a_{l_1,l_2}$ della seconda permutazione, e si risale alla lettera corrispondente nella prima, si dovrà trovare una lettera $a_{k_1,k_2}$ dove gli indici $k_1, k_2$ saranno perfettamente determinati. È necessario quindi che, qualunque siano $l_1$ e $l_2$, si abbia per le due equazioni

$$m_1k_1 + n_1k_2 + \alpha_1 = l_1 \quad m_2k_1 + n_2k_2 + \alpha_2 = l_2$$

valori di $k_1$ e $k_2$ determinati e finiti. Così la condizione affinché una simile trasformazione sia realmente una sostituzione, è che $m_1n_2 - m_2n_1$ non sia né nulla né divisibile per il modulo $p$, ciò che è la stessa cosa.

Dico ora che, benché questo gruppo a sostituzioni lineari non appartenga sempre, come si vedrà, a equazioni risolvibili per radicali, godrà tuttavia di questa proprietà, che se in una qualunque delle sue sostituzioni vi sono $n$ lettere fisse, $n$ dividerà il numero delle lettere. E, infatti, qualunque sia il numero delle lettere che rimangono fisse, si potrà esprimere questa circostanza con equazioni lineari che daranno tutti gli indici di una delle lettere fisse, per mezzo di un certo numero tra loro. Dando a ciascuno di questi indici, rimasti arbitrari, $p$ valori, si avranno $p^m$ sistemi di valori, essendo $m$ un dato numero. Nel caso che ci occupa, $m$ è necessariamente $< 2$ ,e si trova, di conseguenza essere 0 o 1. Quindi il numero delle sostituzioni non potrà essere più grande di

$$p^2\left(p^2-1\right)\left(p^2-p\right)$$

Consideriamo ora che le sostituzioni lineari dove la lettera $a_{0,0}$ non varia; se, in questo caso, troviamo il numero totale delle permutazioni del gruppo che contiene tutte le sostituzioni lineari possibili, non basterà moltiplicare questo numero per $p^2$.

Ora, in primo luogo, sostituendo $p$ all'indice $k_2$, tutte le sostituzioni della forma

$$(a_{k_1,k_2}, a_{m_1k_1,k_2})$$

daranno in tutto $p-1$ sostituzioni. Se ne avrà $p^2 - p$ aggiungendo al termine $k_2$ il termine $m_2k$, così che segue:

$$(k_1 \cdot K_2, m_1k_1 \cdot m_2k_1 + k_2) \tag{0.0.10}$$

Da un altro lato, è facile trovare un gruppo lineare di $p^2 - 1$ permutazioni, tale che, in ognuna delle sostituzioni, tutte le lettere, ad eccezione di $a_{0,0}$, variano. Poiché, sostituendo il doppio indice $k_1k_2$ con l'indice semplice $k_1 + ik_2$, essendo $i$ una radice primitiva di

$$x^{p^2-1} - 1 = 0 \quad (mod\, p)$$

È chiaro che ogni sostituzione della forma

$$\left[a_{k_1+k_2i}, a_{(m_1+m_2)(k_1+k_2)}\right]$$

sarà una sostituzione lineare; ma, in queste sostituzioni, nessuna lettera rimane allo stesso posto, ed esse sono nel numero di $p^2 - 1$.

Abbiamo quindi un sistema di $p^2 - 1$ permutazioni tale che, in ognuna delle sue sostituzioni, tutte le lettere variano, tranne $a_{0,0}$. Combinando queste sostituzioni con le $p^2 - p$ di cui si è parlato prima, avremo

$$\left(p^2-1\right)\left(p^2-p\right)$$

sostituzioni.

Ora, abbiamo visto a priori che il numero delle sostituzioni dove $a_{0,0}$ rimane fisse non poteva essere maggiore di $(p^2-1)(p^2-p)$. Pertanto è precisamente uguale a $(p^2-1)(p^2-p)$, e il gruppo lineare totale avrà in tutto

$$p^2\left(p^2-1\right)\left(p^2-p\right)$$

permutazioni.

Rimangono da cercare i divisori di questo gruppo, che possono godere della proprietà di essere risolvibili per radicali. Per questo, faremo una trasformazione che ha per scopo di abbassare il più possibile le equazioni generali di grado $p^2$ il cui gruppo sarebbe lineare.

In primo luogo, siccome le sostituzioni circolari di un simile gruppo sono tali che ogni altra sostituzione del gruppo trasforma le une nelle altre, si potrà abbassare l'equazione di un grado, e considerare un'equazione di grado $p^2-1$ il cui gruppo avrà solo sostituzioni della forma

$$(b_{k_1,k_2}, b_{m_1k_2+m_1k_2\cdot m_2k_1+n_2k_2})$$

essendo le lettere $p^2-1$

$$\begin{array}{ccccc} & b_{0\cdot1} & b_{0\cdot2} & b_{0\cdot3} & .... \\ b_{1\cdot0} & b_{1\cdot1} & b_{1\cdot2} & b_{1\cdot3} & .... \\ b_{2\cdot0} & b_{2\cdot1} & b_{2\cdot2} & b_{2\cdot3} & .... \\ ... & ... & ... & ... & .... \end{array}$$

Osservo ora che questo gruppo non primitivo, in modo che tutte le lettere dove il rapporto dei due indici è lo stesso sono lettere congiunte. Se si sostituisce con una sola lettera ogni sistema di lettere congiunte, si avrà un gruppo in cui tutte le sostituzioni saranno della forma

$$\left(b_{\frac{k_1}{k_2}}, b_{\frac{m_1k_1+n_1k_2}{m_2k_1+n_2k_1}}\right)$$

essendo $\frac{k_1}{k_2}$ i nuovi indici. Sostituendo questo rapporto con un solo indice $k$, si vede che le $p+1$ lettere saranno

$$b_0, b_1, b_2, b_3, ...., b_{p-1}, b_{\frac{1}{0}}$$

e le sostituzioni saranno della forma

$$\left(k, \frac{mk+n}{rk+s}\right)$$

Cerchiamo quante lettere, in ognuna delle sostituzioni, rimangono allo stesso posto; bisogna per questo risolvere l'equazione

$$(rk+s)k - m(mk+n) = 0$$

che avrà due, o una, o nessuna radice, a seconda che $(m-s)^2+4nr$ sarà resto quadratico, nullo o non resto quadratico. Secondo questi tre casi, la sostituzione sarà dell'ordine $p-1$, o $p$, o $p+1$.

Si può prendere per tipo dei due primi casi le sostituzioni della forma

$$(k, mk+n)$$

dove la sola lettera $b_{\frac{1}{0}}$ non varia, e da ciò si vede che il numero totale delle sostituzioni del gruppo ridotto è

$$(p+1)p(p-1)$$

Dopo aver così ridotto questo gruppo, lo tratteremo generalmente. Cercheremo dapprima in quale caso un divisore di questo gruppo, che conterrebbe sostituzioni dell'ordine $p$, potrebbe appartenere a un'equazione risolvibile per radicali.

In questo caso, l'equazione sarà primitiva e non potrà essere risolvibile per radicali, a meno che non si abbia $p+1=2^n$, essendo $n$ un dato numero.

Possiamo supporre che il gruppo contenga solo sostituzioni dell'ordine $p$ e dell'ordine $p+1$. Tutte le sostituzioni dell'ordine $p+1$ saranno di conseguenza simili, e il loro periodo sarà di due termini.

Prendiamo quindi l'espressione

$$\left(k, \frac{mk+n}{rk+s}\right)$$

e vediamo in quale caso questa sostituzione può avere un periodo di due termini. Serve per questo che la sostituzione inversa si confonda con essa. La sostituzione inversa è

$$\left(k, \frac{-sk+n}{rk-m}\right)$$

Pertanto, si deve avere $m = -s$, e tute le sostituzioni in questione saranno

$$\left(k, \frac{mk+n}{k-m}\right)$$

o ancora

$$k, m + \frac{N}{k-m}$$

essendo $N$ un certo numero che è lo stesso per tutte le sostituzioni, poiché queste sostituzioni devono essere trasformate le une nelle altre da tutte le sostituzioni dell'ordine $p, (k, k+m)$; ora queste sostituzioni devono, inoltre, essere coniugate le une alle altre. Se quindi

$$\left(k, m + \tfrac{N}{k-m}\right) \quad \left(k, n + \tfrac{N}{k-n}\right)$$

sono due simili sostituzioni, bisogna che si abbia

$$n + \frac{N}{\frac{N}{k-m} + m - n} = m + \frac{N}{\frac{N}{k-n} + n - m}$$

cioè,

$$(m-n)^2 = 2N$$

Quindi la differenza tra due valori di $m$ non può acquisire se non due valori differenti; quindi $m$ non può avere più di tre valori; quindi infine $p = 3$. Così, è solo in questo caso che il gruppo ridotto potrà contenere sostituzioni dell'ordine $p$.

E, infatti, la ridotta sarà allora di quarto grado, e di conseguenza risolvibile per radicali.

Sappiamo per questo che in generale, tra le sostituzioni del nostro gruppo ridotto, non si dovranno trovare sostituzioni dell'ordine $p$, Forse ve ne sono dell'ordine $p-1$? È quanto vado a ricercare[23].

[23]Ho cercato inutilmente nei fogli di Galois la continuazione di quanto si legge. A. Ch.