SULLA RISOLUZIONE

DELLE

EQUAZIONI ALGEBRICHE

MEMORIA

DEL DOTT. ENRICO BETTI

Professore di Matematiche
nel liceo Forteguerri
di Pistoja.

ESTRATTA DAGLI ANNALI
DI SCIENZE MATEMATICHE E FISICHE
PUBBLICATI IN ROMA
FEBBRAIO E MARZO 1852

ROMA
TIPOGRAFIA DELLE BELLE ARTI
1852

SULLA RISOLUZIONE DELLE EQUAZIONI ALGEBRICHE

Nella presente memoria ho preso a trattare colla massima generalità i problemi relativi alla risolubilità delle equazioni algebriche, che si proposero i due sommi geometri *Abel* e *Galois*, e intorno ai quali, per la morte che li rapì ambedue alla scienza ancor giovanissimi, non poterono lasciare altro che poche traccie della via tenuta per raggiunger lo scopo, e molti dei più importanti teoremi, ma privi in gran parte delle loro dimostrazioni.

Dopo che *Paolo Ruffini* di Modena ebbe dimostrata l' impossibilità di risolvere per radicali le equazioni di grado superiore al quarto in generale, *Abel* il primo si propose di determinare le condizioni da verificarsi, affinchè una equazione di grado qualunque fosse in particolare risolubile per radicali. Il metodo da lui seguito in queste ardue ricerche si trova in parte abbozzato in un frammento di memoria ritrovato tra le sue carte, e pubblicato nella collezione delle sue opere fatta per cura del professore *Holmboe*. I chiarissimi Sigg. *Malmsten* e *Luther* hanno sviluppato, ed esteso nel Giornale di *Crelle* questo bel metodo, per applicarlo, il primo, alla dimostrazione del teorema di *Abel* sulla risolubilità delle equazioni di grado primo, il secondo alla determinazione dei criterj di risolubilità delle equazioni di 5° e 6° grado.

Galois quasi contemporaneamente all' *Abel* meditava sullo stesso problema, e 17 mesi dopo la morte di questi, presentava all'Accademia delle Scienze di Parigi una memoria dove esponeva una nuova e profonda teoria da lui creata per risolvere il problema preso sotto un punto di vista più generale, e l' applicava alla dimostrazione di un teorema sulla risolubilità per

radicali delle equazioni di grado primo, il quale non è, come io ho già fatto conoscere (*), che una trasformazione di quello di *Abel*, poi dimostrato da *Malmsten*, e del quale egli non poteva aver cognizione. *Poisson* e *Lacroix* eletti a riferire sulla medesima la ritennero quasi inintelligibile, e rimproverarono al giovine autore la mancanza della chiarezza.

Il chiarissimo Sig. *Liouville*, pubblicando questa memoria, e altri frammenti sullo stesso soggetto ritrovati dopo la morte di *Galois*, annunziò di esser giunto, dopo aver colmato alcune leggiere lacune, a riconoscere l'esattezza intera del metodo col quale è provato in particolare il rammentato teorema, e fece conoscere la intenzione che egli aveva di pubblicare un Commentario per completare certi passaggi, e rischiarare certi punti delicati di quella memoria.

Le condizioni di risolubilità per radicali delle equazioni di grado primo possono pertanto ritenersi determinate e dimostrate con ambedue i metodi dei due sommi geometri. Rimanevano però fin ora da determinarsi quelle relative alle equazioni di grado non primo, molte delle quali trovansi annunziate da essi sotto forme differenti, può dirsi senza dimostrazione, nei frammenti postumi. Riempire questa lacuna è l'oggetto principale del mio lavoro.

Io ho instituita con qualche novità una teoria delle sostituzioni, e per mezzo di essa ho potuto dedurre con facilità e rigore dalla bella teoria del *Galois* che ho sviluppata ed estesa, la determinazione delle condizioni di risolubilità per radicali, delle equazioni di un grado qualunque, e dimostrare tutti i teoremi relativi, tanto sotto la forma nella quale li annunziò *Abel*, quanto sotto quella colla quale li annunziò *Galois*, e aggiungerne alcuni nuovi per completare la soluzione del problema.

Le condizioni generali necessarie e sufficienti alla risolubilità di una equazione di grado qualunque non le ho date

(*) Vedi Annali di scienze Fis. e Mat. compilati da B. Tortolini. gennajo 1851.

soltanto per il caso in cui vogliasi una risoluzione per radicali, ma anche per quello in cui ci contentiamo di averla con radici di altre equazioni algebriche; e ho accennato un principio di classificazione degl'irrazionali, il quale spero di potere sviluppare in altro lavoro.

Ho divisa la memoria in due parti. Nella prima ho esposta la teoria delle sostituzioni: nella seconda la determinazione delle condizioni di risolubilità delle equazioni algebriche.

PARTE PRIMA

CAPITOLO PRIMO

DELLE SOSTITUZIONI

I.

PRINCIPJ DEL CALCOLO DELLE SOSTITUZIONI

1.° Una *sostituzione* è la operazione mediante la quale si passa da una ad un altra permutazione di più quantità.

Ci serviremo di una sola lettera x con diversi indici i posti al basso per distinguer tra loro tutte le quantità che entrano nelle permutazioni. Perciò potremo ritenere che ogni sostituzione si eseguisca sostituendo a tutti gli apici i una funzione $\varphi(i)$ dei medesimi; e la indicheremo colla notazione

$$\begin{pmatrix} x_i \\ x_{\varphi(i)} \end{pmatrix}.$$

La funzione $\varphi(i)$ dovrà godere la proprietà di prendere per tutti i valori successivi di i, li stessi valori che prende i, ma in ordine differente.

2.° Adotteremo diversi sistemi di apici secondo il numero n delle lettere.

1.° Se

$$n = p,$$

e p numero primo, prenderemo per apici le p radici della congruenza

$$i^p \equiv i \pmod{p},$$

le quali saranno i numeri naturali da zero a $p - 1$; poichè riguarderemo eguale a zero la parte di ogni numero multipla di p.

2.° Quando sia

$$n = p^\nu,$$

p un numero primo e ν un numero qualunque, ci serviremo per apici, delle p^ν radici della congruenza

$$(1) \qquad i^{p^\nu} \equiv i \pmod{p}.$$

Galois ha osservato che, se

$$F(t) \equiv 0 \pmod{p}$$

è una congruenza irriduttibile di grado ν, e t una radice incommensurabile della medesima; tutte le radici della (1) sono date dalla espressione

$$i = a_0 + a_1 t + a_2 t^2 + \ldots + a_{\nu-1} t^{\nu-1};$$

dove $a_0, a_1 \ldots a_{\nu-1}$ prendono successivamente tutti i valori interi minori di p, e si riguardano eguali a zero le quantità multiple di p (*). Le proprietà principali di questa specie di numeri complessi sono state poi dimostrate con molta chiarezza e rigore dal Sig. *Schönemann* in una Memoria inserita nel tomo 31 del giornal di Crelle, intitolata *Grandzüge einer allgemeiner Theorie von höhern Congruenzen.*

3.° Se

$$n = p^\nu q^\mu r^\sigma \ldots,$$

e p, q, r numeri primi, e ν, μ, σ . . . qualunque, distingue-

(*) Vedi Journal de Liouville T. XI, pag. 398, ovvero Bullettin de Ferrussac T. XIII, pag. 428.

remo le quantità con più apici per ciascuna lettera, i quali siano della natura dei precedenti, cioè radici delle congruenze

$$k^{p^\nu} \equiv k \pmod{p}, \quad h^{q^\mu} \equiv h \pmod{q}, \quad l^{r^\sigma} \equiv l \pmod{r} \ldots\ldots$$

Per brevità, in questa prima parte, indicheremo le sostituzioni col semplice segno delle funzioni degli apici che debbono sostituirsi ai medesimi per eseguirle, servendoci per il segno di funzione, sempre di lettere greche. Così scriveremo φ in luogo di $\begin{pmatrix} x_i \\ x_{\varphi(i)} \end{pmatrix}$.

4.° Le operazioni successive di più sostituzioni $\theta_0\, \theta_1\, \theta_2 \ldots \theta_{n-1}$ equivalgono a una sola sostituzione φ che rappresenteremo, come il primo fece *Cauchy* (*), col prodotto di quelle:

$$\varphi = \theta_0\, \theta_1\, \theta_2 \ldots \theta_{n-1} ;$$

disponendo i fattori nell'ordine col quale sono state eseguite le rispettive sostituzioni

Se fosse

$$\theta_0 = \theta_1 = \theta_2 \ldots = \theta_{n-1},$$

si avrebbe

$$\varphi = \theta^n.$$

5.° Se θ è una sostituzione circolare sopra p lettere, ripetuta p volte riprodurrà la permutazione d'onde siamo partiti; perciò si avrà la stessa permutazione eseguendola a o b volte, quando sia

$$a \equiv b \pmod{p},$$

e si potrà porre

$$\theta^{mp+a} = \theta^n :$$

onde si dovrà stabilire

$$\theta^p = 1.$$

6.° Ogni sostituzione, che non è circolare sopra un certo numero di lettere, equivale a più sostituzioni circolari effet-

(*) Vedi Iournal de l'Ecole Pol. T. X.

tuate sopra lettere differenti, e quindi con un ordine qualunque (*).

Siano $\varphi_0\ \varphi_1\ \ldots\ \varphi_{m-1}$ queste sostituzioni circolari, avremo

$$\theta = \varphi_0\ \varphi_1\ \varphi_2\ \ldots\ \varphi_{m-1}$$

e ripetendola n volte, poichè è indifferente l'ordine con cui si eseguiscono le sostituzioni su lettere differenti, si otterrà

$$\theta^n = \varphi_0^n\ \varphi_1^n\ \varphi_2^n\ \ldots\ \varphi_{m-1}^n\ .$$

Affinchè $\theta^n = 1$ è evidente che dovranno esser soddisfatte le seguenti equazioni

$$\varphi_0^n = 1\ ,\quad \varphi_1^n = 1\ ,\quad \varphi_2^n = 1\ ,\ \ldots\ \varphi_{m-1}^n = 1\ .$$

Se $p_0 p_1 \ldots p_{m-1}$ sono i numeri delle lettere sopra le quali rispettivamente sono eseguite le sostituzioni $\varphi_0\ \varphi_1\ \ldots\ \varphi_{m-1}$, queste equazioni non potranno esser soddisfatte a meno che n non sia divisibile per $p_o\ ,\ p_1\ ,\ \ldots\ p_{m-1}$.

7.° Chiameremo *ordine* di una sostituzione il numero che indica quante permutazioni differenti si possono ottenere eseguendola più volte successive, e che è la minima potenza della sostituzione, che dà per risultato l'unità. Ciò che si è stabilito nei due paragrafi precedenti dà i seguenti teoremi:

1. *Le potenze di una sostituzione, gli esponenti delle quali sono congrui rispetto all'ordine, sono eguali tra loro.*

2. *L'ordine di una sostituzione circolare su p lettere è eguale a p.*

3. *L'ordine di una sostituzione qualunque è eguale al minimo divisibile per tutti gli ordini delle sostituzioni circolari sopra lettere differenti, delle quali è il prodotto.*

4. *Se il numero p delle lettere è primo, ogni sostituzione di* p^{esimo} *ordine sarà circolare su tutte le lettere.*

5. *Una sostituzione di ordine primo p, o è circolare su p lettere, o è il prodotto di più circolari su p lettere differenti ciascuna.*

(*) V. Serret, Cours d'Alg. sup. pag. 252 o Journal de l'Ecole Polithecnique T.X.

8.° La sostituzione mediante la quale dalla permutazione ottenuta colla θ^m, si torna a quella d'onde siamo partiti è θ^{p-m}; se p è l'ordine di θ. Ora poichè $\theta^p = 1$ si potrà stabilire che

$$\theta^{p-m} = \theta^{-m},$$

ossia che un esponente negativo indica una sostituzione inversa a quella che rappresenterebbe quando si prendesse positivamente.

Per passare dalla permutazione ottenuta colla sostituzione θ^n a quella ottenuta colla ψ^m, la sostituzione da farsi potrà rappresentarsi con $\theta^{-n}\psi^m$.

9. Se si ha eguaglianza tra due prodotti di più sostituzioni si potranno moltiplicare ambedue a destra per una stessa sostituzione, come pure a sinistra; ma non però in generale uno a destra e l'altro a sinistra.

II.

DELLE SOSTITUZIONI DERIVATE.

10.° Allorché più sostituzioni sono tali che le lettere cangiate da ciascuna di esse sono lasciate ferme da tutte le altre, il loro prodotto non varia se si cangia l'ordine col quale sono disposti i fattori. Ma se due sostituzioni θ e ψ inducono cangiamento anche sulle stesse lettere, non è più indifferente l'ordine dei fattori, non è più in generale

$$\theta\psi = \psi\theta,$$

ma invece

$$\theta\psi = \psi\theta_1 ; \tag{1}$$

dove θ_1 è un altra sostituzione.

Moltiplicando da ambe le parti per ψ^{-1} si ricava

$$\theta_1 = \psi^{-1}\theta\psi. \tag{2}$$

La sostituzione θ_1 la diremo la *derivata di* θ *per mezzo di* ψ, θ la sostituzione *primitiva* e ψ la *derivante*.

La derivata di θ_1 la chiameremo derivata seconda di θ, la derivata della derivata seconda, derivata terza, e così di seguito.

Indichiamo colla notazione D_{ψ}^{m} la derivata m^{sima} di θ per mezzo di ψ; avremo

$$(3) \quad D_{\psi}^{n}\,\theta.\psi = \psi\, D_{\psi}^{n+1}\,\theta\;; \quad D_{\psi}^{m}\, D_{\psi}^{n}\,\theta = D_{\psi}^{m+n}\theta\;; \; D_{\psi}^{0}\,\theta = \theta;$$

La quantità m la chiameremo l'*indice* della derivata.

11.° Prendiamo le equazioni

$$D_{\psi}\theta = \psi^{-1}\,\theta\psi\,, \qquad D_{\psi}\varphi = \psi^{-1}\,\varphi\psi\,, \qquad D_{\psi}\chi = \psi^{-1}\,\chi\psi$$

. . . . . .

Moltiplicandole tra loro, avremo

$$D_{\psi}\,\theta\,.D_{\psi}\,\varphi\,.D_{\psi}\,\chi\,\ldots = \psi^{-1}\,\theta\varphi\chi\ldots\psi = D_{\psi}\,\theta\varphi\chi\ldots.$$

ossia : *la derivata del prodotto di più sostituzioni è eguale al prodotto delle derivate delle medesime.*

Se

$$\theta = \varphi = \chi = \ldots\;; \quad \text{sarà} \quad (D_{\psi}\,\theta)^{n} = D_{\psi}\theta^{n}\;;$$

essendo n il numero delle sostituzioni : dunque *la derivata della potenza n^{esima} di una sostituzione è la potenza n^{esima} della derivata.*

12.° Se

$$\theta^{n} = 1\,,$$

sarà

$$(D_{\psi}\,\theta)^{n} = D_{\psi}1 = \psi^{-1}\,\psi = \psi^{0} = 1\,:$$

viceversa, quando

$$(D_{\psi}\,\theta)^{n} = 1\,,$$

è

$$D_{\psi}\,\theta^{n} = 1\,;$$

e quindi

$$1 = \psi^{-1}\,\theta^{n}\,\psi\,, \qquad \psi = \theta^{n}\,\psi\,, \qquad 1 = \theta^{n}\,.$$

Di quì è facile dedurre che *la sostituzione e la sua derivata sono dello stesso ordine.*

13.° *La derivata per mezzo di una sostituzione φ, della derivata per mezzo di un altra ψ, di una qualunque θ, è eguale alla derivata della medesima θ per mezzo del prodotto $\psi\varphi$.*

Infatti

$$\theta\psi = \psi \mathrm{D}_\psi \theta\,, \qquad \mathrm{D}_\psi\, \theta\,.\,\varphi = \varphi \mathrm{D}_\varphi\, \mathrm{D}_\psi\, \theta\,:$$

moltiplichiamo a sinistra la 2.ª per ψ, avremo riducendo colla 1ª

$$\theta\psi\varphi = \psi\varphi \mathrm{D}_\varphi\, \mathrm{D}_\psi\, \theta\,;$$

ma

$$\theta\psi\varphi = \psi\varphi \mathrm{D}_{\psi\varphi}\theta\,;$$

dunque

$$\mathrm{D}_\varphi\, \mathrm{D}_\psi\, \theta = \mathrm{D}_{\psi\varphi}\theta\,:$$

e in generale si può dedurre da queste

$$(4) \qquad \theta\gamma \ldots \chi\psi\varphi = \gamma \ldots \chi\psi\varphi\, \mathrm{D}_\varphi\, \mathrm{D}_\psi\, \mathrm{D}_\chi \ldots . \mathrm{D}_\gamma\theta$$

$$(5) \qquad \mathrm{D}_\varphi\, \mathrm{D}_\psi\, \mathrm{D}_\chi \ldots . \mathrm{D}_\gamma\, \theta = \mathrm{D}_\gamma \ldots \chi\psi\varphi\, \theta\,.$$

Se

$$\varphi = \psi = \chi \ldots = \gamma\,,$$

la (4) e la (5) divengono

$$(6) \quad \theta\psi^p = \psi^p \mathrm{D}_\psi^p\, \theta,$$

o

$$(7) \quad \mathrm{D}_{\psi^p}\, \theta = \mathrm{D}_\psi^p\, \theta;$$

quindi *la derivata per mezzo della potenza p^{esima} di una sostituzione è eguale alla derivata p^{esima} per mezzo della medesima sostituzione.*

14.° Quando

$$\mathrm{D}_\psi^p\, \theta = \mathrm{D}_\psi^p\, \varphi$$

è anche (v. n.° 13.°)

$$\mathrm{D}_{\psi^p}\, \theta = \mathrm{D}_{\psi^p}\, \varphi,$$

quindi

$$\theta\psi^p = \varphi\psi^p\,, \quad \theta = \psi\,;$$

dunque *derivate dello stesso indice eguali hanno eguali le loro primitive.*

Se $\psi^p = 1$, la (6) dà

$$(8) \qquad D_\psi^p \theta = \theta \ ;$$

dalla quale si ricava

$$D_\psi^a \theta = D_\psi^b \theta$$

quando è

$$a \equiv b \ (\text{mod. } p) :$$

le derivate gl'indici delle quali sono congrui rispetto all'ordine della derivante sono eguali tra loro.

Sia ora n il minimo numero per il quale si abbia

$$(9) \qquad D_\psi^n \theta = \theta,$$

e

$$(10) \qquad p = mn + r \ ,$$

essendo p l'ordine di ψ.

Derivando $(m-1)n$ volte la (7), si ha

$$(11) \qquad D_\psi^{mn} \theta = D_\psi^{(m-1)n} \theta = \theta:$$

e dalla (8) sostituendo in essa a p il valore (10),

$$(12) \qquad D_\psi^{mn} \theta . D_\psi^r \theta = \theta \ .$$

Eguagliando la (11) e la (12), si ha

$$D_\psi^{mn} \theta . D_\psi^r \theta = D_\psi^{mn} \theta:$$

onde

$$D_\psi^r \theta = \theta,$$

e perché $r < n$, dovrà essere

$$r = 0 \ .$$

Dunque *l'indice minimo di una derivata eguale alla primitiva, è un divisore dell' ordine della derivante ; e sono eguali le derivate che hanno gl'indici congrui rispetto al medesimo.*

Se l' ordine di ψ é un numero primo p le derivate differenti di una sostituzione qualunque rispetto a ψ saranno p.

CAPITOLO SECONDO

DEI GRUPPI DI PERMUTAZIONI

I.

DELLE SOSTITUZIONI DI UN GRUPPO.

15.° Dicesi *Gruppo di permutazioni* una serie di permutazioni tali che una sostituzione mediante la quale si passa da una ad un altra qualunque di esse, eseguita su tutte, non faccia che permutarle tra loro, senza produrne nessuna nuova che non appartenga già al gruppo. Si dicono sostituzioni del gruppo quelle colle quali si passa da una a tutte le altre permutazioni del medesimo. Se queste siano ψ_0, ψ_1, ψ_2 ... ψ_{p-1} dovrà aversi

$$\psi_m \ \psi_n = \psi_r ,$$

essendo r un valore intero dipendente da m e da n, e minore di p.

Un gruppo che contenga n permutazioni lo diremo di *grado* n^{simo}.

Una funzione di più quantità che non muti valore altro che per le sostituzioni di un gruppo, avrà altrettanti valori quante sono le permutazioni di questo.

16.° Sia q l'ordine di una sostituzione ψ_0 del gruppo ; q, o sarà eguale al numero delle permutazioni del gruppo medesimo, e si avranno con essa tutte le permutazioni: o sarà minore di quel numero, e se ne avranno soltanto q, e vi saranno poi delle altre sostituzioni. Sia una di queste ψ_1 di ordine n; da ambedue si avranno qn permutazioni differenti ; poichè supponiamone due eguali

$$\psi_0^r \ \psi_1^s = \psi_0^{r'} \ \psi_1^{s'} :$$

moltiplicando a destra per $\psi_0^{-s'}$, a sinistra per ψ_0^{-r} ,

$$\psi_1^{s-s'} = \psi_0^{r-r'} ,$$

Prendiamo $(s - s')\,k \equiv 1 (\text{mod. } n)$, e inalziamo alla potenza k, si avrebbe

$$\psi_1 = \psi_0^{(r-r')k} ,$$

e quindi la sostituzione ψ_1 non sarebbe altro che una potenza di ψ_0, e non una nuova che potesse dare delle altre permutazioni. Se qn non è eguale al numero delle permutazioni del gruppo, si avrà anche un altra sostituzione ψ_2, colla quale si otterranno altre qn permutazioni, tutte differenti dalle precedenti : poichè supponiamo

$$\psi_0^r \; \psi_1^s = \psi_0^u \; \psi_2 ,$$

si avrebbe

$$\psi_2 = \psi_0^{r-u} \; \psi_1^s ,$$

ossia ψ_2 eguale a una delle precedenti sostituzioni, contro il supposto. Se con queste $q(n+1)$ permutazioni non sono esaurite tutte quelle del gruppo, le altre sostituzioni non potranno egualmente dare che un numero multiplo di q : dunque *l' ordine di una sostituzione qualunque di un gruppo è un divisore del numero delle permutazioni del gruppo.*

Se un gruppo avrà un numero primo di permutazioni, le sostituzioni del medesimo saranno tutte potenze di una sola di ordine p.

17.° Chiameremo *eguali* due gruppi quando tutte le sostituzioni di uno saranno eguali a quelle dell'altro, ancorchè differenti siano le permutazioni.

Se le sostituzioni saranno differenti, ma nello stesso numero e di ordini eguali, i gruppi conterranno anche uno stesso numero di permutazioni, e li diremo *simili.*

II.

DEI GRUPPI DERIVATI SIMILI.

18.° Siano $\theta_0 \; \theta_1 \; \theta_2 \ldots \theta_{p-1}$ tutte le sostituzioni di un gruppo G; $\psi_0 \; \psi_1 \ldots \psi_{n-1}$ quelle di un altro Γ. Un gruppo ottenuto

eseguendo sulle permutazioni di G una sostituzione ψ_m ha le sue sostituzioni derivate di quelle di G per mezzo di ψ_m, e perciò lo diremo *Gruppo derivato di* G *per mezzo di* ψ_m, e lo indicheremo colla notazione

$$\mathbf{D}_{\psi_m} \mathbf{G}$$

Poichè le sostituzioni derivate sono dello stesso ordine delle primitive (v. n.° 12), *i gruppi derivati saranno o simili, o eguali al primitivo o tra loro.*

I gruppi derivati di uno G per mezzo delle sostituzioni di un altro Γ si dicono *derivati di* G *per mezzo di* Γ, che dicesi *derivante.* Se sono simili e sommandoli si ha un gruppo, questo si chiamerà *gruppo della somma dei derivati di* G *per mezzo di* Γ.

19.° *Una sostituzione* φ *che converte una permutazione di un gruppo* G *in una di un suo derivato, cangia il primo gruppo intieramente nel secondo.*

Infatti, sia

$$\theta_m \varphi = \psi_r \mathbf{D}_{\psi_r} \theta_{m'} .$$

Moltiplichiamo per θ_q a sinistra, avremo

$$\theta_q \theta_m \varphi = \theta_q \psi_r \mathbf{D}_{\psi_r} \theta_{m'} = \psi_r \mathbf{D}_{\psi_r} \theta_q \theta_{m'}$$

Ora

$$\theta_q \theta_m = \theta_a , \qquad \theta_q \theta_{m'} = \theta_a \theta_m^{-1} \theta_{m'} = \theta_b :$$

onde

$$\theta_a \varphi = \psi_r \mathbf{D}_{\psi_r} \theta_b$$

Poichè q e quindi a possono esser qualunque, se ne deduce che tutte le permutazioni di un gruppo rimangono cangiate in quelle di un suo derivato, quando rimanga cangiata una sola di esse in una di quelle dell'altro, come volevamo dimostrare.

20.° Se tutti i gruppi derivati sono soltanto simili, tutte le sostituzioni del gruppo H che ne è somma, li permuteranno tra loro; e il gruppo K somma di queste permutazioni conterrà un numero di sostituzioni eguale al numero delle sostituzioni

di H, e tutte di ordini rispettivamente eguali a quelli di queste ultime, e perciò sarà simile a H.

Il gruppo K lo diremo *gruppo delle permutazioni sopra i derivati*, e potremo stabilire *che il gruppo delle permutazioni sopra i derivati è simile al gruppo della somma dei derivati, allorquando questi sono soltanto simili tra loro.*

III.

DEI GRUPPI DERIVATI EGUALI.

21.° Quando i gruppi derivati per mezzo di un gruppo Γ sono tutti eguali ma non identici tra loro, cioè quando hanno eguali le sostituzioni, ma non le permutazioni, e si ha

$$G = D_{\psi_0} G = D_{\psi_1} G = \ldots = D_{\psi_{n-1}} G ;$$

il gruppo *derivante* Γ delle sostituzioni $\psi_0 \psi_1 \ldots \psi_{n-1}$, prenderà il nome di *moltiplicatore* del gruppo primitivo G; e anche quello di *divisore* del gruppo H che risulta dalla somma di tutti i gruppi derivati.

Il gruppo H lo chiameremo il prodotto di G per Γ, e porremo

$$H = G\Gamma.$$

Se

$$\Gamma = G_1 \Gamma_1 , \quad \Gamma_1 = G_2 \Gamma_2 , \ldots \Gamma_{n-2} = G_{n-2} G_{n-1} ,$$

sarà

$$H = G G_1 G_2 \ldots G_{n-1} ;$$

e poichè l'ordine di questi fattori non è indifferente, distingueremo questi gruppi tra loro, chiamando G_{n-1} il 1.° divisore, G_{n-2}, il 2.° ..... G l' n^{simo}, ultimo divisore; e G_1 il primo, G_2 il 2.° .... G_{n-1} l'$(n-1)^{esimo}$ moltiplicatore di G.

Se non possono esistere altri moltiplicatori dopo Γ, si dirà questo *il massimo moltiplicatore di* G.

Un gruppo che non ammette nessun divisore lo diremo *primo*. Uno che non abbia nessun moltiplicatore *gruppo massimo*.

Poichè del gruppo H le sole sostituzioni che ha comuni con Γ permutano tra loro i derivati di G; si può stabilire che

il gruppo delle permutazioni sopra i derivati per mezzo di un moltiplicatore di essi è simile a questo moltiplicatore.

22.° *Il derivato del prodotto di più gruppi è eguale al prodotto dei derivati di ciascuno di essi presi nello stesso ordine.*

Sia

$$H = G\Gamma ,$$

e θ_m le sostituzioni di G, ψ_n quelle di Γ; avremo

$$D_{\psi_n}\ \theta_m = \theta_{m'} .$$

Deriviamo H per mezzo di φ; nel gruppo che si otterrà, alle θ_m corrisponderanno le $D_\varphi\ \theta_m$, alle ψ_n, le $D_\varphi\ \psi_n$. Ora si ha (v. n.° 11.)

$$D_\varphi \theta_m\ D_\varphi \psi_n = D_\varphi\ \theta_m\ \psi_n = D_\varphi \psi_n\ \theta_{m'} = D_\varphi \psi_n\ D_\varphi\ \theta_{m'} ;$$

onde

$$D_{D_\varphi \psi_n} D_\varphi\ \theta_m = D_\varphi\ \theta_{m'},$$

e il gruppo $D_\varphi H$ sarà il prodotto dei due derivati

$$D_\varphi G \quad \text{e} \quad D_\varphi \Gamma ;$$

$$D_\varphi G\Gamma = D_\varphi\ G\ D_\varphi \Gamma :$$

e in generale se

$$H = G\ G_1\ G_2 \ldots . G_{n-1} ;$$

$$D_\varphi\ H = D_\varphi\ G\ D_\varphi\ G_1\ D_\varphi\ G_2 \ldots D_\varphi\ G_{n-1} .$$

CAPITOLO TERZO

DELLA DETERMINAZIONE DEI MOLTIPLICATORI E DIVISORI DI UN GRUPPO.

I.

EQUAZIONI DEL MASSIMO MOLTIPLICATORE E DEI DIVISORI DI UN GRUPPO.

23.° Dato un gruppo, possono esser proposti due problemi; determinarne, 1.° i gruppi moltiplicatori, 2.° i divisori.

La soluzione di ambedue questi problemi richiede prima la determinazione di una funzione θ degli apici che dia tutte le sostituzioni del gruppo per i differenti valori che prendono le costanti o parametri che entrano nella medesima.

1. Per la determinazione dei moltiplicatori osserviamo che, indicando con ψ le loro sostituzioni, e con θ quelle del gruppo dato H, dovranno i derivati per mezzo delle ψ essere eguali tra loro, e quindi le sostituzioni derivate delle θ per mezzo di ψ eguali ad altre delle medesime θ; onde deve aversi la equazione

$$(13) \qquad D_\psi \, \theta_n = \theta_m ;$$

dove essendo θ_n una sostituzione del gruppo dato, θ_m ne è un altra le costanti della quale sono dipendenti da quelle di θ_n. Questa equazione corrisponde all'altra

$$(14)' \qquad \psi[\theta_n (i)] = \theta_m [\psi(i)].$$

Il valore di ψ che è l'integrale più generale di questa conterrà tutti i valori che sodisfano la (14), e quindi tutte le sostituzioni del massimo moltiplicatore del gruppo proposto.

2. Passiamo ora alla decomposizione di un gruppo nei suoi successivi divisori primi.

Siano

$$(a) \qquad \theta_{a_0} \; \theta_{a_1} \; \theta_{a_2} \; \ldots \; \theta_{a_{\nu-2}} ,$$

le sostituzioni di un gruppo G,

$$(b) \qquad \theta_{b_0} \; \theta_{b_1} \; \theta_{b_2} \; \ldots \; \theta_{b_{\mu-2}} ;$$

quelle di un altro Γ_n: affinchè un gruppo H sia il prodotto di questi, cioè

$$H = G\Gamma_n ,$$

sarà necessario e sufficiente che le (a) formino un gruppo effettivo, e che quindi soddisfacciano la equazione

$$(15) \qquad \theta_{a_n} \theta_{a_m} = \theta_{a_r}$$

(v. n.° 15.°); e che inoltre siano eguali i derivati di G per mezzo di Γ_n (v. n.° 21.°), cioè

$$(16) \qquad D_{\theta_b}\, \theta_{a_n} = \theta_{a_m} ,$$

$$(17) \qquad \theta_b\, [\theta_{a_n}(i)] = \theta_{a_m} [\theta_b\, (i)] .$$

Le sostituzioni di Γ_n che sono il prodotto di una medesima sostituzione per due differenti delle (a), danno dei derivati non solo eguali, ma anche identici, cioè colle stesse permutazioni, e quindi esse dovranno ritenersi eguali tra loro nel gruppo Γ_n; il grado del quale sarà dato perciò dal numero di quelle sostituzioni soltanto che permutano effettivamente tra loro i derivati, e che perciò non hanno per fattore nessuna delle (a), e potranno anche non formare un vero gruppo. Con questa considerazione riman *sempre* vero il teorema del num.° 21, e inoltre si può stabilire che *il prodotto dei gradi dei divisori di un gruppo è eguale al grado del gruppo stesso.*

I valori più generali che soddisfanno le equazioni (15) e (17) danno le sostituzioni del secondo divisore G, sul quale operando come sopra H, se ne potrà ottenere un terzo G_1, e così seguitando si giungerà finalmente a un ultimo divisore primo Γ_1.

Le sostituzioni dell'ultimo gruppo G_{n-2} di cui è divisore Γ_1, private dei fattori eguali a qualcuna delle sostituzioni di Γ_1, daranno un primo moltiplicatore Γ_2, quelle di G_{n-3}, tolti da essi fattori eguali a alcuna di quelle di G_{n-2}, daranno un secondo moltiplicatore Γ_3, e così di seguito avremo tutti i moltiplicatori fino all' ultimo Γ_n', e sarà

$$H = \Gamma_1\ \Gamma_2\ \Gamma_3 \ldots \Gamma_n .$$

Tutti questi divisori saranno primi, perchè altrimenti non si sarebbero presi per i valori che sodisfanno la (15) e la (17) tutti i possibili come abbiamo supposto.

Quando si trovassero una serie di valori (a) che soddisfacessero la (15) e non la (17), le sostituzioni che essi rappre-

senterebbero, darebbero tanti gruppi derivati simili, quante fossero quelle di H non comprese nelle (a). La decomposizione di un gruppo nei suoi divisori primi corrisponde a quella che *Galois* chiamava *decomposizione propria*. La determinazione di più derivati simili dei quali un gruppo dato sia la somma, corrisponde alla decomposizione che egli chiamava *impropria*.

Nella ricerca dei moltiplicatori di un gruppo distingueremo tre casi: 1.° quello nel quale il numero delle lettere è primo: 2.° quando è il prodotto di numeri primi differenti tra loro: 3.° quando è una potenza di un numero primo.

II.

MASSIMO MOLTIPLICATORE DEI GRUPPI DI UN NUMERO PRIMO DI PERMUTAZIONI SOPRA UN NUMERO EGUALE DI LETTERE.

24.° Sia p il numero primo delle lettere, e delle permutazioni del gruppo. Le sostituzioni del gruppo saranno tutte le potenze differenti di una sola di ordine p (v. n. 16), circolare sopra tutte le lettere (v. n. 7. 4), la quale disponendo convenientemente gli apici numerici i della prima permutazione, sarà

$$\varphi(i) = i + 1.$$

La equazione (14) da integrarsi per avere il massimo moltiplicatore diverrà

$$\psi(i + 1) = \psi(i) + a\ ,$$

la quale ha per integrale generale

$$\psi(i) = ai + b = a(i + c) = a\ [\ \varphi(i)\ ]^c\ ,$$

dove $ac \equiv b$.

Le potenze di $\varphi(i)$ essendo poi sostituzioni del gruppo primitivo, tutte le sostituzioni del massimo moltiplicatore saranno date da

$$\psi(i) = ai\ :$$

ed essendo λ una radice primitiva di p, e ponendo

$$\theta(i) = \lambda i\ ;$$

tutte saranno potenze di $\theta(i)$: dunque *le sostituzioni del massimo moltiplicatore di un gruppo di un numero primo di permutazioni sopra un numero primo di lettere, e che perciò ha per sostituzioni le potenze di* $\binom{i}{i+1}$ *soltanto, sono tutte potenze della unica*

$$\binom{i}{\lambda i};$$

e quindi *il gruppo le cui sostituzioni sono tutte comprese nella notazione*

$$\binom{i}{ai+b}$$

è un massimo.

III.

MASSIMO MOLTIPLICATORE DI UN GRUPPO DI UN NUMERO PRIMO DI PERMUTAZIONI SOPRA UN NUMERO DI LETTERE CHE HA DEI FATTORI PRIMI DIFFERENTI TRA LORO.

25.° Sia primo il numero p delle permutazioni di un gruppo G, e il numero m delle lettere che entrano nelle medesime, sia il prodotto di più fattori primi differenti tra loro. Avremo che tutte le sostituzioni di G saranno potenze di una sola di ordine p (V. num. 16) che risulterà dal prodotto di q circolari , ciascuna sopra un sistema di p lettere differenti (v. n.° 7. 5) Distinguiamo tra loro con un primo apice k le lettere di un sistema, con un secondo h indichiamo il sistema al quale appartengono. Il simbolo

$$\binom{x_{k,\,h}}{x_{k+a,\,h}}$$

comprenderà tutte le sostituzioni di G.

Un primo moltiplicatore, per ciò che si è detto precedentemente (v. n.° 24) sarà un gruppo Γ le sostituzioni del quale sono potenze di

$$\binom{x_{k,\,h}}{x_{\lambda k,\,h}}.$$

Moltiplicatore del gruppo GΓ, che ne risulta, sarà ogni gruppo H che non abbia altre sostituzioni che sui sistemi; cioè comprese nella notazione

$$\begin{pmatrix} x_{k\,,\,h} \\ x_{k\,,\,\varphi(h)} \end{pmatrix};$$

perchè evidentemente queste non cangiano le permutazioni delle lettere di ogni sistema in particolare.

26.° Un gruppo $L = KH$, dove K non abbia altre sostituzioni che sopra gl'indici k, H sopra gli h, lo diremo *a lettere congiunte*, e *lettere congiunte* quelle che hanno uno stesso indice h. Tra le sostituzioni di K ve ne potranno essere anche alcune che permutino soltanto gl'indici k di uno, o di alcuni sistemi; come pure alcune che permutino quelli di un sistema in un modo, e quelli di un altro in un modo differente. Ma vi dovranno essere insieme tutte le derivate differenti di queste sostituzioni, per mezzo di un altra qualunque sopra gl'indici h soltanto.

Se non esiste alcun moltiplicatore del gruppo, che dia un prodotto a lettere congiunte, L sarà un gruppo *massimo*, a meno, che il numero delle lettere che entrano nelle permutazioni non abbia tutti eguali tra loro i suoi fattori primi come passiamo a dimostrare.

Supponiamo che sia un moltiplicatore di L il gruppo Γ di ν permutazioni. Le sostituzioni $\psi_0\ \psi_1 \ldots \psi_{\nu-2}$ di esso non potranno essere nè sugl'indici h, nè sui k soltanto, perchè altrimenti L non sarebbe il massimo gruppo a lettere congiunte, come abbiamo supposto.

Le lettere che in un gruppo derivato $D_{\psi_n} L$ corrispondono a quelle di ciascuno dei diversi sistemi di lettere congiunte nel primitivo L, formeranno altrettanti nuovi sistemi di lettere congiunte nel derivato, e poichè i gruppi L e $D_{\psi_n} L$ sono eguali, le lettere congiunte nell'uno sono congiunte anche nell' altro, e quindi nel gruppo L le m lettere si potranno disporre almeno in ν differenti modi in q sistemi di p lettere congiunte ciascuno.

Fra questi modi ve ne sarà sempre uno tale, che faccia appartenere due lettere qualunque per es. x_a, x_b, allo stesso sistema.

Infatti tutte le lettere che fanno parte dei sistemi che contengono la lettera x_a non potranno esser differenti da tutte quelle dei sistemi che contengono x_b; perchè altrimenti tanto quelle che queste farebbero un sistema di lettere congiunte nel gruppo LΓ, contro il supposto. Sia per tanto x_c una lettera che fa parte di un sistema con x_a e di uno con x_b. Nel gruppo L non vi saranno sostituzioni che cangiano x_c in una lettera di un sistema qualunque, e che non permutino contemporaneamente x_a e x_b in due altre del medesimo; dunque x_a e x_b faranno parte di uno stesso sistema, *c. v. d.*

27.° Due lettere non possono far parte altro che di un solo sistema di lettere congiunte. È chiaro se $p=2$. Se $p>2$, supponiamo che x_a e x_b facciano parte di due sistemi differenti in tutte le altre lettere. Nel gruppo L, in questo caso, non vi sarebbe sostituzione che permutasse x_a senza permutare anche x_b, e viceversa: poichè anche cangiando x_a in una x_c a lei congiunta, x_a formando parte con x_b anche di un altro sistema che non contiene x_c, dovrebbero tutte le lettere di questo ultimo rimaner cangiate in quelle del primo, e qnindi anche la x_b. Quelle lettere poi nelle quali rimarrebbero cangiate x_a e x_b, verrebbero a far parte di due sistemi, e sarebbero nello stesso caso; e così di seguito. Dunque L sarebbe un gruppo a lettere congiunte, i sistemi del quale sarebbero di due lettere, contro il supposto.

Ugualmente si dimostrerebbe lo stesso per un numero di lettere >2 e $<p$. Dunque *i sistemi differenti di lettere congiunte avranno una sola lettera eguale.*

28.° Disposte le lettere in un modo qualunque in sistemi congiunti, sarà sempre possibile anche un altra disposizione (v. n.° 26), nella quale un sistema non potrà contenere che una lettera di ciascuno dei primi (v. n.° 27); dunque, le lettere di ogni sistema essendo p, i sistemi saranno almeno p, e le lettere p^2. Siano le seguenti linee orizzontali i primi p sistemi

di lettere congiunte, e quello formato da una di ciascuno di essi sia la prima linea verticale

$$(A)\quad \begin{cases} x_{0,0} \quad x_{1,0} \quad x_{2,0} \ldots\ldots x_{p-1,0} \\ x_{0,1} \quad x_{1,1} \quad x_{2,1} \ldots\ldots x_{p-1,1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_{0,p-1} \; x_{1,p-1} \; x_{2,p-1} \; \ldots\ldots x_{p-1,p-1} \; ; \end{cases}$$

e poichè nei sistemi di lettere congiunte non si possono mutare alcune di uno in alcune di un altro senza mutarle tutte quante; le sostituzioni sulle lettere di una linea orizzontale, o lasceranno ferma la prima linea verticale, o ne convertiranno tutte quante le lettere in altre corrispondenti rispettivamente alla stessa linea orizzontale, e congiunte tra loro : le quali potremo supporre essere quelle di una delle altre linee verticali: poichè la prima permutazione è arbitraria. In conseguenza nel quadro (A) saranno linee congiunte tanto quelle situate in una stessa linea orizzontale, quanto quelle della medesima verticale.

Ora osserviamo che le sostituzioni del gruppo L non possono lasciare una linea verticale ferma, e permutar le altre; perchè altrimenti contro ciò che abbiamo dimostrato al n.° 26, due lettere di due sistemi verticali non potrebbero esser congiunte; lo stesso può dirsi delle orizzontali ; dunque tutte le sostituzioni di L non potranno essere che le circolari comprese nella notazione

$$\begin{pmatrix} x_{k,\,h} \\ x_{k+a,\,h+b} \end{pmatrix} ;$$

e saranno congiunte anche tutte le lettere che si trovano sulla stessa diagonale.

Se le lettere sono in numero maggiore di p^2, a quelli del quadro (A) andranno aggiunti altri sistemi; e sarà possibile un' altra disposizione in sistemi di lettere congiunte, in ciascuno dei quali entri una sola delle lettere del quadro A (ved. num. 26, 27); dunque per ciascuna delle p^2 lettere ve ne saranno

altre $p-1$; onde le lettere saranno almeno p^3. E poichè non si può permutare una lettera del quadro (A) in una che non si trovi in esso, senza convertirle tutte quante in altre egualmente congiunte; le p^3 lettere si potranno disporre in p sistemi di lettere congiunte simili ad (A).

Distinguiamo con un terzo apice l le lettere di questi sistemi: poichè non si può tener fermo nessuno di questi sistemi permutandone alcuni tra loro, anche rispetto all'apice l saranno in L le sostituzioni tutte circolari; e quindi tutte quante comprese nel simbolo

$$\begin{pmatrix} x_{k\,,\,h,\,l} \\ x_{k+a,\,h+b,\,l+c} \end{pmatrix}.$$

Generalizzando si può finalmente stabilire il seguente Teorema:

Affinchè un gruppo a lettere congiunte ammetta un moltiplicatore per il quale moltiplicato, il prodotto non sia a lettere congiunte, è necessario che il numero delle lettere sia la potenza di un numero primo, e che esso non contenga altre sostituzioni che quelle comprese nel simbolo

$$\begin{pmatrix} x_{k\,,\,h\,,\,l\,,\cdots} \\ x_{k+a\,,\,h+b\,,\,l+c\,,\,\cdots\cdots} \end{pmatrix}.$$

Un gruppo di permutazioni di un numero di lettere che ammette dei fattori primi differenti tra loro, non può aver per divisore nessun gruppo a lettere congiunte, a meno che non sia a lettere congiunte esso stesso.

IV.

MASSIMO MOLTIPLICATORE DI UN GRUPPO DI UN NUMERO PRIMO DI PERMUTAZIONI SOPRA UN NUMERO DI LETTERE CHE È POTENZA DI UN NUMERO PRIMO

29.° Sia p^ν il numero delle lettere, p numero primo e ν qualunque. Il gruppo di p permutazioni sarà a lettere congiunte, e un divisore di quello, le sostituzioni del quale sono comprese tutte nella notazione

$$(a) \qquad \begin{pmatrix} x_k , h , l , m \cdots \\ x_{k+a} , h+b , l+c , m+d , \ldots\ldots \end{pmatrix}$$

Determineremo perciò il massimo moltiplicatore di questo ultimo gruppo.

Adottiamo per apici delle lettere, come abbiam detto in principio, le p radici della congruenza

$$(b) \qquad k^{p^\nu} \equiv k (\text{mod. } p) ;$$

le quali sappiamo essere espresse da

$$k = a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1} ;$$

dove i è radice incommensurabile della congruenza di grado ν, irriduttibile

$$(c) \qquad F(i) \equiv 0 \ (\text{mod. } p) .$$

I coefficienti della i corrisponderanno agli apici k, l, m, n,..., onde le sostituzioni (a) saranno tutte date da

$$\left\{ \begin{matrix} x \\ x \end{matrix} \right. \left. \begin{matrix} a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1} \\ a_0 + a + (a_1 + b) i + (a_2 + c) i^2 + \ldots + (a_{\nu-1} + g) i^{\nu-1} \end{matrix} \right\}$$

o anche, poichè $a + bi + ci^2 + \ldots\ldots + gi^{\nu-1}$ è una radice k_0 della (b), queste sostituzioni possono rappresentarsi con

$$(d) \qquad \begin{pmatrix} x_k \\ x_{k+k_0} \end{pmatrix} ,$$

dove k_0 può avere per valori tutte le radici della (b). Onde le permutazioni che con esse si ottengono saranno p^ν; e, poichè $pk_0 \equiv 0$, tutte quelle sostituzioni saranno di ordine p.

Sia $\psi(k)$ una sostituzione del moltiplicatore Γ del gruppo G che nasce dalle sostituzioni (d); dovrà aversi (v. n.° 23°.)

$$(e) \qquad \psi(k + k_0) \equiv \psi(k) + h_0$$

dove h_0 è pure una radice della (b) dipendente da k_0.

L'integrale più generale della congruenza (e) alle differenze finite è

$$\psi(k) \equiv \sum_{n=0}^{n=\nu-1} B_n k^{p^n} + B_\nu ;$$

dove i B_n sono radici della (b) tali che

$$\sum_{n=0}^{n=\nu-1} B_n k_0^{p^n} \equiv h_0 .$$

È facile verificare questo integrale ponendo mente alla proprietà, della quale godono questa specie di quantità, che cioè

$$(k + k_0)^{p^n} \equiv k^{p^n} + k_0^{p^n} .$$

Poichè le sostituzioni

$$\begin{pmatrix} x_k \\ x_{k+B_\nu} \end{pmatrix}$$

appartengono tutte al gruppo G; tutte le sostituzioni del massimo moltiplicatore Γ saranno soltanto quelle comprese nel simbolo

$$(f) \qquad \left\{ \begin{matrix} x_k \\ x_{\sum_{n=0}^{n=\nu-1} B_n k^{p^n}} \end{matrix} \right\}$$

Esprimendo le B_n e k in funzione di i, è facile ottenere la (7) sotto la forma

$$(f') \left\{ \begin{matrix} x_{a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1}} \\ x_{m_0 a_0 + m_1 a_1 + \ldots + m_{\nu-1} a_{\nu-1} + (m'_0 a_0 + m'_1 a_1 + \ldots + m'_{\nu-1} a_{\nu-1}) i + \ldots} \\ \qquad + (m_0^{(n-1)} a_0 + m_1^{(\nu-1)} a_1 + \ldots + m_{\nu-1}^{(\nu-1)} a_{\nu-1}) i^{\nu-1} \end{matrix} \right\}$$

dove tutte le a e le m sono numeri interi eguali o maggiori di zero, e $< p$.

Per qualunque valore dei B_n non si hanno sempre sostituzioni. Poichè tutte le permutazioni non devono contenere

che una sola volta una medesima lettera, sarà necessario che i B_n siano tali che la congruenza

$$\sum_{n=0}^{n=\nu-1} B_n k^{p^n} \equiv k_0$$

non abbia che una sola radice comune colla (b) qualunque sia k_0.

30.° Tutte le sostituzioni (f) di Γ lasciano ferma la x_0; ed esso è un gruppo a lettere congiunte rispetto alle altre $p^\nu - 1$. Infatti se

$$\sum_{n=0}^{n=\nu-1} B_n k_0^{p^n} \equiv k_1 ,$$

anche

$$\sum_{n=0}^{n=\nu-1} B_n (ak_0)^{p^n} \equiv ak_1$$

dove a è un intero qualunque $< p$; poichè

$$a^{p^n} \equiv a ;$$

dunque nel gruppo massimo moltiplicatore le $p^\nu - 1$ lettere che hanno per indici le radici della congruenza

$$k^{p^\nu - 1} \equiv 1 \pmod{p},$$

si dividono in $\frac{p^\nu - 1}{p - 1}$ sistemi di $p-1$ lettere congiunte ciascuno, e queste sono precisamente quelle gli apici delle quali hanno un rapporto numerico.

31.° Il numero di lettere che può lasciar ferme una sostituzione (e) è sempre un divisore p^m di p^ν.

Sia x_{k_0} una lettera che rimanga ferma per una delle (f); si avrà

$$(g) \qquad \sum_{n=0}^{n=\nu-1} B_n k_0^{p^n} = k_0 ;$$

della quale saranno radici tutti gli apici dello stesso sistema di lettere congiunte, ak_0 : dunque se stà ferma una lettera ne staranno ferme almeno p.

Sia k_1 un'altra radice della (g) diversa dalle precedenti; ne saranno radici anche tutti i p^2 valori, che prende la espressione

$$ak_0 + bk_1 ,$$

ponendo in essa per a e per b tutti i numeri intieri $< p$. Questi p^2 valori saranno differenti, poichè altrimenti si avrebbe

$$ak_0 + bk_1 \equiv a_1 k_0 + b_1 k_1 \text{ (mod. } p),$$

ossia

$$(a - a_1)k_0 \equiv (b_1 - b)k_1.$$

Moltiplicando per un numero h tale, che

$$(b_1 - b)\, h \equiv 1,$$

si ha

$$k_1 \equiv (a - a_1)hk_0$$

contro il supposto: dunque se stanno ferme più di p lettere, ne staranno ferme almeno p^2.

Se sta ferma un altra lettera, sia l'apice di questa k_2, che sarà una radice della (g) differente dalle precedenti: e ne saranno radici tutte le p^3 comprese al solito nella espressione

$$ak_0 + bk_1 + ck_2 ;$$

e queste saranno tutte differenti; che altrimenti si avrebbe

$$ak_0 + bk_1 + ck_2 \equiv a_1 k_0 + b_1 k_1 + c_1 k_2 ;$$

ossia

$$(a - a_1)k_0 + (b - b_1)k_1 \equiv (c_1 - c)k_2 ;$$

e moltiplicando per il numero h che dà

$$(c_1 - c)\, h \equiv 1,$$

si ha

$$k_2 \equiv h(a - a_1)k_0 + h(b - b_1)k_1 ,$$

contro ciò che avevamo supposto: così seguitando si può stabilire, che le lettere che stanno ferme saranno sempre in numero p^m divisore di p^ν.

32.° Le ν lettere che hanno per apici $k_0\, k_1\, k_2 \ldots . k_\nu$ tali, che uno qualunque di essi non si può esprimere linearmente per gli altri, non possono esser lasciate ferme da nessuna sostituzione che non lasci ferme altresì tutte quante le lettere, cioè che non equivalga a nessuna operazione. Queste lettere possono essere una radice primitiva λ di p, e le potenze di una radice i della congruenza (c).

Per le sostituzioni potenze di

$$\begin{pmatrix} x_k \\ x_{k^p} \end{pmatrix}$$

non possono esser lasciate ferme che le p lettere

$$x_0\,,\ x_1\,,\ x_2 \ldots . x_{p-1}\,:$$

poichè i numeri intieri $< p$ sono le uniche radici della congruenza

$$k^p \equiv k \pmod{p}.$$

33.° Dal non esser contenute nel gruppo Γ le sostituzioni che lasciano ferme un numero di lettere differente da p^m, dove m é un intero qualunque minore di ν, si deduce che tutte le sostituzioni di Γ sono di ordine $p^\nu - p^m$, e che quindi (vedi n.° 16.) *il numero delle permutazioni del gruppo massimo che non è a lettere congiunte, e che ammette un divisore a lettere congiunte è eguale a* **M** *o a un divisore di* **M**, *essendo*

$$\mathbf{M} = p^\nu(p^\nu - 1)(p^\nu - p) \ldots . (p^\nu - p^{\nu-1}).$$

V.

DECOMPOSIZIONE DI UN GRUPPO NEI SUOI DIVISORI PRIMI.

34°. Abbiamo già osservato (v. n.° 23) che quando sia dato un gruppo, e si voglia decomporlo nei gruppi primi dei quali

è il prodotto, è necessario determinare prima la funzione $\theta(i)$ degl' indici, la quale dà per tutti i differenti valori dei suoi parametri, tutte le sostituzioni del gruppo; poi risolvere le equazioni (15) e (17). Quando non esistano valori dei parametri di θ, che le sodisfacciano, il gruppo è primo. La classificazione dei gruppi primi farà soggetto di un altro mio lavoro, se avrò agio a seguitare con risultato le ricerche intraprese. Ora mi contenterò di parlare dei gruppi di prima classe, dei quali solo abbisognano le applicazioni che fo nella seconda parte di questa Memoria.

Gruppi di *prima classe* diremo quelli che contengono un numero primo di permutazioni; e che perciò hanno tutte le loro sostituzioni potenze di una soltanto (v. n.° 16).

35.° *I gruppi le sostituzioni dei quali sono tutte quante potenze di una sola θ di ordine m, sono decomponibili in tanti gruppi di prima classe quanti sono i fattori primi di m, e che sono di grado rispettivamente eguale a questi fattori.*

Infatti, se $m = pn$, dove p è un fattore primo; la funzione che da tutte le sostituzioni del gruppo è θ^t. La equazione (17) diviene in questo caso

$$\theta^{a+b}(i) = \theta^{c+a}(i);$$

la quale è soddisfatta da

$$b = c,$$

qualunque sia a. La equazione (15) poi diviene

$$\theta^{b_m}\ \theta^{b_n} = \theta^{b_r};$$

che è sodisfatta da $b_i = pi$. L' ultimo divisore avrà dunque per sostituzioni

$$\theta^p\ \theta^{2p}\ \theta^{3p}\ \ldots\ \theta^{p(n-1)}$$

e per l'altro rimarranno

$$\theta,\ \theta^2\ \theta^3\ \ldots\ \theta^{p-1}.$$

Questo è di prima classe e di grado p, e quello è pure di prima classe se n è primo, altrimenti è decomponibile nuo-

vamente in uno di prima classe e in un altro che è di prima classe, oppure decomponibile, e così di seguito.

36.° *Un gruppo di grado pq, le permutazioni del quale si ottengono tutte con due sostituzioni una di ordine p l'altra di ordine q, è sempre il prodotto di due gruppi di prima classe, o prodotti di gruppi di prima classe, e se $p > q$ il primo divisore è di grado q^{simo}, il secondo di grado p^{simo}.*

Se θ è la sostituzione di ordine p, ψ quella di ordine q, è evidente che tutte le permutazioni si otterranno eseguendo sopra una sola le sostituzioni

$$\theta^m \ \psi^n$$

prendendo per m tutti i valori da 0 a $p-1$ inclusivamente, e per n da 0 a $q-1$.

Se si eseguissero invece prima tutte le sostituzioni

$$\theta^m \psi,$$

e poi su queste nuovamente tutte le potenze di θ, si avrebbero p^2 permutazioni, cioè un numero $> pq$, e in conseguenza alcune dovrebbero esser eguali, e quindi si avrebbero alcuni valori a, a', b e b' per i quali

$$\theta^a \psi \theta^{a'} = \theta^b \psi \theta^{b'},$$

o anche

$$\theta^{a-b} \psi = \psi \theta^{b'-a'};$$

ed essendo h dato dalla congruenza

$$h(a-b) \equiv 1 (\text{mod. } p),$$

risulterebbe

$$\theta\psi = \psi\theta^{h(b'-a')} = \psi\theta^k,$$

posto

$$k = h(b'-a');$$

e quindi

$$D_\psi \theta = \theta^k:$$

dalla quale si ha qualunque sia m (v. n.° 11)

$$D_\psi \theta^m = \theta^{mk};$$

onde chiamando G il gruppo delle θ

$$D_\psi G = G:$$

e detto Γ il gruppo delle ψ, sarà il proposto eguale al prodotto $G\Gamma$, come volevamo dimostrare.

Le sostituzioni di un gruppo pq, quando p e q siano primi, sono di ordine p o di ordine q (v. n.° 16): *dunque ogni gruppo il grado del quale è il prodotto di due numeri primi differenti non è mai primo.*

37.° È evidente una prima decomposizione dei gruppi a lettere congiunte in due, uno dei quali contenga tutte le sostituzioni sulle lettere congiunte, e l'altro quelle sui sistemi delle medesime; e per avere i gruppi primi, in questo caso basta determinare i divisori primi di questi due

38.° Il massimo moltiplicatore Γ del gruppo a lettere congiunte (d) nel caso che le lettere siano la potenza di un numero primo p^ν è sempre decomponibile in più gruppi primi, ma che in generale non sono tutti di prima classe.

Le sostituzioni di questo moltiplicatore sono tutte date dalla funzione

$$\theta(k) = \sum_{n=0}^{n=\nu-1} B_n k^{p^n};$$

o anche da

$$\theta(a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1})$$

$$= \sum_{n=0}^{n=\nu-1} \left(m_0^{(n)} a_0 + m_1^{(n)} a_1 + m_2^{(n)} a_2 + \ldots + m_{\nu-1}^{(n)} a_{\nu-1} \right) i^n$$

(v. n.° 29). Ora gl'indici che hanno un rapporto numerico appartengono a lettere congiunte (v. n.° 30); onde queste si potranno distinguer con un indice eguale al numero che esprime il rapporto che hanno, a una qualunque tra loro, che sarà intiero e $< p$, ritenendo al solito eguali a zero i multipli di p; i sistemi poi ai quali esse appartengono si potranno contrassegnare con un indice funzione del primitivo, che rimanga

lo stesso moltiplicando questo per un fattore numerico. Ciò si ottiene ponendo

$$x_{a_0 + a_1 i + \ldots a_{\nu-1} i^{\nu-1}} = x_{a_0,\ \frac{a_1}{a_0} i + \frac{a_2}{a_0} i^2 + \cdots + \frac{a_{\nu-1}}{a_0} i^{\nu-1}},$$

e meglio

$$x_{a_0 + a_1 i + \ldots a_{\nu-1} i^{\nu-1}} = x_{t,\ k_1 i + k_2 i^2 + \ldots + k_{\nu-1} i^{\nu-1}};$$

dove $k_n = \frac{a_n}{a_0}$ dovrà prendere i $p + 1$ valori $0, 1, 2, \ldots p - 1, \frac{1}{0}$; t poi prenderà i soli $1, 2, 3 \ldots p - 1$.

Questa mutazione d'indici trasforma la (f') nella seguente

$$(h)\left\{\begin{array}{l} x_{t,\ k_0 i + k_1 i^2 + \ldots + k_{\nu-1} i^{\nu-1}} \\ x_{\lambda t, \sum_{n=1}^{n=\nu-1} \frac{\left(m_0^{(n)} + m_1^{(n)} k_1 + m_2^{(n)} k_2 + \ldots + m_{\nu-1}^{(n)} k_{\nu-1} \right) i^n}{m_0 + m_1 k_1 + m_2 k_2 + \ldots + m_{\nu-1} k_{\nu-1}}} \end{array}\right\}$$

Chiamiamo *determinante della sostituzione* (h), e indichiamo con D, la determinante del sistema dei ν^2 num eri intieri

$$\begin{array}{l} m_0\ m_1\ m_2 \ldots . m_{\nu-1} \\ m'_0\ m'_1\ m'_2 \ldots . m'_{\nu-1} \\ m''_0\ m''_1\ m''_2 \ldots . m''_{\nu-1} \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ m_0^{(\nu-1)}\ m_1^{(\nu-1)}\ m_2^{(\nu-1)} \ldots m_{\nu-1}^{(\nu-1)}. \end{array}$$

Per moltiplicare la sostituzione (h) per un altra (h'), la determinante D' della quale sia quella del sistema

$$\begin{array}{l} n_0\ n_1\ n_2\ \ldots\ n_{\nu-1} \\ n'_0\ n'_1\ n'_2\ \ldots\ n'_{\nu-1} \\ n''_0\ n''_1\ n''_2\ \ldots\ n''_{\nu-1} \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ n_0^{(\nu-1)}\ n_1^{(\nu-1)}\ n_2^{(\nu-1)}\ \ldots\ n_{\nu-1}^{(\nu-1)} \end{array}$$

basta porre in luogo di $k_1\ k_2\ \ldots\ k_{\nu-1}$ nella (h') i coefficienti delle corrispondenti potenze d'i della (h). Quindi dal noto teorema della moltiplicazione delle determinanti è facile dedurre che, se si chiama Δ la determinante del prodotto delle due sostituzioni (h) e (h'), avremo

$$(i) \qquad \Delta = DD';$$

cioè, *la determinante del prodotto di due sostituzioni è eguale al prodotto delle loro determinanti.*

Siano

$$(a) \qquad \theta_{a_0}\ \theta_{a_1}\ \theta_{a_2}\ \ldots\ \theta_{a_M}$$

tutte quante le sostituzioni comprese nella notazione (h), la determinante delle quali è residuo quadratico di p. Poichè il prodotto di due residui è residuo, esse sodisfaranno la (15) del n.° 23, e formeranno un gruppo L. Se s'indica poi con θ_b una sostituzione qualunque compresa nella (h), la determinante della quale è non residuo quadratico di p, avremo sodisfatta la (17) del n.° 23, che diviene

$$\theta_{a_n}\ \theta_b = \theta_b\ \theta_{a_m};$$

perchè, il primo prodotto avendo la determinante non residuo, dovrà averla non residuo anche il secondo, ed essendo non

residuo la determinante di θ_b, dovrà esser residuo quella di θ_{a_m}. Dunque se si chiama G_2 il gruppo delle θ_b avremo

$$\Gamma = LG_2 .$$

Ma tutte le sostituzioni a determinante non residuo si ottengono facendo il prodotto di una sola e medesima a determinante non residuo con tutte quelle a determinante residuo; dunque G_2 è di 2° grado (v. n.° 23).

Ora se indichiamo con G il gruppo che si ottiene colle $p-1$ potenze della sostituzione

$$\left\{ \begin{array}{c} x_{t,\ k_1 i + k_2 i^2 + \ldots k_{\nu-1} i^{\nu-1}} \\ \\ x_{\lambda t,\ k_1 i + k_2 i^2 + \ldots k_{\nu-1} i^{\nu-1}} \end{array} \right\}$$

nella quale λ è una radice primitiva di p; e con G_1 il gruppo di tutte le sostituzioni che rimangono del gruppo L, tolti dalle medesime i fattori eguali a qualcuna delle sostituzioni di G, che saranno perciò

$$\left\{ \begin{array}{l} x_{t,\ k_1 i + k_2 i + \cdots + k_{\nu-1} i^{\nu-1}} \\ \\ x_{t,\ \sum \frac{m_1^{(n)} + m_1^{(n)} k_1 + \ldots + m_{\nu-1}^{(n)} k_{\nu-1}}{m_0 + m_1 k_1 + \ldots + m_{\nu-1} k_{\nu-1}} i^n} \end{array} \right\};$$

è evidente che si avrà

$$L = GG_1 ,$$

$$\Gamma = GG_1G_2 .$$

G è di grado $(p-1)^{simo}$ e decomponibile in gruppi di prima classe, G_2 di 2° grado, G_1 sarà di grado

$$\frac{(p^\nu - 1)(p^\nu - p)(p^\nu - p^2) \ldots (p^\nu - p^{\nu-1})}{2(p-1)} ;$$

Onde Γ sarà decomponibile in gruppi di prima classe soltanto quando lo sarà G_1.

Questo avviene quando

1.° $p = 2$, $\nu = 2$:

2.° $p = 3$, $\nu = 2$:

nel 1.° caso G_1 essendo di 3° grado, e quindi primo, nel 2° essendo un gruppo di 24 permutazioni su 4 lettere, che è decomponibile sempre in gruppi di prima classe, come si vede nell'esempio che abbiamo sviluppato qui appresso.

39.° Quando un gruppo G ha le sostituzioni tutte comprese nel simbolo

$$(k) \qquad \left\{ \begin{matrix} x_k \\ x_{(Bk+C)^{p^n}} \end{matrix} \right\},$$

avremo sempre

$$G = \Gamma\, \Gamma_1\, \Gamma_2;$$

essendo le sostituzioni di Γ date da

$$\begin{pmatrix} x_k \\ x_{k+c} \end{pmatrix},$$

e quindi

$$\Gamma = G_1\, G_2\, G_3 \ldots, G_\nu,$$

indicando con G_t il gruppo le sostituzioni del quale sono le p differenti potenze di

$$\begin{pmatrix} x_k \\ x_{k+t} \end{pmatrix}.$$

Le sostituzioni di Γ_1 poi saranno le $p^\nu - 1$ potenze differenti di

$$\begin{pmatrix} x_k \\ x_{Bk} \end{pmatrix};$$

dove B è una radice primitiva della (b) : e quelle di Γ_2 le ν potenze di

$$\begin{pmatrix} x \\ x_{k^p} \end{pmatrix}$$

Dunque il gruppo G conterrà $p^{\nu}(p^{\nu}-1)\nu$ permutazioni (v. n.° 23), e sarà il prodotto di gruppi tutti di prima classe (vedi num. 35).

ESEMPIO

Per indicare che le sostituzioni di un gruppo sono comprese in un dato simbolo, stabiliremo l'eguaglianza della lettera che indica il gruppo, col simbolo stesso.

Se

$$i^2 + i + 1 \equiv 0 \pmod 2,$$

le radici della congruenza

$$k^{2^2} \equiv k \pmod 2$$

saranno

$$k_0 \equiv 0 \quad k_1 \equiv i \quad k_1^2 \equiv i+1 \qquad k_1^3 \equiv 1 .$$

Il gruppo H che comprende tutte le 24 permutazioni che si posson fare con 4 lettere, sarà sempre decomponibile in gruppi di prima classe ; poichè le sue sostituzioni possono ottenersi tutte dalla (k), e se

$$G = \begin{pmatrix} x_k \\ x_{k+k_1^3} \end{pmatrix}, \qquad G_1 = \begin{pmatrix} x_k \\ x_{k+k_1} \end{pmatrix}$$

$$G_2 = \begin{pmatrix} x_k \\ x_{k_1 k} \end{pmatrix}, \qquad G_3 = \begin{pmatrix} x_k \\ x_{k^2} \end{pmatrix}$$

sarà

$$H = GG_1G_2G_3 :$$

e avremo la seguente decomposizione, rappresentando le lettere cogli esponenti degl'indici, e con zero x_{k_0} ,

$$
\left.\begin{array}{l}
\left.\begin{array}{l}
(G)\left\{\begin{array}{l}0123\\3210\end{array}\right.^{(G_1)}\ (G)\left\{\begin{array}{l}1032\\2301\end{array}\right. \\
(G)\left\{\begin{array}{l}0231\\3102\end{array}\right.^{(G_1)}\ (G)\left\{\begin{array}{l}1320\\2013\end{array}\right. \\
(G)\left\{\begin{array}{l}0312\\3021\end{array}\right.^{(G_1)}\ (G)\left\{\begin{array}{l}1203\\2130\end{array}\right.
\end{array}\right\}(G_2) \\
\left.\begin{array}{l}
(G)\left\{\begin{array}{l}0213\\3120\end{array}\right.^{(G_1)}\ (G)\left\{\begin{array}{l}1302\\2031\end{array}\right. \\
(G)\left\{\begin{array}{l}0321\\3012\end{array}\right.^{(G_1)}\ (G)\left\{\begin{array}{l}1230\\2103\end{array}\right. \\
(G)\left\{\begin{array}{l}0132\\3201\end{array}\right.^{(G_1)}\ (G)\left\{\begin{array}{l}1023\\2310\end{array}\right.
\end{array}\right\}(G_2)
\end{array}\right\}(G_3)
$$

PARTE SECONDA

CAPITOLO PRIMO

DELLE CONDIZIONI GENERALI DI RISOLUBILITA' DELLE EQUAZIONI ALGEBRICHE PER RADICI DI EQUAZIONI AUSILIARIE.

I.

DELLA RISOLVENTE DI GALOIS.

1.° È noto che una funzione razionale delle radici di una equazione irriduttibile di grado μ

$$(1) \qquad f(x) = 0,$$

la quale prende, per qualunque sostituzione eseguita sulle radici, valori tutti differenti tra loro, gode la proprietà che le μ radici della (1) possono essere espresse razionalmente in funzione della medesima (*).

Siano

$$V = F(x_0 , x_1 , x_2 \ldots . x_{\mu-1})$$

questa funzione, e

$$(2) \qquad V_0 \; V_1 \; V_2 \ldots V_{M-1}$$

gli M valori che essa prende per tutte le diverse permutazioni delle radici: sarà

$$M = 1.2.3. \ldots \mu - 1 . \mu,$$

e potranno esprimersi tutti i valori (2) in funzione razionale di uno qualunque tra loro (**).

2.° Sia

$$(3) \qquad \Theta (V) = 0$$

la equazione di grado M che ha per radici i valori (2), e che perciò avrà i coefficienti funzioni simmetriche delle radici , e quindi razionali dei coefficienti della (1). Questa equazione la quale ha alcune proprietà scoperte da Galois, che fanno il fondamento della presente Teoria, la chiameremo ad onore di questo profondo geometra la *risolvente di Galois.*

Indicheremo con

$$\varphi_0(V) , \; \varphi_1(V) , \; \varphi_2(V) \ldots . \varphi_{\mu-1}(V)$$

le μ funzioni razionali di un valore qualunque di V, che danno le radici della (1).

3.° La Risolvente di Galois in generale sarà irriduttibile , ma potrà decomporsi in fattori irrazionali, cioè in fattori che contengono delle radici di equazioni algebriche ausiliarie. Queste radici, quando si stabilisca d'introdurle nel calcolo , come

---

(*) Vedi Serret. Cours. d'Alg. sup. pag. 149.

(**) V. Ivi, pag. 152.

quantità conosciute, si diranno quantità *aggiunte*, e *razionale* si chiamerà ogni funzione che sia tale dei coefficienti della proposta e delle quantità aggiunte; e *riduttibile* o *irriduttibile* una equazione secondo che può o non può decomporsi in fattori, i coefficienti dei quali siano razionali.

Siano aggiunte tali radici di equazioni ausiliarie che rendano la (3) riduttibile; $\psi(V)$ sia uno dei fattori razionali della medesima di grado ν, e

$$(4) \qquad V_0 , V_1 , V_2 \ldots . V_{\nu-1}$$

le radici di

$$(5) \qquad \psi(V) = 0 .$$

Potremo prendere per radici della (1) quelle date da una qualunque delle seguenti linee orizzontali, che formano ν differenti permutazioni delle medesime :

$$(A) \quad \left\{ \begin{array}{l} \varphi_0(V_0) , \varphi_1(V_0) , \varphi_2(V_0) \ldots . \varphi_{\mu-1}(V_0) \\ \varphi_0(V_1) , \varphi_1(V_1) , \varphi_2(V_1) \ldots . \varphi_{\mu-1}(V_1) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \varphi_0(V_{\nu-1}) , \varphi_1(V_{\nu-1}) , \varphi_2(V_{\nu-1}) \ldots . \varphi_{\mu-1}(V_{\nu-1}) \end{array} \right.$$

4.° Per eseguire una sostituzione che converta la n^{esima} delle permutazioni (A) in un altra m^{esima}, è necessario e sufficiente il cangiamento di uno dei valori (4) V_n in un altro dei medesimi V_m.

Ora sappiamo che

$$V_m = \lambda(V_n) ,$$

indicando con λ una funzione razionale; e poichè la (5) è irriduttibile saranno altrettanti valori (4) i seguenti (*)

$$(6) \qquad V_n , \lambda(V_n) , \lambda^2(V_n) \ldots . \lambda^{p-1}(V_n) ,$$

essendo p il più piccol numero per cui

(*) Vedi Serret Cours d'Alg. Sup. pag. 345.

$$\lambda^p(V_n) = V_n :$$

e se la serie dei valori (6) non esaurisce la (4), saranno $\mu(V_n)$, $\mu_1(V_n)$, $\mu_2(V_n)$ . . . altre funzioni razionali che daranno altrettante radici,

$$(7)\quad \begin{cases} \mu(V_n)\ ,\ \ \mu\lambda(V_n)\ ,\ \ \mu\lambda^2(V_n) \ldots . \mu\lambda^{p-1}(V_n) \\ \mu_1(V_n)\ ,\ \mu_1\lambda(V_n)\ ,\ \mu_1\lambda^2(V_n) \ldots . \mu_1\lambda^{p-1}(V_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Ora cangiando V_n in V_m, ossia V_n in $\lambda(V_n)$, si permutano circolarmente in tutti i loro termini ciascuna delle linee orizzontali di valori (6) e (7), ossia si permutano tra loro tutti i valori (4): dunque eseguendo su tutte le (A) una sostituzione qualunque che faccia passare da una ad un altra delle medesime, esse si permutano tutte quante tra loro, senza che nasca nessuna nuova permutazione; dunque *le ν permutazioni* (A) *constituiscono un gruppo.*

Questo gruppo lo chiameremo *gruppo della equazione ridotto dalle quantità che si sono aggiunte.*

Se non si fosse aggiunta nessuna quantità irrazionale il grado del gruppo della equazione in generale sarebbe stato M.

5.° *Tutte le funzioni razionali delle radici della* (1) *invariabili per tutte le sostituzioni del gruppo* (A), *sono esprimibili razionalmente per i coefficienti della* (1) *e per le quantità aggiunte dalle quali è stato ridotto.*

Esprimendo tutte le radici della (1) per uno qualunque V_0 dei valori (4), una funzione razionale qualunque delle radici sarà eguale a una funzione razionale di V_0

$$\chi(V_0).$$

Se essa è invariabile per tutte le sostituzioni del gruppo (A), equivalendo queste alle permutazioni dei valori (4) tra loro, avremo

$$\chi(V_0) = \chi(V_1) = \chi(V_2) = \ldots = \chi(V_{\nu-1}) ,$$

e quindi

$$\chi(V_0) = \frac{1}{\nu}\Big(\chi(V_0) + \chi(V_1) + \ldots + \chi(V_{\nu-1})\Big).$$

Dunque una funzione razionale qualunque delle radici della (1), che sia invariabile per le sostituzioni del gruppo (A), sarà simmetrica delle radici della (5), e perciò esprimibile razionalmente per i coefficienti della (5), ossia di quelli della (1) e delle quantità aggiunte.

Una funzione razionale delle radici e irrazionale dei coefficienti e delle quantità aggiunte dovrà esser variabile per alcune delle sostituzioni del gruppo.

6.° *Se una funzione razionale delle radici, e invariabile per alcune sostituzioni soltanto, è esprimibile razionalmente per i coefficienti e per alcune quantità aggiunte, il gruppo ridotto non conterrà nessuna sostituzione per la quale essa non sia invariabile.*

Sia

$$(8) \qquad \psi(V_0) = B ;$$

e il primo membro una funzione razionale delle radici della (1), il secondo dei coefficienti e delle quantità aggiunte. Poichè la (5) é irriduttibile, e la (8) ha i coefficienti razionali di quelli della (5), ed è soddisfatta da una radice della medesima, dovrà esserlo anche da tutte le altre. Dunque sostituendovi a V_0 qualunque altro valore (4), ossia facendo qualunque sostituzione del gruppo (A) sulle radici della (1), rimarrà invariabile; come volevamo dimostrare.

7.° Allorchè una funzione ra zionale delle radici variabile per ogni sostituzione che muta il posto di alcune soltanto di esse, è cognita razionalmente; il gruppo non può contenere sostituzioni che sull'altre radici; e quelle essendo invariabili per tutte le sostituzioni del gruppo saranno cognite razionalmente, e la equazione non sarà irriduttibile.

Da ciò ne segue che *le sostituzioni del gruppo di una equa-*

zione irriduttibile non potranno mai esser in numero minore del grado della equazione stessa.

8.° *Quando la Risolvente di Galois si decompone in fattori, ciascuno dei quali è razionale dei coefficienti e di una sola delle radici*

$$(9) \qquad r_0, \quad r_1, \quad r_2 \ldots . \ r_{n-1}$$

di una equazione ausiliare irriduttibile di grado n.

$$(10) \qquad \varphi(r) = 0 \ ;$$

il gruppo della proposta si divide in n gruppi derivati simili, e ciascuno di questi diviene gruppo della equazione quando si aggiunga una sola delle (9)*; e il gruppo della* (10) *è simile a quello della proposta.*

I fattori della risolvente (3) dovranno esser n, e differenti tra loro soltanto per i valori di r; perchè altrimenti $\Theta(V)$ razionale dei coefficienti della (10) o non sarebbe invariabile per alcuna sostituzione sopra le r, e unicamente per quelle che mutano il posto di alcune soltanto di esse, e quindi la (10) (V. n.° 7) non sarebbe irriduttibile. Pertanto potremo porre

$$\Theta(V) = \theta(V, r_0)\,\theta(V, r_1) \ldots . \ \theta(V, r_{n-1}).$$

Questi fattori saranno in V di grado

$$m = \frac{\nu}{n} \ ,$$

e posti a zero daranno tutte le radici della (3).

Siano

$$(11) \qquad V_{0,t} \ V_{1,t} \ V_{2,t} \ldots . \ V_{m-1,t}$$

le radici di una qualunque delle equazioni che ne nascono

$$(12) \qquad \theta(V, r_t) = 0.$$

Se si aggiunga la sola radice r_t, il gruppo della proposta sarà

$$(A_t)\begin{cases} \varphi_0(V_{0,t}),\ \varphi_1(V_{0,t}),\ \varphi_2(V_{0,t}) \cdots \varphi_{\mu-1}(V_{0,t}) \\ \varphi_0(V_{1,t}),\ \varphi_1(V_{1,t});\ \varphi_2(V_{1,t}) \cdots \varphi_{\mu-1}(V_{1,t}) \\ \cdot\ ,\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \varphi_0(V_{m-1,t}),\ \varphi_1(V_{m-1,t}),\ \varphi_2(V_{m-1,t}) \cdots \varphi_{\mu-1}(V_{m-1,t}) \end{cases}$$

Dando a t tutti i valori da zero a $n-1$ si ottengono n gruppi, che sono quelli della equazione quando si aggiunga successivamente ciascuna delle (9), e che sommati insieme formano il gruppo dell'equazione quando non le è aggiunta nessuna radice della (10).

Se $V_{0,t}$ e $F(V_{0,t})$ sono due radici della (12), si avrà

$$\theta(V_{0,t}, r_t) = 0, \theta(F(V_{0,t}), r_t) = 0 : \tag{13}$$

e poichè la 1.^{a} è irriduttibile, e la 2.^{a} razionale delle quantità che entrano nei coefficienti della 1.^{a}, sarà il resto della divisione della 2.^{a} per la 1.^{a}

$$\bar{\omega}(r_t) = 0. \tag{14}$$

Questa che ha tutti i suoi coefficienti razionali, e ammette una radice della (10) che è irriduttibile, dovrà ammettere anche tutte le altre. Perciò essendo $r_{t'}$ un altra qualunque delle (9) si avrà

$$\bar{\omega}(r_{t'}) = 0\ ,\quad \text{e}\quad \theta(F(V_{0,t'}), r_{t'})$$

divisibile per

$$\theta(V_{0,t'}, r_{t'})\ .$$

Da ciò ne segue che, essendo le radici di un fattore (12) date da certe funzioni razionali di una tra loro, anche quelle di un altro fattore qualunque saranno date dalle stesse funzioni di una tra loro. Dunque, cangiando uno dei valori $V_{0,t}$. che entrano in un gruppo (A_t), in uno $V_{0,t'}$, di un altro gruppo $(A_{t'})$, tutte le permutazioni di (A_t) si cangiano rispettiva-

mente in quelle di $(A_{t'})$: e poichè il cangiamento di un valore V, in un altro, corrisponde a una sostituzione sulle radici della (1), una sola e medesima sostituzione converte tutte le permutazioni di un gruppo in quelle di un altro, e i gruppi $(A_0), (A_1) \ldots . (A_{n-1})$ sono derivati uno dell'altro.

Poichè un gruppo A_t appartiene alla equazione quando è aggiunta una sola delle (9) r_t, e tutte le altre (9) rimangono irrazionali; ciascuna di esse espressa razionalmente per le radici della proposta dovrà risultare invariabile per le sostituzioni del gruppo corrispondente e variabile per quelle di tutti gli altri: dunque il gruppo della equazione (10) dovrà essere eguale a quello delle permutazioni sopra i derivati, e simile a quello della proposta (v. n.° 20. Parte I).

9.° *Se la risolvente può decomporsi in più fattori razionali dei coefficienti della proposta, e di tutte le radici*

$$(15) \qquad r_0 , \quad r_1 , \quad r_2 \ldots r_{n-1}$$

di una equazione ausiliaria irriduttibile

$$(16) \qquad \varphi(r) = 0 ;$$

il gruppo deve essere il prodotto di due altri; il primo dei quali è il gruppo della equazione stessa quando siano aggiunte tutte le (15) ; *il secondo è simile al gruppo dell'ausiliaria* (16).

Sia

$$\Theta(V) = \theta_0(V, r_0 , r_1 \ldots . r_{n-1})\ \theta_1 (V, r_0 , r_1 \ldots . r_{n-1}) \ldots .$$
$$\theta_{n-1}(V, r_0 , r_1 \ldots . r_{n-1}).$$

Poichè la risolvente ha i coefficienti razionali delle quantità che entrano in quelli della (16), dovrà essere invariabile per le sostituzioni del gruppo di queste, e quindi i fattori θ_t non dovranno differire che per l'ordine nel quale sono disposte le (15) ed esser tanti quante sono le permutazioni del gruppo della (16). Indicando, come nel caso precedente, con

$$(17) \qquad V_{0,t} , \quad V_{1,t} , \quad V_{2,t} , \ldots . , V_{m-1,t}$$

le m radici del fattore irriduttibile di grado $m = \frac{\nu}{n}$

(18) $$\theta_t(V, r_0, r_1, r_2 \ldots r_{m-1}) = 0,$$

si dimostrerà ugualmente che tutti i gruppi (A_0) (A_1) ... (A_{n-1}) ottenuti dando a t tutti i valori interi da zero a $n-1$, e che appartengono alla equazione quando si aggiungano tutte le radici (15), sono derivati uno dell'altro.

Se una radice $V_{a,t}$ di un fattore (18) è data in funzione razionale di una radice $V_{a,t'}$ di un altro, per mezzo della equazione

$$V_{a,t'} = \psi(V_{a,t});$$

si avrà

$$\theta_t(V_{a,t}) = 0, \quad \theta_{t'}(\psi(V_{a,t})) = 0:$$

e poichè la prima è irriduttibile, e ambedue sono razionali delle stesse quantità, le radici della prima saranno tutte radici anche dell'altra, e se queste sono

$$V_{0,t}, \; F_1(V_{0,t}), \; F_2(V_{0,t}) \ldots F_{m-1}(V_{0,t})$$

saranno radici della $\theta_{t'} = 0$

$$\psi(V_{0,t}), \; \psi F_1(V_{0,t}), \; \psi F_2(V_{0,t}), \ldots \psi F_{m-1}(V_{0,t}).$$

Onde si passerà dall'una all'altra permutazione del gruppo $(A_{t'})$ facendo li stessi cangiamenti delle $V_{a,t}$ l'una nell'altra, come per passar da una permutazione all'altra di (A_t): dunque i gruppi derivati in questo caso sono tutti eguali, e il gruppo dell'ausiliaria che definisce le quantità aggiunte che sono invariabili per le sole sostituzioni dei gruppi (A_t), è simile a quello per il quale bisogna moltiplicare uno dei derivati per ottenere il gruppo stesso che appartiene alla proposta quando non siano aggiunte le (15) (v. P. I. n.° 21); come volevamo dimostrare.

10.° *Se si aggiunga a una equazione una funzione* U *razionale delle radici, la quale prenda per tutte le sostituzioni del primo divisore del gruppo altrettanti valori differenti, e sia invariabile per le sostituzioni dell'altro fattore, il gruppo della equazione diverrà il solo fattore per le sostituzioni del quale la* U *è invariabile.*

Poichè ogni funzione aggiunta diviene razionale, e perciò invariabile per tutte le sostituzioni del gruppo, il quale non potrà più contenere le sostituzioni per le quali essa è variabile (*).

11.° Se il gruppo è primo, non si potrà ridurre altro che aggiungendo una funzione variabile per tutte le sostituzioni del gruppo, con che il gruppo non conterrà più nessuna sostituzione, ossia una permutazione soltanto; perchè se si prenda una funzione U simmetrica dei valori, che riceve una funzione delle radici, per le sostituzioni di uno G dei derivati dei quali è somma il gruppo proposto, essa non sarà che apparentemente invariabile per queste sostituzioni; perchè eseguita una che lo converta in un altro derivato, diviene variabile anche per le sostituzioni di G. Dunque *se una equazione ha un gruppo primo, non esiston funzioni delle radici che aggiunte lo riducano, tranne quelle che lo riducono a una sola permutazione.*

12.° Il gruppo di una equazione, finchè non sia aggiunta una irrazionale che non si trovi già nei coefficienti, sarà in generale di grado 1. 2. 3 ... $\mu-1$. μ: perchè le sole funzioni simmetriche sono sempre cognite razionalmente senza l'aggiunta di nessuna quantità. Se il gruppo sarà di grado minore, dovranno esistere delle relazioni particolari tra le radici, che rendano impossibili le sostituzioni che non compariscono nel gruppo. Infatti, si aggiunga una funzione delle radici variabile per tutte le sostituzioni del gruppo, e invariabile per qualunque altra, e precisamente di queste una U che contenga il minimo numero di radici; il gruppo non conterrà più nessuna sostituzione, e quindi ogni funzione delle radici, e le radici stesse risulteranno razionalmente cognite; e si potranno tutte esprimere per U e per i coefficienti:

$x_0 = F_0(U)$, $x_1 = F_1(U)$, $x_2 = F_2(U) \ldots x_{\mu-1} = F_{\mu-1}(U)$.

Ora eseguendo in questo sistema di equazioni una sostituzione

(*) Per conoscere come di fatto avviene che aggiunta una sola funzione delle radici, rimangono aggiunte tutte quelle che le son *simili*, e quindi anche quelle che riducono la risolvente e il gruppo, vedasi la Lez: XI dell'Algebra superiore di *Serret*.

qualunque che non appartenga al gruppo , i secondi membri rimarrebbero fermi, e i primi si permuterebbero tra loro; ciò che è impossibile, perchè la equazione essendo irriduttibile le radici sono tutte differenti tra loro. Perciò le sostituzioni del gruppo di una equazione alla quale non é aggiunta nessuna irrazionale, le chiameremo *possibili,* e le altre *impossibili.*

Così se sulle radici di una equazione non sono possibili altre sostituzioni che quelle le quali non lasciano nessuna lettera allo stesso posto; per U potrà prendersi una radice qualunque, poichè essa sarà variabile per tutte le sostituzioni del gruppo , e invariabile per tutte le altre : quindi tutte le radici saranno funzioni razionali di una qualunque tra loro. Se non sono possibili altro che quelle che non lasciano più di due lettere allo stesso posto, si può prendere per U una funzione non simmetrica di due radici qualunque: e perciò tutte quante sono funzioni razionali di due qualunque tra loro.

13.° Reciprocamente quando esistono delle relazioni razionali tra le radici, il gruppo non contiene altre sostituzioni che quelle *possibili* nel sistema di equazioni che dà quelle relazioni, o, ciò che è lo stesso, in quello che se ne può dedurre per esprimer tutte le radici razionalmente per il minimo numero di esse. Infatti, aggiunte queste, le radici sono tutte cognite razionalmente, e il gruppo non contiene più nessuna sostituzione; dunque quelle per le quali le radici aggiunte sono invariabili, che sono le impossibili nel sistema , non le poteva contenere avanti la loro aggiunzione.

Così quando le radici sono tutte funzioni razionali di una qualunque tra loro, è evidente che, cangiata una, si debbono cangiar tutte le altre che ne sono funzioni razionali, e non son possibili altre sostituzioni che quelle che non lasciano ferma nessuna lettera : e queste sono le uniche che appartengono al gruppo.

Puiseux in questi ultimi tempi ha determinato le sostituzioni che si operano sulle radici quando si faccia percorrere con continuità una serie di valori immaginari, finchè non si torni a quello da cui siamo partiti, a una quantità della quale sono

funzioni razionali i coefficienti (*). *Hermite* ha dimostrato che queste sostituzioni sono quelle stesse del gruppo della equazione (**). Le considerazioni precedenti spiegano facilmente questa rimarchevole coincidenza.

II.

DELLA RISOLUZIONE DELLE EQUAZIONI.

14.° *Risolvere una equazione algebrica significa renderne razionali le radici coll'aggiunzione di radici di equazioni ausiliarie.*

Affinchè una equazione sia risoluta è necessario e sufficiente che il suo gruppo non contenga più nessuna sostituzione: perchè ogni funzione anche variabile per qualunque sostituzione deve essere razionalmente cognita quando una equazione è risoluta, e reciprocamente, se il gruppo è ridotto a non contenere più nessuna sostituzione, tutte le radici sono cognite razionalmente.

Bisogna qui distinguere due casi: o non esistono equazioni ausiliarie di gruppo inferiore per le radici delle quali siano esprimibili razionalmente quelle della proposta; e la operazione mediante la quale coll' aggiunzione di radici di equazione di gruppo simile si riduce il gruppo della proposta a non contenere nessuna sostituzione, la diremo *trasformazione della equazione*, o *risoluzione impropria*, e le radici di queste equazioni le diremo *irrazionali primitivi*; o esisteranno equazioni di gruppo inferiore, per le radici delle quali possano darsi razionalmente quelle della proposta, e allora la equazione si dirà *risolubile propriamente*.

Il primo caso ha luogo quando il gruppo è primo: il secondo quando è il prodotto di più gruppi primi.

15.° I. Caso. Noi qui toccheremo soltanto la Teoria delle trasformazioni delle equazioni in quanto é necessario per i problemi relativi alla risoluzione propria che ci siamo proposti in

(*) V. Journal de Liouville T. XV.

(**) V. Comptes Rendus. Avril 1851.

questa Memoria. Gl'irrazionali primitivi, di gruppo simile che possono esprimersi razionalmente gli uni per gli altri potranno essere definiti da equazioni irriduttibili di gradi differenti, o anche di grado eguale, e di maggiore o minore semplicità relativamente all'applicazione dei metodi di risoluzione numerica: noi però non ci fermeremo su queste distinzioni: e li terremo tutti della stessa classe. Osserveremo soltanto che da quanto abbiam detto al numero 11, si deduce facilmente il seguente teorema: *affinché una equazione irriduttibile sia impropriamente risolubile per radici di equazioni di grado inferiore è necessario e sufficiente che il suo gruppo sia decomponibile in un numero di derivati simili minore del suo grado.*

Gl'irrazionali primitivi di gruppi non simili li distingueremo in classi corrispondenti alle classi dei loro gruppi.

16.° *Gl'irrazionali primitivi di prima classe, il gruppo dei quali è di grado primo, sono tutti esprimibili razionalmente per soli radicali.*

Il Gruppo della equazione che li definisce non contiene che le potenze di una sola sostituzione di ordine eguale al numero delle radici (v. P. I. n.° 16), e circolare sopra tutte le medesime (v. P. I. n.° 7. 4.): quindi distinguendo le radici con apici numerici, poichè il loro numero è primo (v. P. I. n.° 2), le sostituzioni del gruppo saranno soltanto le potenze di

$$(19) \qquad \begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix}.$$

Costruiamo la funzione

$$U = (x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{\mu-1} x_{\mu-1})^\mu,$$

dove

$$\alpha^{\mu-1} + \alpha^{\mu-2} + \ldots + \alpha^2 + \alpha + 1 = 0.$$

U è invariabile per tutte le sostituzioni del gruppo (*), e perciò razionalmente cognita. Il radicale $\sqrt[\mu]{U}$ espresso per le ra-

(*) V. Serret. Cours d'Alg. sup. pag. 358.

dici è variabile per tutte le potenze della (19) : dunque aggiunto ridurrà il gruppo a non contenere più alcuna sostituzione, e gl' irrazionali primitivi x risulteranno razionalmente espressi per $\sqrt[\mu]{U}$, e per α, che è esprimibile per radicali, come dimostrò *Gauss* per il primo (*).

17.° *Tutti gl'irrazionali primitivi esprimibili per soli radicali sono di prima classe.*

Aggiunte le radici p^{esime} immaginarie della unità, una equazione binomia di grado p ha tutte le sue radici funzioni razionali di una qualunque tra loro : talchè queste non si possono che aggiunger tutte insieme : e quindi il gruppo di una equazione o non è riduttibile per questa aggiunta, oppure è il prodotto di un gruppo che potrà essere anche di primo grado, per un altro di grado p (v. n.° 8); dunque gl' irrazionali esprimibili per soli radicali o non sono primitivi, o sono di prima classe.

La determinazione degl'irrazionali, per i quali converrà di esprimere gl' irrazionali primitivi di classi superiori, sarà un applicazione delle proprietà dei gruppi delle classi corrispondenti.

18.° II. Caso. *Una equazione, il gruppo della quale è il prodotto di più gruppi primi, è risolubile per irrazionali primitivi, i gruppi dei quali sono rispettivamente simili ai divisori del gruppo della proposta : e viceversa.*

Sia il gruppo della proposta

$$H = \Gamma'\Gamma'' \ldots \Gamma^{(i)}$$

e $\Gamma' \Gamma'' \ldots\ldots \Gamma^{(i)}$ siano tutti primi. Decomponiamo il primo gruppo $\Gamma^{(i)}$ in un numero p di derivati simili (v. P. I. num. 23. 2.), e costruiamo una funzione θ delle radici, invariabile per tutte le sostituzioni degli altri gruppi $\Gamma' \Gamma''$... e per quelle

(*) V. Gauss. Disquisitiones Aritmeticae, ovvero Serret. Cours d'Alg. Sup. pag. 373.

di uno dei derivati dei quali è somma $\Gamma^{(i)}$. La funzione θ avrà p valori che saranno dati da una equazione di grado p, e di gruppo simile a $\Gamma^{(i)}$ (v. n.° 8). Aggiunte tutte le p radici di questa equazione, saranno cognite razionalmente delle funzioni variabili per le sostituzioni di $\Gamma^{(i)}$, e perciò il gruppo della proposta si ridurrà al solo prodotto degli altri. Coll'aggiunta d'irrazionali primitivi analogamente construiti e di gruppi simili a $\Gamma^{(i-1)}$, $\Gamma^{(i-2)}$...., si potrà ridurre successivamente il gruppo a contenere quanti divisori di meno si vuole, e quindi a non contenere più nessuna sostituzione, e così otterremo la risoluzione completa della equazione.

La proposizione inversa è una conseguenza immediata di ciò che si è stabilito al n. 9.

Dal Teorema precedente se ne deducono immediatamente i seguenti corollarj.

1. *Affinchè una equazione irriduttibile sia risolubile per irrazionali primitivi di classi determinate, è necessario è sufficiente, che il suo gruppo sia il prodotto di gruppi di classi eguali a quelle degl'irrazionali medesimi.*

2. *Affinchè una equazione sia risolubile per radicali è necessario e sufficiente che il suo gruppo sia il prodotto di gruppi tutti di prima classe.*

3. *Il prodotto dei gradi dei gruppi delle equazioni che definiscono gl'irrazionali primitivi per i quali una equazione irriduttibile è risolubile, è eguale almeno al grado del gruppo di questa medesima.*

4. *Il prodotto degl' indici dei radicali per i quali è risolubile una equazione è eguale almeno al grado della medesima, se è irriduttibile.*

19.° *Il grado dell'ultimo divisore del gruppo di una equazione, o è eguale al grado della equazione, o n'è un divisore.*

L'aggiunzione dell'irrazionale U variabile per le μ sostituzioni di questo divisore rende razionali le radici, e quindi decompone la equazione in μ fattori tutti di primo grado. L'aggiunta degli altri irrazionali poteva aver già decomposta la

equazione in fattori tutti di grado eguale tra loro, e quindi μ deve essere o eguale al grado, o a un divisore del medesimo; e qui, ragionando come per istabilire il numero dei fattori nei quali si decompone la risolvente, ai n.° 8 e 9, si dimostra che μ è eguale o al grado della equazione irriduttibile che dà U, o al gruppo, e quindi a un multiplo del grado della medesima; con che rimane provato ciò che volevamo.

Da ciò che precede derivano i corollarj seguenti:

1. *Una equazione irriduttibile di grado primo non può risolversi senza irrazionali di grado eguale al proprio.*

2.° *Una equazione irriduttibile di grado qualunque non può risolversi senza irrazionali di grado divisore del proprio.*

3. *Gl'irrazionali primitivi esterni nella espressione delle radici, cioè quelli che non compariscono nei coefficienti di nessuna delle ausiliarie o sono dati da equazioni di grado eguale a quello della proposta, o a un divisore del medesimo : teorema già dimostrato da* Malmsten *per il caso particolare dei radicali* (*).

CAPITOLO SECONDO

DELLA RISOLUBILITÀ DELLE EQUAZIONI PER RADICALI.

I.

DELLE RISOLVENTI LAGRANGIANE.

20.° Non sempre sono date immediatamente le relazioni razionali che passano tra le diverse radici di una equazione irriduttibile da risolversi, e quindi non sempre se ne conoscono i loro gruppi direttamente, come nelle equazioni che danno la divisione delle funzioni circolari ed ellittiche. Perciò non basta conoscere le condizioni da verificarsi sui gruppi di risolubilità per radicali; ma è necessario di trasformar quelle in altre facili a verificarsi direttamente sui coefficienti. Galois ebbe

(*) Crelle, Journal für die Mathematik. B. 34. In solutionem aequationum algebraicarum disquisitio : auct. *Malmsten.*

in vista più specialmente le condizioni relative ai gruppi, Abel ai coefficienti. Io ho sviluppato prima quelle, e poi le ho trasformate in questo.

La determinazione in particolare della natura dei gruppi di tutte le equazioni risolubili per radicali, consisterà nella ricerca del massimo moltiplicatore decomponibile in divisori di prima classe, dell'ultimo gruppo che dev' esser pure di prima classe, e di grado eguale a quello della equazione o a un divisore del medesimo (v. n.i 18° 2 e 19°).

21.° Passiamo ora a determinare come si possano coi coefficienti costruire alcune risolventi che abbiano proprietà particolari meno difficili a verificarsi di quelle della risolvente generale di Galois, quando appartengono a equazioni risolubili per radicali.

Abbiamo già veduto che il gruppo di queste equazioni è il prodotto di più gruppi di prima classe. Sia H il gruppo totale, e G, G', G'', ... $G^{(\nu)}$ i suoi divisori respettivamente di grado μ, μ', μ'' ... $\mu^{(\nu)}$, dove μ è eguale al grado n della equazione, o a un divisore del medesimo, e tutti sono numeri primi.

L' ultimo radicale da aggiungersi dovrà esser variabile per le sostituzioni dell'ultimo divisore G (v. n.° 19), e quindi per le sostituzioni circolari su tutte quante le radici se μ è primo, e se nò, per il prodotto di più sostituzioni circolari su μ radici ciascuna: dovrà inoltre esser radice di una equazione binomia, la quale abbia il termine noto R razionale, allorchè siano state aggiunte altre funzioni variabili per le sostituzioni di tutti gli altri divisori, e quindi invariabile per le sostituzioni circolari sopra μ radici: dunque potrà sempre prendersi per ultimo radicale da aggiungersi $\sqrt[\mu]{R}$, essendo μ un divisore del grado, e R la nota espressione di Lagrange

$$R = \left\{ \sum_{t=0}^{t=n-1} \alpha^t x_t \right\}^{\mu},$$

dove α è dato dalla equazione

$$\sum_{r=0}^{r=\mu-1} \alpha^r = 0.$$

I gradi μ', μ'', ... $\mu^{(\nu)}$ degli altri divisori di H sono tutti $< n$, perchè il numero delle permutazioni di un gruppo non può contenere fattori primi maggiori del numero delle lettere; dunque si potrà prendere un gruppo prodotto dei divisori di H

$$\Gamma = G' G'' \ldots G^{(i)},$$

il grado del quale sia

$$\delta = \mu' \mu'' \ldots \mu^{(i)} < n.$$

Eseguiamo sulle x_t contenute in R tutte le sostituzioni di Γ, avremo δ valori per R. Construiamo la equazione di grado δ che li ha per radici. Per averne i coefficienti basta determinare una sola funzione F simmetrica dei δ valori delle R; poichè la nota teorica delle funzioni simili ci dà il modo di esprimer quelli in funzion razionale di questa. Eseguendo quante e quali si vogliono sostituzioni sulle x_t contenute nella F, si avranno altrettanti valori che tutti saranno radici di una equazione in generale di grado molto elevato a coefficienti razionali, e che potrà chiamarsi *Risolvente Lagrangiana* dal sommo geometra che la usò il primo. Poichè ogni funzione simmetrica dei valori che prende F per le δ' sostituzioni di Γ', sono razionali se

$$\Gamma' = G^{(i+1)} G^{(i+2)} \ldots G^{(\nu)},$$

e in conseguenza

$$\delta' = \mu^{(i+1)} \mu^{(i+2)} \ldots \mu^{(\nu)};$$

la Risolvente Lagrangiana dovrà esser riduttibile, e avere un fattore razionale di grado δ'. Se non è $\delta' < n$, operando sopra questo fattore posto a zero, il gruppo del quale è Γ', come abbiamo operato sulla proposta, si farà dipendere da una di grado $< n$, e da un altra che sarà di grado $< \delta'$, e così

seguitando si avranno tante equazioni tutte di grado minore della proposta, dalla risoluzione delle quali dipenderà la risoluzione di questa. I gruppi di tutte le risolventi sono tutti evidentemente i successivi divisori di H; dunque esse saranno risolubili per radicali quando é la proposta.

L'applicazione diretta e generale di questo metodo suppone la cognizione precedente del gruppo della equazione da risolversi. Ma vedremo come anche senza conoscere il gruppo, essendo dati soltanto i coefficienti della equazione esistono certi modi di applicarlo, differenti secondo la natura del numero al quale è eguale il grado della equazione, tali che se con essi non si può ottenere la risoluzione voluta, possiamo esser certi che essa è impossibile. Questi modi sono quelli stessi proposti da *Lagrange*. L' *Abel* aveva veduto questo pregio del metodo inventato da quel sommo Geometra, e i Teoremi annunziati nel frammento della sua Memoria postuma *Sur la resolution algebrique des equations* sono diretti tutti a dimostrarlo.

22.° La Risolvente Lagrangiana in tutti i casi, tranne alcuni nei quali il grado è potenza di un numero primo, deve sempre avere un fattore razionale di primo grado. È curioso di conoscere se, tolto questo fattore, è ulteriormente riduttibile, e se lo è, di determinare il grado e la natura dei fattori razionali che la dividono. Io ho trovato un metodo generale per risolvere questo problema, e quì passo ad esporlo.

La radice U della Risolvente Lagrangiana, data dal fattore razionale di primo grado, è invariabile per tutte le sostituzioni del gruppo H della equazione. Le altre radici sono tutti i valori che prende U per tutte le sostituzioni che non appartengono a H. Deriviamo H per mezzo di una di queste φ, e poi il gruppo derivato deriviamolo successivamente per tutte le sostituzioni $\theta_0\ \theta_1\ \theta_2 \ldots . \theta_{n-2}$ di H; le funzioni invariabili rispettivamente per tutte le sostituzioni di questi derivati

$$(20) \qquad D_\varphi H, D_{\varphi\theta_0}, H,\ D_{\varphi\theta_1} H,\ D_{\varphi\theta_2} H,\ \ldots\ D_{\varphi\theta_{n-2}} . H$$

saranno altrettante radici della risolvente, che indicheremo con le lettere

$$(21) \qquad R_0\ R_1\ R_2\ \ldots\ R_{n-1}\ .$$

Alcune di queste potranno anche essere eguali tra loro; ma ancorchè siano tutte differenti le sostituzioni di H non faranno che permutarle una nell'altra; dunque le funzioni simmetriche delle medesime saranno invariabili per le sostituzioni di H e quindi razionali; onde *la risolvente Lagrangiana se avrà un fattore di grado primo ammetterà anche più fattori razionali di grado non superiore al grado del gruppo della equazione, quando questa sia risolubile per radicali.*

Poichè il gruppo di una equazione non contiene altre sostituzioni che quelle per le quali é invariabile una funzione delle radici razionalmente esprimibile per i coefficienti (v. n. 6); il gruppo della equazione che ha per radici le (21) sarà eguale a H: dunque *i fattori razionali nei quali è riduttibile la risolvente Lagrangiana sono tutti risolubili per radicali, se lo é la proposta.*

Affinchè alcune delle (21) siano eguali tra loro, e che il grado del fattore razionale sia perciò minore del grado del gruppo H, è necessario che alcuni dei (20) siano eguali, ossia per alcuni valori di m e m_1

$$(22) \qquad D_{\varphi\theta_m} H = D_{\varphi\theta_{m_1}} H\ ;$$

e quindi

$$\theta_a\ \varphi\theta_m = \theta_{a_1}\ \varphi\theta_{m_1}$$

e moltiplicando a destra per θ_α a sinistra per θ_μ essendo

$$\theta_\alpha\,\theta_{a_1} = 1 \qquad \theta_m\,\theta_\mu = 1$$

e

$$\theta_\alpha\,\theta_a = \theta_b\ , \qquad \theta_{m_1}\,\theta_\mu = \theta_c\ ;$$

si ottiene

$$(23) \qquad \theta_b\varphi = \varphi\theta_c\ ;$$

dunque φ dovrà essere φ una sostituzione di un moltiplicatore di alcuno dei divisori di H. Questo poi è sufficiente, perchè con un processo inverso dalla (23) si può facilmente dedurre la (22). Duuque *il numero dei fattori razionali della risolvente Lagrangiana di grado* α *(e* α *sarà sempre un divisore del grado* n *del gruppo della equazione) è eguale al numero delle sostituzioni dei massimi moltiplicatori dei gruppi di grado* $\frac{n}{\alpha}$ *divisori del gruppo* H *della proposta.*

II.

DELLA RISOLUBILITA' PER RADICALI DELLE EQUAZIONI DI GRADO PRIMO.

23°. *Affinchè una equazione irriduttibile di grado primo sia risolubile per radicali, è necessario e sufficiente che il suo gruppo non ammetta altre sostituzioni che quelle comprese nel simbolo*

$$(24) \qquad \begin{pmatrix} x_i \\ x_{ai+b} \end{pmatrix},$$

e che in conseguenza tutte le sue radici siano funzioni razionali di due qualunque tra loro.

L'ultimo divisore del gruppo di una equazione di grado primo risolubile per radicali non ha altre sostituzioni che le potenze di

$$(25) \qquad \begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix}$$

(v. n.° 19): il suo massimo moltiplicatore contiene solo le potenze di

$$(26) \qquad \begin{pmatrix} x_i \\ x_{i\rho} \end{pmatrix},$$

dove ρ è radice primitiva del grado (v. P. I. n. 24); e quindi ha tutti i divisori di prima classe (v. P. I. num. 35); dunque è necessario e sufficiente che tutte le sostituzioni del gruppo siano i prodotti delle differenti potenze della (25) con quelle della (26), cioè le sostituzioni comprese nel simbolo (24).

Le (24) non possono dare due permutazioni che abbiano più

di una lettera allo stesso posto (*): dunque tutte le radici debbono esser funzioni razionali di due qualunque tra loro (v. n.° 12); e questo è sufficiente, come già dimostrai in una mia Nota *sulla risolubilità per radicali delle equazioni di grado primo* (**) : e come si deduce facilmente dal num.° 13. Le (24) dando non più di $\mu(\mu-1)$ permutazioni , e per il numero 3 solo avendosi 1. 2.... $\mu=\mu(\mu-1)$, tutte le equazioni di grado primo superiore a 3 non sono in generale risolubili per radicali.

24.° *Affinchè una equazione di grado μ primo sia risolubile per radicali è necessario e sufficiente che la risolvente Lagrangiana ammetta un fattore razionale di primo grado.*

Le radici della risolvente Lagrangiana sono in questo caso

$$\sum_{h=1}^{h=\mu-1}\left(\sum_{i=0}^{i=\mu-1} x^i x_{i\rho^h}\right)^{\mu},$$

dove

$$\sum_{m=0}^{m=\mu-1}\alpha^m = 0$$

e ρ radice primitiva di μ (***). Questa funzione è evidentemente invariabile per tutte le sostituzioni (25) e (26) del gruppo (****): dunque la risolvente ha una radice razionale; e questo basta perchè col metodo di Lagrange si possano ottenere tutte le radici espresse per radicali.

Passiamo a determinare gli altri fattori razionali della *risolvente*. Poichè il gruppo delle (25) ha per massimo moltiplicatore quello delle sostituzioni date dalle (26), basterà deter-

---

(*) Vedi Tortolini Annali di Mat. Anno 1851, pag. 8.

(**) Ivi, pag. 14.

(***) Vedi Ann di Mat. compilati da B. Tortolini genn. 1851. *Nota sulla risolubilità* ec.

(****) Ivi.

minare il moltiplicatore di questo ultimo. In questo caso la equazione (14) della prima parte, diviene

$$\psi(\rho i) = \rho^m \psi(i)$$

che ha per integrale

$$\psi(i) = i^m$$

dunque la *risolvente Lagrangiana delle equazioni di grado μ primo ha tanti fattori razionali di grado μ, quante sono le sostituzioni ψ cioè quanti i numeri primi inferiori a μ : gli altri sono di grado $\mu(\mu-1)$, e tutti poi risolubili per radicali.*

III.

DELLE EQUAZIONI IL GRADO DELLE QUALI È IL PRODOTTO DI PIU' NUMERI PRIMI DIFFERENTI

25.° *Una equazione il grado della quale è il prodotto di numeri primi differenti non può esser risolubile per radicali , se il suo gruppo non è a lettere congiunte.*

Poiché abbiamo veduto che l'ultimo gruppo di una equazione risolubile per radicali dev'esser di grado primo p divisore del grado μ della equazione (v. n.° 19); e che il massimo gruppo che lo abbia per divisore è (v. P. I. n.^{i} 26, 27, 28) a lettere congiunte quando i fattori di μ sono differenti tra loro.

26.° *Una equazione irriduttibile il grado $\mu = pq$ della quale ha dei fattori primi differenti non può esser risolubile per radicali, se non è decomponibile in p fattori razionali di grado q, coll'aggiunzione delle sole radici di una equazione di grado p..*

Distinguiamo con un apice h le lettere di uno stesso sistema, con un altro k il sistema al quale appartengono, avremo per il teorema precedente che tutte le sostituzioni del gruppo dovranno essere della forma

$$\begin{pmatrix} x_{h,\,k} \\ x_{\varphi(h),\,\varphi(k)} \end{pmatrix}.$$

Siano $F_0\ F_1\ F_2\ \ldots\ F_{p-1}$ altrettante funzioni ciascuna delle lettere di uno stesso sistema, e invariabili per le sostituzioni

$$(27) \qquad \begin{pmatrix} x_{h,k} \\ x_{\varphi(h),k} \end{pmatrix}.$$

Esse saranno radici di una equazione di grado p il gruppo della quale, contiene soltanto le sostituzioni

$$(28) \qquad \begin{pmatrix} x_{h,k} \\ x_{h,\psi k} \end{pmatrix};$$

e poichè esse sono variabili per tutte le sostituzioni (28), aggiunte ridurranno il gruppo alle sole (27). Dunque le funzioni invariabili per quelle saranno razionalmente cognite; e quindi anche le funzioni simmetriche di ogni sistema di radici: dunque per l'aggiunzione delle p radici F_k la proposta si ridurrà in p fattori razionali di grado q, come volevamo dimostrare.

È evidente che le funzioni simmetriche delle F , ossia i coefficienti della equazione della quale esse sono radici, saranno invariabili per tutte le sostituzioni del gruppo, e quindi razionali; e la risolvente Lagrangiana , che in questo caso è di grado

$$\frac{1.\,2.\,3.\ldots\mu}{(p-1)p(1.2\ldots q)^p} \quad (*)$$

dovrà avere un fattore razionale di primo grado se p è primo; se no, dovrà esser riduttibile parimente la equazione che dà le F, e così di seguito, finchè non si arrivi a una di grado primo; per la quale vale quello che abbiamo stabilito nel paragrafo precedente. Lo stesso deve dirsi dei fattori razionali di grado q, i quali posti a zero danno direttamente le radici.

Le condizioni esposte nei due teoremi dei num. 25° e 26°, non son sufficienti; ma le condizioni sufficienti sono già in esse contenute: perchè rimangono ridotte a quelle delle equazioni di grado primo, che tali sono le ultime equazioni irriduttibili alle quali si arriva con questo metodo.

Quando una equazione irriduttibile è di grado pq, e p e q

(*) V. Serret, Cours d'Alg. sup. pag. 240.

sono numeri primi differenti, indicando le radici colle lettere

$$x_{0,0} \quad x_{1,0} \ldots\ldots x_{p-1,0}$$
$$x_{0,1} \quad x_{1,1} \ldots\ldots x_{p-1,1}$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$x_{0,q-1}, \; x_{1,q-1} \ldots\ldots x_{p-1,q-1}$$

i casi di risolubilità sono i soli tre seguenti:

1.° Quando il gruppo della equazione è di grado

$$p^q(p-1)^q \, q(q-1)$$

e le sue sostituzioni sono date da

$$\binom{x_{i,0}}{x_{\varphi(i),0}}, \binom{x_{i,1}}{x_{\varphi(i),1}}, \ldots\ldots \binom{x_{i,q-1}}{x_{\varphi(i),q-1}}; \binom{x_{i,h}}{x_{i,\psi(h)}}.$$

2.° Quando è di grado

$$q^p(q-1)^p \, p(p-1)$$

e le sostituzioni sono

$$\binom{x_{0,i}}{x_{0,\varphi(i)}}, \binom{x_{1,i}}{x_{1,\varphi(i)}}, \ldots \binom{x_{p-1,i}}{x_{p-1,\varphi(i)}}, \binom{x_{h,i}}{x_{\psi(h),i}}.$$

3.° Se il gruppo è di grado

$$pq(p-1)(q-1)$$

e le sostituzioni

$$\binom{x_{i,h}}{x_{\varphi(i),\psi'(h)}}.$$

In tutti questi simboli dovrà aversi

$$\varphi(i) = ai + b, \; \psi(h) = a'h + b'$$

essendo a e b numeri interi qualunque $< p$, a' e $b' < q$.

Le risolventi Lagrangiane delle equazioni di grado p e q dalle quali si fa dipendere la proposta, debbono inoltre aver tutte un fattore razionale di primo grado (v. num.° 24). Facendo $p = 2$, $q = 3$ si hanno i tre casi di risolubilità delle

equazioni di 6.° grado, sviluppati e dimostrati da *Luther* nel T. 36 del Giornale di Crelle.

27.° Da ciò che abbiamo stabilito nel numero precedente si deduce immediatamente che il grado del gruppo di una equazione di grado $m = pq$, dove p e q sono differenti, non deve esser maggiore di 1, 2 ... q. 1. 2... p. Ora il Gruppo di una equazione di grado pq in generale è di grado 1.2.3... pq; dunque affinchè sia risolubile per radicali dovrà aversi

$$1.\,2.\,3\ldots pq \leqq 1.\,2.\,3\ \ldots\ q.\ 1.\,2.\,3\ldots p\,;$$

o anche

$$q+1\,.\,q+2\ldots pq \geqq 1.\,2.\,3\ \ldots\ p$$

lo che evidentemente non può essere se p e $q > 1$; dunque l'equazioni i gradi delle quali ammettono dei fattori primi differenti, non sono *in generale* risolubili per radicali.

IV.

DELLE EQUAZIONI IL GRADO DELLE QUALI È LA POTENZA DI UN NUMERO PRIMO.

28.° *Se il gruppo K di una equazione risolubile per radicali di grado* p^ν (*p essendo un numero primo*) *non è a lettere congiunte, deve necessariamente* 1.° *non contenere altre sostituzioni che della forma*

$$(29)\qquad \left\{ \begin{array}{c} x_k \\ x_{\sum_{r=0}^{r=\nu-1} \mathrm{B}_r k^{p^r} + \mathrm{B}_\nu} \end{array} \right\}$$

(*k e i* B_r *essendo radici di* $x^{p^\nu} \equiv x \pmod{p}$); *e in conseguenza essere di grado, o eguale a*

$$\mathrm{M} = p^\nu(p^\nu - 1)(p^\nu - p) \ldots (p^\nu - p^{\nu-1}),$$

o a un divisore di M; *e tutte le radici della equazione debbon*

essere funzioni razionali di $\nu+1$ *tra loro.* 2.° *Essendo sempre*

$$K = K_0 G G_1 G_2 ,$$

dove K_0 *ha soltanto sostituzioni della forma*

$$\begin{pmatrix} x_k \\ x_{k+k_0} \end{pmatrix} ,$$

e G, G_1, G_2 *hanno il medesimo significato che al n.°* 38; *il gruppo* G_1 *il grado del quale è un divisore di*

$$\frac{(p^\nu - 1)(p^\nu - p) \ldots (p^\nu - p^{\nu-1})}{2(p-1)} ,$$

deve essere decomponibile in gruppi di prima classe.

L'ultimo gruppo deve essere di grado p (v. n.° 19), dunque (v. n.° 28) il massimo gruppo che lo ha per ultimo divisore o è a lettere congiunte, o non contiene altre sostituzioni che le (29) e il suo grado è un divisore di M, e non é decomponibile in gruppi di prima classe altro che quando lo é G_1 (v. P. I. n.° 38).

Le funzioni non simmetriche delle $\nu+1$ radici che hanno per apici

$$0, \lambda, i, i^2 \ldots i^{\nu-1},$$

o di altre $\nu+1$ delle radici della congruenza $x^{p^\nu} \equiv x \pmod{p}$, delle quali nessuna si possa esprimere linearmente per le altre (v. P. I. num.° 32) sono variabili per tutte le sostituzioni del gruppo: dunque (v. n.° 6), tutte le radici possono esprimersi razionalmente per esse.

Le prime condizioni del teorema contiene la seconda quando $p^\nu = 4$, $= q$ (v. P. I. n.° 38).

29.° *Affinchè una equazione irriduttibile di grado* p^ν *(*p *essendo numero primo e* ν *qualunque) sia risolubile per radicali, è neceesario e sufficiente o che essa sia decomponibile in* $p^{\nu-\beta}$ *equazioni ognuna di grado* p^β, *i coefficienti delle quali siano funzioni razionali delle radici di una sola equazione di grado* $p^{\nu-\beta}$, *o che ciascuna delle radici possa prender la forma*

$$x = A + \sqrt[\mu]{S_0} + \sqrt[\mu]{S_1} + \ldots + \sqrt[\mu]{S_\delta},$$

essendo A *razionale , e le* S , *radici di una equazione di grado* $\delta < p^\nu$, *i coefficienti della quale siano o razionali o funzioni razionali di equazioni di gradi minori di* $p^\nu - 1$: *e che sì nell'un caso che nell'altro le equazioni dalle quali si fa così dipender la proposta siano risolubili per radicali.*

Il gruppo della equazione o sarà a lettere congiunte , o sarà il gruppo K del numero precedente. Se è a lettere congiunte è evidente che si verifica il primo caso del Teorema (v. n.° 27). Se è eguale a K passiamo a dimostrare che si deve necessariamente verificare il secondo.

La espressione Lagrangiana del numero 21 sarà in questo caso

$$S_0 = \left\{ \sum_{t=0}^{t=p-1} \alpha^t \sum_{t=1}^{h=p^{\nu-1}} x_{t+\sigma_h} \right\}^p,$$

essendo α radice immaginaria p^{esima} della unità, e rappresentando con σ_h la espressione

$$a_1 i + a_2 i^2 + \ldots . a_{\nu-1} i^{\nu-1}$$

per una combinazione qualunque di valori numerici delle a minori di p. Essa è invariabile per le p^ν sostituzioni circolari del gruppo K_0. Ora tra i seguenti e successivi moltiplicatori di K_0 nel gruppo K se ne potranno prendere alcuni in modo che il loro prodotto sia del più alto grado $< p^\nu$, cioè al più eguale a $p^\nu - 1$. Chiamiamo questo gruppo Γ e δ il suo grado.

Se eseguiamo tutte le sostituzioni immaginabili sulle x_t contenute nella S_0 , avremo M valori differenti per la medesima,

(30) $\qquad S_0 S_1 S_2 \ldots S_{M-1}$,

essendo, come è facile a dimostrarsi,

$$M = \frac{1.2.3.4 \ldots . (p^\nu - 1) p^\nu}{p(1.2.3 \ldots . p^{\nu-1})^p} .$$

Le sostituzioni di K eseguite sulle x_t della S_0 non potranno dare più di m dei valori (30), chiamando m il massimo comun divisore di M e di

$$M'=(p^\nu-1)(p^\nu-p)(p^\nu-p^2)\ldots(p^\nu-p^{\nu-1}).$$

Quelle di Γ non potranno dare più di δ valori (30), e δ dovrà essere divisore di m.

Ora costruiamo la equazione che ha per radici i δ valori (30) ottenuti colle sostituzioni di Γ. Il grado della risolvente Lagrangiana che ne darà i coefficienti sarà al più eguale a $\frac{M}{\delta}$: e poichè facendo tutte le sostituzioni di K nelle funzioni simmetriche F di quei δ valori, le quali sono invariabili per le sostituzioni di $K_0\Gamma$, non si possono avere più di $\frac{m}{\delta}$ valori differenti, essendo $K_0\Gamma$ un divisore di K, la risolvente sarà riduttibile, e avrà un fattore razionale di grado non maggiore di $\frac{m}{\delta}$.

Dalla forma delle S è facile dedurre, rammentando il metodo già usato nell'Algebra, che le radici avranno la forma

$$x = A + \sqrt[\mu]{S_0} + \sqrt[\mu]{S_1} + \ldots + \sqrt[\mu]{S_{\delta-1}} ,$$

A essendo il coefficiente del secondo termine della equazione.

Se $\frac{m}{\delta} < p^\nu - 1$ è già dimostrato il Teorema: ma quando non è, col metodo Lagrangiano è evidente che si potrà abbassare la equazione che dà le F finchè non si giunga a una risolvente di grado $< p^\nu - 1$.

Consideriamo ora alcuni casi particolari.

1.° Sia $\nu = 2$, $p = 2$, sarà $M = \frac{1.2.3.4}{2(1.2)^2} = 3$, $M' = 3.2$, onde $m = 3$, e poichè δ deve essere un fattore di m, sarà

eguale a 3; e il grado del fattore razionale della risolvente Lagrangiana sarà eguale a $\frac{m}{\delta} = 1$.

2.° Se $\nu=2$, $p=3$; sarà $M=\frac{1.2.3 \ldots 7.8.9}{3(1.2.3)^3}=2^4.5.7, M'=2^4.3$;

$m=2^4$, $\delta = 8$; $\frac{m}{\delta} = 2$.

3.° Se $\nu=3$, $p=2$; $M=\frac{1.2 \ldots 7.8}{2(1.2.3.4)^2} = 5.7$, $M'=7.6.4$,

$m=7$, $\delta=7$; $\frac{m}{\delta}=1$.

Le risolventi Lagrangiane per l'equazioni di 4° e 8° grado debbono aver un fattor razionale di 1.° grado: per quelle di 9° al più di secondo.

30.° Una equazione il gruppo della quale sia $>M$, avendo M il valore del n.° 28, e che abbia per grado una potenza di un numero primo, non può esser risolubile per radicali (v. n.° 28). Deve dunque aversi, se le radici non hanno delle particolari relazioni tra loro

$$p^\nu(p^\nu-1)(p^\nu-p) \ldots (p^\nu-p^{\nu-1}) \geqq p^\nu(p^\nu-1)(p^\nu-2) \ldots 3.2.1,$$

o anche

$$(p^\nu-p)(p^\nu-p^2) \ldots (p^\nu-p^{\nu-1}) \geqq (p^\nu-2)(p^\nu-3) \ldots 3.2.1.$$

Ora questo non ha luogo in generale altro che per i casi seguenti

$$\begin{array}{llll} \nu=1, & p=1; & \nu=2, & p=1 \\ & p=2; & & p=2; \\ & p=3; & & \end{array}$$

dunque le equazioni il grado delle quali è potenza di un numero primo ed è >4, non sono risolubili per radicali *in generale*; ma di quelle il grado delle quali non è potenza di un numero primo non ve ne è alcuna (v. n.° 23 e 26); quindi *nes-*

suna equazione di grado >4 può essere in generale risolubile per radicali.

Determinato se una equazione algebrica è o non è risolubile per radicali, o per irrazionali primitivi di altre date classi, rimane a eseguire la risoluzione effettiva. Abbiamo avuto luogo di accennare il modo che può tenersi per la medesima; però, appena il grado della equazione è un poco elevato, i calcoli necessarj divengono di una lunghezza da stancare ogni paziente calcolatore. Ma le ricerche intraprese con successo da molti distinti geometri in questi ultimi tempi sulle quantità complesse della natura della espressione di Lagrange, fanno sperare che l'Algebra potrà non solo vantaggiarsi dell'acquisto di nozioni più determinate e più estese sulla natura degl'irrazionali primitivi, ma giungerà anche ad arrichirsi di Tavole che diano gli elementi coi quali si possa con più speditezza condurre il calcolo della costruzione dei valori delle radici coi coefficienti; come ne abbiamo un esempio per le equazioni binomie, nei bei lavori dei Sigg. *Plana* e *Kummer*.

Pag.	*Lin.*	*Errori*	*Correzioni*
12	16.18	$D_{\psi}^{m''}\theta \,.\, D_{\psi}^{r}\theta$	$D_{\psi}^{m.n} D_{\psi}^{r}\theta$
14	8	qn	q
19	24	essi fattori	esse i fattori

Pag.	*lin.*	ERRORI	CORREZIONI
54	27-28	condizioni da verificarsi sui gruppi di risolubilità per radicali	condizioni di risolubilità per radicali da verificarsi sui gruppi
57	33	$D_{\varphi\theta_0}$, H $D_{\varphi\theta_{n-2}}$. H	$D_{\varphi\theta_0}$ H $D_{\varphi\theta_{n-2}}$ H
65	22	Le prime condizioni	La prima condizione
—	23	q	9
66	4	*razionali di equazioni*	*razionali di radici di equazioni*
—	10	(v. n.° 27)	(v. n.° 26.°)