Intorno all'interpretazione della Teoria di Galois in un campo di razionalità finito.

(*Di* U. SCARPIS, *a Bologna.*)

Ho constatato in una breve precedente Nota (*), che applicando alla risoluzione di una congruenza di terzo grado (mod. p) la formola cardanica, in dipendenza dal carattere quadratico di certi elementi, essa, in certi casi, diviene illusoria quando la congruenza ammette tre radici, ed efficace quando ne possiede una sola; mentre, in altri, succede precisamente il contrario. Ho quindi accennato alle modificazioni che potrebbe subire la Teoria di GALOIS ove si volesse applicare ad equazioni i cui coefficienti e le cui radici appartenessero ad un campo composto di un numero finito di elementi.

Scopo di questo lavoro è di presentare alcuni risultati ottenuti intorno a tale questione, i quali potrebbero forse servire di incentivo ad altri più profondi ed esaurienti.

1) Data una funzione dell'indeterminata i

$$f(i) = a_0 i^n + a_1 i^{n-1} + \cdots + a_n$$

i cui coefficienti sono interi qualunque appartenenti al sistema completo di residui del modulo primo p e che si suppone irriducibile mod. p, è noto che i p^n elementi:

$$a_{0h} i^{n-1} + a_{1h} i^{n-2} + \cdots + a_{n-1h} = r_h \qquad (1)$$

che si ottengono attribuendo ai coefficienti a_{kh}, indipendentemente l'uno dall'altro, p valori congrui mod. p ad uno qualunque dei p residui

$$0, 1, 2, \ldots, (p-1)$$

costituiscono un esempio di un dominio « pseudo-ortoide » chiamato « campo

(*) *Periodico di Matematica.* Volume XXVII, Fasc. II, 1911.

di GALOIS » definito dalla funzione modulare $f(i)$ e dal numero primo p, e che indicheremo brevemente con (r).

Agli elementi (1), altri si possono sostituire che ad essi siano rispettivamente congrui rispetto alla $f(i)$ ed a p, i quali si identificheranno coi precedenti.

Manifestamente (r) contiene in sè come divisore il campo

$$0,\ 1,\ 2,\ \ldots,\ (p-1)$$

che si può considerare generato dall'irriducibile

$$f(i) = a_0\, i + a_1$$

e come è noto (*) in (r) sono sempre univoche e possibili le operazioni razionali esclusa la divisione per l'elemento nullo.

Per quanto concerne le equazioni, si dimostra che una

$$\varphi(x) = 0$$

i cui coefficienti appartengono ad (r) non può avere nello stesso campo più radici che unità il suo grado e che in particolare l'equazione

$$x^m = 1$$

possiede in (r) un numero di radici eguale al m. c. d di m e $(p^n - 1)$.

Notiamo inoltre che gli elementi di (r) (*marche*, secondo il DICKSON), ove si escluda lo 0, formano un gruppo abeliano rispetto alla moltiplicazione; mentre, includendovi lo 0, costituiscono un gruppo pure abeliano rispetto all'addizione.

Se ora, in luogo del sistema completo di residui mod. p, assumiamo come *base* il campo di GALOIS precedentemente definito:

$$r_0,\ r_1,\ r_2,\ \ldots,\ r_s \quad (r)$$

dove $s = p^n - 1$, detta $f(i)$ una funzione di grado m dell'indeterminata i a coefficienti ed irriducibile in (r), considerando il sistema di $p^{n \cdot m}$ elementi:

$$a_{0h}\, i^{m-1} + a_{1h}\, i^{m-2} + \cdots a_{m-1h} = R_h \qquad (2)$$

verremo così a costruire un campo più esteso (R) contenente (r) come di-

(*) DICKSON, *Linear groups with an exposition of the Galois field theory*. Teubner, Leipzig.

visore e relativamente al quale si può ripetere quanto si è affermato pel precedente.

2) Data ora una funzione $\varphi(x)$ irriducibile in (r) si dimostra (*) che la condizione necessaria e sufficiente perchè $\varphi(x)$ divida il binomio

$$x^{p^{n \cdot k}} - x$$

è che il grado ν di $\varphi(x)$ sia divisore di k.

Ciò premesso, sia

$$\varphi(x) = 0 \tag{1}$$

un'equazione a coefficienti ed irriducibile in (r) il cui grado ν è divisore di m. In quest'ipotesi $\varphi(x)$ divide

$$x^{p^{nm}} - x$$

e poichè l'equazione:

$$x^{p^{nm}} - x = 0$$

ha per radici le $p^{n \cdot m}$ marche di (R), se ne conclude che la (1) avrà essa pure nello stesso campo ν radici distinte e fuori di (r) in conseguenza della sua irriducibilità.

Poichè se α è radice di (1) lo è pure

$$\alpha^{p^n},$$

segue che la successione

$$\alpha,\ \alpha^{p^n},\ \alpha^{p^{2n}}, \ldots,\ \alpha^{p^{kn}}, \ldots \tag{2}$$

risulterà composta di radici di (1).

I termini della (2) non possono risultare tutti tra loro diversi, per cui se ne incontreranno senza dubbio due tra loro eguali, ed i primi soddisfacenti a tale condizione siano:

$$\alpha^{p^{rn}} = \alpha^{p^{(r+s)n}}$$

per cui dividendo per $\alpha^{p^{rn}} \neq 0$ risulta:

$$1 = (\alpha^{p^{rn}})^{p^{sn}-1} = (\alpha^{p^{sn}-1})^{p^{rn}}.$$

Dico che $\alpha^{p^{sn}-1} = 1$.

(*) Dickson, Op. cit., Cap. II, § 25.

Infatti, ove ciò non fosse, posto:

$$\alpha^{p^{sn}-1} = \beta \neq 1$$

si dovrebbe avere

$$\beta^{p^{rn}} = 1,$$

il che non può essere, poichè la

$$x^{p^{rn}} = 1$$

essendo p^{rn} primo con $p^{n \cdot m} - 1$, ammette in (R) l'unica radice $x = 1$.

Segue che

$$\alpha^{p^{sn}-1} = 1$$

e se ne conclude che α appartiene all'esponente $p^{sn} - 1$, o ad un suo divisore, e che intanto si ha:

$$\alpha^{p^{sn}} = \alpha$$

cioè che il primo a riprodursi dei (2) è lo stesso α e che quindi $r = 0$.

Ne viene che le s radici di (1)

$$\alpha,\ \alpha^{p^n},\ \alpha^{p^{2n}},\ \ldots,\ \alpha^{p^{(s-1)n}} \tag{3}$$

sono tutte diverse, e che quindi non potrà aversi

$$\alpha^{p^{\sigma \cdot n}-1} = 1 \quad \sigma < s,$$

vale a dire che, se α non appartiene a $p^{sn} - 1$ deve aver per periodo un suo divisore proprio.

Poichè la:

$$x^{p^{ns}} = x$$

ammette la radice α dell'irriducibile (1), le possiede tutte; vale a dire

$$x^{p^{ns}} - x$$

è divisibile per $\varphi(x)$ e quindi ν è divisore di s, per cui $\nu \leq s$. D'altra parte, poichè le (3), tutte diverse, sono radici di (1) dovrà pur essere $s \leq \nu$, e se ne conclude:

$$s = \nu.$$

Abbiamo quindi che, se α è una qualunque delle radici di (1), il loro

insieme vien dato da:

$$\alpha,\ \alpha^{p^n},\ \alpha^{p^{2n}},\ \ldots,\ \alpha^{p^{(\nu-1)n}}, \tag{4}$$

dal che segue che la (1) è normale ed abeliana.

Supponiamo ora che il grado ν di (1) non sia divisore di m, e che essa possieda una radice α in (R). Come prima si dimostrerà che in questa ipotesi dovrebbero esser pure radici:

$$\alpha,\ \alpha^{p^n},\ \alpha^{p^{2n}},\ \ldots,\ \alpha^{p^{(\nu-1)n}} \tag{5}$$

appartenendo α a $p^{\nu \cdot n} - 1$ o ad un suo divisore proprio, essendo le (5) tutte tra loro diverse.

Ma avendo la

$$x^{p^{m \cdot n}} - x = 0$$

una radice a comune con l'irriducibile (1) dovrebbe ammetterle tutte, ed essere

$$x^{p^{m \cdot n}} - x$$

divisibile per $\varphi(x)$, vale a dire m multiplo di ν, il che è contro l'ipotesi, per cui non è ammissibile che la (1) abbia radici in (R). Concludiamo col Teorema seguente: « Un'equazione di grado ν

$$\varphi(x) = 0$$

a coefficienti ed irriducibile in (r), possiede in (R) o ν radici o nessuna secondochè ν è o no divisore di m ».

Se α è una qualunque di tali radici, il loro insieme è dato dalla successione:

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

e la data equazione è abeliana ».

Segue da questo Teorema che il problema che si riferisce alla risoluzione in (R) di una irriducibile in (r), rimane limitato al caso in cui ν è divisore di m.

3) Detta α una qualunque delle radici dell'irriducibile in (r):

$$\varphi(x) = 0 \tag{1}$$

di grado ν divisore di m, sappiamo che il loro insieme è dato da

$$\alpha,\ \alpha^{p^n},\ \ldots,\ \alpha^{p^{(\nu-1)n}}. \tag{2}$$

Se ora in (2), ad α sostituiamo una qualunque $\alpha^{p^{nr}}$, esse si riproducono permutandosi secondo la potenza r^{esima} della sostituzione circolare:

$$g = (\alpha\ \alpha^{p^n}\ \alpha^{p^{2n}} \ldots\ \alpha^{p^{(\nu-1)n}})$$

e reciprocamente, l'effetto della sostituzione g^r in (2) equivale a sostituire $\alpha^{p^{rn}}$ ad α.

Le operazioni che rimpiazzano α con $\alpha^{p^{nr}}$ $(r = 0, 1, 2, \ldots, (\nu - 1))$ sono suscettibili di composizione (*), ed il prodotto di due di esse si risolve in una delle stesse: indicandole con

$$1 = \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}, \begin{pmatrix} \alpha^{p^n} \\ \alpha \end{pmatrix}, \begin{pmatrix} \alpha^{p^{2n}} \\ \alpha \end{pmatrix}, \ldots, \begin{pmatrix} \alpha^{p^{(\nu-1)n}} \\ \alpha \end{pmatrix}$$

si scorge subito che costituiscono un gruppo isomorfo al gruppo ciclico

$$G = \left| g^0 = 1,\ g,\ g^2, \ldots,\ g^{\nu-1} \right|.$$

Dimostriamo ora le proprietà fondamentali del gruppo G.

a) « Se una funzione razionale delle radici di (1) con coefficienti in (r), rimane *numericamente* invariata per tutte le sostituzioni di G, essa ha valore razionale, cioè in (r) ».

Sia $F(\alpha_1, \alpha_2, \ldots, \alpha_\nu)$ una tale funzione, e se ne esprimano le radici mediante una qualunque di esse. Si avrà:

$$F(\alpha,\ \alpha^{p^n}, \ldots,\ \alpha^{p^{(\nu-1)n}}) = \psi(\alpha). \tag{3}$$

Se ora si eseguisce sul primo membro di (3) la g^r, ciò equivale a sostituire $\alpha^{p^{nr}}$ ad α, per cui:

$$F_{g^r} = \psi(\alpha^{p^{nr}}).$$

Ma, per ipotesi, la F non muta di valore qualunque sia g^r, per cui ne viene:

$$F = \frac{1}{\nu}\left(\psi(\alpha) + \cdots \psi(\alpha^{p^{(\nu-1)n}})\right)$$

ed essendo la somma tra parentesi funzione simmetrica delle α, se ne deduce che F è razionale.

(*) WEBER, *Lehrbuch der Algebra*. I, § 154.

b) Reciprocamente, sia:

$$F(\alpha_1\ \alpha_2 \ldots \alpha_\nu) = \psi(\alpha) = \rho$$

dove ρ appartiene ad (r).

L'equazione

$$\psi(x) = \rho$$

avendo una radice in comune coll'irriducibile (1), le ammetterà tutte, per cui:

$$\psi(\alpha) = \psi(\alpha^{p^n}) = \cdots \psi(\alpha^{p^{(\nu-1)n}}) = \rho$$

e parimenti:

$$F_{g^0} = F_g = \cdots F_{g^{\nu-1}} = \rho.$$

c) « Se una sostituzione sulle α lascia numericamente invariata qualunque funzione razionale delle radici a coefficienti e valore in (r), essa appartiene a G ».

Sia infatti γ una sostituzione dotata della detta proprietà, e si ponga

$$F(\alpha_1\ \alpha_2 \ldots \alpha_\nu) = \psi(\alpha) = \rho.$$

Applicando la γ alla relazione

$$\psi(\alpha) = \rho$$

questa continua, per ipotesi, a sussistere, per cui si avrà:

$$\psi(\alpha^{p^{kn}}) = \rho$$

essendo $\alpha^{p^{kn}}$ la radice che γ sostituisce ad α. Ripetendo la γ sulla precedente si otterrà:

$$\psi(\alpha^{p^{2kn}}) = \rho,$$

dal che segue che γ^2 ad α sostituisce $\alpha^{p^{2kn}}$. Così continuando si conclude che

$$\gamma = (\alpha,\ \alpha^{p^{kn}},\ \alpha^{p^{2kn}}, \ldots),$$

vale a dire che:

$$\gamma = g^k,$$

cioè che γ appartiene a G (*).

Ammettendo il gruppo G le tre proprietà *a*), *b*), *c*) caratteristiche del gruppo di Galois di un'equazione algebrica, lo si dirà, esso pure, gruppo di Galois dell'irriducibile (1).

(*) Se γ lasciasse ferma quella particolare α in funzione della quale si immaginano espresse le $\alpha_1, \alpha_2, \ldots, \alpha_\nu$, basterebbe, come è lecito, supporla sostituita con una qualunque di quelle che vengono spostate dalla γ.

Dalla forma stessa di G risulta senz'altro che esso è transitivo: reciprocamente data una

$$F(x) = 0 \tag{3}$$

a coefficienti in (r) e riducibile, ammesso che possieda radici, e che esista un gruppo Γ su di esse dotato delle proprietà $a)$ $b)$ $c)$, si dimostra che esso dev'essere intransitivo.

Detto infatti $f_1(x)$ uno dei fattori irriducibili di $F(x)$ che possieda μ radici in (R), siano esse:

$$\alpha_1, \alpha_2, \ldots, \alpha_\mu. \tag{4}$$

Le funzioni simmetriche elementari delle (4), come razionali, dovranno ammettere tutte le sostituzioni di Γ, le quali dovranno limitarsi a permutarle tra loro; poichè, ove esistesse una γ che trasformasse il sistema (4) in un altro totalmente o parzialmente diverso

$$\alpha'_1 \alpha'_2 \ldots \alpha'_\mu, \tag{5}$$

le (4) e (5) dovrebbero soddisfare alla stessa equazione $f_1(x) = 0$, il che è assurdo.

Risulta da ciò che le (4) costituiscono un sistema d'intransitività.

Teorema: « Un'equazione

$$\varphi(x) = 0$$

a coefficienti ed irriducibile in (r) e con radici in (R), possiede un gruppo di Galois transitivo; reciprocamente se un'equazione

$$F(x) = 0$$

a coefficienti in (r) e riducibile in questo campo ammette radici in (R) ed esiste per essa un gruppo di Galois, questo dev'essere intransitivo. »

4) Supposto ora che il grado m della funzione modulare $f(i)$ (§ 1) non sia maggiore di p^n ordine del campo (r) che si è assunto come base di (R), passiamo a riassumere quelle tra le proposizioni della Teoria di Galois che ne costituiscono il nucleo.

Per brevità, indicheremo costantemente nel seguito una funzione razionale delle radici di una $\varphi(x) = 0$ a coefficienti ed irriducibile in (r), col simbolo F; specificando volta a volta il campo a cui si intenderà appartengano i suoi coefficienti ed il suo valore.

Per quei Teoremi, la cui dimostrazione procede parallelamente a quella che si dà nell'Algebra ordinaria (*), si riporterà il solo enunciato.

Teorema 1.°: « Quelle sostituzioni del gruppo di GALOIS della $\varphi(x) = 0$ che lasciano numericamente invariata una F a coefficienti in (r) ed a valore qualunque, ne formano un sottogruppo. »

Teorema 2.°: Se G è il gruppo di GALOIS di una

$$\varphi(x) = 0$$

a coefficienti ed irriducibile in (r), e G' è il sottogruppo di G cui appartiene una F a coefficienti in (r), applicando a quest'ultima tutte le sostituzioni di G, essa assumerà $\frac{\nu}{\nu_1} = q$ valori

$$F = y_1, y_2, \ldots, y_q$$

essendo q l'indice di G' in G, i quali saranno radici di una:

$$\psi(y) = 0$$

a coefficienti in (r) ed in esso irriducibile, ed il cui gruppo di GALOIS è il gruppo complementare

$$\Gamma = \frac{G}{G'} \text{ ».}$$

Teorema 3.°: « Se F ed F' appartengono allo stesso sottogruppo G' di G, esse si possono esprimere razionalmente l'una nell'altra ».

Detto q l'indice di G', siano

$$F = y_1, y_2, \ldots, y_q$$

i valori diversi che assume la F per tutte le sostituzioni di G, i quali sono radici dell'irriducibile

$$\psi(y) = 0.$$

Se $\gamma_1 = 1, \gamma_2, \ldots, \gamma_q$ sono sostituzioni di G che fanno assumere alla F i valori $y_1 = F, y_2, \ldots, y_q$, lo stesso effetto produrranno le:

$$g' \cdot \gamma_1;\ g' \cdot \gamma_2; \ldots;\ g' \gamma_q$$

dove g' è una qualunque di G'.

(*) Cfr. BIANCHI, *Teoria dei gruppi di sostituzioni, etc.*

Ciò premesso, costruendo la funzione:

$$\Phi(y) = \left(\frac{F'_{g'\gamma_1}}{y - y_1} + \frac{F'_{g'\cdot\gamma_2}}{y - y_2} + \cdots \frac{F'_{g'\cdot\gamma_q}}{y - y_q}\right) \cdot \psi(y)$$

ed eseguendo sulle α una qualsiasi sostituzione di G, le y_i si permutano nei denominatori, come le $F'_{g'\gamma}$ nei numeratori: $\Phi(y)$ è quindi funzione di y i cui coefficienti, funzioni alla lor volta delle α, ammettono tutte le sostituzioni di G e sono quindi razionali, cioè in (r). Facendo $y = y_i$ risulta:

$$\Phi(y_i) = F'_{g'\gamma_i} \cdot \psi'(y),$$

dove $\psi'(y) \neq 0$ poichè la $\psi(y) = 0$ come irriducibile non ha radici multiple, e ne segue quindi che $F'_{g'\gamma_i}$ è razionale in y ed in particolare che F' è razionale in $y_1 = F$.

Corollario: « Se F' rimane invariata per tutte le sostituzioni di G' e per altre ancora; vale a dire se appartiene relativamente a G ad un gruppo contenente G' come sottogruppo, la F' sarà sempre esprimibile razionalmente mediante la F, ma non viceversa ».

Teorema 4.°: « Data una

$$\varphi(x) = 0$$

a coefficienti ed irriducibile in (r) aggregando al suo campo di razionalità una $F = y_1$, il sottogruppo G' cui F appartiene, diventa il gruppo dell'equazione nel campo (r, y_1).

In (r, y_1), la $\varphi(x)$ diviene riducibile spezzandosi in q fattori $\varphi_i(x)$ irriducibili di grado $\frac{\nu}{q} = \nu_1$ essendo q l'indice di G' in G, e ν_1 l'ordine di G'.

Ciascuna poi delle q equazioni:

$$\varphi_i(x) = 0$$

ha per gruppo il corrispondente fattore circolare della base di G' ».

Che G' ammetta la proprietà *b*) (§ 3) del gruppo di Galois, ogni qualvolta il valore della funzione delle radici appartenga, insieme ai suoi coefficienti, al primitivo campo di razionalità, è manifesto poichè G' è sottogruppo di G.

Sia ora $U(\alpha_1\, \alpha_2 \ldots \alpha_\nu)$ una funzione che in generale supponiamo a valore e coefficienti in (r, y_1), per cui:

$$U(\alpha_1\, \alpha_2 \ldots \alpha_\nu) = \theta(y_1).$$

Ma la $(U - \theta(y_1))$, che in ultimo si riduce ad una funzione razionale delle α con coefficienti in (r), come nulla ammette tutte le sostituzioni di G e quindi di G' per cui:

$$U_{g'} - \theta(F_{g'}) = 0.$$

Ma $F_{g'} = F = y_1$ e quindi:

$$U_{g'} = \theta(y_1) = U.$$

Resta così provato che G' possiede la proprietà b).

Per la proprietà a), basta osservare che, in base al Teorema e Corollario precedenti, se una F' rimane numericamente invariata per tutte le sostituzioni di G' sarà F' razionale in $F = y_1$, cioè apparterrà al nuovo campo di razionalità. Rimane ancora a provarsi che G' risponde pure alla condizione c). A tal uopo, ricordiamo che essendo G ciclico, G' avrà la forma:

$$\left| (\alpha\ \alpha^{p^{nq}}\ \alpha^{p^{2nq}} \dots \alpha^{p^{(\nu_1-1)nq}})\ (\alpha^{p^n}\ \alpha^{p^{n(q+1)}} \dots \alpha^{p^{((\nu_1-1)q+1)n}}) \right.$$
$$\left. \dots\dots (\gamma^{p^{n(q-1)}}\ \alpha^{p^{n(2q-1)}} \dots \alpha^{p^{n(\nu_1 q-1)}}) \right|$$
$$= \left| C_1\, C_2 \dots C_q \right|.$$

Ciò premesso, essendo ρ in (r, y_1), consideriamo la funzione

$$(\rho - \alpha)(\rho - \alpha^{p^{nq}}) \dots (\rho - \alpha^{p^{(\nu_1-1)nq}}) = \theta$$

i cui coefficienti, ammettendo tutte le sostituzioni di G' appartengono ad (r, y_1). Se ora γ è una sostituzione di G che lasci numericamente invariata qualunque funzione razionale delle radici a coefficienti e valore in (r, y_1) e quindi anche la θ, dovrà necessariamente permutare tra loro le:

$$\alpha,\ \alpha^{p^{nq}}, \dots,\ \alpha^{p^{(\nu_1-1)nq}}$$

sostituendo ad α una $\alpha^{p^{knq}}$, a questa la $\alpha^{p^{2knq}}$ e così di seguito, per cui γ conterrà come fattore la potenza k^{esima} del ciclo C_1.

Nello stesso modo si dimostrerà che dovrà pure contenere una potenza h^{esima} di C_2 e così di seguito; e poichè le sostituzioni di G sono regolari ed è quindi $k = h = \cdots$ si conclude che

$$\gamma = C_1^k \cdot C_2^k \dots C_q^k,$$

vale a dire γ appartiene a G'.

Il gruppo G', soddisfacendo alle condizioni *a*) *b*) *c*), è quindi il gruppo di GALOIS della $\varphi(x) = 0$ nel campo ampliato (r, y_1). Essendo G' intransitivo, la $\varphi(x) = 0$ nel nuovo campo diviene riducibile in fattori irriducibili di egual grado ciascuno dei quali ha per radici quelle appartenenti ad uno stesso sistema d'intransitività, e se indichiamo con $\varphi_1(x)$ quelle dei fattori di $\varphi(x)$ le cui radici appartengono al ciclo C_1, è facile il vedere che C_1 diventa il gruppo di GALOIS in $(r\,y_1)$ dell'irriducibile:

$$\varphi_1(x) = 0.$$

Teorema 5.°: « Per ogni sottogruppo di G, esistono funzioni ad esso appartenenti ».

Sia G' tale sottogruppo: esso avrà la forma già notata nel Teorema precedente, ed eseguendo le sue sostituzioni sulla funzione $F = y_1$:

$$\begin{aligned} y_1 &= (\rho - \alpha)(\rho - \alpha^{p^{nq}}) \ldots (\rho - \alpha^{p^{(\nu_1-1)nq}}) \\ &= \rho^{\nu_1} + c_{11}\rho^{\nu_1-1} + c_{12}\rho^{\nu_1-2} + \cdots c_{1\nu_1} \end{aligned}$$

dove ρ è un'indeterminata in (r), la predetta funzione non muta, mentre per una sostituzione di G non in G', si cambia in:

$$y'_1 = (\rho - \alpha^{p^{\lambda n}})(\rho - \alpha^{p^{\lambda n+nq}}) \ldots (\rho - \alpha^{p^{(\nu_1-1)nq+\lambda n}}).$$

Se ora immaginiamo effettuate sulla y_1 tutte le sostituzioni di G, otterremo $q = \frac{\nu}{\nu_1}$ funzioni algebricamente distinte:

$$\left.\begin{aligned} y_i &= \rho^{\nu_1} + c_{i1}\rho^{\nu_1-1} + \cdots + c_{i\nu_1} \\ &(i = 1, 2, 3, \ldots, q). \end{aligned}\right\} \qquad (1)$$

Dico che potremo sempre scegliere l'indeterminata ρ in modo che le y_i risultino numericamente diverse.

Premesso che nella successione:

$$c_{1k},\ c_{2k}, \ldots,\ c_{qk}; \qquad (k = 1, 2, \ldots, \nu_1)$$

ciascun termine si deduce dal precedente sostituendo α^{p^n} ad α, e che lo stesso avviene quindi nella:

$$y_1,\ y_2, \ldots,\ y_q$$

notiamo che se due delle y, y_r ed y_s per un certo ρ assumono valori eguali,

esse diventano tutte eguali se q è dispari; mentre se q è pari od accade lo stesso, o risultano tra loro eguali quelle d'indice pari, e quelle d'indice dispari.

Infatti dall'ipotesi

$$y_r = y_s$$

segue che $y_r - y_s = 0$ ha valore razionale e che rimarrà quindi invariata per tutta la sostituzione di G per cui:

$$y_{r+1} - y_{s+1} = 0; \quad y_{r+2} - y_{s+2} = 0 \ldots$$

e di qui, facilmente, quanto si è asserito.

Ne viene che, se per un certo ρ due qualunque delle y se q è dispari, o due con indice di egual parità nel caso opposto, risultano tra loro diverse, per lo stesso ρ tutte indistintamente le y assumeranno valori diversi. Consideriamo dopo ciò la:

$$y_r - y_s = (c_{r1} - c_{s1})\rho^{\nu_1 - 1} + (c_{r2} - c_{s2})\rho^{\nu_1 - 2} + \cdots + c_{r\nu_1} - c_{s\nu_1} = 0$$

soddisfacendo gli indici r, s alla predetta condizione.

Una tale equazione che non può mai ridursi ad una identità, potrà avere al più $(\nu_1 - 1)$ radici in (r) e siccome $\nu_1 < m \leq p^n$, esisterà in (r) per lo meno un ρ per cui le due y_r, y_s assumeranno valori diversi e tali risulteranno tutti i termini della successione

$$y_1, y_2, \ldots, y_q.$$

Resta così provata l'esistenza di una funzione appartenente a G'.

Osservazione: « Confrontando questa dimostrazione con quella che si dà nel caso ordinario (*), si scorge il perchè dell'ipotesi restrittiva $m \leq p^n$ ».

Teorema 6.°: « Se ampliando (r) con una qualsiasi marca di (R), il gruppo di $\varphi(x) = 0$ si abbassa ad un suo sottogruppo G', lo stesso risultato si può conseguire aggregando ad (r) una F appartenente a G' ».

Teorema 7.°: « Siano

$$\varphi(x) = 0; \quad \psi(x) = 0$$

due irriducibili a coefficienti in (r) con radici in (R), e G, Γ i loro gruppi di Galois: se aggregando ad (r) le radici β di $\psi(x) = 0$, G discende a G' d'indice q, reciprocamente ampliando il campo (r) con le radici α di $\varphi(x) = 0$, Γ si riduce ad un suo sottogruppo Γ' d'indice q ».

(*) Bianchi, Op. cit., § 69.

Anche la dimostrazione di questo importante Teorema è del tutto simile a quella sua corrispondente nell'Algebra (*), ed è una conseguenza diretta delle precedenti proposizioni.

Da quanto precede risulta che le proposizioni fondamentali della Teoria di GALOIS conservano il loro significato anche se applicate ad equazioni in uno speciale campo di razionalità finito.

Nel paragrafo seguente vedremo come esse si possano applicare alla risoluzione e discussione del problema che ha per scopo la determinazione delle radici mediante radicali.

5) Data la

$$\varphi(x) = 0 \tag{1}$$

a coefficienti ed irriducibile in (r) di grado ν divisore di m e quindi dotata di ν radici in (R), indichiamo con ε una radice primitiva ν^{esima} dell'unità, e si ponga quindi:

$$y_1 = (\varepsilon,\ \alpha) = \alpha + \varepsilon\,\alpha^{p^n} + \varepsilon^2\,\alpha^{p^{2n}} + \cdots \varepsilon^{\nu-1}\,\alpha^{p^{n(\nu-1)}},$$

Applicando ad y_1 la sostituzione fondamentale

$$g = (\alpha\ \ \alpha^{p^n}\ \ \alpha^{p^{2n}} \ldots\ \alpha^{p^{n(\nu-1)}})$$

del gruppo della (1) si ottiene:

$$y_{1g} = y_2 = \alpha^{p^n} + \varepsilon\,\alpha^{p^{2n}} + \cdots \varepsilon^{\nu-1}\,\alpha = \varepsilon^{-1}\,.\,y_1\,,$$

dal che segue che la potenza ν^{esima} di y_1

$$y_1^{\nu} = (\varepsilon,\ \alpha)^{\nu}$$

rimane numericamente invariata per la g e per le sue potenze, e ne viene che essa è razionalmente esprimibile mediante ε e gli elementi di (r).

Ponendo in generale

$$(\varepsilon^r,\ \alpha)^{\nu} = B_r \tag{2}$$

le B_r saranno tutte razionalmente note e però le B_r si otterranno estraendo una radice ν^{esima}.

Facendo successivamente in (2) $r = 0, 1, 2, \ldots, (\nu - 1)$, ne risulta un si-

(*) BIANCHI, Op. cit., § 72.

stema di ν equazioni lineari a ν incognite α, α^{p^m},..., $\alpha^{p^{(\nu-1)m}}$ da cui, sommando, la formula di risoluzione:

$$\alpha = \frac{-a_1 + \sqrt[\nu]{B_1} + \sqrt[\nu]{B_2} + \cdots \sqrt[\nu]{B_{\nu-1}}}{\nu} \tag{3}$$

essendo a_1 il coefficiente del secondo termine di (1) supposto quello del primo ridotto all'unità, e sulla quale si possono ripetere le stesse osservazioni che valgono pel caso analogo nell'Algebra ordinaria (*) e intorno a cui non insistiamo.

Poniamo ora che il grado ν della (1) sia primo con $S = p^{n \cdot m} - 1$. In questa ipotesi la:

$$x^\nu = 1$$

ha in (R) l'unica radice $x = 1$, e la (3) diviene evidentemente illusoria. Se invece ν non è primo con S, ma non è nemmeno un suo divisore, possono presentarsi due casi: che ν sia composto di soli fattori primi di S, oppure che contenga qualche fattore estraneo. Nel primo caso si raggiungerà la soluzione della (1) mediante quella di una catena di equazioni i cui gradi risulteranno tutti divisori di S ed alle quali si potrà sempre applicare il procedimento su indicato.

Nel secondo caso, posto $\nu = \nu_1 \cdot q$ dove ν_1 è il prodotto di tutti i fattori di ν estranei ad S, determinando una $F = y_1$ appartenente a G' d'ordine ν_1 e d'indice q (§ 4) che si otterrà risolvendo una $\psi(y) = 0$ di grado q, ampliando poi il campo (r) con la y_1, la (1) verrà ad avere per gruppo G' divenendo riducibile. La sua risoluzione si potrà bensì far dipendere da quella dell'equazione che si ottiene eguagliando a zero uno dei suoi fattori irriducibili in (r, y_1) di grado ν_1, ma essendo ν_1 primo con S, la (3) risulta nuovamente illusoria. Facciamo ancora vedere come, applicando il Teorema 7.° del § 4, si possa dimostrare l'impossibilità di abbassare comunque il gruppo della (1) quando sia ν primo con S.

Supponiamo infatti che ampliando (r) con le radici β di una qualsiasi ausiliaria $\psi(x) = 0$, irriducibile in (r) e di grado μ divisore di S, o composto di soli fattori primi di S, e di gruppo Γ, sia possibile ridurre quello della (1) ad un suo sottogruppo G' d'indice q: per il citato Teorema, l'aggregare ad (r)

(*) BIANCHI, Op. cit., § 73 e seguenti.

le radici α di (1) dovrebbe pure abbassare Γ ad un suo sottogruppo Γ' d'indice q. Ne verrebbe allora:

$$\nu = \nu_1 \cdot q \quad \mu = \mu_1 \cdot q$$

e poichè μ risulta di soli fattori primi di S, non sarebbe più ν primo con S.

Dovrà quindi essere necessariamente

$$q = 1$$

e $G' = G$.

Se il grado μ non è composto di soli fattori primi di S, potrà anche ottenersi un abbassamento del gruppo di (1), ma allora bisogna supporre *date* le radici di $\psi(x) = 0$, poichè ove si volessero costruire per radicali, si urterebbe nella stessa difficoltà. Un caso che sembra a primo aspetto contradire ai risultati precedenti, è quello in cui la (1) fosse della forma:

$$x^\nu = \rho \tag{4}$$

con ν non composto di soli fattori primi di S: ma è facile vedere che in questa ipotesi la (4) non può soddisfare alla duplice condizione di essere irriducibile e di avere il suo grado divisore di m.

In vero posto:

$$\nu = \nu_1 \cdot \delta; \quad \delta = D(S, \nu)$$

le potenze di grado ν delle S marche di (R) (lo zero escluso) danno luogo ad un sistema di $\frac{S}{\delta}$ residui diversi ciascuno dei quali è ripetuto δ volte (*). La (1) possiede quindi o δ radici o nessuna ($\delta < \nu$), mentre se fosse irriducibile con ν divisore di m, dovrebbe ammetterne ν.

Osservazione: « La formula di risoluzione (3) qualora sia ν composto di soli fattori primi di S è valida in generale poichè viene dedotta da proposizioni che sussistono indipendentemente dall'ipotesi restrittiva $m \leq p^n$; non sarebbe però legittimo l'uso dei Teoremi 5.°, 6.°, 7.° del § 4 alla sua discussione nel caso ν primo con S, qualora fosse $m > p^n$ ».

6). Esempi:

I.° $p = 2$; $f(i) = i^6 - i - 1$; $n = 1$; $m = 6$

$$\varphi(x) = x^3 + x + 1 = 0. \tag{1}$$

(*) Dickson, Op. cit., Cap. III.

Come base di (R) assumiamo

$$(r) = (0,\ 1)$$

ed (R) risulta costituito dai 2^6 elementi:

$$a_0 i^5 + a_1 i^4 + \cdots + a_5$$

che si ottengono attribuendo alle a i valori 0, 1.

La (1), il cui grado $\nu = 3$ è divisore di $m = 6$ ed è irriducibile in (r), ha tre distinte radici in (R) e poichè ν è divisore di

$$S = 2^6 - 1 = 63$$

potremo applicare la formula (3) § 5.

Detta ε una radice cubica primitiva dell'unità, avremo:

$$B_1 = (\alpha_1 + \varepsilon\,\alpha_2 + \varepsilon^2\,\alpha_3)^3 = \sum \alpha_1^3 + 6\,.\,\alpha_1\,\alpha_2\,\alpha_3$$

$$+ \varepsilon^2\,(\alpha_1\,\alpha_2^2 + \alpha_1^2\,\alpha_3 + \alpha_2\,\alpha_3^2) + \varepsilon\,(\alpha_1^2\,\alpha_2 + \alpha_1\,\alpha_3^2 + \alpha_2^2\,\alpha_3).$$

Posto, in base al Teorema del § 2, $\alpha_1 = \alpha$; $\alpha_2 = \alpha^2$; $\alpha_3 = \alpha^4$, risulta:

$$\alpha_1\,\alpha_2^2 + \alpha_1^2\,\alpha_3 + \alpha_2\,\alpha_3^2 = \alpha^5 + \alpha^6 + \alpha^{10}$$

e poichè:

$$\alpha^8 = \alpha$$

ne viene:

$$\alpha^6 = \alpha^8\,.\,\alpha^8\,.\,\alpha^4 = \alpha^{20} = (\alpha^4)^5$$

$$\alpha^{10} = (\alpha^2)^5$$

per cui:

$$\alpha^5 + \alpha^6 + \alpha^{10} = \alpha^5 + (\alpha^2)^5 + (\alpha^4)^5 =$$

$$= \alpha_1^5 + \alpha_2^5 + \alpha_3^5 = \sum \alpha_i^5\,.$$

Parimenti:

$$\alpha_1^2\,\alpha_2 + \alpha_1\,\alpha_3^2 + \alpha_2^2\,\alpha_3 = \alpha^4 + \alpha^8 + \alpha^9 = \alpha + \alpha^2 + \alpha^4 = \sum \alpha_i\,.$$

Avremo così per B_1:

$$B_1 = \sum \alpha_i^3 + 6\,\alpha_1\,\alpha_2\,\alpha_3 + \varepsilon^2 \sum \alpha_i^5 + \varepsilon \sum \alpha_i$$

e dalle formule di NEWTON (*):

$$\Sigma \alpha_i^3 = 1; \quad \Sigma \alpha_i^5 = 1; \quad \Sigma \alpha_i = 0$$

$$6 \cdot \alpha_1 \cdot \alpha_2 \cdot \alpha_3 = -6 = 0$$

per cui in fine:

$$B_1 = 1 + \varepsilon^2$$

e sostituendo ad ε, ε^2:

$$B_2 = 1 + \varepsilon.$$

Fissata la radice ε, e supposta stabilita la corrispondenza tra i simboli α_1, α_2, α_3 e le radici di (1), il radicale

$$\sqrt[3]{B_1} = \sqrt[3]{(\alpha_1 + \varepsilon \alpha_2 + \varepsilon^2 \alpha_3)^3} = \sqrt[3]{1 + \varepsilon^2}$$

è suscettibile di tre diverse determinazioni che, convenendo di indicare col semplice radicale la determinazione $\alpha_1 + \varepsilon \alpha_2 + \varepsilon^2 \alpha_3$, si possono esprimere ponendo:

$$\sqrt[3]{B_1} = \alpha_1 + \varepsilon \alpha_2 + \varepsilon^2 \alpha_3$$

$$\varepsilon^2 \sqrt[3]{B_1} = \alpha_2 + \varepsilon \alpha_3 + \varepsilon^2 \alpha_1$$

$$\varepsilon \sqrt[3]{B_1} = \alpha_3 + \varepsilon \alpha_1 + \varepsilon^2 \alpha_2$$

a cui corrispondono tre valori per $\sqrt[3]{B_2}$ che si deducono sostituendo ε^2 ad ε:

$$\sqrt[3]{B_2} = \alpha_1 + \varepsilon^2 \alpha_2 + \varepsilon \alpha_3$$

$$\varepsilon \sqrt[3]{B_2} = \alpha_2 + \varepsilon^2 \alpha_3 + \varepsilon \alpha_1$$

$$\varepsilon^2 \sqrt[3]{B_2} = \alpha_3 + \varepsilon^2 \alpha_1 + \varepsilon \alpha_2 .$$

Le formole di risoluzione, osservando che $\alpha_1 = 0$ e che nel campo $(r) = (0, 1)$ si ha: $\frac{1}{3} = 1$, diventano:

$$\alpha_1 = \sqrt[3]{B_1} + \sqrt[3]{B_2}$$

$$\alpha_2 = \varepsilon^2 \sqrt[3]{B_1} + \varepsilon \sqrt[3]{B_2}$$

$$\alpha_3 = \varepsilon \sqrt[3]{B_1} + \varepsilon^2 \sqrt[3]{B_2}$$

(*) DICKSON, Op. cit., Cap. III.

ciascuna delle quali soddisfa la (1), purchè si ponga:

$$(\sqrt[3]{B_1})^3 = 1 + \varepsilon^2; \quad (\sqrt[3]{B_2})^3 = 1 + \varepsilon; \quad \sqrt[3]{B_1} \,.\, \sqrt[3]{B_2} = 1.$$

Supposta ora costruita la tavola di moltiplicazione del gruppo costituito dagli elementi di (R) escluso l'elemento nullo, si potrà col suo sussidio risolvere la questione che ha per oggetto di determinare se e da quali marche risulti soddisfatta un'equazione del tipo:

$$x^\lambda = r_h \quad (r_h \text{ in } (R))$$

e ricaveremo quindi:

$$\varepsilon = i^5 + i^4 + i^3 + i; \quad \varepsilon^2 = i^5 + i^4 + i^3 + i + 1$$

$$\sqrt[3]{1+\varepsilon} = i^4 + i^3 + i^2; \quad \sqrt[3]{1+\varepsilon^2} = i^3 + i + 1.$$

I valori assunti per $\sqrt[3]{B_1} = \sqrt[3]{1+\varepsilon^2}$, e per $\sqrt[3]{B_2} = \sqrt[3]{1+\varepsilon}$ soddisfano alla condizione:

$$\sqrt[3]{B_1} \,.\, \sqrt[3]{B_2} = 1.$$

Infatti rammentando che:

$$2 = 0; \quad i^6 = i + 1; \quad i^7 = i^2 + i$$

risulta:

$$(i^4 + i^3 + i^2)(i^3 + i + 1) = i^7 + i^6 + 2i^5 + 2i^4 + 2i^3 + i^2$$

$$= 2i^2 + 2i + 1 = 1.$$

Avremo quindi:

$$\alpha_1 = i^3 + i + 1 + i^4 + i^3 + i^2 = i^4 + i^2 + i + 1$$

$$\alpha_2 = i^4 + i^3 + 1$$

$$\alpha_3 = i^3 + i^2 + i$$

II.° $p = 7$; $f(i) = i^3 - i + 2$; $n = 1$; $m = 3$

$$\varphi(x) = x^3 - 2x + 2 = 0 \tag{2}$$

$$(r) = (0,\ 1,\ 2, \ldots,\ 6)$$

$$(R) = (a_0 i^2 + a_1 i + a_2) \quad S = 7^3 - 1 = 342$$

$$B_1 = (\alpha_1 + \varepsilon\,\alpha_2 + \varepsilon^2\,\alpha_3)^3; \quad B_2 = (\alpha_1 + \varepsilon^2\,\alpha_2 + \varepsilon\,\alpha_3)^3$$

$$\alpha_1 = \alpha\,; \quad \alpha_2 = \alpha^7\,; \quad \alpha_3 = \alpha^{49}$$

$$\alpha_1\,\alpha_2^2 + \alpha_1^2\,\alpha_3 + \alpha_2\,\alpha_3^2 = \alpha^{15} + (\alpha^7)^{15} + (\alpha^{49})^{15} = \sum \alpha_i^{15}$$

$$\alpha_1^2\,\alpha_2 + \alpha_1\,\alpha_3^2 + \alpha_2^2\,\alpha_3 = \alpha^9 + (\alpha^7)^9 + (\alpha^{49})^9 = \sum \alpha_i^9$$

$$B_1 = \sum \alpha_i^8 + 6\,\alpha_1\,\alpha_2\,\alpha_3 + 3\,\varepsilon^2 \sum \alpha_i^{15} + 3\,\varepsilon \sum \alpha_i^9$$

$$\sum \alpha_i^3 = 1\,; \quad \sum \alpha_i^9 = 0\,; \quad \sum \alpha_i^{15} = 6\,; \quad \alpha_1\,\alpha_2\,\alpha_3 = -2$$

e quindi sostituendo

$$B_1 = 3\,(1 - \varepsilon^2)\,; \quad B_2 = 3\,(1 - \varepsilon).$$

Supposto fissata la ε e stabilito l'ordinamento delle radici, ripetendo le stesse considerazioni dell'esempio precedente, posto $a_1 = 0\,;\ \frac{1}{3} = 5$, si trova:

$$\alpha_1 = 5\sqrt[3]{B_1} + 5\sqrt[3]{B_2}$$

$$\alpha_2 = 5\,\varepsilon^2\sqrt[3]{B_1} + 5\,\varepsilon\sqrt[3]{B_2}$$

$$\alpha_3 = 5\,\varepsilon\sqrt[3]{B_1} + 5\,\varepsilon^2\sqrt[3]{B_2}$$

ciascuna delle quali soddisfa alla (2) purchè si faccia:

$$(\sqrt[3]{B_1})^3 = 3\,(1 - \varepsilon^2)\,; \quad (\sqrt[3]{B_2})^3 = 3\,(1 - \varepsilon)$$

$$\sqrt[3]{B_1}\,.\,\sqrt[3]{B_2} = (\alpha_1 + \varepsilon\,\alpha_2 + \varepsilon^2\,\alpha_3)\,(\alpha_1 + \varepsilon^2\,\alpha_2 + \varepsilon\,\alpha_3) = 6.$$

Rimarrebbe ora a compiersi l'estrazione dei radicali cubici in (R), ma per l'estensione del campo che risulta di 343 elementi, l'operazione diviene eccessivamente prolissa.

Bologna, Settembre 1913.