ATTI

DELLA

REALE ACCADEMIA DEI LINCEI

ANNO CCCXVI.

1919

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME XXVIII.

1° Semestre.

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA DEI LINCEI

PROPRIETÀ DEL DOTT. PIO BEFANI

1919

questo appartiene alla retta limite $Cx_1 + C'y_1 + C'' = 0$ del sistema trasformato, poichè, evidentemente

$$\begin{aligned} & Cx_0 + C'Y_0 + C'' = \\ & = [(aC + a'C' + a''C'')\,X + (bC + b'C' + b''C'')\,Y]\,(a''X + b''Y)^{-1} = 0\,; \end{aligned}$$

epperò, ove X, Y siano le componenti d'una forza costante in grandezza e direzione, le X_1, Y_1 saranno le componenti d'una forza centrale col centro nel punto x_0, y_0, proporzionale alla distanza dal centro, ed inversamente proporzionale al cubo della distanza dalla retta $Cx_1 + C'y_1 + C'' = 0$ che passa per esso. Questa retta e quel punto sono, rispettivamente una tangente ed il relativo punto di contatto della conica trasformata della parabola percorsa dal punto mobile sotto l'azione della forza costante. Così, tenuto conto che dalle (10) con la omografia inversa delle (8) si passa di nuovo alle X, Y, nella supposizione che queste siano costanti, si arriva al risultato secondo il quale *a tutti i moti liberi su coniche, per forze centrali col centro in un punto della curva, o per forze di direzione e grandezza costante, si arriva, partendo da uno qualunque di essi, col trasformarlo per mezzo delle omografie di Appell.* E da ciò segue, allora, il carattere d'*invarianza*, per questi tipi di moti liberi, cui si è accennato in fine del n. 1.

5. Tutto quanto abbiamo esposto, in questa e nella precedente Nota, facile è riassumere in un enunciato unico che noi, per brevità, lasciamo a cura del lettore.

Matematica. — *Sul problema dell'irriducibilità di un'equazione in un campo di razionalità generale.* Nota di PACIFICO MAZZONI, presentata dal Socio L. BIANCHI.

1. Nella teoria che Galois pose a fondamento per la risoluzione e lo studio generale delle equazioni algebriche, si presenta questo problema:

Data un'equazione algebrica, priva di radici multiple:

$$f(x) = (x - \alpha_1)\,.\,(x - \alpha_2) \dots (x - \alpha_m) = 0\,, \tag{1}$$

con coefficienti appartenenti a un dato campo di razionalità, vedere se e come si abbassi il suo gruppo di Galois, per l'aggiunta di una data grandezza β_1, radice di un'altra data equazione $f_1(x) = 0$.

Considerata l'equazione $f_2(x) = 0$ risolvente di Galois della proposta (1), è noto che il problema equivale a quest'altro: vedere come si scomponga $f_2(x)$ in fattori irriducibili, dopo l'aggiunta di β_1 al campo di razionalità primitivo.

Noi supporremo che le due equazioni $f(x)=0$ e $f_1(x)=0$ abbiano i coefficienti *numeri razionali*, e che il campo di razionalità da cui si parte sia quello dei numeri razionali, che si indica sempre con $[1]$; invece con $[\beta_1]$ indicheremo il campo ampliato, dopo l'aggiunta di β_1. Sicchè il problema di cui vogliamo occuparci è il seguente, di indole pratica, e che è fondamentale nella teoria di Galois delle equazioni e delle grandezze algebriche:

Dare dei metodi pratici per decomporre un dato polinomio a coefficienti razionali $f(x)$ in fattori irriducibili nel corpo algebrico $[\beta_1]$ (¹).

A questo problema è parso sinora che avesse già risposto il Kronecker, poichè egli lo tratta nel § 4 dei suoi *Grundzüge*, dopo di aver risoluto quello di decomporre $f(x)$ nel corpo $[1]$. Qui ci proponiamo di dimostrare che quel metodo dato dal Kronecker per decomporre $f(x)$ in fattori irriducibili nel corpo $[\beta_1]$ è *inesatto*, e in generale non risolve affatto il problema proposto; sicchè *il detto problema rimaneva, sino ad oggi, per quanto è a nostra conoscenza, insoluto.* Noi qui lo risolveremo, modificando opportunamente lo stesso metodo del Kronecker.

Ricordiamo prima quale è quel metodo. Posto $x=z+\lambda\beta_1$, con λ numero razionale indeterminato, e posto, per brevità, $f(z+\lambda\beta_1)=F(z_1,\beta_1)$, si supponga che

$$F_1(z,\beta_1)\,;\ F_2(z,\beta_1)\,;\ \ldots\,;\ F_t(z,\beta_1) \tag{2}$$

siano i fattori irriducibili cercati di $F(z,\beta_1)$ in $[\beta_1]$. Supposto inoltre $f_1(x)$ già irriducibile in $[1]$, si dicano $\beta_1,\beta_2,\ldots,\beta_n$ le sue radici, coniugate di β_1 rispetto a $[1]$. Si formi il quadro

$$\left\{\begin{array}{l} f(z+\lambda\beta_1)=F(z,\beta_1)=F_1(z,\beta_1)\,.\,F_2(z,\beta_1)\ldots F_t(z,\beta_1)\,;\\ f(z+\lambda\beta_2)=F(z,\beta_2)=F_1(z,\beta_2)\,.\,F_2(z,\beta_2)\ldots F_t(z,\beta_2)\,;\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ f(z+\lambda\beta_n)=F(z,\beta_n)=F_1(z,\beta_n)\,.\,F_2(z,\beta_n)\ldots F_t(z,\beta_n)\,. \end{array}\right. \tag{3}$$

Si eseguisca il prodotto delle funzioni che si trovano in una stessa colonna di questo quadro. Posto

$$\Phi(z)=F(z,\beta_1)\,.\,F(z,\beta_2)\,..\,F(z,\beta_n),\ \text{e}\ \varphi_i(z)=F_i(z,\beta_1)\,.\,F_i(z,\beta_2)\ldots F_i(z,\beta_n),$$

per $i=1,2,\ldots,t$, le funzioni $\Phi(z)$, $\varphi_1(z)$, $\varphi_2(z)$, ..., $\varphi_t(z)$ saranno tutte a coefficienti razionali, che si trovano con dei calcoli di funzioni simmetriche. Si decomponga $\Phi(z)$ in fattori irriducibili in $[1]$: ciò che si sa fare. Per fissar le idee, si supponga infine che $\alpha_1+\lambda\beta_1$ sia una radice di

(¹) Per quanto riguarda le denominazioni che usiamo, seguiamo il Weber, nel suo trattato, *Algèbre supérieure*, 1898.

Per es., ricordiamo che si chiamano *coniugate* le radici d'un'equaz. *irriducibile*.

$F_1(z, \beta_1)$, e che $\theta_1(z)$ sia un fattore irriducibile di $\Phi(z)$ avente quella radice. Giunto a questo punto, il Kronecker così prosegue:

« *Il massimo comune divisore tra* $F(z, \beta_1)$ *e questo fattore* $\theta_1(z)$ *ci* « *dà il polinomio cercato* $F_1(z, \beta_1)$; analogamente per gli altri fattori: « trovati così questi fattori (2) di $f(z + \lambda\beta_1)$, irriducibili in $[\beta_1]$, si tro- « vano poi subito da essi i fattori di $f(x)$ irriducibili in $[\beta_1]$, sostituendo « in essi di nuovo $x - \lambda\beta_1$ al posto di z. È poi da notare che la sostitu- « zione di $z + \lambda\beta_1$ al posto di x è fatta col fine di far comparire effetti- « vamente β_1 nei coefficienti ».

2. Orbene osserviamo che in generale *non è esatto che*, ad esempio, $F_1(z, \beta_1)$ sia *sempre* il massimo comune divisore dei due polinomi $F(z, \beta_1)$ e $\theta_1(z)$: in generale esso è soltanto un loro divisore comune, e per convincerci di ciò, lo vediamo subito con un esempio (1).

Prendiamo un polinomio $G(x)$ *irriducibile* in $[1]$, e diciamo

$$(4) \qquad F_1(z, \beta_1)\ ;\ F_2(z, \beta_1)\ ;\ \dots\ ;\ F_r(z, \beta_1)$$

i suoi fattori irriducibili in $[\beta_1]$, e poniamo che sia $r \geq 3$ (2). Detto poi t un numero ≥ 2, e $< r$, poniamo

$$(5) \qquad F(z, \beta_1) = F_1(z, \beta_1) \,.\, F_2(z, \beta_1) \dots F_t(z, \beta_1),$$

dimodochè $F(z, \beta_1)$ conterrà effettivamente β_1 nei suoi coefficienti, e le radici di $F(z, \beta_1) = 0$ saranno tutte coniugate tra loro rispetto a $[1]$, poichè tali sono quelle di $G(x) = 0$. Poniamo $z = x - \lambda\beta_1$, e consideriamo la funzione

$$F(z, \beta_1) = F(x - \lambda\beta_1, \beta_1).$$

(1) Basta pensare che $F_2(z, \beta_1)$ può avere qualche radice comune, per esempio, con $F_1(z, \beta_2)$, perchè si presenti subito il dubbio sull'affermazione di Kronecker.

(2) Se ne potranno certamente costruire di tali polinomi irriducibili in $[1]$, che in un corpo $[\beta_1]$ si scindano in più di due fattori irriducibili. Basta prendere infatti una equazione razionale in $[1]$:

$$f(z) = (z - \alpha_1) \,.\, (z - \alpha_2) \dots (z - \alpha_m) = 0,$$

avente per gruppo di Galois il gruppo totale sulle sue radici. Considerata la sostituzione

$$S = (\alpha_1, \alpha_2, \dots, \alpha_\mu) \,.\, (\alpha_{\mu+1}, \dots, \alpha_\nu) \,.\, (\alpha_{\nu+1}, \dots, \alpha_m),$$

si indichi con Γ il gruppo generato dalle potenze di S, e si dica β_1 un elemento del corpo $[\alpha_1, \alpha_2, \dots, \alpha_m]$ che abbia per sottogruppo numerico Γ. Rispetto al corpo $[\beta_1]$ il gruppo di Galois di $f(z) = 0$ sarà ridotto a Γ, e $f(z)$ si scinderà nei tre fattori irriducibili

$$(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_\mu)\ ;\ (x - \alpha_{\mu+1}) \dots (x - \alpha_\nu)\ ;\ (x - \alpha_{\nu+1}) \dots (x - \alpha_m).$$

Analogamente se si vogliono più di tre fattori irriducibili.

Partiamo ora da questa funzione $F(x - \lambda\beta_1, \beta_1)$; sostituendo in essa la quantità $z + \lambda\beta_1$ al posto di x, si ottiene precisamente $F(z, \beta_1)$. Questa funzione si decomporrà in fattori irrriducibili secondo la (5); si potrà formare il quadro analogo al (3). Siccome le radici dei varî fattori $F_i(z, \beta_1)$, per $i = 1, 2, \dots t$, sono coniugate rispetto a $[1]$, esse soddisferanno tutte all'equazione irriducibile $\theta_1(z) = 0$, e perciò il prodotto $F(z, \beta_1)$ è contenuto in $\theta_1(z)$: vale a dire che *il massimo comune divisore a* $F(z, \beta_1)$ *e a* $\theta_1(z)$ *sarà* $F(z, \beta_1)$ *stesso*, e non sarà $F_1(z, \beta_1)$: ciò che dimostra che è errata l'affermazione del Kronecker che il detto massimo comune divisore sia proprio il polinomio irriducibile richiesto $F_1(z, \beta_1)$. Dunque col suo metodo non si può decomporre questa funzione $F(z, \beta_1)$ in fattori irriducibili in $[\beta_1]$.

E se $\Psi(x)$ è un polinomio razionale in $[1]$ che contenga $F(x - \lambda\beta_1, \beta_1)$, posto:

$$\Psi(x) = \Psi(z + \lambda\beta_1) = \Theta(z, \beta_1),$$

questo polinomio $\Theta(z, \beta_1)$ conterrà $F(z, \beta_1)$; e siccome per quest'ultimo il metodo di Kronecker non è valido, neppure il polinomio dato $\Psi(x)$ *non si potrà decomporre* con quel metodo in fattori irriducibili in $[\beta_1]$.

3. Ora vogliamo modificare il metodo di Kronecker, in modo da renderlo valido. Dimostriamo che:

Se $f(x)$ è *irriducibile in* $[1]$, *allora il detto metodo è valido, cioè allora il massimo comune divisore tra* $F(z, \beta_1)$ *e* $\theta_1(z)$ *è veramente* $F_1(z, \beta_1)$.

Infatti siano $\alpha_1, \alpha_2, \dots, \alpha_m$ le radici della (1): siccome $z = x + \lambda\beta_1$, le radici di $F(z, \beta_1) = 0$ saranno le seguenti:

$$\alpha_i + \lambda\beta_1, \quad \text{per} \quad i = 1, 2, \dots, m.$$

Se dimostriamo che due di queste radici non sono coniugate rispetto a $[1]$, se non lo sono rispetto a $[\beta_1]$, seguirà che il prodotto

$$F_2(z, \beta_1) . F_3(z, \beta_1) \dots F_t(z, \beta_1)$$

non ha radici comuni col fattore irriducibile $\theta_1(z)$, il quale ammette come radici tutte le coniugate di $\alpha_1 + \lambda\beta_1$ rispetto a $[1]$; cioè seguirà che $F_1(z, \beta_1)$ è il massimo comune divisore tra $F(z, \beta_1)$ e $\theta_1(z)$.

Supponiamo che $\alpha_i + \lambda\beta_1$ sia coniugata di $\alpha_1 + \lambda\beta_1$ rispetto a $[1]$; vi sarà una sostituzione S del corpo normale $[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \dots, \beta_n]$ che porterà $\alpha_1 + \lambda\beta_1$ in $\alpha_i + \lambda\beta_1$. Si vede subito che la S porterà α_1 in α_i e β_1 in β_1 stessa [1]; cioè la S lascerà ferma β_1, e sarà una sostituzione

[1] Se la S porta α_1 in α_1', e β_1 in β_1', deve essere $\alpha'_1 + \lambda\beta'_1 = \alpha_i + \lambda\beta_1$; donde, siccome λ è un numero indeterminato, e le quantità $\alpha_r + \lambda\beta_s$ sono tutte distinte, segue che deve essere $\alpha_1' = \alpha_i$, e $\beta_1' = \beta_1$.

del suddetto corpo normale *rispetto a* $[\beta_1]$; perciò $\alpha_i + \lambda\beta_1$ sarà coniugata di $\alpha_1 + \lambda\beta_1$ *rispetto a* $[\beta_1]$ come campo fondamentale. Dunque $\alpha_i + \lambda\beta_1$ non è coniugata di $\alpha_1 + \lambda\beta_1$ rispetto a $[1]$, se non lo è pure rispetto a $[\beta_1]$, cioè se non appartiene allo stesso fattore $F_1(x, \beta_1)$, cui appartiene l'altra. C. d. d. Dunque se $f(x)$ è irriducibile in $[1]$, allora il massimo comune divisore a $F(z, \beta_1)$ e a $\theta_1(z)$ è proprio il fattore richiesto $F_1(z, \beta_1)$. E siccome ciò che si è detto per il primo fattore $F_1(z, \beta_1)$ vale anche per gli altri, segue il teorema finale:

Se $f(x)$ è irriducibile in $[1]$, allora per esso vale il metodo del Kronecker, per decomporlo in fattori irriducibili in $[\beta_1]$. Se invece $f(x)$ è riducibile in $[1]$, allora basta decomporlo prima in fattori irriducibili in $[1]$, e applicare poscia a ognuno di questi separatamente il metodo del Kronecker.

Abbiamo così risoluto il problema proposto, che il metodo primitivo incompleto del Kronecker non risolveva in generale [1].

Se poi la funzione che si vuole decomporre contiene già β_1, poniamola $f(x, \beta_1)$, allora basta formare il prodotto

$$f(x, \beta_1) \cdot f(x, \beta_2) \ldots f(x, \beta_n),$$

che è una funzione $F(x)$ razionale in $[1]$, e decomporre questa prima in fattori irriducibili in $[1]$, e poi in $[\beta_1]$, e prendere alla fine soltanto quei fattori che sono contenuti in $f(x, \beta_1)$.

Terminiamo, osservando che il Kronecker non pensò affatto al caso che $f(x) = 0$ fosse irriducibile in $[1]$, e il Molk, suo commentatore, neppure; essi si limitarono soltanto a supporla priva di radici multiple, sicchè dovettero ritenere quel metodo valido in ogni caso: il che, si è visto, non è esatto. Qui abbiamo risposto in modo definitivo alla questione.

[1] Il Molk, in una sua Memoria (*Sur une notion* ecc., negli Acta Mathematica, vol. 6, anno 1885), commenta, amplia e precisa molte considerazioni del suo maestro Kronecker. Orbene, anch'egli si lascia sfuggire lo stesso errore, perchè giunge alla stessa conclusione dell'altro, la quale, si è visto, è assurda. Precisamente egli tenta di dimostrare che i fattori irriducibili in $[1]$ di $\Phi(z)$ sono tutti distinti, il che non è affatto vero in generale, nemmeno se $f(x)$ è irriducibile in (1); e da questa premessa errata egli giunge alla conclusione che abbiam vista del maestro (L'errore di ragionamento del Molk è, parmi, a pag. 44).