ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

LUIGI FANTAPPIÈ

Le forme decomponibili coordinate alle classi di ideali nei corpi algebrici

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 1re série, tome 15 (1927), exp. no 2, p. 1-58

<http://www.numdam.org/item?id=ASNSP_1927_1_15__A2_0>

LE FORME DECOMPONIBILI

COORDINATE ALLE CLASSI DI IDEALI

NEI

CORPI ALGEBRICI

TESI DI LAUREA

DI

LUIGI FANTAPPIÈ

DISCUSSA NELL'AULA MAGNA DELLA R. UNIVERSITÀ DI PISA

IL 4 LUGLIO 1922.

Capitolo I.

Generalità. Alcune osservazioni sugli ideali.

1. La teoria delle forme a coefficienti interi razionali deve la sua origine al problema della rappresentazione di un numero intero mediante una forma data. Primo il nostro Lagrangia dette i fondamenti per una teoria generale delle forme quadratiche in una sua memoria letta all'Accademia di Berlino nel 1768; [1] questa particolare teoria fu poi condotta a compimento da Legendre e, principalmente, da Gauss.[2]

A ben maggiore importanza assurse la teoria delle forme dopo le numerose ricerche sui corpi di numeri algebrici, quando, poste le basi, per merito di Kummer, della teoria degli ideali e, per merito di Dirichlet, di quella delle unità si riconobbe che tanto l'una che l'altra di queste due fondamentali teorie potevano esser considerate come teorie d'aritmetica razionale introducendo in considerazione convenienti forme a coefficienti interi razionali.[3]

---

[1] Lagrange. « Sur la solution des problèmes indeterminés du second degré ». Mem. de l'Acad. royale de Berlin. T. XXIII, 1769.

[2] Gauss. « Disquisitiones Arithmeticae », art. 154.

[3] Cfr. Bianchi. « Lezioni sulla teoria dei numeri algebrici e principi d'aritmetica analitica ». Pisa, Spoerri, 1921, §§ 37 e 38.

Ed è di queste particolari forme, coordinate agli ideali di un corpo algebrico, e sempre decomponibili nel prodotto di forme lineari con coefficienti appartenenti al corpo e ai suoi coniugati, che io intendo occuparmi nel presente lavoro.

Dopo alcune osservazioni preliminari, e dopo aver dimostrato alcune semplici proprietà degli ideali di un corpo, passo, nel 2.° capitolo, a studiare alcune proprietà fondamentali del gruppo automorfo G_x, contenente le sostituzioni che trasformano una forma X in se o nell'eguale ed opposta, e del corrispondente gruppo associato Γ_ν delle sostituzioni sugli iperpiani o forme lineari componenti la X medesima.

Nel 3.° capitolo considero poi le proprietà dei gruppi $\Gamma_\nu(K)$ associati alle varie classi K di ideali, le loro mutue relazioni e l'influenza che la struttura dell'equazione irriducibile, le cui radici generano il corpo considerato e i suoi coniugati, ha su di essi.

Infine nel 4.° capitolo esamino la natura delle varie sostituzioni componenti il gruppo G_x, sia di quelle appartenenti al sottogruppo G_e originato dalle unità del corpo sia di quelle di G_x ma non di G_e: e considero poi quel che accade quando ci si voglia limitare a considerare soltanto quelle sostituzioni di G_x che trasformino la X in sè, escludendo quelle che la trasformano nell'eguale e contraria.

2. Prima di passare allo studio delle forme decomponibili coordinate agli ideali di un corpo algebrico $H(\vartheta)$, premettiamo dunque alcune osservazioni generali sugli ideali stessi. E prima di tutto dimostriamo che:

Condizione necessaria e sufficiente perchè un numero ϱ *sia un'unità di un corpo algebrico* $H(\vartheta)$ *di grado* n *è che esistano*

due basi $(\alpha_1, \alpha_2, \ldots \alpha_n)$ *e* $(\beta_1, \beta_2, \ldots \beta_n)$ *di uno stesso ideale A di* $H(\vartheta)$ *per cui sia, per qualunque r da 1 a n*

$$1) \qquad \beta_r = \varrho\, \alpha_r, \quad r = 1, 2, \ldots n,$$

Che la condizione sia necessaria è evidente; se infatti ϱ è una unità del corpo e $(\alpha_1, \alpha_2, \ldots \alpha_n)$ una base dell'ideale A, anche $(\beta_1, \beta_2, \ldots \beta_n) = (\varrho\alpha_1, \varrho\alpha_2, \ldots \varrho\alpha_n)$ sarà un'altra base dello stesso ideale, poichè, essendo ϱ un intero sarà

$$2) \qquad \varrho\, \alpha_i = \sum_k c_{ik}\, \alpha_k \qquad \beta_i = \sum_k c_{ik}\, \alpha_k$$

colle c_{ik} interi razionali, e, essendo anche $\frac{1}{\varrho}$ intero,

$$\frac{1}{\varrho}\, \alpha_k = \sum_i C_{ik}\, \alpha_i$$

$$\alpha_k = \sum_i C_{ik}\, \varrho\, \alpha_i \qquad \alpha_k = \sum_i C_{ik}\, \beta_i$$

colle C_{ik} pure interi razionali; da cui si vede che i determinanti delle c_{ik} e delle C_{ik} sono eguali a ± 1 e che l'unità ϱ soddisferà all'equazione

$$3) \qquad \begin{vmatrix} c_{11} - \varrho, & c_{12}, \ldots . & c_{1n} \\ c_{21}, & c_{22} - \varrho, \ldots . & c_{2n} \\ \cdots\cdots\cdots & & \\ \cdots\cdots\cdots & & \\ \cdots\cdots\cdots & & \\ c_{n1}, & c_{n2}, \ldots . & c_{nn} - \varrho \end{vmatrix} = 0.$$

Passiamo ora a dimostrare che la condizione è sufficiente.

Se $(\alpha_1, \dots \alpha_n)$ e $(\beta_1, \dots \beta_n)$ sono due basi di uno stesso ideale A, soddisfacenti alla condizione 1), si avrà

$$N(A) = \sqrt{\frac{\Delta(\alpha_1, \alpha_2, \dots \alpha_n)}{D}} = \sqrt{\frac{\Delta(\beta_1, \beta_2, \dots \beta_n)}{D}} =$$

$$= \sqrt{\frac{N(\varrho)^2 \Delta(\alpha_1, \alpha_2, \dots \alpha_n)}{D}}$$

dove con D abbiamo indicato il numero fondamentale del corpo; e con $\Delta(\alpha_1, \alpha_2, \dots \alpha_n)$ il discriminante degli n numeri indipendenti $\alpha_1, \alpha_2, \dots \alpha_n$. Segue di qui intanto

$$N(\varrho) = \pm 1 .$$

D'altra parte, costituendo le β_i un'altra base dell'ideale A, sarà

2) $\quad \beta_i = \sum_k c_{ik} \alpha_k \quad$ cioè $\quad \varrho \alpha_i = \sum_k c_{ik} \alpha_k \qquad i = 1, 2, \dots n$

con $|c_{ik}| = \pm 1$; quindi ϱ dovrà soddisfare all'equazione a coefficienti interi e primo coefficiente ± 1

$$\begin{vmatrix} c_{11} - \varrho & c_{12}, \dots & c_{1n} \\ c_{21} & c_{22} - \varrho, \dots & c_{2n} \\ \dots & \dots & \dots \\ c_{n1}, & c_{n2}, \dots & c_{nn} - \varrho \end{vmatrix} = 0$$

e sarà perciò un intero algebrico. Dunque ϱ è un numero del corpo, essendo uguale a $\frac{\beta_r}{\alpha_r}$, intero e di norma ± 1, perciò è una unità.

Da ciò che abbiamo visto segue quindi che la ricerca delle unità di un corpo è perfettamente equivalente alla ricerca di due basi proporzionali di un qualunque ideale del corpo stesso.

3. Dimostriamo immediatamente che

Se dati due corpi $H(\vartheta)$ *e* $H'(\eta)$ *di grado* n *si possono trovare due sistemi di* n *numeri indipendenti,* $(\alpha_1, \alpha_2, \ldots \alpha_n)$ *in* H *e* $(\beta_1, \beta_2, \ldots \beta_n)$ *in* H', *tali che sia*

$$1) \qquad \alpha_i = \sigma \beta_i \qquad i = 1, 2, \ldots n$$

necessariamente i due corpi coincidono, e quindi anche il fattore di proporzionalità $\sigma = \frac{\alpha_i}{\beta_i}$ è un numero del corpo, $H = H'$.

Per far ciò dimostreremo che ogni numero γ di H è in H' e viceversa. Osserviamo perciò che un qualunque numero del corpo H, essendo $\alpha_1, \alpha_2, \ldots \alpha_n$ indipendenti, potrà sempre esprimersi sotto la forma $\sum_i \alpha_i x_i$, colle x_i numeri razionali, e ogni numero del corpo H' sotto la forma $\sum_i \beta_i y_i$, colle y_i pure razionali.

Se allora γ è un qualunque numero di H si avrà

$$2) \qquad \gamma \alpha_k = \sum_1^n{}_i \, a_{ik} \alpha_i \qquad k = 1, 2, \ldots n$$

colle a_{ik} numeri razionali da cui

$$\gamma = \frac{\sum_i a_{ik} \alpha_i}{\alpha_k} .$$

Ma è, per ipotesi, $\alpha_i = \sigma \beta_i$ dunque

$$\gamma = \frac{\sum_i a_{ik} \sigma \beta_i}{\sigma \beta_k} = \frac{\sum_i a_{ik} \beta_i}{\beta_k} ,$$

cioè γ si può esprimere come funzione razionale a coefficienti razionali delle β_i; e quindi risulta un numero del corpo H'. Analogamente si dimostrerebbe che un qualunque numero di H' è anche un numero di H, e in conclusione si ha quindi che H e H' coincidono.

Come caso particolare abbiamo che se si possono trovare due ideali, A in un corpo H (di grado n), e B in un corpo H' (pure di grado n) con basi proporzionali, i due corpi H e H' coincidono e i *due ideali sono quindi equivalenti nel senso ordinario.*

Possiamo perciò adottare per l'equivalenza degli ideali la seguente definizione:

Due ideali A e B contenuti in corpi dello stesso grado si dicono equivalenti quando in essi si possono trovare due basi proporzionali, senza bisogno di aggiungere che debbano appartenere al medesimo corpo, essendo ciò una conseguenza della definizione stessa.

4. Ricordiamo infine che se A è un ideale in un corpo $H(\vartheta)$ e $\alpha_1 \ldots . \alpha_n$ una sua base, i suoi numeri sono rappresentati dall'espressione

$$h_1 \alpha_1 + h_2 \alpha_2 + \ldots . . + h_n \alpha_n$$

in cui le h_i prendano valori interi razionali qualunque e che se in questa espressione $\sum_1^n{}_i \, h_i \alpha_i(\vartheta)$ sostituiamo a ϑ il numero coniugato $\vartheta^{(s)}$ si ha un altro insieme di numeri, coniugati di quelli dell'ideale A, i quali formano un nuovo ideale $A^{(s)}$, che diremo *coniugato* di A, nel corpo coniugato $H^{(s)}$.[1] Inoltre i numeri $\alpha_1^{(s)}, \alpha_2^{(s)}, \ldots . \alpha_n^{(s)}$ formano ancora una base dell'ideale $A^{(s)}$ che diremo coniugata di quella $(\alpha_1, \alpha_2, \ldots \alpha_n)$ dell'ideale A; e sarà $N(A^{(s)}) = N(A)$.

---

[1] Cfr. ad es. HILBERT. «Jahresbericht des Deutschen Mathematiker Vereinigung». Berlino, 1897. Parte I, cap. III.

Capitolo II.

Le forme decomponibili coordinate agli ideali. - Gruppo automorfo G_X di una forma e gruppo $\Gamma_\nu(K)$ associato a una classe K di ideali.

5. Consideriamo un ideale $A = (\alpha_1, \alpha_2, \ldots \alpha_n)$ di un corpo $H(\vartheta)$ e costruiamo la forma

$$1) \qquad X = \frac{1}{N(A)} \prod_1^n (\alpha_1^{(s)} x_1 + \alpha_2^{(s)} x_2 + \ldots + \alpha_n^{(s)} x_n)$$

che diremo coordinata all'ideale A mediante la base α_1, $\alpha_2, \ldots \alpha_n$; essa ha coefficienti interi razionali[1] ed è coordinata anche, cambiata eventualmente di segno, a tutti gli ideali della stessa classe mediante basi proporzionali; inoltre il suo discriminante è sempre uguale al numero fondamentale D del corpo.[2] Una forma X coordinata a un ideale A mediante una certa base, è coordinata evidentemente anche a tutti gli ideali coniugati $A^{(s)}$ mediante le rispettive basi coniugate. Se alle x_i si danno valori interi essa rappresenta, come è noto, cambiata, se occorre, di segno, tutti e soli i numeri che sono norme di ideali M moltiplicatori di A ed è quindi primi-

[1] Bianchi. Op. cit., § 37.

[2] Cfr. Bianchi. Op. cit. e Dedekind. « Sulla teoria dei numeri interi algebrici ». Suppl. XI della Teoria dei numeri del Dirichlet. Venezia, 1881, § 176.

tiva in senso stretto,[1] poichè questi numeri non hanno alcun fattore comune.[2] Considerando poi le $x_1, x_2, \ldots x_n$ come coordinate di un punto di un S_n, diremo *associato* all'ideale A mediante la base $(\alpha_1, \alpha_2, \ldots \alpha_n)$ l'iperpiano.

$$2) \qquad \alpha_1 x_1 + \alpha_2 x_2 + \ldots . \alpha_n x_n = 0$$

passante per l'origine, ed *equivalenti* due iperpiani associati a due ideali equivalenti, e quindi trasformabili l'uno nell'altro mediante una sostituzione lineare intera a coefficienti interi razionali sulle coordinate, di determinante ± 1 (la sostituzione trasposta di quella con cui si passa dalla base di uno degli ideali a un'altra proporzionale alla base dell'altro). È da notare infatti che un iperpiano associato ad A mediante una certa base, è anche associato a tutti gli equivalenti di A mediante basi proporzionali all'originaria.

Due iperpiani, associati a due ideali A e $A^{(s)}$ rispettivamente mediante basi coniugate, li diremo essi stessi *coniugati.*

6. L'equazione

$$1) \qquad X = 0$$

ci rappresenta quindi un'ipersuperficie d'ordine n che, a causa della 1) del N precedente si spezza in n iperpiani

---

[1] FURTWÄNGLER nella memoria «Punktgitter und Idealtheorie» (Math Ann. — 82 Bd., 3-4 Heft. 1921) chiama «ganz primitiv» queste forme che io dico primitive in senso stretto in contrapposto ad altre forme decomponibili dei corpi algebrici che, pure essendo a coefficienti interi razionali senza fattori comuni, rappresentano però solo numeri divisibili per un certo numero, forme che egli chiama «halbprimitiv» (semiprimitive).

[2] BIANCHI. Op. cit., § 37.

coniugati *diversi* poichè il determinante

$$\begin{vmatrix} \alpha_1^{(1)}, \alpha_2^{(1)}, \ldots\ldots \alpha_n^{(1)} \\ \ldots\ldots\ldots\ldots \\ \alpha_1^{(s)}, \alpha_2^{(s)}, \ldots\ldots \alpha_n^{(s)} \\ \ldots\ldots\ldots\ldots \end{vmatrix} = \sqrt{\Delta(\alpha_1, \alpha_2, \ldots \alpha_r)} = N(A)\sqrt{D}$$

è diverso da 0. Se facciamo una sostituzione

$$2) \qquad x_i = \sum_1^n{}_k \, c_{ik}\, y_k \qquad i = 1, 2, \ldots n$$

con determinante $|c_{ik}| = \pm 1$, la forma X si trasforma in un'altra Y

$$Y = \frac{1}{N(A)} \prod_1^n{}_s \, (\beta_1^{(s)} y_1 + \beta_2^{(s)} y_2 + \ldots\ldots + \beta_n^{(s)} y_n)$$

ove

$$\beta_k^s = \sum_i c_{ik}\, \alpha_i^{(s)}$$

che diremo *equivalente* alla primitiva, poichè rappresenta i medesimi interi di X solo che per le y_k si sostituiscano i valori che si ottengono dalle x_i mediante le 2). La forma Y è evidentemente coordinata all'ideale A mediante la base $(\beta_1, \beta_2, \ldots \beta_n)$ ed è quindi anch'essa primitiva in senso stretto

L'equazione

$$3) \qquad Y = 0$$

rappresenterà un ipersuperficie d'ordine n, composta pure di n iperpiani coniugati, diversa, in generale, da quella data dall'equazione 1). Può però accadere che, per particolari sostituzioni 2), queste due ipersuperficie coincidano, cioè

$$Y(x_i) = k X(x_i)$$

Dimostriamo che allora necessariamente $k = \pm 1$: Dovendo pel principio d'identità essere uguali i coefficienti dei ter-

mini simili nei due membri, ed essendo le due forme a coefficienti interi razionali, dovrà intanto k essere razionale, $k = \frac{p}{q}$, con p e q interi senza fattori comuni, quindi

$$q\,Y(x_i) = p\,X(x_i)\,.$$

Ma allora q dovrà dividere tutti i coefficienti della forma del secondo membro, e, essendo primo con p, dovrà dividere tutti i coefficienti della X, ma questa è primitiva, quindi $q = \pm 1$; analogamente, essendo anche Y primitiva, $p = \pm 1$, da cui $k = \pm 1$. In questo caso le due forme equivalenti X e Y sono uguali, oppure uguali e di segno contrario; noi però almeno fino ad avvertimento contrario, le considereremo sempre come una stessa, e diremo che la sostituzione 2) trasforma in sè la forma X.

Dimostriamo ora più generalmente che *due forme* X e Y coordinate agli ideali A e B mediante le basi $\alpha_1, \alpha_2, \ldots \alpha_n$, $\beta_1, \beta_2, \ldots \beta_n$ rispettivamente, *tali che* le $X = 0$ e $Y = 0$ *abbiano a comune uno stesso iperpiano, necessariamente coincidono.* Potremo sempre supporre, cambiando, se occorre, le denominazioni, che l'iperpiano comune sia dato da

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots\ldots + \alpha_n x_n = 0$$

per la prima forma $X = 0$, e da

$$\beta_1 x_1 + \beta_2 x_2 + \ldots\ldots + \beta_n x_n = 0.$$

per la $Y = 0$; cioè

$$\alpha_i = \sigma\,\beta_i \qquad i = 1, 2, \ldots n\,.$$

Di qui segue allora (n. 3) che i due ideali A e B apparterranno allo stesso corpo, non solo, ma saranno anche equivalenti; ed essendo la base $(\beta_1 \ldots \beta_n)$ di B proporzionale alla base $(\alpha_1 \ldots \alpha_n)$ di A, le due forme X e Y coordi-

nate a questi due ideali equivalenti mediante basi proporzionali dovranno essere uguali (cfr. n. 5) a meno, naturalmente, del segno.

7. Passiamo ora a considerare le sostituzioni

1) $\qquad x_i = \sum_k c_{ik}\, y_k \qquad i = 1, 2 \ldots . n \qquad |c_{ik}| = \pm 1$

che trasformano in sè una forma

$$X = \frac{1}{N(A)} \Pi_s (\alpha_1^{(s)} x_1 + \ldots . + \alpha_n^{(s)} x_n).$$

Che esistano sempre di tali sostituzioni è evidente; se infatti $\varepsilon^{(s)}$ indica un'unità del corpo $H(\vartheta^{s})$ si ha

2) $\qquad \varepsilon^{(s)}\, \alpha_k^{(s)} = \sum_i e_{ik}\, \alpha_i^{(s)} \qquad k = 1, 2, \ldots n$

colle e_{ik} interi razionali e $|e_{ik}| = \pm 1$. Facendo ora la sostituzione trasposta della 2)

3) $\qquad x_i = \sum_k e_{ik}\, y_k$

la forma $X(x_i)$ si trasforma nell'altra

$$Y(y) = \frac{1}{N(A)} \prod_1^n{}_s (\sum_i \alpha_i^{(s)} \sum_k e_{ik}\, y_k) =$$

$$= \frac{1}{N(A)} \Pi_s (\sum_k y_k \sum_i e_{ik}\, \alpha_i^{(s)})$$

e per le 2)

$$Y(y) = \frac{1}{N(A)} \Pi_s\, \varepsilon^{(s)} (\sum_k \alpha_k^{(s)}\, y_k) =$$

$$= \frac{1}{N(A)} N(\varepsilon)\, \Pi_s (\sum_k \alpha_k^{(s)}\, y_k) = \pm \frac{1}{N(A)} X(y)$$

poichè $N(\varepsilon) = \pm 1$. Siccome in ogni corpo esistono sempre delle unità (almeno $+1$ e -1), anzi, tranne il caso del corpo razionale e dei corpi quadratici immaginari, ne esistono infinite, e siccome ogni sostituzione 3) individua perfettamente la $\varepsilon^{(s)}$ corrispondente

$$\varepsilon^{(s)} = \frac{\sum_i e_{ij}\ \alpha_i^{(s)}}{\alpha_k^{(s)}}$$

si ha quindi in generale, che *esistono infinite sostituzioni* 3) che trasformano in se la X.

Consideriamo tutte le sostituzioni 1) che trasformano in se la X; è chiaro che formano un *gruppo,* che chiameremo il *gruppo automorfo* G_X della forma; esso *contiene evidentemente la sostituzione identica* che indicheremo con *1* e *insieme a ogni sostituzione* T *la sua inversa* T^{-1}; se infatti T lascia la X in se, siccome anche $1 = TT^{-1}$ lascia la X in sè anche T^{-1} dovrà lasciare la X in sè e apparterrà quindi al gruppo automorfo.

A questo gruppo apparterranno tutte le sostituzioni del tipo 3), provenienti dalle unità del corpo, le quali formeranno evidentemente un *sottogruppo* G_e (in generale effettivamente diverso da G_X) *di sostituzioni commutabili* (abeliano); se infatti S è una costituzione 3) corrispondente all'unità $\varepsilon^{(s)}$ e T un'altra sostituzione corrispondente all'unità $\eta^{(s)}$, il prodotto ST corrisponderà ancora all'unità $\varepsilon^{(s)}\eta^{(s)}$ e TS a $\eta^{(s)}\varepsilon^{(s)}$, quindi, essendo $\varepsilon^{(s)}\eta^{(s)} = \eta^{(s)}\varepsilon^{(s)}$ e risultando ogni sostituzione perfettamente individuata mediante le 2) dall'unità corrispondente, si avrà sempre $ST = TS$.

8. Osserviamo poi che non solo la forma X individua il sottogruppo G_e delle unità, ma anche viceversa, nei corpi

in cui esistano unità primitive [1] (cioè d'ordine n e bastanti quindi a generare da sole il corpo), il *sotto gruppo* G_e *delle unità individua perfettamente la forma* X *corrispondente, cioè non possono esistere due forme* X e Y diverse, coordinate a due ideali dello stesso corpo o anche di corpi diversi, *che ammettano il medesimo sotto gruppo* G_e.

Prendiamo infattti una E di queste sostituzioni 3) di G_e corrispondente a una unità primitiva $\varepsilon^{(s)}$; si avrà

$$D(\varepsilon^{(s)}) = \begin{vmatrix} e_{11} - \varepsilon^{(s)}, & e_{12}, \ldots . & e_{1n} \\ e_{21}, & e_{22} - \varepsilon^{(s)}, \ldots . & e_{2n} \\ \ldots\ldots\ldots\ldots & & \\ \ldots\ldots\ldots\ldots & & \\ e_{1n}, & e_{n2}, \ldots . & e_{nn} - \varepsilon^{(s)} \end{vmatrix} = 0$$

e questa equazione di grado n, essendo $\varepsilon^{s)}$ di grado n, avrà le n radici tutte diverse ed eguali precisamente a $\varepsilon^{(1)}, \varepsilon^{2)}, \ldots \varepsilon^{n)}$.

Nel determinante $D(\varepsilon^{s)})$ non potranno perciò annullarsi tutti i minori d'ordine $n-1$, poichè altrimenti sarebbe anche $D'(\varepsilon^{(s)}) = 0$ e quindi $\varepsilon^{(s)}$ radice almeno doppia. Siano ora X e Y due forme decomponibili, coordinate a certi ideali $A = (\alpha_1, \alpha_2, \ldots \alpha_n)$ e $B = (\beta_1, \beta_2, \ldots \beta_n)$ rispettivamente, che abbiano lo stesso sottogrnppo G_e delle unità e quindi ammettano anche la medesima sostituzione E di G_e. Conformemente alle 2) del numero precedente dovrà aversi, per

---

[1] Tale è il caso, del resto molto generale, *che fra i corpi coniugati ne esista almeno uno reale* (come per es. se n è dispari). Per la dimostrazione vedi la memoria del prof. BIANCHI. « Sugli ideali primari assoluti in un corpo algebrico », pag. 15. Journal de Mathem. pures et appl., 1922.

due convenienti ideali coniugati $A^{(s)}$ e $B^{(s)}$

$$\varepsilon^{(s)}\,\alpha_k^{(s)} = \sum_i e_{ik}\,\alpha_i^{(s)}$$

e anche $k = 1, 2, \ldots n$

$$\varepsilon^{(s)}\,\beta_k^{(s)} = \sum_i e_{ik}\,\beta_i^{(s)}$$

cioè

$$\begin{cases} (e_{11} - \varepsilon^{(s)})\,\alpha_1^{(s)} + e_{12}\,\alpha_2^{(s)} + \ldots\ldots + e_{1n}\,\alpha_n^{(s)} = 0 \\ e_{21}\,\alpha_1^{(s)} + (e_{22} - \varepsilon^{(s)})\,\alpha_2^{(s)} + \ldots\ldots + e_{2n}\,\alpha_n^{(s)} = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ e_{n1}\,\alpha_1^{(s)} + e_{n2}\,\alpha_2^{(s)} + \ldots\ldots + (e_{nn} - \varepsilon^{(s)})\,\alpha_n^{(s)} = 0 \end{cases}$$

$$\begin{cases} (e_{11} - \varepsilon^{(s)})\,\beta_1^{(s)} + e_{12}\,\beta_2^{(s)} + \ldots\ldots + e_{1n}\,\beta_n^{(s)} = 0 \\ e_{21}\,\beta_1^{(s)} + (e_{22} - \varepsilon^{(s)})\,\beta_2^{(s)} + \ldots\ldots + e_{2n}\,\beta_n^{(s)} = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ e_{n1}\,\beta_1^{(s)} + e_{n2}\,\beta_2^{(s)} + \ldots\ldots + (e_{nn} - \varepsilon^{(s)})\,\beta_n^{(s)} = 0 \end{cases}$$

da cui si vede che $\alpha_1^{(s)}, \alpha_2^{(s)}, \ldots \alpha_n^{(s)}$, e $\beta_1^{(s)}, \beta_2^{(s)}, \ldots \beta_n^{(s)}$ sono due sistemi di soluzioni di un medesimo sistema lineare omogeneo con determinante $D(\varepsilon^{(s)}) = 0$ ma di caratteristica $n-1$. Ma allora questi due sistemi di soluzioni dovranno essere proporzionali, cioè $\beta_i^{(s)} = \sigma\,\alpha_i^{(s)}$; quindi i due ideali $A^{(s)}$ e $B^{(s)}$ apparterranno allo stesso corpo (cfr. n. 3) e saranno equivalenti mediante basi proporzionali, e perciò le due forme X e Y coincideranno (v. n. 5).

Dalla dimostrazione fatta si vede di più che *basta soltanto che due forme X e Y abbiano a comune una sola sostituzione E, corrispondente a una unità di grado n, perchè esse coincidano.*

9. Osserviamo che se T è una sostituzione unimodulare *non* appartenente al gruppo automorfo G_X della forma X, essa trasformerà la X in un'altra forma Y certamente diversa dalla primitiva ma ad essa equivalente. Se allora S è una qualunque sostituzione di G_X, la sostituzione trasformata $T^{-1} S T = S'$ lascerà evidentemente la Y in sè e apparterrà quindi al gruppo automorfo G_Y della forma Y, e viceversa, se S' è una sostituzione di G_Y, $S = T S' T^{-1}$ sarà una sostituzione di G_X. Si ha dunque che *se Y è una forma equivalente a X ed è ottenuta da questa mediante una certa sostituzione T sulle variabili, il gruppo automorfo G_Y è il trasformato, mediante T, del gruppo automorfo G_X appartenente alla forma primitiva*: $G_Y = T^{-1} G_X T$.

10. Indichiamo per brevità con $u^{(s)}$ la forma lineare

1) $$u^{(s)} = \sum_i \alpha_i^{(s)} x_i = u^{(s)}(x)$$

che diremo associata alla base $\alpha_1^{(s)}, \alpha_2^{(s)}, \ldots \alpha_n^{(s)}$ dell'ideale $A^{(s)}$

2) $$X = \frac{1}{N(A)} u^{(1)} u^{(2)} \ldots u^{(n)}.$$

Se eseguiamo la sostituzione

3) $$x_i = \sum_k c_{ik} y_k$$

la forma $u^{(s)} x$ diventerà

4) $$u^{(s)}(x) = \sum_i \alpha_i^{(s)} x_i = \sum_{ik} \alpha_i^{(s)} c_{ik} y_k = \sum_k y_k \sum_i c_{ik} \alpha_i^{(s)} =$$
$$= \sum_k \beta_k^{(s)} y_k = \overline{u}^{(s)}(y)$$

e le

5) $$\beta_k^{(s)} = \sum_i c_{ik} \alpha_i^{(s)} \qquad k = 1, 2, \ldots n$$

formeranno un'altra base dell'ideale $A^{(s)}$. Se vogliamo che la 3) trasformi la X in se bisognerà evidentemente che sia

$$6) \qquad u^{(1)}(x)\,u^{(2)}(x)\ldots\ldots u^{(n)}(x) = \pm\,\overline{u}^{(1)}(x)\,\overline{u}^{(2)}(x)\ldots\ldots\overline{u}^{(n)}(x)$$

cioè le nuove forme lineari $\overline{u}^{(s)}$, che eguagliate a 0 debbono dare gli stessi iperpiani della $X=0$, dovranno coincidere, a meno dell'ordine e di un fattore di proporzionalità, colle antiche $u^{s)}$, e dovrà quindi essere

$$7) \qquad \overline{u}^{(s)} = \sigma_s\, u(t_s)$$

e inoltre, a causa della 6)

$$8) \qquad \sigma_1\,\sigma_2\ldots\ldots\,\sigma_n = \pm\,1\,.^{1}$$

Si vede dunque che *a ogni sostituzione* 3) *del gruppo automorfo* G_X *corrisponde una sostituzione sulle n forme lineari* $u^{(s)}$ data dalla 7) $S = \begin{pmatrix} u^{(t_s)} \\ \overline{u}^{(s)} \end{pmatrix}$.

---

[1] Osserviamo che dalle 7) segue $\beta_k^{(s)} = \sigma_s\,\alpha_k^{(t_s)}$ $(k = 1, 2, \ldots n)$ quindi $\prod_1^n{}_s\,\beta_k^{(s)} = \sigma_1\,\sigma_2\ldots\,\sigma_n \prod_1^n{}_s\,\alpha_k^{(t_s)}$; cioè $N(\beta_k^{(s)}) = \sigma_1\,\sigma_2\ldots\,\sigma_n\,N(\alpha_k^{(s)})$, e per la 8), $N(\beta_k^{(s)}) = \pm\,N(\alpha_k^{(s)})$. Dalle 5) segue poi

$$N(\beta_k^{(s)}) = \Pi_s(\textstyle\sum_i \alpha_i^{(s)}\,c_{ik}) = N(A)\,\overline{X}$$

dove abbiamo indicato con $\overline{X}$ il valore che assume la X quando in essa si sostituiscano alle $x_1, x_2, \ldots x_n$ i numeri $c_{1k}, c_{2k}, \ldots c_{nk}$. Vediamo così quale è il significato dei coefficienti c_{ik} delle sostituzioni di G_X; essi sono infatti (per $i = 1, 2, \ldots n$ e k costante) quei numeri che sostituiti in X rappresentano $\dfrac{N(\beta_k^{(s)})}{N(A)}$ cioè la norma di quell'ideale M_k moltiplicatore di A per cui $A\,M_k = (\beta_k^{(s)})$, cambiata eventualmente di segno.

Se poi a una sostituzione T del gruppo automorfo corrisponde una certa sostituzione S sugli n iperpiani della $X=0$, e a un'altra sostituzione T', pure del gruppo automorfo, un'altra sostituzione S', è chiaro che al prodotto $T\,T'$ corrisponderà la sostituzione SS'. Si ha dunque che *le sostituzioni S sugli n iperpiani della $X=0$, corrispondenti alle sostituzioni del gruppo automorfo, formano un gruppo di sostituzioni* Γ_ν *in isomorfismo* (generalmente *meriedrico,* essendo Γ_ν d'ordine finito e invece, per lo più, G_X d'ordine infinito, cfr. n. 7) *col gruppo automorfo stesso.*

Se dalla forma X passiamo a un altra forma equivalente Y mediante una sostituzione unimodulare U il nuovo gruppo Γ'_ν sarà evidentemente in *isomorfismo oloedrico* con Γ_ν poichè mediante la U ogni forma $u^{(s)}(x)$ si trasforma in un altra $v^{(s)}(y)$ e se T porta $u^{(s)}$ in $u^{(t\,s)}$, $U^{-1}TU$ porterà $v^{(s)}$ in $v^{(t\,s)}$ e viceversa. Nella sostituzione $S=\begin{pmatrix} u^{(t\,s)} \\ u^{(s)} \end{pmatrix}$, corrispondente a T in Γ_ν, basterà dunque cambiare semplicemente il nome delle lettere per avere la nuova sostituzione $S'=\begin{pmatrix} v^{(t\,s)} \\ v^{(s)} \end{pmatrix}$, corrispondente in Γ'_ν alla $U^{-1}TU$ del nuovo gruppo automorfo G_y.

Possiamo dunque dire che *a ogni classe K di ideali equivalenti,* essendo associata una classe di forme pure equivalenti, *è coordinato un unico gruppo* Γ_ν *di sostituzioni,* che diremo *associato* alla classe K e indicheremo spesso con $\Gamma_\nu(K)$.

11. Supponiamo di avere ora una sostituzione 3) (n. precedente) del gruppo automorfo che lasci fisso uno degli iperpiani $X=0$, sia cioè, p. es.

$$\overline{u}^{(s)} = \sigma_s\, u^{(s)}.$$

Si avrà identicamente, qualunque siano le x_k

$$\Sigma_k \beta_k^{(s)} x_k = \sigma_s \Sigma_k \alpha_k^{(s)} x_k$$

cioè

1) $$\beta_k^{(s)} = \sigma_s \alpha_k^{(s)} \qquad k = 1, 2, \ldots n .$$

Ma ricordiamo che $\alpha_1^{(s)}, \alpha_2^{(s)}, \ldots \alpha_n^{(s)}$ e $\beta_1^{(s)}, \beta_2^{(s)}, \ldots \beta_n^{(s)}$ sono due basi di uno stesso ideale $A^{(s)}$; d'altra parte sono proporzionali per il fattore σ_s, dunque (n. 2) σ_s *è un unità del corpo* $H^{s)}$. Dalle 1) e dalle 5) del numero precedente si ha poi

$$\sigma_s \alpha_k^{(s)} = \Sigma_i c_{ik} \alpha_i^{(s)} \qquad k = 1, 2, \ldots n$$

da cui risulta che la considerata sostituzione 3) di G_x appartiene al sottogruppo G_e e corrisponde precisamente all'unità σ_s del corpo $H^{(s)}$. *Se dunque una sostituzione di* G_x *lascia fisso un iperpiano della* $X = 0$, *appartiene al sottogruppo* G_e. Viceversa è chiaro che *una qualunque sostituzione*

2) $$x_i = \Sigma_k e_{ik} y_k$$

di G_e, *corrispondente a un' unità* $\varepsilon^{(s)}$ del corpo $H^{(s)}$ *lascia fissi tutti gli iperpiani della* $X = 0$: si ha infatti, per qualunque $s = 1, 2, \ldots n$

$$\varepsilon^{(s)} \alpha_k^{(s)} = \Sigma_i e_{ik} \alpha_i^{(s)} \qquad k = 1, 2, \ldots n$$

da cui

$$\varepsilon^{(s)} \Sigma_k \alpha_k^{(s)} y_k = \Sigma_{ik} e_{ik} \alpha_i^{(s)} y_k$$

e per le 2)

$$\varepsilon^{(s)} \Sigma_k \alpha_k^{(s)} y_k = \Sigma_i \alpha_i^{(s)} x_i$$

e ponendo

$$u^{(s)} = \Sigma_i \alpha_i^{(s)} x_i \qquad \overline{u^{(s)}} = \Sigma_i \varepsilon_i^{(s)} \alpha_i^{(s)} x_i$$

si ha

$$\overline{u}^{(s)} = \varepsilon^{(s)} u^{(s)} \qquad s = 1, 2, \ldots n.$$

Di qui segue che le *sostituzioni S sugli iperpiani della* $X = 0$, *corrispondente alle sostituzioni del gruppo automorfo, sono tali che, se lasciano fisso un iperpiano, debbono lasciar fissi anche tutti gli altri iperpiani e ridursi quindi all'identità. Inoltre l'insieme delle sostituzioni di* G_x *corrispondente all'identità di* Γ_y *è costituito precisamente dal sottogruppo* G_e delle unità, il quale sarà perciò *invariante* in G_x, infatti la $T^{-1}ET$ (T di G_x e E di G_e) scambia gli iperpiani secondo la sostituzione $S^{-1}S = 1$ (se S corrisponde a T in Γ_y) ed è perciò ancora una sostituzione di G_e.

12. Consideriamo una sostituzione S di $\Gamma_y(K)$ decomposta nei vari cicli che la costituiscono, e sia τ il minimo periodo di questi, posseduto p. es., dal ciclo $(u^{(1)}, u^{(2)}, \ldots u^{(\tau)})$; la potenza S^τ lascerà allora fissi tutti gli iperpiani $u^{(1)} = 0, \ldots u^{(\tau)} = 0$ e dovrà perciò, per quel che abbiamo visto, ridursi all'identità. D'altra parte è noto che il periodo di una sostituzione è uguale al minimo comune multiplo dei periodi dei vari cicli che la compongono,[1] dunque tutti i cicli della S dovranno avere dei periodi non inferiori a τ (essendo questo il minimo per ipotesi) e divisori di τ quindi necessariamente proprio uguali a τ. Si ha cioè che le *sostituzioni S del gruppo* Γ_y *godono della proprietà di decomporsi in tanti cicli tutti di un egual numero* τ *di lettere;* ed essendo queste in numero di n, *dovrà necessariamente essere* τ *un divisore di* n.

---

[1] Cfr. L. BIANCHI. «Lezioni sulla teoria dei gruppi di sostituzioni». Pisa, Spoerri, 1900, § 3, pag. 10.

Siano poi S e S' due sostituzioni di Γ_ν, che portino ambedue uno stesso iperpiano $u^{(s)}=0$ in un altro $u^{(t_s)}=0$; la sostituzione SS'^{-1} lascierà allora fisso l'iperpiano $u^{(s)}=0$ e dovrà perciò ridursi all'identità, $SS'^{-1}=1$, da cui $S=S'$. Si ha dunque che, *se due sostituzioni* di Γ_ν *portano ambedue uno stesso iperpiano in un altro, coincidono,* o, ciò che è lo stesso, *ogni sostituzione di* Γ_ν *è perfettamente individuata quando si conosca in che posto essa porti una certa lettera.*

Potremo allora individuare le sostituzioni di Γ_ν indicando in quale lettera $u^{(s)}$ esse portino un'altra lettera fissa, p. es. la $u^{(1)}$. Siccome le $u^{(s)}$ diverse sono n si ha che *l'ordine* ν *del gruppo* Γ_ν *è sempre minore o uguale a* n, poichè due sostituzioni che portino la $u^{(1)}$ nella stessa $u^{(s)}$, dovranno, per quel che si è visto, coincidere.

13. Torniamo ora alle sostituzioni del gruppo automorfo G_x. Se G_e non esaurisce G_x, prendiamo una sostituzione T_2 di G_x fuori di G_e a cui corrisponda una sostituzione S_2 in Γ_ν, e consideriamo l'insieme di tutte le sostituzioni ET_2 con E qualunque in G_e, insieme che indicheremo con $G_e T_2$; se G_e e $G_e T_2$ non esauriscono G_x, prendiamo un'altra sostituzione T_3 fuori di G_e e $G_e T_2$ a cui corrisponda in Γ_ν la S_3, e costruiamo un altro insieme $G_e T_3$, e così via. Verremo così a distribuire le sostituzioni di G_x in tanti insiemi

$$G_e$$
$$G_e\ T_2$$
$$G_e\ T_3$$
$$\ldots\ldots$$
$$G_e\ T_\mu$$
$$\ldots\ldots$$

tali che ognuno (p. es. $G_e T_\mu$) contiene sostituzioni diverse da quelle di tutti gli altri che però scambiano tutte gli iperpiani della X secondo una stessa sostituzione S_μ di Γ_ν. E viceversa, se una sostituzione U di G_x scambia gli iperpiani della $X=0$ secondo la sostituzione S_μ essa appartiene necessariamente all'insieme $G_e T_\mu$. Infatti la $U T_\mu^{-1}$ scambierà gli iperpiani della $X=0$ secondo la sostituzione $S_\mu S_\mu^{-1}=1$ e sarà perciò una sostituzione E di G_e (n. 11), $U T_\mu^{-1}=E$ da cui $U=E T_\mu$. L'insieme $G_e T_\mu$ viene dunque a esser caratterizzato dal fatto di esser formato da *tutte* e *sole* le sostituzioni di G_x che scambiano gli iperpiani della $X=0$ secondo la sostituzione S_μ di Γ_ν. Viene così a porsi una corrispondenza biunivoca tra questi insiemi e le sosiituzioni di Γ_ν, da cui segue che il numero di questi insiemi è pure uguale a ν o, in altre parole.

L'indice del sottogruppo G_e in G_x è finito ed uguale precisamente all'ordine ν del gruppo Γ_ν delle sostituzioni sugli iperpiani della $X=0$.

14. Consideriamo ora una sostituzione T di G_x che scambi gli iperpiani della $X=0$ secondo una certa sostituzione $S=\begin{pmatrix} u^{(t_s)} \\ u^{(s)} \end{pmatrix}$ di Γ_ν, per cui cioè diventi (7) del n. 10

1) $$\overline{u}^{(s)} = \sigma_s u^{(t_s)}.$$

La nuova base $(\beta_1^{(s)}, \ldots \beta_n^{(s)})$ dell'ideale $A^{(s)}$ (con $\beta_k^{(s)} = \sum_i c_{ik} \alpha_i^{(s)}$, cfr. n. 10) risulta dunque proporzionale alla base antica $(\alpha_1^{(t_s)}, \ldots . \alpha_n^{(t_s)})$ dell'ideale coniugato $A^{(t_s)}$, quindi (n. 3) *i due ideali coniugati $A^{(s)}$ e $A^{(t_s)}$ dovranno appartenere al medesimo corpo ed essere equivalenti.* Ma anche viceversa, se supponiamo che i due ideali $A^{(s)}$ e $A^{(t_s)}$ siano equivalenti,

dovrà bene esistere una base $(\beta_1^{(s)}, \beta_2^{(s)}, \ldots \beta_n^{(s)})$ di $A^{(s)}$ proporzionale per un fattore σ_s alla base $(\alpha_1^{(t_s)}, , \ldots \alpha_n^{(t_s)})$ di $A^{(t_s)}$, la qual base delle β_k si esprimerà per l'antica mediante una certa sostituzione a coefficienti interi razionali

$$2) \qquad \beta_k^{(s)} = \sum_i c_{ik}\, \alpha_i^{(s)}$$

con $|c_{ik}| = \pm 1$. Se allora noi facciamo sulle x_i la sostituzione unimodulare trasposta della 2)

$$3) \qquad x_i = \sum_k c_{ik}\, y_k ,$$

questa trasformerà la forma X in una certa altra Y equivalente tale però che la $Y = 0$ avrà un iperpiano comune colla $X = 0$, essendo nelle nostre ipotesi

$$u^{(s)} = \sigma_s\, u^{(t_s)} .$$

Ma allora (n. 6) la Y dovrà coincidere colla X e la 3) sarà quindi una sostituzione del gruppo automorfo G_X. *Se dunque due ideali coniugati $A^{(s)}$ e $A^{(t_s)}$ sono equivalenti esiste sempre una sostituzione 3) di G_X che porta la forma $u^{(s)}$ nella $u^{(t_s)}$* e quindi anche una sostituzione di Γ_v sugli iperpiani della $X = 0$ che porta un iperpiano $u^{(s)} = 0$ in un'altro qualsiasi equivalente $u^{(t_s)} = 0$.

Di questo teorema, del resto, se ne può dare anche un'altra dimostrazione senza ricorrere alla proprietà della fine del n. 6. Se infatti è

$$\beta_k^{(s)} = \sigma_s\, \alpha_k^{(t_s)} \qquad k = 1, 2, \ldots n$$

anche le $\alpha_k^{(t_s)}$ e σ_s apparterranno allo stesso corpo $H^{(s)}$ (cfr. n. 3) e $H^{(t_s)} = H^{(s)}$; quindi anche

$$4) \qquad \vartheta^{(t_s)} = q(\vartheta^{(s)})$$

se $\vartheta^{(s)}$ e $\vartheta^{(t_s)}$ sono i numeri coniugati generatori di $H^{(s)}$ e $H^{(t_s)}$ rispettivamente, e indicando q una funzione razionale.

Dunque

$$\beta_k(\vartheta^{(s)}) = \sigma(\vartheta^{(s)})\,\alpha_k(q(\vartheta^{(s)})).$$

Questa equazione sarà sempre soddisfatta se si sostituisce $\vartheta^{(s)}$ con uno qualunque dei suoi coniugati $\vartheta^{(s')}$, con che $q(\vartheta^{(s)}) = \vartheta^{(t_s)}$ si cambierà ancora in un altro coniugato $\vartheta^{(t_s)'}$ poichè se è $F(x) = 0$ l'equazione irriducibile a cui soddisfano $\vartheta^{(s)}$ e i suoi coniugati, sarà anche $F(\vartheta^{(t_s)}) = F(q(\vartheta^{(s)})) = 0$ e questa equazione, soddisfatta da $\vartheta^{(s)}$, sarà anche soddisfatta da tutti i coniugati di $\vartheta^{(s)}$, quindi anche da $\vartheta^{(s')}$, cioè $F(q(\vartheta^{(s')})) = 0$, da cui risulta che anche $q(\vartheta^{(s')})$ è una radice della $F = 0$ e quindi uguale a un altro coniugato $\vartheta^{(t_s)'}$ di $\vartheta^{(s)}$. Sarà dunque anche

$$\beta_k^{(s')} = \sigma(\vartheta^{(s')})\,\alpha_k(\vartheta^{(t_s)'})$$

cioè la sostituzione 3) non porta soltanto la forma $u^{(s)}$ nella $u^{(t_s)}$, ma anche un'altra qualunque $u^{(s')}$ in un'altra $u^{(t_s)'}$, cioè *scambia fra loro tutti gli iperpiani della* $X = 0$, la quale perciò viene trasformata in sè stessa. Da questa dimostrazione si ha di più che:

Gli n fattori di proporzionalità $\sigma_s = \sigma(\vartheta^{(s)})$ *della* 7) *del n. 10 sono tutti coniugati fra loro, e quindi tutti di norma* ± 1, e anche:

La sostituzione $S = \begin{pmatrix} u^{(t_s)} \\ u^{(s)} \end{pmatrix}$ *sugli iperpiani è pienamente determinata quando si conosca la funzione razionale q per cui*

$$\vartheta^{(t_s)} = q(\vartheta^{(s)}) \qquad 4)$$

poichè infatti *le forme* $u^{(s)}$ *si scambiano tra loro,* per ciò che abbiamo visto, *precisamente come gli n numeri coniugati* ϑ *nella* 4), *quando vi si faccia* $s = 1, 2, \ldots n$.

15. Distribuiamoci ora gli n ideali coniugati di $A = A_{11}$, a cui è coordinata la forma X, in tanti gruppi

$$\begin{gathered} A_{11}, \quad A_{12}, \ldots . A_{1,\nu_1} \\ A_{21}, \quad A_{22}, \ldots . A_{2,\nu_2} \\ \ldots\ldots\ldots\ldots \\ A_{h,1}, \quad A_{h,2}, \ldots . A_{h,\nu_h} \\ \nu_1 + \nu_2 + \ldots . + \nu_h = n \end{gathered}$$

in modo che in ogni orizzontale siano contenuti tutti e soli gli ideali coniugati fra loro equivalenti. Per quel che abbiamo visto, esisteranno certo delle sostituzioni di Γ_ν che porteranno, p. es. l'iperpiano $u_{11} = 0$, corrispondente ad A_{11}, in uno qualunque degli altri ν_1 iperpiani coniugati $u_{1i} = 0$ $(i = 1, 2, \ldots . \nu_1)$, ad esso equivalenti; e tutte queste sostituzioni saranno precisamente in numero di ν_1, poichè esse sono pienamente individuate quando si conosca in quale lettera u_{1i} portino una cert'altra lettera fissa u_{11}. D'altra parte una qualunque sostituzione di Γ_ν dovrà scambiare tra loro iperpiani equivalenti e dovrà perciò portare $u_{11} = 0$ in un altro degli $u_{1,i} = 0$ $(i = 1, 2, \ldots . \nu_1)$, e sarà quindi fra quelle ν_1 sostituzioni considerate prima le quali esauriranno perciò tutto il gruppo Γ_ν. Segue di qui che il numero ν delle sostituzioni di Γ_ν dovrà essere proprio uguale a ν_1; analogamente si vedrebbe che deve essere anche uguale a $\nu_2, \nu_3, \ldots . \nu_h$, ed essendo

$$\nu_1 + \nu_2 + \ldots . + \nu_h = n$$

sarà quindi

$$h\nu = n .$$

Si ha intanto che *gli n ideali coniugati di un ideale* $A = A_{11}$ *si distribuiscono in h gruppi* (h divisore di n) *ognuno contenente uno stesso numero* ν *di ideali tutti equiva-*

lenti fra loro e non equivalenti invece a quelli di un altro gruppo. Inoltre *l'ordine* ν *del gruppo* Γ_ν *delle sostituzioni sugli iperpiani della* $X=0$ *è uguale al numero degli ideali coniugati equivalenti a cui è coordinata la* X *ed è sempre un divisore del grado* n *del corpo.*

16. Supponiamo ora che l'ideale considerato sia un ideale principale, e, per semplicità, potremo sempre supporre che sia proprio l'ideale unità $O^{(s)}$ (equivalente a qualunque altro ideale principale). Esso non è altro che il campo di tutti gli interi del corpo $H^{(s)}$, e così pure i suoi coniugati $O^{(t_s)}$ saranno evidentemente i campi di tutti gli interi dei corpi coniugati $H^{(t_s)}$; se poi $O^{(s)}$ è equivalente ad $O^{(t_s)}$ sarà $H^{(s)}=H^{(t_s)}$ e viceversa, essendo tanto $O^{(s)}$ che $O^{(t_s)}$ il campo degli interi dello stesso corpo $H^{(s)}=H^{(t_s)}$. Applicando allora i teoremi precedenti si ha che *gli* n *corpi coniugati* $H^{(s)}$ *si distribuiscono in gruppi, ognuno contenente uno stesso numero* ν_0 *divisore di* n, *di corpi tutti eguali fra loro e diversi invece da quelli di un altro gruppo*

Inoltre il numero μ di questi gruppi sarà pure un divisore di n, essendo $n=\mu\,\nu_0$ cioè

Il numero μ *dei corpi coniugati effettivamente diversi è sempre un divisore del grado* n *dei corpi stessi.*

In particolare, osserviamo che, *se il grado* n *di un corpo è un numero primo,* possono darsi due sole eventualità, e cioè *o il corpo è normale o è diverso da tutti i suoi coniugati;* questo secondo caso si ha per esempio, per $n>2$, quando esso o qualcuno dei suoi coniugati contiene qualche numero complesso, non potendo infatti un corpo normale di grado dispari contenere altro che numeri reali.[1]

---

[1] Sia infatti $\vartheta=\vartheta^{(1)}$ un numero generatore di questo corpo normale, e $\vartheta^{(2)}$, $\vartheta^{(3)}$,... $\vartheta^{(n)}$ i suoi coniugati. Siccome il grado n del

Segue di qui che *se, data un'equazione irriducibile di grado primo p a coefficienti razionali, è possibile esprimere una sua sola radice* η_1 *razionalmente per un altra* η_1 *l'equazione stessa è risolubile per radicali, anzi si risolve estraendo solo un'unica radice d'indice p.*

Infatti l'equazione stessa per ciò che abbiamo visto risulta in questo caso normale, quindi aggiunta una sua radice η_1 al vecchio campo di razionalità il suo gruppo di Galois G si abbasserà all'identità che è dunque l'unica sostituzione di G che lasci ferma η_s $(s = 1, 2, \ldots p)$. Ogni sostituzione del gruppo risulta allora pienamente determinata quando si sappia in quale lettera essa porti una certa lettera fissa; d'altra parte il gruppo G è transitivo, essendo l'equazione irriducibile; dunque il numero delle sue sostituzioni è proprio p. Essendo allora il gruppo di Galois d'ordine primo p, esso non potrà essere che un gruppo ciclico, e l'equazione si risolverà estraendo soltanto una radice d'indice p.

17. Osserviamo ora che se $A^{(s)}$ è equivalente ad $A^{(s')}$ il corpo $H^{(s)}$ è uguale al coniugato $H^{(s')}$, e siccome gli n ideali coniugati di $A^{(s)}$ ci si presentano divisi in $h = \frac{n}{\nu}$ gruppi contenenti ognuno ν ideali equivalenti si vede che, corrispondentemente, anche gli n corpi coniugati si possono distribuire in $\frac{n}{\nu}$ gruppi contenenti ognuno ν corpi uguali. Segue di qui che il numero ν_0 dei corpi uguali dovrà essere un multiplo di ν, cioè:

---

corpo è dispari, l'equazione, di grado n, a cui soddisfa ϑ avrà certo almeno una radice reale $\vartheta^{(s)}$ e quindi anche tutti i numeri del corpo, potendosi esprimere come funzioni razionali a coefficienti razionali di questo numero $\vartheta^{(s)}$, saranno reali.

Il numero ν *degli ideali coniugati equivalenti di un qualsiasi ideale* A *non solo è un divisore del grado* n *del corpo, ma è anche un divisore del numero* ν_0 *dei corpi coniugati eguali;* o anche

L'ordine ν *del gruppo* Γ_ν *delle sostituzioni sugli iperpiani della* $X=0$ (forma coordinata a un qualsiasi ideale $A^{(s)}$) *è sempre un divisore dell'ordine* ν_0 *del gruppo* Γ_{ν_0} *associato alla classe degli ideali principali.*

Si ha quindi che *in uno stesso corpo* $H=H^{(1)}, H^{(2)}, \ldots H^{(\nu_0)}$, contenente solo i ν_0 ideali coniugati di A,

$$A=A^{(1)}, A^{(2)}, \ldots A^{(\nu_0)}$$

sono contenuti precisamente $\frac{\nu_0}{\nu}$ *ideali coniugati non equivalenti, e quindi anche il numero degli ideali coniugati non equivalenti contenuti in uno stesso corpo è un divisore di* n.

18. Queste $\frac{\nu_0}{\nu}$ classi di ideali coniugati contenute in uno stesso corpo le diremo esse stesse *coniugate.* Se una classe di forme equivalenti è coordinata all'ideale $A=A^{(1)}$, essa è coordinata anche a tutti gli altri ideali coniugati $A^{(2)}, \ldots A^{(n)}$; se quindi non è $\frac{\nu_0}{\nu}=1$, se cioè non tutti gli ideali coniugati di A e contenuti nel corpo sono equivalenti, essa sarà coordinata a ideali di uno stesso corpo appartenenti a classi diverse. Si ha dunque che mentre una classe K di ideali individua perfettamente una classe di forme decomponibili equivalenti, coordinate ai suoi ideali mediante le varie basi (classe che diremo coordinata a K) una classe di forme decomponibili equivalenti può invece essere coordinata a più classi K di ideali, se è $\nu_0 > \nu$, e cioè alle $\frac{\nu_0}{\nu}$ classi coniugate. Dimostriamo però che in ogni

caso queste sono tutte le possibili che cioè *se a due ideali A e B di uno stesso corpo son coordinate due forme decomponibili X e Y equivalenti, necessariamente i due ideali appartengono alla stessa classe o a classi coniugate.*

Sia infatti X coordinata all'ideale A mediante la base $(\alpha_1, \alpha_2, \ldots \alpha_n)$, Y coordinata a B mediante la base $(\beta_1, \beta_2, \ldots \beta_n)$ e sia inoltre

$$1) \qquad x_k = \sum_i C_{ik}\, y_i \qquad k = 1, 2, \ldots n$$

e $|C_{ik}| = \pm 1$ la sostituzione unimodulare che porta la forma Y nell'equivalente X; sarà allora anche $\pm X$ coordinata a B mediante la nuova base $(\beta_1', \beta_2', \ldots \beta_n')$ ove sia

$$\beta_i' = \sum_k C_{ik}\, \beta_k .$$

Ponendo allora

$$u^{(s)} = \sum_i \alpha_i^{(s)}\, x_i$$

$$v^{(t)} = \sum_i \beta_i'^{(t)}\, x_i$$

dovrà dunque aversi

$$X = \frac{1}{N(A)}\, \Pi_s\, u^{(s)}$$

e anche

$$X = \pm \frac{1}{N(B)}\, \Pi_t\, v^{(t)}$$

cioè

$$\frac{1}{N(A)}\, \Pi_s\, u^{(s)} = \pm \frac{1}{N(B)}\, \Pi_t\, v^{(t)}$$

Segue di qui che le forme lineari $v^{(t)}$ dovranno coincidere, a meno dell'ordine e di un fattore di proporzionalità, colle $u^{(s)}$, cioè

$$u^{(s)} = \sigma_s\, v^{(t_s)}$$

ove

$$\sigma_1\, \sigma_{21} \ldots \sigma_n = \pm \frac{N(A)}{N(B)}$$

e quindi

$$\alpha_i^{(s)} = \sigma_s \beta_i'^{(t_s)} \qquad i = 1, 2, \ldots n.$$

Dunque l'ideale $B = (\beta_1' \beta_2' \ldots \beta_n)$ dovrà essere equivalente a qualche coniugato dell'ideale A e dovrà quindi appartenere a una delle $\frac{\nu_0}{\nu}$ classi coniugate in cui si distribuiscono A e i suoi coniugati che appartengono allo stesso corpo, con che il teorema enunciato è dimostrato.

Questo risultato si può anche esprimere dicendo che *se una classe di forme equivalenti è coordinata a un certo ideale A, tutte e sole le classi di ideali dello stesso corpo a cui è coordinata questa medesima classe di forme sono le* $\frac{\nu_0}{\nu}$ *classi coniugate in cui si distribuiscono A e i suoi coniugati.*

Possiamo ora enunciare in modo molto più preciso un teorema riportato da Hilbert,[1] e cioè

Se X è una forma di grado n primitiva decomponibile nel corpo H (pure di grado n), ma non decomponibile in un corpo di grado minore, con discriminante D eguale al numero fondamentale del corpo, esistono in H precisamente $\frac{\nu_0}{\nu}$ *classi coniugate di ideali a cui la forma è coordinata, cioè un numero di classi che è sempre un divisore del numero* ν_0 *dei corpi coniugati eguali ad H, e divisore quindi anche del grado n del corpo,* (Hilbert dice invece semplicemente che esisteranno in H almeno una e non più di n di tali classi).

---

[1] HILBERT. Op. cit., X parte, cap. 8,° teorema 59, pag. 236.

19. Si ha in particolare che *alla classe di forme equivalenti coordinata alla classe degli ideali principali non può esser coordinata alcun'altra classe di ideali dello stesso corpo,* essendo in questo caso $\nu = \nu_0$ e quindi $\frac{\nu_0}{\nu} = 1$ il numero delle classi coniugate del corpo.

20. Così pure *se il corpo H è diverso da tutti i suoi coniugati* (come p. es. è il caso dei corpi di grado primo non normali, cfr. n. 16) *non solo a ogni classe di ideali è coordinata una e una sola classe di forme equivalenti, ma anche viceversa a ogni classe di forme non può corrispondere che una e una sola classe di ideali,* essendo in questo caso $\nu_0 = 1$, e quindi anche ν, divisore di ν_0, e $\frac{\nu_0}{\nu} = 1$.

Capitolo III.

Relazioni fra i vari gruppi $\Gamma(K)$. — Influenza su questi della struttura dell'equazione a cui soddisfa un numero ϑ generatore del corpo.

21. Data una forma X coordinata a una certa classe K di ideali equivalenti, è perfettamente individuato il gruppo di sostituzioni Γ_ν sui suoi iperpiani, che abbiamo chiamato *associato* alla classe K(n. 20). Abbiamo poi visto (n. 14) che per una sostituzione S di questo gruppo, $S=\begin{pmatrix} u^{(t_s)} \\ u^{(s)} \end{pmatrix}$, le forme lineari $u^{(s)}$ componenti la X si scambiavano tra loro come gli n coniugati $\vartheta^{(s)}$ nella sostituzione

$$\Sigma = \begin{pmatrix} q(\vartheta^{(s)}) \\ \vartheta^{(s)} \end{pmatrix} = \begin{pmatrix} \vartheta^{(t_s)} \\ \vartheta^{(s)} \end{pmatrix} \qquad s = 1, 2, \ldots n$$

ove abbiamo indicato con $q(\vartheta^{(s)}) = \vartheta^{(t_s)}$ la funzione razionale per cui si esprime $\vartheta^{t_s)}$ per mezzo di $\vartheta^{(s)}$ (essendo $H^{t_s)} = H^{(s)}$). Invece delle sostituzioni S considereremo allora d'ora innanzi le Σ, potendosi sempre passare dalle une alle altre cambiando semplicemente il nome delle lettere $u^{(s)}$ in $\vartheta^{(s)}$ o viceversa; e considereremo il gruppo Γ_ν delle Σ come addirittura identico al gruppo Γ_ν delle S.

Se allora per la forma X, coordinata alla classe K, esiste una sostituzione Σ del gruppo $\Gamma_\nu(K)$ che porti, p. es., la la lettera $\vartheta^{(s)}$ nella $\vartheta^{(t_s)}$ (una sostituzione S che porti la forma $u^{(s)}$ nella $u^{(t_s)}$), dovranno, per ciò che s'è visto, coinci-

dere i due corpi $H^{(s)}$ e $H^{(t_s)}$, cioè essere eguali (e quindi anche equivalenti) i due ideali principali $O^{(s)}$ e $O^{(t_s)}$. Esisterà allora certamente (n. 14) una sostituzione S' del gruppo $\Gamma_{\nu_0}(K_0)$, associato alla classe K_0 degli ideali principali, che porterà la forma lineare $u_0^{(s)}$ di una forma X_0 decomponibile, coordinata alla classe K_0, nella forma $u_0^{(t_s)}$, e quindi anche una sostituzione Σ' del gruppo $\Gamma_{\nu_0}(K_0)$ che porti la lettera $\vartheta^{(s)}$ nella $\vartheta^{(t_s)}$. Ma essendo sempre $\vartheta^{(ts)} = q(\vartheta^{(s)})$ questa sostituzione Σ' sarà ancora data da

$$\Sigma' = \begin{pmatrix} \vartheta^{(t_s)} \\ \vartheta^{(s)} \end{pmatrix} = \begin{pmatrix} q(\vartheta^{(s)}) \\ \vartheta^{(s)} \end{pmatrix} \qquad s = 1, 2, \ldots . n$$

e coinciderà dunque colla Σ del gruppo $\Gamma_\nu(K)$, precedentemente considerata. Si ha così che ogni sostituzione Σ di un gruppo $\Gamma_\nu(K)$, associato alla classe K, è anche una sostituzione del gruppo $\Gamma_{\nu_0}(K_0)$, cioè:

I gruppi $\Gamma_\nu(K)$, *associati alle varie classi K di ideali, sono tutti sottogruppi del gruppo* $\Gamma_{\nu_0}(K_0)$, *associato alla classe* K_0 *degli ideali principali.*

Si ha di qui una nuova dimostrazione della proprietà del n. 17, che l'ordine ν di $\Gamma_\nu(K)$ è sempre un divisore dell'ordine ν_0 di $\Gamma_{\nu_0}(K_0)$, per un noto teorema sui sottogruppi di un gruppo.[1]

Si ha inoltre che, per l'espressione stessa delle Σ, indipendente dalla classe K e dipendente soltanto dalle funzioni razionali q, due sostituzioni Σ e Σ', *anche di gruppi associati a classi diverse* $\Gamma(K)$ e $\Gamma(K')$ rispettivamente, che portino ambedue una lettera $\vartheta^{(s)}$ in un'altra $\vartheta^{(t_s)}$, necessariamente coincidono.

---

[1] BIANCHI. « Gruppi di sostituzioni », § 7, pag. 16.

22. Siano ora

$$\begin{array}{l} A_{11}, \quad A_{12}, \ldots\ldots A_{1\nu} \\ A_{21}, \quad A_{22}, \ldots\ldots A_{2\nu} \\ \cdots\cdots\cdots\cdots \\ A_{h,1}, \quad A_{h,2}, \ldots\ldots A_{h,\nu} \end{array}$$

gli h gruppi, contenenti ognuno ν ideali equivalenti, in cui si distribuiscono gli $n = h\nu$ ideali coniugati di $A = A_{11}$. Sarà allora, indicando con ϑ_{ir} un numero generatore del corpo H_{ir}, contenente A_{ir}, e cambiando, se occorre, le denominazioni delle ϑ

$$1) \quad \begin{cases} \vartheta_{11} = q_1(\vartheta_{11}) \\ \vartheta_{12} = q_2(\vartheta_{11}) \\ \cdots\cdots\cdots \\ \vartheta_{1,\nu} = q_\nu(\vartheta_{11}) \end{cases} \quad \begin{cases} \vartheta_{21} = q_1(\vartheta_{21}) \ldots\ldots \\ \vartheta_{22} = q_2(\vartheta_{21}) \ldots\ldots \\ \cdots\cdots\cdots\cdots\cdots \\ \vartheta_{2,\nu} = q_\nu(\vartheta_{21}) \ldots\ldots \end{cases} \quad \begin{cases} \vartheta_{h,1} = q_1(\vartheta_{h,1}) \\ \vartheta_{h,2} = q_2(\vartheta_{h,1}) \\ \cdots\cdots\cdots \\ \vartheta_{h,\nu} = q_\nu(\vartheta_{h,1}). \end{cases}$$

Dato ϑ_{1r} esisterà infatti una sostituzione Σ_r di Γ_ν la quale porterà ϑ_{11} in ϑ_{1r}, ma $\vartheta_{1r} = q_r(\vartheta_{11})$ dunque $\Sigma_r = \begin{pmatrix} q_r(\vartheta^{(s)}) \\ \vartheta^{s)} \end{pmatrix}$ e allora anche $q_r(\vartheta_{21}), \ldots q_r(\vartheta_{h,1})$ saranno delle nuove ϑ, appartenenti alla $2^a, \ldots h^{esima}$ verticale, che indicheremo con $\vartheta_{2r}, \ldots \vartheta_{h,r}$ rispettivamente. In generale dunque

$$2) \qquad \vartheta_{ir} = q_r(\vartheta_{i1}).$$

Consideriamo ora una risolvente di Galois dell'equazione irriducibile a cui soddisfano le ϑ, e sia v una sua radice. Tutte le ϑ saranno esprimibili razionalmente per essa e si avrà quindi

$$3) \qquad \vartheta_{i1} = f_{i1}(v)$$

e sostituendo nella 2)

$$4) \qquad \vartheta_{ir} = q_r(f_{i1}(v))\,;$$

ma v è una funzione razionale delle n quantità ϑ, e se in questa equazione 4) facciamo sulle ϑ una sostituzione g del gruppo di Galois, l'equazione stessa, per un noto teorema,[1] resterà ancora soddisfatta. Siano allora ϑ'_{i1} e ϑ'_{ir} le lettere in cui g porta ϑ_{i1} e ϑ_{ir} rispettivamente; eseguendo allora la g nell'equazione 3) si avrà, per il medesimo teorema

$$\vartheta'_{i1} = f_{i1}(v_g)$$

e nella 4)

$$\vartheta'_{ir} = q_r(f_{i1}(v_g)) \qquad \vartheta'_{ir} = q_r(\vartheta'_{i1})$$

e quindi anche ϑ'_{i1} e ϑ'_{ir} apparterranno a una medesima verticale del quadro 1), poichè applicando la funzione razionale q_r si passa da una lettera ϑ alla lettera in cui essa è portata dalla $\Sigma_r = \begin{pmatrix} q_r(\vartheta_s) \\ \vartheta_s \end{pmatrix}$ e quindi a una lettera della medesima verticale.

Si ha dunque che una qualunque sostituzione g del gruppo di Galois porta due lettere ϑ_{i1} e ϑ_{ir} di una medesima verticale del quadro 1) in altre due lettere pure di una medesima verticale. Ma allora queste h verticali, ognuna di ν lettere, formano dei sistemi d'imprimitività per il gruppo G_N di Galois. Dunque:

Se in un corpo $H(\vartheta)$ di grado n esiste una classe K di ideali A equivalenti a cui è associato un gruppo $\Gamma_\nu(K)$ con $1 < \nu < n$, il gruppo di Galois G_N per l'equazione irriducibile $F(x) = 0$ a cui soddisfano ϑ e i suoi coniugati è imprimitivo,

---

[1] BIANCHI. « Gruppi di sostituzioni », § 62, pag. 144.

e se sono $A_{i1}, A_{i2}, \ldots A_{iv}$ $(i=1,2,\ldots h)$ *gli h gruppi di ideali equivalenti in cui si distribuiscono gli n coniugati di* $A=A_{11}$, *saranno precisamente* $\vartheta_{i1}, \vartheta_{i2}, \ldots \vartheta_{iv}$ $(i=1,2,\ldots h)$ *gli h sistemi d'imprimitività in cui si distribuiscono le n lettere* ϑ_{ir}.

Segue di qui [1] che l'equazione $F(x)=0$ si ottiene eliminando y da due altre equazioni

$$5) \qquad \varphi(y)=y^h+c_1 y^{h-1}+\ldots+c_{h-1}y+c_h=0$$

$$6) \qquad x^v+\delta_1(y)x^{v-1}+\ldots+\delta_{v-1}(y)x+\delta_v(y)=0$$

dove le c_i $(i=1,2,\ldots h)$ sono convenienti costanti razionali, e le $\delta_r(y)$ $(r=1,2,\ldots v)$ convenienti funzioni razionali di y a coefficienti pure razionali; cioè *il corpo* $H(\vartheta)$ *può pensarsi come un corpo relativo,* [2] *di grado relativo* v *rispetto al corpo di grado h generato da una certa radice della* 5).

Inoltre *le varie equazioni* 6), *che si hanno sostituendo a y le h radici* y_i *della* 5), *sono tutte normali*, poichè le v radici $\vartheta_{i,1}, \vartheta_{i,2}, \ldots \vartheta_{i,v}$ di un medesimo sistema d'imprimitività sono tutte esprimibili razionalmente l'una per l'altra.

23. Osserviamo infine che se la forma X è coordinata a certe classi di ideali

$$\begin{aligned} A=A_{11},\ & A_{12}, \ldots\ldots A_{1v} \\ & A_{21},\ A_{22}, \ldots\ldots A_{2v} \\ & \ldots\ldots\ldots\ldots \\ & A_{h1},\ A_{h2}, \ldots\ldots A_{hv} \end{aligned}$$

ove è

$$A_{tr} \equiv (\alpha_1^{(tr)},\ \alpha_2^{(tr)}, \ldots\ldots \alpha_n^{(tr)}),$$

---

[1] BIANCHI. « Gruppi di sostituzioni, ecc. », § 71, pag. 161.

[2] HILBERT. Op. cit., parte 1ª, cap. 5°, pag. 203.

sarà

$$X = \frac{1}{N(A)} \Pi_{tr} (\alpha_1^{(tr)} x_1 + \alpha_2^{(tr} x_2 + \ldots + \alpha_n^{(tr)} x_n)$$

$$= \frac{1}{N(A)} \prod_1^h{}_t \prod_1^\nu{}_r (\alpha_1^{(tr)} x_1 + \alpha_2^{(tr)} x_2 + \ldots + \alpha_n^{(tr)} x_n).$$

Ma il secondo prodotto è un polinomio nelle x_i i cui coefficienti sono evidentemente funzioni simmetriche delle $\vartheta_{t,1}, \vartheta_{t,2}, \ldots \vartheta_{t,\nu}$, e quindi esprimibili razionalmente pei coefficienti dell'equazione 6) del n. 22, cioè per y_t, se questa è la radice della 5) corrispondente al sistema d'imprimitività $\vartheta_{t,1}, \vartheta_{t,2}, \ldots \vartheta_{t,\nu}$. Si ha dunque che

La forma X, a cui è associato il gruppo Γ_ν, *moltiplicata per un conveniente numero intero* $N(A)$, *si decompone nel prodotto di altre h forme, ognuna di grado* ν, *con coefficienti interi appartenenti ai corpi di grado h generate dalle radici della* 5), *e tali che ciascuna è trasformata separatamente in sè da tutte le sostituzioni di* G_x, *a meno di un fattore di proporzionalità* $\sigma_{t,1} \sigma_{t,2} \ldots \sigma_{t,\nu}$, appartenente al medesimo corpo di grado h, che vedremo in seguito (n. 32) essere proprio un'unità η_t del corpo.

24. Consideriamo ora quel sottogruppo G_m del gruppo di Galois G_N le cui sostituzioni γ lasciano fissa ϑ_{11}.

Ricordiamo che

1)
$$\vartheta_{11} = f_{11}(v)$$
$$\vartheta_{1r} = q_r(\vartheta_{11})$$

cioè

2)
$$\vartheta_{1r} = q_r(f_{11}(v)).$$

Eseguendo nella 1) una qualsiasi sostituzione del gruppo di Galois, essa, per il solito teorema, resterà sempre veri-

ficata; se in particolare questa sostituzione è una γ del sottogruppo G_m si avrà ancora

$$\vartheta_{11} = f_{11}(v_\gamma).$$

Eseguendo la γ nella 2), e indicando con ϑ'_{1r} la lettera in cui γ porta ϑ_{1r} si avrà

$$\vartheta'_{1r} = q_r(f_{11}(v_\gamma))$$
$$\vartheta'_{1r} = q_r(\vartheta_{11}) = \vartheta_{1r}.$$

Si ha cioè che *tutte le sostituzioni* γ *del gruppo di Galois che lasciano fissa* ϑ_{11} *lasciano fisse anche tutte le altre lettere* $\vartheta_{1r}(r=1,2,\dots\nu)$ *del medesimo sistema d'imprimitività.* Dunque G_m, essendo ϑ_{11} assolutamente qualunque fra le $\vartheta_{11}, \vartheta_{12}, \dots \vartheta_{1\nu}$, è il sottogruppo numerico non della sola ϑ_{11}, ma anche di $\vartheta_{12}, \dots \vartheta_{1\nu}$.

Distribuiamo ora nel solito modo le sostituzioni del gruppo di Galois G_N nel quadro

3)
$$\begin{array}{llll} \gamma_1, & \gamma_2, & \cdots & \gamma_m \\ \gamma_1 g_2, & \gamma_2 g_2, & \cdots & \gamma_m g_2 \\ \cdots & \cdots & \cdots & \cdots \\ \gamma_1 g_\mu, & \gamma_2 g_\mu, & \cdots & \gamma_m g_\mu \end{array}$$

essendo $N = m\mu$. Osserviamo che due sostituzioni g e g' di G_N che portino ambedue ϑ_{11} nella medesima lettera si trovano in una medesima orizzontale che indicheremo con $G_m g_t$; se è infatti $g = \gamma g_t$, essendo $g' g^{-1}$ una sostituzione γ' di G_m, $g' g^{-1} = \gamma'$, sarà $g' = \gamma' g$, da cui segue che anche $g' = \gamma' \gamma g_t$ appartiene all'orizzontale $G_m g_t$. Essendo d'altra parte G_N transitivo, ne segue che le orizzontali saranno precisamente in numero di n, e le potremo quindi indicare con $G_m g_{ir}$ $(i=1,2,\dots h,\ r=1,2,\dots\nu)$, essendo g_{ir} una qualsiasi sostituzione che porti ϑ_{11} in ϑ_{ir}.

Il sottogruppo $G_{\nu m}$ di G_N che lascia fisso il primo sistema d'imprimitività sarà allora dato dalle sostituzioni di

4) $$G_m,\ G_m g_{12},\ldots\ G_m g_{1\nu}$$

e G_m *sarà invariante in* $G_{\nu m}$ poichè, se γ è di G_m, anche $g_{1r}^{-1}\gamma g_{1r}$, lasciando fisso ϑ_{1r}, è ancora una sostituzione di G_m.

Riprendiamo ora la 2)

2) $$\vartheta_{1r} = q_r(f_{11}(v)) \qquad \text{ove}$$

1) $$f_{11}(v) = \vartheta_{11}\,.$$

Dalla 1) si avrà ancora

$$\vartheta_{11} = f_{11}(v_\gamma)$$

e anche

$$\vartheta_{1r} = f_{11}(V_{\gamma g_{1r}}) \qquad \vartheta_{ir} = f_{11}(V_{\gamma g_{ir}})$$

cioè f_{11} assume lo stesso valore ϑ_{ir} per le v corrispondenti a sostituzioni γg_{ir} di una medesima orizzontale del quadro 3) e sostituendo nella 2)

$$f_{11}(V_{\gamma g_{1r}}) = q_r(f_{11}(v_\gamma))\,.$$

Eseguiamo ora in questa equazione una qualunque sostituzione $\overline{\gamma} g_{is}$ del gruppo di Galois; sarà

$$f_{11}(V_{\gamma g_{1r}\overline{\gamma} g_{is}}) = q_r(f_{11}(V_{\gamma_2 g_{is}}))$$

da cui si vede che *se è* $\Sigma_r = \begin{pmatrix} q_r(\vartheta_s) \\ \vartheta_s \end{pmatrix}$ *una sostituzione del gruppo* $\Gamma_\nu(K)$, *le lettere si scambiano per la* Σ_r *come le orizzontali del quadro* 3) *quando si moltiplichino a sinistra tutte le loro sostituzioni per* g_{1r} *o altra sostituzione* γg_{1r} *della medesima orizzontale.* È da osservare che qualunque sia la sostituzione $\overline{\gamma}$ di G_m la $\gamma g_{1r}\overline{\gamma} g_{is}$ appartiene sempre alla me-

desima orizzontale, essendo g_{1r} permutabile col gruppo G_m e quindi

$$\gamma g_{1r} \overline{\gamma g_{1s}} = \gamma \overline{\gamma'} g_{1r} g_{1s} = \gamma'' g_{1r} g_{1s}.$$

Abbiamo così visto come, dato il gruppo di Galois dell'equazione a cui soddisfano le ϑ_{ir}, sia possibile costruire il gruppo $\Gamma_\nu(K)$.

25. Consideriamo il gruppo $G_{\nu m}$ di G_N che lascia fisso il primo sistema d'imprimitività, e delle sostituzioni di questo sottogruppo consideriamo solo le parti che operano sulle ϑ_{11}, $\vartheta_{12}, \ldots \vartheta_{1\nu}$, che formeranno altre sostituzioni (g) su queste sole ν lettere.

Ogni insieme di 4) del numero precedente darà allora evidentemente origine a una sola sostituzione (g_{1r}), poichè tutto il sottogruppo G_m dà origine alla sola identità.

Questo nuovo gruppo (G) *delle* (g), *che, per un noto teorema,*[1] *è appunto il gruppo di Galois per l'equazione* 6) *del n. 22 quando al campo di razionalità si sia aggiunta la radice* y_1, *della* 5) *corrispondente al primo sistema d'imprimitività, sarà dunque costituito dalle* ν *sostituzioni* (g_{1r}), $(r = 1, 2, \ldots \nu)$.

Che il gruppo di Galois della 6) fosse d'ordine ν si poteva del resto prevedere dal fatto che la 6) stessa è un'equazione normale, essendo $\vartheta_{1r} = q_r(\vartheta_{11})$ $(r = 1, 2, \ldots \nu)$.

In quest'equazione

$$1) \qquad \vartheta_{1r} = q_r(\vartheta_{11})$$

potremo, per il solito teorema, eseguire una qualsiasi sostituzione (g_{1s}) senza che l'equazione stessa cessi di essere

[1] Bianchi. Op. cit., § 71, pag. 161.

verificata, con che ϑ_{1r} andrà in ϑ'_{1r} e sarà

$$\vartheta'_{1r} = q_r(\vartheta_{1s}).$$

Ma ϑ'_{1r} è la lettera in cui ϑ_{11} è portata dalla sostituzione (g_{1r}) (g_{1s}). Si ha dunque che se nella 1) si sostituisce a ϑ_{11} un'altra lettera ϑ_{1s}, a cui corrisponda una sostituzione (g_{1s}) che porti ϑ_{11} in ϑ_{1s}, ottengo nel primo membro la lettera ϑ'_{ir} corrispondente alla sostituzione (g_{1r}) (g_{1s}). Si può dunque dire che per la sostituzione $\Sigma_r = \begin{pmatrix} q_r(\vartheta_i) \\ \vartheta_i \end{pmatrix}$ le lettere formanti il primo sistema d'imprimitività $\vartheta_{11}, \vartheta_{12}, \ldots \vartheta_{1s}, \ldots \vartheta_{1\nu}$ si cambiano fra loro come le sostituzioni corrispondenti (g_{1s}) nella sostituzione

$$S_r = \begin{pmatrix} (g_{1r})\,(g_{11}) \ldots . (g_{1r})\ (g_{1s}) \ldots . (g_{1r})\ (g_{1\nu}) \\ (g_{11}) \ldots \ldots . (g_{1s}) \ldots \ldots . (g_{1\nu}) \end{pmatrix}.$$

Si può così a ogni sostituzione Σ_r sulle $\vartheta_{11}, \ldots . \vartheta_{1\nu}$, far corrispondere una sostituzione S_r e quindi una (g_{1r}) e viceversa; e si può quindi stabilire fra *il gruppo* $\Gamma_\nu(K)$ *delle* Σ_r *e il gruppo di Galois* (G_ν) *per l'equazione normale* (6) *una corrispondenza biunivoca che è evidentemente d'isomorfismo oloedrico.* Si può perciò anche dire che i *due gruppi* $\Gamma_\nu(K)$ e (G_ν), *astrattamente considerati, sono identici.*

26. Siano $\Gamma_\nu(K)$ e $\Gamma_{\nu'}(K')$ due gruppi di sostituzioni associati alle due classi K e K' rispettivamente, e supponiamo inoltre che $\Gamma_\nu(K)$ contenga come sottogruppo $\Gamma_{\nu'}(K')$; quindi intanto $\nu = k\nu'$. Ordiniamo allora le ν radici dell'equazione 6) del n. 22, corrispondente al gruppo $\Gamma_\nu(K)$ in modo simile a quello del n. 22, cioè mettendo in una medesima verticale le ν' radici $\vartheta_{i1}, \vartheta_{i2}, \ldots \vartheta_{i\nu'}, \ldots$ $(i = 1, 2, \ldots k)$

scambiate fra loro dalle ν' sostituzioni $\Sigma'_r = \begin{pmatrix} \vartheta_{ir} \\ \vartheta_{i1} \end{pmatrix} = \begin{pmatrix} q_r(\vartheta_{i1}) \\ \vartheta_{i1} \end{pmatrix}$ del gruppo $\Gamma_{\nu'}$ (K').

Se è

$$\vartheta_{ir} = q_r(\vartheta_{i1})$$

questa equazione sarà ancora verificata eseguendovi una qualsiasi sostituzione (g) del gruppo (G_ν) di Galois che porterà ϑ_{i1} in ϑ'_{i1} e ϑ_{ir} in ϑ'_{ir}, cioè

$$\vartheta'_{ir} = q_r(\vartheta'_{i1})$$

da cui si vede che anche ϑ'_{ir} e ϑ'_{i1} apparterranno a una medesima verticale. Quindi *se* $\nu' < \nu$, *il gruppo di Galois* (G_ν) *per l'equazione* 6) *sarà ancora imprimitivo e saranno* $\vartheta_{i1}, \vartheta_{i2}, \ldots \vartheta_{i\nu'}$ $(i = 1, 2, \ldots k)$ *i* k *sistemi d'imprimitività in cui si distribuiscono le radici.* L'equazione stessa

$$1) \qquad x^\nu + \delta_1(y)\, x^{\nu-1} + \ldots + \delta_{\nu-1}(y)\, x + \delta_\nu(y) = 0$$

si otterrà poi eliminando z *da due altre equazioni*

$$2) \qquad z^k + C_1(y)\, z^{k-1} + \ldots + C_{k-1}(y)\, z + C_k(y) = 0$$

$$3) \qquad x^{\nu'} + p_1(y,z)\, x^{\nu'-1} + \ldots + p_{\nu'-1}(y,z),\ x + p_{\nu'}(y,z) = 0\,.$$

Osserviamo inoltre che se Σ è una sostituzione di Γ_ν che lascia fisso un sistema d'imprimitività, per es. il primo, essa porterà ad es. ϑ_{11} in ϑ_{1r} $(r = 1, 2, \ldots \nu')$, sarà quindi (n. 21) una sostituzione Σ' di Γ' e lascerà perciò fissi anche tutti gli altri sistemi d'imprimitività. Segue di qui che trasformando una sostituzione Σ' di Γ' con un'altra sostituzione τ di Γ, si avrà sempre una sostituzione Σ'' di Γ' poichè Σ'' lascia fisso il sistema d'imprimitività in cui τ trasporta il primo e quindi anche tutti gli altri.

Se dunque un gruppo $\Gamma_\nu(K)$, *associato a una classe* K, *contiene un altro gruppo* $\Gamma_{\nu'}(K')$ *associato alla classe* K', *questo è invariante in* $\Gamma_\nu(K)$.

Corrispondentemente si ha che il gruppo (G_ν) per l'equazione 1), in isomorfismo oloedrico con $\Gamma_\nu(K)$, conterrà come *invariante* il sottogruppo $(G'_{\nu'})$, corrispondente a $\Gamma_{\nu'}(K')$, che lascia fissi tutti i sistemi d'imprimità $\vartheta_{i1}, \vartheta_{i2}, \ldots \vartheta_{i\nu'}$ $(i = 1, 2, \ldots k)$ *e perciò non solo sarà normale l'equazione* 3) (essendo $\vartheta_{ir} = q_r(\vartheta_{is})$, *ma anche l'equazione* 2) *avrà un gruppo di Galois proprio d'ordine* k, perchè uguale al gruppo complementare $\frac{(G_\nu)}{(G_{\nu'})}$ e sarà quindi anch'essa normale.

In particolare si ha che non solo i gruppi $\Gamma_\nu(K)$ sono tutti sottogruppi di $\Gamma_{\nu_0}(K_0)$ (n. 21) ma, se è $\nu < \nu_0$, *essi sono sottogruppi invarianti di* $\Gamma_{\nu_0}(K_0)$.

27. Osserviamo che se un ideale $M = (\beta_1(\vartheta), \beta_2(\vartheta), \ldots \beta_n(\vartheta))$ è un moltiplicatore dell'ideale $A = (\alpha_1(\vartheta), \alpha_2(\vartheta), \ldots \alpha_n(\vartheta))$, anche un qualsiasi suo coniugato $M^{(s)} = (\beta_1(\vartheta^{(s)}), \ldots \beta_n(\vartheta^{(s)}))$ sarà un moltiplicatore del corrispondente $A^{(s)} = (\alpha_1(\vartheta^{(s)}), \ldots \alpha_n(\vartheta^{(s)}))$. Infatti l'ideale AM è per ipotesi, un ideale principale (γ); quindi un suo qualunque numero $\Sigma_{ik} \lambda_{ik}(\vartheta)\, \alpha_i(\vartheta)\, \beta_k(\vartheta)$ si potrà sempre porre sotto la forma $\gamma(\vartheta)\, \xi(\vartheta)$ (essendo λ_{ik} e ξ interi algebrici del corpo) cioè

$$\Sigma_{ik} \lambda_{ik}(\vartheta)\, \alpha_i(\vartheta)\, \beta_k(\vartheta) = \gamma(\vartheta)\, \xi(\vartheta)$$

e cambiando, com'è permesso ϑ in $\vartheta^{(s)}$

$$\Sigma_{ik} \lambda_{ik}(\vartheta^{(s)})\, \alpha_i(\vartheta^{(s)})\, \beta_k(\vartheta^{(s)}) = \gamma(\vartheta^{(s)})\, \xi(\vartheta^{(s)})$$

che dimostra l'asserto.

Siano ora

1) $$A_{i1},\ A_{i2},\ldots\ldots A_{i\nu}$$

i ν ideali coniugati equivalenti, appartenenti a una certa classe K_i, e

2) $$M_{i1},\ M_{i2},\ldots\ldots M_{i\nu}$$

i corrispondenti moltiplicatori coniugati. Sarà, per ciò che abbiamo visto

$$A_{i1}\,M_{i1}=(\gamma_{i1}),\ A_{i2}\,M_{i2}=(\gamma_{i2}),\ldots\ldots A_{i\nu}\,M_{i\nu}=(\gamma_{i\nu}).$$

Ma tutti gli A_{ir} $(r=1,2,\ldots\nu)$ sono fra loro equivalenti, se quindi A_{i1}, M_{i1} è un ideale principale, saranno anche $A_{ir}\,M_{i1}$ $(r=1,2,\ldots\nu)$ tanti altri ideali principali; da cui segue che non solo M_{ir} ma anche M_{i1} è un ideale moltiplicatore di A_{ir} e M_{i1} risulta quindi equivalente a M_{ir} $(r=1,2,\ldots\nu)$. Si ha dunque che se i ν ideali coniugati 1) sono fra loro equivalenti, anche i ν ideali coniugati 2) saranno fra loro equivalenti, e siccome la considerazione è perfettamente invertibile si ha in conclusione che *se i coniugati di* $A=A_{11}$ *si distribuiscono nelle* h *classi* K_i *di ideali equivalenti*

$$A_{i1},\ A_{i2},\ldots\ldots A_{i\nu}\qquad i=1,2,\ldots h\qquad h=\frac{n}{\nu}$$

i rispettivi moltiplicatori M_{ir} *si distribuiranno nelle altre* h *classi* K_i'

$$M_{i1},\ M_{i2},\ldots\ldots M_{i\nu}$$

e sarà $K_i\,K_i'=K_{0,i}$ la classe degli ideali principali, e $K_i'=K_i^{-1}$.

A una qualunque di queste classi K_i sarà allora associato un certo gruppo $\Gamma_\nu(K_i)$ di sostituzioni Σ_r sulle ϑ_{ir}, perfettamente individuate quando si sappia in quale lettera ϑ_{ir} esse portino una certa lettera fissa ϑ_{i1}, e ricordiamo a questo proposito che le sostituzioni Σ_r del gruppo $\Gamma_\nu(K_i)$

scambiano tra loro le ϑ_{ir} ($r = 1, 2, \ldots \nu$) corrispondenti ai ν ideali coniugati di una medesima classe K_i. Alla classe K_i^{-1}, che contiene gli ideali coniugati 2) sarà allora associato $\Gamma_\nu(K_i^{-1})$ le cui sostituzioni Σ'_r dovranno pure portare ϑ_{i1} in un'altra lettera ϑ_{ir} del medesimo gruppo $\vartheta_{i1}, \vartheta_{i2}, \ldots \vartheta_{i\nu}$; d'altra parte (n. 21) due sostituzioni Σ_r e Σ'_r che portino ambedue una medesima lettera ϑ_{i1} in un'altra ϑ_{ir} necessariamente coincidono, quindi *i due gruppi* $\Gamma_\nu(K_i)$ *e* $\Gamma_\nu(K_i^{-1})$ *associati a classi inverse sono eguali,* poichè ogni sostituzione Σ_r dell'uno è anche una sostituzione Σ'_r dell'altro, e viceversa.

28. Siano ora $\Gamma_\nu(K)$ e $\Gamma_{\nu'}(K')$ due gruppi associati a classi K e K' rispettivamente di un medesimo corpo, e siano

1) $$A_{11}, A_{12}, \ldots A_{1\nu}$$

ν ideali coniugati equivalenti contenuti in K e

2) $$B_{11}, B_{12}, \ldots B_{1\nu'},$$

ν' ideali coniugati equivalenti contenuti in K'. Supponiamo che i due gruppi $\Gamma_\nu(K)$ e $\Gamma_{\nu'}(K')$ abbiano in comune oltre l'identità anche altre sostituzioni V_s che formeranno un sottogruppo Γ_μ contenuto tanto in $\Gamma(K)$ che in $\Gamma(K')$. Consideriamo allora una di queste sostituzioni V_s di Γ_μ; essa porterà ad es. ϑ_{11} in un altra lettera ϑ_{1s}, che, appartenendo V_s a $\Gamma_\nu(K)$, dovrà corrispondere a un certo ideale A_{1s} del gruppo 1), e appartenendo V_s anche a $\Gamma_{\nu'}(K')$ dovrà anche corrispondere a un ideale B_{1s} del gruppo 2). D'altra parte è chiaro che l'ideale $A_{1s} B_{1s}$, equivalente ad $A_{11} B_{11}$, è anche un coniugato di questo i cui numeri si ottengono semplicemente sostituendo ϑ_{1s} a ϑ_{11} nelle espressioni che

danno i numeri di $A_{11}B_{11}$ in funzione di ϑ_{11}. Contenendo dunque la classe prodotto KK' i due ideali coniugati equivalenti $A_{11}B_{11}$ corrispondenti a ϑ_{11}, e $A_{1s}B_{1s}$, corrispondente a ϑ_{1s}, esisterà certo una sostituzione del gruppo $\Gamma(KK')$ che porterà ϑ_{11} in ϑ_{1s}, la quale sostituzione dovrà quindi, per il solito teorema del n. 21, coincidere precisamente colla V_s.

Si ha così che *il gruppo* $\Gamma(KK')$, *associato alla classe prodotto di due altre classi, contiene necessariamente il sottogruppo* Γ_u *delle sostituzioni* V_s *comuni ai due gruppi* $\Gamma(K)$ *e* $\Gamma(K')$.

Esso non può invece contenere le sostituzioni Z_r di $\Gamma(K)$ che non appartengono a $\Gamma(K')$; se infatti Z_r porta ϑ_{11} in ϑ_{1r}, a cui corrispondono gli ideali A_{1r} e B_{1r}, si ha che A_{11} è equivalente ad A_{1r} ma B_{11} non è equivalente a B_{1r}, quindi $A_{11}B_{11}$ non è equivalente al coniugato $A_{1r}B_{1r}$ e non può perciò esistere in $\Gamma(KK')$ una sostituzione (Z_r) che porti ϑ_{11} in ϑ_{1r}. Analogamente si vede che $\Gamma(KK')$ non può contenere sostituzioni di $\Gamma(K')$ che non siano anche di $\Gamma(K)$, e in conclusione si ha che:

Il gruppo $\Gamma(KK')$ *conterrà certamente le sostituzioni comuni a* $\Gamma(K)$ e $\Gamma(K')$, *e eventualmente ne conterrà altre che non potranno però appartenere nè a* $\Gamma(K)$ *nè a* $\Gamma(K')$.

29. Consideriamo ora le potenze di una classe K. Applicando i risultati precedenti col fare $K=K'$ si ha allora che il gruppo $\Gamma(K^2)$ contiene $\Gamma(K)$ e eventualmente altre sostituzioni; *così pure* $\Gamma(K^3)\ldots\Gamma(K^m)$ *conterranno tutti il gruppo* $\Gamma(K)$ e eventualmente altre sostituzioni. Dimostriamo però che *il primo gruppo* $\Gamma(K^t)$ *della successione*

$$\Gamma(K),\ \Gamma(K^2),\ldots\Gamma(K^m)\ldots.$$

che contenga altre sostituzioni oltre quelle di $\Gamma(K)$, *è necessariamente associato a una potenza* K^t *di* K *con esponente* t *eguale a un divisore del periodo* α *di* K *stessa* (cioè del minimo numero $\alpha > 0$ per cui sia $K^\alpha = K_0$).

Dividendo infatti α per t si abbia

$$\alpha = tq + r \quad \text{con} \quad 0 \leq r < t.$$

Facciamo ora la potenza $(q+1)^{esima}$ di K^t; ad essa sarà associato un gruppo $\Gamma[(K^t)^{q+1}]$ che conterrà certamente, per ciò che s'è visto, $\Gamma(K^t)$ e quindi altre sostituzioni oltre quelle di $\Gamma(K)$. Ma è

$$(K^t)^{q+1} = K^{tq+t} = K^{tq+r+(t-r)} = K^{tq+r} \cdot K^{t-r}$$

da cui, essendo $\alpha = tq + r$ il periodo di K,

$$(K^t)^{q+1} = K^{t-r}.$$

Se dunque r non fosse 0, $t - r$ sarebbe un esponente minore di t per il quale si avrebbe che $\Gamma(K^{t-r}) = \Gamma[(K^t)^{q+1}]$ conterrebbe altre sostituzioni oltre quelle di $\Gamma(K)$ il che è assurdo per l'ipotesi fatta che t sia il minimo.

Capitolo IV.

Ulteriori qualità del gruppo automorfo G_X.

30. Consideriamo un unità ε del corpo H e i ν ideali coniugati di una medesima classe K

$$A_{11}, A_{12}, \dots A_{1\nu}$$

con $A_{1r} = (\alpha_1^{(1r)}, \alpha_2^{(1r)}, \dots \alpha_n^{(1r)})$. Questi ν ideali coniugati appartengono tutti al medesimo corpo di ε; avremo perciò

1) $$\varepsilon \alpha_k^{(1r)} = \sum_i e_{ik}^{(r)} \alpha_i^{(1r)} \qquad k = 1, 2, \dots n$$

essendo le $e_{ik}^{(r)}$ interi razionali e il determinante $|e_{ik}^{(r)}| = \pm 1$; anzi se è ν_0 il numero dei corpi H coniugati eguali, cioè

$$\begin{aligned} H = H_{11} = H_{12} = \dots\dots = H_{1\nu} \\ = H_{21}, = H_{22} = \dots\dots = H_{2\nu} \\ \dots\dots\dots\dots\dots\dots \\ = H_{\frac{\nu_0}{\nu}, 1} = H_{\frac{\nu_0}{\nu}, 2} = \dots = H_{\frac{\nu_0}{\nu}, \nu} \end{aligned}$$

avremo precisamente ν_0 sistemi di equazioni del tipo 1) e cioè

2) $$\varepsilon \alpha_k^{(t,r)} = \sum_i e_{ik}^{(t,r)} \alpha_i^{(t,r)} \qquad k = 1, 2, \dots n$$
$$r = 1, 2, \dots \nu \qquad t = 1, 2, \dots \frac{\nu_0}{\nu}$$

a cui corrisponderanno le ν_0 sostituzioni lineari

3) $$x_i = \sum_k e_{ik}^{(t,r)} y_k$$

che apparterranno tutte al sottogruppo G_e del gruppo automorfo G_X della forma $X = \frac{1}{N(\alpha)} \Pi_{tr} (\alpha_1^{(tr)} x_1 + \ldots + \alpha_n^{(tr)} x_n)$ poichè lasciano fisso l'iperpiano $u_{tr} = 0$ della forma stessa (n. 11).

Di queste ν_0 sostituzioni noi consideriamo però solo le ν che si hanno facendo nelle 3) $t = 1$, che indicheremo per brevità con $E_1, E_2, \ldots E_\nu$, e che si ottengono mediante le 2) dalle basi degli ideali equivalenti

$$A_{11},\ A_{12}, \ldots . A_{1\nu}$$

rispettivamente. Si vede dunque che per ogni unità ε del corpo e per ogni classe K di ideali a cui sia coordinata una certa forma X, risultano pienamente determinate ν sostituzioni E_r del sottogruppo G_e, corrispondente ognuna a uno A_{1r} dei ν ideali coniugati equivalenti di K; e queste sostituzioni sono certamente tutte differenti fra loro se ε è di grado n

31. Distribuiamo ora le sostituzioni del gruppo automorfo G_X nel quadro

$$G_e,\ G_e\ T_2, \ldots . G_e\ T_r, \ldots G_e\ T_\nu$$

essendo G_e, come al solito il sottogruppo delle sostituzioni provenienti dalle unità e che lasciano quindi in sè tutti gli iperpiani della forma X, ed essendo invece $T_r (r = 2, 3 \ldots \nu)$ una qualsiasi sostituzione di G_X, che porti l'iperpiano $u_{11} = \alpha_1^{(11)} x_1 + \alpha_{12}^{(11)} x_2 + \alpha_n^{(11)} x_n = 0$ nell'iperpiano equivalente $u_{1r} = \alpha_1^{(1r)} x_1 + \alpha_2^{(1r)} x_2 + \alpha_n^{(1r)} x_n = 0$.

Se la sostituzione T_r è data da

1) $$x_i = \Sigma_k\, a_{ik}^{(r)}\, y_k$$

si avrà allora, per l'ipotesi fatta che T_r porti $u_{11} = 0$ in $u_{1r} = 0$

2) $$\sum_i a_{ik}^{(r)} \alpha_i^{(11)} = \sigma \alpha_k^{(1r)} \qquad k = 1, 2, \ldots n$$

e moltiplicando ambo i membri per ε

3) $$\sum_i a_{ik}^{(r)} \alpha_i^{(11)} \varepsilon = \sigma \alpha_k^{(1r)} \varepsilon \qquad k = 1, 2, \ldots n .$$

Ma per le 2) del numero precedente si ha

$$\varepsilon \alpha_i^{(11)} = \sum_\lambda e_{\lambda i}^{(11)} \alpha_\lambda^{(11)}$$

$$\varepsilon \alpha_k^{(1r)} = \sum_\lambda e_{\lambda k}^{(1r)} \alpha_\lambda^{(1r)}$$

e sostituendo nelle 3)

$$\sum_{i\lambda} a_{ik}^{(r)} e_{\lambda i}^{(11)} \alpha_\lambda^{(11)} = \sigma \sum_\lambda e_{\lambda k}^{(1r)} \alpha_\lambda^{(1r)} .$$

Per le 2) è però

$$\sigma \alpha_\lambda^{(1r)} = \sum_i a_{i\lambda}^{(r)} \alpha_i^{(11)}$$

con che le 4) diventano

$$\sum_{i\lambda} a_{ik}^{(r)} e_{\lambda i}^{(11)} \alpha_\lambda^{(11)} = \sum_{i\lambda} e_{\lambda k}^{(1r)} a_{i\lambda}^{(r)} \alpha_i^{(11)}$$

e scambiando nel secondo membro i con λ

$$\sum_{i\lambda} a_{ik}^{(r)} e_{\lambda i}^{(11)} \alpha_\lambda^{(11)} = \sum_{i\lambda} e_{ik}^{(1r)} a_{\lambda i}^{(r)} \alpha_\lambda^{(11)}$$

da cui si ha, essendo le $\alpha_\lambda^{(11)}$ $(\lambda = 1, 2, \ldots n)$ indipendenti

5) $$\sum_i a_{ik}^{(r)} e_{\lambda i}^{(11)} = \sum_i e_{ik}^{(1s)} a_{\lambda i}^{(r)} .$$

Ma il primo membro non è altro che il coefficiente $c_{\lambda k}$ della sostituzione $E_1 T_r$

$$x_\lambda = \sum_k y_k \sum_i e_{\lambda i}^{(11)} a_{ik}^{(r)} = \sum_k c_{\lambda k} y_k$$

il secondo membro è il coefficiente $c'_{\lambda k}$ della sostituzione $T_r E_r$

$$x_\lambda = \sum_k c'_{\lambda k} y_k$$

dunque le equazioni 5) ci dicono che è sempre

$$E_1 T_r = T_r E_r$$

o anche

$$E_r = T_r^{-1} E_1 T_r .$$

Si ha cioè che *una sostituzione T_r del gruppo automorfo G_x che porti l'iperpiano u_{11} in u_{1r} trasforma una sostituzione E_1 di G_e, corrispondente all'ideale A_{11} nella sostituzione E_r, pure di G_e, corrispondente all'ideale A_{1r}.*

Vediamo in quale sostituzione $E_{s'}$ la T_r trasforma un'altra qualsiasi E_s. Essendo intanto

$$E_s = T_s^{-1} E_1 T_s$$

sarà

$$E_{s'} = T_r^{-1} E_s T_r = (T_s T_r)^{-1} E_1 (T_s T_r)$$

e se $E_{s'}$ corrisponde all'ideale $A_{1s'}$, $T_s T_r$ dovrà dunque portare l'iperpiano u_{11} nell'iperpiano $u_{1s'}$. Ma T_s porta u_{11} in u_{1s}, $T_s T_r$ porterà quindi u_{11} in quell'iperpiano in cui T_r porta u_{1s}, che dovrà dunque essere proprio $u_{1s'}$. Si ha così in generale che *se la sostituzione T_r porta l'iperpiano u_{1s} in $u_{1s'}$, essa trasforma la E_s nella $E_{s'}$*, o in altre parole.

Trasformando le ν sostituzioni E_1, E_2,... E_ν mediante la T_r, queste sostituzioni si scambiano fra loro nello stesso modo con cui T_r scambia fra loro i ν iperpiani $u_{11}\, u_{12} \ldots u_{1\nu}$ e con cui la sostituzione $\Sigma_r = \begin{pmatrix} q_r(\vartheta_{1s}) \\ \vartheta_{1s} \end{pmatrix}$ del gruppo $\Gamma_\nu(K)$ scambia fra loro le ν lettere ϑ_{11}, ϑ_{12},... $\vartheta_{1\nu}$.

Se ε è di grado n e T_r non appartiene a G_e, ma porta u_{11} in u_{1r}, si ha dunque

$$E_r = T_r^{-1} E_1 T_r$$

ed essendo $E_1 \neq E_r$ (numero precedente) si ha così che la

E_1 non è commutabile colla T_r, poichè altrimenti dovrebbe essere $T_r^{-1} E_1 T_r = E_1$. Vediamo dunque che

Le sostituzioni di G_e corrispondenti a un unità di grado n non sono commutabili altro che colle sostituzioni di G_e stesso.

Abbiamo così visto in quali sostituzioni le altre sostituzioni di G_x trasformino quelle di G_e; è inoltre chiaro che non solo G_x contiene come invariante il sottogruppo G_e (N. 12) ma *se il corpo contiene un'unità* ε *di grado n,* G_X *è il più ampio gruppo che goda di tale proprietà,* cioè *ogni sostituzione T che trasformi una qualsiasi sostituzione di G_e in un altra sostituzione, pure di G_e deve necessariamente appartenere a G_x.* Sia infatti Y la forma equivalente in cui T porta la X; e E una sostituzione di G_e corrispondente a un'unità ε di grado n. $T^{-1} E T$ sarà allora evidentemente una sostituzione del sottogruppo G'_e del nuovo gruppo automorfo G_y; d'altra parte essa è, per ipotesi, una sostituzione di G_e, dunque (N. 8) $X = \pm Y$, cioè T appartiene a G_x.

32. Avevamo visto al n. 10 che per una sostituzione T di G_x che non fosse di G_e, doveva aversi, indicando con c_{ik} i coefficienti della T, con $\bar{u}'$ la nuova forma $\sum_k \beta_k^{(s)} y_k = \sum_{ik} c_{ik} \alpha_i^{(s)} y_k$ e con $u'^{(s)}$ la vecchia forma in cui $u^{(s)}$ è portata da T

$$\bar{u}^{(s)} = \sigma_s u'^{(s)} \qquad s = 1, 2, \ldots n$$

e abbiamo anche visto che, essendo $\sigma_1, \sigma_2, \ldots \sigma_n$ n numeri coniugati, doveva aversi necessariamente $N(\sigma_s) = \pm 1$. Supponiamo ora che sia τ il periodo della sostituzione S secondo cui si scambiano gli iperpiani della $X = 0$ in seguito alla T; Dovrà allora aversi, indicando con

$$(u_1, u_2, \ldots u_\tau)$$

un ciclo della S,

$$\begin{aligned}
\bar{u}_1 &= \sigma_1 u_2 \\
\bar{u}_2 &= \sigma_2 u_3 \\
&\cdots\cdots\cdots \\
\bar{u}_{\tau-1} &= \sigma_{\tau-1} u_\tau \\
\bar{u}_\tau &= \sigma_\tau u_1 .
\end{aligned}$$

La τ^{esima} potenza di T lascerà fissi tutti questi iperpiani, e sarà perciò una sostituzione E di G_e corrispondente a una certa unità η del corpo, e, indicando con gli apici le forme che si ottengono dalle antiche dopo eseguita la T^τ, dovrà evidentemente aversi

$$\begin{aligned}
u'_1 &= \sigma_1 \sigma_2 \ldots\ldots \sigma_\tau u_1 \\
u'_2 &= \sigma_2 \sigma_3 \ldots\ldots \sigma_\tau \sigma_1 u_2 \\
&\cdots\cdots\cdots\cdots \\
u'_\tau &= \sigma_\tau \sigma_1 \sigma_2 \ldots\ldots \sigma_{\tau-1} u_\tau
\end{aligned}$$

da cui segue che sarà $\eta = \sigma_1 \sigma_2 \ldots \sigma_\tau$ e

$$u'_r = \eta u_r \qquad r = 1, 2, \ldots . \tau .$$

Se è allora

$$u_r = \sum_i \alpha_i^{(r)} x_i$$

si avrà quindi, indicando con $c_{ik}^{(\tau)}$ i coefficienti della T^τ

1) $$\sum_i c_{ik}^{(\tau)} \alpha_i^{(r)} = \eta \alpha_k^{(r)} \qquad k = 1, 2, \ldots . n$$

2) $$\eta = \frac{\sum_i c_{ik}^{(\tau)} \alpha_i^{(r)}}{\alpha_k^{(r)}} \qquad r = 1, 2, \ldots \tau$$

da cui si vede che η è di grado inferiore o uguale a $\frac{n}{\tau}$, essendo per la 2) $\eta_1 = \eta_2 = \ldots\ldots = \eta_\tau$. Dunque l'equazione di grado n a cui soddisfa η (n. 2)

$$B(\eta) = \begin{vmatrix} c_{11}^{(\tau)} - \eta, & c_{12}^{(\tau)}, \ldots\ldots c_{1n}^{(\tau)} \\ c_{21}^{(\tau)}, & c_{22}^{(\tau)} - \eta, \ldots\ldots c_{2n}^{(\tau)} \\ \ldots\ldots\ldots\ldots\ldots \\ c_{n1}^{(\tau)}, & c_{n2}^{(\tau)}, \ldots\ldots c_{nn}^{(\tau)} - \eta \end{vmatrix} = 0$$

è certo riducibile, anzi il determinante $D(\eta)$ dovrà avere una caratteristica $\leq n - \tau$, poichè tutti i τ sistemi $\alpha_i^{(r)}$ $(i = 1,2,\ldots n,\ r = 1,2,\ldots \tau)$ sono soluzioni del medesimo sistema lineare omogeneo 1). Siccome quel che si è detto per il ciclo $(u_1, u_2, \ldots u_\tau)$ vale poi evidentemente anche per tutti gli altri cicli, pure d'ordine τ (n. 12), in cui si decompone la S si ha in conclusione che gli n coniugati di η sono certo τ a τ eguali e quindi che *il prodotto* η *delle* τ σ_r *corrispondenti a un medesimo ciclo della* S *è in ogni caso un unità di grado uguale a un divisore di* $\frac{n}{\tau}$.

Se inoltre sono $(u_{11}, u_{12}, \ldots u_{1\tau}) \ldots\ldots (u_{\frac{\nu}{\tau},1}, u_{\frac{\nu}{\tau},2}, \ldots u_{\frac{\nu}{\tau},\tau})$ i $\frac{\nu}{\tau}$ cicli della S che scambiano fra i loro i ν iperpiani coniugati equivalenti u_{ir} della forma X, essendo $\sigma_{i1}, \sigma_{i2}, \ldots\ldots$ $\sigma_{i\tau} = \eta_i$ un'unità sarà anche

$$(\sigma_{11}, \sigma_{12}, \ldots \sigma_{1\tau})\ (\sigma_{21}, \ldots \sigma_{2\tau}) \ldots\ldots (\sigma_{\frac{\nu}{\tau},1} \cdot \sigma_{\frac{\nu}{\tau},2} \ldots \sigma_{\frac{\nu}{\tau},\tau}) = \eta_1 \eta_2 \ldots \eta_{\frac{\nu}{\tau}}$$

un'altra unità.

33. Finora abbiamo considerato sostituzioni lineari intere con coefficienti c_{ik} tali che il determinante $|c_{ik}|$ fosse uguale a ± 1, e abbiamo studiato quelle di tali sostituzioni che lasciano X in sè o la cambiano nell'eguale e contraria. Se ci limitiamo invece a considerare soltanto quelle di tali

sostituzioni che lasciano X in sè, dovrà aversi, invece della 8) del n. 10

$$\sigma_1, \sigma_2, \dots \sigma_n = +1$$

cioè $N(\sigma_i) = +1$. Se nel corpo esiste allora un'unità ε di norma -1 è evidente che per ogni sostituzione S sugli iperpiani della X del gruppo Γ_ν esisterà ancora una sostituzione T di G_X che trasformi X in $+X$ e scambi gli iperpiani secondo la S; se infatti a una sostituzione T', certamente esistente, del gruppo automorfo G_X, corrisponde in Γ_ν la S, ma T' porta la X in $-X$, basterà prendere $T = E T'$, ove E indica la sostituzione di G_e corrispondente a ε, e si avrà ancora una sostituzione che scambia gli iperpiani secondo la S e porta X in $+X$. Se invece tutte le unità del corpo sono di norma positiva, ed esistono sostituzioni T_r di G_X che portano X in $-X$ non esisterà, nel sottogruppo $\overline{G}_X$ delle sostituzioni che portano X in $+X$, nessuna sostituzione $\overline{T}_r$ che scambi ancora gli iperpiani della X come la T_r; altrimenti si avrebbe infatti che la $\overline{T}_r\, T_r^{-1}$ sarebbe una sostituzione di G_e, corrispondente a un'unità ε, che porta X in $-X$, ed essendo in questo caso $\sigma_i = \varepsilon_i$, si avrebbe $\varepsilon_1, \varepsilon_2, \dots$ $\varepsilon_n = -1$, cioè $N(\varepsilon) = -1$ contro l'ipotesi. Potremo allora ordinare le sostituzioni di G_X che portano X in $+X$ nel modo solito

$$G_e,\ G_e \overline{T}_2,\ G_e \overline{T}_3, \dots G_e \overline{T}_\mu.$$

A queste sostituzioni di $\overline{G}_X$, corrisponderà allora in Γ_ν un certo sottogruppo Γ_μ di sostituzioni $\overline{S}$; e moltiplicando queste sostituzioni di $\overline{G}_X$ per una sostituzione T di G_X che non sia di $\overline{G}_X$ che cioè porti X in $-X$, avremo poi evidentemente tutte le sostituzioni di G_X che portano X in $-X$,

alle quali corrisponderanno in Γ_ν le sostituzioni che si ottengono moltiplicando quelle di Γ_μ per la sostituzione T^r corrispondente a T. Si ha così che *tanto* $\overline{G}_X$ *che* Γ_μ *saranno due sottogruppi d'indice* 2, *evidentemente invarianti, dei gruppi* G_X *e* Γ_ν *rispettivamente,* da cui $\nu = 2\ \mu$.

Essendo allora Γ_ν il gruppo di Galois per l'equazione 6) del n. 22 si ha quindi che *mediante l'estrazione di un radicale quadratico* [1] *potremo abbassare questo gruppo al sottogruppo invariante* Γ_μ, e siccome questo scambia tra loro i μ iperpiani della X appartenenti a un medesimo gruppo di iperpiani u_{tr} $(r = 1, 2, \ldots \mu)$ equivalenti in senso stretto (cioè tali che sia $\overline{u}_{tr} = \sigma u_{tr'}$, e $N(\sigma) = +1$) si ha ancora, come al n. 22, che la forma X si decompone nel prodotto di $\frac{n}{\mu}$ forme, ognuna di grado μ, i cui coefficienti, essendo funzioni delle ϑ_{tr} $(r = 1, 2, \ldots \mu)$ invarianti per le sostituzioni di $\overline{\Gamma}_\mu$, appartengono ai corpi di grado $\frac{n}{\mu}$ generati dai radicali quadratici estratti, portanti, pel n. 22, su quantità appartenenti a corpi di grado $h = \frac{n}{\nu} = \frac{n}{2\mu}$.

Inoltre queste $\frac{n}{\mu}$ forme sono, per le sostituzioni di $\overline{G}_X$, trasformate ciascuna separatamente in sè medesima, a meno di un fattore di proporzionalità $\sigma_{t1}, \sigma_{t2}, \ldots \sigma_{t\mu}$ che è evidentemente un'unità del corpo.

34. Se il gruppo $\overline{G}_X$ delle sostituzioni che portano X in $+X$ contenesse poi anche sostituzioni con coefficienti

---

[1] BIANCHI. « Gruppi di sostituzioni », ecc.

c_{ik}, tali che $|c_{ik}| = -1$, e se fosse $\Gamma'_{\mu'}$ il gruppo corrispondente delle sostituzioni sugli iperpiani si vedrebbe, in modo perfettamente analogo che il *sottogruppo* $\overline{G}'_x$ *delle sostituzioni con determinante* $+1$, *e il sottogruppo* $\Gamma'_{\mu'}$ *corrispondente, sarebbero ambedue due sottogruppi invarianti d'indice* 2 *in* $\overline{G}_x$ *e* Γ_μ *rispettivamente,* e sarebbe quindi possibile, mediante l'estrazione di un ulteriore radicale quadratico, abbassare ancora il gruppo di Galois Γ_μ al suo sottogruppo $\Gamma'_{\mu'}$.