LE ALGEBRE NEI CORPI FINITI DOTATE DI MODULO E COMMUTATIVE (*)

La lettura delle due elaborate Memorie del MIGNOSI (1) sui campi di integrità finiti mi ha dato occasione recentemente di rilevare che delle sue ricerche quelle riferentisi ai campi contenenti dei corpi numerici possono ricever luce dalla applicazione metodica della teoria generale delle algebre (2).

Poichè i risultati che così si incontrano non sembrano privi di interesse e completano in qualche punto quelli del MIGNOSI, non credo inutile il fissarli in questa breve Nota.

1. Sia A un'algebra commutativa d'ordine n, in un corpo finito Γ, col modulo u e quindi certo non pseudonulla.

Essa o è priva di elementi eccezionali, indi semi-semplice, o possiede un sotto-algebra eccezionale (propria) E; e in tale ultimo caso l'algebra $A - E$, complementare di E rispetto ad A, è semi-semplice (*C. N. A.* pag. 254, n. 148).

Esaminiamo separatamente le due alternative.

2. Se A è semi-semplice essa o è addirittura semplice, o è una somma diretta di algebre semplici; e se è semplice è il prodotto diretto di due sue sotto-algebre, aventi lo stesso suo modulo, delle

(*) *Rend. Reale Acc. di Scienze Fisiche e Mat. di Napoli,* (4) 4 (1934), pp. 147-153.

(1) G. MIGNOSI, *I campi d'integrità finiti di 1ª specie contenenti un corpo* (Rendiconti del Circolo Matematico di Palermo, t. LVI, 1932); e *Sui campi d'integrità di specie qualunque e su quelli di 2ª specie contenenti un corpo* (Ibid. t. LVII 1933).

(2) Nel seguito per quanto occorre ricordare della teoria in discorso rinvio, con la sigla *C. N. A.*, al mio trattato: *Corpi numerici e algebre* (Messina Principato, 1921).

quali una è primitiva, l'altra regolare (*C. N. A*, pag. 332, n. 230). Intanto un'algebra regolare di ordine > 1 non è certo commutativa, dunque attesa la commutatività di A, A non può esser semplice, se non a patto d'essere addirittura primitiva.

Ma allora A, se è semplice, può considerarsi come un corpo numerico isomorfo al corpo algebrico $[\Gamma, f(\xi)]$ derivato da Γ mediante un polinomio ivi irriducibile $f(\xi)$ di grado n (cfr. *C. N. A.*, pag. 454); e, se y è un elemento di A di rango n (per es. quello corrispondente all'elemento ξ di $[\Gamma, f(\xi)]$ in una corrispondenza di isomorfismo), gli elementi di A sono dati tutti, e ciascuno una volta sola, dall'espressione

$$\lambda_0 y^{n-1} + \lambda_1 y^{n-2} + \ldots + \lambda_{n-2} y + \lambda_{n-1} u \tag{1}$$

al variare delle λ fra i numeri di Γ.

Se invece A è somma diretta di t (> 1) algebre semplici (indi primitive) $A_1, A_2, \ldots, A_t$ degli ordini $n_1, n_2, \ldots, n_t$ ($n_1 + n_2 + \ldots + n_t = n$), con i moduli (mutuamente nullifici) $u_1, u_2, \ldots, u_t$, sarà

$$u = u_1 + u_2 + \ldots + u_t, \tag{2}$$

per ciascun elemento x di A sussisterà un'eguaglianza ed una sola del tipo

$$x = x_1 + x_2 + \ldots + x_t, \tag{3}$$

con x_i in A_i, e ciascuna delle algebre A_i avrà una struttura simile a quella indicata per A nell'ipotesi precedente.

Avvertasi che, poichè le algebre A_i sono primitive, indi prive di divisori dello zero, *l'elemento x di A dato dalla* (3) *riesce un divisore dello zero quando, e solo quando, gli elementi $x_1, x_2, \ldots x_t$ non sono tutti nulli, ma è nullo almeno uno di essi* (*C. N. A.*, pag. 244).

3. Supponiamo ora che A possegga la sotto-algebra eccezionale E e indichiamo con $[x]$ la classe mod E individuata da un elemento di A che sia stato indicato con x, di guisa che, se x percorre A, $[x]$ descriverà $A - E$.

L'algebra $A - E$ è semi-semplice e dotata del modulo $[u]$, dunque o è semplice, e allora, per quanto è detto nel n. prec., è addirittura primitiva, o è somma diretta di algebre primitive.

4. Si dia la prima alternativa e sia ν l'ordine di $A - E$ (cioè, $n - \nu$ l'ordine di E).

Allora, se $[y]$ è un elemento di $A - E$ di rango ν gli elementi di $A - E$ sono dati tutti, e ciascuno una volta sola, dall'espressione

$$(4) \qquad [x] = \lambda_0 [y]^{\nu-1} + \lambda_1 [y]^{\nu-2} + \ldots + \lambda_{\nu-2} [y] + \lambda_{\nu-1} [u]$$

al variare delle λ in Γ, e quindi gli elementi di A sono dati tutti, e ciascuno una volta sola, dall'espressione

$$(5) \qquad x = \lambda_0 y^{\nu-1} + \lambda_1 y^{\nu-2} + \ldots + \lambda_{\nu-2} y + \lambda_{\nu-1} u + e,$$

al variare delle λ in Γ e di e in E.

Si indichi con $\Phi(\xi) = 0$ l'equazione minima di x in A e con $\varphi(\xi) = 0$ quella di $[x]$ in $A-E$. Per un teorema noto (*C. N. A.*, pag. 377, n. 270) $\Phi(\xi)$ sarà divisibile per $\varphi(\xi)$ e le potenze di $\varphi(\xi)$ con esponenti abbastanza elevati saranno divisibili per $\Phi(\xi)$; d'altronde essendo $A - E$ primitiva, $\varphi(\xi)$ è, in Γ, irriducibile (*C. N. A.*, pag. 326, n. 222) duque $\Phi(\xi)$ è una potenza di $\varphi(\xi)$, poniamo $\Phi(\xi) = [\varphi(\xi)]^\tau$.

Ora x riesce privo di inverso, cioè nullo o divisore dello zero, se, e soltanto se, $\Phi(\xi)$ è divisibile per ξ (*C. N. A.*, pag. 228, n. 124 in fine) dunque ciò accade, se, e soltanto se, è $\varphi(\xi) = \xi$, ossia $[x] = [0]$, o, in altri termini, se x sta in E.

Si deduce che:

Nell'ipotesi attuale i divisori dello zero di A sono tutti, e solo, gli elementi non nulli di E.

A proposito dell'esponente τ della potenza di $\varphi(\xi)$ eguale a $\Phi(\xi)$ non è forse inutile osservare che:

Se μ è il grado di $\varphi(\xi)$, è $\tau \leq \dfrac{n-\nu}{\mu} + 1.$

Essendo μ il grado di $\varphi(\xi)$, è $\mu\tau$ quello di $\Phi(\xi)$: ciò significa che i $\mu\tau$ elementi di A

$$(6) \qquad u, x, x^2, \ldots, x^{\mu\tau-1}$$

sono indipendenti: e dunque, supposto $\tau > 1$ — chè, altrimenti, la diseguaglianza da dimostrare sarebbe evidente —, sono tali anche gli elementi

$$(7) \qquad \varphi(x), x\varphi(x), x^2\varphi(x), \ldots, x^{\mu(\tau-1)-1}\varphi(x).$$

Ma essendo

$$\varphi([x]) = [\varphi(x)] = [0],$$

$\varphi(x)$, indi, attesa l'eccezionalità di E, ogni altro elemento della

serie (7), appartiene ad E, dunque i $\mu(\tau-1)$ elementi (7) sono altrettanti elementi indipendenti di E. Ma l'ordine di E è $n-\nu$, per conseguenza si ha $\mu(\tau-1)\leq n-\nu$; cioè, come volevasi,

$$\tau \leq \frac{n-\nu}{\mu}+1. \tag{8}$$

Quanto alla struttura dell'algebra (pseudonulla) E nel caso che qui si esamina, vi è da osservare che:

Se $\nu>1$ e l'indice di E è r, l'ordine di E^{r-1} è necessariamente >1.

Si supponga che E^{r-1} sia del 1^0 ordine e sia $e'\neq 0$ un elemento di E^{r-1}, sicchè ogni altro sarà il prodotto scalare di e' per un numero di Γ.

Ora sia

$$\psi(\xi)=\xi^{\nu}+\alpha_1\xi^{\nu-1}+\ldots+\alpha_{\nu-1}\xi+\alpha_{\nu}=0 \tag{9}$$

l'equazione minima di $[y]$ in $A-E$. Sarà

$$y^{\nu}+\alpha_1 y^{\nu-1}+\ldots+\alpha_{\nu-1}y+\alpha_{\nu}u=e'', \tag{10}$$

con e'' elemento conveniente di E.

Intanto da $ye'=\gamma e'$, con γ in Γ, si trae successivamente,

$$y^2e'=y\cdot\gamma e'=\gamma\cdot ye'=\gamma^2e',\quad y^3e'=\gamma^3e',\ldots,y^{\nu}e'=\gamma^{\nu}e', \tag{11}$$

quindi moltiplicando la (10), membro a membro, per e', badando che $e'e''$, come elemento di E^r, è nullo e tenendo conto delle (11) si ha

$$(\gamma^{\nu}+\alpha_1\gamma^{\nu-1}+\ldots+\alpha_{\nu-1}\gamma+\alpha_{\nu})e'=0.$$

Ma $e'\neq 0$; dunque è

$$\gamma^{\nu}+\alpha_1\gamma^{\nu-1}+\ldots+\alpha_{\nu-1}\gamma+\alpha_{\nu}=0$$

e la (9) ammette la radice γ. Ma la (9) è irriducibile in Γ, dunque è $\nu=1$; cioè, se l'ordine di E^{r-1} è 1, è necessariamente $\nu=1$. Da ciò il teorema.

Si supponga ora $\nu>1$ e si indichino con $n_2,\ldots,n_{r-1}$, gli ordini di $E^2,E^3,\ldots,E^{r-1}$.

Essendo $E > E^2 > E^3 > \ldots > E^{r-1}$ sarà

$$n - \nu \geq n_2 + 1,\ n_2 \geq n_3 + 1, \ldots, n_{r-2} \geq n_{r-1} + 1,\ n_{r-1} \geq 2,$$

ossia $n - \nu \geq r$; dunque:

Se $\nu > 1$, *per l'indice* r *di* E *si ha* $r \leq n - \nu$.

Come è noto, un'algebra pseudonulla potenziale di ordine $n-\nu$ ha per indice $n - \nu + 1$ (*C. N. A.*, pag. 322, n. 218) dunque:

Se $\nu > 1$, *l'algebra* E *non è certo potenziale.*

La (8), per $\mu = \nu$, dà $\tau \leq \frac{n}{2}$; quindi, se fosse $\nu > \frac{n}{2}$ sarebbe necessariamente $\tau = 1$, l'equazione minima di y in A coinciderebbe con quella di $[y]$ in $A - E$, cioè nella (10) sarebbe $e'' = 0$, e lo stesso avverrebbe per ogni altro elemento di A appartenente alla classe $[y]$.

Ora ciò è assurdo. Infatti si indichi con e_1 un elemento non nullo di E^{r-1}, nella classe $[y]$ si consideri l'elemento $y + e_1$, e si supponga, se è possibile, che sia nel tempo stesso

$$\psi(y) = 0 \quad \text{e} \quad \psi(y + e_1) = 0.$$

Poichè e_1 è in E^{r-1} sono nulle tutte le potenze di e_1 con esponenti > 1, quindi è, per ogni intero $k > 1$,

$$(y + e_1)^k = y^k + k y^{k-1} e_1,$$

e, indicata con $\psi'(\xi)$ la derivata di $\psi(\xi)$, si ha

$$0 = \psi(y + e_1) = \psi(y) + \psi'(y)\, e_1 = \psi'(y)\, e_1.$$

Ora la derivata $\psi'(\xi)$, attesa l'irriducibilità di $\psi(\xi)$, non è certo nulla (*C. N. A.*, pp. 162-163); d'altronde il grado di $\psi'(\xi)$ è inferiore a quello di $\psi(\xi)$, dunque $\psi'(y) \not\equiv 0$. Intanto la sotto-algebra potenziale di A generata da y, per l'ipotesi che l'equazione minima di y in A sia $\psi(\xi) = 0$, è primitiva; dunque $\psi'(y)$ non è neppure un divisore dello zero, e da $\psi'(y)\, e_1 = 0$ segue $e_1 = 0$. Ciò contrasta con l'ipotesi fatta su e_1, dunque è certo $\nu \leq \frac{n}{2}$, ossia:

L'ordine di E *è non inferiore ad* $\frac{n}{2}$ [3].

[3] Come mostrerò in una Nota successiva, che uscirà nei Rendiconti dei Lincei, alle algebre nei corpi finiti può essere esteso un teorema dello WEDDERBURN da lui dimostrato per le algebre nei corpi a sottocorpo fondamentale isomorfo al corpo razionale: allora le osservazioni di questo n° potranno essere assai meglio precisate.

5. Supponiamo ora che $A - E$ sia somma diretta di s algebre primitive

$$(A - E)_1 , (A - E)_2 , \dots , (A - E)_s ,$$

degli ordini $\nu_1 , \nu_2 , \dots , \nu_s$, di guisa che l'ordine di E sarà $n - \nu_1 - \nu_2 - \dots - \nu_s$.

Se il modulo di $(A - E)_i$ si indica con $[v_i]$, è lecito supporre, in primo luogo, che v_i sia un automodulo di A (*C.N.A.*, pag. 283), e in secondo luogo che sia

$$u = v_1 + v_2 + \dots + v_s , \tag{12}$$

con $v_1 , v_2 , \dots , v_s$ mutuamente nullifici (cfr. *C. N. A.*, pag. 373 n. 277).

Se $[x]$ è un qualsiasi elemento di $A - E$, per $[x]$ sussiste un'eguaglianza, ed una sola del tipo

$$[x] = [x_1] + [x_2] + \dots + [x_s], \tag{13}$$

con $[x_i]$ in $(A - E)_i$; d'altronde, indicando con $[y_i]$ un conveniente elemento di $(A - E)_i$, per $[x_i]$ sussiste un'eguaglianza ed una sola del tipo

$$[x_i] = \lambda_0^{(i)} [y_i]^{\nu_i - 1} + \lambda_1^{(i)} [y_i]^{\nu_i - 2} + \dots + \lambda_{\nu_i - 1}^{(i)} [v_i],$$

con le $\lambda_j^{(i)}$ numeri di Γ, dunque:

Se x è un elemento qualsiasi di A, per x sussiste un'eguaglianza ed una sola del tipo

$$x = \sum_i^{1 \dots s} (\lambda_0^{(i)} y_i^{\nu_i - 1} + \lambda_1^{(i)} y_i^{\nu_i - 2} + \dots + \lambda_{\nu_i - 1}^{(i)} v_i) + e, \tag{14}$$

con le λ numeri di Γ ed e elemento di E.

Giacchè l'algebra $(A - E)_i$ è primitiva, l'equazione minima $\varphi_i(\xi) = 0$ di $[x_i]$ in $(A - E)_i$ è irriducibile. Intanto, se l'equazione minima di $[x]$ in $A - E$ è $\varphi(\xi) = 0$, $\varphi(\xi)$ è il minimo comune multiplo dei polinomi $\varphi_1(\xi), \varphi_2(\xi) , \dots , \varphi_s(\xi)$ (*C. N. A.*, pag. 243), dunque $\varphi(\xi)$ è il prodotto di quanti fra questi polinomi riescono distinti. Segue, per

il teorema più sopra ricordato, che, se $\Phi(\xi) = 0$ è l'equazione minima di x in A, $\Phi(\xi)$ è un prodotto di potenze dei polinomi $\varphi_i(\xi)$ fra di loro diversi.

Intanto x è privo di inverso, se, e solo se, $\Phi(\xi)$ è divisibile per ξ, indi almeno uno dei polinomi $\varphi_i(\xi)$ eguale a ξ, cioè almeno uno degli elementi $[x_i]$ eguale a $[0]$, dunque:

Supposto che l'elemento x definito dalla (14) *non sia nullo, che cioè nella* (14) *non siano nulli tutti i coefficienti λ e nullo e, esso riesce un divisore dello zero, se, e soltanto se, almeno per un valore di i sono nulle tutte le $\lambda^{(i)}$.*

6. Dire che A è un'algebra in un corpo finito, commutativa e dotata di modulo, è quanto dire, con la terminologia del MIGNOSI, che A è un campo di integrità finito contenente un corpo numerico, per il quale un elemento di A riesce periodico, pseudonullo o pseudoperiodico, secondo che è dotato di inverso, oppure è (pseudonullo, indi, attesa la commutatività di A [*C. N. A.*, pag. 236, n^0 133]) eccezionale, o, infine, è un divisore dello zero, ma non è eccezionale.

Ma allora codesto campo, se non è addirittura un corpo numerico è di 2^a specie ed incompleto, se A è semi-semplice, ma non semplice; di 1^a specie e proprio, se A non è semi-semplice, ed $A—E$ è semplice; di 2^a specie e completo, se $A—E$ è semi-semplice, ma non semplice.

Il numero degli elementi non nulli di A è in ogni caso $p^{mn}—1$, se p^m (con p numero primo) è quello degli elementi di Γ; poi, codesti elementi, per quanto via via è stato osservato:

Se A è un campo di 2^a specie incompleto e per A si mantengono le ipotesi e le notazioni del n. 2, si ripartiscono in

$$\prod_{i}^{1\ldots t}(p^{mn_i} - 1)$$

elementi periodici e

$$p^{mn} - 1 - \prod_{i}^{1\ldots t}(p^{mn_i} - 1)$$

elementi pseudoperiodici;

Se A è un campo di 1^a specie e per esso si mantengono le ipotesi e le notazioni del n. 4, si ripartiscono in $p^{m(n-\nu)} - 1$ elementi pseudonulli, e $p^{mn} - p^{m(n-\nu)}$ elementi periodici;

Se infine A è un campo di 2ª specie completo e per esso sussistono le ipotesi e notazioni del n. 5, si ripartiscono in

$$p^{m(n-\nu_1-\ldots-\nu_s)} \prod_i^{1\ldots t} (p^{m\nu_i} - 1)$$

elementi periodici, in

$$p^{m(\nu_1-\ldots-\nu_s)} - 1$$

elementi pseudonulli, e

$$p^{nm} - p^{m(\nu_1-\ldots-\nu_s)} \left\{ \prod_i^{1\ldots s} (p^{m\nu_i} - 1) + 1 \right\}$$

elementi pseudoperiodici.