SOPRA UN TEOREMA FONDAMENTALE DELLA TEORIA DELLE ALGEBRE (*)

Nella sua classica Memoria *On hypercomplex numbers* lo WEDDERBURN credette di poter stabilire, generalizzando un teorema del CARTAN, che un'algebra, non pseudonulla e non semi-semplice, è, in ogni caso, la somma (in generale, non diretta) di due sotto-algebre, delle quali una è semi-semplice e l'altra è la sotto-algebra eccezionale; ma la sua dimostrazione, assai laboriosa, lasciava l'adito a dubbi non lievi.

Sottoposte più tardi ad un esame più accurato la detta proposizione e la prova relativa, lo WEDDERBURN riescì a semplificare quest'ultima ed a porla al riparo di ogni obiezione, ma dovette introdurre nell'enunciato di quella un'ipotesi restrittiva; e cioè dovette supporre che in esso si parlasse non già di algebre qualsiansi, ma di algebre definite in corpi numerici a sottocorpo fondamentale infinito (indi isomorfo al corpo razionale) (1).

In tal forma appunto si trova presentato il teorema nel libro del DICKSON *Algebras and their arithmetics*, ove apparve per la prima volta la nuova dimostrazione dello WEDDERBURN.

Ma in realtà, il teorema è vero anche per le algebre nei corpi finiti; esso non può cadere in difetto che per algebre in corpi infiniti, ma a sottocorpo fondamentale finito.

È quanto si vuol stabilire in questa Nota, nella quale vengono anche dedotte alcune conseguenze del teorema in discorso, che non sembra siano state mai osservate e che, per quanto semplici, non paiono prive di interesse.

(*) *Rend. Reale Accad. dei Lincei,* (6) 20 (1934), pp. 65-72.

(1) Per questa nozione vedi G. SCORZA, *Corpi numerici e algebre* (Messina, Principato, 1921), p. 19 e sgg.; volume che in tutto il seguito sarà indicato con la sigla *C. N. A.*

1. Premettiamo la seguente osservazione:

Se u è un automodulo principale dell'algebra A, un elemento è eccezionale per la sotto-algebra uAu, quando, e solo quando, è eccezionale per A;

asserzione che sarà evidentemente provata non appena sia fatto vedere che, se y è un elemento eccezionale per uAu, esso è tale anche per A. E per questo giova supporre che A sia priva di modulo, indi dotata di sotto-algebra eccezionale, che diremo E, perchè altrimenti il modulo sarebbe u, e, risultando allora $uAu = A$, l'enunciato si ridurrebbe ad una tautologia.

Essendo u un automodulo principale di A si può porre (*C.N.A.*, p. 277)

$$A = uAu + S, \qquad \text{con } uAu \cap S = 0 \text{ ed } S \leq E;$$

quindi, se x è un elemento qualsiasi di A, sussiste un'eguaglianza (ed una sola) del tipo

$$x = x_1 + s,$$

con x_1 in uAu ed s in S, indi in E.

Data l'invarianza di E in A, risultano contenuti in E, al pari di s, tutti i prodotti che contengono s a fattore, quindi, qualunque sia l'intero positivo h è

$$(xy)^h = (x_1 y + sy)^h = (x_1 y)^h + e_h,$$

con e_h elemento conveniente di E. In virtù dell'ipotesi fatta su y, $x_1 y$ è, al pari di y, contenuto nella sotto-algebra eccezionale di uAu, quindi per h abbastanza elevato, è $(x_1 y)^h = 0$, ossia $(xy)^h = e^h$. Intanto e_h è nullo o pseudonullo, quindi è tale anche xy; e poichè x è un qualsiasi elemento di A, ciò significa che y è eccezionale per A.

2. *Se A è un'algebra, di ordine n, in un corpo finito Γ, dotata di un unico automodulo u, si può porre $A = P + E$, dove P è una algebra primitiva ed E, o è zero, o è la sotto-algebra eccezionale di A.*

Poichè u è l'unico automodulo di A, esso è primitivo e principale; quindi uAu non contiene automoduli diversi dal suo modulo u ed è

$$A = uAu + S,$$

dove S o è zero, o è contenuto nella sotto-algebra eccezionale di A.

Segue, per il lemma precedente, che il teorema sarà stabilito per A quando sia stato dimostrato per uAu; dunque non si vien meno alla generalità se, come appunto vogliamo fare, si suppone che u sia addirittura il modulo di A.

In un'algebra dotata di modulo, ma priva di automoduli diversi dal modulo, ogni eventuale divisore dello zero è addirittura un elemento eccezionale (*C. N. A.*, p. 264); quindi A o è primitiva, o è dotata di sotto-algebra eccezionale. Scartato il primo caso, nel quale il teorema è evidente, supponiamo che si verifichi il secondo, e sia E la sotto-algebra eccezionale di A.

Indichiamo con $[x]$ la classe modulo E individuata da un elemento di A che sia stato denotato con x; di guisa che $[x]$ descriverà l'algebra $A - E$, complementare di E rispetto ad A, allorchè x descrive A.

L'algebra $A - E$ è primitiva (*C. N. A.*, p. 284) e il suo modulo è $[u]$; inoltre il corpo Γ è finito, dunque, se il suo ordine è ν, per un bel teorema dello WEDDERBURN (*C. N. A.*, p. 450 e sgg.), essa è isomorfa ad un corpo algebrico dedotto da Γ mediante un polinomio $\varphi(\xi)$ di grado ν, irriducibile in Γ. Segue che $A - E$ ammette elementi con l'equazione minima $\varphi(\xi) = 0$, e se $[y]$ è uno di essi posto

$$\varphi(\xi) = \xi^\nu + \alpha_1 \xi^{\nu-1} + \ldots + \alpha_{\nu-1} \xi + \alpha_\nu ,$$

si avrà

$$[y]^\nu + \alpha_1 [y]^{\nu-1} + \ldots + \alpha_{\nu-1} [y] + \alpha_\nu [u] = [0],$$

cioè

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

con e' elemento di E.

Poichè $\varphi(\xi)$ è irriducibile in Γ, la sua derivata $\varphi'(\xi)$ non è certo nulla (*C. N. A.*, p. 163); d'altronde $\varphi(\xi) = 0$ è l'equazione minima di $[y]$ in $A - E$, dunque è $[\varphi'(y)] = \varphi'([y]) \neq [0]$, cioè $\varphi'(y)$ è un elemento di A esterno ad E, indi dotato di inverso. Ebbene poniamo

$$e'' = - e' \{\varphi'(y)\}^{-1}, \tag{2}$$

di guisa che e'' sarà, al pari di e', un elemento di E.

La (1) e (2) mostrano che e' ed e'' appartengono alla sotto-algebra potenziale di A generata da y, e questa è commutativa; dunque e' ed e'' sono permutabili con y e $\{\varphi'(y)\}^{-1}$.

Ciò premesso, pongasi

$$z = y + e'',$$

di guisa che z sarà come y un elemento della classe $[y]$.

Per ogni intero positivo $k > 1$ si avrà, indicando con c_k un conveniente elemento di A,

$$z^k = y^k + k y^{k-1} e'' + c_k e''^2;$$

quindi sarà

$$\varphi(z) = \varphi(y) + \varphi'(y) e'' + c e''^2,$$

con c elemento di A. Ma

$$\varphi(y) + \varphi'(y) e'' = \epsilon' - \epsilon' = 0,$$

dunque resta

$$\varphi(z) = c e''^2, \tag{3}$$

ossia $\varphi(z)$ è un elemento di E^2.

Ora si immagini di ripetere per z il ragionamento che si è fatto per y. Come dall'elemento y della classe $[y]$, per il quale $\varphi(y)$ è in E, si è passati all'elemento z della classe stessa per il quale $\varphi(z)$ è in E^2, così da z si passerà ad un elemento t della classe $[z] = [y]$ per il quale $\varphi(t)$ è in E^4.

Si conclude, ripetendo questa argomentazione un conveniente numero di volte, che esiste certo nella classe $[y]$ un elemento, e sia v, per il quale $\varphi(v)$ riesce un elemento di E^s, con s intero positivo non inferiore all'indice di E. Ma per un tale valore di s è $E^s = 0$, dunque è $\varphi(v) = 0$.

Quest'uguaglianza, attesa l'irriducibilità di $\varphi(\xi)$, mostra che $\varphi(\xi) = 0$ è l'equazione minima di v in A; dunque la sotto-algebra potenziale P di A generata da v è dell'ordine ν. Intanto, essendo $[v] = [y]$, l'equazione minima di $[v]$ in $A - E$ è pure $\varphi(\xi) = 0$, dunque $A - E$ coincide con l'algebra potenziale generata da $[v]$ e qualunque sia l'elemento $[x]$ di $A - E$ sussiste un'eguaglianza ed una sola del tipo

$$[x] = \lambda_1 [v]^{\nu-1} + \lambda_2 [v]^{\nu-2} + \ldots + \lambda_{\nu-1} [v] + \lambda_\nu [u],$$

con le λ numeri di Γ.

Ciò significa che qualunque sia x in A, si ha per x un'eguaglianza ed una sola del tipo

$$x = \lambda_1 v^{\nu-1} + \lambda_2 v^{\nu-2} + \ldots + \lambda_{\nu-1} v + \lambda_\nu u + e,$$

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

Ma al variare delle λ in Γ l'elemento

$$\lambda_1 v^{\nu-1} + \lambda_2 v^{\nu-2} + \ldots + \lambda_{\nu-1} v + \lambda_\nu u$$

descrive l'algebra P primitiva (ed isomorfa ad $A - E$), dunque è

$$A = P + E$$

e il teorema è dimostrato.

3. Dopo ciò un ragionamento noto, che qui si riporta solo per comodità del lettore e per chiarezza di quanto segue, mostra che:

Se A è un'algebra in un corpo finito Γ essa o è pseudonulla, o è semi-semplice, o è somma di due sotto-algebre delle quali l'una è semi-semplice e dotata di modulo, l'altra è la sotto-algebra eccezionale.

Suppongasi, infatti, che A non sia nè pseudonulla, nè semi-semplice, indi dotata di sotto-algebra eccezionale (propria) E; e, come è lecito senza venir meno alla generalità, si supponga che A sia dotata di modulo e che questo sia u.

Infine la *segnatura* (*C. N. A.*, p. 355), di $A - E$, cioè di A, sia $(p_1, p_2, \ldots, p_m)$.

Se $m = 1$ e $p_1 = 1$, A è a modulo primitivo, indi non ammette automoduli diversi dal modulo e il teorema ora enunciato si riduce a quello del n. 2.

Se $m = 1$ ma $p_1 > 1$, A è il prodotto diretto di un'algebra B a modulo primitivo e di un'algebra regolare C di ordine p_1^2. Ma per il teorema del n. 2 è

$$B = P + E_1,$$

dove P è un'algebra primitiva ed E_1 è la sotto-algebra eccezionale di B; dunque

$$A = B \times C = P \times C + E_1 \times C.$$

Ora $P \times C$ è un'algebra semplice, ed $E_1 \times C$ è la sotto-algebra eccezionale di A, dunque anche in questo caso il teorema è dimostrato.

Se $m > 1$, è

$$A = H_1 \dot{+} H_2 \dot{+} \ldots \dot{+} H_m + S,$$

dove H_j è un'algebra dotata di modulo con la segnatura (p_j), ed $S < E$.

Ma, per quanto or ora è stato detto, è

$$H_j = K_j + E_j$$

dove K_j è semplice ed E_j zero, o è la sotto-algebra eccezionale di H_j; dunque

$$A = K_1 \dot{+} K_2 \dot{+} \ldots \dot{+} K_m + \sum_{j}^{1\ldots m} E_j + S.$$

Ora

$$\sum_{j}^{1\ldots m} E_j + S = E,$$

e $K_1 \dot{+} K_2 \dot{+} \ldots \dot{+} K_m$ è un'algebra semi-semplice, quindi il teorema è pienamente dimostrato.

4. Giustifichiamo adesso quanto è stato detto nelle righe introduttive a proposito delle algebre nei corpi infiniti, ma a sotto-corpo fondamentale finito, mostrando che esistono in codesti corpi delle algebre per le quali il teorema del n. 3 cade in difetto.

Sia $C[2]$ il corpo costituito dalle due classi in cui si distribuiscono gli interi relativi rispetto al modulo 2, e sia Γ il corpo derivato da $C[2]$ mediante l'aggiunta dell'indeterminata, ξ. Detta ζ un'ulteriore indeterminata, nel corpo Γ l'equazione

$$\varphi(\zeta) = \zeta^2 + \xi = 0 \tag{4}$$

sarà irriducibile.

Ciò posto, si consideri in Γ l'algebra potenziale A col modulo u generata da un elemento j con l'equazione minima

$$j^4 + \xi^2 u = 0. \tag{5}$$

Il suo elemento corrente sarà

$$x = \lambda_0 u + \lambda_1 j + \lambda_2 j^2 + \lambda_3 j^3 \tag{6}$$

con le λ numeri di Γ, cioè frazioni algebriche con l'indeterminata ξ nel corpo $C[2]$.

La (5), badando che *in* Γ è $2 = 0$, può scriversi

$$(j^2 + \xi u)^2 = 0 \tag{7}$$

e dunque, se poniamo

$$\omega = j^2 + \xi u, \tag{8}$$

è $\omega^2 = 0$ ed ω è un elemento (pseudonullo, indi attesa la commutabilità di A) eccezionale. Allora anche

$$j\omega = j^3 + \xi j \tag{9}$$

è eccezionale, con $(j\omega)^2 = 0$; e avvertasi che ω e $j\omega$ sono indipendenti, perchè altrimenti l'equazione minima di j non sarebbe del 4^0 grado.

Poichè *in* Γ è $2\lambda_2 \xi u = 2\lambda_3 \xi j = 0$, l'elemento x può scriversi

$$x = (\lambda_0 + \lambda_2 \xi)\, u + (\lambda_1 + \lambda_3 \xi)\, j + \lambda_2 \omega + \lambda_3 j\omega. \tag{10}$$

Detta E la sotto-algebra eccezionale e indicata con $[x]$ la classe mod. E individuata da x, la (10) dà

$$[x] = (\lambda_0 + \lambda_2 \xi)\, [u] + (\lambda_1 + \lambda_3 \xi)\, [j].$$

Ma per la (8)

$$[j]^2 + \xi\, [u] = [0],$$

e la (4) è irriducibile in Γ; dunque $[x]$, al variar di x, descrive un'algebra primitiva del 2^0 ordine. Ciò significa che anche E è dell'ordine 2 e generata dalle unità ω e $j\omega$.

Se A, in conformità del teorema del n. 3, fosse somma di una algebra primitiva P e di E, riuscendo certo nulla l'intersezione di P ed E, sarebbe P isomorfa ad $A - E$ e dunque dovrebbe esistere in A un elemento x per il quale risultasse, come per l'elemento $[j]$ di $A - E$, $x^2 + \xi u = 0$, o, ciò che *in* Γ fa lo stesso,

$$x^2 = \xi u\,.$$

Ora questo è impossibile. La (10) dà

$$x^2 = (\lambda_0 + \lambda_2 \xi)^2 u + (\lambda_1 + \lambda_3 \xi)^2 j^2 = \tag{11}$$

$$= [(\lambda_0 + \lambda_2 \xi)^2 + (\lambda_1 + \lambda_3 \xi)^2 \xi] u + (\lambda_1 + \lambda_3 \xi)^2 \omega,$$

quindi perchè venga x^2 eguale ad un multiplo scalare di u, occorre che sia $(\lambda_1 + \lambda_3 \xi)^2 = 0$. Ma quando ciò accade la (11) diviene

$$x^2 = (\lambda_0 + \lambda_2 \xi)^2 u,$$

e qui è impossibile avvalersi di λ_0 e λ_2 in modo che riesca

$$(\lambda_0 + \lambda_2 \xi)^2 = \xi,$$

dunque *l'algebra A non è somma di un'algebra primitiva e della sotto-algebra eccezionale.*

5. Sia ora Γ un corpo numerico infinito o finito, secondo che tale è il suo sotto-corpo fondamentale, e sia A un'algebra in Γ; di guisa che ad A sarà applicabile il teorema dello WEDDERBURN.

Supponiamo che A sia dotata di modulo e di sotto-algebra eccezionale E e che l'algebra $A - E$ sia semplice. Dico che:

Se in conformità del detto teorema, si pone

$$A = R + E,$$

con R algebra semplice, l'ordine n_1 di R è un divisore comune degli ordini n ed $n - n_1$ di A ed E, e l'indice r di E non supera il quoziente n/n_1.

Sia (p_1) la segnatura di A; allora è

$$A = B \times C, \quad B = P + E_1, \quad R = P \times C, \quad E = E_1 \times C,$$

dove — dalle algebre B, C, P, E_1 — B è a modulo primitivo, C è regolare e dell'ordine p_1^2, P è primitiva ed E_1 è la sotto algebra eccezionale di B. Sia ν l'ordine di P.

Il modulo di P coincide con quello di B, quindi, per un teorema noto (*C. N. A.*, p. 327), l'ordine di B è divisibile per quello di P. Se l'indichiamo con $q\nu$, in base alle uguaglianze $A = B \times C$ ed $R = P \times C$, sarà

$$n = q \nu p_1^2, \qquad n_1 = \nu p_1^2;$$

per conseguenza n_1 riesce, come volevasi, un divisore di n (ed $n - n_1$).

Da $E = E_1 \times C$ si trae, qualunqne sia l'intero positivo s,

$$E^s = E_1^s \times C^s = E_1^s \times C.$$

Dunque l'indice r di E è quello di E_1.

L'algebra E_1^s, per $s < r$, è, al pari di E_1, invariante in B, perchè da

$$BE_1 = E_1 B = E_1 \ (^2)$$

si trae, se $s > 1$,

$$BE_1^s = BE_1 \cdot E_1^{s-1} = E_1 \cdot E_1^{s-1} = E_1^s \quad \text{e similmente} \quad E_1^s B = E_1^s;$$

inoltre si ha $P^2 = P$ ed $E_1^{2s} < E_1^s$, quindi riesce

$$(P + E_1^s)^2 = P^2 + PE_1^s + E_1^s P + E_1^{2s} = P + E_1^s$$

e $P + E_1^s$ è una sotto-algebra di B avente per modulo quello comune di B e P. Segue che l'ordine di $P + E_1^s$ è un multiplo di ν, e che, per conseguenza, tale è pure l'ordine di E_1^s. Indichiamo quest'ultimo con $q_s \nu$, se $s > 1$; mentre da $B = P + E_1$ e dalle posizioni fatte segue che l'ordine di E_1 è $(q - 1)\nu$.

Essendo $E_1 > E_1^2 > \ldots > E_1^{r-1} > E^r = 0$, sarà

$$(q - 1)\nu > q_2 \nu > \ldots > q_{r-1}\nu > 0,$$

ossia

$$q - 1 \geq q_2 + 1,\ q_2 \geq q_3 + 1, \ldots, q_{r-2} \geq q_{r-1} + 1,\ q_{r-1} \geq 1;$$

e dunque, sommando, sarà $q - 1 \geq r - 1$, cioè, come volevasi, $r \leq q = n/n_1$.

Notisi che, *se n è privo di divisori quadrati* ($\neq 1$), *è* $p_1 = 1$, *indi A a modulo primitivo*; che se poi n è un numero primo, non potendo essere $\nu = n$ (perchè altrimenti sarebbe $n_1 = n$ ed A sarebbe priva di sotto-algebra eccezionale), sarà necessariamente $\nu = 1$; dunque *in tal caso l'ordine* di E *sarà* $n - 1$.

(2) Qui si scrive $BE_1 = E_1 B = E_1$, anzi che $BE_1 \leq E_1$, $E_1 B \leq E_1$, perchè B è dotata di modulo. Lo stesso dicasi per le eguaglianze successive del testo.