LE ALGEBRE DOPPIE (*)

Il CAYLEY ha determinato in un suo lavoro ben noto (1) le algebre complesse di ordine 2, o, com'egli diceva, le *algebre doppie*. Qui si vuole riprendere la ricerca del CAYLEY, e per compierla nell'ipotesi più lata che le algebre di cui si tratta siano definite in un corpo qualunque, e per indicare sommariamente le proprietà più spiccate dei vari tipi di algebre che si incontrano. Aggiungasi che la ricerca viene condotta utilizzando i progressi più recenti della teoria generale delle algebre; per modo che diventa singolarmente rapida ed elegante (2).

Per brevità di discorso estenderemo la denominazione cayleyana di algebra doppia a qualunque algebra di ordine 2.

§ 1.

I VARI TIPI DI ALGEBRE DOPPIE.

1. Sia A un'algebra doppia in un qualsivoglia corpo numerico Γ. Essa può essere:

a) semi-semplice, o

(*) *Rend. Reale Accad. di Scienze Fisiche e Mat. di Napoli*, (3) 28 (1922), pp. 65-79.

(1) CAYLEY, *On double algebra* [Proceedings of the London Mathematical Society, vol. 15 (1884), pp. 185-197].

(2) La classificazione delle algebre di un dato ordine in un dato corpo, di fronte alla relazione di equivalenza, è stata compiuta per il corpo complesso e per i valori dell'ordine non superiori a 6 da B. PEIRCE, A. CAYLEY, E. STUDY, G. SCHEFFERS, ROHR, e G. VOGHERA in lavori ormai classici. Ma vi è luogo a riprendere utilmente tale questione, e per trattarla con tutti i sussidi che oggi porge la più progredita teoria generale delle algebre, e per estenderla al caso di corpi qualunque. È perciò che a questo lavoro ne seguiranno altri, miei o di miei scolari, tutti diretti a raggiungere rapidamente i risultati di quelle classificazioni e ad estenderli, e nel tempo stesso ad approfondire lo studio delle proprietà delle varie algebre che in esse si incontrano.

b) non semi-semplice.

Esaminiamo separatamente le due alternative.

2. *Alternativa* a).

Qui l'algebra A, essendo semi-semplice e doppia, è certo dotata di modulo (3). Poi

a') o è irriducibile e quindi semplice,

a'') o è riducibile e quindi somma diretta di due algebre (semplici) di ordine 1 (4).

Nel caso *a'*), siccome l'ordine di A non ammette divisori quadrati diversi da 1, A è addirittura primitiva (5); inoltre, essendo primitiva e avendo per ordine un numero primo, è anche potenziale (in particolare, commutativa) (6).

Segue che in tal caso A, rispetto alle sue operazioni di addizione e moltiplicazione, può considerarsi come un corpo numerico isomorfo a un corpo algebrico di grado 2 derivato da Γ (mediante un polinomio di 2° grado, in una indeterminata, ivi irriducibile) (7).

Nel caso *a''*), essendo A dotata di modulo, tali sono anche le due algebre di cui è somma diretta (8); e dunque in tal caso possono trovarsi in A due unità u e v rispetto alle quali la tavola di moltiplicazione di A sia

$$u^2 = u, \quad uv = vu = 0, \quad v^2 = v. \tag{1}$$

3. *Alternativa* b).

Anche qui vi sono da distinguere due casi, secondo che A

b') è pseudonulla, o

b'') non è pseudonulla.

Nel caso *b'*) l'indice di A è 2 o 3 (9); quindi A è una zero-algebra, o un'algebra pseudonulla potenziale (10) generata da un suo elemento di grado 2.

Segue che, o la tavola di moltiplicazione di A rispetto a due

(3) Vedi per. es., G. Scorza, *Corpi numerici e algebre* (Messina, Principato, 1921) pag. 277, n. 173.

(4) Loc. cit. in (3) pag. 330, n. 226.

(5) Loc. cit. in (3), pag. 335, n. 232.

(6) Loc. cit. in (3), pag. 329, n. 224.

(7) Loc. cit. in (6).

(8) Loc. cit. in (3), pag. 241, β).

(9) Loc. cit. in (3), pag. 207, n. 98.

(10) Loc. cit. in (3), pag. 322, n. 218.

sue unità qualsiasi u e v è della forma

$$u^2 = uv = vu = v^2 = 0\,, \tag{2}$$

o si possono trovare in A due unità u e v sì che rispetto ad esse la tavola di moltiplicazione di A sia della forma

$$u^2 = v\,, \quad uv = vu = v^2 = 0\,. \tag{3}$$

Nel caso $b'')$ A è dotata di sotto-algebra eccezionale propria, che è, necessariamente, una zero-algebra di ordine 1; inoltre A ammette necessariamente qualche automodulo [11].

Sia u un automodulo di A e v un suo elemento eccezionale; evidentemente u e v potranno considerarsi come due unità di A, e sarà

$$u^2 = u\,, \quad v^2 = 0\,.$$

Siccome v è eccezionale, ciascuno dei prodotti uv e vu è nullo o eccezionale; quindi è intanto

$$uv = \alpha v\,, \quad vu = \beta v\,,$$

con α e β numeri di Γ.

Ora da

$$\alpha v = uv = u^2 v = u(uv) = \alpha uv = \alpha^2 v$$

$$\beta v = vu = vu^2 = (vu)\,u = \beta vu = \beta^2 v\,,$$

essendo $v \neq 0$, si trae

$$\alpha = \alpha^2 \qquad \text{e} \qquad \beta = \beta^2\,,$$

cioè che ciascuno dei numeri α e β o è 0 o è 1; dunque, rispetto ad u, v, la tavola di moltiplicazione di A non può avere che una delle seguenti quattro forme:

$$u^2 = u\,, \quad uv = vu = v\,, \quad v^2 = 0\,, \tag{4}$$

$$u_2 = u\,, \quad uv = v\,, \quad vu = v^2 = 0\,, \tag{5}$$

([11]) Loc. cit. in ([3]), pag. 263, n. 157.

$$u^2 = u\,, \quad uv = 0\,, \quad vu = v\,, \quad v^2 = 0\,, \tag{6}$$

$$u^2 = u\,, \quad uv = vu = v^2 = 0\,. \tag{7}$$

4. Riassumendo la discussione fatta abbiamo che:

Un'algebra doppia nel corpo Γ o può considerarsi come un corpo numerico isomorfo a un corpo algebrico di grado 2 derivato da Γ, o può supporsi definita da una tavola di moltiplicazione della forma (1), (2), ..., *o* (7).

Corrispondentemente noi diremo che essa è del *tipo* I), II), ..., o VIII).

Si vede subito, e del resto risulterà manifestamente da quanto sarà detto nel § 3, che due algebre doppie le quali non appartengano a uno stesso degli ultimi sette tipi non sono certo equivalenti tra di loro.

Inoltre discende subito da un classico teorema di esistenza del Frobenius ([12]) che qualunque sia Γ esistono certo in esso algebre doppie di uno qualunque di questi ultimi sette tipi.

Resta a vedere se, e in quanti modi diversi rispetto alla relazione di equivalenza, può realizzarsi in Γ un'algebra doppia che sia del tipo I).

È quanto passiamo ad esaminare nel paragrafo successivo.

§ 2.

Le algebre doppie primitive nei vari corpi numerici.

5. Perchè esista nel corpo numerico Γ un'algebra doppia primitiva [o, ciò che è lo stesso del tipo I)], occorre e basta, per quanto precede, che esistano in Γ polinomi, con una indeterminata, irriducibili e del 2° grado.

L'esistenza di polinomi sì fatti può essere senz'altro assicurata, se Γ è finito ([13]); ma non più se Γ è infinito, poichè, per es., nel corpo complesso i polinomi irriducibili con una indeterminata sono tutti e solo quelli di primo grado.

Cosicchè intanto:

Dato un corpo numerico non è detto che esistano in esso algebre

([12]) Loc. cit. in ([3]), pag. 304, n. 202.

([13]) Loc. cit. in ([3]), pag. 129, in fine.

doppie primitive; in particolare non ne esistono certo, se esso è isomorfo al corpo complesso.

6. Ebbene supponiamo che Γ sia un corpo numerico nel quale esistano algebre doppie primitive e vediamo a quali forme tipiche possono essere ricondotte le loro tavole di moltiplicazione.

Sia A una tale algebra, sia u il suo modulo e v un suo elemento indipendente dal modulo. Gli elementi u e v costituiranno per essa un aggregato di unità e rispetto a queste la sua tavola di moltiplicazione sarà intanto della forma

$$u^2 = u\,, \quad uv = vu = v\,, \quad v^2 = \alpha u + \beta v\,, \tag{8}$$

con α e β numeri di Γ, tali che il polinomio

$$\xi^2 - \beta\xi - \alpha \tag{9}$$

risulti irriducibile in Γ.

Se w è un elemento di A, indipendente da u, ed è

$$w = \lambda u + \mu v\,,$$

con λ e μ numeri di Γ, μ è diverso da zero, e la tavola di moltiplicazione di A rispetto ad u e w risulta

$$u^2 = u\,, \quad uw = wu = w\,, \quad w^2 = \alpha' u + \beta' w\,, \tag{10}$$

con

$$\alpha' = -\lambda^2 - \beta\lambda\mu + \alpha\mu^2 \tag{11}$$

$$\beta' = 2\lambda + \beta\mu\,. \tag{12}$$

Indichiamo ora con Γ' il sottocorpo fondamentale [14] di Γ e dimostriamo che:

Se Γ' non è isomorfo al corpo $C[2]$, è possibile disporre di λ e μ in Γ, sì che risulti $\mu \neq 0$ e $\beta' = 0$; se invece Γ' è isomorfo a $C[2]$, è possibile disporre di λ e μ in Γ, sì che risulti $\mu \neq 0$ e β' o nullo o eguale ad 1.

[14] Per la definizione di questo sottocorpo vedi loc. cit. in [3], pag. 19 e seguenti.

Se nelle (8) è già $\beta = 0$, basta porre $\lambda = 0$, $\mu = 1$, cioè $w = v$ per riconoscere l'esattezza dell'enunciato. Supponiamo dunque che nelle (8) sia $\beta \neq 0$.

Allora, perchè risulti $\mu \neq 0$ e $\beta' = 0$, occorre e basta che sia

$$(13) \qquad \mu \neq 0 \quad \text{e} \quad \mu = \frac{-2\lambda}{\beta};$$

quindi, se Γ' non è isomorfo a $C[2]$, per modo che in Γ è $2 \neq 0$, (occorre e) basta prendere $\lambda \neq 0$ e $\mu = \frac{-2\lambda}{\beta}$ per raggiungere lo scopo voluto; se invece Γ' è isomorfo a $C[2]$, e quindi in Γ è $2 = 0$, non è possibile soddisfare ad entrambe le (13), comunque si prenda λ; e per conseguenza, in tale ipotesi, se $\beta \neq 0$ non è possibile far riescire $\beta' = 0$.

Ma allora è per altro possibile far risultare

$$\mu \neq 0 \quad \text{e} \quad \beta' = 1,$$

perchè, essendo $2 = 0$, la (12) diventa

$$\beta' = \beta\mu,$$

e quindi, essendo $\beta \neq 0$, per raggiungere tale scopo (occorre e) basta prendere

$$\mu = \frac{1}{\beta}.$$

7. Se si avverte che, quando $\beta = 0$, il polinomio (9) è irriducibile in Γ quando, e solo quando, α non è il quadrato di un numero di Γ; e che se $\beta = 1$ e il sottocorpo fondamentale di Γ è isomorfo a $C[2]$, il polinomio (9) — che allora può scriversi, indifferentemente, $\xi^2 - \xi - \alpha$ o $\xi^2 + \xi \pm \alpha$ ([15]) — è irriducibile in Γ se, e soltanto se, α è un numero di Γ per il quale non è possibile che sussista un'eguaglianza della forma

$$\alpha = \xi + \xi^2,$$

con ξ in Γ, le considerazioni fatte permettono di enunciare i seguenti teoremi:

I) *Se Γ è a sottocorpo fondamentale non isomorfo a $C[2]$, esistono in Γ algebre doppie primitive se, e soltanto se, esistono in Γ*

([15]) Loc. cit. in ([3]), pag. 23, n. 30.

numeri tali che ciascun di essi non sia il quadrato di un numero del corpo stesso; e, in caso affermativo, le dette algebre in Γ sono tutte, e solo, quelle per ciascuna delle quali la tavola di moltiplicazione può esser ricondotta alla forma

$$u^2 = u\,, \quad uv = vu = v\,, \quad v^2 = \alpha u\,, \tag{14}$$

con α in Γ, ma non quadrato di un numero di Γ;

II) *Se Γ è a sottocorpo fondamentale isomorfo a $C[2]$, esistono in Γ algebre doppie primitive se, e soltanto se, esistono in Γ numeri tali che ciascun di essi o non sia il quadrato di un numero di Γ, o non sia la somma di un numero di Γ e del suo quadrato. E, in caso affermativo, le algebre doppie primitive in Γ sono tutte, e solo, quelle per ciascuna delle quali la tavola di moltiplicazione o può esser ricondotta alla forma* (14) *con α in Γ, ma non quadrato di un numero di Γ, o può esser ricondotta alla forma*

$$u^2 = u\,, \quad uv = vu = v\,, \quad v^2 = \alpha u + v\,, \tag{15}$$

con α in Γ, ma non somma di un numero di Γ e del suo quadrato; delle due forme non potendosene verificare per ciascuna di tali algebre che una sola.

8. Andiamo ora a precisare i teoremi I) e II) del n.^{0} prec., proponendoci di trovare un criterio in base al quale distinguere se assegnate algebre doppie primitive siano o no equivalenti.

Siano A ed A' algebre doppie primitive in un corpo Γ col sottocorpo fondamentale non isomorfo a $C[2]$; e, come è lecito, si supponga che la tavola di moltiplicazione di A sia la (14), quella di A' sia la tavola

$$u'^2 = u'\,, \quad u'v' = v'u' = v'\,, \quad v'^2 = \alpha' u'\,. \tag{16}$$

Dico che:

Le algebre A ed A' sono equivalenti quando, e solo quando, sia $\alpha = \alpha' \varrho^2$, con ϱ numero di Γ[16].

Infatti perchè A ed A' siano equivalenti occorre e basta che possa trovarsi in A' un elemento v_1, indipendente dal modulo u',

[16] Questa proposizione si trova già rilevata nel trattatello *Linear Algebras* del Dickson (*Cambridge Tracts in Mathematics and Mathematical Physics*, n. 16).

per il quale si abbia

$$v_1^2 = \alpha u' .$$

Ora per l'elemento corrente di A'

$$x = \lambda u' + \mu v' ,$$

con λ e μ in Γ, si ha, per le (16),

$$x^2 = (\lambda^2 + \mu^2\alpha')\, u' + 2\lambda\mu v' ,$$

e perchè venga

$$x^2 = \alpha u' ,$$

con $\mu \neq 0$, occorre e basta che sia

$$\mu \neq 0 , \quad 2\lambda\mu = 0 , \quad \lambda^2 + \mu^2\alpha' = \alpha ,$$

cioè, essendo certo α e α' non nulli, perchè non quadrati di numeri di Γ,

$$\lambda = 0 \quad \text{e} \quad \mu^2 = \frac{\alpha}{\alpha'},$$

dunque ecc.

Siano invece A ed A' algebre doppie primitive in un corpo Γ col sottocorpo fondamentale isomorfo a $C\,[2]$.

Se le tavole di moltiplicazione di A ed A' non possono ricondursi entrambe alla forma (14), o entrambe alla forma (15), A ed A' non sono certo equivalenti; e se possono ricondursi entrambe alla forma (14) per decidere della loro equivalenza o meno si ha un teorema del tutto analogo a quello or ora dimostrato; dunque non resta se non considerare il caso in cui le dette tavole possono esser ricondotte entrambe alla forma (15).

Suppongasi, come è lecito, che A abbia come tavola di moltiplicazione la (15) e che A' abbia come tavola di moltiplicazione

$$u'^2 = u' , \quad u'v' = v'u' = v' , \quad v'^2 = \alpha' u' + v' . \tag{17}$$

Dico che:

Le algebre A ed A' sono equivalenti quando, e solo quando $\alpha + \alpha'$ è in Γ la somma di un numero e del suo quadrato.

Infatti perchè A ed A' siano equivalenti, occorre e basta che possa trovarsi in A' un elemento v_1, indipendente dal modulo u', per il quale si abbia

$$v_1^2 = \alpha u' + v_1 .$$

Ora per l'elemento corrente di A'

$$x = \lambda u' + \mu v' ,$$

con λ e μ in Γ, si ha, per le (17) e per il fatto che stavolta è, in Γ, $2 = 0$,

$$x^2 = (\lambda^2 + \lambda\mu + \mu^2\alpha')\, u' + \mu x ;$$

e perchè venga

$$x^2 = \alpha u' + x ,$$

con $\mu \neq 0$, occorre e basta che sia

$$\mu = 1 , \quad \lambda^2 + \lambda + \alpha' = \alpha .$$

dunque ecc. ([17]).

9. Avvertasi che, per decidere dell'equivalenza, o meno, di algebre doppie primitive in un dato corpo *finito*, non vi è luogo a ricorrere ai teoremi del n.° prec. Esse infatti possono considerarsi come corpi numerici con N^2 elementi, se N è il numero degli elementi del corpo nel quale sono definite (per modo che N è, notoriamente, una potenza di un numero primo), e quindi esse sono senz'altro equivalenti ([18]).

10. A titolo di esempio e a chiarimento delle cose dette giova indicare un corpo numerico (infinito) col sottocorpo fondamentale isomorfo a $C[2]$ nel quale esistono algebre doppie primitive con tavola di moltiplicazione riconducibile alla forma (14) — e non alla (15) —, e algebre doppie primitive con tavola di moltiplicazione riconducibile alla forma (15) — ma non alla forma (14) —.

Si consideri il corpo Γ che si deriva dal corpo $C[2]$ mediante l'aggiunta della indeterminata ξ ([19]). Dico che *ξ è, in Γ, un numero*

([17]) Si ricordi che, stavolta, è in Γ $\alpha + \alpha' = \alpha - \alpha'$.

([18]) Da ciò deriva, come può verificarsi direttamente, che se Γ è un corpo *finito* con sottocorpo fondamentale isomorfo a $C[2]$, per un'algebra doppia primitiva in esso delle due alternative previste dal teorema II) del n. 7 non può presentarsene che una. Questa è poi la seconda, perchè in un tal corpo Γ ogni numero è *quadrato*.

([19]) Loc. cit. in ([3]), pag. 62, n. 90.

non quadrato, e che, *detta* ζ *una nuova indeterminata, il polinomio* $\zeta^2+\zeta+1$ *è irriducibile in* Γ.

Infatti un elemento qualunque di Γ è della forma $\frac{f(\xi)}{g(\xi)}$, con $f(\xi)$ e $g(\xi)$ polinomi in $C[2]$ e $g(\xi)$ non nullo, quindi, se ξ fosse il quadrato di un numero di Γ, sussisterebbe in $C[2]$ un'eguaglianza della forma

$$\xi\,[g(\xi)]^2=[f(\xi)]^2 \tag{18}$$

coi detti significati di f e g, e se $\zeta^2+\zeta+1$ fosse riducibile in Γ, cioè ammettesse ivi uno zero, sussisterebbe in $C[2]$, con gli stessi significati di f e g, un'eguaglianza della forma

$$[f(\xi)]^2+f(\xi)\,g(\xi)+[g(\xi)]^2=0\,. \tag{19}$$

Ora la (18) è manifestamente assurda, perchè in essa, a primo membro, comparisce un polinomio di grado dispari e, a secondo membro, un polinomio nullo o di grado pari; e anche la (19) è assurda, perchè, essendo in essa $g(\xi)\neq 0$, tale dovrebbe essere anche $f(\xi)$, e allora, una volta che $C[2]$ non contiene altri numeri che 0 ed 1, $f(\xi)$ e $g(\xi)$, ordinati per le potenze discendenti di ξ, sarebbero della forma

$$f(\xi)=\xi^n+\xi^{n-r_1}+\xi^{n-r_2}+\ldots+\xi^{n-r_l} \qquad (n\geq 0, \text{ e se } n>0,\ 0<r_1<r_2\ldots<r_l\leq n)$$

$$g(\xi)=\xi^m+\xi^{m-s_1}+\xi^{m-s_2}+\ldots+\xi^{m-s_t} \qquad (m\geq 0, \text{ e, se } m>0,\ 0<s_1<s_2<\ldots<s_t\leq m)$$

e quindi sarebbe, ordinando sempre per le potenze discendenti di ξ,

$$[f(\xi)]^2=\xi^{2n}+\xi^{2n-2r_1}+\ldots+\xi^{2n-2r_l}\,,$$

$$f(\xi)\,g(\xi)=\xi^{m+n}+\ldots\ldots\ldots+\xi^{m+n-r_l-s_t},$$

$$[g(\xi)]^2=\xi^{2m}+\xi^{2m-2s_1}+\ldots+\xi^{2m-2s_t},$$

e, in nessun caso, siano o no m ed n eguali fra di loro, potrebbe esser soddisfatta la (19).

Segue che nel corpo considerato esistono algebre doppie di entrambe le specie volute.

§ 3.

Gli automoduli e i gruppi automorfi di un'algebra doppia.

11. In base a teoremi generali ben noti si ha subito che:

Un'algebra doppia del tipo I) *ammette un solo automodulo (primitivo e principale), cioè il suo modulo* [20];

che:

Un'algebra doppia del tipo II) *ammette tre soli automoduli, due primitivi, l'altro principale, coincidente con la somma di quei due e col modulo dell'algebra* [21];

e che:

Un'algebra doppia del tipo III) *o* IV) *è priva di automoduli* [22].

Suppongasi ora di avere un'algebra doppia del tipo V) e che la sua tavola di moltiplicazione sia data dalle (4).

Per il quadrato del suo elemento corrente

$$x = \lambda u + \mu v\,,$$

con le coordinate λ e μ, rispetto ad u e v, si avrà in base alle (4),

$$x^2 = \lambda^2 u + 2\lambda\mu v\,,$$

quindi x riescirà un automodulo se, e solo se, λ e μ non sono entrambe nulle ed inoltre

$$\lambda = \lambda^2 \qquad \mu = 2\lambda\mu\,;$$

cioè, se, e solo se, (sia, o no, $2 = 0$ nel corpo in cui è definita l'algebra),

$$\lambda = 1 \qquad \text{e} \quad \mu = 0\,.$$

Segue che anche:

Un'algebra doppia del tipo V) *ammette un solo automodulo (primitivo e principale), coincidente col suo modulo.*

[20] Loc. cit. in [3], pag. 265, n. 159, in fine.
[21] Loc. cit. in [3], pag. 317, n. 211, in fine.
[22] Loc. cit. in [11].

Con un ragionamento analogo si riconosce subito che:

Un'algebra doppia del tipo VI) *[del tipo* VII)*], ove si supponga che la sua tavola di moltiplicazione sia data dalle* (5) *[dalle* (6)*], ha come automoduli tutti e solo gli elementi della forma* $u + \mu v$, *con* μ *numero qualunque del corpo in cui essa è definita. Ciascuno di tali automoduli è primitivo e principale, ed è per l'algebra un modulo sinistro [destro].*

Infine un'algebra doppia del tipo VIII) è, per le (7), somma diretta di due algebre di ordine 1, di cui una sola con modulo, dunque:

Un'algebra doppia del tipo VIII) *ammette un solo automodulo (primitivo e principale) che non è per essa un modulo, nè sinistro, nè destro.*

12. Adesso indichiamo con A un'algebra doppia nel corpo Γ, con G il gruppo dei suoi autoisomorfismi ([23]), o, come anche diremo, per amor di brevità, il suo gruppo automorfo.

Vogliamo determinare G per ognuna delle varie ipotesi che possono esser fatte su A.

13. Se ω è una qualunque operazione di G, e per ω due unità u e v di A vanno in u' e v', posto

$$u' = au + cv \qquad (20)$$
$$v' = bu + dv$$

con a, b, c, d in Γ, sarà

$$ad - bc \neq 0 ,$$

e poi da ω l'elemento corrente di A

$$x = \lambda u + \mu v ,$$

con le coordinate λ e μ rispetto ad u e v, sarà portato nell'elemento

$$x' = \lambda u' + \mu v' = (a\lambda + b\mu)\, u + (c\lambda + d\mu)\, v ,$$

([23]) Loc. cit. in ([3]), pag. 193, n. 75.

cioè nell'elemento avente rispetto ad u e v le coordinate

$$\begin{aligned} \lambda' &= a\lambda + b\mu \\ \mu' &= c\lambda + d\mu\,. \end{aligned} \tag{21}$$

Segue che ω può supporsi *rappresentata* dalla *sostituzione lineare* (21).

Viceversa è chiaro che la sostituzione (21), con a, b, c, d numeri di Γ e $ad - bc \neq 0$, rappresenta un'operazione di G, quando, e solo quando, posto

$$\begin{aligned} u' &= au + cv \\ v' &= bu + dv\,, \end{aligned} \tag{22}$$

u' e v' presentano la stessa tavola di moltiplicazione di u e v.

14. Premessa questa osservazione generale, supponiamo che A sia del tipo I) e che la sua tavola di moltiplicazione per le unità u e v sia della forma

$$u^2 = u\,,\quad uv = vu = v\,,\quad v^2 = \alpha u\,, \tag{23}$$

con α non quadrato in Γ, sia, o non, il sottocorpo fondamentale di Γ isomorfo a $C[2]$.

Dico che, in tal caso:

Il gruppo G è un gruppo (ciclico) di ordine 2, o un gruppo identico, secondo che quel sottocorpo non è, od è, isomorfo a $C[2]$.

Infatti, perchè in tal caso le (21) rappresentino un'operazione di G occorre e basta che sia $ad - bc \neq 0$, e che, fatte le posizioni (22), risulti

$$u' = u\,,\quad v'^2 = \alpha u\,.$$

Ciò implica, intanto, $a = 1$, $c = 0$, $d \neq 0$; poi essendo in base alle (23),

$$v'^2 = (b^2 + d^2\alpha)\,u + 2bdv$$

dovrà essere

$$b^2 + d^2\alpha = \alpha\,,\quad 2bd = 0\,. \tag{24}$$

Ora, se il sottocorpo fondamentale di Γ non è isomorfo a $C[2]$, le (24), essendo $d \neq 0$, $\alpha \neq 0$, dànno

$$b = 0 , \quad d = \pm 1 ;$$

se quel sottocorpo è isomorfo a $C[2]$, delle (24) la seconda è identicamente soddisfatta e la prima può scriversi

$$b^2 = \alpha (1 - d^2) = \alpha (1 - d)^2$$

per modo che, non potendo essere α un quadrato, essa dà

$$d = 1 \quad \text{e} \quad b = 0 ;$$

dunque ecc.

15. Supponiamo in secondo luogo che A sia del tipo I), che il sottocorpo fondamentale di Γ sia isomorfo a $C[2]$ e che la sua tavola di moltiplicazione rispetto ad u e v sia della forma

$$(25) \qquad u^2 = u , \quad uv = vu = v , \quad v^2 = \alpha u + v ,$$

con α in Γ, ma non somma di un numero di Γ e del suo quadrato.

Dico che questa volta:

Il gruppo G è un gruppo (ciclico) di ordine 2.

Infatti, come più sopra, perchè le (21) rappresentino un'operazione di G occorre e basta che sia $ad - bc \neq 0$, e che, fatte le posizioni (22), risulti

$$u' = u , \quad v'^2 = \alpha u + v' .$$

Ciò implica intanto $a = 1$, $c = 0$, $d \neq 0$; poi, essendo in base alle (25),

$$v'^2 = (b^2 - bd + d^2 \alpha) u + dv'$$

dovrà essere $d = 1$, indi

$$b^2 - b + \alpha = \alpha ,$$

cioè $b = 0$ o $b = 1$.

Si conclude che G è costituito dalle due operazioni:

$$\begin{array}{ll} \lambda' = \lambda & \quad \lambda' = \lambda + \mu \\ \mu' = \mu , & \quad \mu' = \mu . \end{array}$$

16. Se A è del tipo II) e la sua tavola di moltiplicazione rispetto ad u e v è data dalle (1), un'operazione di G non può che

tener fermo ciascuno dei suoi due automoduli primitivi u e v, o mutar l'uno di questi nell'altro.

Basta ciò per mostrare che, anche nel caso attuale:

Il gruppo G è un gruppo (ciclico) di ordine 2.

17. Se A è del tipo III), cioè una zero-algebra, ciascuna sostituzione lineare della forma (21), con a, b, c, d numeri di Γ e $ad - bc \neq 0$ rappresenta un'operazione di G [24], e dunque questa volta:

Il gruppo G è oloedricamente isomorfo al gruppo delle sostituzioni lineari proprie in Γ su due variabili.

18. Se A è del tipo IV) e per le sue unità u e v la tavola di moltiplicazione è data dalle (3), perchè le u' e v' date dalle (20) costituiscano per essa due unità con tavola di moltiplicazione dello stesso tipo, occorre e basta che sia $b = 0$, $d = a^2$ e $a \neq 0$.

Infatti la prima delle (20), badando alle (3), dà

$$u'^2 = a^2 v ,$$

e quindi risulta $u'^2 = v'$ se, e solo se, è

$$b = 0 , \quad d = a^2 .$$

Posto poi

$$u' = au + cv$$
$$v' = a^2 v ,$$

risulta subito, per le (3),

$$u'v' = v'u' = v'^2 = 0 ,$$

dunque è dimostrato quanto volevasi.

Segue che, nel caso attuale:

Il gruppo G è il gruppo delle operazioni rappresentate da sostituzioni della forma

$$\lambda' = a\lambda$$
$$\mu' = c\lambda + a^2\mu ,$$

con a, c in Γ e $a \neq 0$.

19. Se A è del tipo V) e per le sue unità u e v la tavola di moltiplicazione è data dalle (4), perchè le u' e v', date dalle (20),

[24] Loc. cit. in [3], pag. 206, n. 97.

costituiscano per essa due unità con tavola di moltiplicazione dello stesso tipo, occorre e basta che sia $a=1$, $c=0$, $b=0$, $d\neq 0$, dunque:

Nel caso in esame il gruppo G è il gruppo delle operazioni rappresentate da sostituzioni della forma

$$\lambda' = \lambda$$

$$\mu' = d\mu\,,$$

con d numero di Γ non nullo.

Alla stessa conclusione si perviene se A è del tipo VIII).

20. Infine se A è del tipo VI), o VII) e per le sue unità u e v si suppongono valide le (5) o le (6) si trova, ragionando come nei casi precedenti, che:

Il gruppo G è il gruppo delle operazioni rappresentate da sostituzioni della forma

$$\lambda' = \lambda$$

$$\mu' = c\lambda + d\mu\,,$$

con c e d in Γ e $d\neq 0$.

21. Quando un'algebra è dotata di modulo, accanto al suo gruppo automorfo vi è luogo a considerare il sottogruppo invariante di questo costituito dagli autoisomorfismi interni dell'algebra, o, come possiamo dire, il gruppo automorfo *interno* (25).

Ma se un'algebra, con modulo, è commutativa, il suo gruppo automorfo interno è evidentemente identico, e un'algebra doppia con modulo [e quindi del tipo I), II) o V)] è commutativa; dunque nel caso delle algebre doppie la considerazione del gruppo automorfo interno è priva di interesse.

Napoli, 24 gennaio 1922.

(25) Loc. cit. in (3), pag. 222, n. 116.