Giampaolo Menichetti

Su una congettura di I. Kaplansky relativa alle algebre con divisione, tridimensionali sopra un campo finito

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **61** (1976), n.1-2, p. 15–19.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1976_8_61_1-2_15_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1976.

Algebra. — *Su una congettura di I. Kaplansky relativa alle algebre con divisione, tridimensionali sopra un campo finito* (*). Nota (**) di GIAMPAOLO MENICHETTI, presentata dal Socio G. ZAPPA.

SUMMARY. — We give here a sketch of the proof of the following Kaplansky conjecture: any three-dimensional division algebra over a finite field is associative or a twisted field. The detailed proof will appear in a forthcoming paper.

I primi importanti esempi di algebre con divisione[1], tridimensionali sopra un campo finito $K = GF(q)$ ($q = p^h \geq 3$, p primo), sono stati dati da L. E. Dickson nel 1905 (cfr. [8]). Successivamente altri Autori hanno studiato classi di algebre, $\mathcal{A}$, di questo tipo. Particolarmente interessante, anche perché non limitata alla sola dimensione tre, è la classe dei cosiddetti *twisted fields*, scoperta da A. A. Albert e poi ampliata dallo stesso Autore (cfr. [1], [2], [3] e [4]).

In una precedente Nota (cfr. [12]) avevo determinato la struttura di tutte le possibili algebre con divisione $\mathcal{A}$ ($\dim_K \mathcal{A} = 3$), fornendo indirettamente una classificazione del loro insieme. In particolare nel caso $q = p = 3m + 1$ – che, per esemplificare, avevo esaminato nei dettagli – il numero delle algebre non associative $\mathcal{A}$ risultava essere $(p^3 - p^2 + p - 10)/3$.

I. Kaplansky, in un recente lavoro (cfr. [11]), ha congetturato la seguente

PROPOSIZIONE A. *Un'algebra con divisione di dimensione tre su un campo finito,* K, *o è associativa oppure è un twisted field.*

Nello stesso articolo l'Autore determina il numero, ν, dei *twisted fields* di dimensione tre su K, trovando che esso è dato da

$$\nu = \begin{cases} (q^3 - q^2 + q - 10)/3\,, & \text{se } q \equiv 1 \pmod 3, \\ (q^3 - q^2 + q - 6)/3\,, & \text{se } q \not\equiv 1 \pmod 3. \end{cases} \tag{1}$$

Se $q = p = 3m + 1$, allora (1) coincide col numero delle algebre non associative $\mathcal{A}$, determinato in [12]; ciò che, in tale ipotesi, dimostra la Proposizione A. Di questo e del contenuto della sua Nota mi aveva gentilmente dato notizia il Prof. Kaplansky prima ancora che essa fosse pubblicata.

Utilizzando essenzialmente alcuni risultati acquisiti in [12], ho dimostrato la Proposizione A provando che la (1) dà il numero delle algebre con divisione $\mathcal{A}$ non associative, di dimensione tre sopra $K = GF(q)$, qualunque sia q.

(*) Lavoro eseguito nell'ambito dell'attività del G.N.S.A.G.A. del C.N.R. (Sezione n. 4).

(**) Pervenuta all'Accademia il 20 luglio 1976.

(1) L'espressione « algebra con divisione » è usata qui nell'accezione di « algebra con unità, priva di divisori dello zero ».

Questa Nota consiste in una esposizione sintetica del procedimento che in ciò ho seguito; le dimostrazioni saranno date in una Nota successiva.

Sia K_3 il campo di rango tre su K. Nel seguito considero prefissati un polinomio

$$f(\xi) = \sum_0^2 {}_i e_i \xi^i - \xi^3 \quad , \quad e_i \in K, \tag{2}$$

irriducibile in K [ξ] ed una sua radice $v \in K_3 - K$.

Posto

$$F = \begin{pmatrix} 0 & 0 & e_0 \\ 1 & 0 & e_1 \\ 0 & 1 & e_2 \end{pmatrix} \in GL(3, K),$$

per ogni $k = \sum_0^2 {}_i x_i v^i \in K_3$ $(x_i \in K)$ è definita la matrice

$$F(k) = \sum_0^2 {}_i x_i F^i, \tag{3}$$

della quale

$$\det(F(k) - tI) = \sum_0^2 {}_i (-1)^i \sigma_{3-i}(F(k)) t^i - t^3$$

indica il polinomio caratteristico. Inoltre

$$\text{l.i. } [v, k]_K \tag{4}$$

esprime la seguente condizione: gli elementi 1, v e

$$\varphi(v, k) = (v + k)(\sigma_1(F(k)) - k) - \sigma_2(F(k))$$

di K_3 sono linearmente indipendenti rispetto a K.

Fissato $k \in K_3 - K$ che soddisfa la (4), indico con $\mathscr{A}(k)$ l'algebra, di dimensione tre su K, le cui costanti di struttura, $c_{ij}^r = c_{ij}^r(k)$, relative ad una base prefissata $U = \{u_0, u_1, u_2\}$ $(u_i u_j = \sum_0^2 {}_r c_{ij}^r u_r)$ sono

$$\begin{gathered} c_{0i}^r = c_{i0}^r = \delta_i^r \,^{(2)}, \qquad c_{11}^0 = c_{11}^1 = 0, \qquad c_{11}^2 = 1, \\ c_{21}^r = (-1)^r \sigma_{3-r}(F(k)), \qquad c_{12}^r = e_r, \\ c_{22}^0 = e_2 \sigma_3(F(k)) + e_0 \sigma_1(F(k)) - \sigma_2(F(vk)), \\ c_{22}^1 = -\sigma_3(F(v + k)), \qquad c_{22}^2 = e_2 \sigma_1(F(k)) - \sigma_1(F(vk)). \end{gathered}$$

Le seguenti Proposizioni B, C e D sintetizzano alcuni risultati acquisiti in [12].

(2) Al solito $\delta_i^i = 1$ e $\delta_i^r = 0$ per $r \neq i$.

PROPOSIZIONE B. *$\mathscr{A}(k)$ è un'algebra con divisione qualunque sia k che soddisfa la* (4).

In particolare:

a) *$\mathscr{A}(k)$ è associativa se e solo se $k = v^{q^s}$, $s = 1, 2$;*

b) *$\mathscr{A}(k)$ è commutativa e non associativa se e solo se $p \neq 2$ e $k = v$.*

PROPOSIZIONE C. *Sia $\mathscr{A}(k)$ non associativa. $\mathscr{A}(k')$ è isomorfa ad $\mathscr{A}(k)$ se e solo se esistono $i \in \{0, 1, 2\}$ e $\lambda_i \in K$ (con $(\lambda_1, \lambda_2) \neq (0, 0)$) tali che*

$$v = \lambda_0 + \lambda_1 v^{q^i} + \lambda_2 \varphi^{q^i}(v, k),$$

$$k' = \lambda_0 + \lambda_1 k^{q^i} + \lambda_2 \varphi^{q^i}(k, v) \text{ [3]}.$$

PROPOSIZIONE D. *Ogni algebra con divisione, $\mathscr{A}$, di dimensione tre su K, è isomorfa ad un'algebra $\mathscr{A}(k)$.*

La condizione espressa dalla Proposizione C mal si presta, da sola, al computo delle algebre $\mathscr{A}(k)$ a due a due non isomorfe; si rende dunque necessario un più approfondito esame di questo punto. La seguente proposizione risponde a tale esigenza.

PROPOSIZIONE E. *Sia $k \neq v^{q^s}$, $s = 1, 2$, un elemento di $K_3 - K$ prefissato in modo che* (4) *sia soddisfatta. Il sistema lineare*

$$\begin{aligned} v &= y_0 + y_1 v^{q^i} + y_2 \varphi^{q^i}(v, k) \\ k &= y_0 + y_1 k^{q^i} + y_2 \varphi^{q^i}(k, v) \end{aligned} \tag{5}$$

ha un'unica soluzione $(y_0, y_1, y_2) \in K^3$ o solamente per $i = 0$ (in corrispondenza del quale è necessariamente $y_0 = y_2 = 0$, $y_1 = 1$) oppure qualunque sia $i \in \{0, 1, 2\}$. Quest'ultima circostanza poi si verifica se e solo se

$$\sigma_1(F(k)) = \sigma_1(F(v)) = e_2 \quad e \quad \sigma_2(F(k)) = \sigma_2(F(v)) = -e_1.$$

È facile dimostare che l'insieme

$$A = \{k \in K_3 - K : \text{l.i. } [v, k]_K, k \neq v^{q^s}, s = 1, 2\},$$

degli elementi, k, in corrispondenza dei quali $\mathscr{A}(k)$ è un'algebra con divisione non associativa, ha ordine $q^3 - q^2 - q - 2$.

In virtù della Proposizione E, gli elementi di A si ripartiscono in due classi disgiunte, A_1 e A_2.

A_1 è l'insieme degli elementi di A per cui il sistema lineare (5) ha una soluzione unicamente per $i = 0$;

$$A_2 = \{k \in A : \sigma_1(F(k)) = e_2, \sigma_2(F(k)) = -e_1\}$$

consiste di quegli elementi $k \in A$ per cui il sistema (5) è risolubile qualunque sia $i \in \{0, 1, 2\}$.

(3) $\varphi(k, v) = (k + v)(\sigma_1(F(v)) - v) - \sigma_2(F(v))$.

Dunque se

$$|A_2| = n, \tag{6}$$

allora

$$|A_1| = q^3 - q^2 - q - 2 - n \tag{7}$$

e, quindi, il numero, ν', delle algebre $\mathscr{A}(k)$ (ovvero, cfr. Proposizione D, di tutte le algebre $\mathscr{A}$) a due a due non isomorfe è

$$\nu' = |A_1|/3 + |A_2|. \tag{8}$$

Dopo queste osservazioni il computo di ν' è ricondotto a quello di n.

Per semplificare alcuni calcoli conviene supporre $e_2 = 0$ ed $e_1 \neq 0$ (cfr. (2)); ciò che, si dimostra, non è limitativo.

Se $k = \sum_0^2 {}_i\, x_i v^i$, allora le condizioni l.i. $[v, k]_K$, $\sigma_1(F(k)) = 0$ e $\sigma_2(F(k)) = -e_1$ si esplicitano in

$$(x_0 + e_1 x_2) x_2 - (x_1 + 1) x_1 \neq 0,$$

$$3 x_0 + 2 e_1 x_2 = 0,$$

$$3 x_0^2 + 4 e_1 x_0 x_2 - e_1 x_1^2 - 3 e_0 x_1 x_2 + e_1^2 x_2^2 = -e_1$$

rispettivamente e, per definizione, n è il numero delle soluzioni del loro sistema, tolte le due che corrispondono ai valori v^q e v^{q^2} di k.

A conti fatti risulta

$$n = \begin{cases} q - 4, & \text{se } q \equiv 1 \pmod 3, \\ q - 2, & \text{se } q \not\equiv 1 \pmod 3. \end{cases}$$

Di qui e dalle (6), (7) e (8) segue $\nu' = \nu$ (cfr. (1)).

Si osservi, per concludere, che tutti i possibili piani proiettivi sopra le algebre con divisione $\mathscr{A}$ ($\dim_K \mathscr{A} = 3$) – del tipo V secondo la classificazione di Lenz–Barlotti (cfr. [7]) – sono completamente determinati dalla Proposizione A (cfr. anche [5] e [6]).

BIBLIOGRAFIA

[1] A. A. ALBERT (1952) – *On nonassociative division algebras*, « Trans. Amer. Math. Soc. », *72*, 296–309.

[2] A. A. ALBERT (1958) – *Finite noncommutative division algebras*, « Proc. Amer. Math. Soc. », *9*, 928–932.

[3] A. A. ALBERT (1960) – *Finite division algebras and finite planes*, « Proc. Symp. Appl. Math. », *10*, 53–70.

[4] A. A. ALBERT (1961) – *Generalized twisted fields*, « Pacif. J. Math. », *11*, 1–8.

[5] A. A. ALBERT (1961) – *Isotopy for generalized twisted fields*, « An. Acad. Brasil. Ci. », *33*, 265–275.

[6] A. A. ALBERT (1963) – *On the collineation groups associated with twisted fields*, Calcutta Math. Soc. Golden Jubilee Commemoration volume (1958/59), part II, 485–497.

[7] P. DEMBOWSKI (1968) – *Finite geometries*, « Ergebn. der Mathem. und ihrer Grenzg. », Band *44*, Springer–Verlag.

[8] L. E. DICKSON (1905) – *On finite algebras*, « Nachr. kgl. Ges. Wiss. », Göttingen, 358–393.

[9] L. E. DICKSON (1906) – *Linear algebras in which division is always uniquely possible*, « Trans. Amer. Math. Soc. », *7*, 370–390.

[10] I. KAPLANSKY (1976) – *Three-dimensional division algebras*, I, « J. Algebra », *40*, 384–391.

[11] I. KAPLANSKY (1975) – *Three-dimensional division algebras*, II, « Houston J. of Math. », *1*, 63–79.

[12] G. MENICHETTI (1973) – *Algebre tridimensionali su un campo di Galois*, « Ann. Mat. Pura Appl. », *97* (4), 283–302.