Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Marcello Cicchese

Sulle cubiche di un piano di Galois

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **32** (1962), n.1, p. 38–42.

Accademia Nazionale dei Lincei

¡http://www.bdim.eu/item?id=RLINA_1962_8_32_1_38_0¿

Geometria. — *Sulle cubiche di un piano di Galois.* Nota di MARCELLO CICCHESE, presentata (*) dal Socio B. SEGRE.

INTRODUZIONE. – Nel presente scritto riassumo ed illustro brevemente i risultati da me conseguiti sulle curve algebriche del terz'ordine (o cubiche) di un piano di Galois; rimandando ad una successiva pubblicazione la trattazione completa degli argomenti affrontati.

I caratteri delle cubiche sono stati ampiamente studiati nel caso in cui tali curve siano pensate appartenenti al piano proiettivo reale o complesso (cioè costruito sul campo degli ordinari numeri reali o complessi); ma relativamente poco si sapeva finora sulle cubiche di un piano di Galois.

Il primo autore che abbia fermato la sua attenzione su tali curve, è stato il Dickson. Egli, tuttavia, non ha mai intrapreso uno studio organico delle cubiche di un piano finito, dal momento che il suo interesse per queste curve era determinato soltanto dal desiderio di risolvere alcune questioni riguardanti certe strutture algebriche.

Un teorema particolarmente interessante, enunciato dal Dickson, può essere espresso nel modo seguente:

« Una cubica di un piano di Galois, che sia priva di punti sul campo base, si spezza, in un'estensione di terzo grado di tale campo, in tre rette fra loro coniugate ».

In una sua Nota (1), il Dickson ha creduto di aver dato una dimostrazione del suddetto teorema. In realtà, come è stato notato da più persone, tale dimostrazione contiene un errore che ne pregiudica la validità.

Molto più tardi, L. Carlitz ha ripreso il teorema (2), e ne ha data una dimostrazione di carattere algebrico, nella quale però – come il prof. B. Segre ha fatto notare nelle sue lezioni presso l'Istituto Nazionale di Alta Matematica – quegli sfrutta, in modo essenziale, un risultato che il Dickson afferma di aver conseguito, ma di cui non porge alcuna prova. Anche in questo caso, non si può dunque parlare di una effettiva dimostrazione.

Il prof. B. Segre ha rilevato che il teorema in questione può essere dedotto facilmente da un importante risultato di A. Weil (3), il quale stabilisce una limitazione per il numero dei punti delle curve algebriche irriducibili di un piano di Galois.

Seguendo una via di ricerca proposta dal prof. B. Segre, sono riuscito – sotto certe ipotesi relative all'ordine e alla caratteristica del campo base –

(*) Nella seduta del 13 gennaio 1962.

(1) L. E. DICKSON, *On triple algebras and ternary cubic forms*, « Bull. Amer. Math. Soc. », vol. 14, pp. 160–169 (1907–1908).

(2) L. CARLITZ, *A theorem of Dickson on nonvanishing cubic forms in a finite field*, « Proc. Amer. Math. Soc. », vol. 8, pp. 975–977 (1957).

(3) A. WEIL, *Sur les courbes algébriques et les variétés qui s'en déduisent*, ed. Hermann, Parigi 1948, p. 70.

a trovare un'altra dimostrazione del teorema del Dickson, basata soltanto su considerazioni algebrico-geometriche. Ciò non può essere considerato privo di interesse, se si pensa che il risultato del Weil fa parte di una trattazione molto complessa, che si giova di procedimenti di carattere assai elevato, piuttosto distanti dalla geometria algebrica classica; senza contare che, per la via da me seguita, si trovano anche varie proposizioni del tutto nuove.

1. Passo ora ad illustrare sommariamente i risultati da me ottenuti.

Denoterò, come al solito, con $S_{2,q}$ un piano di Galois costruito sul campo finito GF (q). Sull'ordine $q = p^h$ (p primo, h intero ≥ 1) di GF (q) ho fatto le seguenti ipotesi:

$$p > 3 \quad , \quad q \not\equiv 1 \pmod 3.$$

Tali limitazioni sono state poste per il desiderio di non discostarsi troppo dal caso classico delle cubiche appartenenti al piano proiettivo reale. Invero, per $p = 2, 3$ si presentano delle peculiarità che richiedono un'analisi del tutto diversa da quella che si può compiere nel caso generale. La necessità della seconda limitazione appare, a prima vista, meno evidente. Le due eventualità:

$$q \not\equiv 1 \pmod 3 \quad , \quad q \equiv 1 \pmod 3$$

sono tuttavia fra loro più distanti di quanto non ci si potrebbe aspettare. Nel primo caso, tutti gli elementi di GF (q) ammettono una ed una sola radice cubica in GF (q) (analogamente a quanto accade nel campo dei numeri reali). Nel secondo caso, si ha invece che soltanto $(q-1)/3$ elementi (non nulli) di GF (q) sono dei cubi in GF (q); e ciascuno di essi possiede esattamente tre radici cubiche nel campo base. Questa diversità conduce a divergenze notevoli, per quanto riguarda gli sviluppi geometrici che competono ai due casi possibili: e ciò giustifica la limitazione introdotta.

2. Le cubiche di $S_{2,q}$ possono classificarsi in: *a*) cubiche spezzate in tre rette [distinte o coincidenti, appartenenti a GF (q) o coniugate in un'estensione di GF (q)]; *b*) cubiche spezzate in una retta ed in una conica irriducibile; *c*) cubiche singolari irriducibili; *d*) cubiche non singolari. Il primo problema da me completamente risolto, e che qui mi limito ad accennare, è quello di contare le cubiche di ciascuno dei tipi suddetti.

3. Nelle ipotesi fatte, una cubica [4] possiede, analogamente al caso classico, nove flessi nella chiusura algebrica di GF (q). Ho trovato che si possono unicamente verificare le seguenti tre possibilità:

« Una cubica può soltanto avere 0, 1, o 3 flessi in GF (q) ».

Denoterò, in tutto il seguito, con C_0, C_1, C_3, tre generiche cubiche aventi rispettivamente 0, 1, 3 flessi in GF (q).

(4) Sottintenderò sempre, salvo esplicito avviso in contrario, che si tratti di una cubica non singolare di $S_{2,q}$.

Ho portato a compimento lo studio della configurazione dei flessi di una qualsiasi cubica. Più precisamente, sono giunto a stabilire che:

i sei flessi non in GF (q) di una C_3 appartengono ciascuno a GF (q^2) [5];

gli otto flessi non in GF (q) di una C_1 appartengono ciascuno a GF (q^4), oppure a GF (q^8);

dei nove flessi di una C_0, tre appartengono a GF (q^3) e sei appartengono a GF (q^6).

Inoltre, per quel che riguarda i trilateri inflessionali ho trovato che:

dei quattro trilateri inflessionali di una C_3, due appartengono a GF (q) [uno di essi essendo composto da tre rette di GF (q), mentre l'altro è composto da una retta di GF (q) e da due rette coniugate di GF (q^2)] e gli altri due si trovano in GF (q^2);

i quattro trilateri inflessionali di una C_1 appartengono ciascuno a GF (q^4) [ognuno di essi essendo composto da una retta di GF (q^4) e da due rette che possono appartenere o a GF (q^4) o a GF (q^8)];

dei quattro trilateri inflessionali di una C_0, due appartengono a GF (q) [uno di essi essendo composto da una retta di GF (q) e da due rette coniugate di GF (q^2), mentre l'altro è composto da tre rette coniugate di GF (q^3)], e gli altri due si trovano in GF (q^2).

4. Un'altra questione compiutamente trattata è quella relativa alle trasformazioni omografiche di una cubica in sé. Ad esempio, circa le 18 omografie che trasformano in sè una cubica generale (cioè che non sia né armonica né equianarmonica), ho dimostrato che:

esistono 6 omografie di GF (q) e 12 di GF (q^2) trasformanti in sé una C_3 generale;

esistono 2 omografie di GF (q) e 16 di GF (q^2) trasformanti in sé una C_1 generale;

esistono 3 omografie di GF (q), 6 di GF (q^2), 3 di GF (q^3), 6 di GF (q^6) trasformanti in sé una C_0 generale.

5. Una cubica possiede un ben noto invariante assoluto $J = S^3/T^2$, dove S e T sono forme, rispettivamente di quarto e di sesto grado, nei coefficienti della cubica; S e T costituiscono poi degli invarianti relativi della cubica, rispettivamente di peso quattro e sei. Tenuto conto di ciò, ho stabilito condizioni necessarie e sufficienti per l'equivalenza proiettiva in GF (q) di due qualsiansi cubiche; ed ho trovato che:

condizione necessaria e sufficiente affinché due cubiche non armoniche siano fra loro proiettive in GF (q) è che esse abbiano uguali l'invariante assoluto $J = S^3/T^2$, il carattere quadratico [cioè il fatto di essere un quadrato o un non-quadrato di GF (q)] dell'invariante di sesto grado T, non nullo per ciascuna di quelle, nonché il numero dei flessi in GF (q).

Per quel che concerne le cubiche armoniche (corrispondenti al caso $T = 0$) ho stabilito che:

(5) Indico con GF (q^n) (n intero ≥ 1) un'estensione di grado n di GF (q).

condizione necessaria e sufficiente affinché due cubiche armoniche siano fra loro proiettive in GF (q) è che il rapporto dei loro invarianti di quarto grado S sia una potenza quarta di un elemento di GF (q), e che inoltre abbiano lo stesso numero di flessi in GF (q).

6. Un altro problema cui ho dato una risposta completa, è quello riguardante la determinazione del numero dei tipi proiettivi distinti delle C_0, o delle C_1, o delle C_3. Più precisamente, ho trovato che:

esistono $q-1$ tipi proiettivi distinti di C_0;

» $q+1$ » » » C_1 (se $q \not\equiv 1 \bmod 4$);

» $q+3$ » » » C_1 (se $q \equiv 1 \bmod 4$);

» $q-1$ » » » C_3.

Inoltre, facendo uso dei precedenti risultati riguardanti le omografie di una cubica in sé, ho stabilito che:

esistono $\frac{q-1}{3}N$ C_0;

» $\frac{q+1}{2}N$ C_1;

» $\frac{q-1}{6}N$ C_3;

denotando con N il ben noto numero delle omografie non degeneri di $S_{2,q}$ in sé [cfr. ad esempio: B. Segre, *Lectures on modern geometry* (Roma, Cremonese, 1961), n. 169].

7. Per quel che riguarda la determinazione del numero dei punti di una cubica, ho visto che alcune cubiche armoniche, ed altre equianarmoniche, contengono esattamente $q+1$ punti. Inoltre, poggiando su considerazioni fatte dal prof. B. Segre sulle radici del polinomio $x^3 - ax + b$, ho stabilito il seguente teorema:

se N e $\bar{N}$ indicano i numeri dei punti di due cubiche non armoniche dotate entrambe di almeno un flesso in GF (q), che abbiano lo stesso invariante assoluto e che non siano fra loro proiettive in GF (q), risulta sempre $N + \bar{N} = 2q + 2$.

Per mettere in risalto l'efficacia di quest'ultimo teorema, occorre avvertire che ho anche stabilito che:

per ogni $J \in GF(q)$, esistono esattamente due tipi proiettivi di cubiche dotate di almeno un flesso in GF (q) ed aventi tale J come invariante assoluto.

Un discorso particolare va fatto per le cubiche armoniche. Anzitutto occorre distinguere i due casi:

$$q \not\equiv 1 \pmod 4 \quad , \quad q \equiv 1 \pmod 4.$$

Nel primo caso, si ha che le cubiche armoniche che abbiano almeno un flesso in GF (q) hanno di necessità esattamente tre flessi in GF (q); esse si suddivi-

dono in due tipi proiettivi, ciascuno dei quali contiene esattamente $q + 1$ punti. Nel secondo caso, si ha che ciascuna cubica armonica ha uno ed un solo flesso in GF (q), le cubiche in questione suddividendosi in quattro tipi proiettivi, i quali sono tali che gli invarianti di quarto grado di due di essi sono dei quadrati, mentre gli invarianti di quarto grado degli altri due sono dei non–quadrati. Ho poi dimostrato che:

se N e $\bar{N}$ indicano i numeri dei punti di due cubiche armoniche fra loro non proiettive in GF (q), tali che il rapporto dei loro invarianti di quarto grado sia un quadrato, risulta sempre $N + \bar{N} = 2q + 2$.

8. Per le C_1 e per le C_3 [cioè per le cubiche dotate di almeno un flesso in GF (q)] ho potuto far uso di una classica equazione canonica, che ha consentito lo studio delle principali proprietà delle cubiche di questo tipo. Restava aperto il problema di trovare un'equazione canonica per le cubiche prive di flessi in GF (q). Tale questione è stata risolta, l'equazione canonica delle C_0 essendo data (in coordinate non omogenee) da

$$y^3 - 3\lambda(x^2 - \rho x + 1)y - (x^3 - 3x + \rho) = 0,$$

dove λ è un parametro variabile in GF (q), e ρ denota un qualsiasi fissato elemento (certamente esistente) di GF (q) tale che il polinomio $x^3 - 3x + \rho$ sia irriducibile in GF (q).

9. Ho inoltre dimostrato che, se J è l'invariante assoluto di una C_0, esistono esattamente due tipi proiettivi di C_3 aventi tale J come invariante assoluto; e viceversa. Ciò significa che i valori degli invarianti assoluti che competono alle C_0 sono tutti e soli quelli che competono alle C_3.

In base a quest'ultimo risultato, e tenendo conto di alcune note proprietà delle trasformazioni birazionali delle cubiche, si può dire che una C_0 che abbia almeno un punto è sempre birazionalmente equivalente [in GF (q)] ad una C_3. Il prof. B. Segre ha proposto di studiare la corrispondenza che così si ottiene, tra i tipi proiettivi delle C_0 e quelli delle C_3, onde cercare di dimostrarne la biunivocità. A ciò sono potuto effettivamente pervenire. Si può dunque affermare che:

ogni C_0 è sempre riconducibile, mediante una trasformazione birazionale su GF (q), ad una C_3; e viceversa.

Da questa proposizione segue che ogni C_0 ha almeno tre punti (corrispondenti ai tre flessi della C_3 birazionalmente equivalente alla C_0); e ciò costituisce una nuova dimostrazione del teorema del Dickson, di cui è detto nell'introduzione.

10. Un breve studio è stato anche fatto sulle cubiche singolari irriducibili, trovando che:

una cubica nodata ha uno ed un solo flesso in GF (q);

una cubica dotata di punto doppio isolato può avere soltanto 0 o 3 flessi in GF (q), entrambi i casi essendo effettivamente possibili.