
ATTI ACCADEMIA NAZIONALE DEI LINCEI
CLASSE SCIENZE FISICHE MATEMATICHE NATURALI
RENDICONTI

FRANCESCO ZIRILLI

Su una classe di k -archi di un piano di Galois

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. 54 (1973), n.3, p. 393–397.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1973_8_54_3_393_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Geometria. — *Su una classe di k -archi di un piano di Galois.*

Nota (*) di FRANCESCO ZIRILLI, presentata (**) dal Socio B. SEGRE.

SUMMARY. — In this paper we prove that, in a Galois plane $S_{2,q}$, every elliptic cubic curve having exactly $N = 2k$ points contains a k -arc. We make use of a new method of investigation, by considering the canonical structure of quasigroup defined (in a natural way) on the set of the simple points of an irreducible cubic curve. In addition we obtain further results, some of which are already known, for a rational cubic in a $S_{2,q}$.

1. Sia $S_{2,q}$ un piano di Galois ($q = p^h$, p primo), [6]. Scopo principale di questo lavoro è provare che:

(1.1) *Ogni cubica ellittica di $S_{2,q}$ su cui giacciono esattamente $N = 2k$ punti contiene almeno un k -arco.*

Osservato che, come mostreremo, qualunque sia $q = p^h$, esistono in $S_{2,q}$ cubiche ellittiche con un numero pari di punti, si perviene così ad una nuova classe di k -archi che (per q sufficientemente grande) *non sono contenuti in una conica* e per i quali, in virtù delle note limitazioni di Hasse-Weil [5], [9], si ha:

$$(1.1.1) \quad (q - 2\sqrt{q} + 1)/2 \leq k \leq (q + 2\sqrt{q} + 1)/2.$$

Al risultato (1.1) si giunge utilizzando la nota struttura di quasigruppo definita nell'insieme, D , dei punti non singolari di una cubica irriducibile, assumendo, per ogni $(a, b) \in D \times D$, il prodotto ab uguale all'ulteriore intersezione con D della retta per a e b , e dimostrando che:

(1.2) *Se D ha numero pari di punti, D ammette almeno un sottoquasigruppo, H , di ordine $|D|/2$: allora, $K = D - H$ è un $|D|/2$ -arco di $S_{2,q}$.*

Dalla (1.2) si deduce, tra l'altro, anche che:

(1.3) *Ogni cubica razionale di $S_{2,q}$, q dispari, con punto doppio isolato contiene un $(q + 3)/2$ -arco.*

(1.4) *Ogni cubica razionale di $S_{2,q}$, q dispari, con punto doppio nodale contiene un $(q + 1)/2$ -arco.*

(1.5) *Ogni cubica razionale con punto doppio cuspidale di $S_{2,2^h}$ contiene un $(2^{h-1} + 2)$ -arco.*

(*) Lavoro eseguito col contributo del C.N.R., nell'ambito del gruppo di ricerca G.N.S.A.G.A.

(**) Nella seduta del 10 marzo 1973.

Con la (1.3) si amplia un risultato ottenuto in [2], p. 821, Proposizione VI, sotto le condizioni $q \equiv 2 \pmod{3}$ e $q \not\equiv 1 \pmod{4}$. La (1.4) trovata già in [1] e la (1.5) in [3], Proposizione I, p. 241.

Si noti che, con la (2.10), noi proveremo una proposizione più ampia della (1.5).

2. In questo numero si dimostrano le proposizioni sopra enunciate.

Sia, dunque, C una cubica irriducibile di un piano di Galois $S_{2,q}$; e si ponga $D = C$, se C è ellittica, $D = C - \{o\}$, se C è razionale ed o è il suo punto doppio. Si indichi con $r(a, b)$, $(a, b) \in S_{2,q} \times S_{2,q}$, $a \neq b$, la retta congiungente i punti a e b ; e sia $\tau: D \rightarrow D$ l'applicazione che a ciascun elemento di D associa il suo tangenziale. Si consideri, quindi, l'applicazione $\omega: D \times D \rightarrow D$ definita nel modo seguente: posto, per ogni $(a, b) \in D \times D$, $\omega(a, b) = ab$, se $a \neq b$ ed $r(a, b)$ non è tangente a C , ab è l'ulteriore intersezione di $r(a, b)$ con D ; se $a \neq b$ ed $r(a, b)$ è tangente a C in a (in b), $ab = a$ (rispettivamente, $ab = b$); se $a = b$, $aa = a^2$ è il tangenziale di a : $a^2 = \tau(a)$.

È noto [4], [10], che D , rispetto all'operazione sopra definita, è un *quasigruppo semisimmetrico, mediale, commutativo*, vale a dire, per ogni $(a, b, c, d) \in D \times D \times D \times D$, le equazioni $ax = b$ e $ya = b$ sono univocamente risolubili, $a(ba) = b$, $(ab)(cd) = (ac)(bd)$, $ab = ba$. La legge di *medialità* (detta anche di *entropia*) discende dal ben noto teorema di Poncelet; le altre sono evidenti.

Per stabilire il risultato che abbiamo in vista, identificheremo D con il quasigruppo (D, ω) e utilizzeremo la teoria dei quasigruppi semisimmetrici mediali (cfr. [10]).

Indichiamo con E l'insieme degli elementi di D che sono tangenziali:

$$(2.1) \quad E = \tau(D) = \{b \in D \mid \text{esiste } a \in D \text{ per cui } a^2 = b\}.$$

E è un sottoquasigruppo di D ([10], p. 213, (6.3)).

Se $b \in E$, l'insieme R_b degli elementi di D il cui tangenziale è b , $R_b = \{a \in D \mid a^2 = b\}$, ha cardinalità $t = |R_b| \geq 1$ che non dipende da $b \in E$. L'intero t è una potenza di 2:

$$(2.2) \quad t = 2^n, \quad n \text{ intero opportuno} \geq 0,$$

([10], p. 221, (10.8)); inoltre risulta

$$(2.3) \quad |D| = t |E|$$

([10], p. 221, (10.7)). Chiaramente t è il numero delle rette passanti per $b \in E$ e tangenti a C altrove, se b non è un flesso, altrove o in b , se b è un flesso. Dal fatto che una retta di $S_{2,q}$ è una 2-secante di D se, e solamente se, è tangente a C in un punto non di flesso, detto $m_i(a)$, $a \in D$,

il numero delle rette i -secanti di D , $i = 1, 2, 3$, e passanti per a , segue allora che:

$$(2.4) \quad \text{se } a \in D - E, m_2(a) = 1; \text{ se } a \in E \text{ e non è un flesso, } m_2(a) = t + 1; \\ \text{se } a \text{ è un flesso, } m_2(a) = t - 1.$$

È poi ben noto che:

$$(2.5) \quad |D| = 1 + m_2(a) + 2 m_3(a).$$

Si verifica subito, tenendo conto del significato geometrico di t , sopra richiamato, e prendendo $b = o_3(0, 0, 1) \in E$, che, se q è pari, $t \in \{1, 2, q = 2^h\}$, risultando $t = q$, se, e soltanto se, la cubica C è cuspidata; se q è dispari, $t \in \{1, 2, 4\}$. Chiamiamo t *indice tangenziale* di C .

Osserviamo che, qualunque sia q , esistono in $S_{2,q}$ cubiche ellittiche con numero pari di punti. Infatti la cubica ellittica di equazione, in coordinate proiettive omogenee x_1, x_2, x_3 :

$$x_1^2 x_2 - x_1 x_2^2 + x_1 x_3^2 + x_2 x_3^2 + \lambda x_1 x_2 x_3 = 0, \quad \text{con } \lambda \neq 0,$$

$$\text{per } q \text{ pari,} \quad \lambda = 0, \quad \text{per } q \text{ dispari,}$$

passante per i punti $o_1(1, 0, 0)$, $o_2(0, 1, 0)$, $o_3(0, 0, 1)$, essendo tangente ad $r(o_1, o_3)$ in o_1 e ad $r(o_2, o_3)$ in o_2 , ha indice tangenziale $t \geq 2$, e quindi, tenuto conto di (2.3), (2.2), numero pari di punti.

Tornando alla cubica C di cui all'inizio del presente numero e al quasi-gruppo D dei suoi punti non singolari, supponiamo, d'ora in poi, che $|D|$ sia pari, e si ponga:

$$(2.6) \quad |D| = 2k.$$

In virtù delle (2.4), (2.5), (2.6), se $b \in E$, risulta $|D| = 2k = t + 2m_3(b)$, ovvero $|D| = 2k = 2 + t + 2m_3(b)$, a seconda che b sia, o non, un flesso. Ne segue, in ogni caso:

$$(2.7) \quad t \geq 2.$$

Si consideri il quasigruppo quoziente D/E (costituito dalle classi laterali di E , $aE = \{a' \in D \mid a' = ab, b \in E\}$, $a \in D$, nel quale gli elementi si compongono mediante la legge: $(aE)(cE) = (ac)E$). Esso è un gruppo di esponente 2 (cioè, per ogni $X \in D/E$, X^2 è l'elemento neutro) ed ha ordine uguale all'indice tangenziale $t \geq 2$ di C ([10], p. 220, (10.6); p. 221, (10.8)). Allora, come è noto, D/E ammette $t - 1 \geq 1$ sottogruppi di ordine $t/2$. Ciò posto, si ha:

$$(2.8) \quad \text{Sia } \mathcal{H} \text{ un sottogruppo di } D/E \text{ di ordine } t/2, \text{ comunque fissato, e siano} \\ H_1, H_2, \dots, H_{t/2} \text{ le classi laterali di } E \text{ che lo costituiscono. Allora,} \\ H = H_1 \cup H_2 \cup \dots \cup H_{t/2} \text{ è un sottoquasigruppo di } D \text{ di ordine } k \text{ e} \\ K = D - H \text{ è un } k\text{-arco di } S_{2,q}.$$

Poichè $|H_i| = |E|$ ($i = 1, 2, \dots, t/2$) e $H_i \cap H_j = \emptyset$, $i \neq j$ ($i, j = 1, 2, \dots, t/2$), è, senz'altro, $|H| = t/2 |E|$ e quindi, per (2.3), (2.6), $|H| = k = |D - H| = |K|$. Da $(a', a'') \in H \times H$ segue $a' \in H_i$, $a'' \in H_j$, onde $a'a'' \in H_i H_j = H_l \subseteq H$ (i, j, l opportuni, appartenenti a $\{1, 2, \dots, t/2\}$). Pertanto, H è un sottoquasigruppo di D ([10], p. 211, (4.1)). Si consideri, ora, il quasigruppo quoziente D/H . Esso è un gruppo di ordine 2, costituito dall'elemento neutro H e da $K = D - H$, e quindi con legge di composizione:

$$(2.9) \quad K^2 = H = H^2, \quad HK = KH = K.$$

Per la prima delle (2.9), da $(a, b) \in K \times K$ segue $ab \in H$. Ciò vuol dire, se $a \neq b$, che $r(a, b) \cap K = \{a, b\}$. Pertanto K è un k -arco. Resta così provata la (2.8) e, con essa, la (1.2).

Col procedimento sopra indicato si costruiscono $t - 1$ (≥ 1) k -archi distinti contenuti in D , tanti quanti sono i sottogruppi $\mathcal{H}$ di ordine $t/2$ di D/E .

La (1.1) discende subito da quanto precede, essendo, per una cubica ellittica C , $D = C$.

Se C è razionale, si osservi che $|D| = |C| - 1$ è pari nei seguenti casi:

- 1) q è dispari e il punto doppio di C è isolato ($|D| = q + 1$);
- 2) q è dispari e il punto doppio di C è un nodo ($|D| = q - 1$);
- 3) q è pari e il punto doppio di C è una cuspidale ($|D| = q = 2^h$).

Nel 1) e 2) caso è $t = 2$. Se al k -arco sopra costruito, contenuto in D , si aggrega il punto doppio o , nel primo caso si ottiene un $(q + 3)/2$ -arco contenuto in C , nel secondo un $(q + 1)/2$ -arco contenuto in C . Di qui le (1.3), (1.4).

Nel 3) caso è $t = q = 2^h$: detto f il flesso di C , è noto che ogni retta per f non passante per il punto doppio o è tangente a C ; ne segue subito che:

(2.10) *aggregando a ciascuno dei $q/2$ -archi, in numero di $q - 1$, contenuti in D , costruiti col procedimento indicato nella (2.8), i punti o ed f , si ottengono altrettanti $(q + 4)/2$ -archi distinti contenuti in C .*

La (1.5) è così provata e si ritrova, fra gli altri, anche il $(q + 4)/2$ -arco di cui alla Proposizione I di [3], p. 241.

BIBLIOGRAFIA

- [1] C. DI COMITE, *Su k -archi contenuti in cubiche piane*, « Rend. Acc. Naz. Lincei, Cl. Sc. Fis. Mat. Nat. » (8), 35, 274-278 (1963).
- [2] C. DI COMITE, *Intorno a certi $(q + 9)/2$ -archi di $S_{2,q}$* , « Rend. Acc. Naz. Lincei, Cl. Sc. Fis. Mat. Nat. » (8), 36, 819-824 (1964).
- [3] C. DI COMITE, *Alcuni k -archi completi di un piano di Galois di caratteristica due*, « Rend. Acc. Naz. Lincei, Cl. Sc. Fis. Mat. Nat. », (8) 47, 240-244 (1969).

- [4] I. M. H. ETHERINGTON, *Quasigroups and cubic curves*, « Proc. Edinburgh Math. Soc. » (2), 14, 273–291 (1964/65).
- [5] H. HASSE, *Zur theorie der abstrakten elliptischen funktionenkörper, III*, « J. Reine Angew. Math. », 175, 193–208 (1936).
- [6] B. SEGRE, *Le geometrie di Galois*, « Annali di Mat. » (4), 48, 1–96 (1959).
- [7] B. SEGRE, *Lectures on Modern Geometry* (Cremonese, Roma, 1961).
- [8] B. SEGRE, *Introduction to Galois geometries*, « Memorie Acc. Naz. Lincei, Cl. Sc. Fis. Mat. Nat. » (8), 8, 133–236 (1967).
- [9] A. WEIL, *Sur les courbes algébriques et les variétés qui s'en déduisent*, « Act. Sci. et Ind. », 1041, Hermann, Paris, 1948.
- [10] F. ZIRILLI, *C-struttura associata ad una cubica piana e C-struttura astratta*, « Ricerche di Matem. », 16, 202–232 (1967).