Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Claudio Di Comite

Alcuni k-archi completi di un piano di Galois di caratteristica due

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **47** (1969), n.5, p. 240–244.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1969_8_47_5_240_0>

Geometria. — *Alcuni k–archi completi di un piano di Galois di caratteristica due* (*). Nota di CLAUDIO DI COMITE, presentata (**) dal Socio B. SEGRE.

RIASSUNTO. — In a Galois plane of order 2^h, with $h \geq 8$, complete k–arcs are constructed, with $k = 2^{h-1} + 2$ for h even and $k = 2^{h-1} + 3$ for h odd.

1. – In un piano di Galois $S_{2,q}$ (cioè in un piano proiettivo sopra un campo di Galois γ di ordine q), con $q = 2^h$, le ovali (archi di $S_{2,q}$ di ordine massimo) contengono, com'è noto (B. Segre [5]), $q + 2$ punti. Un esempio di ovale si ottiene aggregando ad una conica non degenere il suo nucleo (B. Segre [2], [3], [5], [6]). Per $h = 5$ e per $h \geq 7$, mediante una curva rappresentata in coordinate non omogenee (x, y) dall'equazione

$$y = x^r, \tag{1.1}$$

con $r = 2^g$, g intero opportuno, sono state costruite (B. Segre [3], [4], [5], [6]) ovali che non possono ottenersi aggregando ad una conica il suo nucleo.

Si hanno esempi di k–archi completi di $S_{2,q}$ che non sono ovali, oltre che per particolari valori di h (B. Segre [3], M. Scafati [8]), per $h \geq 5$ dispari, nel qual caso è stata provata (M. Tallini Scafati [9]) l'esistenza di $(q + 4)/2$–archi completi.

In questo lavoro, mediante una curva (1.1) con $r = 3$, si costruiscono in $S_{2,q}$ $(q + 4)/2$–archi completi, per $h \geq 8$ pari, e $(q + 6)/2$–archi completi, per $h \geq 9$ dispari.

2. – In un piano di Galois $S_{2,q}$, con $q = 2^h$, si consideri la cubica C^3 rappresentata, in un sistema di coordinate omogenee (x_1, x_2, x_3), dall'equazione.

$$x_1^3 + x_2^2 x_3 = 0.$$

Si verifica facilmente quanto segue: la cubica C^3 è irriducibile, ha un punto doppio in $O_3(0, 0, 1)$ con tangenti principali coincidenti con la retta di equazione $x_2 = 0$, ha un flesso in $O_2(0, 1, 0)$ con tangente la retta di equazione $x_3 = 0$; i restanti $q - 1$ punti di C^3 in $S_{2,q}$ sono semplici non di flesso e la tangente in ciascuno di essi passa per il flesso; i q punti di C^3 diversi da O_3 hanno coordinate $(u, 1, u^3)$, con $u \in \gamma$; indicato con $P(u)$, per ogni $u \in \gamma$, il punto di coordinate $(u, 1, u^3)$, tre punti distinti di C^3, $P(u)$, $P(v)$ e $P(w)$, sono allineati se e solo se

$$u + v + w = 0. \tag{2.1}$$

(*) Lavoro eseguito nell'ambito dell'attività del Contratto di Ricerca del C.N.R. « Geometria, Algebra e Questioni Connesse ».

(**) Nella seduta del 15 novembre 1969.

È noto, cfr. [5], [6], che un elemento $u \in \gamma$ si dice di prima o di seconda categoria a seconda che l'equazione $x^2 + x + u = 0$ ammetta o non ammetta soluzioni x in γ. Indicati con γ_1 e γ_2 rispettivamente l'insieme degli elementi di prima categoria e l'insieme degli elementi di seconda categoria, è ben noto che γ_1 e γ_2 contengono ciascuno $q/2$ elementi e che la somma di due elementi di una stessa categoria è un elemento di prima categoria, mentre la somma di un elemento di prima categoria e di un elemento di seconda categoria è un elemento di seconda categoria.

Allora, la somma di tre qualunque elementi di γ_2 è un elemento di γ_2 e quindi, poiché lo zero appartiene a γ_1, non può mai essere nulla.

Si conclude che:

PROP. 1. – *L'insieme costituito dai punti* O_2, O_3 *e dai punti* $P(u)$, *con* $u \in \gamma_2$, *è un* $(q+4)/2$*–arco* K *di* $S_{2,q}$.

3. – Si proverà che:

PROP. 2. – *Per il punto* $O_1(1, 0, 0)$ *passa una secante di* K *se e solamente se* h *è pari.*

Poiché O_1O_3 è la tangente cuspidale della cubica C^3, le rette congiungenti la cuspide O_3 con i punti semplici di C^3 non passano per O_1. Inoltre, si verifica subito che O_1 è allineato con i punti $P(u)$ e $P(v)$ di C^3, con $u, v \in \gamma$ e $u \neq v$, se e solo se

$$u^2 + uv + v^2 = 0. \tag{3.1}$$

È noto ([5], [6]) che l'unità di γ appartiene a γ_2 se e solo se h è dispari. Ne consegue che, se h è dispari, non esistono due elementi distinti u e v di γ tali che sia soddisfatta la (3.1).

Si conclude che, se h è dispari, le rette congiungenti punti distinti di C_3, e quindi in particolare le secanti di K, non passano per O_1.

Se h è pari, si proverà che esistono due elementi distinti u e v appartenenti a γ_2 i quali verificano la (3.1). A tal fine, detto r un elemento di γ tale che

$$r^2 + r + 1 = 0, \tag{3.2}$$

è sufficiente determinare due elementi u e v di γ_2 tali che

$$u = vr \tag{3.3}$$

(è evidente che se u e v appartengono a γ_2 e verificano la (3.1) o la (3.3), essi sono distinti).

Allora, fissato ad arbitrio un elemento t di γ_2 e posto

$$f(x) = x^2 + x + t \quad , \quad g(y) = y^2 + y + t, \tag{3.4}$$

si consideri, in un piano affine di coordinate (x, y) associato ad $S_{2,q}$, la conica C^2 di equazione

$$f(x) + rg(y) = 0.$$

Si verifica facilmente che C^2 è non degenere. Dette (x_0, y_0) le coordinate di un suo punto proprio Q e posto $u = f(x_0)$, $v = g(y_0)$, poiché $Q \in C^2$ gli elementi u e v verificano la (3.3); inoltre u, essendo somma di $x_0^2 + x_0 \in \gamma_1$ e di $t \in \gamma_2$, è un elemento di γ_2, analogamente risulta $v \in \gamma_2$. Si conclude che O_1 è allineato con i punti $P(u)$ e $P(v)$ di K.

Si proverà ora che:

PROP. 3. – *Se è $h \geq 8$ (h pari o dispari), per ogni punto di $S_{2,q}$ diverso da O_1 passa una secante di* K.

Sia T un qualunque punto di $S_{2,q}$ diverso da O_1. Se T appartiene alla retta O_2O_3, per T passa una secante di K (la retta O_2O_3). Si supponga dunque $T \notin O_2O_3$ e siano $(1, a, b)$ le sue coordinate; essendo $T \neq O_1$, risulta $(a, b) \neq (0, 0)$.

Supposto $a \neq 0$ e $b \neq 0$, si verifica subito che, se $a^{-1} \in \gamma_2$, T appartiene alla secante $O_3 P(a^{-1})$, e, se $a^{-1} \in \gamma_1$ e $a^2 b = 1$, risulta $T = P(a^{-1})$ e quindi, per la (2.1), per ogni $u \in \gamma_2$, T appartiene alla retta $P(u) P(a^{-1} + u)$, secante di K.

Si supponga allora che, se a e b sono entrambi non nulli, sia $a^{-1} \in \gamma_1$ e $a^2 b \neq 1$.

Si verifica subito che T è allineato con i punti $P(u)$ e $P(v)$, con $u, v \in \gamma_2$ e $u \neq v$, se e solo se

$$u^2 + uv + v^2 + auv(u + v) + b = 0. \tag{3.5}$$

Allora, fatte le posizioni (3.4) con $t \in \gamma_2$, per ogni $c \in \gamma$ risulta, come si è visto, $f(c) \in \gamma_2$ e $g(c) \in \gamma_2$; inoltre si ha $f(c) = g(c')$, con $c, c' \in \gamma$, se e solo se $c = c'$ o $c + c' = 1$.

Si consideri ora in un piano affine associato ad $S_{2,q}$ di coordinate (x, y) la curva Γ di equazione

$$[f(x)]^2 + f(x) g(y) + [g(y)]^2 + af(x) g(y) [f(x) + g(y)] + b = 0,$$

e si distinguano i casi seguenti:

(1) $a \neq 0 \quad , \quad b \neq 0$;

(2) $a \neq 0 \quad , \quad b = 0$;

(3) $a = 0 \quad , \quad b \neq 0$.

Nel primo caso, come si può verificare, Γ è una curva irriducibile del sesto ordine la quale ha come unici punti multipli i punti O_1, O_2 e A (1, 1, 0). Tutti e tre questi punti sono doppi per Γ; i primi due hanno tangenti principali coniugate in una estensione quadratica di γ, mentre A ha tangenti principali distinte in γ.

Γ ha ora conseguentemente genere 7 e, detto N il numero dei suoi punti propri, per una formula di Hasse–Weil, cfr. [10], [11], risulta

$$|N + 2 - (q + 1)| \leq 14 \sqrt{q}. \tag{3.6}$$

Dalla (3.6) segue

$$(3.7) \qquad N \geq q - 14\sqrt{q} - 1$$

e quindi, per $h \geq 8$, si ha $N \geq 31$ (1).

Nel caso (2), Γ è una curva del sesto ordine irriducibile la quale ha come unici punti multipli 7 punti doppi a tangenti principali distinte, e precisamente i punti O_1 e O_2, ciascuno dei quali ha tangenti principali coniugate in una estensione quadratica di γ, il punto $A(1, 1, 0)$ a tangenti principali distinte in γ, se $a^{-1} \in \gamma_1$, e coniugate in una estensione quadratica di γ, se $a^{-1} \in \gamma_2$, ed i 4 punti aventi per coordinate, in una estensione quadratica di γ, le soluzioni del sistema $f(x) = g(y) = 0$. Allora Γ ha genere 3. Detto N il numero dei suoi punti propri e supposto $h \geq 8$, per la formula di Hasse–Weil già menzionata, risulta

$$N \geq 159, \qquad \text{se } a^{-1} \in \gamma_1,$$

$$N \geq 161, \qquad \text{se } a^{-1} \in \gamma_2.$$

Nel caso (3), Γ è una curva irriducibile del quarto ordine, priva di punti multipli, tangente alla retta $x_3 = 0$ nei due punti di coordinate $(1, r, 0)$, $(1, r+1, 0)$, con r elemento soddisfacente la (3.2) e quindi appartenente a γ, se h è pari, e ad una estensione quadratica di γ, se h è dispari.

Allora, detto N il numero dei punti propri di Γ e supposto $h \geq 8$, per la suddetta formula di Hasse–Weil si ha

$$N \geq 159, \qquad \text{se } h \text{ è pari},$$

$$N \geq 161, \qquad \text{se } h \text{ è dispari}.$$

In ciascuno dei tre casi esiste quindi un punto proprio Q di Γ di coordinate (x_0, y_0) non appartenente alle due rette aventi rispettivamente l'equazione $x + y = 0$ e $x + y + 1 = 0$.

Posto $u = f(x_0)$ e $v = g(y_0)$, risulta, come già si è osservato, $u, v \in \gamma_2$; inoltre, poiché $Q \in \Gamma$, gli elementi u e v verificano la (3.5) e, poiché Q non appartiene alle rette di equazioni $x + y = 0$ e $x + y + 1 = 0$, si ha $u \neq v$.

Si conclude che T appartiene alla secante $P(u)\,P(v)$ di K, onde resta completamente provato l'asserto.

Dalle proposizioni 2 e 3 segue subito che:

PROP. 4. – *Per* $h \geq 8$, *se* h *è pari* K *è un* $(q+4)/2$*-arco completo di* $S_{2,q}$, *se* h *è dispari, aggregando a* K *il punto* O_1, *si ottiene un* $(q+6)/2$*-arco completo di* $S_{2,q}$.

(1) Si noti che per $h = 7$ il secondo membro della (3.7) risulta negativo.

BIBLIOGRAFIA.

[1] B. SEGRE, *Ovals in a finite projective plane*, « Canadian Journal of Math. », *7*, 414–416 (1955).

[2] B. SEGRE, *Intorno alla geometria sopra un campo di caratteristica due*, « Revue Fac. Sci. Univ. Istanbul », (A) *21*, 97–123 (1956).

[3] B. SEGRE, *Sui k–archi nei piani finiti di caratteristica due*, « Revue de Math. Pures et Appl. », *2*, 289–300 (1957).

[4] B. SEGRE, *Ovali e curve σ nei piani di Galois di caratteristica due*, « Rend. Acc. Naz. Lincei », (8) *32*, 785–790 (1962).

[5] B. SEGRE, *Lectures on Modern Geometry*, Cremonese, Roma 1961.

[6] B. SEGRE, *Istituzioni di Geometria Superiore*, Ist. Mat. Univ. Roma, 1965.

[7] B. SEGRE, *Introduction to Galois geometries*, « Mem. Acc. Naz. Lincei », (8) *8*, 133–236 (1967).

[8] M. SCAFATI, *Sui 6–archi completi di un piano lineare* $S_{2,8}$, Atti Conv. Reticoli e geom. proiettive (Palermo 1957), Cremonese, Roma, pp. 128–132.

[9] M. TALLINI SCAFATI, *Archi completi di un* $S_{2,q}$, *con q pari*, « Rend. Acc. Naz. Lincei », (8) *37*, 48–51 (1964).

[10] A. WEIL, *Number of solutions of equations in finite fields*, « Bull. Amer. Math. Soc. », *55*, 497–508 (1949).

[11] A. WEIL e S. LANG, *Number of points of varieties in finite fields*, « Amer. Journal of Math. », *76*, 818–827 (1954).