Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Giampaolo Menichetti

k—archi completi in piani di Moulton d'ordine q^m

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **60** (1976), n.6, p. 775–781.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1976_8_60_6_775_0>

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

Geometria. — *k–archi completi in piani di Moulton d'ordine* q^m (*). Nota di GIAMPAOLO MENICHETTI (**), presentata (***) dal Corrisp. G. ZAPPA.

SUMMARY. — Existence of ovals, which are contained in a class of Moulton's planes of order q^m (q odd), is proved. This class of Moulton's planes is more general than the one considered for the same purpose by Korchmáros in [2].

Furthermore some examples are given of complete q^2-arcs, which are contained in certain Moulton's planes of order q^2 (q even).

1. Fissato un campo di Galois $K = GF(q)$ di ordine $q = p^h$, sia $\mathcal{K} = GF(q^m)$ la sua estensione algebrica rispetto ad un dato polinomio $P(x) \in K[x]$, di grado $m \geq 2$, irriducibile in K. Sia inoltre T il gruppo dei K–automorfismi, $\tau_i : x \mapsto x^{q^i}$, di $\mathcal{K}$ $(i = 0, 1, \cdots, m-1)$.

$\mu : K^\times \to T$ indica una funzione dal gruppo moltiplicativo $K^\times$ di K, in T, che soddisfa la condizione $\mu(1) = \tau_0$; $\mathcal{F}_\mu$ è la fibrazione di K rispetto a μ e $K_i = \mu^{-1}(\tau_i)$, $i = 0, 1, \cdots, m-1$, ne sono le fibre.

Per ipotesi dunque $1 \in K_0$, ma non è escluso che per qualche $i \in \{1, 2, \cdots, m-1\}$ sia $K_i = \varnothing$.

Osserviamo esplicitamente che, qualunque sia $t \in \mathcal{K}$, è $\prod_{0}^{m-1}{}_i\, t^{q^i} \in K$: onde l'equazione $\prod_{0}^{m-1}{}_i\, x^{q^i} = a \in K - \{0\}$ ha esattamente $1 + q + \cdots + q^{m-1}$ soluzioni in $\mathcal{K}$.

Quasicorpo di André, associato a μ, è (cfr. [1], p. 232) la struttura algebrica $A(m, q, \mu) = (\mathcal{K}^+, \circ)$, dove $\mathcal{K}^+$ è il gruppo additivo di $\mathcal{K}$ e «$\circ$» denota il prodotto definito in $\mathcal{K}^+$ ponendo

$$(1) \qquad \begin{aligned} &a \circ 0 = 0 \\ &a \circ b = a^{q^i} b \qquad \text{se} \quad \prod_{0}^{m-1}{}_j\, b^{q^j} \in K_i . \end{aligned}$$

Se $K_0 = K^\times$, cioè se μ coincide con l'applicazione costante $\mu_0 : K^\times \to \{\tau_0\}$, allora $A(m, q, \mu_0) \cong \mathcal{K}$.

Si dimostra (cfr. [1], p. 233) che per $\mu \neq \mu_0$ il quasicorpo $A(m, q, \mu)$ è sempre non distributivo ed è associativo se e solo se μ è un omomorfismo. In quest'ultima ipotesi dunque $K_0 \lhd K^\times$; pertanto se $|K^\times|/2 = (q-1)/2 < |K_0| < |K^\times| = q - 1$, allora $A(m, q, \mu)$ è sicuramente non associativo.

(*) Con «piano di Moulton» indichiamo il duale di un piano di André.

(**) Lavoro eseguito nell'ambito dell'attività del «Gruppo Nazionale per le Strutture Algebriche e Geometriche e loro Applicazioni» del C.N.R. (Sezione n. 4).

(***) Nella seduta del 10 giugno 1976.

$\mathbf{A}^*(\mathrm{A})$, $\mathrm{A} = \mathrm{A}(m, q, \mu)$, indica il piano affine del quale i punti sono le coppie $(x, y) \in \mathrm{A}\times\mathrm{A} = \mathscr{K}\times\mathscr{K}$ ed i sottoinsiemi $\{(x, y) : y = u \circ x + v\}$ e $\{(x, y) : x = c\}$ di A^2 ne costituiscono le rette. Il piano proiettivo $\mathbf{P}^*(\mathrm{A})$, ottenuto nel solito modo completando $\mathbf{A}^*(\mathrm{A})$ con l'aggiunta degli elementi impropri, è un piano di Moulton (duale di un piano di André).

$\mathbf{P}(\mathscr{K})$ e $\mathbf{A}(\mathscr{K}) \subset \mathbf{P}(\mathscr{K})$ indicano rispettivamente il piano proiettivo ed il piano affine su $\mathscr{K}$.

Come insiemi di punti $\mathbf{P}^*(\mathrm{A})$ e $\mathbf{P}(\mathscr{K})$ coincidono [1] e, quindi, un k-arco, σ, in $\mathbf{P}(\mathscr{K})$ può riguardarsi come un sottoinsieme di $\mathbf{P}^*(\mathrm{A})$; se poi, qualunque sia il punto proprio $\mathrm{P}(x, y) \in \sigma$, è $\prod_{0}^{m-1}{}_i\, x^{q^i} \in \mathrm{K}_0$, allora in virtù di (1), σ è un k-arco anche in $\mathbf{P}^*(\mathrm{A})$ (cfr. anche [2]). Dunque

PROPOSIZIONE 1. *I punti di una conica* $\gamma \in \mathbf{P}(\mathscr{K})$ *non degenere (più il nucleo, se* $p = 2$*) tale che*

$$\prod_{0}^{m-1}{}_i\, x^{q^i} \notin \mathrm{H} \subseteq \mathrm{K}^{\times} - \{1\}, \qquad \forall \mathrm{P}(x, y) \in \gamma, \tag{2}$$

costituiscono un'ovale in ogni piano $\mathbf{P}^*(\mathrm{A}(m, q, \mu(\mathrm{H})))$, *essendo* $\mu = \mu(\mathrm{H})$ *un'applicazione che soddisfa la condizione*

$$\bigcup_{1}^{m-1}{}_i\, \mathrm{K}_i \subseteq \mathrm{H}. \tag{3}$$

Nella ricerca di coniche soddisfacenti una condizione del tipo (2) è opportuno distinguere il caso in cui la caratteristica $p \neq 2$ dal caso in cui $p = 2$.

2. In questo § si suppone $p \neq 2$.

OSSERVAZIONE. Una conica γ che contiene il punto improprio (∞) non può soddisfare (2).

Infatti ogni retta $x = c$ $(c \in \mathscr{K})$, salvo al più una (tangente a γ in (∞)), incontra γ in un punto $\mathrm{P}(c, y)$ e pertanto, qualunque sia $a \in \mathrm{K} - \{0\}$, esiste qualche punto $(x, y) \in \gamma$ tale che $\prod_{0}^{m-1}{}_i\, x^{q^i} = a$.

Se come supporremo, γ non passa per (∞) possiamo scriverne l'equazione nella forma

$$g^2(x, y) + f(x) = 0, \tag{4}$$

essendo $g(x, y) = y - ux - v = 0$ l'equazione della polare, r, di (∞) rispetto a γ ed $f(x) = ax^2 + 2bx + c = 0$ l'equazione complessiva delle tangenti a γ per (∞).

(1) Nel seguito useremo le stesse notazioni sia per i punti di $\mathbf{P}(\mathscr{K})$ che per quelli di $\mathbf{P}^*(\mathrm{A})$. In particolare indicheremo con (u) tanto il punto improprio della retta $y = ux + v$ di $\mathbf{A}(\mathscr{K})$ che quello della $y = u \circ x + v$ di $\mathbf{A}^*(\mathrm{A})$; (∞) denoterà il punto improprio delle rette $x = c$ dei due piani.

Le soluzioni dell'equazione $f(x) = 0$ sono le « ascisse » dei punti comuni a γ e ad r, onde γ è degenere in due rette, distinte oppure coincidenti, a seconda che $f(x) = 0$ abbia due radici coincidenti oppure sia un'identità. Ne segue che γ è non singolare se e solo se $b^2 - ac \neq 0$.

Nel seguito di questo § ci limiteremo a supporre che $b^2 - ac$ sia un quadrato (diverso da 0) ovvero, geometricamente parlando, che r sia secante γ.

Fissato un punto $P_0(x_0, y_0) \in \gamma \cap r$, supposto cioé

$$g(x_0, y_0) = f(x_0) = 0, \tag{5}$$

sia s_t la retta, per P_0, di equazione $y - y_0 = (t + u)(x - x_0)$, $t \in \mathcal{K} \cup \{\infty\}$ (s_∞ è la retta $x - x_0 = 0$).

La s_t interseca ulteriormente γ in un punto proprio di ascissa

$$x(t) = \begin{cases} x_0, & t = \infty \\ x_0 - f'(x_0)(t^2 + a)^{-1}, & t \in \overline{\mathcal{K}}, \end{cases} \tag{6}$$

dove $f'(x_0) = 2ax_0 + 2b$ e $\overline{\mathcal{K}}$ indica l'insieme costituito dagli elementi di $\mathcal{K}$ meno le eventuali radici dell'equazione $t^2 + a = 0$ (cui corrispondono i punti impropri di γ).

Osserviamo esplicitamente che la (6) dà le ascisse di tutti i punti propri di γ.

Indichiamo con Q ed N rispettivamente l'insieme di quadrati e dei non quadrati di $K^\times$; poniamo inoltre $Q' = Q - \{1\}$.

Se $x_0 = 0$ e $a = 0$ (ciò che implica – cfr. (5) – $c = 0$, $b \neq 0$ e $y_0 = v$), allora dalla (6) deduciamo

$$\prod_0^{m-1}{}_i\, x^{q^i}(t) = \begin{cases} 0, & t = \infty \\ \prod_0^{m-1}{}_i\, (-2b)^{q^i} \Big/ \left(\prod_0^{m-1}{}_i\, t^{q^i}\right)^2, & t \in \mathcal{K} - \{0\}, \end{cases}$$

quindi

$$\prod_0^{m-1}{}_i\, x^{q^i}(t) \in Q \iff \prod_0^{m-1}{}_i\, (-2b)^{q^i} \in Q, \qquad t \in \mathcal{K} - \{0\}.$$

In altri termini una conica di equazione

$$(y - ux - v)^2 + 2bx = 0 \tag{7}$$

soddisfa la condizione (2) con $H = Q'$ oppure con $H = N$ a seconda che $\prod_0^{m-1}{}_i\, (-2b)^{q^i}$ appartenga ad N oppure a Q.

In forza della Proposizione 1 possiamo enunciare la seguente

PROPOSIZIONE 2. *In ogni piano di Moulton* $\mathbf{P}^*(\mathrm{A}(m, p^h, \mu'))$, *con* $p \neq 2$ *e* μ' *che soddisfa una delle seguenti condizioni*

$$(8)_1 \qquad \bigcup_1^{m-1}{}_i \mathrm{K}_i \subseteq \mathrm{Q}'$$

oppure

$$(8)_2 \qquad \bigcup_1^{m-1}{}_i \mathrm{K}_i \subseteq \mathrm{N}\,,$$

esistono ovali.

Osserviamo che al verificarsi di $(8)_1$ oppure di $(8)_2$ corrisponde

$$(q+1)/2 = |\mathrm{N} \cup \{1\}| \leq |\mathrm{K}_0| \leq |\mathrm{K}^\times| = q-1$$

oppure

$$(q-1)/2 = |\mathrm{Q}| \leq |\mathrm{K}_0| \leq |\mathrm{K}^\times| = q-1.$$

Ne segue, per quanto abbiamo rilevato nel § 1, che se $|\mathrm{K}_0| < q-1$, cioè se $\mathrm{A}(m, q, \mu')$ e non isomorfo a $\mathcal{K}$ (ciò che ovviamente vogliamo supporre), allora $\mathrm{A}(m, q, \mu')$ può essere associativo solo nel caso in cui valga la $(8)_2$ con l'inclusione in senso debole.

Poiché le tangenti di un'ovale di un piano d'ordine dispari costituiscono un'ovale nel rispettivo piano duale, la Prop. precedente dimostra anche l'esistenza di ovali di ogni piano di André sopra un quasicorpo $\mathrm{A}(m, p^h, \mu')$.

Dalla Proposizione 2 segue in particolare che esistono ovali in ogni piano di Moulton $\mathbf{P}^*(\mathrm{A}(m, p^h, \mu'))$ con μ' tale che

$$\mathrm{K}_i = \begin{cases} \mathrm{K}^\times - \{e\}\,, & i = 0 \\ \{e\} \quad , & i = i_0 \\ \varnothing \quad , & i \neq 0, i_0\ ;\ e \in \mathrm{K}^\times - \{1\}\,, \qquad i_0 \in \{1, 2, \cdots, m-1\}\,. \end{cases}$$

In alcuni piani di questa classe esistono, oltre quelle già viste, altre ovali costituite dai punti di una conica di $\mathbf{P}(\mathcal{K})$. A titolo di esempio dimostriamo la seguente

PROPOSIZIONE 3. *Supponiamo* $m = 2$. *Se* $f(x) = a(x - x_0)(x - dx_0)$ *ed* $a, x_0 \in \mathcal{K} - \{0\}$, $d \in \mathrm{K} - \{0, 1\}$ *sono fissati in modo che* $da^{1+q} \in \mathrm{N}$ *e* $dx_0^{1+q} \neq 1$, *allora la conica di equazione*

$$(y - ux - v)^2 + f(x) = 0$$

soddisfa la condizione (2) *con* $\mathrm{H} = \{e\}$, $e = dx_0^{1+q}$.

Dimostrazione. Da (6) si deduce

$$x(t) = \begin{cases} x_0\,, & t = \infty \\ x_0(t^2 + ad)(t^2 + a)^{-1}\,, & t \in \overline{\mathcal{K}}. \end{cases}$$

Per ipotesi $e \neq ed^{-1} = x_0^{1+q}$ e dunque la tesi risulterà provata dimostrando che

$$(t^2 + ad)^{1+q}/(t^2 + a)^{1+q} \neq d\,, \qquad \forall t \in \overline{\mathcal{K}}\,.$$

Per questo si osservi che l'equazione

$$(t^2 + ad)^{1+q} = d\,(t^2 + a)^{1+q}$$

equivale a

$$(t^{1+q})^2 = da^{1+q}$$

la quale è impossibile qualunque sia $t \in \mathcal{K}$, essendo da^{1+q} un non quadrato.

Il Teorema dimostrato da Korchmáros in [2] si ritrova di qui per $u = v = 0\,, d = -1\,, x_0 = 1\,, a = -s^{-1}$, essendo

$$s \in \begin{cases} Q\,, & q \equiv 3 \pmod 4 \\ N\,, & q \equiv 1 \pmod 4\,. \end{cases}$$

3. Supponiamo ora caratt $\mathcal{K} = 2$.

Un elemento $a \in \mathcal{K}$ si dice di prima (rispettivamente seconda) categoria se il polinomio $x^2 + x + a$ è riducibile (irriducibile) in $\mathcal{K}\,[x]$.

Detti S_1 ed S_2 rispettivamente l'insieme degli elementi di prima e di seconda categoria di $\mathcal{K}$, si dimostra (cfr. [3], p. 104) la seguente

PROPOSIZIONE 4. S_1 *è un sottomodulo di* $\mathcal{K}^+$ *di ordine* $|\mathcal{K}^+|/2$; *inoltre* $S_j + S_j \subseteq S_1\,, j = 1\,, 2$, *e* $S_1 + S_2 \subseteq S_2$.

Indichiamo con $\varphi_b : \mathcal{K} \to \mathcal{K}$ l'applicazione in cui $\varphi\,(t) = t^2 + t + b$ essendo $b \in \mathcal{K}$ prefissato.

PROPOSIZIONE 5. *Se* $b \in S_j$, *allora* $\varphi_b\,(\mathcal{K}) = S_j\,, j = 1, 2$.

Dimostrazione. L'equazione $x^2 + x + \varphi_b\,(t) = 0$, equivalente a $(x + t)^2 + (x + t) + b = 0$, è riducibile oppure irriducibile secondo che $b \in S_1$ oppure $b \in S_2$: onde $b \in S_j \Rightarrow \varphi_b\,(t) \in S_j$.

Fissato $b' \in S_j \ni b$, l'equazione (in t) $t^2 + t + b = b'$ ha sempre (due) soluzioni in $\mathcal{K}$ in virtù della Proposizione 4.

Una conica $\gamma \in \mathbf{P}\,(\mathcal{K})$ di equazione omogenea

$$\mathrm{F}\,(x_1\,, x_2\,, x_3) = \sum_{r \leq s}^{1 \cdots 3} a_{rs}\, x_r\, x_s = 0\,, \tag{9}$$

ha il nucleo in $N\,(a_{23}\,, a_{13}\,, a_{12})$, quindi non è degenere se e solo se

$$\Delta = \mathrm{F}\,(a_{23}\,, a_{13}\,, a_{12}) \neq 0 \qquad \text{(cfr. [4], p. 135).}$$

Essendo ogni retta per N una tangente a γ, oltre le coniche che contengono (∞), ora anche quelle per cui $N = (\infty)$ non possono soddisfare (2) (Cfr. l'Osservazione del § 2). Per questo motivo nel seguito supporremo che nell'equazione (9) sia $a_{22} = 1$ e a_{12}, a_{23} non entrambi nulli.

Una semplice parametrizzazione delle ascisse dei punti propri di γ, analoga alla (6), si ottiene come nel § 2 fissando $P_0 = N$.

Secondo che N sia improprio ($a_{12} = 0$) oppure proprio ($a_{12} \neq 0$) si trova

$$(10)_1 \qquad x(t) = k_1 (t^2 + t + b_1), \qquad t \in \mathscr{K}$$

essendo $k_1 = a_{23}^2/\sqrt{\Delta}$, $b_1 = a_{33}\, a_{23}^{-1}$, oppure

$$(10)_2 \qquad x(t) = \begin{cases} x_N, & t = \infty \\ x_N + k_2 (t^2 + t + b_2)^{-1}, & t \in \overline{\mathscr{K}} \end{cases}$$

dove $k_2 = \sqrt{\Delta}\, a_{12}^{-2}$, $b_2 = \sqrt{a_{11}}\, a_{12}^{-1}$, $x_N = a_{23}\, a_{12}^{-1}$ e $\overline{\mathscr{K}}$ indica l'insieme $\mathscr{K}$ privato delle eventuali radici dell'equazione $t^2 + t + b_2 = 0$.

In virtù della Proposizione 5, a $(10)_1$ e $(10)_2$ possiamo sostituire rispettivamente

$$(10)_1' \qquad x(\theta) = k_1 \theta \quad , \quad \theta \in S_j \quad , \quad b_1 \in S_j$$

$$(10)_2' \qquad x(\theta) = \begin{cases} x_N \quad , \quad \theta = \infty \\ x_N + k_2\, \theta^{-1} \quad , \quad \theta \in S_j - \{0\} \quad , \quad b_2 \in S_j . \end{cases}$$

PROPOSIZIONE 6. *Se* $m = 2^n$, *allora nessuna conica* γ *la cui equazione* (9) *ha coefficienti in* K *può soddisfare la* (2).

Dimostrazione. È sufficiente provare che qualunque sia $c \in K$, esiste $P(x, y) \in \gamma$ tale che $\prod_{0}^{m-1}{}_i\, x^{q^i} = c$.

Nelle ipotesi fatte $K \subset S_1$ (in quanto ogni equazione $x^2 + x + a = 0$, $a \in K$, è riducibile in $\mathscr{K}[x]$); dobbiamo quindi fare riferimento a $(10)_1'$ e $(10)_2'$ supponendo rispettivamente $k_1 \in K$, $\theta \in S_1$ e $k_2 \in K$, $\theta \in \{S_1 - \{0\}\} \cup \{\infty\}$. In ogni caso, qualunque sia $d \in K$ è possibile determinare $\theta \in S_1$ oppure $\theta \in \{S_1 - \{0\}\} \cup \{\infty\}$ in modo che $x(\theta) = d$.

A completamento della dimostrazione basta osservare che qualunque sia $c \in K$, $\exists\, d \in K$ tale che $\prod_{0}^{m-1}{}_i\, d^{q^i} = d^m = c$.

Tra le coniche la cui equazione (9) ha coefficienti in K, ve ne sono che contengono propriamente un k–arco il quale risulta completo in un particolare piano di Moulton. Su questo argomento dimostriamo la seguente

PROPOSIZIONE 7. *L'insieme*, Γ_0, *dei punti impropri e dei punti propri* $P(x, y)$, $x \neq e$, *appartenenti alla conica*, Γ, *di equazione*

$$s^2 x^2 + xy + y^2 + ey = 0$$

in cui $e \in K^{\times} - \{1\}$ *ed* $s \in K$ *è di seconda categoria in* K (2), *costituisce un* q^2*–arco completo nel piano di Moulton* $\mathbf{P}(A(2, 2^h, \mu))$, *essendo* μ *l'applicazione in cui*

$$K_0 = K^{\times} - \{e^2\}, \, K_1 = \{e^2\}.$$

Dimostrazione. Il nucleo di Γ è $N(e, 0)$: quindi (cfr. $(10)_2$) i punti propri $P(x, y) \in \Gamma, x \neq e$ hanno ascissa

$$x(t) = e[1 + s(t^2 + t + s)^{-1}] \quad , \quad t \in \mathscr{K} - \{t_0, t_0^q\} \quad , \quad t_0^2 + t_0 + s = 0.$$

Inoltre $\Gamma - \Gamma_0 = \{P(e, se)\}$.

Γ_0 è un q^2–arco di $\mathbf{P}(A)$ giacché (cfr. § 1)

$$x^{1+q}(t) \neq e^2, \qquad \forall t \in \mathscr{K} - \{t_0, t_0^q\},$$

in quanto

$$x^{1+q}(t) = e^2 \Longleftrightarrow (t + t^q)^2 + (t + t^q) + s = 0,$$

ciò che è impossibile, essendo per ipotesi $x^2 + x + s$ irriducibile in $K[x]$ (3).

Per dimostrare la completezza di Γ_0 è sufficiente provare che le tangenti a Γ_0 nei suoi punti $O(0, 0)$ e $Q(0, e)$ si intersecano (fuori di O e Q) in quattro punti ciascuno dei quali appartiene ad almeno una secante di Γ_0.

A tal fine conviene rilevare che N, P, O e Q, avendo coordinate in K, appartengono a $\mathbf{P}(K)$ che è un subpiano tanto di $\mathbf{P}(\mathscr{K})$ che di $\mathbf{P}(A)$. E dunque le tangenti a Γ_0 di cui sopra si intersecano oltre che in N e P, in due punti T_1 e T_2 di $\mathbf{P}(K)$ i quali sono esterni a Γ ed hanno ascissa diversa da e.

Da ciascun punto T_j escono pertanto $q/2$ secanti la conica $\Gamma \cap \mathbf{P}(K)$ e, quindi, almeno una secante Γ_0.

Le rette di equazione

$$y = t_0^2 \circ x + t_0^{2q} e \quad , \quad y = t_2^0 \circ x + e(s + t_0^{2q})$$

sono secanti Γ_0 – in (t_0^2) e $(es^2, e(t_0^2 s^2 + t_0^{2q}))$ la prima ed in (t_0^2) e $(es(s+1)^{-1}, et_0^{4q}(s+1)^{-1})$ la seconda – e contengono rispettivamente $N(e, 0)$ e $P(e, se)$.

BIBLIOGRAFIA

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

[2] G. KORCHMÁROS (1973) – *Ovali nei piani finiti di Moulton*, Atti del Colloquio Internazionale sulle Teorie Combinatorie, Roma (In corso di stampa).

[3] B. SEGRE (1961) – *Lectures on modern geometry*, With an appendix by L. Lombardo-Radice, Roma, Cremonese.

[4] B. SEGRE (1965) – *Istituzioni di Geometria superiore*, vol. II, Roma, Ed. Istituto Matem. « G. Castelnuovo ».

(2) Supponiamo $q = 2^h \neq 2$ ed $s \neq 1$.

(3) Qualunque sia $t \in \mathscr{K}$, è $t + t^q \in K$.