Note di Matematica Vol. I, 127-136 (1981)

(q^2+q+1)-INSIEMI DI TIPO $(0,1,2,q+1)$ E OVALI NEL PIANO DI HALL DI ORDINE PARI q^2 (°).

Michele CRISMALE (°°)

Summary. *Ovals and* $(q^2 + q + 1)$*-sets of type* $(0,1,2,q+1)$ *are constructed in the Hall plane of order* q^2, *for every* $q=2^h$, $h = 1,2,\dots$.

Scopo della presente Nota è di dare degli esempi - i primi a nostra conoscenza - di $(q^2 + q + 1)$-*insiemi* di *tipo* $(0,1,2,q+1)$ (v.n.1) in un piano proiettivo di ordine q^2 e di *ovali* in un piano di Hall di ordine pari. Più precisamente si costruiscono, in ogni piano di Hall di ordine pari, q^2, due classi, una di ovali, l'altra di insiemi del tipo suindicato.

Si osservi che si sanno costruire ovali in ogni piano di Hall di ordine dispari [6], nonché q^2-archi completi nel piano di Hall di ordine pari q^2, per ogni $q \neq 2$ [11] . Sono noti inoltre svariati esempi di ovali in piani finiti non desarguesiani [5] [6] [7] [8] [9] [10] [13] [14] [15] [20] .

Nei piani di Galois la conoscenza delle ovali è molto più avanzata (cfr.

(°) Lavoro eseguito nell'ambito del G.N.S.A.G.A. del C.N.R..

(°°) Istituto di Geometria - Università di Bari.

[3] , cap. 8 e relativa bibliografia) e del tutto completa in quelli di ordine dispari, nei quali le ovali coincidono con le coniche non degeneri [16] . Per contro l'esistenza di (q^2+q+1)-insiemi di tipo (0,1,2,q+1) in un piano di Galois di ordine q^2 è un problema aperto se $q \neq 2$; se $q = 2$ essa è assicurata dalla costruzione suindicata e dal fatto che il piano di Hall di ordine 4 è desarguesiano (non lo è se $q \neq 2$, v.nota (1)).

1. Sia π un piano proiettivo finito di ordine q e $K \subset \pi$ un k-*insieme* di π, cioé $|K| = k$. Denotato con t_s $(s=0,1,\dots,q+1)$ il numero delle s-secanti di K, cioè delle rette che incontrano K esattamente in s punti, ricordiamo che per i numeri t_s, che diconsi *caratteri* del k-insieme, valgono le relazioni seguenti [18] [19]:

$$\sum_{s=0}^{q+1} t_s = q^2 + q + 1 \tag{1}$$

$$\sum_{s=1}^{q+1} st_s = k(q+1) \tag{2}$$

$$\sum_{s=2}^{q+1} s(s-1)t_s = k(k-1) \tag{3}$$

K si dice *a* ℓ *caratteri* se, posto $L = \{ s : t_s \neq 0 \}$ si ha $|L| = \ell$, piu precisamente, se $L = \{ m_1, m_2, \dots, m_\ell \}$ ed è $m_1 < m_2 < \dots < m_\ell$, K si dice di *tipo* $(m_1, m_2, \dots, m_\ell)$. Ad esempio, se q è pari, un'*ovale* di π altro non è che un (q+2)-insieme di tipo (0,2) con $t_0 = q(q-1)/2$, $t_2 = (q+2)(q+1)/2$. Questa definizione è equivalente a quella di ovale come (q+2)-*arco*, dicendosi k-arco di π ogni insieme di k punti di π tre a tre non allineati. Ogni ovale di π - sempre se q è pari - si può ottenere da un (q+1)-arco di π con l'aggiunta del *nucleo* (punto d'intersezione delle unisecanti il (q+1)-arco).

Sia ora q qualsiasi (pari o dispari). Ricordiamo (cfr. [1], [12], [2], 10, p.224 e 14, p.234, [4], cap. X) che il *piano affine* di *Hall*, di ordine q^2, si può definire assumendo come *punti* quelli di $AG(2,q^2)$ (piano affine sul campo di Galois $GF(q^2)$ di q^2 elementi) e come *rette*:

i) le rette di $AG(2,q^2)$ aventi equazione del tipo

$$y = mx + n \qquad n\in GF(q^2),\ m\in GF(q^2)\setminus GF(q)$$

ii) i subpiani (di Baer) di $AG(2,q^2)$:

$$R(a,b,c) = \{(a\xi+ b,a\eta+c) \mid \xi,\eta \in GF(q)\} \quad a,b,c\in GF(q^2),\ a \neq 0$$

Si osservi ([4],p.212, ex 10.5) che $R(a,b,c)$ è parallela a $R(a',b',c')$ se e solo se $a' = \alpha a$, con $\alpha \in GF(q)$.

Indicheremo con $H(2,q^2)$ il *piano proiettivo* di *Hall* (1) che si ottiene da quello affine con l'usuale procedimento di ampliamento; diremo *rette* - di *prima (seconda) categoria* le rette - affini o proiettive - del tipo i),ii) rispettivamente; *punto all'infinito* di *prima (seconda) categoria* invece di punto all'infinito di una retta di prima (seconda) categoria.

Ricordiamo infine il seguente risultato, [17] § 79; con il simbolo (n,n') si indica, come di consueto, il massimo comun divisore di due numeri interi n,n'.

(1) Si osservi (v. ad es. [2] pp. 233-4 oppure [4], Teor. 10.9,p.205 che $H(2,q^2)$ è desarguesiano se e solo se $q=2$.

LEMMA 1. *Se* $(m,q-1) = 1$, *ogni elemento di* $GF(q)$ *ha una ed una sola radice* m-ima.

2. D'ora in avanti supporremo $q = 2^h$, $h = 1,2,\dots$, e indicheremo con g un intero positivo tale che $(g,2h)=1$; porremo inoltre $2^g=r$. Per una proprietà di teoria dei numeri (v.ad es. [17] , p.287) si ha $(r-1,q^2-1) = 1$, quindi, in base al lemma 1, si ha:

LEMMA 2. *Ogni elemento di* $GF(q^2)$ *ha una ed una sola radice* (r-1)-ima.

Sia ora $m \in GF(q^2)$, denotiamo con $\Gamma = \Gamma(g,m)$ l'insieme dei punti di $AG(2,q^2)$ della curva algebrica di equazione, in coordinate non omogenee di punti (x,y),

$$y = x^r + mx.$$

Siano Y_∞ , $M_\infty \in PG(2,q^2)$ (piano proiettivo sul campo di Galois $GF(q^2)$) rispettivamente i punti all'infinito dell'asse y e della retta di equazione $y= mx$. Poniamo $\Theta = \Theta(g,m) = \Gamma \cup \{M_\infty\}$, $\Delta = \Delta(g,m) = \Theta \cup \{Y_\infty\}$ e osserviamo il seguente

LEMMA 3. $\Theta(g,m)$ *è un* (q^2+1)*-arco,* $\Delta(g,m)$ *un'ovale di* $PG(2,q^2)$.

Dimostrazione. E' ben noto, [17] § 178, che $\Delta(g,0)$ è un'ovale di $PG(2,q^2)$, quindi $\Gamma(g,m)$ è un q^2-arco di $PG(2,q^2)$ dato che, se $x_1,x_2,x_3 \in GF(q^2)$,

$$\begin{vmatrix} x_1 & x_1^r + mx_1 & 1 \\ x_2 & x_2^r + mx_2 & 1 \\ x_3 & x_3^r + mx_3 & 1 \end{vmatrix} = \begin{vmatrix} x_1 & x_1^r & 1 \\ x_2 & x_2^r & 1 \\ x_3 & x_3^r & 1 \end{vmatrix}$$

Inoltre ogni retta di equazione

$$y = mx + n \quad , \qquad n \in GF(q^2)$$

interseca $\Gamma(g,m)$ in un solo punto, essendo notoriamente, [17] § 78, $x \longmapsto x^r$ un automorfismo di $GF(q^2)$. Ciò prova che $\Theta(g,m)$ è un (q^2+1)-arco di $PG(2,q^2)$. Il suo nucleo è ovviamente Y_∞ .

Si può ora provare la

PROPOSIZIONE 1. *Se* $m \in GF(q)$, *aggregando a* $\Gamma(g,m)$ *i* $q+1$ *punti all'infinito di seconda categoria, si ottiene un* (q^2+q+1)*-insieme* $K=K(g,m)$ *di* $H(2,q^2)$ *di tipo* $(0,1,2,q+1)$ *e caratteri*

(4) $$t_0 = q^3(q-1)/2$$

(5) $$t_1 = q(q-1), \; t_2 = q^3(q+1)/2, \; t_{q+1} = q+1.$$

Dimostrazione. Se w è una retta di $H(2,q^2)$ e W_∞ il suo punto all'infinito, si ha evidentemente $w \cap K = w \cap \Gamma$ oppure $w \cap K = \{W_\infty\} \cup (w \cap \Gamma)$ secondo che w sia di prima o di seconda categoria. Per ciascuno dei q^2-q punti all'infinito di prima categoria passano $q^2/2$ rette (di prima categoria) bisecanti $\Gamma(g,m)$ e quindi $q^2/2$ rette (di prima categoria) 0-secanti

$\bar{\Gamma}(g,m)$; ne segue la (4). Sia ora w di seconda categoria, $w = R(a,b,c)$ e $P,P' \in w \cap \Gamma$. Se le coordinate non omogenee di P,P' sono $(a\xi + b, a\eta + c)$, $(a\xi' + b, a\eta' + c)$, con $\xi, \eta, \xi', \eta' \in GF(q)$, $(\xi, \eta) \neq (\xi', \eta')$, dev'essere

$$(6) \qquad \begin{aligned} \eta &= a^{r-1}\xi^r + m\xi + (b^r + mb + c)a^{-1} \\ \eta' &= a^{r-1}\xi'^r + m\xi' + (b^r + mb + c)a^{-1}. \end{aligned}$$

Sommando si ha

$$\eta + \eta' = a^{r-1}(\xi^r + \xi'^r) + m(\xi + \xi').$$

Non potendo essere $\xi = \xi'$, altrimenti $\eta = \eta'$, contro l'ipotesi, dev'essere $a^{r-1} \in GF(q)$, cioè $a \in GF(q)$ per il lemma 2, quindi, in forza della (6), $b^r + mb + c \in GF(q)$. Dunque o w è $(q+1)$-secante K, e ciò accade se e solo se $a \in GF(q)$ e $b^r + mb + c \in GF(q)$, oppure $1 \leq |w \cap K| \leq 2$. Si osservi che esistono, oltre la retta impropria, $(q+1)$-secanti di seconda categoria (basta assumere $a,b,c \in GF(q)$), nonché unisecanti di seconda categoria (basta assumere $a \in GF(q)$, $b^r + mb + c \notin GF(q)$. Da quanto detto segue che K è di tipo $(0,1,2,q+1)$. Scrivendo (1),(2),(3) nel nostro caso e sostituendo nella prima equazione t_0 dato da (4), si ricavano le (5).

Si osservi che dalla dimostrazione svolta si ha la seguente

PROPOSIZIONE 2. *Se* $m \in GF(q)$, $\Gamma(g,m)$ *è un* q^2*-insieme di tipo* $(0,1,2,q)$ *del piano affine di Hall, di caratteri*

$$t'_0 = t_0 + t_1, \quad t'_1 = t_2 - q^2/2, \quad t'_2 = q^2/2, \quad t'_q = q.$$

$(t_0, t_1, t_2$ come in (4) e (5)).

Si prova ora che:

PROPOSIZIONE 3. *Se* $m \notin GF(q)$, $\Theta(g,m)$ *è un* (q^2+1)*-arco di* $H(2,q^2)$.

Dimostrazione. Essendo M_∞ punto all'infinito di prima categoria per l'ipotesi $m \notin GF(q)$ - tutto si riduce a provare che una retta di seconda categoria $R(a,b,c)$ interseca $\Gamma(g,m)$ al più in due punti. Sia

$$(7) \qquad |R(a,b,c) \cap \Gamma(g,m)| \geq 3$$

cioè esistano $\xi_i, \eta_i \in GF(q)(i=1,2,3)$ tali che

$$a\eta_i + c = (a\xi_i + b)^r + m(a\xi_i + b)$$

ovvero

$$\xi_i^r a^{r-1} + \xi_i m + (b^r + mb + c)a^{-1} = \eta_i \qquad (i=1,2,3)$$

Si ha allora - tenendo conto del fatto che q è pari e che $r = 2^g$-

$$D = \begin{vmatrix} \xi_1^r & \xi_1 & 1 \\ \xi_2^r & \xi_2 & 1 \\ \xi_3^r & \xi_3 & 1 \end{vmatrix} = \begin{vmatrix} (\xi_1 - \xi_2)^r & \xi_1 - \xi_2 \\ (\xi_2 - \xi_3)^r & \xi_2 - \xi_3 \end{vmatrix}$$

$D = 0$ implica $\xi_1 = \xi_2$ oppure $\xi_2 = \xi_3$ oppure $(\xi_1 - \xi_2)^{r-1} = (\xi_2 - \xi_3)^{r-1}$ cioè - per il lemma 2 - $\xi_1 - \xi_2 = \xi_2 - \xi_3$ ovvero $\xi_1 = \xi_3$. Si conclude, per la (7), che è $D \neq 0$. Ne segue $m \in GF(q)$ (per il teorema di CRAMER), contro l'ipotesi.

Si indichi ora con U_∞ il punto all'infinito della retta $R(1,0,0)$ e si ponga $\Omega = \Omega(g,m) = \Theta(g,m) \cup \{U_\infty\}$.

PROPOSIZIONE 4. *Se* $m \notin GF(q)$, $\Omega(g,m)$ *è un'ovale di* $H(2, q^2)$.

Dimostrazione. Basta provare che U_∞ è il nucleo di $\Theta(g,m)$. Sia $R(a,b,c) \in U_\infty$, cioé $0 \neq a \in GF(q)$, $b,c \in GF(q^2)$; si ha

$$|R(a,b,c) \cap \Gamma(g,m)| \leq 1$$

poiché da

$$a\eta + c = (a\xi + b)^r + m(a\xi + b)$$

$$a\eta' + c = (a\xi' + b)^r + m(a\xi' + b)$$

segue

$$a(\eta + \eta') = a^r(\xi + \xi')^r + ma(\xi + \xi').$$

L'ipotesi $\xi + \xi' = 0$ implica $\eta + \eta' = 0$; l'ipotesi $\xi + \xi' \neq 0$ implica $m \in GF(q)$.

BIBLIOGRAFIA

[1] A.A.ALBERT, *The finite planes of Ostrom*, Bol.Soc.Mat.Mexicana, (2), 11 (1966), 1-13.

[2] P.DEMBOWSKI, *Finite Geometries*, Spinger Verlag, Berlin-Heidelberg - New York 1968.

[3] J.W.P.HIRSCHFELD, *Projective geometries over finite fields*, Oxford University Press. Oxford 1979.

[4] D.R.HUGHES - F.C.PIPER, *Projective Planes*, Springer Verlag, New York Heidelberg Berlin 1973.

[5] W.KANTOR, *Symplectic Groups, Symmetric Designs and Line Ovals*- J.Algebra, 33 (1975), 43-58.

[6] G.KORCHMÁROS, *Ovali nei piani di Hall di ordine dispari*, Rend.Accad. Naz.Lincei, 56 (1974), 315-317.

[7] G.KORCHMÁROS, *Ovali nei piani finiti di Moulton*, Convegno Internazionale sulle Teorie Combinatorie, Accad.Naz.Lincei,Roma 1976 Tomo II, 395-398.

[8] G.KORCHMÁROS, *Le ovali di linea del piano di Luneburg d'ordine* 2^{2r} *che possono venir mutate in sé da un gruppo di collineazioni isomorfo al gruppo semplice* Sz (2^r) *di Suzuki*, Mem. Accad.Naz.Lincei, (8) 15 (1979), 295-315.

[9] H.LUNEBURG, *Uber projektive Ebenen, in denen jede Fahne von einer nichttrivialen Elation invariant gelassen wird*, Abh. Hamburg, 29 (1965), 37--76.

[10] H.LUNEBURG, *Die Suzukigruppen und ihre Geometrien*, Lect. Notes in Math., 10 (1965).

[11] G.MENICHETTI, *q-archi completi nei piani di Hall di ordine* $q=2^k$, Rend.Accad.Naz.Lincei, (8) 56 (1974), 518-525.

[12] T.G.OSTROM, *Semi-translation planes*, Trans.Amer.Math.Soc. 111 (1964), 1-18.

[13] G.RODRIGUEZ, *Un esempio di ovale che non è una quasi-conica*- Boll.U.M.I. (3), 14 (1959), 500-503.

[14] T.G.ROOM, *Polarities and ovals in the Hughes plane* , J. Austral. Math.Soc., 13 (1972), 196-204.

[15] L.A.ROSATI, *Insiemi di sostituzioni strettamente 3-transitivi e ovali* Boll.U.M.I. (4) 4 (1969), 463-467.

[16] B.SEGRE, *Ovals in a finite projective plane*, Canad. J.Math., 7 (1955) 414-416.

[17] B.SEGRE, *Lectures on modern geometry*, Cremonese, Roma 1961.

[18] G.TALLINI, *Problemi e risultati sulle geometrie di Galois*, Relazione n.30, Ist.Matem.Università di Napoli, 1974.

[19] M.TALLINI SCAFATI, *Sui* $\{k,n\}$ *-archi di un piano grafico finito*, Rend.Accad.Naz.Lincei, (8) 40 (1966), 1-6.

[20] A.WAGNER, *On perspectivities of finite projective planes*, Math. Zeit., 71 (1959), 113-123.

Lavoro pervenuto alla Redazione il 16 Marzo 1981
ed accettato per la pubblicazione l'8 Aprile 1981
su parere favorevole di U.Bartocci e A.Cossu