Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Claudio Di Comite

Calotte complete di un $S_{3,q}$, con q pari

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **46** (1969), n.4, p. 385–389.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1969_8_46_4_385_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1969.

Geometrie finite. — *Calotte complete di un* $S_{3,q}$, *con* q *pari* (*). Nota di CLAUDIO DI COMITE, presentata (**) dal Socio B. SEGRE.

RIASSUNTO. — In a Galois space $S_{3,q}$, with $q = 2^h$, h odd > 3, complete $[(q^2+q+4)/2]$-caps are constructed.

1. In uno spazio di Galois $S_{3,q}$ (cioè in uno spazio proiettivo a tre dimensioni sopra un campo di Galois γ_q) si chiama, com'è noto, [6], k-calotta o calotta d'ordine k un insieme di k punti a tre a tre non allineati. Una k-calotta si dice completa, [6], se non è contenuta in una $(k+1)$-calotta. Se è $q \neq 2$, l'ordine massimo di una calotta è q^2+1, [3], [6] (l'ordine massimo di una calotta di $S_{3,2}$ è 8); una calotta d'ordine massimo si chiama ovaloide. Se q è dispari, tutti e soli gli ovaloidi di $S_{3,q}$ sono le quadriche ellittiche, [1], [3], [6]. Se è q pari, $q \neq 2$, ogni quadrica ellittica è un ovaloide, ma esistono ovaloidi che non sono quadriche ellittiche, [3], [4].

B. Segre ha provato in [3] il seguente teorema:

Dato un qualunque q *(pari o dispari, della forma* $q = p^h$ *con* p *primo), si puo determinare (almeno) un* k *soddisfacente alle limitazioni*

$$(q^2+q+4)/2 \leq k \leq (q^2+3q+6)/2, \tag{1.1}$$

in guisa che in $S_{3,q}$ *esista qualche* k*-calotta completa, la quale non risulti un ovaloide.*

In particolare, se $q \equiv 3 \pmod{4}$, *ciò che precede ha luogo addirittura per* k *uguale al primo membro delle suddette limitazioni. Se invece* q *è dispari* $\neq 3$ *ed inoltre* $q \not\equiv 1 \pmod{3}$, *quanto sopra – oltre che eventualmente per* k *uguale a quel primo membro – ha sempre luogo per almeno un valore di* k *maggiore di esso e soddisfacente alle limitazioni indicate.*

In questo lavoro, sfruttando un risultato di M. Tallini Scafati, [8], sugli archi completi di $S_{2,q}$, con $q = 2^h$ ed h dispari, si dimostra che anche per $q = 2^h$, h dispari ed $h > 3$, esistono $(q^2+q+4)/2$-calotte complete di $S_{3,q}$, cioè esistono k-calotte complete con k uguale al primo membro delle limitazioni (1.1).

2. In uno spazio di Galois $S_{3,q}$, con $q = 2^h$, h dispari ed $h > 3$, si consideri la quadrica Q rappresentata, in un sistema di coordinate omogenee (x_1, x_2, x_3, x_4), dall'equazione

$$x_1^2 + x_1 x_3 + x_3^2 + x_1 x_4 + x_2 x_4 = 0.$$

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

(**) Nella seduta del 19 aprile 1969.

Il piano tangente in $O_2(0, 1, 0, 0)$ a Q interseca Q nella conica di equazioni

$$x_1^2 + x_1 x_3 + x_3^2 = 0 \quad , \quad x_4 = 0,$$

la quale, poiché h è dispari e quindi 1 è un elemento di seconda categoria, [6], si compone di due rette coniugate in una estensione quadratica di γ_q. Ne consegue che Q è una quadrica ellittica e quindi un ovaloide, [3].

Per ogni $a \in \gamma_q - \{1\}$, sia C_a la sezione di Q con il piano π_a di equazione $x_3 = a x_4$ e sia Ω_a la collineazione in $S_{3,q}$ rappresentata dalle equazioni

$$x'_1 = (a+1)\,x_1 \quad , \quad x'_2 = x_2 + a^2 x_4 \quad , \quad x'_3 = (a^2+1)\,x_3 \quad , \quad x'_4 = (a^2+1)\,x_4 .$$

Si verifica facilmente che Ω_a trasforma C_a nella conica C'_a di equazioni

$$x_1^2 + x_1 x_4 + x_2 x_4 = 0 \quad , \quad x_3 = a x_4 .$$

Si indichi con K'_a l'insieme costituito dai $q/2$ punti di C'_a di coordinate $(b, b^2+b, a, 1)$, con b elemento di prima categoria, e dai due punti $O_1(1, 0, 0, 0)$ e $O_2(0, 1, 0, 0)$.

Per [8], K'_a è un $(q+4)/2$–arco completo del piano π_a. Allora anche $\overset{-1}{\Omega}_a(K'_a) = K_a$ è un $(q+4)/2$–arco completo di $\overset{-1}{\Omega}_a(\pi_a) = \pi_a$. Gli elementi di K_a sono i $q/2$ punti di C_a di coordinate

$$(b\,(a+1)\,,\,(b^2+b)\,(a^2+1) + a^2,\, a\,,\, 1), \tag{2.1}$$

con b elemento di prima categoria, il punto $O_1\,(\notin C_a)$ ed il punto $O_2\,(\in C_a)$.

Si consideri ora la conica C_1 sezione di Q con il piano π_1 di equazione $x_3 = x_4$.

C_1, come si verifica facilmente, è una conica non degenere passante per O_2 ed avente per nucleo il punto O_1, quindi, [2], [6], l'insieme K_1 costituito dai punti di C_1 e dal punto O_1 e un $(q+2)$–arco completo (ovale) del piano π_1.

Posto $K = \bigcup_{a \in \gamma_q} K_a$, si proverà che:

PROP. 1. – *L'insieme* K *è una* $(q^2+q+4)/2$*–calotta di* $S_{3,q}$.

Poiché l'intersezione di due qualunque archi K_a, $K_{a'}$ (a e a' appartenenti a γ_q, $a \neq a'$) è costituita dai due soli punti O_1 ed O_2, si ha subito che il numero di punti di K è $(q^2+q+4)/2$.

Inoltre, l'insieme $H = K - \{O_1\}$, essendo contenuto in Q, è una calotta e ogni retta per O_1 o appartiene ad uno dei piani π_a ($a \in \gamma_q$), e quindi contiene al più un punto di H (un punto di K_a diverso da O_1), o appartiene al piano $x_4 = 0$, ed anche in questo caso contiene al più un punto di H (il punto O_2 che è l'unico punto di H sul piano $x_4 = 0$). Si conclude che O_1 ha indice zero rispetto ad H, [3], e quindi K è una calotta.

3. Si proverà che:

PROP. 2. – *La calotta* K *è completa.*

Sia P un qualunque punto di $S_{3,q}$ non appartenente a K. Se P appartiene ad uno dei piani π_a $(a \in \gamma_q)$, poiché K_a è un arco completo di π_a, per P passa una secante di K_a e quindi di K. Se P non appartiene a nessuno dei piani π_a, allora P è un punto del piano $x_4 = 0$ non appartenente alla retta $O_1 O_2$. Per poter concludere che K è completa basta allora dimostrare che anche in questo caso per P passa una secante di K.

A tal fine si indichino con $(m, n, 1, 0)$ le coordinate di P. Si consideri il piano π_P polare di P rispetto a Q, esso ha equazione

$$x_1 + mx_3 + (m + n)\, x_4 = 0. \tag{3.1}$$

Il piano π_P sega Q in una conica non degenere C_P che contiene O_2 ed un punto T di C_1 distinto da O_2 (il punto di coordinate $(n+1, n^2, 1, 1)$).

Sostituendo le coordinate (2.1) in (3.1), si ha

$$a\,(b + m) + b + m + n = 0. \tag{3.2}$$

Si distinguono i seguenti casi:

1) $n \neq 0$, m di seconda categoria,
2) $n \neq 0$, m di prima categoria,
3) $n = 0$, m di seconda categoria,
4) $n = 0$, m di prima categoria.

Nel primo caso, per ogni elemento b di prima categoria risulta $b + m \neq 0$, quindi per ogni b di prima categoria esiste un unico elemento $a \in \gamma_q$ che verifica la (3.2), inoltre, essendo $n \neq 0$, risulta $a \neq 1$. In questo caso quindi C_P contiene, oltre ai due punti O_2 e T di K, esattamente altri $q/2$ punti di K.

Nel secondo caso, per ogni b di prima categoria distinto da m esiste un unico a appartenente a γ_q e distinto da 1 che verifica la (3.2), mentre per $b = m$ non esiste alcun $a \in \gamma_q$ che verifica la (3.2). Quindi in questo caso, oltre ai due punti O_2 e T di K, C_P contiene esattamente altri $(q - 2)/2$ punti di K.

Nel terzo caso, per ogni b di prima categoria risulta $b + m \neq 0$, quindi per ogni b di prima categoria l'unico valore di a che verifica la (3.2) è $a = 1$. In questo caso quindi C_P non contiene alcun punto di K distinto da O_2 e T.

Nel quarto caso infine, la (3.2) è verificata per $b = m$ ed a arbitrario, quindi C_P contiene oltre ai due punti O_2 e T, i $q - 1$ punti di K aventi coordinate (2.1) con $b = m$ ed $a \in \gamma_q - \{1\}$, conseguentemente risulta $C_P \subset K$.

Nei primi tre casi si supponga per assurdo che P abbia indice zero rispetto a K, allora le rette che da P proiettano i punti di K distinti da O_1 sono in numero di $(q^2 + q + 2)/2$ e ciascuna di esse o è tangente a Q o è secante di Q. Poiché nei primi tre casi C_P contiene al più $(q + 4)/2$ punti di K, al più $(q + 4)/2$ di dette rette sono tangenti a Q, quindi almeno $(q^2 - 2)/2$ di esse sono secanti di Q, il che è assurdo essendo $q > 2$ ed essendo $(q^2 - q)/2$ il numero delle secanti di Q passanti per un qualunque punto non appartenente a Q, [3]. Si conclude che P non ha indice zero rispetto a K.

Nel quarto caso, essendo $C_P \subset K$, non può farsi una dimostrazione analoga a quella relativa ai primi tre casi. Si considerino allora due punti di K di coordinate rispettivamente

$$(b_1(a_1+1)\,,\,(b_1^2+b_1)(a_1^2+1)+a_1^2\,,\,a_1\,,\,1),$$
$$(b_2(a_2+1)\,,\,(b_2^2+b_2)(a_2^2+1)+a_2^2\,,\,a_2\,,\,1),$$

con a_1 ed a_2 elementi di γ_q distinti tra loro e diversi da 1, e b_1, b_2 elementi di prima categoria.

Detti punti sono allineati con $P(m, 0, 1, 0)$ se e solamente se sono soddisfatte le relazioni

$$(3.3)\qquad \begin{aligned} &b_1(a_1+1)+b_2(a_2+1)+(a_1+a_2)\,m=0,\\ &b_1(a_1^2+1)+b_2(a_2^2+1)+(a_1^2+a_2^2)(m^2+1)=0. \end{aligned}$$

Si ponga $a_1+1=c_1\,,\,a_2+1=c_2\,,\,\sqrt{b_1}=d_1\,,\,\sqrt{b_2}=d_2$; allora c_1 e c_2 sono due elementi non nulli distinti e d_1 e d_2 sono due elementi di prima categoria, [6].

Con le suddette posizioni le (3.3) si scrivono secondo le

$$c_1 d_1^2+c_2 d_2^2+(c_1+c_2)\,m=0 \quad , \quad (c_1 d_1+c_2 d_2+(c_1+c_2)(m+1))^2=0,$$

dalle quali conseguono le relazioni

$$(3.4)\qquad \begin{aligned} &c_1(d_1^2+m)+c_2(d_2^2+m)=0,\\ &c_1(d_1+m+1)+c_2(d_2+m+1)=0. \end{aligned}$$

Allora, per provare che per P passa una secante di K, è sufficiente far vedere che esistono due elementi c_1 e c_2 di γ_q non nulli e distinti, e due elementi d_1 e d_2 di prima categoria, tali che sussistano le (3.4).

Si supponga per ora di aver provato (il che si farà in seguito) che esistono due elementi di prima categoria d_1 e d_2 distinti e diversi da $\sqrt{m}$ tali che

$$(3.5)\qquad \begin{vmatrix} d_1^2+m & d_2^2+m \\ d_1+m+1 & d_2+m+1 \end{vmatrix}=0;$$

allora, assumendo $c_1=d_2^2+m\,,\,c_2=d_1^2+m$, si ottengono quattro elementi d_1, d_2, c_1, c_2 che soddisfano alle condizioni richieste. Resta così provato, anche nel quarto caso, che per P passa una secante di K e si conclude quindi che la calotta K è completa.

Si proverà ora che esistono due elementi di prima categoria d_1 e d_2 distinti e diversi da $\sqrt{m}$ tali che sussista la (3.5).

Poiché la (3.5) si può scrivere secondo la

$$(d_1+d_2)(d_1 d_2+(m+1)(d_1+d_2)+m)=0,$$

è sufficiente provare che esistono due elementi di prima categoria d_1 e d_2 distinti e diversi da $\sqrt{m}$ tali che

$$d_1 d_2 + (m+1)(d_1+d_2) + m = 0. \tag{3.6}$$

A tal fine si consideri la quartica F di $S_{2,q}$ ($q = 2^h$, h dispari, $h > 3$) rappresentata, in un sistema di coordinate omogenee (x_1, x_2, x_3), dall'equazione

$$(x_1 x_3 + x_1^2)(x_2 x_3 + x_2^2) + (m+1)(x_1 x_3^3 + x_1^2 x_3^2 + x_2 x_3^3 + x_2^2 x_3^2) + m x_3^4 = 0.$$

Come si verifica facilmente, F è irriducibile ed ammette come unici punti multipli i punti $O_1(1, 0, 0)$ ed $O_2(0, 1, 0)$, ciascuno dei quali è doppio a tangenti principali coniugate in una estensione quadratica di γ_q. La F è dunque ellittica e, detto N il numero dei suoi punti semplici (nessuno dei quali appartiene alla retta $O_1 O_2$), per una formula di Hasse-Weil, [9], [10], si ha

$$(\sqrt{q} - 1)^2 \leq N \leq (\sqrt{q} + 1)^2.$$

Essendo $q \geq 2^5$, risulta $N > 21$. Esiste allora un punto appartenente ad F ed avente coordinate $(u, v, 1)$ tali che

$$u^2 + u \neq \sqrt{m} \quad , \quad v^2 + v \neq \sqrt{m}.$$

Posto $d_1 = u^2 + u$, $d_2 = v^2 + v$, si ha subito che d_1 e d_2 sono due elementi di prima categoria diversi da $\sqrt{m}$ che verificano la (3.6). Risulta inoltre $d_1 \neq d_2$ perché in caso contrario si avrebbe $d_1 = d_2 = \sqrt{m}$.

Resta così completamente provata la prop. 2.

BIBLIOGRAFIA.

[1] A. BARLOTTI, *Un'estensione del teorema di Segre-Kustaanheimo*, « Boll. U.M.I. », (3) *10* (1955).

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

[3] B. SEGRE, *Le geometrie di Galois*, « Annali di Mat. », (4) *48* (1959).

[4] B. SEGRE, *On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two*, « Acta Arithmetica », *5* (1959).

[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. TALLINI SCAFATI, *Archi completi in un* S_2, *q*, *con q pari*, « Rend. Acc. Naz. Lincei », (8) *37* (1964).

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

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