Atti Accademia Nazionale Lincei Classe Scienze Fisiche Matematiche Naturali

Rendiconti Lincei Matematica e Applicazioni

Giorgio Faina

Il Teorema di Hasse-Weil e la costruzione di archi completi di cardinalità piccola in piani di Galois di ordine dispari

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Serie 9, Vol. **5** (1994), n.1, p. 69–77.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLIN_1994_9_5_1_69_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Accademia Nazionale dei Lincei, 1994.

Rend. Mat. Acc. Lincei
s. 9, v. 5:69-77 (1994)

Geometrie finite. — *Il Teorema di Hasse-Weil e la costruzione di archi completi di cardinalità* piccola *in piani di Galois di ordine dispari.* Nota di GIORGIO FAINA, presentata (*) dal Socio G. Zappa.

ABSTRACT. — *Hasse-Weil Theorem and construction of complete arcs of* little *cardinality in Galois planes of odd order.* In this *Note* we construct a family F of complete k-arcs in $PG(2,q)$ such that $(11/24)(q+1)+3 \leq |K| \leq (q+1)/2+2$, for every $K \in F$. The Proof of the completeness depends on the classical Hasse-Weil Theorem concerning the number of points of an irreducible algebraic curve in $PG(2,q)$.

KEY WORDS: Projective planes; Complete k-arcs; Ovals.

RIASSUNTO. — In questa *Nota* costruiamo una famiglia F di k-archi completi di $PG(2,q)$ tale che $(11/24)(q+1)+3 \leq |K| \leq (q+1)/2+2$, per ogni $K \in F$. La dimostrazione della completezza si basa sul classico Teorema di Hasse-Weil riguardante il numero dei punti di una curva algebrica irriducibile di $PG(2,q)$.

1. Un k-arco in un piano proiettivo di ordine q, è notoriamente un insieme di k punti a tre a tre non allineati. Un punto $P \notin K$ del piano si dice *aggregabile* al k-arco se $K \cup \{P\}$ è ancora un arco, ossia se nessuna secante a K passa per P. Un k-arco è detto *completo* se non ammette punti aggregabili. È ben noto che, cfr., ad es., [4], il numero massimo di punti che un k-arco di $PG(2,q)$ può avere è uguale a $q+1$ o $q+2$ a seconda che q sia dispari o pari. Un $(q+1)$-arco di un piano proiettivo $PG(2,q)$ si dice *ovale*. Un $(q+2)$-arco di $PG(2,q)$ si dice un *iperovale*. Il primo profondo risultato nella teoria dei k-archi e degli ovali è stato ottenuto da B. Segre in [10] dove si mostra che:

gli ovali di un piano di Galois $PG(2,q)$, q dispari, sono esattamente le coniche irriducibili dello stesso piano.

Se q è dispari, un punto P non appartenente ad una conica di $PG(2,q)$ si dice *esterno* o *interno* alla conica a seconda che esso è contenuto in esattamente due o nessuna tangente alla conica stessa.

Alla costruzione di archi completi che non sono né ovali né iperovali di un $PG(2,q)$ sono stati dedicati moltissimi lavori tutti basati sulla seguente idea di B. Segre e L. Lombardo Radice (cfr., ad es., [14]):

siano Ω una conica di $PG(2,q)$ e P un punto di $PG(2,q) \setminus \Omega$. Se P è un punto interno alla conica, le $(q+1)/2$ secanti di Ω passanti per P determinano l'involuzione di polo P, ottenuta associando a due a due i punti di Ω allineati con P. Scegliendo un punto in ognuna di tali $(q+1)/2$ coppie, si ottengono $(q+1)/2$ punti, ovviamente a tre a tre non allineati. Aggregando P a tali punti,

(*) Nella seduta del 13 novembre 1993.

si hanno così $(q+3)/2$ punti, ancora a tre a tre non allineati, e cioè un $(q+3)/2$-arco H.

Un procedimento analogo al precedente si ha considerando, invece, un punto P esterno alla conica Ω. Proiettando da P i punti di Ω si ottengono le due tangenti e $(q-1)/2$ secanti. Fissati il punto P ed i due punti di tangenza e scelta in Ω, per ognuna delle suddetti secanti, una qualunque delle due intersezioni, si ottiene un $(q+5)/2$-arco K' avente $(q+3)/2$ punti in comune con la conica stessa.

In entrambi i casi è assai spesso molto difficile stabilire se il k-arco ottenuto è completo. Il primo risultato di rilievo ottenuto in proposito è di Lombardo-Radice [7] il quale, nel caso in cui $q \equiv 3 \pmod 4$ ha costruito $(q+5)/2$-archi completi aventi $(q+3)/2$ punti in comune con la conica Ω.

Recentemente è stato dimostrato (cfr. [6, 8]) che, in un piano proiettivo di ordine dispari, con $q \equiv 1 \pmod 4$ e $q \neq 13$, il $(q+5)/2$-arco K' si può completare aggiungendo al più un punto. Per i piani proiettivi di ordine pari, risultati analoghi erano stati ottenuti in [11, 12].

Mediante la costruzione sopra descritta, si ottengono sempre k-archi completi di $PG(2,q)$ di cardinalità k prossima a $q/2$. Per ottenere archi completi di cardinalità *più piccola* in alcuni lavori (cfr. [1, 6]) è stata generalizzata l'idea di Lombardo-Radice e Segre provando che:

se Ω è una conica irriducibile di $PG(2,q)$ e se si prendono due punti (ed eventualmente anche il polo della retta che congiunge tali punti) di $PG(2,q)\setminus\Omega$, allora si possono ottenere k-archi completi tali che, se $q = 2^b$ ed esiste un divisore s di $q-1$ «abbastanza» piccolo rispetto a q, $(q+8)/3 \leqslant k \leqslant (q+5)/2$.

Ad esempio, se h è pari e $h > 6$, in [1] è stata dimostrata l'esistenza di k-archi completi con $k = (q+8)/2$. Nei lavori appena citati la retta congiungente i due punti di $PG(2,q)\setminus\Omega$ è sempre supposta secante rispetto alla stessa conica Ω. Invece, in [13], T. Szönyi ha generalizzato i risultati di V. Abatangelo e G. Korchmàros nel caso in cui la suddetta retta è tangente a Ω.

Scopo di questo lavoro è quello di stabilire alcuni risultati relativi al caso di una retta esterna alla conica e di dimostrare l'esistenza di k-archi completi che hanno $k-2$ punti in comune con una conica e tali che:

$$(11/24)(q+1)+3 \leqslant |K| \leqslant (q+1)/2+2\,.$$

Si ottengono, in quest'ordine di idee, anche k-archi completi con $k=(q+1)/3+2$.

Vale forse la pena di osservare che i procedimenti qui adottati si basano sulla (Ω, h)-*costruibilità*, nozione introdotta in una nota precedente [2]:

sia Ω una conica non singolare di $PG(2,q)$. L'intero q si dice (Ω, h)-*costruibile* se, fissata una coppia di punti distinti E, $I \in PG(2,q)\setminus\Omega$ tali che:

(i) E è un punto esterno ed I un punto interno alla conica Ω,

(ii) la retta EI congiungente i punti E ed I è esterna a Ω,

allora esistono $h-4$ punti distinti di $\Omega \setminus \{C_1, C_2\}$, $P_1, P_2, \ldots, P_{h-4}$, dove C_i denota il punto di intersezione di una tangente, t_i, a Ω uscente da E, $i = 1, 2$, tali che l'insieme $H := \{P_1, \ldots, P_{h-4}, C_1, C_2, E, I\}$ è un h-arco completo di $PG(2, q)$.

Sempre in [2] e, successivamente, in [3] è stata anche dimostrata l'esistenza di interi q che sono (Ω, h)-costruibili sia per $q = 5$ che per $q = 7$.

In questo lavoro dimostreremo che esistono interi q che sono (Ω, h)-costruibili per ogni q dispari tale che $q + 1$ è divisibile per 3 e $q \geq 121$. Questo risultato ci consentirà, quindi, di costruire i primi esempi di k-archi completi di $PG(2, q)$ con $k < (q + 1)/2$ e tali che tutti i loro punti che non appartengono ad una opportuna conica Ω appartengono ad una retta esterna alla stessa conica.

2. In questo paragrafo, utilizzando alcuni risultati sui cosiddetti *sistemi di coordinate orbitali* relativi ad una conica irriducibile di $PG(2, q)$, con q dispari, e ad una retta esterna alla stessa conica (cfr. [9]), forniremo un procedimento per la costruzione di archi con il linguaggio della teoria dei gruppi provando, in modo semplice, che ad essi è possibile aggregare il centro di una conica al fine di farli divenire archi completi.

Sia Ω una conica irriducibile di $PG(2, q)$ ed r una retta esterna a Ω. È ben noto che il gruppo delle omografie che mutano in sé Ω è isomorfo a $PGL(2, q)$ ed opera sui punti di essa come $PGL(2, q)$ nella sua rappresentazione canonica 3-transitiva. Lo stabilizzatore di r in tale gruppo è diedrale di ordine $2(q + 1)$, contiene perciò un sottogruppo ciclico G di ordine $q + 1$, detto *gruppo delle collineazioni assiali* in [9]. Poiché G opera sui punti di Ω (ma anche su quelli di r) come gruppo regolare, è possibile identificare i punti di Ω (e quelli di r) con gli elementi di G. Fissato un generatore γ in G gli elementi di G si possono porre in corrispondenza biunivoca con gli interi mod $q + 1$. Ne segue che scelto arbitrariamente un punto $Q_0 \in \Omega$, i punti di Ω possono essere parametrizzati con gli interi mod $q + 1$ in maniera che Q_0 abbia parametro 0. Indicheremo con Q_k il punto di parametro k. D'accordo con [9], invece di *parametro k* diremo a volte *coordinata orbitale k*. Similmente, fissato un punto $P_0 \in r$, si introduce una parametrizzazione di r mediante Z_{q+1}. È chiaro che ad ogni sottoinsieme T di Z_{q+1} corrispondono un insieme di punti sopra Ω ed uno sopra r: li indicheremo con i simboli $\Omega(T)$ ed $r(T)$ rispettivamente; essi ovviamente constano di tutti i punti con coordinata orbitale in T. In [9], si mostra che se la tangente ad Ω in Q_0 passa per P_0, si hanno le seguenti proprietà:

(2.1) due punti distinti Q_l, $Q_s (l \neq s)$ di Ω sono allineati con il punto P_n di r se, e solo se, risulta $l + s = n \pmod{q + 1}$;

(2.2) a seconda che n è pari oppure dispari, il punto P_n è esterno o interno alla conica Ω;

(2.3) il gruppo $G = \langle \gamma \rangle$ agisce su Ω in modo che $\gamma(Q_x) = \gamma(Q_{x+1})$.

Supponiamo d'ora in avanti che l'intero q sia dispari e che $q+1$ sia divisibile per 3; allora esiste un sottogruppo H di G di cardinalità $(q+1)/3$.

Corrispondentemente si ha un sottogruppo di indice 3 in $(Z_{q+1}, +)$, che indicheremo con lo stesso simbolo H. Possiamo assumere $H = \{0, 3, \dots, q-2\}$. È opportuno osservare che $\Omega(H)$ può essere riguardato quale *poligono affin regolare*, secondo la definizione data in [5]. È di immediata verifica che il polo O di r rispetto a Ω sta su una secante ad Ω per due punti di $\Omega(H)$.

Infatti, se $Q \in \Omega(H)$, i punti O, Q_0 e Q_k, ove $k = (q+1)/2$, sono allineati. Con l'uso del termine di *punto aggregabile* (dovuto a B. Segre, e già richiamato nell'introduzione), possiamo scrivere:

PROPOSIZIONE 1. *Il centro non è aggregabile ad* $\Omega(H)$.

L'identificazione fatta tra i punti di Ω e di r consente di asserire che le rette congiungenti a due a due i $(q+1)/3$ punti di Ω con coordinata orbitale in H passano per tutti i $(q+1)/3$ punti di r con coordinata orbitale in H.

3. Passiamo ora alla costruzione effettiva di un k-arco completo il quale conterrà tutti i punti di $\Omega(H)$ ed alcuni altri punti di Ω nonché due punti di r, uno dei quali è esterno e l'altro è interno rispetto alla Ω. A tale scopo, riprenderemo le considerazioni svolte nel numero precedente pervenendo a mostrare la (Ω, h)-costruibilità di un arco siffatto.

Si ponga, come prima, $H = \{0, 3, \dots, q-2\}$ e $h = (q+1)/6$. Sia s un intero tale che $(h/2) \leqslant s \leqslant h$ e $h+s$ sia pari. Sia $S_1^* = \{0, 3, \dots, 3s\}$ e $S^{**} = \{3(h+s+2)/2, \dots, 3(h-1), 3h\}$, $S^* = S_1^* \cup S^{**}$, $S = S^* + 1$. All'insieme $\Omega(H \cup S)$ di punti di Ω aggreghiamo ora due punti E ed I di r, quelli di coordinate orbitali 2 e $3(h+s+1)+2$, rispettivamente, ottenendo un insieme K di punti del piano. Ci proponiamo di provare il seguente

TEOREMA 2. *K è un arco tale che nessun punto di Ω è aggregabile.*

Per dimostrare il Teorema 2, occorre e basta far vedere che:

a) comunque si prenda un punto P di Ω la cui coordinata orbitale sia in $H \cup S$, gli ulteriori punti di incontro di Ω con PE e PI non hanno coordinate orbitali in $H \cup S$;

b) comunque si prenda un punto $\dot{P}$ di Ω la cui coordinata orbitale non sia in $H \cup S$, almeno una delle rette PI, PE incontra ulteriormente la conica Ω in un punto la cui coordinata orbitale è in $H \cup S$.

Osserviamo che questi asserti si esprimono in Z_{q+1} come segue:

a') né 2, né $3(h+s+1)+2$ risulta essere la somma di due elementi distinti di $H \cup S$;

b') se $c \notin H \cup S$, allora almeno uno degli interi $2-c$, $3(h+s+1)+2-c$ $(\mathrm{mod}\, q+1)$ appartiene a $H \cup S$.

La verifica delle a') e b') è immediata tenuto conto delle diseguaglianze su h ed s, ed è lasciata al Lettore.

Notiamo, intanto, che E è un punto esterno, I è, invece, un punto interno, rispetto ad Ω. Inoltre, i punti di contatto delle tangenti condotte da E stanno su $\Omega(H \cup S)$, in quanto tali punti di contatto hanno coordinate orbitali 1 e $1 + 3h$, rispettivamente.

La dimostrazione della completezza dell'arco K è meno immediata e verrà esposta nel numero successivo.

4. Abbiamo già visto che nessuno dei punti di $\Omega \setminus K$, né il polo di r è aggregabile. Nemmeno fra i punti di r possono esserci punti aggregabili, essendo r secante a K. Basta perciò far vedere che le secanti ad $\Omega(H)$ invadono tutto il piano tranne $\Omega \setminus \Omega(H)$ ed un eventuale sottoinsieme di punti di r. Se conserviamo la parametrizzazione di Ω, la condizione che ogni punto (non situato su Ω né su r) appartenga ad almeno una delle secanti ad $\Omega(H)$ può esprimersi mediante l'annullamento di un determinante dipendente da due parametri u e v, coordinate degli estremi della secante. Detta condizione può perciò essere espressa in termini di esistenza di qualche zero del polinomio ottenuto dallo sviluppo di tale determinante. Sfortunatamente tale polinomio risulta assai poco maneggevole e per questo motivo si rende necessario un artificio che permette di ovviare a tale inconveniente.

A tale scopo consideriamo il piano proiettivo $PG(2, q^2)$ costruito sopra una estensione quadratica di $GF(q)$ relativa ad un polinomio irriducibile $x^2 - k$, la conica Ω risulta allora contenuta in una conica C di $PG(2, q^2)$, che possiamo assumere in forma canonica $xz = y^2$; e la parametrizzazione di Ω introdotta nel n. 2 si estende in modo naturale ad una parametrizzazione di C. Poiché i parametri su C sono elementi di $GF(q^2)$, vi è un insieme di punti su C corrispondentemente al sottogruppo moltiplicativo di ordine $(q + 1)/3$.

Fissati un punto A di tale insieme ed un generatore γ di tale sottogruppo, si ottengono i punti $A_i = \gamma^i(A)$ $(i = 1, \ldots, (q + 1)/3)$; detto insieme, riguardato ora quale poligono $A_1 A_2 \ldots A_{(q+1)/3}$, risulta essere affin regolare se si considera la retta $0\,\infty$ quale retta all'infinito. Osserviamo intanto che posto $j^2 = k$, ogni elemento del sottogruppo in questione può scriversi nella forma seguente: $((1 + wj)/(1 - wj))^3$, $w \in GF(q)$; più precisamente ogni elemento ha tre rappresentazioni siffatte, eccetto -1 che ne ha soltanto due. La sostituzione lineare fratta α: $t \to [(t - 1)/(t + 1)]j$ sui parametri muta ogni parametro della forma $(a + bj)/(a - bj)$ in un parametro appartenente a $GF(q) \cup \cup \{\infty\}$. In particolare, il poligono $A_1 A_2 \ldots A_{(q+1)/3}$ avrà come immagine un poligono $B_1 B_2 \ldots B_{(q+1)/3}$ inscritto in Ω; notiamo esplicitamente che $\Omega(H)$ si ritrova nelle vesti del poligono $B_1 B_2 \ldots B_{(q+1)/3}$. Osserviamo che α è la restrizione di una omografia del piano $PG(2, q^2)$ alla conica C, quindi $B_1 B_2 \ldots B_{(q+1)/3}$ è ancora un poligono affin regolare rispetto alla retta $y = kz$ quale retta all'infinito. Osserviamo inoltre che i punti B risultano essere rappresentati nella forma $B(u) = (1, u, u^2)$ ove $u = (3wk + w^3k^2)/(1 + + 3w^2k)$. Premesso ciò, vediamo quando il punto $(1, a, b)$ sia aggregabile all'arco $\Omega(H)$,

rappresentato ormai quale insieme dei vertici del poligono $B_1B_2 \dots B_{(q+1)/3}$, oppure quale insieme dei punti $(1, u, u^2)$ ove $u = (3wk + w^3k^2)/(1 + 3w^2k)$. Due punti $(1, u, u^2)$, $(1, u', u'^2)$ ed il punto $(1, a, b)$ sono allineati se, e soltanto se,

$$uu' - a(u + u') + b = 0 . \tag{4.1}$$

Al fine di provare la completezza dell'arco, poniamo $u = \alpha(w)$ e $u' = \alpha(w')$. Dalla (4.1), al variare di w e w' otteniamo la seguente curva

$$f(w, w') = b(1 + 3kw^2)(1 + 3kw'^2) - a(3wk + w^3k^2)(1 + 3w'^2k) + \\ -a(3w'k - w'^3k^2) + (3wk + w^3k^2)(3w'k + w'^3k^2) = 0 . \tag{4.2}$$

Possiamo allora formulare il seguente

TEOREMA 3. *Il punto $P = (1, a, b)$ non è aggregabile all'arco $\Omega(H)$ se, e soltanto se, la curva* (4.2) *ammette dei punti $(w, w'), w, w' \in GF(q)$, con $\alpha(w) \neq \alpha(w')$.*

Il grado di $f(w, w')$ è abbastanza piccolo e se tale curva è assolutamente irriducibile allora, dal classico Teorema di Hasse-Weil (cfr., ad es., [4]), discende che esistono sempre dei punti con $\alpha(w) \neq \alpha(w')$ e quindi il punto $P = (1, a, b)$ non sarà aggregabile. Proviamo, quindi, che la curva $f(w, w') = 0$ è assolutamente irriducibile.

Analizziamo, a tal fine, i suoi eventuali punti singolari. Dopo aver calcolato le due derivate parziali prime, f_w e $f_{w'}$, di $f(w, w')$, sostituiamo in entrambe al posto dell'espressione $b(1 + 3kw^2)(1 + 3kw'^2)$ la seguente espressione (4.3), ad essa equivalente in virtù della (4.2):

$$a(3wk + w^3k^2)(1 + 3w'^2k) + a(3w'k + w'^3k^2)(1 + 3w^2k) - \\ -(3wk + w^3k^2) \cdot (3w'k + w'^3k^2) . \tag{4.3}$$

Otterremo, rispettivamente,

$$(3w'k + w'^3k^2 - a(1 + 3w'^2k))(3k(1 + 3kw^2)(1 + kw^2) - 6kw(3wk + w^3k^2)) = 0$$

e

$$(3wk + w^3k^2 - a(1 + 3w^2k))(3k(1 + 3kw'^2)(1 + kw'^2) - 6kw'(3w'k + w'^3k^2)) = 0 .$$

A questo punto si presentano i seguenti quattro possibili casi (che in effetti possono essere ridotti a tre in virtù delle ultime due uguaglianze sopra riportate):

I) $(3wk + w^3k^2) = a(1 + 3w^2k)$ e $(3w'k + w'^3k^2) = a(1 + 3w'^2k)$.

Sostituendo opportunamente i secondi membri delle due uguaglianze di I) in $f(w, w') = 0$, otteniamo che:

$b \neq a^2$ implica $1 + 3kw^2 = 0$ oppure $1 + 3kw'^2 = 0$. Se $1 + 3kw^2 = 0$, allora $3wk + w^3k^2 = 0$, per cui, essendo $w \neq 0$, si deduce che $3 + w^2k = 0$, e quindi che $8w^2k = 0$, vale a dire $w = 0$; ma ciò è assurdo. Pertanto nel caso I) non esistono soluzioni.

II) $3k(1 + 3kw'^2)(1 + kw'^2) = 6kw'(3w'k + w'^3k^2)$ e

$$3k(1 + 3kw^2)(1 + kw^2) = 6kw(3wk + w^3k^2) .$$

Dalla prima uguaglianza di II) si ricava che:

$k^2w'^4-2kw'^2+1=0$ ovvero che $(kw'^2-1)^2=0$ e quindi che $kw'^2=1$ cioè $w'=\pm$ $\pm 1/j$.

Dalla seconda uguaglianza si ricava, simmetricamente, che $w = \pm 1/j$. Sostituendo tali valori in $f(w, w') = 0$ si ottiene: se $t = v = 1/j$ (o $t = v = -1/j$) $bj - 2ak = 0$ $(a, b, k \in GF(q)), j \notin GF(q)$ e quindi che $a = 0, b + k = 0$, vale a dire $b = -k$. Il punto è $(0, -k)$, cioè il centro di Ω. Se $t = 1/j$ e $v = -1/j$ (o viceversa), si ottiene che $b = k$ e quindi che il punto $(1, a, b)$ appartiene alla retta $y = k$.

III) $(3wk + w^3k^2) = a(1 + 3w^2k)$ implica che $wk = a$ e $kw^2 = 1$ e cioè $w = \pm 1/j$.

Da ciò si ricava che $a = \pm j$, il che è assurdo essendo $a \in GF(q)$ e $j \notin GF(q)$.

Possiamo pertanto affermare di aver provato il seguente:

LEMMA 4. *Se* $(1, a, b)$ *non è il centro di* Ω *e non appartiene alla retta* $y = k$, *allora la curva* $f(w, w') = 0$ *non contiene punti singolari affini.*

Ora esaminiamo i punti che appartengono alla retta all'infinito $w'' = 0$. I punti (w, w', w'') con $w'' = 0$ della curva $f(w, w') = 0$ sono esattamente i punti $(0, 1, 0)$ e $(1, 0, 0)$. Poiché il grado di $f(w, w')$ in w (o in w') è 3, all'infinito hanno molteplicità uguale a 3. Il coefficiente di w^3 in $f(w, w')$ è $h(w') = -a(1 + 3w'^2k) + (3w'k +$ $+ w'^3k^2)$. La retta $w' = c$ è tangente se, e soltanto se, $w' = c$ è una radice di $h(w') = 0$. Con calcoli diretti si verifica che l'equazione $h(w') = 0$ non ha radici multiple e quindi che i punti della retta all'infinito $w'' = 0$ sono punti singolari ordinari di molteplicità 3. Da questo calcolo segue anche che la curva non contiene rette. Abbiamo quindi provato che vale il seguente:

LEMMA 5. *La curva* C^6: $f(w, w') = 0$ *non contiene rette ed ha due soli punti singolari:* $(0, 1, 0)$ *e* $(1, 0, 0)$. *Questi due punti sono entrambi singolari ordinari di molteplicità tre.*

Proviamo ora il seguente:

TEOREMA 6. *La curva algebrica* C^6: $f(w, w') = 0$ *è assolutamente irriducibile.*

DIMOSTRAZIONE. La curva $f(w, w') = 0$ è tale che $\deg f(w, w') = 6$. Se fosse riducibile, allora, non contenendo rette, si potrebbero presentare soltanto i seguenti casi:

$C^6 = \Omega \cup \Omega' \cup \Omega''$, con le tre componenti tutte di grado 2; $C^6 = \Omega \cup \Omega'$, con entrambe le componenti di grado 3; $C^6 = \Omega \cup \Omega'$, con $\deg \Omega = 2$ e $\deg \Omega' = 4$.

In virtù del Teorema di Bèzout, in ognuno dei tre singoli casi le componenti presenti hanno, a due a due, punti affini in comune. Ma ogni punto in comune a due componenti deve essere singolare, in contraddizione con il fatto che la C^6 non possiede punti affini singolari. La dimostrazione del Teorema è così completa.

Siamo ora in condizione di applicare nei nostri ragionamenti il già citato Teorema di Hasse-Weil. Essendo la curva $f(w, w') = 0$ di grado 6 e dotata di due punti singolari di molteplicità 3, si deduce che:

$g \leqslant \left(\binom{5}{2}\right) - 2\binom{3}{2} = 4$, dove g indica, come di consueto, il *genere* della curva. Il Teorema di Hasse-Weil ci permette di affermare, quindi, che il numero N dei punti di $f(w, w') = 0$ sopra $GF(q)$ soddisfa la seguente disuguaglianza:

$$|N - (q+1)| \leqslant 8\sqrt{q}\,.$$

Proviamo ora che esistono punti di $f(w, w') = 0$ con $\alpha(w) \neq \alpha(w')$. Osserviamo innanzitutto che $\alpha(w) = \alpha(w')$ soltanto se vale la seguente uguaglianza: $(3wk + w^3k^2)/(1 + 3w^2k) = (3w'k + w'^3k^2)/(1 + 3w'^2k)$ ovvero C^5: $3(wk + w^3k)\cdot(1 + 3w'^2k) = (3w'k + w'^2k)(3w^2k)$.

Otteniamo, così, un'altra curva algebrica, C^5, di ordine 5. Esistono quindi non più di 30 punti in comune tra la C^6 e la C^5 e tra essi si trovano anche i punti singolari della $f(w, w') = 0$. Si può dunque affermare che se $N \geqslant 31$, allora esistono punti affini di $f(w, w') = 0$ con $\alpha(w) \neq \alpha(w')$. Poiché $N \geqslant q + 1 - 8\sqrt{q}$, se $q \geqslant 121$, allora esistono punti di $f(w, w') = 0$ con $\alpha(w) \neq \alpha(w')$. Indicando con $\Omega(H)$ l'arco già definito nel precedente Teorema 3, possiamo, pertanto, affermare di aver dimostrato il seguente:

TEOREMA 7. *Il punto* $(1, a, b)$ *non è aggregabile all'arco* $\Omega(H)$.

Esaminiamo, infine, il caso di un punto P di coordinate $(0, a, b)$. Se un tale punto P è aggregabile all'arco $\Omega(H)$, allora, denotato con γ un elemento del gruppo G di ordine $q + 1$, anche il punto $(0, a, b)^{\gamma^3}$ è aggregabile. Si osservi che γ^3 non fissa la retta $w = 0$ e perciò P^{γ^3} è un punto affine del tipo $(1, a', b')$ e quindi non aggregabile, contro la precedente affermazione. Pertanto P non è aggregabile. Osserviamo inoltre che la cardinalità di K è $5(q+1)/12 + (s+2)/2 + 2$. Infatti $K = H \cup S_1^* \cup S^{**} \cup \cup \{E, I\}$ e così $|K| = (q+1)/3 + (s+2) + (q - 6s - 11)/12 + 2 = 5(q+1)/12 + (s+2)/2 + 2$. Tenendo conto che $(q+1)/12 \leqslant s \leqslant (q+1)/6$ otteniamo che: $(11/24)(q+1) + 3 \leqslant |K| \leqslant (q+1)/2 + 2$.

Ricordando, allora, quanto dimostrato nel precedente Teorema 2, abbiamo concluso la dimostrazione del nostro risultato principale e cioè del seguente:

TEOREMA 8. *Se* $q \geqslant 121$ *ed* s *è un intero tale che* $(q+1)/12 \leqslant s \leqslant (q+1)/6$ *e* $(q+1)/6 + s$ *è un numero pari, allora l'arco*

$$K = \{P \in C: p = 0, 3, \ldots, q-2, p = 1, 4, \ldots, 3s+1, p = (q + 3s + 7)/2, \ldots, (q+1)/2 + 1\} \cup \{E, I\}$$

è completo e soddisfa tutte le condizioni della (Ω, h)*-costruibilità. Il numero dei punti di* K *è* $5(q+1)/12 + (s+2)/2 + 2$ *e soddisfa la seguente disuguaglianza:* $(11/24)(q+1) + 3 \leqslant |K| \leqslant (q+1)/2 + 2$

PROPOSIZIONE 9. *Se* $q \geqslant 121$, *allora l'arco* $K^* = \{P \in \Omega: p = 0, 3, \ldots, q-2\} \cup \cup \{E\} \cup \{\mathbf{1}\}$, *dove* E *è il punto di coordinata orbitale* 2 *ed* $\mathbf{1}$ *è il punto di coordinata orbitale* 1, *è completo, ma non soddisfa tutte le condizioni della* (Ω, h)*-costruibilità.*

DIMOSTRAZIONE. In virtù del Teorema 7 e dalla Proposizione 1, si possono aggrega-

re soltanto i punti di $\Omega \setminus K^*$. Un punto di $\Omega \setminus K^*$ ha coordinata orbitale x, con $x \in H + 1$, oppure $x \in H + 2$. Se $x \in H + 1$, allora esiste un $h \in H$ tale che i punti di coordinate orbitali x, h ed 1 sono allineati ($h = 1 - x \in H$). Se $x \in H + 2$, allora esiste un $h \in H$ tale che i punti di coordinate orbitali x, h e 2 sono allineati ($h = 2 - x \in H$). $c_1 = 1$, $c_2 = 1 + (q + 1)/2$ (i due punti di contatto con Ω delle tangenti condotte da E) non sono contenuti in H, così le condizioni di (C, h)-costruibilità non sono soddisfatte.

Lavoro eseguito con il contributo del Ministero dell'Università e della Ricerca Scientifica e Tecnologica e del G.N.S.A.G.A. del Consiglio Nazionale delle Ricerche.

Bibliografia

[1] V. Abatangelo, *A class of complete* $((q + 8)/3)$*-arcs of* $PG(2, q)$ *with* $q = 2^b$ *and* $h(\geq 6)$ *even.* Ars Comb., 16, 1983, 103-111.

[2] G. Faina, *Complete k-caps in* $PG(3, q)$ *with* $k < (q^2 + q + 4)/2$. Ars Comb., 33, 1992, 311-317.

[3] G. Faina, *The maximum size of a* (Ω, P, Q)*-cap in* $PG(3, 5)$. Combinatorics '88. Proceedings of the International Conference on *Incidence Geometries and Combinatorial Structures.* Mediterranean Press, 1991, vol. I, 373-380.

[4] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields.* Clarendon Press, Oxford 1979.

[5] G. Korchmàros, *Estensione del concetto di poligono regolare ad un qualunque piano affine.* Atti Acc. Lincei Rend. fis., s. 8, 60, 1976, 119-125.

[6] G. Korchmàros, *New examples of k-arcs in* $PG(2, q)$. European J. Comb., 4, 1983, 329-334.

[7] L. Lombardo-Radice, *Sul problema dei k-archi completi di* $S_{2,q}$. Boll. Un. Mat. Ital., 11, 1956, 178-181.

[8] G. Pellegrino, *Un'osservazione sul problema dei k-archi completi in* $S_{2,q}$, $q \equiv 3 \pmod 4$. Atti Acc. Lincei Rend. fis., s. 8, 63, 1977, 33-44.

[9] G. Pellegrino, *Proprietà e applicazioni del gruppo delle collineazioni assiali su una conica del piano di Galois di ordine dispari.* Rend. Mat. Appl., 11, 1991, 591-616.

[10] B. Segre, *Ovals in a finite projective plane.* Canad. J. Math., 7, 1955, 414-416.

[11] B. Segre, *Introduction to Galois Geometries.* Atti Acc. Lincei Mem. fis., s. 8, 8, 1967, 133-236.

[12] M. Scafati Tallini, *Archi completi in un* $S_{2,q}$ *con q pari.* Atti Acc. Lincei Rend. fis., s. 8, 37, 1964, 48-51.

[13] T. Szönyi, *Note on the order of magnitude of k for complete k-arcs in* $PG(2, q)$. Discrete Math., 66, 1987, 279-282.

[14] T. Szönyi, *Complete arcs in Galois planes: a survey.* Quaderni del Sem. Geom. Comb. Univ. Roma, 94, 1989.

[15] G. Zappa, *Fondamenti di Teoria dei Gruppi.* Voll. I, II, Edizioni Cremonese, Roma 1965, 1970.

Dipartimento di Matematica
Università degli Studi di Perugia
Via Vanvitelli, 1 - 06100 Perugia