[6] P. D. T. A. Elliott, *On the Turán–Kubilius inequality and a limitation for the Large Sieve*, to appear in Journ. Amer. Math. Soc. 1970.
[7] P. Erdös and A. Rényi, *Some remarks on the Large Sieve of Yu. V. Linnik*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 11 (1968), pp. 3–13.
[8] P. X. Gallagher, *The Large Sieve*, Mathematika 14 (1967), pp. 14–20.
[9] F. R. Gantmacher, *Matrix Theory*, vol. II, New York 1964.
[10] G. Hálasz, *Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen*, Acta Math. Acad. Sci. Hung. 19 (1968), pp. 365–403.
[11] P. Halmos, *Introduction to Hilbert Space*, New York 1951.
[12] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford 1938.
[13] Yu. V. Linnik, *The Large Sieve*, Dokl. Akad. Nauk SSSR 30 (1947), pp. 292–294.
[14] L. Mirsky, *An Introduction to Linear Algebra*, Oxford 1963.
[15] H. L. Montgomery, *Mean and large values of Dirichlet polynomials*, Inventiones Mathematicae 8 (1969), pp. 334–345.
[16] K. Prachar, *Primzahlverteilung*, Berlin 1957.
[17] A. Rényi, *On the large sieve of Ju. V. Linnik*, Compositio Math. 8 (1950), pp. 68–75.
[18] K. F. Roth, *On the large sieve of Linnik and Rényi*, Mathematika 12 (1965), pp. 1–9.
[19] E. C. Titchmarsh, *An Introduction to the Theory of Fourier Integrals*, Oxford 1959.
[20] — *The Theory of the Riemann Zeta Function*, Oxford 1951.
[21] J. H. Wilkinson, *The Algebraic Eigenvalue Problem*, Oxford 1965.
[22] D. Wolke, *On the inequality of the Large Sieve*, to appear in Math. Zeitschr.

UNIVERSITY OF COLORADO
Boulder, Colorado

UNIVERSITY OF NOTTINGHAM
Nottingham, England

Received on 15. 4. 1970

ACTA ARITHMETICA
XVIII (1971)

Ovali ed altre curve nei piani di Galois di caratteristica due

di

B. Segre ed U. Bartocci (Roma)

Il presente lavoro viene dedicato con profonda ammirazione alla memoria degli eminenti matematici H. Davenport e W. Sierpiński

Prefazione. L'introduzione e lo studio dei k-archi di un piano $S_{2,q}$ di Galois e delle loro estensioni agli spazi superiori devesi essenzialmente a B. Segre ed a suoi discepoli. Ne sono derivate le cosiddette *geometrie di Galois*, vari aspetti salienti delle quali trovansi esposti nella nota [24](1) e nella monografia [27] (in quest'ultima, accanto a nuovi risultati), le quali contengono altresì un'ampia bibliografia sull'argomento, a cui rinviamo con l'aggiunta dei lavori elencati alla fine della presente Memoria.

Un *k-arco* è un insieme di punti di $S_{2,q}$, a tre a tre non allineati; esso denominasi un'*ovale* quando k sia tale che in $S_{2,q}$ non esista nessun $(k+1)$-arco. Riguardo a queste ultime, occorre distinguere due casi a seconda che $q = p^h$ è dispari o pari, ossia a seconda che il numero primo p è maggiore od eguale a 2.

Mentre nel primo caso risulta $k = q+1$ ed ogni $(q+1)$-arco, come insieme di punti, è quello dei punti di una conica non singolare di $S_{2,q}$, e viceversa ([21]; [25], nn. 173–174), nel secondo caso — e cioè se $q = 2^h$ — per un'ovale si ha $k = q+2$, la struttura algebrica dei $(q+2)$-archi (e delle loro estensioni agli spazi superiori) essendo però in generale assai più complessa che nel caso dispari e ben lungi dall'essere pienamente nota.

Più precisamente, qualunque sia $q = 2^h$, si ottiene intanto un'ovale di $S_{2,q}$ coll'aggregare ai punti di una conica non singolare di $S_{2,q}$ il nucleo di questa. Tuttavia ([25], n. 178), mentre per $h = 1, 2, 3$ non vi sono altre ovali all'infuori degli insiemi così definiti, nell'ipotesi che sia $h > 3$ — ad esclusione al più soltanto dei casi $h = 4$, $h = 6$, il primo dei quali è poi stato trattato direttamente con l'uso di un calcolatore elettronico, cfr. [18] — si hanno fra l'altro le *ovali* ottenibili in $S_{2,q}$ con l'aggregare

(1) I numeri tra [ ] rimandano alla bibliografia posta in fine del lavoro.

i punti all'infinito degli assi x, y a quelli del *diagramma di traslazione* di equazione

$$y = x^{2g} \quad [\text{con } 2 \leqslant g \leqslant h-2,\ (g,h)=1], \tag{1}$$

nessun $(q+1)$-arco delle quali risulta una conica.

Altre classi interessanti di ovali possono venire definite e studiate nel caso pari mediante considerazioni astratte di carattere gruppale (cfr. soprattutto F. Buekenhout [5] e J. Tits [29], [30], [31]). La questione può però venire affrontata in tutta generalità ed in modo analitico diretto, secondo quanto specificato da B. Segre nella Nota preventiva [26].

Introdotti i concetti di *diagramma* e di *diagramma di traslazione*, si giunge così al problema di vedere quando l'insieme ottenuto aggregando i punti all'infinito degli assi x, y a quelli del diagramma di equazione

$$y = \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{q-1} x^{q-1} \quad (\alpha_i \in \mathrm{GF}(q)) \tag{2}$$

risulti un'ovale, il quale si riconduce a sua volta allo studio dell'insieme dei punti definiti su $\mathrm{GF}(q)$ di certe superficie algebriche di uno spazio affine. Nel *caso più semplice* in cui la (2) sia della forma

$$y = x^{k+2} \tag{3}$$

si prova che, a quel fine, è necessario e sufficiente che k sia pari e che la forma ternaria

$$\sigma_k(x, x_1, x_2) = \sum_{i+i_1+i_2=k} x^i x_1^{i_1} x_2^{i_2} \tag{4}$$

non ammetta in $\mathrm{GF}(q)$ nessuno zero non banale, ad eccezione al più di $(1,1,1)$; il che può venire ricollegato alla questione dell'*irriducibilità assoluta* di certe curve piane algebriche.

Nel presente lavoro si dànno le dimostrazioni dei risultati enunciati nell'ultima Nota citata, con l'aggiunta di alcuni complementi — dovuti al più giovane degli autori(2) — concernenti le *ovali di traslazione* (§ II) ed alcune condizioni per l'irriducibilità assoluta di una curva piana algebrica (teorema 11, lemma 7). Va rilevato come l'attuale teorema 14 venga a rettificare l'analogo enunciato della Nota suddetta; il che non consente più l'agevole dimostrazione, ivi accennata, relativa all'irriducibilità assoluta delle curve σ_{3n+2} per $n \geqslant 1$, sostituita qui tuttavia da argomentazioni di altro genere.

I. Diagrammi e diagrammi di traslazione. Sia $S_{r+1,q}$ $(r \geqslant 1)$ uno spazio proiettivo su di un campo di Galois $\gamma = \mathrm{GF}(q)$, ove $q = p^h$, essendo p la caratteristica di γ ed $h \geqslant 1$. Fissato un iperpiano $S_r \subset S_{r+1}$, indicheremo con A_{r+1} lo spazio affine $S_{r+1} - S_r$ che se ne deduce.

(2) Questi venne in qualche punto coadiuvato dal dott. J. W. P. Hirschfeld, che qui si ringrazia.

Scelto allora comunque $P \in S_r$, chiameremo *diagramma* relativo a P un qualsiasi insieme di punti $\Omega \subset A_{r+1}$ incontrato in uno ed un sol punto da ogni retta di A_{r+1} uscente da P.

È chiaro che

$$|\Omega| = q^r \tag{5}$$

e che, introdotte in A_{r+1} coordinate affini di punto $(x_1, x_2, \ldots, x_r, y)$ tali che P risulti il punto all'infinito dell'asse y, l'equazione di Ω può venir scritta nella forma

$$y = f(x_1, x_2, \ldots, x_r), \tag{6}$$

ove $f(x_1, x_2, \ldots, x_r)$ designa una funzione univoca delle x, a valori in γ, definita per valori di questi argomenti arbitrari in γ; e viceversa.

Il diagramma Ω verrà detto *di traslazione*, quand'esso sia trasformato in sé da ogni traslazione che muti l'uno nell'altro due punti di Ω comunque scelti.

Proviamo il

LEMMA 1. *Il diagramma Ω di equazione* (6) *risulta di traslazione se, e soltanto se, l'equazione funzionale*

$$f(x_1+c_1, x_2+c_2, \ldots, x_r+c_r) = f(x_1, x_2, \ldots, x_r)+f(c_1, c_2, \ldots, c_r)-f(0,0,\ldots,0) \tag{7}$$

sussiste identicamente nelle x, c.

Dimostrazione. È intanto evidente che la traslazione τ di equazioni

$$x_1 = x_1'+c_1, \quad x_2 = x_2'+c_2, \quad \ldots, \quad x_r = x_r'+c_r, \quad y = y'+c$$

muta il diagramma Ω nel diagramma $\Omega' = \tau(\Omega)$ di equazione

$$y' = f(x_1'+c_1, x_2'+c_2, \ldots, x_r'+c_r) - c.$$

Se vale la (7), si ha

$$y' = f(x_1', x_2', \ldots, x_r') + f(c_1, c_2, \ldots, c_r) - f(0,0,\ldots,0) - c$$

di guisa che, come vedremo, se $\Omega' \cap \Omega \neq \emptyset$ allora $\Omega' = \Omega$.

In tal caso, infatti, si ha che $\exists Q \in \Omega' \cap \Omega$ ove

$$Q = (\xi_1, \xi_2, \ldots, \xi_r, f(\xi_1, \xi_2, \ldots, \xi_r))$$
$$= (\xi_1, \xi_2, \ldots, \xi_r, f(\xi_1, \xi_2, \ldots, \xi_r)+f(c_1, c_2, \ldots, c_r)-f(0,0,\ldots,0)-c),$$

dal che

$$f(c_1, c_2, \ldots, c_r) = f(0,0,\ldots,0)+c$$

e quindi

$$\Omega': \quad y' = f(x_1', x_2', \ldots, x_r') \Rightarrow \Omega' = \Omega, \quad \text{c.v.d.}$$

Viceversa, se

$$\Omega' \cap \Omega \neq \emptyset \Rightarrow \Omega' = \Omega \qquad (\forall \tau)$$

necessariamente vale la (7). Infatti

$$\Omega' \cap \Omega \neq \emptyset \Rightarrow f(c_1, c_2, \ldots, c_r) = f(0, 0, \ldots, 0) + c;$$

d'altronde $\Omega' = \Omega$ si traduce nella

$$f(x_1 + c_1, x_2 + c_2, \ldots, x_r + c_r) - c = f(x_1, x_2, \ldots, x_r),$$

d'onde, sostituendo c tramite la

$$c = f(c_1, c_2, \ldots, c_r) - f(0, 0, \ldots, 0),$$

si ottiene la (7), c.v.d.

La (7) è manifestamente soddisfatta da una qualsiasi funzione lineare delle x; corrispondentemente, la (6) fornisce gli iperpiani di A_{r+1} non contenenti il punto P.

Proviamo ora il

TEOREMA 1. *I diagrammi di traslazione sono tutti e soli quelli rappresentabili con un'equazione della forma*

$$y = a_0 + \sum_{i=1}^{r} \sum_{j=0}^{h-1} a_{ij} x_i^{p^j}, \tag{8}$$

ove le a designano elementi arbitrari di γ.

Dimostrazione. È intanto evidente che la (8) è l'equazione di un diagramma di traslazione, giacché corrispondentemente ad essa la (7) risulta soddisfatta.

Supponiamo, inversamente, che sia dato un diagramma

$$\Omega: \quad y = f(x_1, x_2, \ldots, x_r)$$

con $f(x_1, x_2, \ldots, x_r)$ soddisfacente alla (7). La corrispondenza

$$\gamma^r = \underbrace{\gamma \times \gamma \times \ldots \times \gamma}_{r \text{ volte}} \overset{\Psi}{\to} \gamma$$

definita dalla

$$\Psi(x_1, x_2, \ldots, x_r) = f(x_1, x_2, \ldots, x_r) - f(0, 0, \ldots, 0)$$

risulta allora un omomorfismo tra le strutture di gruppo additivo di γ^r e di γ. È evidente che di tali omomorfismi ve ne sono esattamente q^{rh}, in quanto γ^r è un p-gruppo abeliano elementare di ordine p^{rh}.

Poiché, nella corrispondenza così introdotta tra l'insieme dei diagrammi di traslazione e l'insieme $\mathrm{Hom}(\gamma^r, \gamma)$ (corrispondenza evidentemente suriettiva), vi sono esattamente q diagrammi distinti che individuano lo stesso omomorfismo (corrispondentemente alla scelta di $f(0, 0, \ldots, 0)$ in γ), abbiamo in definitiva che i diagrammi di traslazione distinti sono esattamente in numero di $q^{rh} \cdot q = q^{rh+1}$. Tanto basta per concludere nel modo voluto, giacché la (8) fornisce proprio q^{rh+1} diagrammi di traslazione, in quanto — come ora mostreremo — due diagrammi di equazioni rispettive

$$y = a_0 + \sum_{i=1}^{r} \sum_{j=0}^{h-1} a_{ij} x_i^{p^j} \quad \text{e} \quad y = b_0 + \sum_{i=1}^{r} \sum_{j=0}^{h-1} b_{ij} x_i^{p^j}$$

coincidono se, e soltanto se,

$$a_0 = b_0, \qquad a_{ij} = b_{ij} \qquad (\forall\, i, j).$$

Infatti, se i due diagrammi coincidono, il polinomio

$$(a_0 - b_0) + \sum_{i=1}^{r} \sum_{j=0}^{h-1} (a_{ij} - b_{ij}) x_i^{p^j} \tag{9}$$

è annullato da ogni punto $Q(x_1, x_2, \ldots, x_r, y) \in A_{r+1}$. Se tale polinomio non fosse identicamente nullo nelle x, introdotte in S_{r+1} coordinate proiettive omogenee di punto tramite le

$$x_1 = X_1/X_0, \qquad x_2 = X_2/X_0, \qquad \ldots, \qquad x_r = X_r/X_0, \qquad y = Y/X_0,$$

avremmo che l'ipersuperficie di S_{r+1} di equazione

$$(a_0 - b_0) X_0^{p^h} + \sum_{i=1}^{r} \sum_{j=0}^{h-1} (a_{ij} - b_{ij}) X_i^{p^j} X_0^{p^h - j} = 0 \tag{10}$$

invaderebbe l'intero spazio S_{r+1}, pur avendo ordine minore di $q+1$, il che manifestamente non può essere.

II. Il caso delle ovali di traslazione. Come precedentemente accennato, il problema generale delle ovali in un piano di Galois $S_{2,2^h}$ si riconduce subito a vedere quand'è che l'insieme ottenuto aggregando i punti all'infinito degli assi x, y al diagramma di equazione

$$y = a_1 x + a_2 x^2 + \ldots + a_{2^h - 1} x^{2^h - 1} \qquad [a_i \in \gamma] \tag{11}$$

risulta un'ovale.

Vogliamo ora determinare condizioni necessarie e sufficienti affinché ciò accada, nel caso che il diagramma assegnato sia un diagramma di traslazione:

$$y = a_0 x + a_1 x^2 + \ldots + a_{h-1} x^{2^{h-1}} \qquad [a_i \in \gamma,\ h \geqslant 4]. \tag{12}$$

Chiameremo le ovali così definibili *ovali di traslazione*. È evidente che tutte le ovali ottenute coll'aggregare ai punti di una conica non singolare di $S_{2,2^h}$ il nucleo di questa sono ovali di traslazione; mentre l'esempio (1) mostra che esistono — almeno nei casi $h \neq 4$, $h \neq 6$ — ovali di traslazione all'infuori di quelle.

Cominciamo con lo stabilire il

LEMMA 2. *L'equazione*

$$a_0x+a_1x^2+\ldots+a_{h-1}x^{2^{h-1}}=0 \qquad [a_i\in\gamma] \tag{13}$$

ammette in γ l'unica soluzione $x=0$ se, e soltanto se, posto

$$D=\{a_0,a_1,a_2,\ldots,a_{h-1}\}=\begin{vmatrix} a_0 & a_1 & a_2 & \ldots & a_{h-1}\\ a_{h-1}^2 & a_0^2 & a_1^2 & \ldots & a_{h-2}^2\\ \ldots & \ldots & \ldots & \ldots & \ldots\\ a_1^{2^{h-1}} & a_2^{2^{h-1}} & a_3^{2^{h-1}} & \ldots & a_0^{2^{h-1}}\end{vmatrix}, \tag{14}$$

risulta $D\neq 0$.

Dimostrazione. Cominciamo con l'osservare che, poiché attualmente $p=2$, così il quadrato di un qualsiasi determinante uguaglia il determinante i cui elementi sono i quadrati di quelli del dato. Per il determinante D che figura nella (14) risulta pertanto $D^2=D$; sicché, comunque si scelgano le a, dev'essere $D=0$ oppure $D=1$.

Se l'equazione (13) ha una soluzione $x\neq 0$, allora risulta

$$\begin{aligned} a_0x+a_1x^2+\ldots+a_{h-1}x^{2^{h-1}}&=0,\\ a_0^2x^2+a_1^2x^4+\ldots+a_{h-1}^2x&=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots&\\ a_0^{2^{h-1}}x^{2^{h-1}}+a_1^{2^{h-1}}x+\ldots+a_{h-1}^{2^{h-1}}x^{2^{h-2}}&=0,\end{aligned}$$

ossia

$$\begin{aligned} a_0x+a_1x^2+\ldots+a_{h-1}x^{2^{h-1}}&=0,\\ a_{h-1}^2x+a_0^2x^2+\ldots+a_{h-2}^2x^{2^{h-1}}&=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots&\\ a_1^{2^{h-1}}x+a_2^{2^{h-1}}x^2+\ldots+a_0^{2^{h-1}}x^{2^{h-1}}&=0,\end{aligned}$$

epperò $D=\{a_0,a_1,\ldots,a_{h-1}\}=0$.

Viceversa, proviamo che, se $D=\{a_0,a_1,\ldots,a_{h-1}\}=0$, l'equazione (13) ammette soluzioni $x\neq 0$. Osserviamo a tal fine che la corrispondenza $\gamma\overset{\Psi}{\to}\gamma$ definita dalla

$$\Psi(x)=a_0x+a_1x^2+\ldots+a_{h-1}x^{2^{h-1}}$$

è, come già rilevato nel paragrafo I, un endomorfismo del gruppo additivo di γ. La corrispondenza Ψ risulta un automorfismo se, e soltanto se, il suo nucleo $\mathrm{Ker}\,\Psi$ è uguale a zero, cioè se, e soltanto se, l'unica soluzione dell'equazione (13) è $x=0$. Per provare che la (13) attualmente ammette soluzioni $x\neq 0$, basterà dunque stabilire che Ψ non è un automorfismo, mostrando che la Ψ non è suriettiva. Posto

$$y=a_0x+a_1x^2+\ldots+a_{h-1}x^{2^{h-1}},$$

si ha infatti

$$\begin{aligned} y&=a_0x+a_1x^2+\ldots+a_{h-1}x^{2^{h-1}},\\ y^2&=a_0^2x^2+a_1^2x^4+\ldots+a_{h-1}^2x,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ y^{2^{h-1}}&=a_0^{2^{h-1}}x^{2^{h-1}}+a_1^{2^{h-1}}x+\ldots+a_{h-1}^{2^{h-1}}x^{2^{h-1}};\end{aligned}$$

mentre d'altro canto, in virtù della $D=0$, esistono elementi $\lambda_0,\lambda_1,\ldots,\lambda_{h-1}$ non tutti nulli di γ tali che

$$\begin{aligned} \lambda_0a_0+\lambda_1a_{h-1}^2+\ldots+\lambda_{h-1}a_1^{2^{h-1}}&=0,\\ \lambda_0a_1+\lambda_1a_0^2+\ldots+\lambda_{h-1}a_2^{2^{h-1}}&=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots&\\ \lambda_0a_{h-1}+\lambda_1a_{h-2}^2+\ldots+\lambda_{h-1}a_0^{2^{h-1}}&=0.\end{aligned}$$

Allora

$$\lambda_0y+\lambda_1y^2+\ldots+\lambda_{h-1}y^{2^{h-1}}=0,$$

di guisa che gli elementi y del tipo $\Psi(x)$ sono attualmente al più 2^{h-1}, epperò Ψ non è suriettiva, c.v.d.

Proviamo in secondo luogo il

TEOREMA 2. *Condizione necessaria e sufficiente affinché, aggregando i punti all'infinito degli assi x, y al diagramma di traslazione* (12), *si ottenga un'ovale, è che sussista la*

$$\{a_0+\lambda,a_1,\ldots,a_{h-1}\}=\lambda^{2^{h-1}}+1 \tag{15}$$

identicamente rispetto a λ.

Dimostrazione. Cominciamo col vedere quand'è che le rette del tipo $y=c$ unisecano il diagramma (12). Ciò accade se, e soltanto se, l'equazione

$$c=a_0x+a_1x^2+\ldots+a_{h-1}x^{2^{h-1}}$$

ammette qualche soluzione x in γ per ogni c, cioè, con le notazioni del lemma 2, se, e soltanto se, la corrispondenza Ψ risulta un automorfismo di $\gamma(+)$. Perché ciò accada è necessario e sufficiente che sia $\mathrm{Ker}\,\Psi=\{0\}$, cioè che l'equazione

$$a_0x+a_1x^2+\ldots+a_{h-1}x^{2^{h-1}}=0$$

ammetta l'unica soluzione $x=0$; il che, stante il lemma 2, ha luogo se, e soltanto se, sussiste la

$$\{a_0,a_1,\ldots,a_{h-1}\}=1. \tag{16}$$

Vediamo poi quand'è che le rette del tipo $y=\lambda x$, con $\lambda\neq 0$, esattamente bisecano il diagramma (12). All'uopo è necessario e sufficiente che l'equazione

$$a_0x+a_1x^2+\ldots+a_{h-1}x^{2^{h-1}}=\lambda x$$

ammetta, per ogni $\lambda \neq 0$, qualche soluzione $x \neq 0$; e, di nuovo dal lemma 2, si ha che ciò accade se, e soltanto se, sussiste la

$$\{a_0+\lambda, a_1, \ldots, a_{h-1}\} = 0 \quad (\forall \lambda \neq 0). \tag{17}$$

Le due condizioni (16) e (17), prese assieme, equivalgono a che, aggiungendo al diagramma (12) i punti all'infinito degli assi x, y, si ottenga un'ovale. Infatti, il diagramma essendo di traslazione, il gruppo di trasformazioni su esso indotto dal gruppo delle traslazioni del piano che lo mutano in sé è transitivo. Ne discende che la condizione espressa dalla (17) per le rette del tipo $y = \lambda x$ garantisce un'analoga situazione per le rette del tipo $y+y_0 = \lambda(x+x_0)$ (ove (x_0, y_0) indichi un punto qualsiasi del diagramma (12)).

Il teorema segue ora subito da ciò che, in forza della $q = 2^h$, l'insieme delle (16), (17) equivale precisamente alla (15), c.v.d.

Passiamo ora a stabilire il

LEMMA 3. *Condizione necessaria affinché sussista la* (15) *è che sia*

$$a_0 = 0.$$

Basta osservare che il determinante che figura quale primo membro della (15) ha lo sviluppo:

$$(a_0+\lambda)^{2^h-1}+(a_0+\lambda)^{2^h-4}a_1a_{h-1}^2+\ldots$$

Ordinando secondo le potenze decrescenti di λ questo si scrive

$$\lambda^{2^h-1}+a_0\lambda^{2^h-2}+\ldots,$$

onde la (15) fornisce $a_0 = 0$, c.v.d.

Stante il lemma 3, possiamo riformulare il teorema 2 nel modo seguente (determinazione delle ovali di traslazione):

TEOREMA 3. *Condizione necessaria e sufficiente affinché, aggregando i punti all'infinito degli assi x, y al diagramma di traslazione di equazione*

$$y = a_1x^2+a_2x^4+\ldots+a_{h-1}x^{2^{h-1}},$$

si ottenga un'ovale, è che sussista la

$$\{\lambda, a_1, \ldots, a_{h-1}\} = \lambda^{2^{h-1}}+1 \tag{18}$$

identicamente rispetto a λ.

Concluderemo questo paragrafo esplicitando la condizione (18) nei casi $q = 2^4$ e $q = 2^6$; questi hanno particolare interesse, giacché nello esempio (1) di ovali di traslazione — non ottenibili da una conica aggiungendole il nucleo — essi erano stati esclusi. Possiamo stabilire al riguardo il

TEOREMA 4. *Se $h = 4$ oppure $h = 6$, non esistono ovali di traslazione all'infuori di quelle che si ottengono aggregando il nucleo ai punti di una conica non singolare di $S_{2,2^h}$.*

Dimostrazione. Consideriamo dapprima il caso $h = 4$, per il quale la condizione (18) diventa

$$\begin{aligned}\{\lambda, a_1, a_2, a_3\} &= \lambda^{15}+\lambda^{12}a_1a_3^2+\lambda^{10}a_2^5+\lambda^9a_1^2a_3^4+\lambda^8(a_1^3a_2^4+a_2a_3^6)+\\ &+\lambda^6a_1^8a_3+\lambda^5a_2^{10}+\lambda^4(a_1^9a_2^2+a_2^8a_3^3)+\lambda^3a_1^4a_3^8+\\ &+\lambda^2(a_1^{12}a_2+a_2^4a_3^9)+\lambda(a_1^6a_2^8+a_2^2a_3^{12})+\{0, a_1, a_2, a_3\}\\ &= \lambda^{15}+1.\end{aligned}$$

Da qui, necessariamente, $a_2 = 0$; mentre poi $a_1 \neq 0 \Rightarrow a_3 = 0$ e $a_3 \neq 0 \Rightarrow a_1 = 0$. Le uniche possibilità sono dunque

$$y = a_1x^2, a_1 \neq 0, \quad \text{ovvero} \quad y = a_3x^8, \ a_3 \neq 0.$$

In entrambi i casi (poiché attualmente $q = 16$) si tratta dei punti di una conica, c.v.d.

Se $h = 6$, scriviamo in quest'ipotesi la condizione (18), mettendo in evidenza soltanto alcuni termini dello sviluppo del determinante come polinomio in λ:

$$\begin{aligned}&\{\lambda, a_1, a_2, a_3, a_4, a_5\}\\ &= \lambda^{63}+\lambda^{60}a_1a_5^2+\ldots+\lambda^{56}(a_1^3a_4^4+a_5^6a_2)+\ldots+\\ &+\lambda^{48}(a_1^7a_3^8+a_1^4a_2a_4^2a_5^2+a_2^3a_4^{12}+a_1a_2^2a_4^4a_5^8+a_1^2a_3^9a_5^4+a_3a_5^{14})+\ldots+\\ &+\lambda^{36}(a_2^{18}a_4^9+a_4^9a_5^{18}+a_3^{27}+a_1a_3^{10}a_5^{16}+a_1^8a_3^{17}a_5^2+a_1^9a_4^{18})+\ldots+\\ &+\lambda^{23}a_2^8a_4^{32}+\lambda^{21}(a_2^{42}+a_4^{42})+\ldots\\ &= \lambda^{63}+1.\end{aligned}$$

Se $a_1 \neq 0$, esprimendo che i coefficienti di λ^{60}, λ^{56}, λ^{48}, λ^{21} sono nulli, si ottengono le condizioni

$$a_5 = 0, \quad a_4 = 0, \quad a_3 = 0, \quad a_2 = 0,$$

di guisa che il diagramma di traslazione si riduce a

$$y = a_1x^2, \quad a_1 \neq 0$$

e dunque ad una conica.

Se $a_1 = 0$, si ottengono le condizioni

$$a_2 = 0, \quad a_3 = 0, \quad a_4 = 0$$

confrontando rispettivamente i coefficienti di λ^{36}, λ^{24}, λ^{21}. Abbiamo quindi

$$y = a_5x^{32}, \quad a_5 \neq 0,$$

e dunque (poiché attualmente $q = 64$) ancora una conica, onde l'asserto.

III. Il caso generale. Nel caso di ovali qualsiansi, non pare agevole di trovare condizioni necessarie e sufficienti seguendo una via analoga a quella esposta nel paragrafo II. Proveremo tuttavia il

TEOREMA 5. *Condizioni necessarie affinché, aggregando i punti all'infinito degli assi x, y al diagramma* (11) *si ottenga un'ovale, son date dal sussistere identico rispetto a λ delle*

$$\text{Circ}(\alpha_{q-1}+\lambda, \alpha_1, \alpha_2, \ldots, \alpha_{q-2}) = \lambda^{q-1}+1, \tag{19}$$

$$\text{Circ}(\alpha_1+\lambda, \alpha_2, \ldots, \alpha_{q-2}, \alpha_{q-1}) = \lambda^{q-1}+1, \tag{20}$$

ove il simbolo $\text{Circ}(\beta_1, \beta_2, \ldots, \beta_t)$ *designa il determinante circolante*

$$\begin{vmatrix} \beta_1 & \beta_2 & \cdots & \beta_t \\ \beta_t & \beta_1 & \cdots & \beta_{t-1} \\ \cdots & \cdots & \cdots & \cdots \\ \beta_2 & \beta_3 & \cdots & \beta_1 \end{vmatrix}.$$

Dimostrazione. Supponiamo all'uopo che, aggregando i punti all'infinito degli assi x, y al diagramma (11), si ottenga un'ovale. Le rette del tipo $y = \lambda$ debbono allora risultare unisecanti il diagramma, vale a dire che l'equazione

$$a_1x+a_2x^2+\ldots+a_{q-1}x^{q-1} = \lambda$$

deve ammettere qualche soluzione x in γ, comunque sia fissato $\lambda \epsilon \gamma$. Analogamente, le rette del tipo $y = \lambda x$, con $\lambda \neq 0$, devon essere bisecanti il diagramma, vale a dire che, $\forall \lambda \epsilon \gamma - \{0\}$, l'equazione

$$a_1x+a_2x^2+\ldots+a_{q-1}x^{q-1} = \lambda x$$

deve ammettere qualche soluzione $x \epsilon \gamma - \{0\}$.

Queste due condizioni si possono evidentemente esprimere dicendo che ciascuna delle equazioni

$$(\alpha_{q-1}+\lambda)+a_1x+a_2x^2+\ldots+a_{q-2}x^{q-2} = 0,$$

$$(a_1+\lambda)+a_2x+a_3x^2+\ldots+a_{q-1}x^{q-2} = 0$$

deve ammettere qualche soluzione $x \neq 0$ in γ, comunque sia fissato $\lambda \neq 0$.

Il teorema risulta allora provato, una volta che si sia stabilito il seguente (per i lemmi 2 e 4, cfr. ad esempio [10]):

LEMMA 4. *L'equazione*

$$\beta_0+\beta_1x+\ldots+\beta_{q-2}x^{q-2} = 0$$

ammette in γ soluzioni $x \neq 0$ se, e soltanto se, risulta

$$\text{Circ}(\beta_0, \beta_1, \ldots, \beta_{q-2}) = 0.$$

Dimostrazione. Supponiamo infatti che l'equazione

$$\beta_0+\beta_1x+\ldots+\beta_{q-2}x^{q-2} = 0$$

ammetta in γ una soluzione $x \neq 0$. Si ha allora

$$\begin{aligned} \beta_0x+\beta_1x^2+\ldots+\beta_{q-2}x^{q-1} &= 0, \\ \beta_0x^2+\beta_1x^3+\ldots+\beta_{q-2}x &= 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ \beta_0x^{q-1}+\beta_1x+\ldots+\beta_{q-2}x^{q-3} &= 0, \end{aligned}$$

cioè

$$\begin{aligned} \beta_0x+\beta_1x^2+\ldots+\beta_{q-2}x^{q-1} &= 0, \\ \beta_{q-2}x+\beta_0x^2+\ldots+\beta_{q-3}x^{q-1} &= 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ \beta_1x+\beta_2x^2+\ldots+\beta_0x^{q-1} &= 0, \end{aligned}$$

d'onde $\text{Circ}(\beta_0, \beta_1, \ldots, \beta_{q-2}) = 0$.

Viceversa, se $\text{Circ}(\beta_0, \beta_1, \ldots, \beta_{q-2}) = 0$, allora esistono in γ soluzioni $x \neq 0$. Supponiamo infatti per assurdo che così non sia, e poniamo

$$y = \beta_0+\beta_1x+\ldots+\beta_{q-2}x^{q-2}.$$

Per ogni $x \neq 0$, risulta allora $y \neq 0$ e

$$\begin{aligned} yx &= \beta_0x+\beta_1x^2+\ldots+\beta_{q-2}x^{q-1}, \\ yx^2 &= \beta_0x^2+\beta_1x^3+\ldots+\beta_{q-2}x, \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ yx^{q-1} &= \beta_0x^{q-1}+\beta_1x+\ldots+\beta_{q-2}x^{q-3}, \end{aligned}$$

cioè

$$\begin{aligned} yx &= \beta_0x+\beta_1x^2+\ldots+\beta_{q-2}x^{q-1}, \\ yx^2 &= \beta_{q-2}x+\beta_0x^2+\ldots+\beta_{q-3}x^{q-1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ yx^{q-1} &= \beta_1x+\beta_2x^2+\ldots+\beta_0x^{q-1}. \end{aligned}$$

Essendo poi $\text{Circ}(\beta_0, \beta_1, \ldots, \beta_{q-2}) = 0$, esistono in γ elementi $\lambda_0, \lambda_1, \ldots, \lambda_{q-2}$ non tutti nulli tali che

$$\begin{aligned} \lambda_0\beta_0+\lambda_1\beta_{q-2}+\ldots+\lambda_{q-2}\beta_1 &= 0, \\ \lambda_0\beta_1+\lambda_1\beta_0+\ldots+\lambda_{q-2}\beta_2 &= 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots & \\ \lambda_0\beta_{q-2}+\lambda_1\beta_{q-3}+\ldots+\lambda_{q-2}\beta_0 &= 0, \end{aligned}$$

dal che

$$\lambda_0yx+\lambda_1yx^2+\ldots\ \lambda_{q-2}yx^{q-1} = 0$$

per ogni $x \in \gamma - \{0\}$. Poiché $y \neq 0$, si ha dunque

$$\lambda_0 x + \lambda_1 x^2 + \ldots + \lambda_{q-2} x^{q-1} = 0$$

per ogni elemento x di $\gamma - \{0\}$, il che è assurdo in quanto le λ sono non tutte nulle e γ è d'ordine q, c.v.d.

Osservazione. Si può constatare che, se $q = 8$, le condizioni (19) e (20) sono anche sufficienti. Lasciamo al Lettore la relativa semplice verifica.

Dal teorema 5 segue il

TEOREMA 6. *Condizioni necessarie affinché, aggregando i punti all'infinito degli assi x, y al diagramma* (11), *si ottenga un'ovale, vengono espresse dalle*

$$a_1 = a_3 = \ldots = a_{q-1} = 0,$$

equivalenti a ciò che, nel secondo membro della (11), *non abbiano a comparire che potenze pari della x.*

Dimostrazione. Supponiamo che il diagramma (11) fornisca nel modo indicato un'ovale, e consideriamo la condizione (20) all'uopo necessaria (teorema 5). In conformità con la dimostrazione del teorema 3, da tale condizione si deduce intanto che, necessariamente, $a_1 = 0$. Inoltre, se (x_0, y_0) è un qualunque punto del diagramma, la traslazione di equazioni

$$X = x + x_0, \qquad Y = y + y_0$$

muta il diagramma (11) in un altro diagramma, di equazione $Y = \varphi(X)$, il quale contiene il punto $X = Y = 0$ e da cui si deduce un'ovale aggregando i punti all'infinito degli assi X, Y. L'equazione $Y = \varphi(X)$ si ottiene dalla

$$y = f(x) = a_1 x + a_2 x^2 + \ldots + a_{q-1} x^{q-1}$$

eliminando x ed y con le precedenti equazioni, ed è quindi

$$Y + y_0 = f(X + x_0).$$

Esprimendo il polinomio $f(X + x_0)$ con lo sviluppo di Taylor, si ha

$$Y + y_0 = f(X + x_0) = f(x_0) + f'(x_0) X + \ldots$$

e quindi

$$Y = \varphi(X) = f'(x_0) X + \ldots$$

Per quanto precedentemente visto, si ha che il coefficiente di X in $\varphi(X)$ dev'essere uguale a zero, ossia

$$f'(x_0) = 0 \qquad (\forall\, x_0 \in \gamma),$$

eppertanto

$$a_1 = a_3 = \ldots = a_{q-1} = 0, \qquad \text{c.v.d.}$$

Si raggiunge lo scopo di determinare condizioni necessarie e sufficienti introducendo, per ogni intero $k \geqslant 0$, i polinomi omogenei

$$\sigma_k(x, x_1, x_2) = \sum_{i + i_1 + i_2 = k} x^i x_1^{i_1} x_2^{i_2}, \tag{21}$$

i quali possono anche venir scritti nella forma

$$\sigma_k(x, x_1, x_2) = \sum_{i=0}^{k} x^i \varrho_{k-i}(x_1, x_2) \tag{22}$$

avendo posto $\varrho_0 = 1$ e (per ogni $k > 0$)

$$\varrho_k(x_1, x_2) = x_1^k + x_1^{k-1} x_2 + \ldots + x_1 x_2^{k-1} + x_2^k = (x_1^{k+1} + x_2^{k+1})/(x_1 + x_2). \tag{23}$$

Tenuto conto del teorema 6, proveremo il

TEOREMA 7. *Considerata in uno spazio affine 3-dimensionale su γ, ove (x, x_1, x_2) rappresentino coordinate affini di punto, la superficie algebrica di equazione*

$$\tau(x, x_1, x_2) = \sum_{k=1}^{(q-2)/2} a_{2k} \sigma_{2k-2}(x, x_1, x_2) = 0, \tag{24}$$

condizione necessaria e sufficiente affinché, aggregando il punto all'infinito dell'asse y al diagramma di equazione

$$y = f(x) = a_2 x^2 + a_4 x^4 + \ldots + a_{q-2} x^{q-2}, \tag{25}$$

si ottenga un $(q+1)$-arco, è che la suddetta superficie non contenga su γ nessun punto al di fuori di quelli che appartengono ad almeno uno dei piani di equazione $x = x_1$, $x = x_2$, $x_1 = x_2$.

Dimostrazione. È evidente che il diagramma (25) fornisce nel modo indicato un $(q+1)$-arco se, e soltanto se, tre suoi punti distinti qualsiansi

$$(x, y), \qquad (x_1, y_1), \qquad (x_2, y_2) \qquad (x \neq x_1, x \neq x_2, x_1 \neq x_2)$$

non risultano allineati. Ciò si esprime con il fatto che l'equazione nelle x, x_1, x_2:

$$(x + x_1)/(x_2 + x_1) = (y + y_1)/(y_2 + y_1) = [f(x) + f(x_1)]/[f(x_2) + f(x_1)]$$

non ammetta soluzioni per cui risulti $x \neq x_1$, $x \neq x_2$, $x_1 \neq x_2$; vale a dire che, nello spazio affine 3-dimensionale su γ ove le (x, x_1, x_2) siano coordinate affini di punto, la superficie algebrica di equazione

$$(x + x_1)[f(x_2) + f(x_1)] + (x_2 + x_1)[f(x) + f(x_1)] = 0$$

non deve avere punti (definiti su γ) che non appartengano ad almeno uno dei piani di equazione $x = x_1$, $x = x_2$, $x_1 = x$.

Il risultato consegue allora da ciò che, tenuto conto della (24), sussiste l'identità:

$$\tau(x, x_1, x_2)$$
$$= \{(x+x_1)[f(x_2)+f(x_1)]+(x_2+x_1)[f(x)+f(x_1)]\}/[(x+x_1)(x+x_2)(x_1+x_2)].$$

Si ha invero

$$\{[f(x)+f(x_1)]/(x+x_1)+[f(x_2)+f(x_1)]/(x_2+x_1)\}/(x+x_2)$$
$$= \sum_{k=1}^{(q-2)/2} a_{2k}[\varrho_{2k-1}(x, x_1)+\varrho_{2k-1}(x_1, x_2)]/(x+x_2)$$
$$= \sum_{k=1}^{(q-2)/2} a_{2k}[x_1^{2k-2}\varrho_0(x, x_2)+x_1^{2k-3}\varrho_1(x, x_2)+\ldots+\varrho_{2k-2}(x, x_2)]$$
$$= \sum_{k=1}^{(q-2)/2} a_{2k}\sigma_{2k-2}(x, x_1, x_2), \quad \text{c.v.d.}$$

Nel caso più semplice in cui la (25) si riduca alla

$$y = x^{k+2}, \quad \text{con} \quad k \equiv 0 (\mathrm{mod}\, 2), \tag{26}$$

supposto che sia $(k+2, q-1) = 1$ (traducente l'univoca risolubilità della (26) rispetto a x), dal teorema 7 si trae agevolmente il

TEOREMA 8. *Dal diagramma* (26) *si ottiene un'ovale aggregando i punti all'infinito degli assi x, y se, e soltanto se, in un piano di Galois su γ ove (x, x_1, x_2) rappresentino coordinate proiettive omogenee di punto, la curva algebrica d'ordine k di equazione*

$$\sigma_k(x, x_1, x_2) = 0 \tag{27}$$

non contiene nessun punto definito su γ, ad eccezione al più del punto unità $U(1, 1, 1)$.

Indicando d'ora in poi con σ_k tanto la curva (27) quanto la forma ternaria (21) o (22), sempre che ciò non dia luogo ad equivoci, stabiliamo il

TEOREMA 9. *Non appena q (e quindi h) sia abbastanza grande rispetto a k, affinché σ_k soddisfi alla condizione specificata nell'ultimo enunciato occorre (ma in generale non basta) che la curva σ_k risulti assolutamente riducibile (e cioè abbia a spezzarsi in un'opportuna estensione algebrica di γ).*

Dimostrazione. Supponiamo che σ_k sia assolutamente irriducibile e proviamo che, se $q \gg k$, allora σ_k contiene necessariamente punti distinti da U.

Denotiamo infatti con ν ($\geqslant 0$) il numero dei punti di σ_k definiti su γ, e con i ($\geqslant 0$) la molteplicità con cui σ_k passa per U. Per il genere g di σ_k risulta allora

$$g \leqslant (k-1)(k-2)/2 - i(i-1)/2 = g_0$$

ed inoltre, stante il teorema di Hasse–Weil (cfr. ad es. [32]),

$$|q+1-\nu| \leqslant 2g\sqrt{q} \leqslant 2g_0\sqrt{q}.$$

Di qui, ove fosse $\nu \leqslant 1$, si trarrebbe

$$q \leqslant 2g_0\sqrt{q},$$

onde

$$q \leqslant (k-1)(k-2)\sqrt{q}$$

e quindi $\sqrt{q} \leqslant k^2$; basta dunque assumere $q > k^4$ per ottenere un assurdo, c.v.d.

La riducibilità assoluta di σ_k ha ad esempio luogo se k è della forma $k = 2^t - 2$, sussistendo allora — come vedremo — l'identità

$$\sigma_k(x, x_1, x_2) = \varrho_k(x+x_1, x+x_2); \tag{28}$$

corrispondentemente, si giunge così per nuova via alle ovali di traslazione segnalate nella Prefazione.

Per provare l'identità (28) basta ricordare che, durante la dimostrazione del teorema 7, abbiamo ottenuto l'identità

$$\varrho_i(x, x_1)+\varrho_i(x_1, x_2) = (x+x_2)\sigma_{i-1}(x, x_1, x_2); \tag{29}$$

per giungere alla (28), ossia alla

$$(x_1+x_2)\sigma_k(x, x_1, x_2) = (x+x_1)^{k+1}+(x+x_2)^{k+1},$$

basta dunque mostrare che

$$\varrho_{k+1}(x, x_1)+\varrho_{k+1}(x, x_2) = (x+x_1)^{k+1}+(x+x_2)^{k+1}.$$

Ora infatti si ha

$$\varrho_{k+1}(x, x_1)+\varrho_{k+1}(x, x_2) = (x^{2^t}+x_1^{2^t})/(x+x_1)+(x^{2^t}+x_2^{2^t})/(x+x_2)$$
$$= (x+x_1)^{2^t-1}+(x+x_2)^{2^t-1}$$
$$= (x+x_1)^{k+1}+(x+x_2)^{k+1},$$

come volevasi dimostrare.

È poi evidente che dalla (28) segue l'asserita riducibilità assoluta di σ_k, questa curva venendosi a spezzare in k rette passanti per U.

Un altro caso di riducibilità si ha per $k = 4$, a norma dell'identità

$$\sigma_4(x, x_1, x_2) = [\sigma_2(x, x_1, x_2)+\varepsilon\sigma_1(x, x_1, x_2)^2][\sigma_2(x, x_1, x_2)+\varepsilon^2\sigma_1(x, x_1, x_2)^2],$$

facilmente dimostrabile, nella quale ε designi una radice cubica primitiva dell'unità ($\varepsilon^2+\varepsilon+1 = 0$).

L'identità precedente mostra poi che la curva σ_4 non ha punti su γ se, e soltanto se, l'equazione $x^2+x+1 = 0$ non ammette radici x in γ, il che equivale a ciò che h sia dispari.

Se ne trae così il

TEOREMA 10. *Per ogni $q = 2^h$, h dispari, aggregando i punti all'infinito degli assi x, y a quelli del diagramma di equazione $y = x^6$ si ottiene un'ovale (la quale, come si vede facilmente, risulta poi di traslazione soltanto nei casi $h = 1$ e $h = 3$).*

IV. Riducibilità e singolarità di polinomi ϱ e di curve σ. Gli sviluppi precedenti suggeriscono parecchi interrogativi, a taluno dei quali daremo ora risposta. I risultati così conseguiti, anche quando non hanno riflessi immediati sul problema delle ovali, presentano interesse in sé da vari punti di vista. Precisamente, vogliamo ora indagare casi di irriducibilità assoluta per σ_k ($k \geqslant 2$), almeno nell'ipotesi che k sia pari, avendo riguardo ai teoremi 8 e 9.

Si osservi al riguardo che, naturalmente, la riducibilità assoluta di σ_k non dà ancora nulla *da sola* sull'inesistenza di punti (su σ_k) diversi da U, ossia (teorema 8) sul fornire $y = x^{k+2}$ un'ovale. La cosa resta chiarita dal seguente esempio: se $k = 2^t - 2$ vale l'identità (28) ed abbiamo già visto che, in tal caso, σ_k risulta assolutamente riducibile. Corrispondentemente, però, il diagramma $y = x^{k+2} = x^{2^t}$ non fornisce un'ovale per ogni valore di t ($\geqslant 2$). Ad esempio, se ε è una radice cubica primitiva dell'unità e $\varepsilon \epsilon \gamma$ (vale a dire $q - 1 \equiv 0 (\mathrm{mod}\, 3)$, ovvero $h \equiv 0 (\mathrm{mod}\, 2)$), i punti

$$U, \quad (\varepsilon, \varepsilon^{2^t}), \quad (\varepsilon^2, \varepsilon^{2^{t+1}})$$

stanno su quel diagramma e sono allineati se si suppone $k = 2^t - 2 \not\equiv 0 (\mathrm{mod}\, 3)$. Si vede subito che σ_k contiene allora i punti $(1, \varepsilon, \varepsilon^2)$ e $(1, \varepsilon^2, \varepsilon)$.

Sui punti che σ_k ammette su γ si può dire che, invertendo in un certo senso il teorema 9, vale il

LEMMA 5. *Se la curva σ_k ammette $\nu > [k^2/4]$ punti su γ ed è irriducibile su γ, allora essa è anche assolutamente irriducibile.*

Per provarlo, basta tenere conto del fatto generale espresso dal

TEOREMA 11. *Se f è una curva piana algebrica d'ordine k, definita su di un qualunque campo, E, e se essa contiene almeno $[k^2/4]+1$ punti su E ed è irriducibile su E, allora f è anche assolutamente irriducibile.*

Dimostrazione. Sia $f(x, y) = 0$ l'equazione di f e si denoti con p l'ideale (primo per ipotesi) generato da $f(x, y)$ in $R = E[x, y]$. Se $\bar{E} \supseteq E$ è la chiusura algebrica di E, possiamo considerare l'ideale p* generato da $f(x, y)$ in $S = \bar{E}[x, y] \supseteq R$.

L'estensione del dominio d'integrità R nel dominio S è un'estensione integrale, e la corrispondente estensione dei campi dei quozienti $\bar{E}(x, y) \supseteq E(x, y)$ è un'estensione algebrica quasi-galoisiana. Valgono dunque le ipotesi di due noti teoremi di Cohen-Seidenberg ([28], Ch. III, A):

gli ideali primi associati a p* sono gli ideali primi di S *sopra* p, tali dunque che la loro intersezione con R è esattamente p.

A norma del II teorema di Cohen-Seidenberg, gli ideali primi sopra p (che rappresentano le componenti irriducibili di f nella chiusura algebrica di E) sono fra loro coniugati rispetto agli automorfismi di $\bar{E}(x, y)$ su $E(x, y)$, cioè rispetto agli automorfismi di $\bar{E}$ su E. Se ne trae che i punti di f definiti su E appartengono a tutte le componenti di f nella chiusura algebrica di E. Supponendo ora f assolutamente riducibile, proviamo che detti punti sarebbero al più in numero di $[k^2/4]$, contrariamente al supposto.

Invero, se f avesse almeno due componenti irriducibili distinte, f' e f'', esse avrebbero lo stesso ordine k', con $0 < k' < k$ e $2k' \leqslant k$, e i punti su E di f, dovendo appartenere a $f' \cap f''$, sarebbero, a norma del teorema di Bézout, al più in numero di $(k')^2 \leqslant [k^2/4]$.

Nel caso che f avesse invece una sola componente irriducibile f' (da contarsi più volte), di ordine k', con $0 < k' < k$ e $2k' \leqslant k$, f' non potrebbe contenere più di $[k^2/4] \geqslant (k')^2$ punti su E in quanto, in caso contrario, sarebbe essa stessa definita su E e f risulterebbe allora già riducibile su E.

Dalla precedente dimostrazione si trae come corollario immediato il

LEMMA 6. *Se f è una curva piana algebrica definita su di un qualunque campo E, e se essa è irriducibile su E, ogni punto di f su E appartiene a ciascuna delle componenti di f nella chiusura algebrica di E.*

Teoremi che esprimono condizioni necessarie e sufficienti per l'irriducibilità assoluta di una curva f (o di una varietà algebrica qualunque) sono ben noti (cfr. ad esempio [13], [33]), ma essi non si basano, come invece il teorema 11, soltanto sullo studio dei punti su E contenuti in f (oltre che sulla irriducibilità di f relativa ad E). Delle numerose siffatte condizioni sufficienti che si potrebbero ricavare ne segnaliamo due, di dimostrazione ormai immediata.

LEMMA 7. *Se f è una curva piana algebrica definita su di un qualunque campo E la quale contenga almeno un punto semplice su E, od un punto multiplo per cui passi con un solo ramo, e se essa è irriducibile su E, allora f è anche assolutamente irriducibile.*

LEMMA 8. *Una curva piana algebrica d'ordine $k \geqslant 2$, definita su di un qualunque campo E, risulta di necessità assolutamente irriducibile nelle ipotesi che essa:*

(i) *abbia in un suo punto P incontro di molteplicità k con una retta la quale conti una sola volta fra le tangenti in P,*

(ii) *non contenga come componente nessuna retta per P.*

Torniamo ora al problema dell'irriducibilità assoluta di σ_k (k pari $\geqslant 2$), tenendo conto in parte delle osservazioni precedenti, ma sviluppando soprattutto un metodo consistente nell'analisi delle singolarità di σ_k.

Stabiliamo anzitutto le *identità* ($\forall\, n \geqslant 1$):

$$\sigma_{2n} = \sigma_n^2 + (xx_1 + xx_2 + x_1x_2)\,\sigma_{n-1}^2, \tag{30}$$

$$\sigma_{2n+1} = \sigma_1\sigma_n^2 + xx_1x_2\sigma_{n-1}^2. \tag{31}$$

Si ha

$$\sigma_{2n} = \sum_{i+i_1+i_2=2n} x^i x_1^{i_1} x_2^{i_2},$$

$$\sigma_n^2 + (xx_1 + xx_2 + x_1x_2)\,\sigma_{n-1}^2 = \sum_{j+j_1+j_2=n} x^{2j} x_1^{2j_1} x_2^{2j_2} + (xx_1 + xx_2 + x_1x_2) \sum_{l+l_1+l_2=n-1} x^{2l} x_1^{2l_1} x_2^{2l_2}.$$

La (30) consegue allora dall'osservare che i monomi

$$x^{2j}x_1^{2j_1}x_2^{2j_2}, \quad x^{2l+1}x_1^{2l_1+1}x_2^{2l_2}, \quad x^{2l+1}x_1^{2l_1}x_2^{2l_2+1}, \quad x^{2l}x_1^{2l_1+1}x_2^{2l_2+1}$$

sono tutti distinti e restituiscono, ciascuno una sola volta, ogni monomio del tipo $x^i x_1^{i_1} x_2^{i_2}$ con $i + i_1 + i_2 = 2n$.

Analogamente si prova la (31).

Le forme σ_k si esprimono inoltre tramite le forme binarie ϱ_i, definite dalla (23), mediante *l'identità*:

$$\sigma_k(x, x_1, x_2) = \sum_{(i)_k} x^{k-i}\,\varrho_i(x + x_1, x + x_2), \tag{32}$$

generalizzante la (28) e da non confondersi con la (22), ove la somma a secondo membro va estesa ai valori di i che si ottengono da k nel modo seguente. Si consideri l'espressione di $k+2$ nella numerazione in base 2: allora $i+2$ ($i \geqslant 0$) assume tutti e soli i valori che da tale espressione si ricavano col sostituirvi qualche cifra 1 (eventualmente nessuna, ma non tutte) con 0.

La (32) si prova facilmente basandosi sulla (29). Si ha infatti:

$$\sigma_k(x, x_1, x_2) = [\varrho_{k+1}(x, x_1) + \varrho_{k+1}(x, x_2)]/(x_1 + x_2)$$
$$= [(x^{k+2} + x_1^{k+2})/(x + x_1) + (x^{k+2} + x_2^{k+2})/(x + x_2)]/(x_1 + x_2);$$

di qui, ponendo $x_1 = x + u$, $x_2 = x + v$ (inversamente $u = x + x_1$, $v = x + x_2$), si trae

$$\sigma_k(x, x+u, x+v) = \sum_{i=0}^{k} \binom{k+2}{i+2} x^{k-i}(u^{i+1} + v^{i+1})/(u + v),$$

cioè

$$\sigma_k(x, x+u, x+v) = \sum_{i=0}^{k} \binom{k+2}{i+2} x^{k-i}\,\varrho_i(u, v), \tag{33}$$

ovvero

$$\sigma_k(x, x_1, x_2) = \sum_{i=0}^{k} \binom{k+2}{i+2} x^{k-i}\,\varrho_i(x + x_1, x + x_2). \tag{34}$$

La (32) consegue ora subito dall'osservare che $\binom{k+2}{i+2}$ risulta dispari se, e soltanto se, $i+2$ si ottiene da $k+2$ nel modo indicato, come si ha dal noto (cfr. [20]):

LEMMA 9. *Se a e j sono numeri naturali soddisfacenti alle $a \geqslant 2$, $0 < j < a$, il coefficiente binomiale $\binom{a}{j}$ è dispari se, e soltanto se, scritto a in base 2, j si ottiene da tale espressione sostituendo qualche cifra 1 con 0.*

La (32) permette intanto di stabilire il

LEMMA 10. *La curva σ_k ($k \geqslant 2$) contiene il punto U se, e soltanto se, $k \equiv 2 \pmod 4$ oppure $k \equiv 3 \pmod 4$. σ_k ha allora in U molteplicità m e cono tangente $\varrho_m(x + x_1, x + x_2) = 0$, ove il polinomio ϱ è dato dalla (23) ed m si determina al modo seguente. Si osservi dapprima che, nei due casi considerati, rispettivamente $4 \mid (k+2)$ oppure $4 \mid (k+1)$: detta 2^l la massima potenza di 2 che divide il numero indicato ($l \geqslant 2$), risulta $m = 2^l - 2$.*

Se ne trae senz'altro il

COROLLARIO. *Se la curva σ_k contiene il punto U, questo è per essa almeno doppio.*

Dimostrazione (del lemma 10). Effettuiamo la trasformazione di coordinate

$$x = x, \quad u = x + x_1, \quad v = x + x_2,$$

che porta il punto U nel punto fondamentale $(1, 0, 0)$.

Dalla (33) si ha

$$\sigma_k(x, x+u, x+v) = \sum_{i=0}^{k} \binom{k+2}{i+2} x^{k-i}\,\varrho_i(u, v),$$

e quindi la molteplicità m di σ_k in U è uguale al minimo valore di i, compreso tra 0 e k, tale che $\binom{k+2}{i+2}$ sia dispari (corrispondentemente, se $m > 0$, il cono tangente in U è $\varrho_m(u, v) = 0$).

Risulta perciò $m = 0$ se, e soltanto se, $\binom{k+2}{2}$ è dispari, ovvero se, e soltanto se, $k \equiv 0 \pmod 4$ oppure $k \equiv 1 \pmod 4$.

Nei casi $k \equiv 2 \pmod 4$ e $k \equiv 3 \pmod 4$, ed in essi soltanto, risulta $m > 0$; nel primo caso, se $2^l \mid (k+2)$ e $2^{l+1} \nmid (k+2)$ ($l \geqslant 2$), $k+2$ si scrive in base 2 nel modo seguente: $k + 2 = \ldots + 1 \cdot 2^l + 0 \cdot 2^{l-1} + \ldots + 0 \cdot 2 + 0 \cdot 1$, di guisa che il minimo m richiesto per i, a norma del lemma 9, si ottiene dalla $m + 2 = 2^l$. Analogamente si procede nel secondo caso.

Stabiliamo ora alcuni lemmi ulteriori, che ci saranno utili nello studio delle singolarità di σ_k nel caso che sia $k \equiv 0 \pmod 4$.

LEMMA 11. *I punti multipli di σ_{2n} sono i punti comuni a σ_n e σ_{n-1} con l'aggiunta, eventualmente, del punto unità U.*

Dimostrazione. A norma dell'identità (30) si ha

$$\sigma_{2n} = \sigma_n^2 + (xx_1 + xx_2 + x_1x_2)\sigma_{n-1}^2,$$

e (poiché γ ha la caratteristica $p = 2$) i punti singolari di σ_{2n} sono allora quelli che soddisfanno al sistema:

$$\sigma_{2n} = 0, \quad (x+x_2)\sigma_{n-1}^2 = 0, \quad (x+x_1)\sigma_{n-1}^2 = 0, \quad (x_1+x_2)\sigma_{n-1}^2 = 0.$$

Escludendo l'eventuale soluzione fornita dal punto unità U, se ne deducono le $\sigma_{2n} = 0$, $\sigma_{n-1} = 0$, equivalenti alle $\sigma_n = 0$, $\sigma_{n-1} = 0$, c.v.d.

LEMMA 12. *Per ogni $k \geqslant 0$, il sistema*

$$\sigma_k = 0, \quad \sigma_{k+1} = 0, \quad \sigma_{k+2} = 0 \tag{35}$$

è assolutamente privo di soluzioni non banali.

Dimostrazione. Poiché il teorema è vero per $k = 0$, possiamo supporre $k > 0$ e procedere per induzione rispetto a k.

Se k è pari, $k = 2h$, si ha, usando (30) e (31):

$$\sigma_{2h} = 0, \quad \sigma_{2h+1} = 0 \Rightarrow [\sigma_1(xx_1 + xx_2 + x_1x_2) + xx_1x_2]\sigma_{h-1}^2 = 0,$$

cioè

$$\sigma_{2h} = 0, \quad \sigma_{2h+1} = 0 \Rightarrow (x+x_2)(x+x_1)(x_1+x_2)\sigma_{h-1}^2 = 0.$$

Ora ad esempio, se $x_1 = x_2$, σ_{2h}, σ_{2h+1} e σ_{2h+2} non hanno punti a comune, in quanto

$$\sigma_{2h}(x, x_1, x_1) = \sum_{i=0}^{2h} x^i \varrho_{2h-i}(x_1, x_1) = \sum_{i=0}^{2h} (i+1)\, x^i x_1^{2h-i},$$

$$\sigma_{2h+1}(x, x_1, x_1) = \sum_{i=0}^{2h+1} ix^i x_1^{2h+1-i} = x\sigma_{2h}(x, x_1, x_1),$$

$$\sigma_{2h+2}(x, x_1, x_1) = \sum_{i=0}^{2h+2} (i+1)\, x^i x_1^{2h+2-i} = x_1^2\sigma_{2h}(x, x_1, x_1) + x^{2h+2}.$$

Ne consegue che

$$\sigma_{2h} = 0, \quad \sigma_{2h+1} = 0, \quad \sigma_{2h+2} = 0 \quad \Rightarrow \quad \sigma_{h-1} = 0.$$

Abbiamo dunque

$$\sigma_{2h} = 0, \quad \sigma_{2h+1} = 0, \quad \sigma_{2h+2} = 0 \Rightarrow \sigma_{h-1} = 0, \quad \sigma_h = 0, \quad \sigma_{h+1} = 0;$$

e, poiché $h < k$, si ha il risultato per l'induzione ammessa.

Analogamente si procede nel caso k dispari.

LEMMA 13. *Le curve σ_{2n} e σ_{2n-1} hanno esattamente $2n(2n-1)$ punti distinti in comune.*

OSSERVAZIONE. *Se k è dispari, σ_k e σ_{k-1} non si incontrano necessariamente in punti distinti, come si può ad esempio verificare direttamente nei casi $k = 3$ e $k = 5$.*

Dimostrazione (del lemma 13). Cominciamo col provare che, se $X(a, a_1, a_2)$ è un punto semplice di σ_{2n}, la retta tangente a σ_{2n} in X è proprio la retta XU (certamente $X \neq U$, a norma del corollario del lemma 10).

Dall'identità (30) si ha infatti intanto:

$$\sigma_{2n} = \sigma_n^2 + (xx_1 + xx_2 + x_1x_2)\sigma_{n-1}^2 = 0.$$

La retta tangente a σ_{2n} in X è quindi la retta di equazione

$$(a_1+a_2)x + (a+a_2)x_1 + (a+a_1)x_2 = 0,$$

poiché risulta $\sigma_{n-1}(a, a_1, a_2) \neq 0$ in quanto $\sigma_{n-1}(a, a_1, a_2) = 0$, $\sigma_{2n}(a, a_1, a_2) = 0 \Rightarrow \sigma_n(a, a_1, a_2) = 0$, eppertanto, qualora si avesse $\sigma_{n-1}(a, a_1, a_2) = 0$, X a norma del lemma 11 sarebbe singolare per σ_{2n}, contrariamente al supposto.

Inoltre, poiché secondo l'identità (31) si ha

$$\sigma_{2n-1} = \sigma_1\sigma_{n-1}^2 + xx_1x_2\sigma_{n-2}^2,$$

la prima polare del punto U rispetto a σ_{2n-1} ha l'equazione

$$\sigma_{n-1}^2 + (xx_1 + xx_2 + x_1x_2)\sigma_{n-2}^2 = \sigma_{2n-2} = 0;$$

e questa curva non contiene alcun punto di $\sigma_{2n} \cap \sigma_{2n-1}$, in virtù del lemma 12.

Proviamo ora che i punti di $\sigma_{2n} \cap \sigma_{2n-1}$, i quali a norma della (30) sono contenuti nella curva σ_{4n}, risultano tutti punti semplici di σ_{2n}.

Dal lemma 11 consegue infatti che un punto multiplo di σ_{2n} o è U — e U non appartiene a σ_{4n}, stante il lemma 10 — oppure è un punto di $\sigma_n \cap \sigma_{n-1}$ e quindi, a norma della (31), appartiene anche alla cubica $xx_1x_2 = 0$ non potendo appartenere a σ_{n-2}, in virtù del lemma 12. Per il nostro intento basta dunque provare che il sistema $\sigma_n = 0$, $\sigma_{n-1} = 0$, $xx_1x_2 = 0$ è assolutamente incompatibile. Se (ad esempio) $(0, \xi_1, \xi_2)$ fosse una sua soluzione non banale, in base alla (22) si vede che si avrebbe $\varrho_n(\xi_1, \xi_2) = 0$ e $\varrho_{n-1}(\xi_1, \xi_2) = 0$; ma ciò è assurdo, in quanto ϱ_n e ϱ_{n-1} non hanno zeri non banali in comune.

Siamo ora in grado di stabilire quanto asserito dal lemma 13. Se in un punto $P \in \sigma_{2n} \cap \sigma_{2n-1}$ le due curve σ_{2n}, σ_{2n-1} avessero molteplicità d'intersezione $\geqslant 2$, allora, essendo P semplice per σ_{2n} e con retta tangente PU, il punto P dovrebbe essere o semplice per σ_{2n-1} con retta tangente PU, oppure multiplo per σ_{2n-1}. In entrambi i casi la prima polare di U rispetto a σ_{2n-1} passerebbe per P, contrariamente a quanto visto poc'anzi.

Dai lemmi 10, 11, 13 si trae agevolmente il

LEMMA 14. *La curva σ_{4n} ammette esattamente $2n(2n-1)$ punti multipli distinti.*

L'analisi delle singolarità di σ_{4n} si completa ora mostrando che *i punti singolari di σ_{4n} sono cuspidi o tacnodi ordinari*, giacché ciascuno di essi

conta esattamente 4 volte nell'intersezione di σ_{4n} con la sua generica prima polare. Basta all'uopo osservare che la prima polare di $Z(z, z_1, z_2)$ rispetto alla curva σ_{4n} ha l'equazione

$$[(z+z_1)(x_1+x_2)+(z_1+z_2)(x+x_1)]\,\sigma_{2n-1}^2 = 0,$$

mentre σ_{4n} ha l'equazione

$$\sigma_{2n}^2+(xx_1+xx_2+x_1x_2)\,\sigma_{2n-1}^2 = 0,$$

e ricordare il lemma 13.

Proviamo ora che i punti singolari di σ_{4n} che non appartengono alla conica di equazione

$$xx_1+xx_2+x_1x_2 = 0 \tag{36}$$

sono di fatto cuspidi, ed anzi cuspidi ordinarie (si noti qui la differenza con il caso $p \neq 2$, nel quale la molteplicità d'intersezione tra la generica prima polare e la curva in una cuspide ordinaria vale esattamente 3; per uno studio approfondito di siffatti problemi nel caso $p = 2$, rimandiamo a [22] e [23]).

Sia P uno di questi punti; introduciamo coordinate proiettive non omogenee di punto x, y tali che:

(i) $P \equiv (0, 0)$,

(ii) PU (che è la retta tangente in P a σ_{2n}) abbia l'equazione $x = 0$,

(iii) la tangente in P a σ_{2n-1} (certamente distinta dalla retta PU) abbia l'equazione $y = 0$.

La conica (36) viene così ad avere un'equazione della forma

$$c^2+(ax+by)+\ldots = 0, \tag{37}$$

ove i puntini stanno a significare termini di grado superiore a quelli scritti.

Nella (37) è certamente $c \neq 0$, poiché per ipotesi il punto P non sta sulla (36). Inoltre, essendo U il nucleo della (36), la retta PU è la polare di P rispetto alla conica, e si ha quindi $b = 0$, $a \neq 0$. Valgono pertanto sviluppi del tipo

$$\sigma_{2n} = x+\ldots, \qquad \sigma_{2n-1} = y+\ldots,$$

sicché, tenendo conto della (30), risulta

$$\sigma_{4n} = \sigma_{2n}^2+(c^2+ax+\ldots)\,\sigma_{2n-1}^2 = x^2+c^2y^2+axy^2+\ldots; \tag{38}$$

e questa prova che σ_{4n} ha in P un punto doppio con un'unica tangente, $x = cy$.

La molteplicità d'intersezione tra la retta tangente e la curva in P vale poi esattamente 3, giacché, sostituendo $x = cy$ nella $\sigma_{4n} = 0$, in virtù della (38) si ha

$$acy^3+\ldots = 0, \qquad \text{con} \qquad ac \neq 0,$$

e quindi P è una cuspide ordinaria per la curva σ_{4n}, c.v.d.

Possiamo allora enunciare il

LEMMA 15. *I $2n(2n-1)$ punti singolari di σ_{4n} sono cuspidi o tacnodi ordinari; i tacnodi sono al più in numero di $2n$.*

Dimostrazione. I punti singolari di σ_{4n} che appartengono alla (36) appartengono anche alla curva σ_n (in virtù della (30)); basta dunque provare che la conica (36) non ha componenti a comune con σ_n. Si vede subito che tale conica è assolutamente irriducibile e contiene i punti fondamentali $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, al contrario di σ_n che, in virtù della (32), non passa per nessuno di questi, c.v.d.

Siamo ormai in grado di provare il

TEOREMA 12. *La curva σ_{4n} è assolutamente irriducibile, per ogni $n \geqslant 2$ (ma non per $n = 1$, come visto alla fine del paragrafo* III).

Dimostrazione. Se la forma σ_{4n} si spezzasse nella chiusura algebrica di γ, $\sigma_{4n} = \sigma'\sigma''$, con σ' e σ'' forme prime tra loro e di gradi rispettivi n', $n'' < 4n$ con $n'+n'' = 4n$, in corrispondenza ad ogni punto comune alle $\sigma' = 0$ e $\sigma'' = 0$ si avrebbe un punto singolare della σ_{4n}, il quale, non potendo essere una cuspide, dovrebbe essere uno dei tacnodi ordinari di cui al lemma 15. Ne conseguirebbe che in ogni loro punto comune le curve $\sigma' = 0$ e $\sigma'' = 0$ si toccherebbero semplicemente, di guisa che $n'n''$ dovrebbe risultare pari e vi sarebbero $n'n''/2$ punti distinti comuni alle curve suddette. A norma del lemma 15 deve quindi aversi $n'n''/2 \leqslant 2n$, cioè $n'n'' \leqslant 4n$, il che è però assurdo se $n \geqslant 2$, c.v.d.

Un'analisi più complessa permette di stabilire l'*irriducibilità assoluta della curva σ_{8n+2}, per ogni $n \geqslant 1$* (mentre σ_2 si spezza in due rette uscenti da U, come si vede applicando la (28) per $t = k = 2$).

Ad esempio, nel caso $n = 1$, si ottiene che i punti singolari di σ_{10} sono i punti

$$\begin{array}{lll} U(1,1,1), & U_1(1,\varepsilon,\varepsilon^2), & U_2(1,\varepsilon^2,\varepsilon), \\ V(\varepsilon,1,1), & V_1(1,\varepsilon,1), & V_2(1,1,\varepsilon), \\ W(\varepsilon^2,1,1), & W_1(1,\varepsilon^2,1), & W_2(1,1,\varepsilon^2), \end{array}$$

ove ε denoti una radice cubica primitiva dell'unità. Essi sono tali che ciascuna delle rette congiungenti due punti scritti in righe diverse contiene un punto della riga rimanente. Poiché σ_{10} ammette U_1 e U_2 come punti 4-pli, avendo in ognuno di essi un'unica tangente, data dalla retta $\sigma_1 = U_1U_2$ che ha incontro 5-punto con σ_{10} tanto in U_1 quanto in U_2, così un eventuale spezzamento di σ_{10} potrebbe aver luogo soltanto in due quintiche, passanti l'una per U_1 (con molteplicità 4) ma non per U_2, l'altra per U_2 (con molteplicità 4) ma non per U_1, e contenenti ognuna ciascuno dei punti V, V_1, V_2, W, W_1, W_2. Ora ciò è impossibile, in base agli allineamenti dei punti suddetti, onde l'asserto.

L'analisi suaccennata può venire semplificata nel caso che n sia una potenza del 2 ad esponente dispari, $n = 2^a$, $a \equiv 1 (\mathrm{mod}\, 2)$, $a \geqslant 1$.

In tal caso, infatti, usufruendo del lemma 10 mostreremo che la curva σ_{2n+2} passa per il punto U con molteplicità 2, avendo ivi le tangenti distinte UU_1, UU_2, ciascuna delle quali ha ivi con essa incontro k-punto; l'asserita irriducibilità assoluta consegue allora dal lemma 8.

Invero, essendo $k = 2^{a+3}+2$, la (32) porge:

$$\sigma_k = x^{k-2}\varrho_2(x+x_1, x+x_2)+x^4\varrho_{k-4}(x+x_1, x+x_2)+\varrho_k(x+x_1, x+x_2),$$

di guisa che U è doppio per σ_k con la coppia di tangenti distinte $\varrho_2(x+x_1, x+x_2) = 0$, cioè $x+x_1 = \varepsilon(x+x_2)$, $x+x_1 = \varepsilon^2(x+x_2)$.

La prima retta, ad esempio, ha contatto k-punto con σ_k in U, giacché

$$\varrho_{k-4}\big(\varepsilon(x+x_2), x+x_2\big) = 0. \tag{39}$$

Infatti la (39) equivale alla $\varepsilon^{k-3} = 1$, ovvero alla $k = 2^{a+3}+2 \equiv 0 (\mathrm{mod}\, 3)$; e quest'ultima relazione è soddisfatta se (e soltanto se) l'esponente a è dispari.

Altri criteri di irriducibilità assoluta possono venire stabiliti poggiando ancora sul predetto lemma.

Così, ad esempio, si prova il

Teorema 13. *Se k è della forma $k = 2^a+2^b-2$ $(1 < a < b)$, la curva σ_k risulta assolutamente irriducibile qualora sia $(a, b) > 1$, oppure se, essendo $(a, b) = 1$, si supponga $b \geqslant a+2$ e σ_k irriducibile su γ (si può pensare, per esempio, $\gamma = Z_2$).*

Dimostrazione. Osserviamo intanto che, nelle ipotesi attuali, k è del tipo $k = 4r+2$, con r dispari se $a > 2$ $(r = 2^{a-2}+2^{b-2}-1)$, di guisa che il caso in esame non è compreso in quelli precedenti.

Poniamo $\alpha = 2^a-2$, $\beta = 2^b-2$ $(k = \alpha+\beta+2)$. A norma della (32) si ha allora

$$\sigma_k = x^{k-\alpha}\varrho_\alpha(x+x_1, x+x_2)+x^{k-\beta}\varrho_\beta(x+x_1, x+x_2)+\varrho_k(x+x_1, x+x_2) \qquad (0 < \alpha < \beta < k).$$

In tutti i casi, U risulta di molteplicità α per σ_k ed il cono tangente in U, di equazione $\varrho_\alpha(x+x_1, x+x_2) = 0$, consta di α rette distinte (poiché α è pari). Inoltre, nessuna retta passante per U è componente di σ_k, poiché ϱ_α, ϱ_β, ϱ_k non hanno zeri non banali in comune (infatti i polinomi $x^\lambda-1$ e $x^\mu-1$ hanno radici diverse da 1 in comune se, e soltanto se, $(\lambda, \mu) > 1$; ed ora risulta $(\alpha+1, \beta+1, k+1) = 1$, in quanto $k = (\alpha+1)+(\beta+1)$).

Nel caso che sia $(a, b) > 1$, una almeno tra le rette tangenti a σ_k in U, per la quale dunque $\varrho_\alpha(x+x_1, x+x_2) = 0$, soddisfa anche l'equazione

$$\varrho_\beta(x+x_1, x+x_2) = 0,$$

poiché attualmente

$$(\alpha+1, \beta+1) > 1 \Leftrightarrow (a, b) > 1.$$

Detta retta ammette allora con σ_k in U incontro k-punto, e l'asserto discende dal lemma 8.

Nel caso che sia $(a, b) = 1$, supponiamo $b \geqslant a+2$ e ϱ_k irriducibile su γ, il che implica l'irriducibilità di σ_k relativa a γ. Se la curva σ_k si spezzasse nella chiusura algebrica di γ,

$$\sigma_k = \sigma'_{k'}+\sigma''_{k''} \qquad (k'+k'' = k;\ k', k'' < k)$$

dal lemma 6 avremmo che σ', $\sigma'' \ni U$. Indicando con s' la molteplicità di U per σ' e con s'' la molteplicità di U per σ'', risulterà $s'+s'' = \alpha$, $0 < s', s''$. Siano poi l' una qualunque tangente a σ' in U ed i' $(s' < i' \leqslant k')$ la molteplicità di intersezione di l' con σ' in U; significato analogo abbiano l'' ed i'' $(s'' < i'' \leqslant k'')$ relativamente a σ''. Per quanto precedentemente osservato, l' sarà tangente a σ_k in U e non tangente a σ'' in U, di guisa che la sua molteplicità d'intersezione con σ_k in U sarà esattamente $i'+s'' = \beta$ (in quanto $(a, b) = 1$, tale molteplicità non può infatti valere k). Analogamente si stabilisce la $i''+s' = \beta$.

Si ha allora

$$k = k'+k'' \geqslant i'+i'' = 2\beta-(s'+s'') = 2\beta-\alpha,$$

cioè

$$\alpha+\beta+2 \geqslant 2\beta-\alpha \Rightarrow \beta \leqslant 2\alpha+2;$$

ma l'ultima relazione è assurda se $b \geqslant a+2$, c.v.d.

Nell'enunciato del teorema 13 compare come ipotesi l'irriducibilità della forma ϱ_k relativamente al campo base γ. È facile trovare condizioni necessarie e sufficienti affinchè ciò accada. Si ha precisamente che, considerato più in generale un campo finito $\gamma = \mathrm{GF}(q)$ di caratteristica p qualsiasi, e posto poi

$$\begin{aligned}\varrho_k(x_1, x_2) &= x_1^k+x_1^{k-1}x_2+\ldots+x_1x_2^{k-1}+x_2^k \\ &= (x_1^{k+1}-x_2^{k+1})/(x_1-x_2),\end{aligned} \tag{40}$$

vale il

Teorema 14. *Condizione necessaria e sufficiente affinché la forma binaria ϱ_k $(k \geqslant 2)$ sia irriducibile su γ, è che valgano le:*

$$(k+1, p) = 1, \tag{41}$$

$$(k+1, q^i-1) = 1 \qquad (i = 1, 2, \ldots, [k/2]). \tag{42}$$

Ove queste relazioni siano soddisfatte, la (42) sussiste di conseguenza per $i = [k/2]+1, \ldots, k-1$, ma non per $i = k$, e $k+1$ risulta primo.

Dimostrazione. $\varrho_k(x_1, x_2)$ è irriducibile su γ se, e soltanto se, è irriducibile su γ il polinomio

$$\tau_k(x) = x^k+x^{k-1}+\ldots+x+1 = (x^{k+1}-1)/(x-1). \tag{43}$$

È evidente allora la necessità della (41), in quanto, se p dividesse $k+1$, risulterebbe

$$x^{k+1}-1 = [x^{(k+1)/p}-1]^p.$$

Supposto dunque $p\nmid(k+1)$, di guisa che il polinomio $x^{k+1}-1$ non ha radici multiple e $\tau_k(x)$ ha come radici le k radici $(k+1)$-esime dell'unità diverse da 1, si ha che $\tau_k(x)$ è irriducibile su γ se, e soltanto se, non contiene radici in nessuna delle estensioni

$$\gamma_q \subset \gamma_{q^2} \subset \ldots \subset \gamma_{q^{k-1}}$$

(mentre le contiene invece tutte in γ_{q^k}); cioè se, e soltanto se, valgono le

$$(k+1, q^i-1) = 1 \qquad (i = 1, 2, \ldots, k-1) \tag{44}$$

(esprimenti che nel gruppo moltiplicativo di γ_{q^i} non esistano elementi che abbiano per periodo un divisore di $k+1$).

Poiché, se esiste un fattore proprio di $\tau_k(x)$ su γ, ne esiste certamente qualcuno di grado al più $[k/2]$, è evidente che basta che le (44) sussistano soltanto per i valori di i da 1 fino a $[k/2]$, d'onde la conclusione.

Il fatto che $k+1$ è allora necessariamente primo, consegue dall'osservare che tale condizione è, come ben noto, necessaria e sufficiente per l'irriducibilità del polinomio (43) sul campo $\boldsymbol{Q}$ dei numeri razionali (o sull'anello $\boldsymbol{Z}$ dei numeri interi).

Bibliografia

[1] A. Barlotti, *Un'osservazione intorno a un teorema di B. Segre sui q-archi*, Le Matematiche 21 (1966), pag. 23–29.

[2] — *Sulle 2-curve nei piani grafici*, Rend. Sem. Mat. Univ. Padova, 37 (1967), pag. 91–97.

[3] U. Bartocci, *Una nuova classe di ovali proiettive finite*, Rend. Accad. Naz. Lincei, (8), 43 (1967), pag. 312–316.

[4] — *Ancora su di una nuova classe di ovali proiettive finite*, Rend. di Mat., (VI) 1 (1968), pag. 118–125.

[5] F. Buekenhout, *Étude intrinsèque des ovales*, Rend. Mat. e Appl., (V) 25 (1966), pag. 333–393.

[6] P. V. Ceccherini, *Su certi $\{k, n\}$-archi dedotti da curve piane, e sulle $\{k, n\}$-calotte di tipo $(0, n)$ di un $S_{r,q}$ $(r \geqslant 2)$*, Rend. di Mat., (VI) 2 (1969), pag. 185–196.

[7] A. Cossu, *Su alcune proprietà dei $\{k, n\}$-archi di un piano proiettivo sopra un corpo finito*, Rend. di Mat. e Appl., (V) 20 (1961), pag. 271–277.

[8] P. Dembowski, *Finite geometries*, Ergebn. der Math., (44), Springer-Verlag 1968.

[9] R. H. F. Denniston, *Some maximal arcs in finite projective planes*, J. Combinat. Theory 6 (1969), pag. 317–319.

[10] L. E. Dickson, *Linear groups*, Leipzig 1901.

[11] B. d'Orgeval, *Sur certains $\{k, 3\}$-arcs en géometrie de Galois*, Acad. Roy. Bélgique Bull. Cl. Sci., (V) 46 (1960), pag. 597–603.

[12] N. Krier, *Ovals in infinite spaces*, Proc. of the Projective Geometry Conf., Chicago (1967), pag. 87–90.

[13] S. Lang, *An introduction to algebraic geometry*, Interscience 1958.

[14] G. E. Martin, *On arcs in a finite projective plane*, Canad. J. Math. 13 (1967), pag. 376–393.

[15] G. Menichetti, *Sopra i k-archi completi nel piano grafico di traslazione di ordine 9*, Le Matematiche, 21 (1966), pag. 150–156.

[16] G. Rodriguez, *Un esempio di ovale che non è una quasi-conica*, Boll. Un. Mat. Ital. 14 (1959), pag. 500–503.

[17] M. Sce, *Preliminari ad una teoria aritmetico-gruppale dei k-archi*, Rend. di Mat. e Appl., (V) 19 (1960), pag. 241–291.

[18] — L. Lunolli, *k-archi completi nei piani proiettivi desarguesiani di rango 8 e 16*, Politecnico di Milano, Centro di calcoli numerici, (1958), pag. 1–11.

[19] — — *Considerazioni aritmetiche e risultati sperimentali sui $\{k, n\}_q$-archi*, Ist. Lombardo Acc. Sc., (A) 98 (1964), pag. 3–52.

[20] B. Segre, *Sui sistemi di forme quadratiche nel campo reale*, Comm. Math. Helv. (28) (1954), pag. 288–300.

[21] — *Ovals in a finite projective plane*, Canad. J. Math. 7 (1955), pag. 414–416.

[22] — *Intorno alla geometria sopra un campo di caratteristica due*, Rev. Fac. Sc. Univ. Istanbul, (A) 2 (1956), pag. 97–123.

[23] — *Intorno alla geometria sopra un corpo di caratteristica $p \neq 0$, con particolare riguardo al caso $p = 2$*, Roma, Ist. Mat. dell'Univ. (1957).

[24] — *On Galois geometries*, Proc. Intern. Congr. Math. (1958), Cambridge 1960, pag. 488–499.

[25] — *Lectures on modern geometry* (with an Appendix by Lucio Lombardo-Radice), Roma 1961.

[26] — *Ovali e curve σ nei piani di Galois di caratteristica due*, Rend. Accad. Naz. Lincei, (8) 32 (1962), pag. 785–790.

[27] — *Introduction to Galois geometries*, Memorie Accad. Naz. Lincei (VIII), vol. VIII, 5 (1967).

[28] J. P. Serre, *Algèbre locale — Multiplicités*, Lecture Notes in Math., Springer-Verlag 1965.

[29] J. Tits, *Les groupes simples de Suzuki et de Ree*, Seminaire Bourbaki, N. 210 (1960–1961).

[30] — *Ovoides à translations*, Rend. Mat. e Appl. 21 (1962), pag. 37–59.

[31] — *Ovoides et groupes de Suzuki*, Archiv. der Math. 13 (1962), pag. 187–198.

[32] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Paris 1948.

[33] O. Zariski, P. Samuel, *Commutative algebra*, II, Princeton 1960.

Reçu le 6. 5. 1970