Bollettino
Unione Matematica Italiana

Luigi Antonio Rosati

# L'equazione delle 27 rette della superficie cubica generale in un corpo finito. Nota II.

*Bollettino dell'Unione Matematica Italiana, Serie 3*, Vol. **13** (1958), n.1, p. 84–99.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1958_3_13_1_84_0>

# L'equazione delle 27 rette della superficie cubica generale in un corpo finito.

Nota II di LUIGI ANTONIO ROSATI (a Firenze)

**Sunto.** - *Si conclude un lavoro iniziato nel numero precedente di questo Bollettino.*

**Summary.** - *We conclude a paper begun in anhoter part of this Bulletin.*

Nella prima parte di questo lavoro (1), dopo aver dimostrato che in un campo di GALOIS di caratteristica dispari, $GF(q)$, l'equazione (1) delle 27 rette della superficie cubica generale $F$ è riducibile, abbiamo utilizzato convenienti rappresentazioni piane della $F$ per scomporre la (1) in equazioni irriducibili in $GF(q)$. Inoltre abbiamo dato alcuni teoremi atti a escludere certe scomposizioni della (1) a priori ritenute possibili.

In questa seconda parte si classificano i modi in cui la (1) può spezzarsi in equazioni irriducibili, e si riesce a mostrare la possibilità di realizzare quasi tutti i casi possibili.

TEOREMA 12. – *Se la* (1) *possiede una componente irriducibile di terzo grado, o le tre rette da questa determinate sono complanari oppure sono sghembe due a due*; *in questo caso le componenti irriducibili della* (1) *hanno per grado un divisore di 6.*

Consideriamo una terna, $T_1$, di rette della $F$, due a due sghembe, determinate da un'equazione di terzo grado a coefficienti in $GF(q)$; a queste tre rette si appoggiano le rette due a due sghembe di un'altra terna, $T_2$, determinate da un'equazione razionale in $GF(q)$. A due rette qualsiasi di $T_1$ si appoggiano 5 rette della $F$, quindi altre due oltre quelle di $T_2$. In tutto le rette della $F$, distinte da quelle di $T_2$, che si appoggiano alle tre coppie di rette di $T_1$ sono 6 (perchè nessuna di queste si può appoggiare a tutte e tre le rette di $T_1$, che sono incidenti soltanto alle tre rette di $T_2$), e

(1) La nota I è stata pubblicata in questo Bollettino, serie III, anno XII (1957) n. 4, pp. 612-626.
La numerazione della nota II prosegue quella della nota I.

queste 6 rette sono determinate da una equazione di sesto grado razionale in $GF(q)$. Analogamente le rette di $F$, distinte da quelle di $T_1$, che si appoggiano alle coppie di rette di $T_2$ sono 6, distinte dalle precedenti, e anche queste sono determinate da un'equazione di sesto grado razionale in $GF(q)$.

Supponiamo che una di queste due equazioni di sesto grado abbia una componente razionale lineare; allora alle due rette $r_1$, $r_2$ di $T_1$ o di $T_2$ alle quali si appoggia la retta, $r_3$, individuata da quella equazione si appoggiano quattro rette della $F$ sghembe due a due determinate da un'equazione di quarto grado a coefficienti in $GF(q)$ ($r_3$ e le tre rette di $T_2$ o di $T_1$). Siccome a quattro rette della $F$ se ne appoggiano altre due, e non più, e, se le quattro hanno un'equazione razionale in $GF(q)$, lo stesso accade anche per le due, la $r_1$ e la $r_2$, sghembe fra loro, avranno un'equazione razionale in $GF(q)$. Tenuto conto del teorema 3 e del n° 2, si vede che tutti i fattori irriducibili della (1) hanno per grado un divisore di 6.

Lo stesso accade evidentemente nel caso che una delle due equazioni di sesto grado abbia una componente razionale di secondo grado che determina due rette sghembe.

Consideriamo invece il caso che una delle due equazioni di sesto grado abbia una componente razionale in $GF(q)$ di secondo grado, che determina due rette complanari. Il piano che le contiene entrambe taglia la $F$ secondo una retta appartenente a $GF(q)$ e che coincide con quella retta, necessariamente appartenente a $T_2$, dato che la terna $T_1$ è irriducibile, che le taglia entrambe. Allora le altre due rette di $T_2$, sghembe fra loro, hanno una equazione razionale in $GF(q)$ e quindi ancora si ha che tutti i fattori irriducibili della (1) hanno per grado un divisore di 6.

Supponiamo infine che entrambe le equazioni siano irriducibili o, essendo (almeno) una di esse riducibile, questa si spezzi in due fattori irriducibili di terzo grado. Allora in $GF(q^6)$ la $F$ possiede le rette di $T_1$ e quelle di $T_2$ e le 12 rette determinate dalle due equazioni di sesto grado considerate. In tutto 18 rette e quindi [5] la $F$ possiede 27 rette in $GF(q^6)$ e ancora in questo caso è dimostrato che ogni componente irriducibile della (1) ha per grado un divisore di 6.

La prima parte dell'enunciato del teorema deriva immediatamente dal teorema 2.

TEOREMA 13. - *La* (1) *non può spezzarsi:* a) *in tre equazioni lineari e tre equazioni irriducibili di grado 8;* b) *in una equazione lineare, una equazione irriducibile di grado 2 e sei equazioni irri-*

*ducibili di grado 4*; c) *in tre equazioni lineari, sei equazioni irriducibili di grado 2, tre equazioni irriducibili di grado 4*; d) *in tre equazioni lineari, due equazioni irriducibili di grado 2, cinque equazioni irriducibili di grado 4.*

Supponiamo per assurdo che la (1) si spezzi nel modo $a$). Allora tenuto conto del teorema 3 e del n° 2, le tre equazioni lineari determinano tre rette complanari, $a$, $b$, $c$; mentre una componente della (1) di grado 8 determina rette che si appoggiano alla stessa retta razionale della $F$. Consideriamo una delle tre componenti di grado 8 e sia $a$ la retta a cui si appoggiano le rette da essa determinate, che indicheremo con 1, 2, ..., 8. Il gruppo di GALOIS, $G$, di questa equazione è ciclico di ordine 8 e transitivo [3]. Sia $g$ un elemento di $G$ di ordine massimo; possiamo supporre che esso porti 1 in 2, 2 in 3, ..., 7 in 8, 8 in 1, e che quindi le rette di ciascuna di queste otto coppie siano fra di loro sghembe. Saranno invece incidenti 1 e 5, 2 e 6, 3 e 7, 4 e 8.

Consideriamo poi le 16 quaterne di rette due a due sghembe che si possono formare con le rette 1, 2, ..., 8. Tenuto conto che a quattro rette della $F$ due a due sghembe se ne appoggiano altre due sghembe fra loro, alle quattro rette di ciascuna di queste quaterne si appoggerà una retta della $F$ distinta da $a$; e questa, non potendosi appoggiare ad $a$, si appoggerà a sua volta o alla retta $b$ o alla retta $c$. Quindi ad ognuna delle suddette quaterne si può associare nel modo anzidetto o la retta $b$ o la retta $c$. Per effetto di $g$ si ha:

$$1234 \rightarrow 2345 \rightarrow 3456 \rightarrow 4567 \rightarrow 5678 \rightarrow 6781 \rightarrow 7812 \rightarrow 8123 \rightarrow 1234;$$

$$1274 \rightarrow 2385 \rightarrow 3416 \rightarrow 4527 \rightarrow 5638 \rightarrow 6741 \rightarrow 7852 \rightarrow 8163 \rightarrow 1274.$$

Sia poi $r$ la retta distinta da $a$ che si appoggia ad 1234 ed $r$ si appoggi a $b$; allora la retta associata a 1234 è $b$. Invece la retta associata a 2345 è $c$. Infatti la retta che si appoggia a 2345 e diversa da $a$, essendo 1 e 5 complanari, è distinta da $r$ (che si appoggia a 1234); chiamiamo $s$ questa retta. Quindi, se la retta associata a 2345 fosse $b$, le quattro rette $234b$ due a due sghembe sarebbero incontrate, oltre che da $a$, anche da $r$ e da $s$ e questo è impossibile. Così alle quaterne che si ottengono da 1234 per mezzo di potenze dispari di $g$ sarà associata la retta $c$, mentre alle quaterne che si ottengono da 1234 per mezzo di potenze pari di $g$ sarà associata la retta $b$. Consideriamo poi la quaterna 1274. Siccome alla quaterna 1234 è associata la retta $b$, a questa sarà associata la retta $c$; e quindi alle quaterne che si ottengono da 1274 per mezzo di potenze dispari di $g$ sarà associata la retta $b$,

mentre alle quaterne che si ottengono da 1274 per mezzo di potenze pari di $g$ sarà associata la retta $c$.

In definitiva gli elementi di $G$ di ordine 8 dovrebbero scambiare fra di loro le rette $b$ e $c$ e queste pertanto, contrariamente all'ipotesi fatta, non potrebbero essere razionali, perchè se lo fossero, dovrebbero essere lasciate ferme da tutti gli elementi di $G$. Rimane così dimostrato che la (1) non può spezzarsi nel modo $a$).

Supponiamo ora per assurdo che la (1) possa spezzarsi nel modo $b$). Sia $a$ la retta razionale della $F$; la componente di secondo grado della (1) determina due rette complanari (se fossero sghembe la (1) si dovrebbe scomporre secondo il n° 2) e quindi incidenti all'unica retta razionale della $F$, $a$. Chiamiamo $b$ e $c$ queste due rette. Le rimanenti otto rette della $F$ che si appoggiano alla $a$ saranno determinate da due componenti di quarto grado della (1). Chiamiamo 1, 2, 3, 4 e 5, 6, 7, 8 le otto rette determinate da queste due equazioni. I gruppi di GALOIS di queste sono ciclici di ordine 4 [3], e quindi isomorfi. Li identificheremo in un gruppo che chiameremo $G$ e potremo supporre che, detto $g$ un elemento di $G$ di ordine 4, $g$ porti 1 in 2, 2 in 3, 3 in 4, 4 in 1 e inoltre 5 in 6, 6 in 7, 7 in 8, 8 in 5 e che quindi 1 e 2, 2 e 3, ... siano sghembe fra loro. Saranno invece incidenti 1 e 3, 2 e 4, 5 e 7, 6 e 8 perchè, se per esempio 1 e 3 fossero sghembe, lo sarebbero anche 2 e 4 e tenuto conto che anche 1 e 2, 1 e 4 sono sghembe fra loro, le quattro rette 1234 sarebbero due a due sghembe. Allora, poichè a quattro rette della $F$ sghembe due a due e determinate da un'equazione razionale se ne appoggiano due anch'esse determinate da un'equazione razionale, le quattro rette 1234 sarebbero incontrate, oltre che da $a$, da un'altra retta razionale della $F$, contro il supposto.

Per effetto di $g$ si ha:

$$1256 \rightarrow 2367 \rightarrow 3478 \rightarrow 4185 \rightarrow 1256;$$
$$1258 \rightarrow 2365 \rightarrow 3476 \rightarrow 4187 \rightarrow 1258;$$
$$1276 \rightarrow 2387 \rightarrow 3458 \rightarrow 4165 \rightarrow 1276;$$
$$1278 \rightarrow 2385 \rightarrow 3456 \rightarrow 4167 \rightarrow 1278.$$

Come sopra, a ciascuna di queste quaterne si può associare o la retta $b$ o la retta $c$. Si vede allora facilmente che alle quaterne di ogni ciclo è associata la stessa retta, che risulta quindi trasformata in se stessa dagli elementi di $G$. Pertanto contrariamente al supposto, le rette $b$ e $c$ risultano razionali e risulta dimostrato che la (1) non può spezzarsi nel modo $b$).

Supponiamo infine che la (1) possa spezzarsi in uno dei modi *c*) o *d*). Siano $a$, $b$, $c$ le tre rette razionali della $F$. Esse sono complanari e ad ognuna di esse si appoggiano 8 rette della $F$ distinte dalle altre due, di cui 4, per il teorema 10, sono determinate da un'equazione irriducibile di quarto grado, mentre quindi le altre 4 sono determinate da due equazioni di secondo grado o da un'altra equazione irriducibile di quarto grado . Siano $r$ e $r_1$, $s$ e $s_1$ 4 rette determinate da due equazioni irriducibili di secondo grado e appoggiate alla stessa retta razionale, $a$; 1234 le quattro rette appoggiate alla $a$ e determinate da un'equazione irriducibile di quarto grado. $r$ e $r_1$ sono complanari, così $s$ e $s_1$; mentre si può supporre che siano sghembe 1 e 2, 2 e 3, 3 e 4, 4 e 1 e siano invece incidenti 1 e 3, 2 e 4. Sia $G$ il gruppo di GALOIS dell'equazione delle quattro rette 1234 e $g$ un elemento di $G$ di ordine 4 che porti 1 in 2, 2 in 3, 3 in 4, 4 in 1. Esso porterà anche $r$ in $r_1$ e $s$ in $s_1$. Consideriamo le quaterne di rette due a due sghembe che si possono formare con le rette appoggiate alla $a$. Per effetto di $g$ si ha:

$$r\,s\,12 \rightarrow r_1s_1 23 \rightarrow r\,s\,34 \rightarrow r_1s_1 41 \rightarrow r\,s\,12\,;$$
$$r\,s_1 12 \rightarrow r_1 s\,23 \rightarrow r\,s_1 34 \rightarrow r_1 s\,41 \rightarrow r\,s_1 12\,;$$
$$r_1 s\,12 \rightarrow r\,s_1 23 \rightarrow r_1 s\,34 \rightarrow r\,s_1 41 \rightarrow r_1 s\,12\,;$$
$$r_1 s_1 12 \rightarrow r\,s\,23 \rightarrow r_1 s_1 34 \rightarrow r\,s\,41 \rightarrow r_1 s_1 12\,.$$

A ciascuna di queste quaterne si può associare o la retta $b$ o la retta $c$, e si vede facilmente che alle quaterne di ognuno dei quattro cicli vengono associate alternativamente le rette $b$ e $c$. Quindi gli elementi di $G$ di ordine 4 scambiano fra di loro le rette $b$ e $c$ che, contrariamente all'ipotesi non possono essere perciò razionali. Dunque la (1) non può spezzarsi neanche nei modi *c*) e *d*) e il teorema è completamente dimostrato.

THEOREMA 14. – *L'equazione* (1) *non possiede componenti irriducibili di grado superiore a 12.*

Cominciamo col dimostrare che la (1) non possiede componenti irriducibili di grado 13. Infatti la (1) non può avere due componenti irriducibili di grado 13 perchè allora avrebbe anche una componente lineare e in questo caso, per il teorema 9, le componenti irriducibili della (1) avrebbero grado inferiore a 10. Inoltre la (1) non può avere neanche soltanto una componente irriducibile di grado 13 perchè, se questo fosse possibile, in una conveniente estensione di $GF(q)$ la $F$ conterrebbe soltanto le 14 rette della superficie cubica determinate dalle rimanenti componenti irriducibili dell'equazione (1) e questo non è possibile [5].

Siccome poi l'equazione (1) non possiede componenti irriducibili di grado 7 e 11 (teoremi 6 e 7), non possiede neanche componenti irriducibili di grado 14 o 21 o 22 perchè una equazione di grado 14 o 21 o 22, irriducibile in $GF(q)$, in $GF(q^2)$ o in $GF(q^3)$ si spezza in due o tre equazioni irriducibili di grado 7 o 11.

La (1) non possiede componenti irriducibili di grado 15 perchè allora in $GF(q^3)$ avrebbe almeno tre componenti irriducibili di grado 5 e quindi, secondo il teorema 4, la (1) in $GF(q^3)$ si dovrebbe scomporre in 5 equazioni irriducibili di quinto grado e in due equazioni lineari, cioè in $GF(q)$ la (1) si dovrebbe scomporre in una equazione irriducibile di grado 15, due equazioni irriducibili di grado 5 e in due equazioni lineari, contro il teorema 4.

La (1) non possiede neanche componenti irriducibili di grado $g = 16$, 17, 19. 23, perchè, se questo fosse, in una conveniente estensione di $GF(q)$ di grado non multiplo di $g$ potrebbero essere risolte tutte le rimanenti componenti irriducibili della (1) e in questa estensione la $F$ conterrebbe $27 - g$ rette, cioè o 11 o 10 o 8 o 4 rette, e questo è impossibile [5].

La (1) non possiede componenti irriducibili di grado 18. Infatti, se la (1) possiede in $GF(q)$ una componente irriducibile di grado 18, allora in $GF(q^2)$ la (1) possiede almeno due componenti irriducibili di grado 9 e quindi per il teorema 11 in $GF(q^2)$ la (1) si decompone in tre componenti irriducibili di grado 9. Perciò in $GF(q)$ la (1) si decompone in una componente irriducibile di grado 18 e in una componente irriducibile di grado 9, e questo per il teorema 11 è assurdo.

La (1) non possiede componenti irriducibili di grado 20 perchè, se questo fosse possibile, la (1) avrebbe in una estensione quadratica due componenti irriducibili di grado 10, contro il teorema 8.

La (1) non possiede componenti irriducibili di grado 24, perchè se questo fosse, la (1) dovrebbe contenere, oltre la componente di grado 24, anche una componente irriducibile di grado 3, e in $GF(q^3)$ la (1) si spezzerebbe in 3 equazioni lineari e in 3 equazioni irriducibili di grado 8, contro il teorema 13. Il teorema è così completamente dimostrato.

TEOREMA 15. – *Se la* F *non contiene nessuna retta in* GF(q) *e il grado di una componente irriducibile della* (1) *è 3 ogni altra componente irriducibile della* (1) *ha per grado un multiplo di 3.*

Supponiamo che la (1) non abbia componenti razionali lineari e abbia una componente irriducibile di terzo grado. Allora la (1) non ha componenti irriducibili di secondo grado: infatti se una

componente di secondo grado determinasse due rette complanari, la $F$ conterrebbe in $GF(q)$ la retta intersezione col piano che contiene queste due rette; se invece determinasse due rette sghembe, tenuto conto del teorema 3 e del n. 2, si avrebbe ancora in $GF(q)$ almeno una retta della $F$. Di conseguenza la (1) non ha neanche componenti irriducibili di quarto grado, perchè, se avesse una componente irriducibile di quarto grado, non avendo componenti irriducibili di secondo grado, in $GF(q^2)$ avrebbe componenti irriducibili di secondo e terzo grado, senza avere componenti lineari.

Tenuto conto dei teoremi 4, 6, 7, 8, 11, 14, risulta completamente dimostrato il teorema.

TEOREMA 16. - *Se la* (1) *ha una componente irriducibile di grado 8, allora essa ha tre componenti irriducibili di grado 8, una componente lineare, una componente irriducibile di secondo grado.*

Se la (1) ha una componente irriducibile di grado 8, allora tenuto conto dei teoremi 4, 6, 7, 14, la (1) non ha componenti di grado dispari diverso da 1 o da 3. D'altra parte il numero delle rette della $F$ è dispari; perciò la (1) avrà una componente irriducibile di grado 1 o 3; tenuto conto del teorema 15 si può concludere che la (1) ha una componente lineare. Sia $r$ la retta determinata da questa equazione. Per il teorema 9 l'equazione delle 10 rette che si appoggiano alla $r$ avrà una componente di grado 8 e quindi una componente, non necessariamente irriducibile, di grado 2, e tutte le componenti irriducibili della (1) avranno per grado un divisore di 8. Allora in $GF(q^4)$ la $F$ possiede $27 - 8a$ rette, essendo $a > 0$ il numero delle componenti della (1) irriducibili e di grado 8. Tenuto conto dei valori del numero delle rette della $F$, si ha $a = 3$ e per il teorema 13 il teorema è dimostrato.

TEOREMA 17. - *Se la* (1) *ha una componente irriducibile di grado 4, o tutte le componenti irriducibili della* (1) *hanno per grado un divisore di 4, oppure la* (1) *si spezza in una equazione lineare, in due equazioni irriducibili di quarto grado, in una di sesto e in una di dodicesimo.*

Con ragionamenti analoghi a quelli fatti nella dimostrazione del teorema precedente si prova che, se la (1) ha una componente irriducibile di grado 4, essa ha anche una componente lineare e quindi per il teorema 9 ogni sua componente irriducibile ha un grado non superiore a 8. L'equazione delle 10 rette che si appoggiano a quella determinata dalla componente lineare della (1)

avrà una componente irriducibile di grado multiplo di 4, e quindi per il teorema 16, di grado 4. Se questa equazione non ha componenti di grado multiplo di 3, allora, tenuto conto del teorema 9, ogni componente irriducibile della (1) ha per grado un divisore di 4. Se invece l'equazione delle 10 rette ha una componente di grado multiplo di 3, il grado di ogni componente irriducibile della (1) risulta per il teorema 9 un divisore di 12, e in $GF(q^4)$ la $F$ contiene almeno 5 rette. Poichè è necessaria una estensione di terzo ordine di $GF(q^4)$ perchè tutte le rette della $F$ risultino razionali, tenuto conto del teorema 3 e del n. 2, la $F$ possiede in $GF(q^4)$ 9 rette e una retta in $GF(q^2)$. cioè possiede in $GF(q)$ una componente lineare e due (e due sole) componenti irriducibili di grado 4. Di conseguenza in $GF(q^6)$ la $F$ possiede o 7 o 19 rette e quindi 7 [5]. In $GF(q^3)$ la $F$ possiede solo una retta, perchè, se anche in $GF(q^3)$ contenesse 7 rette, tutte le rette della $F$ apparterrebbero a $GF(q^6)$ (teorema 3 e n. 2). Allora in $GF(q)$ la (1) si spezza in una equazione lineare, due equazioni irriducibili di grado 4, una equazione irriducibile di grado 6, un'equazione irriducibile di grado 12 e il teorema è dimostrato.

TEOREMA 18. - *L'equazione delle 27 rette della superficie cubica di equazione*

$$z(x^2 - 2y^2) + y^2t + z^2t + 2xt^2 + 2yt^2 + 2zt^2 + t^3 = 0$$

*si spezza in* GF($5^h$) (h *dispari*) *in una equazione lineare, una equazione irriducibile di grado 2 e tre equazioni irriducibili di grado 8, e in* GF($5^{2h}$) (h *dispari*) *in tre equazioni lineari e sei equazioni irriducibili di grado 4.*

In un campo di GALOIS di caratteristica dispari, $GF(q)$, consideriamo la superficie cubica, $F_1$, di equazione:

$$(3) \qquad z(x^2 - ly^2) + a_{22}y^2t + a_{33}z^2t + 2a_{12}xyt + 2a_{14}xt^2 + \\ + 2a_{24}yt^2 + 2a_{34}zt^2 + a_{44}t^3 = 0$$

(a questa forma si può ricondurre l'equazione di ogni superficie cubica generale di $GF(q)$ che in $GF(q^2)$ contenga tre rette complanari [2]), e supponiamo che $l$ in $GF(q)$ non sia un quadrato. $F_1$ contiene allora in $GF(q)$ la retta $r$ di equazioni $z = t = 0$, mentre altre due rette di $F_1$, $s$ e $t$, appartenenti a $GF(q^2)$, sono determinate dalle equazioni $x^2 - ly^2 = 0$, $t = 0$.

Un piano per la retta $r$, di equazione $z = kt$, taglia $F_1$, fuori

di $r$, in una conica che risulta degenere se

$$(4) \qquad la_{33}k^4 + (2la_{34} - a_{22}a_{33})k^3 + (la_{44} + a_{12}^2a_{33} - 2a_{22}a_{34})k^2 +$$

$$+ (a_{24}^2 + 2a_{12}^2a_{34} - a_{22}a_{44} - la_{14}^2)k + a_{14}^2a_{22} + a_{12}^2a_{44} - 2a_{12}a_{14}a_{24} = 0.$$

Supponiamo ora che la $F_1$ non contenga punti multipli in nessuna estensione di $GF(q)$ e che la (4) sia irriducibile in $GF(q)$. Allora l'equazione delle 27 rette della $F_1$ si spezza in $GF(q)$ in una equazione lineare, una equazione irriducibile di grado 2, tre equazioni irriducibili di grado 8, e quindi in $GF(q^2)$ in tre equazioni lineari e sei equazioni irriducibili di grado 4. Infatti le otto rette appoggiate alla $r$ e distinte da $s$ e da $t$ si ottengono risolvendo la (4) che fornisce i quattro piani contenenti queste 8 rette, e successivamente 4 equazioni di secondo grado a coefficienti in $GF(q^4)$. Ora, se queste equazioni di secondo grado risultassero tutte riducibili in $GF(q^4)$, la $F_1$ conterrebbe almeno una retta in $GF(q)$, almeno tre rette in $GF(q^2)$, 27 rette in $GF(q^4)$ e le otto rette appoggiate alla $r$ e distinte da $s$ e da $t$ sarebbero determinate da due equazioni irriducibili di quarto grado. Di più ciascuna di queste due equazioni dovrebbe fornire quattro rette due a due sghembe. Siano $a_1$, $a_2$, $a_3$, $a_4$ quattro tali rette. Siccome a quattro rette di $F_1$ due a due sghembe ne sono appoggiate altre due sghembe fra loro, la $F_1$ dovrebbe contenere in $GF(q)$ due rette appoggiate ad $a_1$, $a_2$, $a_3$, $a_4$, cioè, oltre ad $r$, una retta sghemba con essa e l'equazione delle 27 rette della $F_1$, per il teorema 3 ed il n° 2, dovrebbe spezzarsi in 5 equazioni lineari, una equazione irriducibile di secondo grado, 5 equazioni irriducibili di quarto grado. La $F_1$ conterrebbe allora 5 rette razionali e quindi [5] una di queste dovrebbe essere incidente alle altre quattro distribuite in due coppie di rette incidenti. Allora, presa una qualsiasi delle rette razionali (per esempio $r$) di $F_1$, almeno un piano per essa dovrebbe contenere altre due rette razionali di $F_1$, contrariamente all'ipotesi che $l$ non sia un quadrato in $GF(q)$ e che l'equazione (4) sia irriducibile in $GF(q)$. Di conseguenza non tutte le rette della $F_1$ saranno contenute in $GF(q^4)$, ma saranno invece tutte contenute in $GF(q^8)$ (teorema 9). L'equazione delle 27 rette di $F_1$ avrà dunque in $GF(q)$ una componente irriducibile di grado 8 e in $GF(q)$ per il teorema 16 essa si spezzerà in una equazione lineare, una equazione irriducibile di secondo grado, tre equazioni irriducibili di ottavo grado.

Facciamo ora $q = 5^h$ ($h$ dispari). In $GF(5)$ 2 non è un quadrato e quindi, per il teorema I, non lo è neanche in $GF(5^h)$ ($h$ dispari). Nella (3) poniamo poi $l = 2$, $a_{12} = 0$, $a_{ij} = 1 (ij \neq 12)$. La (3) e la (4)

diventano rispettivamente

$$z(x^2 - 2y^2) + y^2t + z^2t + 2xt^2 + 2yt^2 + 2zt^2 + t^3 = 0 \tag{5}$$

$$2k^4 + 3k^3 - 2k + 1 = 0. \tag{6}$$

Moltiplicando la (6) per 3 si ha

$$k^4 - k^3 - k + 3 = 0. \tag{7}$$

Ebbene la (7) è irriducibile in $GF(5)$. Infatti essa non ha nessuna radice in $GF(5)$; d'altra parte, posto

$$k^4 - k^3 - k + 3 = 0 = (k^2 + Ak + B)(k^2 + ak + b) =$$
$$= k^4 + (A + a)k^3 + (Aa + B + b)k^2 + (Ab + aB)k + Bb,$$

si ottiene il seguente sistema

$$A + a = -1,\ Aa + B + b = 0,\ Ab + aB = -1,\ Bb = 3. \tag{8}$$

Dall'ultima equazione, tenuto conto della simmetria del sistema, si ottiene $b = 1$, $B = 3$ oppure $b = 2$, $B = 4$.

Per $b = 1$, $B = 3$ si ha $A + a = -1$, $Aa = 1$, $A + 3a = -1$. Dalla prima e dalla terza di queste tre equazioni si ricava $a = 0$, $A = -1$ e questa soluzione non soddisfa la seconda equazione.

Per $b = 2$, $B = 4$ si ha $A + a = -1$, $Aa = -1$, $A + 2a = 2$. Dalla prima e dalla terza di queste equazioni si ricava $a = 3$, $A = 1$ e questa soluzione non soddisfa la seconda equazione. Il sistema (8) risulta dunque impossibile e la (7) è irriducibile in $GF(5)$. Essa sarà quindi irriducibile anche in $GF(5^h)$ ($h$ dispari) (se fosse riducibile in $GF(5^h)$, per il teorema I in $GF(5^{2h})$ avrebbe almeno una radice, contrariamente allo stesso teorema I).

Per dimostrare che la superficie cubica (5) non ha singolarità in nessuna estensione di $GF(5^h)$ consideriamo il sistema che le determina

$$2xz + 2t^2 = 0,\ -4yz + 2yt + 2t^2 = 0, \tag{9}$$
$$x^2 - 2y^2 + 2zt + 2t^2 = 0,\ y^2 + z^2 + 4xt + 4yt + 4zt + 3t^2 = 0.$$

Si vede subito che tale sistema non ha soluzioni non banali per $z = t = 0$, cioè non esistono punti singolari della superficie sulla sua retta $z = t = 0$. Un eventuale punto singolare della superficie sul piano $t = 0$ dovrebbe essere il punto comune alle due rette di equazioni complessive $x^2 - 2y^2 = 0$, $t = 0$, cioè il punto $(0, 0, 1, 0)$, le cui coordinate non soddisfano il sistema (9). Si può allora porre

$t = 1$ e il sistema (9), con ovvie semplificazioni, diventa

$$xz + 1 = 0,\ 2yz - y - 1 = 0,\ x^2 - 2y^2 + 2z + 2 = 0,$$
$$y^2 + z^2 + 4x + 4y + 4z + 3 = 0.$$

Eliminando $x$ ed $y$ fra le prime tre equazioni di questo sistema si ottiene

$$3z^5 - z^3 + 4z^2 - 4z + 1 = 0. \tag{10}$$

Le soluzioni $z_i$ di questa equazione forniscono i piani $z = z_i t$ sui quali possono trovarsi i punti singolari della superficie (5), a ciascuno dei quali, trovandosi fuori della retta $z = t = 0$, dovrebbero corrispondere due rette della superficie diverse dalla retta $z = t = 0$. Quindi una soluzione $z_i$ della (10) alla quale corrisponde un punto singolare dovrebbe soddisfare anche la (7) e il primo membro della (7), essendo irriducibile nel campo di GALOIS $GF(5)$ che contiene i coefficienti della (7) e della (10) dovrebbe dividere il primo membro della (10). Siccome questo non è, rimane dimostrato che la nostra superficie è priva di singolarità in qualunque estensione di $GF(5^h)$.

Tenuto conto di quanto già visto risulta allora che l'equazione delle 27 rette della superficie cubica di equazione (5) si spezza in $GF(5^h)$ in una equazione lineare, una equazione irriducibile di grado 2, tre equazioni irriducibili di grado 8, e in $GF(5^{2h})$ in tre equazioni lineari e sei equazioni irriducibili di grado 4. Il teorema è così completamente dimostrato.

TEOREMA 19. - *In* GF($7^h$) (h *dispari non divisibile per* 3) *l'equazione delle 27 rette della superficie cubica* $F_2$ *di equazione*

$$2xyz + x^2t + y^2t - z^2t + 3xt^2 + yt^2 - t^3 = 0 \tag{11}$$

*si spezza in tre equazioni lineari, tre equazioni irriducibili di grado 2, tre equazioni irriducibili di grado 6.*

La $F_2$ contiene le tre rette complanari $x = t = 0$, $y = t = 0$, $z = t = 0$ che chiameremo rispettivamente $r$, $s$, $t$. Un piano passante per la retta $r$, di equazione $z = kt$ taglia ulteriormente $F_2$ in una conica che risulta degenere se $k^4 - 2k = 0$, cioè se $k = 0$ oppure se

$$k^3 - 2 = 0. \tag{12}$$

Per $k = 0$ si ottiene una conica degenere che taglia la $r$ nei due punti $x^2 + y^2 = z = t = 0$. Ora l'equazione $x^2 + y^2 = 0$ è irriducibile in $GF(7)$; sarà perciò irriducibile anche in $GF(7^h)$ ($h$ è dispari).

Dunque $F_2$ possiede due rette complanari, $m$, $n$, determinate da un'equazione di secondo grado irriducibile in $GF(7^h)$.

L'equazione (12) non possiede radici in $GF(7)$; è quindi irriducibile in $GF(7)$ e perciò, essendo $(h, 3) = 1$, è irriducibile anche in $GF(7^h)$. Di conseguenza le rette della $F_2$ appoggiate alla $r$ e contenute nei tre piani determinati dalla (12) sono determinate o da un'equazione di sesto grado irriducibile in $GF(7^h)$ o da due equazioni di terzo grado irriducibili in $GF(7^h)$.

Per dimostrare che la $F_2$ non ha singolarità in nessuna estensione di $GF(7^h)$ consideriamo il sistema che le determina

$$(13) \qquad \begin{gathered} 2yz + 2xt + 3t^2 = 0,\ 2xz + 2yt + t^2 = 0, \\ 2xy - 2zt = 0,\ x^2 + y^2 - z^2 + 6xt + 2yt - 3t^2 = 0. \end{gathered}$$

Si vede subito che questo sistema non ha soluzioni (non banali) per $t = 0$. Perciò la $F_2$ non ha singolarità sul piano $t = 0$ e quindi neanche sulla retta $r$; allora un punto singolare di $F_2$ o sarà sul piano $z = 0$ o su un piano di equazione $z = kt$, essendo $k$ una radice della (12) e nel sistema (13) si potrà porre $t = 1$. Esso allora con ovvie semplificazioni diventerà

$$(14) \qquad \begin{gathered} yz + x - 2 = 0,\ xz + y - 3 = 0,\ xy - z = 0, \\ x^2 + y^2 - z^2 + 6x + 2y - 3 = 0. \end{gathered}$$

Per $z = 0$ dalle prime due equazioni del sistema (14) si ottiene $x = 2$, $y = 3$, mentre la terna (2, 3, 0) non soddisfa la terza equazione. Perciò la $F_2$ non ha singolarità sul piano $z = 0$.

Eliminando $x$ ed $y$ fra le prime tre equazioni del sistema (14) si ha l'equazione

$$(15) \qquad z^5 - 2z^3 + z^2 + 1 = 0.$$

Le soluzioni $z_i$ di questa equazione forniscono i piani $z = z_i t$ sui quali possono trovarsi i punti singolari della $F_2$; quindi una soluzione $z_i$ della (15) alla quale corrisponde un punto singolare di $F_2$ dovrà soddisfare anche la (12), e il primo membro di questa, essendo irriducibile nel campo di GALOIS $GF(7)$ che contiene i coefficienti della (12) e della (15), dovrebbe dividere il primo membro della (15). Siccome questo non è, rimane dimostrato che la $F_2$ è priva di singolarità in qualunque estensione di $GF(7^h)$. Allora, poichè sei rette di $F_2$ appoggiate alla $r$ sono determinate o da una equazione irriducibile di sesto grado o da due equazioni irriducibili di terzo grado, per il teorema 9 anche alla $s$ e alla $t$ saranno appoggiate sei rette determinate da un'equazione irriducibile di sesto grado o da due equazioni irriducibili di terzo grado. Supponiamo che

tre rette, $a$, $b$, $c$, appoggiate a una delle tre rette $r$, $s$, $t$ siano determinate da un'equazione irriducibile di grado 3. $a$, $b$, $c$ ammettono tre trasversali comuni determinate da un'equazione di terzo grado a coefficienti in $GF(7^h)$ e quindi le due trasversali (sghembe fra loro) diverse dalla retta razionale a cui si appoggiano $a$, $b$, $c$ saranno determinate da un'equazione di secondo grado a coefficienti in $GF(7^h)$. Pertanto la $F_2$ si può rappresentare su un piano $\alpha$ sopra $GF(7^h)$ per mezzo di un sistema lineare di quartiche passanti semplicemente per cinque punti 1, 2, 3, 4, 5 formanti un gruppo razionale e doppiamente per altri due punti 6, 7 anch'essi formanti un gruppo razionale, e tenuto conto che le due rette di $F_2$ $m$ e $n$ sono determinate da un'equazione irriducibile di secondo grado e altre tre da un'equazione irriducibile di terzo grado, i gruppi dei punti base si dovranno spezzare in gruppi irriducibili tali che due di essi contengano rispettivamente due e tre punti. D'altra parte $F_2$ possiede almeno tre rette razionali quindi per lo spezzamento dei gruppi dei punti base si avrà (1, 2)(3, 4, 5)(6)(7) oppure (1)(2)(3, 4, 5)(6, 7). In questa maniera le uniche tre rette di $F_2$ appartenenti a $GF(7^h)$ sarebbero sghembe a due a due, mentre in realtà $F_2$ possiede tre rette complanari appartenenti a $GF(7^h)$. Pertanto l'equazione delle 27 rette di $F_2$ non ha componenti di terzo grado irriducibili in $GF(7^h)$ che determinino rette appoggiate a $r$, o $s$, o $t$ e avrà di conseguenza tre componenti di sesto grado irriducibili in $GF(7^h)$ che determinano ciascuna sei rette appoggiate a $r$, o $s$, o $t$. Allora le rette di $F_2$ in $GF(7^h)$ non sono più di tre (se fossero più di tre l'equazione delle 27 rette di $F_2$ non avrebbe componenti irriducibili di grado 6) e perciò, tenuto conto che a ogni retta razionale di $F_2$ se ne appoggiano altre 10 determinate da un'equazione razionale di grado 10, l'equazione delle 27 rette di $F_2$ avrà tre componenti irriducibili di grado 2. Pertanto, come si voleva dimostrare, in $GF(7^h)$ ($h$ dispari e primo con 3) l'equazione delle 27 rette di $F_2$ si spezza in tre equazioni lineari, tre equazioni irriducibili di grado 2 e tre equazioni irriducibili di grado 6.

TEOREMA 20. – *L'equazione* (1) *o si spezza in uno dei modi considerati nel n° 2 e nei teoremi 18 e 19, oppure per i gradi delle sue componenti irriducibili si hanno le seguenti possibilità:*

*a*) 1, 4, 4, 6, 12;

*b*) 9, 9, 9;

*c*) 3, 12, 12.

Nel caso che la $F$ contenga in $GF(q)$ due rette sghembe, per il teorema 3 la (1) si spezza in $GF(q)$ secondo il n° 2. Lo stesso

accade, per i teoremi 4 e 8, quando la (1) ha una componente irriducibile di grado 5 o 10.

Ci limiteremo dunque a vedere come si può spezzare la (1) quando essa non ha componenti irriducibili di grado 5 o 10 (allora, tenuto conto dei teoremi 6, 7, 14, gli unici divisori primi dei gradi delle componenti irriducibili della (1) sono 2 e 3) e inoltre:

I - $F$ contiene qualche retta in $GF(q)$, ma nessuna coppia di rette sghembe (cioè le rette della $F$ in $GF(q)$ sono una o tre complanari); oppure:

II - $F$ non contiene nessuna retta in $GF(q)$.

Consideriamo il primo di questi due casi. Per il teorema 9 la (1) possiede almeno una componente di grado non superiore a 8.

Se possiede una componente di grado 8, per il teorema 16 i gradi delle componenti irriducibili della (1) sono 1, 2, 8, 8, 8 (per la scomposizione della (1) in equazioni irriducibili di tali gradi vedi teorema 18).

Se possiede una componente di grado 4, per il teorema 17 i gradi delle sue componenti irriducibili sono 1, 4, 4, 6, 12 oppure tutte le sue componenti irriducibili hanno per grado un divisore di 4. In questo caso, siccome $27 \equiv 3 \pmod 4$, in $GF(q^2)$ la $F$ contiene o 3 o 7 o 15 rette. Se in $GF(q^2)$ la $F$ contiene 3 rette, allora, tenuto conto del teorema 13, i gradi delle componenti irriducibili della (1) in $GF(q)$ sono 1, 1, 1, 4, 4, 4, 4, 4, 4 (v. teorema 18). Se in $GF(q^2)$ la $F$ contiene 7 rette, allora i gradi delle componenti irriducibili della (1) sono 1, 2, 2, 2, 4, 4, 4, 4, 4 (v. n° 3) (Per il teorema 13 i gradi delle componenti irriducibili della (1) non possono essere 1, 1, 1, 2, 2, 4, 4, 4, 4, 4). La $F$ non può contenere 15 rette in $GF(q^2)$. Infatti per il teorema 13 si può escludere che i gradi delle componenti irriducibili della (1) siano 1, 1, 1, 2, 2, 2, 2, 2, 2, 4, 4, 4, e d'altra parte non possono essere neanche 1, 2, 2, 2, 2, 2, 2, 2, 4, 4, 4 perchè le 14 rette determinate dalle 7 componenti di secondo grado non possono certamente essere tutte incidenti alla retta determinata dalla componente lineare. Quindi una componente di secondo grado della (1) dovrebbe determinare due rette sghembe e, tenuto conto del teorema 3, dal n° 2 si ricava che questo non è possibile.

La (1) non contenga componenti irriducibili di grado 8 o 4 e contenga almeno una componente irriducibile di grado 6 o 3. Considerata una retta, $r$, della $F$ appartenente a $GF(q)$, l'equazione delle 10 rette che vi si appoggiano, per il teorema 9, ha o due componenti di grado 3 o una componente di grado 6, e poichè tale equazione non ha componenti di grado 4, quattro rette della $F$ appoggiate alla $r$ sono determinate da equazioni di primo o secondo

grado irriducibili in $GF(q)$. Perciò la $F$ in $GF(q^2)$ contiene almeno 5 rette di cui certo due sono sghembe e, per il teorema 3, in $GF(q^2)$ la (1) si spezza in uno dei modi indicati nel n° 2; poichè la (1) ha in $GF(q)$ una componente di grado 6 o 3, in $GF(q^2)$ la (1) avrà una componente di grado 3. Di conseguenza, tenuto conto del n° 2, in $GF(q^2)$ la $F$ possiede 9 rette e le componenti irriducibili della (1) che determinano in $GF(q)$ le 18 rette rimanenti sono di grado 3 o 6. Secondo che le componenti di grado 6 sono 3, 2, 1, 0 e le componenti lineari 1 o 3, per i gradi delle componenti della (1) irriducibili in $GF(q)$ si hanno le seguenti possibilità:

1) 1, 2, 2, 2, 2, 6, 6, 6; 2) 1, 1, 1, 2, 2, 2, 6, 6, 6;

3) 1, 2, 2, 2, 2, 3, 3, 6, 6; 4) 1, 1, 1, 2, 2, 2, 3, 3, 6, 6;

5) 1, 2, 2, 2, 2, 3, 3, 3, 3, 6; 6) 1, 1, 1, 2, 2, 2, 3, 3, 3, 3, 6;

7) 1, 2, 2, 2, 2, 3, 3, 3, 3, 3, 3; 8) 1, 1, 1, 2, 2, 2, 3, 3, 3, 3, 3, 3.

Si possono subito scartare le possibilità 5), 7), 8) perche in questi casi in $GF(q^3)$ sulla $F$ si avrebbero rispettivamente 13, 19, 21 rette. Si può anche scartare la possibilità 1) perchè ovviamente l'equazione delle 10 rette appoggiate alla retta razionale, $s$, che in questo caso si troverebbe sulla $F$ dovrebbe contenere una componente di sesto grado. Quindi due delle componenti di secondo grado non determinerebbero rette appoggiate alla $s$, ma ciascuna determinerebbe due rette sghembe, e questo, tenuto conto del teorema 3 e del n° 2 è impossibile. Così la possibilità 4) può essere scartata perchè in questo caso in $GF(q^3)$ la (1) si scomporrebbe in 9 equazioni lineari e in 9 equazioni irriducibili di secondo grado e ciò non è possibile (tale scomposizione non si trova fra quelle del n° 2). Tenuto conto che i casi 3) e 6) sono già stati considerati nel n° 2, rimane possibile il caso 2) (v. teorema 19).

Se infine la (1) non contiene componenti irriducibili di grado o 8 o 4 o 6 o 3, le sue componenti irriducibili avranno, tenuto conto del teorema 10, grado 1 o 2. Ripetendo il ragionamento fatto per escludere che la (1) si possa spezzare in componenti irriducibili di gradi rispettivi 1, 2, 2, 2, 2, 2, 2, 2, 4, 4, 4, si può escludere che la (1) contenga una sola componente lineare. Le componenti lineari saranno perciò 3 e i gradi delle componenti irriducibili della (1) saranno 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2 (v. n° 2).

Consideriamo il caso che la $F$ non contenga rette in $GF(q)$. Siccome il numero delle rette della $F$ è dispari, la (1) avrà una componente di grado dispari che sarà pertanto o 3 o 9. Se questa componente ha grado 9, allora per il teorema 11 la (1) si spezza in 3 equazioni irriducibili di grado 9. Se questa ha grado 3, per

i teoremi 11, 14, 15, le altre componenti irriducibili hanno grado o 3 o 6 o 12. Inoltre in $GF(q^3)$ la $F$ deve possedere o 3 o 15 o 27 rette (non ne può contenere 9 perchè, come abbiamo già visto, in questo caso sarebbe necessaria un'estensione di terzo grado di $GF(q^3)$ per determinare le rimanenti rette, mentre la (1) non ha componenti irriducibili di grado 9, e, se possiede 15 rette in $GF(q^3)$, ne possiede 27 in $GF(q^6)$ (teorema 3 e n° 2); perciò le componenti irriducibili di terzo grado della (1) saranno o 1 o 5 o 9 e per i gradi delle componenti irriducibili della (1) si avranno le seguenti possibilità:

1) 3, 12, 12; 2) 3, 6, 6, 12; 3) 3, 6, 6, 6, 6;
4) 3, 3, 3, 3, 3, 6, 6; 5) 3, 3, 3, 3, 3, 3, 3, 3, 3.

Di queste la 3), la 4), la 5) sono già state realizzate nel n° 2, mentre la 2) non è realizzabile, perche se lo fosse, la (1) in $GF(q^3)$ si scomporrebbe in 3 equazioni lineari, 6 equazioni irriducibili di grado 2, 3 equazioni irriducibili di grado 4, contro il teorema 13. Rimane dunque la possibilità 1).

Dai risultati dell'analisi fatta risulta dimostrato il teorema.

Da questo teorema, dai teoremi 18 e 19 e dal n° 2 risulta che, data una superficie cubica generale $F$ definita in $GF(q)$, il grado della minima estensione di $GF(q)$ nella quale la $F$ possiede 27 rette non supera mai 12.

D'altra parte, se $F$ contiene in $GF(Q)$ 27 rette, ivi contiene $Q^2 + 7Q + 1$ punti [2]; ne viene quindi che il grado della minima estensione di $GF(q)$, $GF(Q)$, nella quale $F$ possiede $Q^2 + 7Q + 1$ punti non supera mai 12. Questo migliora un risultato ottenuto in [2].

## BIBLIOGRAFIA

[1] E. Bertini, *Contribuzione alla teoria delle 27 rette e dei 45 piani tritangenti di una superficie del 3° ordine*, « Annali di Matematica », vol. XII, s. II, (1883), pp. 301-346.

[2] L. A. Rosati, *Sul numero dei punti di una superficie cubica in uno spazio lineare finito*, « Boll. U. M. I. », 1956, Serie III, Anno XI, n° 3, pp. 412-418.

[3] U. Scarpis, *Intorno all'interpretazione della Teoria di Galois in un campo di razionalità finito*, « Annali di Matematica », vol. XXIII, s. III, (1914).

[4] G. Scorza, *Corpi numerici e algebre*, Principato, Messina, 1921.

[5] B. Segre, *Le rette delle superficie cubiche nei corpi commutativi*, « Boll. U. M. I. », 1949, Serie III, anno IV, n° 3, pp. 223-228.