BOLLETTINO UNIONE MATEMATICA ITALIANA

LUIGI ANTONIO ROSATI

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

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. 12
(1957), n.4, p. 612–626.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1957_3_12_4_612_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)*

SIMAI & UMI

<http://www.bdim.eu/>

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

Nota I di LUIGI ANTONIO ROSATI (a Firenze)

Sunto. - *Si dimostra che in un corpo finito l'equazione delle 27 rette e l'equazione dei 45 piani tritangenti di una superficie cubica sono riducibili e si classificano i modi in cui l'equazione delle 27 rette può spezzarsi in equazioni irriducibili. Si realizzano anche quasi tutti i casi dimostrati possibili.*

Summary. - *It is shown that in a finite field the equation of the 27 lines and the equation of the 45 planes tritangents of a cubic surface are reducible and the various manners in which the equation of the 27 lines can be decomposed in irreducible equations are classified. Almost all the possibilities are realised.*

B. SEGRE [5] ha determinato i vari casi che può presentare la configurazione delle rette di una superficie cubica generale, F , in qualunque corpo commutativo, γ , di caratteristica dispari. Fra l'altro ha riconosciuto che la determinazione delle rette della F dipende dalla risoluzione di un'equazione di grado 27 e che la F , in una opportuna estensione di γ , contiene precisamente 27 rette, aventi fra loro le proprietà di incidenza ben note nel campo complesso.

In questo lavoro si studia l'equazione delle 27 rette della F in un corpo finito, $GF(q)$, di caratteristica dispari; si fa vedere che essa e l'equazione dei 45 piani tritangenti alla F sono sempre riducibili e si classificano i modi in cui tale equazione può spezzarsi in componenti irriducibili in $GF(q)$. Si riconosce precisamente che per i gradi delle componenti irriducibili dell'equazione delle 27 rette della F si hanno le seguenti possibilità:

- 1) 1, 1, ..., 1_{27} ; 2) 1, 1, ..., 1_{15} , 2, 2, ..., 2_6 ; 3) 1, 1, ..., 1_9 , 3, 3, ..., 3_6 ;
- 4) 1, 1, ..., 1_7 , 2, 2, ..., 2_{10} ; 5) 1, 1, ..., 1_5 , 2, 4, 4, ..., 4_5 ; 6) 1, 1, 1, 2, 2, ..., 2_{12} ;
- 7) 1, 1, 1, 2, 2, 2, 3, 3, 3, 3, 6; 8) 1, 1, 5, 5, 5, 5, 5; 9) 1, 2, 2, 2, 4, 4, 4, 4, 4;
- 10) 1, 2, 2, 2, 2, 3, 3, 6, 6; 11) 2, 5, 5, 5, 10; 12) 3, 3, ..., 3_9 ;
- 13) 3, 3, 3, 3, 3, 6, 6; 14) 3, 6, 6, 6, 6; 15) 1, 2, 8, 8, 8; 16) 1, 1, 1, 4, 4, 4, 4, 4, 4;
- 17) 1, 1, 1, 2, 2, 2, 6, 6, 6; 18) 3, 12, 12; 19) 1, 4, 4, 6, 12; 20) 9, 9, 9.

Come conseguenza risulta che il grado della minima estensione di $GF(q)$ nella quale la F possiede 27 rette non supera mai 12. Questo permette di migliorare un precedente risultato ⁽¹⁾ dell'autore [2] a proposito della minima estensione di $GF(q)$, $GF(Q)$ in cui la F possiede $Q^2 + 7Q + 1$ punti.

Inoltre per mezzo di convenienti rappresentazioni piane della F si realizzano le prime 15 possibilità in campi di GALOIS di ordine non troppo basso. Le possibilità 15), 16), 17) vengono realizzate dall'autore solo in campi di GALOIS di ordine particolare, anche se comunque alto.

Per necessità di carattere tipografico il lavoro viene diviso in due parti. Nella prima, dopo avere dimostrato la riducibilità dell'equazione delle 27 rette e dell'equazione dei 45 piani tritangenti della F , si utilizzano convenienti rappresentazioni piane della F per scomporre l'equazione delle 27 rette in equazioni irriducibili in $GF(q)$ e si danno dei teoremi atti a escludere l'esistenza di certe scomposizioni dell'equazione delle 27 rette della F , a priori ritenute possibili.

1. Sia F una superficie cubica di uno spazio a tre dimensioni definita in un campo di GALOIS $GF(q)$ di caratteristica dispari. La F non possieda punti multipli in nessuna estensione di $GF(q)$, sia cioè una superficie cubica generale. Essa [5] in una conveniente estensione di $GF(q)$, possiede 27 rette, la cui configurazione è caratterizzata dalle proprietà di incidenza note nel caso di una superficie cubica definita nel campo complesso. Supponiamo ora, come faremo in tutto il resto del lavoro, anche senza dirlo esplicitamente, che q non sia troppo piccolo e sia

$$(1) \quad A = 0$$

l'equazione (ad un'incognita) di grado 27 che determina tali rette. Le radici della (1) saranno tutte distinte e tutti i coefficienti

(1) A proposito di questo risultato il recensore di « Mathematical Reviews », (1957, n° 6) scrive: « Some of the arguments at the end of n° 2 (concerning extensions of γ in which $N = q^2 + 7q + 1$) are incorrect ».

Il risultato in realtà è corretto, ed è una conseguenza del noto teorema (cfr. [3]), non esplicitamente citato in [2], secondo cui se $f(x)$ è un polinomio a coefficienti in un campo di GALOIS K , e irriducibile rispetto ad esso, e se un ampliamento H di K contiene una radice di $f(x)$, H contiene tutte le radici di $f(x)$. Il carattere marginale del risultato in questione indusse l'autore ad accennare appena alla linea della dimostrazione, il che rese oscuro il testo e trasse in inganno il recensore.

della (1) apparterranno a $GF(q)$. I coefficienti delle equazioni delle 27 rette saranno funzioni razionali, a coefficienti in $GF(q)$, delle 27 radici della (1) ⁽²⁾.

Come nel caso del campo complesso i piani tritangenti alla F saranno 45. Sia

$$(2) \quad B = 0$$

l'equazione di grado 45 che li determina; i coefficienti della (2) apparterranno a $GF(q)$.

Cominciamo col provare che le equazioni (1) e (2) sono riducibili in $GF(q)$. Per questo richiamiamo il noto [3, 4]

TEOREMA I. - *Un'equazione di grado ν , irriducibile in $GF(q)$, ha in $GF(q^m)$ ν radici, se ν divide m ; nessuna se ν non divide m .*

Da questo discende un corollario che in seguito ci occorrerà più volte:

TEOREMA II. - *Un'equazione $E = 0$ di grado mn , irriducibile in $GF(q)$, si spezza in $GF(q^n)$ in m equazioni irriducibili di grado n .*

Infatti per il teorema I è sufficiente un'estensione di $GF(q^m)$ di grado n , $GF(q^{mn})$, perchè in questa risultino razionali tutte le mn radici dell'equazione considerata. Questo significa che in $GF(q^m)$ l'equazione $E = 0$ è riducibile, perchè, se fosse invece irriducibile, essendo di grado mn , in $GF(q^{mn})$ non avrebbe nessuna radice. Ora il grado di una qualsiasi delle componenti della $E = 0$ irriducibili in $GF(q^m)$ è proprio n : infatti, se fosse più grande di n , non sarebbe sufficiente un'estensione di grado n di $GF(q^m)$, cioè $GF(q^{mn})$, perchè in questa risultassero razionali tutte le radici della $E = 0$; se invece fosse più piccolo di n , in un'estensione di $GF(q)$ di grado più piccolo di mn sarebbero razionali alcune radici della $E = 0$, e questo è impossibile per il teorema I.

Ciò premesso dimostriamo il

TEOREMA 1. - *Le equazioni (1) e (2) sono riducibili in $GF(q)$.*

Cominciamo col provare che la (2) è riducibile in $GF(q)$. Infatti supposto che la (2) sia irriducibile, il grado delle estensioni di $GF(q)$ nelle quali risultano razionali tutte le rette della F è un

(²) Se q non è troppo piccolo, con opportuna scelta del sistema di riferimento, le 27 rette della F possono rappresentarsi con le equazioni $y = l_i z + m_i$, $x = r_i z + s_i$ ($i = 1, 2, \dots, 27$) (appartenendo l_i, m_i, r_i, s_i a una conveniente estensione di $GF(q)$), in modo tale che per $i \neq j$ sia $s_i \neq s_j$. Allora p. es. il procedimento usato da L. E. DICKSON (Miller, Blichfeldt, Dickson, « Finite groups ») nel campo complesso conduce a un'equazione $A(s) = 0$ di grado 27 le cui radici forniscono s_i ($i = 1, 2, \dots, 27$) e l_i, m_i, r_i risultano funzioni razionali a coefficienti in $GF(q)$ di s_i .

multiplo di 45 (e ciò perchè, note tutte le rette della F , sono determinabili razionalmente tutti i suoi piani tritangenti, e d'altra parte, per il teorema I, perchè un'equazione di grado 45, irriducibile in $GF(q)$, quale è supposta la (2), si spezzi in 45 equazioni razionali, è necessaria un'estensione di $GF(q)$ di grado m multiplo di 45). Quindi, siccome nessuna componente della (1) può avere un grado multiplo di 45, una componente irriducibile della (1) dovrà avere un grado multiplo di 5 e non divisibile per 9 ed un'altra un grado multiplo di 9 e non divisibile per 5. Considerata quest'ultima, essa determina, in un'estensione di $GF(q)$, $GF(q^r)$, di grado r non multiplo di 45, almeno 9 rette. Ora è noto che di $t > 6$ rette di una superficie cubica almeno due sono incidenti; quindi delle 9 rette considerate almeno 2 sono complanari, perciò in $GF(q^r)$ risulta razionale un piano tritangente e questo contrasta con l'ipotesi che la (2) sia irriducibile in $GF(q)$. La (2) è quindi riducibile.

Facciamo ora vedere la riducibilità della (1). Supponiamo per assurdo che l'equazione (1) sia irriducibile in $GF(q)$. Consideriamo insieme ad essa, l'equazione (2). Siccome, note le 27 rette della F , sono determinabili razionalmente i 45 piani tritangenti, il grado di ciascuna delle componenti irriducibili della (2) sarà un divisore (proprio o improprio) di 27; più precisamente una componente irriducibile della (2) avrà proprio grado 27, perchè in caso contrario in $GF(q^9)$ sarebbero razionali tutti i piani tritangenti e quindi siccome ogni retta si può determinare come intersezione di due piani tritangenti, in $GF(q^9)$ sarebbero razionali tutte le rette della F , contrariamente all'ipotesi che la (1) sia irriducibile in $GF(q)$. Allora i 18 triangoli determinati dalle componenti irriducibili della (2) di grado inferiore a 27 risultano razionali in $GF(q^9)$ e almeno due di essi hanno una retta in comune (in caso contrario la F conterrebbe 54 rette), che risulta determinata razionalmente in $GF(q^9)$ come intersezione dei due piani che contengono i due triangoli e questo contrasta con l'ipotesi che la (1) sia irriducibile. La (1) è quindi riducibile.

TEOREMA 2. - *Sia $A_1 = 0$ una componente irriducibile della (1) e siano $r_1, r_2, \dots, r_l$ ($1 \leq l < 27$) le rette da essa determinate. Allora, se una delle rette r_i ($i = 1, 2, \dots, l$) è incidente a k ($0 \leq k \leq l$) delle altre e sghemba con le $l - k - 1$ rette rimanenti, lo stesso succede per un'altra qualsiasi delle r_i .*

Sia, per esempio, r_1 incidente a $r_2, r_3, \dots, r_{k+1}$ e sghemba con $r_{k+2}, r_{k+3}, \dots, r_l$. Siccome [3] il gruppo di GALOIS di una equazione a coefficienti in un campo di GALOIS $GF(q)$ e ivi irriducibile è transitivo, detto G il gruppo di GALOIS della $A_1 = 0$, esisterà

un elemento di G , g , che porta r_1 in una qualsiasi delle rette rimanenti, r_{i_1} , e le rette $r_1, r_2, \dots, r_k, \dots, r_l$ saranno portate da g rispettivamente nelle rette $r_{i_1}, r_{i_2}, \dots, r_{i_k}, \dots, r_{i_l}$, essendo $i_1, i_2, \dots, i_k, \dots, i_l$ una permutazione degl'indici $1, 2, \dots, l$. Se P è il punto comune a due rette incidenti, r_1 ed r_j ($2 \leq j \leq k+1$) e se g porta P in un altro punto P' , due rette per P vengono portate in altre due per P' , cioè due rette incidenti vengono portate in due rette incidenti. Analogamente due rette sghembe, r_1 e r_{k+h} ($2 \leq h \leq l-k$), sono portate da g in due rette sghembe, r_{i_1} e $r_{i_{k+h}}$, perchè, considerato l'inverso di g , g^{-1} , questo porterà r_{i_1} e $r_{i_{k+h}}$ in r_1 e r_{k+h} e se r_{i_1} e $r_{i_{k+h}}$ fossero incidenti, lo sarebbero anche r_1 e r_{k+h} , contro l'ipotesi. Quindi, come si voleva dimostrare, il numero delle rette incidenti alla r_1 e il numero delle rette sghembe con essa sono uguali rispettivamente al numero delle rette incidenti con qualsiasi altra delle rette rimanenti e al numero delle rette sghembe con questa.

2. Consideriamo su un piano proiettivo α sopra $GF(q)$ un sistema lineare $|C_4|$, di grado e dimensione 3, di quartiche passanti semplicemente per 5 punti $B_1, B_2, \dots, B_5$, formanti un gruppo razionale in $GF(q)$, e doppiamente per due punti C_6, C_7 , formanti anch'essi un gruppo razionale in $GF(q)$, e supponiamo che su una retta qualsiasi passante per uno dei C si trovi al massimo uno dei punti base rimanenti e che una conica passante per i due C e per tre qualsiasi dei B non passi per nessuno degli altri punti base. Questo sistema rappresenta proiettivamente su α una superficie cubica F , definita in $GF(q)$, priva di singolarità in qualunque estensione di $GF(q)$, le cui 27 rette sono rappresentate su α dai 5 punti base semplici del sistema lineare, dalle 10 rette che congiungono ognuno dei C con ciascuno dei B , dalle 10 coniche passanti ciascuna per i due C e per tre qualsiasi dei B , e dalle due cubiche ciascuna delle quali ha un punto doppio in uno dei C e passa semplicemente per l'altro punto C e per tutti i B .

Vogliamo vedere come si spezza in $GF(q)$ l'equazione delle 27 rette della F secondo i diversi modi in cui si possono spezzare in $GF(q)$ in gruppi irriducibili il gruppo dei punti base semplici e il gruppo dei punti base doppi. Per brevità indicheremo i 7 punti base con i rispettivi indici e scriveremo per esempio (1, 2, 3) per indicare il gruppo irriducibile in $GF(q)$ formato da B_1, B_2, B_3 . Si hanno i seguenti 14 casi:

1. - (1) (2) (3) (4) (5) (6) (7). La F possiede 27 rette in $GF(q)$ e l'equazione (1) si spezza in $GF(q)$ in 27 equazioni lineari.

2. - (1) (2) (3) (4) (5) (6, 7). La F possiede in $GF(q)$ 15 rette e in $GF(q^2)$ 27 rette. La (1) si spezza quindi in $GF(q)$ in 15 equazioni lineari e in 6 equazioni irriducibili di secondo grado.

3. - (1) (2) (3) (4, 5) (6) (7). La F possiede 15 rette in $GF(q)$ e 27 rette in $GF(q^2)$. Come sopra la (1) si spezza in $GF(q)$ in 15 equazioni lineari e in 6 equazioni irriducibili di secondo grado.

4. - (1) (2) (3) (4, 5) (6, 7). La F possiede 7 rette in $GF(q)$ e 27 rette in $GF(q^2)$. La (1) si spezza in $GF(q)$ in 7 equazioni lineari e in 10 equazioni irriducibili di secondo grado.

5. - (1) (2) (3, 4, 5) (6) (7). La F possiede 9 rette in $GF(q)$ e 27 rette in $GF(q^2)$. La (1) si spezza in $GF(q)$ in 9 equazioni lineari e in 6 equazioni irriducibili di terzo grado.

6. - (1) (2) (3, 4, 5) (6, 7). La F possiede 3 rette (sghembe a due a due) in $GF(q)$ e, tenuto conto rispettivamente dei risultati 5, 2, 1, 9 rette in $GF(q^2)$, 15 rette in $GF(q^3)$, 27 rette in $GF(q^6)$. La (1) si spezza in $GF(q)$ in 3 equazioni lineari, 3 equazioni irriducibili di secondo grado, 4 equazioni irriducibili di terzo grado, 1 equazione irriducibile di sesto grado.

7. - (1) (2, 3) (4, 5) (6) (7). La F possiede 7 rette in $GF(q)$ e 27 rette in $GF(q^2)$. La (1) si spezza in $GF(q)$ in 7 equazioni lineari e in 10 equazioni irriducibili di secondo grado.

8. - (1) (2, 3) (4, 5) (6, 7). La F possiede 3 rette in $GF(q)$ e 27 rette in $GF(q^2)$. La (1) si spezza in $GF(q)$ in 3 equazioni lineari e in 12 equazioni irriducibili di secondo grado.

9. - (1) (2, 3, 4, 5) (6) (7). La F possiede 5 rette in $GF(q)$ e, tenuto conto rispettivamente dei risultati 7 e 1, 7 rette in $GF(q^2)$ e 27 rette in $GF(q^4)$. La (1) si spezza in $GF(q)$ in 5 equazioni lineari, in una equazione irriducibile di secondo grado e in 5 equazioni irriducibili di quarto grado.

10. - (1) (2, 3, 4, 5) (6, 7). La F possiede una retta in $GF(q)$ e, tenuto conto dei risultati 7 e 1, 7 rette in $GF(q^2)$ e 27 rette in $GF(q^4)$. La (1) si spezza in $GF(q)$ in una equazione lineare, 3 equazioni irriducibili di secondo grado, 5 equazioni irriducibili di quarto grado.

11. - (1, 2) (3, 4, 5) (6) (7). La F possiede 3 rette sghembe due a due in $GF(q)$ e, tenuto conto rispettivamente dei risultati 5, 3 e 1, 9 rette in $GF(q^2)$, 15 rette in $GF(q^3)$, 27 rette in $GF(q^6)$. La (1) si spezza in $GF(q)$ in 3 equazioni lineari, 3 equazioni irriducibili di secondo grado, 4 equazioni irriducibili di terzo grado, 1 equazione irriducibile di sesto grado.

12. - (1, 2) (3, 4, 5) (6, 7). La F possiede 1 retta in $GF(q)$ e, tenuto conto rispettivamente dei risultati 5, 4 e 1, 9 rette in $GF(q^3)$, 7 rette in $GF(q^4)$, 27 rette in $GF(q^6)$. La (1) si spezza in $GF(q)$ in una equazione lineare, 4 equazioni irriducibili di secondo grado, 2 equazioni irriducibili di terzo grado, 2 equazioni irriducibili di sesto grado.

13. - (1, 2, 3, 4, 5) (6) (7). La F contiene due rette in $GF(q)$ e 27 rette in $GF(q^5)$. La (1) si spezza in $GF(q)$ in due equazioni lineari e in 5 equazioni irriducibili di quinto grado.

14. - (1, 2, 3, 4, 5) (6, 7). La F non contiene rette in $GF(q)$ e, tenuto conto dei risultati 13, 2 e 1, ne contiene 2 in $GF(q^2)$, 15 in $GF(q^5)$, 27 in $GF(q^{10})$. La (1) si spezza in $GF(q)$ in una equazione irriducibile di secondo grado, 3 equazioni irriducibili di quinto grado e una equazione irriducibile di decimo grado.

Consideriamo ora su un piano β sopra $GF(q)$ un sistema lineare $|C_3|$ di grado e dimensione 3 di cubiche di β passanti semplicemente per 6 punti $A_1, A_2, \dots, A_6$, formanti un gruppo razionale in $GF(q)$, non situati sulla stessa conica e tali che tre qualsiasi di essi non siano mai allineati. $|C_2|$ è l'immagine proiettiva sopra β di una superficie cubica generale F' definita su $GF(q)$, le cui 27 rette sono rappresentate su β dai 6 punti base, dalle 15 rette che li congiungono due a due e dalle 6 coniche che passano per 5 di essi. Se A_1 risulta razionale, F' possiede 2 rette sghembe razionali, rappresentate su β da A_1 e dalla conica $A_2A_3A_4A_5A_6$. D'altra parte una superficie cubica dotata di due rette sghembe, r_1, r_2 , determinate da un'equazione razionale, per mezzo della proiezione sghemba dei suoi punti nei punti di un piano α , mediante le rette che si appoggiano a r_1 e r_2 , viene rappresentata su α da un sistema lineare ∞^3 di quartiche passanti semplicemente per 5 punti, formanti un gruppo razionale, e doppiamente per altri due punti, anch'essi formanti un gruppo razionale. Quindi, se A_1 risulta razionale, l'equazione delle 27 rette di F' si spezza in uno dei modi indicati per la F . Analogamente, se A_1 e A_2 formano un gruppo razionale, una trasformazione quadratica avente per punti fondamentali A_1, A_2 e un terzo punto diverso da tutti gli A , cambia $|C_2|$ in un sistema ∞^3 , $|C_4|$, di quartiche passanti semplicemente per 5 punti formanti un gruppo razionale e doppiamente per altri due punti, anch'essi formanti un gruppo razionale. Quindi anche in questo caso l'equazione delle 27 rette di F' si spezza in uno dei modi indicati per la F . Ci limiteremo dunque a vedere come si può spezzare l'equazione delle 27 rette

di F' quando il gruppo dei sei punti base $A_1, A_2, \dots, A_6$ sia irriducibile, oppure quando si spezzi in due gruppi irriducibili di tre punti. Nel secondo di questi due casi F' non possiede nessuna retta in $GF(q)$ e 27 rette in $GF(q^3)$. L'equazione delle 27 rette della F' si spezza perciò in 9 equazioni irriducibili di grado 3. Nell'altro caso F' non possiede rette nè in $GF(q)$ nè in $GF(q^3)$, mentre possiede 27 rette in $GF(q^6)$ e tre rette in $GF(q^3)$. Di conseguenza l'equazione delle 27 rette della F' si spezza in $GF(q)$ in una equazione irriducibile di grado 3 e in quattro equazioni irriducibili di grado 6.

Trasformiamo ora il sistema lineare $|C_4|$ delle quartiche di α passanti semplicemente per i cinque punti B_i e doppiamente per i due punti C_j , per mezzo di una trasformazione quadratica avente per punti fondamentali B_1, B_2 e un terzo punto C_3 diverso dai punti base di $|C_4|$. Si ottiene un sistema lineare $|C_6|$, di grado e dimensione tre, di sestiche di un piano γ passanti semplicemente per 3 punti A_3', A_4', A_5' , doppiamente per tre punti B_1', B_2', C_3' , triplamente per due punti C_1', C_2' . Questo sistema lineare è, come $|C_4|$, un'immagine della superficie cubica generale F e le 27 rette di F sono rappresentate su α dai tre punti A_3', A_4', A_5' ; dalle sei rette $C_1'B_1', C_1'B_2', C_1'C_3', C_2'B_1', C_2'B_2', C_2'C_3'$; dalle nove coniche passanti per i due punti tripli, per due dei punti doppi, per uno dei punti semplici; dalle sei cubiche aventi un punto doppio in C_1' o in C_2' e passanti semplicemente per C_2' o C_1' , per i punti doppi e per due dei punti semplici di $|C_6|$; dalle tre quartiche aventi due punti doppi in C_1' e C_2' , un terzo punto doppio in uno dei tre punti doppi di $|C_6|$ e passanti semplicemente per gli altri due punti doppi di $|C_6|$ e per i tre punti A_3', A_4', A_5' .

Ebbene, se i punti A_3', A_4', A_5' , i punti B_1', B_2', C_3' , i punti C_1', C_2' formano gruppi razionali irriducibili in $GF(q)$, la F non contiene rette in $GF(q)$ e in $GF(q^3)$, e ne contiene 15 in $GF(q^3)$ e 27 in $GF(q^6)$. Quindi in questo caso l'equazione (1) si spezza in cinque equazioni irriducibili di terzo grado e in due equazioni irriducibili di sesto grado.

3. Esaminiamo la questione nel caso generale.

TEOREMA 3. - *Se una superficie cubica generale F possiede due rette sghembe, r_1, r_2 , determinate da un'equazione a coefficienti in $GF(q)$, allora la (1) si spezza in uno dei modi indicati nel n° 2.*

Infatti in questo caso la F , mediante la proiezione sghemba dei suoi punti sui punti di un opportuno piano α , per mezzo delle rette che si appoggiano a r_1 ed r_2 , si rappresenta su α col sistema

lineare delle quartiche che passano doppiamente per le intersezioni C_6 e C_7 di r_1 ed r_2 con α e semplicemente per le intersezioni B_1, B_2, B_3, B_4, B_5 delle 5 rette della F che si appoggiano a r_1 e r_2 . Tenuto conto che C_6, C_7 e B_1, B_2, B_3, B_4, B_5 formano due gruppi razionali in $GF(q)$, risulta quanto si voleva dimostrare.

TEOREMA 4. - *Se l'equazione (1) possiede una componente irriducibile di grado 5, allora la (1) possiede anche una componente di secondo grado che determina due rette sghembe e quindi secondo il n° 2 si spezza o in due equazioni lineari e in cinque equazioni irriducibili di quinto grado, oppure in una equazione irriducibile di secondo grado, tre equazioni irriducibili di quinto grado, una equazione irriducibile di decimo grado.*

Infatti, risolte in una conveniente estensione di $GF(q)$ le componenti irriducibili della (1) il cui grado è primo con 5, in questa estensione per il numero N delle rette della F si ha $N \equiv 27 \pmod{5}$ e quindi [5] N è uguale a 2 o a 7. Non può essere $N=7$ perchè due di queste rette sarebbero certamente sghembe, e questo, tenuto conto del teorema 3 e dei risultati del n° 2 è impossibile, dato che per $N=7$ la (1) non ha nell'estensione considerata e quindi neanche in $GF(q)$ una componente irriducibile il cui grado sia multiplo di 5. Allora $N=2$ e queste due rette, come si voleva dimostrare sono sghembe, poichè, se non lo fossero, il piano che le contiene entrambe incontrerebbe la F in una terza retta appartenente al campo che contiene le altre due, contro l'ipotesi che sia $N=2$.

TEOREMA 5. - *Se la (1) possiede una componente irriducibile di grado 4, le quattro rette da questa determinate o si distribuiscono in due coppie di rette complanari, oppure ognuna è incidente a due delle rimanenti in modo da formare un quadrilatero sghembo, oppure esse sono due a due sghembe; in quest'ultimo caso la (1) si spezza in uno dei modi considerati nel n° 2.*

Consideriamo una componente irriducibile della (1) determinante quattro rette della F sghembe due a due; è noto che a queste quattro rette si appoggiano altre due rette, sghembe fra loro, della F . Queste due rette sono determinate da una equazione a coefficienti in $GF(q)$. Il teorema 3 assicura allora che in questo caso la (1) si spezza in uno dei modi considerati nel n° 2.

Il resto dell'enunciato deriva immediatamente dal teorema 2.

TEOREMA 6. - *La (1) non possiede componenti irriducibili di grado 7.*

Infatti, se la (1) avesse una componente irriducibile di grado 7, risolte in una conveniente estensione di $GF(q)$ le componenti irriducibili della (1) il cui grado è primo con 7, in questa estensione la F conterrebbe un numero di rette uguale a $27 - 7 = 20$, oppure a $27 - 14 = 13$, oppure a $27 - 21 = 6$ e questo non è possibile [5].

TEOREMA 7. - *La (1) non possiede componenti irriducibili di grado 11.*

Infatti, supposto che la (1) possieda una componente irriducibile di grado 11, risolte in una conveniente estensione di $GF(q)$ le componenti irriducibili della (1) di grado primo con 11, in questa estensione il numero delle rette della F è congruo 27 (mod 11) e quindi uguale a 5 [5]. D'altra parte, tenuto conto del teorema 4 e dei risultati del n° 2, la (1) non ha nell'estensione considerata, e quindi neanche in $GF(q)$, componenti irriducibili di grado multiplo di 11, contro l'ipotesi fatta. Dall'assurdo discende quanto si voleva dimostrare.

TEOREMA 8. - *Se la (1) possiede in $GF(q)$ una componente irriducibile di grado 10, allora la (1) contiene ulteriormente una componente irriducibile di secondo grado e tre componenti irriducibili di quinto grado.*

Infatti, se la (1) possiede in $GF(q)$ una componente irriducibile di grado 10, non ne può contenere anche una di grado 20; quindi in $GF(q^2)$ per il teorema II la (1) possiede almeno due componenti irriducibili di quinto grado e nessuna di grado 10. Allora, tenuto conto del teorema 4 e del n° 2, la (1) si spezza in $GF(q^2)$ in 5 equazioni irriducibili di quinto grado e in due equazioni lineari. Ora una di queste equazioni di quinto grado o è razionale anche in $GF(q)$ e quindi irriducibile, oppure in $GF(q)$ è una componente irrazionale di un'equazione irriducibile di decimo grado a coefficienti in $GF(q)$; ne viene allora che, essendo dispari il numero delle componenti di quinto grado della (1) in $GF(q^2)$, la (1), oltre la componente irriducibile di decimo grado, avrà almeno una componente irriducibile di quinto grado anche in $GF(q)$. Tenuto conto del teorema 4 risulta perciò dimostrato il teorema.

Se F possiede una retta razionale, r , ad essa se ne appoggiano altre 10 distribuite in 5 coppie di rette complanari e determinate da un'equazione razionale.

TEOREMA 9. - *L'equazione delle 10 rette della F che si appoggiano ad una retta, r , appartenente a $GF(q)$, è riducibile in $GF(q)$ e, se ammette una componente di grado dispari, ne ammette un'altra di eguale grado. Inoltre, se questa equazione in una estensione*

di $GF(q)$ si spezza razionalmente in equazioni lineari, lo stesso accade per la (1).

Supposto, per assurdo, che l'equazione delle 10 rette che si appoggiano alla r sia irriducibile, la (1), di cui è una componente, ammette una componente irriducibile di grado 10; e quindi, per il teorema 8, non ammette componenti razionali, contro l'ipotesi che la F contenga in $GF(q)$ una retta. L'equazione in questione è dunque riducibile.

Supponiamo ora che essa abbia una componente irriducibile di grado dispari, d . Per il teorema 2 le d rette da questa determinate sono sghembe due a due e i piani passanti per queste rette e contenenti la r tagliano la F secondo d rette determinate da una equazione irriducibile in $GF(q)$. Con ciò è dimostrato che, se l'equazione delle 10 rette appoggiate alla r ammette una componente irriducibile di grado dispari, ne ammette un'altra di eguale grado.

Sia $GF(Q)$ l'estensione di $GF(q)$ nella quale la F possiede, oltre la r , anche le 10 rette che vi si appoggiano. In $GF(Q)$ la F contiene $Q^2 + 7Q + 1$ punti [2], e, considerata una qualsiasi delle 10 rette che si appoggiano alla r , diciamo s , anche a questa si appoggiano 10 rette della F appartenenti a $GF(q)$, perchè da [2] si ha che la F possiede in $GF(Q)$ $Q^2 + 7Q + 1$ punti solo se a una sua retta appartenente a $GF(Q)$ se ne appoggiano 10, tutte appartenenti a $GF(Q)$. La F contiene dunque in $GF(Q)$ almeno le 19 rette che si appoggiano alla r o alla s ; ora, se una superficie cubica generale contiene in un corpo commutativo più di 15 rette, ne contiene 27 [5]; quindi in $GF(Q)$ la F contiene tutte le sue 27 rette. Ne viene allora che, come si voleva dimostrare, la (1) si spezza razionalmente in $GF(Q)$ in equazioni lineari e il teorema è completamente dimostrato.

Usando una denominazione introdotta da E. BERTINI [1], chiameremo triedro di prima specie di una superficie cubica generale un insieme di tre piani a questa tritangenti, facce del triedro, che si tagliano in rette non appartenenti alla superficie e tali che tre rette qualsiasi della F appartenenti a tre diverse facce non siano mai complanari. Questi triedri sono stati studiati da E. BERTINI e il loro numero è 2880 [1]. Consideriamo sulla F uno di questi triedri e siano 1, 4, 7; 2, 5, 8; 3, 6, 9 le rette appartenenti rispettivamente alle tre facce. Siccome, presi due trilateri appartenenti a una superficie cubica generale e non aventi nessun lato in comune, ogni retta di uno qualsiasi è incidente a una e a una sola retta dell'altro, potremo supporre che 1 sia incidente a 2 e 2 incidente a 3; 4 incidente a 5 e 5 incidente a 6; 7 incidente a 8 e

8 incidente a 9. 3 che deve incontrare anche un lato del primo trilatero, non può incontrare 1, data la natura del triedro considerato; incontrerà allora un altro lato del primo trilatero che chiameremo 4. A sua volta 6 deve incontrare un lato del primo trilatero che, per una ragione analoga a quella detta per 3, non può essere 4; e non può essere neanche 1, perchè, se 6 incontrasse 1, allora 9 dovrebbe incontrare 7, e si verrebbe così a formare un trilatero di lati 7, 8, 9 contrariamente all'ipotesi che il triedro sia di prima specie. Quindi 6 incontra 7; analogamente 9, che deve incontrare un lato del primo trilatero, poichè 3 incontra 4 e 6 incontra 7, incontrerà 1. Allora le 9 rette 1, 2, ..., 9 di un triedro di prima specie si possono ordinare in modo che ogni retta incontri quella indicata con l'intero successivo, 9 incontri 1 e in modo tale che 1, 4, 7; 2, 5, 8; 3, 6, 9 siano complanari.

Facciamo ora vedere che sulla F non esistono insiemi di 9 rette tali che ognuna di esse incontri due e solo due delle altre rette.

Ricorriamo per questo alla rappresentazione piana della F che abbiamo già usato e che si ottiene mediante la proiezione sghemba e notiamo che le due rette sghembe rappresentate dalle cubiche che hanno un punto doppio in C_6 o C_7 (per brevità indicheremo con C_6 e C_7 queste due cubiche) incontrano quelle due a due sghembe rappresentate dai punti B_1, B_2, B_3, B_4, B_5 ; che una delle rette della F rappresentate dalle rette $B_i C_j$ o dalle coniche $C_6 C_7 B_i B_j B_k$ (che per brevità indicheremo in seguito con il simbolo $(i j k)$) incontra una delle rette rappresentate dalle figure rimanenti quando le due rappresentazioni hanno un punto in comune fuori dei B_i e dei C_j ; che la retta rappresentata dalla cubica $C_6 (C_7)$ incontra una delle rette rappresentate da una retta o da una conica quando il punto $C_6 (C_7)$ appartiene alla retta o alla conica; e che infine una delle rette rappresentate dai 5 punti base semplici incontra una di quelle rappresentate da una retta o da una conica quando il punto appartiene alla retta o alla conica.

Ciò premesso, osserviamo che se la configurazione in questione esiste, tre rette consecutive delle nove rette considerate possono sempre essere rappresentate da C_6, B_1, C_7 .

Scriviamo le (figure rappresentative delle) rette che si appoggiano alla C_6 , alla C_7 , alla B_1 , indicando per semplicità i punti base con i rispettivi indici.

6: 1, 2, 3, 4, 5, 61, 62, 63, 64, 65;

1: 6, 7, 61, 71, (123), (124), (125), (134), (135), (145);

7: 1, 2, 3, 4, 5, 71, 72, 73, 74, 75.

Le rette che si appoggiano alla 7 ma non a nessuna di quelle che si appoggiano alla 6 o alla 1 sono la 72, la 73, la 74 e la 75. Come quarta retta della configurazione dobbiamo scegliere una qualunque di queste, e senza restrizioni possiamo supporre di scegliere la 72.

Scriviamo ora le 10 rette che si appoggiano alla 72.

72: 7, 2, 61, 63, 64, 65, (134), (135), (145), (345).

Di queste solo la (345) può essere assunta come quinta retta della configurazione perchè è l'unica incidente solo alla 72. Le rette incidenti alla (345) sono:

(345): 3, 4, 5, 61, 62, 71, 72, (123), (124), (125).

Dall'esame di queste risulta che non ve ne è nessuna che non si appoggi a due almeno dei lati già determinati della configurazione, quindi è impossibile proseguire nella costruzione e l'asserto è dimostrato.

TEOREMA 10. — *Se la (1) contiene una componente irriducibile di grado 9, le 9 rette da questa determinate si distribuiscono su un triedro di prima specie.*

Supponiamo che la (1) abbia una componente irriducibile di grado 9, $f=0$, e sia G il gruppo di GALOIS di tale equazione: $G [3]$ è ciclico di ordine 9 e transitivo; sia g un elemento di G di ordine massimo; 1 una delle nove rette determinate dall'equazione $f=0$; 2, 3, ..., 9 le rette in cui $g, g^2, \dots, g^8$ portano la 1. È evidente che se un elemento qualsiasi di G porta i ($1 \leq i \leq 9$) in una retta ad essa incidente (sghemba), lo stesso elemento porterà un'altra qualsiasi delle rimanenti 8 rette in una retta ad essa incidente (sghemba).

Sia allora 1 incidente a 2; di conseguenza i ($1 \leq i < 9$) sarà incidente a $i+1$ e 9 incidente a 1. Per quanto abbiamo già visto subito prima di enunciare questo teorema, 1, oltre che incidente a 2 e 9, sarà incidente a una almeno delle altre rette. Possono capitare i seguenti casi:

a) 1 è anche incidente a 3. Allora le rette 1, 2, 3 e le rette 2, 3, 4 formano due trilateri piani appartenenti alla F .

b) 1 è anche incidente a 5. Allora, per $1 \leq i \leq 5$, è i incidente a $i+4$, e per $5 < i \leq 9$ è i incidente a $i+4-9$. Pertanto le rette 1, 2, 6 e le rette 6, 1, 5 formano due trilateri piani appartenenti alla F .

c) 1 è anche incidente a 6. Allora $1 = 6 + 4 - 9$ è incidente a $5 = 1 + 4$, e si ricade nel caso b).

d) 1 è anche incidente a 8. Allora $1 = 8 + 2 - 9$ è incidente a $3 = 1 + 2$, e si ricade nel caso a).

e) 1 è anche incidente a 4 e non è incidente nè a 3, nè a 5, nè a 6, nè a 8. Essendo 1 incidente a 4, 4 è incidente a 7, 7 incidente a 1 e le rette 1, 4, 7 formano un trilatero piano. In definitiva 1 risulta incidente a 2, 4, 7, 9 e sghemba con le rimanenti rette. Analogamente 2 risulta incidente a 3, 5, 8, 1 e così via e, come le rette 1, 4, 7, anche le rette 2, 5, 8 e 3, 6, 9 formano trilateri piani.

I casi a), b), c), d) portano a un assurdo, perchè, in ognuno di questi casi sulla F esistono due trilateri piani aventi due lati in comune. Rimane possibile il caso e) e in questo caso, per quanto abbiamo già visto, le nove rette determinano un triedro di prima specie.

Supponiamo infine che ogni elemento di G di ordine 9 porti una retta in una retta ad essa sghemba. Allora, siccome fra nove rette della F ve ne sono due almeno incidenti, un elemento di G di ordine 3 porterà una retta in un'altra ad essa incidente; si avranno allora sulla F i trilateri piani 1, 4, 7; 2, 5, 8; 3, 6, 9 e nessuna retta di un trilatero sarà incidente a qualche retta di un altro. D'altra parte, presi sulla F due trilateri piani non aventi nessun lato in comune, ogni lato del primo è incidente a un lato del secondo e quindi un elemento di G di ordine 9 non può portare una retta della F in una retta con essa sghemba. L'unica configurazione per le nove rette determinate dalla $f=0$ è dunque la e) ed è dimostrato che queste rette costituiscono un triedro di prima specie.

TEOREMA 11. — *Se la (1) contiene una componente irriducibile di grado 9, allora essa si spezza in tre componenti irriducibili di grado 9.*

Supponiamo che la (1) abbia una componente irriducibile di grado 9. Allora in $GF(q^9)$ la F possiede 9 o 15 o 27 rette.

Se in $GF(q^9)$ la F possiede 9 rette, due di esse sono certamente sghembe e quindi, tenuto conto del teorema 3 e del n° 2, in $GF(q^9)$ la (1) oltre che componenti lineari, contiene anche componenti irriducibili di grado 3. Allora in $GF(q)$ la (1) possiede, oltre la componente di grado 9, anche una componente irriducibile di grado 27, cosa manifestamente assurda.

Se in $GF(q^9)$ la F possiede 15 rette, allora la (1) in $GF(q)$ pos-

siede, oltre la componente di grado 9, componenti irriducibili di grado 1 o 3. Di più le 12 rette della F non appartenenti a $GF(q^3)$, per il teorema 3 ed il n° 2, saranno determinate in $GF(q^9)$ da 6 equazioni irriducibili di grado 2 e in $GF(q)$, per il teorema II, da equazioni di grado 2 o 6. In questa maniera la F in $GF(q^9)$ possiede 18 rette, cosa assurda [5].

Supponiamo che in $GF(q^9)$ la F possegga 27 rette. Allora se in $GF(q)$ la (1) possiede componenti irriducibili di grado diverso da 9, queste saranno di grado 1 o 3. Quindi se la (1) possiede in $GF(q)$ una sola componente irriducibile di grado 9, in $GF(q^3)$ possiede 18 rette, cosa impossibile [5].

Se invece la (1) possiede in $GF(q)$ due componenti irriducibili di grado 9, allora in $GF(q^3)$ la (1) contiene 9 rette che pertanto costituiscono un sistema di STEINER [5], e questo risulta razionale in $GF(q)$. D'altra parte l'equazione che determina tutti i sistemi di STEINER è di grado 120 e siccome, essendo razionali tutte le rette della F , sono razionali tutti i sistemi di STEINER, in $GF(q^3)$ l'equazione dei sistemi di STEINER si spezzerà in equazioni lineari e in $GF(q)$ potrà avere soltanto componenti irriducibili di grado 9 o 3 o 1. Quindi, poichè la F possiede in $GF(q)$ un sistema di STEINER, ne dovrà possedere almeno altri due. Ciò significa che le due componenti della (1) di grado 9 determinano ciascuna un sistema di STEINER, perchè un sistema di STEINER razionale determina una componente razionale della (1) di grado 9. Tenuto conto del teorema 10 si ha quindi ancora un assurdo.

Rimane dunque l'unica possibilità che la (1) si spezzi in tre componenti irriducibili di grado 9 e il teorema è dimostrato.

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.