SULLE VARIETÀ ABELIANE CONTENENTI CONGRUENZE ABELIANE (*) (1).

Per dare un'idea del genere di questioni trattate in questo lavoro sarà bene partire da un esempio concreto.

Si consideri una varietà abeliana (2) a tre dimensioni con tre integrali ellittici, e quindi dotata di tre fasci ellittici di superficie iperellittiche e di tre congruenze iperellittiche di curve ellittiche.

Due superficie appartenenti a fasci distinti si tagliano secondo curve formate da una o più parti che, al variar delle superficie nei due fasci, variano in una delle tre congruenze; e tre superficie appartenenti a fasci diversi si tagliano in un numero finito di punti.

Come calcolare il numero di quelle parti o di questi punti?

Si vede *a priori* che i numeri in discorso debbono corrispondere a invarianti aritmetici dei sistemi di periodi (non ridotti) dei tre integrali ellittici posseduti dalla varietà; e quindi il cercar quei numeri corrisponde a caratterizzar questi invarianti e studiarne le proprietà.

È appunto tale caratterizzazione l'oggetto del presente lavoro; ove la ricerca viene compiuta per una qualunque varietà abeliana dotata di sistemi regolari di integrali (semplici, di 1ª specie) riducibili, o, ciò che fa lo stesso, di *congruenze abeliane* (3), facendola dipendere da uno studio particolareggiato di alcuni notevoli invarianti simultanei aritmetici di due o più assi di una matrice rie-

(*) Rend. Circolo Mat. di Palermo, 43 (1918-19), pp. 213-238.

(1) Questa Memoria fu presentata all'Accademia Gioenia di Catania nella sua ultima seduta del 1918; ma le difficoltà del momento ne hanno impedita la pubblicazione negli *Atti* relativi.

(2) Per la definizione di varietà abeliana che qui si intende adottata, veggasi la mia Memoria: *Intorno alla teoria generale delle matrici di* Riemann *e ad alcune sue applicazioni* [Rendiconti del Circolo Matematico di Palermo, t. XLI (1916), pp. 263-380], pag. 269 annotazione 13) e pag. 331.

(3) Veggasi più innanzi il n° 16.

manniana. Studio che, come mostro con alcuni esempi verso la fine del lavoro, è suscettibile di altre applicazioni geometriche non prive di interesse.

§.

LE BASI MINIME DI UNO SPAZIO RAZIONALE.

1. Sia S uno spazio lineare ad r dimensioni, nel quale sia fissato un sistema di coordinate proiettive omogenee, per modo da poter distinguere i suoi elementi (punti, rette, piani, S_3, ...) in *reali* o *imaginari, razionali* o *irrazionali;* e sia A un S_t *razionale* di S $(0 \leq t \leq r)$.

Lo spazio A potrà considerarsi, o come lo spazio congiungente $t+1$ punti razionali indipendenti di S, o (se $t < r$) come lo spazio intersezione di $r-t$ iperpiani razionali indipendenti di S.

Diciamo I l'insieme dei gruppi (ordinati) di numeri interi $(x_1, x_2, \dots, x_{r+1})$, ciascun dei quali può pensarsi come il gruppo delle coordinate di un punto razionale di A, e J (se $t < r$) quello dei gruppi di numeri interi $(\xi_1, \xi_2, \dots, \xi_{r+1})$ ciascun dei quali può pensarsi come il gruppo delle coordinate di un iperpiano razionale passante per A.

È chiaro che a ciascun elemento di I (di J) corrisponde *un* punto (*un* iperpiano) razionale appartenente ad A; mentre a ciascun punto (iperpiano) sì fatto corrispondono infiniti elementi di I (di J) costituiti da gruppi di interi fra loro proporzionali.

Se è $t < r$ e se

$$[\xi_1^{(\mu)}, \xi_2^{(\mu)}, \dots, \xi_{r+1}^{(\mu)}] \qquad (\mu = 1, 2, \dots r-t) \tag{1}$$

sono $r-t$ elementi di J *indipendenti,* l'insieme I può definirsi come la totalità delle soluzioni *proprie* con numeri interi $(x_1, x_2, \dots, x_{r+1})$ delle $r-t$ equazioni a coefficienti interi

$$\xi_1^{(\mu)} x_1 + \xi_2^{(\mu)} x_2 + \dots + \xi_{r+1}^{(\mu)} x_{r+1} = 0 \quad (\mu = 1, 2, \dots, r-t); \tag{2}$$

se invece $r = t$ l'insieme I è l'insieme di tutti i possibili gruppi di interi $(x_1, x_2, \dots, x_{r+1})$ per ciascun dei quali almeno un intero è diverso da zero.

Basta ricordare allora i teoremi fondamentali dell'analisi indeterminata di primo grado per riconoscere che:

α) *È sempre possibile scegliere entro I $t+1$ elementi indipendenti*

$$[x_1^{(m)}, x_2^{(m)}, \dots, x_{r+1}^{(m)}] \qquad (m = 1, 2, \dots, t+1) \tag{3}$$

tali che gli elementi $(x_1, x_2, \ldots, x_{r+1})$ *di* I *siano dati tutti, e ciascuno una volta sola, dalle formule*

$$x_s = l_1 x_s^{(1)} + l_2 x_s^{(2)} + \ldots + l_{t+1} x_s^{(t+1)} \qquad (s = 1, 2, \ldots, r+1) \tag{4}$$

ponendovi per $(l_1, l_2, \ldots, l_{t+1})$ *tutti i possibili gruppi di* $t+1$ *interi, per ciascun dei quali almeno un intero è diverso da zero;*

β) *Se* $t+1$ *elementi indipendenti di* I *si dicono costituire una* BASE MINIMA *di* I *quando soddisfanno alla condizione di cui si parla in* α), *e una tal base minima è data dagli elementi* (3), *le basi minime di* I

$$[y_1^{(m)}, y_2^{(m)}, \ldots, y_{r+1}^{(m)}] \qquad (m = 1, 2, \ldots, t+1)$$

sono date tutte e ciascuna una volta sola dalle formule

$$y_s^{(m)} = a_{m,1}\, x_s^{(1)} + a_{m,2}\, x_s^{(2)} + \ldots + a_{m,t+1}\, x_s^{(t+1)} \quad (s = 1, 2, \ldots r+1),$$

quando si immagini di far percorrere alla matrice $\| a_{m,n} \|$ *l'insieme delle matrici di ordine* $t+1$ *a elementi interi e unimodulari;*

γ) *La condizione necessaria e sufficiente perchè* $t+1$ *elementi di* I *costituiscano una base minima è che i minori d'ordine massimo della matrice ad* $r+1$ *colonne di cui essi dànno le righe siano numeri primi fra loro;*

δ) *Se due* $(t+1)$*-ple di elementi di* I *costituiscono due sue basi minime, i minori d'ordine massimo della matrice formata con gli elementi dell'una sono tutti eguali o tutti opposti a quelli corrispondenti della matrice formata con gli elementi dell'altra.*

Quel che fin qui è stato detto per I, può dirsi anche (se $t < r$) per J, mutando l'ufficio di I e J; quindi anche per J si avranno delle *basi minime* (formate ciascuna da $r - t$ elementi indipendenti) e per queste varranno proprietà analoghe a quelle indicate per le basi minime di I.

Le basi minime di I (di J) si diranno anche le *basi minime per i punti di* (*gli iperpiani per*) A, dove è sottinteso che si vuol parlare soltanto dei punti (degli iperpiani) *razionali* appartenenti ad A.

2. Supposto $t < r$ si consideri una base minima per i punti di A e una base minima per gli iperpiani contenenti A, e siano, rispettivamente,

$$(c_1, c_2, \ldots), \qquad (\gamma_1, \gamma_2, \ldots) \tag{5}$$

i valori dei minori d'ordine massimo delle matrici formate con gli elementi dell'una base minima o dell'altra. Essendo

$$\binom{r+1}{t+1}=\binom{r+1}{r-t},$$

il numero degli interi c_j eguaglia quello degli interi γ_j.

Ebbene si ha subito che:

A meno, eventualmente, dell'ordine, gli interi c_j o coincidono con gli interi γ_j o coincidono con gli interi $-\gamma_j$.

E infatti tanto i numeri c_j quanto i numeri γ_j possono riguardarsi come le coordinate grassmanniane dello spazio A; quindi, a meno, eventualmente, dell'ordine, gli uni coincidono con gli altri moltiplicati per un fattore di proporzionalità. Questo fattore di proporzionalità è evidentemente razionale; poi esso è anche intero ed eguale a ± 1, perchè tanto i numeri c_j, quanto i numeri γ_j sono primi fra di loro; quindi, etc.

I numeri c_j (o $-c_j$) si diranno le *coordinate* (*intere*) *minime di* A.

Se $d_1, d_2, \ldots$ sono i minori d'ordine massimo della matrice formata con $t+1$ elementi indipendenti qualunque di I (o $r-t$ elementi indipendenti qualunque di J), e d è il massimo comun divisore di $d_1, d_2, \ldots$, le coordinate minime di A saranno date evidentemente dai numeri $\frac{d_j}{d}$ o dai numeri $-\frac{d_j}{d}$.

3. Interessa per il seguito dimostrare una proposizione che generalizza il teorema γ) del n^0 1.

Essa è la seguente:

Perchè t' elementi di I (e lo stesso dicasi, se $t<r$, per I) *faccian parte di qualche base minima di I occorre e basta che siano primi fra di loro i minori d'ordine massimo della matrice formata con essi.*

Che la condizione sia necessaria è evidente, appunto per il teorema γ); basta dunque limitarsi a far vedere che essa è sufficiente.

Siano pertanto

$$(6)\qquad |y_1^{(j)}, y_2^{(j)}, \ldots, y_{r+1}^{(j)}| \qquad (j=1,2,\ldots,t')$$

t' elementi di I soddisfacenti alla condizione di cui parla l'enunciato, per modo che sarà certo $t'\leq t+1$; e supponiamo, per non ricadere nel caso contemplato dal teorema γ), che sia $t'<t+1$.

Siano gli elementi (3) i $t+1$ elementi di una base minima di I e si ponga

(7) $$y_s^{(j)} = \varrho_{j,1}\, x_s^{(1)} + \varrho_{j,2}\, x_s^{(2)} + \dots + \varrho_{j,t+1}\, x_s^{(t+1)} \qquad (s = 1, 2, \dots, r+1)$$

con le $\varrho_{j,m}$ intere.

In base alle (7), il prodotto per righe e colonne della matrice

(8) $$\| \varrho_{j,1}, \varrho_{j,2}, \dots, \varrho_{j,t+1} \| \qquad (j = 1, 2, \dots, t')$$

per la matrice

(9) $$\| x_1^{(m)}, x_2^{(m)}, \dots, x_{r+1}^{(m)} \| \qquad (m = 1, 2, \dots, t+1)$$

è la matrice

(10) $$\| y_1^{(j)}, y_2^{(j)}, \dots, y_{r+1}^{(j)} \| \qquad (j = 1, 2, \dots, t'),$$

quindi ogni minore della matrice (10) d'ordine t' è una somma di prodotti di minori d'ordine t' della matrice (8) per minori dello stesso ordine della matrice (9).

Di qua e dall'ipotesi fatta sugli elementi (6) segue subito che i minori d'ordine massimo della matrice (8) sono numeri primi fra loro.

Ma allora, per un teorema noto [4], si ha che è possibile costruire dei determinanti, eguali a ± 1, d'ordine $t+1$ e ad elementi interi, per ciascun dei quali t' righe coincidano con quelle della matrice (8); e quindi, in virtù del teorema β) del n° 1, esistono basi minime di I contenenti gli elementi (6).

Anzi di codeste basi minime ne esistono infinite o ne esiste una sola, secondo che è $t' < t+1$ o $t' = t+1$.

La proposizione dimostrata può anche enunciarsi nel modo che segue:

Se A' è uno spazio razionale di S contenuto nello spazio A, ogni base minima per i punti di A' fa parte di qualche base minima per i punti di A; e ogni base minima per gli iperpiani (ove esistano) contenenti A fa parte di qualche base minima per gli iperpiani contenenti A'.

§ 2.

Invariante (simultaneo) aritmetico di due o più spazi razionali.

4. Siano $A_1, A_2, \dots, A_k$, $k\,(\geq 2)$ spazi razionali indipendenti di S delle dimensioni rispettive $t_1, t_2, \dots, t_k$, per modo che lo spazio A

(4) Veggasi per es. G. Frobenius, *Theorie der linearen Formen mit ganzen Coefficienten* [Journal für die reine und angewandte Mathematik, Bd. LXXXVI (1879), pp. 146-208], § 8.

che li congiunge sarà della dimensione

$$t = t_1 + t_2 + \dots + t_k + k - 1$$

e sarà

$$t \leq r.$$

Indichiamo con

$$[x_{j,1}^{(m_j)}, x_{j,2}^{(m_j)}, \dots, x_{j,r+1}^{(m_j)}] \qquad (m_j = 1, 2, \dots, t_j + 1) \tag{11}$$

gli elementi di una base minima per i punti di A_j, e costruiamo la matrice M a $t+1$ righe ed $r+1$ colonne le cui righe sono date dagli elementi delle considerate basi minime per $A_1, A_2, \dots, A_k$.

I minori d'ordine massimo di questa matrice, come si riconosce subito sviluppando ciascuno di essi secondo i minori contenuti nei k gruppi delle sue righe provenienti dalle k basi minime (11) e tenendo presente il teorema δ) del n^0 1, non variano al più che per un cambiamento simultaneo di segni, al variare della scelta delle basi minime (11) fra le basi minime per i punti dei singoli spazi A_j; quindi il loro massimo comun divisore è un intero (positivo) Δ che *dipende soltanto dagli spazi* $A_1, A_2, \dots, A_k$.

Tale intero potrà, dunque, essere indicato, molto opportunamente, col simbolo

$$[A_1, A_2, \dots, A_k].$$

Si noti che nel caso in cui sia $t = r$, la matrice M risulta quadrata e Δ è semplicemente il valore assoluto del suo determinante. Che se poi $t = r$ e $k = 2$, Δ è anche (n^0 2) il valore assoluto del determinante le cui righe sono date dagli elementi di una base minima per gli iperpiani contenenti A_1 e dagli elementi di una base minima per gli iperpiani contenenti A_2.

5. Il *carattere* Δ degli spazi $A_1, A_2, \dots, A_k$, or ora definito, si dirà il loro *invariante* (*simultaneo*) *aritmetico.* Tale denominazione è giustificata dalla seguente proprietà:

Il carattere $[A_1, A_2, \dots, A_k]$ *è invariante di fronte alle trasformazioni di coordinate o alle omografie di* S *rappresentate da sostituzioni lineari (omogenee) a coefficienti interi e unimodulari.*

Infatti l'intero Δ è quello che col FROBENIUS [5] si direbbe l'ultimo divisore elementare della matrice M; ed è noto che per una trasformazione di coordinate o per una omografia del tipo di cui si

[5] Loc. cit. [4]).

parla nell'enunciato i divisori elementari della matrice M restano tutti inalterati.

6. *L'invariante* $[A_1, A_2, \dots, A_k]$ *è multiplo dell'invariante aritmetico di ogni gruppo di due o più spazi scelti comunque fra gli spazi* A_j.

Per es. se è $k \geq 3$ l'invariante considerato è multiplo di $[A_1, A_2, A_3]$. Infatti ogni minore d'ordine massimo della matrice M che occorre considerare per il calcolo di $[A_1, A_2, \dots, A_k]$ è divisibile per $[A_1, A_2, A_3]$, come si vede subito sviluppandolo secondo i minori che sono contenuti nelle sue righe provenienti dalle basi minime di A_1, A_2, A_3.

Questa proposizione sarà precisata più innanzi (n^0 9); qui si osservi che, tenendo conto del n^0 3, essa può essere generalizzata come segue:

L'intero $[A_1, A_2, \dots, A_k]$ *è divisibile per l'intero* $[B_1, B_2, \dots B_l]$ *se gli spazi* $B_1, B_2, \dots, B_l$ *sono ordinatamente contenuti, ad es., negli spazi* $A_1, A_2, \dots, A_l$.

7. Grazie al teorema γ) del n^0 1 è chiaro che:

L'eguaglianza.

$$[A_1, A_2, \dots, A_k] = 1$$

esprime la condizione necessaria e sufficiente perchè k *basi minime per i punti dei* k *spazi* A_j *diano luogo per riunione a una base minima per i punti dello spazio che li congiunge*;

e quindi, in virtù del teorema del n^0 3:

Se A *è un qualsivoglia spazio razionale di* S *e* A' *è uno spazio razionale contenuto in* A *(in senso stretto) esistono in* A *infiniti spazi razionali tali che, detto* A'' *uno qualunque di essi, lo spazio* A *sia lo spazio congiungente* A' *e* A'' *e risulti inoltre*

$$[A', A''] = 1.$$

Ciascun tale spazio A'' si dirà un *residuo* di A' rispetto ad A.

Naturalmente se A'' è un residuo di A' rispetto ad A, anche A' è un residuo di A'' rispetto ad A.

8. *Se gli spazi razionali* $A_1, A_2, \dots, A_k$ *sono indipendenti e lo spazio* A *che li congiunge non è* S, *detto* B *un residuo di* A *rispetto ad* S *si ha*:

$$[A_1, A_2, \dots, A_k] = [A_1, A_2, \dots, A_k, B].$$

Infatti si consideri uno dei determinanti, che con il loro valore assoluto dànno il valore di $[A_1, A_2, \ldots, A_k, B]$, e si sviluppi secondo i minori contenuti nelle righe che provengono dagli elementi di una base minima di B.

Allora si riconosce immediatamente che da ogni termine dello sviluppo si raccoglie il fattore $[A_1, A_2, \ldots, A_k]$ e che, raccoltolo, resta (n⁰ 2 in fine) lo sviluppo di un determinante atto a rappresentare col suo valore assoluto il valore di $[A, B]$. È dunque

$$[A_1, A_2, \ldots, A_k, B] = [A_1, A_2, \ldots, A_k] \cdot [A, B];$$

da cui segue subito l'eguaglianza da dimostrare, una volta che

$$[A, B] = 1.$$

9. Indichiamo in generale con $A_1 + A_2 + \ldots$ lo spazio congiungente più spazi dati $A_1, A_2, \ldots$ e dimostriamo che:

Se $A_1, A_2, \ldots, A_k$ sono spazi razionali indipendenti di S ed è $k \geq 3$ si ha

$$[A_1, A_2, \ldots, A_k] = [A_1, \ldots, A_{k-2}, A_{k-1} + A_k] \cdot [A_{k-1}, A_k].$$

Si supponga in primo luogo che sia

$$A_1 + A_2 + \ldots + A_k = S,$$

e si dica A_k' uno spazio residuo di A_{k-1} rispetto ad $A_{k-1} + A_k$.

Poichè due basi minime per i punti di A_{k-1} e A_k' dànno luogo per riunione a una base minima per i punti di $A_{k-1} + A_k' = A_{k-1} + A_k$, è chiaro intanto che:

$$[A_1, A_2, \ldots, A_{k-2}, A_{k-1}, A_k'] = [A_1, A_2, \ldots, A_{k-2}, A_{k-1} + A_k].$$

Ma, come più sopra, sviluppando uno dei determinanti che dà col suo valore assoluto il carattere $[A_1, A_2, \ldots, A_k]$ secondo i minori contenuti nella matrice delle righe provenienti da basi minime di $A_1, A_2, \ldots, A_{k-2}$, si ricava che è

$$[A_1, A_2, \ldots, A_k] = [A_1, A_2, \ldots, A_{k-1}, A_k'] \cdot [A_{k-1}, A_k],$$

dunque si ha, come volevasi,

$$[A_1, A_2, \ldots, A_k] = [A_1, \ldots, A_{k-2}, A_{k-1} + A_k] \cdot [A_{k-1}, A_k].$$

Suppongasi in secondo luogo che non sia

$$A_1 + A_2 + \dots + A_k = S$$

e si dica A' uno dei residui di $A_1 + A_2 + \dots + A_k$ rispetto ad S.

Sarà (n^0 8)

$$[A_1, A_2, \dots, A_k] = [A', A_1, \dots, A_k].$$

Ma per la dimostrazione compiuta è

$$[A', A_1, \dots, A_k] = [A', A_1, \dots, A_{k-2}, A_{k-1} + A_k] \cdot [A_{k-1}, A_k]$$

ed è, sempre per il n^0 8,

$$[A', A_1, \dots, A_{k-2}, A_{k-1} + A_k] = [A_1, \dots, A_{k-2}, A_{k-1} + A_k],$$

dunque resta, come volevasi,

$$[A_1, A_2, \dots, A_k] = [A_1, \dots, A_{k-2}, A_{k-1} + A_k] \cdot [A_{k-1}, A_k].$$

Il teorema ora stabilito può essere evidentemente generalizzato.

Così, per es., se A, B, C, D, E, F sono spazi razionali indipendenti di S si ha:

$$\begin{aligned}[A, B, C, D, E] &= [A, B, C + D + E] \cdot [C, D + E] \cdot [D, E] \\ &= [A, B, C + D + E] \cdot [C, D, E]\end{aligned}$$

e

$$[A, B, C, D, E, F] = [A + B, C + D, E + F] \cdot [A, B] \cdot [C, D] \cdot [E, F].$$

Più in generale:

Se è $l < k$, *il quoziente dei caratteri* $[A_1, A_2, \dots, A_k]$ *e* $[A_1, A_2, \dots, A_l]$ *è dato dal carattere*

$$[A_1 + A_2 + \dots + A_l, A_{l+1}, \dots, A_k].$$

10. Un'altra utile osservazione è la seguente:

Se A, B, C *sono spazi razionali indipendenti di* S *e* C' *è un residuo di* B *rispetto a* $B + C$, *è*

$$[A, B + C] = [A, B] \cdot [A + B, C'].$$

Infatti, per quanto è stato dimostrato nel n⁰ 9, è

$$[A+B,\ C]=\frac{[A,\ B,\ C]}{[A,\ B]};$$

ed è pure

$$[A,\ B+C]=[A,\ B,\ C].$$

11. Si supponga, riprendendo le ipotesi e le notazioni del n⁰ 4 che lo spazio

$$A=A_1+A_2+\dots+A_k$$

non coincida con lo spazio S e si fissi in A una base minima per i punti.

Allora se $(x_1, x_2, \dots, x_{r+1})$ è un elemento qualunque dell'insieme I relativo ad A, nel senso del n⁰ 1, ad esso viene a corrispondere un ben determinato gruppo di $t+1$ interi $(y_1, y_2, \dots, y_{t+1})$, cioè il gruppo degli interi che servono ad esprimere $(x_1, x_2, \dots, x_{r+1})$ mediante i $t+1$ elementi della fissata base minima di A, e $(y_1, y_2, \dots, y_{t+1})$ può considerarsi come il gruppo delle coordinate *in* A di un punto (razionale) di A.

Ciò porta che *entro* A si possono fare le stesse considerazioni che in S, riferendosi per i punti (razionali) di A ai gruppi di interi $(y_1, y_2, \dots, y_{t+1})$; e quindi si potrà parlare di un *carattere aritmetico* di $A_1, A_2, \dots, A_k$ *entro* lo spazio A.

Ebbene *questo carattere è sempre quello che più sopra è stato indicato con* $[A_1, A_2, \dots, A_k]$.

La cosa è evidente, se lo spazio A coincide con lo spazio A' rappresentato in S dalle equazioni

$$x_{t+2}=\dots=x_{r+1}=0,$$

e se a base minima in A' si sceglie quella formata dagli elementi $(x_1, x_2, \dots, x_{r+1})$ per cui tutti i numeri x_s sono nulli, tranne uno che cade fra i primi $t+1$ ed è eguale a 1.

In tal caso infatti, per i gruppi corrispondenti di interi $(x_1, x_2, \dots, x_{r+1})$ e $(y_1, y_2, \dots, y_{t+1})$ considerati più sopra, si ha

$$(x_1, x_2, \dots, x_{r+1})\equiv(y_1, y_2, \dots, y_{t+1}, 0, 0, \dots, 0),$$

e questa circostanza basta a giustificare immediatamente l'asserzione fatta.

Ma allora questa asserzione è valida anche se A non coincide con A', perchè ci si può sempre ridurre al caso precedente, fissando una base minima per i punti di S che contenga come parte la base minima fissata già per A, e poi effettuando in S una trasformazione di coordinate rappresentata da una sostituzione lineare a coefficienti interi e unimodulare, che muti la considerata base minima di S nella base minima formata dagli elementi $(x_1, x_2, \dots, x_{r+1})$ per cui tutti i numeri x_s sono nulli, tranne uno che è eguale a 1.

§ 3.

Un teorema sulle matrici riemanniane.

12. Il teorema che ora stabiliremo potrebbe esser dedotto per via incidentale dalle considerazioni che saranno fatte nel seguito sulle varietà abeliane; ma poichè esso interessa la teoria generale delle matrici riemanniane ci pare conveniente di darne una dimostrazione diretta.

13. *Se in una matrice riemanniana del genere p sono nulli tutti gli elementi secondo cui si incrociano q righe $(0 < q < p)$ e $2(p-q)$ colonne, gli elementi secondo cui si incrociano queste stesse colonne e le rimanenti $p-q$ righe costituiscono una matrice riemanniana del genere p.*

Sia

$$\omega \equiv \left\| \begin{array}{cccccccc} \omega_{1,1} & \omega_{1,2} & \dots & \omega_{1,2q} & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \omega_{q,1} & \omega_{q,2} & \dots & \omega_{q,2q} & 0 & 0 & \dots & 0 \\ \omega_{q+1,1} & \omega_{q+1,2} & \dots & \omega_{q+1,2q} & \omega_{q+1,2q+1} & \dots & & \omega_{q+1,2p} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \omega_{p,1} & \omega_{p,2} & \dots & \omega_{p,2q} & \omega_{p,2q+1} & \dots & & \omega_{p,2p} \end{array} \right\|$$

una matrice riemanniana del tipo detto nell'enunciato: si tratta di far vedere che anche la matrice

$$\omega_1 \equiv \left\| \begin{array}{ccc} \omega_{q+1,2q+1} & \dots & \omega_{q+1,2p} \\ \dots & \dots & \dots \\ \omega_{p,2q+1} & \dots & \omega_{p,2p} \end{array} \right\|$$

è riemanniana.

In uno spazio rappresentativo Σ, $(x_1, x_2, \ldots, x_{2p})$, a $2p-1$ dimensioni, siano τ e $\bar{\tau}$ le *imagini* di ω (6), sia Q lo spazio a $2q-1$ dimensioni congiungente i $2q$ vertici della piramide fondamentale delle coordinate, stabilite in Σ, aventi nulle le ultime $2(p-q)$ coordinate, e Q_1 lo spazio a $2(p-q)-1$ dimensioni congiungente i vertici rimanenti della piramide. Poi sia O_j il punto di τ avente per coordinate gli elementi della j^{ma} riga di ω.

I punti $O_1, O_2, \ldots, O_q$ sono situati nello spazio (razionale) Q, quindi Q è un *asse* (7) di ω (di genere q) e ω è impura (8).

I punti $O_{q+1}, \ldots, O_p$ determinano in τ uno S_{p-q-1} indipendente da Q, e quindi sono proiettati da Q su Q_1 in $p-q$ punti $O'_{q+1}, \ldots,$ $, \ldots, O'_p$ congiunti da uno S_{p-q-1} che indicheremo con α'. Naturalmente lo spazio α' sarà (al pari di τ) imaginario e sarà indipendente dallo spazio imaginario coniugato $\bar{\alpha}'$ situato al pari di esso nello spazio (razionale) Q_1.

Sia Q' un asse di ω *complementare* (9) a Q e si dicano α e $\bar{\alpha}$ gli S_{p-q-1} (imaginari coniugati) secondo cui Q' si appoggia a τ e $\bar{\tau}$; inoltre si indichi con σ un sistema nullo riemanniano di ω, certo esistente, che abbia per *asse* Q e che induca in Q' un sistema nullo riemanniano *principale* per Q' (10). Val quanto dire (11) (guardando al modo secondo cui σ opera non nello spazio Σ ma nella stella di vertice Q) che σ è un sistema nullo razionale nella stella di vertice Q, per il quale a un S_{2q} (imaginario) che congiunga Q con un punto, comunque scelto, di α risponde un iperpiano (per Q e per τ), il quale *non* contiene mai il corrispondente punto imaginario coniugato di $\bar{\alpha}$, cioè *non* contiene mai lo S_{2q} della stella Q (imaginario) coniugato a quello preso in esame.

Ma allora σ è *tagliato* da Q_1 in un sistema nullo razionale *non degenere*, trasformante in sè lo spazio α' e tale che per esso un punto comunque preso di α' è portato in un iperpiano (di Q_1) non contenente mai il punto imaginario coniugato di $\bar{\alpha}'$.

Ciò dimostra che α' e $\bar{\alpha}'$ sono *nello* spazio rappresentativo Q_1 le imagini di una matrice riemanniana del genere $p-q$.

(6) Loc. cit. 2), I, n⁰ 9.
(7) Loc. cit. 2), I, n⁰ 32.
(8) Loc. cit. 2), I, n⁰ 32.
(9) Loc. cit. 2), I, n⁰ 36.
(10) Loc. cit. 2), I, n^{i} 38, 31, 10.
(11) Loc. cit. 2), I, n⁰ 12.

Ora le coordinate *entro* Q_1 del punto O'_{q+l} $(l = 1, 2, \dots, p-q)$ si possono appunto supporre come date dagli elementi della l^{ma} riga di ω_1, dunque ω_1 è, come volevasi, una matrice riemanniana (avente per imagini, entro Q_1, α' e $\overline{\alpha}'$).

§ 4.

Le varietà abeliane contenenti congruenze abeliane.

14. Sia V_p una varietà abeliana della dimensione p immersa in un S_d e rappresentata parametricamente da

$$(12) \qquad \begin{cases} x_1 = f_1(u_1, u_2, \dots, u_p) \\ \dots\dots\dots \\ x_d = f_d(u_1, u_2, \dots, u_p) \end{cases}$$

dove le $f_1, \dots, f_d$ sono funzioni abeliane delle variabili indipendenti $u_1, \dots, u_p$ appartenenti a una matrice riemanniana

$$\omega \equiv \| \omega_{j,r} \| \qquad (j = 1, \dots, p; r = 1, \dots, 2p).$$

Data V_p, la matrice ω è individuata di fronte alla relazione di *equivalenza* (12); e viceversa, data ω, V_p è individuata di fronte alle trasformazioni birazionali.

15. Supponiamo ora che la matrice ω sia impura e dette τ e $\overline{\tau}$ le imagini di ω nello S_{2p-1} rappresentativo Σ, sia Q un asse di ω del genere $q\,(0 < q < p)$, cioè un S_{2q-1} *razionale* di Σ appoggiato a τ (o $\overline{\tau}$) secondo un S_{q-1}.

Applicando, ove occorra, ad ω un'*operazione A* (13), cioè effettuando, ove occorra, una sostituzione lineare omogenea propria sulle variabili $u_1, u_2, \dots, u_p$, si può supporre che le prime q righe di ω, formate coi periodi riferentisi alle variabili $u_1, \dots, u_q$, siano costituite dalle coordinate di q punti indipendenti comuni a τ e Q; dopo di che, se

$$(13) \qquad [\xi_1^{(\mu)}, \xi_2^{(\mu)}, \dots, \xi_{2p}^{(\mu)}] \qquad [\mu = 1, \dots, 2(p-q)]$$

(12) Loc. cit. 2), I, n° 2.

(13) Loc. cit. 2), I, n° 1.

sono i $2(p-q)$ elementi di una base minima per gli iperpiani contenenti Q si ha

$$(14) \qquad \xi_1^{(\mu)}\omega_{l,1}+\xi_2^{(\mu)}\omega_{l,2}+\dots+\xi_{2p}^{(\mu)}\omega_{l,2p}=0 \qquad \begin{bmatrix}\mu=1,\dots,2(p-q)\\ l=1,\dots,q\end{bmatrix}$$

e i minori d'ordine massimo della matrice le cui righe sono date dagli elementi (13) sono numeri (interi) primi fra di loro.

Ciò posto si considerino tutti i punti $(u_1, u_2, \dots, u_p)$ di V_p per cui è

$$(15) \qquad u_1=c_1, \qquad u_2=c_2, \dots, u_q=c_q$$

essendo $c_1, c_2, \dots, c_q$ delle costanti comunque assegnate.

Il loro luogo è una varietà abeliana (della dimensione $p-q$).

Infatti si costruisca, come è certo possibile [cfr. la nota (4) a piè di pagina], una matrice unimodulare a elementi interi d'ordine $2p$

$$(16) \qquad \| \xi_1^{(r)}, \xi_2^{(r)}, \dots, \xi_{2p}^{(r)} \| \qquad (r=1,\dots,2p)$$

le cui prime $2(p-q)$ righe siano date dagli elementi (13), e si ponga

$$(17) \qquad \Omega_{j,r}=\xi_1^{(r)}\omega_{j,1}+\xi_2^{(r)}\omega_{j,2}+\dots+\xi_{2p}^{(r)}\omega_{j,2p}.$$

La matrice

$$\Omega=\|\Omega_{j,r}\|$$

sarà una matrice riemanniana equivalente ad ω, perchè dedotta da ω con un'*operazione* B (14) unimodulare; e le funzioni abeliane $f_1, \dots, f_d$ che intervengono nella rappresentazione parametrica di V_p potranno anche riguardarsi come appartenenti alla matrice Ω.

Intanto, grazie alle (14), nella matrice Ω è

$$(18) \qquad \Omega_{j,r}=0 \qquad [j=1,\dots,q; r=1,\dots,2(p-q)],$$

(14) Loc. cit. 2), I, n[i] 1 e 2.

quindi la matrice

$$\Omega_1 = \begin{Vmatrix} \Omega_{q+1,1} & \ldots & \Omega_{q+1,2(p-q)} \\ \cdot & \cdot & \cdot \\ \Omega_{p,1} & \ldots & \Omega_{p,2(p-q)} \end{Vmatrix}$$

è (n⁰ 13) una matrice riemanniana del genere $p - q$.

In virtù delle (18), le funzioni

$$f_1(c_1, \ldots, c_q, u_{q+1}, \ldots, u_p), \ldots, f_d(c_1, \ldots, c_q, u_{q+1}, \ldots, u_p)$$

delle variabili indipendenti $u_{q+1}, \ldots, u_p$ sono funzioni abeliane appartenenti alla matrice Ω_1, dunque il nostro luogo è intanto una varietà *algebrica* a $p - q$ dimensioni, V_{p-q}, rappresentabile parametricamente per funzioni abeliane.

Per dimostrare che esso è addirittura una varietà *abeliana* (15) resta a far vedere che se a due gruppi di valori $(u'_{q+1}, \ldots, u'_p)$ e $(u''_{q+1}, \ldots, u''_p)$ delle variabili $u_{q+1}, \ldots, u_p$ risponde uno stesso punto di V_{p-q}, questi due gruppi di valori sono congrui rispetto alla matrice Ω_1 (16).

Ora ciò è immediato; infatti da

$$\begin{gathered} f_1(c_1, \ldots, c_q, u'_{q+1}, \ldots, u'_p) = f_1(c_1, \ldots, c_q, u''_{q+1}, \ldots, u''_p) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ f_d(c_1, \ldots, c_q, u'_{q+1}, \ldots, u'_p) = f_d(c_1, \ldots, c_q, u''_{q+1}, \ldots, u''_p) \end{gathered}$$

in base al fatto che V_p è abeliana, segue che i due gruppi di numeri

$$(c_1, \ldots, c_q, u'_{q+1}, \ldots, u'_p), \qquad (c_1, \ldots, c_q, u''_{q+1}, \ldots, u''_p)$$

sono congrui rispetto a ω, cioè rispetto a Ω, e quindi debbono esistere degli interi $a_1, a_2, \ldots, a_{2p}$ sì che risulti

$$(19) \quad \left\{ \begin{aligned} 0 &= \qquad a_{2(p-q)+1}\Omega_{l,2(p-q)+1} + \ldots + a_{2p}\Omega_{l,2p} \\ &\qquad\qquad (l = 1, \ldots, q) \\ u'_{q+m} - u''_{q+m} &= a_1\Omega_{q+m,1} + \ldots + a_{2(p-q)}\Omega_{q+m,2(p-q)} + \ldots + a_{2p}\Omega_{q+m,2p} \\ &\qquad\qquad (m = 1, \ldots, p-q). \end{aligned} \right.$$

(15) Vedi l'annotazione 2).

(16) Per la definizione di questo tipo di *congruenza* veggasi G. SCORZA, *Alcune questioni di geometria sopra una varietà abeliana qualunque* [Atti dell'Accademia Gioenia di Scienze Naturali in Catania. Serie 5ª, vol. XI (1918), Memoria XX].

Ma siccome la matrice

$$\Omega_2 \equiv \begin{Vmatrix} \Omega_{1,2(p-q)+1} & \cdot & \cdot & \cdot & \Omega_{1,2p} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \Omega_{q,2(p-q)+1} & \cdot & \cdot & \cdot & \Omega_{q,2p} \end{Vmatrix}$$

è riemanniana, le prime q relazioni (19) non possono coesistere se non a patto che sia

$$a_{2(p-q)+1} = a_{2(p-q)+2} = \dots = a_{2p} = 0\,;$$

dunque resta

$$u'_{q+m} - u''_{q+m} = a_1\, \Omega_{q+m,1} + \dots + a_{2(p-q)}\, \Omega_{q+m,2(p-q)} \quad (m = 1, \dots, p-q),$$

cioè si ha, come volevasi, che i gruppi di numeri $(u'_{q+1}, \dots, u'_p)$ e $(u''_{q+1}, \dots, u''_p)$ sono congrui rispetto ad Ω_1.

16. Adesso suppongasi di far variare nelle (15) le costanti $c_1, \dots, c_q$ in tutte le maniere possibili. La V_{p-q} di V_p da esse rappresentata varierà in una totalità ∞^q, Σ_q, e le posizioni assunte da V_{p-q} saranno tutte birazionalmente identiche, perchè appartenenti tutte alla matrice riemanniana Ω_1.

Le V_{p-q} di Σ_q possono ottenersi applicando a una qualunque di esse le singole trasformazioni birazionali di 2ª specie di V_p in sè (17); da ciò risulta di nuovo che esse sono tutte birazionalmente identiche e risulta pure che Σ_q è una totalità *algebrica* ∞^q.

Delle V_{p-q} di Σ_q ne passa una ed una sola per ciascun punto di V_p; quindi Σ_q è ciò che dicesi una *congruenza* (18) di V_{p-q} situata su V_p.

Aggiungasi che:

La congruenza Σ_q, concepita come insieme delle sue V_{p-q}, è una varietà abeliana della dimensione q appartenente alla matrice riemanniana Ω_1.

(17) Cfr. G. Castelnuovo, *Sugli integrali semplici appartenenti ad una superficie irregolare* [Rendiconti della R. Accademia dei Lincei, serie V, vol. XIV, I° semestre 1905, pp. 545-556, 593-598, 655-663], pag. 597. Avvertasi che il Castelnuovo dice di 1ª specie le trasformazioni che qui vengon dette di 2ª specie.

(18) Denominazione introdotta dal compianto Dr. R. Torelli nella sua Memoria: *Sulle serie algebriche semplicemente infinite di gruppi di punti appartenenti a una curva algebrica* [Rendiconti del Circolo Matematico di Palermo, t. XXXVII (I° semestre 1914), pp. 25-46], n° 7.

Infatti si riscontra subito che due V_{p-q} di Σ_q corrispondenti ai due sistemi di valori $(c'_1, c'_2, \dots, c'_q)$, $(c''_1, c''_2, \dots, c''_q)$ per le costanti $c_1, c_2, \dots, c_q$ coincidono quando e solo quando quei due sistemi sono congrui rispetto alla matrice Ω_1.

Infine si osservi che le matrici Ω_1 e Ω_2 sono entrambe individuate di fronte alla relazione di equivalenza appena sia dato l'asse Q di ω.

17. Le osservazioni dei n[i] 15 e 16 possono esser raccolte nel seguente teorema:

La varietà abeliana V_p, in corrispondenza a ciascun asse del genere q della matrice riemanniana ω, contiene una congruenza abeliana ∞^q di varietà abeliane, birazionalmente identiche, della dimensione $p-q$; l'asse e la congruenza individuandosi reciprocamente.

Inversamente, suppongasi che la varietà abeliana V_p contenga una congruenza ∞^q di varietà della dimensione $p-q$ $(0 < q < p)$, la congruenza avendo il genere q, se $q = 1$ (cioè essendo in tal caso un fascio ellittico), o l'irregolarità superficiale q, se $q > 1$,

Allora, per una osservazione ben nota V_p contiene, corrispondentemente alla congruenza, un sistema regolare ∞^{q-1} di integrali (semplici, di 1[a] specie) riducibili, per cui le varietà della congruenza sono le varietà di livello costante.

Segue che V_p appartiene a una matrice riemanniana dotata di assi ([19]) e che la congruenza coincide con una delle congruenze abeliane individuate su V_p dagli assi della matrice o è una *involuzione* in una di codeste congruenze.

Abbiamo pertanto il teorema:

Condizione necessaria e sufficiente perchè una varietà abeliana contenga congruenze abeliane è che essa (appartenga a una matrice riemanniana impura, cioè) sia impura; nel qual caso vi è corrispondenza biunivoca tra gli assi della matrice e le congruenze abeliane di varietà abeliane appartenenti alla varietà considerata.

18. Ferme rimanendo le ipotesi fatte nel n[0] 15 su ω e sulle variabili $u_1, \dots, u_q$, diciamo Q' un asse di ω complementare a Q, e supponiamo che nella matrice ω le righe rispondenti alle variabili $u_{q+1}, \dots, u_p$ siano formate dalle coordinate di $p-q$ punti indipendenti dello S_{p-q-1} secondo cui Q' si appoggia a τ.

([19]) Loc. cit. [2]), annotazione 36).

Ciò corrisponde ad imaginare eseguita, ove occorra, sulle u_1, $u_2, \ldots, u_p$ una sostituzione lineare omogenea propria che lasci *ferme* le variabili $u_1, u_2, \ldots u_q$; e dunque l'ipotesi ulteriore ora fatta può essere introdotta senza alterare la circostanza che le equazioni

$$u_1 = c_1, \quad u_2 = c_2, \ldots, u_q = c_q$$

rappresentano su V_p, fissate le costanti $c_1, c_2, \ldots, c_q$, una varietà abeliana V_{p-q} della dimensione $p - q$.

Ma adesso per le variabili $u_{q+1}, \ldots, u_p$ può esser ripetuto lo stesso ragionamento che nel n⁰ 15 è stato fatto per le variabili $u_1, u_2, \ldots, u_q$ e quindi le equazioni

$$u_{q+1} = \gamma_{q+1}, \ldots, u_p = \gamma_p,$$

dove le γ sono costanti comunque assegnate, rappresentano su V_p una varietà abeliana V_q della dimensione q.

Come abbiamo già indicata con Σ_q la congruenza abeliana ∞^q descritta da V_{p-q} al variare delle costanti $c_1, \ldots, c_q$, così diciamo Σ_{p-q} la congruenza abeliana ∞^{p-q} descritta da V_q al variare delle costanti $\gamma_{q+1}, \ldots, \gamma_p$.

Ebbene:

Una varietà di Σ_q e una varietà di Σ_{p-q} hanno un numero finito (non nullo) di punti comuni eguale all'invariante aritmetico degli assi Q e Q' di ω.

Supponiamo sempre che gli elementi (13) costituiscano una base minima per gli iperpiani contenenti Q, e siano

$$[\xi_1^{(\mu)}, \xi_2^{(\mu)}, \ldots, \xi_{2p}^{(\mu)}] \qquad [\mu = 2(p-q)+1, \ldots, 2p] \tag{20}$$

gli elementi di una base minima per gli iperpiani contenenti Q'.

Poi siano

$$\begin{gathered} x_1 = f_1(c_1, \ldots, c_q, u_{q+1}, \ldots, u_p) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_d = f_d(c_1, \ldots, c_q, u_{q+1}, \ldots, u_p) \end{gathered}$$

le equazioni parametriche di una varietà V_{p-q} di Σ_q e

$$\begin{gathered} x_1 = f_1(u_1, \ldots, u_q, \gamma_{q+1}, \ldots, \gamma_p) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_d = f_d(u_1, \ldots, u_q, \gamma_{q+1}, \ldots, \gamma_p) \end{gathered}$$

le equazioni parametriche di una varietà V_q di Σ_{p-q}.

Perchè il punto $(u_1, \dots, u_q, \gamma_{q+1}, \dots \gamma_p)$ di V_q coincida col punto $(c_1, \dots, c_q, u_{q+1}, \dots, u_p)$ di V_{p-q} occorre e basta che sia

$$(21) \qquad \begin{cases} c_l = u_l + \sum\limits_r^{1\dots 2p} \varrho_r \, \omega_{l,r} & (l = 1, \dots, q) \\ u_{q+m} = \gamma_{q+m} + \sum\limits_r^{1\dots 2p} \varrho_r \, \omega_{q+m,r} & (m = 1, \dots, p-q) \end{cases}$$

con le $\varrho_1, \varrho_2, \dots, \varrho_{2p}$ intere; quindi i punti comuni a V_q e V_{p-q} sono tanti quanti sono i gruppi di valori per le variabili $u_{q+1}, \dots, u_q$ incongrui rispetto alla matrice Ω_1 forniti dalle ultime $p-q$ equazioni (21), al variare in tutte le maniere possibili degli interi ϱ_1, $\varrho_2, \dots, \varrho_{2p}$.

Siano $(u'_{q+1}, \dots, u'_p)$ e $(u''_{q+1}, \dots, u''_p)$ i gruppi di valori per le nostre variabili rispondenti ai due sistemi di interi $(\varrho'_1, \varrho'_2, \dots, \varrho'_{2p})$ e $(\varrho''_1, \varrho''_2, \dots, \varrho''_{2p})$.

Perchè essi risultino congrui rispetto ad Ω_1 occorre e basta che sia

$$\sum_r^{1\dots 2p} (\varrho'_r - \varrho''_r)\, \omega_{q+m,r} = \sum_\mu^{1\dots 2(p-q)} \lambda_\mu \, \Omega_{q+m,\mu} \quad (m = 1, \dots, p-q),$$

con le $\lambda_1, \dots, \lambda_{2(p-q)}$ intere; ma, per le (17),

$$\Omega_{q+m,\mu} = \sum_r^{1\dots 2p} \xi_r^{(\mu)} \, \omega_{q+m,r},$$

dunque occorre e basta che sia

$$(22) \qquad \sum_r^{1\dots 2p} \left[\varrho'_r - \varrho''_r - \sum_\mu^{1\dots 2(p-q)} \lambda_\mu \, \xi_r^{(\mu)} \right] \omega_{q+m,r} = 0.$$

Ora gli elementi (20) costituiscono una base minima per gli iperpiani di Q', dunque le (22) non possono coesistere se non a patto che esistano degli interi $\lambda_{2p-q+1}, \dots, \lambda_{2p}$ tali che sia

$$\varrho'_r - \varrho''_r - \sum_\mu^{1\dots 2(p-q)} \lambda_\mu \, \xi_r^{(\mu)} = \sum_{\nu=2(p-q)+1}^{\nu=2p} \lambda_\nu \, \xi_r^{(\nu)} \qquad (r = 1, \dots, 2p)$$

cioè

$$(23) \qquad \varrho'_r - \varrho''_r = \sum_s^{1\dots 2p} \lambda_s \, \xi_r^{(s)} \qquad (r = 1, \dots, 2p).$$

Ora si indichi con Δ il determinante della matrice quadrata

$$\| \xi_r^{(1)}, \xi_r^{(2)}, \dots, \xi_r^{(2p)} \| \qquad (r = 1, \dots, 2p)$$

per modo che $|\Delta|$ (n^0 4, in fine) sarà l'invariante aritmetico di Q e Q', e si indichi con $X_r^{(s)}$ l'aggiunto di $\xi_r^{(s)}$ in Δ.

Allora le (23) equivalgono alle:

$$\Delta \lambda_s = \sum_r^{1\dots 2p} X_r^{(s)} (\varrho_r' - \varrho_r'') \qquad (s = 1, \dots, 2p);$$

e quindi infine perchè i sistemi di valori $(u_{q+1}', \dots, u_p')$ e $(u_{q+1}'', \dots u_p'')$ risultino congrui rispetto a Ω_1 occorre e basta che sia, rispetto al modulo $|\Delta|$,

$$\sum_r^{1\dots 2p} X_r^{(s)} (\varrho_r' - \varrho_r'') \equiv 0 \qquad (s = 1, \dots, 2p). \tag{24}$$

Di qua risulta in primo luogo che nelle ultime $p-q$ equazioni (21) gli interi $\varrho_1, \varrho_2, \dots, \varrho_{2p}$ posson esser calcolati, per il nostro scopo, rispetto al modulo $|\Delta|$; poi, che due sistemi di valori $(\varrho_1', \dots, \varrho_{2p}')$ e $(\varrho_1'', \dots, \varrho_{2p}'')$ per le ϱ_r, incongrui rispetto a $|\Delta|$, dànno luogo a uno stesso punto di V_{p-q} se le differenze $\varrho_r' - \varrho_r''$ costituiscono una soluzione delle congruenze (24).

Ora le (24), concepite come congruenze nelle incognite $\varrho_r' - \varrho_r''$, ammettono $|\Delta|^{2p-1}$ soluzioni incongrue rispetto al modulo $|\Delta|$ ([20]), dunque infine il numero dei punti comuni a V_{p-q} e V_q è dato, come volevasi, da

$$\frac{|\Delta|^{2p}}{|\Delta|^{2p-1}} = |\Delta|.$$

19. Il fatto che i $|\Delta|$ punti comuni a V_{p-q} e V_q sono dati su V_{p-q} dai gruppi di valori per le variabili $(u_{q+1}, \dots, u_p)$, forniti dalle ultime $p-q$ equazioni (21) ponendo per $(\varrho_1, \dots, \varrho_{2p})$ certi $|\Delta|$ sistemi di $2p$ interi, *indipendenti* dalla considerata V_q di Σ_{p-q}, significa evidentemente che:

Le ∞^{p-q} V_q di Σ_{p-q} segnano sopra ciascuna V_{p-q} di Σ_q un'involuzione abeliana di ordine $|\Delta|$, birazionalmente identica a Σ_{p-q}, ge-

([20]) Veggasi per es. A. KRAZER, *Lehrbuch der Thetafunktionen* (Leipzig, Teubner, 1903), pag. 59.

nerabile sulla V_{p-q} mediante un gruppo d'ordine $|\Delta|$ di trasformazioni birazionali (periodiche) di 2^a specie.

Notisi che la matrice riemanniana cui appartiene Σ_{p-q} è isomorfa a quella cui appartengono le V_{p-q} di Σ_q (21); dalla quale osservazione si può dedurre, volendo, una nuova dimostrazione del teorema, già noto, che *se Q ammette più assi complementari* (nel qual caso ne ammette senz'altro infiniti) *questi assi sono tutti isomorfi tra di loro* (22).

20. Il teorema stabilito nel n⁰ 18 è suscettibile di una notevole generalizzazione, alla quale guidano le seguenti osservazioni.

In primo luogo si vede subito che:

α) *Se Σ_{q_1} e Σ_{q_2} sono le due congruenze abeliane di V_p rispondenti a due assi di ω, Q_1 e Q_2, dei generi q_1 e q_2, che non abbiano come spazio congiungente lo spazio rappresentativo di ω, Σ_{q_1} e Σ_{q_2} sono entrambe composte con la congruenza abeliana Σ_q di V_p rispondente all'asse Q di ω, di genere q, che congiunge Q_1 e Q_2;*

e che:

β) *Se Σ_{q_1} e Σ_{q_2} sono le due congruenze abeliane di V_q rispondenti a due assi non indipendenti di ω, Q_1 e Q_2, la congruenza abeliana $\Sigma_{q'}$ di V_p rispondente all'asse Q' di ω, intersezione di Q_1 e Q_2, è composta tanto con Σ_{q_1} quanto con Σ_{q_2};*

dove, secondo l'uso, una congruenza si dice *composta* con un'altra se ciascuna varietà della prima contiene ogni varietà della seconda di cui contenga un punto.

21. Ciò premesso, si supponga che gli assi Q_1 e Q_2 di ω, di cui si parla nell'enunciato α), siano indipendenti. Allora l'asse congiungente Q è del genere $q = q_1 + q_2$, ogni varietà abeliana V_{p-q_1} di Σ_{q_1} è luogo di ∞^{q_2} varietà abeliane V_{p-q} o $V_{p-q_1-q_2}$ di Σ_q e ogni varietà abeliana V_{p-q_2} di Σ_{q_2} è luogo di ∞^{q_1} varietà abeliane $V_{p-q_1-q_2}$ di Σ_q.

Insomma, *entro* la varietà abeliana ∞^q Σ_q (i cui elementi sono delle $V_{p-q_1-q_2}$), Σ_{q_1} e Σ_{q_2} possono considerarsi come due *congruenze* aventi con essa la stessa relazione, che le congruenze Σ_q e Σ_{p-q} del n⁰ 18 avevano con V_p.

Di qua si ricava facilmente che:

(21) Loc. cit. (2), annotazione (20), (5).

(22) Loc. cit. (2), I, n⁰ 43.

Nelle ipotesi attuali l'invariante aritmetico di Q_1 e Q_2 è il numero delle $V_{p-q_1-q_2}$ di Σ_q comuni a una V_{p-q_1} di Σ_{q_1} e una V_{p-q_2} di Σ_{q_2}.

Per convincersene basta infatti supporre, come è lecito, che l'asse Q sia lo spazio di Σ congiungente i vertici della piramide fondamentale delle coordinate che hanno tutti nulle certe $2(p-q)$ coordinate fissate a piacere, per modo da mettere in evidenza e la matrice riemanniana cui appartiene Σ_q e il fatto che per questa matrice Q si può considerare come lo spazio rappresentativo e Q_1 e Q_2 si possono riguardare come due assi.

22. Adesso, tenute ferme le ipotesi e le notazioni del n⁰ precedente, si supponga che Q_3 sia un asse di ω complementare a Q.

Se q_3 è il genere di Q_3, sarà

$$q_1 + q_2 + q_3 = q + q_3 = p,$$

e a Q_3 risponderà su V_p una congruenza ∞^{q_3} Σ_{q_3} di varietà abeliane $V_{q_1+q_2}$ o V_{p-q_3} della dimensione $q_1 + q_2 = p - q_3$.

Il numero dei punti in cui una $V_{p-q_1-q_2}$ di Σ_q incontra una $V_{q_1+q_2}$ di Σ_{q_3}, per il teorema del n⁰ 18, è dato dall'invariante aritmetico

$$[Q, Q_3] = [Q_1 + Q_2, Q_3],$$

e il numero delle $V_{p-q_1-q_2}$ di Σ_q in cui si tagliano una V_{p-q_1} di Σ_{q_1} e una V_{p-q_2} di Σ_{q_2} è dato dall'invariante aritmetico

$$[Q_1, Q_2],$$

dunque *il numero dei punti comuni a una V_{p-q_1} di Σ_{q_1}, una V_{p-q_2} di Σ_{q_2} e una V_{p-q_3} di Σ_{q_3} è dato da*

$$[Q_1, Q_2] \cdot [Q_1 + Q_2, Q_3],$$

cioè (n⁰ 9) *da*

$$[Q_1, Q_2, Q_3].$$

23. Ormai è evidente come procedendo di passo in passo si possano generalizzare ulteriormente le proposizioni ottenute nei n¹ 21 e 22, per modo da arrivare al seguente teorema:

Se $Q_1, Q_2, \dots, Q_t$ sono t assi indipendenti di ω, dei generi q_1, $q_2, \dots, q_t$ e $\Sigma_{q_1}, \Sigma_{q_2}, \dots, \Sigma_{q_t}$ sono le congruenze abeliane di V_p che ad essi corrispondono, t varietà appartenenti rispettivamente a queste t

congruenze si tagliano in un numero finito di punti, se è $q_1 + q_2 + \dots + q_t = p$ *o in un numero finito di varietà abeliane della congruenza* $\Sigma_{q_1+q_2+\dots+q_t}$ *di* V_p *corrispondente all'asse* $Q_1 + Q_2 + \dots + Q_t$, *se è* $q_1 + q_2 + \dots + q_t < p$; *e questo numero è dato in ogni caso dall'invariante aritmetico*

$$[Q_1, Q_2, \dots, Q_t].$$

§ 5.

Applicazioni alle superficie iperellittiche con fasci ellittici di curve ellittiche.

24. I teoremi esposti nel § 4 sono suscettibili di svariate applicazioni; qui basti indicarne alcune relative al caso delle superficie iperellittiche.

25. Una superficie iperellittica F contenga fasci ellittici di curve ellittiche (23).

Allora essa apparterrà a una matrice riemanniana di genere 2 dotata di assi; a ciascun fascio ellittico situato sulla superficie risponderà un asse della matrice (che sarà una retta), e, viceversa, a ciascun tale asse risponderà un fascio ellittico situato sulla superficie.

Se l'indice di singolarità (certo positivo) (24) della matrice, o di F, è 1, la matrice non avrà che due assi e la superficie non conterrà che due fasci ellittici di curve ellittiche. Se invece quell'indice è 2 o 3 (25), gli assi della matrice e i fasci ellittici della superficie sono infiniti.

In ogni caso, se le coordinate minime (n^0 2) di due assi distinti a e b della matrice sono date da

$$a_{r,s} \quad \text{e} \quad b_{r,s} \qquad (r, s = 1, 2, 3, 4),$$

dove, secondo il solito, è

$$a_{r,s} + a_{s,r} = 0, \; b_{r,s} + b_{s,r} = 0,$$

(23) È noto che se una superficie iperellittica contiene fasci irrazionali questi sono ellittici, e che le loro curve sono ellittiche, se sono irriducibili.

(24) Loc. cit. (2), I, n^0 32.

(25) Nè, come è ben noto, può essere maggiore di 3.

e inoltre

$$(aa) \equiv a_{12}\, a_{34} + a_{13}\, a_{42} + a_{14}\, a_{23} = 0,$$

$$(bb) \equiv b_{12}\, b_{34} + b_{13}\, b_{42} + b_{14}\, b_{23} = 0,$$

il numero N dei punti, in cui una curva del fascio A rispondente all'asse a incontra una curva del fascio B rispondente all'asse b, è dato (n° 18) dall'invariante aritmetico di a e b cioè dal valore assoluto dell'espressione

$$(ab) \equiv a_{12}\, b_{34} + a_{13}\, b_{42} + a_{14}\, b_{23} + a_{34}\, b_{12} + a_{42}\, b_{13} + a_{23}\, b_{14}\,.$$

26. *Se la superficie F contiene infiniti fasci ellittici, quali sono gli infiniti valori di cui è suscettibile l'intero N al variare di A e B tra gli infiniti fasci di F?*

La risposta è ormai presso che immediata.

Si dica k ($= 2, 3$) l'indice di singolarità di F o della matrice a cui F appartiene, e siano

$$C_j \equiv \sum_{r,s}^{1\ldots 4} c_{r,s}^{(j)}\, x_r\, y_s \qquad (j = 0, 1, \ldots, k)$$

$k + 1$ forme riemanniane alternate intere (primitive) indipendenti della matrice, costituenti una *base minima* per l'insieme delle forme riemanniane alternate intere della matrice stessa ([26]); cosicchè queste forme saranno date tutte e ciascuna una volta sola da

$$C = \lambda_0\, C_0 + \lambda_1\, C_1 + \ldots + \lambda_k\, C_k$$

al variare degli interi $\lambda_0, \lambda_1, \ldots, \lambda_k$ e gli assi della matrice risponderanno alle forme C, che risultano degeneri (ma non identicamente nulle).

Ora se si indica con δ_j lo pfaffiano del determinante (emisimmetrico) di C_j e con $I_{j,l}$ l'invariante simultaneo bilineare delle forme C_j e C_l ([27]), lo pfaffiano di C è dato da

$$\delta_0\, \lambda_0^2 + \ldots + \delta_k\, \lambda_k^2 + I_{0,1}\, \lambda_0\, \lambda_1 + \ldots + I_{k-1,k}\, \lambda_{k-1}\, \lambda_k\,,$$

([26]) Loc. cit. ([2]), I, n° 19.

([27]) Cfr. loc. cit. ([2]), II, n° 14.

dunque gli assi della matrice risponderanno alle forme C per cui gli interi $\lambda_0, \dots \lambda_k$ non sono tutti nulli e soddisfanno all'equazione

$$(25) \qquad \delta_0 \lambda_0^2 + \dots + \delta_k \lambda_k^2 + I_{0,1} \lambda_0 \lambda_1 + \dots + I_{k-1,k} \lambda_{k-1} \lambda_k = 0.$$

Siano $(\lambda_0', \dots, \lambda_k')$ e $(\lambda_0'', \dots, \lambda_k'')$ due soluzioni con numeri interi *primi fra loro* (e quindi non tutti nulli) dell'equazione (25), e supponiamo che esse siano *essenzialmente distinte*, cioè diverse e non differenti soltanto per un cambiamento simultaneo di segni.

Allora ad esse risponderanno due assi distinti A' e A'' della matrice le cui coordinate minime saranno date da

$$\sum_j^{0\dots k} \lambda_j' c_{r,s}^{(j)} \quad \text{e} \quad \sum_j^{0\dots k} \lambda_j'' c_{r,s}^{(j)} \qquad (r, s = 1, 2, 3, 4)$$

e quindi il numero N relativo ai fasci di F corrispondenti agli assi A' e A'' sarà dato dal valore assoluto dell'espressione

$$(26) \quad 2\delta_0\lambda_0'\lambda_0'' + \dots + 2\delta_k\lambda_k'\lambda_k'' + I_{0,1}(\lambda_0'\lambda_1'' + \lambda_1'\lambda_0'') + \dots + I_{k-1,k}(\lambda_{k-1}'\lambda_k'' + \lambda_k'\lambda_{k-1}'').$$

Segue che:

Gli infiniti valori di N richiesti più sopra sono dati tutti dal valore assoluto della (26) *quando vi si pongano per* $(\lambda_0', \dots, \lambda_k')$ *e* $(\lambda_0'', \dots, \lambda_k'')$ *tutte le possibili coppie essenzialmente distinte di soluzioni della* (25) *con numeri interi primi fra loro.*

27. Il teorema generale or ora stabilito è suscettibile in taluni casi particolari di un enunciato o più semplice o più espressivo.

Suppongasi ad es. che F sia la varietà delle coppie ordinate di punti di una curva ellittica C, per modo che la matrice cui appartiene F si potrà supporre della forma

$$\omega \equiv \begin{Vmatrix} 1 & \tau & 0 & 0 \\ 0 & 0 & 1 & \tau \end{Vmatrix},$$

dove τ è un numero imaginario, non quadratico se C non è singolare, quadratico se C è singolare.

Poniamoci nella prima alternativa.

Allora l'indice di singolarità di F è 2, tre forme riemanniane alternate intere formanti base minima per ω sono

$$C_0 \equiv x_1y_2 - x_2y_1\,;\; C_1 \equiv x_3y_4 - x_4y_3\,;\; C_2 \equiv (x_1y_4 - x_4\,y_1) - (x_2y_3 - x_3y_2),$$

e per queste è

$$\delta_0 = 0\,; \quad \delta_1 = 0, \quad \delta_2 = -1\,; \quad I_{0,1} = 1, \quad I_{1,2} = 0, \quad I_{0,2} = 0\,;$$

dunque l'equazione (25) è data qui da:

$$\lambda_0\lambda_1 - \lambda_2^2 = 0. \tag{27}$$

Le soluzioni intere della (27) con numeri primi fra loro sono date tutte dalle formule

$$\lambda_0 = \eta x^2, \qquad \lambda_1 = \eta y^2, \qquad \lambda_2 = xy \qquad (\eta = \pm 1) \tag{28}$$

ponendovi per x e y due interi qualunque primi fra loro, dunque nel caso attuale i valori di N sono dati tutti da:

$$N = (x'y'' - \eta\, x''y')^2$$

ponendovi per (x', y') e (x'', y'') due qualunque coppie (ordinate) di interi primi fra loro cui rispondano soluzioni della (27) essenzialmente distinte; cioè, in sostanza, dagli interi della successione

$$1, \quad 4, \quad 9, \quad 16, \ldots$$

Si ha pertanto il teorema:

Sopra una superficie iperellittica che rappresenti la varietà delle coppie ordinate di punti di una curva ellittica non singolare esistono infiniti fasci ellittici di curve ellittiche, ma il numero dei punti comuni a due curve situate in fasci differenti è sempre un quadrato perfetto. Di più fissato comunque il fascio cui appartiene una delle due curve si può sempre (e in infinite maniere diverse) scegliere quello cui appartiene l'altra per modo che quel numero sia un qualunque quadrato (positivo) assegnato.

28. Supponiamo adesso che C sia singolare e sia

$$P\tau^2 + Q\tau + R = 0 \qquad (P > 0,\ 4PR - Q^2 > 0)$$

l'equazione quadratica a coefficienti interi primi fra loro cui soddisfa τ.

Allora F è tre volte singolare; quattro forme riemanniane alternate intere formanti base minima per ω sono

$$C_0 \equiv x_1y_2 - x_2y_1, \quad C_1 \equiv x_3y_4 - x_4y_3, \quad C_2 \equiv (x_1y_4 - x_4y_1) - (x_2y_3 - x_3y_2),$$
$$C_3 \equiv P(x_2y_4 - x_4y_2) + Q(x_1y_4 - x_4y_1) + R(x_1y_3 - x_3y_1),$$

e per queste è

$$\delta_0 = 0, \quad \delta_1 = 0, \quad \delta_2 = -1, \quad \delta_3 = -PR, \quad I_{0,1} = 1, \quad I_{0,2} = 0, \quad I_{0,3} = 0,$$
$$I_{1,2} = 0, \qquad I_{1,3} = 0, \qquad I_{2,3} = -Q;$$

dunque l'equazione (25) diventa

$$-\lambda_2^2 - PR\lambda_3^2 + \lambda_0\lambda_1 - Q\lambda_2\lambda_3 = 0. \tag{29}$$

Indicando, secondo l'uso, con

$$D(a, b, \dots, l)$$

il massimo comun divisore degli interi (non tutti nulli) $a, b, \dots, l$, le soluzioni della (29) con numeri interi primi fra loro sono date tutte dalle formule ([28])

$$\left\{\begin{aligned} \lambda_0 &= \eta \frac{y^2 + Qyz + PRz^2}{D(x, y^2 + Qyz + PRz^2)} \\ \lambda_1 &= \eta \frac{x^2}{D(x, y^2 + Qyz + PRz^2)} \\ \lambda_2 &= \eta \frac{xy}{D(x, y^2 + Qyz + PRz^2)} \\ \lambda_3 &= \eta \frac{xy}{D(x, y^2 + Qyz + PRz^2)} \end{aligned}\right. \qquad (\eta = \pm 1) \tag{30}$$

([28]) Per dimostrare l'asserzione del testo si osservi in primo luogo che le soluzioni $\lambda_0 = \pm 1$, $\lambda_1 = \lambda_2 = \lambda_3 = 0$ sono date dalle (30), quando vi si supponga $x = 0$. Per ogni *altra* soluzione $(\lambda_0, \lambda_1, \lambda_2, \lambda_3)$ della (29), con interi primi fra loro, si può porre

$$\lambda_0 = u, \qquad \lambda_1 = tx, \qquad \lambda_2 = ty, \qquad \lambda_3 = tz$$

con

$$t \neq 0, \qquad D(x, y, z) = 1, \qquad D(t, u) = 1.$$

Ma allora, sostituendo nella (29), è

$$tux - t^2(y^2 + Qyz + PRz^2) = 0$$

cioè

$$ux - t(y^2 + Qyz + PRz^2) = 0;$$

quindi, essendo $D(t, u) = 1$, è pure

$$u = \eta \frac{y^2 + Qyz + PRz^2}{D(x, y^2 + Qyz + PRz^2)} \qquad t = \eta \frac{x}{D(x, y^2 + Qyz + PRz^2)} \qquad (\eta = \pm 1).$$

Da tutto ciò segue subito l'asserzione fatta nel testo.

ponendovi per (x, y, z) tutti i sistemi di interi per cui risulta

$$D(x, y, z) = 1\,;$$

dunque questa volta i valori di N sono dati tutti dall'espressione

$$(31)\qquad \frac{(x'y''-x''y')^2 + Q(x'y''-x''y')(x'z''-x''z') + PR(x'z''-x''z')^2}{D(x', y'^2+Qy'z'+PRz'^2)\,D(x'', y''^2+Qy''z''+Pz''^2)},$$

dove (x', y', z') e (x'', y'', z'') sono due qualunque terne di numeri primi tra loro che, sostituite nelle (30) alla terna (x, y, z), diano luogo a due soluzioni della (29) essenzialmente distinte.

29. La (31), per

$$x' = x'' = 1,$$

diventa

$$(y''-y')^2 + Q(y''-y')(z''-z') + PR(z''-z')^2\,;$$

e quindi tra i valori di cui è suscettibile N compariscono *certo* tutti gli interi (non nulli e quindi) positivi rappresentabili mediante la forma quadratica

$$(32)\qquad y^2 + Qyz + PRz^2\,;$$

ma, *in generale*, questi interi non esauriscono tutti quei valori.

Per es., se è

$$P = 3, \qquad Q = 0, \qquad R = 1,$$

il numero 2 non è rappresentabile mediante la forma (32), ma comparisce tra i valori di N, come si vede facendo nella (31)

$$x' = 2, \qquad y' = 1, \qquad z' = 1,$$

$$x'' = 2, \qquad y'' = 0, \qquad z'' = 1.$$

La cosa sta per altro, come ora mostreremo, nel caso in cui C sia una curva ellittica armonica o equianarmonica.

30. Supponga si infatti che C sia armonica.

Allora si può imaginare che sia

$$P = R = 1, \qquad Q = 0$$

e la (31) diviene

$$\frac{(x'y''-x''y')^2+(x'z''-x''z')^2}{D(x',y'^2+z'^2).D(x'',y''^2+z''^2)}; \tag{33}$$

inoltre tra i valori di cui è suscettibile N compariscono certo tutti gli interi positivi rappresentabili mediante la forma quadratica

$$y^2+z^2.$$

Si tratta di far vedere che questi interi esauriscono nel caso attuale i valori di cui è suscettibile N.

Per questo, in virtù di un teorema noto ([29]), basta dimostrare che ogni valore di N è un intero tale, che ogni suo eventuale fattore primo del tipo $4n+3$ lo ammette con esponente pari.

Si sa che, se un numero primo della forma $4n+3$ divide la somma di due quadrati, esso divide anche le loro basi ([30]); quindi, una volta che nella (33) (x', y', z') e (x'', y'', z'') sono due terne di numeri primi tra loro, nessuno dei due numeri

$$D(x',y'^2+z'^2), \qquad D(x'',y''^2+z''^2)$$

ammette alcun fattore primo del tipo $4n+3$.

Ora ogni valore di N è rappresentabile nella forma (33), e il numeratore della frazione (33) è appunto un intero che ciascun suo eventuale fattore primo del tipo $4n+3$ lo ammette con esponente pari; dunque la stessa proprietà sussiste per l'intero rappresentato dalla frazione (33) e l'asserzione fatta più sopra è dimostrata.

Abbiamo dunque il seguente teorema:

Sopra una superficie iperellittica armonica (cioè rappresentante la varietà delle coppie ordinate di punti di una curva ellittica armonica) esistono infiniti fasci ellittici di curve ellittiche, ma il numero dei punti comuni a due curve appartenenti a fasci differenti è sempre la somma di due quadrati. E le due curve possono essere scelte in maniera che il numero dei punti ad esse comuni sia un numero positivo somma di due quadrati comunque assegnato.

([29]) Veggasi per es. GAUSS, *Disquisitiones Arithmeticae*, art. 182, I, 2ª nota a piè di pagina.

([30]) Questa asserzione può esser dedotta subito dal teorema che GAUSS dà nel luogo or ora citato, o anche dal teorema di LAGRANGE che viene ricordato nell'annotazione ([31]).

Il caso della curva equianarmonica si discute in una maniera del tutto analoga, quando si tenga presente che:

α) *Gli interi rappresentabili mediante la forma quadratica* $y^2 + yz + z^2$ *sono tutti e soli gli interi che contengono con esponente pari ciascun loro eventuale fattore primo del tipo* $3n + 2$;

e che:

β) *Se un numero primo della forma* $3n + 2$ *divide un intero della forma* $y^2 + yz + z^2$ *con* y *e* z *interi, esso divide anche* y *e* z (31).

(31) Poichè le proposizioni α) e β) del testo non si trovano nei trattati di teoria dei numeri, che ho potuto consultare, credo utile, per comodità del lettore, di indicarne brevemente le dimostrazioni.

Si ha subito intanto che:

Se l'intero $3h$ *è rappresentabile mediante la forma quadratica* $y^2 + yz + z^2$, *tale è pure* h; *e viceversa.*

Da

$$3h = a^2 + ab + b^2$$

con a, b interi si trae facilmente che $a \equiv b \pmod{3}$; quindi

$$a' = \frac{2a + b}{3} \qquad \text{e} \qquad b' = \frac{b - a}{3} \tag{1}$$

sono interi. Dopo di che, essendo

$$h = a'^2 + a'b' + b'^2,$$

anche h è rappresentabile mediante la forma $y^2 + yz + z^2$.

L'asserzione inversa è evidente, perchè dalle (1) si trae

$$a = a' - b'$$

$$b = a' + 2b',$$

e quindi se nelle (1) a' e b' sono interi, tali sono anche a e b.

Ciò posto, sia M un intero positivo rappresentabile mediante la nostra forma, e sia

$$M = a^2 + ab + b^2,$$

con a, b interi (non entrambi nulli).

Se si pone

$$\sigma = D(a, b), \qquad a = \sigma a', \qquad b = \sigma b',$$

si ha

$$\frac{M}{\sigma^2} = a'^2 + a'b' + b'^2,$$

Si trova così il teorema:

Sopra una superficie iperellittica equianarmonica (cioè rappresentante la varietà delle coppie ordinate di punti di una curva ellittica equianarmonica) esistono infiniti fasci ellittici; e il numero dei punti comuni a due curve appartenenti a fasci differenti è un intero suscettibile di tutti e soli i valori della forma $y^2 + yz + z^2$, *con* y, z *interi non entrambi nulli.*

Catania, 25 dicembre 1918

con a', b' primi tra loro; quindi $\frac{M}{\sigma^2}$ è rappresentabile *propriamente* mediante la forma $y^2 + yz + z^2$.

In virtù dell'osservazione fatta or ora e di un teorema noto (vedi per es. DIRICHLET, *Lezioni sulla teoria dei numeri*, tradotte dal FAIFOFER, Venezia, Tipografia Emiliana, 1881, pag. 160 e seg.), segue che gli eventuali fattori primi di $\frac{M}{\sigma^2}$, diversi da 3, sono tutti della forma $3n + 1$; dunque ogni eventuale fattore primo di M della forma $3n + 2$ comparisce in M con esponente pari.

Viceversa, sia M un intero positivo tale, che ogni suo eventuale fattore primo della forma $3n + 2$ comparisca in esso con esponente pari.

Si potrà determinare un intero $\sigma \geqq 1$ tale, che il quoziente $M' = \frac{M}{\sigma^2}$ risulti un intero non contenente fattori primi del tipo $3n + 2$; quindi, per l'osservazione fatta più sopra e per il teorema cui or ora è stato alluso, esistono due interi a' e b' per cui è

$$M' = a'^2 + a'b' + b'^2,$$

ossia

$$M = (\sigma a')^2 + \sigma a' . \sigma b' + (\sigma b')^2 .$$

Con questo la proposizione α) è dimostrata.

Dopo di che la proposizione β) segue subito da un teorema classico di LAGRANGE, sui divisori di una forma quadratica, quando si ricordi che ogni forma quadratica definita positiva $Py^2 + Qyz + Rz^2$, con P, Q, R interi e $4PR - Q^2 = 3$, è equivalente alla forma $y^2 + yz + z^2$.