Lettura XV - addendum

ALGEBRAIC CURVES & RIEMANN SURFACES

Prof. M. Spera UCSC Brescia

provisional material

Nel secondo caso, quando $c' = 1 - c$, scegliamo invece:

$$\begin{cases} x \mapsto x - 1 \\ y \mapsto iy \end{cases}$$

e il teorema è dimostrato. □

L'ultimo teorema conclude la classificazione delle curve non singolari di terzo grado, e afferma che esistono un'infinità non numerabile di classi di equivalenza proiettiva per le cubiche. Infatti per ogni $j(c)$ dove c è un numero complesso qualsiasi (purché diverso da 0,1) esiste una classe di equivalenza, e poiché $j(c)$ si muove in un insieme continuo, allora tale deve essere la cardinalità del numero di classi.

1.3 Legge di gruppo

(trattazione alternativa)

Su una cubica non singolare è possibile definire in modo geometrico una somma tra punti che rende la curva un gruppo abeliano. In questo paragrafo verrà illustrato dal punto di vista geometrico come si costruisce la somma tra punti, e verrà ricavata una formula che, dati due punti, consente di trovare il loro punto-somma. Vediamo ora la costruzione geometrica.

Scegliamo un punto O sulla cubica. Presi due punti A, B qualsiasi sulla curva congiungiamoli con una retta. Avendo la curva grado 3 esiste sempre un terzo punto di intersezione tra cubica e retta; chiamiamo tale punto P. Prendiamo ora la retta passante per P e per il punto O precedentemente scelto e colleghiamoli con una seconda retta. Di nuovo esisterà un terzo punto di intersezione tra curva e retta, e diciamo che quest'ultimo è la somma tra A e B. Se conveniamo di porre $R(A, B)$ il terzo punto di intersezione tra la cubica e la retta per A, B, allora la somma tra punti è una funzione definita nel seguente modo:

$$+ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$$
$$(A, B) \mapsto R(O, R(A, B))$$

Osserviamo che se i punti A e B coincidono possiamo comunque definire la somma considerando la retta tangente ad A anziché la retta secante, e dal punto di vista geometrico il tutto è perfettamente definito.

Se la cubica è in forma $y^2 = g(x)$ con $g(x)$ polinomio di terzo grado in x allora è facile dimostrare che essa ammette $Y_\infty = [0, 1, 0]$ come punto di flesso. Allora risulta comodo scegliere come punto O proprio il punto Y_∞.

Ivan P. Galvagno (Brescia)
relatore: MS

2-V-13

deve stare per costruzione in $\mathcal{E}$, assurdo. Allora abbiamo dimostrato che i punti P_i sono a tre a tre non allineati.

In modo simile si dimostra che sei punti qualsiasi scelti tra i nove non possono stare su una conica. Infatti per assurdo supponiamo che ci stiano e chiamiamo $\mathcal{B}$ la conica su cui stanno. Chiamiamo poi r la retta per i restanti due punti. A questo punto scegliamo due ulteriori punti distinti dagli altri otto: $A \in \mathcal{B}$ e B esterno sia alla retta che alla conica. La cubica del sistema di cubiche passante per questi dieci punti ricade in una contraddizione simile a quella trovata precedentemente.

Abbiamo quindi appurato che i nove punti ottenuti intersecando due cubiche $\mathcal{C}, \mathcal{C}'$ non saranno mai sulla stessa retta tre a tre, o sulla stessa conica sei a sei. Siamo ora pronti per dimostrare che una cubica per $P_1, ..., P_8$ deve passare per forza per P_9

Sia r la retta per P_1, P_2 e sia $\mathcal{B}$ la conica per $P_3, ..., P_7$. Per quanto dimostrato sopra P_8 resta esterno sia a r che a $\mathcal{B}$. Prendiamo due ulteriori punti $A, B \in r$ e consideriamo la cubica $\mathcal{E}$ del sistema di cubiche passante per questi dieci punti. Tale cubica è forzata a essere degenere poiché contiene una retta e una conica, dunque $\mathcal{E} = r \cup \mathcal{B}$, ma il punto P_8 non sta né sulla retta né sulla conica, quindi $\mathcal{E} \neq r \cup \mathcal{B}$. Assurdo. □

Teorema 1.9. *Sia $\mathcal{C}$ una cubica non singolare, e sia $+ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ definita come sopra. Allora $(\mathcal{C}, +)$ è un gruppo abeliano con elemento neutro O.*

Dimostrazione. Dimostriamo che valgono le proprietà associativa e commutativa, che O è l'elemento neutro e che preso un punto arbitrario questo ammette inverso. In questa dimostrazione conveniamo di indicare con r_{AB} la retta passante per A, B.

Elemento neutro. Sommiamo un generico A con O e vediamo che il risultato è A. Per sommare A con O costruiamo la retta r_{AO} e prendiamo il punto $B = R(A, O)$. Da qui dovremmo tracciare la retta tra B e l'origine O, ma questa nuova retta è ovviamente la retta costruita poco fa. Quindi il terzo punto di intersezione è di nuovo A e quindi $A + O = A$.

Opposto. Preso un $A \in \mathcal{C}$ deve esistere un B tale che $A + B = O$. Per trovare un siffatto B prendiamo la retta tangente in O. Questa intersecherà $\mathcal{C}$ in un punto $P = R(O, O)$. Congiungiamo A e P con una retta e chiamiamo B il terzo punto, che sarà proprio l'inverso di A.

Proprietà commutativa. Questa proprietà è una banale conseguenza del fatto che la retta passante per A, B è la stessa retta passante per B, A.

Proprietà associativa. Dimostriamo che $(A + B) + C = A + (B + C)$, ovvero

$$R(O, R(A + B, C)) = R(O, R(A, B + C)).$$

Basta dunque dimostrare che $R(A+B, C) = R(A, B+C)$. Per trovare $R(A + B, C)$ prendiamo la retta r_{AB} che individua un terzo punto P, poi prendiamo la retta r_{OP} che individua il punto $Q := A + B$. Ora manca da sommare il punto C, quindi facciamo la retta r_{CQ} e otteniamo il punto $R((A + B), C)$. Per trovare invece $R(A, B + C)$ prendiamo la retta r_{BC} che individuerà il terzo punto P'. Prendiamo poi la retta $r_{OP'}$ che individuerà il punto $Q' := B + C$, e infine congiungiamo con A tramite la retta $r_{AQ'}$ ottenendo $R(A, B + C)$.

In questo insieme di rette possiamo distinguere due cubiche (degeneri), ognuna composta da una terna di rette: definiamo dunque

$$\mathcal{D} := r_{AB} \cup r_{OP'} \cup r_{CQ}$$
$$\mathcal{D}' := r_{BC} \cup r_{OP} \cup r_{CQ'}.$$

Queste due cubiche intersecano la cubica $\mathcal{C}$ in nove punti che supponiamo essere distinti.[10] In particolare avremo

$$\mathcal{C} \cup \mathcal{D} = \{A, B, C, O, P, P', Q, Q', R(A + B, C)\}$$
$$\mathcal{C} \cup \mathcal{D}' = \{A, B, C, O, P, P', Q, Q', R(A, B + C)\}.$$

Grazie al lemma 1.8 possiamo affermare che

$$R(A + B, C) = R(A, B + C).$$

□

Un'importante osservazione che segue dalla legge di addizione sulle cubiche non degeneri è la seguente:

Corollario 1.10. *Tre punti A, B, C su una cubica non degenere sono allineati se e solo se $A + B + C = O$.*

Dimostrazione. Supponiamo che i tre punti siano allineati. Sommiamo $A+B$: tracciamo la retta r_{AB} che definirà un terzo punto $R(A, B)$. Ma essendo i tre punti allineati per ipotesi questo terzo punto deve essere proprio C. Proseguiamo: colleghiamo C con O per ottenere $A + B$. Infine colleghiamo

[10] Se i punti non sono distinti la dimostrazione fatta in questo modo non è più valida. Più avanti nella trattazione daremo una dimostrazione completa per l'associatività, passando per un'altra strada.

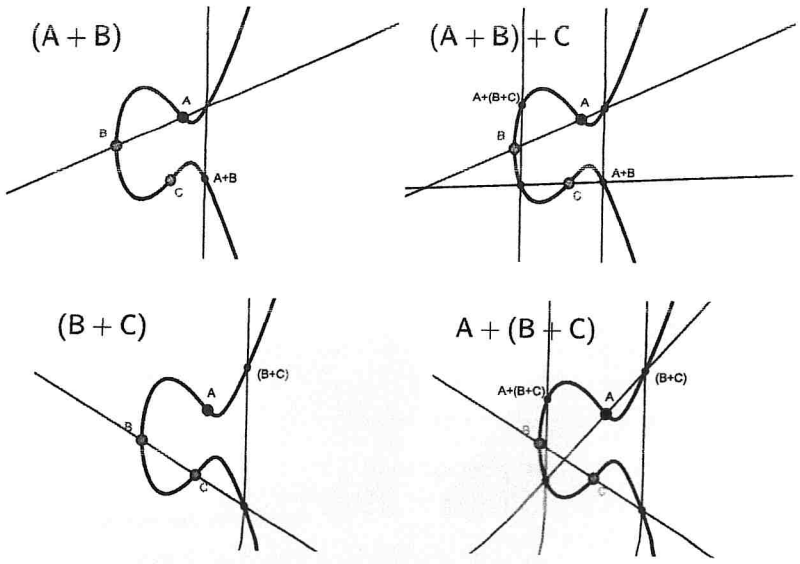

Figura 1.3: Illustrazione grafica della proprietà associativa.

$A + B$ con C ottenendo $R(A + B, C)$ che però è proprio O per costruzione. Come ultimo passo dobbiamo tracciare la retta r_{OO} per trovare $(A+B)+C$, e il risultato dell'intersezione è proprio O da cui $A + B + C = O$. Viceversa se $A + B + C = O$ allora $A + B$ è l'opposto di C ovvero $-C = A + B$, che possiamo riscrivere

$$R(O, C) = -C = A + B = R(O, R(A, B)).$$

Segue che $C = R(A, B)$ ovvero A, B, C allineati. □

Mettiamoci ora nel caso semplificato in cui il punto O è il flesso all'infinito. Concludiamo la sezione ricavando esplicitamente la formula che, dati due punti su $\mathcal{C}$, restituisce la loro somma. Per ricavarla si può partire da una curva di equazione (1.1), ma per semplicità di calcolo facciamo la dimostrazione con una cubica nella forma

$$y^2 = 4x^3 - px - q. \tag{1.5}$$

L'equivalenza tra questa forma (detta *forma canonica di Weierstrass*) e la forma canonica (1.1) verrà dimostrata più avanti (si veda la proposizione 2.13), così come il fattore 4 che compare come coefficiente del termine cubico.

Prendiamo la retta passante per due punti $A, B \in \mathcal{C}$. Se $A = (a_1, a_2)$ e $B = (b_1, b_2)$ la retta in forma parametrica sarà data da:

$$x(t) = a_1 + t(b_1 - a_1)$$
$$y(t) = a_2 + t(b_2 - a_2).$$

XV-17

Intersechiamo tale retta con la cubica, che avrà equazione (1.5):

$$\begin{aligned} P(t) &= 4(b_1 - a_1)^3 t^3 + [-(b_2 - a_2)^2 + 12a_1(b_1 - a_1)^2]t^2 \\ &+ [-2a_2(b_2 - a_2) + 12a_1^2(b_1 - a_1) - p(p_1 - a_1)]t \\ &+ [-a_2^2 + 4a_1^3 - pa_1 - q] = 0. \end{aligned}$$

Questo è un polinomio di grado tre in t, e ammetterà tre radici. Due di queste radici sono però note: sono i punti A e B che abbiamo scelto inizialmente, che corrispondono rispettivamente ai valori $t = 0$ e $t = 1$. Dunque il polinomio si può fattorizzare così:

$$P(t) = 4(b_1 - a_1)^3[(t - 0)(t - 1)(t - \gamma)]$$

dove γ è la terza radice ed è la nostra incognita. Se sviluppiamo quest'ultima equazione otteniamo

$$P(t) = 4(b_1 - a_1)^3[t^3 - (\gamma + 1)t^2 + \gamma t].$$

A questo punto confrontiamo i termini di secondo grado nelle due scritture ottenendo la seguente identità:

$$4(b_1 - a_1)^3(\gamma + 1) = (b_2 - a_2)^2 + 12a_1(b_1 - a_1)^2.$$

Isolando γ otteniamo

$$\gamma = \frac{1}{b_1 - a_1}\left[-b_1 - 2a_1 + \frac{1}{4}\left(\frac{b_2 - a_2}{b_1 - a_1}\right)^2\right].$$

Sostituiamo ora γ nelle coordinate del punto $(x(t), y(t))$ e ricaviamo la seguente formula per la prima coordinata[11]:

$$x(\gamma) = -a_1 - b_1 + \frac{1}{4}\left(\frac{b_2 - a_2}{b_1 - a_1}\right)^2. \tag{1.6}$$

Queste che abbiamo trovato non sono ancora le coordinate della somma $A+B$, ma semplicemente del terzo punto $R(A, B)$. Ma siccome siamo nel caso con $O = Y_\infty$ è facile a questo punto trovare le coordinate del punto somma: basta cambiare segno alla y ottenendo $(x(t), -y(t))$.

[11] La seconda coordinata può venire facilmente ricavata una volta nota la prima tramite sostituzione nell'equazione della retta, quindi è inutile cercare una formula anche per la y.