ALGEBRAIC CURVES & RIEMANN SURFACES
Prof. M. Spira UCSC

Lecture XV

Elliptic curves

Provisional material

whereas differentiating with respect to v :

$$(auv - 2uv^3 + UV)(1 + u^2v^2) - 2u^2v(uV^2 + vUV) = 0.$$

Replacing in both the derivatives U^2 with $1 + au^2 - u^4$ and rearranging terms, these two expressions have in common the value

$$(UV + auv)(1 - u^2v^2) - 2uv(u^2 + v^2).$$

It follows that

$$\frac{du}{U} + \frac{dv}{V} = 0,$$

which implies Euler's addition theorem.
This formula had been found by Euler at first in an even simpler form, holding only for the lemniscate integrals.
Similar formulae were used even before for the doubling of a lemniscate arc, due to the studies of earl Fagnano, where r was meant as the radius-vector joining the origin to the curve and making a series of substitutions aimed at rationalizing the integral; substitutions that suggested more and more general ones, until reaching the form of r seen above.

Comment: Retrospectively, we notice that elliptic functions provide a far reaching generalization of circular function: take for instance

$$\arcsin x = \int_0^x \frac{1}{\sqrt{1-t^2}}\, dt\ .$$

Its inverse function is the sinus, which is holomorphic, periodic and gets the standard addition theorem $\sin(x + y) = \sin x \cos y + \sin y \cos x$. In a similar way, the Weierstrass $\wp$-function inverts the elliptic integral $\int \frac{dx}{y}$, it is meromorphic and doubly periodic and satisfies an analogous addition theorem.

3.6 The Group Law for elliptic curves

Let an elliptic curve $\mathcal{E}$ be written in the Weierstrass form $C_\Lambda = C_\Lambda(\xi, \eta, \zeta)$ (this can be always assumed):

$$4\xi^3 - g_2\xi\zeta^2 - g_3\zeta^3 - \eta^2\zeta = 0$$

that is a cubic nonsingular curve in $\mathbb{P}^2$, and let be O one of its flexes.

A flex of a plane algebraic curve is a point wherein the curve and its tangent have at least three points in common. It can be shown that the flexes of the curve are precisely the nonsingular intersections with its associated Hessian curve. From Bezout's theorem one concludes that $\mathcal{E}$ has nine flexes.

We shall define the mapping $+ : \mathcal{E} \times \mathcal{E} \to \mathcal{E}$ such that for every $A, B \in \mathcal{E}$ let $R(A, B)$ the intersection point with $\mathcal{E}$ and the line $L(A, B)$, counted with its multiplicity; then we define $A + B = R(R(A, B), O)$.

tesi S. Rigo (Verona) relatore MS

Riemann surfaces & elliptic integrals

XV-1

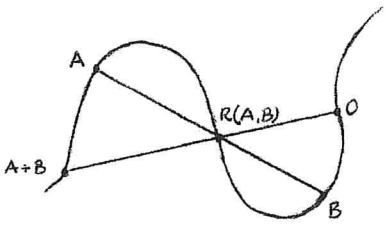

Figure 17: Definition of the mapping $+ : \mathcal{E} \times \mathcal{E} \to \mathcal{E}$

Theorem 17 *With the operation $+$ introduced above, the nonsingular cubic curve $\mathcal{E}$ becomes an abelian group, whose neutral element is the chosen flex O.*

To prove our assertion, we need some preliminary results.

Already proved !

Theorem 18 *If two projective curves of degree n have $N = n^2$ distinct points in common, and if mn points belong to an irreducible curve of degree $m < n$, then the remaining $N - mn$ points are on a curve of degree $n - m$.*

Proof. Let $\mathcal{E}_1, \mathcal{E}_2$ be the two curves of degree n and let $\mathcal{F}$ be the irreducible curve of degree m, containing mn of the intersection points between $\mathcal{E}_1, \mathcal{E}_2$. Upon fixing an arbitrary point $P \in \mathcal{F}$ different from the mn points, there exists a curve $\mathcal{E}$ of the pencil determined by $\mathcal{E}_1, \mathcal{E}_2$ containing P. Having $mn+1$ points in common with $\mathcal{F}$, $\mathcal{E}$ shares an irreducible part with $\mathcal{F}$. But $\mathcal{F}$ is irreducible, so $\mathcal{E} = \mathcal{F} + \mathcal{G}$, where $\mathcal{G}$ is a curve whose degree is $n - m$. Since the n^2 points of $\mathcal{E}_1 \cap \mathcal{E}_2$ belong to $\mathcal{E}$ and $\mathcal{F}$, because of its irreducibility, contains only mn of them (or else $\mathcal{F}$ would be an irreducible component of $\mathcal{E}_1$ and $\mathcal{E}_2$ otherwise $\mathcal{E}_1$ and $\mathcal{E}_2$ would have an infinite number of points in common), the remaining points $N - mn$ belong to $\mathcal{G}$.
This theorem will be fundamental in the proof of Theorem 17, which is given right below.

Proof of 17. First we prove that O is the zero of the group; so letting A be an arbitrary point of $\mathcal{E}$, we will show $A + O = A$. In accordance with the definition of $+$, we draw the secant passing through A and O, that intersects the curve in another point $R(A, O)$; then we join $R(A, O)$ and O, and so find that the point $R(R(A, O))$ is precisely A.
The second property to check is that $\forall A \in \mathcal{E}, -A = R(A, O)$. This is easily verified thanks to the construction above: the only point which, added to A, can give O is exactly $R(A, O)$, so $-A = R(A, O)$.
The third property to verify is the commutative one; but clearly the line joining A to B is the same line that joins B to A, so the construction and, consequently, the result are the same: $A + B = R(R(A, B), O) = R(R(B, A), O) = B + A$.

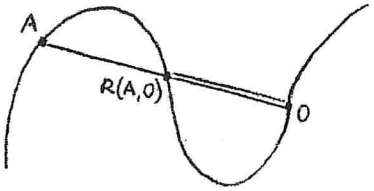

Figure 18: Checking the neutral element and the opposite element.

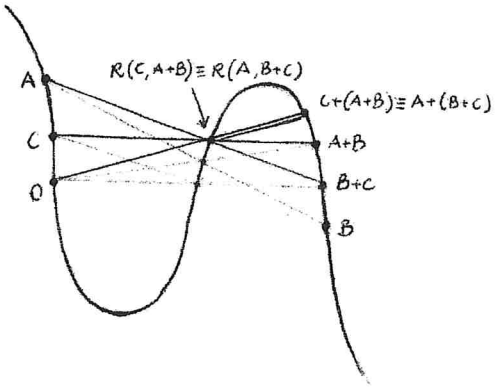

Figure 19: Associativity.

The last property and more difficult to show is associativity, that is $A + (B + C) = R(R(A, B + C)) = R(R(A + B, C)) = (A + B) + C$. Let $\mathcal{F} = L(A, B) + L(A+B, C) + L(O, B+C)$ be a degenerate cubic curve, then we have $\mathcal{E} \cap \mathcal{F} = \{O, A, B, C, A+B, B+C, R(A, B), R(A+B, C), R(B, C)\}$. We will prove the assertion only in the case that these points are distinct. Since the points $B, C, R(B, C)$ from (18) are collinear, it follows that the remaining 6 points belong to a conic; but $O, A + B, R(A, B)$ are collinear again. Therefore thanks again to (18) the remaining 3 points are collinear, so we get the assertion.

Further we can remark that from the definition of $+$ follows that three points on our cubic curve are collinear if and only if their sum is zero.

Capitolo 1

Cubiche non singolari

1.1 Fatti generali sulle cubiche

L'obiettivo di questa prima parte è quello di dare la classificazione proiettiva delle cubiche non singolari, associando a ogni cubica una classe di equivalenza proiettiva. L'idea è quella di applicare alla curva una serie di proiettività che la portino ad una forma standardizzata, e vedere quante di queste forme esistono. Nel caso dello studio delle coniche ad esempio si riuscivano a ricondurre proiettivamente tutte le coniche non singolari a una stessa forma canonica affermando quindi che esiste un'unica classe di equivalenza proiettiva. Infatti tutte le coniche dal punto di vista proiettivo sono in realtà lo stesso oggetto: tutte possono essere fatte combaciare purché adeguatamente trasformate con delle proiettività[1]. Un primo passo per giungere a una classificazione analoga per le cubiche è dato dal seguente teorema.

Teorema 1.1. *Ogni cubica non singolare $\mathcal{C}$ di $\mathbb{P}^2(\mathbb{C})$ è proiettivamente equivalente a una cubica di equazione affine*

$$y^2 = x(x-1)(x-c) \tag{1.1}$$

con $c \in \mathbb{C}\backslash\{0,1\}$.

Dimostrazione. Conveniamo che, per il resto di questa sezione, la cubica generale abbia la seguente equazione (in coordinate omogenee $[x_0, x_1, x_2]$ con $(x_0, x_1, x_2) \neq (0,0,0)$):

$$\begin{aligned} F(x_0,x_1,x_2) = {} & a_{000}x_0^3 + a_{111}x_1^3 + a_{222}x_2^3 + a_{112}x_1^2x_2 + a_{122}x_1x_2^2 + a_{011}x_0x_1^2 \\ & + a_{022}x_0x_2^2 + a_{012}x_0x_1x_2 + a_{001}x_0^2x_1 + a_{002}x_0^2x_2 = 0. \end{aligned}$$

[1] Per le coniche si dà in genere anche un'ulteriore classificazione, quella affine, che porta a distinguere parabole, iperboli ed ellissi. Una classificazione analoga fatta per le cubiche non viene affrontata in questa sede.

tesi R. Galvagni (Brescia)
relatore: MS
Aspetti geometrici e algebrici delle curve ellittiche

Dato che $\mathcal{C}$ ha almeno un flesso possiamo trovare una proiettività che mandi tale flesso nel punto all'infinito $Y_\infty = [0,0,1]$ facendo in modo che la tangente inflessionale vada nella retta impropria $r_\infty = \{x_0 = 0\}$. In concreto ciò significa imporre che $F_0'(Y_\infty) \neq 0, F_1'(Y_\infty) = 0, F_2'(Y_\infty) = 0$ per avere la tangenza in Y_∞ e imporre che $C \cap r_\infty$ sia un punto triplo per avere un flesso in Y_∞. Per quanto riguarda la prima condizione, le derivate sono:

$$F_1'(x_0,x_1,x_2) = 3a_{111}x_1^2 + a_{012}x_0x_2 + 2a_{011}x_0x_1 + a_{001}x_0^2 + 2a_{112}x_1x_2 + a_{122}x_2^2$$
$$F_2'(x_0,x_1,x_2) = 3a_{222}x_2^2 + a_{012}x_0x_1 + 2a_{022}x_0x_2 + a_{022}x_0^2 + 2a_{122}x_1x_2 + a_{112}x_1^2$$

che calcolate in $Y_\infty = [0,0,1]$ risultano nulle quando $a_{122} = 0$, $a_{222} = 0$.

Vediamo la seconda condizione. Intersecando la cubica con r_∞ otteniamo

$$a_{111}x_1^3 + a_{112}x_1^2x_2 = 0$$

che deve dare tre radici coincidenti. Se poniamo $a_{112} = 0$ abbiamo proprio $x_1^3 = 0$ cioè x_1 è radice tripla, quindi Y_∞ è di flesso.

La curva allora avrà la seguente equazione, che scriviamo direttamente in forma non omogenea (ovvero ponendo $x = \frac{x_1}{x_0}, y = \frac{x_2}{x_0}$):

$$a_{000} + a_{001}x + a_{002}y + a_{012}xy + a_{011}x^2 + a_{022}y^2 + a_{111}x^3 = 0.$$

Applicando un'adeguata affinità[2] possiamo trasformare la cubica in una curva di equazione $y^2 = b(x-e_1)(x-e_1)(x-e_3)$. L'affinità $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$

$$\varphi : \begin{cases} x \mapsto (e_2 - e_1)x + e_1 \\ y \mapsto \sqrt{b(e_2-e_1)^3}y \end{cases}$$

infine trasforma ulteriormene la cubica, portandola in

$$y^2 = x(x-1)(x-c)$$

con $c = (e_3 - e_1)/(e_2 - e_1)$. □

D'ora in avanti diremo che una cubica è *in forma canonica (di Legendre)* se è scritta in forma (1.1). Dire che ogni cubica esistente è equivalente a una

[2]Si può dimostrare per verifica diretta che tale affinità è

$$\begin{cases} x \mapsto \alpha x + \gamma \\ y \mapsto -\frac{a_{012}}{2a_{022}}\alpha x - \beta y - \frac{a_{002}+a_{012}\gamma}{2a_{022}} \end{cases}$$

con $\alpha, \beta, \gamma \in \mathbb{C}$.

curva di equazione (1.1) per un certo $c \in \mathbb{C}$ non esaurisce la classificazione, perché potrebbero esistere due cubiche equivalenti che però vengono portate in curve aventi c differenti. Oppure addirittura delle cubiche che appaiono nella forma canonica (1.1) ma sono singolari. In altre parole, abbiamo bisogno di una sorta di inverso del teorema precedente, che associ univocamente a ogni cubica non singolare una sua forma canonica e, viceversa, associ a ogni forma canonica una classe di cubiche non singolari, contenente curve tutte tra loro proiettivamente equivalenti.

Un primo problema viene risolto dal seguente risultato

Teorema 1.2. *Ogni cubica in forma canonica è non singolare.*

Dimostrazione. Dimostriamo che una cubica di equazione (1.1) ammette in ogni punto retta tangente. Data una curva di equazione

$$f(x,y) = x^3 - (c+1)x^2 + cx - y^2 = 0$$

andiamo a studiare le derivate,

$$\begin{aligned} f'_x(x,y) &= 3x^2 - 2(c+1)x + c \\ f'_y(x,y) &= -2y. \end{aligned}$$

Se $y \neq 0$ allora di certo $f'_y \neq 0$ e il teorema è dimostrato. In caso contrario, deve essere $f'_x \neq 0$ e infatti se abbiamo $y = 0$, per verificare la (1.1) deve essere per forza $x = 0, 1, c$. Ma questi tre valori sono distinti per ipotesi ed essendo radici semplici non annullano la derivata, che quindi è diversa da zero quando $y = 0$. □

1.2 Il birapporto

Per poter dire che ogni c di (1.1) individua una e una sola classe di equivalenza proiettiva, dobbiamo premettere alcuni concetti. Primo fra tutti il concetto di *birapporto.*

Definizione 1.3. *Dati quattro punti allineati P_1, P_2, P_3, P_4 con P_1, P_2, P_3 distinti, definiamo* birapporto della quaterna di punti *il numero*

$$\beta(P_1, P_2, P_3, P_4) = \frac{P_1P_4 \cdot P_2P_3}{P_1P_3 \cdot P_2P_4} \tag{1.2}$$

dove P_iP_j denota la lunghezza con segno del segmento orientato.

Se definiamo il *rapporto semplice* tra tre punti P_1, P_2, P_3 come

$$(P_1, P_2, P_3) := \frac{P_3P_1}{P_3P_2}$$

di fatto possiamo vedere il birapporto come rapporto tra i rapporti semplici di quattro punti, ovvero

$$\beta(P_1, P_2, P_3, P_4) = \frac{P_4P_1}{P_4P_2} : \frac{P_3P_1}{P_3P_2} = \frac{(P_1, P_2, P_4)}{(P_1, P_2, P_3)}.$$

Il birapporto è una quantità fondamentale in geometria proiettiva, in quanto gode di molte interessanti proprietà. Si può infatti dimostrare che esso non cambia se applichiamo alla retta su cui giacciono i punti una rotazione, una dilatazione lineare (omotetia), una riflessione, una traslazione o una combinazione di queste. Ma la proprietà che rende il birapporto preferibile al rapporto semplice tra distanze è che il esso è invariante anche per *trasformazioni proiettive* sulla retta $\mathbb{P}^1(\mathbb{C})$.

Per dare un'idea intuitiva dell'invarianza proiettiva, consideriamo un arbitrario punto O esterno alla retta r su cui giacciono i punti. Scegliamo poi una retta s qualsiasi, non contenente O. A questo punto se proiettiamo i punti P_i dalla retta r alla retta s, con una proiezione di centro O il birapporto non cambia, mentre è immediato vedere che il rapporto semplice tra le lunghezze dei vari segmenti in generale non è affatto invariante (a meno che s non si parallela a r). Tra poco daremo la dimostrazione formale dell'invarianza proiettiva.

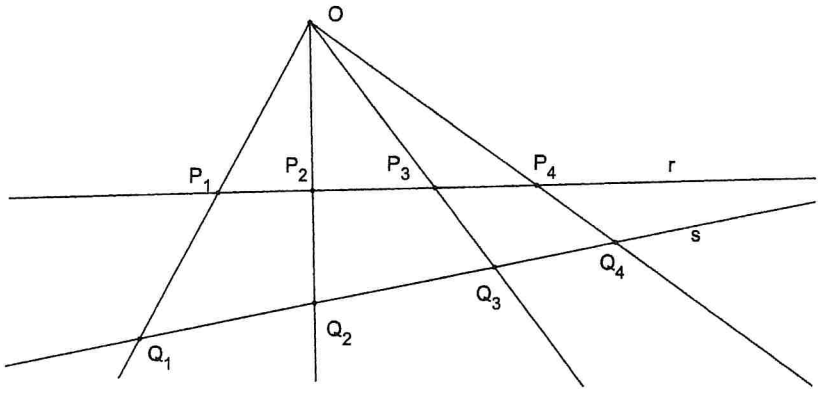

Figura 1.1: Invarianza proiettiva del birapporto.

Spesso risulta comodo identificare la retta proiettiva $\mathbb{P}^1(\mathbb{C})$ con la *sfera di Riemann*, ovvero il piano complesso a cui è stato aggiunto il punto all'infinito, che denoteremo con $\bar{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$. In tale contesto, le trasformazioni

proiettive sono rimpiazzate dalle *trasformazioni di Möbius*, che ora andiamo a introdurre.

Definizione 1.4. *Definiamo* trasformazione di Möbius *o* trasformazione lineare fratta (TLF) *una funzione* $f : \bar{\mathbb{C}} \to \bar{\mathbb{C}}$ *che si possa scrivere nella forma*

$$f(z) = \frac{az + b}{cz + d}$$

con $a, b, c, d \in \mathbb{C}$, *con* $ad - bc \neq 0$.

Una trasformazione lineare fratta $\bar{\mathbb{C}} \to \bar{\mathbb{C}}$ è essenzialmente equivalente a una proiettività $\mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ e ha un significato geometrico molto interessante. Infatti possiamo ottenere una trasformazione di Möbius proiettando il piano $\bar{\mathbb{C}}$ su una sfera tramite proiezione stereografica, ruotare a piacere la sfera, e infine riproiettare la sfera sul piano. Quindi una siffatta trasformazione mappa cerchi in cerchi (dove le rette sono considerate cerchi degeneri con raggio infinito) e preserva gli angoli. Inoltre, si può facilmente dimostrare per verifica diretta che componendo trasformazioni lineari fratte si ottiene ancora una trasformazione lineare fratta e che l'identità $z \mapsto z$ è una particolare trasformazione di questa categoria. Queste proprietà rendono l'insieme delle trasformazioni lineari fratte un gruppo con l'operazione di composizione.

Il fatto che il birapporto risulti invariante sotto azione di una trasormazione lineare fratta f si può esprimere dicendo che

$$\beta(z_1, z_2, z_3, z_4) = \beta(f(z_1), f(z_2), f(z_3), f(z_4)).$$

Qui naturalmente gli argomenti del birapporto non sono punti di $\mathbb{P}^1(\mathbb{C})$ bensì numeri complessi, ma la definizione è analoga.[3] Diamo una dimostrazione dell'invarianza del birapporto basata sul fatto che il gruppo delle TLF è generato da tre trasformazioni elementari: la traslazione $z \mapsto z+k$, l'omotetia $z \mapsto kz$ e l'inversione $z \mapsto 1/z$ che scambia 0 e ∞.[4] Infatti, per ogni $k \in \mathbb{C}$, otteniamo

$$\begin{aligned}
\beta(z_1 + k, z_2 + k, z_3 + k, z_4 + k) &= \beta(z_1, z_2, z_3, z_4) \\
\beta(kz_1, kz_2, kz_3, kz_4) &= \beta(z_1, z_2, z_3, z_4) \\
\beta(1/z_1, 1/z_2, 1/z_3, 1/z_4) &= \beta(z_1, z_2, z_3, z_4)
\end{aligned}$$

[3] Nel caso complesso il birapporto è definto anche se i punti non sono allineati. Tuttavia esso è reale solo quando i punti giacciono su una circonferenza generalizzata, ovvero una circonferenza o una retta.

[4] Il motivo per cui si usa la retta proiettiva anziché la retta affine per definire il birapporto è che in questo modo l'inversione risulta ben definita anche per lo 0.

com'è facile verificare per sostituzione. Siccome ogni proiettività (e analogamente ogni trasformazione di Möbius) è scomponibile in funzioni dei tre tipi detti, abbiamo dimostrato l'invarianza.[5]

Anziché considerare il birapporto di una quaterna di punti, risulta utile studiare il birapporto di una quaterna di *rette*. Infatti per quanto detto poco fa, il birapporto non cambia se si proiettano i punti da una retta all'altra nel modo mostrato in figura 1.1, e quindi può essere visto come una grandezza dipendente non tanto dai quattro punti $P_1, ..., P_4$ ma piuttosto dalle quattro rette passanti per O e per P_i, con $i = 1, 2, 3, 4$. Risulta dunque ben posta la seguente definizione.

Definizione 1.5. *Siano r_1, r_2, r_3, r_4 quattro rette uscenti da un punto O arbitrario. Chiamiamo* birapporto della quaterna di rette *il birapporto tra i quattro punti che si ottengono tagliando le quattro rette r_i, $i = 1, 2, 3, 4$ con una retta arbitraria non passante per O.*

La retta proiettiva $\mathbb{P}^1(\mathbb{C})$ è l'ambiente adatto a introdurre il birapporto poiché quest'ultimo è perfettamente definito anche se uno dei quattro punti è all'infinito. In questo caso per evitare forme indeterminate o divisioni per zero (che potrebbero comparire nella definizione che abbiamo dato) è preferibile utilizzare la seguente espressione, dove si ipotizza che i punti abbiano coordinate complesse omogenee $P_i = [a_i, b_i]$

$$\beta(P_1, P_2, P_3, P_4) = \frac{\begin{vmatrix} a_1 & a_4 \\ b_1 & b_4 \end{vmatrix} \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}}{\begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} \begin{vmatrix} a_2 & a_4 \\ b_2 & b_4 \end{vmatrix}}$$

Se i punti sono propri, ovvero con la prima coordinata riscalabile a 1, possiamo porre $P_i = [a_i, b_i] = [1, \frac{b_i}{a_i}] = [1, z_i]$ e la formula si riduce a

$$\beta(P_1, P_2, P_3, P_4) = \frac{\begin{vmatrix} 1 & 1 \\ z_1 & z_4 \end{vmatrix} \begin{vmatrix} 1 & 1 \\ z_2 & z_3 \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ z_1 & z_3 \end{vmatrix} \begin{vmatrix} 1 & 1 \\ z_2 & z_4 \end{vmatrix}} = \frac{(z_4 - z_1)(z_3 - z_2)}{(z_4 - z_2)(z_3 - z_1)}$$

che è esattamente la (1.2). È immediato verificare che il birapporto di una quaterna di punti (o di rette) è *dipendente* dall'ordine di ingresso dei parametri. A priori abbiamo $4! = 24$ modi diversi di riordinare quattro elementi,

[5] Osserviamo che se avessimo considerato il rapporto semplice tra tre punti la condizione sull'inversione non sarebbe stata soddisfatta, come è facile verificare. Infatti l'inversione è una trasformazione proiettiva, ma non affine.

ma si dimostra facilmente che i diversi risultati che si possono ottenere permutando i punti sono solo sei[6], e precisamente, detto $b = \beta(P_1, P_2, P_3, P_4)$, le sei possibilità che compaiono sono le seguenti:

$$b, \quad \frac{1}{b}, \quad 1-b, \quad \frac{1}{1-b}, \quad \frac{b-1}{b}, \quad \frac{b}{b-1} \tag{1.3}$$

È interessante notare che queste sei funzioni formano un gruppo (non commutativo) rispetto alla composizione, che è un sottogruppo del gruppo delle trasformazioni di Möbius. Ci chiediamo a questo punto se esiste un'espressione che sia simile al birapporto ma indipendente dall'ordine in cui vengono scelti i punti. In effetti possiamo considerare la seguente funzione razionale

$$j(b) = \frac{(b^2-b+1)^3}{b^2(b-1)^2}$$

che è definita per ogni $b \in \mathbb{C}\backslash\{0,1\}$. Si può infatti dimostrare che $j(b) = j(b')$ se si scelgono b e b' tra le sei possibilità date da (1.3). La quantità così definita si chiama *modulo* di una quaterna di punti (o di rette) e risulta fondamentale nella classificazione delle cubiche non singolari grazie al prossimo teorema.

Teorema 1.6 (di Salmon). *Sia $\mathcal{C}$ una cubica non singolare di $\mathbb{P}^2(\mathbb{C})$ e sia F un suo flesso. Allora $\mathcal{C}$ possiede in F quattro tangenti distinte inclusa la retta tangente in F, e il modulo delle quattro tangenti non dipende dal flesso che si sceglie.*

Dimostrazione. Si scelga un flesso F. Per il teorema 1.1 esiste una proiettività che porta $\mathcal{C}$ in forma canonica (portando F in Y_∞), per un certo $c \neq 0, 1$. La proiettività conserva rette tangenti e flessi, quindi basta dimostrare l'asserto per una cubica in forma canonica ed esso è in automatico verificato per qualsiasi cubica non singolare. Una cubica in forma canonica ha in Y_∞ quattro tangenti distinte: la retta impropria r_∞ (che è la tangente di flesso) e le rette $\{x = 0\}$, $\{x = 1\}$ e $\{x = c\}$, che sono tre rette verticali[7], e questo è sufficiente per affermare che in ogni flesso possiamo trovare 4 tangenti alla cubica, qualunque sia la cubica. Per vedere che il modulo delle quattro tangenti è lo stesso, qualsiasi flesso si scelga, basta osservare che preso un flesso

[6] Ad esempio

$$\beta(A,B,C,D) = \frac{(A-C)(B-D)}{(A-D)(B-C)} = \frac{(C-A)(D-B)}{(C-B)(D-A)} = \beta(C,D,A,B)$$

e così via.

[7] È facile convincersi di questo fatto osservando che innanzitutto r_∞ è una delle quattro rette essendo proprio la tangente in Y_∞, e le altre tre rette non possono che essere verticali, dovendo avere Y_∞ come direzione, cioè sono in forma $x = k$. Allora basta intersecare $\mathcal{C}$

F' diverso da F possiamo portare F' in Y_∞ portando $\mathcal{C}$ in forma canonica. Ora in Y_∞ le tangenti sono le stesse di prima, perché la forma canonica è la stessa, indipendentemente da quale flesso viene portato in Y_∞, quindi i due flessi F e F' hanno tangenti con lo stesso modulo. □

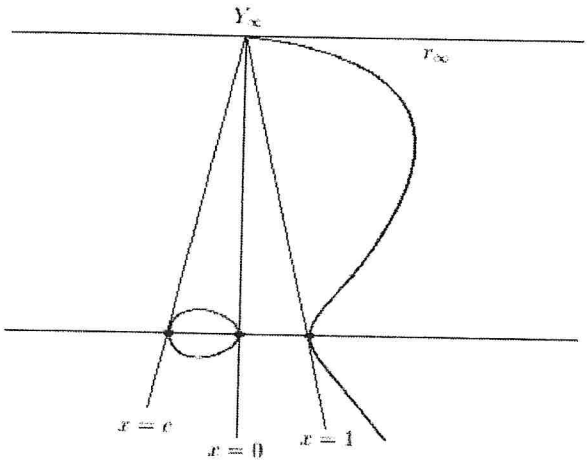

Figura 1.2: Le quattro tangenti alla cubica $y^2 = x(x-1)(x-c)$ nel punto Y_∞

Grazie al teorema di Salmon possiamo dire che a ogni cubica non singolare resta associata una quaterna di rette. Se calcoliamo il birapporto di queste rette otteniamo un numero complesso c associato alla cubica $\mathcal{C}$. Dimostreremo tra poco che proprio questo numero c definisce una classe di equivalenza tra cubiche. Prima però proviamo a vedere, per esempio, quale numero è associato a una cubica in forma canonica.

Sia $\mathcal{C} : y^2 = x(x-1)(x-c)$ con $c \neq 0, 1$. Calcoliamo il modulo di una quaterna di tangenti a un flesso e scegliamo ovviamente le più comode ovvero le tangenti passanti per Y_∞. Per farlo consideriamo ad esempio le intersezioni tra le quattro tangenti e l'asse x, che ci daranno altrettanti punti: in coordinate proiettive, $O = [1, 0, 0]$, $X_\infty = [0, 1, 0]$, $[1, 1, 0]$, $[1, c, 0]$. Questi

---

con $\{x = k\}$, e imporre che il punto di contatto sia doppio, ovvero

$$\begin{cases} x = k \\ y^2 = x(x-1)(x-c) \end{cases}$$

da cui $y^2 = k(k-1)(k-c)$ che ha radice doppia se e solo se $k = 0$, $k = 1$ o $k = c$.

quattro punti sono allineati sull'asse x; calcoliamo dunque il loro birapporto (usiamo i determinanti, dato che uno dei quattro punti è improprio)[8]

$$\beta(O, X_\infty, [1,1], [1,c]) = \frac{\begin{vmatrix} 1 & 1 \\ 0 & c \end{vmatrix} \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} \begin{vmatrix} 0 & 1 \\ 1 & c \end{vmatrix}} = \frac{c(-1)}{(1)(-1)} = c.$$

Dunque il birapporto dei quattro punti in questo specifico ordine è proprio c. Se il birapporto è c il modulo sarà

$$j(c) = \frac{(c^2 - c + 1)^3}{c^2(c-1)^2} \tag{1.4}$$

e questa quantità è proprio ciò che cercavamo: un numero associato univocamente alla cubica. Chiamiamo allora $j(\mathcal{C})$ il modulo comune delle quaterne di tangenti a un qualunque flesso, ovvero $j(\mathcal{C}) := j(c)$.

Teorema 1.7. *Due cubiche non singolari $\mathcal{C}$ e $\mathcal{C}'$ sono proiettivamente equivalenti se e solo se $j(\mathcal{C}) = j(\mathcal{C}')$.*

Dimostrazione. Se $\mathcal{C}$ e $\mathcal{C}'$ sono proiettivamente equivalenti, allora $\mathcal{C}$ è trasformabile in (1.1) ma d'altra parte $\mathcal{C}'$ è trasformabile in $\mathcal{C}$ per ipotesi, e quindi per transitività $\mathcal{C}'$ è trasformabile in (1.1). Allora $j(\mathcal{C}) = j(c) = j(\mathcal{C}')$.

Viceversa siano $\mathcal{C}$ una cubica proiettivamente equivalente a (1.1) e $\mathcal{C}'$ un'altra cubica proiettivamente equivalente a $y^2 = x(x-1)(x-c')$, tali che, per ipotesi, $j(\mathcal{C}) = j(\mathcal{C}')$. Allora deve essere che c e c' sono legati da una delle (1.3). Per dimostrare l'equivalenza proiettiva tra le due basta trovare una proiettività che trasformi la (1.1) nella $y^2 = x(x-1)(x-\frac{1}{c})$ e nella $y^2 = x(x-1)(x-(1-c))$. Infatti dimostrato questo, per composizione si può ricondurre c a una qualsiasi delle (1.3). Nel primo caso, in cui $c' = 1/c$, la proiettività da operare è la seguente:

$$\begin{cases} x \mapsto cx \\ y \mapsto c^{3/2} y \end{cases}$$

[8] Nel calcolo omettiamo la terza coordinata che è sempre 0 siccome i punti sono tutti sull'asse x. In alternativa senza ricorrere ai determinanti e alle coordinate proiettive si poteva semplicemente calcolare

$$\beta(0, \infty, 1, c) = \frac{(c-0)(1-\infty)}{(1-0)(c-\infty)} = c$$

dove si sottintende un opportuno procedimento di limite.