Alma Mater Studiorum · Università di Bologna

facoltà di scienze matematiche, fisiche e naturali
Corso di Laurea Triennnale in Matematica

CUBICHE ELLITTICHE

Tesi di Laurea in Geometria

Relatore:
Chiar.ma Prof.ssa
MONICA IDÀ

Presentata da:
MATTEO TOMMASINI

Sessione I
Anno Accademico 2006-2007

"Se la gente non crede che la matematica sia semplice, è semplicemente perché non si rende conto di quanto sia complicata la vita."
(John Von Neumann)

Indice

Introduzione

Classificare un certo insieme di curve significa in generale determinare classi di curve equivalenti, cioè curve che possono essere trasformate le une nelle altre per mezzo di applicazioni opportune (affinità, isometrie, proiettività o altro a seconda dell'ambito di lavoro).

In particolare, diremo che due curve del piano proiettivo sono proiettivamente equivalenti se esiste una proiettività che muta l'una nell'altra. Per esempio, la classificazione proiettiva delle coniche fatta su $\mathbb{R}$ o $\mathbb{C}$ mostra che esiste solo un numero finito di classi di coniche distinte, in particolare solo una classe di coniche non singolari se lavoriamo sul campo complesso.

Siamo ora interessati ad un analogo problema di classificazione nel caso proiettivo per quanto riguarda le cubiche piane non singolari, ossia le curve nel piano proiettivo complesso descritte da un'equazione algebrica omogenea di terzo grado, con la proprietà che la curva sia a supporto "liscio" in ogni punto, ossia in ogni punto ammetta esattamente una retta tangente.

Tali cubiche si dicono anche "cubiche ellittiche".

A differenza del caso delle coniche, mostreremo che esiste un numero infinito di classi distinte di cubiche equivalenti per proiettività. Tali classi saranno indicizzate da un parametro λ che varierà in un insieme con la cardinalità del continuo. Accenneremo inoltre alla classificazione delle cubiche singolari irriducibili.

Una volta classificate le cubiche, mostremo che su quelle ellittiche, per mezzo di un metodo puramente geometrico, si può costruire un gruppo abeliano, cioè si può introdurre sul supporto della curva un'operazione "$+$" che

ad ogni coppia di punti associ un terzo punto, detto loro somma.

Per mostrare che in effetti si ottiene un gruppo l'unica proprietà non banale da dimostrare sarà la proprietà associativa. Per verificarla useremo strumenti di analisi complessa in una variabile, di geometria e di algebra. L'idea di fondo è che le cubiche ellittiche come varietà complesse di dimensione 1 sono biolomorfe, e quindi in particolare omeomorfe, a tori considerati anch'essi come varietà complesse di dimensione 1.

Da un punto di vista algebrico possiamo definire un toro come $\mathbb{C}$ quozientato con un sottogruppo additivo generato da due vettori linearmente indipendenti (considerati come vettori di $\mathbb{R}^2$); a seconda dei vettori scelti si otterranno tori diversi dal punto di vista algebrico (anche se omeomorfi). A tori diversi corrisponderanno cubiche ellittiche diverse.

Ora sul toro è definita in modo banale una operazione di somma che deriva dalla somma in $\mathbb{C}$ modulo la relazione di equivalenza data dal sottogruppo con cui si quozienta. Così basterà dimostrare che coincidono il "$+$" già definito sulla cubica ellittica e la legge di gruppo ottenuta trasportando alla cubica la somma sul toro, tramite l'omeomorfismo tra il toro e la cubica.

Capitolo 1

Classificazione delle cubiche piane non singolari

A meno che non sia specificato esplicitamente, d'ora in poi lavoreremo sempre sul campo dei numeri complessi $\mathbb{C}$. Nel passaggio dal piano proiettivo al piano affine, cioè nel passaggio da coordinate omogenee a coordinate non omogenee (e viceversa), a meno che non sia indicato diversamente, useremo la mappa j_0, dove:

$$\begin{array}{rccc} j_o: & \mathbb{A}^2 & \to & \mathbb{P}^2 \\ & (x,y) & \to & (1,x,y) \end{array}$$

cioè deomogenizziamo rispetto ad x_0 ponendo:

$$x = \frac{x_1}{x_0}, \quad y = \frac{x_2}{x_0}.$$

1.1 Preliminari

Ricordiamo brevemente alcune definizioni che serviranno nel seguito.

Definizione 1.1. Una *curva affine piana* $\mathcal{C}$ è la classe di proporzionalità di un polinomio non costante $F(x,y) \in \mathbb{C}[x,y]$. Diremo che $F(x,y) = 0$ è una equazione di $\mathcal{C}$, e scriveremo anche $\mathcal{C} : F(x,y) = 0$.

Il *grado* di una curva affine $\mathcal{C}$ è il grado di un qualunque polinomio associato alla curva.

Il *supporto* di una curva affine è l'insieme:

$$supp\ \mathcal{C} := \{(x, y) \in \mathbb{A}^2 \mid F(x, y) = 0\}$$

dove la definizione chiaramente non dipende dal rappresentante F scelto per $\mathcal{C}$.

Una *curva proiettiva piana* è la classe di proporzionalità di $F(x_0, x_1, x_2)$, dove F è un polinomio *omogeneo* nelle variabili x_0, x_1, x_2. Il grado della curva è il grado di tale polinomio e la definizione del supporto è analoga alla precedente.

Definizione 1.2. Una curva $\mathcal{C}$ affine, rispettivamente proiettiva, si dice *irriducibile* se è irriducibile il polinomio $F(x, y)$, rispettivamente $F(x_0, x_1, x_2)$, che rappresenta tale curva; in caso contrario il polinomio si scriverà sotto la forma $F(x, y) = G_1(x, y) \cdots G_r(x, y)$ con $G_1, \cdots, G_r$ irriducibili. Se poniamo $\mathcal{C}_1 : G_1(x, y) = 0, \cdots, \mathcal{C}_r : G_r(x, y) = 0$, diremo che la curva $\mathcal{C}$ è somma delle sue *componenti* irriducibili $\mathcal{C}_1, \cdots, \mathcal{C}_r$ e scriveremo:

$$\mathcal{C} = \mathcal{C}_1 + \cdots + \mathcal{C}_r.$$

Definizione 1.3. La *molteplicità di intersezione* di una curva affine $\mathcal{C}$ con una retta L, data mediante una sua parametrizzazione:

$$\begin{cases} x = a + \alpha t \\ y = b + \beta t \end{cases}$$

in un suo punto $P = (a + \alpha t_0, b + \beta t_0)$ è il numero $m \in \mathbb{N} \cup \{\infty\}$ che rappresenta la molteplicità di t_0 come radice dell'equazione ottenuta sostituendo l'equazione di L in quella di $\mathcal{C}$, convenendo di porre tale molteplicità uguale a zero se il punto non appartiene alla curva e ∞ se la retta è componente della curva.

Definizione 1.4. Un punto P del supporto di una curva si dice *semplice* o *non singolare* se esiste almeno una retta nel fascio per P con molteplicità 1 di intersezione con la curva in tale punto. In caso contrario il punto si dice *multiplo* o *singolare*. Una curva si dice *singolare* se almeno un suo punto è singolare, *non singolare* o *liscia* in caso contrario.

Osservazione 1. Una condizione equivalente alla non singolarità di una curva affine $\mathcal{C}$ di equazione $F(x, y) = 0$ in suo punto P di coordinate (a, b) è che almeno una delle derivate $\frac{\partial F}{\partial x}\big|_P$ e $\frac{\partial F}{\partial y}\Big|_P$ sia non nulla. In tal caso la curva ammette retta tangente in P, di equazione:

$$\frac{\partial F}{\partial x}\Big|_P (x-a) + \frac{\partial F}{\partial y}\Big|_P (y-b) = 0.$$

In modo analogo se $\mathcal{D} : G(x_0, x_1, x_2) = 0$ è una curva proiettiva, essa è non singolare in un suo punto $Q = (a, b, c)$ se almeno una delle tre derivate parziali di G è non nulla in Q; in tal caso la curva ammette retta tangente in tale punto, data da:

$$\frac{\partial G}{\partial x_0}\Big|_Q x_0 + \frac{\partial G}{\partial x_1}\Big|_Q x_1 + \frac{\partial G}{\partial x_2}\Big|_Q x_2 = 0.$$

Si veda ad esempio [S], proposizione 34.2.

Definizione 1.5. Un punto del supporto di una curva proiettiva si dice di *flesso* se è non singolare e se esiste una retta per tale punto con molteplicità di intersezione ≥ 3. Si può mostrare che questa seconda condizione è equivalente a richiedere in tale punto l'annullamento del determinante della matrice hessiana associata al polinomio $F(x_0, x_1, x_2)$ (si veda [S], prop. 34.8).

Definizione 1.6. Una *cubica piana affine* o *proiettiva* è una curva di grado 3 di $\mathbb{A}^2$, rispettivamente di $\mathbb{P}^2$.

Siamo ora interessati alla classificazione proiettiva delle cubiche piane non singolari, le cosiddette *"cubiche ellittiche"*.

1.2 Classificazione di cubiche piane non singolari

Proposizione 1.2.1. *Ogni cubica proiettiva non singolare possiede almeno un flesso.*

Dimostrazione. Data una curva proiettiva $\mathcal{C} : F(x_0, x_1, x_2) = 0$ (F polinomio omogeneo), un flesso è un punto P non singolare nel suo supporto e le cui coordinate annullino il determinate $\mathcal{H}_F(x_0, x_1, x_2)$ della matrice hessiana di F. Ora consideriamo la curva proiettiva:

$$\mathcal{D} \ : \ \mathcal{H}_F(x_0, x_1, x_2) = 0;$$

affinchè P sia di flesso, essendo ogni punto di $\mathcal{C}$ non singolare per ipotesi, è sufficiente che sia $P \in supp\ \mathcal{D}$.

Basta quindi mostrare che le curve $\mathcal{C}$ e $\mathcal{D}$ ammettono almeno un'intersezione, ma questo è conseguenza del teorema generale che afferma che due qualunque curve proiettive piane si intersecano sempre in almeno un punto (si veda [S], teorema 33.1). □

Teorema 1.2.2. *Ogni cubica non singolare in $\mathbb{P}^2(\mathbb{C})$ è proiettivamente equivalente ad una cubica di equazione affine:*

$$y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathbb{C} \setminus \{0, 1\}. \tag{1.1}$$

Dimostrazione. Data una cubica $\mathcal{C}$ di $\mathbb{P}^2(\mathbb{C})$, essa possiede almeno un flesso per il teorema precedente. Eventualmente utilizzando una proiettività, possiamo assumere che tale flesso sia il punto $P = (0, 1, 0)$ e che la retta tangente in tale punto (che esiste perché $\mathcal{C}$ è liscia) sia la retta $x_2 = 0$.

Essendo $\mathcal{C}$ una cubica proiettiva, essa è definita mediante un polinomio $F(x_0, x_1, x_2)$ omogeneo di grado 3. Così, grazie all'osservazione 1, le condizioni precedenti si traducono nell'imporre che:

$$F(0,1,0) = 0, \quad \left.\frac{\partial F}{\partial x_0}\right|_{(0,1,0)} = 0, \quad \left.\frac{\partial F}{\partial x_1}\right|_{(0,1,0)=0} = 0, \quad \left.\frac{\partial F}{\partial x_2}\right|_{(0,1,0)} \neq 0. \tag{1.2}$$

Verifichiamo ora a cosa equivalgono le condizioni (1.2) scrivendo esplicitamente il polinomio F come polinomio di terzo grado omogeneo in x_0, x_1, x_2, cioè:

$$F(x_0,x_1,x_2) = a_1{x_0}^3 + a_2{x_1}^3 + a_3{x_2}^3 + a_4{x_0}^2x_1 + a_5{x_0}^2x_2 +$$

$$+a_6x_0{x_1}^2 + a_7{x_1}^2x_2 + a_8x_0{x_2}^2 + a_9x_1{x_2}^2 + a_{10}x_0x_1x_2.$$

Otteniamo allora:

$$F(0,1,0) = a_2 \quad \Rightarrow \quad a_2 = 0; \tag{1.3}$$

inoltre derivando in x_0:

$$\frac{\partial F}{\partial x_0} = 3a_1{x_0}^2 + 2a_4x_0x_1 + 2a_5x_0x_2 + a_6{x_1}^2 + a_8{x_2}^2 + a_{10}x_1x_2$$

$$\Rightarrow \quad \left.\frac{\partial F}{\partial x_0}\right|_{(0,1,0)} = a_6 \quad \Rightarrow \quad a_6 = 0. \tag{1.4}$$

Infine derivando in x_1 otteniamo:

$$\frac{\partial F}{\partial x_1} = 3a_2{x_1}^2 + a_4{x_0}^2 + 2a_6x_0x_1 + 2a_7x_1x_2 + a_9{x_2}^2 + a_{10}x_0x_2$$

$$\Rightarrow \quad \left.\frac{\partial F}{\partial x_1}\right|_{(0,1,0)} = 3a_2 \quad \Rightarrow \quad a_2 = 0. \tag{1.5}$$

cioè di nuovo la condizione (1.3).

Quindi la $\mathcal{C}$ ha equazione:

$$a_1{x_0}^3 + a_3{x_2}^3 + a_4{x_0}^2x_1 + a_5{x_0}^2x_2 + a_7{x_1}^2x_2 +$$

$$+a_8x_0{x_2}^2 + a_9x_1{x_2}^2 + a_{10}x_0x_1x_2 = 0,$$

e, deomogenizzando rispetto ad x_1, cioè ponendo $x = \frac{x_0}{x_1}, \quad y = \frac{x_2}{x_1}$, si ha:

$$\mathcal{C} \ : \ a_1x^3 + a_3y^3 + a_4x^2 + a_5x^2y + a_7y + a_8xy^2 + a_9y^2 + a_{10}xy = 0.$$

Quindi la tangente $y = 0$ in $P = (0, 0)$ ha molteplicità di intersezione con $\mathcal{C}$ almeno 3 se e solo se l'equazione $a_1x^3+a_4x^2 = 0$ ha una radice tripla, cioè se e solo se $a_4 = 0$. Ricordiamo infatti che l'equazione non è identicamente nulla perchè $\mathcal{C}$ è per ipotesi irriducibile, dunque la retta $y = 0$ non è componente della curva.

Infine ricordiamo la condizione:

$$\left.\frac{\partial F}{\partial x_2}\right|_{(0,1,0)} \neq 0,$$

che si traduce nel vincolo:

$$0 \neq \left.(3a_3{x_2}^2 + a_5{x_0}^2 + a_7{x_1}^2 + 2a_8x_0x_2 + 2a_9x_1x_2 + a_{10}x_0x_1)\right|_{(0,1,0)} = a_7.$$

Così concludiamo che per il polinomio F vale:

$$a_2 = 0, \quad a_4 = 0, \quad a_6 = 0, \quad a_7 \neq 0.$$

Quindi:

$$F(x_0, x_1, x_2) = a_1{x_0}^3+a_3{x_2}^3+a_5{x_0}^2x_2+a_7{x_1}^2x_2+a_8x_0{x_2}^2+a_9x_1{x_2}^2+a_{10}x_0x_1x_2 =$$

$$= (a_1{x_0}^3 + a_3{x_2}^3 + a_5{x_0}^2x_2 + a_8x_0{x_2}^2) + x_1x_2(a_{10}x_0 + a_7x_1 + a_9x_2).$$

Ponendo ora $\alpha = a_{10}$, $\beta = a_7$, $\gamma = a_9$ e $\phi(x_0, x_2) = a_1{x_0}^3 + a_3{x_2}^3 + a_5{x_0}^2x_2 + a_8x_0{x_2}^2$, otteniamo:

$$F(x_0, x_1, x_2) = x_1x_2(\alpha x_0 + \beta x_1 + \gamma x_2) + \phi(x_0, x_2).$$

Ricordando che $\beta = a_7 \neq 0$, possiamo definire la proiettività:

$$G(x_0, x_1, x_2) := \left(x_0, x_1 - \frac{\alpha x_0 + \gamma x_2}{2\beta}, x_2\right).$$

Così la curva $\mathcal{C}$ viene portata dalla proiettività G^{-1} nella curva $\mathcal{D}$: $\tilde{F}(x_0, x_1, x_2) = 0$, dove $\tilde{F}$ è il polinomio omogeneo di grado 3:

$$\tilde{F}(x_0, x_1, x_2) := F\left(x_0, x_1 - \frac{\alpha x_0 + \gamma x_2}{2\beta}, x_2\right) =$$

$$= \left(x_1 - \frac{\alpha x_0}{2\beta} - \frac{\gamma x_2}{2\beta}\right) x_2 \left(\alpha x_0 + \beta x_1 - \frac{\alpha x_0}{2} - \frac{\gamma x_2}{2} + \gamma x_2\right) + \phi\left(x_0, x_2\right) =$$

$$= \left(x_1 x_2 - \frac{\alpha x_0 x_2}{2\beta} - \frac{\gamma {x_2}^2}{2\beta}\right) \left(\frac{\alpha x_0}{2} + \beta x_1 + \frac{\gamma x_2}{2}\right) + \phi(x_0, x_2) =$$

$$= \frac{\alpha}{2} x_0 x_1 x_2 + \beta {x_1}^2 x_2 + \frac{\gamma}{2} x_1 {x_2}^2 - \frac{\alpha^2}{4\beta} {x_0}^2 x_2 - \frac{\alpha}{2} x_0 x_1 x_2 +$$

$$- \frac{\alpha\gamma}{4\beta} x_0 {x_2}^2 - \frac{\alpha\gamma}{4\beta} x_0 {x_2}^2 - \frac{\gamma}{2} x_1 {x_2}^2 - \frac{\gamma^2}{4\beta} {x_2}^3 + \phi(x_0, x_2) =$$

$$= \beta {x_1}^2 x_2 + \left(\phi(x_0, x_2) - \frac{\alpha^2}{4\beta} {x_0}^2 x_2 - \frac{\alpha\gamma}{2\beta} x_0 {x_2}^2 - \frac{\gamma^2}{4\beta} {x_2}^3\right) =$$

$$= \beta {x_1}^2 x_2 + \psi(x_0, x_2) \tag{1.6}$$

dove ψ è un polinomio omogeneo di grado 3 in x_0, x_2.

Ora x_2 non divide il polinomio ψ, infatti se lo dividesse, allora x_2 dividerebbe anche il polinomio $\tilde{F}$, che sarebbe quindi riducibile. Ma per ipotesi il polinomio F è irriducibile e questa è una proprietà invariante per proiettività.

Scriviamo ora l'equazione della nuova curva in $\mathbb{A}^2$ deomogenizzando rispetto a x_2, ponendo cioè $x = \frac{x_0}{x_2}$, $y = \frac{x_1}{x_2}$; otterremo così la curva:

$$\tilde{\mathcal{D}} \ : \ \beta y^2 = G(x), \quad \beta \neq 0 \tag{1.7}$$

dove $G(x)$ è un polinomio nella x di grado 3 perché x_2 non divideva il polinomio $\psi(x_0, x_2)$.

Ora dal momento che lavoriamo in $\mathbb{C}$, il polinomio G si scompone come:

$$G(x) = \delta(x - t_1)(x - t_2)(x - t_3), \quad \delta \neq 0, \quad t_1, t_2, t_3 \in \mathbb{C}$$

cioè, ricordando che $\beta \neq 0$, possiamo scrivere la curva piana affine nella forma:

$$\tilde{\mathcal{D}} \ : \ H(x, y) = 0, \quad H(x, y) := y^2 - \frac{\delta}{\beta}(x - t_1)(x - t_2)(x - t_3).$$

Osserviamo che le tre radici t_1, t_2, t_3 sono necessariamente distinte, infatti se $G(x)$ avesse una radice multipla, ad esempio t_1, sarebbe $G'(t_1) = 0$, così

avremmo:

$$H(t_1,0)=0, \quad \left.\frac{\partial H}{\partial x}\right|_{(t_1,0)} = -\frac{G'(t_1)}{\beta}=0, \quad \left.\frac{\partial H}{\partial y}\right|_{(t_1,0)}=0.$$

Così il punto $(t_1,0)$ sarebbe un punto singolare per la curva $\tilde{\mathcal{D}}$, assurdo perché la curva $\mathcal{C}$ era non singolare per ipotesi e questa è una proprietà invariante per proiettività (e restringendosi dal piano proiettivo al piano affine).

Consideriamo ora l'affinità:

$$(x,y)\mapsto((t_2-t_1)X+t_1,\gamma Y)$$

dove γ sia uno dei due numeri complessi tali che $\gamma^2=\frac{\delta}{\beta}(t_2-t_1)^3$.

Se applichiamo tale affinità a $\tilde{\mathcal{D}}$, otteniamo la cubica di equazione affine:

$$0=\frac{\delta}{\beta}(t_2-t_1)^3Y^2-\frac{\delta}{\beta}X(t_2-t_1)\left[X(t_2-t_1)+(t_1-t_2)\right]\left[X(t_2-t_1)+(t_1-t_3)\right]=$$

$$=\frac{\delta}{\beta}(t_2-t_1)^3\left[Y^2-X(X-1)\left(X-\frac{t_3-t_1}{t_2-t_1}\right)\right].$$

Ora dividendo per $\frac{\delta}{\beta}$ e per $(t_2-t_1)^3$ entrambi diversi da zero per quanto detto finora, e ponendo $\lambda:=\frac{t_3-t_1}{t_2-t_1}$, otteniamo la cubica di equazione:

$$Y^2=X(X-1)(X-\lambda), \quad \lambda\in\mathbb{C}\setminus\{0,1\}.$$

□

Questo teorema non esaurisce la classificazione delle cubiche piane non singolari, dal momento che non sappiamo se tra le cubiche di equazione (1.1) ce ne siano di proiettivamente equivalenti, nè se tra di esse ve ne siano o meno di singolari.

Per concludere dobbiamo in primo luogo dimostrare il seguente:

Lemma 1.2.3. *Ogni cubica $\mathcal{C}$ di equazione affine:*

$$y^2=x(x-1)(x-\lambda), \quad \lambda\in\mathbb{C}\setminus\{0,1\}$$

è non singolare.

Dimostrazione. Un polinomio associato alla cubica è

$$F = -y^2 + x^3 - (\lambda + 1)x^2 + \lambda x \quad \text{con } \lambda \in \mathbb{C} \setminus \{0, 1\}.$$

Per dimostrare che la cubica è non singolare, è sufficiente provare che almeno una delle due derivate di F in x o y è non nulla. Calcoliamo allora:

$$\frac{\partial F}{\partial x} = 3x^2 - 2(\lambda + 1)x + \lambda, \qquad \frac{\partial F}{\partial y} = -2y.$$

Ora se $\frac{\partial F}{\partial y} \neq 0$, abbiamo finito; in caso contrario:

$$\frac{\partial F}{\partial y} = 0 \quad \Rightarrow \quad y = 0 \quad \Rightarrow \quad x = 0 \text{ oppure } x = 1 \text{ oppure } x = \lambda.$$

D'altra parte i tre valori 0, 1 e λ sono radici semplici per il polinomio $x^3 - (\lambda + 1)x^2 + \lambda x$, quindi non sono radici per la sua derivata prima $3x^2 - 2(\lambda + 1)x + \lambda$, cioè $\frac{\partial f}{\partial x} \neq 0$.

Questo basta per assicurare che la cubica sia non singolare nei suoi punti propri; d'altra parte si vede subito che è non singolare anche nel suo unico punto improprio $(0, 0, 1)$. □

Per concludere la classificazione dobbiamo prima ricordare le seguenti definizioni:

Definizione 1.7. Siano assegante quattro rette L_1, L_2, L_3, L_4 di $\mathbb{P}^2(\mathbb{C})$ (le prime 3 distinte) appartenenti al fascio (proiettivo) di rette passanti per un punto P. Tale fascio può essere considerato come $\mathbb{P}^1(\mathbb{C})$; ricordiamo infatti che se $r : p(x_0, x_1, x_2) = 0$ e $s : q(x_0, x_1, x_2) = 0$ sono due rette proiettive distinte del fascio, un'equazione del fascio stesso è:

$$\alpha p(x_0, x_1, x_2) + \beta q(x_0, x_1, x_2) = 0, \quad (\alpha, \beta) \in \mathbb{P}^1(\mathbb{C});$$

così possiamo associare alla generica retta del fascio le sue "coordinate omogenee" (α, β). Si dice allora *birapporto della quaterna di rette* L_1,L_2,L_3,L_4, nell'ordine dato, il birapporto dei quattro punti $(\alpha_1, \beta_1), \cdots, (\alpha_4, \beta_4)$ di $\mathbb{P}^1(\mathbb{C})$,

nell'ordine dato, dove L_i ha coordinate (α_i, β_i). Il birapporto β sarà allora dato da:

$$\beta = \frac{\begin{vmatrix} \alpha_1 & \alpha_4 \\ \beta_1 & \beta_4 \end{vmatrix} \begin{vmatrix} \alpha_2 & \alpha_3 \\ \beta_2 & \beta_3 \end{vmatrix}}{\begin{vmatrix} \alpha_2 & \alpha_4 \\ \beta_2 & \beta_4 \end{vmatrix} \begin{vmatrix} \alpha_1 & \alpha_3 \\ \beta_1 & \beta_3 \end{vmatrix}}.$$

La definizione è ben posta perché le prime tre rette sono distinte, quindi lo sono anche i corrispondenti primi 3 punti, per cui il birapporto dei 4 punti è ben definito.

Per le proprietà del birapporto di 4 punti, rimandiamo a [S], teorema 27.7.

Definizione 1.8. Data una quaterna di punti P_1, P_2, P_3, P_4 tutti distinti e detto β il birapporto dei 4 punti presi in un certo ordine, si dice *modulo della quaterna di punti* il numero:

$$j(\beta) := \frac{(\beta^2 - \beta + 1)^3}{\beta^2(\beta - 1)^2}.$$

Si può dimostare ([S], lemma 27.8) che il modulo $j(\beta)$ dipende solo dalla quaterna e non dall'ordine scelto per i punti. In effetti se β è il birapporto di tali punti presi nell'ordine indicato, il birapporto di ogni altra possibile loro permutazione (a priori 24 possibilità) può assumere solo i 6 valori:

$$\beta, \quad \frac{1}{\beta}, \quad 1 - \beta, \quad \frac{1}{1-\beta}, \quad \frac{\beta}{\beta - 1}, \quad \frac{\beta - 1}{\beta},$$

e d'altra parte si dimostra che $j(\beta) = j(\beta')$ se e solo se β' coincide con uno dei valori precedenti.

Quindi date quattro rette distinte appartenenti allo stesso fascio, si dice *modulo della quaterna di rette* il valore $j(\beta)$ dove β è il birapporto della quaterna di rette ordinata in un modo qualunque. Quindi il modulo di una quaterna di rette dipende solo dalla quaterna e non dall'ordine scelto su di essa.

Osservazione 2. Si dimostra ([S], teorema 27.9) che due quaterne di punti distinti di $\mathbb{P}^1$ sono proiettivamente equivalenti se e solo se sono uguali i loro moduli. Quindi ciò vale anche per due quaterne di rette distinte di due fasci di rette.

Teorema 1.2.4. *Dati due flessi qualunque di una cubica non singolare $\mathcal{C}$, esiste un terzo flesso sulla curva allineato con i primi due. Inoltre fissati due flessi qualunque, esiste una proiettività $\Phi : \mathbb{P}^2 \to \mathbb{P}^2$ che porti il primo flesso nel secondo e trasformi $\mathcal{C}$ in se stessa.*

Per la dimostrazione, si veda [S], teorema 36.2.

Teorema 1.2.5. *(Salmon, 1851) Data una cubica piana non singolare $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ e un suo flesso P, esistono esattamente quattro rette distinte passanti per P e tangenti a $\mathcal{C}$, inclusa la tangente in P. Il loro modulo è indipendente dalla scelta del flesso P.*

Dimostrazione. In base al teorema 1.2.2 è sempre possibile portare mediante una proiettività la cubica $\mathcal{C}$ nella cubica di equazione affine:

$$\mathcal{D} \ : \ y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathbb{C} \setminus \{0,1\} \tag{1.8}$$

e di equazione proiettiva $F(x_0, x_1, x_2) = 0$, dove:

$$F(x_0, x_1, x_2) := x_0 {x_2}^2 - x_1(x_1 - x_0)(x_1 - \lambda x_0), \quad \lambda \in \mathbb{C} \setminus \{0,1\}. \tag{1.9}$$

Ora la proiettività utilizzata manda flessi in flessi e rette tangenti in rette tangenti, così se dimostriamo che ogni flesso P' della cubica $\mathcal{D}$ ammette quattro tangenti distinte (compresa la tangente per P'), lo stesso varrà per la cubica $\mathcal{C}$ nel flesso P corrispondente. Inoltre, dato che una proiettività di $\mathbb{P}^2$ induce una proiettività tra i due fasci di rette, il modulo delle 4 rette tangenti in P e in P' sarà lo stesso (si veda l'osservazione 2). Non è quindi restrittivo esaminare solo i flessi di una cubica di equazione (1.9).

Inoltre dato un qualunque flesso di una cubica in tale forma, grazie al teorema 1.2.4, si può esibire una proiettività che porti tale punto nel flesso $P = (0, 0, 1)$, lasciando invariata la cubica. Come sopra, la proiettività conserva il numero di rette tangenti alla cubica e passanti per un punto assegnato, e il loro modulo.

È quindi sufficiente provare che per una cubica di equazione (1.9), dal flesso $P = (0, 0, 1)$ escono 4 tangenti distinte.

Ora in primo luogo la retta impropria $x_0 = 0$ è la tangente alla curva in P, infatti:

$$\left.\frac{\partial F}{\partial x_0}\right|_{(0,0,1)} = {x_2}^2 - x_1[-(x_1 - \lambda x_0) - \lambda(x_1 - x_0)]\big|_{(0,0,1)} = 1,$$

$$\left.\frac{\partial F}{\partial x_1}\right|_{(0,0,1)} = -[(x_1 - x_0)(x_1 - \lambda x_0) + x_1(x_1 - \lambda x_0) + x_1(x_1 - x_0)]|_{(0,0,1)} = 0,$$

$$\left.\frac{\partial F}{\partial x_2}\right|_{(0,0,1)} = (2x_0x_2)|_{(0,0,1)} = 0;$$

così la tangente in P ha equazione $x_0 = 0$.

Ora oltre alla retta impropria, che abbiamo già verificato essere retta tangente alla cubica in P, le eventuali altre rette tangenti e passanti per P devono avere P come punto improprio, cioè devono avere equazione affine $x = c,\ \ c \in \mathbb{C}$. D'altra parte per essere tangenti alla curva, lo devono essere in un punto proprio, così si può utilizzare l'equazione (1.8). Troviamo quindi che $x = c$ è tangente alla cubica se e solo se l'equazione nella variabile y:

$$y^2 = c(c - 1)(c - \lambda)$$

ha una radice doppia, dunque se $c = 0 \quad \text{o} \quad c = 1 \quad \text{o} \quad c = \lambda$.

Così la cubica possiede esattamente 4 tangenti distinte per il flesso $P = (0, 0, 1)$; esse sono la retta impropria e le rette di equazione affine $x = 0,\ \ x = 1 \quad \text{e} \quad x = \lambda$. □

Definizione 1.9. In base al teorema precedente, possiamo definire il *modulo di una cubica non singolare* $\mathcal{C}$ come il modulo della quaterna di tangenti pas-

santi per un suo qualunque flesso. Tale modulo, che è un numero complesso, si indica con $j(\mathcal{C})$.

Abbiamo verificato che il modulo di una cubica $\mathcal{C}$ non dipende dal flesso in cui si calcola, ed è invariante per proiettività. Così, per trovare tale valore, è sufficiente calcolarlo nel punto $P = (0, 0, 1)$ della cubica in forma (1.8) a cui $\mathcal{C}$ è proiettivamente equivalente.

Ora possiamo scegliere come rette generatrici del fascio per P le rette $x_0 = 0$ e $x_1 = 0$, cioè la retta impropria e l'asse y del piano affine. Il fascio di centro P ha quindi equazione:

$$\alpha x_1 + \beta x_0 = 0, \quad (\alpha, \beta) \in \mathbb{P}^1(\mathbb{C}).$$

Chiaramente le rette generatrici del fascio $x_1 = 0$ e $x_0 = 0$ avranno coordinate rispettivamente $(1, 0)$ e $(0, 1)$. La retta affine $x = 1$, cioè la retta proiettiva $x_1 - x_0 = 0$ è associata al punto $(1, -1)$ e infine alla retta $x = \lambda$, cioè alla retta proiettiva $x_1 - \lambda x_0 = 0$, viene associato il punto $(1, -\lambda)$. Con i 4 punti $(1, 0), (0, 1), (1, -1), (1, -\lambda)$ trovati calcoliamo il birapporto β:

$$\beta = \frac{\begin{vmatrix} 1 & 1 \\ 0 & -\lambda \end{vmatrix} \begin{vmatrix} 0 & 1 \\ 1 & -1 \end{vmatrix}}{\begin{vmatrix} 0 & 1 \\ 1 & -\lambda \end{vmatrix} \begin{vmatrix} 1 & 1 \\ 0 & -1 \end{vmatrix}} = \frac{(-\lambda)(-1)}{(-1)(-1)} = \lambda.$$

Così:

$$j(\mathcal{C}) = j(\beta) = j(\lambda) = \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

Proposizione 1.2.6. *Due cubiche piane non singolari $\mathcal{C}$ e $\mathcal{D}$ sono proiettivamente equivalenti se e solo se $j(\mathcal{C}) = j(\mathcal{D})$.*

Dimostrazione. Siano $\mathcal{C}$ e $\mathcal{D}$ due cubiche piane non singolari, allora esse sono proiettivamente equivalenti a due cubiche $\tilde{\mathcal{C}}$ e $\tilde{\mathcal{D}}$ di equazioni rispettivamente:

$$\tilde{\mathcal{C}} \ : \ y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathbb{C} \setminus \{0, 1\},$$

$$\tilde{\mathcal{D}} \ : \ y^2 = x(x-1)(x-\mu), \quad \mu \in \mathbb{C} \setminus \{0,1\}.$$

Se $\mathcal{C}$ e $\mathcal{D}$ sono proiettivamente equivalenti, allora per quanto detto finora, i loro moduli $j(\mathcal{C})$ e $j(\mathcal{D})$ coincidono.

Viceversa, se $j(\mathcal{C}) = j(\mathcal{D})$, allora:

$$j(\lambda) = j(\tilde{\mathcal{C}}) = j(\mathcal{C}) = j(\mathcal{D}) = j(\tilde{\mathcal{D}}) = j(\mu).$$

Quindi per quanto detto nella definizione 1.8, necessariamente μ può assumere solo uno dei sei valori:

$$\lambda, \quad \frac{1}{\lambda}, \quad 1-\lambda, \quad \frac{1}{1-\lambda}, \quad \frac{\lambda}{\lambda-1}, \quad \frac{\lambda-1}{\lambda}.$$

Nel primo caso non c'è niente da dimostrare, nei restanti casi è sufficiente esibire delle proiettività che mutino l'equazione di $\tilde{\mathcal{C}}$ in quella di $\tilde{\mathcal{D}}$. In effetti è sufficiente mostrare delle affinità che portino le rispettive equazioni affini l'una nell'altra.

Nel secondo caso ($\mu = \frac{1}{\lambda}$) l'affinità è quella di equazioni:

$$(x, y) \mapsto (\lambda x, \alpha y) \tag{1.10}$$

dove $\alpha \in \mathbb{C}$ è un numero complesso tale che $\alpha^2 = \lambda^3$.

Infatti con tale sostituzione $\tilde{\mathcal{C}}$ viene portata nella curva di equazione:

$$\lambda^3 y^2 = \lambda x(\lambda x - 1)(\lambda x - \lambda)$$

o anche, dividendo per λ^3, ricordando che $\lambda \neq 0$,

$$y^2 = x\left(x - \frac{1}{\lambda}\right)(x-1)$$

cioè quanto volevamo.

Nel terzo caso ($\mu = 1 - \lambda$) l'affinità da usare è quella di equazioni:

$$(x, y) \mapsto (-x+1, iy) \tag{1.11}$$

In tal caso, infatti, l'equazione di $\tilde{\mathcal{C}}$ assume la forma:

$$-y^2 = (-x+1)(-x+1-1)(-x+1-\lambda)$$

o anche, cambiando i segni ad entrambi i membri:

$$y^2 = (x-1)x(x-(1-\lambda)).$$

Infine, per quanto riguarda i tre casi rimanenti, basta comporre le affinità usate in questi due casi. In particolare, per il caso $\mu = \frac{1}{1-\lambda}$ è sufficiente comporre l'affinità (1.10) e la (1.11), ottenendo:

$$(x, y) \mapsto ((\lambda - 1)x + 1, i\eta y) \tag{1.12}$$

dove $\eta^2 = (1-\lambda)^3$.

Per quanto riguarda il caso $\mu = \frac{\lambda}{\lambda-1} = 1 - \frac{1}{1-\lambda}$, si compongono le affinità (1.11) e (1.12):

$$(x, y) \mapsto ((1-\lambda)x + \lambda, \eta y). \tag{1.13}$$

Infine per il quinto caso, cioè $\mu = \frac{\lambda-1}{\lambda}$ basta comporre la (1.10) e la (1.13), ottenendo l'affinità:

$$(x.y) \to (\lambda(1-x), \xi y) \tag{1.14}$$

dove $\xi^2 = -\lambda^3$. □

I teoremi 1.2.2 e 1.2.6 permettono di enunciare il teorema di classificazione delle cubiche piane non singolari di $\mathbb{P}^2(\mathbb{C})$:

Teorema 1.2.7. *Ogni cubica non singolare di $\mathbb{P}^2(\mathbb{C})$ è proiettivamente equivalente ad una cubica di equazione affine:*

$$\mathcal{C}_\lambda \ : \ y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathbb{C} \setminus \{0, 1\}.$$

Due cubiche $\mathcal{C}_\lambda$ e $\mathcal{C}_\mu$ sono proiettivamente equivalenti se e solo se $j(\lambda) = j(\mu)$.

Quindi se chiamiamo $\mathcal{M}$ l'insieme di tutte le cubiche non singolari e definiamo su di esso la relazione di equivalenza $\sim$:

$$\mathcal{C} \sim \mathcal{D} \overset{def}{\iff} \mathcal{C} \text{ è proiettivamente equivalente a } \mathcal{D}$$

otteniamo che l'insieme quoziente $\mathcal{M}/\sim$ delle classi di equivalenza proiettiva è in corrispondenza biunivoca con l'insieme:

$$\{j(\lambda) \mid \lambda \in \mathbb{C} \setminus \{0,1\}\}.$$

Ora dal momento che un numero della forma $j(\lambda)$ è immagine al più di 6 valori distinti di $\mathbb{C}$, ne segue che $\mathcal{M}/\sim$ ha la stessa cardinalità di $\mathbb{C}$, cioè la cardinalità del continuo. Questo è un risultato completamente diverso da quello ottenuto nella classificazione proiettiva di coniche, in cui si otteneva solo un numero finito di classi di equivalenza, in particolare solo una classe di equivalenza per coniche non singolari.

1.3 Classificazione di cubiche singolari irriducibili

In questa sezione mostreremo rapidamente alcuni dei principali risultati sulle cubiche singolari irriducibili, omettendo le dimostrazioni. Si veda, ad esempio, [S], proposizione 34.6 e teorema 36.5.

Definizione 1.10. Abbiamo già visto (definizione 1.4) che un punto singolare per una curva $\mathcal{C}$ è un punto della curva tale che ogni retta passante per esso ha molteplicità di intersezione ≥ 2 con $\mathcal{C}$. Diremo che tale punto singolare è un *punto m-uplo* (in particolare *doppio*, *triplo*, ...) di $\mathcal{C}$ se il minimo delle molteplicità di intersezione è esattamente $m = 2, 3, ...$

In particolare, si può mostrare che un punto P è doppio per una curva affine di equazione $F(x,y) = 0$ se e solo se $\frac{\partial F}{\partial x}\big|_P = \frac{\partial F}{\partial y}\Big|_P = 0$ e almeno una delle derivate seconde di F in x e y è diversa da zero in P.

Vale allora la seguente proposizione:

Proposizione 1.3.1. *Ogni cubica irriducibile possiede al più un punto singolare, che deve essere necessariamente un punto doppio.*

Ne segue che le cubiche irriducibili singolari possiedono esattamente un punto singolare doppio.

Diamo inoltre la seguente definizione:

Definizione 1.11. Una *tangente principale* ad una curva nel suo punto doppio P è una retta del fascio per tale punto e con molteplicità di intersezione ≥ 3 con la curva.

Si può mostrare che questa condizione è soddisfatta per un punto doppio da almeno una retta e al più da due, cioè in un suo punto doppio una curva piana ammette una o due tangenti principali. Se ne ammette due distinte, il punto si dirà *nodo*, in caso contrario *cuspide*.

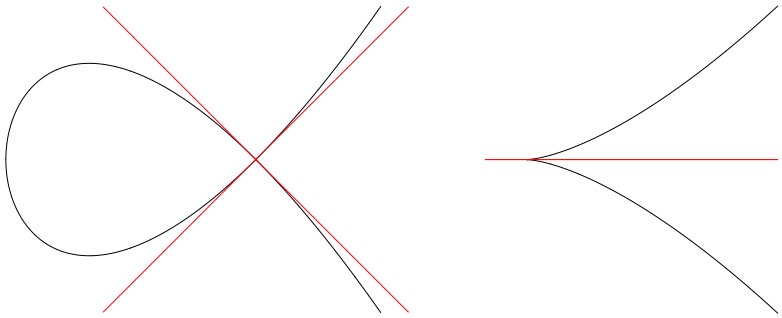

Figura 1.1: Sulla sinistra un nodo, sulla destra una cuspide, insieme alle loro tangenti principali nei punti doppi.

Vale allora il seguente teorema:

Teorema 1.3.2. *Ogni cubica singolare irriducibile con un nodo è proiettivamente equivalente alla cubica di equazione affine:*

$$\mathcal{C} : y^2 = x^2(x-1).$$

Ogni cubica singolare irriducibile con una cuspide è proiettivamente equivalente alla cubica di equazione affine:

$$\mathcal{D} : y^2 = x^3.$$

Entrambe possiedono un punto singolare doppio nell'origine e un flesso in $(0, 0, 1)$.

Questo conclude la classificazione delle cubiche singolari irriducibili. Questo teorema e l'analogo per le cubiche non singolari permettono di affermare che ogni cubica piana irriducibile possiede sempre almeno un flesso.

Capitolo 2

La legge di gruppo per le cubiche

Sul supporto di una cubica non singolare $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ è possibile definire una struttura di gruppo abeliano in modo puramente geometrico; tale operazione di gruppo sarà indicata nel seguito con "+". Vogliamo cioè descrivere la costruzione che a partire da due punti A e B nel supporto di $\mathcal{C}$ permette di definire un terzo punto C (detto somma di A e B), ancora nel supporto della curva.

2.1 Costruzione geometrica

In primo luogo è necessario scegliere un qualunque punto O di $\mathcal{C}$. Tale punto sarà fissato lungo tutta la costruzione seguente e a scelte diverse di tale punto corrisponderanno leggi di gruppo diverse. Diamo ora la seguente:

Definizione 2.1. Se A e B sono due punti distinti sulla cubica, si dice $R(A, B)$ il terzo punto di intersezione della retta per A e B con $\mathcal{C}$. Se invece $A = B$, allora come retta si considera quella tangente alla curva in A. Tale retta esiste perché stiamo lavorando su una cubica non singolare, quindi in ogni punto esiste la retta tangente. Anche in questo caso, chiamiamo $R(A, B)$ il terzo punto di intersezione di tale retta con la cubica. In entrambi i casi non escludiamo che il punto $R(A, B)$ coincida con i precedenti.

Si tratta in primo luogo di verificare se il punto $R(A, B)$ è ben definito,

cioè se esiste come terzo punto di intersezione della retta con la cubica. Ora se $A = (a_0, a_1, a_2)$ e $B = (b_0, b_1, b_2)$, la retta per A e B (con $A \neq B$) nel piano proiettivo ha equazioni parametriche della forma:

$$(x_0, x_1, x_2) = \alpha(a_0, a_1, a_2) + \beta(b_0, b_1, b_2), \quad (\alpha, \beta) \in \mathbb{P}^1(\mathbb{C}).$$

Quindi se intersechiamo tale retta con la cubica di equazione $F(x_0, x_1, x_2) = 0$, otteniamo:

$$\begin{cases} x_0 = a_0\alpha + b_0\beta \\ x_1 = a_1\alpha + b_1\beta \\ x_2 = a_2\alpha + b_2\beta \\ F(x_0, x_1, x_2) = 0. \end{cases}$$

Così, sostituendo x_0, x_1 e x_2, ricaviamo un polinomio $G(\alpha, \beta)$ omogeneo di grado 3 eguagliato a zero. Le radici di tale polinomio sostituite nelle equazioni parametriche della retta danno le coordinate dei punti di intersezione. Ora tale polinomio non è identicamente nullo perché questo avviene se e solo se la retta è componente irriducibile della cubica, ma abbiamo richiesto che la cubica su cui lavoriamo sia irriducibile. Quindi G ammette tre radici, contate con molteplicità.

Ora il polinomio $G(\alpha, \beta)$ è già divisibile per i due fattori lineari α e β perché ammette le coppie di soluzioni $(\alpha = 1, \beta = 0)$ e $(\alpha = 0, \beta = 1)$ che corrispondono ai punti A e B rispettivamente, quindi G si spezza come $G(\alpha, \beta) = \alpha\beta(c_1\alpha + c_2\beta)$.

Se invece A coincide con B, la retta usata è tangente la cubica, quindi la molteplicità di intersezione della retta con la cubica in A è 2; in questo caso G sarà divisibile per α^2.

Così G ammette come zero la coppia $(c_2, -c_1)$. Alla radice trovata, sostituendo nelle equazioni parametriche della retta, corrisponde un punto sull'intersezione della cubica e della retta, eventualmente coincidente con i precedenti.

È importante sottolineare che il risultato trovato non dipende affatto dalla natura di $\mathbb{C}$ come campo algebricamente chiuso, ma vale in generale su un

qualsiasi campo su cui il polinomio G sia definito, cioè in un qualsiasi campo in cui sia definita la cubica usata.

Questo porta da un lato ad affermare che se consideriamo, come usualmente, il grafico della cubica non in $\mathbb{P}^2(\mathbb{C})$, ma solo la sua porzione rappresentabile in $\mathbb{A}^2(\mathbb{R})$ e consideriamo 2 punti di $\mathbb{A}^2(\mathbb{R})$ sulla cubica, il terzo punto di intersezione, che abbiamo già dimostrato esistere, sarà ancora nel piano $\mathbb{A}^2(\mathbb{R})$ o eventualmente nella retta impropria di tale piano, e quindi si potrà visualizzare come una direzione.

In secondo luogo questo è uno dei motivi per cui le cubiche ellittiche assumono importanza in teoria dei numeri e in crittografia, in quanto si possono definire leggi di gruppo anche nel caso in cui il campo sia $\mathbb{Q}$ o un campo di Galois, a patto che la caratteristica del campo sia diversa da 2.

Ritorniamo alla costruzione della legge di gruppo dando la seguente:

Definizione 2.2. Nel seguito, con un abuso di notazione, denoteremo con $\mathcal{C}$ anche il supporto di $\mathcal{C}$. L'operazione di gruppo è allora l'operazione binaria data da:

$$\begin{array}{rccc} + : & \mathcal{C} \times \mathcal{C} & \rightarrow & \mathcal{C} \\ & (A, B) & \rightarrow & R(R(A, B), O) \end{array}$$

La costruzione geometrica è quindi la seguente:

1. dati due punti A e B sulla curva $\mathcal{C}$, si costruisce la retta r passante per A e B nel caso in cui essi siano distinti o tangente alla curva in A se i due punti coincidono;

2. si determina C', terzo punto di intersezione di r con con $\mathcal{C}$;

3. si trova la retta s passante per C' e per il punto O fissato sulla cubica;

4. si chiama C il terzo punto di intersezione di s con $\mathcal{C}$;

5. infine si definisce $A + B := C$.

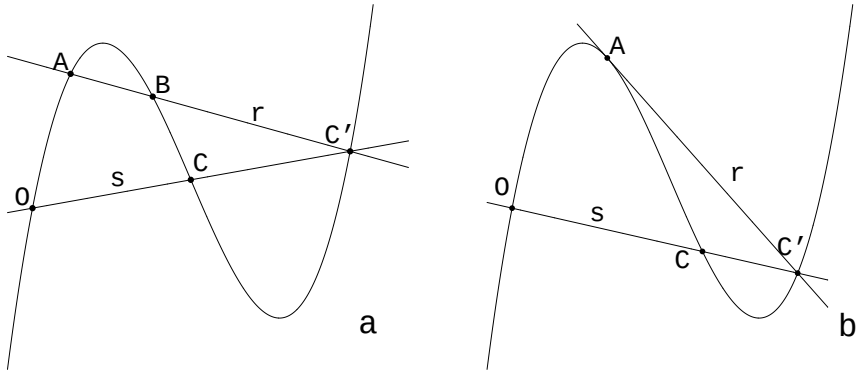

Figura 2.1: La legge di gruppo per punti distinti (a) e coincidenti (b). Nel primo caso la somma è data da $A+B=C$, nel secondo da $A+A=2A=C$.

In tutta la costruzione precedente (figura 2.1) si intende sempre che la retta per due punti è la retta tangente alla curva per uno dei due punti se essi coincidono. Ciò avviene se $A = B$, oppure se $A = R(A, B)$, oppure $B = R(A, B)$. Se accade che $A = B = R(A, B)$, allora il punto è di flesso.

Nella rappresentazione grafica in $\mathbb{A}^2(\mathbb{R})$, se uno dei punti è un punto improprio si traccia la retta con quella direzione e passante per l'altro punto.

Quanto detto sopra permette di garantire che tutti i punti e le rette usati nella costruzione esistano effettivamente, così $+$ come operazione binaria è ben definita, cioè ha senso una scrittura della forma $A + B = C$.

Vale il seguente:

Teorema 2.1.1. *L'operazione $+$ su $\mathcal{C}$ definisce un gruppo abeliano.*

Di questo teorema daremo una dimostrazione completa (si veda il teorema 3.3.7) nel caso che O sia un punto di flesso. Cominciamo a fare qualche osservazione nel caso generale.

Per dimostrare il risultato, è sufficiente verificare le proprietà seguenti:

1. esistenza di un elemento neutro O in $\mathcal{C}$ per l'operazione $+$;

2. esistenza dell' opposto di ogni elemento, cioè $\forall A \in \mathcal{C}$, $\exists(-A) \in \mathcal{C}$ tale che $A + (-A) = O$;

3. proprietà commutativa: $A + B = B + A \quad \forall (A, B) \in \mathcal{C} \times \mathcal{C}$;

4. proprietà associativa: $\forall A, B, C \in \mathcal{C}$ vale $(A + B) + C = A + (B + C)$.

In primo luogo non a caso abbiamo chiamato O il punto scelto sulla cubica, perché in effetti proprio tale punto rappresenta lo zero del gruppo, infatti se A è un punto qualunque della cubica, per calcolare $A+O$ dobbiamo procedere così: determiniamo la retta r per A e O, essa interseca $\mathcal{C}$ in un terzo punto A'. Ora consideriamo la retta per A' e O: il terzo punto di intersezione è il punto cercato, ma tale punto per costruzione è proprio A, così $A + O = A \quad \forall A \in \mathcal{C}$ (si veda la figura 2.2).

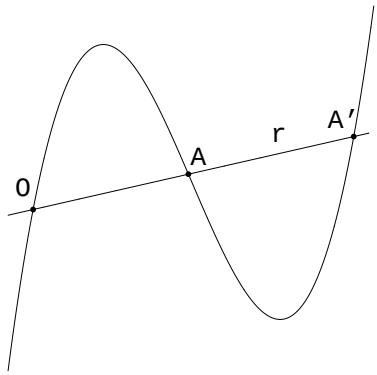

Figura 2.2: Il punto O è l'elemento neutro del gruppo.

Ora scelto un qualunque punto A di $\mathcal{C}$, vogliamo provare che esiste il suo opposto. In primo luogo chiamiamo O' il terzo punto di intersezione con $\mathcal{C}$ della retta r tangente alla cubica in O. Ora definiamo A' come il terzo punto di intersezione di $\mathcal{C}$ con la retta s per A e O'.

Calcoliamo ora $A + A'$: la retta per A e A' è la retta s, che ha O' come terza intersezione con $\mathcal{C}$; ora la retta per O' e O è per costruzione la retta t,

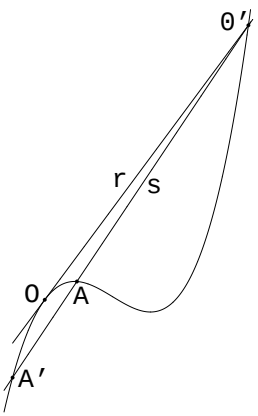

Figura 2.3: Il punto A' è l'opposto di A, cioè $A + A' = O$.

che ha molteplicità 2 di intersezione con $\mathcal{C}$ in O, quindi O è il punto cercato. In simboli:

$$A + A' = R(R(A, A'), O) = R(O', O) = O.$$

Quindi A ammette opposto $-A = A'$.

Mostrare la proprietà commutativa è banale: infatti $R(A, B)$ è il terzo punto di intersezione di $\mathcal{C}$ con la retta r per A e B, quindi tale punto coincide con $R(B, A)$. Così:

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

L'unica proprietà non banale da dimostrare è l'associatività, che si può dimostrare geometricamente solo se tutti i punti usati nelle costruzioni sono distinti. Nelle figure 2.4 a) e b) mostriamo un esempio di associatività. Nella a) prima abbiamo trovato $E = A+B$ e poi il punto $\mathbf{G} = E+C = \mathbf{(A+B)+C}$; nella b), invece, prima abbiamo calcolato $L = B + C$ e poi abbiamo ricavato il punto $\mathbf{N} = A + L = \mathbf{A+(B+C)}$.

Chiedere che valga la proprietà associativa equivale allora a chiedere che i due punti G ed N coincidano per ogni scelta della terna (A, B, C). Per la dimostrazione di quest'ultima proprietà, si rimanda al prossimo capitolo.

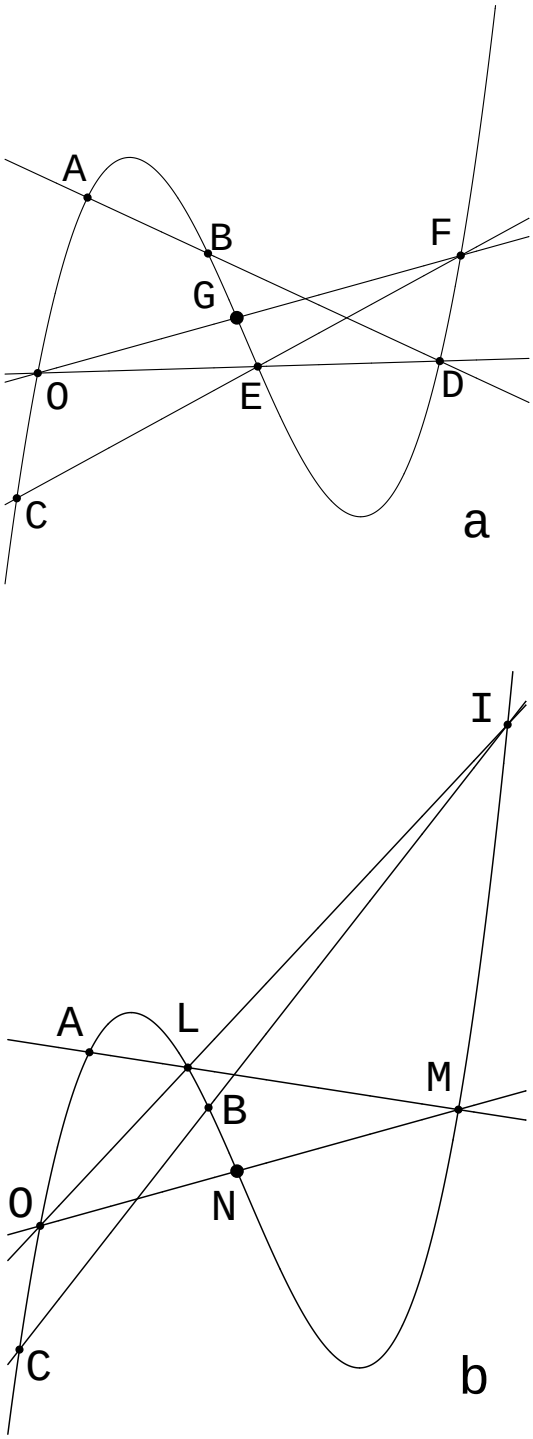

Figura 2.4: Due diversi modi di sommare i tre punti A, B e C.

2.2 Forma normale

La legge di gruppo per le cubiche assume una forma leggermente più semplice se, invece di scegliere come O un punto qualunque, si sceglie tale punto tra i 9 flessi della cubica. In tal caso sarà più semplice calcolare l'opposto di ogni punto.

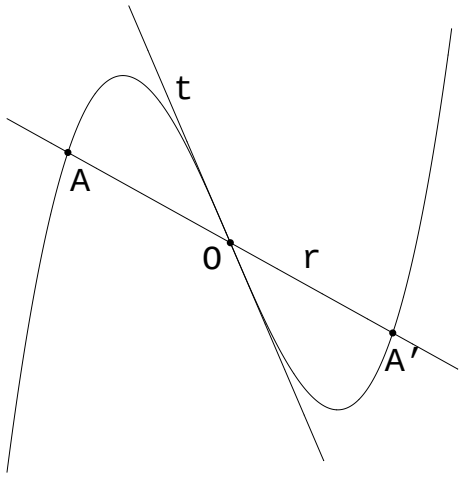

Figura 2.5: L'opposto di A è A' nel caso si scelga O tra i flessi della cubica.

Infatti i punti O e O' definiti nella costruzione precedente in realtà coincidono; infatti la retta tangente a $\mathcal{C}$ in O, essendo O un flesso per la curva, ha molteplicità di intersezione 3, così la terza intersezione cercata coincide ancora con O. Ora l'opposto di A è il punto $A' = -A$ dato come $R(A, O)$, cioè come terzo punto di intersezione della retta per A e O con la cubica (si veda la figura 2.5).

Oltre a questo prima semplificazione, una molto più radicale consiste nel ricordare che lavoriamo su cubiche non singolari e, in base al teorema 1.2.2, ogni cubica non singolare si può portare mediante una proiettività nella forma normale, che in coordinate affini è data da:

$$\mathcal{C} \ : \ y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathbb{C} \setminus \{0, 1\}$$

dove questa equazione descrive tutti i punti della cubica, eccetto l'unico punto improprio $(0, 0, 1)$, che è anche punto di flesso, con tangente inflessionale la retta impropria.

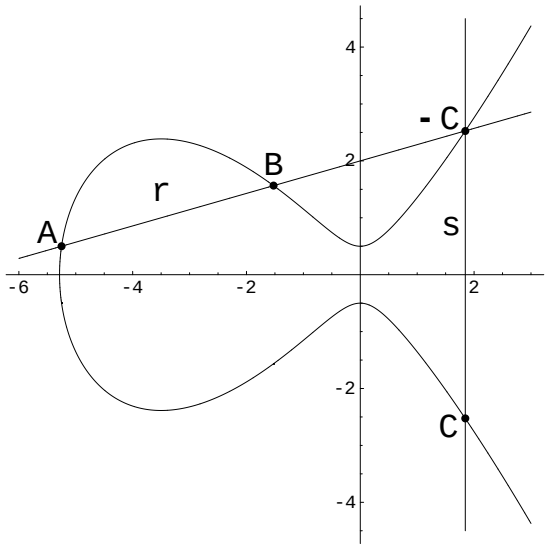

Figura 2.6: La legge di gruppo in forma normale.

Se tra i flessi della cubica scegliamo proprio tale punto come punto O del gruppo, la descrizione geometrica della legge di gruppo si semplifica: $R(A, B)$ si calcola esattamente come al solito, ma $R(A, O) = -A$ per quanto detto sopra, dato che lavoriamo con un flesso come punto O; inoltre dato che ogni retta per O e per un punto proprio del piano affine è una retta della forma $x = k$, se A è un punto proprio, $-A$ non è altro che il simmetrico di A rispetto all'asse x.

Quindi la legge di gruppo può anche essere enunciata in questi termini: dati due punti A e B sulla cubica, si traccia la retta per essi o la tangente alla cubica nel caso essi siano coincidenti; essa interseca la cubica in un terzo punto $-C$; il punto C, simmetrico del precedente rispetto all'asse x, è la somma di A e B (si veda la figura 2.6).

2.3 Descrizione algebrica

Osservazione 3. Molto spesso invece della forma normale vista finora per le cubiche non singolari, se ne usa un'altra ad essa equivalente, cioè la forma:

$$y^2 = x^3 + ax + b. \tag{2.1}$$

Questa forma risulta più facile da utilizzare nelle costruzioni che seguono, perciò ci baseremo d'ora in poi su di essa, dopo aver dimostrato l'equivalenza con la (1.1).

Si osservi che se $\mathcal{C}$ ha equazione (2.1) e si sceglie come O il punto $(0, 0, 1)$, si vede, esattamente come per la cubica di equazione $y^2 = x(x-1)(x-\lambda)$ con $O = (0, 0, 1)$, che $A + B$ è il punto simmetrico rispetto all'asse x di $R(A, B)$, e che se $A = (x, y)$, allora $-A = (x, -y)$.

Proposizione 2.3.1. *Ogni cubica non singolare è proiettivamente equivalente ad una cubica di equazione affine (2.1) con opportune condizioni sui coefficienti a e b in $\mathbb{C}$.*

Dimostrazione. Per il teorema 1.2.2 ogni cubica non singolare può essere portata nella forma $y^2 = x(x-1)(x-\lambda)$ o anche sviluppando i calcoli: $y^2 = x^3 - (\lambda+1)x^2 + \lambda x$ con le opportune condizioni su λ. Ora applichiamo a tale curva l'affinità:

$$(x, y) \mapsto \left(x + \frac{\lambda+1}{3}, y\right).$$

Visto che in y non abbiamo operato alcuna sostituzione effettiva, è sufficiente considerare solo l'immagine del polinomio in x mediante tale sostituzione; otterremo allora:

$$\begin{aligned} &x^3+(\lambda+1)x^2+\tfrac{(\lambda+1)^2}{3}x+\tfrac{(\lambda+1)^3}{27}-(\lambda+1)\left(x^2+\tfrac{2(\lambda+1)x}{3}+\tfrac{(\lambda+1)^2}{9}\right)+\lambda x+\tfrac{\lambda(\lambda+1)}{3} = \\ &= x^3+(\lambda+1)x^2+\tfrac{(\lambda+1)^2}{3}x+\tfrac{(\lambda+1)^3}{27}-(\lambda+1)x^2-\tfrac{2}{3}(\lambda+1)^2x-\tfrac{(\lambda+1)^3}{9}+\lambda x+\tfrac{\lambda(\lambda+1)}{3} = \\ &= x^3 + \left(-\tfrac{1}{3}(\lambda+1)^2+\lambda\right)x + \left(-\tfrac{2}{27}(\lambda+1)^3+\tfrac{\lambda(\lambda+1)}{3}\right). \end{aligned}$$

Quindi definendo gli scalari complessi a e b rispettivamente come coefficiente di primo grado e termine noto dell'espressione precedente, otteniamo l'equazione

$$y^2 = x^3 + ax + b.$$

□

Sia dunque $\mathcal{C} : y^2 = x^3 + ax + b$; si può allora cercare di descrivere la legge di gruppo anche in termini algebrici, note le coordinate di A e B. Mostriamo come procede il calcolo di $A + B$, noti $A = (x_1, y_1)$ e $B = (x_2, y_2)$ e la cubica non singolare $\mathcal{C}$ nella forma precedente. Distinguiamo per comodità due casi: $x_1 \neq x_2$ e $x_1 = x_2$.

Nel primo caso procediamo così: prima determiniamo $R(A, B)$ come terzo punto di intersezione di $\mathcal{C}$ con la retta L per A e B scritta in forma parametrica:

$$L : \begin{cases} x &= x_1 + t(x_2 - x_1) \\ y &= y_1 + t(y_2 - y_1). \end{cases}$$

Mettendo a sistema con l'equazione di $\mathcal{C}$ otteniamo:

$$L \cap \mathcal{C} : \begin{cases} x &= x_1 + t(x_2 - x_1) \\ y &= y_1 + t(y_2 - y_1) \\ y^2 &= x^3 + ax + b. \end{cases}$$

Sostituendo x e y otteniamo:

$$y_1{}^2 + t^2(y_2 - y_1)^2 + 2t(y_2 - y_1)y_1 =$$

$$= x_1{}^3 + 3x_1{}^2 t(x_2 - x_1) + 3x_1 t^2(x_2 - x_1)^2 + t^3(x_2 - x_1)^3 + ax_1 + at(x_2 - x_1) + b.$$

Riscriviamo l'equazione come un'equazione polinomiale in t di grado 3:

$$t^3(x_2 - x_1)^3 + t^2[3x_1(x_2 - x_1)^2 - (y_2 - y_1)^2] +$$

$$+t[3x_1{}^2(x_2 - x_1) + a(x_2 - x_1) - 2y_1(y_2 - y_1)] + [x_1{}^3 + ax_1 + b - y_1^2] = 0 \quad (2.2)$$

dove osserviamo che il termine noto è zero perché il punto $A = (x_1, y_1) \in \mathcal{C}$. Ora osserviamo che necessariamente i valori $t = 0$ e $t = 1$ sono radici del polinomio perché corrispondono rispettivamente ai punti di intersezione A e B. Quindi, se chiamiamo $P(t)$ il polinomio in t scritto sopra, esso si spezza necessariamente nel prodotto di 3 fattori lineari, di cui 2 già noti; la radice γ del terzo fornirà le coordinate del terzo punto di intersezione. Precisamente deve essere:

$$P(t) = (x_2 - x_1)^3 t(t-1)(t-\gamma) = (x_2 - x_1)^3[t^3 - (\gamma+1)t^2 + \gamma t]. \quad (2.3)$$

In particolare, eguagliando il coefficiente del termine di grado 2 nelle espressioni (2.2) e (2.3) trovate per il polinomio $P(t)$, otteniamo che deve essere:

$$-(x_2 - x_1)^3(\gamma + 1) = 3x_1(x_2 - x_1)^2 - (y_2 - y_1)^2$$

cioè

$$\gamma = -\frac{3x_1}{x_2 - x_1} + \frac{(y_2 - y_1)^2}{(x_2 - x_1)^3} - 1.$$

Ora sostituendo nell'equazione parametrica della retta, posto $R(A, B) := (x_3, y_3)$, otteniamo:

$$\begin{cases} x_3 &= x_1 + \gamma(x_2 - x_1) = x_1 - 3x_1 + \frac{(y_2-y_1)^2}{(x_2-x_1)^2} - x_2 + x_1 \\ y_3 &= y_1 + \gamma(y_2 - y_1) = y_1 - \frac{3x_1(y_2-y_1)}{x_2-x_1} + \frac{(y_2-y_1)^3}{(x_2-x_1)^3} - y_2 + y_1. \end{cases}$$

Ora ricordiamo che $A + B = (x_3, -y_3)$, cioè le coordinate (x_4, y_4) del punto somma di A e B sono date da:

$$\begin{cases} x_4 &= \frac{(y_2-y_1)^2}{(x_2-x_1)^2} - (x_1 + x_2) \\ y_4 &= -2y_1 + y_2 + \frac{3x_1(y_2-y_1)}{x_2-x_1} - \frac{(y_2-y_1)^3}{(x_2-x_1)^3}. \end{cases}$$

Chiaramente in questi calcoli abbiamo usato l'ipotesi $x_1 \neq x_2$ in maniera essenziale. Se invece $x_1 = x_2$ si possono presentare due casi: essendo i

punti sulla cubica nella forma (2.1), ad $\tilde{x}$ fissata corrispondono al più due valori distinti $\tilde{y}$ e $\hat{y}$, necessariamente uno opposto dell'altro; così dobbiamo ulteriormente distinguere:

1. se $x_1 = x_2$ e $y_1 = -y_2$, allora i due punti sono uno l'opposto dell'altro, quindi $A + B = O$;

2. se invece $x_1 = x_2$ e $y_1 = y_2$ i due punti A e B coincidono, così stiamo calcolando il punto $A + A = 2A$. Per trovare tale punto bisogna usare la retta tangente a $\mathcal{C}$ e passante per A, di equazione:

$$\left.\frac{\partial F}{\partial x}\right|_{(x_1,y_1)} (x - x_1) + \left.\frac{\partial F}{\partial y}\right|_{(x_1,y_1)} (y - y_1) = 0$$

dove $F(x, y) = y^2 - x^3 - ax - b$. Si ha:

$$\left.\frac{\partial F}{\partial x}\right|_{(x_1,y_1)} = -3{x_1}^2 - a, \quad \left.\frac{\partial F}{\partial y}\right|_{(x_1,y_1)} = 2y_1.$$

Dunque la tangente è della forma $x = k$ se e solo se $y_1 = 0$, quindi siamo nel caso $x_1 = x_2$ e $y_1 = -y_2 = 0$; questa è la situazione precedente, già trattata, così sarà $A + A = 2A = O$, cioè il punto in questione ha periodo 2 nel gruppo della cubica. Osserviamo per inciso che gli unici punti con tale proprietà saranno i punti $(\alpha, 0)$ con α soluzione dell'equazione $x^3 + ax + b = 0$.

Quindi escludendo il caso $y_1 = 0$, possiamo scrivere la retta tangente nella forma:

$$y = \frac{3{x_1}^2 + a}{2y_1}(x - x_1) + y_1.$$

Sostituendo nell'equazione (2.1) di $\mathcal{C}$, otteniamo l'equazione in x di grado 3:

$$\frac{(3{x_1}^2 + a)^2}{4{y_1}^2}(x^2 - 2x_1x + {x_1}^2) + (3{x_1}^2 + a)(x - x_1) + {y_1}^2 = x^3 + ax + b$$

che può essere riscritta nella forma:

$$x^3 - x^2\frac{(3{x_1}^2+a)^2}{4{y_1}^2} + x\left(a + 2x_1\frac{(3{x_1}^2+a)^2}{4{y_1}^2} - 3{x_1}^2 - a\right) +$$
$$+\left(b - {x_1}^2\frac{(3{x_1}^2+a)^2}{4{y_1}^2} - {y_1}^2 + 3{x_1}^3 + ax_1\right) = 0. \qquad (2.4)$$

Ora osserviamo che detto $Q(x)$ il polinomio sopra, esso per costruzione deve ammettere x_1 come radice doppia e una terza radice x_3, che corrisponderà alla prima coordinata del terzo punto di intersezione. Essendo il polinomio in questione monico, allora esso si può anche scrivere sotto la forma:

$$Q(x) = (x-x_1)^2(x-x_3) = (x^2 - 2x_1x + {x_1}^2)(x-x_3) =$$
$$= x^3 - x_3x^2 - 2x_1x^2 + 2x_1x_3x + {x_1}^2x - {x_1}^2x_3 =$$
$$= x^3 - x^2(x_3+2x_1) + x(2x_1x_3 + {x_1}^2) - {x_1}^2x_3. \qquad (2.5)$$

Ora eguagliando nelle due espressioni (2.4) e (2.5) trovate per $Q(x)$ i termini di grado 2, otteniamo:

$$x_3 = \frac{(3{x_1}^2+a)^2}{4{y_1}^2} - 2x_1.$$

Quindi il terzo punto di intersezione ha seconda coordinata y_3:

$$y_3 = \frac{3{x_1}^2+a}{2y_1}(x_3 - x_1) + y_1.$$

Dunque il punto $2A$ avrà coordinate $(x_4, y_4) = (x_3, -y_3)$:

$$\begin{cases} x_4 &= \frac{(3{x_1}^2+a)^2}{4{y_1}^2} - 2x_1 \\ y_4 &= -\frac{3{x_1}^2+a}{2y_1}(x_4 - x_1) - y_1. \end{cases}$$

Osserviamo che si può anche dare la legge di gruppo per le cubiche non singolari direttamente in questa forma, a prescindere dall'interpretazione geometrica, ma in tal caso non si spiega perché si usino certi coefficienti e non altri.

Ovviamente a questo punto si potrebbe tentare di dimostrare la proprietà associativa usando queste formule, ma questo non è un metodo molto efficiente e soprattutto non fornisce nessun significato geometrico alla proprietà dimostrata. Nel prossimo capitolo, invece, daremo una prova della proprietà associativa come conseguenza di un'altra interpretazione geometrica delle cubiche piane non singolari.

Capitolo 3

La funzione $\mathscr{P}$ di Weierstrass

In questo capitolo studieremo le cubiche piane non singolari da un'altra angolazione, le vedremo cioè come tori. Questo mette in luce la loro struttura topologica come superfici reali e pone le basi per capire anche la loro struttura come superfici di Riemann, cioè la loro struttura di varietà complesse, che qui sfioriamo soltanto.

Inoltre, pensare ad una cubica piana non singolare come ad un quoziente di $\mathbb{C}$ permette di reinterpretarne la struttura di gruppo abeliano, e la proprietà associativa, che abbiamo lasciato in sospeso nel capitolo precedente, seguirà automaticamente.

Per i concetti fondamentali delle funzioni complesse di una variabile complessa, si rimanda a [C].

3.1 Reticoli in $\mathbb{C}$ e funzione di Weierstrass

Definizione 3.1. Dati due elementi ω_1 e ω_2 di $\mathbb{C}$ linearmente indipendenti se considerati come vettori di $\mathbb{R}^2$, definiamo il *reticolo* Λ come l'insieme:

$$\Lambda = \Lambda_{\omega_1,\omega_2} := \{z \in \mathbb{C} \mid z = m\omega_1 + n\omega_2, \ \ m, n \in \mathbb{Z}\}.$$

Se non è ambiguo, la dipendenza di Λ da ω_1, ω_2 sarà di norma omessa.

Osservazione 4. Il reticolo Λ è un sottogruppo additivo di $\mathbb{C}$, isomorfo a $\mathbb{Z} \times \mathbb{Z}$.

Osserviamo inoltre che uno stesso reticolo Λ può essere associato a coppie di vettori diverse, ad esempio $\Lambda_{\omega_1,\omega_2} = \Lambda_{-\omega_2,\omega_1}$, e così via.

Definizione 3.2. Dati due vettori ω_1 e ω_2 di $\mathbb{R}^2$, linearmente indipendenti, si dice *parallelogramma fondamentale* generato da tali vettori il sottoinsieme di $\mathbb{R}^2$:

$$\mathcal{P}_{\omega_1,\omega_2} = \mathcal{P}_\Lambda = \{\lambda\omega_1 + \eta\omega_2 \mid \lambda, \eta \in [0,1]\}.$$

Teorema 3.1.1. *(M-test di Weierstrass) Sia $\{F_n : W \to \mathbb{C}\}_n$ una successione di funzioni olomorfe su un dominio aperto W di $\mathbb{C}$. Supponiamo che esista una successione di numeri reali M_n tali che la serie*

$$\sum_n M_n$$

converga e che

$$|F_n(z)| \leq M_n \quad \forall z \in W.$$

Allora la serie

$$\sum_n F_n(z)$$

converge assolutamente uniformemente su W ad una funzione olomorfa $F(z)$ tale che

$$F'(z) = \sum_n F'(z).$$

Una dimostrazione di questo risultato, si può trovare in [K], teorema 5.8.

Definizione-Proposizione 3.3. *Sia Λ un reticolo; poniamo:*

$$\mathscr{P}_\Lambda(z) = \mathscr{P}(z) := z^{-2} + \sum_{\omega \in \Lambda \smallsetminus \{0\}} ((z-\omega)^{-2} - \omega^{-2}).$$

Si ha che $\mathscr{P}$ è una funzione meromorfa su $\mathbb{C}$, detta $\mathscr{P}$ di Weierstrass*, e la sua derivata è:*

$$\mathscr{P}'(z) = \sum_{\omega \in \Lambda} -2(z-\omega)^{-3}.$$

Chiaramente a reticoli diversi corrisponderanno funzioni di Weiertrass diverse; come sopra, se non è ambiguo ometteremo la dipendenza di $\mathscr{P}$ da Λ, oltre che di Λ da ω_1, ω_2.

Dimostrazione. Osserviamo che la somma di una funzione olomorfa con una funzione meromorfa (sull'intersezione dei rispettivi domini) è ancora una funzione meromorfa con poli negli stessi punti della precedente. Lo stesso vale per somme di 2 o più funzioni meromorfe.

Di conseguenza nel nostro caso è sufficiente dimostrare che $\mathscr{P}$ è somma di una funzione olomorfa su $\mathbb{C}$ e di un numero *finito* di funzioni meromorfe su $\mathbb{C}$.

Per fare ciò basta mostrare che questo vale sviluppando la parte olomorfa attorno a 0 per ogni raggio $R > 0$. Infatti se vale tale risultato, fissato un punto qualunque $z_o \in \mathbb{C}$, posto $R := |z_0|$, si ha che il disco di centro z_0 e raggio 1 è contenuto nel disco di centro l'origine e raggio $R+1$, su cui la funzione sarà meromorfa.

Vogliamo allora scrivere, fissato $R > 0$:

$$\mathscr{P}(z) = \sum_{\omega \in \Lambda \setminus \Lambda_R} ((z-\omega)^{-2} - \omega^{-2}) + \sum_{\omega \in \Lambda_R} ((z-\omega)^{-2} - \omega^{-2}) \tag{3.1}$$

dove Λ_R sia un sottoinsieme *finito* di Λ contente l'origine, e la prima delle due sommatorie sia assolutamente uniformemente convergente per $|z| \leq R$.

Per farlo abbiamo bisogno del seguente risultato (si veda sotto il lemma 3.1.2): fissati ω_1, ω_2 come sopra, esiste $\delta > 0$ tale che:

$$|x\omega_1 + y\omega_2| \geq \delta\sqrt{x^2+y^2} \quad \forall (x,y) \in \mathbb{R}^2.$$

Se vale questo, allora poniamo:

$$\Lambda_R := \{\omega \in \Lambda \quad \text{tali che} \quad |\omega| < 2R\}.$$

Di conseguenza, se $\omega = m\omega_1 + n\omega_2$ appartiene a Λ_R, allora:

$$2R > |\omega| = |m\omega_1 + n\omega_2| \geq \delta\sqrt{m^2+n^2}.$$

Dunque elevando a quadrato:

$$m^2 + n^2 < \frac{4R^2}{\delta^2},$$

quindi l'insieme Λ_R è necessariamente finito, così la seconda sommatoria nella (3.1) è la somma di un numero finito di funzioni meromorfe, ognuna con un solo polo di molteplicità 2 in un punto di Λ_R.

Allora tutto quello che si tratta di dimostrare è che la prima delle due sommatorie è assolutamente uniformemente convergente sul disco di centro l'origine e raggio R: osserviamo ora che se $|z| \leq R$, allora $|z| \leq \frac{1}{2}|\omega|$ per ogni ω in $\Lambda \setminus \Lambda_R$. Ora analizziamo il generico termine della prima sommatoria in (3.1):

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\left(\frac{1}{z-\omega} - \frac{1}{\omega}\right)\left(\frac{1}{z-\omega} + \frac{1}{\omega}\right)\right| =$$

$$= \left|\left(\frac{\omega - z + \omega}{\omega(z-\omega)}\right)\left(\frac{\omega + z - \omega}{\omega(z-\omega)}\right)\right| = \frac{|z||2\omega - z|}{|\omega|^2(|z-\omega|)^2} \leq \frac{R(|2\omega| + |z|)}{|\omega|^2(|\omega| - |z|)^2} \leq$$

$$\leq \frac{\frac{5}{2}R|\omega|}{|\omega|^2(|\omega| - \frac{1}{2}|\omega|)^2} = \frac{\frac{5}{2}R|\omega|}{\frac{1}{4}|\omega|^4} = \frac{10R}{|\omega|^3} \leq \frac{10R}{\delta^3(m^2+n^2)^{3/2}}$$

dove nell'ultimo passaggio abbiamo nuovamente usato il lemma 3.1.2. Ora

$$\sum_{\omega \in \Lambda \setminus \Lambda_R} |(z-\omega)^{-2} - \omega^{-2}| \leq \sum_{(m,n)\neq(0,0)} \frac{10R}{\delta^3(m^2+n^2)^{3/2}} =$$

$$= \frac{10R}{\delta^3} \sum_{(m,n)\neq(0,0)} (m^2+n^2)^{-3/2} \leq \frac{10R}{\delta^3} \sum_{k\geq 1} \sum_{max\{|m|,|n|\}=k} (m^2+n^2)^{-3/2} =$$

$$= \frac{10R}{\delta^3} \sum_{k\geq 1} (2k^2)^{-3/2} = \frac{10R}{\delta^3} \sum_{k\geq 1} \frac{1}{2\sqrt{2}k^3} < \infty.$$

Dunque la prima sommatoria della (3.1) soddisfa le condizioni del teorema 3.1.1, quindi abbiamo dimostrato che $\mathscr{P}$ è meromorfa sul piano complesso, in particolare è olomorfa fuori dai punti del reticolo Λ. Sempre grazie al teorema 3.1.1, si può derivare termine a termine intorno ad ogni punto $z \in \mathbb{C} \setminus \Lambda$; derivando otteniamo:

$$\mathscr{P}'(z) = -2z^{-3} + \sum_{\omega \in \Lambda \setminus \{0\}} -2(z-\omega)^{-3} = \sum_{\omega \in \Lambda} -2(z-\omega)^{-3}.$$

□

Per concludere dobbiamo solo mostrare il seguente:

Lemma 3.1.2. *Per ogni coppia di numeri complessi (ω_1, ω_2) linearmente indipendenti come vettori di $\mathbb{R}^2$, esiste $\delta > 0$ tale che:*

$$|x\omega_1 + y\omega_2| \geq \delta\sqrt{x^2+y^2} \quad \forall (x,y) \in \mathbb{R}^2.$$

Dimostrazione. Per provare questo risultato è sufficiente considerare la funzione:

$$F : [0, 2\pi] \to \mathbb{R}$$

$$F(\theta) := |(\cos\theta)\omega_1 + (\sin\theta)\omega_2|.$$

Ora $F(\theta) > 0 \quad \forall \theta \in [0, 2\pi]$, infatti i due vettori ω_1 e ω_2 sono per ipotesi linearmente indipendenti, quindi la loro unica combinazione linerare nulla è quella a coefficienti nulli, ma $(\cos\theta, \sin\theta) \neq (0,0)$ per ogni valore di θ.

Inoltre la funzione F è chiaramente continua e definita su un compatto, quindi assume massimo e minimo. In particolare sia:

$$\delta := \min_{\theta \in [0,2\pi]} F = F(\bar{\theta}) > 0, \quad \bar{\theta} \in [0, 2\pi].$$

Ora data una qualunque coppia $(x, y) \in \mathbb{R}^2$, vale:

$$(x, y) = \sqrt{x^2+y^2}(\cos\theta, \sin\theta),$$

dove $\theta \in [0, 2\pi]$ sia argomento di (x, y); dunque:

$$|x\omega_1 + y\omega_2| = \sqrt{x^2+y^2}|(\cos\theta)\omega_1 + (\sin\theta)\omega_2| \geq \delta\sqrt{x^2+y^2}.$$

□

Elenchiamo ora una serie di risultati relativi alla funzione $\mathscr{P}$ di Weierstrass:

Proposizione 3.1.3. *La funzione $\mathscr{P}$ di Weierstrass gode delle seguenti proprietà:*
i) $\mathscr{P}(-z) = \mathscr{P}(z)$ per ogni z in $\mathbb{C} \setminus \Lambda$;
ii) $\mathscr{P}(z) = \mathscr{P}(z+\xi)$ per ogni z in $\mathbb{C} \setminus \Lambda$ e per ogni ξ in Λ;
iii) la funzione $\mathscr{P} : \mathbb{C} \setminus \Lambda \to \mathbb{C}$ è suriettiva. Inoltre $\mathscr{P}(z) = \mathscr{P}(v)$ se e solo se $z \in \Lambda + v$ oppure $z \in \Lambda - v$, dove con $\Lambda + v$ indichiamo il laterale di Λ individuato da v.

Per la dimostrazione di questi risultati si veda [K], lemma 5.13 e proposizione 5.18.

Definizione 3.4. Una funzione F tale che

$$F(z+\xi) = F(z) \quad \forall z \in \mathbb{C}, \quad \forall \xi \in \Lambda$$

dove $\Lambda = \Lambda_{\omega_1,\omega_2}$ sia un reticolo di $\mathbb{C}$, si dice *doppiamente periodica* con reticolo dei periodi Λ o con periodi ω_1, ω_2.

Una funzione F su $\mathbb{C}$ è doppiamente periodica di periodi ω_1 e ω_2 se e solo se:

$$F(z+\omega_1) = F(z) = F(z+\omega_2) \quad \forall z \in \mathbb{C}.$$

Osservazione 5. Per il secondo punto della proposizione precedente, la funzione $\mathscr{P}$ è una funzione meromorfa su $\mathbb{C}$ doppiamente periodica con reticolo dei periodi Λ.

Osserviamo inoltre che per definire una funzione F doppiamente periodica su $\mathbb{C}$ e non costante, è necessario che essa abbia poli, come la funzione di Weierstrass definita sopra. Infatti, una funzione olomorfa su $\mathbb{C}$ e doppiamente periodica è limitata, perché i valori che assume su tutto il piano complesso sono esattamente quelli che assume sul parallelogramma fondamentale $\mathcal{P}_\Lambda$, dominio compatto. In tal caso il teorema di Liouville ([C], teorema III.1.2.) assicura che la funzione sia costante.

Definizione 3.5. Dato un reticolo Λ, possiamo definire la cubica proiettiva:

$$\mathcal{C}_\Lambda \ : \ Q_\Lambda(x_0, x_1, x_2) = 0,$$

dove

$$Q_\Lambda(x_0, x_1, x_2) := x_0 {x_2}^2 - 4{x_1}^3 + g_2 {x_0}^2 x_1 + g_3 {x_0}^3$$

con:

$$g_2 = g_2(\Lambda) := 60 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-4}, \qquad g_3 = g_3(\Lambda) := 140 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-6}.$$

Quello che vogliamo dimostrare è che la cubica definita sopra è non singolare. Per fare ciò abbiamo bisogno del seguente:

Lemma 3.1.4. *La funzione $\mathscr{P}$ di Weierstrass soddisfa la seguente relazione:*

$$\mathscr{P}'(z)^2 = 4\mathscr{P}^3(z) - g_2\mathscr{P}(z) - g_3,$$

dove g_2 e g_3 sono definiti come sopra.

Dimostrazione. La funzione

$$\mathscr{P}(z) - z^{-2} = \sum_{\omega \in \Lambda \setminus \{0\}} ((z-\omega)^{-2} - \omega^{-2})$$

è olomorfa attorno all'origine, in cui vale 0. Inoltre è una funzione pari della z, quindi sviluppando in serie di Taylor intorno all'origine si ottengono solo le potenze pari della z. Quindi attorno a 0 possiamo scrivere:

$$\mathscr{P}(z) = z^{-2} + \lambda z^2 + \mu z^4 + z^6 H(z) \tag{3.2}$$

dove λ e μ sono numeri complessi e H è una funzione olomorfa attorno all'origine. Derivando allora questa espressione otteniamo:

$$\mathscr{P}'(z) = -2z^{-3} + 2\lambda z + 4\mu z^3 + 6z^5 H(z) + z^6 H'(z). \tag{3.3}$$

Definiamo ora la funzione K:

$$K(z) := \mathscr{P}'(z)^2 - 4\mathscr{P}^3(z) + g_2\mathscr{P}(z) + g_3$$

dove $g_2 := 20\lambda$ e $g_3 := 28\mu$.

Ora sostituendo le espressioni (3.2) e (3.3), e svolgendo i calcoli, si può mostrare che K è una funzione olomorfa intorno all'origine e in tale punto vale 0. Essendo K una funzione ottenuta come somma di funzioni meromorfe, è essa stessa meromorfa con poli al più nei punti del reticolo Λ, ed è certamente olomorfa fuori da essi. Inoltre essendo $\mathscr{P}$ doppiamente periodica di periodo Λ, anche la sua derivata prima lo è, quindi vale:

$$\mathscr{P}(z+\xi) = \mathscr{P}(z), \quad \mathscr{P}'(z+\xi) = \mathscr{P}'(z) \quad \forall z \in \mathbb{C}, \quad \forall \xi \in \Lambda.$$

Quindi K stessa è doppiamente periodica di periodo Λ e intorno ad ogni punto di Λ è olomorfa, perché lo è attorno all'origine.

Dunque K è olomorfa su $\mathbb{C}$ e limitata sull'intero piano complesso perché doppiamente periodica. Grazie al teorema di Liouville concludiamo allora che K è una funzione costante, dunque:

$$K(z) = K(0) = 0 \quad \forall z \in \mathbb{C}.$$

Questo basta per dimostrare il lemma. Per ottenere i valori espliciti di g_2 e g_3 osserviamo che per costruzione gli scalari 2λ e $24\mu = 4!\mu$ sono rispettivamente la derivata seconda e la derivata quarta (valutate in 0) della

funzione $\sum_{\omega\in\Lambda\setminus\{0\}}((z-\omega)^{-2}-\omega^{-2})$, che, come già visto, può essere derivata in tale punto termine a termine, quindi:

$$2\lambda = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{d^2((z-\omega)^{-2}-\omega^{-2})}{dz^2}\Big|_0 = \sum_{\omega\in\Lambda\setminus\{0\}} (6(z-\omega)^{-4})\big|_0 = \sum_{\omega\in\Lambda\setminus\{0\}} 6\omega^{-4}.$$

Analogamente si ottiene che

$$24\mu = 120 \sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-6}.$$

Sostituendo nelle espressioni di $g_2 = 20\lambda$ e $g_3 = 28\mu$ otteniamo le formule esplicite per tali coefficienti date nella definizione 3.5. □

Teorema 3.1.5. *Per ogni reticolo Λ, la cubica $\mathcal{C}_\Lambda$ è non singolare.*

Dimostrazione. Poniamo:

$$\alpha := \mathscr{P}(\frac{1}{2}\omega_1), \qquad \beta := \mathscr{P}(\frac{1}{2}\omega_1), \qquad \gamma := \mathscr{P}(\frac{1}{2}(\omega_1+\omega_2)).$$

Osserviamo in primo luogo che:

$$\frac{1}{2}\omega_1 \notin \Lambda \pm \frac{1}{2}\omega_2, \quad \frac{1}{2}\omega_1 \notin \Lambda \pm \frac{1}{2}(\omega_1+\omega_2) \quad \text{e} \quad \frac{1}{2}\omega_2 \notin \Lambda \pm \frac{1}{2}(\omega_1+\omega_2)$$

così grazie alla proposizione 3.1.3 possiamo affermare che i tre valori α, β, γ sono tutti distinti.

La $\mathscr{P}'$ è una funzione dispari e periodica di periodi ω_1 e ω_2, dunque otteniamo che:

$$\mathscr{P}'(\frac{1}{2}\omega_1) = \mathscr{P}'(\frac{1}{2}\omega_1 - \omega_1) = \mathscr{P}'(-\frac{1}{2}\omega_1) = -\mathscr{P}'(\frac{1}{2}\omega_1).$$

Quindi:

$$\mathscr{P}'(\frac{1}{2}\omega_1) = 0.$$

Di conseguenza, sfruttando il lemma 3.1.4, otteniamo:

$$0 = \mathscr{P}'(\frac{1}{2}\omega_1)^2 = 4\mathscr{P}(\frac{1}{2}\omega_1)^3 - g_2\mathscr{P}(\frac{1}{2}\omega_1) - g_3 = \alpha^3 - g_2\alpha - g_3.$$

In modo analogo, si dimostra che $\beta^3 - g_2\beta - g_3 = 0$ e che $\gamma^3 - g_2\gamma - g_3 = 0$.

Abbiamo quindi provato che α, β, γ sono i tre zeri *distinti* della funzione polinomiale in u: $4u^3 - g_2u - g_3$. Equivalentemente, possiamo scrivere:

$$4{x_1}^3 - g_2{x_o}^2x_1 - g_3{x_0}^3 = 4(x_1 - \alpha x_0)(x_1 - \beta x_0)(x_1 - \gamma x_0).$$

Quindi:

$$\mathcal{C}_\Lambda \ : \ x_0{x_2}^2 - 4(x_1 - \alpha x_0)(x_1 - \beta x_0)(x_1 - \gamma x_0) = 0,$$

o anche, deomogenizzando rispetto ad x_0,

$$\mathcal{C}_\Lambda \ : \ y^2 = 4(x - \alpha)(x - \beta)(x - \gamma).$$

Ora come nel lemma 1.2.3 del capitolo 1, essendo le tre radici α, β, γ distinte, la curva $\mathcal{C}_\Lambda$ è non singolare. □

3.2 Tori e cubiche ellittiche

Abbiamo già osservato sopra che ogni reticolo Λ di $\mathbb{C}$ costituisce un sottogruppo del gruppo abeliano $(\mathbb{C}, +)$; quindi possiamo considerare il gruppo quoziente:

$$\mathbb{C}/\Lambda := \{\Lambda + z \mid z \in \mathbb{C}\}$$

dove $\Lambda + z = \Lambda + w$ se e solo se $z - w \in \Lambda$.

Il gruppo quoziente ammette una struttura naturale di spazio topologico, cioè quella data dalla topologia quoziente; se consideriamo la mappa di proiezione sul quoziente: $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$, un sottoinsieme L di $\mathbb{C}/\Lambda$ è aperto se e solo se la sua controimmagine $\pi^{-1}(L)$ è aperta in $\mathbb{C}$ (su $\mathbb{C}$ consideriamo sempre la topologia euclidea).

Da un punto di vista topologico, lo spazio così costruito è un toro $T^2 = S^1 \times S^1$. Infatti, quozientare $\mathbb{C}$, cioè $\mathbb{R}^2$, con Λ equivale topologicamente ad identificare i lati opposti del parallelogramma fondamentale $\mathcal{P}_{\omega_1,\omega_2}$ secondo le indicazioni della figura 3.1.

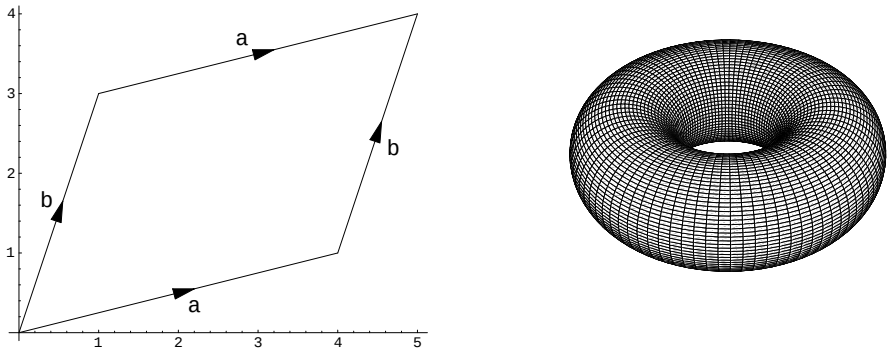

Figura 3.1: Come incollare lati opposti del parallelogramma fondamentale per ottenere un toro.

Da questo punto di vista non esiste nessuna differenza tra scelte di reticoli diversi con cui quozientare: in tutti i casi lo spazio in questione è omeomorfo al toro. D'altra parte, tale oggetto si può anche considerare come una varietà reale (di dimensione 2) o come varietà complessa (di dimensione 1); in tal caso a seconda della scelta del reticolo Λ si ottengono sul toro strutture differenziali diverse.

Quanto detto finora permette di dimostrare il seguente:

Teorema 3.2.1. *Dato un reticolo Λ, il supporto della cubica non singolare $\mathcal{C}_\Lambda$ (con la topologia indotta dalla topologia naturale di $\mathbb{P}^2(\mathbb{C})$) e il toro $\mathbb{C}/\Lambda$ sono omeomorfi.*

Un omemorfismo è dato mediante la mappa $u: \ \mathbb{C}/\Lambda \to \mathcal{C}_\Lambda$,

$$u(\Lambda + z) := \begin{cases} (1, \mathscr{P}(z), \mathscr{P}'(z)) & \text{se } z \notin \Lambda \\ (0, 0, 1) & \text{se } z \in \Lambda. \end{cases}$$

Dimostrazione. Prima di tutto mostriamo che l'applicazione è ben definita sullo spazio quoziente: siano $z, w \in \mathbb{C} \setminus \Lambda$ tali che $\Lambda + z = \Lambda + w$, quindi

$z - w \in \Lambda$, cioè $z = w + m\omega_1 + n\omega_2$ per un'opportuna coppia di interi (m, n). Allora ricordando che $\mathscr{P}$ è doppiamente periodica di periodi ω_1 e ω_2, si ha:

$$\mathscr{P}(z) = \mathscr{P}(w + m\omega_1 + n\omega_2) = \mathscr{P}(w).$$

e analogamente per la derivata prima di $\mathscr{P}$, anch'essa periodica. Dunque:

$$u(\Lambda + z) = (1, \mathscr{P}(z), \mathscr{P}'(z)) = (1, \mathscr{P}(w), \mathscr{P}'(w)) = u(\Lambda + w).$$

Inoltre, la u così definita ha immagine contenuta in $\mathcal{C}_\Lambda$ per il lemma 3.1.4.

Per mostrare che u è un omeomorfismo, dobbiamo provare che è un'applicazione iniettiva e suriettiva e che u e u^{-1} sono funzioni continue. Cominciamo mostrando l'iniettività.

Siano $z, w \in \mathbb{C} \setminus \Lambda$ tali che $u(\Lambda + z) = u(\Lambda + w)$, vogliamo provare che $\Lambda + z = \Lambda + w$, cioè che $z \in \Lambda + w$. Per definizione di u, allora:

$$\begin{cases} \mathscr{P}(z) &= \mathscr{P}(w) \\ \mathscr{P}'(z) &= \mathscr{P}'(w). \end{cases}$$

Per la proposizione 3.1.3, si ha $\Lambda + z = \Lambda \pm w$.

Supponiamo ora che sia $z \in \Lambda - w$, cioè che sia $z = -w + m\omega_1 + n\omega_2$, con m, n interi opportuni. Allora ricordando che $\mathscr{P}'$ è periodica di periodi ω_1 e ω_2, e dispari perché derivata di una funzione pari, otteniamo:

$$\mathscr{P}'(z) = \mathscr{P}'(-w + m\omega_1 + n\omega_2) = \mathscr{P}'(-w) = -\mathscr{P}'(w).$$

Combinando questo con il risultato $\mathscr{P}'(z) = \mathscr{P}'(w)$ già trovato, concludiamo che

$$\mathscr{P}'(z) = \mathscr{P}'(w) = 0.$$

Ricordiamo ora che nella dimostrazione del teorema 3.1.5 avevamo provato che se $\mathscr{P}'(w) = 0$, allora necessariamente $\mathscr{P}(w)$ è uguale ad uno (ed uno solo) tra

$$\alpha = \mathscr{P}(\frac{1}{2}\omega_1), \quad \beta = \mathscr{P}(\frac{1}{2}\omega_2), \quad \gamma = \mathscr{P}(\frac{1}{2}(\omega_1 + \omega_2)).$$

Quindi grazie al punto iii) della proposizione 3.1.3, w appartiene ad uno ed uno solo dei seguenti laterali:

$$\Lambda \pm \frac{1}{2}\omega_1, \quad \Lambda \pm \frac{1}{2}\omega_2, \quad \Lambda \pm \frac{1}{2}(\omega_1 + \omega_2).$$

Equivalentemente, esistono $\bar{m}, \bar{n}$ interi tali che:

$$\omega = (\frac{1}{2}\bar{m} + \hat{m})\omega_1 + (\frac{1}{2}\bar{n} + \hat{n})\omega_2.$$

Così

$$\omega + \omega = (\bar{m} + 2\hat{m})\omega_1 + (\bar{n} + 2\hat{n})\omega_2 \in \Lambda,$$

dunque

$$\omega - (-\omega) = \omega + \omega \in \Lambda \quad \Rightarrow \quad \Lambda + \omega = \Lambda - \omega.$$

Quindi $\Lambda + z = \Lambda - w = \Lambda + w$, così l'iniettività è provata.

Per mostrare la suriettività della mappa u, scegliamo un generico punto (a, b, c) nel supporto della cubica $\mathcal{C}_\Lambda$ e distinguiamo i casi $a = 0$ e $a \neq 0$.

Nel primo caso ricordando che l'equazione della cubica è:

$$x_0 {x_2}^2 - 4{x_1}^3 + g_2 {x_0}^2 x_1 + g_3 {x_0}^3 = 0$$

vediamo che l'unico punto (a, b, c) di $\mathcal{C}_\Lambda$ con $a = 0$ è il flesso $(0, 0, 1)$, immagine di Λ.

Se invece $a \neq 0$, possiamo assumere che il punto abbia la forma $(1, b, c)$; ora sappiamo che $\mathscr{P}$ è suriettiva per la proposizione 3.1.3, quindi esiste $z \in \mathbb{C}$ tale che $\mathscr{P}(z) = \mathscr{P}(-z) = b$. Ora tramite il lemma 3.1.4 e avendo assunto che $(1, b, c)$ sia un punto della cubica $\mathcal{C}_\Lambda$, otteniamo:

$$\mathscr{P}'(z)^2 = 4\mathscr{P}(z)^3 - g_2\mathscr{P}(z) - g_3 = 4b^3 - g_2 b - g_3 = c^2,$$

dunque $\mathscr{P}'(z) = \pm c$.

Se $\mathscr{P}'(z) = c$, allora $u(\Lambda + z) = (1, b, c)$, altrimenti ricordando che $\mathscr{P}$ è una funzione pari e $\mathscr{P}'$ è dispari, otteniamo:

$$u(\Lambda - z) = (1, \mathscr{P}(-z), \mathscr{P}'(-z)) = (1, \mathscr{P}(z), -\mathscr{P}'(z)) = (1, b, c).$$

Questo basta per provare la suriettività della mappa.

Ora la funzione u è chiaramente continua su tutti i punti di $\mathbb{C}/\Lambda$ con al più l'eccezione del punto Λ, perché le sue componenti sono olomorfe su $\mathbb{C} \setminus \Lambda$, e quindi continue.

L'unico punto in cui bisogna verificare la continuità è allora Λ; sia allora $\Lambda + z$ vicino a tale punto: questo nella topologia sul toro equivale a chiedere che un qualunque rappresentante di $\Lambda + z$ sia vicino ad un opportuno punto del reticolo Λ. Dal momento che abbiamo già dimostrato che u è ben definita su $\mathbb{C}/\Lambda$, non è restrittivo chiedere semplicemente che z sia in un intorno di 0. Ora le funzioni $\mathscr{P}$ e $\mathscr{P}'$ hanno in 0 un polo di molteplicità 2 e 3 rispettivamente, quindi per z vicino a 0, $z \neq 0$ possiamo scrivere:

$$\mathscr{P}(z) = \frac{H(z)}{z^2}, \quad \mathscr{P}'(z) = \frac{K(z)}{z^3},$$

con H, K olomorfe intorno a 0, $H(0), K(0) \neq 0$.

Per z vicino a 0, $z \neq 0$, possiamo scrivere allora:

$$u(\Lambda + z) = \left(1, \frac{H(z)}{z^2}, \frac{K(z)}{z^3}\right) = (z^3, zH(z), K(z)).$$

Così:

$$\lim_{z \to 0} u(\Lambda + z) = (0, 0, K(z)) = (0, 0, 1) = u(\Lambda + 0).$$

Quindi u è continua in ogni punto del toro $\mathbb{C}/\Lambda$.

Ora $\mathbb{C}/\Lambda$ è compatto perché immagine mediante l'applicazione continua π (proiezione sul quoziente) del parallelogramma fondamentale $\mathcal{P}_\Lambda$, dominio compatto. Invece $\mathcal{C}_\Lambda$ è un sottoinsieme del piano proiettivo $\mathbb{P}^2(\mathbb{C})$, spazio topologico di Hausdorff, e quindi è esso stesso di Hausdorff.

Dunque u è una funzione continua e biettiva con dominio compatto e codominio di Hausdorff; per un noto lemma (si veda per esempio [S2], capitolo 3, proposizione 9.10), u è un omeomorfismo. □

Si possono inoltre considerare i due spazi topologici descritti sopra come varietà complesse di dimensione 1, dette anche superfici di Riemann. In tal caso si può dimostrare che l'applicazione u, definita tra tali spazi, è una biolomorfia. Per una trattazione completa di questi risultati, si veda ad esempio [K], capitolo 5.2.

Si osservi inoltre che il teorema precedente fornisce una parametrizzazione *non algebrica* della cubica ellittica $\mathcal{C}_\Lambda$, cioè:

$$\mathcal{C}_\Lambda = \{(1, \mathscr{P}(z), \mathscr{P}'(z)) \mid z \in \mathbb{C} \setminus \Lambda\} \cup \{(0,0,1)\}.$$

3.3 La legge di gruppo sul toro

Come ben noto, $(\mathbb{C}, +)$ è un gruppo abeliano. L'operazione $+$ induce mediante la proiezione π un'operazione, denotata ancora con $+$, sul gruppo quoziente $T^2 = \mathbb{C}/\Lambda$ così:

$$\begin{array}{rccc} + : & T^2 \times T^2 & \to & T^2 \\ & (\Lambda + A, \Lambda + B) & \to & \Lambda + A + B; \end{array}$$

In tal modo $(T^2, +)$ risulta essere un gruppo abeliano.

Abbiamo appena definito un omeomorfismo u tra il toro $\mathbb{C}/\Lambda$ e la cubica $\mathcal{C}_\Lambda$, per cui possiamo indurre sulla cubica un'operazione, che indicheremo con $+_{toro}$, così definita:

$$\begin{array}{rccc} +_{toro} : & \mathcal{C}_\Lambda \times \mathcal{C}_\Lambda & \to & \mathcal{C}_\Lambda \\ & (P, Q) & \to & u(u^{-1}(P) + u^{-1}(Q)) \end{array}$$

Essendo u una biezione, $(\mathcal{C}_\Lambda, +_{toro})$ è un gruppo, isomorfo tramite u al gruppo $(\mathbb{C}/\Lambda, +)$. In altre parole, $+_{toro}$ agisce così:

$$(1, \mathscr{P}(z), \mathscr{P}'(z)) +_{toro} (1, \mathscr{P}(w), \mathscr{P}'(w)) =$$

$$= \begin{cases} (1, \mathscr{P}(z+w), \mathscr{P}'(z+w)) & \text{se } z+w \notin \Lambda \\ (0,0,1) & \text{se } z+w \in \Lambda. \end{cases}$$

Osserviamo che l'elemento neutro per $+_{toro}$ è il flesso $O = (0,0,1)$ e che se $A \in \mathcal{C}_\Lambda$, l'opposto di A è $u(-u^{-1}(A))$.

Di conseguenza su una cubica della forma $\mathcal{C}_\Lambda$ sono definite due operazioni binarie: $+$ e $+_{toro}$. Finora abbiamo dimostrato che la seconda è un'operazione di gruppo, mentre per la prima abbiamo dimostrato nel capitolo 2 tutti gli assiomi tranne l'associatività. La proprietà in questione deriva dal seguente teorema:

Teorema 3.3.1. *Su una cubica della forma $\mathcal{C}_\Lambda$ l'operazione $+$ ottenuta scegliendo $O = (0,0,1)$ e l'operazione $+_{toro}$ appena definita coincidono, equivalentemente: $(\mathcal{C}_\Lambda, +) = (\mathcal{C}_\Lambda, +_{toro})$.*

Dimostrazione. Essendo la cubica $\mathcal{C}_\Lambda$ in forma normale con la scelta di $O = (0,0,1)$ su di essa la legge di gruppo è quella descritta nella sezione 2.2 e illustrata nella figura 2.6. Osserviamo allora che gli elementi neutri dei due gruppi coincidono entrambi con il flesso $(0,0,1)$; tale punto è anche l'unico punto improprio della cubica rispetto alla mappa j_0.

Vogliamo in primo luogo determinare esplicitamente l'opposto di ogni elemento (diverso dall'elemento neutro) rispetto a $+_{toro}$.

Possiamo limitarci a considerare punti della forma $(1, b, c)$, in quanto l'unico punto che non ha questa forma è il punto improprio, che è anche l'elemento neutro del gruppo, quindi con opposto se stesso. Sia allora $A = (1, \mathscr{P}(z), \mathscr{P}'(z))$ con $z \in \mathbb{C} \setminus \Lambda$ un punto della cubica.

Posto:

$$A' := (1, \mathscr{P}(-z), \mathscr{P}'(-z)) = (1, \mathscr{P}(z), -\mathscr{P}'(z)),$$

si ha che $z - z \in \Lambda$, quindi:

$$A +_{toro} A' = (0, 0, 1).$$

Abbiamo quindi dimostrato che l'opposto secondo $+_{toro}$ di $A = (1, x, y)$ è il simmetrico A' di A rispetto all'asse x, $A' = (1, x, -y)$, cioè coincide con l'opposto secondo $+$ di A, e d'ora in poi sarà quindi denotato con $-A$.

Vogliamo ora calcolare $A +_{toro} B$ per una generica coppia di punti A e B sul supporto della cubica; i casi in cui A o B siano l'elemento neutro sono banali e abbiamo già trattato il caso $A = -B$.

Osserviamo inoltre che essendo $\mathcal{C}_\Lambda$ in forma normale, il caso $A = -B$ è l'unico in cui i punti A e B distinti abbiano prima coordinata uguale nel piano affine ottenuto deomogenizzando rispetto ad x_0. In tutti gli altri casi $x_A \neq x_B$. Inoltre avendo già escluso il punto $(0, 0, 1)$, tutti i rimanenti punti della cubica appartengono al piano affine ottenuto deomogenizzando rispetto a x_0. Quindi i punti che useremo saranno tutti della forma $(\mathscr{P}(z), \mathscr{P}'(z))$.

Allora consideriamo la retta r per i punti $A = (\mathscr{P}(z_1), \mathscr{P}'(z_1))$ e $B = (\mathscr{P}(z_2), \mathscr{P}'(z_2))$; essa avrà equazione affine della forma $y = mx + q$. Questo equivale ad affermare che i punti z_1 e z_2 sono soluzioni dell'equazione:

$$\mathscr{P}'(z) - m\mathscr{P}(z) - q = 0. \tag{3.4}$$

Ora se definiamo la funzione $F(z) := \mathscr{P}'(z) - m\mathscr{P}(z) - q$, essa è meromorfa e non costante, doppiamente periodica con reticolo dei periodi Λ quindi, fissato α come nel successivo lemma 3.3.2, possiamo applicare il lemma 3.3.3 e troviamo:

$$\frac{1}{2\pi i} \int_{\partial(\alpha+\mathcal{P})} \frac{F'(z)}{F(z)} dz = Z - P.$$

Inoltre osserviamo che F possiede su $\alpha + \mathcal{P}$ un solo polo di ordine 3, in un punto del reticolo Λ, quindi $P = 3$. Inoltre l'integrale scritto sopra è nullo perché la funzione integrata è periodica con reticolo dei periodi Λ, quindi i contributi dati dall'integrazione su lati opposti del parallelogramma si annullano a vicenda.

Concludiamo allora che $0 = Z - P = Z - 3$, quindi $Z = 3$. Questo ci dice che la funzione F possiede 3 zeri (contati con molteplicità) a_1, a_2, a_3.

Applichiamo ora alla funzione $F(z)$ il lemma 3.3.4, ricordando che i poli di F sono $b_1 = b_2 = b_3 \in \Lambda$; quindi:

$$a_1 + a_2 + a_3 - 3b_1 \in \Lambda \quad \Rightarrow \quad a_1 + a_2 + a_3 \in \Lambda.$$

In sintesi, abbiamo dimostrato che sul compatto $\alpha + \mathcal{P}$ la funzione F possiede esattamente 3 zeri (non necessariamente distinti) e tali che la loro somma sia un punto del reticolo Λ. Nel nostro caso, essendo già z_1 e z_2 zeri, ne segue che deve esistere z_3 soluzione della (3.4) (eventualmente coincidente con i precedenti) e tale che:

$$z_1 + z_2 + z_3 \in \Lambda \quad \Rightarrow \quad \Lambda + z_3 = \Lambda - (z_1 + z_2).$$

Supponiamo che i tre zeri della (3.4) siano distinti; in tal caso ad ognuno di essi corrisponde un punto distinto di intersezione della retta $y = mx + q$ con la cubica $\mathcal{C}_\Lambda$.

Quindi la retta per i punti A e B interseca la cubica in un terzo punto:

$$C' = (\mathscr{P}(-(z_1 + z_2)), \mathscr{P}'(-(z_1 + z_2))) = (\mathscr{P}(z_1 + z_2), -\mathscr{P}'(z_1 + z_2)) = -C,$$

dove $C = (\mathscr{P}(z_1 + z_2), \mathscr{P}'(z_1 + z_2)) = A +_{toro} B$.

In sintesi nel caso in cui i punti usati siano distinti, l'operazione di gruppo $+_{toro}$ su $\mathcal{C}_\Lambda$ si può descrivere così: dati due punti A e B sul supporto della cubica, con $x_A \neq x_B$, si considera la retta r per tali punti; essa interseca la cubica in un terzo punto (eventualmente coincidente con i precedenti) C'; il punto C simmetrico rispetto all'asse x di tale punto è la somma di A e B.

Quella che abbiamo appena descritto è l'operazione di gruppo + già definita nel capitolo 2 nel caso in cui la cubica non singolare sia posta in forma normale e il punto base della cubica sia il flesso $(0, 0, 1)$, quindi le due leggi di gruppo coincidono, che è quanto volevamo dimostrare.

Se però esistono intersezioni multiple (doppie o triple), dobbiamo ancora verificare che la molteplicità di intersezione della cubica con la retta coincida con la molteplicità del corrispondente valore di z come soluzione della (3.4). Siano allora come sopra z_1, z_2 e $-z_3$ soluzioni di tale equazione. Tali radici non sono nessuna l'opposta di un'altra perché la retta $y = mx + q$ non è parallela all'asse y.

I corrispondenti punti di intersezione della retta con la cubica avranno prima componente rispettivamente x_1, x_2 e x_3, dove $x_i = \mathscr{P}(z_i)$. Ricordando che $\mathcal{C}_\Lambda : y^2 = 4x^3 - g_2x - g_3$, tali coordinate si calcolano anche risolvendo il sistema:

$$\begin{cases} y^2 &= 4x^3 - g_2x - g_3 \\ y &= mx + q. \end{cases}$$

Sostituendo y, otteniamo che le coordinate x_i si trovano come zeri del polinomio $4x^3 - g_2x - g_3 - (mx + q)^2$, cioè:

$$4x^3 - g_2x - g_3 - (mx + q)^2 = 4(x - x_1)(x - x_2)(x - x_3).$$

D'altra parte per costruzione i punti z_1, z_2 e $-z_3$ sono soluzioni dell'equazione $\mathscr{P}'(z) - m\mathscr{P}(z) - q = 0$, quindi i punti $-z_1, -z_2$ e z_3 sono soluzioni dell'equazione $\mathscr{P}'(z) + m\mathscr{P}(z) + q = 0$.

Dunque i sei punti $\pm z_1, \pm z_2, \pm z_3$ sono gli zeri di $\mathscr{P}'(z)^2 - (m\mathscr{P}(z) + q)^2 = 0$. D'altra parte, possiamo scrivere:

$$\mathscr{P}'(z)^2 - (m\mathscr{P}(z) + q)^2 = 4\mathscr{P}(z)^3 - g_2\mathscr{P}(z) - g_3 - (m\mathscr{P}(z) + q)^2 =$$

$$= 4(\mathscr{P}(z) - x_1)(\mathscr{P}(z) - x_2)(\mathscr{P}(z) - x_3).$$

Consideriamo allora ad esempio $\mathscr{P}(\pm z_1) = x_1$: la molteplicità di intersezione della retta con la cubica nel punto di prima coordinata x_1 per definizione è uguale ad 1 + il numero delle radici x_2, x_3 uguali ad x_1. Essendo $x_2 = \mathscr{P}(\pm z_2)$ e $x_3 = \mathscr{P}(\pm z_3)$, tale valore, a sua volta, è uguale ad 1 +

il numero di $\pm z_2$, $\pm z_3$ tali che x_1 sia uguale a $\mathscr{P}(\pm z_2)$ e a $\mathscr{P}(\pm z_3)$, cioè il numero di $\pm z_2, \pm z_3$ tali che $\pm z_1$ sia uguale a $\pm z_2, \pm z_3$.

Quindi la molteplicità di intersezione in x_1 è anche uguale a 1 + il numero di $z_2, -z_3$ che sono uguali a z_1, cioè la molteplicità di z_1.

Quello che abbiamo provato, allora, è che la molteplicità di intersezione della retta con la cubica in un punto di prima coordinata x_i è uguale alla molteplicità della corrispondente radice z_i dell'equazione (3.4), come si voleva. □

Nel teorema precedente abbiamo usato i seguenti lemmi:

Lemma 3.3.2. *Per ogni funzione F meromorfa non costante su $\mathbb{C}$ e doppiamente periodica con reticolo dei periodi Λ, con $\mathcal{P} := \{\lambda\omega_1 + \eta\omega_2 \mid \lambda, \eta \in [0,1]\}$ parallelogramma fondamentale associato a Λ, esiste $\alpha \in \mathbb{C}$ tale che il bordo del parallelogramma traslato $\alpha + \mathcal{P}$ non contenga nè zeri nè poli di F.*

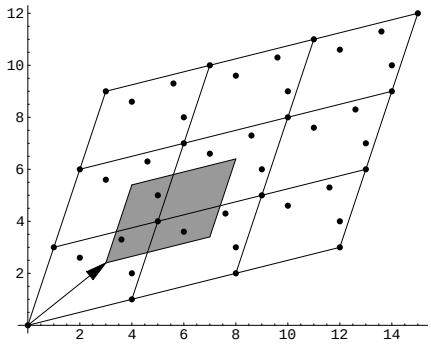

Figura 3.2: Il parallelogramma $\mathcal{P}$ traslato di α.

Dimostrazione. Consideriamo il parallelogramma $\mathcal{P}$: essendo compatto, contiene necessariamente un numero finito di zeri e di poli di F; detti $\{z_i\}_{i=1,\dots n}$ tali punti, essi possono essere considerati come vettori di $\mathbb{R}^2$. Possiamo allora scriverne le coordinate rispetto alla base ω_1, ω_2, cioè:

$$\begin{array}{ccccc} z_1 & = & a_1\omega_1 & + & b_1\omega_2 \\ \vdots & & \vdots & & \vdots \\ z_n & = & a_n\omega_1 & + & b_n\omega_2. \end{array}$$

Osserviamo che, essendo F doppiamente periodica con reticolo dei periodi Λ, tutti gli altri zeri e poli di tale funzione hanno la forma $z_i + m\omega_1 + n\omega_2,\ \ n, m \in \mathbb{Z}$.

Allora basta scegliere $\alpha = a\omega_1 + b\omega_2$ con l'accortezza di prendere $a \neq a_i$, $b \neq b_i\ \forall i = 1, \dots n$. In tal modo se consideriamo il lato del parallelogramma $\alpha + \mathcal{P}$, costituito dai punti della forma $\{\omega_1(a + \lambda) + b\omega_2 \mid \lambda \in [0, 1]\}$, tale lato non contiene nessuno $z_i + m\omega_1 + n\omega_2$ perché la seconda componente è diversa, idem sugli altri lati.

□

Lemma 3.3.3. *(dell'indicatore logaritmico) Sia F una funzione meromorfa non costante su un sottoinsieme aperto D di $\mathbb{C}$ e sia K un compatto contenuto in D e con bordo orientato Γ. Se F non ha nè poli nè zeri sul bordo di K, allora:*

$$\frac{1}{2\pi i}\int_\Gamma \frac{F'(z)}{F(z)}dz = Z - P$$

dove con Z e P intendiamo rispettivamente la somma delle molteplicità degli zeri e la somma delle molteplicità dei poli di F in K.

Per una dimostrazione di questo risultato classico della teoria di una variabile complessa, si veda, ad esempio, [C], proposizione III.4.1.

Lemma 3.3.4. *Sia F una funzione meromorfa su $\mathbb{C}$, doppiamente periodica di periodo un reticolo Λ e sia $\mathcal{P}$ il parallelogramma fondamentale associato a Λ.*

Sia $\alpha \in \mathbb{C}$ tale che F non abbia nè zeri nè poli sul bordo di $\mathcal{P}$ traslato di α, cioè su $\partial(\alpha + \mathcal{P})$.

Siano inoltre $\{a_i\}$ e $\{b_j\}$ rispettivamente gli zeri e i poli di F nel compatto $\alpha + \mathcal{P}$, ciascuno ripetuto un numero di volte pari alla sua molteplicità. Allora

$$\sum_i a_i - \sum_j b_j \in \Lambda.$$

Una prova di questo lemma si può ad esempio trovare in [KO], sezione I.7.

Sia ora $\mathcal{C}$ una cubica non singolare di $\mathbb{P}^2$, per la proposizione 2.3.1 essa è proiettivamente equivalente a $y^2 = x^3 + ax + b$. Ora applicando a tale curva l'affinità:

$$(x, y) \mapsto \left(x, \frac{y}{2}\right),$$

otteniamo la curva di equazione $y^2 = 4x^3 + 4ax + 4b$. Ponendo allora $\alpha := -4a$, $\beta = -4b$ e ricordando il teorema 1.2.2, si ha che ogni cubica piana non singolare $\mathcal{C}$ è proiettivamente equivalente a due cubiche non singolari $\mathcal{C}', \mathcal{C}''$ di equazioni affini:

$$\begin{aligned} \mathcal{C}' : \quad y^2 &= x(x-1)(x-\lambda), \quad \lambda \in \mathbb{C} \setminus \{0, 1\}, \\ \mathcal{C}'' : \quad y^2 &= 4x^3 - \alpha x - \beta. \end{aligned}$$

Proposizione 3.3.5. *Ponendo* $\Delta(\mathcal{C}'') := \alpha^3 - 27\beta^2$, *si trova che* $\Delta(\mathcal{C}'') = 16\lambda^2(\lambda - 1)^2 \neq 0$.

Dimostrazione. Ricordiamo che nella dimostrazione della proposizione 2.3.1, abbiamo posto:

$$a := -\frac{1}{3}(\lambda + 1)^2 + \lambda, \quad b := -\frac{2}{27}(\lambda + 1)^3 + \frac{\lambda(\lambda + 1)}{3}.$$

Dunque:

$$\begin{aligned} \Delta = -64a^3 - 27 \cdot 16b^2 = -16(4a^3 + 27b^2) = \\ = -16\left(-\frac{4}{27}(\lambda+1)^6 + \frac{4}{3}\lambda(\lambda+1)^4 - 4\lambda^2(\lambda+1)^2 + 4\lambda^3 + \right. \\ \left. + \frac{4}{27}(\lambda+1)^6 - \frac{4}{3}\lambda(\lambda+1)^4 + 3\lambda^2(\lambda+1)^2\right) = \\ = -16\left(-\lambda^2(\lambda+1)^2 + 4\lambda^3\right) = \end{aligned}$$

$$= -16\lambda^2(-\lambda + 2\lambda - 1) =$$
$$= 16\lambda^2(\lambda - 1)^2.$$

Tale valore è diverso da zero poichè $\lambda \neq 0, 1$ □

Si dimostra inoltre il seguente:

Teorema 3.3.6. *Dati $g_2, g_3 \in \mathbb{C}$, con $\Delta = {g_2}^3 - 27{g_3}^2 \neq 0$, esiste $\tau \in \mathbb{C}$, $\tau \notin \mathbb{R}$ tale che il reticolo $\Lambda = \Lambda_{1,\tau}$ generato da 1 e da τ abbia $g_2(\Lambda) = g_2$ e $g_3(\Lambda) = g_3$.*

(si veda [H-C], 1.II.4, §4)

Quindi se $\mathcal{C}$ è una cubica non singolare di $\mathbb{P}^2$, esiste un reticolo Λ tale che $\mathcal{C}$ sia proiettivamente equivalente a $\mathcal{C}_\Lambda$.

Grazie ai risultati precedenti possiamo provare il seguente:

Teorema 3.3.7. *Sia $\mathcal{C}$ una cubica non singolare di $\mathbb{P}^2(\mathbb{C})$; l'operazione + definita nella sezione 2.2 scegliendo come O un suo punto di flesso rende $\mathcal{C}$ un gruppo abeliano.*

Dimostrazione. Per quanto appena detto, esiste un reticolo Λ tale che $\mathcal{C}$ sia proiettivamente equivalente a $\mathcal{C}_\Lambda$. Fissato un qualunque flesso $F \in \mathcal{C}$, si può supporre, grazie al teorema 1.2.4, che la proiettività Φ che manda $\mathcal{C}$ su $\mathcal{C}_\Lambda$ mandi F in $(0, 0, 1)$.

Su $\mathcal{C}_\Lambda$ per il teorema 3.3.1 l'operazione + descritta nella sezione 2.2 con la scelta di $O = (0, 0, 1)$ è ben definita e, in particolare, gode della proprietà associativa.

La proiettività Φ manda rette in rette, flessi in flessi e punti di intersezione in punti di intersezione, conservando anche le molteplicità di intersezione, così il + su $\mathcal{C}_\Lambda$ con $O = (0, 0, 1)$ si trasforma mediante la proiettività inversa nel + su $\mathcal{C}$ con $O = F$. □

Questo teorema, come abbiamo detto nel capitolo 2, è vero anche senza nessuna limitazione nella scelta del punto O elemento neutro del gruppo, cioè anche quando O non è un flesso per la cubica non singolare $\mathcal{C}$; per questo si veda, ad esempio, [SH], corollario al teorema 3 di III.4.3.

Capitolo 4

Appendice

Finora abbiamo solo dimostrato che scegliendo come O il punto di flesso $(0,0,1)$ sulla cubica ellittica $\mathcal{C} = \mathcal{C}_\Lambda$, otteniamo una legge di gruppo. Per evitare dubbi, scriveremo d'ora in poi $+_O$ per indicare la legge di gruppo con $O = (0,0,1)$ come elemento neutro e $+_{O'}$ per l'operazione binaria definita scegliendo come elemento neutro un generico punto O' del supporto della cubica. Vogliamo allora mostrare il seguente:

Teorema 4.0.8. *L'applicazione $+_{O'}$ è un'operazione di gruppo sulla cubica $\mathcal{C}$*

Dimostrazione. Ricordiamo che per dimostrare che $(\mathcal{C}, +_O)$ è un gruppo abbiamo usato in maniera essenziale l'omeomorfismo:

$$\begin{array}{rccl} u: & T^2 = \mathbb{C}/\Lambda & \to & \mathcal{C} = \mathcal{C}_\Lambda \\ & \Lambda + z & \to & \begin{cases} (1, \mathscr{P}(z), \mathscr{P}'(z)) & \text{se } z \notin \Lambda \\ (0,0,1) & \text{se } z \in \Lambda. \end{cases} \end{array}$$

dove $\mathscr{P}(z) = \mathscr{P}_\Lambda(z)$.

Vogliamo ora descrivere una applicazione biunivoca $\mathcal{C} \to \mathcal{C}$ che porti O in O' e che muti la legge di gruppo $+_O$ nella legge $+_{O'}$. Definiamo tale applicazione come composizione di tre applicazioni:

$$\begin{array}{rccccccc} F: & \mathcal{C} & \to & T^2 & \to & T^2 & \to & \mathcal{C} \\ & P & \to & u^{-1}(P) & \to & u^{-1}(P)-\alpha & \to & u(u^{-1}(P)-\alpha) \end{array}$$

dove $\Lambda + \alpha := u^{-1}(O')$

In primo luogo osserviamo che F è ben definita, oltre che 1-1 e su perchè composizione di applicazioni 1-1 e su. Inoltre l'inversa di F si calcola facilmente come:

$$F^{-1}(Q) = u(u^{-1}(Q) + \alpha) \quad \forall Q \in \mathcal{C}.$$

Inoltre per costruzione:

$$F(O') = u(u^{-1}(O') - \alpha) = u(\Lambda + \alpha - \alpha) = u(\Lambda) = (0, 0, 1) = O$$

Date queste proprietà, F induce una nuova legge di gruppo su $\mathcal{C}$:

$$\begin{array}{rccc} +_F: & \mathcal{C} \times \mathcal{C} & \to & \mathcal{C} \\ & (A, B) & \to & A +_F B := F^{-1}(F(A) +_O F(B)). \end{array}$$

Tale applicazione binaria è automaticamente una legge di gruppo (con elemento neutro $O' = F^{-1}(O)$) grazie al fatto che $+_O$ è una legge di gruppo su $\mathcal{C}$.

Vogliamo ora calcolare esplicitamente $A +_F B$; siano A e B due punti qualunque di $\mathcal{C}$, essi saranno allora della forma $A = u(\Lambda + z_1)$, $B = u(\Lambda + z_2)$. Allora:

$$A +_F B = F^{-1}(F(A) +_O F(B)) = F^{-1}(u(u^{-1}(A) - \alpha) +_O u(u^{-1}(B) - \alpha)) =$$

$$= F^{-1}(u(\Lambda + z_1 - \alpha) +_O u(\Lambda + z_2 - \alpha)) = F^{-1}(u(\Lambda + z_1 + z_2 - 2\alpha)) =$$

$$= u(u^{-1}(u(\Lambda + z_1 + z_2 - 2\alpha)) + \alpha) = u(\Lambda + z_1 + z_2 - 2\alpha + \alpha) =$$

$$= u(\Lambda + z_1 + z_2 - \alpha).$$

Ora ricordiamo quanto detto a pagina 52: dati due punti propri della cubica $A = (1, \mathscr{P}(z_1), \mathscr{P}'(z_1))$ e $B = (1, \mathscr{P}(z_2), \mathscr{P}'(z_2))$, allora il terzo punto di intersezione della retta per tali punti con la cubica è:

$$R(A, B) = (1, \mathscr{P}(-z_1 - z_2), \mathscr{P}'(-z_1 - z_2)) = u(\Lambda - z_1 - z_2)$$

nel caso in cui la retta non sia parallela all'asse y, cioè se $\Lambda + z_1 \neq \Lambda - z_2$. In tal caso, invece, il terzo punto di intersezione è il punto improprio:

$$R(A, B) = (0, 0, 1) = u(\Lambda) = u(\Lambda - z_1 - z_2)$$

Calcoliamo ora $R(A, O)$: per costruzione la retta è parallela all'asse y, quindi il terzo punto di intersezione è:

$$R(A, O) = R(u(\Lambda + z_1), u(\Lambda)) = (1, \mathscr{P}(z_1), -\mathscr{P}'(z_1)) = u(\Lambda - z_1).$$

Infine essendo il punto O un flesso per la cubica,

$$R(O, O) = R(u(\Lambda), u(\Lambda)) = (0, 0, 1) = u(\Lambda).$$

Possiamo quindi concludere che:

$$R(u(\Lambda + z_1), u(\Lambda + z_2)) = u(\Lambda - z_1 - z_2) \quad \forall z_1, z_2 \in \mathbb{C}.$$

Ricordiamo ora che per definizione $A +_{O'} B = R(R(A, B), O')$, quindi se assumiamo come sopra $A = u(\Lambda + z_1)$ e $B = u(\Lambda + z_2)$, allora:

$$A +_{O'} B = R(R(u(\Lambda + z_1), u(\Lambda + z_2)), u(\Lambda + \alpha)) =$$
$$= R(u(\Lambda - z_1 - z_2), u(\Lambda + \alpha)) = u(\Lambda + z_1 + z_2 - \alpha) = A +_F B.$$

Quindi la legge di gruppo $+_F$ definita sopra coincide con l'applicazione $+_{O'}$ definita fissando come elemento neutro un punto arbitrario O' della cubica. Questo basta per concludere la dimostrazione.

□

Bibliografia

[C] Henri Cartan, *Elementary theory of analytic functions of one or several complex variables*, Dover, New York (1995).

[HA] Robin Hartshorne, *Algebraic Geometry*, Springer, New York (1977).

[H-C] Adolf Hurwitz, Richard Courant, *Allgemeine Funktionentheorie und elliptische Funktionen - Geometrische funktionentheorie*, Springer, Berlino (1922).

[K] Frances Kirwan, *Complex algebraic curves*, London Mathematical Society, Cambridge (1992).

[KN] Antony W. Knapp, *Elliptic curves*, Princeton University Press, Princeton (1992).

[KO] Neal Koblitz, *Introduction to elliptic curves and modular forms*, Springer, New York (1984).

[R] Miles Reid, *Undergraduate algebraic geometry*, Cambridge University Press, Cambridge (1988).

[S] Edoardo Sernesi, *Geometria 1*, Bollati Boringhieri, Torino (1989).

[S2] Edoardo Sernesi, *Geometria 2*, Bollati Boringhieri, Torino (1989).

[SH] Igor R. Shafarevich, *Basic Algebraic Geometry 1 - Revised Edition*, Springer, Berlino (1994).

[SI] Joseph H. Silverman, *The arithmethic of elliptic curves*, Springer, New York (1986).

Ringraziamenti

E adesso, la parte forse più difficile della tesi, soprattutto per la paura di dimenticare qualcuno, perciò chiedo perdono in partenza!

È d'obbligo ringraziare la professoressa Monica Idà per l'aiuto dato in tutti questi mesi per la mia tesi, ma soprattutto per aver sopportato la mia parlantina un po' troppo vivace; un grazie ai prof. della facoltà di Matematica di Bologna, in particolare alla prof. Mirella Manaresi che ho importunato spesso per il mio tirocinio.

Un GRAZIE enorme (per chi conosce il LaTeX, il comando dovrebbe essere `\Huge`) a tutti i compagni di facoltà, del mio anno e degli altri anni, in particolare un grazie di cuore a Cris (grazie di tutto!), Ivan (con cui ho affrontato perfino Topologia Algebrica), Stefano (i grafici di questa tesi devono molto a lui), Giulio, Federico, Susy, Elena, Eleonora, Francesca, Yannick, Giacomo, Filippo, Licia, Agnese, Martina, Michela, Alessandra, Enrico, Sara, Paolo, Marcello.. È stato un piacere conoscervi e condividere con voi 3 anni di studio, ma soprattutto di vita..

Naturalmente un grazie a tutti i miei amici per i quali la matematica rimane tuttora un "Gran Casino Generale", e nonostante ciò mi hanno sostenuto nella mia scelta di questa facoltà, continuando però a chiedere perplessi: "Ma tu hai solo esami di matematica?" e sentendosi invariabilmente rispondere "No, purtroppo!" (chi mi conosce sa a che esami mi riferisco..). Grazie quindi in particolare a Germana, Anna, Chiara, Serena, Valentina, Eleonora, Nicola, Chicco, Michele, Ester, Alberto, Viviana, Carlotta e Carlotta, Guglielmo, Peter, Lorenzo, Matteo, Elisa, Giulia,..

Grazie inoltre a chi ha pensato che io fossi bravo a spiegare trigonometria, limiti, derivate e prodotti notevoli; in altre parole grazie per avermi sopportato a tutti gli studenti delle superiori a cui ho dato ripetizioni in questi anni, in particolare grazie ad Emanuela.

Grazie anche a tutte le prof. delle superiori che mi hanno aiutato: alla prof. Giovanna Pedicini che mi ha convinto a iscrivermi a Matematica, alla prof. Roberta Faldella, alle prof. Elena Tenze e Claudia Francesconi che mi hanno aiutato per il tirocinio, oltre a tutti i loro studenti che mi hanno sopportato per tante ore a Ravenna.

Grazie inoltre a chi 3 anni fa mi ha regalato il portatile con cui ho scritto questa tesi.

Infine **GRAZIE** soprattutto alla mia famiglia e ai miei parenti, per avermi sempre sostenuto e per aver sopportato stoicamente per tre anni le mie disquisizioni di matematica, a tavola e non solo...

Per concludere, per confermare nelle proprie convinzioni chi mi crede matto, ma soprattutto a beneficio di tutti i fanatici dello scrittore britannico Douglas Adams, trovo giusto finire così: “Addio e grazie per tutto il pesce”...