9.2. Curve proiettive di genere 1. *Una curva proiettiva $\mathscr{C}$ è di genere* 1*, se e solo se è birazionale ad una cubica liscia nel piano proiettivo complesso.*

Infatti, usando $D = 3P$ con $P \in \mathscr{C}$, che sappiamo essere un divisore molto ampio, e usando ripetutamente Riemann-Roch, possiamo studiare gli spazi $\mathscr{L}(nP)$:

$$\begin{array}{ll} \ell(P) = 1 & \mathscr{L}(P) = \langle 1\rangle_K \\ \ell(2P) = 2 & \mathscr{L}(2P) = \langle 1, x\rangle_K \\ \ell(3P) = 3 & \mathscr{L}(3P) = \langle 1, x, y = x'\rangle_K \\ \ell(4P) = 4 & \mathscr{L}(4P) = \langle 1, x, y, x^2\rangle_K \\ \ell(5P) = 5 & \mathscr{L}(5P) = \langle 1, x, y, x^2, xy\rangle_K \\ \ell(6P) = 6 & \mathscr{L}(6P) = \langle 1, x, y, x^2, xy, y^2, x^3\rangle_K \end{array}$$

e vediamo che nell'ultimo scritto, che è di dimensione 6, si trovano 7 funzioni razionali: dunque ci deve essere tra loro una relazione di dipendenza lineare su K, cioè una equazione algebrica, che necessariamente coinvolge le ultime due funzioni incontrate, cioè y^2, x^3: si tratta quindi di una relazione cubica nel piano affine di coordinate X, Y.

Usando invece il divisore $D = 4P$ con $P \in \mathscr{C}$, anch'esso molto ampio, otteniamo una immersione proiettiva in dimensione 3, la cui immagine è definita dalla intersezione di due quadriche, la prima relazione essendo $Z = X^2$ nelle coordinate affini X, Y, Z.

9.2.1. Una curva proiettiva è di genere 1 se e solo se ammette sistemi lineari completi di dimensione pari al grado diminuito di uno.

9.2.2. Costruzione della legge di gruppo sulle curve di genere 1. Noi abbiamo visto la costruzione geometrica, nel caso di curve ellittiche piane, della legge di gruppo di Poincaré. Vediamo ora come quella stessa struttura può essere definita usando essenzialmente il teorema di Riemann-Roch.

Lo strumento fondamentale è il seguente: se $n \geqslant 1$ e $D + Q \sim nO \sim D + Q'$ (D un divisore, qualsiasi sia il punto O, serve solo per dire il grado dei divisori), allora $Q = Q'$; infatti lo spazio $\mathscr{L}(nO - D)$ ha dimensione 1, e l'ulteriore zero delle funzioni ivi contenute è unico. In particolare: $Q \sim Q'$ implica $Q = Q'$.

Scelto arbitrariamente un posto O della curva, dati due qualsiasi posti P e Q, consideriamo il divisore $3O - P - Q$; poiché si tratta di un divisore di grado 1, abbiamo $\ell(3O - P - Q) = 1$, e quindi esiste una funzione razionale non costante avente polo triplo in O, e zeri in P e Q. Questa funzione deve avere un ulteriore zero su $\mathscr{C}$ che chiamiamo $P * Q$. Definiamo allora la legge di gruppo tramite $P \oplus Q = O * (P * Q)$ (usiamo il simbolo $\oplus$ per non confondere l'operazione di Poincaré con la somma di divisori!).

Verificare che O è elemento neutro, che la somma è commutativa, che ogni elemento ha l'elemento opposto è facile.

Per esempio, che $P \oplus O = P$ per ogni punto viene dal fatto che $P + (P * O) \sim 2O \sim (P * O) + (P \oplus O)$, da cui $P \sim P \oplus O$, dunque uguali.

Altro esempio: che $\ominus P$ (opposto di P) sia $O * P$, cioè che $P \oplus (O * P) = O$ è equivalente a $P * (O * P) = O$ e si vede per differenza da $3O \sim P + (O * P) + (P * (O * P))$ e $2O \sim P + (O * P)$, che dà $O \sim P * (O * P)$, dunque uguali.

Per verificare la proprietà associativa $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ si può ragionare così: basta verificare che $(P \oplus Q) * R = P * (Q \oplus R)$, e abbiamo le seguenti equivalenze:

$$\begin{gathered} P + Q + (P * Q) \sim 3O \sim Q + R + (Q * R) \\ (P * Q) + (P \oplus Q) \sim 2O \sim (Q * R) + (Q \oplus R) \\ (P \oplus Q) + R + ((P \oplus Q) * R) \sim 3O \sim P + (Q \oplus R) + (P * (Q \oplus R)) \end{gathered}$$

e la somma alternata dà

$$P + Q + R + ((P \oplus Q) * R) \sim 4O \sim P + Q + R + (P * (Q \oplus R))$$

da cui la conclusione. Si osservi anche che per trovare $\ominus(P \oplus Q \oplus R)$ basta trovare il quarto zero delle funzioni razionali non nulle in $\mathscr{L}(4O - P - Q - R)$.

9.2.3. Si osservi che per ogni insieme $P_1, P_2, \ldots, P_n$ di punti di $\mathscr{C}$ si ha che

$$P_1 \oplus P_2 \oplus \ldots \oplus P_n \sim P_1 + P_2 + \ldots + P_n - (n-1)O$$