UNIVERSITÀ DEGLI STUDI DI CAGLIARI
Facoltà di Scienze
Corso di Laurea in Matematica

Il gruppo abeliano associato ad una curva ellittica

Monica Bottaru

Anno accademico 2017-2018

Definizione 1. (Piano proiettivo $\mathbf{P}^2\mathbb{C}$)

Sia $\mathbb{C}$ il campo dei numeri complessi.
Il piano proiettivo $\mathbf{P}^2\mathbb{C}$ sul campo $\mathbb{C}$ è l'insieme delle rette passanti per l'origine O di $\mathbb{C}^3$. Equivalentemente, $\mathbf{P}^2\mathbb{C}$ è l'insieme degli spazi vettoriali di dimensione 1 di $\mathbb{C}^3$.

Definizione 2. (Curva algebrica piana proiettiva)

Una curva algebrica di $\mathbf{P}^2\mathbb{C}$ è una classe di proporzionalità di polinomi omogenei non costanti di $\mathbb{C}[x_0, x_1, x_2]$, dove con $\mathbb{C}[x_0, x_1, x_2]$ indichiamo l'anello dei polinomi nelle incognite x_0, x_1, x_2 a coefficienti nel campo $\mathbb{C}$.

Se $F(x_0, x_1, x_2)$ è un rappresentante della curva allora

$$\boxed{F(x_0, x_1, x_2) = 0} \qquad (i)$$

si dice **equazione della curva**, ovvero equazione che definisce la curva.

Il sottoinsieme $\mathcal{C} \subset \mathbf{P}^2\mathbb{C}$ costituito dai punti le cui coordinate soddisfano l'equazione (i) è il **supporto** della curva.

Il grado del polinomio F si dice **grado** della curva.

Definizione 3. Punto Singolare

Sia C una curva algebrica definita dal polinomio omogeneo F.
Si dice che P$\in$ C è un **punto singolare** se **(gradF)(P)=0**.

Definizione 4. Curva algebrica non singolare o liscia

Una curva algebrica C si dice **non singolare** o **liscia** se non contiene punti singolari.

Definizione 5. Genere di una curva algebrica

Data una curva algebrica C, il **genere** di C è definito come
$g = \frac{1}{2}(d-1)(d-2)$ dove d è il grado della curva.

Curva ellittica

Una **curva ellittica** definita sul campo $\mathbb{C}$ è una curva algebrica proiettiva liscia di genere 1 su cui viene specificato un punto O.

E' descritta da un'equazione di grado 3 della forma

$y^2 = x^3 + ax + b \qquad a,b \in \mathbb{C}$ (**Equazione di Weierstrass**)

senza punti singolari.

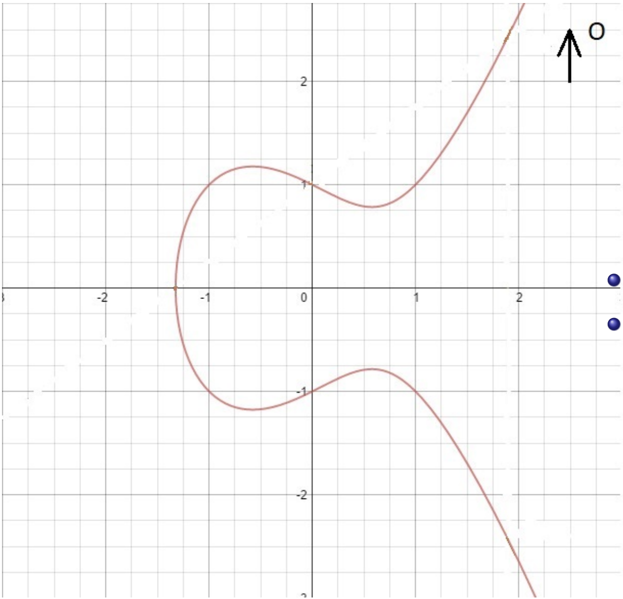
Ogni curva ellittica può essere scritta come luogo degli zeri di un'equazione cubica in $\mathbf{P}^2\mathbb{C}$, con un solo punto sulla retta all'infinito.

Sia $\mathtt{C}$ una **curva ellittica**

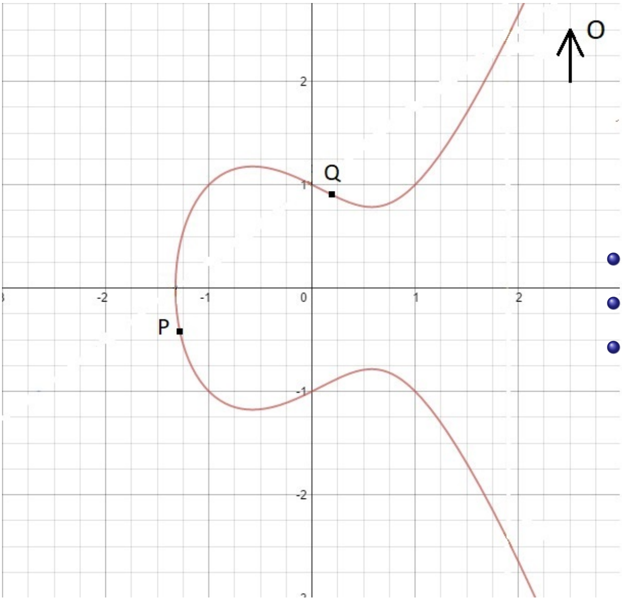
Dotiamo $\mathtt{C}$ dell'operazione somma definita nel modo seguente:

$$
\begin{aligned}
+ \ : \quad \mathtt{C} \times \mathtt{C} \quad &\rightarrow \quad \mathtt{C} \\
(\mathrm{P},\mathrm{Q}) \ &\mapsto \ P + Q = \mathrm{R}(\ \mathrm{R}(\mathrm{P},\mathrm{Q})\ ,\ \mathrm{O}\ )
\end{aligned}
$$

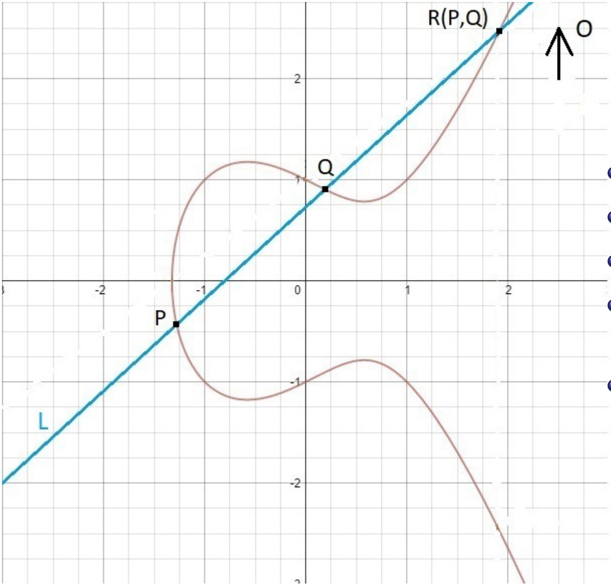
dove O è un punto fissato



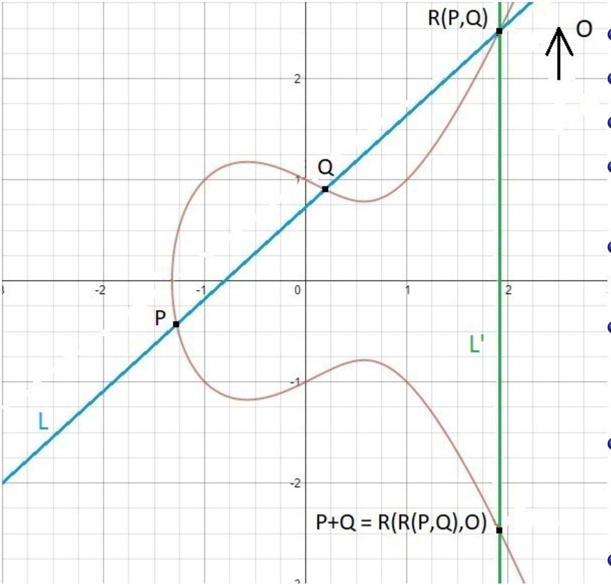
- $\mathcal{C}$ curva ellittica
- O punto all'infinito su $\mathcal{C}$



- $\mathbb{C}$ curva ellittica
- O punto all'infinito su $\mathbb{C}$
- P,Q $\in \mathbb{C}$

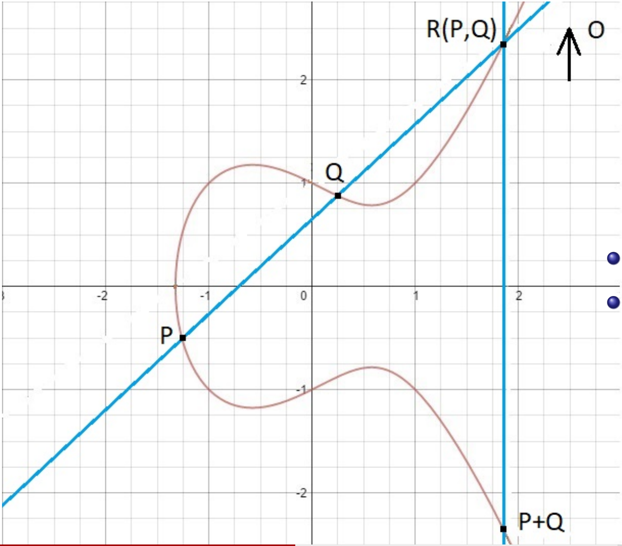


- $\mathcal{C}$ curva ellittica
- O punto all'infinito su $\mathcal{C}$
- P,Q $\in \mathcal{C}$
- L retta che congiunge P con Q
- R(P,Q) terzo punto d'intersezione di $\mathcal{C}$ con L



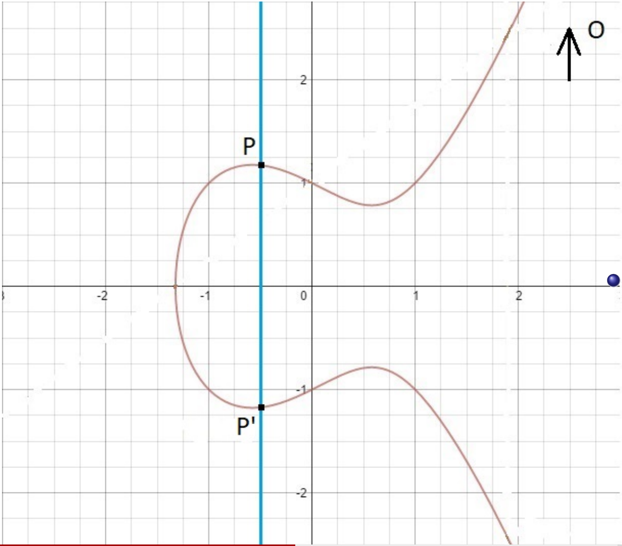
- $\mathcal{C}$ curva ellittica
- O punto all'infinito su $\mathcal{C}$
- P,Q $\in \mathcal{C}$
- L retta che congiunge P con Q
- R(P,Q) terzo punto d'intersezione di $\mathcal{C}$ con L
- L' retta passante per R(P,Q) ed il punto all'infinito O
- P+Q = R(R(P,Q) , O) terzo punto d'intersezione tra $\mathcal{C}$ e L'
- Teorema di Bézout

Proprietà commutativa



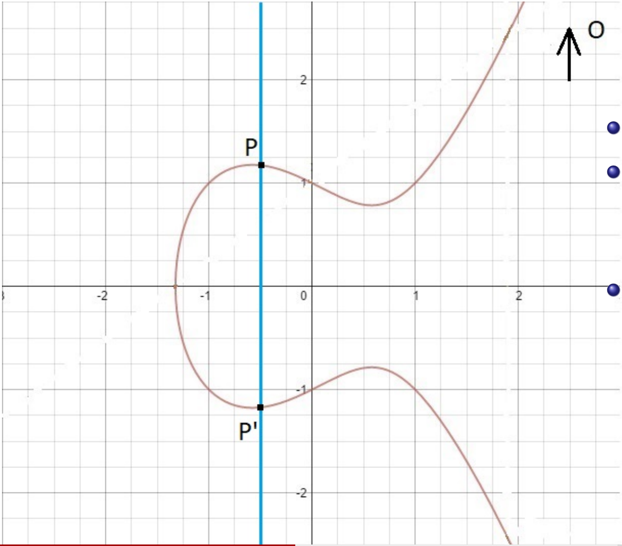
- R(P,Q) = R(Q,P)
- P+Q = R(R(P,Q),O) = R(R(Q,P),O) = Q+P

Elemento neutro



- P+O = R(R(P,O),O) = R(P',O) = P

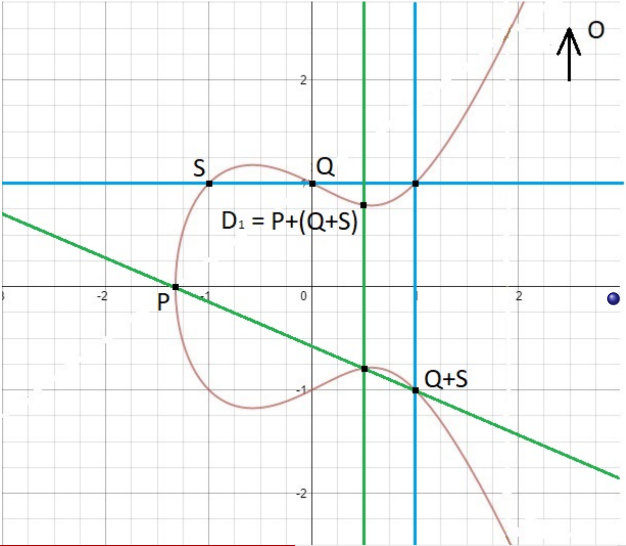
Elemento opposto



- R(P,P') = O
- P+P' = R(R(P,P'),O) = R(O,O) = O

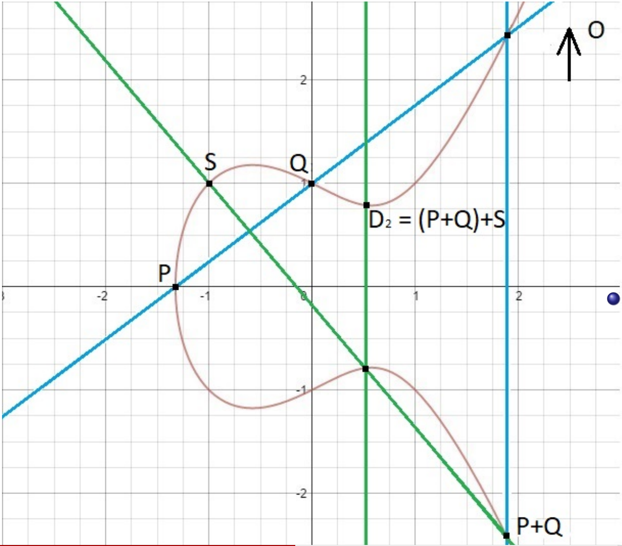
- **Osservazione**: P'=R(P,O) ⇒ R(P,P') = R(P,R(P,O)) ⇒ R(P,R(P,O)) = O ⇒ P e R(P,O) sono uno l'opposto dell'altro.

Proprietà associativa



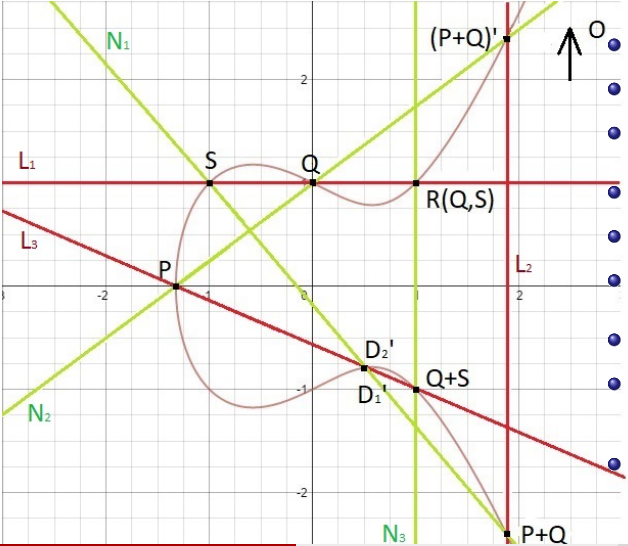
- $\mathrm{P} + (\mathrm{Q}{+}\mathrm{S}) = D_1$

Proprietà associativa



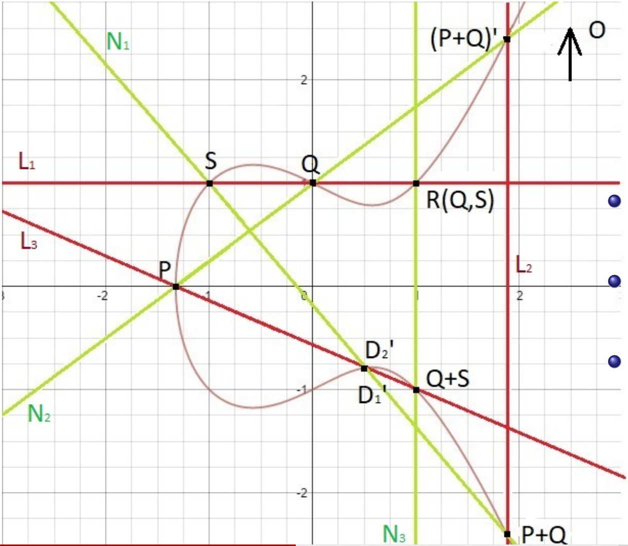
- $(P+Q) + S = D_2$

Proprietà associativa



- $L_1 = QSR(Q,S)$
- $L_2 = O(P+Q)(P+Q)'$
- $L_3 = PD_1'(Q+S)$
- $N_1 = S(P+Q)D_2'$
- $N_2 = PQR(P,Q)$
- $N_3 = R(Q,S)O(S+Q)$
- $\mathcal{C}_1$ curva ellittica
- $\mathcal{C}_2 = L_1 \cup L_2 \cup L_3$ cubica degenere (rette rosse)
- $\mathcal{C}_3 = N_1 \cup N_2 \cup N_3$ cubica degenere (rette verdi)

Proprietà associativa

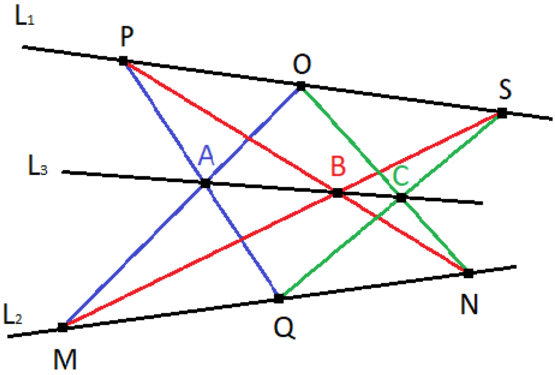


- $\mathcal{C}_1$ e $\mathcal{C}_2$ s'intersecano in 9 punti
- Teorema di Cayley - Bacharach
- $D_1' \in \mathcal{C}_3 \Rightarrow D_1' \in N_1 \Rightarrow D_1' = D_2' \Rightarrow D_1 = D_2$

Teorema

($\mathbb{C}$,+) è un gruppo abeliano.

Teorema di Pappo



- L_1, L_2 rette nel piano
- $P, O, S \in L_1$
- $M, N, Q \in L_2$
- A = PQ ∩ OM
- B = PN ∩ SM
- C = ON ∩ SQ

$$\Downarrow$$

A,B,C sono collineari

Dimostrazione

Osserviamo che:
P+Q = R(R(P,Q),O) = R(A,O) = M
Q+S = R(R(Q,S),O) = R(C,O) = N

Se da un lato:
B = R(M,S) = -((P+Q)+S)

D'altra parte:
PN$\cap L_3$ = R(P,N) = -(P+(Q+S))

Per l'associatività:
(P+Q)+S = P+(Q+S) $\Rightarrow$ B = PN$\cap L_3$ $\Rightarrow$ B$\in L_3$ $\Rightarrow$ A,B,C sono collineari.

GRAZIE PER L'ATTENZIONE