§12.2 Legge di gruppo abeliano delle curve ellittiche

DEF Sia $\mathcal{C}$ una cubica piana liscia su $\mathbb{K}=\mathbb{C}$.
Nel proiettivo ogni retta L interseca $\mathcal{C}$ in esattamente 3 punti, non necessariamente distinti e contati con molteplicità, grazie al teorema di Bézout.

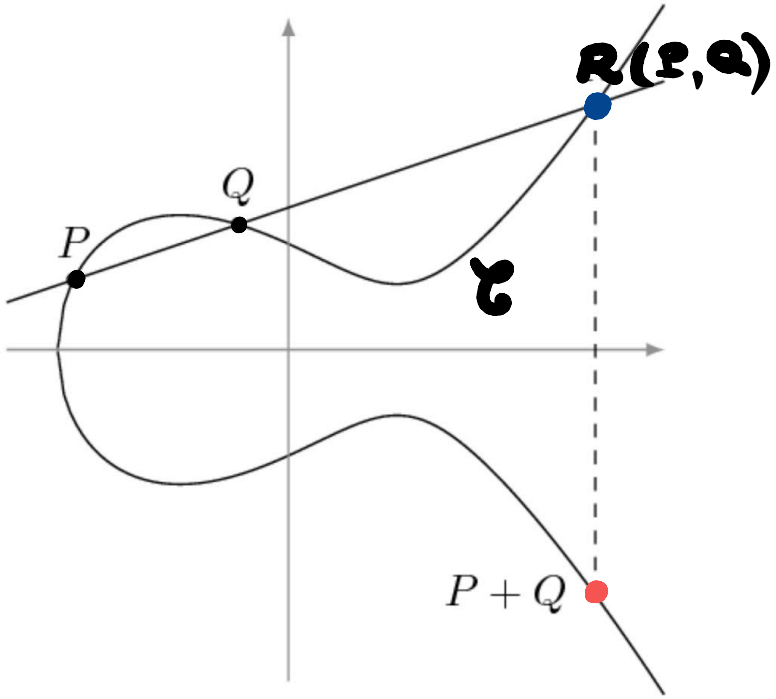
Siano dati $A, B \in \mathcal{C}$, allora è unica retta $L_{\overrightarrow{AB}}$ interseca $\mathcal{C}$ anche in un terzo punto (non necessariam. distinto da A, B) che chiamiamo $R(A,B)$. Se $A=B \Rightarrow L_{\overrightarrow{AA}} := \tau_A(\mathcal{C})$ ← PER BÉZOUT COMUNQUE INTERSECA $\mathcal{C}$ IN UN TERZO PUNTO

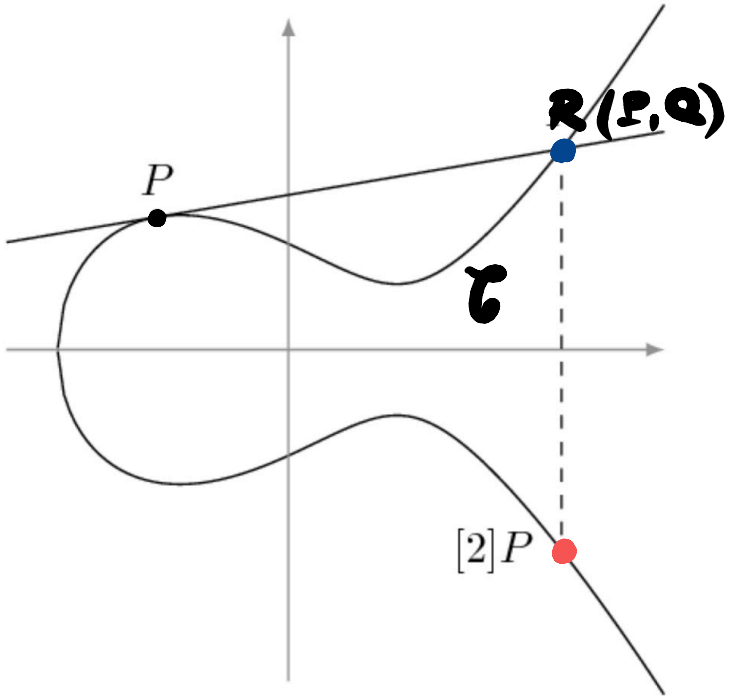
Questo definisce un'operazione binaria

$$R : \mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}$$
$$(A,B) \longmapsto R(A,B)$$

OSS Si hanno le seguenti proprietà

1. R è **COMMUTATIVA** per costruzione
2. $R(A,A) = A \iff A$ **FLESSO**





DEF Si fissi O, uno dei 9 flessi di C, e si definisca l'operazione

$$+ : C \times C \longrightarrow C$$

$$(A,B) \longmapsto R(R(A,B),O)$$

Q: Perché + invece di R e a che serve?

LISCIA — UNO DEI FLESSI COME ELEMENTO NEUTRO

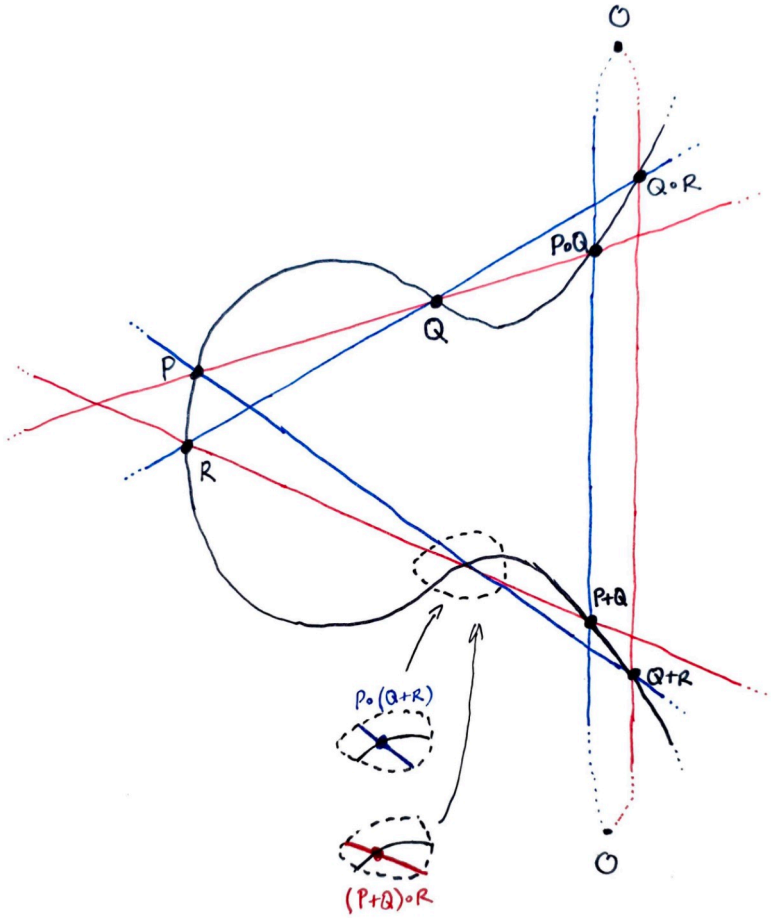
THM $(C, +, O)$ è **GRUPPO ALGEBRICO ABELIANO**

Dimostrazione:

- **CHIUSURA**: C è chiuso rispetto ad $\mathbb{R} \Rightarrow$ C è chiuso rispetto a $+ \Rightarrow (C, +)$ è un magma algebrico.
- **COMMUTATIVITÀ**: La commutatività di $+$ segue dalla commutatività di $\mathbb{R}$
- **ASSOCIATIVITÀ**:

Dimostrazione grafica della associatività:

$$(P+Q)+R = P+(Q+R)$$



Dimostriamo formalmente che $\underbrace{(A+B)+C}_{=R(R(A+B,C),0)} = \underbrace{A+(B+C)}_{=R(R(A,B+C),0)}$

Quindi è sufficiente mostrare che $R(A+B,C) = R(A,B+C)$.
Definiamo la cubica completamente riducibile:

$$D := \overrightarrow{AB} \cup \overrightarrow{A+B,C} \cup \overrightarrow{0,B+C}$$

Allora abbiamo:

$$C \cap D = \{0, A, B, C, A+B, B+C, R(A,B), R(B,C), R(A+B,C)\}$$

e supponiamo che siano tutti distinti (vero generalmente). ← PER ESERCIZIO VEDERE CASO DEGENERE

Sappiamo anche $B, C, R(B,C)$ ALLINEATI.
Allora con $d=3$, $n=1$ abbiamo d^2 PUNTI in $C \cap D$
con $d = \deg(C) = \deg(D) \wedge \exists n<d : n \cdot d$ PUNTI in una curva di grado n IRRID $\Rightarrow$ i rimanenti $d(d-n)=6$ PUNTI sono contenuti in una curva di $\deg = d-n=2 \Rightarrow$ in una conica

Allora i 6 punti

$$\{O,\ A,\ A+B,\ B+C,\ R(A,B),\ R(A+B,C)\} \in \tilde{C}$$

appartengono ad una conica, ma $O,\ A+B,\ R(A,B)$ sono **ALLINEATI** $\Rightarrow \tilde{C}$ DEGENERE $\quad = R(R(A,B),O)$

e quindi possiamo concludere che:

$$A,\ B+C,\ R(A+B,C) \qquad \text{ALLINEATI}$$

Ma per definizione sappiamo che dati A, $B+C$, l'unico terzo punto su $\tilde{C}$ e sulla retta $L_{\overrightarrow{A,B+C}}$ è $R(A,B+C)$ quindi per unicità dobbiamo avere che:

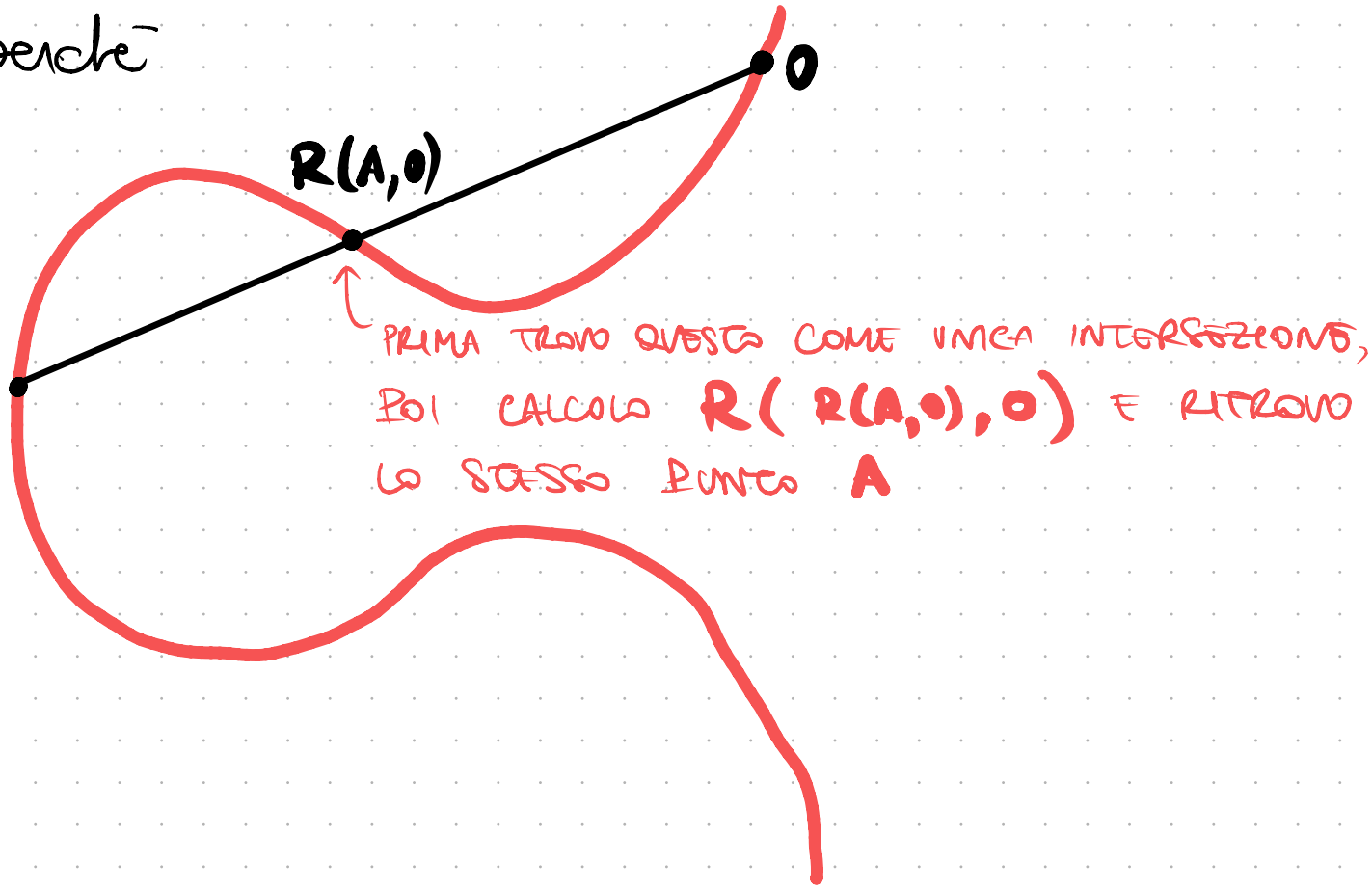
$$R(A+B,C) = R(A,B+C)$$

Proprio come volevasi dimostrare.

- **ELEMENTO NEUTRO 0**: Dobbiamo verificare che $\forall A \in \mathcal{C}$ si abbia $A + 0 = A$, ovvero che

$$R(R(A,0),0) = A$$

⚠ Si osservi che $R(0,0) = 0$ proprio perché **0 è FLESSO**



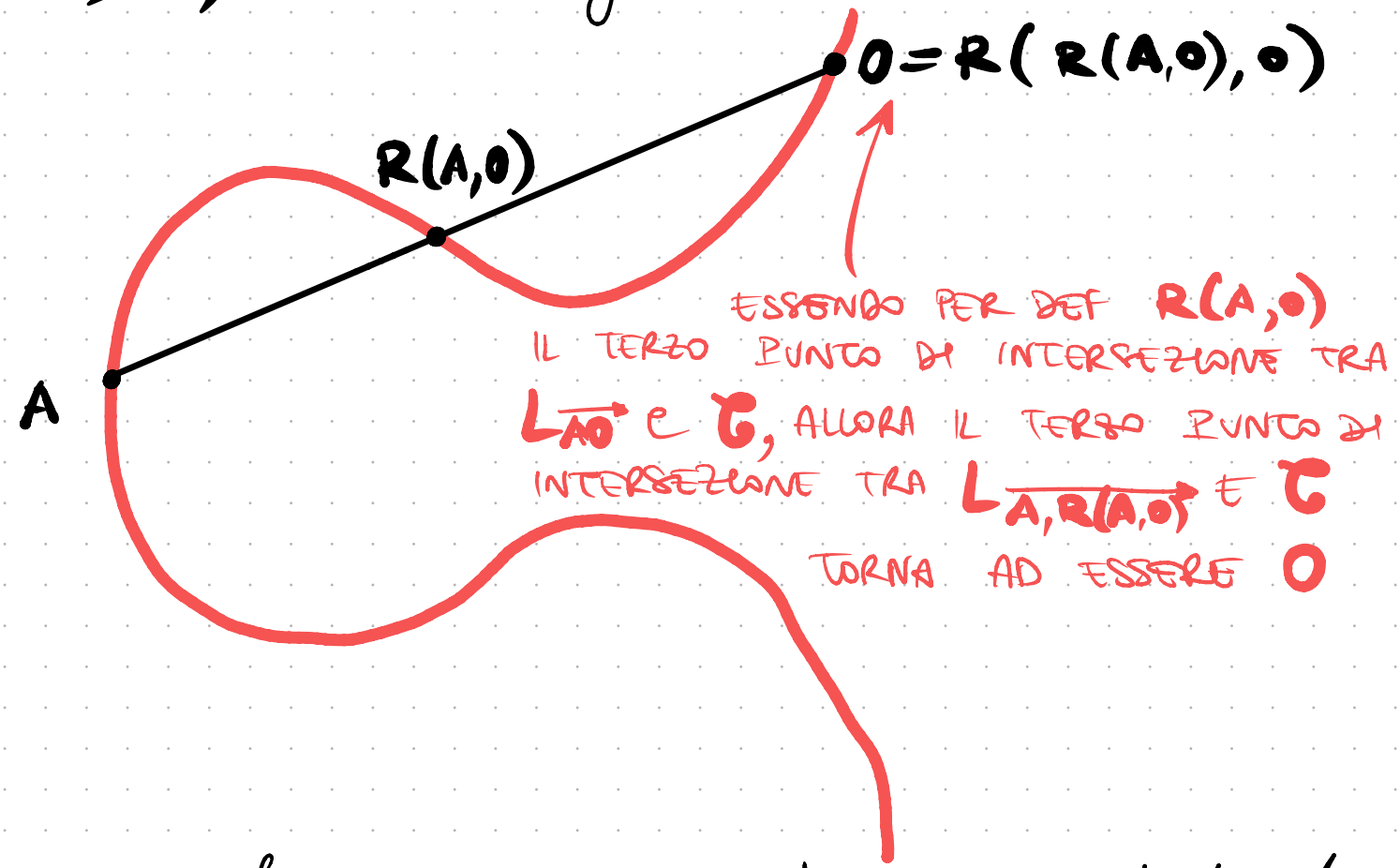
$R(R(A,0),0) = A$

Quindi $(\mathcal{C}, +, 0)$ si qualifica come MONOIDE COMMUTATIVO

- **ELEMENTO INVERSO**: $\forall A \in \mathcal{C}$ dobbiamo esibire un elemento $B \in \mathcal{C}$ tale che $A + B = O \wedge \underbrace{B + A = O}_{\text{automatica dalla commutatività}}$ ovvero che:

$$2(R(A, \exists B), O) = O$$

Scegliamo: $B := R(A, O)$



Allora $(\mathcal{C}, +, O)$ si qualifica come gruppo abeliano, concludendo la dimostrazione □

D: E se invece che il flesso O avessimo scelto un altro qualunque dei flessi O' di $\mathcal{C}$?

R: Otteniamo due gruppi abeliani:

$$(\mathcal{C}, +, O) \qquad (\mathcal{C}, +', O')$$

connessi dalla seguente relazione:

$$A +' B = A + B - O'$$

UN SEMPLICE SHIFT DATO DALL'INVERSO DELL'ALTRO FLESSO, È UN CAMBIO DI SISTEMI di RIFERIMENTO

Prop.: per esercizio.

COR Ogni curva ellittica ha 9 strutture di gruppo abeliano, tutte isomorfe l'una con l'altra.

~ Fine del

corso I.A.G. ~

Buono studio!