(*e*) Se una conica interseca la curva ellittica in tre punti tutti doppi (si dice che la conica è tritangente alla cubica), come sono disposti i tre punti residui?
(*f*) Dato un punto P su una curva ellittica, esistono, e quanti, punti Q tali che $Q+Q=P$ (cioè $2Q=P$, ovvero come si può dividere per due in una curva ellittica?).
(*g*) Dato un punto P su una curva ellittica, esistono, e quanti, punti Q tali che $Q+Q+Q=P$ (cioè $3Q=P$, ovvero come si può dividere per tre in una curva ellittica?).
(*h*) Dati tre punti allineati, come possono essere disposti tre punti i cui doppi siano i punti dati?
(*i*) Dato un punto P non appartenente alla curva ellittica, i sei punti di tangenza di tangenti spiccate da P stanno su una conica, ovvero sono di somma nulla.
(*i'*) Tre rette per un flesso hanno intersezioni residue su una conica?
(*l*) Esistono coniche esatangenti ad una curva ellittica, e come devono essere i punti di esatangenza?
(*m*) Esistono cubiche aventi tre flessi non allineati con tangenti concorrenti? Esistono cubiche aventi tre flessi allineati con tangenti concorrenti? (non c'entra nulla con la struttura di gruppo).

♠ **7.6.** Nozione di gruppo algebrico. In generale si può definire la nozione di "gruppo algebrico" nel modo seguente: si tratta di una varietà algebrica (luogo degli zeri di polinomi in uno spazio affine o proiettivo) con una struttura di gruppo tale che le mappe "somma" e "opposto" siano morfismi di varietà algebriche, che significa che si scriveranno come funzioni razionali delle coordinate in qualche (e allora ogni) scelta di un riferimento.

È un risultato fondamentale, ma fuori della portata degli strumenti di cui disponiamo, mostrare che le uniche curve algebriche (a meno di isomorfismi) su un corpo algebricamente chiuso che ammettono struttura di gruppo algebrico sono:
(1) la retta affine (con la struttura della somma del corpo), si indica con $\mathbb{G}_a$, o $\mathbb{G}_{a,K}$ se serve indicare il corpo, e si dice gruppo addittivo;
(2) il complementare dell'origine nella retta affine (con la struttura del prodotto del corpo), si indica con $\mathbb{G}_m$, o $\mathbb{G}_{m,K}$ se serve indicare il corpo, e si dice gruppo moltiplicativo; per vedere che si tratta di una curva affine, basta notare che è in biiezione con l'iperbole $XY=1$ del piano, tramite la proiezione sull'ascissa (si osservi che la legge di composizione diventa $\binom{x_1}{y_1}+\binom{x_2}{y_2}=\binom{x_1x_2}{y_1y_2}$ e l'opposto $-\binom{x}{y}=\binom{y}{x}$);
(3) le curve ellittiche; in particolare queste sono le uniche curve proiettive che ammettono una struttura di gruppo algebrico.

7.6.1. Altri esempi affini. Si determini una legge di gruppo sulla parabola affine (in forma canonica) copiando la legge addittiva del corpo K (tramite proiezione sull'ascissa). Si dovrebbe trovare che $-\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)=\left(\begin{smallmatrix}-x\\y\end{smallmatrix}\right)$ e $\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)+\left(\begin{smallmatrix}x'\\y'\end{smallmatrix}\right)=\left(\begin{smallmatrix}x+x'\\y+2xx'+y'\end{smallmatrix}\right)$.

7.6.2. Gruppi tòrti (twist). Consideriamo il cerchio reale $\mathbb{S}^1$ (curva affine di equazione $X^2+Y^2=1$) e dotiamolo della seguente operazione: $\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}x'\\y'\end{smallmatrix}\right)=\left(\begin{smallmatrix}xx'-yy'\\xy'+yx'\end{smallmatrix}\right)$. Si verifichi che si tratta di un gruppo algebrico, con elemento neutro $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ e inverso di $\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)$ dato da $\left(\begin{smallmatrix}y\\-x\end{smallmatrix}\right)$. Che relazioni vi sono tra $\mathbb{S}^1$ con questa struttura e $\mathbb{G}_{m,\mathbb{C}}$?

Più in generale, per ogni corpo K e ogni elemento non quadrato α di K (significa che $X^2-\alpha$ non ha soluzioni in K, e quindi K non è algebricamente chiuso) consideriamo la curva affine definita da $X^2-aY^2=1$, e dotiamola della seguente operazione: $\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}x'\\y'\end{smallmatrix}\right)=\left(\begin{smallmatrix}xx'+ayy'\\xy'+yx'\end{smallmatrix}\right)$. Si verifichi che si tratta di un gruppo algebrico.

Questi gruppi vengono indicati con $\mathbb{G}_{m,K}[a]$ e detti forme tòrte (twist) del gruppo moltiplicativo. In effetti, se usiamo il corpo $L=K[\sqrt{a}]$, allora l'operazione descritta sopra corrisponde a quella di $\mathbb{G}_{m,L}$ ristretta agli elementi di L di norma unitaria (se $\alpha+\beta\sqrt{a}$ è un generico elemento di L, allora la sua norma è l'elemento di K dato da $(\alpha+\beta\sqrt{a})(\alpha-\beta\sqrt{a})=\alpha^2-a\beta^2$). Si osservi che $\mathbb{S}^1$ è esattamente $\mathbb{G}_{m,\mathbb{R}}[-1]$.

Su corpi che non siano algebricamente chiusi, i gruppi affini di dimensione 1 si classificano in addittivo $\mathbb{G}_a$, motiplicativo $\mathbb{G}_m$ e forme twistate $\mathbb{G}_m[a]$ per $a\in K\smallsetminus K^2$.

7.6.3. Casi delle cubiche singolari. Ovviamente una curva algebrica, proiettiva o affine, che abbia struttura di gruppo algebrico, non può avere punti singolari; infatti visto che le traslazioni sono isomorfismi transitivi, se un punto fosse singolare lo sarebbero tutti.