Prop.: C cubica liscia, la legge di gruppo è associativa.

Dim.:
$$\begin{tikzcd} C\times C\times C \arrow[r] \arrow[rr, bend right, "f"] & C\times C \arrow[r] & C \end{tikzcd}$$
$(P,Q,R)\mapsto(P\oplus Q,R)\mapsto(P\oplus Q)\oplus R$, analogamente ho $(P,Q,R)\overset{g}{\longmapsto}P\oplus(Q\oplus R)$.

Voglio $f=g$.

Nota: all'inizio c'è un WLOG $\mathbb{K}=\overline{\mathbb{K}}$ a cui bisogna prestare attenzione, c'entra con la condizione di cubica liscia. Inoltre, vediamo il caso char $\mathbb{K}\neq 2,3$.

Sappiamo:
(a) $C\times C\times C$ irr. ($\Leftarrow C$ irr.)
(b) $f=g$ su un aperto $\emptyset\neq U\subset C\times C\times C$ (dal caso particolare dell'associatività che avevamo visto).

Vedremo: f e g morfismi, da cui la tesi.

È sufficiente mostrare che lo è la legge di gruppo.
$P\oplus Q=R(R(P,Q),O)$, allora basta R morfismo.

Fisso O un flesso e metto (C,O) in forma di Weierstrass:
$C=\{y^2=x^3+ax+b\}=\{G(x,y)=0\}$. $Q_1=(x_1,y_1)$, $Q_2=(x_2,y_2)\in C$.
$L(P,Q)$: $y=y_1+\alpha(x-x_1)$, $\alpha=\frac{y_2-y_1}{x_2-x_1}$, $x_2\neq x_1$.
$(y_1+\alpha(x-x_1))^2=x^3+ax+b\overset{=p(x)}{\Longrightarrow}\alpha^2=x_1+x_2+x_3$, $R(Q_1,Q_2)=(x_3,y_3)$.
$x_3=\alpha^2-x_1-x_2$ è funzione regolare di x_1,x_2,y_1,y_2 e y_3 pure usando l'equazione della retta.

$$\begin{matrix} y_1^2=x_1^3+ax_1+b \\ y_2^2=x_2^3+ax_2+b\end{matrix} \Rightarrow y_2^2-y_1^2=x_2^3-x_1^3+a(x_2-x_1)=(x_2-x_1)(x_2^2+x_1x_2+x_1^2+a)\Rightarrow$$
$\Rightarrow \alpha=\frac{y_2-y_1}{x_2-x_1}=\frac{x_2^2+x_1x_2+x_1^2+a}{y_2+y_1}$ per $x_2\neq x_1$, $y_2\neq -y_1$. Allora α è regolare su $\{x_2\neq x_1\}\cup\{y_2\neq -y_1\}$. E se $x_1=x_2$, $y_1=y_2\neq 0$?
$\alpha=\frac{3x_1^2+a}{2y_1}=\frac{p'(x_1)}{2y_1}=\frac{-\frac{\partial G}{\partial x}(Q_1)}{\frac{\partial G}{\partial y}(Q_1)}$, coefficiente angolare della retta tangente.

Se $Q_1=Q_2$ e $y_1\neq 0$, $R(Q_1,Q_1)$ è chi vogliamo.
Quindi abbiamo R morfismo su
$V_0=C\times C\setminus(\{(Q_1,Q_2)\mid Q_1\neq Q_2,\ O\in L(Q_1,Q_2)\}\cup\{(Q,Q)\mid T_QC\ni O\}\cup\{O\}\times C\cup C\times\{O\})$.
V_0 è aperto e al variare di O nell'insieme dei flessi $\{V_0\}$ è un ricoprimento di $C\times C$. □

Teo.: $X\subseteq\mathbb{P}^n$ chiuso, Y var. q.p.. $q: X\times Y\to Y$ è chiusa.

Dim.: (a) posso supporre Y affine. Infatti, scrivo $Y=\bigcup_i Y_i$, ↳aperti affini
$q_i: X\times Y_i\to Y_i$, $Z\subseteq X\times Y$ chiuso, $Z_i=Z\cap(X\times Y_i)$.
$q(Z)\cap Y_i=q_i(Z_i)$. Se so che $q_i(Z_i)$ è chiuso (caso affine), ho $q(Z)\cap Y_i$ chiuso $\Rightarrow q(Z)$ chiuso.
(b) Posso supporre $Y=\mathbb{A}^m$. Infatti, se $Y\subseteq\mathbb{A}^m$ chiuso e $Z\subseteq X\times Y$ è chiuso, allora Z è chiuso in $X\times\mathbb{A}^m$.
$$\begin{tikzcd} X\times Y \arrow[r, hook] \arrow[d, "q"] & X\times\mathbb{A}^m \arrow[d] \\ q(Z)\subseteq Y \arrow[r, hook] & \mathbb{A}^m \end{tikzcd}$$
(c) allo stesso modo, se $X\subseteq\mathbb{P}^n$ basta verificare l'enunciato su $\mathbb{P}^n\times\mathbb{A}^m$.

Sia $Z\subseteq\mathbb{P}^n_x\times\mathbb{A}^m_y$ chiuso. $Z=V(F_i(x,y), i\in I)$ dove
$F_i(x,y)\in\mathbb{K}[x_0,\dots,x_n,y_1,\dots,y_m]$ omogeneo nelle x.
$\bar{y}\in\mathbb{A}^m$ fissato, $I_{\bar y}=(F_i(x,\bar y))_{i\in I}\subseteq\mathbb{K}[x_0,\dots,x_n]$ ideale omogeneo.
$\mathbb{P}^n\supseteq V(I_{\bar y})=p(Z\cap(\mathbb{P}^n\times\{\bar y\}))\subseteq\mathbb{P}^n$.
$\bar y\in q(Z)\iff V(I_{\bar y})\neq\emptyset$.
NSS proiettivo: $V(I_{\bar y})=\emptyset\iff\sqrt{I_{\bar y}}\supseteq(x_0,\dots,x_n)\iff$
$\iff\exists d$ t.c. $\mathbb{K}[x_0,\dots,x_n]_d\subseteq I_{\bar y}\iff$
$\iff\exists d$ t.c. $\mathbb{K}[x_0,\dots,x_n]_d=(I_{\bar y})_d$.
Conclusione: $\bar y\in q(Z)\iff\forall d\ (I_{\bar y})_d\subsetneq\mathbb{K}[x_0,\dots,x_n]_d$.
Fisso d e fisso una base di monomi per $\mathbb{K}[x_0,\dots,x_n]_d$. finito, si usa la Segre
Generatori di $(I_{\bar y})_d$: se $d_i=\deg_x F_i(x,y)$,
$(I_{\bar y})_d$ è generata dai pol. del tipo $x^j F_i(x,\bar y)$ al variare di $i\in I$ e j multiindice t.c. $|j|=d-d_i$.
Metto le coordinate di questi rispetto alla base di monomi in una matrice $M(y)$ con le entrate che sono pol. in $\bar y$.
$(I_{\bar y})_d\subsetneq\mathbb{K}[x_0,\dots,x_n]_d\overset{(*)_d}{\iff}\operatorname{rk}M(\bar y)<\binom{n+d}{d}$, condizione pol. in $\bar y$. $\bar y\in q(Z)\iff(*)_d$ è verificata $\forall d\in\mathbb{N}$.
Quindi $q(Z)$ è chiuso (intersezione di chiusi). □

Cor.: $X\subseteq\mathbb{P}^n$ chiuso, $f: X\to Y$ morfismo $\Rightarrow f(X)\subseteq Y$ è chiuso.

Dim.: $\underbrace{\Gamma_f}_{\text{chiuso}}\subseteq X\times Y\xrightarrow{q}Y\Rightarrow q(\Gamma_f)=f(X)$ chiuso. □

Def.: X è una varietà proiettiva se è chiuso in $\mathbb{P}^n$.

Cor.: X proiettiva e connessa, $\varphi: X\to\mathbb{K}$ regolare $\Rightarrow\varphi$ costante.

Dim.:
$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[rr, bend right, "\bar\varphi"] & \mathbb{K}=\mathbb{A}^1 \arrow[r, hook] & \mathbb{P}^1 \end{tikzcd}$$
$\bar\varphi$ morfismo, $\infty\notin\operatorname{Im}\bar\varphi$,
$\operatorname{Im}\bar\varphi\subseteq\mathbb{A}^1$ è chiuso e connesso $\Rightarrow$ è un pto. □

Cor.: X varietà affine e proiettiva $\Rightarrow X$ è un insieme finito.

Dim.: decompongo $X=X_1\cup\dots\cup X_k$ con X_i irr. Se $\exists\, p\neq q\in X_1$, $\exists\varphi: X\to\mathbb{K}$ reg. t.c. $\varphi(p)\neq\varphi(q)$ (le funzioni separano i pti nelle varietà affini) $\Rightarrow\varphi|_{X_1}$ è regolare e non costante, assurdo perché X_1 irr. $\Rightarrow X_1$ connessa, ed essendo chiuso in X è proiettiva. □