e

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

(cioè $\ominus \bigoplus P_i$ è l'ulteriore zero delle funzioni in $\mathscr{L}((n{+}1)O - \sum P_i)$).

In particolare: la somma (nel senso dell'operazione di gruppo di $\mathscr{C}$) dei punti di intersezione di $\mathscr{C}$ con una qualsiasi curva del piano è nulla.

9.2.4. Come verificare che la legge di gruppo definita tramite i divisori è la stessa che abbiamo definito con la costruzione geometrica delle intersezioni con rette nel caso di una curva piana? È facile osservando che lo spazio $\mathscr{L}(3O - P - Q)$ dev'essere generato da una funzione razionale avente esattamente 3 zeri sulla curva ellittica, che è di grado 3 nel piano, e quindi deve corrispondere alla equazione di una retta...

9.2.5. Punti notevoli. Consideriamo la legge di gruppo di Poincaré su una curva ellittica piana $\mathscr{E}$, scegliendo un flesso come elemento neutro O.

(1) Un divisore $P_1 + \cdots + P_{3n}$ è divisore di intersezione di $\mathscr{E}$ con una curva $\mathscr{C}$ di grado n se e solo se risulta $P_1 \oplus \cdots \oplus P_{3n} = O$ (infatti questo è equivalente a $P_1 + \cdots + P_{3n} \sim 3nO$, che è divisore di intersezione di $\mathscr{E}$ con la n-esima potenza della sua tangente in O).

(2) Punti di 2-torsione: dal punto O vi sono tre rette tangenti a $\mathscr{E}$ non in O (la tangente in O è (non) contata tre volte), e i tre punti di tangenza $O_1, O_2, O_3 \in \mathscr{E}$ sono gli unici punti tali che $2O_i \oplus O = O$, cioè $2O_i = O$, o anche $O_i = \ominus O_i$. Dunque vi sono quattro punti di 2-torsione, e sono dati dalle intersezioni residue con $\mathscr{E}$ delle tangenti spiccate da O.
Siccome abbiamo che $O_1 \oplus O_2$ è di 2-torsione, e non è nessuno tra O, O_1, O_2, deve risultare $O_1 \oplus O_2 = O_3$ cioè $O_1 \oplus O_2 \oplus O_3 = O$, e i tre punti risultano allineati, come già comunque sapevamo.

(3) Consideriamo ora un punto P qualsiasi si $\mathscr{E}$; vi sono quattro tangenti ad $\mathscr{E}$ spiccate da P (la tangente in P viene (non) contata due volte), e diciamo P_0, P_1, P_2, P_3 i quattro punti di tangenza. Per ciascuno risulta $2P_i \oplus P = O$, cioè $2P_i = \ominus P$ e da questo sono caratterizzati. Siccome anche i punti $P_0 \oplus O_i$ hanno questa proprietà, deve essere (a meno di cambiare gli indici) che $P_i = P_0 \oplus O_i$ per $i = 1, 2, 3$.
Inoltre si calcola subito che

$$P_0 \oplus P_1 \oplus P_2 \oplus P_3 = 4P_0 \oplus O_1 \oplus O_2 \oplus O_3 = 4P_0 = \ominus 2P$$

cioè $P_0 \oplus P_1 \oplus P_2 \oplus P_3 \oplus 2P = O$, e quindi esiste una conica per i punti P_i tangente alla cubica in P.
Si osservi inoltre che per $\{i, j, k, l\} = \{0, 1, 2, 3\}$ si ha che le rette $P_i \vee P_j$ e $P_k \vee P_l$ si incontrano in $\mathscr{E}$, perché per esempio $P_0 \oplus P_1 = 2P_0 \oplus O_1 = P_2 \oplus P_3$, e dunque $\ominus(P_0 \oplus P_1)$ (intersezione residua di $P_0 \vee P_1$ con $\mathscr{E}$) coincide con $\ominus(P_2 \oplus P_3)$ (intersezione residua di $P_2 \vee P_3$ con $\mathscr{E}$) ed è il punto $\ominus(2P_0 \oplus O_1) = P \oplus O_1$, che appartiene alla curva $\mathscr{E}$.

(4) Punti di quattro torsione: sono i punti Z per cui $4Z = O$. Naturalmente $2Z$ dev'essere un punto di 2-torsione, e quindi ogni O_i determina (altri) quattro punti di 4-torsione, che sono proprio le intersezioni residue delle tangenti a $\mathscr{E}$ da O_i. In tutto vi sono 16 punti di 4-torsione. Si provi a scrivere una tabellina dei punti di 4-torsione, del tipo

$$\begin{array}{cccc} O & P_1 & P_2 & P_1 \oplus P_2 \\ O_1 & \ominus P_1 & P_2 \oplus O_1 & ??? \\ O_2 & P_1 \oplus O_2 & \ominus P_2 & \ominus ??? \\ O_3 & P_1 \oplus O_3 & P_2 \oplus O_3 & \ominus(P_1 \oplus P_2) \end{array}$$

e a capirne le posizioni geometriche sulla curva (allineamenti? coniche?).

(5) Punti di tre torsione: sono i punti Z per cui $3Z = O$, cioè $2Z = \ominus Z$; come si vede, ma lo sapevamo già, sono tutti e soli i flessi di $\mathscr{E}$, che sono 9.
Si osservi che se A, B son punti di tre torsione, allora anche $\ominus(A \oplus B)$ lo è: questo ci conferma che ogni retta per due flessi ne contiene un altro.
Detti U e V due flessi diversi da O e $U \neq U, \ominus U$, possiamo elencare i flessi nella tabellina seguente:

$$\begin{array}{ccc} O & U & \ominus U \\ V & U \oplus V & V \ominus U \\ \ominus V & U \ominus V & \ominus U \ominus V \end{array}$$

(quali sono quelli allineati?).