Exercise sheet on isogenies

(1) Let $\phi\colon E_1 \to E_2, \psi\colon E_2 \to E_3$ be two isogenies of elliptic curves. Show that:
  (a) $\psi \circ \phi\colon E_1 \to E_3$ is an isogeny;
  (b) $\deg(\psi \circ \phi) = \deg \psi \cdot \deg \phi$.

(2) Let $\phi\colon E_1 \to E_2$ be an isogeny of elliptic curves. Show that, for every $P, Q \in E_1$, one has $\phi(P+Q) = \phi(P) + \phi(Q)$.

(3) Let E be an elliptic curve over a field K. Show that
  (a) for every $n \in \mathbb{Z} \setminus \{0\}$, the isogeny $[n] \in End(E)$ has degree n^2;
  (b) $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$;
  (c) the characteristic of $\mathrm{End}(E)$ is 0;
  (d) there are no zero-divisors in $\mathrm{End}(E)$.

(4) Let $\phi\colon E_1 \to E_2$ be an isogeny of elliptic curves, and let $\hat{\phi}$ be its dual. Show that:
  (a) $\deg \phi = \deg \hat{\phi}$;
  (b) $\hat{\hat{\phi}} = \phi$

(5) (Harder) Let $E/\mathbb{F}_q$ be an elliptic curve over the finite field with q elements, and let

$$F_q\colon E \to E, (x,y) \mapsto (x^q, y^q)$$

the the q-th Frobenius. Show that
  (a) $\deg F_q = q$;
  (b) $F_q^2 - [a_q]F_q + [q] = [0] \in \mathrm{End}(E)$, where $a_q := q + 1 - \#E(K)$.
  (c) $\hat{F_q} = [a_q] - F_q$.

(6) Compute Vélu isogeny for the following couples $(E/K, G)$, where E is an elliptic curve over K and G a finite subgroup of $E(\overline{K})$.
  (a) $E\colon y^2 = x^3 + x \,/\, \mathbb{F}_{431}$ and $G = \{O, (0,0)\}$.
  (b) $E\colon y^2 = x^3 + x \,/\, \mathbb{C}$ and $G = \{O, (0,0)\}$.
  (c) $E\colon y^2 = x^3 - x \,/\, \mathbb{C}$ and $G = \{O, (0,0)\}$.
  (d) $E\colon y^2 = x^3 - x \,/\, \mathbb{C}$ and $G = \{O, (1,0)\}$.
  (e) $E\colon y^2 = x^3 - x \,/\, \mathbb{C}$ and $G = \{O, (-1,0)\}$.
  (f) $E\colon y^2 = x^3 - x \,/\, \mathbb{C}$ and $G = \{O, (0,0), (-1,0), (1,0)\}$.

(7) Let m and d denote the month and the day of your birthday, respectively. Define $E\colon y^2 = x^3 \pm mx \pm d$. Check that E si an elliptic curve and then compute $\mathrm{End}(E)$. [Hint: compute $j(E)$; is it algebraic over $\mathbb{Q}$?]