MAT 562 - Examen - 13 mars 2023 - 3 heures

Exercice 1

1) On écrit $F = \prod_i F_i^{r_i}$ avec les F_i irréductibles et $r_i > 0$. On a alors $V_p(F) = \bigcup_i V_p(F_i)$, et donc :

$$V_p(F) \smallsetminus V_p(G) = \bigcup_i (V_p(F_i) \smallsetminus V_p(G)).$$

Pour chaque i, la variété $V_p(F_i)$ est irréductible et le sous-ensemble $V_p(F_i) \smallsetminus V_p(G)$ est un ouvert de $V_p(F_i)$. Du coup, $V_p(F_i) \smallsetminus V_p(G)$ est soit vide, soit dense dans $V_p(F_i)$. Pour conclure, il ne nous reste donc plus qu'à montrer qu'aucun des $V_p(F_i) \smallsetminus V_p(G)$ n'est vide.

Par l'absurde, supposons que $V_p(F_i) \smallsetminus V_p(G)$ soit vide pour un certain i. Cela implique que $V_p(F_i) \subset V_p(G)$. Par le théorème des zéros, $G \in \sqrt{(F_i)} = (F_i)$, ce qui contredit l'hypothèse que F et G sont premiers entre eux.

2) a) Ecrivons :

$$\begin{aligned}(X_0S + X_1T + X_2)(X_3S + X_4T + X_5) \\ = X_0X_3S^2 + X_1X_4T^2 + (X_0X_4 + X_1X_3)ST + \\ (X_0X_5 + X_2X_3)X + (X_1X_5 + X_2X_4)T + X_2X_5, \quad (1)\end{aligned}$$

puis définissons :

$$\begin{aligned}f : \mathbb{P}^5_k &\to \mathbb{P}^5_k \\ x &\mapsto [x_0x_3 : x_1x_4 : x_0x_4 + x_1x_3 : x_0x_5 + x_2x_3 : x_1x_5 + x_2x_4 : x_2x_5]\end{aligned}$$

et $U := \mathbb{P}^5_k \smallsetminus (V_p(X_0, X_1) \cup V_p(X_3, X_4))$. L'égalité (1) montre immédiatement que f est définie sur U et que $f(U) = Z$.

b) Comme U est un ouvert non vide de $\mathbb{P}^5_k$, il est irréductible. Mais l'application f est continue sur U. On en déduit que $Z = f(U)$ est irréductible.

3) a) On a :

$$Z \cap V_p(X_1, X_2, X_4, X_5) = V_p(X_1, X_2, X_4, X_5) \smallsetminus \{[0 : 0 : 0 : 1 : 0 : 0]\}.$$

On déduit que $Z \cap V_p(X_1, X_2, X_4, X_5)$ n'est pas fermé dans $\mathbb{P}^5_k$ et donc Z non plus.

b) i) Soit $A = [0 : 0 : x_2 : x_3 : x_4 : x_5] \in V_p(X_0, X_1)$. On a :

$$\begin{aligned} A \in Z &\Leftrightarrow x_2ST + x_3S + x_4T + x_5 \text{ n'est ni constant ni irréductible} \\ &\Leftrightarrow x_2 \neq 0 \text{ et } \exists a, b \in k,\ ST + \frac{x_3}{x_2}S + \frac{x_4}{x_2}T + \frac{x_5}{x_2} = (S+a)(T+b) \\ &\Leftrightarrow x_2 \neq 0 \text{ et } \exists a, b \in k,\ \frac{x_3}{x_2} = b, \frac{x_4}{x_2} = a, \frac{x_5}{x_2} = ab \\ &\Leftrightarrow x_2 \neq 0 \text{ et } x_3x_4 = x_5x_2 \\ &\Leftrightarrow A \in (V_p(F) \smallsetminus V_p(X_2)) \end{aligned}$$

avec $F = X_3X_4 - X_5X_2$.

ii) On a $x_2^2 \neq 4x_0x_1$ et $x_0 \neq 0$. On peut donc factoriser :

$$x_0S^2 + x_1T^2 + x_2ST = x_0\,(S - \alpha_1 T)\,(S - \alpha_2 T)$$

avec :

$$\alpha_1 = \frac{-x_2 + \sqrt{x_2^2 - 4x_0x_1}}{2x_0}, \qquad \alpha_1 = \frac{-x_2 - \sqrt{x_2^2 - 4x_0x_1}}{2x_0}.$$

On a du coup :

$$\begin{aligned} \pi_A = x_0\,(S + \alpha_1 T)\,(S - \alpha_2 T) + \frac{-\alpha_2 x_3 - x_4}{\alpha_1 - \alpha_2}\,(S + \alpha_1 T) \\ + \frac{\alpha_1 x_3 + x_4}{\alpha_1 - \alpha_2}\,(S - \alpha_2 T) + x_5. \end{aligned}$$

On en déduit que $V(\pi_A) \cong V(\pi_B)$ avec :

$$B = \left[0 : 0 : x_0 : \frac{-\alpha_2 x_3 - x_4}{\alpha_1 - \alpha_2} : \frac{\alpha_1 x_3 + x_4}{\alpha_1 - \alpha_2} : x_5\right].$$

iii) Des questions a) et b) on déduit que :

$$\begin{aligned} &Z \smallsetminus V_p(X_0(X_2^2 - 4X_0X_1)) \\ &= \{x \in \mathbb{P}_k^5 : x_2^2 \neq 4x_0x_1, x_0 \neq 0, \frac{-\alpha_2 x_3 - x_4}{\alpha_1 - \alpha_2}\frac{\alpha_1 x_3 + x_4}{\alpha_1 - \alpha_2} = x_0x_5\} \\ &= \{x \in \mathbb{P}_k^5 : x_2^2 \neq 4x_0x_1, x_0 \neq 0, \frac{-(x_4^2 - \frac{x_2}{x_0}x_3x_4 + \frac{x_1}{x_0}x_3^2)}{\frac{x_2^2 - 4x_0x_1}{x_0^2}} = x_0x_5\} \\ &= V_p(G) \smallsetminus V_p(X_0(X_2^2 - 4X_0X_1)) \end{aligned}$$

avec $G = X_5(X_2^2 - 4X_0X_1) + X_4^2X_0 - X_2X_3X_4 + X_1X_3^2$. Par la question 1), on déduit que l'adhérence de $Z \smallsetminus V_p(X_0(X_2^2 - 4X_0X_1))$ est :

$$V_p(X_5(X_2^2 - 4X_0X_1) + X_4^2X_0 - X_2X_3X_4 + X_1X_3^2).$$

Mais $Z \smallsetminus V_p(X_0(X_2^2 - 4X_0X_1))$ est un ouvert non vide de Z et Z est irréductible. Donc les adhérences de Z et de $Z \smallsetminus V_p(X_0(X_2^2 - 4X_0X_1))$ coïncident. On conclut que :

$$\overline{Z} = V_p(X_5(X_2^2 - 4X_0X_1) + X_4^2X_0 - X_2X_3X_4 + X_1X_3^2).$$

c) On a $\dim \overline{Z} = 4$ et :

$$\begin{aligned} Z_1^{\text{sing}} &= V_p(X_4^2 - 4X_1X_5, X_3^2 - 4X_0X_5, 2X_2X_5 - X_3X_4, 2X_1X_3 - X_2X_4, \\ &\qquad 2X_0X_4 - X_2X_3, X_2^2 - 4X_0X_1, G) \\ &= V_p(X_4^2 - 4X_1X_5, X_3^2 - 4X_0X_5, 2X_2X_5 - X_3X_4, X_2^2 - 4X_0X_1). \end{aligned}$$

Les points dans $V_p(X_4^2 - 4X_1X_5, X_3^2 - 4X_0X_5, X_2^2 - 4X_0X_1)$ sont ceux de la forme $[y_0^2 : y_1^2 : 2\varepsilon_2 y_0y_1 : 2\varepsilon_3 y_0y_5 : 2\varepsilon_4 y_1y_5 : y_5^2]$ avec $\varepsilon_2, \varepsilon_3, \varepsilon_4 \in \{\pm 1\}$. Un tel point est dans $V_p(X_4^2 - 4X_1X_5, X_3^2 - 4X_0X_5, 2X_2X_5 - X_3X_4, X_2^2 - 4X_0X_1)$ si, et seulement si :

$$4\varepsilon_2 y_0y_1y_5^2 = 4\varepsilon_3\varepsilon_4 y_0y_1y_5^2.$$

Exercice 2

1) Supposons que Δ et Δ' soient parallèles. La relation $P_1 + P_2 = P_1' + P_2' \neq O$ implique que $P_1 \star P_2 = P_1' \star P_2' \neq O$. Du coup, $\Delta \cap \Delta' \neq \emptyset$. Comme Δ et Δ' sont parallèles, on déduit que $\Delta = \Delta'$. En particulier, on a l'égalité :

$$(P_1) + (P_2) + (P_1 \star P_2) = (P_1') + (P_2') + (P_1' \star P_2').$$

En réutilisant l'égalité $P_1 \star P_2 = P_1' \star P_2'$, on déduit que :

$$(P_1) + (P_2) = (P_1') + (P_2'),$$

et donc que $\{P_1, P_2\} = \{P_1', P_2'\}$. La réciproque est évidente.

2) a) On a, pour $\omega \in \Lambda \smallsetminus \{0\}$ et $z \neq \omega$:

$$\left| \frac{1}{z - \omega} + \frac{z}{\omega^2} + \frac{1}{\omega} \right| = \left| \frac{z^2}{(z - \omega)\omega^2} \right|.$$

Du coup, la série :

$$\zeta(z) = \frac{1}{z} + \sum_{\omega \in \Lambda \smallsetminus \{0\}} \left(\frac{1}{z-\omega} + \frac{z}{\omega^2} + \frac{1}{\omega} \right).$$

converge normalement sur tout compact de $\mathbb{C} \smallsetminus \Lambda$. En particulier, c'est une fonction holomorphe sur $\mathbb{C} \smallsetminus \Lambda$ telle que :

$$\forall z \in \mathbb{C} \smallsetminus \Lambda, \;\; \zeta'(z) = -\wp(z).$$

Comme :

$$\begin{aligned} \zeta(-z) &= -\frac{1}{z} + \sum_{\omega \in \Lambda \smallsetminus \{0\}} \left(\frac{1}{z+\omega} - \frac{z}{\omega^2} - \frac{1}{\omega} \right) \\ &= -\frac{1}{z} - \sum_{\omega \in \Lambda \smallsetminus \{0\}} \left(\frac{1}{z-\omega} + \frac{z}{\omega^2} + \frac{1}{\omega} \right) = -\zeta(z), \end{aligned}$$

la fonction ζ est impaire. Comme la série

$$\sum_{\omega \in \Lambda \smallsetminus \{0\}} \left(\frac{1}{z-\omega} + \frac{z}{\omega^2} + \frac{1}{\omega} \right)$$

converge normalement sur un voisinage de 0, la fonction ζ est méromorphe au voisinage de 0 (avec un pôle d'ordre 1 en 0). Pour $\omega_0 \in \Lambda \smallsetminus \{0\}$, comme la série

$$\sum_{\omega \in \Lambda \smallsetminus \{0, \omega_0\}} \left(\frac{1}{z-\omega} + \frac{z}{\omega^2} + \frac{1}{\omega} \right)$$

converge normalement sur un voisinage de ω_0, la fonction ζ est méromorphe au voisinage de ω_0 (avec un pôle d'ordre 1 en ω_0). Cela établit la méromorphicité de ζ sur $\mathbb{C}$.

On notera que la fonction ζ ne peut pas être Λ-elliptique puisqu'elle serait alors de degré 1.

b) La fonction $\wp$ étant Λ-elliptique, il en est de même de la fonction φ. Montrons que ψ est Λ-elliptique. Pour ce faire, on observe que, pour $\omega \in \Lambda$ et $z \in \mathbb{C} \smallsetminus \Lambda$:

$$\zeta'(z+\omega) = -\wp(z+\omega) = -\wp(z) = \zeta'(z).$$

Comme $\mathbb{C} \smallsetminus \Lambda$ est connexe, on déduit qu'il existe une constante $C(\omega)$ telle que, pour $z \in \mathbb{C} \smallsetminus \Lambda$:

$$\zeta(z+\omega) = \zeta(z) + C(\omega).$$

En particulier, on a $\psi(z+\omega) = \psi(z)$ pour $z \in \mathbb{C} \smallsetminus (\Lambda \cup (-y_0 + \Lambda))$. La fonction ψ est donc Λ-elliptique.

c) On commence par étudier les pôles de φ et ψ.

- Les pôles de φ sont contenus dans $\Lambda \cup (y_0 + \Lambda) \cup (-y_0 + \Lambda)$. Au voisinage de 0 :

$$\varphi(z) = \frac{1}{2}\frac{-2/z^3}{1/z^2} + O(1) = -\frac{1}{z} + O(1),$$

au voisinage de y_0 :

$$\varphi(z) = \frac{1}{2}\frac{\wp''(y_0)(z-y_0) + O((z-y_0)^2)}{\wp'(y_0)(z-y_0) + O((z-y_0)^2)} = O(1)$$

(puisque $\wp'$ ne s'annule pas en y_0), et au voisinage de $-y_0$:

$$\varphi(z) = \frac{1}{2}\frac{-2\wp'(y_0)}{-\wp'(y_0)(z+y_0)} + O(1) = \frac{1}{z+y_0} + O(1).$$

- Les pôles de ψ sont contenus dans $\Lambda \cup (-y_0 + \Lambda)$. Au voisinage de 0 :

$$\psi(z) = \zeta(y_0) - \frac{1}{z} - \zeta(y_0) + O(1) = -\frac{1}{z} + O(1),$$

et au voisinage de $-y_0$:

$$\psi(z) = \frac{1}{z+y_0} - \zeta(-y_0) - \zeta(y_0) + O(1) = \frac{1}{z+y_0} + O(1).$$

On déduit que ρ n'a pas de pôles et est donc holomorphe sur le plan complexe.

d) La fonction ρ est Λ-elliptique et holomorphe sur $\mathbb{C}$. Elle est donc constante. De plus, au voisinage de 0 :

$$\varphi(z) = \frac{1}{2}\frac{-2/z^3 - \wp'(y_0) + o(1)}{1/z^2 + o(1)} = -\frac{1}{z} + o(1),$$
$$\psi(z) = -\frac{1}{z} + o(1),$$

de sorte que $\rho(0) = 0$. On déduit que ρ est la fonction nulle, et donc que :

$$\frac{1}{2} \cdot \frac{\wp'(z) - \wp'(y)}{\wp(z) - \wp(y)} = \zeta(z+y) - \zeta(z) - \zeta(y)$$

pour tous $y \in \mathbb{C} \setminus \frac{1}{2}\Lambda, z \in \mathbb{C} \setminus \Lambda$ tels que $z \pm y \in \mathbb{C} \setminus \Lambda$. Par continuité, l'égalité reste vraie lorsque $y \in \frac{1}{2}\Lambda$.

3) On suppose d'abord que $z_1 - z_2 \notin \Lambda$ et $z_3 - z_4 \notin \Lambda$. On a :

$$\zeta(z_1 + z_2) - \zeta(z_1) - \zeta(z_2) = \zeta(z_1' + z_2') - \zeta(z_1') - \zeta(z_2').$$

Donc, par la question 2) :

$$\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)} = \frac{\wp'(z_2') - \wp'(z_1')}{\wp(z_2') - \wp(z_1')}.$$

Or $\frac{\wp'(z_2)-\wp'(z_1)}{\wp(z_2)-\wp(z_1)}$ (resp. $\frac{\wp'(z_2')-\wp'(z_1')}{\wp(z_2')-\wp(z_1')}$) est la pente de la droite passant par les points $\psi_\Lambda(z_1)$ et $\psi_\Lambda(z_2)$ (resp. $\psi_\Lambda(z_1')$ et $\psi_\Lambda(z_2')$) de la courbe elliptique E_Λ. Par la question 1), on déduit que $\{z_1, z_2\} = \{z_1', z_2'\}$.
On ne fait plus d'hypothèses sur z_1, z_2, z_1', z_2'. On considère des suites $(y_n)_n$ et $(y_n')_n$ qui convergent respectivement vers z_2 et z_2' et telles que, pour tout n :

(i) les nombres complexes $z_1 \pm y_n$ et $z_1' \pm y_n'$ ne sont pas dans Λ ;

(ii) $z_1 + y_n = z_1' + y_n'$.

On a alors :

$$\begin{aligned}
0 &= \zeta(z_1) + \zeta(z_2) - \zeta(z_1') - \zeta(z_2') \\
&= \lim_{n\to\infty} (\zeta(z_1) + \zeta(y_n) - \zeta(z_1') - \zeta(y_n')) \\
&= \lim_{n\to\infty} (-\zeta(z_1 + y_n) + \zeta(z_1) + \zeta(y_n) + \zeta(z_1' + y_n') - \zeta(z_1') - \zeta(y_n')) \\
&= -\frac{1}{2} \lim_{n\to\infty} \left(\frac{\wp'(y_n) - \wp'(z_1)}{\wp(y_n) - \wp(z_1)} - \frac{\wp'(y_n') - \wp'(z_1')}{\wp(y_n') - \wp(z_1')} \right).
\end{aligned}$$

En introduisant les droites :

$$\Delta := \begin{cases} \text{droite passant par } \psi_\Lambda(z_1) \text{ et } \psi_\Lambda(z_2) \text{ si } \psi_\Lambda(z_1) \neq \psi_\Lambda(z_2) \\ \text{droite tangente à } \psi_\Lambda(z_1) \text{ si } \psi_\Lambda(z_1) = \psi_\Lambda(z_2), \end{cases}$$

$$\Delta' := \begin{cases} \text{droite passant par } \psi_\Lambda(z_1') \text{ et } \psi_\Lambda(z_2') \text{ si } \psi_\Lambda(z_1') \neq \psi_\Lambda(z_2') \\ \text{droite tangente à } \psi_\Lambda(z_1') \text{ si } \psi_\Lambda(z_1') = \psi_\Lambda(z_2'), \end{cases}$$

on voit que la suite $\left(\frac{\wp'(y_n)-\wp'(z_1)}{\wp(y_n)-\wp(z_1)}\right)_n$ converge vers la pente de Δ et $\left(\frac{\wp'(y_n')-\wp'(z_1')}{\wp(y_n')-\wp(z_1')}\right)_n$ converge vers la pente de Δ'. Du coup, par la question 1), on a $\{z_1, z_2\} = \{z_1', z_2'\}$.

Exercice 3

1) La courbe E est une courbe elliptique si, et seulement si, $\mathrm{car}(k) \notin \{2, 3\}$.

2) a) Les points de 2 torsion sont :

$$[0:1:0], [\rho:0:1], [\zeta\rho:0:1], [\zeta^2\rho:0:1]$$

où ρ est une racine cubique de -3 dans $\overline{k}$ et ζ est une racine cubique primitive de l'unité.

b) Un point $P = [x:y:z] \neq [0:1:0]$ est de 3-torsion si, et seulement si, $2P = -P$. Avec la formule de duplication, cela équivaut à :

$$\frac{x^4 - 24x}{4(x^3+3)} = x,$$

c'est-à-dire :

$$x^4 + 12x = 0.$$

Les points de 3-torsion sont donc :

$$[0:1:0], [0:\sqrt{3}:1], [0:-\sqrt{3}:1], [\omega:3\sqrt{-1}:1], [\omega:-3\sqrt{-1}:1],$$
$$[\zeta\omega:3\sqrt{-1}:1], [\zeta\omega:-3\sqrt{-1}:1], [\zeta^2\omega:3\sqrt{-1}:1], [\zeta^2\omega:-3\sqrt{-1}:1],$$

où ζ est une racine cubique primitive de l'unité et ω est une racine cubique de -12.

3) On a $E(\mathbb{F}_5) = \{[0:1:0], (1,2), (1,3), (2,1), (2,4), (3,0)\}$. Donc $E(\mathbb{F}_5) \cong \mathbb{Z}/6\mathbb{Z}$. Il existe de plus $\alpha, \beta \in \mathbb{C}$ tels que $\alpha\beta = 5$ et $|E(\mathbb{F}_{5^n})| = 5^n + 1 - \alpha^n - \beta^n$ pour tout n. On en déduit que :

$$\alpha + \beta = 5 + 1 - |E(\mathbb{F}_5)| = 6 - 6 = 0,$$
$$\alpha^2 + \beta^2 = (\alpha+\beta)^2 - 2\alpha\beta = -10,$$
$$\alpha^3 + \beta^3 = (\alpha+\beta)(\alpha^2 + \beta^2 - \alpha\beta) = 0,$$
$$|E(\mathbb{F}_{25})| = 25 + 1 + 10 = 36,$$
$$|E(\mathbb{F}_{125})| = 125 + 1 = 126.$$

Le corps $\mathbb{F}_{25}$ contient une racine cubique de -3, une racine primitive cubique de l'unité, les racines carrées de 3 et de -1, et une racine cubique de -12. Du coup, la question 2) montre que $E(\mathbb{F}_{25})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ et $E(\mathbb{F}_{25})[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$. On déduit que $E(\mathbb{F}_{25}) \cong (\mathbb{Z}/6\mathbb{Z})^2$.

Le corps $\mathbb{F}_{125}$ contient les racines carrées de -1 et une racine cubique de -12, mais pas les racines carrées de 3, ni les racines primitives cubiques de l'unité. Du coup, la question 2) montre que $E(\mathbb{F}_{125})[3] \cong \mathbb{Z}/9\mathbb{Z}$. On déduit que $E(\mathbb{F}_{125}) \cong \mathbb{Z}/126\mathbb{Z}$.

4) a) i) On voit que $22P = -21P$, et donc que $43P = 0$. Comme 43 est premier, $r = 43$.

ii) Par la borne de Hasse, on a :

$$|E(\mathbb{F}_{31})| \leqslant 32 + 2\sqrt{31} < 44.$$

Mais 43 divise $|E(\mathbb{F}_{31})|$. Donc $|E(\mathbb{F}_{31})| = 43$ et P engendre bien $E(\mathbb{F}_{31})$.

b) i) La clé privée de Bulbizarre est 16 car $16P = P_b$.

ii) La clé secrète commune est $17P_b = 272P = 14P = (28, 21)$.

c) La clé secrète de Bulbizarre est 26 car $26P = -17P = (20, 25)$. Le message est $M_2 - 26M_1 = 24P + 17 \times 13P = 245P = 30P = -13P = (6, 8)$.

d) La clé secrète d'Arcanin est 7 car $Q = 7P$. On calcule :

$$z^{-1}m = \frac{16}{13} = 16 \times 10 = 160 = 31 \in \mathbb{Z}/43\mathbb{Z},$$
$$z^{-1}x_R = \frac{11}{13} = 11 \times 10 = 110 = 24 \in \mathbb{Z}/43\mathbb{Z},$$
$$z^{-1}mP + z^{-1}x_R Q = 31P + 24 \times 7P = 199P = 27P = (7, 6) \neq R.$$

Le message n'a donc pas été envoyé par Arcanin.

Exercice 4

1) On calcule le discriminant $\Delta = -4 \times 64^3 + 27 \times 16^2 = -2^8 \times 13 \times 313$. Comme $\Delta \neq 0$, la courbe E est bien une courbe elliptique.

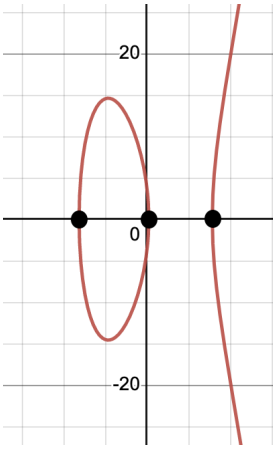
2) Les nombres premiers 3 et 5 ne divisent pas Δ. On calcule alors :

$$E(\mathbb{F}_3) = \{[0 : 1 : 0], (0, \pm 1), (1, \pm 1), (2, \pm 1)\},$$
$$E(\mathbb{F}_5) = \{[0 : 1 : 0], (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}.$$

En particulier, $|E(\mathbb{F}_3)| = 7$ et $|E(\mathbb{F}_5)| = 9$. Comme $E(\mathbb{Q})_{\text{tors}}$ s'injecte dans $E(\mathbb{F}_3)$ et $E(\mathbb{F}_5)$, on déduit que $E(\mathbb{Q})_{\text{tors}} = 0$. Par le théorème de Mordell, il existe $r \geqslant 0$ tel que $E(\mathbb{Q}) \cong \mathbb{Z}^r$. Comme $(0, 4) \in E(\mathbb{Q})$, on a $r \geqslant 1$.

3) Supposons que les points P_1, P_2, P_3 existent. Supposons par l'absurde que $r = 1$. Soit alors P_0 un générateur de $E(\mathbb{Q})$. On écrit $P_1 = n_1 P$, $P_2 = n_2 P$ et $P_3 = n_3 P$ avec $n_1, n_2, n_3 \in \mathbb{Z}$. Comme P_1, P_2, P_3 ne sont pas dans $2E(\mathbb{Q})$, les entiers n_1, n_2, n_3 sont tous impairs. Mais la relation $P_1 + P_2 + P_3 = O$ équivaut à $n_1 + n_2 + n_3 = 0$: absurde !

4) a)



b) L'étude des variations de la fonction $f : x \mapsto x^3 - 64x + 16$ montre qu'il existe $\alpha_1 < \alpha_2 < 1 < \alpha_3$ tels que :

(i) $f(\alpha_1) = f(\alpha_2) = f(\alpha_3) = 0$,

(ii) f est positive sur $[\alpha_1, \alpha_2] \cup [\alpha_3, +\infty[$,

(iii) f est négative ailleurs.

On pose alors :

$$C_0^+ := \{(x,y) \in E(\mathbb{R}) : x > 1, y > 0\} = \{(x, \sqrt{x^3 - 64x + 16}) : x \in [\alpha_3, +\infty[\},$$
$$C_0^- := \{(x,y) \in E(\mathbb{R}) : x > 1, y < 0\} = \{(x, -\sqrt{x^3 - 64x + 16}) : x \in [\alpha_3, +\infty[\},$$
$$C_1^+ := \{(x,y) \in E(\mathbb{R}) : x < 1, y > 0\} = \{(x, \sqrt{x^3 - 64x + 16}) : x \in [\alpha_1, \alpha_2]\},$$
$$C_1^- := \{(x,y) \in E(\mathbb{R}) : x < 1, y < 0\} = \{(x, -\sqrt{x^3 - 64x + 16}) : x \in [\alpha_1, \alpha_2]\}.$$

On a $E(\mathbb{R}) \setminus E[2] = C_0^+ \sqcup C_0^- \sqcup C_1^+ \sqcup C_1^-$. Comme la fonction $x \mapsto \sqrt{x^3 - 64x + 16}$ est continue sur $[\alpha_1, \alpha_2] \cup [\alpha_3, +\infty[$, les ensembles C_0^+, C_0^-, C_1^+ et C_1^- sont tous connexes. Ce sont donc les composantes connexes de $E(\mathbb{R}) \setminus E[2]$. Comme $\sqrt{x^3 - 64x + 16} \xrightarrow[x \to +\infty]{} +\infty$, les composantes C_0^+ et C_0^- sont non bornées. Comme $C_1^+ \cup C_1^- \subset [\alpha_1, \alpha_2] \times [-M, M]$ avec $M := \max_{x \in [\alpha_1, \alpha_2]} \sqrt{x^3 - 64x + 16}$, les composantes C_1^+ et C_1^- sont compactes.

c) Considérons la fonction :

$$\begin{aligned} g : E(\mathbb{R}) \setminus E[2] &\to [\alpha_1, \alpha_2] \cup [\alpha_3, +\infty[\\ P = (x_P, y_P) &\mapsto x_{2P}, \end{aligned}$$

où x_{2P} est l'abscisse de $2P$:

$$x_{2P} = \frac{x_P^4 + 2^7 x_P^2 - 2^7 x_P + 2^{12}}{4(x_P^3 - 2^6 x_P + 2^4)}.$$

La fonction g est continue. Donc $g(C_0^+)$, $g(C_0^-)$, $g(C_1^+)$ et $g(C_1^-)$ sont tous connexes. Chacun d'entre eux est donc contenu dans $[\alpha_1, \alpha_2]$ ou dans $[\alpha_3, +\infty[$. Mais pour chaque i, on a :

$$g(x, \pm\sqrt{x^3 - 64x + 16}) \xrightarrow[x\to\alpha_i]{} +\infty.$$

Du coup $g(C_0^+), g(C_0^-), g(C_1^+)$ et $g(C_1^-)$ sont tous contenus dans $[\alpha_3, +\infty[$. Autrement dit, $C_1 \cap 2(E(\mathbb{R}) \smallsetminus E[2]) = \emptyset$. Comme $2P = O$ pour tout $P \in E[2]$, on conclut que $C_1 \cap 2E(\mathbb{R}) = \emptyset$.

5) a) Par la formule de duplication :

$$x_P = \frac{x_Q^4 + 2^7 x_Q^2 - 2^7 x_Q + 2^{12}}{4(x_Q^3 - 2^6 x_Q + 2^4)},$$
$$x_Q^4 - 4x_P x_Q^3 + 2^7 x_Q^2 + 2^7(2x_P - 1)x_Q + 2^6(2^6 - x_P) = 0.$$
$$x_Q^4 + 2^7 x_Q^2 - 2^7 x_Q + 2^{12} = 0$$

b) On étudie deux cas :

(i) Si $v_2(x_Q) \leqslant 2$, on a :

$$v_2(x_Q^4) < \min\{v_2(4x_P x_Q^3), v_2(2^7 x_Q^2), v_2(2^7(2x_P - 1)x_Q), v_2(2^6(2^6 - x_P))\},$$
$$v_2(x_Q^4 - 4x_P x_Q^3 + 2^7 x_Q^2 + 2^7(2x_P - 1)x_Q + 2^6(2^6 - x_P)) = 4v_2(x_Q) < \infty.$$

Contradiction !

(ii) Si $v_2(x_Q) \geqslant 3$:

$$v_2(2^6(2^6 - x_P)) < \min\{v_2(x_Q^4), v_2(4x_P x_Q^3), v_2(2^7 x_Q^2), v_2(2^7(2x_P - 1)x_Q)\},$$
$$v_2(x_Q^4 - 4x_P x_Q^3 + 2^7 x_Q^2 + 2^7(2x_P - 1)x_Q + 2^6(2^6 - x_P)) = 6 + v_2(x_P) < \infty.$$

Contradiction !

On déduit que $P \notin 2E(\mathbb{Q})$.

6) Choisissons les points $P_1 = (0, 4)$, $P_2 = (8, 4)$ et $P_3 = (-8, 4)$. Les points P_1, P_2 et P_3 sont dans $E(\mathbb{Q})$ et comme ils sont alignés, on a $P_1 + P_2 + P_3 = O$. Par la question 4), les points P_1 et P_3 ne sont pas dans $2E(\mathbb{Q})$. Par la question 5), le point P_2 n'est pas dans $2E(\mathbb{Q})$. On déduit alors de la question 3) que $r \geqslant 2$.