**Corrigé du problème ENS Ulm-Lyon 2003, filière MP.**

R.Krust (romain.krust@prepas.org)

# I

1. (a) $0 \in \Gamma_{\text{tors}}$ et si $nx = 0$ et $n'x' = 0$ (où $n, n' \in \mathbb{Z} \setminus \{0\}$), alors $nn'(x - x') = 0$, d'où $x - x' \in \Gamma_{\text{tors}}$. Ceci montre que $\Gamma_{\text{tors}}$ est un sous-groupe de $\Gamma$ (appelé sous-groupe de torsion).

   (b) $\Gamma_{\text{tors}}$ n'est pas forcément fini. Si, par exemple, $\Gamma = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathbb{N}}$, alors $\Gamma_{\text{tors}} = \Gamma$.

2. (a) On déduit de la définition de $h$, en substituant $x$ à $y$ et en posant $M_0 = M + |h(0)|$ :

$$|h(2x) - 4h(x)| \leqslant M_0$$

Soient alors $p \leqslant q$ des entiers naturels. On a :

$$\begin{aligned}
-\frac{M_0}{4^{p+1}} &\leqslant \frac{1}{4^{p+1}}h(2^{p+1}x) - \frac{1}{4^p}h(2^p x) \leqslant \frac{M_0}{4^{p+1}} \\
-\frac{M_0}{4^{p+2}} &\leqslant \frac{1}{4^{p+2}}h(2^{p+2}x) - \frac{1}{4^{p+1}}h(2^{p+1}x) \leqslant \frac{M_0}{4^{p+2}} \\
-\frac{M_0}{4^{p+3}} &\leqslant \frac{1}{4^{p+3}}h(2^{p+3}x) - \frac{1}{4^{p+2}}h(2^{p+2}x) \leqslant \frac{M_0}{4^{p+3}} \\
&\cdots \\
-\frac{M_0}{4^q} &\leqslant \frac{1}{4^q}h(2^q x) - \frac{1}{4^{q-1}}h(2^{q-1}x) \leqslant \frac{M_0}{4^q}
\end{aligned}$$

et, en sommant :

$$\left|\frac{1}{4^q}h(2^q x) - \frac{1}{4^p}h(2^p x)\right| \leqslant \frac{M_0}{3 \times 4^p}$$

Ceci montre que la suite $\left(\frac{1}{4^n}h(2^n x)\right)_n$ est de Cauchy, donc converge.
De plus, en substituant 0 à $p$ et $n$ à $q$ dans l'inégalité précédente :

$$\left|\frac{1}{4^n}h(2^n x) - h(x)\right| \leqslant \frac{M_0}{3}$$

En posant $M' = \frac{M_0}{3}$ et en passant à la limite quand $n \to \infty$ :

$$|\hat{h}(x) - h(x)| \leqslant M'$$

   (b) On a, pour tous $x, y \in \Gamma$, $|h(2^n x + 2^n y) + h(2^n x - 2^n y) - 2h(2^n x) - 2h(2^n y)| \leqslant M$, d'où $\left|\frac{1}{4^n}h(2^n(x+y)) + \frac{1}{4^n}h(2^n(x-y)) - 2\frac{1}{4^n}h(2^n x) - 2\frac{1}{4^n}h(2^n y)\right| \leqslant \frac{M}{4^n}$. En passant à la limite quand $n \to \infty$ :

$$\hat{h}(x+y) + \hat{h}(x-y) = 2\hat{h}(x) + 2\hat{h}(y)$$

   (c) En substituant 0 à $x$ et $y$ dans la relation I.2.b, on voit que $\hat{h}(0) = 0$, puis $\forall y,\ \hat{h}(-y) = \hat{h}(y)$. Par ailleurs, en substituant $nx$ à $x$ et $x$ à $y$, toujours dans I.2.b, on a :

$$\hat{h}((n+1)x) = 2\hat{h}(nx) - \hat{h}((n-1)x) + 2\hat{h}(x)$$

Une récurrence immédiate fournit alors :

$$\forall n \in \mathbb{Z},\ \hat{h}(nx) = n^2\hat{h}(x)$$

3. (a) Soit $B \in \mathbb{R}^+$. Si $\hat{h}(x) \leqslant B$ alors, d'après l'inégalité I.2.a, $h(x) \leqslant B + M'$. Comme $h$ est admissible, l'ensemble des $x \in \Gamma$ vérifiant cette relation est fini et $\hat{h}(x)$ est admissible.

   (b) Si $\hat{h}(x) = 0$, alors $\hat{h}(nx) = n^2\hat{h}(x) = 0$ pour tout $n \in \mathbb{N}$. $\hat{h}$ étant admissible, cela entraîne que $\{nx, n \in \mathbb{N}\}$ est fini. En particulier, il existe $p < q \in \mathbb{N}$ tels que $px = qx$, d'où $(q-p)x = 0$ et $x \in \Gamma_{\text{tors}}$.

   Réciproquement, si $x \in \Gamma_{\text{tors}}$, alors il existe $n \in \mathbb{Z} \setminus \{0\}$ tel que $nx = 0$, d'où $n^2\hat{h}(x) = \hat{h}(nx) = 0$ et $\hat{h}(x) = 0$.

   (c) C'est clair.

   (d) $2\hat{h}(y) - (\hat{h}(x) + \hat{h}(z)) = \frac{1}{2}(\hat{h}(2y) - 2\hat{h}(x) - 2\hat{h}(z)) = \frac{1}{2}(\hat{h}(x-z) - 2\hat{h}(x) - 2\hat{h}(z)) = -\frac{1}{2}\hat{h}(x+z) \leqslant 0$

   (e) Soit $Z \subset \Gamma$ fini vérifiant

$$\forall x \in \Gamma, \exists z \in Z, \exists y \in \Gamma;\ x = z + 2y$$

   Soient $m = \max_Z \hat{h}$, et $Z' = \{y \in \Gamma;\ \hat{h}(y) \leqslant m + 1\}$. On va montrer que $Z'$, qui est fini, engendre $\Gamma$.

   Soit $x \in \Gamma$. D'après la propriété ci-dessus, il existe deux suites $(z_k)_k \in Z^{\mathbb{N}^*}$ et $(y_k)_k \in \Gamma^{\mathbb{N}}$ vérifiant : $y_0 = x$ et $y_k = z_{k+1} + 2y_{k+1}$. On a, d'après l'inégalité I.3.d et pour tout $k$ :

$$\hat{h}(y_{k+1}) \leqslant \frac{1}{2}(\hat{h}(y_k) + \hat{h}(z_k)) \leqslant \frac{1}{2}(\hat{h}(y_k) + m)$$

   d'où, par récurrence,

$$\forall k,\ \hat{h}(y_k) \leqslant \frac{1}{2^k}\hat{h}(x) + m$$

   Ce qui montre l'existence d'un entier $N$ tel que $y_N \in Z'$. En conséquence,

$$x = z_1 + 2z_2 + 4z_3 + \ldots + 2^{N-1}z_N + 2^N y_N$$

   appartient bien au sous-groupe de $\Gamma$ engendré par $Z'$.

# II

1. (a) Les intersections de $D_{u,v}$ et $C$ sont les solutions $(x, y)$ du système $P_{u,v} = 0$, $y = ux + v$, $x > 0$. Comme $P_{u,v}$ est un polynôme de degré 3, $n(u, v) \leqslant 3$.

   (b) $n(u, v)$ est clairement égal au nombre de racines distinctes de $P_{u,v}$. Munissons $\mathbb{R}_3[X]$ d'une norme quelconque et considérons l'ensemble $V$ des polynômes de $\mathbb{R}_3[X]$ admettant trois racines réelles distinctes. Pour $A \in \mathbb{R}_3[X]$, $A \in V$ équivaut à dire qu'il existe $x_0 < x_1 < x_2 < x_3$ tels que $A(x_i)A(x_{i+1}) < 0$. $A \mapsto A(x_i)A(x_{i+1})$ étant continue, $V$ est un ouvert de $\mathbb{R}_3[X]$. Et comme l'application $\phi : (u, v) \mapsto P_{u,v}$ est continue, $U = \phi^{-1}(V)$ est un ouvert de $\mathbb{R}^2$.

   (c) Si $n(u, v) \geqslant 2$, $P_{u,v}$ s'annule au moins deux fois et est par conséquent scindé sur $\mathbb{R}$. Or, si $D_{u,v}$ n'est pas tangente à $C$, $P_{u,v}$ n'a, d'après l'équivalence T1-T2, pas de racine double. $P_{u,v}$ admet alors trois racines réelles distinctes et $n(u, v) = 3$.

   (d) Un point $P = (x, y)$ appartient à $C$ et voit sa tangente passer par $(a, b)$ si et seulement si $y^2 = x^3 - Dx$ et $2y(b-y) = (3x^2 - D^2)(x-a)$, ce qui entraîne $2by = 2(x^3 - D^2x) + (3x^2 - D^2)(x-a)$, puis, en élevant au carré $4b^2(x^3 - D^2x) = [2(x^3 - D^2x) + (3x^2 - D^2)(x-a)]^2$. Cette équation admet au plus 6 racines, et il existe au plus 12 points $P$ de $C$ dont la tangente passe par $(a, b)$ (il s'agit bien sûr d'une majoration grossière).

2. (a) Un point $(x,y) \in C$ vérifie $x^3 - D^2x = y^2 \geqslant 0$ et $x > 0$, donc $x \geqslant D$. Comme $x \mapsto x^3 - D^2x$ induit une bijection de $[D, +\infty[$ dans $\mathbb{R}_+$, il est clair qu'étant donné $t \in \mathbb{R}$, il existe un unique $x \in \mathbb{R}_+^*$ vérifiant $t^2 = x^3 - D^2x$. Ceci permet de définir $F(t) = x$ et $P(t) = (F(t), t)$, de sorte que $C = \{(F(t), t),\ t \in \mathbb{R}\}$.

   (b) Les trois premières propriétés de $F$ sont immédiates. Montrons que $F$ est $C^1$. L'application $g : x \mapsto x^3 - D^2x$ de $[D, +\infty[$ dans $\mathbb{R}_+$ est de classe $C^1$, et sa dérivée ne s'annule pas. Donc $F\ :\ y \mapsto g^{-1}(y^2)$ est de classe $C^1$ sur $\mathbb{R}_+$ et sur $\mathbb{R}_-$. Sa dérivée étant nulle en $0^+$ et $0^-$, elle est de classe $C^1$.

   (c) On a $\lim\limits_{x\to+\infty} g(x) = +\infty$, donc $\lim\limits_{z\to+\infty} g^{-1}(z) = +\infty$, et $\lim\limits_{y\to\pm\infty} F(y) = +\infty$. Il en résulte, lorsque $y \to \pm\infty$, $F(y) = o(F(y)^3)$ et $y^2 = F(y)^3 - D^2F(y) \sim F(y)^3$, d'où $\lim\limits_{y\to\pm\infty} |y|^{-2/3}F(y) = 1$.

   (d) $D(a,t)$ est la droite d'équation $X = F(a) + \dfrac{F(a) - F(t)}{a - t}(Y - a)$. Les points d'intersection de $D(a,t)$ et de $C$ ont donc une ordonnée annulant le polynôme (en $Y$) :

$$Y^2 - \left(F(a) + \frac{F(a) - F(t)}{a - t}(Y - a)\right)^3 - D^2\left(F(a) + \frac{F(a) - F(t)}{a - t}(Y - a)\right)$$

   Ses racines sont $a$, $t$, et une troisième racine $\xi$. D'après l'équivalence admise entre (T1) et (T3), $a$ (resp. $t$) est une racine double lorsque $D(a,t)$ est la tangente en $a$ (resp. $t$), tandis que dans le cas général ($\xi \neq a$ et $\xi \neq t$), $\xi$ est l'ordonnée du troisième point d'intersection de $D(a,t)$ et $C$. Or, en calculant le coefficient de $Y^3$ et le coefficient constant de ce polynôme, on voit que

$$at\xi = -\left(\frac{t - a}{F(t) - F(a)}\right)^3 \left[\left(\frac{tF(a) - aF(t)}{t - a}\right)^3 - D^2\frac{tF(a) - aF(t)}{t - a}\right]$$

   Donc $\xi = H_a(t)$, et on a prouvé les équivalences demandées.

   (e) Un calcul immédiat donne

$$\lim_{t\to\pm\infty} H_a(t) = -\frac{1}{a}(F(a)^3 - D^2F(a)) = -a$$

   La droite $D(a,t)$ "tend" vers la droite $X = F(a)$ (il est donc naturel de considérer que cette droite intersecte $\overline{C}(\mathbb{Q})$ en $\infty$).

   *Remarque : On aura besoin du résultat suivant. Soient $a \in \mathbb{R}^*$. La tangente en $P(a)$ à $C$ intersecte $C$ en un "troisième" point d'ordonnée $b$ (qui peut être confondu avec $P(a)$), et l'on a $b = \lim\limits_{t\to a} H_a(t)$. En effet, la tangente en $a$ à $C$ a pour équation $X = F(a) + F'(a)(Y - a)$, et les racines du polynôme*

$$Y^2 - \left[(F(a) + F'(a)(Y - a))^3 - D^2(F(a) + F'(a)(Y - a))\right]$$

   *sont, d'après l'équivalence T1-T3, $a$ (racine double) et $b$. Il vient*

$$a^2b = -\frac{1}{F'(a)^3}\left[(F(a) - aF'(a))^3 - D^2(F(a) - aF'(a))\right]$$

   *c'est-à-dire, en effet, d'après 2.d., $b = \lim\limits_{t\to a} H_a(t)$.*

3. (a) On a, pour tout $t \in \mathbb{R}$, $F(t) \geqslant D$, d'où $\dfrac{2}{3F(t)^2 - D^2} > 0$. $L$ est donc strictement croissante, évidemment continue, tandis que $\lim\limits_{y\to-\infty} L(y) = 0$, $\lim\limits_{y\to+\infty} L(y) = \Omega$. Ceci montre que $L$ induit une bijection de $\mathbb{R}$ sur $]0, \Omega[$.

   (b) $L$ est de classe $C^1$ et l'on a $\dfrac{d}{dy}(L(y) + L(-y)) = \dfrac{2}{3F(y)^2 - D^2} - \dfrac{2}{3F(-y)^2 - D^2} = 0$. Donc $L(y) + L(-y)$ est indépendant de $y$. En examinant la limite quand $y \to +\infty$, on voit que $L(y) + L(-y) = \Omega$.

4. (a) $Q$ et $\displaystyle\sum_{i=1}^{n} Q(x_i)\left(\prod_{j\neq i}\frac{X-x_j}{x_i-x_j}\right)$ sont deux polynômes de degré au plus $n-1$ qui prennent les mêmes valeurs aux $n$ points $x_i$. Ils sont donc égaux.

   (b) La relation précédente peut s'écrire :

$$\sum_{i=1}^{n}\frac{Q(x_i)}{P'(x_i)}\frac{X}{X-x_i}=\frac{XQ(X)}{P(X)}$$

En substituant $X^k$ à $Q$ ($0\leqslant k\leqslant n-1$), $t$ à $X$, puis en prenant la limite quand $t\to+\infty$, on obtient :

$$\begin{aligned}\sum_{i=1}^{n}\frac{x_i^k}{P'(x_i)} &= 0 \quad \text{si } 0\leqslant k\leqslant n-2\\ \sum_{i=1}^{n}\frac{x_i^{n-1}}{P'(x_i)} &= 1\end{aligned}$$

5. (a) Une équation de la droite contenant les $P_i(t)$ est $Y=\dfrac{y_2(t)-y_1(t)}{x_2(t)-x_1(t)}(X-x_1(t))+y_1(t)$ ($x_2(t)\neq x_1(t)$ puisque la droite en question intersecte $C$ en trois points distincts et n'est donc pas parallèle à $Oy$). Elle est donc de la forme $Y=u(t)X+v(t)$, où $u$ et $v$ sont de classe $C^1$. On va montrer

$$\frac{dL(y_i(t))}{dt}=2\frac{u'(t)x_i(t)+v'(t)}{P'_{u(t),v(t)}(x_i(t)}$$

Pour cela, dérivons les relations $y_i(t)^2=x_i(t)^3-D^2x_i(t)$ et $P_{u(t),v(t)}(x_i(t))=0$. Il vient :

$$\begin{cases}2y_i(t)y_i'(t)=(3x_i(t)^2-D^2)x_i'(t)\\ P'_{u(t),v(t)}(x_i(t))x_i'(t)=2(u(t)x_i(t)+v(t))(u'(t)x_i(t)+v'(t))=2y_i(t)(u'(t)x_i(t)+v'(t))\end{cases}$$

Puis, si $y_i(t)\neq 0$,

$$\begin{aligned}\frac{dL(y_i(t))}{dt} &= L'(y_i(t))y_i'(t)=\frac{2y_i'(t)}{3F(y_i(t))^2-D^2}\\ &= \frac{2y_i'(t)}{3x_i(t)^2-D^2}=\frac{x_i'(t)}{y_i(t)}\\ &= 2\frac{u'(t)x_i(t)+v'(t)}{P'_{u(t),v(t)}(x_i(t))}\end{aligned}$$

Maintenant, si $y_i(t_0)=0$ et que $t_0$ est un zéro isolé de $y_i$, cette relation subsiste en $t_0$ par continuité. Tandis que si $t_0$ est un zéro non isolé de $y_i$, alors $P_i(t_n)=(D,0)$ pour une certaine suite $(t_n)_{n\in\mathbb{N}^*}$ qui converge vers $t_0$ ($t_n\neq t_0$), ce qui montre que $x_i'(t_0)=y_i'(t_0)=0$. On a aussi $u(t_n)D+v(t_n)=0$, d'où $u'(t_0)D+v'(t_0)=0$ et

$$\frac{dL(y_i(t))}{dt}|_{t=t_0}=2\frac{y_i'(t_0)}{3x_i(t_0)^2-D^2}=0=2\frac{u'(t_0)x_i(t_0)+v'(t_0)}{P'_{u(t_0),v(t_0)}(x_i(t_0))}$$

On a ainsi montré que, pour tout $t$ :

$$\frac{d}{dt}\left(\sum_{i=1}^{3}L(y_i(t))\right)=2u'(t)\sum_{i=1}^{3}\frac{x_i(t)}{P'_{u(t),v(t)}(x_i(t))}+2v'(t)\sum_{i=1}^{3}\frac{1}{P'_{u(t),v(t)}(x_i(t))}$$

Comme les $x_i(t)$ sont les trois racines de $P_{u(t),v(t)}$, on peut conclure, grâce à 4.b.,

$$\frac{d}{dt}\left(\sum_{i=1}^{3}L(y_i(t))\right)=0$$

(b) L'application $t \mapsto L(a)+L(t)+L(H_a(t))$ est continue sur $]a,+\infty[$, et, d'après 5.a., constante sur chaque intervalle sur lequel $H_a(t) \neq a$ et $H_a(t) \neq t$. Or, d'après 2.d, $H_a(t) = a$ si et seulement si $D(a,t)$ est la tangente en $P(a)$ à $C$, ce qui ne peut arriver que pour au plus une valeur de $t$ (ordonnée du "troisième" point d'intersection de la tangente en $P(a)$ à $C$), tandis que $H_a(t) = t$ si et seulement si la tangente en $P(t)$ à $C$ passe par $P(a)$, ce qui, d'après 1.d., ne peut se produire que pour un nombre fini de valeurs de $t$. Tout ceci montre que $t \mapsto L(a) + L(t) + L(H_a(t))$ est constante sur $]a,+\infty[$. Comme $\lim\limits_{t\to+\infty} H_a(t) = -a$, il vient, en examinant la limite en $+\infty$ : $\forall t > a,\ L(a) + L(t) + L(H_a(t)) = L(a) + \Omega + L(-a) = 2\Omega$.

(c) Notons que si l'un des $y_i$ est nul, alors les deux autres sont (non nuls et) de mêmes signes. Par conséquent, soit deux des $y_i$ sont strictement positifs, soit deux d'entre eux sont strictement négatifs.

Or, si deux des $y_i$ sont strictement positifs, par exemple $0 < y_1 < y_2$, alors $y_3 = H_{y_1}(y_2)$ et il résulte de la question précédente que $L(y_1) + L(y_2) + L(y_3) = 2\Omega$. Mais, de la même manière, pour tout $a < 0$, et pour tout $t < a$, $L(a) + L(t) + L(H_a(t)) = L(a) + L(-a) = \Omega$. Donc si deux des $y_i$ sont strictement négatifs, $L(y_1) + L(y_2) + L(y_3) = \Omega$.

(d) $y_1 = 0$ n'est pas clairement pas possible, et l'on a, d'après la remarque faite en II.2.e, $y_2 = \lim\limits_{t\to y_1} H_{y_1}(t)$. Donc, si $y_1 > 0$, $2L(y_1) + L(y_2) = \lim\limits_{t\to y_1^+} L(y_1) + L(t) + L(H_{y_1}t) = 2\Omega$ (d'après 5.b.). De même, si $y_1 < 0$, $2L(y_1) + L(y_2) = \Omega$.

(e) On peut bien sûr supposer $y_1 < y_2 < y_3$. Notons que, puisque $L(y_i) \in ]0,\Omega[$, $L(y_1)+L(y_2)+L(y_3) \in \Omega\mathbb{Z}$ équivaut à $L(y_1) + L(y_2) + L(y_3) \in \{\Omega, 2\Omega\}$.

Supposons $L(y_1) + L(y_2) + L(y_3) = \Omega$. Cela entraîne $y_2 < 0$ puisque, dans le cas contraire, $y_3 > y_2 \geqslant 0$, d'où $L(y_2) \geqslant \dfrac{\Omega}{2}$, $L(y_3) > \dfrac{\Omega}{2}$ et $L(y_2) + L(y_3) > \Omega$. Donc $y_1$ et $y_2$ sont strictement négatifs et il vient, d'après ce qui a été vu en 5.c., $L(y_1)+L(y_2)+L(H_{y_2}(y_1)) = \Omega$, d'où $L(y_3) = L(H_{y_2}(y_1))$ et $y_3 = H_{y_2}(y_1)$. Les points $P(y_i)$ sont donc alignés. Le même type de raisonnement s'applique lorsque $L(y_1) + L(y_2) + L(y_3) = 2\Omega$.

*Remarque : De la même manière, si $y_1$ et $y_2 \in \mathbb{R}$ sont tels que $2L(y_1) + L(y_2) \in \Omega\mathbb{Z}$, alors $P(y_2)$ est sur la tangente en $P(y_1)$ à $C$. En effet, si, par exemple, $2L(y_1) + L(y_2) = 2\Omega$, alors $y_1 > 0$ et, en notant $y_3$ l'ordonnée du "troisième" point d'intersection de la tangente en $P(y_1)$ à $C$ (voir remarque en 2.e.), on a, d'après 5.d., $L(y_2) = L(y_3)$, d'où $y_2 = y_3$.*

6. (a) L'application $y \mapsto \dfrac{2\pi}{\Omega}L(y)$ réalise une bijection de $\mathbb{R}$ dans $]0,2\pi[$. Donc $E$ est une bijection de $\overline{C}$ dans $G$, et il existe une unique loi $+$ sur $\overline{C}$ définie par $E(P+Q) = E(P)E(Q)$. Cette loi fait naturellement de $\overline{C}$ un groupe commutatif isomorphe à $G$.

Soient maintenant $P, Q \in C$ tels que $P + Q \neq \infty$. On a

$$\begin{aligned}
\exp\left(\frac{2i\pi}{\Omega}L(y(P+Q))\right) &= E(P+Q) = E(P)E(Q) \\
&= \exp\left(\frac{2i\pi}{\Omega}L(y(P))\right)\exp\left(\frac{2i\pi}{\Omega}L(y(Q))\right) \\
&= \exp\left(\frac{2i\pi}{\Omega}(L(y(P)) + L(y(Q)))\right)
\end{aligned}$$

d'où $L(y(P+Q)) \equiv L(y(P))+L(y(Q)) \mod \Omega$. Il en résulte, puisque $L(y(P+Q)) \in ]0,\Omega[$ et $L(y(P)) + L(y(Q)) \in ]0,2\Omega[$, que $L(y(P)) + L(y(Q)) \neq \Omega$ et

$$\begin{aligned}
L(y(P+Q)) &= L(y(P)) + L(y(Q)) \text{ si } L(y(P)) + L(y(Q)) < \Omega \\
L(y(P+Q)) &= L(y(P)) + L(y(Q)) - \Omega \text{ si } L(y(P)) + L(y(Q)) > \Omega
\end{aligned}$$

(b) $\infty$ est neutre pour + puisque $E(\infty) = 1$ et que 1 est le neutre de $G$. Par ailleurs

$$\begin{aligned} P_1 + P_2 + P_3 = \infty &\iff E(P_1 + P_2 + P_3) = 1 \\ &\iff E(P_1)E(P_2)E(P_3) = 1 \\ &\iff \exp\left(\frac{2i\pi}{\Omega}(L(y(P_1)) + L(y(P_2)) + L(y(P_3)))\right) = 1 \\ &\iff L(y(P_1)) + L(y(P_2)) + L(y(P_3)) \in \Omega\mathbb{Z} \end{aligned}$$

ce qui équivaut, d'après 5.e., à $P_1$, $P_2$, $P_3$ alignés.

*Remarque : De la même façon, si $P_1$ et $P_2$ sont deux éléments distincts de $C$, alors $2P_1 + P_2 = \infty$ si et seulement si $P_2$ est sur la tangente en $P_1$ à $C$. Et $3P_1 = \infty$ si et seulement si $P_1$ est un point d'intersection "triple" de la tangente en $P_1$ à $C$ et de $C$, c'est-à-dire si le polynôme correspondant $P_{u,v}$ admet une racine triple (la démonstration est identique, sur la base de la remarque faite en 5.e.) ).*

(c) On a, d'après 3.b., $L(y) + L(-y) = \Omega$, donc $E(P(y) + P(-y)) = 1$ et $P(y) + P(-y) = \infty$. Ceci montre que l'opposé de $P(y)$ est $P(-y)$, soit, en effet, son symétrique par rapport à l'axe $Ox$.

(d) $\overline{C}$ et $G$ sont deux groupes isomorphes. Or, pour $a \in G$, l'équation $z^2 = a$ d'inconnue $z \in G$ possède deux solutions exactement. Donc l'équation $2Q = P$ dans $\overline{C}$ possède deux solutions exactement.

(e) On sait, d'après le cours, que $\theta \mapsto e^{i\theta}$ est un homéomorphisme (c'est-à-dire une bijection continue dont la réciproque est continue) de $]-\pi, \pi[$ dans $G \setminus \{1\}$. Donc $h : t \mapsto \exp\left(\frac{2i\pi}{\Omega}L(t)\right)$ réalise un homéomorphisme de $\mathbb{R}$ dans $G \setminus \{1\}$. Notons que l'on a, pour tout $P \in C$, $h(y(P)) = E(P)$. Soient $y_1$ et $y_2 \in \mathbb{R}$. On a, lorsque $(z_1, z_2) \to (y_1, y_2)$,

$$\begin{aligned} E(P(z_1) + P(z_2)) &= E(P(z_1))E(P(z_2)) = h(z_1)h(z_2) \\ &\to h(y_1)h(y_2) = E(P(y_1))E(P(y_2)) = E(P(y_1) + P(y_2)) \end{aligned}$$

Si $y_1 + y_2 \neq 0$, alors $z_1 + z_2 \neq 0$ pour $z_i$ assez proche de $y_i$ et l'on a $P(y_1) + P(y_2)) \neq \infty$, $P(z_1) + P(z_2) \neq \infty$, d'où $E(P(y_1) + P(y_2)) \neq 1$, $E(P(z_1) + P(z_2)) \neq 1$, et, en composant par $h^{-1}$,

$$y(P(z_1) + P(z_2)) \to y(P(y_1) + P(y_2))$$

Si $y_1 + y_2 = 0$, alors $E(P(y_1) + P(y_2)) = E(\infty) = 1$, d'où $E(P(z_1) + P(z_2)) \to 1$. Or $|h^{-1}(w)| \underset{w\to 1}{\to} +\infty$, d'où $|y(P(z_1) + P(z_2))| = |h^{-1}(E(P(z_1) + P(z_2)))| \underset{z_1+z_2\neq 0}{\to} +\infty$.

# III

1. (a) Soient $P_1$, $P_2$ et $P_3$ deux à deux distincts. On sait que $P_1+P_2+P_3 = \infty$ signifie que $P_1$, $P_2$, et $P_3$ sont alignés. La droite passant par $P_1$ et $P_2$ a pour équation $Y = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(X - x_1)$. Les $P_i$ sont alors les points d'intersection de cette droite et de $C$. Donc $x_1$, $x_2$, et $x_3$ sont les trois racines (distinctes) du polynôme $P(X) = X^3 - D^2X - \left(y_1 + \frac{y_2 - y_1}{x_2 - x_1}(X - x_1)\right)^2$. La somme des racines de $P$ vaut alors $x_1+x_2+x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2$. Or, en effectuant la différence des deux relations $y_i^2 = x_i^3 - D^2 x_i$ $(i = 1, 2)$, il vient $\frac{y_2 - y_1}{x_2 - x_1} = \frac{x_1^2 + x_1x_2 + x_2^2 - D^2}{y_1 + y_2}$ et $x_3 = \left(\frac{x_1^2 + x_1x_2 + x_2^2 - D^2}{y_1 + y_2}\right)^2 - x_1 - x_2$. De plus, $y_3 = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) = y_1 + \frac{x_1^2 + x_1x_2 + x_2^2 - D^2}{y_1 + y_2}(x_3 - x_1)$.

Dans le cas où, par exemple, $P_3 = P_1$, la remarque faite en II.6.b. et l'équivalence admise T1-T2 montrent que $x_1 = x_3$ est racine double du polynôme $P(X) = X^3 - D^2X - \left(y_1 + \dfrac{y_2 - y_1}{x_2 - x_1}(X - x_1)\right)^2$, et ces résultats subsistent.

(b) $x_1 + D$, $x_2 + D$ et $x_3 + D$ sont les trois racines du polynôme $(X - D)^3 - D^2(X - D) - \left(y_1 + \dfrac{y_2 - y_1}{x_2 - x_1}(X - D - x_1)\right)^2$. Donc

$$(x_1 + D)(x_2 + D)(x_3 + D) = \left(y_1 - \frac{y_2 - y_1}{x_2 - x_1}(D + x_1)\right)^2 = \left(\frac{(x_1 + D)y_2 - (x_2 + D)y_1}{x_2 - x_1}\right)^2$$

2. (a) Posons $y_1 = y$, $P_1 = P$ $(= P(y))$, et considérons $P_2 = P(y_2)$ quand $y_2$ tend vers $y$. Puisque $y + y_2 \neq 0$ pour $y_2$ assez proche de $y$ (car $y \neq 0$), on a, d'après II.6.e, $y(P(y_1) + P(y_2)) \underset{y_2 \to y_1}{\to} y(2P(y_1))$. En notant, comme en 1., $P_3$ le point tel que $P_1 + P_2 + P_3 = \infty$, on a donc $y(P_3) = -y(P_1 + P_2) \underset{y_2 \to y_1}{\to} -y(2P(y_1)) = -y'$, ainsi que, en appliquant $F$, $x(P_3) \underset{y_2 \to y_1}{\to} x'$. Les formules désirées s'obtiennent alors en passant à la limite quand $y_2 \to y_1$ dans les formules obtenues en 1.a.

(b) $x' = \left(\dfrac{3x^2 - D^2}{2y}\right)^2 - 2x = \dfrac{(3x^2 - D^2)^2 - 8xy^2}{(2y)^2}$. En développant et en utilisant $y^2 = x^3 - D^2x$, il vient $x' = \left(\dfrac{x^2 + D^2}{2y}\right)^2$.

(c) Il suffit de vérifier, outre $\infty \in \overline{C}(Q)$, que $P_1 \in \overline{C}(Q)$, $P_2 \in \overline{C}(Q)$ entraînent $P_1 - P_2 \in \overline{C}(Q)$, ce qui résulte immédiatement des formules démontrées en 1.a et 2.a., les cas particuliers s'étudiant aisément.

(d) On a, d'après 1.b. appliqué à $(P_1, P_2, -P_3)$ et à $(P_1, -P_2, -P_4)$,

$$\begin{aligned}
& (x_1 + D)^2(x_2 + D)^2(x_3 + D)(x_4 + D) \\
= \; & (x_1 + D)(x_2 + D)(x_3 + D) \times (x_1 + D)(x_2 + D)(x_4 + D) \\
= \; & \left(\frac{(x_1 + D)y_2 - (x_2 + D)y_1}{x_2 - x_1}\right)^2 \left(\frac{(x_1 + D)(-y_2) - (x_2 + D)y_1}{x_2 - x_1}\right)^2 \\
= \; & \frac{[(x_1 + D)^2y_2^2 - (x_2 + D)^2y_1^2]^2}{(x_2 - x_1)^4} \\
= \; & \frac{[(x_1 + D)^2(x_2^3 - D^2x_2) - (x_2 + D)^2(x_1^3 - D^2x_1)]^2}{(x_2 - x_1)^4} \\
= \; & \frac{[x_2(x_1 + D)^2(x_2 + D)(x_2 - D) - x_1(x_2 + D)^2(x_1 + D)(x_1 - D)]^2}{(x_2 - x_1)^4} \\
= \; & (x_1 + D)^2(x_2 + D)^2 \frac{[x_2(x_1 + D)(x_2 - D) - x_1(x_2 + D)(x_1 - D)]^2}{(x_2 - x_1)^4} \\
= \; & (x_1 + D)^2(x_2 + D)^2 \frac{(x_2 - x_1)^2(x_1x_2 + D(x_1 + x_2) - D^2)^2}{(x_2 - x_1)^4}
\end{aligned}$$

d'où

$$(x_3 + D)(x_4 + D) = \left(\frac{x_1x_2 + D(x_1 + x_2) - D^2}{x_2 - x_1}\right)^2$$

# IV

## IV. A

1. (a) Si $a = b^2$, alors $a > 0$ et, pour tout $p$ premier, $v_p(a) = 2v_p(b)$, d'où $\overline{v_p(a)} = 0$. Réciproquement, si $a > 0$ et $\overline{v_p(a)} = 0$ pour tout $p$, alors $a = \prod_p p^{v_p(a)} = \left(\prod_p p^{v_p(a)/2}\right)^2$.

(b) Écrivons $a = p^{v_p(a)}\dfrac{u}{v}$, $b = p^{v_p(b)}\dfrac{r}{s}$, où $u, v, r, s \in \mathbb{Z} \setminus \{0\}$, $v_p(u) = v_p(v) = v_p(r) = v_p(s) = 0$. On a $a + b = p^{v_p(a)}\left(\dfrac{u}{v} + p^{v_p(b)-v_p(a)}\dfrac{r}{s}\right) = p^{v_p(a)}\dfrac{us + p^{v_p(b)-v_p(a)}rv}{vs}$. Puisque $v_p(b) - v_p(a) > 0$, $p$ ne divise pas $us + p^{v_p(b)-v_p(a)}$. Donc $v_p(a + b) = v_p(a)$.

2. (a) Puisque $c$ est un carré, $v_p(c)$ est pair et, bien sûr, $v_p(c) \geqslant 1 \implies v_p(c) \geqslant 2$. On a par ailleurs, par définition de $c$,

$$\begin{array}{lll} v_p(x) < 0 \text{ et } v_p(x) \text{ pair} & \implies & v_p(c) = -v_p(x) \\ v_p(x) < 0 \text{ et } v_p(x) \text{ impair} & \implies & v_p(c) = -v_p(x) + 1 \\ v_p(x) \geqslant 0 & \implies & v_p(c) = 0 \end{array}$$

Donc

$$v_p(c) \geqslant 1 \implies v_p(x) < 0 \implies v_p(c) + v_p(x) \in \{0, 1\} \implies v_p(a) \in \{0, 1\}$$

(b) On a $y^2 = x(x - D)(x + D)$, d'où

$$c^3y^2 = a(a - Dc)(a + Dc)$$

Comme $c$ est un carré, $a(a-Dc)(a+Dc)$ est le carré d'un rationnel. S'agissant d'un entier, c'est le carré d'un entier.

*Remarque : Soit $p$ un nombre premier. Si $v_p(c) \geqslant 1$ alors, d'après la question précédente, $v_p(a) \leqslant 1$, $v_p(c) \geqslant 2$, d'où*

$$v_p(a - Dc) = v_p(a + Dc) = v_p(a)$$

*Il vient $3v_p(c)+2v_p(y) = 3v_p(a)$, et, puisque $v_p(c)$ est pair, $v_p(a)$ pair, et même nul puisque $v_p(a) \in \{0, 1\}$. On a ainsi montré que $a$ et $c$ sont premiers entre eux.*

(c) Si $p|c$, alors $v_p(a) = 0$ d'après ce qui précède, et $v_p(a + Dc) = 0$ (par 1.b).

Si $p \nmid c$, distinguons deux cas :

Soit $p|a$, auquel cas $p \nmid Dc$ entraîne $p \nmid (a - Dc)$, $p \nmid (a + Dc)$, d'où $v_p(a) = v_p(y^2)$ pair ainsi que $v_p(a + Dc) = 0$.

Soit $p \nmid a$, auquel cas $v_p(a) = 0$, et $2v_p(y) = v_p(a - Dc) + v_p(a + Dc)$. Or, puisque $(a + Dc) - (a - Dc) = 2Dc$ et $p \notin S \cup \{2\}$, $p$ ne peut diviser simultanément $(a - Dc)$ et $(a + Dc)$. Donc $v_p(a + Dc)$ est pair.

3. (a) Soient $P_1, P_2 \in \overline{C}$, et $P_3 = P_1 + P_2$. Si $P_1 = \infty$ ou $P_2 = \infty$, on a clairement $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$. Si $P_1 + P_2 = \infty$, alors $P_1 = -P_2$, $\phi(P_1) = \phi(P_2)$, et $\phi(P_1) + \phi(P_2) = (0, 0, \ldots, 0) = \phi(\infty)$.

Sinon, en posant $P_i = (x_i, y_i)$ et d'après III.1.b, $x_1x_2x_3$ et $(x_1 + D)(x_2 + D)(x_3 + D)$ sont des carrés dans $\mathbb{Q}$. Donc, pour tout nombre premier $p$, $\overline{v_p(x_3)} = \overline{v_p(x_1)} + \overline{v_p(x_2)}$, $\overline{v_p(x_3 + D)} = \overline{v_p(x_1 + D)} + \overline{v_p(x_2 + D)}$ et l'on a $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$.

(b) $P \neq (D, 0)$ car $2D$ n'est pas un carré dans $\mathbb{Q}$. Posons $Q = (x, y)$. D'après III.2.b, si $x'$, $x' - D$ et $x' + D$ sont des carrés dans $\mathbb{Q}$, alors $\dfrac{x^2 + D^2}{y}$, $\dfrac{x^2 + 2Dx - D^2}{y}$ et $\dfrac{x^2 - 2Dx - D^2}{y}$ sont dans $\mathbb{Q}$. Ce qui entraîne

$$\begin{aligned} \frac{x}{y} &= \frac{1}{4D}\left(\frac{x^2 + 2Dx - D^2}{y} - \frac{x^2 - 2Dx - D^2}{y}\right) \in \mathbb{Q} \\ \frac{1}{y} &= \frac{1}{4D^2}\left(2\frac{x^2 + D^2}{y} - \frac{x^2 + 2Dx - D^2}{y} - \frac{x^2 - 2Dx - D^2}{y}\right) \in \mathbb{Q} \end{aligned}$$

d'où $(x, y) \in \mathbb{C}(\mathbb{Q})$.

(c) On va montrer

$$\mathrm{Ker}(\phi) = \{2Q,\ Q \in \overline{C}(\mathbb{Q})\}$$

On a bien sûr $\infty = 2\infty$.

Soit maintenant $P = (x, y) \in C(\mathbb{Q}) \cap \mathrm{Ker}(\phi)$. On a, pour tout $p$ premier, $\overline{v_p(x)} = \overline{v_p(x+D)} = 0$ (d'après 2.c. si $p \notin S \cup \{2\}$, et parce $\phi(x) = 0$ sinon). Puisque $x > 0$, $x$ et $x+D$ sont des carrés dans $\mathbb{Q}$. Comme $y^2 = x(x-D)(x+D)$, $x-D$ est aussi un carré, et, d'après II.6.d et 3.b., $P$ est de la forme $2Q$, $Q \in C(\mathbb{Q})$.

Réciproquement, si $P = (x, y) \in C(\mathbb{Q}) \setminus \{(D, 0)\}$ est de la forme $2Q$ ($Q \in C(\mathbb{Q})$), les formules III.2.b. montrent que $x$ et $x + D$ sont des carrés dans $Q$. Donc $\phi(P) = 0$.

Il reste à voir, puisque $\phi((D, 0)) \neq 0$ (car $D$ est impair), que $P = (D, 0)$ n'est pas de la forme $2Q$, $Q \in C(\mathbb{Q})$. Soit $Q = (x, y) \in C$ tel que $P = 2Q$. La tangente en $Q$ à $C$, d'équation $2y(Y - y) = (3x^2 - D^2)(X - x)$ doit passer par $-P = P$, et $Q \in C$ :

$$\begin{cases} -2y^2 = (3x^2 - D^2)(D - x) \\ y^2 = x(x - D)(x + D) \end{cases}$$

d'où, après éliminition de la solution parasite $(x, y) = (D, 0)$, $x^2 - 2xD - D^2 = 0$ et, puisque $x > 0$, $x = D(1 + \sqrt{2}) \notin \mathbb{Q}$.

(d) Soit $Z$ une partie (forcément finie) de $\overline{C}(\mathbb{Q})$ telle que chaque élément de l'image de $\phi$ possède un unique antécédent dans $\overline{C}(\mathbb{Q})$. Alors un élément quelconque $P$ de $\overline{C}(\mathbb{Q})$ peut s'écrire sous la forme $P_0 + Q$, où $\phi(P_0) = \phi(P)$, $P_0 \in Z$, et $Q \in \mathrm{Ker}(\phi)$. Compte tenu du résultat prouvé dans la question précédente, ceci exprime que $\overline{C}(\mathbb{Q})$ est de type fini modulo 2.

## IV. B

1. Puisque $h$ est manifestement positive, et que $h(\infty) = 0$, le résultat est clair si $P = \infty$ ou $P = (D, 0)$ ($2(D, 0) = \infty$). Supposons $P \in C(\mathbb{Q}) \setminus \{(D, 0)\}$, posons $2P = (x', y')$ (voir IV.B.3.a) et désignons par $c'$ le plus petit carré rendant $c'x'$ entier. D'après III.2.b., $x' = \left(\dfrac{x^2 + D^2}{2y}\right)^2$, donc $c^4(2y)^2x' = (a^2 + D^2c^2)^2$ est entier. Comme $c^4(2y)^2 = 4c(a^3 - D^2a)$ est un carré (de rationnel) et un entier, c'est un carré entier et $c'$ divise $c^4(2y)^2$. Il vient, en utilisant à nouveau une formule de III.2.b.,

$$h(2P) = \log(c'(x' + D)) \leqslant \log(c^4(x^2 + 2Dx - D^2)^2) \leqslant \log(c^4(x + D)^4) \leqslant 4h(P)$$

2. (a) On a, modulo $d$ :

$$2a_1(a_2 + Dc_2) = T + U + DV \equiv 0$$

$$2a_2(a_1 + Dc_1) = T + U - DV \equiv 0$$

Mais aussi

$$2D^2a_1c_2^2 = (2Da_1c_2)(Dc_2) \equiv -2Da_1a_2c_2 \text{ (car } 2a_1(a_2 + Dc_2) \equiv 0)$$

$$2D^2a_1c_2^2 = (2D^2c_2)(a_1c_2) \equiv 2D^2a_2c_1c_2 \equiv -2a_1a_2^2 \text{ (car } a_1c_2 \equiv a_2c_1 \text{ et } a_1a_2 + D^2c_1c_2 \equiv 0)$$

d'où

$$4D^2a_1c_2^2 \equiv -2Da_1a_2c_2 - 2a_1a_2^2 \equiv -2a_2a_1(a_2 + Dc_2) \equiv 0$$

De même, $4D^2a_2c_1^2 \equiv 0$.

(b) Il résulte de la remarque faite en IV.A.2.b. que $\mathrm{pgcd}(a_1, c_1) = \mathrm{pgcd}(a_2, c_2) = 1$. Si $p$ premier $\notin S \cup \{2\}$ divise $4D^2a_1c_2^2$ et $4D^2a_2c_1^2$ alors, clairement, $p$ divise soit $a_1$ et $a_2$ mais ni $c_1$ ni $c_2$, soit $c_1$ et $c_2$ mais ni $a_1$ ni $a_2$. Dans les deux cas, $p$ ne peut diviser $a_1a_2 + D^2c_1c_2$.

(c) Soit $p \in S \cup \{2\}$, de sorte que $v_p(2D) = 1$. Si $p^4$ divise $4D^2a_1c_2^2$ et $4D^2a_2c_1^2$, alors soit $p^2$ divise $a_1$ et $a_2$, tandis que $p$ ne divise ni $c_1$ ni $c_2$, soit $p$ divise $c_1$ et $c_2$, mais ni $a_1$ ni $a_2$. On a dans le premier cas $v_p(a_1a_2) \geqslant 4$, $v_p(4D^2c_1c_2) = 2$, d'où $v_p(a_1a_2 + 4D^2c_1c_2) = 2$, et dans le second, $v_p(a_1a_2) = 0$, $v_p(4D^2c_1c_2) \geqslant 4$, d'où $v_p(a_1a_2 + 4D^2c_1c_2) = 0$.

(d) Soient $\delta = \text{pgcd}(a_1a_2+D^2c_1c_2, a_1a_2-D^2c_1c_2+D(a_1c_2+a_2c_1), a_1c_2-a_2c_2)$, et $p$ un nombre premier. D'après 2.a., 2.b. et 2.c., $v_p(\delta) = 0$ si $p \notin S \cup \{2\}$, et $v_p(\delta) \leqslant 3$ si $p \notin S \cup \{2\}$. Donc $v_p(\delta) \leqslant v_p((2D)^3)$ et $\delta | (2D)^3$.

(e) Tout d'abord, $c_3c_4\delta = \text{pgcd}(c_3c_4d, c_3c_4d', c_3c_4e) = \text{pgcd}(a_3a_4e, (a_3+Dc_3)(a_4+Dc_4)e, c_3c_4e)$, donc $e$ divise $c_3c_4\delta$. Ensuite,

$$\begin{aligned} h(P_3) + h(P_4) &= \log[(c_3c_4(x_3 + D)(x_4 + D)] \\ &= \log\left(c_3c_4\frac{d'}{e}\right) \\ &= \log\left(\frac{c_3c_4\delta}{e}\right) + \log(d') - \log(\delta) \end{aligned}$$

et, puisque $\dfrac{c_3c_4\delta}{e} \geqslant 1$, $h(P_3) + h(P_4) \geqslant \log(d') - \log(\delta)$.

(f) Les hypothèses $x_1 \neq x_2$ et $P_1 \pm P_2 = \infty$ sont équivalentes. On peut, d'après III.4., choisir $d = (a_1a_2 + D^2c_1c_2)^2$, $d' = (a_1a_2 + D(a_1c_2 + a_2c_1) - D^2c_1c_2)^2$, $e = (a_1c_2 - a_2c_1)^2$. Comme $\delta | [(2D)^3]^2$ d'après 2.d., on a $\log(\delta) \leqslant 2\log((2D)^3)$. Par ailleurs, en utilisant $x_i \geqslant D$ (donc $a_i \geqslant c_iD$) :

$$\begin{aligned} \log(d') &= 2\log((a_1 + Dc_1)(a_2 + Dc_2) - 2D^2c_1c_2) \\ &= 2(h(P_1) + h(P_2)) + 2\log\left(1 - \frac{2D^2c_1c_2}{(a_1 + Dc_1)(a_2 + Dc_2)}\right) \\ &\geqslant 2(h(P_1) + h(P_2)) + 2\log\left(1 - \frac{2D^2c_1c_2}{(Dc_1 + Dc_1)(Dc_2 + Dc_2)}\right) \\ &\geqslant 2(h(P_1) + h(P_2)) - 2\log(2) \end{aligned}$$

d'où, en utilisant 2.e.,

$$h(P_1 + P_2) + h(P_1 - P_2) \geqslant 2(h(P_1) + h(P_2)) - 2\log(2(2D)^3)$$

3. (a) Les solutions, dans $G$, de l'équation $z^2 = 1$ sont 1 et $-1$. Or $E(\infty) = 1$, $L(0) = \Omega/2$ (car $L(0) + L(-0) = \Omega$), d'où $E(D, 0) = -1$. Et les solutions dans $\overline{C}$ de $2P = \infty$ sont $\infty$ et $(D, 0)$. Comme elles sont rationnelles, ce sont aussi les solutions dans $\overline{C}(\mathbb{Q})$.

(b) Résolvons, en préliminaire, les équations $2P = \infty$, $3P = \infty$, $4P = \infty$ dans $C(\mathbb{Q})$.

Si $2P = \infty$, $P = (D, 0)$ d'après 3.a.

$4P = \infty$ équivaut à $2P = \infty$ ou $2P = (D, 0)$ (ce qui, d'après ce qui a été vu en IV.A.3.c, n'est pas possible), donc à $P = (D, 0)$.

Enfin, l'équation $3P = \infty$ n'a pas de solution dans $C(\mathbb{Q})$. Elle peut en effet s'écrire $2P + P = \infty$, c'est-à-dire que le "troisième" point d'intersection de la tangente $Y = uX + v$ en $P$ à $C$ est $P$ lui-même (voir remarque faite en II.6.b.). Or, si le polynôme $P_{u,v} = X^3 - D^2X - (uX + v)^2$ admet une racine triple, c'est la racine de $P''_{u,v} = 3X - 2u^2$. Donc $x = \dfrac{u^2}{3}$, $P_{u,v} = \left(X - \dfrac{u^2}{3}\right)^3$, d'où $u^6 = 27v^2$, $u^4 = -3(D^2 + 2uv)$. Le point $P = (x, y) = (\dfrac{u^2}{3}, ux + v)$ devant être à coordonnées rationnelles, on voit successivement que $u^2 \in \mathbb{Q}$, $uy = u^2x + uv = u^2x - \dfrac{u^4}{6} - \dfrac{D^2}{2} \in \mathbb{Q}$, donc $u = \dfrac{uy}{y} \in \mathbb{Q}$ et $v = y - ux \in \mathbb{Q}$, ce qui n'est pas compatible avec la relation $u^6 = 27v^2$ (valuation de 3).

La relation désirée est clairement satisfaite lorsque $P = \infty$ ou $P = (D, 0)$ (car $h((D, 0)) = \log(2D)$). Supposons $P \in C(\mathbb{Q}) \setminus \{(D, 0)\}$ (donc $3P \pm P \neq \infty$, $2P \pm P \neq \infty$). On a en utilisant 1. et 2.f.,

$$\begin{aligned} 4h(2P) + h(2P) &\geqslant h(4P) + h(2P) \\ &\geqslant h(3P + P) + h(3P - P) \\ &\geqslant 2(h(3P) + h(P)) - 2\log(2(2D)^3) \\ &\geqslant 2(h(2P + P) + h(2P - P)) - 2\log(2(2D)^3) \\ &\geqslant 4(h(2P) + h(P)) - 6\log(2(2D)^3) \end{aligned}$$

d'où, en effet,

$$h(2P) \geqslant 4h(P) - 6\log(2(2D)^3)$$

(c) Cela résulte immédiatement de IV.B.2.f. et IV.B.3.b.

(d) En appliquant 3.c. à $P+Q$ et $P-Q$, il vient $h(2P)+h(2Q) \geqslant 2(h(P+Q)+h(P-Q))-A$. Puis, en utilisant 1., $h(P + Q) + h(P - Q) \leqslant h(P) + h(Q) + \dfrac{A}{2}$. Ce qui, avec 3.c., montre que $h$ (qui est bien positive) est une hauteur sur $\overline{C}(\mathbb{Q})$.

(e) Soit $B \in \mathbb{R}_+$. Si $P = (x, y) \in C(\mathbb{Q})$ est tel que $h(P) \leqslant B$, alors, avec les notations utilisées auparavant, $c(x + D) \leqslant e^B$ d'où, puisque $x \geqslant D$, $c \leqslant \dfrac{1}{2D} e^B$ et $a = cx \leqslant c(x + D) \leqslant e^B$. Les valeurs possibles pour $x = \dfrac{a}{c}$ sont donc en nombre fini, $\{P \in \overline{C}(\mathbb{Q});\ h(P) \leqslant B\}$ est fini et $h$ est une hauteur admissible.

(f) L'existence d'une hauteur admissible sur $\overline{C}(\mathbb{Q})$ montre, en vertu de I.3.c, que $\overline{C}(\mathbb{Q})_{\text{tors}}$ est fini et, en vertu de I.3.e et IV.A.3.d., que $\overline{C}(\mathbb{Q})$ est de type fini.