Correction
ENS (Filière MP) Paris, Lyon
Mathématiques

R. LOUBOUTIN
Lycée Chateaubriand
Trabujo.Louboutin@wanadoo.fr

29 août 2003

Partie I

I.1.a : $n.0 = 0$, si $n.x = 0$ et $m.y = 0$ alors $mn.(x - y) = 0$, donc Γ_{tors} est un sous-groupe.

I.1.b : Prenons pour Γ le groupe multiplicatif des racines de l'unité dans $\mathbb{C}$. Il est infini et tout élément est de torsion.

I.2.a : Soit z dans Γ, posons $u_n = 4^{-n}h(2^n z)$. En prenant $x = y = 2^n z$ et en multipliant l'inégalité vérifiée par h par $4^{-(n+1)}$ on obtient :

$$|u_{n+1} - u_n + h(0)4^{-(n+1)}| \leq M \times 4^{-(n+1)}.$$

Soit $|u_{n+1} - u_n| \leq (M + h(0))4^{-(n+1)}$. Or $\sum 4^{-(n+1)}$ converge et par conséquent $\sum u_{n+1} - u_n$ converge (absolument) et la suite (u_n) est convergente. $\hat{h}(x)$ existe.

$$h(x) - \hat{h}(x) = u_0 - \lim u_n = \sum_{n=0}^{+\infty} u_n - u_{n+1}$$

donc

$$|h(x) - \hat{h}(x)| \leq \sum_{n=0}^{+\infty}(M + h(0))4^{-(n+1)} = \frac{M + h(0)}{3} = M'.$$

I.2.b : On remplace x par $2^n x$, y par $2^n y$, on divise par 4^n puis on fait tendre n vers $+\infty$, on obtient

$$|\hat{h}(x + y) + \hat{h}(x - y) - 2\hat{h}(x) - 2\hat{h}(y)| \leq 0$$

soit :

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

I.2.c : $x = y = 0$ donne $\hat{h}(0) = 0$. On a aussi

$$\hat{h}((n + 1).x) = 2\hat{h}(n.x) + 2\hat{h}(y) - \hat{h}((n - 1).x),$$

donc $\hat{h}(2x) = 4\hat{h}(x)$ puis par récurrence $\hat{h}(n.x) = n^2\hat{h}(x)$. En prenant $x = 0$ on a $\hat{h}(-y) = \hat{h}(y)$ et finalement, pour tout n dans $\mathbb{Z}$: $\hat{h}(n.x) = n^2\hat{h}(x)$.

I.3.a : $\hat{h}(x) \leq B$ implique $h(x) \leq B + M'$. Or h est admissible donc pour tout B $\{x \in \Gamma; h(x) \leq M' + B\}$ est fini. Pour tout B il en est de même de $\{x \in \Gamma; \hat{h}(x) \leq B\}$ et $\hat{h}$ est admissible.

I.3.b : Soit x tel que $\hat{h}(x) = 0$, alors, pour tout n dans $\mathbb{Z}$ $\hat{h}(n.x) = 0$. En prenant $B = 0$ on peut affirmer que $\{y; \hat{h}(y) = 0\}$ est fini. Il existe donc m et n avec $m > n$ tels que $m.x = n.x$, soit $(m - n).x = 0$, et $x \in \Gamma_{\text{tors}}$. Réciproquement, si $x \in \Gamma_{\text{tors}}$, il existe $n \neq 0$ tel que $n.x = 0$. Donc $n^2\hat{h}(x) = \hat{h}(n.x) = 0$ et $\hat{h}(x) = 0$.

I.3.c : On a déjà dit que $\{x; \hat{h}(x) = 0\}$ est fini.

I.3.d : Si $x = z + 2y$ on a

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

Or $\hat{h}(2.(x + y)) \geq 0$ et $\hat{h}(2.y) = 4\hat{h}(y)$ donc

$$\hat{h}(y) \leq \frac{\hat{h}(x) + \hat{h}(z)}{2}.$$

I.3.e : Soit Z fini tel que

$$\forall x \in \Gamma \ \exists y \in \Gamma \ \exists z \in Z \quad x = z + 2y.$$

Soit $M = 1 + \max_{z \in Z} \hat{h}(z)$, alors $\mathcal{E} = \{y; \hat{h}(y) \leq 2M\}$ est fini et contient Z. Notons $\mathcal{E} = \{x_1, \ldots, x_n\}$. Tout élément x tel que $\hat{h}(x) \leq 2M = (2^0 + 1)M$ s'écrit sous la forme $x = \sum n_i x_i$ où les n_i sont entiers. Soit x tel que $\hat{h}(x) \leq (2^{n+1} + 1)M$, on peut l'écrire $x = z + 2y$ avec $z \in Z$ et $\hat{h}(y) \leq (2^n + 1)M$ d'après l'inégalité de la question précédente.
On en déduit par récurrence sur n que tout élément x de Γ tel que $\hat{h}(x) \leq (2^n + 1)M$ peut s'écrire sous la forme $x = \sum n_i x_i$ où les n_i sont entiers. Puisque $M > 0$, tout élément de Γ s'écrit donc sous la forme $x = \sum n_i x_i$ où les n_i sont entiers.

Partie II

II.1.a : $P_{u,v}$ possède au plus trois racines et la donnée de x détermine (x, y) sur $D_{u,v}$.

II.1.b : $P_{u,v}$ est exactement de degré 3. Il posséde donc trois racines réelles distinctes et strictement positives si et seulement si :
– $P'_{u,v}$ possède deux racines distinctes strictement positives, notée α et β ;
– $P_{u,v}(\alpha)P_{u,v}(\beta) < 0$;
– $P_{u,v}(0) < 0$.
Toutes ces conditions se transcrivent en des inégalités strictes sur des fonctions polynomiales des coefficients de $P_{u,v}$ c'est-à-dire polynomiales donc continues en (u, v). L'ensemble des (u, v) vérifiant ces conditions est donc un ouvert de $\mathbb{R}^2$.
Explicitement ces conditions deviennent respectivement
– $\Delta' = u^4 + 3(D^2 + 2uv) > 0$, $3(\alpha + \beta) = u^2 > 0$, $3\alpha\beta = -(D^2 + 2uv) > 0$;
– $R(u, v) = 27\left(\frac{2u^6}{27} + \frac{u^2(D^2+2uv)}{3} + v^2\right)^2 - 4\left(D^2 + 2uv + \frac{u^4}{3}\right)^3 < 0$;
– $-v^2 < 0$.

II.1.c : Si $P_{u,0}(x) = x^3 - D^2x^2 - u^2x$, donc si $v = 0$, $P_{u,v}$ possède pour racine 0 et deux racines réelles dont le produit est $-u^2 < 0$. Si $P_{u,v}$ possède deux racines réelles strictement positives, alors il possède nécessairement une troisième racine réelle et le produit de ces trois racines est v^2 qui est strictement positif ; la troisième racine est donc strictement positive. Si on suppose de plus que $D_{u,v}$ n'est pas tangente à C, $P_{u,v}$ n'a pas de zéro double d'après $T2$ et $n(u, v) = 3$.

II.1.d : Au vu de l'équation de la tangente, il n'y a qu'un seul point où elle soit verticale ($P_0 = (D, 0)$) et il n'existe aucun point où elle soit horizontale (car $x_0 > 0$).
Une droite non verticale et non horizontale passant pas (a, b) est de la forme $D_{u,b-ua}$, $u \neq 0$. Pour qu'une telle droite soit tangente à C il est nécessaire que $R(u, b - ua) = 0$. Or $T(X) = R(X, b - aX)$ est non identiquement nul (Il existe au moins une droite passant par (a, b) qui n'est pas tangente à C (la limite quand x tend vers $+\infty$ de $y'(x) - \frac{y(x)-b}{x-a}$ est infinie), on peut aussi expliciter T (merci Maple) :

$$T(X) = \left(-4\,a^3 + 4\,D^2a\right)X^6 + \left(-4\,D^2b + 12\,ba^2\right)X^5 + \left(-12\,b^2a + 27\,a^4 - D^4 - 30\,D^2a^2\right)X^4 +$$
$$\left(-108\,ba^3 + 4\,b^3 + 60\,D^2ba\right)X^3 + \left(24\,D^4a - 30\,D^2b^2 + 162\,b^2a^2\right)X^2 + \left(-108\,b^3a - 24\,D^4b\right)X - 4\,D^6 + 27\,b^4.$$

Il n'existe donc qu'un nombre fini de u tels que $R(u, b - ua) = 0$ (au maximum 6 d'après l'expression de T, en fait 4 car on ne considère qu'une branche de la courbe. Ce nombre est atteint par exemple pour $(\frac{D}{2}, 0)$.)

II.2.a : Il s'agit de prouver que $x^3 - D^2x - t^2$ possède une et une seule racine réelle strictement positive. Soit $f_t(x) = x^3 - D^2x - t^2$, cette fonction est strictement inférieure à $-t^2$ sur $]0, D[$ strictement croissante sur $[D, +\infty[$ et continue. De plus elle tend vers $+\infty$ en $+\infty$. Il suffit d'appliquer le théorème des valeurs intermédiaires.

II.2.b : $F(y) \geq 2$ a été vu à la question précédente. F est de classe $\mathcal{C}^1$, d'après le théorème des fonctions implicites, puisque $\phi : (x, y) \mapsto x^3 - D^2x - y^2$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}^2$ et $\frac{\partial \phi}{\partial x} : (x, y) \mapsto 3x^2 - D^2$ ne s'annule pas sur C. (Ce théorème, plutôt hors-programme, peut avoir été vu en géomètrie. On peut aussi conclure en appliquant la caractérisation des difféomorphismes à $x \mapsto \sqrt{x^3 - D^2x}$ et $x \mapsto -\sqrt{x^3 - D^2x}$ pour prouver que F est $\mathcal{C}^1$ sur $\mathbb{R}^{*+}$ et $\mathbb{R}^{*-}$ puis montrer que les limites de F et F' esistent en 0.)

II.2.c : On a $F(y)^3 \geq y^2$ donc lorsque $|y|$ tend vers $+\infty$ $F(y)$ tend vers $+\infty$. Ensuite $1 = \frac{D^2}{F(y)^2} + \frac{y^2}{F(y)^3}$ donc $\frac{y^2}{F(y)^3}$ tend vers 1.

II.2.d : $D(a, t)$ a pour équation

$$y - t = \frac{a - t}{F(a) - F(t)}(x - F(t))$$

(remarquons que $F(a) - F(t) \neq 0$ car $t \notin \{a, -a\}$). $D(a, t) = D_{u,v}$ avec

$$u = \frac{a - t}{F(a) - F(t)} \quad v = \frac{tF(a) - aF(t)}{F(a) - F(t)}.$$

On peut associer à (u, v) le couple (u', v') :

$$u' = \frac{F(a) - F(t)}{a - t} \quad v' = \frac{tF(a) - aF(t)}{t - a}.$$

Le produit des trois racines de $Q_{u',v'}$ (qui possède bien trois racines réelles puisqu'il en possède au moins deux : a et t) est $-\frac{v'^3 - D^2v'}{u'^3}$, donc

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

On en déduit que trois cas sont possibles, qui s'excluent l'un l'autre :
- $H_a(t) \notin \{a, t\}$, $Q_{u',v'}$ possède trois racines distinctes. D'après $T3$ $D(a, t)$ n'est pas tangente à C. Or, d'après $II.1.c$, puisque $n(u, v) \geq 2$, $n(u, v) = 3$ et $P(H_a(t))$ est le troisième point d'intersection.
- $H_a(t) = a$ et $Q_{u',v'}$ a un zéro double en a, donc $D(a, t)$ est tangente à C en $P(a)$.
- $H_a(t) = t$ et $Q_{u',v'}$ a un zéro double en t, donc $D(a, t)$ est tangente à C en $P(t)$.

II.2.e : $F(t) \sim t^{2/3}$ en $+\infty$, donc

$$atH_a(t) = -\left(\frac{t}{t^{2/3}}\right)^3 (1 + \mathrm{o}(1))\left(F(a)^3 - D^2F(a) + \mathrm{o}(1)\right).$$

Or $F(a)^3 - D^2F(a) = a^2$ donc $H_a(t)$ tend vers $-a$. La droite $D(a, t)$ devient verticale. Elle tend vers la parallèle à l'axe des ordonnées passant par $P(a)$.

II.3.a : $t \mapsto 3F(t)^2 - D^2$ est continue sur $\mathbb{R}$ et strictement positive. En $\pm\infty$ $\frac{2}{3F(t)^2 - D^2} \sim \frac{2}{|t|^{4/3}}$ avec $\frac{4}{3} > 1$. Donc $\phi : t \mapsto \frac{2}{3F(t)^2 - D^2}$ est intégrable sur $\mathbb{R}$.
ϕ est continue donc L est de classe $\mathcal{C}^1$ sur $\mathbb{R}$ et $L' = \phi > 0$. L est par conséquent un difféomorphisme de $\mathbb{R}$ sur $L(\mathbb{R})$ qui est un intervalle. $\lim_{y \to -\infty} L(y) = 0$, $\lim_{y \to +\infty} L(y) = \Omega$, donc L est un difféomorphisme de $\mathbb{R}$ sur $]0, \Omega[$.

II.3.b :

$$L(y) + L(-y) = \int_{-\infty}^{y} \frac{2}{3F(t)^2 - D^2} dt + \int_{-\infty}^{-y} \frac{2}{3F(t)^2 - D^2} dt.$$

Or F est paire, en effectuant le changement de variable $t = -u$ dans la deuxième intégrale on obtient :

$$L(y) + L(-y) = \int_{-\infty}^{y} \frac{2}{3F(t)^2 - D^2} dt + \int_{y}^{+\infty} \frac{2}{3F(t)^2 - D^2} dt = \Omega.$$

II.4.a : Le membre de droite est un polynôme R de degré au plus $n-1$ tel que pour tout i $R(x_i) = Q(x_i)$. $R - Q$ est de degré au plus $n-1$, il possède au moins n racines, donc il est nul et $R = Q$.

II.4.b : On choisit $Q(X) = X^k$ $k \in \{0, \ldots, n-2\}$.

$$X^k = \sum_{i=1}^{n} x_i^k \prod_{j \neq i} \frac{(X - x_j)}{(x_i - x_j)}.$$

En identifiant X^{n-1}

$$0 = \sum_{i=1}^{n} \frac{x_i^k}{\prod_{j \neq i}(x_i - x_j)} = \sum_{i=1}^{n} \frac{x_i^k}{P'(x_k)}.$$

De même

$$1 = \sum_{i=1}^{n} \frac{x_i^{n-1}}{P'(x_k)}.$$

II.5.a : (La question qui m'a vraiment posé un problème, il y a peut être plus simple que ma solution.) Puisque F est de classe $\mathcal{C}^1$ les x_i sont de classe $\mathcal{C}^1$. u et v se déterminent en résolvant un système et s'expriment donc rationnellement à l'aide de x_1, x_2, y_1 et y_2 et sont donc de classe $\mathcal{C}^1$.

$$G'(t) = \frac{2y_1'(t)}{3y_1^2(t) - D^2} + \frac{2y_2'(t)}{3y_2^2(t) - D^2} + \frac{2y_3'(t)}{3y_3^2(t) - D^2} = 2\sum_{i=1}^{3} \frac{2y_1'(t)}{3y_1^2(t) - D^2}.$$

Or

$$\begin{cases} y & = & ux + v \\ y^2 = x^3 - D^2 x & & \end{cases}$$

et u et v sont de classe $\mathcal{C}^1$. En dérivant

$$\begin{aligned} y' &= u'x + v' + ux' && (1) \\ 2yy' &= (3x^2 - D^2)x' && (2) \\ & && (3) \end{aligned}$$

En multipliant (1) par $3x^2 - D^2$:

$$(3x^2 - D^2)y' = (u'x + v')(3x^2 - D^2) + 2uyy'$$

soit

$$(3x^2 - D^2 - 2uy)y' = (u'x + v')(3x^2 - D^2),$$

puis

$$\frac{y'}{3x^2 - D^2} = \frac{u'x + v'}{3x^2 - D^2 - 2u(ux + v)}.$$

Par conséquent, si

$$P_{u,v} = X^3 - D^2 X - (uX + v)^2 = (X - x_1)(X - x_2)(X - x_3) \ :$$

$$\frac{y_i'}{3x_i^2 - D^2} = u' \frac{x_i}{P'_{u,v}(x_i)} + v' \frac{1}{P'_{u,v}(x_i)}.$$

D'après la question précédente :

$$G' = \sum_{i=1}^{3} \frac{2y_i'}{3x_i^2 - D^2} = 0$$

et G est constante.

II.5.b : La formule de la question $II.2.d$ montre que H_a est de classe $\mathcal{C}^1$ sur $]-\infty, -a[$, $]-a, 0[$, $]0, a[$ et $]a, +\infty[$ si $a > 0$. La fonction $L(a) + L(t) + L(H_a(t))$ est constante sur $]a, +\infty[$. En faisant tendre t vers $+\infty$ on obtient la valeur constante $L(a) + \Omega + L(-a) = 2\Omega$.

II.5.c : Soient y_1, y_2 et y_3 distincts deux à deux et tels que $P(y_1)$, $P(y_2)$ et $P(y_3)$ soit alignés. Deux au moins des y_i sont non nuls et il ne peut y avoir de couple de valeurs opposées sinon dans ce cas la droite passant par ces deux points serait verticale et ne pourrait couper C en un troisième point. On peut supposer $y_1 < y_2 < y_3$.

Dans un premier temps supposons les y_i non nuls. Si $0 < y_2 < y_3$ on prend $a = y_2$ et $t = y_3$ donc $y_1 = H_a(t)$. D'après la proposition précédente $L(y_1) + L(y_2) + L(y_3) = 2\Omega$. Si $y_1 < y_2 < 0$, on se ramène au cas précédent en passant à l'opposé

$$L(-y_1) + L(-y_2) + L(-y_3) = 2\Omega = 3\Omega - L(y_1) - L(y_2) - L(y_3)$$

donc $L(y_1) + L(y_2) + L(y_3) = \Omega$.
Si un des y_i est nul en utilisant la symétrie précédente on se ramène aux cas $y_1 = 0$ ou $y_2 = 0$. On conclue en utilisant un argument de continuité.
Si $y_1 = 0$, on prend $y_{1,\epsilon} = \epsilon$, $y_{2,\epsilon} = y_2$ et $y_{3,\epsilon} = H_{y_2}(\epsilon)$. Les valeurs u'et v' associées à la doite passant par $P(y_{1,\epsilon})$ et $P(y_{2,\epsilon})$ sont des fonctions continues de ϵ dans un voisinage de 0 (ce sont des fonctions rationnelles de ϵ) or

$$y_{1,\epsilon} + y_{2,\epsilon} + y_{3,\epsilon} = -\frac{3u'^2v' - 1}{u'^3}$$

Donc $y_{3,\epsilon}$ est une fonction continue de ϵ. En composant par L et en passant à la limite on obtient $L(y_1) + L(y_2) + L(y_3) = 2\Omega$.
Le cas $y_2 = 0$ est impossible. Cela se voit géométriquement, nécessairement $x_2 = D$, suivant le signe de u' on aura $x_1 < D$ ou $x_3 < D$ ce qui est impossible.

II.5.d : On utilise la même technique de passage à la limite en prenant $y_{1,\epsilon} = y_1$, $y_{2,\epsilon} = y_1 + \epsilon$ et $y_{3,\epsilon} = y_2$.

II.5.e : L'application $y \mapsto L(y_1) + L(y_2) + L(y)$ est injective et à valeurs dans un intervalle $]\alpha, \alpha + \Omega[$ et ne peut prendre une valeur dans $\mathbb{Z}\Omega$ que pour une valeur de y. Or elle vaut Ω ou 2Ω pour $y = y_4$ tel que $P(y_1)$, $P(y_2)$ et $P(y_4)$ soient alignés. Donc si $L(y_1) + L(y_2) + L(y_3)$ appartient à $\mathbb{Z}\Omega$ alors $y_3 = y_4$ et $P(y_1)$, $P(y_2)$ et $P(y_3)$ sont alignés.

II.6.a : L est à valeurs dans $]0, \Omega[$ donc puisque L est injective et $t \mapsto e^{it}$ est injective sur $]0, 2\pi[$, E est injective sur C et pour tout P de C $E(P) \neq 1$, donc E est injective sur $\overline{C}$ et à valeurs dans U. L'image de L est $]0, \Omega[$ donc l'image de C par E est $U - \{1\}$ et E réalise donc une bijection de $\overline{C}$ sur U. On peut donc transporter à l'aide de cette bijection la structure de groupe multiplicatif sur U, ce qui définit $+$ de manière unique par $E(P + Q) = E(P)E(Q)$.
On a $L(y(P+Q)) \equiv L(y(P) + L(y(Q)) \bmod \Omega$ or $L(y(P) + L(y(Q)) \in]0, 2\Omega[$ et $L(y(P+Q)) \in]0, \Omega[$. Le résultat demandé en découle car le cas $L(y(P) + L(y(Q)) = \Omega$ est impossible puisque $P + Q \neq \infty$. Si P ou Q est égal à ∞ le résultat reste valable en prenant la convention $y(\infty) = -\infty$ et $L(-\infty) = 0$.

II.6.b : ∞ est l'image réciproque de 1 par l'isomorphisme E, c'est l'élément neutre de $(\overline{C}, +)$.

$$P_1 + P_2 + P_3 = \infty \Longleftrightarrow L(y(P_1)) + L(y(P_2)) + L(y(P_3)) \in \mathbb{Z}\Omega.$$

Et d'après *IV.5.c* cette deuxième condition veut dire que les P_i sont alignés (on passe rapidement sur le cas particulier ou l'un des P_i est ∞, qui se traite à part.)

II.6.c : Résulte de $L(-y) = \Omega - L(y)$.

II.6.d : Si $P = \infty$ alors $2Q = P$ et $Q = L(z)$ équivaut à $2L(z) \in \mathbb{Z}\Omega$ c'est à dire $L(z) = 0$ ou $L(z) = \frac{\Omega}{2}$. Il y a deux solutions $P = \infty$ et $P = (D, 0)$. Sinon $P = P(y)$ et $2Q = P$ et $Q = L(z)$ équivaut à $2L(z) \equiv L(y) \bmod \Omega$. Nous obtenons encore deux solutions $L(z) = \frac{L(y)}{2}$ et $L(z) = \frac{L(y)+\Omega}{2}$

II.6.e : Si $y_1 + y_2 > 0$ par exemple, alors $z_1 + z_2 > 0$ pour z_1 et z_2 respectivement assez proches de y_1 et y_2. Donc $P(z_1) + P(z_2) \neq \infty$ et est bien de la forme $(F(y), y)$. La continuité de F, donc de P, permet de conclure. Si $y_1 + y_2 = 0$ alors $|y(P(z_1) + P(z_2))|$ tend vers $+\infty$ mais $y(P(z_1) + P(z_2))$ peut ne pas avoir de limite.

Partie III

III.1.a : Il suffit de déterminer explicitement les coefficients u et v de la droite passant par les deux points distincts (x_1, y_1) et (x_2, y_2). Elle a bien pour équation

$$y = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1).$$

Si les P_i sont distincts alors cette équation admet exactement x_1, x_2 et x_3 pour racines distinctes (condition T) si P_3 est égal à P_1 ou P_2 le résultat reste valide en considérant les racines doubles (toujours la condition T). Dans tous les cas $P(x) = (x-x_1)(x-x_2)(x-x_3)$. Les relations entre les coefficients et les racines donnent alors :

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

car $y_1 + y_2 \neq 0$ puisque $x_1 \neq x_2$. De plus

$$y_2^2 - y_1^2 = x_2^3 - x_1^3 - D^2(x_2 - x_1) = (x_2 - x_1)(x_1^2 + x_1x_2 + x_2^2 - D^2).$$

Le résultat annoncé en découle et

$$y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) + y_1 = \frac{x_1^2 + x_1x_2 + x_2^2 - D^2}{y_2 + y_1}(x_3 - x_1) + y_1$$

par le même calcul.

III.1.b : Si x_1, x_2 et x_3 sont les racines de $P(x)$ alors $x_1 + D$, $x_2 + D$ et $x_3 + D$ sont les racines de $P(x - D)$ leur produit est donc

$$-P(0 - D) = \left(y_1 + \frac{y_2 - y_1}{x_2 - x_1}(-D - x_1)\right)^2 = \left(\frac{(x_1 + D)y_2 - (x_2 + D)y_1}{x_2 - x_1}\right)^2.$$

III.2.a : On utilise un argument de continuité comme en $II.5.d$ pour faire tendre (x_1, y_1) et (x_2, y_2) vers (x, y), avec $x_1 \neq x_2$, c'est possible car $y \neq 0$ (prendre $y_{1\epsilon} = y - \epsilon$, $y_{2\epsilon} = y + \epsilon$.)Si P_3 est tel que $2P + P_3 = \infty$ alors $(x_3, y_3) = (x' - y')$, et il suffit de passer à la limte dans $III.1.a$.

III.2.b : Trivial $(x^2 + D^2)^2 = (3x^2 - D^2)^2 - 8xy^2$ car $y^2 = x^3 - D^2x$.

III.3 : Toutes les questions précédentes montrent que $\overline{C}(\mathbb{Q})$ est stable pour $+$ et passage au symétrique (Il y a un certain nombre de cas à étudier suivant que $P = Q$ ou $P + Q = \infty$).

III.4 : On a $P1 + P2 + (-P3) = \infty$ et $P1 + (-P2) + (-P4) = \infty$. La formule de la question $III.1.b$ donne pour ces deux relations :

$$\begin{aligned}(x_1 + D)(x_2 + D)(x_3 + D) &= \left(\frac{(x_1 + D)y_2 - (x_2 + D)y_1}{x_2 - x_1}\right)^2 \\ (x_1 + D)(x_2 + D)(x_4 + D) &= \left(\frac{(x_1 + D)y_2 + (x_2 + D)y_1}{x_2 - x_1}\right)^2\end{aligned}$$

On effectue le produit

$$(x_1 + D)^2(x_2 + D)^2(x_3 + D)(x_4 + D) = \left(\frac{(x_1 + D)^2y_2^2 - (x_2 + D)^2y_1^2}{(x_2 - x_1)^2}\right)^2.$$

Or $y_2^2 = x_2(x_2 + D)(x_2 - D)$ avec une formule similaire pour y_1^2. On simplifie par $(x_1 + D)^2(x_2 + D)^2$ qui est non nul.

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

Une ultime simplification de la fraction rationnelle donne le résultat voulu.

Partie IV

IV.A

IV.1.a : Si a dans $\mathbb{Q}^*$ est un carré alors $a > 0$ et $a = b^2$ et $v_p(a) = 2v_p(b)$ pour tout p c'est-à-dire $\overline{v_p(a) = 0}$. De même si $a > 0$ et $\overline{v_p(a) = 0}$ pour tout p, alors $v_p(a) = 2k_p$ pour tout p si $b = \prod_p p^{k_p}$ alors $a = b^2$.

IV.A.1.b : $a = p^{v_p(a)}\frac{n}{d}$ où sont des entiers premiers entre eux et non divisibles par p. De même $b = p^{v_p(b)}\frac{n'}{d'}$ et

$$a+b = p^{v_p(a)}\frac{nd' + p^{v_p(b)-v_p(a)}n'd}{dd'} = p^{v_p(a)}\frac{n''}{d''}.$$

D'après le théorème de Gauss dd' n'est pas divisible par p, ainsi que nd'. On en déduit que n'' et d'' ne sont pas divisibles par p puis que $v_p(a+b) = v_p(a)$.

IV.A.2.a : $v_p(c)$ est pair car c est un carré, donc $v_p(c) \geq 1$ implique $v_p(c) \geq 2$.
$v_p(a) \geq 0$ car a est entier. Si $v_p(c) \geq 1$ (donc ≥ 2) et $v_p(a) \geq 2$ on peut remplacer c par $\frac{c}{p^2}$ ce qui contredit la minimalité de c.

IV.A.2.b : $x(x-D)(x+D) = y^2$ donc $a(a-Dc)(a+Dc) = c^3y^2 = (z^3y)^2$. Puisque $a(a-Dc)(a+Dc)$ est un entier, z^3y est aussi un entier (utiliser $IV.A.1.a$)

IV.A.2.c : On vient de voir $a(a-Dc)(a+Dc) = b^2$. Soit $p \notin S \cup \{2\}$ tel que $v_p(b) \geq 1$ alors $v_p(a(a-Dc)(a+Dc))$ est pair.
Si $v_p(a) \geq 1$ deux cas sont possibles :
– $v_p(c) \geq 1$ et dans ce cas $v_p(a) = 1$ et $v_p(c) \geq 2$ d'après $IV.A.2.a$ donc $v_p(a-Dc) = v_p(a+Dc) = 1$ et $v_p(a)$ est pair (ce cas n'est en fait donc pas possible) ;
– $v_p(c) = 0$ alors puisque $v_p(D) = 0$ on a $v_p(a-Dc) = v_p(a+Dc) = 0$ et $v_p(a)$ est pair.
De même, puisque $a - Dc) = (a+Dc) - 2Dc$ et $a = (a+Dc) - Dc$ et $v_p(2D) = 0$, on prouverait que $v_p(a+Dc)$ est pair.

IV.A.3.a : Si $P = (x,y) = P_1 + P_2$ alors $x = x_3$ ou $x = x'$ où $P_1 + P_2 + P_3 = \infty$ ou $2P_1 + P' = \infty$, suivant que $P_1 \neq P_2$ ou non. Il résulte des formules de $III.1.b$ et $III.2.b$ que

$$\begin{aligned}
\overline{v_p(x_1+D)} + \overline{v_p(x_2+D)} + \overline{v_p(x_3+D)} &= 0,\\
\overline{v_p(x_1)} + \overline{v_p(x_2)} + \overline{v_p(x_3)} &= 0,\\
\overline{v_p(x'+D)} &= 0,\\
\overline{v_p(x')} &= 0.
\end{aligned}$$

Dans les deux cas ($P_1 = P_2$ ou non)

$$\begin{aligned}
\overline{v_p(x+D)} &= \overline{v_p(x_1+D)} + \overline{v_p(x_2+D)}\\
\overline{v_p(x)} &= \overline{v_p(x_1)} + \overline{v_p(x_2)}
\end{aligned}$$

et ϕ est bien un morphisme.

IV.A.3.b : Si x', $x'-D$ et $x'+D$ sont des carrés et si $2Q = P$ alors

$$\frac{x^2+D^2}{2y}, \quad \frac{x^2+2Dx-D^2}{2y} \text{ et } \frac{x^2-2Dx-D^2}{2y}$$

sont des rationnels.
Par addition et soustraction

$$\frac{x^2+D^2}{2y}, \quad \frac{x^2-D^2}{2y} \text{ et } \frac{x}{y}$$

sont des rationnels. Finalement $\frac{D^2}{y}$ et $\frac{x}{y}$ sont des rationnels, puis x et y sont des rationnels.
On remarquera que nécessairement $y \neq 0$ ce qui justifie a posteriori le calcul.

IV.A.3.c :

$$x \in \ker\phi \iff \forall p \in S \cup \{2\} \quad \overline{v_p(x)} = 0 = \overline{v_p(x+D)}.$$

Or puisque

$$\forall p \in S \cup \{2\} \quad \overline{v_p(2D)} = 1$$

on a

$$\forall p \in S \cup \{2\} \quad \overline{v_p(x+D)} = 0 \Longrightarrow \overline{v_p(x-D)} = \overline{v_p((x+D)-2D)} = 0.$$

On a vu auparavant que

$$\forall p \notin S \cup \{2\} \quad \overline{v_p(x)} = \overline{v_p(a)} - \overline{v_p(c)} = 0 = \overline{v_p(x+D)} = \overline{v_p(x-D)}.$$

En conclusion

$$x \in \ker\phi \iff \forall p \quad \overline{v_p(x)} = 0 = \overline{v_p(x+D)} = \overline{v_p(x-D)}.$$

La condition nécessiare et suffisante peut s'exprimer plus simplement en disant que x, $x+D$ et $x-D$ sont des carrés.

IV.A.3.d : Soit Z une partie finie de $\overline{C}(\mathbb{Q})$ telle que $\phi(Z) = \operatorname{Im}\phi$. Cette image est finie car $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{2s+2}$ est fini. Soit P dans $\overline{C}(\mathbb{Q})$ et z dans Z tels que $\phi(z) = \phi(P)$, alors $\phi(z-P) = 0$. Or d'après les deux questions précédentes tout élément de $\ker\phi$ est de la forme $2Q$ où $Q \in \overline{C}(\mathbb{Q})$, donc tout élément de $\overline{C}(\mathbb{Q})$ est de la forme $z+2Q$ avec z dans une partie finie et $\overline{C}(\mathbb{Q})$ est de type fini modulo 2.

IV.B

IV.B.1 : On rappelle $x \geq D$ pour tout x de $C(\mathbb{Q})$. d'après la formule de $III.2.b$, si $2P = (x', y')$, $4c^4y^2(x'+D)$ est un entier donc

$$h(2P) \leq \ln(4c^4y^2(x'+D)) = \ln\left((c(x+D))^2 - 2c^2D^2\right)^2 \leq 4\ln(c(x+D)) \leq 4h(P).$$

IV.B.2.a : $2a_1(a_2+Dc_2) = T+U+DV$, $2a_2(a_1+Dc_1) = T+U-DV$. De même $4D^2a_1c_2^2 =?$ et $4D^2a_2c_1^2 =?$.

IV.B.2.b :

IV.B.2.c :

IV.B.2.d :

IV.B.2.e :

IV.B.2.f :

IV.B.3.a : Ce résultat a déjà été vu en $II.6.d$.

IV.B.3.b :

IV.B.3.c : D'après $IV.B.2.f$ et $IV.B.3.b$ on peut choisir $A = 6\ln(2(2D)^3)$.

IV.B.3.d : En substituant $(P+Q, P-Q)$ à (P,Q) dans l'inégalité précédente, puis en utilisant $IV.B.1$ on obtient

$$h(P+Q) + h(P-Q) \leq 2(h(P)+h(Q)) + \frac{A}{2}.$$

Avec l'autre inégalité, ceci implique

$$|h(P+Q) + h(P-Q) - 2(h(P)+h(Q))| \leq A.$$

h est bien une hauteur.

IV.B.3.e : Si $B > 0$ alors $1 \leq c \leq e^B$ et $D \leq a \leq e^B$ dès que $h(x) \leq B$. Il y a donc un nombre fini de tels x. h est admissible.

IV.B.3.f : C'est $I.3.c$ et $I.3.e$.