Devoir de Mathématiques n°10

Kévin Polisano
MP*

Vendredi 15 janvier 2010

Partie I - Groupe commutatif de type fini

1. Soit $(x,y) \in \Gamma_{\text{tors}}^2$, alors $\exists n_1, n_2 \in \mathbb{Z} - \{0\}$ tels que $n_1 x = n_2 y = 0$.
Posons $n = \text{ppcm}(n_1, n_2)$ alors $n = k_1 n_1 = k_2 n_2$ et Γ_{tors} est un sous-groupe de Γ car :

$$n(x-y) = k_1(n_1 x) - k_2(n_2 x) = 0 \Rightarrow x - y \in \Gamma_{\text{tors}}$$

2. Considérons le groupe $(\mathbb{U}, \times)$ (ensemble des complexes de module 1 muni de la multiplication). Alors $\left(\bigcup_{k\in\mathbb{N}^*} \mathbb{U}_{2^k}, \times\right)$ où $\mathbb{U}_n$ est l'ensemble des racines n-ième de l'unité, est un sous-groupe (infini) de $(\mathbb{U}, \times)$ puisque $\mathbb{U}_2 \subset \mathbb{U}_4 \subset \cdots \subset \mathbb{U}_{2^k} \subset \cdots$, et pour tout élément x appartenant à cette réunion, il existe un $n \in \mathbb{Z} - \{0\}$ tel que $x^n = 1$ puisqu'elle est constituée des racines 2^k-ième de l'unité. Donc Γ_{tors} n'est pas nécessairement fini.

Un autre exemple avec un groupe additif cette fois : comme $(\mathbb{Z}, +)$ est clairement un sous-groupe distingué de $(\mathbb{Q}, +)$ on considère le groupe quotient $(\mathbb{Q}/\mathbb{Z}, +)$ formé des classes d'équivalences de la relation sur $\mathbb{Q}$: $x\mathcal{R}y \Leftrightarrow x - y \in \mathbb{Z}$ compatibles avec l'addition $\bar{x} + \bar{y} = \overline{x+y}$. Le neutre est donc $\bar{0} = \mathbb{Z}$, et $\mathbb{Q}/\mathbb{Z} = \{r + \mathbb{Z}, r \in \mathbb{Q}\}$. Par ailleurs les rationnels $0 \leqslant \frac{p}{q} < 1$ ne diffèrent pas d'un entier donc sont dans des classes distinctes, et comme il y en a une infinité (par exemple les $\frac{1}{n}$) alors l'ensemble $\mathbb{Q}/\mathbb{Z}$ est infini. Enfin remarquons que $\forall r = \frac{p}{q} \in \mathbb{Q}$ on a :

$$q\bar{r} = \underbrace{\overline{\frac{p}{q}} + \cdots + \overline{\frac{p}{q}}}_{q} = \underbrace{\overline{\frac{p}{q} + \cdots + \frac{p}{q}}}_{q} = \overline{\frac{qp}{q}} = \overline{p} = \overline{0}$$

Pour tout élément x du groupe quotient $(\mathbb{Q}/\mathbb{Z})$ on a donc exhibé un entier n tel que $nx = 0$.

2.a Soit h une hauteur de Γ, $\forall (t,z) \in \Gamma^2$ on a : $|h(t+z) + h(t-z) - 2h(t) - 2h(z)| \leqslant M$.
$x \in \Gamma$, on prend $t = z = 2^n x \in \Gamma$ d'où $|h(2^{n+1}x) - 4h(2^n x) + h(0)| \leqslant M$ on multiplie par $4^{-(n+1)}$

$$|4^{-(n+1)}h(2^{n+1}x) - 4^n h(2^n x) + h(0)| \leqslant 4^{-(n+1)}M \Rightarrow |u_{n+1}(x) - u_n(x)| \leqslant 4^{-(n+1)}(M + h(0))$$

en ayant posé $u_n(x) = 4^{-n}h(2^n x)$. Par l'inégalité triangulaire on a :

$$\begin{aligned} |u_{n+p}(x) - u_n(x)| &\leqslant |u_{n+p}(x) - u_{n+p-1}(x)| + |u_{n+p-1}(x) - u_{n+p-2}(x)| + \cdots + |u_{n+1}(x) - u_n(x)| \\ &\leqslant (M + h(0))\left[4^{-(n+p)} + 4^{-(n+p-1)} + \cdots + 4^{-(n+1)}\right] \\ &\leqslant (M + h(0))\tfrac{4}{3}\left(\tfrac{1}{4}\right)^{n+1}\left[1 - \left(\tfrac{1}{4}\right)^p\right] \\ &\leqslant (M + h(0))\tfrac{4}{3}\left(\tfrac{1}{4}\right)^{n+1} \longrightarrow 0 \end{aligned}$$

La suite $(u_n(x))$ vérifie le critère de Cauchy donc converge vers $\widehat{h}(x)$ pour tout $x \in \Gamma$. (car $\mathbb{R}^+$ complet). De plus en prenant $n = 0$ et en faisant tendre $p \to +\infty$ on a $|h(x) - \widehat{h}(x)| \leqslant \frac{1}{3} = M'$.

2.b On prend maintenant $t = 2^n x$ et $z = 2^n y$ et on multiplie par 4^{-n} :

$$|4^{-n}h(2^n(x+y)) + 4^{-n}h(2^n(x-y)) - 2(4^{-n}h(2^n x)) - 2(4^{-n}h(2^n y))| \leqslant 4^{-n}M \longrightarrow 0$$

et vu que $(4^{-n}h(2^n z))$ converge il vient : $\forall (x,y) \in \Gamma^2,\ \hat{h}(x+y) + \hat{h}(x-y) = 2\hat{h}(x) + 2\hat{h}(y)$.

2.c En prenant $x = y = 0$ on a $\hat{h}(0) = 0$, puis en prenant $x = 0$: $\hat{h}(-y) = \hat{h}(y)$.
Avec $x = y$ on a $\hat{h}(2x) = 4\hat{h}(x)$. Montrons alors par récurrence que $\forall n \in \mathbb{N}, \hat{h}(nx) = n^2\hat{h}(x)$.
Supposons la propriété vraie au rang $n-1$ et n et montrons qu'elle le reste au rang $n+1$:
$\hat{h}(nx+x)+\hat{h}(nx-x)+2\hat{h}(nx)+2\hat{h}(x) \Leftrightarrow \hat{h}((n+1)x) = 2n^2\hat{h}(x)+2\hat{h}(x)-(n-1)^2\hat{h}(x) = (n+1)^2\hat{h}(x)$
Et comme $\hat{h}(-nx) = \hat{h}(nx) = n^2\hat{h}(x) = (-n)^2\hat{h}(x)$ cela étend la propriété à $\mathbb{Z}$.

3.a $\hat{h}$ est clairement une hauteur vu 2.b (avec $M = 0$). Montrons alors qu'elle est admissible, raisonnons par l'absurde, supposons qu'il existe $B \geqslant 0$ tel que $A = \left\{x \in \Gamma, \hat{h}(x) \leqslant B\right\}$ soit infini, alors comme d'après 2.a $h(x) \leqslant M' + \hat{h}(x)$, l'ensemble $C = \{x \in \Gamma, h(x) \leqslant M' + B\}$ serait infini car $A \subset C$, ce qui est contradictoire car h est admissible. Ainsi $\forall B \geqslant 0$, l'ensemble des $x \in \Gamma$ tels que $\hat{h}(x) \leqslant B$ est fini, d'où $\hat{h}$ est admissible.

3.b Si $\hat{h}(x) = 0$ alors $\forall n \in \mathbb{Z}, \hat{h}(nx) = n^2\hat{h}(x) = 0$. Et comme $\hat{h}$ est admissible les zéros de $\hat{h}$ sont en nombre fini (prendre $B = 0$), notons E l'ensemble des zéros et m son cardinal. Si deux des kx pour $k \in [\![1, m]\!]$ sont égaux $k_1 x = k_2 x$ alors $(k_1 - k_2)x = 0$, si les kx sont tous distincts, alors $(m+1)x$ annulant $\hat{h}$ il appartient à E, donc $\exists k \in [\![1, m]\!]$ tel que $kx = (m+1)x \Leftrightarrow (m+1-k)x = 0$, par conséquent $x \in \Gamma_{\text{tors}}$.

Réciproquement si $x \in \Gamma_{\text{tors}}$, $\exists n \in \mathbb{Z} - \{0\}$ tel que $nx = 0 \Rightarrow \hat{h}(nx) = 0 \Rightarrow \hat{n}^2 h(x) = 0 \Rightarrow \hat{h}(x) = 0$.

3.c On a montré que les zéros de $\hat{h}$ (soit les $x \in \Gamma_{\text{tors}}$) sont en nombre fini donc Γ_{tors} est fini.

3.d $x = z+2y$ donc $\hat{h}(2y) = \hat{h}(x-z) = 2(\hat{h}(x)+\hat{h}(z)) - \hat{h}(x+z) \leqslant 2(\hat{h}(x)+\hat{h}(z))$ car $\hat{h}(x+z) \geqslant 0$, et comme $\hat{h}(2y) = 4\hat{h}(y)$ on en déduit $\hat{h}(y) \leqslant \frac{1}{2}(\hat{h}(x) + \hat{h}(z))$.

3.e Soit $x \in \Gamma$, puis comme Γ est de type fini modulo 2, $x = z_1 + 2y_1$ avec $z_1 \in Z$, $y_1 \in \Gamma$ et $\hat{h}(y_1) \leqslant \frac{1}{2}(\hat{h}(x) + \hat{h}(z_1))$. On réitère la décomposition à partir de y_1 : $y_1 = z_2 + 2y_2$ avec $z_2 \in Z$, $y_2 \in \Gamma$ et $\hat{h}(y_2) \leqslant (\hat{h}(y_1)+\hat{h}(z_2)) \leqslant \frac{1}{2}(\frac{1}{2}(\hat{h}(x)+\hat{h}(z_1))+\hat{h}(z_2))$. On construit de proche en proche la suite (y_n) qui constitue une sorte de « descente infinie » puisque $\hat{h}(y_n) \leqslant \frac{\hat{h}(x)}{2^n} + \sum_{i=1}^{n} \frac{\hat{h}(z_i)}{2^i}$, et en notant $M = \max_{z_i \in Z} \hat{h}(z_i)$ on a :

$$\hat{h}(y_n) \leqslant \frac{\hat{h}(x)}{2^n} + M\sum_{i=1}^{n} \frac{1}{2^n} \leqslant \frac{\hat{h}(x)}{2^n} + M$$

Pour tout n supérieur à un certain rang n_0 on a alors $\hat{h}(y_n) \leqslant M + 1$, et les y_n appartiennent à l'ensemble fini $P = \left\{x \in \Gamma, \hat{h}(x) \leqslant M + 1\right\}$ (car $\hat{h}$ est une hauteur admissible) qui contient l'ensemble Z. Finalement x s'exprime comme une somme $\sum_{i=1}^{r} n_i x_i$ avec $r = \text{Card}(P)$ et (x_i) la liste des éléments de P. Ceci étant valable pour tout $x \in \Gamma$ on en déduit que Γ est de type fini.

Partie II - $\bar{C}$ muni d'une structure de groupe commutatif de type fini

1.a Les points d'intersections de $D_{u,v}$ avec C sont donnés par $P_{u,v}(x) = 0$ et $y = ux+v$. Comme $P_{u,v}$ est un polynôme de degré 3 il a au plus 3 racines d'où $n(u,v) \leqslant 3$.

1.c $n(u,v) \geqslant 2$ donc $P_{u,v}$ admet au moins 2 racines réelles distinctes donc est scindé sur $\mathbb{R}$, et comme $D_{u,v}$ n'est pas tangente à C, $P_{u,v}$ n'admet pas de racines doubles, donc a 3 racines distinctes d'où $n(u,v) = 3$.

1.d Soit $P(x_0,y_0) \in C$ tel que la tangente à C en P passe par le point (a,b). On a donc :

$$\begin{cases} y_0^2 = x_0^3 - D^2x_0 \\ 2y_0(y-y_0) = (3x_0^2 - D^2)(x-x_0) \end{cases}$$

On a donc $2y_0y = (3x_0^2 - D^2)(x-x_0) + 2(x_0^3 - D^2x_0)$ puis on élève au carré $4(x_0^3 - D^2x_0) = [(3x_0^2 - D^2)(x-x_0) + 2(x_0^3 - D^2x_0)]^2$, on développe et on obtient un polynôme en x_0 de degré 6, ainsi le nombre de points P vérifiant ces conditions est fini (limité par le degré).

2.a Commençons par remarquer que $y^2 = x^3 - D^2x \geqslant 0 \Rightarrow x \geqslant D$. Pour $t \in \mathbb{R}$ fixé montrons qu'il existe un unique point $P(t)$ tel que $y(P(t)) = t$ i.e que la fonction $f : x \mapsto x^3 - D^2x - t^2$ s'annule une seule fois. Calculons sa dérivée $f'(x) = 3x^2 - D^2 > 0$ pour $x \geqslant D$, donc f est continue strictement croissante sur $[D, +\infty[$, $f(D) = -t^2 < 0$ et de limite $+\infty$ en $+\infty$ donc f s'annule une unique fois (d'après le théorème des valeurs intermédiaires).

Comme f induit une bijection de $[D,+\infty[$ sur $[0,+\infty[$ on peut écrire $x = F(t)$ et donc C est l'ensemble des points $(F(t),t)$ pour t décrivant $\mathbb{R}$.

2.b On a vu que $x \geqslant D$ donc $F(y) \geqslant D$ pour tout $y \in \mathbb{R}$. Et aussi qu'il existe un unique point $P(-t)$ tel que $y(P(-t)) = -t$, la fonction f étudiée précédemment reste la même donc s'annule en $x(P(-t)) = x(P(t))$ d'où $F(-t) = F(t)$ pour tout $t \in \mathbb{R}$, F est paire. Pour une abscisse x fixée il y a 2 ordonnées possibles y et $-y$ ($y^2 = x^3 - D^2x$) donc $F(y_1) = F(y_2) \Rightarrow y_1 = \pm y_2$, l'autre sens résulte de la parité.

2.c Vu ce qu'il précède on a la relation : $\forall y \in \mathbb{R}, F(y)^3 = y^2 + D^2F(y) \geqslant y^2$ donc quand $|y| \to +\infty$, $F(y) \to +\infty$ (parité de F). En divisant la relation par $F(y)^3$ on a : $\frac{y^2}{F(y)^3} + \frac{D^2}{F(y)} = 1$ et en faisant tendre $|y| \to +\infty$ il vient $\frac{y^2}{F(y)^3} \to 1$ d'où $|y|^{2/3}F(y) \to 1$.

2.d Commençons par donner l'équation de la droite $D(a,t)$: $y = \left(\frac{t-a}{F(t)-F(a)}\right)x + \frac{aF(t)-tF(a)}{t-a}$. On prends donc avec les notations de l'énoncé $u = \frac{t-a}{F(t)-F(a)}$ et $v = \frac{aF(t)-tF(a)}{F(t)-F(a)}$, puis $u' = \frac{F(t)-F(a)}{t-a}$ et $v' = \frac{tF(a)-aF(t)}{t-a}$. Si $H_a(t) \notin \{a,t\}$, $F(H_a(t))$ est le troisième point d'intersection ssi $H_a(t)$ est racine de $Q_{u',v'}$. On remarque que $atH_a(t)$ est le produit des 3 racines de $Q_{u',v'}$ donc en développant le polynôme et en appliquant les relations coefficients-racines on obtient ce qu'il faut.

Dans les deux autres cas on a une racine double et l'équivalence $(T_1) \Leftrightarrow (T_2) \Leftrightarrow (T_3)$ donne la réponse.

2.e Dans l'expression de $H_a(t)$, le premier facteur tend vers -1 car $\frac{t^2}{F(t)^3} \to 1$, quant à celui entre crochets, on développe le premier numérateur et compte tenu de 2.c seul le premier terme

ne tend pas vers 0, de même pour le premier terme de l'autre quotient. La limite du crochet est alors $\frac{1}{a}[F(a)^3 - D^2F(a)] = \frac{1}{a} \times a^2 = a$, on en déduit $\lim\limits_{t\to+\infty} H_a(t) = -a$, et donc la droite $D(a,t)$ tend à être verticale (d'équation $x = x(P(a))$).

3.a Justifions au préalable l'intégrabilité : la fonction $t \mapsto \frac{2}{3F(t)^2-D^2}$ est $\mathcal{C}^\circ_m$ (même $\mathcal{C}^\circ$), strictement positive sur $\mathbb{R}$ (puisque F est $\mathcal{C}^1$ et $F(t) \geqslant D$) et $\frac{2}{3F(t)^2-D^2} \sim \frac{2}{3|t|^{4/3}}$ en $\pm\infty$ donc l'intégrale a un sens. En outre $L'(y) = \frac{2}{3F(t)^2-D^2} > 0$ sur $\mathbb{R}$, donc L est (continue) strictement croissante sur $\mathbb{R}$ à valeur dans $\left]\lim\limits_{y\to-\infty} F(y), \lim\limits_{y\to+\infty} F(y)\right[$ soit bijective de $\mathbb{R}$ sur $]0,\Omega[$.

3.b Sachant que F est paire, effectuons le changement de variable $u = -t$ (licite car $\mathcal{C}^1$ bijectif), on obtient $L(y) = \int_{-\infty}^{-y} \frac{2dt}{3F(t)^2-D^2}$ d'où par la relation de Chasles $L(y)+L(-y) = \Omega$ pour tout $y \in \mathbb{R}$.

4.a La famille $(L_i(X))$ forme une base de $\mathbb{R}_{n-1}[X]$ (en effet elle possède n éléments et si $\sum\limits_{i=1}^{n} \alpha_i L_i(X) = 0$ en évaluant en les x_i on a les $\alpha_i = 0$). Il existe ainsi des β_i tels que $Q(X) = \sum\limits_{i=1}^{n} \beta_i L_i(X)$ et de nouveau en évaluant en les x_i on détermine les β_i : $Q(X) = \sum\limits_{i=1}^{n} Q(x_i)L_i(X)$.

4.b Remarquons que l'on a $L_i(X) = \frac{P(X)}{P'(x_i)(X-x_i)}$ donc $L_i(0) = (-1)^{n-1}\frac{\prod\limits_{j\neq i} x_j}{P'(x_i)}$. Puis dans la relation *supra* prenons $Q(X) = X^{k+1}$ et évaluons en 0, ce qui donne pour $k \in \{0,...,n-2\}$: $0^{k+1} = (-1)^{n-1}\sum\limits_{i=1}^{n} x_i^{k+1}\frac{\prod_{j\neq i} x_j}{P'(x_i)} = \left((-1)^{n-1}\prod\limits_{i=1}^{n} x_i\right)\sum\limits_{i=1}^{n}\frac{x_i^k}{P'(x_i)}$. D'où si les x_i non nuls $\sum\limits_{i=1}^{n}\frac{x_i^k}{P'(x_i)} = 0$.
Pour $k = n-1$, décomposons $P(X)-A(X) = \sum\limits_{i=1}^{n}(P-A)(x_i)L_i(X)$ avec $A(X) = X^n$ (ainsi $P-A$ est degré $n-1$). Comme les $P(x_i) = 0$ on a $P(X) - A(X) = -\sum\limits_{i=1}^{n} x_i^n L_i(X)$ et évalue de même en 0 : $P(0) - A(0) = P(0) = \left((-1)^{n-1}\prod\limits_{i=1}^{n} x_i\right)\sum\limits_{i=1}^{n}\frac{x_i^{n-1}}{P'(x_i)}$ d'où $\sum\limits_{i=1}^{n}\frac{x_i^{n-1}}{P'(x_i)} = 1$.
Etudions le cas où un x_{i_0} est nul (cela s'extrapolera à plusieurs x_i nuls), alors on peut écrire $P(X) = XR(X)$ et remarquer que $P'(x_i) = x_iR(x_i)$. Ainsi on applique ce qui précède à R puis on multiplie numérateur et dénominateur par x_i pour se ramener à P. (Il reste le cas $k = 0$ que je n'ai pas réussi à traiter).

5.b Sur $]a,+\infty[$, la fonction $t \mapsto H_a(t)$ introduite en 2.d est C^1, de même pour $t \mapsto a$ et $t \mapsto t$, et on a vu que si $H_a(t) \notin \{a,t\}$ les points $P(H_a(t))$, $P(a)$ et $P(t)$ sont alignés, donc d'après 5.a la fonction $t \mapsto L(a) + L(t) + L(H_a(t))$ est constante sur ces intervalles. Par continuité de cette fonction on en déduit qu'elle est constante sur $]a,+\infty[$. Pour connaître la valeur de celle-ci on fait tendre $t \to +\infty$, ainsi par continuité $L(H_a(t)) \to L(-a)$, $L(t) \to \Omega$ et donc $L(a) + L(t) + L(H_a(t)) \to L(a) + L(-a) + \Omega = 2\Omega$.

5.c Comme les y_i sont distincts on peut supposer (quitte à réindexer) $y_1 < y_2 < y_3$. Puisqu'il y a 3 réels, au moins 2 sont de même signe, disons $0 < y_2 < y_3$. On choisit alors $a = y_2$, $t = y_3 > a$ (et donc on a $y_1 = H_a(t)$) ainsi d'après 5.b $L(y_1) + L(y_2) + L(y_3) = 2\Omega$. Le cas où $y_1 < y_2 < 0$ se traite de prenant l'opposée $0 < -y_2 < -y_1$ et en appliquant de nouveau 5.b $L(-y_1) + L(-y_2) + L(-y_3) = 2\Omega \Rightarrow L(y_1) + L(y_2) + L(y_3) = \Omega$ car $L(-y_i) = \Omega - L(y_i)$.

5.e Comme L est à valeur dans $]0,\Omega[$ on ne peut avoir que $L(y_1) + L(y_2) + L(y_3) \in \{\Omega, 2\Omega\}$.

Supposons $L(y_1)+L(y_2)+L(y_3)=\Omega$. On remarque qu'on doit avoir $y_1<y_2<0$ sinon pour $0<y_2<y_3$ on aurait $\Omega=L(0)<L(y_2)<L(y_3)$ et par suite $L(y_1)+L(y_2)+L(y_3)>\Omega$ absurde. Alors d'après ce qu'on a vu en 5.c on a $L(y_1)+L(y_2)+L(y_3)=\Omega$ avec $y_3=H_{y_1}(y_2)$ et donc les points $P(y_1)$, $P(y_2)$ et $P(y_3)$ sont alignés. Si $L(y_1)+L(y_2)+L(y_3)=2\Omega$ on se ramène au cas précédent en prenant les opposés.

6.a D'après 3.a L est une bijection de $\mathbb{R}$ sur $]0,\Omega[$, donc la fonction $y\mapsto\frac{2\pi L(y)}{\Omega}$ est une bijection de $\mathbb{R}$ sur $]0,2\pi[$ donc E est une bijection de $\bar{C}$ sur G. Comme G possède une structure de groupe commutatif multiplicatif, par bijection $\bar{C}$ lui est isomorphe et la loi $+$ est définie de manière unique par $E(P+Q)=E(P)E(Q)$. De plus si $P+Q\neq\infty$ on a $E(P)E(Q)=\exp\left(\frac{2i\pi}{\Omega}L(y(P))\right)\exp\left(\frac{2i\pi}{\Omega}L(y(Q))\right)=\exp\left(\frac{2i\pi}{\Omega}(L(y(P))+L(y(Q)))\right)=E(P+Q)=\exp\left(\frac{2i\pi}{\Omega}L(y(P+Q))\right)$. Par conséquent modulo Ω on a $L(y(P))+L(y(Q))\equiv L(y(P+Q))$. Or comme L est à valeur dans $]0,\Omega[$ on a 2 possibilités : si $L(y(P))+L(y(Q))<\Omega$ on a égalité $L(y(P))+L(y(Q))=L(y(P+Q))$ et si $L(y(P))+L(y(Q))>\Omega$ on a $L(y(P))+L(y(Q))-\Omega=L(y(P+Q))$.

6.b On peut procéder directement par équivalence $P_1+P_2+P_3=\infty\Leftrightarrow E(P_1+P_2+P_3)=1\Leftrightarrow E(P_1)E(P_2)E(P_3)=1\Leftrightarrow\exp\left(\frac{2i\pi}{\Omega}(L(y(P_1))+L(y(P_2))+L(y(P_3)))\right)=1\Leftrightarrow L(y(P_1))+L(y(P_2))+L(y(P_3))\in\Omega\mathbb{Z}\Leftrightarrow P_1,P_2,P_3$ alignés d'après 5.c et 5.e.

6.c Comme $L(y)+L(-y)=\Omega$, il vient $E(P(y)+P(-y))=E(P(y))E(P(-y))=\exp\left(\frac{2i\pi}{\Omega}(L(y)+L(-y))\right)=\exp(2i\pi)=1\Leftrightarrow P(y)+P(-y)=\infty$ soit $-P(y)=P(-y)$ qui est le symétrique de P par rapport à (O_x).

6.d L'équation $x^2=z$ pour un complexe $z\in G$ fixé admet 2 solutions. Donc puisque G est isomorphe à $\bar{C}$ on a de même 2 solutions pour l'équation $2Q=P$.

Partie III - Formules relatives à cette loi de groupe

1.a $P_1+P_2+P_3=\infty$ donc P_1,P_2,P_3 sont alignés d'après 6.b. La droite les joignant a pour équation $y=y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)$ donc d'après les résultats admis dans le préambule, les abscisses x_1,x_2,x_3 des points $P_1,P_2,P_3\in D_{u,v}\cap C$ sont racines du polynômes $P(x)=x^3-D^2x-\left(y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)\right)^2$. On développe l'expression et en utilisant les relations coefficients-racines on tie $x_1+x_2+x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2$. Par ailleurs $\frac{y_2-y_1}{x_2-x_1}=\frac{y_2^2-y_1^2}{(y_1+y_2)(x_2-x_1)}=\frac{(x_2^3-D^2x_2)-(x_1^3-D^2x_1)}{(y_1+y_2)(x_2-x_1)}=\frac{x_1^2+x_1x_2+x_2^2-D^2}{y_1+y_2}$, on obtient la relation que l'on devait démontrer. L'autre provient du fait que $y_3=y_1+\frac{y_2-y_1}{x_2-x_1}(x_3-x_1)$.

1.b Même principe, on effectue $X\leftarrow X-D$ dans le polynôme P de sorte que les x_i+D en soient racines, et toujours grâce aux relations coefficients racines on tire $(x_1+D)(x_2+D)(x_3+D)=\left(y_1-\frac{y_2-y_1}{x_2-x_1}(x-x_1)\right)^2=\left(\frac{(x_1+D)y_2-(x_2+D)y_1}{x_2-x_1}\right)^2$.

2.a On s'aperçoit qu'au signe près il s'agit des formules de 1.a en faisant tendre (x_2,y_2) vers (x_1,y_1). Justifions cette opération : prenons $P_1=(x_1,y_1)=(x,y)\in C$, $P_2=(x_2,y_2)\in C$ et $P_3=(x_3,y_3)\in C$ le troisième points tels que les P_i soient alignés c'est-à-dire $(P_1+P_2)+P_3=\infty$. D'après 6.c on a $y(P_3)=-y(P_1+P_2)$ et d'après $y(P(y_1)+P(y_2))\to y(2P(y_1))$ quand $y_2\to y_1$ d'où $y_3\to -y'$ quand $y_2\to y_1$. Et par continuité de F : $x_3=F(y_3)\to F(-y')=F(y')=x'$.

2.b Direct : on réduit au même dénominateur et on utilise que $y^2 = x^3 - D^2x$.

3. On pose $\bar{C}(Q) = C(Q) \cup \{\infty\}$ ainsi le neutre $\infty \in \bar{C}(Q)$. Vérifions maintenant que si $(P_1, P_2) \in \bar{C}(Q)^2$ alors $-P_1 \in \bar{C}(Q)$ et $P_1 + P_2 \in \bar{C}(Q)$. Supposons déjà $P_1 \neq P_2$. Le premier point est vérifié par 6.c car $y(-P_1) = -y(P_1)$, $x(-P_1) = x(P_1)$ qui sont rationnels car $P_1 \in \bar{C}(Q)$. Quant au deuxième point on a $P_1 + P_2 = -P_3$ où P_3 est défini par $P_1 + P_2 + P_3 = \infty$, et d'après les relations de 1.a ses coordonnées sont rationnelles puisque celles de P_1 et P_2 le sont, donc $P_3 \in \bar{C}(Q)$ et par le premier point $-P_3 = P_1 + P_2 \in \bar{C}(Q)$. Pour $P_1 = P_2$ le deuxième point est vérifié d'après 2.a.

Partie IV - $\bar{C}(Q)$ de type fini

Partie A

1.a Si $a \in \mathbb{Q}^*$ est un carré, $a = b^2$ avec $b = \prod p^{v_p(b)} \in \mathbb{Q}^*$. Ainsi $a = \prod p^{2v_p(b)}$ et donc $v_p(a) = 2v_p(b) \Rightarrow \overline{v_p(a)} = 0$ pour tout nombre premier p. Réciproquement si les $\overline{v_p(a)} = 0$ alors les valuations p-adiques sont paires donc on peut écrire $v_p(a) = 2v_p(b)$ et $a = \prod p^{v_p(a)} = (\prod p^{v_p(b)})^2 = b^2$.

1.b Ecrivons $a = p^{v_p(a)}\frac{m}{n}$ et $b = p^{v_p(b)}\frac{m'}{n'}$ avec m, m', n, n' non divisible par p. Alors $a + b = p^{v_p(a)}\left(\frac{m}{n} + p^{v_p(b)-v_p(a)}\frac{m'}{n'}\right) = p^{v_p(a)}\left(\frac{mn' + p^{v_p(b)-v_p(a)}m'n}{nn'}\right)$. Au numérateur le deuxième terme est divisible par p (car $v_p(b) - v_p(a) > 0$) mais mn' ne l'est pas, donc la parenthèse n'est pas divisible par p et donc $v_p(a+b) = v_p(a)$.

2.a c est un carré donc $v_p(c)$ est pair, et $v_p(c) \geqslant 1$ donc $v_p(c) \geqslant 2$. Posons $x = \frac{m}{n}$ avec $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$ et $m \wedge n = 1$. Comme on veut $cx = \frac{c}{n}m \in \mathbb{Z}$ et $m \wedge n = 1$ d'après le théorème de Gauss $n|c \Leftrightarrow c = nq$. Ecrivons $n = \prod p_i^{v_{p_i}(n)}$, si n est un carré $c = n^2$ convient, sinon on multiplie n par $q = \prod p_i$ où $\overline{v_{p_i}(n)} = 1$ pour avoir c minimal. Donc c est composé des même facteurs premiers que n, ainsi si $v_p(c) \geqslant 1$, $p|n$ et $p \nmid m$. Donc $v_p(a) = v_p\left(\frac{c}{n}\right) + v_p(m) = v_p\left(\frac{c}{n}\right) = v_p(c) - v_p(n)$. Vu la construction citée c on a soit $v_p(c) = v_p(n)$ soit $v_p(c) = v_p(n) + 1$ d'où $v_p(a) \in \{0, 1\}$.

2.b $a(a-Dc)(a+Dc) = a(a^2 - D^2c^2) = a^3 - D^2ac^2 = (cx)^3 - D^2c^3x = c^3(x^3 - D^2c) = c^3y^2 = (b^3y)^2$.

2.c Si $v_p(c) = 0$, comme $v_p(D) = 0$ (car $p \notin S \cup \{2\}$) on a $v_p(Dc) = 0$ et d'après 1.b si $v_p(a) \geqslant 1$ (sinon $v_p(a) = 0$ pair), $v_p(a + Dc) = v_p(a - Dc) = 0$ sont pairs et comme $a(a + Dc)(a - Dc)$ est un carré $\overline{v_p(a)} + \overline{v_p(a + Dc)} + \overline{v_p(a - Dc)} = \overline{0}$ d'où $\overline{v_p(a)} = 0$ soit $v_p(a)$ pair.
Si $v_p(c) \geqslant 1$ alors d'après 2.a $v_p(c) \geqslant 2$ et $v_p(a) \leqslant 1$ d'où $v_p(a) < v_p(c)$ et par 1.b $v_p(a + Dc) = v_p(a - Dc) = v_p(a)$. Or $a(a - Dc)(a + Dc) = c^3y^2$ donc $3v_p(a) = 3v_p(c) + 2v_p(y)$, et $v_p(c)$ est pair car c est un carré d'où $v_p(a)$ est pair et $v_p(a + Dc), v_p(a - Dc)$ également puisque égaux.

3.a Notons $P(x_1, y_1)$, $Q(x_2, y_2)$ et $P + Q(x_3, y_3)$. Supposons tout d'abord que $P \neq Q$, alors d'après III.1.b les produits $(x_1 + D)(x_2 + D)(x_3 + D)$ et $x_1x_2x_3$ sont des carrés donc $\forall p$ premier $\overline{(v_p(x_1 + D) + v_p(x_2 + D))} + \overline{v_p(x_3 + D)} = 0$ soit $\overline{v_p(x_3 + D)} = \overline{v_p(x_1 + D)} + \overline{v_p(x_2 + D)}$ et de même $\overline{v_p}(x_3) = \overline{v_p(x_1)} + \overline{v_p(x_2)}$, ce qui prouve que $\varphi(P + Q) = \varphi(P) + \varphi(Q)$. De même si $P = Q$ on a x_3 et $x_3 + D$ des carrés (cf III.2.b) donc $x_1x_2x_3 = x_1^1x_3$ et $(x_1 + D)(x_2 + D)(x_3 + D) = (x_1 + D)^2(x_3 + D)$ sont des carrés.

3.b $Q(x,y) \in C$ vérifie $2Q = P$ donc d'après 2.b $x' = \left(\frac{x^2+D^2}{2y}\right)^2$, $x'+D = \left(\frac{x^2+2Dx-D^2}{2y}\right)^2$ et $x'-D = \left(\frac{x^2-2Dx-D^2}{2y}\right)^2$. Comme par hypothèse x', $x'+D$ et $x'-D$ sont des carrés de rationnels on en déduit que les trois fractions f_1, f_2 et f_3 entre parenthèses sont rationnelles. Puis on remarque que $\frac{2f_1-f_2-f_3}{2D^2} = \frac{1}{y}$ et $\frac{f_2-f_3}{2D} = \frac{x}{y}$ sont rationnels donc $Q(x,y) \in C(Q)$.

3.c $\varphi(P) = 0 \Leftrightarrow \forall p \in S \cup \{2\}, \overline{v_p(x)} = \overline{v_p(x+D)} = 0$. Et d'après 2.c $\forall p \notin S \cup \{2\}, v_p(a) = v_p(c) + v_p(x) = v_p(x)$ et $v_p(a+Dc) = v_p(c) + v_p(x+D) = v_p(x+D)$ sont pairs, donc finalement $\forall p$ premier $\overline{v_p(x)} = \overline{v_p(x+D)} = 0$, et comme $a(a-Dc)(a+Dc)$ est un carré on en tire aussi $v_p(x-D) = 0$. On en conclut que $P \in \mathrm{Ker}(\varphi)$ si et seulement si x, $x+D$ et $x-D$ sont des carrés.

3.d Comme $\mathrm{Im}(\varphi) \subset (\mathbb{Z}/2\mathbb{Z})^{2s+2}$ qui est fini, on a $\mathrm{Im}(\varphi)$ fini, donc il existe une partie fini $Z \subset \bar{C}(Q)$ telle que $\varphi(Z) = \mathrm{Im}(\varphi)$. Soit alors $P \in \bar{C}(Q)$, il existe $z \in Z$ tel que $\varphi(P) = \varphi(z)$ d'où par morphisme $\varphi(P-z) = 0 \Leftrightarrow P - z \in \mathrm{Ker}(\varphi)$. Ainsi d'après 3.b et 3.c il existe $Q \in C(Q)$ tel que $2Q = P - z \Leftrightarrow P = z + 2Q$. Par conséquent $\bar{C}(Q)$ est de type fini modulo 2.

Partie B

1. Il s'agit de montrer que $h(2P) \leqslant 4h(P)$, en notant $2P(x',y')$ et c' le plus petit carré rendant $a' = c'x'$ entier, cela revient à montrer que $\ln(c'(x'+D)) \leqslant \ln(c^4(x+D)^4)$. Nous allons de nouveau réutiliser les formules de la partie III : $x' = \left(\frac{x^2+D^2}{2y}\right)^2$. Multiplions par $4y^2c^4$ de telle sorte que $4y^2c^4x' = (c^2x^2+c^2D^2)^2 = (a^2+c^2D^2)^2$ soit entier. Comme $4y^2c^4 = 4(x^3-D^2x)c^4 = 4c(a^3-c^2D^2a)$ est entier, par minimalité $c'|4y^2c^4$ et par positivité $c' \leqslant 4y^2c^4$. Par ailleurs $x'+D = \left(\frac{x^2-2Dx-D^2}{2y}\right)^2$ donc par croissance du logarithme : $\ln(c'(x'+D)) \leqslant \ln\left[4y^2c^4\left(\frac{x^2-2Dx-D^2}{2y}\right)^2\right] = \ln(c^4(x^2-2Dx-D^2)^2)$. Reste à remarquer en développant que $(x^2-2Dx-D^2)^2 \leqslant (x+D)^4$.

2.a Si d divise T, U et V alors il divise $T+U+DV$ et $T+U-DV$ ce qui est justement $2a_1(a_2+Dc_2)$ et $2a_2(a_1+Dc_1)$. En revanche je n'ai pas trouvé de combinaisons permettant de montrer que d divise $4D^2a_1c_2^2$ et $4D^2a_2c_1^2$.

2.b On a montré dans la partie A, question 2.c que si $v_p(c) \geqslant 1$ alors $v_p(a)$ est pair, mais à plus forte raison est nul puisque $v_p(a) \in \{0,1\}$, ce qui prouve que $a \wedge c = 1$. Par l'absurde, supposons que p divise ces trois quantités, si $p \notin S \cup \{2\}$ et $p|4D^2a_1c_2^2$ alors $p|a_1c_2^2$. De même $p|a_2c_1^2$. Deux cas se présentent : si p est un diviseur de a_1 alors p ne divise pas c_1 (car $a_1 \wedge c_1 = 1$), donc $p|a_2$ et par conséquent ne divise pas c_2. Par symétrie si $p|c_1$ il divise c_2 et ne divise pas a_1 et a_2. On en déduit que p ne diviserait pas $a_1a_2 + D^2c_1c_2$. Absurde, donc p ne divise pas l'une des trois quantités.

2.d Notons d le pgcd de T, U et V. d les divise tous les trois, donc d'après 2.a divise $4D^2a_1c_2^2$ et $4D^2a_2c_1^2$. Soit p un facteur premier de d, par contraposée de 2.b on a $p \in S \cup \{2\}$ (donc c'est aussi un facteur de $2D$). D'après 2.c p^4 ne divise pas d, donc au mieux $p^3|d$, or comme p^3 est un facteur de $(2D)^3$ on en déduit que $d|(2D)^3$.

2.e On veut montrer que $e|c_3c_4\delta$. On a $c_3c_4\delta$ le pgcd de c_3c_4d, c_3c_4d' et c_3c_4e, or $d = x_3x_4e$ et $d' = (x_3+D)(x_4+D)e$ donc $c_3c_4d = a_3a_4e$, $c_3c_4d' = (a_3+c_3D)(a_4+c_4D)e$. Donc e divise ces trois quantités donc leur pgcd, ce que l'on voulait. Puis $h(P_3) + h(P_4) = \ln(c_3(x_3+D)) + \ln(c_4(x_4+D)) = \ln(c_3c_4(x_3+D)(x_4+D)) = \ln(c_3c_4\frac{d'}{e})$, on fait apparaître δ de cette façon :

$\ln(\frac{c_3c_4\delta}{e}\frac{d'}{\delta}) = \ln(\frac{c_3c_4\delta}{e}) + \ln(d') - \ln(d) \geqslant \ln(d') - \ln(d)$ car $\frac{c_3c_4\delta}{e}$ est un entier plus grand que 1.

2.f Posons $P_3 = P_1 + P_2$ et $P_4 = P_1 - P_2$, d'après III.4 on dispose des formules $(x_3+D)(x_4+D) = \left(\frac{x_1x_2+D(x_1+x_2)-D^2}{x_2-x_1}\right)^2$ et $x_3x_4 = \left(\frac{x_1x_2-D^2}{x_2-x_1}\right)^2$. Ou encore en multipliant haut et bas par c_1c_2 dans les parenthèses : $(x_3+D)(x_4+D) = \left(\frac{a_1a_2+D(a_1c_2+a_2c_1)-c_1c_2D^2}{a_1c_2-a_2c_1}\right)^2$ et $x_3x_4 = \left(\frac{a_1a_2-c_1c_2D^2}{a_1c_2-a_2c_1}\right)^2$. Vu ce que l'on vient de faire en 2.e posons $d = (a_1a_2 - c_1c_2D^2)^2$, $d' = (a_1a_2 + D(a_1c_2 + a_2c_1) - c_1c_2D^2)^2$ et $e = (a_1c_2 - a_2c_1)^2$. Notons δ leur pgcd. D'après 2.e on a $h(P_3) + h(P_4) \geqslant \ln(d') - \ln(\delta)$. Pour faire apparaître $2(h(P_2) + h(P_1)) = 2\ln[c_1c_2(x_1 + D)(x_2 + D)] = \ln[(a_1 + c_1D)(a_2 + c_2D)]$ on écrit $a_1a_2 + D(a_1c_2 + a_2c_1) - c_1c_2D^2 = (a_1 + c_1D)(a_2 + c_2D) - 2c_1c_2D^2 = (a_1 + c_1D)(a_2 + c_2D)[1 - \frac{2c_1c_2D^2}{(a_1+c_1D)(a_2+c_2D)}]$. Ainsi en passant au logarithme : $\ln(d') - \ln(\delta) = 2\ln[(a_1 + c_1D)(a_2 + c_2D)] + 2\ln\left(1 - \frac{2c_1c_2D^2}{(a_1+c_1D)(a_2+c_2D)}\right) - \ln(\delta)$. On utilise maintenant le résultat de 2.d (sans oublier les carrés) : $\delta|(2D)^6$ donc $\ln(\delta) \leqslant 2\ln((2D)^3)$. On a alors $\ln(d') - \ln(\delta) \geqslant 2(h(P_1) + h(P_2)) + 2\ln\left(1 - \frac{2c_1c_2D^2}{(a_1+c_1D)(a_2+c_2D)}\right) - 2\ln((2D)^3)$. Donc il reste à montrer que le terme central est supérieur à $-2\ln(2)$. Pour cela il "suffit" (j'ai mis un certain temps à m'en rappeler) de remarquer que $x \geqslant D \Rightarrow a \geqslant cD$ et la majoration est immédiate.

3.a D'après II.6.d l'équation $2P = Q$ admet exactement 2 solutions (du fait de l'isomorphisme E de G sur $\bar{C}$ et que $x^2 = z$ possède 2 solutions dans G). On résout donc $x^2 = 1$ (puisque $E(\infty) = 1$) dont les 2 solutions sont ± 1. On a $E(\infty) = 1$ et montrons que $E((D,0)) = -1$, en effet d'après II.3.b $L(0) = \frac{\Omega}{2}$ donc $E((D,0)) = \exp\left(\frac{2i\pi}{\Omega}L(0)\right) = \exp(i\pi) = -1$.

3.c Immédiat d'après les questions 2.f et 3.b.

3.d On peut réécrire 3.c de la façon suivante : $2(h(P) + h(Q)) - h(P + Q) - h(P - Q) \leqslant A$ avec $A > 0$. On souhaite maintenant minorer cette quantité, pour cela effectuons $P \leftarrow P + Q$ et $Q \leftarrow P - Q$ de telle sorte que $2(h(P + Q) + h(P - Q)) - h(2P) - h(2Q) \leqslant A$ d'où d'après 1. $2(h(P+Q)+h(P-Q))-4h(P)-4h(Q) \leqslant A \Leftrightarrow 2(h(P)+h(Q))-h(P+Q)-h(P-Q) \geqslant -\frac{1}{2}A \geqslant -A$. Donc finalement $|h(P+Q)+h(P-Q)-2h(P)-2h(Q)| \leqslant A$ et h est bien une hauteur sur $\bar{C}(Q)$.

3.e Soit $B \geqslant 0$, montrons que l'ensemble $\left\{P \in \bar{C}(Q), h(P) \leqslant B\right\}$ est fini. Donnons nous un tel P d'abscisse x et c le plus petit carré tel que $a = cx$ soit entier. $x = \frac{a}{c}$, on va alors majorer a et c, ce qui démontrera la clause. En effet $h(P) = \ln(c(x + D)) \leqslant B \Leftrightarrow c(x + D) \leqslant \exp(B)$. D'une part $a = cx \leqslant c(x + D) = \exp(B)$ et d'autre part comme $D \leqslant x$ on a $c \leqslant \frac{\exp(B)}{2D}$. Ainsi h est une hauteur admissible sur $\bar{C}(Q)$.

3.f On a montré dans la partie II que l'on pouvait munir $\bar{C}(Q)$ d'une structure de groupe commutatif. Les résultats de la partie III ont permis de démontrer dans la partie IV.A que $\bar{C}(Q)$ est de type fini modulo 2, et la partie IV.B nous a fait construire une hauteur admissible sur $\bar{C}(Q)$. Par conséquent les questions 3.c et 3.e de la partie I nous permettent de conclure que $\bar{C}(Q)_{\text{tors}}$ est fini et que $\bar{C}(Q)$ est de type fini.