INTRODUCTION À L'ARITHMÉTIQUE DES COURBES ELLIPTIQUES
MASTER 2 – SORBONNE UNIVERSITÉ (2024)
FEUILLE DE TD 3

Definition (Différentielles de Kähler)**.** Soit A un anneau et B une A-algèbre. On définit $\Omega_{B/A}$ comme le B-module engendré par les symboles db ($b \in B$) quotienté par le sous-B-module engendré par les relations de

- (i) linéarité : $d(f+g) = df + dg$ $(f, g \in B)$,
- (ii) Leibniz : $d(fg) = fdg + gdf$,
- (iii) constance : $da = 0$ $(a \in A)$.

On note $d : B \to \Omega_{B/A}$ le morphisme canonique.

Soit M un B-module. Une dérivation à valeurs dans M est un morphisme $d_M : B \to M$ de B-modules vérifiant les relations (i), (ii) et (iii).

Le morphisme $d : B \to \Omega_{B/A}$ est la dériviation initiale ; i.e. pour toute dérivation d_M, il existe une unique factorisation

$$\begin{array}{ccc} B & \xrightarrow{d_M} & M \\ {\scriptstyle d}\downarrow & \nearrow_{h} & \\ \Omega_{B/A} & & \end{array}$$

La commutation du diagramme impose $h(db) = d_M(b)$ et il suffit de vérifier que cette assignation définit bien un morphisme de A-modules.

Exercice 1. Soit A un anneau (commutatif, unitaire) et B une A-algèbre. On se propose d'étudier le module des différentielles de B sur A.

1. Montrer que si B est engendré par une famille d'éléments $(x_i)_{i\in I}$ comme A-algèbre, alors $\Omega_{B/A}$ est engendré par $(dx_i)_{i\in I}$ comme B-module.
2. Soit $B = A[X_1, \dots, X_n]$. En déduire que $\Omega_{B/A}$ est libre de rang n, de base $(dX_i)_{i=1,\dots,n}$.
3. Soit $S \subset B$ une partie multiplicative. Montrer que
$$S^{-1}\Omega_{B/A} \cong \Omega_{S^{-1}B/A} = \Omega_{S^{-1}B/(S\cap A)^{-1}A}.$$
4. Montrer que si L/K est une extension séparable de corps, alors $\Omega_{L/K} = (0)$.

Solution: (1) Pour $d \geq 0$ un entier, on note B_d le sous-A-module de B engendré par les polynômes en les x_i de degré $\leq d$. Clairement, les $(B_d)_{d\geq 0}$ forment une suite croissante d'union B. On considère l'hypothèse de récurrence :

$$d(B_d) \text{ est contenu dans le B-module engendré par les } (dx_i)_{i\in I}.$$

Pour $d = 0$, comme $B_0 = A$ puis $dB_0 = 0$, le résultat est clair.
On suppose le résultat vrai pour $d-1$. Écrivons $b \in B_d$ comme $b = c + \sum_i b_i x_i$ où $c \in A$ et $b_i \in B_{d-1}$. On a alors

$$db = \sum_i x_i db_i + b_i dx_i$$

ce qui montre que db s'écrit comme une somme de dx_i.
(2) D'après ce qui précède, on sait que $\Omega_{A[X_1,\dots,X_n]/A}$ est engendré par les $(dX_i)_{i=1,\dots,n}$. Pour montrer que cette famille est libre, on considère la dérivation par rapport à X_i :

$$\partial_i : A[X_1, \dots, X_n] \longrightarrow A[X_1, \dots, X_n].$$

C'est une dérivation qui correspond à l'application $\Omega_{B/A} \to A[X_1, \dots, X_n]$ envoyant dX_j sur $\mathbf{1}_{ij}$. C'est donc une famille libre.
(3) On commence par remarquer que si $f : B \to C$ est un morphisme de A-algèbres, alors on a un morphisme induit $\Omega_{B/A} \to \Omega_{C/A}$. En appliquant ce fait à $B \to S^{-1}B$, on obtient un morphisme $\Omega_{B/A} \to \Omega_{S^{-1}B/A}$. La cible est un $S^{-1}B$-module, et donc cette flèche se factorise par $S^{-1}\Omega_{B/A}$. Pour montrer que c'est un isomorphisme, on construit l'application inverse : il suffit de définir une dériviation

$$\delta : S^{-1}B \longrightarrow S^{-1}\Omega_{B/A}.$$

On laisse le soin de vérifier que $\delta(b/s) := (1/s)db - (1/s^2)bds$ fait le job [on devine cette formule, car on veut $\delta(b) = \delta(s \cdot (b/s)) = s\delta(b/s) + (b/s)\delta(s)$.]
Pour la deuxième égalité, il y a une inclusion claire $\Omega_{S^{-1}B/(S\cap A)^{-1}A} \subset \Omega_{S^{-1}B/A}$. Réciproquement, si $s \in S \cap A$, alors $0 = d(ss^{-1}) = s^{-1}ds + sd(s^{-1}) = sd(s^{-1})$ et alors $d(s^{-1}) = 0$, puis

$d(s^{-1}a) = ad(s^{-1}) + s^{-1}da = 0$ pour $a \in \mathrm{A}$.
(4) Soit $\ell \in \mathrm{L}$ tel que $d\ell \neq 0$. Soit $p(x)$ le polynôme minimal de ℓ sur k. Alors $0 = dp(\ell) = p'(\ell)d\ell$, puis $p'(\ell) = 0$ et donc ℓ n'est pas séparable.

Exercice 2 (Suites exactes fondamentales)**.** (1) Soit A un anneau. Démontrer qu'une suite de A-modules $\mathrm{M}' \to \mathrm{M} \to \mathrm{M}'' \to 0$ est exacte si, et seulement si, la suite induite $0 \to \mathrm{Hom}(\mathrm{M}'', \mathrm{N}) \to \mathrm{Hom}(\mathrm{M}, \mathrm{N}) \to \mathrm{Hom}(\mathrm{M}', \mathrm{N})$, pour tout A-module N, l'est.

En déduire les assertions suivantes :

(2) Pour $\mathrm{A} \to \mathrm{B} \to \mathrm{C}$ des morphismes d'anneaux, la suite suivante est exacte :

$$\mathrm{C} \otimes_{\mathrm{B}} \Omega_{\mathrm{B/A}} \longrightarrow \Omega_{\mathrm{C/A}} \longrightarrow \Omega_{\mathrm{C/B}} \longrightarrow 0.$$

(3) Pour $\mathrm{I} \subset \mathrm{B}$ un idéal, la suite

$$\mathrm{I}/\mathrm{I}^2 \longrightarrow (\mathrm{B}/\mathrm{I}) \otimes_{\mathrm{B}} \Omega_{\mathrm{B/A}} \longrightarrow \Omega_{(\mathrm{B/I})/\mathrm{A}} \longrightarrow 0,$$

où la première flèche envoie la classe de i vers celle de $1 \otimes di$, est exacte.

Solution: (2) On applique (1) à la suite de C-modules en question

$$0 \longrightarrow \mathrm{Hom}_{\mathrm{C}}(\Omega_{\mathrm{C/B}}, \mathrm{N}) \longrightarrow \mathrm{Hom}_{\mathrm{C}}(\Omega_{\mathrm{C/A}}, \mathrm{N}) \longrightarrow \mathrm{Hom}_{\mathrm{C}}(\mathrm{C} \otimes_{\mathrm{B}} \Omega_{\mathrm{B/A}}, \mathrm{N})$$

pour trouver

$$0 \longrightarrow \mathrm{Der}_{\mathrm{B}}(\mathrm{C}, \mathrm{N}) \longrightarrow \mathrm{Der}_{\mathrm{A}}(\mathrm{C}, \mathrm{N}) \longrightarrow \mathrm{Der}_{\mathrm{A}}(\mathrm{B}, \mathrm{N})$$

Que cette suite soit exacte découle presque immédiatement des définitions des dérivations.
(3) On commence par vérifier que la première flèche est bien définie : on a bien $1 \otimes d(ij) = 0$ dès lors que $i, j \in \mathrm{I}$ par la relation de Leibniz : $1 \otimes d(ij) = 1 \otimes (idj + jdi) = i \otimes dj + j \otimes di$. De plus, la composition des deux flèches est bien nulle car di est envoyé sur zéro pour tout $i \in \mathrm{I}$.
Pour l'exactitude, on applique (1) à nouveau cette suite de B/I-modules, et il revient de montrer que la suite

$$0 \longrightarrow \mathrm{Der}_{\mathrm{A}}(\mathrm{B/I}, \mathrm{N}) \longrightarrow \mathrm{Der}_{\mathrm{A}}(\mathrm{B}, \mathrm{N}) \longrightarrow \mathrm{Hom}_{\mathrm{B}}(\mathrm{I}, \mathrm{N})$$

est exacte pour tout B/I-module N, où la deuxième flèche n'est autre que la restriction de B à I. C'est alors clair.

Exercice 3. Soit K un corps de fonctions sur un corps parfait k, P un point de K. Soit $t \in \mathrm{K}$ une uniformisante en P.

(1) Montrer que $\Omega_{\mathcal{O}/k}$ est libre de rang 1 sur $\mathcal{O}$, engendré par dt.

(2) Soient $\mathrm{F} \subset \mathrm{K}$ une extension finie de corps de fonctions, $\mathfrak{p}$ le point de F au-dessous [1] de P. Soit $t_{\mathrm{F}} \in \mathrm{F}$ une uniformisante en $\mathfrak{p}$. Montrer que le module $\Omega_{\mathcal{O}_{\mathrm{P}}/\mathcal{O}_{\mathfrak{p}}}$ est isomorphe à $(\mathcal{O}_{\mathrm{P}}/\delta\mathcal{O}_{\mathrm{P}})dt$ où $\delta = dt_{\mathrm{F}}/dt$.

(3) En déduire qu'il est de longueur finie $\geq e(\mathrm{P}/\mathfrak{p}) - 1$ avec égalité si, et seulement si, $e(\mathrm{P}/\mathfrak{p})$ est non nul dans k.

(4) Montrer que l'ensemble des points P tels que $e(\mathrm{P}/\mathfrak{p}) > 1$ est fini si K/F est séparable.

(5) Soit $\omega \in \Omega_{\mathrm{K}/k}$ et soit f_t l'unique élément de K tel que $\omega = f_t dt$. Montrer que l'entier $v_{\mathfrak{m}}(f_t)$ est indépendant de l'uniformisante t. On le note $v_{\mathrm{P}}(\omega)$.

(6) Soit $\omega \in \Omega_{\mathrm{K}/k} \setminus \{0\}$. Montrer que l'expression

$$\sum_{\mathrm{P}} v_{\mathrm{P}}(\omega) \cdot \mathrm{P}$$

est un diviseur.

(7) En déduire que le diviseur ci-dessus est indépendant du choix de $\omega \in \Omega_{\mathrm{K}/k} \setminus \{0\}$.

Solution: (1) On sait que $\mathcal{O}$ est une k-algèbre de type fini ; donc $\Omega_{\mathcal{O}/k}$ est un $\mathcal{O}$-module de type fini. Comme $\mathrm{K}/k(t)$ est séparable, la suite (2) pour $k \subset k(t) \subset \mathrm{K}$ donne une surjection $\mathrm{K} \otimes_{k(t)} \Omega_{k(t)/k} \to \Omega_{\mathrm{K}/k}$, puis une surjection

$$\mathrm{K} \otimes_{k[t]} \Omega_{k[t]/k} \to \mathrm{K} \otimes_{\mathcal{O}} \Omega_{\mathcal{O}/k}$$

d'après les propriétés de localisation. Comme $\Omega_{k[t]/k}$ est libre de rang 1, on trouve que $\Omega_{\mathcal{O}/k}$ est de rang au plus un. Pour montrer qu'il n'a pas de torsion, on considère la surjection

$$\mathfrak{m}/\mathfrak{m}^2 \longrightarrow (\mathcal{O}/\mathfrak{m}) \otimes_{\mathcal{O}} \Omega_{\mathcal{O}/k}$$

donnée par l'Exercice 2.(3) et le fait que $k \subset \mathcal{O}/\mathfrak{m}$ est séparable (k est parfait). D'un côté $\mathfrak{m}/\mathfrak{m}^2$ est un $(\mathcal{O}/\mathfrak{m})$-espace vectoriel de dimenision 1 engendré par l'image de t ; de l'autre, on a un $(\mathcal{O}/\mathfrak{m})$-espace vectoriel de dimension ≥ 1 avec égalité si, et seulement si, $\Omega_{\mathcal{O}/k}$ est sans torsion.
(2) La suite exacte de l'Exercice 2.(2) donne $\mathcal{O}_{\mathrm{P}} dt_{\mathrm{F}} \to \mathcal{O}_{\mathrm{P}} dt \to \Omega_{\mathcal{O}_{\mathrm{P}}/\mathcal{O}_{\mathfrak{p}}} \to 0$, ce que l'on

1. Pour définir $\mathfrak{p}$ on considère $v_{\mathrm{P}}|_{\mathrm{F}}$ renormalisée de telle sorte à obtenir une valuation surjective.

cherchait à montrer.
(3) On a $\mathfrak{p}\mathcal{O}_p = \mathrm{P}^e$ et donc $t_\mathrm{F} = ut^e$ pour une certaine unité $u \in \mathcal{O}_\mathrm{P}^\times$. En dérivant, on obtient $\delta\mathcal{O}_\mathrm{P}dt \subset t^{e-1}\mathcal{O}_\mathrm{P}dt$ avec égalité si et seulement si e est non nul dans k.
(4) D'après ce qu'on a montré précédemment, $e(\mathrm{P}/\mathfrak{p}) > 1$ équivaut à $\Omega_{\mathcal{O}_\mathrm{P}/\mathcal{O}_\mathfrak{p}} \neq 0$. Si t_F est une uniformisante en $\mathfrak{p}$, A la clôture intégrable de $\mathrm{A_F} = k[t_\mathrm{F}]$ dans K, on trouve

$$\Omega_{\mathcal{O}_\mathrm{P}/\mathcal{O}_\mathfrak{p}} = \mathcal{O}_\mathrm{P} \otimes_\mathrm{A} \Omega_{\mathrm{A}/\mathrm{A_F}}.$$

Pour que ce module soit non nul, il faut et il suffit que P soit dans le support de $\Omega_{\mathrm{A}/\mathrm{A_F}}$. Mais ce module est de type fini et de torsion car $\mathrm{K} \otimes \Omega_{\mathrm{A}/\mathrm{A_F}} = \Omega_{\mathrm{K}/\mathrm{F}} = (0)$ (car K/F séparable), donc de support fini.
(5) Si t' est une autre uniformisante en P, alors $\mathcal{O}dt = \Omega_{\mathcal{O}/k} = \mathcal{O}dt'$ et donc $dt' \in \mathcal{O}^{\times}dt$.
(6) Il nous faut démontrer que l'ensemble $\{\mathrm{P} \text{ point de } \mathrm{K} | v_\mathrm{P}(\omega) > 0\}$ est fini. Puisque $\Omega_{\mathrm{K}/k}$ est de dimension 1 sur K, il suffit de ne traiter qu'une différentielle. Par exemple, dt, avec t tel que $\mathrm{K}/k(t)$ soit une extension finie séparable. Soit $\varphi_t : \mathrm{C} \to \mathbb{P}^1_k$ le morphisme associé. Pour P dans $\varphi_t^{-1}(\mathbb{A}^1_k)$, on note $t(\mathrm{P}) \in k$ l'élément tel que $\varphi_t(\mathrm{P}) = [t(\mathrm{P}) : 1]$. La fonction $t - t(\mathrm{P})$ est une uniformisante en $\varphi_t(\mathrm{P})$. D'après la question (4), φ_t se ramifie en un nombre fini de points, et donc $t - t(\mathrm{P})$ est une uniformisante en presque tous points P de C. En un tel point on a donc $v_\mathrm{P}(dt) = v_\mathrm{P}(d(t - t(\mathrm{P}))) = 0$.
(7) Si c'est vrai pour une différentielle ω de K, c'est vrai pour toute car $\Omega_{\mathrm{K}/k} = \mathrm{K}\omega$.

Exercice 4 (Trouver des uniformisantes)**.** Soit $f(x, y) \in k[x, y]$ et C_0 la courbe d'équation $f(x, y) = 0$. Soit également $\mathrm{P} = (x_0, y_0)$ un point k-rationel de C.

(1) Montrer que $(\partial_y f)_{|\mathrm{P}} \neq 0$ implique que $x - x_0 \in k(\mathrm{C}_0)$ est une uniformisante en P, et que $(\partial_x f)_{|\mathrm{P}} \neq 0$ implique que $y - y_0 \in k(\mathrm{C}_0)$ est une uniformisante en P .
(2) En déduire en si P est un point lisse, alors l'une des deux fonctions $x - x_0$ ou $y - y_0$ est une uniformisante en P.

Solution: (1) Le problème étant symmétrique en x et y, il suffit de traiter celui où $(\partial_y f)_{|\mathrm{P}} \neq 0$. Il nous faut montrer que, dans $\mathcal{O}_\mathrm{P} \subset k(\mathrm{C}_0)$, tout élement s'annulant en P est divisible par $x - x_0$. Soit $\mathfrak{m}$ l'idéal $(x - x_0, y - y_0) \subset k[x, y]$. On développe f au voisinage de P :

$$f(x, y) = f(x_0, y_0) + (y - y_0)\left((\partial_y f)_{|\mathrm{P}} + (y - y_0)\sum_{i\geq 0} a_i(y - y_0)^i\right) + (x - x_0)k[x, y]$$

Comme $(\partial_y f)_{|\mathrm{P}} \neq 0$, le terme en facteur de $(y - y_0)$ est une unité de $\mathcal{O}_\mathrm{P}$. Si l'on réduit modulo l'idéal $(f(x, y))$, on trouve alors que $y - y_0$ est divisible par $x - x_0$. Si maintenant g désigne une fonction de $k(\mathrm{C})$ s'annulant sur P, g s'écrit comme une série formelle en $x - x_0$ et $y - y_0$ sans terme constant. Comme $y - y_0$ est divisible par $x - x_0$, il en est de même pour $g(x, y)$.
(2) Si P est lisse alors le vecteur $(\partial_x f, \partial_y f)_{|\mathrm{P}}$ est non nul d'après le critère de la jacobienne.

Exercice 5 (Une courbe de genre 1 qui n'est pas une courbe elliptique)**.** Soit k un corps de caractéristique $\neq 2$. Soit $f(x) \in k[x]$ un polynôme de degré d de discriminant non nul. On considère la courbe affine C_0/k d'équation

$$\mathrm{C}_0 : \quad y^2 = f(x) = a_0x^d + a_1x^{d-1} + \ldots + a_d$$

(1) Montrer que C_0 est lisse.
(2) On considère l'homogénéisation de C_0 dans $\mathbb{P}^2_k$:

$$\mathrm{C}_0^\mathrm{h} : \quad z^{d-2}y^2 = a_0x^d + a_1zx^{d-1} + \ldots + a_dz^d \quad ([x : y : z] \in \mathbb{P}^2_k).$$

Montrer que le point à l'infini $[0 : 1 : 0]$ de $\mathrm{C}_0^\mathrm{h}/k$ est singulier si $d \geq 4$.
(3) On suppose à présent $d = 4$. Considérons le morphisme $\mathrm{C}_0 \to \mathbb{P}^3_k$, $(x, y) \mapsto [1 : x : y : x^2]$, et soit $\mathrm{C} \subset \mathbb{P}^3_k$ la clôture de son image. Soit $\mathscr{H}$ l'hyperplan de $\mathbb{P}^3_k$ définit par l'équation $\mathrm{X}_0 = 0$. Montrer que C est lisse, que $\mathrm{C} \cap (\mathbb{P}^3_k \setminus \mathscr{H})$ est isomorphe à C_0 et que $(\mathrm{C} \cap \mathscr{H})(k)$ est vide si $a_0 \notin k^2$ ou $\{[0 : 0 : \pm\sqrt{a_0} : 1]\}$ sinon.
(4) En déduire l'existence d'une courbe de genre un sur $\mathbb{Q}$ qui ne possède pas de point rationnel.

Solution: (1) Soit $\mathrm{P} = (x_0, y_0)$ un point singulier. Le critère de la jacobienne en ce point donne $2y_0 = f'(x_0) = 0$. Comme 2 est inversible dans K, on trouve $f(x_0) = y_0^2 = 0$. En particulier x_0 est racine double de $f(x)$ ce qui contredit la non nullité de son discriminant.
(2) Soit $g(x, y, z)$ la différence du terme de gauche et de droite, de sorte que C_0^h soit définie par $g(x, y, z) = 0$. On a

$$\begin{aligned}
\partial_x g(x, y, z) &= -(a_0dx^{d-1} + a_1(d-1)zx^{d-2} + \ldots + a_1z^{d-1}),\\
\partial_y g(x, y, z) &= 2z^{d-2}y,\\
\partial_z g(x, y, z) &= (d-2)z^{d-3}y^3.
\end{aligned}$$

Si $d > 3$, en l'évaluant en $(x, y, z) = (0, 1, 0)$, on trouverait un vecteur nul.
(3) Soit I(C) l'idéal homogène de $k[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3]$ des fonctions qui s'annulent sur C (resp. l'image de C_0). Cet idéal contient les fonctions $\mathrm{F} = \mathrm{X}_3\mathrm{X}_0 - \mathrm{X}_1^2$ et

$$\mathrm{G} = \mathrm{X}_2^2\mathrm{X}_0^2 - (a_0\mathrm{X}_1^4 + a_1\mathrm{X}_1^3\mathrm{X}_0 + a_2\mathrm{X}_1^2\mathrm{X}_0^2 + a_3\mathrm{X}_1\mathrm{X}_0^3 + a_4\mathrm{X}_0^4).$$

Dans G, en remplaçant X_1^2 par $\mathrm{X}_3\mathrm{X}_0$, on trouve un troisième polynôme s'annulant sur C :

$$\mathrm{H} = \mathrm{X}_2^2 - a_0\mathrm{X}_3^2 - a_1\mathrm{X}_1\mathrm{X}_3 - a_2\mathrm{X}_0\mathrm{X}_3 - a_3\mathrm{X}_0\mathrm{X}_1 - a_4\mathrm{X}_0^2$$

On a alors $(\mathrm{H}, \mathrm{F}) \subset \mathrm{I(C)}$ et l'on prétend que l'on a une égalité.
D'abord, si $\mathrm{X}_0 \neq 0$ on "déshomogénéise" par rapport à X_0 (i.e. on pose $x = \mathrm{X}_1/\mathrm{X}_0$, $y = \mathrm{X}_2/\mathrm{X}_0$ et $z = \mathrm{X}_3/\mathrm{X}_0$), de sorte à obtenir :

$$z = x^2, \quad y^2 = a_0z^2 + a_1xy + a_2z + a_3x + a_4.$$

Si l'on substitue la première équation dans la deuxième, on retrouve l'équation de la courbe C_0.
Si $\mathrm{X}_0 = 0$, alors nécessairement $\mathrm{X}_1 = 0$ puis $\mathrm{X}_2 := \pm\sqrt{a_0}\mathrm{X}_3$. En particulier C a deux $\bar{k}$-points $(0, 0, \pm\sqrt{a_0}, 1)$ sur l'hyperplan d'équation $\mathrm{X}_0 = 0$. Ces points sont distincts puisque $a_0 \neq 0$ (sinon f aurait degré < 4). Pour montrer que C est non singulière en ces deux points, on déshomogénéise par rapport à X_3 en posant $u = \mathrm{X}_0/\mathrm{X}_3$, $v = \mathrm{X}_1/\mathrm{X}_3$ et $w = \mathrm{X}_2/\mathrm{X}_3$ pour obtenir

$$u = v^2, \quad w^2 = a_0 + a_1v + a_2u + a_3uv + a_4u^2,$$

puis l'équation affine

$$w^2 = a_0 + a_1v + a_2v^2 + a_3v^3 + a_4v^4. \tag{1}$$

Puisque $a_0 \neq 0$, les points $(v, w) = (0, \pm\sqrt{a_0})$ sont non singuliers. On les notera ∞_+ et ∞_-
(4) Il suffit de prendre $f(x) = -(x^4 + 1)$ et C la courbe obtenue par la question précédente. Pour démontrer qu'elle a genre 1, on peut par exemple utiliser la formule de Riemann-Hurwitz pour le morphisme $\mathbb{Q}(\mathrm{C}) \to \mathbb{P}^1_k$ corresponding to the projection $(x, y) \mapsto x$. Ici, on va plutôt démontrer que l'espace des formes différentielles holomorphes de $\mathbb{Q}(\mathrm{C})$ est de dimension 1.
Comme $f(x)$ est première à $f'(x)$, il existe $\mathrm{P}(x)$ et $\mathrm{Q}(x)$ tels que $\mathrm{P}f + \mathrm{Q}f' = 1$. On pose $\omega = \mathrm{P}ydx + 2\mathrm{Q}xdy$; on prétend que ω est non nulle et que $\mathrm{div}(\omega) = 0$, ce qui revient à ce que l'on cherche puisque $\Omega_{\mathrm{C}/\mathbb{Q}} = \mathbb{Q}(\mathrm{C})\omega$. On commence par vérifier que $y\omega = dx$ ce qui démontre sa nulité. Pour obtenir $\mathrm{div}(\omega) = 0$, il suffit de vérifier que

$$\mathrm{div}(y) = \mathrm{div}(dx).$$

Soit x_0, x_1, x_2, x_3 les zéros de f. D'après l'Exercice 4, y est une uniformisante en chacun des $\mathrm{P}_i = (x_i, 0)$. Ainsi y a des zéros simples en les P_i. De même $dx = d(x - x_i)$ où $x - x_i$ possède un zéro d'ordre 2 en $x - x_i$ (car $x - x_i = y^2/\prod_{j\neq i}(x - x_j)$), et donc dx a des zéros simples en les P_i. Reste à connaître le diviseur en les deux points manquants. Pour cela, on peut utiliser l'équation (1). Dans ces coordonnées,

$$x = \frac{\mathrm{X}_1}{\mathrm{X}_0} = \frac{\mathrm{X}_1}{\mathrm{X}_3} \cdot \frac{\mathrm{X}_3}{\mathrm{X}_0} = \frac{v}{u} = \frac{1}{v}, \quad y = \frac{\mathrm{X}_2}{\mathrm{X}_0} = \frac{\mathrm{X}_2}{\mathrm{X}_3} \cdot \frac{\mathrm{X}_3}{\mathrm{X}_0} = \frac{w}{v^2}.$$

D'ou $\mathrm{div}(y) = \mathrm{div}(w) - 2\mathrm{div}(v)$. La fonction w est régulière en les points $\infty_\pm$ et v a des zéros simples en les $\infty_\pm$. On en déduit

$$\mathrm{div}(y) = \mathrm{P}_1 + \mathrm{P}_2 + \mathrm{P}_3 + \mathrm{P}_4 - 2\infty_+ - 2\infty_-.$$

Un calcul similaire donne $\mathrm{div}(dx) = \mathrm{div}(y)$.