Examen du cours M2 2012 (Courbes Elliptiques sur un corps fini)

C. Huyghe

Sont proscrits pendant l'examen tous les documents relatifs au cours ou pas, ainsi que tous les appareils électroniques, y compris les téléphones portables, et les calculatrices.

On rappelle les deux résultats suivants :

1. Soit X une courbe lisse, intègre, projective, D un diviseur sur X, $l(D) = dim_k H^0(X, \mathcal{L}(D))$, K un diviseur canonique sur X (tel que $\mathcal{L}(K) \simeq \Omega^1_X$), alors on a la formule de Riemann Roch

$$l(D) - l(K - D) = deg(D) + 1 - g.$$

2. Soient k un corps, $f : X \to Y$, un morphisme fini séparable de courbes lisses, projectives, intègres de genre respectif $g(X), g(Y)$ et R le diviseur de ramification de f (dont le support est l'ensemble des points où f est ramifiée, pris avec coefficient $e - 1$ où e est l'indice de ramification en ce point, quand e est premier à la caractéristique de k). Alors, on a la formule d'Hurwitz :

$$2g(X) - 2 = deg(f)(2g(Y) - 2) + deg(R).$$

1. Exercice 1.

   Soient k un corps, $\mathbf{A}^3_k$ l'espace affine de dimension 3, muni des coordonnées x, y, z et C la courbe affine d'équations $y = x^4$ et $z = x^6$. Ainsi, en notant $A = k[x, y, z]$

$$C = spec\left(A \Big/ A(y - x^4) + A(z - x^6)\right).$$

   1- Montrer que C est une courbe affine, intègre, lisse, isomorphe à la droite affine. Montrer que pour toute extension finie l de k, les points de $C(l)$ sont les points de coordonnées t, t^4, t^6 pour $t \in l$.

   2- Dans la suite, on note I l'idéal $A(y - x^4) + A(z - x^6)$. Soit J l'idéal de A engendré par $x^2y - z$, $x^2z - y^2$ et $y^3 - z^2$. Montrer que $J \subset I$.

3- On pose $D = spec\,(A/J)$ et on identifie $\mathbf{A}^2_k$ au sous-schéma fermé de $\mathbf{A}^3_k$ défini par l'idéal $A \cdot x$. Soit i cette immersion fermée. Montrer que la fibre i^*C est réduite à un point et que la fibre i^*D est supportée par un point et n'est pas réduite.

4- Montrer que $J \neq I$.

5- Montrer que

$$J \cdot A\left[\frac{1}{x}\right] = y(y - x^4)A\left[\frac{1}{x}\right] + z(z - x^6)A\left[\frac{1}{x}\right].$$

6- Montrer que D contient une droite E donnée dans $\mathbf{A}^3_k$ par deux équations que l'on explicitera et que D possède deux composantes irréductibles la courbe C et la droite E. Ainsi, D est défini par des équations de degré 3, alors qu'une de ses composantes irréductibles est définie par une équation de degré 6.

7- On compactifie la courbe C en $\overline{C}$, dans $\mathbf{P}^3_k$, muni des coordonnées homogènes $[u, v, w, t]$, et on plonge $\mathbf{A}^3_k$ dans $\mathbf{P}^3_k$, en posant $x = u/t$, $y = v/t$ et $z = w/t$. Déterminer un système d'équations de $\overline{C}$. Montrer que le point de coordonnées homogènes $[0, 1, 0, 0]$ est l'unique point à l'infini de la courbe C. Est-ce que $\overline{C}$ est isomorphe à $\mathbf{P}^1_k$?

2. Exercice 2.

Dans tout l'exercice, X est une courbe projective lisse, intègre, sur un corps k et possédant un point rationnel P_0 sur k (i.e. $X(k) \neq \emptyset$). Si D est un diviseur de X, on note $l(D) = dim_k H^0(X, \mathcal{L}(D))$.

On munit $\mathbf{P}^1_k$ des coordonnées homogènes $[u, v]$. On pose $t = v/u$ et $s = u/v$.

1- On suppose que X est de genre g. Redémontrer le résultat du cours : $deg(K) = 2g - 2$.

2- On rappelle que se donner un morphisme $X \to \mathbf{P}^1_k$ revient à se donner une fonction rationnelle $f \in K(X)$. Montrer que $l((g+1)P_0) \geq 2$. En déduire qu'il existe un morphisme fini $X \to \mathbf{P}^1_k$ de degré $g + 1$.

3- On suppose que X est de genre 2. En considérant le diviseur canonique, montrer qu'il existe un morphisme fini $X \to \mathbf{P}^1_k$, de degré 2. On dit dans ce cas que X est hyperelliptique.

4- Pour cette partie, on suppose que le corps k est algébriquement clos. Soit $f : X \to \mathbf{P}^1_k$ un morphisme fini séparable.

   i. Montrer que f est ramifié en au moins un point. Dans la suite, on suppose que f est ramifié en l'infini (le point $[1, 0]$ de $\mathbf{P}^1_k$) avec un indice de ramification égal à 1.

ii. On pose

$$S = \left(k[t,y] \Big/ y^2 - P(t) \right)$$

pour P un polynôme de $k[t]$, unitaire de degré d, séparable. On suppose de plus que $U = f^{-1}(D_+(u))$ est un ouvert de X, isomorphe à $specS$, et que $g = f_{|U}$ est défini par l'application $k[t] \to S$ définie par $t \mapsto t$. Montrer que g est fini, de degré 2.

iii. On étudie la ramification de g. Plaçons-nous en un point fermé (x_0, y_0) de U. Notons $= x - x_0$, $= y - y_0$, $\mathcal{M} = (x - x_0)S + (y - y_0)S$, $S_{\mathcal{M}}$ le localisé de S en ce point, et $k(x_0, y_0)$ le corps résiduel en ce point (isomorphe à k). On notera h le morphisme d'anneaux locaux induit par g en ce point (x_0, y_0).

A. Supposons d'abord $y_0 \neq 0$. En calculant $y^2 - y_0^2$, montrer que est un générateur de $\mathcal{M}$. En déduire que f n'est pas ramifié en ce point.

B. On suppose maintenant que $y_0 = 0$. Montrer que $P(x) = (x - x_0)Q(x)$ avec $Q(x_0) \neq 0$ et que y engendre $\mathcal{M}$. En déduire que g est ramifié en ce point d'indice de ramification 2.

iv. Soit R le diviseur de ramification de f. Montrer que $deg(R) = deg(P) + 1$ et que $deg(P) = 2g + 1$

Dans la partie suivante, on donne une réciproque à cette constatation.

5- Dans toute la suite k est un corps de caractéristique différente de 2. Soient P un polynôme séparable, unitaire, de degré $2g + 1$, $Q(s) = s^{2g+2}P(1/s)$. On considère

$$U = spec \left(k[t,y] \Big/ y^2 - P(t) \right),$$

et

$$V = spec \left(k[s,z] \Big/ z^2 - Q(s) \right).$$

Montrer que l'on dispose de morphismes de degré 2 : $U \to D_+(u)$ et $V \to D_+(v)$ et que les schémas U et V se recollent le long de $D(t) \simeq D(s)$, en un schéma X, muni d'un morphisme de degré 2 : $X \to \mathbf{P}^1_k$.

6- Montrer que X ainsi défini est lisse.

7- On se propose de calculer le genre de X.

i. Montrer que Ω^1_X est libre sur $U \bigcap D(y)$ de base

$$\frac{dt}{2y}.$$

ii. Montrer que $U = D(y) \bigcup D(P')$, et que Ω^1_X est libre sur $U \bigcap D(y)$ de base

$$\frac{dy}{P'(t)}.$$

Vérifier que ces deux éléments coïncident sur $D(y) \bigcap D(P')$ et définissent un élément de $H^0(U, \Omega^1_X)$, qui est une base de Ω^1_X sur l'ouvert U.

iii. De même le faisceau Ω^1_X admet une base sur V engendré par l'élément

$$\frac{ds}{2z}.$$

Montrer que $H^0(X, \Omega^1_X)$ est le k-espace vectoriel, engendré par les éléments

$$! \ _i = \frac{t^i dt}{2y}, \ 0 \leq i \leq g-1,$$

et que la courbe X ainsi considérée est de genre g.

iv. On considère la courbe elliptique X d'équation $y^2 = x(x-1)(x- \ )$ pour $\in k$. Donner une base de $H^0(X, \Omega^1_X)$.

8- Montrer que $:K(X) \to K(X)$, qui envoie y sur $-y$ est un générateur du groupe de Galois $Gal(K(X)/k(t))$, qui induit une involution sur X. Montrer que agit par $-Id$ sur $H^0(X, \Omega^1_X)$.