Corrigé de l'examen de M2 2007-2008

C. Noot-Huyghe

1. 1- Soit $h(X) = X^{p-1} - \in \mathbf{Z}_p[X]$. Dans $\mathbf{F}_p$ il y a $p-1$ racines distinctes à l'équation $h(X) = 0$. De plus, si α est une telle racine, $h'(\alpha) = (p-1)\alpha^{p-2}$ est non nul. Une conséquence du lemme de Hensel est alors que chaque racine se relève en une racine de h dans $\mathbf{Z}_p$. ces racines sont distinctes puisqu'elles sont distinctes *modulo* p et cela montre que $\mathbf{Z}_p$ et donc $\mathbf{Q}_p$ contient les racines $p-1$-ièmes de l'unité.

   2- On peut supposer que f est unitaire et de degré n. Si $f = gh$, avec g et h unitaires, alors, on a une décomposition *mod* p $\overline{f} = \overline{g}\overline{h}$, en notant $\bar{t}$ la classe dans $\mathbf{F}_p[X]$ d'un polynôme $t \in \mathbf{Z}_p[X]$. Comme $\overline{f}$ est irréductible, cela donne que $\overline{g} = 1$ ou $\overline{h} = 1$, par exemple $\overline{g} = 1$. Comme g est unitaire, $deg(g) = deg(\overline{g}) = 0$ de sorte que f est irréductible.

   3- L'anneau A est un $\mathbf{Z}_p$-module libre de rang fini n, de base $1, X, \ldots, X^{n-1}$ (on utilisera par la suite le plongement $\mathbf{Z}_p \to A$ qui envoie x sur $x \cdot 1 \in \mathbf{Z}_p$). La valuation proposée est la restriction de la valuation $v(x) = \{max\, i |\, x \in p^i A\}$, ce qui est une valuation par les vérifications usuelles. La topologie induite par cette valuation est la topologie produit induite par $\mathbf{Z}_p$ sur A, si bien que A est complet pour la topologie induite par la valuation. L'idéal pA est maximal car le quotient A/pA est isomorphe à $\mathbf{Z}_p[X]/\overline{f}$, et est un corps car $\overline{f}$ est irréductible. Si $x \notin pA$, alors x est inversible dans A/pA, ce qui signifie qu'il existe $y \in A$, $u \in A$ tels que $xy = 1 + pu$. Soit $v = \sum_{k\in\mathbf{N}}(-1)^k p^k u^k$ qui converge dans A qui est p-adiquement complet, alors $vu = 1$, ce qui montre que x est inversible dans A et que pA est un idéal maximal. L'anneau A est un anneau local, de corps résiduel A/pA qui est un corps fini, isomorphe à $\mathbf{F}_q$ avec $q = p^n$.

   4- Si g est un autre relèvement de $\overline{f}$, alors g est irréductible et g est alors le polynôme minimal de x la classe de X dans l'algèbre $B = \mathbf{Z}_p[X]/g$. Dans $A/pA = \mathbf{F}_p[X]/\overline{f}$, $\overline{g}(X) = \overline{f}(X) = 0$ et $\overline{f}'(X) \neq 0$ car sinon $f(X)$ ne serait pas irréductible sur $\mathbf{Z}_p$, donc on peut relever la racine x de g en une racine de g dans A (puisque le lemme de Hensel est valide dans A d'après la question précédente), ce qui donne un morphisme $B \to A$. Symétriquement, on a un morphisme de $\mathbf{Z}_p$-algèbres $A \to B$. Le morphisme composé de ces 2 morphismes envoie une racine de f dans A sur une autre racine et est un isomorphisme (étendu au corps des fractions de A ce morphisme est un élément du groupe de Galois de ce corps). Cela montre que A et B sont isomorphes.

   5- Comme A/pA est isomorphe à $\mathbf{F}_q$, et que A est un anneau de valuation discrète où le lemme de Hensel est valide, c'est la même question que la question 1-.

2. 1- C'est du cours : $A = \Gamma(U, \mathcal{O}_U) = K[x][1/Q] = K[x, Q^{-1}]$.

   2- Le faisceau des formes différentielles sur $\mathbf{A}^1_K$ est un $\mathcal{O}_{\mathbf{A}^1_K}$-module libre de rang 1 engendré par dx. Par le théorème de changement de base pour le module des différentielles, $\Omega^1_U = \Omega^1_{\mathbf{A}^1_K|U}$ est un $\mathcal{O}_U$-module libre de rang 1 engendré par dx et $\Omega = \Gamma(U, \Omega^1_U) = A.dx = K[x, Q^{-1}]dx$.

   3- i. Soit $u = f/Q^n$, avec $f \in K[x]$ tel que f n'est pas divisible par Q. On calcule

$$d\left(\frac{f}{Q^n}\right) = \frac{Qf' - nQ'f}{Q^{n+1}}.$$

Si $d(u) = 0$, on a $Qf' = nQ'f$ et donc $Q|f$ puisque $Q \wedge Q' = 1$, ce qui est absurde, sauf pour $n = 0$ et $f' = 0$, c'est-à-dire si $u \in K$. Cela montre que $H^0_{DR}(U) = Ker(d) = K$. Calcul de $C = coker(d) = \Omega/Im(d)$.

ii. Soit $u = f/Q^n$ comme précédemment avec f non divisible par Q. Si on a $du = x^i/Q$ pour $0 \leq i \leq d-1$, cela donne la relation $Q(f' - x^iQ^{n-1}) = nQ'f$ et donc $Q|f$ sauf si $n = 0$ mais dans ce cas u est un polynôme et on ne peut pas avoir $d(u) = x^i/Q$.

iii. Il est évident que $\Omega = \bigcup_{n\geq 0} G_n$ et que $G_{n-1} \subset G_n$. Si $u = f/Q^n \in G_n$, on effectue la division euclidienne de f par Q : $f = aQ + b$ avec $deg(b) < d$ et ainsi $u = a/Q^{n-1} + b/Q^n \in G_{n-1} + \sum_{0\leq i\leq d-1} \frac{x^i}{Q^n}$, ce qui montre l'assertion.

iv. Comme Q' est premier avec Q, Q' est inversible modulo Q et la multiplication par Q' est un isomorphisme du K-espace vectoriel $K[x]/P$. Cette application transforme une base en une base, de sorte que les éléments $\overline{b_0}, \ldots, \overline{b_{d-1}}$ forment une base de $K[x]/P$. Soit maintenant x^j/Q^n pour $j \in \{0, \ldots, d-1\}$. Comme les éléments $\overline{b_i}$ forment une base de $K[x]/P$, il existe des scalaires $\mu_1, \ldots, \mu_{d-1}$, un polynôme $RdeK[x]$ tels que $x^j = \sum_{t=0}^{d-1} \mu_t b_t + QR$, de sorte que $x^j/Q^n \in G_{n-1} + \sum_{0\leq i\leq d-1} \frac{b_i}{Q^n} dx$, ce qui donne l'énoncé cherché.

v. On montre par récurrence sur $n \geq 0$ que $G_n \subset E + Im(d)$, cela montre l'assertion sur $H^1_{DR}(U)$ car alors E est une base de ce K-espace vectoriel. Pour $n = 0$, $G_0 = K[x]dx$. Soit $f = \sum_{l=1}^M c_l x^l$, alors $f(x)dx = d(\sum_{l=1}^M)c_l x^{l+1}/l+1)$ car le corps K est de caractéristique 0 et donc $G_0 \subset E + Im(d)$. Pour $0 \leq i \leq d-1$ et $n \geq 0$, on a

$$d\left(\frac{x^i}{Q^{n-1}}\right) = \frac{ix^{i-1}}{Q^{n-1}} - (n-1)\frac{x^iQ'}{Q^n}$$

soit encore

$$d\left(\frac{x^i}{Q^{n-1}}\right) = \frac{ix^{i-1} - (n-1)a_i}{Q^{n-1}} - (n-1)\frac{b_i}{Q^n}.$$

Si $G_{n-1} \subset E + Im(d)$, les termes $\frac{b_i}{Q^n}$ sont aussi dans $E + Im(d)$, ce qui montre que $G_n \subset E + Im(d)$.

3. 1- Les polynômes définissant f sont homogènes de sorte que f définit une application birationnelle de $\mathbf{P}^1_K$. Pour voir que cette application est bien définie, il faut vérifier qu'on ne peut pas avoir $u_0^n + \lambda u_0^{n-1}u_1 = 0$ et $u_1^n = 0$. Or ces égalités donnent $u_0 = u_1 = 0$, ce qui ne correspond pas à un point de l'espace projectif. Cela montre que f est bien définie.

2- Si $u_1 \neq 0$, alors $u_1^n \neq 0$, donc U_1 est stable par f. On munit u_1 de la coordonnée t. L'application $f : U_1 \to U_1$ est alors donnée $\mathcal{O}_{U_1} \to \mathcal{O}_{U_1}$ par $t \mapsto \lambda t^n + \lambda t^{n-1} = t^{n-1}(\lambda + t)$. Soit A l'anneau local en $t = 0$ de U_1 (qui correspond à l'∞). L'élément $\lambda + t$ est inversible dans A et, par définition, f est ramifié en ∞ d'indice $n-1$ (ramification modérée par hypothèse). Etudions $f^*\Omega^1_X \to \Omega^1_X$. L'image de dt est $d(t^n + \lambda t^{n-1}) = nt^{n-1} + \lambda(n-1)t^{n-2}dt$. L'application f est ramifiée aux points où cette dérivée s'annule, i.e. en ∞ (déjà traité) et en $t = \frac{-\lambda}{(}n-1)/n$. Comme l'ordre d'annulation de la dérivée en ce point est 1 et que 2 est premier avec $car(K)$, la ramification en ce point est modérée et est égale à 2.

3- On remarque que $f[1, s] = [1 + \lambda s, s^n]$, de sorte que f induit une application $D(1 + \lambda s) \to U_0$. On note encore f la restriction de cette application à $D(1 + \lambda s)$. L'ouvert $D(1 + \lambda s)$ contient 0. Comme on a étudié la ramification de f sur U_1, il suffit, pour étudier toute la ramification de f d'étudier ce qui se passe dans le complémentaire de U_1 c'est-à-dire en 0. Or, en restriction à $D(1 + \lambda s)$, f correspond à $s \mapsto s^n/(1 + \lambda s)$, et est donc modérément ramifiée d'indice n en 0.

Comme $f(U_1) \subset U_1$, $f^{-1}\{0\} = \{0\}$, avec ramification n. La formule du cours donne $f^*[0] = n = deg(f)deg([0]) = deg(f)$ et f est de degré n.

4- On a déjà répondu à cette question. On peut retrouver la réponse avec la formule d'Hurwitz, qui s'applique simplement car toute la ramification est modérée. Soit e la ramification cherchée. On trouve : -2=n(-2)+n-1+(n-2)+(e-1) et $e = 2$.

4. 1- D'après le cours $f^*[P] = \sum Q \in f^{-1}(P) e_Q[Q]$ où e_Q est l'indice de ramification du morphisme d'anneaux locaux $\mathcal{O}_P \to \mathcal{O}_Q$. De plus, $deg(f^*[P]) = deg(f)deg(P)$ et $P \in X(K)$ est de degré 1 par définition, ce qui donne $deg(f^*[P]) = deg(f) = n$.

2- La formule d'Hurwitz donne $2g(X) - 2 = -2n + deg(R)$ où, comme la ramification est modérée, où $deg(R) = \sum_{Q \in X} e_Q - 1$, cette somme étant en fait finie. Avec nos hypothèses $deg(R) = \sum Q \in f^{-1}\{P\}(e_Q - 1)deg(Q) = deg(f^*[P] - \sum Q \in f^{-1}\{P\})deq(Q) = n - \sum Q \in f^{-1}\{P\})$. En écrivant que $g(X) \geq 0$, on voit que $2 - n - \sum Q \in f^{-1}\{P\} \geq 0$ et $n \leq 2 - \sum Q \in f^{-1}\{P\}$. Comme $\sum Q \in f^{-1}\{P\} \geq 1$, cela montre que $n = 1$ et que f est un isomorphisme.

3- On procède comme précédemment. Dans ce cas, on a $deg(R) = deg(f^*[0]) + deg(f^*[\infty]-) \sum Q \in f^{-1}\{0\}) - \sum Q \in f^{-1}\{\infty\}) \leq 2n - 2$. La formule d'Hurwitz donne alors $2g(X) - 2 \leq -2$ et $g(X) \leq 0$, i.e. $g(X) = 0$ et X est isomorphe à $\mathbf{P}^1_K$.

5. 1- On vérifie d'abord que l'ouvert U' est lisse. Les points fermés où U' n'est pas lisse correspondent aux idéaux maximaux contenant y, P, P'. Or, ces 3 éléments engendrent $A = \Gamma(U', \mathcal{O}_X)$ car P et P' sont premiers entre eux. Sur V' il suffit de vérifier que si P et P' sont premiers entre eux, P_1 et P'_1 sont premiers entre eux. On traite ici le cas où $deg(P) = 2g + 1$, qui est le cas de l'énoncé avec $g = 2$. Les polynômes P_1 et P'_1 sont premiers entre eux si et seulement si $\mathbf{A}^1_K = D(P_1) \bigcup D(P'_1)$. Or comme les polynômes P et P' sont premiers entre eux et que $P'_1(t) = -t^{2g}P'(1/t) + (2g+2)t^{2g+1}P(1/t)$, l'ouvert $W = \mathbf{A}^1_K \backslash \{0\}$ est la réunion $W \bigcap D(P_1) \bigcup W \bigcap D(P'_1)$. Pour conclure, il suffit de vérifier que $\{0\} \in D(P_1) \bigcup D(P'_1)$. Or, on a toujours $P_1(0) = 0$ et si a est le coefficient du terme de plus haut degré de P, on a que $P'_1(0) = a \neq 0$, d'où l'assertion. On peut aussi montrer que P_1 et P'_1 sont premiers entre eux, en utilisant les formules et sans recourir à des arguments de géométrie.

2- Le genre g est égal à 2 d'après le cours.

3- Le module $\Gamma(U', \Omega^1_{U'})$ est le A-module libre $Ady + Ads/2ydy = P'(s)ds$. Donc, sur $D(y)$, ce module est libre engendré par ds et sur $D(P')$ ce module est libre engendré par dy. De plus, comme U' est lisse, $U' = D(y) \bigcup D(P')$. L'élément ω_0 est clairement une section sur $D(P')$. Sur $D(P') \bigcap D(y)$, on a $\omega_0 = dy/P'(s)$, qui est la restriction d'une section de $\Omega^1_{U'}$ sur $D(P')$, de sorte que ω_0 est une section globale de $\Omega^1_{U'}$ qui engendre ce faisceau sur chacun des ouvert $D(y)$ et $D(P')$. Le raisonnement pour ω_1 est identique.

4- Il reste à voir que ω_0 est une section de $\Omega^1_{V'}$, pour voir que c'est une section globale. Or, cela vient de la relation $ds/2y = -t^{g-1}dt/2z$ et $dt/2z \in \Gamma(V', \Omega^1_{V'})$ pour les mêmes raisons que précédemment. On a aussi $sds/2y = -t^{g-1}dt/2z \in \Gamma(V', \Omega^1_{V'})$ puisque $g \geq 2$. Les sections ω_0 et ω_1 sont linéairement indépendantes et $dimH^0(X, \Omega^1_X) = 2$ car X est de genre 2 : ces sections forment dont une base de ce K-espace vectoriel.

5- Comme Ω^1_X est libre, il suffit de calculer l'action de σ sur les éléments ω_0 et ω_1 vus comme sections sur U'. Comme $\sigma^{-1}(dy) = -dy$ et $\sigma^{-1}(s) = s$, σ agit par $-Id$ sur $H^0(X, \Omega^1_X)$.

6- On applique la formule de Riemann-roch : ${\Omega^1_X}^{\otimes 3}$ est associé au diviseur $D = 3K$ où K est le diviseur canonique. Comme le degré de $K - D = -2K$ est $-2(2g-2) < 0$ pour $g \geq 2$, $l(K - D) = 0$, ce qui donne $l(D) = deg(D) + 1 - g = 5(g-1)$, ce qui est égal à 5 pour $g = 2$.

7- Par fonctorialité, tout automorphisme de X induit un automorphisme de $H^0(X, \Omega^1_X)$ et donc aussi de $H^0(X, {\Omega^1_X}^{\otimes 3})$. Si cette application est injective, alors $Aut(X)$ se plonge dans le groupe d'automorphismes de $H^0(X, {\Omega^1_X}^{\otimes 3})$, qui est un K-espace vectoriel de dimension finie, et est un groupe fini si K est fini. Dans notre cas, ce cardinal est inférieur à $card(M_5(K))$ et donc à $card(K)^{25}$. Précisément, si K est de cardinal $q = p^i$, le cardinal de $H^0(X, {\Omega^1_X}^{\otimes 3})$ est égal à $(q^5-1)(q^5-q)(q^5-q^2)(q^5-q^3)(q^5-q^4)$, qui est donc un majorant de $card(Aut(X))$.