MAT 562 - Corrigé de l'examen - 2023-2024

Exercice 1

1) La variété V est équidimensionnelle de dimension 1.

2) Supposons que V soit irréductible et lisse. Montrons d'abord que $I(V(Y^n - P(X))) = (Y^n - P(X))$. Pour ce faire, on se donne un polynôme R dans $k[X,Y]$ tel que R^2 divise $Y^n - P(X)$. Le polynôme R divise alors $\frac{\partial(Y^n - P(X))}{\partial Y} = nY^{n-1}$. Donc $R = \lambda Y^\alpha$ avec $\lambda \in k^\times$ et $\alpha \leqslant n-1$. Du coup Y^α divise $P(X)$, et donc $\alpha = 0$ et R est constant. On déduit que le polynôme $Y^n - P(X)$ n'a pas de facteurs carrés, ce qui montre bien que $I(V(Y^n - P(X))) = (Y^n - P(X))$. Par ailleurs, la variété V étant lisse, le système d'équations :

$$\begin{cases} y^n = P(x), \\ ny^{n-1} = 0, \\ P'(x) = 0, \end{cases} \tag{1}$$

n'a pas de solutions dans k. Cela équivaut à ce que P et P' n'aient pas de racines communes, autrement dit à ce que P soit scindé à racines simples.

Réciproquement, supposons P scindé à racines simples. Soit α une de ses racines. Alors le polynôme $Y^n - P(X) \in k[X][Y]$ est Eisenstein pour l'irréductible $X - \alpha$. En particulier, c'est un polynôme irréductible et la variété V est irréductible. Elle est de plus lisse puisque le système (1) n'a pas de solutions dans k.

3) Supposons que V soit isomorphe à $\mathbb{A}^1_k$. En particulier, V est irréductible et lisse, donc P est scindé à racines simples. On peut donc écrire $P(X) = \prod_{i=1}^d (X - \alpha_i)$ avec les α_i deux à deux distincts. De plus, en réutilisant l'hypothèse que V est isomorphe à $\mathbb{A}^1_k$, on sait qu'il existe un isomorphisme de k-algèbres :

$$f : k[X,Y]/(Y^n - P(X)) \to k[T].$$

Posons $A(T) := f(X)$ et $B(T) := f(Y)$, de sorte que $B(T)^n = P(A(T))$. Du coup :

$$B(T)^n = \prod_{i=1}^d (A(T) - \alpha_i).$$

Mais les $A(T) - \alpha_i$ sont deux à deux premiers entre eux. Donc il existe des polynômes $B_1, ..., B_d$ tel que $A(T) - \alpha_i = B_i(T)^n$ pour chaque i. En particulier, $B_2(T)^n - B_1(T)^n$ est constant non nul. Mais $B_2 - B_1$ divise $B_2^n - B_1^n$. Donc $B_2 - B_1 = \lambda$ pour un certain $\lambda \in k^\times$. Le polynôme :

$$B_2^n - B_1^n = (B_1 + \lambda)^n - B_1^n = \sum_{i=0}^{n-1} C_n^i B_1^i \lambda^{n-i}$$

étant constant, une étude de son dégré montre immédiatement que B_1 est constant. Il en est donc de même de $A = B_1^n + \alpha_1$, ainsi que de B puisque $B(T)^n = P(A(T))$. L'image de f est donc contenue dans k, et f ne peut pas être surjectif : absurde ! On déduit que V ne peut pas être isomorphe à $\mathbb{A}^1_k$.

4) On a $\overline{V} = V_p(Y^n Z^{d-n} - Z^d P(X/Z))$. C'est une variété projective de dimension 1.

5) Supposons $\overline{V}$ irréductible et lisse. Alors V l'est aussi, et donc, par la question 2), le polynôme P est scindé à racines simples. Par ailleurs, en posant $\Psi(X,Z) := Z^d P(X/Z)$ et $\Phi(X,Y,Z) := Y^n Z^{d-n} - \Psi(X,Z)$, on a :

$$\frac{\partial \Phi}{\partial X} = -\frac{\partial \Psi}{\partial X}, \qquad \frac{\partial \Phi}{\partial Y} = nY^{n-1}Z^{d-n}, \qquad \frac{\partial \Phi}{\partial X} = (d-n)Y^n Z^{d-n-1} - \frac{\partial \Psi}{\partial Z}.$$

Du coup, en remarquant que Ψ est un polynôme homogène de degré $d > 2$ en X et Z :

$$\frac{\partial \Phi}{\partial X}(0,1,0) = 0, \qquad \frac{\partial \Phi}{\partial Y} = 0, \qquad \frac{\partial \Phi}{\partial Z} = \begin{cases} 0 \text{ si } d > n+1, \\ 1 \text{ si } d = n+1. \end{cases}.$$

Comme $\overline{V}$ est lisse au point $O := [0:1:0]$, on déduit que $d = n+1$.

Réciproquement, si P est scindé à racines simples et $d = n+1$, alors V est irréductible et lisse d'après la question 2), et $\overline{V}$ est lisse au point $O := [0:1:0]$ d'après les calculs précédents. Comme V est dense dans $\overline{V}$ et $\overline{V} = V \cup \{O\}$, on déduit que $\overline{V}$ est irréductible et lisse.

6) D'après le théorème de Bezout, pour tout point $Q \in \overline{V}$, on a :

$$m_Q(\overline{V}, T_Q(\overline{V})) \leqslant \deg(\overline{V}) \deg(T_Q(\overline{V})) = d.$$

7) Prenons $Q = O = [0:1:0]$. Par les calculs de la question 5), on voit que $T_O(\overline{V})$ est la droite d'équation $Z = 0$. Cette droite n'intersecte la courbe $\overline{V}$ qu'au point O. Le théorème de Bezout montre donc que :

$$m_O(\overline{V}, T_O(\overline{V})) = \deg(\overline{V}) \deg(T_O(\overline{V})) = d.$$

8) Supposons que $\overline{V}$ contient au moins deux points pour lesquels l'inégalité de la question 6) est une égalité. Par la question 7), cela signifie que V contient au moins un point $Q = (x_Q, y_Q)$ vérifiant cette propriété. La tangente $T_Q(V)$ à V en Q est paramétrisée par :

$$(x_Q, y_Q) + t(ny_Q^{n-1}, P'(x_Q)), \quad t \in k.$$

En réinjectant cette paramétrisation dans l'équation définissant V, on obtient :

$$(y_Q + tP'(x_Q))^n - P(x_Q + tny_Q^{n-1}) = 0.$$

On a alors $m_Q(\overline{V}, T_Q(\overline{V})) = d$ si, et seulement si :

$$(y_Q + P'(x_Q)T)^n - P(x_Q + ny_Q^{n-1}T) = \lambda T^d$$

pour un certain $\lambda \in k^\times$. En particulier, $y_Q \neq 0$, et en faisant le changement de variable $X = x_Q + ny_Q^{n-1}T$, on obtient :

$$P(X) = \left(y_Q + P'(x_Q)\frac{X - x_Q}{ny_Q^{n-1}}\right)^n - \lambda\left(\frac{X - x_Q}{ny_Q^{n-1}}\right)^d.$$

Il existe donc $\alpha, \beta, \gamma \in k, \delta \in k^\times$ tels que

$$P(X) = (\alpha + \beta X)^n - \lambda\,(\gamma + \delta X)^d$$

et $n(\delta\alpha - \gamma\beta)^{n-1} = \delta^{n-2}$. Réciproquement, soit P un polynôme de cette forme. Soient $x_Q := -\gamma\delta^{-1}$ et y_Q une racine n-ième de $P(x_Q) = \left(\frac{\alpha\delta-\beta\gamma}{\delta}\right)^n = \frac{\alpha\delta-\beta\gamma}{n\delta^2}$. Posons $Q = (x_Q, y_Q) \in V$. La tangente à V en Q est paramétrisée par :

$$(x_Q, y_Q) + t(ny_Q^{n-1}, P'(x_Q)), \quad t \in k,$$

avec $P'(x_Q) = n\beta\left(\frac{\alpha\delta-\beta\gamma}{\delta}\right)^{n-1} = \beta\delta^{-1}$. En réinjectant cette paramétrisation dans l'équation définissant V, on obtient :

$$(y_Q + t\beta\delta^{-1})^n - P(-\gamma\delta^{-1} + tny_Q^{n-1}) = 0.$$

Or :

$$\begin{aligned}
&(y_Q + \beta\delta^{-1}T)^n - P(-\gamma\delta^{-1} + ny_Q^{n-1}T) \\
&\quad = (y_Q + \beta\delta^{-1}T)^n - \left(\alpha - \beta\gamma\delta^{-1} + n\beta y_Q^{n-1}T)\right)^n - \lambda\left(ny_Q^{n-1}\right)^d T^d \\
&\quad = (y_Q + \beta\delta^{-1}T)^n - y_Q^{-n}\left(y_Q\frac{\alpha\delta - \beta\gamma}{\delta} + n\beta y_Q^n T)\right)^n - \lambda\left(ny_Q^{n-1}\right)^d T^d \\
&\quad = (y_Q + \beta\delta^{-1}T)^n - y_Q^{-n}\left(y_Q\frac{\alpha\delta - \beta\gamma}{\delta} + n\beta y_Q^n T)\right)^n - \lambda\left(ny_Q^{n-1}\right)^d T^d \\
&\quad = -\lambda\left(ny_Q^{n-1}\right)^d T^d.
\end{aligned}$$

On déduit que $m_Q(\overline{V}, T_Q(\overline{V})) = d$.

9) Les points vérifiant l'égalité dans la question 6) correspondent aux points de 3-torsion de la courbe elliptique $\overline{V}$. Du coup, les polynômes P trouvés à la question 8) correspondent aux courbes elliptiques ayant des points de 3-torsion non triviaux.

Exercice 2

1) Soient $\lambda \in \mathbb{C}$ et $f, g \in L(D)$. Si $f = 0$ ou $\lambda = 0$, on a bien sûr $\lambda f = 0 \in L(D)$. Sinon, on a $\mathrm{ord}_z(\lambda f) = \mathrm{ord}_z(f)$ pour tout $z \in M$, donc $\mathrm{div}(\lambda f) = \mathrm{div}(f)$ et $\lambda f \in L(D)$. Par ailleurs, si $f = 0$, $g = 0$ ou $f + g = 0$, on a bien sûr $f + g \in L(D)$. Sinon, on a $\mathrm{ord}_z(f + g) \geqslant \min\{\mathrm{ord}_z(f), \mathrm{ord}_z(g)\} \geqslant \min\{-n_z, -n_z\} = -n_z$ pour tout $z \in M$. On déduit que $\mathrm{div}(f+g) + D \geqslant 0$, c'est-à-dire que $f + g \in L(D)$.
2) Pour toute fonction Λ-elliptique non nulle f, on a $\deg(\mathrm{div}(f)) = 0$, et donc :
$$\deg(\mathrm{div}(f) + D) = \mathrm{D} < 0.$$
On ne peut donc pas avoir $\mathrm{div}(f) + D \geqslant 0$, et $\ell(D) = 0$.
3) Supposons que $\ell(D) > 0$. Pour tout $f \in L(D) \smallsetminus \{0\}$, on a $\mathrm{div}(f) + D \geqslant 0$. Comme $\deg(\mathrm{div}(f)) = \deg(-D) = 0$, on déduit que $\mathrm{div}(f) + D = 0$. Du coup, si f et g sont deux fonctions non nulles dans $L(D)$, on a $\mathrm{div}(f/g) = 0$. Autrement dit, f/g est holomorphe, donc constante. Cela étant vrai pour toutes f et g non nulles dans $L(D)$, on déduit que $\ell(D) \leqslant 1$.
4) a) i) Les fonctions 1, $\wp$, $\wp'$, ..., $\wp^{(n-2)}$ sont holomorphes hors de Λ et elles ont des pôles en 0 d'ordres respectifs 0, 2, 3, ..., n. Elles sont donc toutes dans $L(n[0])$, et commes les ordres de leurs pôles en 0 sont deux à deux distincts, elles forment une famille libre. Par ailleurs, si $f \in L(n[0])$, on peut trouver $\lambda_0, \ldots, \lambda_{n-2} \in \mathbb{C}$ tels que :
$$\mathrm{ord}_0(f - \sum_{i=0}^{n-2} \lambda_i \wp^{(i)}) \in \{-1, 0\}.$$
Supposons que $\mathrm{ord}_0(f - \sum_{i=0}^{n-2} \lambda_i \wp^{(i)}) = -1$. La fonction $f - \sum_{i=0}^{n-2} \lambda_i \wp^{(i)}$ étant holomorphe hors de Λ, elle a exactement un zéro z_0 dans $M \smallsetminus \{0\}$, nécessairement simple. Du coup :
$$\sum_{z \in M} z \cdot \mathrm{ord}_z(f - \sum_{i=0}^{n-2} \lambda_i \wp^{(i)}) = 0 \cdot (-1) + z_0 \cdot 1 = z_0 \in \Lambda,$$
ce qui est absurde puisque $z_0 \neq 0$. On déduit que
$$\mathrm{ord}_0(f - \sum_{i=0}^{n-2} \lambda_i \wp^{(i)}) = 0.$$
Du coup, la fonction Λ-elliptique $f - \sum_{i=0}^{n-2} \lambda_i \wp^{(i)}$ est holomorphe donc constante. Il existe alors $\lambda \in \mathbb{C}$ tel que $f = \lambda + \sum_{i=0}^{n-2} \lambda_i \wp^{(i)}$, ce qui montre que la famille $(1, \wp, \wp', ..., \wp^{(n-2)})$ est donc une base de $L(n[0])$, et $\ell(n[0]) = n$.

ii) L'espace vectoriel $L(D)$ est un sous-espace vectoriel de $L(n_{z_0}[0])$. Par la question i), $L(n_{z_0}[0])$ est un espace vectoriel de dimension n_0 de base :

$$(1, \wp, \wp', \dots, \wp^{(n_0-2)}).$$

Une fonction Λ-elliptique $f = \lambda + \sum_{i=0}^{n_0-2} \lambda_i \wp^{(i)}$ est dans $L(D)$ si, pour tout $z \in M$ tel que $n_z < 0$, on a :

$$\lambda + \sum_{i=0}^{n_0-2} \lambda_i \wp^{(i)}(z) = 0$$

et :

$$\sum_{i=0}^{n_0-2} \lambda_i \wp^{(i+r)}(z) = 0$$

pour $1 \leqslant r \leqslant -n_z + 1$. Autrement dit, $L(D)$ est un sous-espace vectoriel de $L(n_0[0])$ défini par :

$$\sum_{z \in M, n_z < 0} (-n_z) = n_0 - \deg(D)$$

équations linéaires. En particulier, $\ell(D) \geqslant n_0 - (n_0 - \deg(D)) = \deg(D)$.

iii) Soit S l'ensemble des zéros de D dans $M \smallsetminus \{0\}$. On considère la fonction :

$$f_0 = \prod_{s \in S} (\wp - \wp(s)).$$

Comme $\mathrm{div}(f_0) \geqslant -2|S|[0] + \sum_{s \in S}[s]$, il existe un entier $N > 0$ tel que 0 est l'unique zéro de $D - N\mathrm{div}(f_0)$. Du coup, $\ell(D - N\mathrm{div}(f_0)) \geqslant \deg(D - N\mathrm{div}(f_0)) = \deg(D)$. Or on a un isomorphisme :

$$\begin{aligned} L(D) &\to L(D - N\mathrm{div}(f_0)) \\ f &\mapsto f f_0^N. \end{aligned}$$

On déduit que $\ell(D) \geqslant \deg(D)$.

b) i) Posons :

$$E = \sum_{z \in M, n_z < 0} n_z [z] - \left(\sum_{z \in M, n_z < 0} n_z \right) [z_0]$$

avec $z_0 \in M$ tel que $n_{z_0} = 0$ et :

$$\sum_{z \in M, n_z < 0} n_z z - \left(\sum_{z \in M, n_z < 0} n_z \right) z_0 \notin \Lambda. \tag{2}$$

On a bien sûr $\deg(E) = 0$ et $D - E \geqslant 0$. De plus, par (2), il n'existe pas de fonction Λ-elliptique non nulle telle que $\mathrm{div}(f) + E = 0$. Or, comme $\deg(E) = 0$, la réponsé à la question 3) montre que :

$$L(E) = \{0\} \cup \{f \text{ fonction } \Lambda\text{-elliptique non nulle} : \mathrm{div}(f) + D = 0\}.$$

On déduit que $L(E) = 0$, puis que $\ell(E) = 0$.

ii) Par un argument similaire à la question 4.a)ii), comme $D - E \geqslant 0$ et $\deg(E) = 0$, l'espace $L(E)$ est un sous-espace vectoriel de $L(D)$ défini par $\deg(D)$ équations linéaires. Du coup :

$$0 = \ell(E) \geqslant \ell(D) - \deg(D),$$

et donc $\ell(D) \leqslant \deg(D)$.

Exercice 3

1) a) On a $\phi_q^2 + 2\sqrt{q} \cdot \phi_q + q = 0$. Donc $(\phi_q + \sqrt{q})^2 = 0$. Or l'anneau $\mathrm{End}(E)$ est intègre. Donc $\phi_q + \sqrt{q} = 0$.

b) Soit $x \in E(\overline{\mathbb{F}})[\sqrt{q} + 1]$. Alors :

$$\phi_q(x) = -\sqrt{q} \cdot x = -(1 + \sqrt{q})x + x = x.$$

Donc $x \in E(\mathbb{F})$.

c) On a $E(\overline{\mathbb{F}})[\sqrt{q} + 1] \cong \mathbb{Z}/(\sqrt{q} + 1) \oplus \mathbb{Z}/(\sqrt{q} + 1)$. On peut donc voir $\mathbb{Z}/(\sqrt{q}+1) \oplus \mathbb{Z}/(\sqrt{q}+1)$ comme un sous-groupe de $E(\mathbb{F})$. De plus, par la borne de Hasse :

$$|E(\mathbb{F})| \leqslant (\sqrt{q} + 1)^2.$$

On déduit que :

$$E(\mathbb{F}) \cong \mathbb{Z}/(\sqrt{q} + 1) \oplus \mathbb{Z}/(\sqrt{q} + 1).$$

2) a) Les racines du polynôme $T^3 + 7T^2 - 30T$ sont 0, 3 et -10. Elles sont deux à deux distictes dans $\mathbb{F}_p$ si, et seulement si, $p \notin \{2, 3, 5, 13\}$. Ainsi les nombres premiers tels que E est une courbe elliptique sont tout les nombres premier sà l'exception de 2, 3, 5 et 13.

b) i) Les points dans $E(\mathbb{F}_7)$ sont 0, $(0, 0)$, $(2, 2)$, $(2, 5)$, $(3, 0)$, $(-3, 0)$, $(-1, 1)$, $(-1, 6)$. Donc $E(\mathbb{F}_7)$ est d'ordre 8. De plus, $E(\mathbb{F}_7)$ contient 4 points de 2-torsion : 0, $(0, 0)$, $(3, 0)$ et $(-3, 0)$. C'est donc un groupe abélien d'ordre 8 dont la 2-torsion est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. On déduit que $E(\mathbb{F}_7) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

ii) Il existe deux nombres complexes α, β tels que :

$$\begin{cases} 8 = |E(\mathbb{F}_7)| = 7 + 1 - \alpha - \beta \\ \alpha\beta = 7 \\ |E(\mathbb{F}_{49})| = 49 + 1 - \alpha^2 - \beta^2. \end{cases}$$

En résolvant, on obtient $\alpha^2 + \beta^2 = (\alpha+\beta)^2 - 2\alpha\beta = -14$, et donc :

$$|E(\mathbb{F}_{49})| = 50 + 14 = 64 = (7+1)^2.$$

Par la question 1) :

$$E(\mathbb{F}_{49}) \cong (\mathbb{Z}/8\mathbb{Z})^2$$

3) a) On remarque que $13P$ est de 2-torsion, donc P est de 26-torsion. De plus, $2P \neq O$ et $13P \neq O$. Donc P est d'ordre 26. De plus, $E(\mathbb{F}_{41})$ contient 4 points de 2-torsion : O, $(0,0)$, $(3,0)$ et $(-10,0)$. Du coup, $E(\mathbb{F}_{41})$ contient un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$. Par la borne de Hasse, on sait aussi que :

$$|E(\mathbb{F}_{41})| \leqslant 42 + 2\sqrt{41} \leqslant 56.$$

Comme le seul multiple de 52 inférieur ou égal à 56 est 52 lui-même, on déduit que $|E(\mathbb{F}_{41})| = 52$, puis que :

$$E(\mathbb{F}_{41}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}.$$

b) La clé secrète de Dark Vador est un entier s tel que $M_2 - sM_1 = (15, 21)$. Autrement dit, $(16 - 5s)P = 7P$, c'est-à-dire $16 - 5s \equiv 7 \mod 26$. On trouve $s = 7$. Le message déchiffré de Maître Yoda est donc $M_2' - 7M_1'$. Dans le cas A), on obtient $M_2' - 7M_1' = 4P - 7 \cdot 6P = 14P = (40, 6)$. Dans le cas B), on obtient $M_2' - 7M_1' = 7P - 7 \cdot 11P = 8P = (21, 22)$. Dans le cas C), on obtient $M_2' - 7M_1' = 18P - 7 \cdot 15P = 17P = (29, 3)$. Dans le cas D), on obtient $M_2' - 7M_1' = 10P - 7 \cdot 19P = 7P = (15, 21)$. Maître Yoda doit donc choisir l'option C).

4) a) En faisant le changement de variable $x' = 9x + 21z$, $y' = 27y$ et $z' = z$, on voit que l'équation de $\tilde{E}$ équivaut à :

$$y'^2 z' = x'^3 - 139 \cdot 3^3 x' z'^2 + 2576 \cdot 3^3 z'^3.$$

On peut donc prendre $a = -139 \cdot 3^3$ et $b = 2576 \cdot 3^3$.

b) Le changement de variable précédent est inversible modulo 7 et modulo 41. Il montre donc que la réduction de la courbe elliptique d'équation $y^2z = x^3 + axz^2 + bz^3$ modulo 7 (resp. modulo 41) est isomorphe à la courbe elliptique étudiée à la question 2) (resp. à la question 3)). Donc $\tilde{E}(\mathbb{Q})_{\text{tors}}$ s'identifie à un sous-groupe de $E(\mathbb{F}_7) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et à un sous-groupe de $E(\mathbb{F}_{41}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$. On déduit que $\tilde{E}(\mathbb{Q})_{\text{tors}}$ s'identifie à un sous-groupe de $(\mathbb{Z}/2\mathbb{Z})^2$. Mais $\tilde{E}(\mathbb{Q})_{\text{tors}}$ contient les points 0, $(0,0)$, $(3,0)$ et $(-10,0)$. On déduit que :

$$\tilde{E}(\mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

c) La courbe elliptique $\tilde{E}$ contient le point $(-1,6)$, qui n'est pas de torsion. On déduit que $r \geqslant 1$. Par ailleurs, d'après la question 2)a), il existe 4 nombres premiers p tels que E n'est pas une courbe elliptique sur $\mathbb{F}_p$, à savoir 2, 3, 5 et 13. De plus, le changement de variable de la question 4)a) est inversible modulo tout nombre premier autre que 3. On déduit que la réduction de la courbe elliptique d'équation $y^2z = x^3 + axz^2 + bx^3$ modulo un nombre premier autre que 2, 3, 5 et 13 est encore une courbe elliptique. Autrement dit, les diviseurs premiers du discriminant $4a^3 + 27b^2$ sont parmi 2, 3, 5 et 13. En particulier, le rang de $\tilde{E}$ vérifie :

$$r \leqslant 2 \cdot 4 - 1 = 7.$$