Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

Corrigé de l'examen

Exercice 1.
On considère la courbe algébrique $\mathcal{C}$ d'équation

$$F = X^3 + Y^3 - 3XY$$

1. Montrer que $\mathcal{C}$ est un ensemble infini.
2. Montrer que $\mathcal{C}$ est *irréductible*
3. Montrer que $\mathcal{C}$ possède un unique point singulier.
4. Préciser la *nature* de ce point.

Corrigé.
1. On a $F = Y^3 - 3XY + X^3$.
Pour tout $x \in \mathbb{C}$, le polynôme $F(x, Y) = Y^3 - 3xY + x^3 \in \mathbb{C}[Y]$ possède une racine y dans $\mathbb{C}$.
On peut aussi dire que $\langle F \rangle \cap \mathbb{C}[X] = \{0\}$ donc que $Z(F)$ est infini.

2. On se place dans $\mathbb{C}[X][Y]$ et l'on suppose que :

$$F = Y^3 - 3XY + X^3 = (Y + a)\big(Y^2 + bY + c\big) = Y^3 + (a + b)\,Y^2 + (ab + c)\,Y + ac$$

de sorte que l'on a le système

$$a + b = 0 \tag{1}$$
$$ab + c = -3XY \tag{2}$$
$$ac = X^3 \tag{3}$$

On a alors $c - a^2 = 3XY$ mais $a = \lambda X^i$ et $c = \mu X^j$ avec $i + j = 3$ et $\lambda\mu = 1$
d'où $\mu X^j - \lambda^2 X^{2i} = 3XY$ ce qui n'est pas possible.

3. On a $\dfrac{\partial F}{\partial X} = 3\,X^2 - 3\,Y$ et
$\dfrac{\partial F}{\partial Y} = 3\,Y^2 - 3\,X$.
On a le système :

$$x^3 + y^3 - 3xy = 0 \tag{4}$$
$$x^2 - y = 0 \tag{5}$$
$$y^2 - x = 0 \tag{6}$$

en multipliant par x l'équation (2), par y l'équation (3) est en effectuant la somme on a

$$x^3 + y^3 - 6xy = 0 \tag{7}$$

d'où $xy = 0$ d'où une seule solution $x = 0$ et $y = 0$.

4. Le cône tangent à pour équation $-3XY$ d'où un point double ordinaire.

Exercice 2.

1. Soient $\mathcal{I} = \langle f_1, \cdots, f_r \rangle$ et $\mathcal{J} = \langle g_1, \cdots, g_s \rangle$ deux idéaux de $K[X_1, \cdots, X_n]$ où K est un corps ; on considère l'idéal
$$\mathcal{K} = \langle Y\, f_1, \cdots, Y\, f_r, (1-Y)\, g_1, \cdots, (1-Y)\, g_s \rangle$$
de $K[X_1, \cdots, X_n, Y]$. Montrer que $\mathcal{K} \cap K[X_1, \cdots, X_n] = \mathcal{I} \cap \mathcal{J}$.
2. En *déduire* un algorithme qui étant donnés un système générateur $[f_1, \cdots, f_r]$ de $\mathcal{I}$ et un système générateur $[g_1, \cdots, g_s]$ de $\mathcal{J}$ permet de construire un système générateur de $\mathcal{I} \cap \mathcal{J}$.
3. Montrer que si la *formule de Bezout* est valide dans $K[X_1, \cdots, X_n]$, on a $n = 1$.
4. Expliquer comment calculer le *pgcd* de deux polynômes $f, g \in K[X_1, \cdots, X_n]$ $(n \geq 2)$ *sans factoriser f et g.*

Corrigé.

1. Soit $F \in \mathcal{I} \cap \mathcal{J}$; on a $F = Y\, F + (1-Y)\, F \in \mathcal{K} \cap K[X_1, \cdots, X_n]$.
Réciproquement soit $F \in \mathcal{K} \cap K[X_1, \cdots, X_n]$; on a :
$$F = \sum_{i=1}^{r} Y\, h_i f_i + \sum_{j=1}^{s} (1-Y)\, h_{r+j} g_j \text{ avec } h_i \in K[X_1, \cdots, X_n, Y] \text{ pour } 1 \leq i \leq r+s$$
En prenant $Y = 1$ on obtient $F \in \mathcal{I}$ et en prenant $Y = 0$ on obtient $F \in \mathcal{J}$.

2. Soit $\mathbf{G}$ une base de Gröbner de $\mathcal{K}$ pour un ordre d'élimination tel que $Y \succ X_1, \cdots, X_n$. Alors, par le th d'élimination, $\mathbf{G} \cap K[X_1, \cdots, X_n]$ est une base de Gröbner de $\mathcal{K} \cap K[X_1, \cdots, X_n]$ donc un système générateur de cet idéal.

3. La formule de Bezout signifie qu'un idéal engendré par deux éléments $\langle f, g \rangle$ est principal. Par récurrence sur le nombre de générateurs, tout idéal de type fini est principal. Il en résulte que $K[X_1, \cdots, X_n]$ est principal, donc que $n = 1$.

4. Posons $\mathcal{I} = \langle f \rangle$, $\mathcal{J} = \langle g \rangle$ idéaux de $K[X_1, \cdots, X_n]$ Considérons $h = \text{ppcm}(f, g)$. On a $h \in \mathcal{I} \cap \mathcal{J}$.
Réciproquement si $H \in \mathcal{I} \cap \mathcal{J}$ on a $f | H$ et $g | H$ donc $h | H$ ainsi $\mathcal{I} \cap \mathcal{J} = \langle h \rangle$.
Considérons $\mathcal{K} = \langle Y\, f, (1-Y)\, g \rangle$ idéal de de $K[X_1, \cdots, X_n, Y]$. On a $\mathcal{K} \cap K[X_1, \cdots, X_n] = \mathcal{I} \cap \mathcal{J} = \langle h \rangle$.
Ainsi si $\mathbf{G}$ est la base de Gröbner réduite de $\mathcal{K}$ pour un ordre d'élimination tel que $Y \succ X_1, \cdots, X_n$, on a $\mathbf{G} \cap K[X_1, \cdots, X_n] = \{h\}$ avec $h = \text{ppcm}(f, g)$.
On a finalement $\text{pgcd}(f, g) = \dfrac{fg}{h}$.

Exercice 3.

Soient $\mathbb{F}_q$ un corps fini de caractéristique p avec $\text{Card}(\mathbb{F}_q) = q$ et Ω une clôture algébrique de $\mathbb{F}_q$. Pour *tout* sous-corps $K \subset \Omega$ de Ω et *tout* idéal I de $K[X_1, \cdots, X_n]$, on désigne par $Z_K(I) \subset K^n$ l'ensemble des zéros de I dans K^n.
De même, pour toute partie algébrique $E \subset \Omega^n$ on désigne par $\mathcal{I}_K(E)$ l'idéal de $K[X_1, \cdots, X_n]$ formé des polynômes $f \in K[X_1, \cdots, X_n]$ tels que $\widetilde{f}|_E = 0$ où $\widetilde{f} : \Omega^n \longrightarrow \Omega$ est l'*application polynomiale* associée à f.

1. Montrer que $V = \mathbb{F}_q^n$ est une *partie algébrique* de Ω^n.
2. Montrer que $\mathbf{G} = \{X_1^q - X_1, \cdots, X_n^q - X_n\}$ est une base de Gröbner *universelle* de l'idéal $\mathcal{N} = \langle X_1^q - X_1, \cdots, X_n^q - X_n \rangle$ de $\mathbb{F}_q[X_1, \cdots, X_n]$.

3. Montrer que $\mathcal{N} = \mathcal{I}_{\mathbb{F}_q}(V)$
4. Déterminer le *rang* de la $\mathbb{F}_q$-algèbre $\mathbb{F}_q[X_1, \cdots, X_n]/\mathcal{N}$.
5. On désigne par $\mathcal{F}(\mathbb{F}_q^n, \mathbb{F}_q)$ la $\mathbb{F}_q$-algèbre des applications de $\mathbb{F}_q^n$ dans $\mathbb{F}_q$. Montrer que l'homomorphisme canonique :

$$\begin{array}{ccc} \mathbb{F}_q[X_1, \cdots, X_n] & \longrightarrow & \mathcal{F}(\mathbb{F}_q^n, \mathbb{F}_q) \\ f & \longrightarrow & \widetilde{f}|_{\mathbb{F}_q^n} \end{array}$$

induit un *isomorphisme* de $\mathbb{F}_q$-algèbres :

$$\mathbb{F}_q[X_1, \cdots, X_n]/\mathcal{N} \xrightarrow{\simeq} \mathcal{F}(\mathbb{F}_q^n, \mathbb{F}_q)$$

6. Montrer que toute partie $E \subset \mathbb{F}_q^n$ de $\mathbb{F}_q^n$ est une partie *algébrique* de Ω^n.
7. Pour tout idéal I de $\mathbb{F}_q[X_1, \cdots, X_n]$, montrer que $\mathcal{I}_{\mathbb{F}_q}(Z_{\mathbb{F}_q}(I)) = I + \mathcal{N}$
8. Montrer que l'application $I \longrightarrow Z_\Omega(I)$ est une bijection de l'ensemble des idéaux $I \supset \mathcal{N}$ de $\mathbb{F}_q[X_1, \cdots, X_n]$ contenant $\mathcal{N}$ sur l'ensemble des parties de $\mathbb{F}_q^n$.
9. Pour tout idéal I de $\mathbb{F}_q[X_1, \cdots, X_n]$, montrer que $\mathrm{Card}(Z_{\mathbb{F}_q}(I))$ est égal au rang de la $\mathbb{F}_q$-algèbre $\mathbb{F}_q[X_1, \cdots, X_n]/\,(I + \mathcal{N})$.
10. On prend $q = 7$ et $n = 2$ et on considère la *courbe elliptique* $\mathcal{C}$ d'équation :

$$F = Y^2 - X^3 - 2X - 4$$

Déterminer le nombre de *points rationnels* de $\mathcal{C}$ (*ie.* les points $(x, y) \in \mathcal{C} \cap \mathbb{F}_7^2$).
La base de Gröbner réduite de l'idéal $\langle F, X^7 - X, Y^7 - Y\rangle$ *de* $\mathbb{F}_7[X, Y]$*, pour l'ordre lexicographique tel que* $X \prec Y$*, calculée avec* SAGE*, est :*

$$B = \left[Y^2 - X^3 + 5X + 3, YX^4 + 3YX^3 + YX^2 - YX, X^5 + 2X^4 + 5X^3 + 5X^2 + X\right]$$

Corrigé.
1. Soit $x \in \Omega^n$; pour $1 \leq i \leq n$ on a $x_i^q = x_i$ si et seulement si $x \in \mathbb{F}_q^n$ de sorte que $Z_\Omega(\mathcal{N}) = \mathbb{F}_q^n$.

2. On a $X_i | X_i^q$; quelque soit l'ordre admissible choisi on a donc donc $X_i \prec X_i^q$ et par suite $\mathrm{lm}_\preceq(X_i^q - X_i) = X_i^q$ pour $1 \leq i \leq n$ $(q \geq 2)$. Ainsi les éléments de $\mathrm{lm}_\preceq(\mathbf{G})$ sont deux à deux premiers entre eux et $\mathbf{G}$ est une base de Gröbner de $I = \langle X_1^q - X_1, \cdots, X_n^q - X_n\rangle$.

3. On a évidemment $\mathcal{N} \subset \mathcal{I}_{\mathbb{F}_q}(V)$.
Remarquons aussi que $V = Z_\Omega(\mathcal{N}) = Z_{\mathbb{F}_q}(\mathcal{N})$.
On a alors , par le théorème des zéros de Hilbert : $\mathcal{I}_{\mathbb{F}_q}(V) = \mathcal{I}_{\mathbb{F}_q}(Z_\Omega(\mathcal{N})) = \mathrm{rac}(\mathcal{N})$ mais, pour $1 \leq i \leq n$, le polynôme $X_i^q - X_i$ à pour dérivée -1 donc est séparable, le lemme de Seidenberg montrer que $\mathcal{N}$ est radiciel et finalement on a $\mathcal{N} = \mathcal{I}_{\mathbb{F}_q}(V)$.

4. Par le théorème de Macaulay on a $\mathbb{F}_q[X_1, \cdots, X_n] = \mathcal{N} \oplus \mathcal{R}$; le $\mathbb{F}_q$-espace vectoriel $\mathcal{R}$ a pour base les monômes standards $X_1^{\alpha_1}. \cdots .X_n^{\alpha_n}$ avec $0 \leq \alpha_i \leq q-1$ pour $1 \leq i \leq n$ de sorte que $\dim_{\mathbb{F}_q}(\mathcal{R}) = q^n$.

5. On a l'application $\mathbb{F}_q$-linéaire injective :

$$\begin{array}{cccc} \varphi : & \mathbb{F}_q[X_1, \cdots, X_n]/\mathcal{N} & \longrightarrow & \mathcal{F}(\mathbb{F}_q^n, \mathbb{F}_q) \\ & \overline{f} & \longrightarrow & \widetilde{f} \end{array}$$

mais $(\delta_a)_{a\in\mathbb{F}_q^n}$ avec $\delta_a(x)=\begin{cases}1 & \text{si } x=a\\ 0 & \text{sinon}\end{cases}$ est une base de $\mathcal{F}(\mathbb{F}_q^n,\mathbb{F}_q)$ donc $\dim_{\mathbb{F}_q}(\mathcal{F}(\mathbb{F}_q^n,\mathbb{F}_q))=q^n$ et φ et un isomorphisme.
On pourrait aussi utiliser que le cardinal de chacun des deux membres est q^{q^n}.

6. Soit $E\subset\mathbb{F}_q^n$; on prend un polynôme $F\in\mathbb{F}_q[X_1,\cdots,X_n]$ tel que $\widetilde{F}|_{\mathbb{F}_q^n}$ soit la fonction caractéristique de E. Alors si $I=\langle F\rangle+\mathcal{N}$ on a $Z_\Omega(I)=E$.

7. Notons d'abord que $I+\mathcal{N}$ est radiciel par le lemme de Seidenberg.
Par le théorème des zéros de Hilbert appliqué à l'idéal $I+\mathcal{N}$ de $\mathbb{F}_q[X_1,\cdots,X_n]$ on a alors :

$$Z_\Omega(I+\mathcal{N})=Z_\Omega(I)\cap Z_\Omega(\mathcal{N})=Z_\Omega(I)\cap V=Z_{\mathbb{F}_q}(I)$$

et par suite :

$$\mathcal{I}_{\mathbb{F}_q}(Z_{\mathbb{F}_q}(I))=\mathcal{I}_{\mathbb{F}_q}(Z_\Omega(I+\mathcal{N}))=\mathrm{rac}(I+\mathcal{N})=I+\mathcal{N}$$

8. Si $I\supset\mathcal{N}$ on a $\mathcal{I}_{\mathbb{F}_q}(Z_{\mathbb{F}_q}(I))=I$ de sorte que l'application $I\longrightarrow Z_{\mathbb{F}_q}(I)$ est injective ; en reprenant l'idéal $I=\langle F\rangle+\mathcal{N}$ de la question 6. on a $I\supset\mathcal{N}$ et $Z_{\mathbb{F}_q}(I)=Z_\Omega(I)=E$.

9. Puisque l'idéal $I+\mathcal{N}$ est radiciel on a $\mathrm{Card}(Z_{\mathbb{F}_q}(I))=\dim_{\mathbb{F}_q}(\mathbb{F}_q[X_1,\cdots,X_n]/\left(I+\mathcal{N}\right)$.

10. On a $\mathrm{Card}(\mathcal{C}\cap\mathbb{F}_7^2)=\dim_{\mathbb{F}_7}(\mathbb{F}_7[X,Y]/\langle F,X^7-X,Y^7-Y\rangle$. Cette dimension est le nombre de monômes réduits. On considère la base de Grôbner B. Les monômes dominants sont X^5,Y^2,X^4Y de sorte que les monômes réduits sont $1,X,X^2,X^3,X^4,Y,XY,X^2Y,X^3Y$.
On a donc $\mathrm{Card}(\mathcal{C}\cap\mathbb{F}_7^2)=9$.