

Contrôle terminal du 16 avril 2014

durée 2h

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.

Exercice 2.

1. Soient $\mathcal{I} = \langle f_1, \dots, f_r \rangle$ et $\mathcal{J} = \langle g_1, \dots, g_s \rangle$ deux idéaux de $K[X_1, \dots, X_n]$ où K est un corps ; on considère l'idéal

$$\mathcal{K} = \langle Y f_1, \dots, Y f_r, (1 - Y) g_1, \dots, (1 - Y) g_s \rangle$$

de $K[X_1, \dots, X_n, Y]$. Montrer que $\mathcal{K} \cap K[X_1, \dots, X_n] = \mathcal{I} \cap \mathcal{J}$.

2. En *déduire* un algorithme qui étant donnés un système générateur $[f_1, \dots, f_r]$ de $\mathcal{I}$ et un système générateur $[g_1, \dots, g_s]$ 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 $K[X_1, \dots, X_n]$, on a $n = 1$.
4. Expliquer comment calculer le *pgcd* de deux polynômes $f, g \in K[X_1, \dots, X_n]$ ($n \geq 2$) *sans factoriser f et g .*

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 $K[X_1, \dots, X_n]$, 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 $K[X_1, \dots, X_n]$ formé des polynômes $f \in K[X_1, \dots, X_n]$ tels que $f|_E = 0$ où $f : \Omega^n \rightarrow \Omega$ 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 $\mathbf{G} = \{X_1^q - X_1, \dots, X_n^q - X_n\}$ est une base de Gröbner *universelle* de l'idéal $\mathcal{N} = \langle X_1^q - X_1, \dots, X_n^q - X_n \rangle$ de $\mathbb{F}_q[X_1, \dots, X_n]$.
3. Montrer que $\mathcal{N} = \mathcal{I}_{\mathbb{F}_q}(V)$
4. Déterminer le *rang* de la $\mathbb{F}_q$ -algèbre $\mathbb{F}_q[X_1, \dots, X_n]/\mathcal{N}$.

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 :

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

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

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

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 $\mathbb{F}_q[X_1, \dots, X_n]$, 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 $\mathbb{F}_q[X_1, \dots, X_n]$ contenant $\mathcal{N}$ sur l'ensemble des parties de $\mathbb{F}_q^n$.
 9. Pour tout idéal I de $\mathbb{F}_q[X_1, \dots, X_n]$, montrer que $\text{Card}(Z_{\mathbb{F}_q}(I))$ est égal au rang de la $\mathbb{F}_q$ -algèbre $\mathbb{F}_q[X_1, \dots, X_n]/(I + \mathcal{N})$.
 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 :

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