N1MA8W02 Algèbre et Calcul Formel

Examen Final

19 avril 2012, durée 3h

Documents interdits, calculatrices autorisées

1 Dans cet exercice on revisite l'algorithme de Berlekamp. Soit q une puissance d'un nombre premier et soit $\mathbb{F}_q$ le corps fini à q éléments. Soit $P(X) \in \mathbb{F}_q[X]$ un polynôme unitaire de degré n. Soit

$$E := \{V(X) \in \mathbb{F}_q[X]/(P(X)) : V(X)^q = V(X)\}.$$

1. Montrez que, pour tout $V \in \mathbb{F}_q[X]$, $V(X)^q = V(X^q)$.
2. Montrez que E est un $\mathbb{F}_q$-espace vectoriel.
3. Si $P(X) = \prod_{i=1}^{k} R_i(X)$ où les polynômes R_i sont irréductibles et deux à deux distincts, quelle est la dimension de E ?
4. Soit $V \in E$. Montrez que
$$\prod_{a \in \mathbb{F}_q} (V(X) - a) = 0.$$
Indication : on pourra utiliser que $Y^q - Y = \prod_{a \in \mathbb{F}_q}(Y - a)$.
5. En déduire que, pour tout $V \in \mathbb{F}_q[X]$, $V \neq 0$, tel que $V(X) \bmod P(X) \in E$,
$$P(X) = \prod_{a \in \mathbb{F}_q} \mathrm{pgcd}(P(X), V(X) - a).$$
6. Maintenant on suppose $q = 5$ et $P(X) = X^{12} - 1$. Montrez que P n'a que des facteurs irréductibles simples (i.e. de multiplicité 1).
7. Calculez (toujours pour ce cas) une base de E. Quelle est sa dimension ?
8. Soit $V(X) = X^3$. Si vous n'avez pas résolu la question précédente, vérifiez directement que $V \in E$. Calculez $\mathrm{pgcd}(P(X), X^3 - a)$ pour $a \in \mathbb{F}_5$ et en déduire que
$$X^{12} - 1 = \prod_{a \in \mathbb{F}_5^*} (X^3 - a).$$
9. Recommencez avec $X^3 - a$ pour obtenir la factorisation complète de $X^3 - a$, puis celle de $P(X)$.

2 Dans cet exercice on va démontrer le théorème suivant (qui a été énoncé mais non démontré en cours) :

Théorème 0.1 *Soit $B = \{g_1, \ldots, g_k\}$ une base de Gröbner d'un idéal I de $K[X_1, \ldots, X_n]$ pour l'ordre lexicographique inversé $\prec$ pour lequel $X_1 \prec X_2 \prec \cdots \prec X_n$. Alors, pour tout $1 \leq i \leq n$,*

$$K[X_1, \ldots, X_i] \cap I = (K[X_1, \ldots, X_i] \cap B)K[X_1, \ldots, X_i].$$

On note $\mathrm{lt}(f)$ le terme dominant de $f \in K[\underline{X}]$.

1. Soit $f \in I$. Montrez que l'algorithme de division multivariée de f par B rend une expression pour f de la forme $f = \sum_{j=1}^{k} h_j g_j$ avec $\mathrm{lt}(h_j g_j) \preceq \mathrm{lt}(f)$.
2. En déduire que, si $f \in K[X_1, \ldots, X_i] \cap I$, alors, pour tout $1 \leq i \leq k$, $\mathrm{lt}(h_j g_j) \in K[X_1, \ldots, X_i]$, puis que, si $h_j \neq 0$, $\mathrm{lt}(g_j) \in K[X_1, \ldots, X_i]$.
3. Déduire finalement que, sous les hypothèses précédentes, si $h_j \neq 0$, $g_j \in K[X_1, \ldots, X_i]$.
4. Terminer la démonstration du théorème.

3 Soit I un idéal de $K[\underline{X}]$ où $\underline{X} = (X_1, \ldots, X_n)$. Soit $f_1, \ldots, f_s$ des générateurs de I. On suppose que le quotient $K[\underline{X}]/I$ est de dimension finie (en tant que K-espace vectoriel). Soit $P \in K[\underline{X}]$, on considère l'application :

$$\begin{aligned} \phi_P : K[\underline{X}]/I &\to K[\underline{X}]/I \\ f &\mapsto Pf. \end{aligned}$$

1. Montrez que ϕ_P est une application linéaire.
2. Soit $(b_1, \ldots, b_d)$ une base de $K[\underline{X}]/I$. Soit A_P la matrice de l'application ϕ_P dans cette base. On a donc :
$$\phi_P(b_j) = \sum_{i=1}^{d} (A_P)_{i,j} b_i.$$
Soit $x \in K^n$ un zéro commun aux polynômes $f_1, \ldots, f_s$. Montrez que le vecteur colonne $(b_1(x), \ldots, b_d(x))^t$ est vecteur propre de A_P pour la valeur propre $P(x)$.
3. Déduisez de ce qui précède une méthode algorithmique pour calculer les valeurs possibles des coordonnées x_i des zéros communs des polynômes $f_1, \ldots, f_s$.

Application : on prend $K = \mathbb{R}$ et $f_1 = X^2 + 2Y^2 - 2Y$, $f_2 = XY^2 - XY$, $f_3 = Y^3 - 2Y^2 + Y$.

4. Vérifiez que $\{f_1, f_2, f_3\}$ est une base de Gröbner pour l'ordre lexicographique vérifiant $X \succ Y$.
5. En déduire une base de $\mathbb{R}[\underline{X}]/I$.
6. Écrire les matrices A_X et A_Y et calculer leurs polynômes caractéristiques.
7. En déduire les valeurs possibles de x et y vérifiant
$$\begin{cases} f_1(x, y) = 0 \\ f_2(x, y) = 0 \\ f_3(x, y) = 0 \end{cases}$$
puis vérifiez.