Université de Bordeaux — **Algèbre et calcul formel – Master**
Mathématiques — Année 2023–2024

FEUILLE D'EXERCICES n° 10

Exercice 1 – [Berlekamp et irréductibilité]
Soient p un nombre premier et $P = x^p - x - 1 \in \mathbb{F}_p[x]$. En utilisant l'endomorphisme de $F_p[x]/(P)$ qui à a associe a^p et la matrice de cet endomorphisme dans la base des $[X^i]_P$, montrer que P est irréductible.

Exercice 2 – [Autre preuve d'irréductibilité dans ce cas particulier]
On reprend p un nombre premier et $P = x^p - x - 1 \in \mathbb{F}_p[x]$. Soient Q un facteur non constant de P et r une racine de Q dans un corps de décomposition de Q.

1) Montrer que pour tout $i \in \mathbb{Z}$, $Q(r + [i]_p) = 0$.

2) En déduire que $Q = P$, et donc que P est irréductible.

Exercice 3 – [Cantor-Zassenhaus en caractéristique 2]
On rappelle l'algorithme de Cantor-Zassenhaus en caractéristique impaire.

Algorithme 1. Factorisation dans $\mathbb{F}_q[x]$.

Entrées: $q = p^k$, où p est un nombre premier impair, $Q \in \mathbb{F}_q[x]$ de degré n, produit de polynômes irréductibles deux à deux distincts de degré d.
Sorties: Un diviseur non trivial de Q, ou bien "échec".
1: Tirer au hasard $A \in \mathbb{F}_q[x]$ de degré inférieur à n.
2: Calculer $D = \mathrm{pgcd}(A, Q)$. Si $D \neq 1$, sortir D.
3: Calculer $B = A^{(q^d-1)/2} - 1 \bmod Q$
4: Calculer $D = \mathrm{pgcd}(B, Q)$. Si $D \neq 1$ et $D \neq Q$, sortir D. Sinon, sortir "échec".

---

1) En appliquant cet algorithme, factoriser le polynôme $x^4 + x^3 + x - 1$ de $\mathbb{F}_3[x]$, en prenant $d = 2$ et $A = x - 1$.

2) Soit $m \geqslant 1$, et soit

$$T_m = x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^4 + x^2 + x \in \mathbb{F}_2[x].$$

a) Montrer que $T_m(T_m + 1) = x^{2^m} + x$.

b) En déduire que si $\alpha \in \mathbb{F}_{2^m}$, alors $T_m(\alpha) \in \mathbb{F}_2$.

c) Montrer que l'application $\alpha \mapsto T_m(\alpha)$ de $\mathbb{F}_{2^m}$ dans $\mathbb{F}_2$ est une application linéaire de F_2-espaces vectoriels. En déduire que les ensembles $\{\alpha \in \mathbb{F}_{2^m} \ : \ T_m(\alpha) = 0\}$ et $\{\alpha \in \mathbb{F}_{2^m} \ : \ T_m(\alpha) = 1\}$ ont même cardinal, soit 2^{m-1}.

Soient maintenant $q = 2^k$ et $Q \in \mathbb{F}_q[x]$ de degré n. On suppose que Q est produit de r polynômes irréductibles sur $\mathbb{F}_q$ qu'on note $P_1, \ldots, P_r$, deux à deux distincts et tous de même degré d. On note $R = \mathbb{F}_q[x]/(Q)$, $R_i = \mathbb{F}_q[x]/(P_i)$ et φ_i l'application canonique de R dans R_i définie par $\varphi_i(P \bmod Q) = P \bmod P_i$.

3) Soit $A \in R$. Montrer que pour tout i, $\varphi_i(T_{kd}(A)) \in \mathbb{F}_2$ (dans $\mathbb{F}_2[X]/(P_i)$) et que si A est choisi au hasard dans R avec probabilité uniforme, $T_{kd}(A)$ appartient à $\mathbb{F}_2$ (dans $\mathbb{F}_2[X]/(P)$) avec probabilité 2^{1-r}.

4) En déduire un algorithme pour factoriser Q et montrer que sa probabilité d'échec est inférieure à $1/2$.

Exercice 4 – [Partie sans facteur carré]

Soient p un nombre premier et $q = p^k$. Ce travail porte sur un algorithme permettant de calculer la partie sans facteur carré d'un polynôme de $\mathbb{F}_q[x]$, au sens rappelé ci-dessous.

Soit P un polynôme non nul de $\mathbb{F}_q[x]$. Alors il existe un entier naturel r, des polynômes unitaires irréductibles deux à deux distincts $P_1, \ldots, P_r$ de $\mathbb{F}_p[x]$, des entiers naturels non nuls $e_1, \ldots, e_r$ et un élément $\alpha \in \mathbb{F}_p^*$ tels que $P = \alpha \prod_{i=1}^{r} P_i^{e_i}$.

La partie sans facteur carré de P est égale à $\prod_{i=1}^{r} P_i$.

1) Soit $Q = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_q[x]$. Montrer que $Q^p = \sum_{i=0}^{n} a_i^p x^{pi}$.

2) Soit $R \in F_q[x]$. Montrer que la dérivée R' de R est nulle si et seulement s'il existe $Q \in \mathbb{F}_q[x]$ tel que $R = Q^p$.

3) Soit P un polynôme unitaire de $\mathbb{F}_q[x] \setminus \{0\}$. On l'écrit comme ci-dessus (avec $\alpha = 1$ puisque P est unitaire) $P = \prod_{i=1}^{r} P_i^{e_i}$. Soient

$$I = \{i \in \{1, \ldots, r\} \ : \ p \not| e_i\} \quad , \quad J = \{i \in \{1, \ldots, r\} \ : \ p | e_i\}\,,$$

$$U = \frac{P}{\operatorname{pgcd}(P, P')} \quad \text{et} \quad V = \frac{P}{\operatorname{pgcd}(U^d, P)},$$

où $d = \deg P$. Montrer que $U = \prod_{i \in I} P_i$ et $V = \prod_{i \in J} P_i^{e_i}$.

4) Montrer que V s'écrit $V = W^p$, où $W \in \mathbb{F}_q[x]$.

5) Soit $P = x^{11} + x^{10} + 2x + 2 \in \mathbb{F}_5[x]$. Calculer successivement P', $\operatorname{pgcd}(P, P')$, U, $\operatorname{pgcd}(U^d, P)$, V et W. En déduire la partie sans facteur carré de P.

6) On peut calculer la partie sans facteur carré de P en utilisant la méthode suivante. On calcule les polynômes U et V de la question 3. On cherche $W \in \mathbb{F}_q[x]$ tel que $V = W^p$, puis on recommence en appliquant le même processus à W (à la place de P), jusqu'à obtenir un polynôme V égal à 1. La partie sans facteur carré est alors le produit des polynômes U obtenus à chacune des étapes de cet algorithme.

Écrire cet algorithme sur sage.