Université de Bordeaux
Mathématiques

Calcul formel – Master
2025–2026

FEUILLE D'EXERCICES n° 10

Exercice 1 – [Matrices]
Il existe différentes façons de définir une matrice. Nous allons ici définir d'abord l'espace des matrices qui nous intéresse. Par exemple, on définit $\mathcal{M}_3(\mathbb{F}_3)$ par la commande

```
MF3=MatrixSpace(GF(3),3,3)
```

Alors, la commande

```
M=MF3([1,2,0,1,0,1,2,2,1])
```

définit une matrice.

Il peut aussi être commode de définir une matrice par une formule donnant ses coefficients. Par exemple, la matrice $A = (a_{ij})$ de $\mathcal{M}_6(\mathbb{Q})$ telle que $a_{ij} = i + j$ peut être définie comme suit.

```
A=matrix(QQ,6,6,lambda i,j:i+j)
```

Revenons à la matrice M. Pour obtenir son noyau à droite, on utilise la commande

```
KerM=M.right_kernel()
```

Pour une base du noyau

```
KerM.basis()
```

Comme d'habitude, pour un élément au hasard dans ce noyau, on peut utiliser la commande

```
KerM.random_element()
```

Enfin, la commande

```
MF3(1)
```

donne la matrice identité dans $\mathcal{M}_3(\mathbb{F}_3)$.

Exercice 2 – [Algorithme de Berlekamp : un exemple simple]
Soit $f = x^6 + 2x^5 + x^4 + 2x^3 + x - 1 \in \mathbb{F}_5[x]$.

1) Calculer $\text{pgcd}(f, f')$.

2) Calculer $\text{pgcd}(f, x^5 - x)$.

3) Sachant cela, quelles sont les structures possibles de l'anneau $A = \mathbb{F}_5[x]/(f)$?

4) Soit F l'aplication de A dans lui-même qui à x associe x^5. Écrire la matrice de $F - \text{Id}$ dans la base $1, x, \ldots, x^5$ de A, et calculer son noyau N.

5) Combien f possède-t-il de facteurs irréductibles ? Quel est leur degré ?

6) Prendre un élément a au hasard dans N et calculer $\text{pgcd}(a, f)$ et $\text{pgcd}(a^2 - 1, f)$. Recommencer jusqu'à obtenir un facteur non trivial de f.

Exercice 3 – [Algorithme de Berlekamp]
Le programmer.

Exercice 4 – [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 5 – [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 6 – [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 $1/2$.