Université de Bordeaux
Mathématiques

Calcul formel – Master
2025–2026

FEUILLE D'EXERCICES n° 9

Travail sur machine

Ce travail porte sur l'algorithme de Cantor-Zassenhaus pour factoriser des polynômes à coefficients dans un corps fini.

Exercice 1 – [Calculs sur les corps finis]

1) $\mathbb{F}_p$: soit p un nombre premier. On rappelle que pour définir $\mathbb{F}_p$ sur sage, on peut écrire `k=GF(p)` (où p est bien sûr préalablement défini).

2) Si p est un nombre premier, comparez les types de $\mathbb{F}_p =$ `GF(p)` et $\mathbb{Z}/p\mathbb{Z} =$ `Zmod(p)` en Sage. Dans la suite, il faudra bien faire attention de toujours utiliser la première.

3) $\mathbb{F}_q$: soit $q = p^k$ une puissance de p.

a) Pour définir $\mathbb{F}_q$, on peut utiliser un polynôme irréductible P de degré k de $\mathbb{F}_p[x]$ de la manière suivante.

```
k.<a>=GF(q, modulus=P)
```

Alors, $\mathbb{F}_q$ est défini par $\mathbb{F}_p[x]/(P)$ et a est la classe de x dans ce quotient.

b) On peut aussi laisser sage choisir le polynôme P en tapant `k.<a>=GF(q)`. Alors a est la classe de x dans un certain quotient $\mathbb{F}_p[x]/(P)$. Pour connaître P, il suffit d'utiliser la commande `k.modulus()`.

c) On peut même taper simplement `k=GF(q)`. Pour retrouver le P et le a, on utilise alors les commandes `k.modulus()` et `k.gen()`.

4) Anneau de polynômes. Si k est un corps codé `k`, on définit l'anneau $k[x]$ par

```
kx.<x>=PolynomialRing(k).
```

Pour tirer au hasard un polynôme de degré entre 0 et n :

```
kx.random_element((0,n))
```

5) Exponentiation rapide. Soient f et g deux polynômes de $k[x]$ et n un entier. Pour calculer $f^n \mod g$ rapidement, on dispose de la commande `pow(f,n,g)`.

6) Anneaux quotients. On peut s'en passer pour la suite de ce travail. La commande suivante permet de définir l'anneau quotient $A = k[x]/(f)$.

```
A.<z>=kx.quotient(f)
```

Alors z est la classe de x dans le quotient $k[x]/(f)$.

Exercice 2 – [Racines dans $\mathbb{F}_q$ d'un polynôme f de $\mathbb{F}_q[x]$]

En Sage, il est possible de tester l'irréductibilité d'un polynôme $P \in \mathbb{F}_q[X]$ via la commande

`P.is_irreducible()`.

Pour factoriser, vous pourrez (pour l'instant) utiliser la commande

`P.factor()`.

Remarque : L'algorithme utilisé par Sage pour tester l'irréductibilité dépend de l'implémentation du corps sous-jacent, et en réalité peut parfois utiliser des algorithmes de factorisation, mais laissons ça de côté et utilisons-le pour le moment comme une boîte noire.

1) En choisissant des polynômes P non irréductibles, vérifiez que $\texttt{gcd}(X^q - X, P)$ est bien un produit de polynômes de degré 1.

2) En déduire une méthode générale pour calculer les racines d'un polynôme univarié à coefficients dans $\mathbb{F}_q$.

3) Voyez-vous comment généraliser à la résolution d'un système d'équations polynomiales (univariées) ?

Exercice 3 – [Algorithme de Cantor-Zassenhaus]

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 (à la main) le polynôme $x^4 + x^3 + x - 1$ de $\mathbb{F}_3[x]$, en prenant $d = 2$ et $A = x - 1$.

2) Programmer l'algorithme de Cantor-Zassenhaus et le tester sur l'exemple ci-dessus. Vous pouvez aussi modifier l'algorithme pour qu'il continue tant que vous obtenez une erreur à la dernière étape.

3) Tester également votre fonction sur $x^8 + 8x^6 + 9x^4 + 6x^2 + 4 \in \mathbb{F}_{11}[x]$. Ici, le degré des polynômes irréductibles est égal à 2.

4) Le n-ème polynôme cyclotomique Φ_n est un polynôme important à coefficiants entiers. Il est donné en Sage par `cyclotomic_polynomial(n)`. Tester votre fonction sur le polynôme cyclotomique Φ_{16} vu comme un polynôme de $\mathbb{F}_3[x]$ avec $d = 4$, puis de $\mathbb{F}_9[x]$ avec $d = 2$.

5) On peut montrer que dans $\mathbb{F}_q[x]$, le polynôme Φ_n est produit de polynômes irréductibles de degré d, où d est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$. Pour calculer cet ordre, on peut faire les opérations suivantes.

```
A=Integers(n)
Aq=A(q)
Aq.multiplicative_order()
```

Ici, `A` est l'anneau $\mathbb{Z}/n\mathbb{Z}$ et `Aq` est la classe de q dans cet anneau. Sachant cela, tester l'algorithme de Cantor-Zassenhaus sur $\Phi_{25} \in \mathbb{F}_9[x]$.

Exercice 4 – [Calcul de tous les facteurs]

Écrire une fonction `DegresEgaux` qui, étant donné un polynôme Q sans facteur carré dont tous les facteurs irréductibles sont de degré d, rend ces facteurs irréductibles. Cette fonction utilisera l'algorithme de Cantor-Zassenhaus de la question précédente pour trouver un facteur D et s'appellera elle-même récursivement sur D et Q/D.

Exercice 5 – [Factorisation complète]

Les polynômes sont dans $\mathbb{F}_q[x]$.

1) Soit $P = x^{11} + 3x^{10} + 2x^9 + 3x^8 + x^7 + x^5 + 3x^4 + 2x^2 + 4x \in \mathbb{F}_5[x]$.

a) Calculer le produit D_1 des éléments de $\mathrm{Irr}(5, 1)$ qui divisent P (en calculant $\mathrm{pgcd}(x^5 - x, P)$).

b) En utilisant `DegresEgaux`, calculer la factorisation de D_1.

c) Pour tout irréductible $P_{1,i}$ divisant D_1, calculer la plus grande puissance $\alpha_{1,i}$ de $P_{1,i}$ qui divise P, et remplacer P par $P/P_{1,i}^{\alpha_{1,i}}$.

d) calculer le produit D_2 des éléments de $\mathrm{Irr}(5, 2)$ qui divisent le nouveau P (en calculant $\mathrm{pgcd}(x^{5^2} - x, P)$).

e) En utilisant `DegresEgaux`, calculer la factorisation de D_2.

f) Pour tout irréductible $P_{2,i}$ divisant D_2, calculer la plus grande puissance $\alpha_{2,i}$ de $P_{2,i}$ qui divise P, et remplacer P par $P/P_{2,i}^{\alpha_{2,i}}$.

g) En déduire la factorisation complète de P.

2) Écrire une fonction qui, étant donné un polynôme quelconque, donne sa décomposition complète, en utilisant la stratégie de la question précédente.

Exercice 6 – [Cantor-Zassenhaus en caractéristique 2]

Tel que nous l'avons décrit jusqu'à présent, l'algorithme de Cantor-Zassenhaus ne fonctionne qu'en caractéristique impaire. Le but de cet exercice est de l'adapter à la caractéristique 2.

1) Soit $m \geqslant 1$. On définit le polynôme

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

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 $\mathbb{F}_2$-espaces vectoriels. On l'appelle *trace* de $\mathbb{F}_{2^m}$ sur $\mathbb{F}_2$.

d) 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}.

On fixe maintenant $q = 2^k$ et on considère $Q \in \mathbb{F}_q[x]$ 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 $R = \mathbb{F}_q[x]/(Q)$, et $R_i = \mathbb{F}_q[x]/(P_i)$. Soit φ_i l'application canonique de R dans R_i définie par $\varphi_i(P \mod Q) = P \mod P_i$.

2) 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}.

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