Corps finis

Exercice 1. — Soient $A = X^4 + 2X + 1$ et $B = 2X^2 + X + 2 \in \mathbf{Z}[X]$

a) Calculer la division euclidienne de $\overline{A}$ par $\overline{B}$ dans $\mathbf{F}_3[X]$.

b) Calculer la division euclidienne de $\overline{A}$ par $\overline{B}$ dans $\mathbf{F}_5[X]$.

c) Comparer les pgcd de $\overline{A}$ et $\overline{B}$ dans $\mathbf{F}_3[X]$ et $\mathbf{F}_5[X]$.

d) Qu'en déduit-on sur le pgcd de A et B dans $\mathbf{Z}[X]$?

Exercice 2. — Soit p premier et $Q \in \mathbf{F}_p[X]$ un polynôme irréductible de degré n.

a) Montrer que $K := \mathbf{F}_p[X]/(Q)$ est un corps fini à p^n éléments.

b) **A.N.** : pour $p = 2$ et $Q = X^2 + X + 1$ (resp. $p = 3$ et $Q = X^3 + X^2 + 2$) dresser la liste de tous les éléments, ainsi que leurs produits et leurs inverses.

c) Montrer que K contient un unique sous-corps à p éléments.

d) Montrer que $K^\times$ est cyclique. Combien $K^\times$ a-t-il de générateurs ?
Trouver un générateur pour les deux exemples ci-dessus.

Exercice 3. — En en dressant la liste exhaustive, combien y a-t-il de polynômes irréductibles de degré 2 et 3 dans $\mathbf{F}_2[X]$.

Exercice 4. — Soient $m, n \geqslant 1$ des entiers.

a) Comparer la division euclidienne de $X^n - 1$ par $X^m - 1$ en fonction de celle de n par m.

b) En déduire que dans $\mathbf{F}_{p^n}$ admet un sous-corps à p^m élément ssi m divise n.

Exercice 5. — Soit $n \geqslant 0$ et P_1, P_2 deux polynômes irréductibles de $\mathbf{F}_p[X]$ de même degré n. On note $K_1 := \mathbf{F}_p[X]/(P_1)$ et $K_2 := \mathbf{F}_p[X]/(P_2)$. Le but est de montrer que les corps K_1 et K_2 sont isomorphes.

a) Si A est une $\mathbf{F}_p$-algèbre. Montrer que la donnée d'un morphisme de $\mathbf{F}_p$algèbre de K_1 dans A équivaut à la donnée d'une racine de P_1 dans A.

b) Montrer que K_2 est l'ensemble des racines de $X^{p^n} - X$ dans une clôture algébrique de K_2. En déduire que P_1 admet une racine α dans K_2.

c) Quel est le polynôme minimal de cet élément $\alpha \in K_2$?

d) En déduire un isomorphisme entre K_1 et K_2.
[**Indication:** Utiliser la question **c)** pour montrer que le morphisme est injectif.]

e) **A.N.** Expliciter l'isomorphisme lorsque $P_1 = X^2 + X + 2$ et $P_2 = X^2 + 2X + 2 \in \mathbf{F}_3[X]$.

f) L'isomorphisme entre K_1 et K_2 est-il unique ?

Exercice 6. — Soit $P = X^4 + 1 \in \mathbf{F}_7[X]$.

a) P est-il sans facteur carré ?

b) En utilisant l'algorithme de Berlekamp, montrer que P n'est pas irréductible.

c) Factoriser P dans $\mathbf{F}_7[X]$.

***Exercice 7* (Exam 2018)**. — On considère le polynôme $P = X^3 + X^2 + X + 1$ dans $\mathbb{F}_3[X]$.

a) Expliciter une base du $\mathbb{F}_3$-espace vectoriel $\mathbb{F}_3[X]/(P)$ et la matrice de l'endomorphisme $\varphi : y \mapsto y^3$ dans cette base.

b) Donner une base du noyau de $\varphi - \mathrm{id}$. Que dit cette base sur l'irréductibilité de P ?

c) Quelles sont les racines de P dans $\mathbb{F}_3$?
En déduire les facteurs irréductibles de P dans $\mathbb{F}_3[X]$ puis, avec une relation de Bezout, un isomorphisme explicite d'un produit de corps finis de la forme $\mathbb{F}_3[X]/(Q)$ dans $\mathbb{F}_3[X]/(P)$.

d) Avec cet isomorphisme retouver une base de $\mathrm{Ker}(\varphi - \mathrm{id})$.