Corps finis

I. Groupes abéliens finis

Exercice 1. — Soient m et n deux entiers positifs.

a) Si m et n sont premiers entre eux, rappeler l'énoncé du lemme chinois.
Dans ce cas, expliciter l'isomorphisme inverse.

b) Lorsque m et n ne sont plus premiers entre eux, existe-t-il isomorphisme entre ces anneaux (éventuellement donné par une autre formule) ?

c) Résoudre dans $\mathbf{Z}$:

$$\begin{cases} x \equiv 1\ [7] \\ x \equiv 3\ [5] \end{cases} , \quad \begin{cases} x \equiv 1\ [45] \\ x \equiv 3\ [6] \end{cases} , \quad \begin{cases} x \equiv 4\ [45] \\ x \equiv 1\ [6] \end{cases}$$

Exercice 2. — Combien y a t-il (à isomorphisme près) de groupes abéliens de cardinal 48 ? Parmi ces groupes, lequel est isomorphe à $(\mathbf{Z}/105\mathbf{Z})^\times$?

II. Corps finis

Exercice 3. — Soit K un corps fini et $\varphi : \mathbf{Z} \to K$ le morphisme canonique.

a) Montrer que $\ker\varphi$ est un idéal de la forme (p), avec p premier.

b) Montrer que K est de cardinal une puissance de p.
[**Indication:** Remarquer que K est naturellement un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel.]

c) Quel est à isomorphisme près le groupe abélien fini $(K, +)$?

Exercice 4. — Soit $q = p^n$ une puissance d'un nombre premier et $\mathbf{F}_q$ un corps fini à q éléments.

a) Montrer que $\mathbf{F}_q^*$ est cyclique.
[**Indication:** Soit $d_1|\dots|d_r$ les facteurs invariants de $\mathbf{F}_q^*$. Considérer les racines dans $\mathbf{F}_q$ du polynôme $X^{d_r} - 1$.]

b) Donner tous les générateurs des groupes $(\mathbf{Z}/5)^\times$, $(\mathbf{Z}/7)^\times$ et $(\mathbf{Z}/11)^\times$.

Exercice 5. — Soit $Q \in (\mathbf{Z}/p\mathbf{Z})[X]$ un polynôme irréductible unitaire de degré n.

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

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

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

Exercice 6. — **[Algorithme de Berlekamp]**
Soit $P \in \mathbf{F}_p[X]$ un polynôme sans facteur carré ; on note $P = P_1 \dots P_r$ la décomposition de P en facteurs irréductibles. Soit $E := \mathbf{F}_p[X]/(P)$.

a) Montrer que E est un produit de corps finis.

b) Soit $\varphi : E \to E,\ e \mapsto e^p$. Montrer que φ est une linéaire et que l'on a $\dim\ker(\varphi - \mathrm{id}) = r$.
En déduire un test d'irréductibilité dans $\mathbf{F}_p[X]$.

c) Si $r > 1$, justifier qu'il existe un élément $\overline{Q} \in \ker(\varphi - \mathrm{id})$ "non constant".
Montrer qu'il existe $\lambda \in \mathbf{F}_p$, tel que $\mathrm{pgcd}(P, Q - \lambda)$ soit un diviseur non trivial de P.

d) Programmer cet algorithme de factorisation. Comment traiter également les polynômes ayant éventuellement des facteurs irréductibles avec multiplicités ?