

Feuille d'exercices n° 5  
Rappels sur les corps finis

**Exercice 1 (caractéristique des corps finis, Fröbenius).** Soit  $k$  un corps fini. Rappeler :

1. Sa caractéristique  $p$  est un nombre premier.
2. Le cardinal de  $k$  est de la forme  $p^n$ .
3. L'application  $x \in k \mapsto x^p$  est un automorphisme de corps (appelé *automorphisme de Fröbenius*).
4. L'application  $x \in k \mapsto x^{p^i}$  est un automorphisme de corps pour tout entier  $i \geq 0$ .
5. Caractériser parmi les éléments de  $k$  les éléments de son sous-corps premier.

**Exercice 2.** Soit  $q = p^n$  avec  $p$  premier et  $n \geq 1$ , et soit  $K = \mathbb{F}_q$ .

1. Montrer si  $k$  est un sous-corps de  $K$ , alors  $k$  est d'ordre  $p^d$ , où  $d$  est un diviseur de  $n$ .
2. Réciproquement, montrer que pour tout diviseur  $d$  de  $n$ , le corps  $\mathbb{F}_q$  a exactement un sous-corps d'ordre  $p^d$ .

**Exercice 3.** Soit  $k$  un corps fini d'ordre  $q$ , et soit  $K = k(\beta)$  une extension de corps de degré  $n \geq 1$ . Soit  $\beta_i$  les puissances  $q^e$  successives de  $\beta$  :

$$\beta_0 = \beta, \quad \beta_{i+1} = \beta_i^q, \quad i = 0, \dots, n-1.$$

On a donc  $\beta_n = \beta$ . On considère enfin  $g(X)$  le polynôme à coefficients dans  $K$  donné par :

$$g(X) = \prod_{i=0}^{n-1} (X - \beta_i).$$

1. Montrer que  $g(X^q) = (g(X))^q$  et en déduire que  $g(X)$  est à coefficients dans  $k$ .
2. Montrer que les  $\beta_i$  sont tous distincts pour  $i = 0, \dots, n-1$ . *Indication* : sinon il existe  $i < n$  avec  $\beta^{q^i} = \beta$ , ce qui contredit que  $\beta$  est de degré  $n$ .
3. Montrer que  $g(X)$  est le polynôme minimal de  $\beta$  dans  $k$ .

**Exercice 4.** Soit  $k \subset K$  une extension de corps de degré  $n$  entre deux corps finis  $k$  et  $K$ . Soit  $P$  un polynôme à coefficients dans  $k$  et irréductible sur  $k[X]$ . Montrer que les trois propriétés suivantes sont équivalentes :

- i.  $P$  est scindé sur  $K$  ;
- ii.  $P$  a une racine dans  $K$  ;
- iii. le degré de  $P$  divise  $n$ .

**Exercice 5.** Soit  $k \subset K$  une extension entre deux corps finis  $k$  et  $K$ . Soit  $q = |K|$ .

1. Montrer l'égalité suivante dans  $K[x]$  :

$$x^q - x = \prod_{\beta \in K} (x - \beta).$$

2. Montrer que  $x^q - x$  est le produit dans  $k[x]$  des polynômes minimaux distincts des éléments de  $K$ .

**Exercice 6.** Soit  $k$  un corps fini d'ordre  $q$ , et soit  $m = q^n$  avec  $n \geq 1$ .

1. Montrer que, dans  $k[x]$ , le polynôme  $x^n - x$  est le produit de tous les polynômes unitaires irréductibles dont le degré divise  $n$  (utiliser le résultat de l'exercice précédent).
2. Soit  $I_q(n)$  le nombre de polynômes irréductibles sur  $\mathbb{F}_q$ . Montrer la formule suivante :

$$q^n = \sum_{d|n} d I_q(d).$$

**Exercice 7 (formule d'inversion de Möbius).**

1. *La fonction de Möbius.* Soit  $\mu : \mathbb{N}^* \rightarrow \{-1, 0, 1\}$  la fonction de Möbius définie par  $\mu(n) = 0$  si  $n$  contient un facteur premier carré, et  $\mu(p_1 \dots p_r) = (-1)^r$  si les  $p_i$  sont des nombres premiers distincts. Montrer les propriétés suivantes de la fonction de Möbius :
  - (a)  $\mu$  est multiplicative, c'est-à-dire :  $n \wedge m = 1 \Rightarrow \mu(mn) = \mu(m)\mu(n)$ .
  - (b) Pour tout entier  $n > 1$ , on a  $\sum_{d|n} \mu(d) = 0$ , et  $\mu(1) = 1$ .
2. *Formule d'inversion.* Soit  $f : \mathbb{N}^* \rightarrow G$  une fonction à valeurs dans un semi-groupe abélien  $G$  noté additivement (on peut prendre  $G = \mathbb{Z}$  ou  $G = \mathbb{C}$ ). On considère la fonction  $g : \mathbb{N}^* \rightarrow G$  définie par

$$\forall n > 0 \quad g(n) = \sum_{d|n} f(d).$$

Montrer qu'alors

$$\forall n > 0 \quad f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

**Exercice 8 (équivalent de  $I_q(n)$  pour  $q$  fixé).** On désigne comme dans l'exercice 6 par  $I_q(n)$  le nombre de polynômes irréductibles sur  $\mathbb{F}_q$ .

1. Montrer la formule

$$n I_n(q) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

2. On pose

$$r_n = \sum_{\substack{d|n \\ d < n}} \mu\left(\frac{n}{d}\right) q^d.$$

Montrer que  $r_n = o(q^n)$  et en déduire l'équivalent :  $I_n(q) \sim_{n \rightarrow \infty} \frac{q^n}{n}$ .