Leonid Monin
Léo Navarro Chafloque

EPFL, semestre de printemps 2026
Rings and fields

Exercice – Semaine 11

Exercice 1.
Soit $\alpha \in \mathbb{F}_{27}^\times$ un élément différent de 1 et -1. Montrer que soit α, soit $-\alpha$, est un générateur du groupe cyclique $\mathbb{F}_{27}^\times$.

Exercice 2.
Fixons un nombre premier p.

1. Pour $r > 0$, énumérez les sous-corps de $\mathbb{F}_{p^r}$. Si s divise r, énumérez les corps intermédiaires $\mathbb{F}_{p^s} \subseteq L \subseteq \mathbb{F}_{p^r}$.

2. Montrez que l'ensemble $\{0 \neq a \in \mathbb{F}_{16} \mid \mathbb{F}_2(a) = \mathbb{F}_{16} \text{ et } \langle a \rangle \neq \mathbb{F}_{16}^\times\}$ possède 4 éléments. Ici $\langle a \rangle$ désigne le sous-groupe de $\mathbb{F}_{16}^\times$ généré par l'élément $a \neq 0$.
Indication : Etudiez la structure du groupe $\mathbb{F}_{16}^\times$.

3. Plus généralement, montrez que l'ensemble $\{0 \neq a \in \mathbb{F}_{p^4} \mid \mathbb{F}_p(a) = \mathbb{F}_{p^4} \text{ et } \langle a \rangle \neq \mathbb{F}_{p^4}^\times\}$ possède $p^4 - p^2 - \varphi(p^4 - 1)$ éléments, où φ est la fonction de comptage d'Euler.

Exercice 3 (Corps de décomposition sur $\mathbb{F}_p$)**.**
Fixons un nombre premier $p > 0$ et un polynôme $f(x) \in \mathbb{F}_p[x]$ irréductible de degré d.

1. Montrez que f divise $x^{p^d} - x$ dans $\mathbb{F}_p[x]$.
Indication : A l'aide du Théorème fondamental des corps finis, montrez que $\mathbb{F}_{p^d}$ *contient une racine de* f.

2. Montrez que $f(x)$ se scinde sur $\mathbb{F}_{p^d}$.

3. Montrez que f n'a pas de racines multiples.

4. Soit $g \in \mathbb{F}_p[x]$ un polynôme irréductible de degré d qui n'est pas associé à f. Montrez que f et g n'ont pas de racines en commun.

5. Montrez que
$$x^{p^d} - x = \prod_{\substack{h \text{ unitaire irréd.} \\ \text{dans } \mathbb{F}_p[x] \\ \deg h \text{ divise } d}} h.$$

Exercice 4.
Soit $f(t) \in \mathbb{F}_p[t]$ un polynôme de degré n. Montrez que $f(t)$ est irréductible si et seulement si $f(t)$ n'a pas de racines dans $\mathbb{F}_{p^k}$ pour tout $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$.

Une application de ce principe permet de montrer que $t^4 + 2 \in \mathbb{F}_5[t]$ est irréductible (qui avait été vu dans une série précédente). En effet, montrez qu'une racine α de ce polynôme a pour ordre multiplicatif* 16, mais que cela n'est pas possible pour des éléments de $\mathbb{F}_{25}$.

Exercice 5 (Polynômes irréductibles sur $\mathbb{F}_p$)**.**
Fixons un nombre premier $p > 0$. Nous allons calculer le nombre N_d de polynômes irréductibles unitaires d'un degré fixé sur $\mathbb{F}_p$. (Rappelons qu'un polynôme est unitaire si son coefficient dominant vaut 1).

*Plus petit entier n tel que $\alpha^n = 1$.

1. Montrez que
$$d \cdot N_d = \left| \mathbb{F}_{p^d} \setminus \bigcup_{L \subsetneq \mathbb{F}_{p^d}} L \right|$$
où L parcourt l'ensemble des sous-corps strictement inclus dans $\mathbb{F}_{p^d}$.
Indication : Utilisez les résultats des exercices précédents et le Théorème fondamental des corps finis.

2. Montrez que
$$N_2 = \frac{p^2 - p}{2}, \quad N_3 = \frac{p^3 - p}{3}, \quad N_4 = \frac{p^4 - p^2}{4}, \quad N_5 = \frac{p^5 - p}{5}, \quad N_6 = \frac{p^6 - p^3 - p^2 + p}{6}.$$

Pour établir une formule générale, il sera utile d'introduire la **fonction de Möbius**. Il s'agit de la fonction
$$\mu \colon \mathbb{N}_{>0} \longrightarrow \{-1, 0, 1\}$$
définie par
$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par } p^2 \text{ pour un premier } p, \\ 1 & \text{si } n = 1 \text{ ou si } n \text{ est le produit d'un nombre pair de premiers distincts,} \\ -1 & \text{si } n \text{ est le produit d'un nombre impair de premiers distincts.} \end{cases}$$

Ceci étant, passons au cas général :

3. Si n, m divisent d et sont premiers entre eux, montrez que $\mathbb{F}_{p^{d/n}} \cap \mathbb{F}_{p^{d/m}} = \mathbb{F}_{p^{d/nm}}$ dans $\mathbb{F}_{p^d}$.

4. Montrez que
$$N_d = \frac{1}{d} \sum_{r \mid d} \mu\left(\frac{d}{r}\right) p^r.$$
Indication : Soit $d = s_1^{i_1} \cdots s_n^{i_n}$ la décomposition en produit de nombres premiers. Montrez d'abord que
$$dN_d = \left| \mathbb{F}_{p^d} \setminus \bigcup_{j=1}^{n} \mathbb{F}_{p^{d/s_j}} \right|$$
puis développez le terme de droite grâce à la formule d'inclusion-exclusion.