École polytechnique 2022-2023
Théorie de Galois

Feuille d'exercices 5

Exercice 1. Soient p un nombre premier, $f \in \mathbb{F}_p[X]$ un polynôme irréductible de degré d et k un corps fini de cardinal $q = p^d$. Montrer que f est *scindé* sur k.

Exercice 2. Soit p un nombre premier. Montrer que pour tout entier $d \geq 1$, il existe un polynôme irréductible de degré d dans $\mathbb{F}_p[X]$. (*Indication : on pourra utiliser le fait que le groupe multiplicatif d'un corps fini est cyclique.*)

Exercice 3. Soient p un nombre premier impair et Ω une clôture algébrique de $\mathbb{F}_p$.

1. Rappeler pourquoi $\mathbb{F}_p = \{x \in \Omega, x^p = x\}$.
2. Montrer qu'il existe $\zeta \in \Omega$ tel que $\zeta^2 = -1$. En déduire que -1 est un carré dans $\mathbb{F}_p$ si et seulement si
$$p \equiv 1 \bmod 4.$$
3. Montrer qu'il existe $\zeta \in \Omega$ tel que $\zeta^4 = -1$. En considérant l'élément $\zeta + \zeta^{-1}$, montrer que 2 est un carré dans $\mathbb{F}_p$ si et seulement si
$$p \equiv \pm 1 \bmod 8.$$

Exercice 4. Soient p un nombre premier et $P \in \mathbb{F}_p[X]$ un polynôme de degré d.

1. Montrer que P est irréductible dans $\mathbb{F}_p[X]$ si et seulement si P n'a pas de racine dans $\mathbb{F}_{p^r}$ pour tout $r \leq \frac{d}{2}$.
2. Montrer que $\mathbb{F}_4 = \{0, 1, j, j^2\}$ avec $j^2 = 1 + j$.
3. En déduire que les polynômes
$$1 + X^2 + X^5 \ , \ 1 + X^3 + X^5 \ , \ 1 + X + X^2 + X^3 + X^5 \ , \ 1 + X + X^2 + X^4 + X^5,$$
$$1 + X + X^3 + X^4 + X^5 \ , \ 1 + X^2 + X^3 + X^4 + X^5$$
sont les polynômes irréductibles de degré 5 de $\mathbb{F}_2[X]$.

Exercice 5. Soient p un nombre premier, Ω une clôture algébrique de $\mathbb{F}_p$ et $x \in \Omega$.

1. Montrer que le degré de l'extension $[\mathbb{F}_p[x] : \mathbb{F}_p]$ est le plus petit entier $d \geq 1$ tel que $\mathrm{Frob}_p^d(x) = x$.
2. On suppose $x \neq 0$ et on désigne par N l'ordre de x dans $\Omega^\times$. Montrer que N est premier à p, puis que $[\mathbb{F}_p[x] : \mathbb{F}_p]$ est l'ordre de p dans $(\mathbb{Z}/N\mathbb{Z})^\times$.
3. Montrer que les $\mathbb{F}_p$-conjugués de x dans Ω sont exactement les $\mathrm{Frob}_p^n(x)$ avec $0 \leq n < d$.

4. En déduire que pour tout $a \in \mathbb{F}_p^\times$, le polynôme (d'Artin-Schreier) $X^p - X - a$ est irréductible dans $\mathbb{F}_p[X]$.

Exercice 6. Soit p un nombre premier.

1. Rappeler pourquoi
$$\Phi_p(X) = X^{p-1} + \cdots + X + 1$$
est irréductible dans $\mathbb{Q}[X]$.

   La suite de cet exercice est consacrée à l'étude de la réduction $\Phi_{p,l}$ de Φ_p modulo un nombre premier $l \neq p$.

2. Montrer que $\Phi_{p,l} \in \mathbb{F}_l[X]$ se factorise en $P_1 \cdots P_g$, où tous les P_i sont des irréductibles unitaires distincts de même degré, égal à l'ordre de l dans $\mathbb{F}_p^\times$.

3. En déduire que $\Phi_{p,l}$ est irréductible sur $\mathbb{F}_l$ si et seulement si l engendre $\mathbb{F}_p^\times$.

4. Montrer que $\Phi_{p,l}$ admet une racine dans $\mathbb{F}_l$ si et seulement si $l \equiv 1 \bmod p$.

5. Déduire du (iv) qu'il existe une infinité de nombres premiers l tels que $l \equiv 1 \bmod p$. (*Indication : on pourra s'inspirer de la preuve d'Euclide de l'infinité des nombres premiers.*)

Exercice 7.

1. Trouver le plus petit nombre premier p tel que $\sum_{i=0}^{22} T^i$ soit irréductible dans $\mathbb{F}_p[T]$.

2. Trouver les dix plus petits nombres premiers p tels que $\sum_{i=0}^{p-1} T^i$ soit irréductible dans $\mathbb{F}_2[T]$.

Exercice 8. Soit p un nombre premier fixé. Quelle est la probabilité qu'un polynôme unitaire $f \in \mathbb{F}_p[T]$ de degré d soit un produit de polynômes irréductibles de degrés 1 ou 2 ? Évaluer ces nombres (rationnels) pour $p = 2$ et $d \leq 7$.