ÉNS de Lyon
M2 FEADéP

Cours d'algèbre
2020–2021

TD Extensions de corps, corps finis

Exercice 1 —

1. Soit p un nombre premier. Déterminer le degré de l'extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$.
2. Calculer le degré de l'extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ et déterminer le polynôme minimal de $\alpha = \sqrt{2}+\sqrt{3}$ sur $\mathbb{Q}$.

Exercice 2 — Montrer que les corps de rupture de X^3-2 dans $\mathbb{C}$, à savoir $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, sont deux à deux distincts.
Indication : On pourra établir que $j^2\sqrt[3]{2} \notin \mathbb{Q}(j\sqrt[3]{2})$.

Exercice 3 —

1. Soit L/K une extension de corps. Soient $x, y \in L$ de degrés respectifs m, n sur K. On suppose que m et n sont premiers entre eux. Montrer que $[K(x,y):K] = mn$.
2. Soit L/K une extension de corps de degré m. Soit $P \in K[X]$ un polynôme irréductible de degré n. Montrer que si m et n sont premiers entre eux, alors P est irréductible dans $L[X]$.
3. Montrer que si les extensions M/L et L/K sont algébriques, alors M/K est algébrique.

Exercice 4 — Construction de $\mathbb{F}_4$ —

1. Donner une construction de $\mathbb{F}_4$ et dresser les tables d'addition et de multiplication dans $\mathbb{F}_4$.
2. Déterminer un polynôme irréductible de degré 2 dans $\mathbb{F}_4[X]$.

Exercice 5 — Le polynôme $X^2+X+1 \in \mathbb{F}_2[X]$ admet-il une racine dans $\mathbb{F}_8$?

Exercice 6 — Exhiber un isomorphisme de corps

$$\mathbb{F}_2[X]/(X^3+X+1) \cong \mathbb{F}_2[Y]/(Y^3+Y^2+1).$$

Exercice 7 — Critère d'irréductibilité —
Soit K un corps, et $P \in K[X]$ de degré $d \geq 2$.

1. Montrer que P est irréductible sur K si et seulement si, pour toute extension L/K de degré $\leq d/2$, le polynôme P n'a pas de racine dans L.
2. Utiliser ce critère pour montrer que $P = X^5+X^2+1$ est irréductible dans $\mathbb{F}_2[X]$.

Exercice 8 — Réductibilité de Φ_8 sur les corps finis —

1. Calculer $\Phi_8 \in \mathbb{Z}[X]$ et donner sa décomposition en irréductibles dans $\mathbb{F}_2[X]$.
2. Soit $p \geq 3$ premier.
   (a) Montrer que Φ_8 est réductible dans $\mathbb{F}_p[X]$ si et seulement si Φ_8 admet une racine dans $\mathbb{F}_{p^2}$.
   (b) Montrer que Φ_8 admet une racine dans $\mathbb{F}_{p^2}$ si et seulement si 8 divise $p^2 - 1$.
   (c) En déduire que Φ_8 est réductible dans $\mathbb{F}_p[X]$.

Exercice 9 — Factorisation des polynômes sur $\mathbb{F}_p$: algorithme de Berlekamp —

Soit p un nombre premier. Soit $P \in \mathbb{F}_p[X]$ unitaire et sans facteur carré. On note A la $\mathbb{F}_p$-algèbre $\mathbb{F}_p[X]/(P)$.

1. Montrer que $\varphi\colon A \to A$, $x \mapsto x^p$ est un automorphisme de $\mathbb{F}_p$-algèbre.
2. Montrer que $r = \dim_{\mathbb{F}_p} \ker(\varphi - \mathrm{Id})$ est le nombre de facteurs irréductibles de P.
3. On suppose $r \geq 2$. Montrer qu'il existe $Q \in \ker(\varphi - \mathrm{Id})$ tel que $Q \notin \mathbb{F}_p$.
4. Montrer que $P = \prod_{a \in \mathbb{F}_p} \mathrm{pgcd}(P, Q - a)$.
5. Montrer que cette décomposition est non triviale.
6. En déduire un algorithme de factorisation dans $\mathbb{F}_p[X]$.

Exercice 10 — Automorphisme de Frobenius —

Soit $K = \mathbb{F}_q$ un corps fini à $q = p^n$ éléments. On note $F\colon K \to K$ le morphisme de Frobenius, défini par $F(x) = x^p$.

1. Montrer que F est un automorphisme de K, d'ordre n dans le groupe $\mathrm{Aut}(K)$.

Soit maintenant $P \in \mathbb{F}_q[X]$ un polynôme irréductible de degré d, et L un corps de décomposition de P.

2. Montrer que $F_q\colon x \mapsto x^q$ est un $\mathbb{F}_q$-automorphisme de L.
3. Montrer que si $\alpha \in L$ est racine de P, alors $F_q(\alpha)$ est racine de P.
4. Montrer que les $F_q^i(\alpha)$ pour $0 \leq i \leq d-1$ sont deux à deux distincts.
   Indication : On pourra observer que pour $1 \leq e \leq d$, l'ensemble des racines de $X^{q^e} - X$ dans L forme un sous-corps de L.