# TD n°9 : Corps de rupture, corps de décomposition et corps finis

Dans toute la feuille, $p$ est un nombre premier et $q = p^n$. On notera $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ un corps à $p$ éléments.

**Exercice 1.** Calculer les corps de rupture et les corps de décomposition des polynômes suivants sur $\mathbf{Q}$, et donner leurs degrés :

1. $X^2 + 7$
2. $X^3 - 2$
3. $X^3 - 11$
4. $X^4 + 1$
5. $X^4 - 1$
6. $X^4 + 2$
7. $X^4 - 2$
8. $X^4 + X^2 + 1$
9. $X^4 - 5X^2 + 6$
10. $X^p - 1$, où $p$ est un nombre premier

**Exercice 2.** [Vrai ou faux]

Dire si les assertions suivantes sont vraies ou fausses, et justifier la réponse par un contre-exemple ou une démonstration.

1. Deux corps de rupture d'un polynôme irréductible sont isomorphes.
2. Deux corps de rupture d'un polynôme irréductible sont isomorphes à un unique isomorphisme de corps près.
3. Deux corps de décomposition d'un polynôme sont isomorphes.
4. Deux corps de décomposition d'un polynôme sont isomorphes à un unique isomorphisme près.
5. Le corps de rupture d'un polynôme irréductible est isomorphe à son corps de décomposition.
6. Il existe une fonction $f$ telle que le degré de l'extension du corps de décomposition de tout polynôme $P$ soit majoré par $f(deg(P))$.

**Exercice 3.** [Corps à huit, neuf et seize éléments]

On se propose dans cet exercice de construire tous les corps à 8, 9 et 16 éléments qui peuvent être obtenus comme corps de rupture de polynômes irréductibles sur $\mathbb{F}_2$ et $\mathbb{F}_3$.

1. Donner tous les polynômes irréductibles de degré inférieur à 4 sur $\mathbb{F}_2$ et inférieurs à 3 sur $\mathbb{F}_3$.
2. Utiliser un polynôme irréductible de degré 3 pour construire une extension $\mathbb{F}_8/\mathbb{F}_2$ de degré 3, et en donner la table de multiplication.
3. Montrer que les extensions obtenues pour les différents polynômes irréductibles choisis sont isomorphes, en exhibant un isomorphisme explicite.
4. Montrer que $\mathbb{F}_8^\times$ est cyclique en en exhibant un générateur.
5. Dans chacun des corps $\mathbb{F}_8$ précédemment obtenus, dire si l'élément primitif canonique est un générateur du groupe multiplicatif $K^\star$.
6. Choisir un corps $\mathbb{F}_8$ parmi les précédents, et donner le polynôme minimal de tous ses éléments sur $\mathbb{F}_2$.

7. Adapter et reprendre ces cinq dernières questions pour une extension $\mathbb{F}_9/\mathbb{F}_3$ de degré 2, et une extension $\mathbb{F}_{16}/\mathbb{F}_2$ de degré 4.

**Exercice 4.** [Sous-corps d'un corps fini]

1. Soit $K$ un sous-corps de $\mathbb{F}_q$. Montrer qu'il existe $d$ divisant $n$ tel que $K \sim \mathbb{F}_{p^d}$.
2. Réciproquement, étant donné $d$ un diviseur de $n$ montrer qu'il existe un unique sous-corps de $F_q$ isomorphe à $\mathbb{F}_{p^d}$.
3. Dessiner un diagramme montrant les inclusions possibles entre $F_2$, $F_4$, $F_8$, $F_{16}$, $F_{32}$, $F_{64}$, $F_{128}$ et $F_{256}$.

**Exercice 5.** [Polynômes irréductibles sur $\mathbb{F}_p$]

1. Montrer que $X^q - X$ est scindé à racines simples dans $\mathbb{F}_q$.
2. Soit $P$ un facteur irréductible de $X^q - X$. Montrer que le degré de $P$ divise $n$.
3. Réciproquement, soit $P$ un polynôme unitaire irréductible dans $\mathbb{F}_p[X]$ dont le degré divise $n$. Montrer que $P$ est un facteur simple de $X^q - X$.
4. Pour tout $d \in \mathbf{N}$ on note $\mathcal{I}(p,d)$ l'ensemble des polynômes unitaires irréductibles dans $\mathbf{F}_p[X]$ de degré $d$. Montrer que dans $\mathbf{F}_p[X]$ on a
$$X^q - X = \prod_{d|n} \prod_{P \in \mathcal{I}(p,d)} P$$
5. On note $I(p,d)$ le cardinal de $\mathcal{I}(p,d)$. Montrer que $p^n = \sum_{d|n} dI(p,d)$. En déduire que l'ensemble $\mathcal{I}(p,d)$ est non vide.
6. Montrer que $\frac{p^n - p^{\lfloor n/2 \rfloor + 1}}{n} \leq I(p,n) \leq \frac{p^n}{n}$ En déduire qu'un polynôme unitaire de degré $n$ "assez grand" choisi au hasard a au moins une chance sur $n$ d'être irréductible.

**Exercice 6.** [De l'algèbre linéaire sur les corps finis]

1. Soit $K$ un corps commutatif. Montrer que tout sous-groupe fini de $K^*$ est cyclique.
2. Montrer que $GL_m(\mathbb{F}_q)$ contient un élément d'ordre $p^{nm} - 1$.