

TD 4 : Extensions de corps, corps finis, théorie de Galois

Exercice 1. Quels sont les idéaux d'un corps ? Montrer qu'un morphisme d'anneaux entre deux corps est toujours injectif.

Exercice 2. Les réels e et π sont transcendants. Que peut-on en déduire de l'extension $\mathbb{Q} \subset \mathbb{R}$?

Exercice 3. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de degré impair. Démontrer que si $a \in \mathbb{K}$ est un carré dans \mathbb{L} , alors c'est un carré dans \mathbb{K} .

Exercice 4. Calculer les corps de rupture et de décomposition des polynômes suivants, et donner les degrés des extensions correspondantes :

- | | | |
|----------------------|---------------------------|--|
| a) $P_1 = X^2 + 7.$ | e) $P_5 = X^4 - 1.$ | i) $P_9 = X^4 - 5X^2 + 6.$ |
| b) $P_2 = X^3 - 2.$ | f) $P_6 = X^4 + 2.$ | j) $P_{10} = X^p - 1$ (où p
est premier). |
| c) $P_3 = X^3 - 11.$ | g) $P_7 = X^4 - 2.$ | |
| d) $P_4 = X^4 + 1.$ | h) $P_8 = X^4 + X^2 + 1.$ | |

Exercice 5. Les assertions suivantes sont-elles vraies ou fausses ? Justifier la réponse par une démonstration ou un contre-exemple.

- a) Deux corps de rupture d'un polynôme sont isomorphes.
- b) Deux corps de rupture d'un polynôme irréductible sont isomorphes à unique isomorphisme près.
- c) Deux corps de décomposition d'un polynôme sont isomorphes.
- d) Deux corps de décomposition d'un polynôme sont isomorphes à unique isomorphisme près.
- e) Le corps de rupture d'un polynôme irréductible est isomorphe à son corps de décomposition.
- f) Il existe une fonction $f: \mathbb{N} \rightarrow \mathbb{N}$ telle que pour tout corps \mathbb{K} , pour tout polynôme $P \in \mathbb{K}[X]$, le degré du corps de décomposition de P sur \mathbb{K} est majoré par $\deg(f(P))$.

Exercice 6. Soit \mathbb{K} un corps et $P \in \mathbb{K}[X]$. À quel condition l'anneau quotient $\mathbb{K}[X]/(P)$ est-il un corps ? Dans ce cas, quel est le degré de l'extension $\mathbb{K} \subset \mathbb{K}[X]/(P)$?

Exercice 7. Existe-t-il un corps à 8 éléments ? 9 éléments ? 12 éléments ?

Exercice 8. Soit q, q' deux puissances de nombres premiers. À quelle condition le corps $\mathbb{F}_{q'}$ est-il une extension de \mathbb{F}_q ?

Exercice 9. Déterminer les degrés des extensions suivantes :

- a) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}).$
- b) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{5}).$
- c) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{5}).$
- d) $\mathbb{Q} \subset \mathbb{Q}(i + \sqrt{5}).$

Exercice 10. Quels sont les sous-corps de \mathbb{F}_{64} ? Combien existe-t-il de générateurs de l'extension $\mathbb{F}_2 \subset \mathbb{F}_{64}$, c'est-à-dire d'éléments $x \in \mathbb{F}_{64}$ tels que $\mathbb{F}_{64} = \mathbb{F}_2(x)$? Combien le groupe \mathbb{F}_{64}^\times a-t-il de générateurs ? Est-ce qu'il y a un lien entre ces deux notions ?

Exercice 11. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie de corps.

- Si $[\mathbb{L} : \mathbb{K}]$ est un nombre premier, démontrer que l'extension est monogène.
- Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Démontrer que si $\deg(P)$ et $[\mathbb{L} : \mathbb{K}]$ sont premiers entre eux, alors P est irréductible sur \mathbb{L} .
- Soit $\alpha \in \mathbb{K}$ un élément algébrique de degré impair. Démontrer que $\mathbb{K}(\alpha) = \mathbb{K}(\alpha^2)$.

Exercice 12. Corps à huit, neuf et seize éléments.

- Dresser une liste de tous les polynômes irréductibles de degré ≤ 4 sur les corps \mathbb{F}_2 et \mathbb{F}_3 .
- Parmi les polynômes précédents, lesquels ont pour corps de rupture \mathbb{F}_9 et \mathbb{F}_8 ? Écrire la table de multiplication du corps correspondant dans ces cas.
- Donner des isomorphismes explicites entre les corps ainsi obtenus.
- Dans chacun des cas, est-ce que l'élément primitif canonique (la classe de X dans le quotient $\mathbb{K}[X]/(P)$) est-il un générateur de \mathbb{K}^\times ?
- Démontrer que \mathbb{F}_8^\times est cyclique.
- Démontrer que tous les éléments de \mathbb{F}_8 sont algébriques sur \mathbb{F}_2 et donner leurs polynômes minimaux.
- Reprendre les trois dernières questions en remplaçant \mathbb{F}_8 par \mathbb{F}_{16} .

Exercice 13. Démontrer que les extensions suivantes sont galoisiennes, déterminer leur degré et leur groupe de Galois :

- $\mathbb{R} \subset \mathbb{C}$.
- $\mathbb{F}_q \subset \mathbb{F}_{q^n}$.
- $\mathbb{Q} \subset \mathbb{Q}(\exp(2i\pi/n))$ (où $n \geq 2$).

Exercice 14. On considère l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Quel est son degré ? Démontrer que c'est une extension galoisienne. Déterminer ses sous-corps. Déterminer un élément primitif.

Exercice 15. On note $\alpha = \sqrt[4]{2}$ et $\beta = \sqrt[5]{2}$ et on pose $\mathbb{K} = \mathbb{Q}(\alpha) \subset \mathbb{L} = \mathbb{Q}(\alpha, \beta)$.

- Déterminer les polynômes minimaux P et Q de α et β sur \mathbb{Q} . Quelles sont les racines (complexes) de ces polynômes ?
- On note $\mathbb{L}' \subset \mathbb{C}$ le sous-corps engendré par les racines de P et Q . Combien y-a-t-il de morphismes $\mathbb{L} \rightarrow \mathbb{L}'$? Décrire les.
- Déterminer le polynôme minimal de β sur $\mathbb{Q}(\alpha)$.
- Que vaut $[\mathbb{L} : \mathbb{Q}]$?
- Déterminer $\text{Gal}(\mathbb{K}/\mathbb{Q})$ et $\text{Gal}(\mathbb{L}/\mathbb{Q})$.
- Les extensions $\mathbb{Q} \subset \mathbb{K}$ et $\mathbb{Q} \subset \mathbb{L}$ sont-elles galoisiennes ?