

Corps et extensions

Exercice 1 : Caractéristique et morphisme de Frobenius

Soit K un corps de caractéristique $p > 0$.

1. Rappeler pourquoi p est un nombre premier.
2. Montrer que p divise $\binom{p}{k}$ pour $1 \leq k \leq p-1$. En déduire que $F : x \rightarrow x^p$ est un morphisme de corps de K dans K .
3. Montrer que F est injectif, puis qu'il est bijectif lorsque K est fini.
4. En calculant $(1 + 1 + \dots + 1)^p$ dans $\mathbb{F}_p$, retrouver le petit théorème de Fermat : $a^p \equiv a \pmod{p}$ pour tout entier a .
5. Montrer que, pour tous $x, y \in K$ et tout $n \geq 0$, $(x - y)^{p^n} = x^{p^n} - y^{p^n}$.

Exercice 2 : Sous-corps premier et morphismes de corps

1. Montrer qu'un morphisme de corps $\sigma : K \rightarrow L$ est injectif, et que K et L ont alors la même caractéristique.
2. En déduire qu'il n'existe aucun morphisme de corps de $\mathbb{Q}$ dans $\mathbb{F}_5$, ni de $\mathbb{F}_3$ dans $\mathbb{F}_5$.
3. Déterminer le sous-corps premier de chacun des corps suivants : $\mathbb{Q}(\sqrt{2})$, $\mathbb{R}$, $\mathbb{F}_3[X]/(X^2 + 1)$, $\mathbb{F}_7(T)$.
4. Montrer que le seul morphisme de corps de $\mathbb{Q}$ dans un corps L de caractéristique nulle est

l'injection canonique.

Exercice 3 : Degré d'une extension biquadratique

1. Montrer que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.
2. En déduire $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ et une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbb{Q}$.
3. Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{6})$.
4. Le polynôme $X^2 - 3$ est-il irréductible sur $\mathbb{Q}(\sqrt{2})$? Et $X^2 - 18$?

Exercice 4 : Calculs dans un corps de rupture de $X^3 - 2$

On pose $K = \mathbb{Q}[X]/(X^3 - 2)$ et $\alpha = \overline{X}$.

1. Justifier que K est un corps de degré 3 sur $\mathbb{Q}$, dont $(1, \alpha, \alpha^2)$ est une base.
2. Calculer l'inverse de $1 + \alpha$ dans cette base.
3. Calculer l'inverse de $\alpha^2 + \alpha$.
4. Déterminer le polynôme minimal de α^2 , puis celui de $1 + \alpha$, sur $\mathbb{Q}$.

Exercice 5 : Polynôme minimal de $\sqrt{2} + \sqrt{3}$

On pose $\gamma = \sqrt{2} + \sqrt{3}$.

1. Trouver un polynôme unitaire P de degré 4 à coefficients entiers tel que $P(\gamma) = 0$.

2. Calculer γ^3 et en déduire que $\sqrt{2}$ et $\sqrt{3}$ appartiennent à $\mathbb{Q}(\gamma)$.
3. En déduire que $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et que P est le polynôme minimal de γ . Quelles sont ses racines ?
4. Soit p un nombre premier impair. Vérifier les identités

$$P = (X^2 - 1)^2 - 8X^2 = (X^2 + 1)^2 - 12X^2 = (X^2 - 5)^2 - 24$$
. En utilisant le fait que $\mathbb{F}_p^*$ est cyclique, montrer que l'un des éléments $2, 3, 6$ est un carré dans $\mathbb{F}_p$, puis que P est réductible dans $\mathbb{F}_p[X]$. Que se passe-t-il pour $p = 2$?

Exercice 6 : Polynôme minimal de $2\cos(2\pi/7)$

On pose $\zeta = e^{2i\pi/7}$ et $\theta = \zeta + \zeta^{-1} = 2\cos\frac{2\pi}{7}$.

1. Justifier que $1 + \zeta + \zeta^2 + \dots + \zeta^6 = 0$.
2. Exprimer $\zeta^2 + \zeta^{-2}$ et $\zeta^3 + \zeta^{-3}$ en fonction de θ . En déduire que

$$\theta^3 + \theta^2 - 2\theta - 1 = 0$$
.
3. Montrer que $X^3 + X^2 - 2X - 1$ est le polynôme minimal de θ sur $\mathbb{Q}$.
4. Montrer que ses deux autres racines sont $2\cos\frac{4\pi}{7}$ et $2\cos\frac{6\pi}{7}$, et les exprimer comme polynômes en θ . Que peut-on dire du corps $\mathbb{Q}(\theta)$?

Exercice 7 : Corps de décomposition de $X^3 - 2$

On note $j = e^{2i\pi/3}$ et $\alpha = \sqrt[3]{2}$, racine cubique réelle de 2 .

1. Montrer que $X^3 - 2$ est irréductible sur $\mathbb{Q}$ et donner ses racines complexes.
2. Montrer que $L = \mathbb{Q}(\alpha, j)$ est le corps de décomposition de $X^3 - 2$ dans $\mathbb{C}$, et calculer $[L : \mathbb{Q}]$.

3. Montrer que $\mathbb{Q}(a)$, $\mathbb{Q}(ja)$ et $\mathbb{Q}(j^2 a)$ sont trois sous-corps de L deux à deux distincts mais isomorphes.
4. Montrer que $X^3 - 2$ est irréductible sur $\mathbb{Q}(j)$.

Exercice 8 : Corps de décomposition de $X^4 - 2$

On note $\alpha = \sqrt[4]{2}$, racine quatrième réelle positive de 2.

1. Montrer que $X^4 - 2$ est irréductible sur $\mathbb{Q}$ et donner ses racines complexes.
2. Montrer que le corps de décomposition de $X^4 - 2$ dans $\mathbb{C}$ est $L = \mathbb{Q}(\alpha, i)$, et que $[L : \mathbb{Q}] = 8$.
3. Montrer que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha)$ et calculer $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})]$. Donner le polynôme minimal de α sur $\mathbb{Q}(\sqrt{2})$.
4. Montrer que $X^4 - 2$ reste irréductible sur $\mathbb{Q}(i)$.
5. Montrer que $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(i\alpha)$ sont isomorphes et distincts. Montrer enfin que $\mathbb{Q}(i\sqrt{2})$ est un sous-corps de L de degré 2 sur $\mathbb{Q}$, distinct de $\mathbb{Q}(i)$ et de $\mathbb{Q}(\sqrt{2})$.

Exercice 9 : Extensions de degré 2

Soit K un corps de caractéristique différente de 2 et L une extension de K de degré 2.

1. Montrer que $L = K(\alpha)$ pour tout $\alpha \in L \setminus K$.
2. Montrer qu'il existe $\delta \in L$ tel que $L = K(\delta)$ et $\delta^2 \in K$.
3. En déduire que toute extension de degré 2 de $\mathbb{Q}$ contenue dans $\mathbb{C}$ est de la forme $\mathbb{Q}(\sqrt{d})$, où $d \neq 1$ est un entier sans facteur carré.

4. Montrer que 2 n'est pas un carré dans $\mathbb{Q}(\sqrt{3})$. En déduire que les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ ne sont pas isomorphes.

Exercice 10 : Nombres transcendants

1. Montrer que l'ensemble $\mathbb{Q}[X]$ est dénombrable. En déduire que l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est dénombrable, puis qu'il existe des nombres réels transcendants.
2. Soit $\alpha \in \mathbb{C}$ transcendant sur $\mathbb{Q}$. Montrer que $\mathbb{Q}[\alpha]$ est isomorphe à $\mathbb{Q}[X]$ et que $\mathbb{Q}[\alpha] \neq \mathbb{Q}(\alpha)$.
3. Montrer que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est infini.
4. Montrer que $\alpha^2 + 1$ est transcendant, et que tout $\beta \in \mathbb{C}$ tel que $\beta^2 = \alpha$ est transcendant.

Exercice 11 : Les nombres algébriques forment un corps

On note $\overline{\mathbb{Q}}$ l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$.

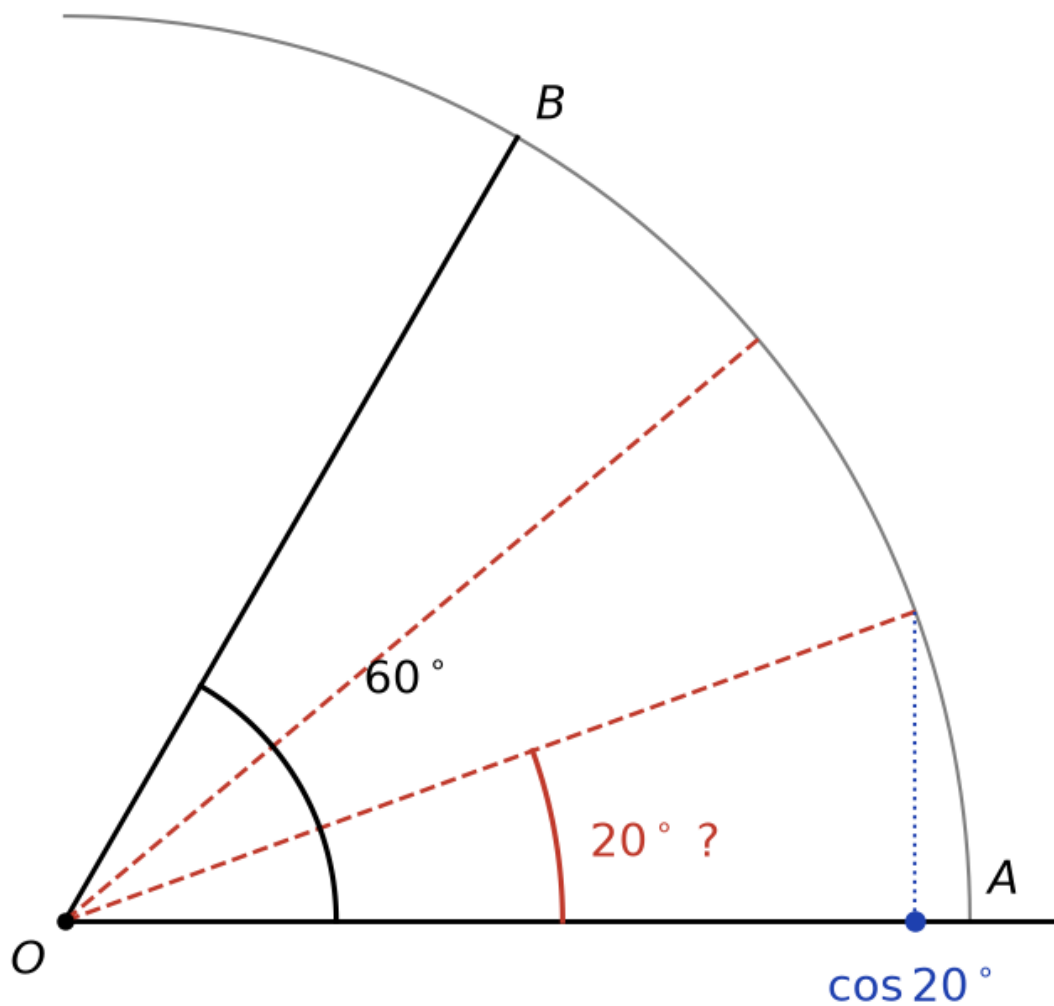
1. Soient $\alpha, \beta \in \overline{\mathbb{Q}}$, de degrés m et n . Montrer que $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leq mn$, puis que $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.
2. On pose $\gamma = \sqrt{2} + \sqrt[3]{3}$. Montrer que $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}] = 6$.
3. En développant $(\gamma - \sqrt{2})^3 = 3$, montrer que $\sqrt{2} \in \mathbb{Q}(\gamma)$. En déduire le degré de γ .
4. Trouver le polynôme minimal de γ sur $\mathbb{Q}$.
5. Soit $z \in \mathbb{C}$ racine d'un polynôme non nul à coefficients dans $\overline{\mathbb{Q}}$. Montrer que $z \in \overline{\mathbb{Q}}$.

Exercice 12 : Duplication du cube et racines non constructibles

1. Rappeler pourquoi le degré sur $\mathbb{Q}$ d'un réel constructible est une puissance de 2.
2. Montrer que $\sqrt[3]{2}$ n'est pas constructible. Interpréter géométriquement.
3. Montrer que $\sqrt[4]{2}$ est constructible et donner son degré sur $\mathbb{Q}$.
4. Montrer que $\sqrt[6]{2}$ et $1 + \sqrt[3]{2}$ ne sont pas constructibles.
5. Calculer $(1 + \sqrt{2})^3$. Le réel $\sqrt[3]{7 + 5\sqrt{2}}$ est-il constructible ?

Exercice 13 : Trisection de l'angle

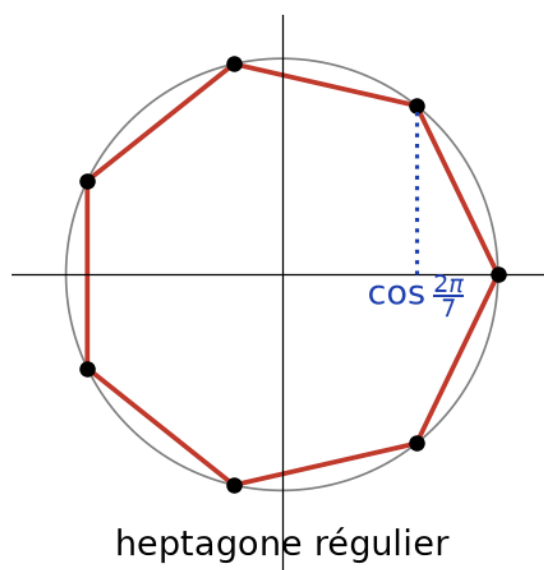
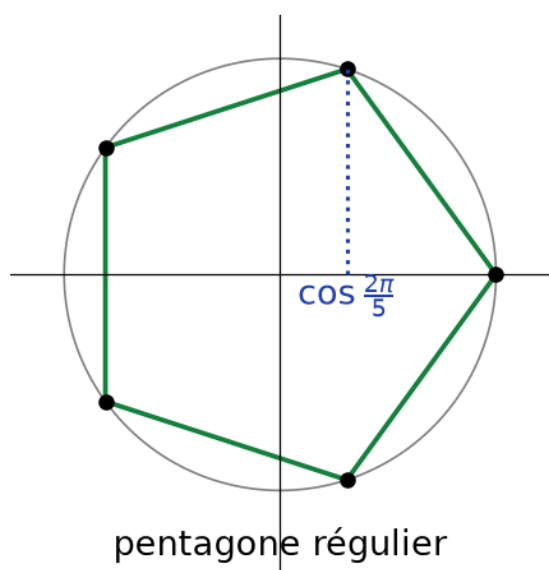
Un angle θ est dit constructible si $\cos\theta$ est un réel constructible. La figure ci-dessous montre l'angle $\widehat{AOB} = 60^\circ$, constructible, et les deux demi-droites qui le partageraient en trois angles de 20° .



1. Montrer que $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ pour tout réel θ .
2. En déduire que $x = 2\cos 20^\circ$ vérifie $x^3 - 3x - 1 = 0$.
3. Montrer que ce polynôme est irréductible sur $\mathbb{Q}$ et conclure qu'on ne peut pas trisecter l'angle de 60° à la règle et au compas.
4. Montrer en revanche que l'angle de 90° se trisecte.

Exercice 14 : Pentagone, heptagone et enneagone réguliers

Un polygone régulier à n côtés est constructible si et seulement si $\cos \frac{2\pi}{n}$ est constructible. La figure ci-dessous représente le pentagone et l'heptagone réguliers inscrits dans le cercle unité.



1. Soit $\omega = e^{2i\pi/5}$ et $t = \omega + \omega^{-1}$. Montrer que $t^2 + t - 1 = 0$, puis calculer $\cos \frac{2\pi}{5}$.
2. En déduire que le pentagone régulier est constructible.
3. En utilisant l'exercice 6, montrer que l'heptagone régulier n'est pas constructible.
4. Montrer que $2\cos 40^\circ$ est racine de $X^3 - 3X + 1$. En déduire que l'enneagone régulier (9 côtés) n'est pas constructible.

Exercice 15 : Construction de $\mathbb{F}_4$ et $\mathbb{F}_8$

1. Montrer que $X^2 + X + 1$ est l'unique polynôme irréductible de degré 2 sur $\mathbb{F}_2$.
2. On pose $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$ et $\alpha = \overline{X}$. Dresser les tables d'addition et de multiplication de $\mathbb{F}_4$.
3. Montrer que $X^3 + X + 1$ est irréductible sur $\mathbb{F}_2$. On pose $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$ et $\beta = \overline{X}$. Calculer β^k pour $0 \leq k \leq 7$ dans la base

$$(1, \beta, \beta^2).$$

4. En déduire l'inverse de $\beta^2 + 1$ et de $\beta^2 + \beta$.
5. Montrer sans calcul que $\mathbb{F}_8$ ne contient aucun sous-corps à 4 éléments.

Exercice 16 : Le corps $\mathbb{F}_9$ et ses générateurs

1. Montrer que $X^2 + 1$ est irréductible sur $\mathbb{F}_3$. On pose $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2 + 1)$ et $\alpha = \overline{X}$.
2. Déterminer l'ordre de α dans $\mathbb{F}_9^*$. Est-ce un générateur ?
3. Montrer que $1 + \alpha$ est un générateur de $\mathbb{F}_9^*$.
4. Combien $\mathbb{F}_9^*$ a-t-il de générateurs ? Les écrire sous la forme $a + b\alpha$.
5. Déterminer le polynôme minimal de $1 + \alpha$ sur $\mathbb{F}_3$, et en déduire une autre description de $\mathbb{F}_9$ comme quotient.

Exercice 17 : Générateurs et racines dans $\mathbb{F}_{13}$

1. Montrer que 2 engendre le groupe $\mathbb{F}_{13}^*$, en calculant le moins possible de puissances.
2. Dresser la liste des puissances de 2 modulo 13, puis donner tous les générateurs de $\mathbb{F}_{13}^*$.
3. Déterminer les carrés de $\mathbb{F}_{13}^*$. L'élément -1 est-il un carré ?
4. Résoudre dans $\mathbb{F}_{13}$ les équations $x^2 = 10$ et $x^3 = 5$.

Exercice 18 : Deux constructions de $\mathbb{F}_{16}$

1. Montrer que $P = X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.
2. On pose $\mathbb{F}_{16} = \mathbb{F}_2[X]/(P)$ et $\alpha = \overline{X}$. Montrer que α est un générateur de $\mathbb{F}_{16}^*$.
3. Montrer que $Q = X^4 + X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$, et que la classe β de X dans $\mathbb{F}_2[X]/(Q)$ n'engendre pas le groupe multiplicatif.
4. Déterminer, dans $\mathbb{F}_2[X]/(P)$, le sous-corps à 4 éléments. On l'exprimera dans la base $(1, \alpha, \alpha^2, \alpha^3)$.

Exercice 19 : Sous-corps de $\mathbb{F}_{4096}$

On note $K = \mathbb{F}_{4096} = \mathbb{F}_{2^{12}}$.

1. Donner la liste des sous-corps de K avec leurs cardinaux, et préciser les inclusions entre eux.
2. Montrer qu'un élément $x \in K$ vérifie $\mathbb{F}_2(x) = K$ si et seulement s'il n'appartient ni à $\mathbb{F}_{64}$ ni à $\mathbb{F}_{16}$.
3. Dénombrer les éléments x de K tels que $\mathbb{F}_2(x) = K$.
4. En déduire le nombre de polynômes unitaires irréductibles de degré 12 sur $\mathbb{F}_2$.

Exercice 20 : Dénombrement des polynômes irréductibles

Soit p un nombre premier. On note I_d le nombre de polynômes unitaires irréductibles de degré d sur $\mathbb{F}_p$.

1. Soit Q unitaire irréductible de degré d sur $\mathbb{F}_p$. Montrer que Q divise $X^{p^n} - X$ si et seulement si d divise n .
2. En déduire que $X^{p^n} - X$ est le produit des polynômes unitaires irréductibles de degré divisant n .

$$n, \text{ puis que } p^n = \sum_{d|n} d I_d.$$

3. Calculer $I_1, \dots, I_6$ pour $p = 2$, et I_2 pour $p = 3$ en donnant les polynômes.
4. Montrer que $I_n \geq 1$ pour tout $n \geq 1$. Qu'en déduit-on pour les corps finis ?

Exercice 21 : Carrés dans un corps fini

Soit q une puissance d'un nombre premier impair.

1. Montrer que $\mathbb{F}_q^*$ contient exactement $\frac{q-1}{2}$ carrés, et que $x \in \mathbb{F}_q^*$ est un carré si et seulement si $x^{(q-1)/2} = 1$.
2. Montrer que -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1 \pmod{4}$.
3. Montrer que tout élément de $\mathbb{F}_q$ est somme de deux carrés.
4. Application : -1 est-il un carré dans $\mathbb{F}_7$? Écrire 3 comme somme de deux carrés dans $\mathbb{F}_7$.

Exercice 22 : Isomorphisme explicite entre deux corps à 8 éléments

On pose $K_1 = \mathbb{F}_2[X]/(X^3 + X + 1)$, avec $\beta = \overline{X}$, et $K_2 = \mathbb{F}_2[Y]/(Y^3 + Y^2 + 1)$, avec $\gamma = \overline{Y}$.

1. Justifier que K_1 et K_2 sont deux corps à 8 éléments.
2. Montrer que β^{-1} est racine de $Y^3 + Y^2 + 1$, et l'exprimer dans la base $(1, \beta, \beta^2)$.
3. En déduire un isomorphisme explicite $\sigma : K_2 \rightarrow K_1$, en donnant l'image de γ et de γ^2 .
4. Combien existe-t-il d'isomorphismes de K_2 sur K_1 ?

Exercice 23 : Problème : cyclicité du groupe multiplicatif

Soit K un corps et G un sous-groupe fini de K^* , d'ordre n . Pour $d \mid n$, on note $N(d)$ le nombre d'éléments de G d'ordre d , et φ l'indicatrice d'Euler.

1. Montrer que $\sum_{d \mid n} \varphi(d) = n$. On pourra classer les éléments de $\mathbb{Z}/n\mathbb{Z}$ selon leur ordre.
2. Montrer que $N(d) \in \{0, \varphi(d)\}$ pour tout diviseur d de n .
3. En déduire que $N(d) = \varphi(d)$ pour tout $d \mid n$, puis que G est cyclique.
4. Montrer que 3 engendre $\mathbb{F}_{17}^*$ et donner le nombre de générateurs de $\mathbb{F}_{17}^*$ et de $\mathbb{F}_{25}^*$.
5. Soit g un générateur de $\mathbb{F}_{p^n}^*$. Montrer que $\mathbb{F}_{p^n} = \mathbb{F}_p(g)$. En déduire l'existence d'un polynôme irréductible de degré n sur $\mathbb{F}_p$ et que $\mathbb{F}_{p^n}$ est isomorphe à un quotient $\mathbb{F}_p[X]/(P)$.
6. Montrer en revanche que les groupes $\mathbb{Q}^*$ et $\mathbb{R}^*$ ne sont pas cycliques.

Exercice 24 : Problème : polynômes d'Artin-Schreier

Soit p un nombre premier, $a \in \mathbb{F}_p^*$ et $P = X^p - X - a \in \mathbb{F}_p[X]$.

1. Montrer que P n'a aucune racine dans $\mathbb{F}_p$.
2. Soit L un corps de décomposition de P et $\alpha \in L$ une racine de P . Montrer que les racines de P sont les $\alpha + k$, $k \in \mathbb{F}_p$, et que $P = \prod_{k \in \mathbb{F}_p} (X - \alpha - k)$.
3. Supposons $P = QR$ avec Q unitaire de degré d , $1 \leq d \leq p-1$. En étudiant le coefficient de X^{d-1} dans Q , aboutir à une contradiction. Conclure que P est irréductible.
4. En déduire que $L = \mathbb{F}_p(\alpha)$, que $|L| = p^p$, et que $\mathbb{F}_p[X]/(P)$ est un corps de

décomposition de P .

5. Montrer que le Frobenius F vérifie $F(\alpha) = \alpha + a$, et que F est un automorphisme d'ordre exactement P de L .
6. Expliciter les cas $p = 2$ et $p = 3$ avec $a = 1$.

Le corrigé des exercices

Chaque exercice est corrigé en détail, question par question, sur la page suivante.



Pour aller plus loin en L3

- Le cours : [corps et extensions, cours de maths en L3](#)
- À maîtriser avant : [Anneaux, idéaux et arithmétique](#)
- Chapitre précédent : [Anneaux, idéaux et arithmétique](#)
- Chapitre suivant : [Réduction de Jordan et décomposition de Dunford](#)
- Tester vos connaissances : [QCM de maths en L3 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L3](#) et la [licence de maths de L1 à L3](#)