

Feuille d'exercice 4 extensions de corps, racines de l'unité, polynômes cyclotomiques, corps finis, normes et traces

Exercices à faire (dans cet ordre de priorité) pour le 10 mai

Exercice 4 feuille 2 à finir

Exercices 1,2,3 feuille 4 à faire

Exercices 14, 15, 16 feuille 3 à faire

Exercices 8, 10, 11, 12 feuille 2 à faire (ils ne seront pas corrigés, mais à rendre si vous voulez)

Compléments sur les extensions de corps

Exercice 1 Soit $K \subset L$ une extension de corps de degré $[L : K] = n$ et $P \in K[X]$ un polynôme irréductible de degré m sur K . Montrez que si m ne divise pas n alors P n'a pas de racine dans L .

Exercice 2 Soit $K \subset L$ une extension de corps, et α et β des éléments de L algébriques sur K tels que $n = [K(\alpha) : K]$ et $m = [K(\beta) : K]$ soient premiers entre eux.

a) Montrez que $[K(\alpha, \beta)] = mn$.

b) Montrez que le polynôme minimal P de α sur K est irréductible sur $K(\beta)$.

Exercice 3 Soient $P, Q \in \mathbb{Q}[X]$ deux polynômes irréductibles sur \mathbb{Q} , et x (resp. y) une racine de P (resp. de Q) dans L . Montrez que P est irréductible sur $\mathbb{Q}[y]$ ssi Q est irréductible sur $\mathbb{Q}[x]$.

Racines de l'unité, polynômes cyclotomiques

Exercice 4 a) Montrez que si m et n sont premiers entre eux, alors $\Phi_m(X^n) = \prod_{d|n} \Phi_{dm}(X)$.

b) Si m et n ont les mêmes facteurs premiers montrez que $\Phi_m(X^n) = \Phi_{nm}(X) = \Phi_n(X^m)$.

c) Soit $n = mp^k$, avec p un nombre premier qui ne divise pas m . Montrez que l'image de $\Phi_n(X)$ par l'application canonique $P \rightarrow \bar{P}$ de $\mathbb{Z}[X]$ dans $\mathbb{F}_p[X]$ est $(\bar{\Phi}_m(X))^{p^k - p^{k-1}}$.

Exercice 5 Soit $P(X) = X^n + a_1X^{n-1} + \dots + a_n$ un polynôme irréductible de $\mathbb{Z}[X]$ dont toutes les racines complexes vérifient $0 < |z| \leq 1$. Montrez que P est un polynôme cyclotomique.

Exercice 6 Soit $n \geq 3$ un entier, et $\varphi(n)$ le nombre d'entiers entre 1 et n premiers avec n . Soit $a = e^{2i\pi/n}$.

a) Pourquoi $\mathbb{Q}[a] = \{f(a), f \in \mathbb{Q}[X]\}$ est-il un corps? Calculez $[\mathbb{Q}(a) : \mathbb{Q}]$.

b) Soit $b = a + \frac{1}{a}$. Pourquoi l'ensemble $\mathbb{Q}[a] \cap \mathbb{R}$ est-il un corps? Montrez qu'il contient $\mathbb{Q}[b]$. L'inclusion $\mathbb{Q}[b] \subset \mathbb{Q}[a]$ est-elle stricte?

c) Calculez $[\mathbb{Q}(a) : \mathbb{Q}(b)]$. Déduisez-en que $\mathbb{Q}[a] \cap \mathbb{R} = \mathbb{Q}[b]$. Que vaut $[\mathbb{Q}(b) : \mathbb{Q}]$?

d) Pour tout entier $k \geq 1$, on note $b_k = a^k + \frac{1}{a^k}$. Combien y a-t-il d'éléments b_k distincts quand k décrit \mathbb{N} ?

e) Montrez que pour k premier avec n , on a $[\mathbb{Q}(b_k) : \mathbb{Q}] = \frac{\varphi(n)}{2}$.

f) Considérons le polynôme $B_n(X)$ introduit dans la feuille 2. Quelles sont ses racines dans $\mathbb{Q}[a]$?

g) Quel est le polynôme minimal sur \mathbb{Q} de $2 \cos \frac{2\pi}{n}$? Explicitez celui de $\cos \frac{2\pi}{5}$.

Exercice 7 Soit $\theta = 2 \cos \frac{2\pi}{9}$.

a) Montrez que θ est racine d'un polynôme de degré 3 de $\mathbb{Q}[X]$ irréductible sur \mathbb{Q} .

b) Donnez les autres racines θ_1 et θ_2 de ce polynôme et montrez qu'elles sont dans $\mathbb{Q}(\theta)$.

c) Montrez que $\theta \mapsto \theta_i$ détermine un automorphisme de $\mathbb{Q}(\theta)$. Déduisez-en que le groupe des automorphismes de $\mathbb{Q}(\theta)$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Corps finis

Exercice 8 Donnez la liste des éléments, la table d'addition et de multiplication de \mathbb{F}_8 et \mathbb{F}_9 . Comparez respectivement avec $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/9\mathbb{Z}$.

Exercice 9 Soit E un \mathbb{F}_q espace vectoriel. En calculant le nombre de bases possibles de E montrez que

$$\begin{aligned}\#GL(E) &= (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) \\ &= (q - 1)^n q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n-1} (1 + q + \dots + q^k)\end{aligned}$$

Exercice 10 Soit p un nombre premier, k un entier et $f : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$ l'application définie par $f(x) = x^k$.

- a) À quelle(s) condition(s) f est-elle une bijection?
 b) Si l'équation $x^k = a$ a une solution, combien en a-t-elle?

Exercice 11 Soit $p \neq 2$ un nombre premier. On considère l'extension $\mathbb{Z}/p\mathbb{Z} \subset L$, où L est un corps à p^2 éléments. On note α une racine du polynôme $X^4 + 1$ dans une extension de L . L'objectif de cet exercice est de montrer que ce polynôme n'est pas irréductible sur $\mathbb{Z}/p\mathbb{Z}$.

- a) Montrez que $p^2 - 1$ est divisible par 8. Déduisez-en que $\alpha^{p^2-1} = 1$ et que $\alpha \in L$.
 b) On suppose que $X^4 + 1$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Que vaut le degré de α sur $\mathbb{Z}/p\mathbb{Z}$?
 c) Déduisez des questions précédentes que $X^4 + 1$ n'est pas irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

Exercice 12 Soit K un corps de caractéristique $p \neq 0$ et $f : x \mapsto x^p$. Montrez que f est un homomorphisme de corps différent de l'identité si $K \neq \mathbb{F}_p$.

Normes et Traces

Exercice 13 Soit $p \geq 3$ un nombre premier, et $\Phi_p(X) = X^{p-1} + \dots + 1$ le polynôme cyclotomique associé. Soit ζ une racine de Φ_p .

- a) Montrez que $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = -1$ et $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1) = p - 1$. Déduisez-en que pour tout $k \geq 1$, $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta^k) = p$.
 b) Montrez que $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta) = p$, et déduisez-en que $p = (1 - \zeta)(1 - \zeta^2) \dots (1 - \zeta^{p-1})$.
 c) On appelle *entier de $\mathbb{Q}(\zeta)$* tout élément θ de $\mathbb{Q}(\zeta)$ racine d'un polynôme unitaire à coefficients dans \mathbb{Z} . On *admet* que les entiers de $\mathbb{Q}(\zeta)$ forment un sous-anneau $A(\zeta)$ de $\mathbb{Q}(\zeta)$.
 • Montrez que $(1 - \zeta)A(\zeta) \cap \mathbb{Z} = p\mathbb{Z}$.
 • Si $\theta \in A(\zeta)$, montrez que $p | Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\theta(1 - \zeta))$.
 • Déduisez-en que $A(\zeta)$ est l'ensemble des éléments de $\mathbb{Q}(\zeta)$ qui sont des combinaisons linéaires à coefficients dans \mathbb{Z} de ζ et de ses puissances.