

Premier devoir

Exercice 1

Soient K un corps et L/K une extension finie de K . L'objectif de cet exercice est de démontrer le résultat suivant :

Proposition. *L'ensemble des sous-corps de L contenant K est fini si et seulement si L/K a un élément primitif (autrement dit s'il existe $\alpha \in L$ tel que $L = K(\alpha)$).*

- 1) En utilisant un résultat démontré en cours, vérifier que cet énoncé est vrai si K est un corps fini.

On suppose désormais que K est un corps infini.

- 2) Supposons que l'ensemble des sous-corps de L contenant K soit fini.

2.1) Soient α_1 et α_2 deux éléments de L . Démontrer que l'extension $K(\alpha_1, \alpha_2)/K$ a un élément primitif.

2.2) En déduire que L/K a un élément primitif.

- 3) Inversement, supposons qu'il existe $\alpha \in L$ tel que $L = K(\alpha)$. Soit $f \in K[X]$ le polynôme minimal de α sur K .

3.1) Soit E un sous-corps de L contenant K . Démontrer qu'il existe un polynôme unitaire $g \in L[X]$, qui divise f dans $L[X]$, tel que E soit le sous-corps de L engendré par K et les coefficients de g .

3.2) En déduire que l'ensemble des sous-corps de L contenant K est fini et la proposition.

Exercice 2

Un corps K est dit pythagoricien si pour tous x et y dans K l'élément $x^2 + y^2$ est un carré dans K .

- 1) Donner des exemples de corps pythagoriciens.
- 2) Démontrer qu'un corps K est pythagoricien si et seulement si toute somme de carrés dans K est un carré dans K .
- 3) Soient (p_n) la suite des nombres premiers et $K := \mathbb{Q}(\sqrt{2}, \sqrt{3}, \dots, \sqrt{p_n}, \dots)$ le sous-corps de \mathbb{C} engendré par les éléments $\sqrt{p_n}$. Démontrer que K n'est pas une extension finie de \mathbb{Q} .

- 4) En déduire qu'aucune extension finie de \mathbb{Q} n'est un corps pythagoricien.

Exercice 3

Étant donné un groupe H opérant sur un ensemble E , rappelons que H opère transitivement sur E si pour tous x et y dans E il existe $g \in H$ tel que $gx = y$. On dit que H opère deux fois transitivement sur E si pour tous couples (x, y) et (z, t) d'éléments distincts de E il existe $g \in H$ tel que $gx = z$ et $gy = t$.

On considère un entier $n \geq 2$ et un sous-groupe G de \mathbb{S}_n . Posons $X = \{1, \dots, n\}$. Le groupe G opère sur X via l'application $G \times X \rightarrow X$ qui à (σ, a) associe $\sigma(a)$. Pour tout $a \in X$, on note $\text{stab}(a)$ le sous-groupe de G formé des éléments qui fixent a . Il opère sur l'ensemble $X - \{a\}$.

- 1) On suppose que G opère transitivement sur X .

1.1) Démontrer que les assertions suivantes sont équivalentes :

- (i) G opère deux fois transitivement sur X ;
- (ii) pour tout $a \in X$ le groupe $\text{stab}(a)$ opère transitivement sur $X - \{a\}$.
- (iii) il existe $a \in X$ tel que $\text{stab}(a)$ opère transitivement sur $X - \{a\}$.

1.2) En déduire que si G contient un $n - 1$ -cycle et une transposition, alors $G = \mathbb{S}_n$.

Application

On utilisera le rappel 3 de la feuille d'exercices. Pour tout nombre premier p , désignons par $s_p : \mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$ la surjection canonique.

- 2) On pose $f = X^5 + 3X + 1 \in \mathbb{Z}[X]$.

2.1) Déterminer les décompositions en produit de polynômes irréductibles de $s_2(f)$ et $s_3(f)$.

2.2) En déduire que f est irréductible sur \mathbb{Q} puis que le groupe de Galois de f sur \mathbb{Q} est isomorphe à \mathbb{S}_5 .

Exercice 4

Soient ζ une racine primitive 11-ième de l'unité de \mathbb{C} et K le corps $\mathbb{Q}(\zeta)$. On rappelle que K est une extension galoisienne de \mathbb{Q} de degré 10 et que le groupe de Galois G de K sur \mathbb{Q} est cyclique.

- 1) Déterminer un générateur de G .

2) Décrire toutes les extensions de \mathbb{Q} contenues dans K . Pour chacune d'entre elles on explicitera le polynôme minimal sur \mathbb{Q} d'un élément primitif.

Exercice 5

Soient Ω une clôture algébrique du corps fini \mathbb{F}_3 et K l'extension de degré 3 de \mathbb{F}_3 contenue dans Ω (rappelons qu'il existe une unique telle extension de \mathbb{F}_3).

- 1) Soit $\alpha \in \Omega$ une racine du polynôme $X^3 - X + 1 \in \mathbb{F}_3[X]$. Montrer que l'on a $K = \mathbb{F}_3(\alpha)$.
- 2) Montrer que α est un générateur du groupe multiplicatif K^* .

Pour tout $k \in \mathbb{Z}$ on pose

$$f_k = (X - \alpha^k)(X - \alpha^{3k})(X - \alpha^{9k}) \in K[X].$$

- 3) Montrer que f_k appartient à $\mathbb{F}_3[X]$.
 - 4) Montrer que lorsque k varie, l'ensemble des polynômes f_k est formé de dix polynômes distincts sur \mathbb{F}_3 , dont huit sont irréductibles. Vérifier que l'on obtient ainsi tous les polynômes irréductibles unitaires de degré trois sur \mathbb{F}_3 .
 - 5) Trouver une relation simple entre f_k et f_{26-k} .
 - 6) En déduire les coefficients des polynômes f_k .
-