

Barème : 2+2 , 1,5+1,5+1,5+1,5+2 , 1,5+1,5+1,5 , 2.

Exercice 1. (a) Donner exemples de deux polynômes $P, Q \in \mathbb{Q}[X]$ irréductibles, de degré ≥ 2 , tels que pour P un corps de décomposition est aussi corps de rupture, et pour Q un corps de décomposition n'est pas corps de rupture. (Justifier.)

(b) Soit $P \in \mathbb{Q}[X]$ défini par $P(X) = X^4 + 2$. Décider si un corps de décomposition pour P est aussi corps de rupture. (Justifier.)

Exercice 2. Soit $\mathbb{F}_q$ un corps à q éléments, extension finie de $\mathbb{F}_p$. Posons $[\mathbb{F}_q : \mathbb{F}_p] = n$ (donc $q = p^n$). Soit $\text{Aut}(\mathbb{F}_q)$ le groupe des automorphismes de corps de $\mathbb{F}_q$. Soit $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ l'endomorphisme de Frobenius de $\mathbb{F}_q$, défini par $F(x) = x^p$.

(a) Montrer que tous les éléments x de $\mathbb{F}_q$ vérifient $x^q = x$.

(b) Montrer que F est bijectif.

(c) Montrer que pour tout entier k tel que $1 \leq k \leq n - 1$ on ne peut pas avoir $F^k = \text{Id}$. (Ici, F^k veut dire F composé avec lui-même k fois.)

(d) Montrer que $\text{Aut}(\mathbb{F}_q) = \{\text{Id}, F, F^2, \dots, F^{n-1}\}$.

(e) Si K est un sous-corps de $\mathbb{F}_q$, montrer que K a p^m éléments où m divise n .

(f) Si m est un diviseur de n , montrer que $\mathbb{F}_q$ a un et un seul sous-corps à p^m éléments.

Exercice 3. Soit K un corps de caractéristique p non nulle. Si $n \in \mathbb{N}^*$, on note U_n le groupe des éléments x de K qui vérifient $x^n = 1$.

(a) Montrer que pour tout $a \in \mathbb{N}^*$ on a $U_{np^a} = U_n$.

(b) Montrer que pour tout $k \in \mathbb{N}^*$, on a $|U_k|$ (le cardinal de U_k) divise k .

(c) Montrer que tout sous-groupe fini de $K^\times$ est égal à un groupe U_k .

Exercice 4. Soient K un corps et $m, n \in \mathbb{N}^*$ premiers entre eux. Si pour un certain $a \in K$ on a que $X^m - a$ et $X^n - a$ sont irréductibles sur K , montrer que $X^{mn} - a$ est irréductible sur K .