
 Algorithme de Berlekemp, extension monogène, clôture algébrique.

Exercice 1.

Soit $\mathbb{F}_q$ un corps fini et $P \in \mathbb{F}_q[X]$ un polynôme sans facteur carré.

1. Montrer que l'application

$$\varphi: \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \longrightarrow & \mathbb{F}_q[X]/(P) \\ Q(X) \bmod P & \longmapsto & Q(X^q) \bmod P \end{array}$$

est bien définie et est un morphisme d'anneaux $\mathbb{F}_q$ -linéaire.

2. Soit r le nombre de facteurs irréductibles de P . Montrer que $\ker(\varphi - \text{Id})$ est un $\mathbb{F}_q$ -espace vectoriel de dimension r .
3. On suppose désormais que $r \geq 2$.
 - (a) Montrer qu'il existe $S \in \mathbb{F}_q[X]$ non constant modulo P tel que l'on a l'égalité $P = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(P, S - \alpha)$.
 - (b) En déduire un algorithme de factorisation en facteurs irréductibles dans $\mathbb{F}_q[X]$.

Exercice 2.

1. Soit L/K une extension.
 - (a) On suppose que $L = K[\alpha]$ pour un certain $\alpha \in L$, et soit P le polynôme minimal de α sur K . Montrer qu'on a une application injective naturelle de l'ensemble des sous extensions K' de L/K vers l'ensemble des diviseurs unitaires de P dans $L[X]$.
 - (b) On suppose que K est infini et qu'il n'existe qu'un nombre fini de sous-extensions de L/K . Montrer que si $\alpha, \beta \in L$, alors l'extension $K(\alpha, \beta)$ est monogène. *Indice : considérer des extensions de la forme $K[\alpha + t\beta]$.*
En déduire que L est une extension monogène.
2. Soit K un corps de caractéristique $p > 0$.
 - (a) Montrer que $X^p - T \in (K(T))[X]$ est irréductible.
 - (b) Montrer que tout corps de rupture de $X^p - T$ sur $K(T)$ est un corps de décomposition.
3. Soit $K = \text{Frac}(\mathbb{F}_p[T, U])$, et L un corps de décomposition de $(X^p - T)(X^p - U)$.
 - (a) Montrer que $[L : K] = p^2$.
 - (b) Montrer que si $x \in L$, alors $x^p \in K$.
 - (c) En déduire que l'extension L/K n'est pas monogène.

Exercice 3.

Soit Ω un corps algébriquement clos. Soit $K \subset \Omega$ un sous corps. Soit enfin $L = \{x \in \Omega \mid x \text{ est algébrique sur } K\}$. Montrer que L est un corps, et que c'est une clôture algébrique de K .