Fiche 5
25 février 2015

Exercice 1 (Propriétés élémentaires des extensions normales).

1. Soit L/K une extension de degré fini de corps. Montrer que L/K est normale si et seulement si L est le corps de décomposition d'un polynôme de $K[X]$.
2. Soit L/K une extension normale de corps. Montrer que si $K \leq E \leq L$, alors L/E est aussi une extension normale.
3. Soit L/K une extension normale de degré fini. Si P est un polynôme irréductible dans $K[X]$, montrer que ses facteurs irréductibles dans $L[X]$ sont tous du même degré.

Exercice 2 (Éléments primitifs).
Soient K un corps *infini* et $L = K(\alpha, \beta)$ une extension algébrique. On suppose aussi que β est séparable sur K. L'objectif de cet exercice est de montrer que L/K contient un élément primitif.

On définit P et Q les polynômes minimaux de α et de β sur K respectivement. Leurs degrés sont notés d_P et d_Q respectivement. On fixe une extension Ω de L où P et Q sont scindés. On note leurs ensembles de racines respectifs $\{\alpha_1, \ldots, \alpha_{d_P}\}$ et $\{\beta_1, \ldots, \beta_{d_Q}\}$, avec $\alpha_1 = \alpha$ et $\beta_1 = \beta$.

1. Montrer qu'il existe $t \in K$ tel que $t \neq \frac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$ pour tous $1 \leq i, k \leq d_P$ et $1 \leq j \neq l \leq d_Q$. En déduire que $\alpha_i + t\beta_j \neq \alpha_k + t\beta_l$ pour tous $1 \leq i, k \leq d_P$ et $1 \leq j \neq l \leq d_Q$.
2. Montrer que le PGCD unitaire $h(X)$ des polynômes $Q(X)$ et $P(\alpha+t\beta-tX)$ dans $K(\alpha+t\beta)[X]$ est de degré au moins 1. (*Vous pouvez expliciter une racine commune*)
3. Montrer que h est linéaire. Quel est son terme constant ? (*Le polynôme Q n'a pas de racine multiple*).
4. Déduire du point précédent que $K(\alpha, \beta) = K(\alpha + t\beta)$.

Exercice 3 (Perfection/Imperfection).
A. Corps parfaits
Un corps K est dit parfait si toute extension algébrique de K est séparable.

1. Soit K un corps de caractéristique p non nulle. Si f est un polynôme irréductible dans $K[X]$, alors f est inséparable si et seulement si $f(X) \in K[X^p]$.
2. Soit K un corps de caractéristique p. Montrer alors l'équivalence suivante : K est parfait si et seulement si l'endomorphisme de Frobenius $F : x \longmapsto x^p$ est surjectif. En particulier, les corps finis sont parfaits.

B. Corps imparfaits
Soit K un corps de caractéristique p non nul. On supposera que le sous-corps $K^p = \{x^p | x \in K\}$ soit strictement contenu dans K.

1. Si $a \in K \setminus K^p$, alors pour tout $e \in \mathbb{N}$, le polynôme $X^{p^e} - a$ est irréductible dans $K[X]$.
2. Montrer que si $a \in L$, où L est une extension algébrique de K, et que pour un certain $e \in \mathbb{N}$, $a^{p^e} \in K$, alors a est la seule racine de son polynôme minimal sur K. On dit alors que a est *purement inséparable sur K*.
3. Montrer qu'un élément d'une extension de K est séparable et purement inséparable sur K si et seulement s'il appartient à K.

Exercice 4 (Caractéristique non nulle : du polynôme au groupe).
On définit le polynôme $f(X) = X^p - X - t$ dans $\mathbb{F}_p(t)[X]$, avec t transcendant sur $\mathbb{F}_p$.

1. Montrer que si α est une racine de f, alors $\alpha + i$ en est une aussi ($i \in \mathbb{Z}$).
2. Montrer que $f(X)$ est irréductible dans $\mathbb{F}_p(t)[X]$ et qu'il est séparable sur $\mathbb{F}_p(t)$.
3. Montrer que le groupe de Galois de $f(X)$ sur $\mathbb{F}_p(t)$ est cyclique d'ordre p.

Exercice 5 (Caractéristique non nulle : du groupe au polynôme).
Soit k un corps de caractéristique non nulle p. Soit F une extension galoisienne cyclique de degré p de k. Soit σ un générateur du groupe de Galois de F sur k.
(a) Montrer que l'endomorphisme $k-$linéaire de F :

$$S : \alpha \mapsto \alpha - \sigma(\alpha)$$

est nilpotent.
(b) Soit $\alpha \in \ker S^2 \setminus \ker S$. Montrer que $\beta = \frac{\alpha}{\sigma(\alpha)-\alpha}$ vérifie $\sigma(\beta) = \beta + 1$.
(c) En déduire que β vérifie une équation de la forme $X^p - X - a = 0$ avec $a \in k$.