Fiche 4

11 février 2015

Exercice 1 (Existence d'éléments primitifs : caractérisation ; conditions suffisantes).
Soit L/K une extension algébrique.

1. On suppose qu'il existe α tel que $L = K(\alpha)$. Soit P le polynôme minimal de α sur K.
   (a) Soit M un sous-corps de L, contenant K. Montrer qu'il existe un facteur unitaire Q de P dans $L[X]$ tel que M soit engendré sur K par les coefficients de Q.
   (b) En déduire que l'extension L/K n'a qu'un nombre fini de sous-extensions.
2. Réciproquement, on suppose que l'extension L/K n'a qu'un nombre fini de sous-extensions.
   (a) Montrer que $[L : K]$ est fini.
   (b) Si K est fini, prouver qu'il existe α avec $L = K(\alpha)$.
   (c) Si K est infini, montrer que pour tous α, β dans L, il existe $\lambda \in K$ tel que $K(\alpha, \beta) = K(\alpha + \lambda\beta)$. En déduire qu'il existe α tel que $L = K(\alpha)$.
3. Montrer que si L/K est une extension séparable de dimension finie, alors il existe $\alpha \in L$ tel que $L = K(\alpha)$. Donner un exemple d'extension inséparable qui contient un élément primitif.

Exercice 2 (Manque de séparabilité).
On fixe un nombre premier p, un corps k de caractéristique p et deux indéterminées X, Y sur k. En d'autres termes, X et Y sont algébriquement indépendants sur k. On définit $E = k(X, Y)$ et $K = k(X^p, Y^p)$.

1. Montrer que $X \notin K$ et $Y \notin K(X) = K[X]$.
2. Déduire de 1 que $T^p - X^p$ est irréductible dans $K[T]$ et que $T^p - Y^p$ est irréductible dans $K(X)[T]$. Conclure que $[E : K] = p^2$.
3. Montrer que si $\alpha \in E$ alors $[K(\alpha) : K] \leq p$. En déduire que l'extension E/K ne contient pas d'élément primitif.
4. Déduire du point précédent et de la preuve du théorème primitif pour les corps infinis que pour tous $t_1, t_2 \in K$, $K(X + t_1Y) = K(X + t_2Y)$ si et seulement si $t_1 = t_2$. (*L'extension E/K a donc une infinité de sous-extensions, et en particulier, elle n'est pas galoisienne. En effet, E/K n'est pas une extension séparable.*)

Exercice 3 (Théorème fondamental de l'algèbre).
L'objectif de cet exercice est de montrer que $\mathbb{C}$ est algébriquement clos, qu'en d'autres termes, tout polynôme d'une seule variable et à coefficients complexes se scinde dans $\mathbb{C}$. On admettra que tout polynôme réel de degré impair a une racine réelle et que tout réel positif a une racine carrée (réelle). Cette dernière est la seule donnée analytique de la preuve.

1. Montrer que $\mathbb{C}$ n'a pas d'extension de degré 2.
2. Montrer qu'il suffit de vérifier que la seule extension propre algébrique de $\mathbb{R}$ est $\mathbb{C}$.
   On étudiera donc le corps de décomposition d'un polynôme non constant $f \in \mathbb{R}[X]$.
3. On note E le corps de décomposition de f. Montrer qu'on peut supposer que $\mathbb{C} \subset E$.
4. Montrer que $\mathrm{Gal}(E/\mathbb{R})$ est un $2-$groupe (en considérant ses 2-Sylow).
5. Conclure.

6. **(Coin culture)** Montrer que les racines de l'unité dans $(\mathbb{C}^*, .)$ forment un sous-groupe infini G non monogène. Montrer que pour tout $n \in \mathbb{N}^*$, G possède un sous-groupe et un seul d'ordre n. Montrer que G est divisible, en d'autres termes, pour tout $n \in \mathbb{N}^*$, tout élément de G a une nième racine par rapport à la loi de groupe.