Université Claude Bernard - Lyon 1 Semestre de printemps 2019-2020

MG1 - Algèbre commutative

Fiche de TD no 5

Exercice 1. Soit $P(X) = X^4 - X - 1 \in \mathbb{Q}[X]$.

1. Montrer que P est irréductible sur $\mathbb{Q}$ et possède exactement deux racines réelles notées x_1 et x_2.

On écrit $P(X) = (X - x_1)(X - x_2)(X^2 - aX + b') = (X^2 + aX + b)(X^2 - aX + b')$ avec $a, b, b' \in \mathbb{R}$.

2. Montrer que $c = a^2$ satisfait l'équation $c^3 + 4c - 1 = 0$.
   Indication : remarquer que $a^2 = b + b'$ $a(b - b') = 1$; $bb' = -1$.
3. En déduire que le degré du corps de décomposition de P est multiple de 12.
4. En déduire que les racines du polynôme P (qui sont de degré 4) ne sont pas constructibles.

Exercice 2. On va montrer le résultat suivant : une extension algébrique $\mathbb{L}/\mathbb{K}$ est engendrée par un élément primitif si et seulement si elle n'a qu'un nombre fini de sous-extensions.

1. Soit $\mathbb{L} = \mathbb{K}[a]$ une extension algébrique, P le polynôme minimal de a.
   Soit M un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$.
   (a) Montrer qu'il existe un facteur unitaire Q de P dans $\mathbb{L}[X]$ tel que $\mathbb{L}$ soit engendré sur $\mathbb{K}$ par les coefficients de Q.
   (b) En déduire que l'extension $\mathbb{L}/\mathbb{K}$ n'a qu'un nombre fini de sous-extensions.
2. Soit $\mathbb{L}/\mathbb{K}$ une extension qui n'a qu'un nombre fini de sous-extensions.
   (a) Montrer que $[\mathbb{L} : \mathbb{K}]$ est fini.
   (b) Si $\mathbb{K}$ est fini, en déduire qu'il existe un élément primitif pour $\mathbb{L}$.
   (c) Si $\mathbb{K}$ est infini, montrer que pour tout $a, b \in \mathbb{L}$ il existe $t \in \mathbb{K}$ tel que $\mathbb{K}[a, b] = \mathbb{K}[a + tb]$. En déduire qu'il existe un élément primitif pour $\mathbb{L}$.

On rappelle qu'étant donné un polynôme $P \in \mathbb{K}[X]$ séparable dont les racines sont $x_1, \dots, x_n \in \overline{\mathbb{K}}$, on définit $\delta = \prod_{i<j}(x_i - x_j) \in \overline{\mathbb{K}}$ et son discriminant $\Delta = \delta^2 \in \mathbb{K}$.
On rappelle que : Δ est un carré dans $\mathbb{K}$ si et s. si $\mathrm{Gal}(P)$ est inclus dans A_n.

Exercice 3. Quel est le groupe de Galois d'un polynôme de degré 2 ?

Exercice 4 (Équation de degré 3)**.** Soit $P \in \mathbb{K}[X]$ un polynôme irréductible de degré 3. Soit $\mathbb{L}$ son corps de décomposition. On garde les notations δ et Δ vues plus haut.

1. Quelles sont les valeurs possibles de $[\mathbb{L} : \mathbb{K}]$?
2. Quelles sont les structures possibles de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$?
3. Montrer que si Δ n'est pas un carré dans $\mathbb{K}$, alors $[\mathbb{L} : \mathbb{K}] = 6$.

4. Montrer que si Δ est un carré dans $\mathbb{K}$, alors $[\mathbb{L} : \mathbb{K}] = 3$. (On montrera que L est engendré par δ et une des racines de P.

Exercice 5. Soient p premier et $n \in N$ tel que $\sqrt[p]{n}$ soit irrationnel.

1. Montrer que $P(X) = X^p - n$ est irréductible sur $\mathbb{Z}$. (voir ex. 6 fiche 1)

Soit ζ une racine primitive p-ième de 1 et soit $\mathbb{L}$ le corps de décomposition de P.

2. Montrer que $\mathbb{L} = \mathbb{Q}[\sqrt[p]{n}, \zeta]$.
   Quel est le degré de $\mathbb{L}$ sur $\mathbb{Q}$?
3. Montrer que pour tout couple (i, j), $0 \leq i < p$, $1 \leq j < p$, il existe un unique automorphisme $\sigma_{i,j}$ de $\mathbb{L}$ tel que $\sigma_{i,j}(\sqrt[p]{n}) = \zeta^i \sqrt[p]{n}$ et $\sigma_{i,j}(\zeta) = \zeta^j$.
4. Soient $H = \{\sigma_{i,1} \,|0 \leq i < p\}$ et $G = \{\sigma_{0,j} \mid 1 \leq j < p\}$. Montrer que H et G sont des sous-groupes cycliques de $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$.
5. Montrer que H est distingué dans $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$.
6. Montrer que $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ est le produit semi-direct de H et G.