Feuille de TD n° 2

Exercice 1 Indépendance linéaire des racines carrées d'entiers

a) Montrer que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. En déduire que $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ forment une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ comme $\mathbb{Q}-$espace vectoriel.

b) Soient $p_1, ..., p_n$ des nombres premiers distincts. Montrer par récurrence sur $n \in \mathbb{N}$ que les nombres

$$\sqrt{\prod_{i \in I} p_i},\ I \subseteq \{1, ..., n\}$$

forment une base de $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$.

c) Montrer que $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1} + ... + \sqrt{p_n})$.

d) Montrer que les nombres

$$\sqrt{n}\,,$$

où $n \in \mathbb{N}$ est sans facteur carré, sont $\mathbb{Q}-$linéairement indépendants.

Exercice 2 Le groupe diédral D_4 comme groupe de Galois sur $\mathbb{Q}$

On note $x_k = i^{k-1}\sqrt[4]{2}$, $k = 1, 2, 3, 4$, les racines complexes du polynôme $X^4 - 2$. On pose $K = \mathbb{Q}(x_1, x_2, x_3, x_4)$.

a) Montrer que $K = \mathbb{Q}(i, \sqrt[4]{2})$. et que le groupe $\mathrm{Aut}K$ est d'ordre ≤ 8.

b) En utilisant la multiplicativité des degrés, justifier que le polynôme $X^4 - 2$ est irréductible sur le corps $\mathbb{Q}(i)$.

c) En déduire l'existence d'un automorphisme $\sigma \in \mathrm{Aut}K$ tel que :

$$\sigma(i) = i,\ \sigma(x_1) = x_2\ .$$

d) On pose $\tau : K \to K$ la conjugaison complexe. On fait agir $\mathrm{Aut}K$ sur les racines x_1, x_2, x_3, x_4. On obtient un morphisme injectif

$$\mathrm{Aut}K \to \mathfrak{S}_4\ .$$

Déterminer les images de $\sigma, \tau, \sigma\tau, \tau\sigma$ dans $\mathfrak{S}_4$. En déduire que le groupe $\mathrm{Aut}K$ est engendré par σ et τ.

e) Soit $\alpha = i + \sqrt[4]{2}$. Déterminer un polynôme rationnel P de degré 8 qui annule α.

f) Montrer que $\mathbb{Q}(\alpha) = K$ et que P est le polynôme minimal de α sur $\mathbb{Q}$.
Indication. Vérifier que le polynôme minimal doit annuler aussi les $\varphi(\alpha)$, $\varphi \in \mathrm{Aut}(K)$.

Exercice 3 Un polynôme de groupe de Galois $\mathfrak{S}_n$

Soit $P(X) = X^n - X - 1$.

a) Montrer que P n'a pas de racine dans $\mathbb{Q}$.

b) Montrer que les racines complexes de P sont simples.

c) Si Q est un polynôme à coefficients entiers qui divise P, on pose $S(Q) = \sum_z (z - \frac{1}{z})$ où z décrit les racines de Q. Montrer que $S(Q) \in \mathbb{Z}$.

d) Soit z une racine de P. On pose $z = re^{i\theta}$ où $r > 0$ et $\theta \in \mathbb{R}$. Montrer que $r \neq 1$ puis que $2\mathrm{R}e(z - \frac{1}{z}) > \frac{1}{r^2} - 1$.
Indication. $z^n - z - 1 = 0 \Rightarrow |z|^{2n} = |z+1|^2$ ...

e) Montrer que $S(Q) \geq 1$.
Indication. On rappelle que si $x_1, ..., x_n \geq 0$, *alors* $\frac{x_1 + ... + x_n}{n} \geq \sqrt[n]{x_1 ... x_n}$.

f) En déduire que P est irréductible sur $\mathbb{Q}$.

Exercice 4 $\mathbb{C}$ est algébriquement clos

d'après P. Samuel, Théorie algébrique des nombres, appendice du chap. II

a) Soit $P \in \mathbb{R}[X]$ de degré impair. Montrer que P a une racine réelle. *Indication : utiliser le TVI !*

b) Soit $P \in \mathbb{R}[X]$ de degré n. On factorise dans une extension de $\mathbb{C}$. On note $x_1, ..., x_n$ les racines (éventuellement avec des répétitions).
On raisonne par récurrence sur $v_2(n)$, l'exposant de la plus grande puissance de 2 qui divise n. Montrer que P a une racine complexe. *Indication : si* $c \in \mathbb{R}$, *considérer le polynôme* $\prod_{1 \leq i < j \leq n} X - (x_i + x_j + cx_ix_j)$ *est à coefficients réels et en déduire qu'il a au moins une racine complexe ; puis utiliser que* $\mathbb{R}$ *est infini pour trouver deux réels* $c \neq c'$ *et* $1 \leq i < j \leq n$ *tels que*

$$x_i + x_j + cx_ix_j \text{ et } x_i + x_j + c'x_ix_j \in \mathbb{C}$$

...