

Corrigé devoir 5

Exercice 1 — Groupe de Galois d'un polynôme de degré 3. Soient $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré 3 tel que P aient 2 racines complexes non réelles. Déterminer $G = \text{Gal}_{\mathbb{Q}}(P)$.

Corrigé Par définition, $\text{Gal}_{\mathbb{Q}}(P) = \text{Gal}(K \mid \mathbb{Q})$ où K est le corps de décomposition de P sur $\mathbb{Q}$. Comme $\mathbb{Q}$ est de caractéristique nulle, P a trois racines distinctes dans toute extension où il est scindé. On les note $\theta_1, \theta_2, \theta_3$. L'application

$$\Delta: \begin{cases} G \longrightarrow \mathfrak{S}_{\{\theta_1, \theta_2, \theta_3\}} \\ g \longmapsto g|_{\{\theta_1, \theta_2, \theta_3\}} \end{cases}$$

est alors bien définie puisque $g(\theta_i)$ est une racine de P . De plus, Δ est évidemment un morphisme de groupes. Comme K est le corps de décomposition de P sur $\mathbb{Q}$, le morphisme Δ est injectif. En effet, si $g(\theta_i) = \theta_i$ pour tout $i \in \llbracket 1, 3 \rrbracket$ alors $g = \text{id}_K$ puisque les θ_i engendrent le corps K . En terme d'action de groupes, on vient de montrer que G agit sur l'ensemble des racines de P de façon fidèle.

Ainsi G est (s'identifie à) un sous-groupe de $\mathfrak{S}_3$. Montrons (de deux façons différentes) que $|G|$ est divisible par 3.

Première méthode : théorie des groupes. Comme P est irréductible, le groupe $\text{Gal}_{\mathbb{Q}}(P)$ agit transitivement sur les racines de P qui sont au nombre de 3. La théorie des actions de groupes donne une bijection entre G/G_x (quotient du groupe qui agit par le stabilisateur d'un point $x \in X$ où X est l'ensemble sur lequel G agit) et $\mathcal{O}(x)$ (l'orbite de ce point x). Ici, on a $G = \text{Gal}_{\mathbb{Q}}(P)$ et $X = \{\theta_1, \theta_2, \theta_3\}$, la transitivité de l'action signifie que l'orbite d'un point est X tout entier. Ainsi $|G/G_x| = |X| = 3$ et donc $3 \mid |G|$.

Deuxième méthode : théorie des corps. On a $\mathbb{Q}(\theta_1) \subset K$. Par multiplicativité des degrés, on en déduit que $[K : \mathbb{Q}] = [K : \mathbb{Q}(\theta_1)][\mathbb{Q}(\theta_1) : \mathbb{Q}]$. L'irréductibilité de P sur $\mathbb{Q}$ assure que P est le polynôme minimal de θ_1 sur $\mathbb{Q}$ et donc $[\mathbb{Q}(\theta_1) : \mathbb{Q}] = 3$. Ainsi $[K : \mathbb{Q}]$ est divisible par 3. Par ailleurs, l'extension $\mathbb{Q} \subset K$ est galoisienne puisqu'elle est normale (c'est un corps de décomposition) et séparable (on est en caractéristique nulle). Ainsi $|\text{Gal}_{\mathbb{Q}}(P)| = |\text{Gal}(K \mid \mathbb{Q})| = [K : \mathbb{Q}]$ et donc $|G|$ est divisible par 3.

Jusqu'ici nous n'avons pas utilisé l'hypothèse que P a deux racines complexes non réelles (le raisonnement est en fait valable pour tout polynôme irréductible P de degré 3 et séparable). Utilisons-la. Considérons σ la conjugaison complexe et notons $\overline{\mathbb{Q}}$ l'ensemble des éléments de $\mathbb{C}$ algébrique sur $\mathbb{Q}$ (c'est une clôture algébrique $\mathbb{Q}$). On a bien sûr $\sigma(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}}$. Ainsi σ induit un $\mathbb{Q}$ -automorphisme qui est d'ordre 2 (puisque σ l'est et $\sigma(i) = -i$) de $\overline{\mathbb{Q}}$. Comme l'extension $\mathbb{Q} \subset K$ est normale, $\sigma(K) = K$ (c'est l'une des définitions équivalentes des extensions normales) et donc σ induit un $\mathbb{Q}$ -automorphisme de K (qu'on note encore σ). C'est automorphisme est d'ordre inférieur ou égal à 2. De plus, il n'est pas trivial puisque P a une racine non réelle. Ainsi il existe dans G un élément d'ordre 2. Finalement, grâce au théorème de Lagrange, $|G|$ est divisible par 2.

Comme 2 et 3 sont premiers entre eux, $|G|$ est divisible par 6 et donc comme G est un sous-groupe de $\mathfrak{S}_3$, on en déduit que $G = \mathfrak{S}_3$.