Corrigé devoir 2

Exercice 1 — Extension de degré 2. Soit K une extension de degré 2 de k. Déterminer $\mathrm{Aut}_k(\mathrm{K})$.

Corrigé Soit $x \in \mathrm{K} \smallsetminus k$. On a alors $[k(x) : k] \geqslant 2$ et $k(x) \subset \mathrm{K}$. Finalement $\mathrm{K} = k(x)$ est une extension monogène.

Par ailleurs, on note $\mathrm{P} = \mathrm{X}^2 + u\mathrm{X} + v \in k[\mathrm{X}]$ le polynôme minimal de x sur k. Pour $\sigma \in \mathrm{Aut}_k(\mathrm{K})$, on a $\mathrm{P}(\sigma(x)) = \sigma(\mathrm{P}(x)) = 0$ puisque $\mathrm{P} \in k[\mathrm{X}]$. Ainsi $\sigma(x)$ est une racine de P. On en déduit une application

$$\Delta\colon \begin{cases} \mathrm{Aut}_k(\mathrm{K}) \longrightarrow \{\text{Racines de P}\} \\ \quad \sigma \qquad \longmapsto \sigma(x)\,. \end{cases}$$

Comme x est un générateur (sur k) de $\mathrm{K} = k(x)$, l'application Δ est injective. De plus, si y est une racine de P (contenue dans K), il existe un élément σ de $\mathrm{Aut}_k(\mathrm{K})$ vérifiant $\sigma(x) = y$. Construisons-le. La famille $(1, x)$ est une base de K. On définit alors σ en posant $\sigma(a + bx) = a + by$ pour $a, b \in k$. C'est évidemment un morphisme de k-espaces vectoriels. Comme P est irréductible sur k, on a $y \notin k$ et donc $(1, y)$ est une k-base de K. Ainsi σ est une bijection k-linéaire. Il reste à voir que σ est un automorphisme d'anneau ce qui résulte du fait que x et y sont des racines du polynôme P à coefficient dans k : on a

$$\begin{aligned} \sigma((a + bx)(c + dx)) &= \sigma(ac + (bc + ad)x + bdx^2) \\ &= \sigma(ac - bdv + (bc + ad - bdu)x) \\ &= ac - bdv + (bc + ad - bdu)y \\ &= ac + (bc + ad)y + bdy^2 \\ &= (a + by)(c + dy)\,. \end{aligned}$$

Finalement, on obtient que Δ réalise une bijection entre $\mathrm{Aut}_k(\mathrm{K})$ et $\{\text{Racines de P contenues dans K}\}$. C'est un résultat parfaitement général et fondamental sur les extensions monogènes : **déterminer le nombre d'automorphismes d'une extension monogène, c'est déterminer le nombre de racines contenu dans le corps du polynôme minimal d'un générateur.**

Il s'agit donc de déterminer le nombre de racines de P dans K. Comme P est de degré 2, il y a au plus deux racines dans K et au moins une x. Les relations coefficients-racines montrent que la « deuxième » racine de P est $a - x$ et donc aussi dans K. Finalement, P a exactement deux racines dans K si elles sont distincts. Sinon, P n'a qu'une seule racine (double).

Supposons que P ait une racine double qui est forcément x. Alors x est racine de P' et donc $\mathrm{P} \mid \mathrm{P}'$ puisque P est le polynôme minimal de P. Mais $\deg \mathrm{P}' < \deg \mathrm{P}$ et donc $\mathrm{P}' = 0$. On en déduit que $2\mathrm{X} + u = 0$. Ainsi $2 = 0$ dans k et $u = 0$. Finalement $\mathrm{car}\, k = 2$ et $u = 0$. Réciproquement, lorsque $\mathrm{car}\, k = 2$ et $u = 0$, on a $\mathrm{P} = \mathrm{X}^2 - v = \mathrm{X}^2 - x^2 = (\mathrm{X} - x)^2$ dans $\mathrm{K}[\mathrm{X}]$ (la dernière égalité résultant du morphisme de Frobenius) et P a une racine double.

Finalement $\mathrm{Aut}_k(\mathrm{K})$ a deux éléments et donc est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ sauf si $\mathrm{car}\, k = 2$ et $\mathrm{P} = \mathrm{X}^2 - v$ auquel cas $\mathrm{Aut}_k(\mathrm{K}) = \{\mathrm{id}_\mathrm{K}\}$.

Remarquez que la condition porte sur le polynôme minimal d'un générateur de K, on en déduit donc que si $\mathrm{car}\, k = 2$ et s'il existe un élément de K dont le polynôme minimal est de la forme $\mathrm{X}^2 - v$, c'est le cas pour tous les éléments de K qui engendrent K.