Exercice 5.9 – solutions partielles

Exercice 5.9

Le corollaire 5.11 du cours est habituellement appelé *théorème de l'élément primitif*. Il dit qu'une extension finie séparable K/k est toujours simple (ou monogène). Par ailleurs, la preuve montre que si k est infini, et si l'on note $\alpha_1, \ldots, \alpha_r$ des générateurs de K/k, on peut toujours trouver un élément primitif de la forme $m_1\alpha_1 + \cdots + m_r\alpha_r$ où les m_i sont des éléments de k. Lorsque k est de caractéristique 0, on peut même choisir des m_i entiers.

La méthode la plus directe pour trouver un élément primitif est d'essayer de montrer que $x = m_1\alpha_1 + \cdots + m_r\alpha_r$ est primitif, et pour cela qu'il est de degré égal à $[K : \mathbb{Q}]$. On commence par prendre $m_1 = \cdots = m_r = 1$. Si cela échoue, on esaie avec $m_1 = 2$ et $m_2 = \cdots = m_r = 1$, etc. Ci-dessous nous allons donner deux situations différentes dans lesquelles on essaie d'appliquer cette méthode de deux manières différentes, essayant de minimiser les calculs.

Considérons le corps $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ avec $\omega^2 + \omega + 1$, i.e. ω est une racine primitive troisième de l'unité. C'est une extension de degré 6 de $\mathbb{Q}$. D'après le lemme de la base téléscopique on sait que $\mathscr{B} = \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \sqrt[3]{2}\omega, (\sqrt[3]{2})^2\omega\}$ est une $\mathbb{Q}$-base de K.

Notons $\alpha = \sqrt[3]{2} + \omega$ et $d = \deg_{\mathbb{Q}}(\alpha)$. On a $d \mid 6$ donc pour montrer que α est un élément primitif de l'extension (i.e. $d = 6$) il suffit de montrer que $d > 3$. Pour cela il suffit de montrer que $1, \alpha, \alpha^2, \alpha^3$ sont linéairement indépendants sur $\mathbb{Q}$. Il ne nous reste qu'à vérifier que la matrice qui exprime les éléments $1, \alpha, \alpha^2, \alpha^3$ en lignes sur les éléments de la base $\mathscr{B}$ en colonnes, est de rang maximal c'est-à-dire 4. On calcule $\alpha^2 = (\sqrt[3]{2})^2 + 2\sqrt[3]{2}\omega + (-\omega - 1)$ et $\alpha^3 = 2 + 3(\sqrt[3]{2})^2\omega + 3\sqrt[3]{2}(-\omega - 1) + 1$. Ainsi la matrice en question est:

$$\begin{array}{c} \\ 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & \sqrt[3]{2} & (\sqrt[3]{2})^2 & \omega & \sqrt[3]{2}\omega & (\sqrt[3]{2})^2\omega \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & -1 & 2 & 0 \\ 3 & -3 & 0 & 0 & -3 & 3 \end{pmatrix} \end{array}$$

On voit que les colonnes 1,2,3 et 6 forment une matrice extraite carrée qui est triangulaire avec 1,1,1,3 sur la diagonale. Cette matrice extraite est donc inversible, donc le rang de la matrice initiale est 4, i.e. maximal.

Considérons maintenant $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Une $\mathbb{Q}$-base de K est la famille $\mathscr{B} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$. On a déjà travaillé avec des corps semblables, et on sait que K est une extension de $\mathbb{Q}$ de degré 8, galoisienne de groupe de Galois $G = (\mathbb{Z}/2\mathbb{Z})^3$. Les automorphismes sont les $\sigma : K \to K$ déterminés par $\sigma(\sqrt{2}) = \epsilon\sqrt{2}$, $\sigma(\sqrt{3}) = \eta\sqrt{3}$ et $\sigma(\sqrt{5}) = \delta\sqrt{5}$ pour les huit choix possibles de $(\epsilon, \eta, \delta) \in \{\pm 1\}^3$. Posons $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$. Pour un σ comme celui décrit précédemment, on a donc : $\sigma(\alpha) = \epsilon\sqrt{2} + \eta\sqrt{3} + \delta\sqrt{5}$. Comme $\sqrt{2}, \sqrt{3}, \sqrt{5}$ sont tous trois éléments de la base $\mathscr{B}$, on voit que $\sigma(\alpha) \neq \alpha$ lorsque $\sigma \neq \mathrm{id}$. Il s'ensuit que α n'appartient à aucun corps de points fixes K^H, pour un sous-groupe $H \subset G$ distinct de $\{\mathrm{id}\}$. D'après le théorème principal de la correspondance de Galois, toutes les sous-extensions $L \subset K$ distinctes de K sont de la forme K^H pour un sous-groupe $H \neq \{\mathrm{id}\}$. Ceci montre que α n'appartient à aucune sous-extension stricte de K, donc il engendre K, ce qui signifie que c'est un élément primitif.