Fiche IV, exercice 2 :

2) Comme $\sqrt{3}$ est de degré 2 sur $\mathbb{Q}$, $\sqrt{(3)}$ est de degré 1 ou 2 sur $\mathbb{Q}(\sqrt{2})$. Or, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ donc :

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$
$$= 4 \ .$$

3) Si $\alpha := \sqrt{2}+\sqrt{3}$, alors $\alpha^{-1} = \sqrt{3}-\sqrt{2}$. Donc : $\sqrt{2}+\sqrt{3}$ et $\sqrt{2}-\sqrt{3} \in \mathbb{Q}(\alpha)$ d'où : $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha)$.

On a aussi : $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}) + \mathbb{Q}(\sqrt{2})\sqrt{3} = \mathbb{Q} + \mathbb{Q}(\sqrt{2}) + \mathbb{Q}(\sqrt{3}) + \mathbb{Q}(\sqrt{6}$. Comme de plus $\mathbb{Q}(\alpha)$ est de dimension 4 sur $\mathbb{Q}$, la famille génératrice $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ est une base.

4) Comme α est de degré 4 sur $\mathbb{Q}$, pour trouver le polynôme minimal de α sur $\mathbb{Q}$, il suffit de trouver un polynôme rationnel de degré 4 qui annule α.

Or, on a :

$$\alpha^2 = 5 + 2\sqrt{6} \Rightarrow (\alpha^2 - 5)^2 = 24$$

donc le polynôme minimal de α sur $\mathbb{Q}$ est : $P(X) = X^4 - 10X^2 + 1$. Les racines de P sont :

$$\alpha_1 := \alpha = \sqrt{2}+\sqrt{3}, \alpha_2 := \sqrt{2}-\sqrt{3}, \alpha_3 := -\sqrt{2}+\sqrt{3}, \alpha_4 := \sqrt{2}-\sqrt{3}, \ .$$

5) Un automorphisme σ de $\mathbb{Q}(\alpha)$ est déterminé par $\sigma(\alpha)$. Les 4 automorphismes de $\mathbb{Q}(\alpha)$ sont donc :

$$\sigma_1 : \alpha \mapsto \alpha \ , \ \sigma_2 : \alpha \mapsto \alpha_2 \ , \ \sigma_3 : \alpha \mapsto \alpha_\text{»} \ , \ \sigma_4 : \alpha \mapsto \alpha_4 \ .$$

Dans la base $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ de $\mathbb{Q}(\alpha)$, on obtient la représentation matricielle suivante :

$$\sigma_1 = \mathrm{Id}, \sigma_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

on a donc un isomorphisme de groupes :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Aut}(\mathbb{Q}(\alpha))$$
$$(i,j) \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & (-1)^i & 0 & 0 \\ 0 & 0 & (-1)^j & 0 \\ 0 & 0 & 0 & (-1)^{i+j} \end{pmatrix} \ .$$

6) Soit $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\alpha)$. Soit $Q(X) \in K[X]$ le polynôme minimal de α sur K. Alors $Q(X)$ divise $P(X)$ sur K (donc sur $\mathbb{R}$). De plus le degré de $Q(X)$ est aussi $[\mathbb{Q}(\alpha) : K]$ donc $\deg Q | 4$ et $\deg Q = 1, 2$ ou 4. Or : $P(X) = (X-\alpha)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)$.

Comme de plus, $Q(\alpha) = 0$, on a :

$$\deg Q(X) = 1 \Rightarrow K = \mathbb{Q}(\alpha)$$

$$\deg Q(X) = 4 \Rightarrow K = \mathbb{Q}$$

$$\deg Q = 2 \Rightarrow Q(X) = (X-\alpha)(X-\alpha_2) = X^2 - 2\sqrt{2}X - 1 \Rightarrow K = \mathbb{Q}(\sqrt{2})$$

ou

$$Q(X) = (X-\alpha)(X-\alpha_3) = (X^2 - 2\sqrt{3}X + 1) \Rightarrow K = \mathbb{Q}(\sqrt{3})$$

ou

$$Q(X) = (X-\alpha)(X-\alpha_4) = (X^2 - 5 - 2\sqrt{6}) \Rightarrow K = \mathbb{Q}(\sqrt{6}) \ .$$

Fiche IV exercice 4 : a) Soit $f(X)$ le polynôme minimal de $\alpha := \sqrt{2+\sqrt{2}}$ sur $\mathbb{Q}$. Comme α est de degré 2 sur $\mathbb{Q}(\sqrt{2})$, α est de degré 4 sur $\mathbb{Q}$. On a : $f(X) = X^4 - 4X^2 + 2$.

b) Les racines de $f(X)$ sont $\pm\sqrt{2 \pm \sqrt{2}}$. Or, $\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}$ donc $\mathbb{Q}(\alpha)$ contient déjà toutes les racines de $f(X)$. En particulier tout plongement de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$ est un automorphisme de $\mathbb{Q}(\alpha)$.

c) Soit σ l'automorphisme de $\mathbb{Q}(\alpha)$ tel que $\sigma(\alpha) = \sqrt{2-\sqrt{2}}$. Alors $\mathrm{Aut}(\mathbb{Q}(\alpha)) = \{\mathrm{Id}, \sigma, \sigma^2, \sigma^3\} \simeq \mathbb{Z}/4\mathbb{Z}$.

Fiche IV exercice 5 : Soit $K \subseteq L$ une extension finie de corps. On suppose que $L = K(x, y)$ avec y séparable sur K. On note P_x, P_y les polynômes minimaux de x et y sur K. Notons $x_1, ..., x_p$, $y_1, ..., y_q$ les racines distinctes de P_x et P_y dans Ω, un corps de décomposition de P_x, P_y). On suppose que $x_1 = x$ et $y_1 = y$. Comme P_y est séparable, toutes ses racines sont simples donc :

$$P_y = (X - y_1)...(X - y_q) \ .$$

Si K est infini, on choisit

$$t \in K \ \setminus \ \{\frac{x_i - x_{i'}}{y_j - y_{j'}} \ : \ 1 \leq i, i' \leq p, 1 \leq j \neq j' \leq q\} \ .$$

Alors les $x_i + ty_j$ sont des nombres deux à deux distincts.

b) On pose $z := x + ty$ et $R(X) := P_x(z - tX) \in K(z)[X]$. Alors le pgcd de $R(X)$ et $P_y(X)$ est le même calculé dans $\Omega[X]$ et dans $K(z)[X]$. Or dans Ω, la

seule racine commune à $R(X)$ et $P_y(X)$ est y. Donc $X-y$ est le pgcd de $R(X)$ et $P_y(X)$. En particulier, $X - y \in K(z)[X]$ et $y \in K(z) \Rightarrow K(x, y) = K(z)$.

Fiche IV exercice 6 : Soit L/K une extension finie de la forme $L = K(x)$. Soit M un corps tel que $K \subseteq M \subseteq L$. Soit $P(X)$ le polynôme minimal de x sur K et soit $Q(X)$ le polynôme minimal de x sur M. Alors $Q(X) \in M[X]$ et $Q(X)|P(X)$ sur M. En particulier si on note Ω une extension de L où $P(X)$ est scindé, on voit qu'il n'y a qu'un nombre fini de diviseurs $Q(X)$ possibles. Notons M' le sous-corps de L engendré par K et les coefficients de $Q(X)$. Alors $M' \subseteq M$. De plus $Q(X)$ est irréductible sur M donc sur M'. Donc $Q(X)$ est aussi le polynôme minimal de x sur M'. Donc :

$$M' \subseteq M \subseteq L \text{ et } [L : M] = [L : M'] = \deg Q(X)$$

donc $M = M'$.

Il n'y a donc qu'un nombre fini de corps intermédiaires M possibles.

Réciproque : supposons que L/K est une extension algébrique telle qu'il n'existe qu'un nombre fini de corps intermédiaires $K \subseteq M \subseteq L$.

Si $[L : K]$ n'était pas fini, alors on pourrait construire par récurrence une suite $x_1, ..., x_n, ...$ d'éléments de L tels que $x_{n+1} \notin K(x_1, ..., x_n)$ pour tout n : *absurde !*

Donc $[L : K]$ est fini.

Si K est fini, L aussi donc $L^\times$ est un groupe cyclique. Il est clair qu'un générateur de $L^\times$ engendre aussi L.

Soient $x, y \in L$. Si K est infini. Il existe un nombre fini de corps de la forme $K(x + \lambda y), \lambda \in K$. Donc, il existe $\lambda \neq \lambda' \in K$ tels que

$$K(x + \lambda y) = K(x + \lambda' y) \ .$$

On a alors $y = \frac{x+\lambda' y-(x+\lambda y)}{\lambda'-\lambda} \in K(x + \lambda y$. Donc $K(x, y) = K(x + \lambda y)$.

Or $[L : K]$ est fini. Il existe donc $x_1, ...x_n \in L$ tels que $L = K(x_1, ..., x_n)$. Par récurrence sur n, on peut passer de n générateurs à $n-1$ puis à $n-2$,..., puis à un seul : on voit qu'il existe $z \in L$ tel que $K(z) = L$.