Corrigé de l'exercice 4 de la fiche 3

On considère $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\alpha = (2+\sqrt{2})(3+\sqrt{6})$.

1. a. $[K:\mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] \times [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$. (On avait vérifié que dans la première fiche que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ et donc qu $[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$.)
   Le corps K est le corps des racines sur $\mathbb{Q}$ du polynôme $(X^2-2)(X^2-3)$ donc $K/\mathbb{Q}$ est une extension galoisienne de degré 4.

   b. Le groupe $G_{K/\mathbb{Q}(\sqrt{2})}$ est d'ordre 2 et est évidemment engendré par l'unique $\mathbb{Q}(\sqrt{2})$-automorphisme τ_1 qui envoie $\sqrt{3}$ sur $-\sqrt{3}$. De même le groupe $G_{K/\mathbb{Q}(\sqrt{2})}$ est engendré par l'unique $\mathbb{Q}(\sqrt{3})$-automorphisme τ_2 qui envoie $\sqrt{2}$ sur $-\sqrt{2}$. Alors τ_1 et τ_2 engendrent un sous-groupe de $G_{K/\mathbb{Q}}$ d'ordre strictement supérieur à 2. Ils engendrent donc $G_{K/\mathbb{Q}}$.

2. a. On a $\tau_1(\alpha) = (2+\sqrt{2})(3-\sqrt{6})$, $\tau_2(\alpha) = (2-\sqrt{2})(3-\sqrt{6})$ et $\tau_2\tau 1(\alpha) = (2-\sqrt{2})(3+\sqrt{6})$. On vérifie facilement que α et les trois nombres ci-dessus sont deux à deux distincts. (Par exemple si on avait $2+\sqrt{2})(3+\sqrt{6}) = (2-\sqrt{2})(3-\sqrt{6})$ alors $(2+\sqrt{2})^2/2 = (3+\sqrt{6})^2/3$ ce qui entrainerait que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.)

   b. L'élément $\alpha \in K$ a quatre conjugués sur $\mathbb{Q}$ et comme $[K:\mathbb{Q}] = 4$, on en déduit que α est un élément primitif de K sur $\mathbb{Q}$.

   c. Le polynôme minimal de $3+\sqrt{6}$ sur $\mathbb{Q}$ est égal à

$$Q(X) = (X-(3+\sqrt{6}))(X-(3-\sqrt{6})) = X^2 - 6X + 3.$$

   Donc α est racine de $Q\left(\dfrac{X}{2+\sqrt{2}}\right)$ et son polynôme minimal sur $\mathbb{Q}(\sqrt{2})$ est égal à

$$S(X) = (2+\sqrt{2})^2 Q\left(\frac{X}{2+\sqrt{2}}\right) = X^2 - 6(2+\sqrt{2})X + 3(6+4\sqrt{2}).$$

   Le polynôme minimal $P(X)$ de α sur $\mathbb{Q}$ est alors :

$$P(X) = S(X) \cdot \tau_2(S(X)) = X^4 - 24X^3 + 108X^2 - 144X + 36.$$

3. On a $\alpha \times \tau_1(\alpha) = (2+\sqrt{2})(3+\sqrt{6})(2+\sqrt{2})(3-\sqrt{6}) = (2+\sqrt{2})^2\sqrt{3}^2 \in K^2$. Mais $K^{\langle\tau_1\rangle} = \mathbb{Q}(\sqrt{2})$, et si $\alpha \times \tau_1(\alpha)$ est un carré dans ce corps alors $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, ce qui est faux.
   On fait un raisonnement similaire pour τ_2 et $\tau_1\tau_2$.

4. a. Supposons que $\theta \in K$, alors pour $\sigma \in G$ non trivial, on a $\alpha \times \sigma(\alpha) = \theta^2 \times \sigma(\theta)^2 = (\theta \times \sigma(\theta))^2$. Puisque σ est d'ordre 2, il suit que $\theta \times \sigma(\theta) \in K^{\langle\sigma\rangle}$ et donc une contradiction avec la question précédente.

   b. Comme $\theta \notin K$ et $\theta^2 = \alpha \in K$, $L \supseteq K$ et $[L:K] = 2$. D'où $[L:\mathbb{Q}] = [L:K][K:\mathbb{Q}] = 8$.

   c. Rappelons que le polynôme minimal de α sur $\mathbb{Q}$ est égal à

$$P(X) = S(X) \cdot \tau_2(S(X)) = X^4 - 24X^3 + 108X^2 - 144X + 36.$$

   Donc f est obtenu en posant :

$$f(X) = P(X^2) = X^8 - 24X^6 + 108X^4 - 144X^2 + 36.$$

   Les racines de f sont alors $\pm\sqrt{\alpha'}$ où α' parcourt les conjugués de α.

d. On montre que tous les conjugués de θ sur $\mathbb{Q}$ sont dans L. Soit θ' un de ces conjugués, alors $\theta' = \pm\sqrt{\sigma(\alpha)}$ avec $\sigma \in G$. Maintenant, on a $(\theta\theta')^2 = \alpha \times \sigma(\alpha) = {\beta_\sigma}^2$ pour un certain $\beta_\sigma \in K$ par la question précédente. D'où il suit que $\theta\theta' = \pm\beta_\sigma \in K$ et donc $\theta' \in L$.

5. a. Il suffit de prendre $\sigma = \tau_{|K}$.

   b. Supposons pour commencer que σ n'est pas trivial. On a $\theta\tau(\theta) = \beta_\sigma$ (en choisissant β_σ de telle manière que le signe soit positif), mais $\beta_\sigma \in K \setminus K^{\langle\sigma\rangle}$ puisque $\alpha \times \sigma(\alpha)$ n'est pas un carré dans $K^{\langle\sigma\rangle}$, d'où le résultat.
   Si $\sigma = 1$, alors $(\theta\tau(\theta))^2 = \alpha\sigma(\alpha) = \alpha^2$, donc $\theta\tau(\theta) = \pm\alpha$ et le résultat suit.

   c. $L^{\langle\tau\rangle}$ contient $K^{\langle\sigma\rangle}$ et aussi $\theta\tau(\theta)$ puisque τ est d'ordre 2, don $L^{\langle\tau\rangle} \supseteq K$ par la question précédente. On conclut en comparant les degrés.

6. a. La question précédente montre que L a une unique sous-extension d'indice 2 donc, par la correspondance de Galois, G a un unique sous-groupe d'ordre 2, c'est-à-dire un unique élément d'ordre 2. Le K-automorphisme ν qui envoie θ sur $-\theta$ est clairement cet élément.

   b. Le groupe G a au moins trois sous-groupes d'ordre 4 puisque L a trois sous-extensions quadratiques (les extensions $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\sqrt{6})$). Puisque G a un seul élément ν d'ordre 2, ces trois sous-groupes sont cycliques, engendrés par μ_1, μ_2 et μ_3 avec $\mu_i^2 = \nu$ pour $i = 1, 2, 3$. Le groupe G est alors le groupe $\mathbb{H}_8$ des quaternions :

$$\mathbb{H}_8 = \langle i, j, k : i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j\rangle.$$