1. On se propose de montrer que l'extension de corps $\mathbb{Q}(\sqrt{(2 + \sqrt{2})(3 + \sqrt{6})})/\mathbb{Q}$ est galoisienne avec pour groupe de Galois le groupe Q des quaternions (i.e., Q est le groupe ayant huit éléments $1, s_i, s_j, s_k, t, ts_i, ts_j, ts_k$, où t est central, $t^2 = 1$, et $s_i^2 = s_j^2 = s_k^2 = s_i s_j s_k = t$).

(1) Posons $\alpha = (2 + \sqrt{2})(3 + \sqrt{6})$, et soit $K = \mathbb{Q}(\alpha)$: expliquer pourquoi l'extension $K/\mathbb{Q}$ est galoisienne de groupe de Galois produit de deux groupes cycliques d'ordre 2. On notera $\sigma_i, \sigma_j, \sigma_k \in \text{Gal}(K/\mathbb{Q})$ les trois éléments non triviaux.

(2) Montrer que pour chaque $\sigma = \sigma_i, \sigma_j, \sigma_k$ la quantité $\sigma(\alpha)/\alpha$ est le carré d'un élément de K que l'on précisera.

(3) Soit $\delta = \sqrt{\alpha}$ et $L = \mathbb{Q}(\delta)$. Montrer que $\delta \notin K$ (on pourra utiliser la question précédente). Quel est le groupe de Galois de L/K ? On note τ son générateur, qu'on considérera également comme un élément de $\text{Gal}(L/\mathbb{Q})$ (dont $\text{Gal}(L/K)$ est un sous-groupe).

(4) Définir des automorphismes $\tilde{\sigma}_i$ et $\tilde{\sigma}_j$ de $L = K(\sqrt{\alpha})$ sur $\mathbb{Q}$ qui prolongent σ_i et σ_j respectivement. On posera $\tilde{\sigma}_k = \tilde{\sigma}_i \tilde{\sigma}_j$.

(5) Calculer la loi de groupe et conclure.

2. On fait agir $C_4 = \mathbb{Z}/4\mathbb{Z}$ sur $\mathbb{R}^2$ en envoyant un générateur sur $\sigma : (x, y) \mapsto (-y, x)$ la rotation d'angle $\frac{\pi}{2}$ autour de l'origine. Cette action linéaire définit une action de C_4 sur $\mathbb{R}[x, y]$ (donnée par $x^\sigma = -y$ et $y^\sigma = x$). Déterminer explicitement le corps $K = \mathbb{R}(x, y)^{C_4}$ des invariants de $\mathbb{R}(x, y)$ sous cette action (on pourra par exemple commencer par trouver les invariants sous le sous-groupe $\{1, \sigma^2\}$ sous une forme qui rende facile l'action de σ). On montrera qu'il est transcendant pur sur $\mathbb{R}$.

(†) Plus généralement, en considérant l'action du groupe cyclique $C_n = \mathbb{Z}/n\mathbb{Z}$ d'ordre n sur $\mathbb{R}^2$ par rotation d'angle $\frac{2\pi}{n}$ autour de l'origine, montrer que le corps $K_n = \mathbb{R}(x, y)^{C_n}$ des invariants est transcendant pur sur $\mathbb{R}$. (On pourra commencer par le cas où n est pair.)

3. (†) Soit $P \in \mathbb{Z}[t]$ unitaire irréductible de degré 7, dont on note $\theta_1, \dots, \theta_7$ les racines. On considère le polynôme résolvant $R(t) \in \mathbb{Z}[t]$ produit des $t - \theta_i - \theta_j - \theta_k$ (de degré $C_7^3 = 35$) où $\{i, j, k\}$ parcourt les parties de $\{1, \dots, 7\}$ de cardinal 3 avec $i < j < k$. On suppose que R se factorise comme produit d'un polynôme de degré 7 et d'un polynôme de degré 28 irréductibles. Montrer que le groupe de Galois de P est isomorphe à $PSL_3(\mathbb{F}_2)$ (qui s'écrit encore $PSL_2(\mathbb{F}_7)$, l'unique groupe simple de cardinal 168). *Exemple* : Si $P(t) = t^7 - 7t^3 + 14t^2 - 7t + 1$ alors $R(t)$ est produit de $t^7 - 14t^4 + 7t^3 + 14t^2 - 56t - 32$ par un polynôme de degré 28 tous deux étant irréductibles, donc le groupe de Galois de P est $PSL_2(\mathbb{F}_7)$ (c'est apparemment l'exemple le plus simple de ce cas).

Motivations : L'exercice 1 est l'exemple classique (apparemment dû à Dirichlet) d'une extension des rationnels dont le groupe de Galois est celui des quaternions. Il est un problème ouvert de savoir si tout groupe fini est un groupe de Galois sur les rationnels, mais on sait (de façon non constructive) que c'est vrai pour tout groupe fini résoluble. L'exercice 2 donne quelques situations où il n'est pas évident *a priori* (cela ne résulte pas, par exemple, du lemme de Fischer, cf. exercice 2 de la feuille n°8) que le corps des invariants sera transcendant pur. Enfin, l'exercice 3 n'est pas gratuit : c'est effectivement l'algorithme standard pour calculer le groupe de Galois d'un polynôme irréductible du septième degré que de former le résolvant indiqué ici et d'étudier sa factorisation. En outre, ceci donne un exemple (assez compliqué à réaliser, il faut l'admettre) de groupe de Galois simple autre que le groupe alterné $\mathfrak{A}_5$.