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 $s_i^2 = s_j^2 = s_k^2 = s_is_js_k = t$).

(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 $\sigma_i, \sigma_j, \sigma_k \in \mathrm{Gal}(K/\mathbb{Q})$ 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 $\mathrm{Gal}(L/\mathbb{Q})$ (dont $\mathrm{Gal}(L/K)$ 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.

Corrigé. (1) Tout d'abord, $K' = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ est bien de degré 4 sur $\mathbb{Q}$ avec pour groupe de Galois le produit de deux groupes cycliques (en envoyant $\sqrt{2}$ sur $\pm\sqrt{2}$ et $\sqrt{3}$ sur $\pm\sqrt{3}$, ce qui fait quatre possibilités) : en effet, $\sqrt{3}$ n'appartient pas à $\mathbb{Q}(\sqrt{2})$ (cf. aussi l'exercice 3 du partiel du 2005-04-08). On notera $\sigma_i \in \mathrm{Gal}(K'/\mathbb{Q})$ l'automorphisme envoyant $\sqrt{2}$ sur $-\sqrt{2}$ et $\sqrt{3}$ sur $-\sqrt{3}$ et $\sigma_j \in \mathrm{Gal}(K'/\mathbb{Q})$ envoyant $\sqrt{3}$ sur $-\sqrt{3}$ et fixant $\sqrt{2}$, et naturellement $\sigma_k = \sigma_i\sigma_j$ envoyant $\sqrt{2}$ sur $-\sqrt{2}$ et fixant $\sqrt{3}$.

Reste à s'assurer que $K = K'$, l'inclusion $K \subseteq K'$ étant claire ; il s'agit donc simplement de vérifier que le degré de K sur $\mathbb{Q}$ est bien 4 (et pas 1 ou 2). Or on a $\sigma_i(\alpha) = (2-\sqrt{2})(3+\sqrt{6})$ et $\sigma_j(\alpha) = (2+\sqrt{2})(3-\sqrt{6})$, qui sont manifestement distincts de α, donc α a quatre conjugués sous l'action de Galois et ainsi $[K : \mathbb{Q}] = 4$ avec groupe de Galois $\{\mathrm{id}, \sigma_i, \sigma_j, \sigma_k\}$ produit de deux groupes cycliques d'ordre 2.

(2) On a $\sigma_i(\alpha)/\alpha = \frac{2-\sqrt{2}}{2+\sqrt{2}} = \frac{1}{2}(2-\sqrt{2})^2$ qui est le carré de $-1+\sqrt{2}$ dans K. De même, $\sigma_j(\alpha)/\alpha = \frac{3-\sqrt{6}}{3+\sqrt{6}} = \frac{1}{3}(3-\sqrt{6})^2$ est le carré de $-\sqrt{2}+\sqrt{3}$ dans K. Conséquemment, $\sigma_k(\alpha)/\alpha$ peut alors s'écrire comme $\sigma_i(\sigma_j(\alpha)/\alpha)\cdot(\sigma_i(\alpha)/\alpha)$, qui est donc le carré de $(\sqrt{2}-\sqrt{3})(-1+\sqrt{2})$.

(3) Comme $\delta = \sqrt{\alpha}$ et $L = K(\delta)$, il s'agit de vérifier que α n'est pas un carré dans K, ce qui assurera que $\delta \notin K$ donc $[L : K] = 2$ avec groupe de Galois cyclique d'ordre 2. Mais si on avait $\delta \in K$, on pourrait lui appliquer, disons, σ_i, et on aurait $\sigma_i^2(\delta) = \delta$ (puisque σ_i est un automorphisme d'ordre 2 de K sur $\mathbb{Q}$) : en particulier, $\sigma_i(\sigma_i(\delta)/\delta)\cdot(\sigma_i(\delta)/\delta) = 1$. Mais $\sigma_i(\delta)/\delta$ doit être une racine carrée de $\sigma_i(\alpha)/\alpha$, et d'après la question précédente, c'est donc $-1+\sqrt{2}$ ou $1-\sqrt{2}$; or $\sigma_i(-1+\sqrt{2})\cdot(-1+\sqrt{2}) = -1$ et pareil pour $1-\sqrt{2}$, ce qui est une contradiction : c'est donc que α n'est pas un carré dans K.

On a donc posé $\tau \in \mathrm{Gal}(L/K) \leq \mathrm{Gal}(L/\mathbb{Q})$ qui envoie δ sur $-\delta$ (et fixe tous les éléments de K).

(4) Définissons $\tilde\sigma_i$ sur L par $\tilde\sigma_i(x+y\delta) = \sigma_i(x)+(-1+\sqrt{2})\,\sigma_i(y)\,\delta$. La $\mathbb{Q}$-linéarité de $\tilde\sigma_i$ est évidente, ainsi que le fait que $\tilde\sigma_i(az) = \sigma_i(a)\,\tilde\sigma_i(z)$ si $a \in K$ et $z \in L$. Le point restant à vérifier pour que $\tilde\sigma_i$ soit un morphisme de corps est alors que $\tilde\sigma_i(\delta z) = \tilde\sigma_i(\delta)\,\tilde\sigma_i(z)$ si $z \in L$, et cela même se ramène au cas $z = \delta$, donc tout revient à voir que $\sigma_i(\alpha) = (-1+\sqrt{2})^2\,\alpha$, et cela a été fait à la question (2). De même on définit $\tilde\sigma_j$ sur L par $\tilde\sigma_i(x+y\delta) = \sigma_i(x)+(-\sqrt{2}+\sqrt{3})\,\sigma_i(y)\,\delta$, qui pour les mêmes raisons est un automorphisme de corps de L sur $\mathbb{Q}$, et enfin on pose $\tilde\sigma_k = \tilde\sigma_i\tilde\sigma_j$, qui envoie $x+y\delta$ sur $\sigma_k(x)+(\sqrt{2}-\sqrt{3})(-1+\sqrt{2})\,\sigma_k(y)\,\delta$.

(5) Il découle immédiatement de la définition de $\tilde\sigma_i, \tilde\sigma_j, \tilde\sigma_k$ que τ commute à eux. De plus,

$\sigma_i(-1+\sqrt{2})\cdot(-1+\sqrt{2})=-1$ donne immédiatement $\tilde{\sigma}_i^2=\tau$, et de même $\tilde{\sigma}_j^2=\tau$ et $\tilde{\sigma}_k^2=\tau$. Avec $\tilde{\sigma}_k=\tilde{\sigma}_i\tilde{\sigma}_j$, on a bien trouvé le groupe Q des quaternions. Et puisque $[L:\mathbb{Q}]=[L:K]\cdot[K:\mathbb{Q}]=8$, tous les automorphismes de L ont été trouvés : c'est bien que $\mathrm{Gal}(L/\mathbb{Q})=Q$. ✓

2. On fait agir $C_4=\mathbb{Z}/4\mathbb{Z}$ sur $\mathbb{R}^2$ en envoyant un générateur sur $\sigma\colon(x,y)\mapsto(-y,x)$ 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.)

Corrigé. Posons $\tau=\sigma^2$. On a manifestement $\mathbb{R}[x,y]^{\{1,\tau\}}=\mathbb{R}[x^2,xy,y^2]$. Son corps des fractions peut s'écrire, par exemple, $\mathbb{R}(x,y)^{\{1,\tau\}}=\mathbb{R}(x^2+y^2,\frac{y}{x})$: en effet, si $d=x^2+y^2$ et $r=\frac{y}{x}$, on a bien d et r invariants par $\tau=\sigma^2$, et $x^2=\frac{d}{1+r^2}$ et $xy=\frac{dr}{1+r^2}$ et $y^2=\frac{dr^2}{1+r^2}$, de sorte que $\mathbb{R}[x,y]^{\{1,\tau\}}=\mathbb{R}(x^2,xy,y^2)$ est bien contenu dans $\mathbb{R}(d,r)$, et il y a égalité. De plus, comme le degré de transcendance est 2, les quantités d et r sont algébriquement indépendantes.

À présent, l'action de σ sur $\mathbb{R}(d,r)$ est donnée par $d\mapsto d$ et $r\mapsto-\frac{1}{r}$. Tout se ramène donc à l'étude du corps $\mathbb{R}(r)^{\{1,\bar{\sigma}\}}$ des invariants de $\mathbb{R}(r)$ par $\bar{\sigma}\colon r\mapsto-\frac{1}{r}$. Or on voit bien que $t=\frac{2r}{1-r^2}$ (le 2 est introduit uniquement pour évoquer la formule donnant $\tan(2\theta)$ en fonction de $\tan\theta$) est invariant : et comme r s'écrit comme solution d'une équation de degré 2 sur $\mathbb{R}(t)$ (à savoir $tr^2+2r-t=0$) et que $\mathbb{R}(r)$ est de degré justement 2 sur $\mathbb{R}(r)^{\{1,\bar{\sigma}\}}$ (car le groupe de Galois est $\{1,\bar{\sigma}\}$), on a bien $\mathbb{R}(r)^{\{1,\bar{\sigma}\}}=\mathbb{R}(t)$. Ainsi, $K=\mathbb{R}(x,y)^{C_4}=\mathbb{R}(d,r)^{\{1,\bar{\sigma}\}}=\mathbb{R}(d,t)$ où $d=x^2+y^2$ et $t=\frac{2xy}{x^2-y^2}$, ces quantités étant algébriquement indépendantes.

Considérons à présent l'action de $C_n=\mathbb{Z}/n\mathbb{Z}$ sur $\mathbb{R}^2$ par rotation d'angle $\frac{2\pi}{n}$.

Si n est pair, disons $n=2m$, le même raisonnement que ci-dessus s'applique : on considère le sous-groupe $\{1,\tau\}$ avec $\tau=\sigma^m$, de sorte que les invariants sous $\{1,\tau\}$ s'écrivent $\mathbb{R}(d,r)$ avec $d=x^2+y^2$ et $r=\frac{y}{x}$. Or en écrivant $t=R_m(r)$ où R_m est la fraction rationnelle telle que $R_m(\tan\theta)=\tan(m\theta)$ (qui se définit facilement par récurrence sur m), dont le numérateur et le dénominateur sont de degré $\leq m$, on a pour les mêmes raisons que précédemment $K_n=\mathbb{R}(x,y)^{C_n}=\mathbb{R}(d,t)$, toujours transcendant pur sur $\mathbb{R}$.

À présent, si n est impair, on vient d'expliquer qu'on peut écrire $K_{2n}=\mathbb{R}(x,y)^{C_{2n}}=\mathbb{R}(d,t)$, l'extension $\mathbb{R}(d,t)\subseteq\mathbb{R}(x,y)$ étant galoisienne de groupe de Galois C_{2n}. Le corps K_n recherché est le corps fixe de $\mathbb{R}(x,y)$ sous le groupe $C_n\leq C_{2n}$ engendré par σ^2, et il est de degré 2 sur $\mathbb{R}(d,t)$: on cherche donc à extraire une unique racine carrée. À présent, remarquons que $t=R_n(r)=R_n(y/x)$ s'écrit encore $P_n(x,y)/Q_n(x,y)$ où Q_n,P_n sont des polynômes homogènes de degré n exprimant $\cos(n\theta)$ et $\sin(n\theta)$ respectivement en fonction de $\cos\theta$ et $\sin\theta$, avec, donc, $P_n(x,y)^2+Q_n(x,y)^2=d^n$. Il s'ensuit que $\frac{d}{1+t^2}=\frac{P_n^2}{d^{n-1}}$ est un carré dans $\mathbb{R}(x,y)$, et c'est le carré d'un élément $\frac{P_n}{d^{(n-1)/2}}$ invariant par C_n mais pas par C_{2n} : donc $K_n=\mathbb{R}(\sqrt{\frac{d}{1+t^2}},t)$ (remarquer que $d=(1+t^2)\sqrt{\frac{d}{1+t^2}}^2$ de sorte qu'on peut bien retirer la variable d), et il est bien trancendant pur puisque engendré par deux éléments. ✓

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).

Corrigé. Il s'agit d'un exercice de théorie des groupes. Soit G le groupe de Galois de P et $\Theta = \{\theta_i\}$ l'ensemble des racines (donc $\operatorname{card}\Theta = 7$) : on a une action fidèle et transitive de G sur Θ. Comme le corps de décomposition de P décompose également R (par construction !), le groupe de Galois G doit opérer transitivement sur les racines de chaque facteur irréductible de R. Autrement dit : on a une action fidèle et transitive d'un groupe G sur un ensemble Θ de cardinal 7, on suppose que l'action de G sur l'ensemble $\mathscr{P}_3(\Theta)$ des parties à trois éléments de Θ a exactement deux orbites, dont une, qu'on notera $\mathscr{C}$, a cardinal 7 et l'autre a (donc) cardinal 28, et on souhaite déterminer G.

L'action de G sur Θ étant fidèle, on peut considérer G comme un sous-groupe de tout le groupe $\mathfrak{S}(\Theta)$ des permutations sur Θ ; comme $\operatorname{card} G$ est multiple de 7 (puisque Θ est l'unique orbite et qu'elle a cardinal 7), on voit que G doit contenir un élément d'ordre 7, qui est manifestement un 7-cycle. Quitte à renommer les éléments de Θ, on peut supposer que $\Theta = \{0, \dots, 6\}$, qu'on identifiera à $\mathbb{Z}/7\mathbb{Z}$, et que G contient le 7-cycle $0 \mapsto 1 \mapsto 2 \mapsto \cdots \mapsto 6 \mapsto 0$, qu'on appellera σ (soit $\sigma\colon k \mapsto k+1$).

L'action de σ (c'est-à-dire de $\langle\sigma\rangle \cong \mathbb{Z}/7\mathbb{Z}$ par translation) sur $\mathscr{P}_3(\Theta)$ a cinq orbites (chacune de cardinal 7), comme on le voit facilement : à savoir celles de $\{0,1,6\}$, $\{0,2,5\}$, $\{0,3,4\}$, $\{0,1,5\}$ et $\{0,2,6\}$. Cherchons à déterminer ce que peut être $\mathscr{C}$.

Montrons d'abord par l'absurde que $\mathscr{C}$ ne peut pas être l'orbite de $\{0,1,6\}$ (c'est-à-dire : $\{\{0,1,6\},\{0,1,2\},\{1,2,3\},\{2,3,4\},\{3,4,5\},\{4,5,6\},\{0,5,6\}\}$). Pour cela, soit $\varphi \in G \leq \mathfrak{S}(\Theta)$ une permutation qui laisse invariante cette orbite, et on se propose de montrer que φ est soit une puissance de σ soit une puissance de σ composée avec $\tau\colon k \mapsto -k$ (ou, si on veut, φ appartient au groupe diédral évident). Nous dirons que deux éléments de Θ sont « adjacents » lorsque l'un des eux est envoyé sur l'autre par σ (donc chaque élément de Θ est adjacent à exactement deux autres). D'après l'hypothèse, $\{\varphi(0), \varphi(1), \varphi(6)\}$ a deux paires d'éléments adjacents (comme tout élément de l'orbite de $\{0,1,6\}$ sous σ) : donc soit $\varphi(0)$ et $\varphi(1)$ sont adjacents soit $\varphi(0)$ et $\varphi(6)$ le sont, et ce dernier cas se ramène au premier quitte à remplacer φ par $\varphi\sigma$. Bref, mettons que $\varphi(0)$ et $\varphi(1)$ soient adjacents : alors, comme $\varphi(\{0,1,2\})$ doit encore être dans l'orbite, $\varphi(2)$ est l'unique élément de Θ adjacent à $\varphi(1)$ qui n'est pas $\varphi(0)$, puis $\varphi(3)$ est l'unique élément de Θ adjacent à $\varphi(2)$ qui n'est pas $\varphi(1)$, et ainsi de suite. Ceci prouve bien l'affirmation voulue : si on se ramène (quitte à composer par la bonne puissance de σ) à $\varphi(0) = 0$, on a soit $\varphi = \mathrm{id}_\Theta$ (si $\varphi(1) = 1$) soit $\varphi(k) = 6 - k$ (si $\varphi(1) = 6$). Mais alors on a prouvé que tout élément φ de G est contenu dans le groupe diédral de l'heptagone, D_7, engendré par $\sigma\colon k \mapsto k+1$ et $\tau\colon k \mapsto -k$: or l'action de D_7 sur $\mathscr{P}_3(\Theta)$ a plus de deux orbites, et on a la contradiction voulue.

À présent, remarquons que les orbites de $\{0,2,5\}$ et de $\{0,3,4\}$ (sous l'action de σ) s'obtiennent comme images de celle de $\{0,1,6\}$ par les permutations $k \mapsto 2k$ et $k \mapsto 3k$ respectivement de Θ. Par conséquent, le même raisonnement que ci-dessus s'applique.

On en déduit que $\mathscr{C}$ est l'orbite de $\{0,1,5\}$ sous l'action de σ (le cas de $\{0,2,6\}$ s'y ramenant en appliquant de nouveau $\tau\colon k \mapsto -k$), et G préserve cette orbite. À présent, identifions Θ à $\mathbb{P}^2(\mathbb{F}_2)$, l'espace (plan projectif) des droites dans $(\mathbb{F}_2)^3$ de la façon suivante : $0 \leftrightarrow (1{:}0{:}0)$, $1 \leftrightarrow (0{:}1{:}0)$, $2 \leftrightarrow (0{:}0{:}1)$, $3 \leftrightarrow (1{:}0{:}1)$, $4 \leftrightarrow (1{:}1{:}1)$, $5 \leftrightarrow (1{:}1{:}0)$, $6 \leftrightarrow (0{:}1{:}1)$. De cette manière, $\mathscr{C}$ est bien l'ensemble des droites projectives de $\mathbb{P}^2(\mathbb{F}_2)$, et comme G préserve cette

structure, on a $G \leq PSL_3(\mathbb{F}_2)$.

Or $\operatorname{card} G$ vaut au moins 28 (puisqu'il est censé agir transitivement sur l'ensemble $\mathscr{P}_3(\Theta) \setminus \mathscr{C}$, qui a 28 éléments), et il est « bien connu » que les ordres possibles d'un sous-groupe de $PSL_3(\mathbb{F}_2)$ sont 1, 2, 3, 4, 6, 7, 8, 12, 21, 24 et 168. Il s'ensuit que $G = PSL_3(\mathbb{F}_2)$. Si on ne veut pas admettre ce fait sur les ordres des sous-groupes de $PSL_3(\mathbb{F}_2)$, on peut également remarquer que si σ est la matrice (inversible d'ordre 7) $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \in \mathbb{M}_3(\mathbb{F}_2)$ et si ψ est une des six matrices dont les lignes sont $(\,0 \quad 1 \quad 0\,)$, $(\,0 \quad 0 \quad 1\,)$ et $(\,1 \quad 1 \quad 1\,)$ (les ordres possibles de ψ étant 2, 3 ou 4), alors σ et ψ engendrent tout $PSL_3(\mathbb{F}_2)$ (la vérification dans chaque cas est sans difficulté, quoique l'ensemble soit assez fastidieux) ; or $\sigma \in G$ par hypothèse, et il existe au moins un des six ψ possibles qui est dans G puisque G est censé contenir un élément envoyant $\{(1{:}0{:}0), (0{:}1{:}0), (0{:}0{:}1)\} \in \mathscr{P}_3(\Theta) \setminus \mathscr{C}$ sur $\{(0{:}1{:}0), (0{:}0{:}1), (1{:}1{:}1)\} \in \mathscr{P}_3(\Theta) \setminus \mathscr{C}$. ✓

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 $\mathfrak{A}_5$.