1. Exprimer les racines des polynômes suivants (on indiquera une éventuelle simplification), puis calculer leurs groupes de Galois sur $\mathbb{Q}$: (a) $t^4 - 4t^2 = 0$, (b) $t^4 - 4t^2 - 45 = 0$, (c) $t^4 - 4t^2 - 5 = 0$, (d) $t^4 - 4t^2 - 1 = 0$, (e) $t^4 - 4t^2 + 2 = 0$ et (f) $t^4 - 4t^2 + 1 = 0$.

Corrigé. Il s'agit d'équation biquadratiques : les racines sont donc : (a) 0 et ± 2 (le polynôme se factorise comme $t^2(t-2)(t+2)$), (b) ± 3 et $\pm\sqrt{-5}$ (le polynôme se factorise comme $(t-3)(t+3)(t^2+5)$), (c) $\pm\sqrt{5}$ et $\pm\sqrt{-1}$ (le polynôme se factorise comme $(t^2-5)(t^2+1)$), (d) $\pm\sqrt{2\pm\sqrt{5}}$ (le polynôme est irréductible), (e) $\pm\sqrt{2\pm\sqrt{2}}$ (polynôme irréductible) et (f) $\pm\sqrt{2\pm\sqrt{3}}$ (polynôme irréductible).

Calculons maintenant le groupe de Galois sur $\mathbb{Q}$ des corps de décomposition (extensions engendrées par les racines) de ces différents polynômes. Dans le cas (a), les racines sont déjà dans $\mathbb{Q}$, donc le groupe de Galois est trivial. Dans le cas (b), le corps de décomposition est $\mathbb{Q}(\sqrt{-5})$, et le groupe de Galois est donc $\{\mathrm{id}, \tau\} \cong \mathbb{Z}/2\mathbb{Z}$ (avec pour unique élément non trivial l'automorphisme τ qui envoie $\sqrt{-5}$ sur $-\sqrt{-5}$).

Dans le cas (c), on sait qu'on au moins un automorphisme τ qui échange $\sqrt{-1}$ et $-\sqrt{-1}$ en laissant $\pm\sqrt{5}$ fixes (la conjugaison complexe !), et comme par ailleurs l'automorphisme de $\mathbb{Q}(\sqrt{5})$ (sur $\mathbb{Q}$) envoyant $\sqrt{5}$ sur $-\sqrt{5}$ soit se prolonger au corps de décomposition $\mathbb{Q}(\sqrt{5}, \sqrt{-1})$, on en déduit qu'il y aussi un automorphisme τ' qui échange $\sqrt{5}$ et $-\sqrt{5}$ et dont on peut supposer qu'il laisse $\pm\sqrt{-1}$ fixes, et enfin un $\tau'' = \tau\tau'$ qui échange $\sqrt{5}$ et $-\sqrt{5}$ et $\sqrt{-1}$ et $-\sqrt{-1}$. Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\sqrt{5}, \sqrt{-1})/\mathbb{Q})$ est donc $\{\mathrm{id}, \tau, \tau', \tau''\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. (Essentiellement, le seul point à signaler était que les extensions $\mathbb{Q}(\sqrt{-1})$ et $\mathbb{Q}(\sqrt{5})$ ne coïncident pas : donc $\mathbb{Q}(\sqrt{5}, \sqrt{-1})$ est de degré 4 sur $\mathbb{Q}$ comme on le pense, et alors il est clair que le groupe de Galois doit avoir les quatre éléments qui permutent ou ne permutent pas chaque paire $\pm\sqrt{5}$ et $\pm\sqrt{-1}$.)

Dans le cas (d), le corps de décomposition $\mathbb{Q}(\sqrt{2\pm\sqrt{5}}) = \mathbb{Q}(\sqrt{2+\sqrt{5}}, \sqrt{2-\sqrt{5}})$ de $t^4 - 4t^2 - 1 = 0$ possède au moins l'automorphisme non trivial $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2\pm\sqrt{5}})/\mathbb{Q}(\sqrt{2+\sqrt{5}})) \leq \mathrm{Gal}(\mathbb{Q}(\sqrt{2\pm\sqrt{5}})/\mathbb{Q})$ donné par la conjugaison complexe, qui fixe $\sqrt{5}$ et $\sqrt{2+\sqrt{5}}$ et envoie $\sqrt{2-\sqrt{5}}$ sur $-\sqrt{2-\sqrt{5}}$. Par ailleurs, puisque $\mathbb{Q}(\sqrt{2\pm\sqrt{5}})$ est galoisien sur $\mathbb{Q}$ (il est normal et séparable !) il admet au moins un automorphisme $\tilde{\sigma}$ sur $\mathbb{Q}$ qui prolonge l'automorphisme $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ envoyant $\sqrt{5}$ sur $-\sqrt{5}$: cet automorphisme $\tilde{\sigma}$ doit donc envoyer $\sqrt{2+\sqrt{5}}$ sur $\pm\sqrt{2-\sqrt{5}}$, et on voit alors que $\tau' = \tilde{\sigma}^{-1}\tau\tilde{\sigma}$ échange $\sqrt{2+\sqrt{5}}$ et $-\sqrt{2+\sqrt{5}}$ mais laisse $\sqrt{5}$ et $\sqrt{2-\sqrt{5}}$ fixes. On connaît donc déjà au moins $\mathrm{Gal}(\mathbb{Q}(\sqrt{2\pm\sqrt{5}})/\mathbb{Q}(\sqrt{5})) = \{\mathrm{id}, \tau, \tau', \tau''\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ (avec $\tau'' = \tau\tau'$). Quitte à composer $\tilde{\sigma}$ par τ et/ou par τ', on peut alors supposer que $\tilde{\sigma}$ envoie $\sqrt{2+\sqrt{5}}$ sur $\sqrt{2-\sqrt{5}}$ et $\sqrt{2-\sqrt{5}}$ sur $-\sqrt{2+\sqrt{5}}$, auquel cas il est d'ordre 4. Les relations $\tilde{\sigma}^4 = \tau^2 = \tau\tilde{\sigma}\tau\tilde{\sigma} = \mathrm{id}$ témoignent que le groupe de Galois recherché, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2\pm\sqrt{5}})/\mathbb{Q}) = \{\mathrm{id}, \tilde{\sigma}, \tilde{\sigma}^2, \tilde{\sigma}^3, \tau, \tau\tilde{\sigma}, \tau\tilde{\sigma}^2, \tau\tilde{\sigma}^3\}$, est isomorphe au groupe diédral du carré. Remarquons au passage que $\mathbb{Q}(\sqrt{2+\sqrt{5}})$ *n'est pas* galoisien sur $\mathbb{Q}$ puisqu'il est le corps fixe associé au sous-groupe $\{1, \tau\}$ du groupe de Galois de $\mathbb{Q}(\sqrt{2\pm\sqrt{5}})$, lequel sous-groupe n'est pas distingué (on a $\tilde{\sigma}^{-1}\tau\tilde{\sigma} = \tau'$) ; il est cependant galoisien sur $\mathbb{Q}(\sqrt{5})$ (de groupe de Galois $\{1, \tau\} \cong \mathbb{Z}/2\mathbb{Z}$) qui est lui-même galoisien sur $\mathbb{Q}$ (de groupe de Galois $\{1, \sigma\}$).

Passons au cas (e). La différence essentielle avec le cas précédent est que $\sqrt{2-\sqrt{2}}$ appartient à $\mathbb{Q}(\sqrt{2+\sqrt{2}})$: en effet, $(2+\sqrt{2})(2-\sqrt{2}) = 2$ donc $2-\sqrt{2} = \frac{2}{2+\sqrt{2}}$, donc $\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = \frac{\sqrt{2}\sqrt{2+\sqrt{2}}}{2+\sqrt{2}} = (\sqrt{2}-1)\sqrt{2+\sqrt{2}}$ et finalement $\sqrt{2-\sqrt{2}} = -\sqrt{2+\sqrt{2}} + \sqrt{2}\sqrt{2+\sqrt{2}}$. On a donc prouvé $\mathbb{Q}(\sqrt{2\pm\sqrt{2}}) = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ (et cette extension est galoi-

sienne, ce qui est clair sur la forme de gauche, mais surprenant *a priori* sur celle de droite). Appelons $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ l'automorphisme de $\mathbb{Q}(\sqrt{2})$ échangeant $\sqrt{2}$ et $-\sqrt{2}$. Comme $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ est galoisienne, il doit y avoir un automorphisme $\tilde{\sigma}$ de $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ qui prolonge σ : notamment, il envoie $\sqrt{2+\sqrt{2}}$ sur $\sqrt{2-\sqrt{2}}$ ou $-\sqrt{2-\sqrt{2}}$. À présent, observons que $\sqrt{2+\sqrt{2}}$ n'appartient pas à $\mathbb{Q}(\sqrt{2})$: en effet, si $2+\sqrt{2}$ était le carré de $x+y\sqrt{2}$ (avec $x, y \in \mathbb{Q}$), on aurait $x^2+2y^2=2$ et $2xy=1$, donc $x^4-2x^2+\frac{1}{2}=0$ et on vérifie que cette équation n'a pas de solution dans $\mathbb{Q}$; une autre façon de le prouver consiste à remarquer que $\sqrt{2+\sqrt{2}}\,\tilde{\sigma}(\sqrt{2+\sqrt{2}}) = \pm\sqrt{2}$ n'appartient pas à $\mathbb{Q}$, donc $\sqrt{2+\sqrt{2}}$ ne peut pas appartenir à $\mathbb{Q}(\sqrt{2})$ (vu que $x\,\sigma(x) \in \mathbb{Q}$ pour tout $x \in \mathbb{Q}(\sqrt{2})$). Ainsi, l'extension $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ de $\mathbb{Q}(\sqrt{2})$ est bien de degré 2. On peut donc appeler $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}(\sqrt{2})) \leq \mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q})$ l'automorphisme qui fixe $\sqrt{2}$ et échange $\sqrt{2+\sqrt{2}}$ et $-\sqrt{2+\sqrt{2}}$: d'après le calcul effectué ci-dessus, on a $\tau(\sqrt{2-\sqrt{2}}) = -\sqrt{2-\sqrt{2}}$. Et quitte à composer $\tilde{\sigma}$ par τ on peut supposer qu'il envoie $\sqrt{2+\sqrt{2}}$ sur $\sqrt{2-\sqrt{2}}$: alors le même calcul montre que $\tilde{\sigma}(\sqrt{2-\sqrt{2}}) = -\sqrt{2-\sqrt{2}} - \sqrt{2}\sqrt{2-\sqrt{2}} = -\sqrt{2+\sqrt{2}}$. On voit donc que $\tilde{\sigma}$ est d'ordre 4, et le groupe de Galois recherché est $\{\mathrm{id}, \tilde{\sigma}, \tilde{\sigma}^2, \tilde{\sigma}^3\} \cong \mathbb{Z}/4\mathbb{Z}$.

Traitons enfin le cas (f). De nouveau, $\sqrt{2-\sqrt{3}}$ appartient à $\mathbb{Q}(\sqrt{2+\sqrt{2}})$: en effet, $(2+\sqrt{3})(2-\sqrt{3}) = 1$ donc $2-\sqrt{3} = \frac{1}{2+\sqrt{3}}$, donc $\sqrt{2-\sqrt{3}} = \frac{1}{\sqrt{2+\sqrt{3}}} = \frac{\sqrt{2+\sqrt{3}}}{2+\sqrt{3}} = (2-\sqrt{3})\sqrt{2+\sqrt{3}}$ et finalement $\sqrt{2-\sqrt{3}} = 2\sqrt{2+\sqrt{3}} - \sqrt{3}\sqrt{2+\sqrt{3}}$. On a donc prouvé $\mathbb{Q}(\sqrt{2\pm\sqrt{3}}) = \mathbb{Q}(\sqrt{2+\sqrt{3}})$ (de nouveau, cette extension est galoisienne, ce qui est clair sur la forme de gauche, mais surprenant *a priori* sur celle de droite). Mais on a mieux : $\frac{1}{\sqrt{3}}(\sqrt{2+\sqrt{3}} + \sqrt{2-\sqrt{3}}) = \sqrt{2}$, donc $\mathbb{Q}(\sqrt{2\pm\sqrt{3}}) = \mathbb{Q}(\sqrt{2+\sqrt{3}}) = \mathbb{Q}(\sqrt{3},\sqrt{2})$, et on est ramené essentiellement à la situation du cas (c) : dès lors qu'on a vu que $\sqrt{2}$ n'appartient pas à $\mathbb{Q}(\sqrt{3})$, le groupe de Galois recherché s'écrit $\{\mathrm{id}, \tau, \tilde{\sigma}, \tau\tilde{\sigma}\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, où $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{3}})/\mathbb{Q}(\sqrt{3})) \leq \mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{3}})/\mathbb{Q})$ fixe $\sqrt{3}$ et envoie $\sqrt{2}$ ou $\sqrt{2+\sqrt{3}}$ ou $\sqrt{2-\sqrt{3}}$ sur leurs opposés, et $\tilde{\sigma}$ fixe $\sqrt{2}$ et envoie $\sqrt{3}$ sur $-\sqrt{3}$ et échange $\sqrt{2+\sqrt{3}}$ et $\sqrt{2-\sqrt{3}}$. ✓

2. Déterminer le groupe de Galois des équations suivantes sur $\mathbb{Q}$ (on pourra réduire modulo 2, 3 et/ou 5) : (a) $t^4+2t^2+t+3=0$, (b) $t^4+3t^3-3t-2=0$, (c) $t^6+22t^5-9t^4+12t^3-37t^2-29t-15=0$.

Corrigé. (a) En réduisant modulo 2 on trouve le polynôme t^4+t+1, qui est irréductible (car il n'a aucune racine dans $\mathbb{F}_4$ comme on le vérifie immédiatement) donc le polynôme t^4+2t^2+t+3 est lui-même irréductible et il y a un 4-cycle dans son groupe de Galois. En réduisant modulo 3 on trouve le polynôme t^4-t^2+t sur $\mathbb{F}_3$, qui se factorise comme $t(t^3-t+1)$ avec deux facteurs irréductibles (car il n'y a pas d'autre racine), donc il existe un élément d'ordre 3 dans le groupe de Galois qui permute cycliquement les trois racines de t^3-t+1 modulo 3. (On peut aussi réduire modulo 5, et on trouve $t^4+2t^2+t-2=(t+1)(t+2)(t^2+2t-1)$, donc il existe une transposition dans le groupe de Galois.) Le groupe de Galois de t^4+2t^2+t+3 sur $\mathbb{Q}$ est un donc un sous-groupe de $\mathfrak{S}_4$ qui contient un 4-cycle et un 3-cycle, donc c'est $\mathfrak{S}_4$ tout entier.

(b) En réduisant modulo 2 on trouve le polynôme $t^4+t^3+t=t(t^3+t^2+1)$ (et il n'y a pas d'autre racine, donc le second facteur est irréductible) ; en réduisant modulo 3 on trouve $t^4+1=(t^2+t-1)(t^2-t-1)$ (et les deux facteurs sont irréductibles). On en déduit que le polynôme est irréductible (les décompositions en degré 1 plus degré 3 d'une part et degré 2 plus degré 2 de l'autre sont incompatibles), et que son groupe de Galois est $\mathfrak{S}_4$ ou $\mathfrak{A}_4$. Pour éliminer

cette dernière possibilité, il faut soit réduire modulo 5 (alors t^4+3t^3-3t-2 est irréductible, donc il y a un 4-cycle dans le groupe de Galois) soit calculer le discriminant (-2183, qui n'est pas un carré — mais on peut se contenter de le calculer modulo 5, ce qui est sans doute le plus efficace) soit observer qu'il y a exactement deux racines réelles (ce qui fournit un 2-cycle).

(c) La réduction modulo 3 est $t^6+t^5-t^2+t=t(t^5+t^4-t+1)$ et le second facteur n'a pas de racine dans $\mathbb{F}_3$ ni $\mathbb{F}_9$ donc il est irréductible : on en déduit l'existence d'un 5-cycle dans le groupe de Galois. La réduction modulo 5 est $t^6+2t^5+t^4+2t^3-2t^2+t=t(t+1)(t+2)(t-1)(t^2+2)$ (et le dernier facteur est irréductible) : on en déduit l'existence d'une transposition dans le groupe de Galois. Enfin, en réduisant modulo 2, le polynôme $t^6+t^4+t^2+t+1$ n'a pas de racine dans $\mathbb{F}_2$ ni $\mathbb{F}_4$: donc si $t^6+22t^5-9t^4+12t^3-37t^2-29t-15$ était réductible sur les rationnels, ce serait en deux facteurs de degré 3, ce qui est en contradiction avec la réduction modulo 3. Ainsi, le groupe de Galois est un sous-groupe transitif de $\mathfrak{S}_6$ contenant une transposition et un 5-cycle, donc c'est $\mathfrak{S}_6$ tout entier. ✓

3. 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 $\mathbb{Q}(\sqrt{2})$ (ce qui se vérifie directement en cherchant à résoudre $(\alpha+\beta\sqrt{2})^2=3$ avec $\alpha,\beta\in\mathbb{Q}$, mais on l'a déjà vu dans le cas (f) de l'exercice 1 ; 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 distincts sous l'action de Galois (son polynôme minimal — qui a ces conjugués pour racines — est donc bien de degré 4, i.e. $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$) ce qui prouve $K=K'$. 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).

Remarque : Le point important, ici, est que si on compte prolonger $\sigma = \sigma_i, \sigma_j, \sigma_k$ à $L = \mathbb{Q}(\delta)$ (en un automorphisme $\tilde{\sigma} \in \mathrm{Gal}(L/\mathbb{Q})$), on devra faire en sorte que $\frac{\tilde{\sigma}(\delta)}{\delta}$ soit une racine carrée, mettons ε, de $\frac{\sigma(\alpha)}{\alpha}$, et alors cette condition détermine complètement $\tilde{\sigma}$ (ce qui va conduire à la réponse à la question suivante) et permet notamment de s'assurer qu'il n'est pas d'ordre 2 (contrairement à σ).

(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 $\mathrm{Gal}(L/\mathbb{Q}) = Q$. ✓

4. On considère $\mathbb{C}(\lambda)$ le corps des fractions rationnelles en une indéterminée (λ) sur $\mathbb{C}$, et sur ce corps l'équation du cinquième degré $t^5 - \lambda t^2 + \lambda^2 - \lambda = 0$ ($\star$). On se propose de prouver que le groupe de Galois (du corps de décomposition) de cette équation est le groupe symétrique $\mathfrak{S}_5$ sur cinq objets. L'idée pour cela sera de considérer des développements des solutions (algébriques) de l'équation autour de $\lambda = 0$ et de $\lambda = 1$.

(1) On considère le corps $\mathbb{C}(\!(\lambda)\!)$ des « séries de Laurent » en l'indéterminée λ, c'est-à-dire des expressions formelles $f = \sum_{k=-\infty}^{\infty} a_k \lambda^k$ où $a_k \in \mathbb{C}$ et où seul un nombre fini des a_k avec $k < 0$ est non nul, l'addition et la multiplication se faisant formellement. (Le plus petit k tel que $a_k \neq 0$, ou bien ∞ si tous les a_k sont nuls, s'appellera la *valuation*, notée $v(f)$, de l'élément f de $\mathbb{C}(\!(\lambda)\!)$ ainsi défini.) Expliquer brièvement pourquoi il s'agit bien d'un corps et pourquoi il contient $\mathbb{C}(\lambda)$. L'équation $t^5 - \lambda t^2 + \lambda^2 - \lambda = 0$ a-t-elle des solutions dans $\mathbb{C}(\!(\lambda)\!)$? (On pourra raisonner sur la valuation des hypothétiques solutions.)

(2) On appelle $\mathbb{C}(\!(\lambda^{1/5})\!)$ le corps (analogue) des séries de Laurent en l'indéterminée $\lambda^{1/5}$ qui vérifie $(\lambda^{1/5})^5 = \lambda$ (expliquer brièvement pourquoi cela a bien un sens). Combien de racines a l'équation ($\star$) dans ce corps ? Quel est le groupe de Galois de $\mathbb{C}(\!(\lambda^{1/5})\!)$ sur $\mathbb{C}(\!(\lambda)\!)$, et comment opère-t-il sur les racines de l'équation ($\star$) ? Qu'en déduit-on sur le groupe de Galois de ($\star$) sur $\mathbb{C}(\lambda)$?

(3) En considérant de façon analogue les racines de ($\star$) dans les corps $\mathbb{C}(\!(\lambda-1)\!)$ et dans $\mathbb{C}(\!((\lambda-1)^{1/2})\!)$, que déduit-on cette fois ? Conclure.

Corrigé. (1) Il est assez clair que $\mathbb{C}(\!(\lambda)\!)$ est un anneau, et il est intègre car $v(fg) = v(f)+v(g)$ avec v la valuation. Le fait qu'il s'agisse d'un corps se ramène, quitte à multiplier f par $\lambda^{-v(f)}$ (pour se ramener à $v(f) = 0$) et quitte à inverser le coefficient constant (pour se ramener à $f = 1+g$ avec $v(g) \geq 1$), à vérifier que si $f = 1+g$ avec $v(g) \geq 1$ est une série formelle de coefficient constant 1 alors f est inversible : mais c'est clair en développant $f^{-1} = 1 - g + g^2 - g^3 + \cdots$ (cette somme infinie a un sens clair dans $\mathbb{C}(\!(\lambda)\!)$ puisque $v(g) \geq 1$).

On note pour la suite que $v(fg) = v(f) + v(g)$ mais aussi que $v(f+g) \geq \min(v(f), v(g))$ avec égalité si $v(f) \neq v(g)$ (la preuve est évidente).

Si $t \in \mathbb{C}(\!(\lambda)\!)$, de deux choses l'une : soit $v(t) \leq 0$ soit $v(t) \geq 1$. Mais dans le premier cas $v(t^5 - \lambda t^2 + \lambda^2 - \lambda) = -5v(t) \leq 0$ et dans le second $v(t^5 - \lambda t^2 + \lambda^2 - \lambda) = 1$. Dans les deux cas, $t^5 - \lambda t^2 + \lambda^2 - \lambda \neq 0$ donc $(\star)$ n'a pas de solution dans $\mathbb{C}(\!(\lambda)\!)$.

(2) Si on appelle $\mathbb{C}(\!(\mu^5)\!)$ le sous-anneau de $\mathbb{C}(\!(\mu)\!)$ formé des séries de Laurent dont tous les termes sont de valuation multiple de 5, il est évident par construction que $\mathbb{C}(\!(\mu^5)\!)$ est un sous-corps isomorphe à $\mathbb{C}(\!(\lambda)\!)$: on peut donc les identifier, ce qui fait de $\mathbb{C}(\!(\mu)\!)$ l'extension de degré 5 de $\mathbb{C}(\!(\lambda)\!)$ qui rajoute une racine μ à l'équation $t^5 - \lambda = 0$, c'est-à-dire $\mathbb{C}(\!(\lambda)\!)(\lambda^{1/5})$. La notation $\mathbb{C}(\!(\lambda^{1/5})\!)$ est donc justifiée, et le groupe de Galois de ce corps sur $\mathbb{C}(\!(\lambda)\!)$ est $\mathbb{Z}/5\mathbb{Z}$ identifié au groupe des racines 5-ièmes de l'unité dans $\mathbb{C}$ (agissant par $\sum_k a_k \lambda^{k/5} \mapsto \sum_k \zeta^k a_k \lambda^{k/5}$).

Dans le corps $\mathbb{C}(\!(\lambda^{1/5})\!)$, l'équation $(\star)$ admet des racines, par exemple $t_0 = \lambda^{1/5} + \frac{1}{5}\lambda^{3/5} - \frac{1}{5}\lambda^{6/5} - \frac{1}{125}\lambda^{7/5} + \frac{2}{25}\lambda^{8/5} + O(\lambda^{9/5})$ (ceci définit manifestement une série de Laurent, les coefficients étant déterminés par récurrence à partir de l'équation $(\star)$). Mais même, comme les cinq images de t_0 par $\mathrm{Gal}(\mathbb{C}(\!(\lambda^{1/5})\!)/\mathbb{C}(\!(\lambda)\!))$ sont distinctes (vu que déjà le premier terme non nul, $\zeta^i \lambda^{1/5}$ pour $i \in \mathbb{Z}/5\mathbb{Z}$, est déjà distinct), l'équation $(\star)$ a cinq racines distinctes dans $\mathbb{C}(\!(\lambda^{1/5})\!)$ (qui est son corps de décomposition sur $\mathbb{C}(\!(\lambda)\!)$), et elle est irréductible dans $\mathbb{C}(\!(\lambda)\!)$ (et à plus forte raison dans $\mathbb{C}(\lambda)$).

Ceci prouve que le groupe de Galois de $E_\star/\mathbb{C}(\lambda)$, corps de décomposition de l'équation $(\star)$ sur $\mathbb{C}(\lambda)$, doit contenir un 5-cycle.

(3) On plonge maintenant $\mathbb{C}(\lambda)$ dans $\mathbb{C}(\!(\lambda-1)\!)$, c'est-à-dire qu'on développe formellement autour de $\lambda = 1$ cette fois.

L'équation $(\star)$ admet déjà trois racines dans $\mathbb{C}(\!(\lambda-1)\!)$, notamment $1 - \frac{1}{3}(\lambda-1)^2 - \frac{2}{9}(\lambda-1)^3 + O((\lambda-1)^4)$ (les deux autres ont $e^{2i\pi/3}$ et $e^{-2i\pi/3}$ pour terme constant). Elle acquiert ses deux dernières racines sur l'extension $\mathbb{C}(\!((\lambda-1)^{1/2})\!)$, à savoir $(\lambda-1)^{1/2} + \frac{1}{2}(\lambda-1)^2 - \frac{1}{2}(\lambda-1)^3 + O((\lambda-1)^{7/2})$ et $-(\lambda-1)^{1/2} + \frac{1}{2}(\lambda-1)^2 - \frac{1}{2}(\lambda-1)^3 + O((\lambda-1)^{7/2})$. Le groupe de Galois du corps de décomposition $\mathbb{C}(\!((\lambda-1)^{1/2})\!)$ de $(\star)$ sur $\mathbb{C}(\!(\lambda-1)\!)$ agit en permutant ces deux dernières racines. Or ce groupe de Galois se voit comme un sous-groupe du groupe de Galois de $E_\star$ sur $\mathbb{C}(\lambda)$. Il y a donc une transposition dans le groupe de Galois de $(\star)$ sur $\mathbb{C}(\lambda)$.

Or un sous-groupe de $\mathfrak{S}_5$ qui agit transitivement et contient une transposition est $\mathfrak{S}_5$ tout entier, qui est donc le groupe de Galois recherché. ✓

5 (l'endécagone régulier). Expliquer de façon détaillée (mais sans faire les calculs) comment on peut démontrer que $\cos\frac{2\pi}{11}$ vaut

$$
\begin{aligned}
-\frac{1}{10} + \frac{1}{40}\sqrt[5]{\frac{11}{4}}\Bigg(&\left(-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}\right)\sqrt[5]{-89-25\sqrt{5}-20\,i\sqrt{10+2\sqrt{5}}+25\,i\sqrt{10-2\sqrt{5}}}\\
&+\left(-1+\sqrt{5}-i\sqrt{10+2\sqrt{5}}\right)\sqrt[5]{-89-25\sqrt{5}+20\,i\sqrt{10+2\sqrt{5}}-25\,i\sqrt{10-2\sqrt{5}}}\\
&+\left(-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}\right)\sqrt[5]{-89+25\sqrt{5}-25\,i\sqrt{10+2\sqrt{5}}-20\,i\sqrt{10-2\sqrt{5}}}\\
&+\left(-1+\sqrt{5}-i\sqrt{10+2\sqrt{5}}\right)\sqrt[5]{-89+25\sqrt{5}+25\,i\sqrt{10+2\sqrt{5}}+20\,i\sqrt{10-2\sqrt{5}}}\Bigg)
\end{aligned}
$$

(ici $\sqrt[5]{z}$ désigne la détermination principale de la racine cinquième, c'est-à-dire celle dont l'argument est compris entre $-\frac{\pi}{5}$ et $\frac{\pi}{5}$).

Corrigé. Appelons $\xi = e^{2i\pi/11}$ et $\omega = \frac{1}{2}(\xi + \xi^{-1}) = \cos\frac{2\pi}{11}$ et posons $\zeta = e^{2i\pi/5}$. Tout d'abord, il est bien connu, ou facile de vérifier, que $\zeta = \frac{1}{4}\left(-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}\right)$:

l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne de groupe de Galois $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ engendré par $\tau\colon \zeta \mapsto \zeta^2,\ \zeta^2 \mapsto \zeta^4,\ \zeta^4 \mapsto \zeta^3,\ \zeta^3 \mapsto \zeta$ (et $\mathbb{Q}(\sqrt{5})$ est le sous-corps fixe par $\{\mathrm{id}, \tau^2\}$).

Le corps $\mathbb{Q}(\zeta, \xi)$ est celui des racines 55-ièmes de l'unité, de dimension $\phi(55) = 40$ sur $\mathbb{Q}$, et de groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta,\xi)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ (par le théorème chinois, si l'on veut). Le facteur de gauche de ce produit est le groupe cyclique $\{\mathrm{id}, \tau, \tau^2, \tau^3\}$ (voir plus haut) où on a prolongé τ en un élément de $\mathrm{Gal}(\mathbb{Q}(\zeta,\xi)/\mathbb{Q}(\zeta))$ en le faisant agir comme l'identité sur ξ ; et le facteur de droite est le groupe cyclique à dix éléments engendré par σ où σ envoie $\xi, \xi^2, \xi^3, \xi^4, \ldots, \xi^{10}$ respectivement sur $\xi^2, \xi^4, \xi^6, \xi^8, \ldots, \xi^9$ (et fixe toutes les puissances de τ). Le sous-corps de $\mathbb{Q}(\xi)$ fixé par $\{\mathrm{id}, \sigma^5\}$ est $\mathbb{Q}(\omega)$, et $\mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}$ est le groupe cyclique à cinq éléments engendré par $\bar\sigma$ (la restriction de σ à $\mathbb{Q}(\omega)$, c'est-à-dire sa classe dans le groupe quotient par $\{\mathrm{id}, \sigma^5\}$). Ainsi, les conjugués de $\omega = \frac12(\xi + \xi^{-1}) = \omega_1 = \cos\frac{2\pi}{11}$ sont $\sigma(\omega) = \frac12(\xi^2 + \xi^{-2}) = \omega_2 = \cos\frac{4\pi}{11}$ puis $\sigma^2(\omega) = \frac12(\xi^4 + \xi^{-4}) = \omega_4 = \cos\frac{8\pi}{11}$ puis $\sigma^3(\omega) = \frac12(\xi^3 + \xi^{-3}) = \omega_3 = \cos\frac{6\pi}{11}$ et enfin $\sigma^4(\omega) = \frac12(\xi^5 + \xi^{-5}) = \omega_5 = \cos\frac{10\pi}{11}$.

On pose $\alpha = \omega_1 + \zeta\omega_2 + \zeta^2\omega_4 + \zeta^3\omega_3 + \zeta^4\omega_5 \in \mathbb{Q}(\zeta, \omega)$. Alors on a $\sigma(\alpha) = \omega_2 + \zeta\omega_4 + \zeta^2\omega_3 + \zeta^3\omega_5 + \zeta^4\omega = \zeta^{-1}\,\alpha$. Par conséquent, si $a = \alpha^5$, on voit que $\sigma(a) = a$, c'est-à-dire $a \in \mathbb{Q}(\zeta)$. On sait donc qu'on peut écrire a comme combinaison linéaire à coefficients rationnels de $1, \sqrt5, i\sqrt{10+2\sqrt5}, i\sqrt{10-2\sqrt5}$. Pour calculer effectivement ces coefficients, on utilise le fait qu'on connaît les quatre conjugués $a, \tau(a), \tau^2(a), \tau^3(a)$ (par exemple, $\tau(a) = (\omega_1 + \zeta^2\omega_2 + \zeta^4\omega_4 + \zeta\omega_3 + \zeta^3\omega_5)^5$). Plus précisément : on écrit $a = r + s\sqrt5 + u\,i\sqrt{10+2\sqrt5} + v\,i\sqrt{10-2\sqrt5}$ (avec $r, s, u, v \in \mathbb{Q}$) puis $\tau(a) = r - s\sqrt5 - v\,i\sqrt{10+2\sqrt5} + u\,i\sqrt{10-2\sqrt5}$ et $\tau^2(a) = r + s\sqrt5 - u\,i\sqrt{10+2\sqrt5} - v\,i\sqrt{10-2\sqrt5}$ et $\tau^3(a) = r - s\sqrt5 + v\,i\sqrt{10+2\sqrt5} - u\,i\sqrt{10-2\sqrt5}$, ce qui donne quatre équations dans les quatre inconnues r, s, u, v, donc on peut les calculer au moins numériquement ; or étant plus attentif on peut majorer leurs dénominateurs (par exemple, 4α est manifestement un entier algébrique[1] donc au pire $1024\,a$ en est un, et en résolvant le système linéaire on peut facilement majorer les numérateurs qui interviennent), ce qui permet de convertir une valeur numérique en une valeur rationnelle exacte. Précisément, on trouve : $a = \frac{11}{128}(-89 - 25\sqrt5 - 20\,i\sqrt{10+2\sqrt5} + 25\,i\sqrt{10-2\sqrt5})$ et on connaît alors $\alpha = \zeta^t\sqrt[5]{a}$ (où t est un entier modulo 5, facile à calculer d'après des valeurs numériques, qui sert à préciser la détermination de la racine cinquième).

Enfin, comme manifestement $\omega = -\frac{1}{10} + \frac15(\alpha + \tau(\alpha) + \tau^2(\alpha) + \tau^3(\alpha))$, il n'y a plus qu'à écrire l'expression en question. ✓

([1]) C'est-à-dire racine d'un polynôme unitaire à coefficients entiers. Rappelons que les entiers algébriques forment un anneau $\mathcal{O}$, et que ceux qui sont rationnels sont exactement les entiers relatifs : $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$ (cela se démontre facilement en constatant qu'il ne peut pas y avoir de nombre premier au dénominateur).