1. Montrer que les extensions $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ et $\mathbb{Q}(\sqrt{2+\sqrt{3}})$ de $\mathbb{Q}$ sont galoisiennes, et calculer leurs groupes de Galois. L'extension $\mathbb{Q}(\sqrt{2+\sqrt{5}})$ est-elle galoisienne sur $\mathbb{Q}$?

Corrigé. Commençons par $\mathbb{Q}(\sqrt{2+\sqrt{2}})$: manifestement, elle est galoisienne sur le corps $\mathbb{Q}(\sqrt{2})$, qui est lui-même galoisien sur $\mathbb{Q}$ avec un groupe de Galois engendré par $\sigma\colon \sqrt{2} \mapsto -\sqrt{2}$. La chose à vérifier, donc, est qu'il existe un automorphisme de $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ qui prolonge σ. Cet automorphisme $\tilde{\sigma}$ doit envoyer $\sqrt{2+\sqrt{2}}$ sur une racine carrée de $\sigma(2+\sqrt{2}) = 2-\sqrt{2}$. La question est donc de savoir si $\sqrt{2-\sqrt{2}}$ « existe » dans $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ (pour que tous les conjugués de $\sqrt{2+\sqrt{2}}$, donc $-\sqrt{2+\sqrt{2}}$, $\sqrt{2-\sqrt{2}}$ et $-\sqrt{2-\sqrt{2}}$, soient dans $\mathbb{Q}(\sqrt{2+\sqrt{2}})$). Or $(2+\sqrt{2})(2-\sqrt{2}) = 2$ 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 $\sqrt{2-\sqrt{2}} = -\sqrt{2+\sqrt{2}} + \sqrt{2}\sqrt{2+\sqrt{2}}$. Ceci montre que l'extension est galoisienne (elle est engendrée par tous les conjugués de $\sqrt{2+\sqrt{2}}$ donc normale). Pour ce qui est de son groupe de Galois, on a évidemment un élément $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}(\sqrt{2}) \subseteq \mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ qui laisse $\sqrt{2}$ fixe et envoie $\sqrt{2+\sqrt{2}}$ sur $-\sqrt{2+\sqrt{2}}$. Et on a un $\tilde{\sigma}$ qui envoie $\sqrt{2}$ sur $-\sqrt{2}$ et $\sqrt{2+\sqrt{2}}$ sur $\sqrt{2-\sqrt{2}} = -\sqrt{2+\sqrt{2}} + \sqrt{2}\sqrt{2+\sqrt{2}}$. On vérifie alors $\tilde{\sigma}^2(\sqrt{2+\sqrt{2}}) = -\sqrt{2-\sqrt{2}} - \sqrt{2}\sqrt{2-\sqrt{2}} = -\sqrt{2+\sqrt{2}}$, donc $\tilde{\sigma}^2 = \tau$ et le groupe de Galois est le groupe cyclique à quatre éléments engendré par $\tilde{\sigma}$.

Considérons maintenant $\mathbb{Q}(\sqrt{2+\sqrt{3}})$: manifestement, elle est galoisienne sur le corps $\mathbb{Q}(\sqrt{3})$, qui est lui-même galoisien sur $\mathbb{Q}$ avec un groupe de Galois engendré par $\sigma\colon \sqrt{3} \mapsto -\sqrt{3}$. La chose à vérifier, de nouveau, est qu'il existe un automorphisme de $\mathbb{Q}(\sqrt{2+\sqrt{3}})$ qui prolonge σ. Cet automorphisme $\tilde{\sigma}$ doit envoyer $\sqrt{2+\sqrt{3}}$ sur une racine carrée de $\sigma(2+\sqrt{3}) = 2-\sqrt{3}$. La question est donc une fois de plus de savoir si $\sqrt{2-\sqrt{3}}$ « existe » dans $\mathbb{Q}(\sqrt{2+\sqrt{3}})$ (pour que tous les conjugués de $\sqrt{2+\sqrt{3}}$ soient dans $\mathbb{Q}(\sqrt{2+\sqrt{3}})$). Or $(2+\sqrt{3})(2-\sqrt{3}) = 1$ 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 $\sqrt{2-\sqrt{3}} = -2\sqrt{2+\sqrt{3}} - \sqrt{3}\sqrt{2+\sqrt{3}}$. Ceci montre que l'extension est galoisienne (elle est engendrée par tous les conjugués de $\sqrt{2+\sqrt{3}}$ donc normale). Pour ce qui est de son groupe de Galois, on a un élément $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{3}})/\mathbb{Q}(\sqrt{3}) \subseteq \mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{3}})/\mathbb{Q}$ qui laisse $\sqrt{3}$ fixe et envoie $\sqrt{2+\sqrt{3}}$ sur $-\sqrt{2+\sqrt{3}}$. Et on a un $\tilde{\sigma}$ qui envoie $\sqrt{3}$ sur $-\sqrt{3}$ et $\sqrt{2+\sqrt{3}}$ sur $\sqrt{2-\sqrt{3}} = 2\sqrt{2+\sqrt{3}} - \sqrt{3}\sqrt{2+\sqrt{3}}$. On vérifie alors $\tilde{\sigma}^2(\sqrt{2+\sqrt{3}}) = 2\sqrt{2-\sqrt{3}} + \sqrt{3}\sqrt{2-\sqrt{3}} = \sqrt{2+\sqrt{3}}$, donc $\tilde{\sigma}^2 = \mathrm{id}$ et le groupe de Galois est le produit d'un groupe cyclique à deux éléments engendré par τ et un groupe cyclique à deux éléments engendré par $\tilde{\sigma}$.

Enfin, pour $\mathbb{Q}(\sqrt{2+\sqrt{5}})$, pour montrer qu'elle n'est pas normale, on constate simplement qu'elle est incluse dans $\mathbb{R}$ (ou du moins elle peut l'être) donc ne contient pas le complexe $\sqrt{2-\sqrt{5}}$ (pour une détermination quelconque de cette racine carrée) qui est imaginaire pur. Or ce complexe est un conjugué de $\sqrt{2+\sqrt{5}}$. Donc l'extension $\mathbb{Q}(\sqrt{2+\sqrt{5}})$ de $\mathbb{Q}$ n'est pas galoisienne. ✓

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 (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 $\xi,\xi^2,\xi^3,\xi^4,\dots,\xi^{10}$ respectivement sur $\xi^2,\xi^4,\xi^6,\xi^8,\dots,\xi^9$ (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. ✓

4. Déterminer le groupe de Galois des équations suivantes sur le corps $\mathbb{C}(\lambda)$ des fractions rationnelles en une indéterminée : (a) $t^n+\lambda=0$, (b) $t^3+t+\lambda=0$, (c) $t^4+2(1-2\lambda)t^2+1=0$, (†) (d) $t^5-\lambda t^2+\lambda^2-\lambda=0$.

Corrigé. (a) Il s'agit de l'extraction d'une racine n-ième, et comme toutes les racines de l'unité sont dans le corps de base (puisqu'il contient $\mathbb{C}$), le groupe de Galois est $\mathbb{Z}/n\mathbb{Z}$ engendré par $\sqrt[n]{\lambda}\mapsto\zeta\sqrt[n]{\lambda}$ (avec $\zeta=e^{2i\pi/n}$).

(b) Le discriminant du polynôme $t^3+t+\lambda$ (voir l'exercice 5 de la feuille n°4) est $\Delta=-4-27\lambda^2$; or ceci n'est pas un carré dans $\mathbb{C}(\lambda)$, donc le groupe de Galois de l'équation cubique est $\mathfrak{S}_3$.

(c) On renvoie à l'exercice 1 (2e cas notamment) : on a $\sqrt{2\lambda-1-2\sqrt{\lambda(\lambda-1)}}=(2\lambda-1)\sqrt{2\lambda-1+2\sqrt{\lambda(\lambda-1)}}-2\sqrt{\lambda(\lambda-1)}\sqrt{2\lambda-1+2\sqrt{\lambda(\lambda-1)}}$ donc l'élément du groupe de Galois qui envoie $\sqrt{2\lambda-1+2\sqrt{\lambda(\lambda-1)}}$ sur $\sqrt{2\lambda-1-2\sqrt{\lambda(\lambda-1)}}$ est involutif, et le groupe de Galois est $(\mathbb{Z}/2\mathbb{Z})^2$.

(d) Plongeons $\mathbb{C}(\lambda)$ dans le corps $\mathbb{C}(\!(\lambda)\!)$ des séries de Laurent[2] en l'indéterminée λ : manifestement il acquiert ses racines sur l'extension $\mathbb{C}(\!(\lambda^{1/5})\!)$ de degré 5, par exemple $t=$

([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).

([2]) Autrement dit les séries formelles $\sum_{k=-\infty}^{\infty}a_k\lambda^k$ où seul un nombre fini des a_k avec $k<0$ est non nul.

$\lambda^{1/5}+\frac{1}{5}\,\lambda^{3/5}-\frac{1}{5}\,\lambda^{6/5}-\frac{1}{125}\,\lambda^{7/5}+\frac{2}{25}\,\lambda^{8/5}+O(\lambda^{9/5})$. Donc l'équation est irréductible et le groupe de Galois opère transitivement sur les racines. Maintenant, en plongeant $\mathbb{C}(\lambda)$ dans $\mathbb{C}(\!(\lambda-1)\!)$, c'est-à-dire en développant formellement autour de $\lambda = 1$ cette fois, il a déjà trois racines (notamment $1-\frac{1}{3}\,(\lambda-1)^2-\frac{2}{9}(\lambda-1)^3+O((\lambda-1)^4)$) et il acquiert les deux dernières sur l'extension $\mathbb{C}(\!(\lambda-1)^{1/2}\!)$ (notamment $(\lambda-1)^{1/2}+\frac{1}{2}(\lambda-1)^2-\frac{1}{2}(\lambda-1)^3+O((\lambda-1)^{7/2})$) ; il y a donc une transposition dans le groupe de Galois. 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. ✓

Motivations : L'exercice 1 est un cas flagrant mais assez facile où la théorie de Galois n'est pas triviale : les équations biquadratiques $t^4-4t^2+2=0$, $t^4-4t^2+1=0$ et $t^4-4t^2-1=0$, bien que d'apparence semblable (et toutes irréductibles) ont des groupes de Galois différents (on pourrait d'ailleurs rajouter $t^4-4t^2=0$ ou encore $t^4-4t^2-5=0$ pour avoir encore deux autres groupes de Galois, mais ces polynômes ne sont bien sûr pas irréductibles). L'exercice 2 montre comment la réduction modulo p peut servir à calculer des groupes de Galois. L'exercice 3 est une application concrète de la méthode de résolution par radicaux. L'exercice 4 est en quelque sorte analogue du 2 sur les corps de fonctions, et il touche à la géométrie algébrique.