Exercice 1 (Correspondance de Galois)**.**
Dans chacun des cas suivantes déterminer le groupe de Galois de l'extension donnée, déterminer tous ses sous-groupes et tous les sous-corps de points fixes correspondants.

1. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{7})$.
2. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
3. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.
4. $\mathbb{Q} \subset E$ où E est le corps de décomposition de $t^4 - 2t^2 - 1 \in \mathbb{Q}[t]$.

Indication. Ce corps de décomposition est de degré 8 et on montrera qu'il s'agit de $\mathbb{Q}(\sqrt{1+\sqrt{2}}, i)$. On explicitera alors un automorphisme d'ordre 2 et un autre d'ordre 4 qui ne commutent pas entre eux, si bien que le groupe de Galois est le groupe dihédral d'ordre 8.

Solution.

1. Let $L = \mathbb{Q}(\sqrt{7})$. We have that $[L : \mathbb{Q}] = 2$, as $\sqrt{7} \notin \mathbb{Q}$ is a root of the irreducible polynomial $x^2 - 7 \in \mathbb{Q}[x]$. Now, $\mathbb{Q}$ is a perfect field and L is the splitting field of $x^2 - 7 \in \mathbb{Q}[x]$ over $\mathbb{Q}$, hence the extension $\mathbb{Q} \subseteq L$ is Galois. By Proposition 4.6.5(d), it follows that $|\operatorname{Gal}(L/\mathbb{Q})| = 2$ and so $\operatorname{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. The only subgroups of $\operatorname{Gal}(L/\mathbb{Q})$ are $\operatorname{Gal}(L/\mathbb{Q})$ and $\{\mathrm{Id}_L\}$, therefore the only sub-extensions of L are $\mathbb{Q} = L^{\operatorname{Gal}(L/\mathbb{Q})}$ and $L = L^{\{\mathrm{Id}_L\}}$.

2. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We have seen in 3.4 of sheet 10 that $[L : \mathbb{Q}] = 4$, that Galois group is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ and that it is generated by σ and τ, where $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$, respectively $\tau(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{3}) = -\sqrt{3}$.

   Now, $\operatorname{Gal}(L/\mathbb{Q})$ admits 3 non-trivial proper subgroups: $<\sigma>$, $<\tau>$ and $<\sigma\tau>$, each isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Let H be one of these subgroups. We therefore need to determine $L^H \subseteq L$. By the main theorem of Galois theory, we know that $[L : L^H] = |H| = 2$. Therefore, $[L^H : \mathbb{Q}] = 2$. One checks that $\mathbb{Q}(\sqrt{3}) \subseteq L^{<\sigma>}$, as $\sigma(\sqrt{3}) = \sqrt{3}$, and, similarly, that $\mathbb{Q}(\sqrt{2}) \subseteq L^{<\tau>}$ and $\mathbb{Q}(\sqrt{6}) \subseteq L^{<\sigma\tau>}$, respectively. We conclude that

$$L^{<\sigma>} = \mathbb{Q}(\sqrt{3}),\ L^{<\tau>} = \mathbb{Q}(\sqrt{2}) \text{ and } L^{<\sigma\tau>} = \mathbb{Q}(\sqrt{6}).$$

3. As in the previous point, we already computed that $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ is Galois, with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. It is generated by $\sigma_1, \sigma_2, \sigma_3 \in \operatorname{Gal}(L/\mathbb{Q})$ with:

$$\sigma_1(\sqrt{2}) = -\sqrt{2},\ \sigma_1(\sqrt{3}) = \sqrt{3} \text{ and } \sigma_1(\sqrt{5}) = \sqrt{5}$$
$$\sigma_2(\sqrt{2}) = \sqrt{2},\ \sigma_2(\sqrt{3}) = -\sqrt{3} \text{ and } \sigma_2(\sqrt{5}) = \sqrt{5}$$
$$\sigma_3(\sqrt{2}) = \sqrt{2},\ \sigma_3(\sqrt{3}) = \sqrt{3} \text{ and } \sigma_3(\sqrt{5}) = -\sqrt{5}$$

   We first consider the subgroups of order 2 of $\operatorname{Gal}(L/\mathbb{Q})$. There are 7 of them and each of these is cyclic and generated by an element of $\operatorname{Gal}(L/\mathbb{Q})$. Let H be one of these subgroups. Then by the main theorem of Galois theory, $L^H \subseteq L$ is Galois with $[L : L^H] = |H| = 2$, so $[L^H : \mathbb{Q}] = 4$.

Let $H =< \sigma_1 >$. One checks that $\mathbb{Q}(\sqrt{3},\sqrt{5}) \subseteq L^H$, as $\sigma_1(\sqrt{3}) = \sqrt{3}$ and $\sigma_1(\sqrt{5}) = \sqrt{5}$. Therefore, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3},\sqrt{5}) \subseteq L^H$, where $[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}] = 4$ and $[L^H : \mathbb{Q}] = 4$. We conclude that $L^H = \mathbb{Q}(\sqrt{3},\sqrt{5})$. Similarly, one shows that:

$$L^{<\sigma_2>} = \mathbb{Q}(\sqrt{2},\sqrt{5}),\ L^{<\sigma_3>} = \mathbb{Q}(\sqrt{2},\sqrt{3}),\ L^{<\sigma_1\sigma_2>} = \mathbb{Q}(\sqrt{6},\sqrt{5})$$

$$L^{<\sigma_1\sigma_3>} = \mathbb{Q}(\sqrt{3},\sqrt{10}),\ L^{<\sigma_2\sigma_3>} = \mathbb{Q}(\sqrt{2},\sqrt{15}),\ L^{<\sigma_1\sigma_2\sigma_3>} = \mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}) = \mathbb{Q}(\sqrt{6},\sqrt{10})$$

We now consider the subgroups of order 4 of $\mathrm{Gal}(L/\mathbb{Q})$. Again, there are 7 of them and each of these is generated by two distinct elements of order 2 of $\mathrm{Gal}(L/\mathbb{Q})$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let H be one of these subgroups. As above, $L^H \subseteq L$ is Galois with $[L : L^H] = |H| = 4$. Therefore we have $[L^H : \mathbb{Q}] = 2$. One shows that:

$$L^{<\sigma_1,\sigma_2>} = \mathbb{Q}(\sqrt{5}),\ L^{<\sigma_1,\sigma_3>} = \mathbb{Q}(\sqrt{3}),\ L^{<\sigma_1,\sigma_2\sigma_3>} = \mathbb{Q}(\sqrt{15}),\ L^{<\sigma_2,\sigma_3>} = \mathbb{Q}(\sqrt{2})$$

$$L^{<\sigma_2,\sigma_1\sigma_3>} = \mathbb{Q}(\sqrt{10}),\ L^{<\sigma_3,\sigma_1\sigma_2>} = \mathbb{Q}(\sqrt{6}),\ L^{<\sigma_1\sigma_2,\sigma_1\sigma_3>} = \mathbb{Q}(\sqrt{30}).$$

4. First, we note that the extension $\mathbb{Q} \subseteq E$ is Galois, as $\mathbb{Q}$ is a perfect field and E is the splitting field of the polynomial $t^4 - 2t^2 - 1 \in \mathbb{Q}[t]$ over $\mathbb{Q}$. It follows that $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$. We see that $t^4 - 2t^2 - 1 = (t^2 - 1 - \sqrt{2})(t^2 - 1 + \sqrt{2}) = (t - \sqrt{1+\sqrt{2}})(t + \sqrt{1+\sqrt{2}})(t - \sqrt{1-\sqrt{2}})(t + \sqrt{1-\sqrt{2}})$. Therefore $E = \mathbb{Q}(\sqrt{1+\sqrt{2}},\sqrt{1-\sqrt{2}})$. Now, we can make a choice of complex square root sucht that we have that $i = \sqrt{1+\sqrt{2}} \cdot \sqrt{1-\sqrt{2}} \in E$ and thus $\mathbb{Q}(\sqrt{1+\sqrt{2}},i) \subseteq E$. Conversely, we have $\sqrt{1-\sqrt{2}} = i \cdot (\sqrt{1+\sqrt{2}})^{-1} \in \mathbb{Q}(\sqrt{1+\sqrt{2}},i)$ and we deduce that $E = \mathbb{Q}(\sqrt{1+\sqrt{2}},i)$. We now consider the extension chain:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\sqrt{1+\sqrt{2}}}) \subseteq E.$$

Since $\sqrt{1+\sqrt{2}}$ is a root of $t^4 - 2t^2 - 1 \in \mathbb{Q}[t]$, it follows that $[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}] \leq 4$. We have already seen that the polynomial $t^4 - 2t^2 - 1$ does not admit roots in $\mathbb{Q}$. We now assume that there exist $a, b, c, d \in \mathbb{Q}$ such that:

$$t^4 - 2t^2 - 1 = (t^2 + at + b)(t^2 + ct + d).$$

Then $\begin{cases} a + c = 0 \\ b + ac + d = -2 \\ ad + bc = 0 \\ bd = -1 \end{cases}$ and so $c = -a$, $d = -\frac{1}{b}$ and $-a(\frac{1}{b} + b) = 0$.

- If $a = 0$, then $c = 0$ and $b + d = -2$. Keeping in mind that $d = -\frac{1}{b}$, it follows that $(b+1)^2 = 2$, hence $\sqrt{2} \in \mathbb{Q}$, which is a contradiction.
- If $\frac{1}{b} + b = 0$, then $b^2 + 1 = 0$ and so $i \in \mathbb{Q}$, which is a contradiction.

We have thus shown that $t^4 - 2t^2 - 1 \in \mathbb{Q}[t]$ is irreducible and therefore $[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}] = 4$. We remark that $\mathbb{Q}(\sqrt{1+\sqrt{2}}) \subseteq \mathbb{R}$ and so $[E : \mathbb{Q}(\sqrt{1+\sqrt{2}})] = 2$, as $i \notin \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is a root of $t^2 + 1 \in \mathbb{Q}(\sqrt{1+\sqrt{2}})[t]$. In conclusion, $[E : \mathbb{Q}] = 8$, hence $|\mathrm{Gal}(E/\mathbb{Q})| = 8$.

Since $E/\mathbb{Q}(\sqrt{1+\sqrt{2}})$ has degree 2 and is Galois, there exists $\tau \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\tau(\sqrt{1+\sqrt{2}}) = \sqrt{1+\sqrt{2}}$ and $\tau(i) = -i$.

Note that $t^4 - 2t^2 - 1$ is a degree 4 polynomial in $\mathbb{Q}(i)$ annihilating $\sqrt{1+\sqrt{2}}$. Since the associated extension $E/\mathbb{Q}(i)$ has degree 4, we deduce that $t^4 - 2t^2 - 1$ is irreducible over $\mathbb{Q}(i)$.

By the course, we know that there exists $\sigma' \in \mathrm{Gal}(E/\mathbb{Q}(i))$ sending $\alpha := \sqrt{1+\sqrt{2}}$ to $\sqrt{1-\sqrt{2}}$. Set $\sigma = \sigma'\tau$. Recall that $\sqrt{1-\sqrt{2}} = i\alpha^{-1}$. Therefore we can write the four roots of

$$t^4 - 2t^2 - 1$$

as

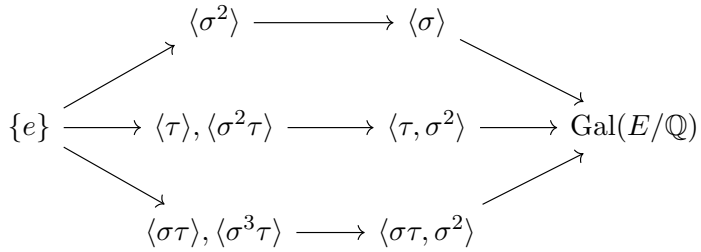
$$\alpha, \quad -\alpha, \quad i\alpha^{-1}, \quad -i\alpha^{-1}.$$

One checks that:

$$\sigma^2(\alpha) = -\alpha, \ \sigma^2(i) = i$$

which implie that σ^2 is of order 2, and therefore that σ is of order 4. Also, as $\sigma\tau(\alpha) = i\alpha^{-1}$ and $\tau\sigma(\alpha) = -i\alpha^{-1}$, we conclude that $\mathrm{Gal}(E/\mathbb{Q})$ is a non-commutative group of order 8. Also as $\sigma^2(i) = i$ and $\tau(i) = -i$, we see that there is two elements of order 2, which implies $\mathrm{Gal}(E/\mathbb{Q}) \cong D_8$.

Subgroups of $\mathrm{Gal}(E/\mathbb{Q})$, arranged by conjugacy classes, are



Recall also that the index of subgroup corresond to the degree of the corresponding fixed extension. To deduce what are the corresponding extensions, notice also that

$$1 + \sigma(\sqrt{2}) = \sigma(1 + \sqrt{2}) = \sigma(\alpha^2) = (i\alpha^{-1})^2 = -\frac{-1}{1+\sqrt{2}} = 1 - \sqrt{2},$$

impliyng that $\sigma(\sqrt{2}) = -\sqrt{2}$. As $\tau(\alpha) = \alpha$, we also get $\tau(\sqrt{2}) = \sqrt{2}$. As a consequence we get,

$$E^{<\sigma>} = \mathbb{Q}(i\sqrt{2}), \ E^{<\tau,\sigma^2>} = \mathbb{Q}(\sqrt{2}) \text{ and } E^{<\tau\sigma,\sigma^2>} = \mathbb{Q}(i).$$

Now as for the degree four extensions corresponding to subgroups of order 2; we can first deduce that

$$E^{\langle\sigma^2\rangle} = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2}).$$

has $\mathbb{Q}(i, \sqrt{2})$ is Galois of order 4 and by the correspondence there is only one sub Galois extension of order 4.

Now, we deduce from the above calculations and from the fact that if H is a subgroup, then $\sigma(E^H) = E^{\sigma H \sigma^{-1}}$, we get

$$E^{<\tau>} = \mathbb{Q}(\sqrt{1+\sqrt{2}}) \quad E^{<\sigma^2\tau>} = \mathbb{Q}(\sqrt{1-\sqrt{2}}).$$

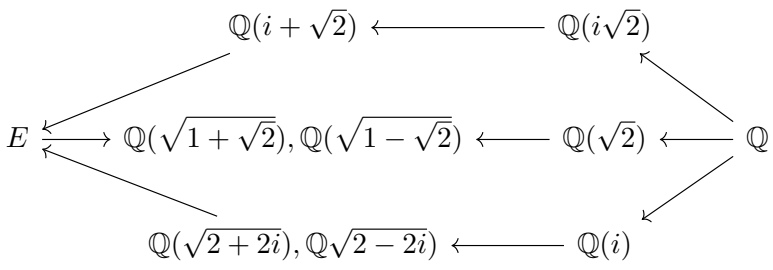
Also, note that squaring we deduce that,

$$\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}} = \sqrt{2+2i} \quad \sqrt{1+\sqrt{2}} - \sqrt{1-\sqrt{2}} = \sqrt{2-2i}.$$

And therefore, we see that

$$E^{<\sigma\tau>} = \mathbb{Q}(\sqrt{2+2i}) \text{ and } E^{<\sigma^3\tau>} = \mathbb{Q}(\sqrt{2-2i}).$$

All in all, we get the following subfields, mirroring the subgroup diagram above.



Exercice 2.
Soit $K \subseteq L = K(\alpha)$ une extension simple de degré 2 de corps de caractéristique différente de 2.

1. Soit $m_{\alpha,K} = x^2 + bx + c$, où $b, c \in K$. Démontrez que la formule quadratique est valide ici. Cela veut dire les deux racines de $m_{\alpha,K}$ sont $\frac{-b+\sqrt{b^2-4c}}{2}$ et $\frac{-b-\sqrt{b^2-4c}}{2}$, où $\beta = \sqrt{b^2-4c} \in L$ est un quelconque élément tel que $\beta^2 = b^2 - 4c$. Cela inclut l'affirmation que tel β n'existe pas dans K. Concluez que L est une extension par une racine (deuxième) d'un élément adéquat de K.

2. Démontrez que $K \subseteq L$ est $\mathbb{Z}/2\mathbb{Z}$-galoisienne .

3. Soit $\mathbb{Q} = K \subseteq L$ une extension de corps $\mathbb{Z}/4\mathbb{Z}$-galoisienne. Démontrez que il existe des entiers rationnels a, $b \neq 0$ et d tel que $L = \mathbb{Q}\Big(\sqrt{a+b\sqrt{d}}\Big)$ et $\sqrt{d} \notin \mathbb{Q}$, $\sqrt{a+b\sqrt{d}} \notin \mathbb{Q}(\sqrt{d})$.

4. Considérons a, $b \neq 0$, $d \in \mathbb{Q}$ tel que $\sqrt{d} \notin \mathbb{Q}$ et $\alpha = \sqrt{a+b\sqrt{d}} \notin \mathbb{Q}\big(\sqrt{d}\big)$. Démontrez que l'extension $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\alpha)$ est $\mathbb{Z}/4\mathbb{Z}$-galoisienne si et seulement si $\sqrt{a-b\sqrt{d}} \in L$ et $\lambda = a^2 - b^2 d$ n'est pas un carré dans $\mathbb{Q}$.

5. Montrez que $\mathbb{Q} \subseteq \mathbb{Q}\big(\sqrt{2+\sqrt{2}}\big)$ est $\mathbb{Z}/4\mathbb{Z}$-galoisienne.

Solution.

1. Comme 2 est inversible, on peut écrire

$$x^2 + bx + c = 0 \iff x^2 + 2\frac{b}{2}x + \frac{b^2}{4} = \frac{b^2}{4} - c$$

c'est à dire

$$(2x+b)^2 = b^2 - 4c.$$

Ainsi, $\beta = 2\alpha + b$ est une racine carrée de $\frac{b^2}{4} - c$. Notons que $L = K(\alpha) = K(\beta)$. Comme $K \neq L$, on a que $\beta \neq\in K$. Cet élément est une racine carrée d'un élément de K. On voit par calcul direct que $\frac{-b+\beta}{2}$ et $\frac{-b-\beta}{2}$ sont les racines du polynôme minimal.

2. On construit un automorphisme de Galois de L sur K par

$$L = K(\beta) \xleftarrow{\mathrm{ev}_\beta} K[t]/(t^2 - \beta^2) \xrightarrow{\mathrm{ev}_{-\beta}} K(\beta) = L.$$

Comme il envoie $\beta \mapsto -\beta$, il n'est pas l'identité. Comme $|\operatorname{Gal}(L \mid K)| \leq 2$ on a égalité et donc que cette extension est Galoisienne.

3. Soit H l'unique sous-groupe d'ordre 2 dans le groupe de galois $G = \operatorname{Gal}(L \mid K)$. Soit $M = L^H$. Ce corps est de degré 2 sur $\mathbb{Q}$ par la correspondance de Galois. Soit donc $d \in \mathbb{Q}$ avec $M = \mathbb{Q}(\sqrt{d})$. Comme $M \subset L$ est de degré 2 par multiplicativité des degré, il existe un élément $a + b\sqrt{d} \in M$ tel que $L = M(\sqrt{a+b\sqrt{d}})$.

Montrons que $b \neq 0$. Si $b = 0$, alors $\sqrt{a} \notin \mathbb{Q}(\sqrt{d})$. Mais alors $L = \mathbb{Q}(\sqrt{a}, \sqrt{d})$ qui a groupe de Galois isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En effet, un élément σ du groupe de Galois doit envoyer $\sqrt{a}$ sur $\pm\sqrt{a}$ et $\sqrt{d}$ sur $\pm\sqrt{d}$, ce qui force $\sigma^2 = id$. Ainsi, le groupe de Galois serait un groupe d'ordre 2 ou tous les éléments sont d'ordre au plus 2, i.e. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Dès lors, notons que $\sqrt{d} \in \mathbb{Q}(\sqrt{a+b\sqrt{d}})$, ce qui permet de conclure que $L = \mathbb{Q}(\sqrt{a+b\sqrt{d}})$.

4. Soit $\alpha = \sqrt{a+b\sqrt{d}}$ et $\beta = \sqrt{a-b\sqrt{d}}$. Notons que $\mathbb{Q}(\sqrt{d})$ est une extension intermédiaire Galoisienne de degré 2 sur $\mathbb{Q}$. Supposons l'extension Galoisienne. Soit $\phi \in \operatorname{Gal}(L \mid K)$ une extension de l'automorphisme de $\mathbb{Q}(\sqrt{d})$ qui envoie $\sqrt{d} \mapsto -\sqrt{d}$ à L par le théorème 4.3.4. On voit alors que $\phi(\alpha) \in L$ est une racine carrée de $a - b\sqrt{d}$. En particulier cet élément

appartient à L. A l'inverse, si $\sqrt{a-b\sqrt{d}} \in L$, alors L contient toutes les racines du polynôme minimal de $\sqrt{a+b\sqrt{d}}$, donc $L/\mathbb{Q}$ est Galoisienne par le théorème 4.6.17.

Ainsi, il suffit de montrer que a^2-b^2d n'est pas un carré si et seulement si $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Notons que $(\alpha\beta)^2 = a^2 - b^2d$.

Supposons tout d'abord que $a^2 - b^2d$ est un carré, et soit $\psi \in \mathrm{Gal}(L/\mathbb{Q})$. Alors $\psi(\alpha) \in \{\pm\alpha, \pm\beta\}$. Si $\psi(\alpha) = \alpha$ ou $-\alpha$, alors $\psi^2(\alpha) = \alpha$ et donc ψ est d'ordre 2. Comme $(\alpha\beta)^2 = a^2 - b^2d$, on a que $\alpha\beta \in \mathbb{Q}$ et donc vu que

$$\frac{1}{\alpha} = \frac{\beta}{\alpha\beta},$$

on a

$$\psi(\alpha) = \psi(\alpha\beta/\beta) = \alpha\beta\psi(1/\beta) = \alpha\beta\psi(\beta)^{-1}.$$

Ainsi, si $\psi(\alpha) = \beta$ ou $-\beta$, on en déduit aussi que $\psi^2(\alpha) = \alpha$, et donc $\psi^2 = id$.

Ainsi, on a dans tous les cas que $\psi^2 = id$, et donc le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ est 2-torsion. Il ne peut donc pas être isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Supposons maintenant que $a^2 - b^2d$ n'est pas un carré. Alors $\mathbb{Q}(\alpha\beta)$ est une sous-extension de degré 2 sur $\mathbb{Q}$. On alors deux extensions ϕ_1, ϕ_2 de l'automorphisme de Galois non-trivial $\phi\colon \mathbb{Q}(\alpha\beta) \to \mathbb{Q}(\alpha\beta)$ qui envoie $\alpha\beta \mapsto -\alpha\beta$. Ces deux extensions sont déterminées par leur valeur sur α. Par exemple, $\phi_1(\alpha) = \beta$ et alors forcément $\phi_1(\beta) = -\alpha$. Ainsi, il est clair que ϕ_1 est d'ordre 4.

5. C'est immédiat par le point précédent.

Exercice 3.
Montrer que tous les groupes finis sont des groupes de Galois. *Indication: il suffit de prouver le cas du groupe S_n! Pour ce cas en particuler, pensez à permuter les variables de $\mathbb{C}(x_1, \ldots, x_n)$.*

Solution. Let G be a finite group and let $|G| = n$. By Cayley's Theorem, we know that we can embed G as a subgroup of S_n.

Now, consider the ring $F = \mathbb{Q}[x_1, \ldots, x_n]$ and for each $\sigma \in G$ define:

$$\phi_\sigma : F \to F \text{ by } \phi_\sigma(x_i) = x_{\sigma(i)} \text{ for all} 1 \leq i \leq n.$$

One shows that ϕ_σ is a ring homomorphism for all $\sigma \in G$. Moreover, we have that $\phi_\sigma \circ \phi_{\sigma^{-1}} = \phi_{\sigma^{-1}} \circ \phi_\sigma = \mathrm{Id}_F$, hence ϕ_σ is invertible for all $\sigma \in G$ with inverse $\phi_\sigma^{-1} = \phi_{\sigma^{-1}}$.

Let $E = \mathbb{Q}(x_1, \ldots, x_n)$ be the field of fractions of F. Then $\phi_\sigma : F \to E$ is an injective ring homomorhism, as it is the composition of two injective ring homomorphisms.We now apply the universal property of the fraction field, to determine that:

$$\phi_\sigma : E \to E, \text{ where } \phi_\sigma(x_i) = x_{\sigma(i)} \text{ for all } 1 \leq i \leq n$$

is a field homomorphism. Now, one checks that, in fact, ϕ_σ is a $\mathbb{Q}$-automorphism of E.

Let $H = \{\phi_\sigma |\ \sigma \in G\}$ be a subset of $\mathrm{Aut}_{\mathbb{Q}}(E)$. Since $\phi_{\sigma_1} \circ \phi_{\sigma_2} = \phi_{\sigma_1\sigma_2}$ for all $\sigma_1, \sigma_2 \in G$, it follows that H is a subgroup of $\mathrm{Aut}_{\mathbb{Q}}(E)$. Moreover, we have that $H \cong G$, hence H is a finite group. We now apply Theorem 4.6.12 to E and H to deduce that $[E : E^H] = |H| = |\mathrm{Gal}(E/E^H)|$, hence $E^H \subseteq E$ is Galois, see Corollary 4.6.13. We conclude that $\mathrm{Gal}(E/E^H) = H \cong G$.

Remarque. En utilisant des techniques de géométrie algébrique et de topologie algébrique on peut montrer que tout groupe fini est réalisé comme un groupe de Galois d'une extension de $\mathbb{C}(t)$.

1. Avec de la géométrie algébrique, on voit que les extensions finies de $\mathbb{C}(t)$ correspondent à des morphismes de *courbes algébriques* $X \to \mathbb{P}^1_{\mathbb{C}}$ tel que si ont enlève un nombre fini de points à $\mathbb{P}^1_{\mathbb{C}}$, le morphisme devient un revêtement au sens topologique.

2. $\mathbb{P}^1_{\mathbb{C}}$ privé d'un nombre fini de points est le plan complexe $\mathbb{C}$ privé d'un nombre fini de points. Par la topologie algébrique, on sait que $\pi_1(\mathbb{C} \setminus \{p_1, \dots, p_n\}) \cong F_n$ le groupe libre sur n-générateurs. On sait également par la théorie des revêtements, comme tout groupe fini G admet une surjection $F_n \to G$ pour un certain n, qu'il existe un revêtement fini de $\mathbb{C} \setminus \{p_1, \dots, p_n\}$ avec groupe de Galois égal à G.

3. En retournant à la géométrie algébrique, on obtient alors un morphisme de *courbes algébriques* $X \to \mathbb{P}^1_{\mathbb{C}}$ avec groupe de Galois G et donc une extension de $\mathbb{C}(t)$ avec groupe de Galois G.

Si ce genre de choses vous intrigue, le rédacteur vous encourage à suivre des cours de géométrie algébrique et de topologie algébrique, et/ou à faire des projets dans ces domaines.

Exercice 4.
Soit $n \geq 1$. Calculez le groupe de Galois $\mathrm{Gal}(L_n/\mathbb{C}(t))$ où est L_n est le corps de décomposition de

$$f = X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1,$$

de la manière suivante:

1. Montrez qu'il existe des automorphismes $\mathbb{C}(\sqrt{t}) \to \mathbb{C}(\sqrt{t})$ envoyant $\sqrt{t}$ sur $\frac{\sqrt{t}-1}{\sqrt{t}+1}$ et $\frac{\sqrt{t}+1}{\sqrt{t}-1}$.

2. Déduisez que les polynômes $X^n - \frac{\sqrt{t}-1}{\sqrt{t}+1}$ et $X^n + \frac{\sqrt{t}-1}{\sqrt{t}+1}$ sont irréductibles sur $\mathbb{C}(\sqrt{t})$, et que f est irréductible sur $\mathbb{C}(t)$.

3. Montrez que
$$L_n = \mathbb{C}(t)\left(\sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}\right).$$

4. Posons $\xi_n = e^{\frac{2i\pi}{n}}$ et
$$x = \sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}.$$
Montrez qu'il existe $r, s \in \mathrm{Gal}(L_n/\mathbb{C}(t))$ tel que $r(x) = \xi_n x$ et $s(x) = \frac{1}{x}$.

5. Déduire que $\mathrm{Gal}(L_n/\mathbb{C}(t)) \cong D_{2n}$.

Solution.

1. Posons $z = \sqrt{t}$, et considérons le morphisme $\mathbb{C}[z] \to \mathbb{C}(z)$ donné en envoyant z sur $\frac{z-1}{z+1}$ (et fixant $\mathbb{C}$). Montrons que ce morphisme est injectif pour le faire passer au corps des fractions.

   Cela peut certainement se faire à la main, mais voici une petite astuce. Considésons I le noyau de ce morphisme, et supposons que $I \neq 0$. Comme $\mathbb{C}(z)$ est en particulier intègre, ce noyau I est premier, et donc maximal vu que $\mathbb{C}[z]$ est principal. Comme $\mathbb{C}$ est algébriquement clos, alors $I = (z-a)$ pour un certain $a \in \mathbb{C}$. Or, on voit à la main que $z - a$ n'est jamais dans le noyau, donc ce morphisme est bien injectif.

   Ainsi, par la propriété universelle du corps des fractions, il existe un morphisme $\phi\colon \mathbb{C}(z) \to \mathbb{C}(z)$ envoyant z sur $\frac{z-1}{z+1}$. Le même argument montre qu'il existe un morphisme $\psi\colon \mathbb{C}(z) \to \mathbb{C}(z)$ envoyant z sur $\frac{z+1}{z-1}$. Il nous reste à montrer que ϕ et ψ sont des automorphismes. Ces morphismes sont certainment injectifs (tout morphisme de corps est injectif). De plus, $\phi \circ \psi$

envoie z sur $-z$, qui est un automorphisme. En particulier, ϕ est forcément surjectif,et donc aussi automorphisme.

Similairement, $\psi \circ \phi$ envoie z sur $\frac{1}{z}$, qui est aussi un isomorphisme. Le même argument qu'avant montre donc que ψ est aussi un automorphisme.

2. Comme $X^n \pm \sqrt{t}$ est irréductible sur $\mathbb{C}[\sqrt{t}][X]$ par le critère d'Eisenstein, on déduit par le lemme de Gauss que ce polynôme est aussi irreductible sur $\mathbb{C}(t)[X]$. Comme l'image d'un polynôme irréductible par un automorphisme est encore irréductible, on en déduit que les polynômes $X^n - \left(\frac{\sqrt{t}+1}{\sqrt{t}-1}\right)$ et $X^n - \left(\frac{\sqrt{t}-1}{\sqrt{t}+1}\right)$ sont aussi irréductibles sur $\mathbb{C}(\sqrt{t})[X]$.

   Montrons maintenant que f est irréductible sur $\mathbb{C}(t)$, donc écrivons $f = gh$ avec $\deg(g), \deg(h) > 1$. Vu que

$$\left(X^n - \left(\frac{\sqrt{t}+1}{\sqrt{t}-1}\right)\right)\left(X^n - \left(\frac{\sqrt{t}-1}{\sqrt{t}+1}\right)\right) = X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1 = f,$$

   on sait par l'unicité de la décomposition en facteurs irréductibles dans $\mathbb{C}(\sqrt{t})[X]$ que g et h doivent être un des facteurs ci-dessus. Or, aucun de ces facteurs n'est à coefficients dans $\mathbb{C}(t)$ (notez que p.ex. $\frac{\sqrt{t}-1}{\sqrt{t}+1} = \frac{t+1-2\sqrt{t}}{t-1}$), donc on a une contradiction.

3. Comme $\mathbb{C}$ contient toutes les racines n'emes de l'unité, la décomposition de f ci-dessus montre que

$$L_n = \mathbb{C}(t)\left(\sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}, \sqrt[n]{\frac{\sqrt{t}-1}{\sqrt{t}+1}}\right)$$

   (notez que le calcul du point précédent montre que $L_n \ni \sqrt{t}$).

   Posons $x = \sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}$ et $y = \sqrt[n]{\frac{\sqrt{t}-1}{\sqrt{t}+1}}$. Vu que $y = 1/x$, on en déduit que

$$L_n = \mathbb{C}(t)\left(\sqrt[n]{\frac{\sqrt{t}+1}{\sqrt{t}-1}}, \sqrt[n]{\frac{\sqrt{t}-1}{\sqrt{t}+1}}\right).$$

4. Vu que $\xi_n x$ et $1/x$ sont aussi des racines de f (rappelez-vous que $y = 1/x$ et de la décomposition de f) et que L_n est générée par une seule racine de f, on sait par la proposition 4.6.5 l'existence de tels s et r.

5. Notez que r est d'ordre n et s est d'ordre 2. Comme s n'est pas une puissance de r, on sait que $\langle r, s\rangle$ est d'ordre $> n$. D'un autre côté, $|\operatorname{Gal}(L_n/\mathbb{C}(t))| = [L_n : \mathbb{C}(t)] = 2n$, vu que L_n est généré par un élément dont le polynôme minimal f est de degré $2n$. Ainsi, on en déduit que $\langle r, s\rangle = \operatorname{Gal}(L_n/\mathbb{C}(t))$.

   Remarquez que $(rs)^2 = id$. Vu que la présentation du groupe D_{2n} est $\langle \sigma, \tau | \sigma^n = 1\ \tau^2 = 1\ (\sigma\tau)^2 = 1\rangle$, on sait qu'il existe un morphisme surjectif $D_{2n} \to \langle r, s\rangle = \operatorname{Gal}(L_n/\mathbb{C}(t))$ envoyant σ sur r et τ sur s. Comme ces deux groupes sont d'ordre $2n$, cette surjection est automatiquement un automorphisme.