Exercice 1.
Dans les cas suivants, montrez que $\mathbb{Q}(\alpha,\beta)$ est le corps de décomposition d'un polynôme, puis calculez $G = \mathrm{Gal}(\mathbb{Q}(\alpha,\beta)/\mathbb{Q})$, et calculez le polynôme minimal de $\alpha, \alpha+\beta, \alpha\cdot\beta$ et α^{-1}. Pour calculer les polynômes minimaux, on calculera l'orbite de ces éléments par G.

1. $\alpha = \sqrt{3}, \beta = \sqrt{7}$
2. $\alpha = e^{(i\pi/3)}, \beta = -1$
3. $\alpha = e^{(i\pi/3)}, \beta = i$
4. $\alpha = e^{(i\pi/6)}, \beta = i$.

Solution. Throughout, we write $K = \mathbb{Q}(\alpha,\beta)$.

In the following solutions, we use the same technique to find the minimal polynomials as in Example 4.6.15. With Proposition 4.6.14, it holds that for an element $z \in \mathbb{Q}(\alpha,\beta)$, the minimal polynomial is $m_{z,\mathbb{Q}} = \prod_{z'}(x-z')$, where z' is a Galois conjugate of z.

1. As in Exercise 3.4 of sheet 10, we see that $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The elements in G are the identity, σ, with $\sigma(\sqrt{3}) = \sqrt{3}$ and $\sigma(\sqrt{7}) = -\sqrt{7}$, τ with $\tau(\sqrt{3}) = -\sqrt{3}$ and $\tau(\sqrt{7}) = \sqrt{7}$, and $\tau\sigma$, with $\tau\sigma(\sqrt{3}) = -\sqrt{3}$ and $\tau\sigma(\sqrt{7}) = -\sqrt{7}$.

   The elements $\{1, \sqrt{3}, \sqrt{7}, \sqrt{3}\sqrt{7}\}$ form a basis of $\mathbb{Q}(\sqrt{3},\sqrt{7})$ over $\mathbb{Q}$. Now let $z \in \mathbb{Q}(\alpha,\beta)$, with $z = a + b\sqrt{3} + c\sqrt{7} + d\sqrt{3}\sqrt{7}$. The conjugates of z are

   $$z, \quad a+b\sqrt{3}-c\sqrt{7}-d\sqrt{3}\sqrt{7}, \quad a-b\sqrt{3}+c\sqrt{7}-d\sqrt{3}\sqrt{7}, \quad a-b\sqrt{3}-c\sqrt{7}+d\sqrt{3}\sqrt{7}.$$

   As noted above, the minimal polynomial is

   $$m_{z,\mathbb{Q}} = (x-z)(x-(a+b\sqrt{3}-c\sqrt{7}-d\sqrt{3}\sqrt{7}))(x-(a-b\sqrt{3}+c\sqrt{7}-d\sqrt{3}\sqrt{7}))(x-(a-b\sqrt{3}-c\sqrt{7}+d\sqrt{3}\sqrt{7})),$$

   if all factors are different. Hence the minimal polynomials of the elements $\sqrt{3}, \sqrt{3}+\sqrt{7}, \sqrt{3}\cdot\sqrt{7}, \sqrt{3}^{-1}$ are

   $$m_{\sqrt{3},\mathbb{Q}} = x^2 - 3$$
   $$m_{\sqrt{3}+\sqrt{7},\mathbb{Q}} = (x-(\sqrt{3}+\sqrt{7})(x+(\sqrt{3}+\sqrt{7}))(x-(\sqrt{3}-\sqrt{7}))(x+(\sqrt{3}-\sqrt{7})) =$$
   $$(x^2-(10+2\sqrt{21}))(x^2-(10-2\sqrt{21})) = x^4 - 20x^2 + 16$$

   $$m_{\sqrt{3}\cdot\sqrt{7},\mathbb{Q}} = (x-\sqrt{3}\sqrt{7})(x+\sqrt{3}\sqrt{7}) = x^2 - 21$$
   $$m_{\sqrt{3}^{-1},\mathbb{Q}} = x^2 - \frac{1}{3}.$$

2. We note that since $\beta = -1 \in \mathbb{Q}$, it holds that $K = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$. Now, α is a root of the polynomial $x^3+1 = (x+1)(x^2-x+1)$. Since $\alpha \neq -1$, we deduce that α is a root of $f = x^2 - x + 1$. Note that this polynomial is irreducible (otherwise $\alpha \in \mathbb{Q}$, which is not correct). Since f has degree 2 and K has one root, it automatically has the other root of f (in fact, this other root is $\overline{\alpha} = 1/\alpha = e^{-i\pi/3}$). Thus, it is indeed the splitting field of f over $\mathbb{Q}$. Since f is a separable polynomial, we know by Proposition 4.6.5.(4) that G has order 2 (hence $G \cong \mathbb{Z}/2\mathbb{Z}$). Since a non-trivial element in G has no other choice but to send α to $\overline{\alpha}$ (the other root of f) and fix $\mathbb{Q}$, we deduce that $G = \langle\tau\rangle$, where $\tau(\alpha) = \overline{\alpha}$ (in fact, τ is the

complex conjugation here). Indeed, if τ defined as above was not a field automorphism, then we would obtain that $|G| < 2$, a contradiction with our previous discussion.

Let us compute minimal polynomials. We will shortcut a bit compared to the previous exercise, although one could have done the exact same computations! We already computed the minimal polynomial of α: it is $f = x^2 - x + 1$. Since $1/\alpha$ is the other root of f, it also has f as its minimal polynomial.

Since $\alpha^3 = -1$, $(-\alpha)^3 = 1$, so $-\alpha$ is a root of $x^3 - 1 = (x-1)(x^2+x+1)$. As before, we deduce that the minimal polynomial of $-\alpha$ is $x^2 + x + 1$.

Finally, since $\alpha^2 = \alpha - 1$, we deduce that $(\alpha - 1)^3 = 1$. Thus, we conclude as above that the minimal polynomial of $\alpha - 1$ is $x^2 + x + 1$.

We get

$$\begin{aligned} m_{\alpha,\mathbb{Q}} &= (x-\alpha)(x-\overline{\alpha}) = x^2 - x + 1 \\ m_{\alpha+\beta,\mathbb{Q}} &= x^2 + x + 1 \\ m_{\alpha\cdot\beta,\mathbb{Q}} &= x^2 + x + 1 \\ m_{\alpha^{-1},\mathbb{Q}} &= x^2 - x + 1 \end{aligned}$$

3. Let $\alpha = e^{(\pi i/3)}$ and $\beta = i$. Since $\alpha = \cos(\pi/3) + i\sin(\pi/3) = \frac{1}{2} + \frac{1}{2}i\sqrt{3}$, it follows that $\alpha \in \mathbb{Q}(i\sqrt{3})$, and $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(i\sqrt{3})$. With $i\sqrt{3} = 2\alpha - 1$, it follows that $i\sqrt{3} \in \mathbb{Q}(\alpha)$, and $\mathbb{Q}(i\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$. With this, it follows that $\mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{3})$. Furthermore, $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(i\sqrt{3}, i) = \mathbb{Q}(\sqrt{3}, i)$. As in Example 4.6.7 (c), we see that $\mathrm{Gal}(\mathbb{Q}(\sqrt{3},i)/\mathbb{Q})$ contains 4 elements, the identity, σ, τ and $\sigma\tau$, where $\sigma(i) = i, \sigma(\sqrt{3}) = -\sqrt{3}, \tau(i) = -i, \tau(\sqrt{3}) = \sqrt{3}$ and $\sigma\tau(i) = -i, \sigma\tau(\sqrt{3}) = -\sqrt{3}$, and that $\mathrm{Gal}(\mathbb{Q}(\sqrt{3},i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On the elements α and β, those four elements act as follows:

$$\sigma(\alpha) = e^{-(i\pi/3)}, \sigma(\beta) = \beta, \quad \tau(\alpha) = e^{-(i\pi/3)}, \sigma(\beta) = -\beta, \quad \sigma\tau(\alpha) = \alpha, \sigma\tau(\beta) = -\beta.$$

As for the first example, we remark that the elements $\{1, i, \sqrt{3}, i\sqrt{3}\}$ form a basis of $\mathbb{Q}(\sqrt{3}, i)$ over $\mathbb{Q}$. Let $z \in \mathbb{Q}(\sqrt{3}, i)$ with $z = a + bi + c\sqrt{3} + d\sqrt{3}i$. Then, as stated above, the minimal polynomial of z is of the following form, if all factors are different

$$\begin{aligned} m_{z,\mathbb{Q}} &= (x-z)(x-\sigma(z))(x-\tau(z))(x-\sigma\tau(z)) \\ &= (x-z)(x-(a+bi-c\sqrt{3}-d\sqrt{3}i))(x-(a-bi+c\sqrt{3}-d\sqrt{3}i))(x-(a-bi-c\sqrt{3}+d\sqrt{3}i)). \end{aligned}$$

This leads for example that

$$m_{\alpha+\beta,\mathbb{Q}} = x^4 - 2x^3 + 5x^2 - 4x + 1.$$

Let us compute the other minimal polynomials in an easier way. We already computed $m_{\alpha,\mathbb{Q}} = m_{1/\alpha,\mathbb{Q}} = x^2 - x + 1$ in the previous point. Note that $\alpha\beta = ie^{i\pi/3}$, which is annihilated by $x^6 + 1 = (x^2+1)(x^4 - x^2 + 1)$. Since it is not killed by $x^2 + 1$, we deduce that it is killed by $x^4 - x^2 + 1$. Since the minimal polynomial of $\alpha\beta$ has degree 4 (c.f. the expression above, since $\alpha\beta$, $\sigma(\alpha\beta)$, $\tau(\alpha\beta)$ and $\sigma\tau(\alpha\beta)$ are all different), we deduce that its minimal polynomial is actually $x^4 - x^2 + 1$.

4. Let $\alpha = e^{(i\pi/6)}$ and $\beta = i$. We first calculate $G = \mathrm{Gal}(\mathbb{Q}(\alpha,\beta)/\mathbb{Q})$. We remark that $\beta = \alpha^3$, and hence $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$. Furthermore, α is a root of the polynomial $x^6 + 1$, which decomposes as $x^6 + 1 = (x^2+1)(x^4 - x^2 + 1)$. The polynomial $x^2 + 1$ has two complex roots $\pm i$. The polynomial $x^4 - x^2 + 1$ has four complex roots $\alpha, \alpha^5, \alpha^7, \alpha^{11}$. Furthermore, this polynomial is irreducible over $\mathbb{Q}$.

Hence the minimal polynomial of α is $m_{\alpha,\mathbb{Q}} = x^4 - x^2 + 1$. Since by adjoining α to $\mathbb{Q}$, all roots of $m_{\alpha,\mathbb{Q}}$ are adjoined as well, we remark that $\mathbb{Q}(\alpha)$ is the splitting field of the polynomial $x^4 - x^2 + 1$ over $\mathbb{Q}$. By Proposition 4.6.3 (4), we get that $|G| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg m_{\alpha,\mathbb{Q}} = 4$. The elements in G are the identity, τ, σ, η, where the root α gets sent to a root of $x^4 - x^2 + 1$ by every element of G. We let $\tau(\alpha) = \alpha^5, \sigma(\alpha) = \alpha^7, \eta(\alpha) = \alpha^{11}$.

The minimal polynomials are calculated as stated above by observing the action of the elements id, τ, σ, η. It follows that

$$m_{\alpha,\mathbb{Q}} = (x-\alpha)(x-\tau(\alpha))(x-\sigma(\alpha))(x-\eta(\alpha)) = (x-\alpha)(x-\alpha^5)(x-\alpha^7)(x-\alpha^{11}) = x^4 - x^2 + 1$$

$$m_{\alpha+\beta,\mathbb{Q}} = m_{\alpha+\alpha^3,\mathbb{Q}} = (x-(\alpha+\alpha^3))(x-\tau(\alpha+\alpha^3))(x-\sigma(\alpha+\alpha^3))(x-\eta(\alpha+\alpha^3))$$
$$= (x-(\alpha+\alpha^3))(x-(\alpha^5+\alpha^3))(x-(\alpha^7+\alpha^9))(x-(\alpha^{11}+\alpha^9)) = x^4 + 3x^2 + 9$$

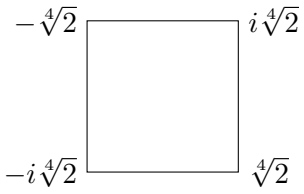
$$m_{\alpha\cdot\beta,\mathbb{Q}} = m_{\alpha^4,\mathbb{Q}} = m_{-0.5+0.5i\sqrt{3},\mathbb{Q}} = (x-\alpha^4)(x-\tau(\alpha^4))(x-\sigma(\alpha^4))(x-\eta(\alpha^4))$$
$$= (x-\alpha^4)(x-\alpha^8)\cancel{(x-\alpha^4)(x-\alpha^8)} = x^2 + x + 1$$

$$m_{\alpha^{-1},\mathbb{Q}} = m_{\alpha^{11},\mathbb{Q}} = (x-\alpha^{11})(x-\tau(\alpha^{11}))(x-\sigma(\alpha^{11}))(x-\eta(\alpha^{11}))$$
$$= (x-\alpha^{11})(x-\alpha^7)(x-\alpha^7)(x-\alpha) = x^4 - x^2 + 1$$

Exercice 2. 1. Montrez que $K = \mathbb{Q}(i, \sqrt[4]{2})$ est le corps de décomposition de $x^4 - 2 \in \mathbb{Q}[x]$.

2. Montrez qu'il existe $r, s \in \mathrm{Gal}(K/\mathbb{Q})$ tel que
   (a) $r(\sqrt[4]{2}) = i\sqrt[4]{2}$ et $r(i) = i$,
   (b) $s(\sqrt[4]{2}) = -\sqrt[4]{2}$ et $s(i) = -i$.

3. Déduire que si l'on nomme les sommets d'un carré selon les racines de $x^4 - 2$ comme ci-dessous



   le groupe $\mathrm{Gal}(K, \mathbb{Q})$ est isomorphe au groupe D_8 des symétries du carré.

4. Donner un élément $\alpha \in K$ avec $\mathbb{Q}(\alpha) = K$.

5. Pour tous les éléments suivants de K

$$3 + \sqrt{2}, \quad i + \sqrt{2}, \quad 1 + \sqrt[4]{2} \quad 1 + i\sqrt[4]{2}, \quad \sqrt[4]{2}(1+i) \quad \sqrt[4]{2}(1-i)$$

   déterminer,
   (a) l'orbite de ces éléments par $\mathrm{Gal}(K/\mathbb{Q})$,
   (b) leur polynôme minimal,
   (c) le stabilisateur de ces éléments dans $\mathrm{Gal}(K/\mathbb{Q})$.*

Solution.

1. Les racines de $x^4 - 2$ sont $\pm\sqrt[4]{2}$ et $\pm i\sqrt[4]{2}$, et l'extension de $\mathbb{Q}$ générée par ces éléments est bel et bien K.

*C'est à dire si α est un tel élément, $\mathrm{Gal}(K/\mathbb{Q}(\alpha))$.

2. Montrons d'abord que $[K:\mathbb{Q}]=8$. Comme x^4-2 est irréductible sur $\mathbb{Z}[x]$ par Eisenstein et primitif, il est aussi irréductible sur $\mathbb{Q}[x]$ par les lemmes de Gauss. Ainsi, $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=4$. Comme $i\notin\mathbb{Q}(\sqrt[4]{2})$, on en déduit que le polynôme minimal de i sur $\mathbb{Q}(\sqrt[4]{2})$ est x^2+1, et donc $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}(\sqrt[4]{2})]=2$. On en déduit donc que $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}]=8$ par multiplicativité des degrés.

   Vu que $8=[K:\mathbb{Q}]=[K:\mathbb{Q}(i)][\mathbb{Q}(i):\mathbb{Q}]$, on en déduit que $[K:\mathbb{Q}(i)]=4$. Ainsi, x^4-2 est nécessairement le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}(i)$ (sinon cette extension serait de degré <4). Par la proposition 4.6.5.(3), le groupe de Galois de $K/\mathbb{Q}(i)$ agit transitivement sur les racines de x^4-2, donc on obtient l'existence de r comme dans (a).

   Montrons maintenant l'existence de s. Notez que $r^2(\sqrt[4]{2})=-\sqrt[4]{2}$ et $r^2(i)=i$. Ainsi, si l'on considère s comme la composée de r^2 et de la conjugaison complexe habituelle, alors $s(\sqrt[4]{2})=-\sqrt[4]{2}$ et $s(i)=-i$.

3. Par le point précédent, cette extension est un corps de décomposition. Vu qu'elle est séparable ($\mathbb{Q}$ est parfait, car de caractéristique zéro), on en déduit par la Proposition 4.6.5 que $|\operatorname{Gal}(K/\mathbb{Q})|=8$. Montrons que $\langle r,s\rangle=\operatorname{Gal}(K/\mathbb{Q})$. Vu que r est d'ordre 4 et que s n'est pas une puissance de r (tout ceci de vérifie à la main), on obtient que $\langle r,s\rangle$ contient au moins 5 éléments. Comme son ordre doit diviser 8, on en déduit que

$$\langle r,s\rangle=\operatorname{Gal}(K/\mathbb{Q}).$$

   Nous allons conclure de deux manières différentes:

   (a) Par la géométrie: notez que r et s agissent par isométries sur le carré de la donnée (r est une rotation d'un quart de tour dans le sens anti-horaire, et s est la symmétrie d'axe d'en bas à gauche vers en haut à droite). Cette action est nécessairement fidèle, car ces quatre sommets génèrent K sur $\mathbb{Q}$.
   Ainsi, $\langle r,s\rangle$ agit fidèlement par isométries sur ce carré. Comme le groupe d'isométries du carré est D_8 (donc d'ordre 8), on a une injection $\langle r,s\rangle\hookrightarrow D_8$ est un isomorphisme. Comme $\operatorname{Gal}(K/\mathbb{Q})=\langle r,s\rangle$ est d'ordre 8, on conclut que $\operatorname{Gal}(K/\mathbb{Q})\cong D_8$.

   (b) Par la théorie des groupes: on calcule à la main que $r^4=id, s^2=id$ et $(rs)^2=id$. Comme D_8 a comme présentation $\langle\sigma,\tau|\sigma^4=1\ \tau^2=1\ (\sigma\tau)^2=1\rangle$, on obtient par définition l'existence d'un morphisme surjectif $D_8\to\langle r,s,\rangle=\operatorname{Gal}(K/\mathbb{Q})$ envoyant σ sur r et τ sur s. Comme ces deux groupes sont d'ordre 8, on conclut que notre morphisme est un isomorphisme.

4. Comme on l'a vu au point précédent, on a que $\operatorname{Gal}(K/\mathbb{Q})=\langle r,s\rangle=\{1,r,r^2,r^3,s,sr,sr^2,sr^3\}$. Prenons $\alpha=\sqrt[4]{2}+i$. Vu qu'une $\mathbb{Q}$-base de K est donnée par $\{1,i,\sqrt[4]{2},\sqrt{2},(\sqrt[4]{2})^3,i\sqrt[4]{2},i\sqrt{2},i(\sqrt[4]{2})^3\}$, un calcul direct montre que cet élément n'est fixé par aucun $g\neq id$ de $\operatorname{Gal}(K/\mathbb{Q})$, donc c'est bien un élément primitif.

5. - $3+\sqrt{2}$: Comme 3 est forcément fixé et que $\sqrt{2}$ ne peut être qu'envoyé sur $\pm\sqrt{2}$ (les racines de $x^2-2\in\mathbb{Q}[x]$), on déduit que l'orbite de $3+\sqrt{2}$ est incluse dans $\{3\pm\sqrt{2}\}$. Vu que $r(3+\sqrt{2})=3-\sqrt{2}$, on conclut que l'orbite de $3+\sqrt{2}$ est bien $\{3+\sqrt{2},3-\sqrt{2}\}$. Par la proposition 4.6.14, on a que son polynôme minimal est

$$(x-(3+\sqrt{2}))(x-(3-\sqrt{2}))=x^2-6x+7.$$

     On voit par un calcul direct que r^2 et s fixent $3+\sqrt{2}$, donc $\operatorname{Gal}(K/\mathbb{Q}(3+\sqrt{2}))$ contient $\{id,r^2,s,sr^2\}$. Vu que $|\operatorname{Gal}(K:\mathbb{Q})/\operatorname{Gal}(K:\mathbb{Q}(3+\sqrt{2}))|$ est égale à la taille de l'orbite de $3+\sqrt{2}$ (qui vaut 2), on déduit que $\operatorname{Gal}(K/\mathbb{Q}(3+\sqrt{2}))$ a taille 4, donc

$$\operatorname{Gal}(K/\mathbb{Q}(3+\sqrt{2}))=\{id,r^2,s,sr^2\}.$$

- $i+\sqrt{2}$: Nous avons déjà vu par le passé que $\mathbb{Q}(i+\sqrt{2}) = \mathbb{Q}(i,\sqrt{2})$, donc il génère une extension d'ordre 4. L'orbite de $i+\sqrt{2}$ est donc de taille 4 par la proposition 4.6.5. Comme i est forcément envoyé sur $\pm i$ et $\sqrt{2}$ sur $\pm\sqrt{2}$, on a au plus 4 éléments dans l'orbite : $\pm\sqrt{2} \pm i$.

  Comme on en a exactement 4, on en déduit que l'orbite est exactement ces quatre éléments ci-dessus. Comme vu en cours, le polynôme minimal est alors

  $$(x-(i+\sqrt{2}))(x+(i+\sqrt{2}))(x-(i-\sqrt{2}))(x+(i-\sqrt{2})) = (x^2-(1+2i\sqrt{2}))(x^2-(1-2i\sqrt{2})) = x^4-2x^2+9.$$

  Le même argument montre que le stabilisateur est d'ordre 2. Comme r^2 stabilise cet élément, on en déduit que le stabilisateur est exactement $\{id, r^2\}$.
- On a que $\mathbb{Q}(1+\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$ est un extension de degré 4 sur $\mathbb{Q}$, donc l'orbite est de taille 4. Comme l'orbite de $1+\sqrt[4]{2}$ par $\langle r\rangle$ est $\{1+\sqrt[4]{2}, 1+i\sqrt[4]{2}, 1-\sqrt[4]{2}, 1-i\sqrt[4]{2}\}$, on a trouvé notre orbite.

  Notez de $(x-1)^4-2$ annule cet élément. Vu que ce polynôme est de degré $4 = [\mathbb{Q}(1+\sqrt[4]{2}) : \mathbb{Q}]$, c'est forcément le polynôme minimal.

  Finalement, on sait comme avant que le stabilisateur est d'ordre 2. Comme sr^2 stabilise cet élément, on en déduit que le stabilisateur est exactement $\{1, sr^2\}$.
- Remarquez que $1+i\sqrt[4]{2}$ est dans l'orbite de $1+\sqrt[4]{2}$, donc ces éléments ont la même orbite, et donc le même polynôme minimal

  Quant au stabilisateur, celui-ci sera conjugué, précisément par un élément du groupe de Galois qui envoie $1+\sqrt[4]{2}$ sur $1+i\sqrt[4]{2}$ – r est un tel élément. On déduit que le stabilisateur est $\{id, s\}$. Cela se voyait aussi directement comme s fixait $1+i\sqrt[4]{2}$.
- L'orbite de $\sqrt[4]{2}(1+i)$ par $\langle r\rangle$ est exactement

  $$\{\sqrt[4]{2}(1+i), i\sqrt[4]{2}(1+i), -\sqrt[4]{2}(1+i), -i\sqrt[4]{2}(1+i)\}.$$

  Vu que la taille de l'orbite divise la taille du groupe de Galois (i.e. 8), on aurait que si l'orbite était plus grande que l'ensemble ci-dessus, alors le stabilisateur serait trivial. Or, sr^3 est dans ce stabilisateur, et donc l'orbite est exactement de taille 4 (et est donnée ci-dessus), et le stabilisateur est exactement $\{id, sr^3\}$.

  On pourrait trouver le polyôme minimal en faisant un calcul fastidieux, mais trouvons-le plutôt à la main. on a que

  $$(\sqrt[4]{2}(1+i))^4 = 2(1+i)^4 = -8,$$

  donc c'est une racine de x^4+8. Vu que l'extension générée est de degré 4, c'est donc le polynôme minimal.
- Comme $\sqrt[4]{2}(1-i) = -i\sqrt[4]{2}(1+i)$ est dans l'orbite de $\sqrt[4]{2}(1+i)$, on conclut qu'ils ont la même orbite, et donc le même polynôme minimal.

  Quant au stabilisateur, il est conjugé au précédent et donc c'est $\{id, sr\}$.

Exercice 3.
Soit $f = x^3+ax+1 \in \mathbb{Q}[x]$ avec $a > 0$, $a \in \mathbb{Z}$.

1. Montrer que f est irréductible sur $\mathbb{Q}$.
2. Montrer que f a une racine réelle, mais pas trois.
3. Soit $K = \mathbb{Q}[x]/(f)$. Montrer que $K/\mathbb{Q}$ est une extension de degré 3 qui n'est pas Galoisienne.
4. Soit L le corps de décomposition de f sur $\mathbb{Q}$. Montrer que $\mathrm{Gal}(L/Q) \cong S_3$.

Solution.

1. As $\deg f = 3$ one just has to verify that f does not have a root over $\mathbb{Q}$. So, we need to show that if b and c are non-zero relatively prime integers, then

$$(b/c)^3 + (ab/c) + 1 \neq 0,$$

or equivalently

$$b^3 + abc^2 + c^3 \neq 0.$$

Suppose the contrary. Then c divides b^3 and b divides c^3. Using the relative prime assumption we obtain both b and c are plus-minus 1, so that a root has to be 1 or -1 but one sees as $a > 0$ that

$$1 + a + 1 \neq 0 \quad \text{and} \quad -1 - a + 1 \neq 0.$$

2. Since $f(x)$ tends to $-\infty$ as x goes to $-\infty$ and goes to $+\infty$ as x goes to $+\infty$, we deduce by the mean value theorem that f has at least one real root. Now, let α, β and γ be the three roots of f in its splitting field, and assume that they are all real. Then we have

$$f = (x - \alpha)(x - \beta)(x - \gamma)$$

and hence

$$\alpha + \beta + \gamma = 0$$

and

$$\alpha\beta + \alpha\gamma + \beta\gamma = a$$

From the first equation we have $\gamma = -\alpha - \beta$. Plugging this into the left side of the second equation yields

$$\alpha\beta + \alpha(-\alpha - \beta) + \beta(-\alpha - \beta) = -\alpha^2 - \beta^2 - \alpha\beta = -\frac{1}{2}(\alpha + \beta)^2 - \frac{\alpha^2}{2} - \frac{\beta^2}{2} \leq 0$$

However, we assumed that $a > 0$. This is a contradiction.

Once we know that not all roots are real, here is a slick way to deduce that f must have a real root. As $\deg f = 3$, and complex roots of a real polynomial come in complex conjugate pairs, f has to have a real root.

3. Let α denote the unique real root. Then, $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is a degree 3 extension and additionally $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Hence, the other two roots of f, say β and γ, cannot be contained in $\mathbb{Q}(\alpha)$. So, every element $g \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ can send α only to α. However, as α generated $\mathbb{Q}(\alpha)$ this means that $g = \mathrm{id}$.

4. Let α, β and γ be as in the previous point. Then both β and γ are roots of $h = \frac{f}{x-\alpha} \in \mathbb{Q}(\alpha)[x]$. As this polynomial has degree 2, and β and γ are not in $\mathbb{Q}[x]$, $h = m_{\beta,\mathbb{Q}(\alpha)} = m_{\gamma,\mathbb{Q}(\alpha)}$. So, $\mathbb{Q}(\alpha, \beta, \gamma)$ has degree 2 over $\mathbb{Q}(\alpha)$. So, by the multiplicativity of the degrees of field extensions, $L = \mathbb{Q}(\alpha, \beta, \gamma)$ has degree 6 over $\mathbb{Q}$. Let G be the Galois group of L over $\mathbb{Q}$. Then, G acts faithfully on α, β and γ, which yields an embedding $G \hookrightarrow S_3$. As both have 6 elements, this is in fact an isomorphism.

Exercice 4.
Soit K un corps de caractéristique $p > 0$, et $\alpha \neq 0 \in K$ tel que le pôlynome $f(x) = x^p - x + \alpha \in K[x]$ n'a pas de racines dans K. Soit L le corps de decomposition de f, et $G = \mathrm{Gal}(L/K)$.

1. Montrez que $G \cong \mathbb{Z}/p\mathbb{Z}$. *Indication: Si β est une racine de f, alors $\beta + \gamma$ l'est aussi, pour tout $\gamma \in \mathbb{F}_p$.*

2. Montrez que le pôlynome f est irréductible sur K.

3. Considérons $K = \mathbb{F}_p(t)$. Montrez que le pôlynome $f(x) = x^p - x + t \in K[x]$ n'a pas de racines dans K.

4. Soit K et f comme dans le point précédent. Donnez le corps de décomposition de f sur K.

Solution.

1. Let β be a root of f. It holds that $\beta^p - \beta + \alpha = 0$. Let $\gamma \in \mathbb{F}_p \subseteq K$. Then, using Fermat's little theorem, which states that $\gamma^p = \gamma$ modulo p, it holds that over a field of characteristic p, we have

$$(\beta+\gamma)^p - (\beta+\gamma) + \alpha = \beta^p + \gamma^p - \beta - \gamma + \alpha = \beta^p + \gamma - \beta - \gamma + \alpha = \beta^p - \beta + \alpha = 0.$$

   Hence all $\beta + \gamma$, where $\gamma \in \mathbb{F}_p$ are roots of f. We get p distinct roots, and as $\mathbb{F}_p \subseteq K$, by adjoining β to K, all roots are contained in $K(\beta)$ and hence $L = K(\beta)$.

   Moreover, we have that $m_{\beta,K} = f$. Let $m_{\beta,K} = \prod_{\gamma\in I}(x-(\beta+\gamma)$ in $L[x]$ with $I \subset \mathbb{F}_p[x]$. Then the coefficients in front of $x^{|I|-1}$ are exactly $-\sum_{\gamma\in I(\beta+\gamma)} = |I|\beta + \sum_{\gamma\in I}\gamma$. If we suppose that $|I| < p$, one contradicts the fact that $\beta \notin K$. Therefore $m_{\beta,K} = f$.

   We use Proposition 4.6.3 and get the following: by (a), G acts on the roots of f. By (b), since $L = K(\beta)$, there is at most one element in G that sends the root β to the root $\beta + \gamma$, for $\gamma \in \mathbb{F}_p$. Therefore, $|G| \leq p$. There are indeed p elements in G, which are of the form σ_γ, with $\sigma_\gamma(\beta) = \beta + \gamma$ for all $k \in \mathbb{F}_p$. We get p automorphisms, and hence $G \cong \mathbb{Z}/p\mathbb{Z}$.

2. The fact that f is irreducible over K follows from Prop 4.6.3 (d), which states that $|G| = [L : K]$, where $L = K(\beta)$ is the splitting field of f. By the previous point, $|G| = p$, and hence $[K(\beta) : K] = \deg m_{\beta,K} = p$. Since β is a root of f, and since its minimal polynomial is of degree p, it follows that $f \sim m_{\beta,K}$, and hence, f is irreducible over K.

3. Let $\frac{g}{h} \in \mathbb{F}_p(t)$ a root of $x^p - x + t$. Then, $g, h \in \mathbb{F}_p[t], h \neq 0$ and it holds that

$$\left(\frac{g}{h}\right)^p - \left(\frac{g}{h}\right) + t = 0 \Leftrightarrow g^p - gh^{p-1} + th^p = 0.$$

   Denote the degree of g by d_g, and the degree of h by d_h. Then, the degree of the following polynomials are

$$\deg(g^p) = pd_g, \quad \deg(gh^{p-1}) = d_g + (p-1)d_h, \quad \deg(th^p) = 1 + pd_h.$$

   In order for the sum $g^p - gh^{p-1} + th^p$ to be zero, the degrees of each of the summands needs to be canceled out.

   If $d_h \geq d_g$, then the degree of th^p, being $1+pd_h$, is strictly bigger than pd_g and $d_g+(p-1)d_h$ and hence th^p can't be canceled out, and the sum of polynomials can only be zero if $h = 0$, but this is a contradiction to the choice of g, h.

   On the other hand, if $d_g > d_h$, then nothing can cancel out g^p, which one sees by a degree comparison, and hence the sum $g^p - gh^{p-1} + th^p$ can only be zero if $g = 0$ and $h = 0$, which is a contradiction.

4. Let u be a root of f : $u^p - u + t = 0 \Leftarrow u^p - u = -t$, and hence $\mathbb{F}(t) \subseteq \mathbb{F}_p(u)$. With u being transcendental over $\mathbb{F}_p$, it follows that the splitting field is $\mathbb{F}_p(u)$. We remark that by the second part of the exercise, all roots are of the form $u + \gamma$, where $\gamma \in \mathbb{F}_p$, and hence all roots are contained in $\mathbb{F}_p(u)$.

Exercice 5.
Soit $K \subseteq L \subseteq E$ une extension algébrique tel que $K \subseteq L$ et $L \subseteq E$ sont Galois. Montrer que $K \subseteq E$ n'est pas forcément Galois.
Indication. Envisager les extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$ ou $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

Solution. We have the following extension tower:

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

The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is Galois, as $\mathbb{Q}$ is a perfect field and $\mathbb{Q}(\sqrt{2})$ is the decomposition field of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$, see Theorem 4.6.15. Similarly, the extension $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is Galois, as $\mathbb{Q}(\sqrt{2})$ is perfect and $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ is the decomposition field of the polynomial $x^2 - 1 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$.

We now consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$. We note that this extension is of degree 4. We also note by devellopping

$$(x^2 - (1+\sqrt{2}))(x^2 - (1-\sqrt{2}))$$

that $\sqrt{1+\sqrt{2}}$ is a root of the polynomial $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$, hence $m_{\sqrt{1+\sqrt{2}},\mathbb{Q}}(x) = x^4 - 2x^2 - 1$ by the degree because $[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}] = 4$. Moreover, the other roots of $x^4 - 2x^2 - 1$ are $-\sqrt{1+\sqrt{2}}$ and $\pm\sqrt{1-\sqrt{2}}$. Now, we remark that $\mathbb{Q}(\sqrt{1+\sqrt{2}}) \subseteq \mathbb{R}$, therefore $\pm\sqrt{1-\sqrt{2}} \notin \mathbb{Q}(\sqrt{1+\sqrt{2}})$.

It follows that the extension is not Galois: indeed in a Galois extension L/K for $\alpha \in L$ the polynominal $m_{\alpha,K}$ has all its roots in L, these roots being the orbit of the element α by the Galois group. But this was just shown no to be the case for $\sqrt{1+\sqrt{2}}$.

A similar argument works also for

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}).$$