Leonid Monin
Léo Navarro Chafloque

Solutions – Semaine 13

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.
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

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

Exercice 3 (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 $\operatorname{Gal}(L/\mathbb{Q})$. Again, there are 7 of them and each of these is generated by two distinct elements of order 2 of $\operatorname{Gal}(L/\mathbb{Q})$ 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 $|\operatorname{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$. 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:

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

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 $|\operatorname{Gal}(E/\mathbb{Q})| = 8$.

Since $E/\mathbb{Q}(\sqrt{1+\sqrt{2}})$ has degree 2 and is Galois, there exists $\tau \in \operatorname{Gal}(E/\mathbb{Q})$ 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 $\sigma' \in \operatorname{Gal}(E/\mathbb{Q}(i))$ 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

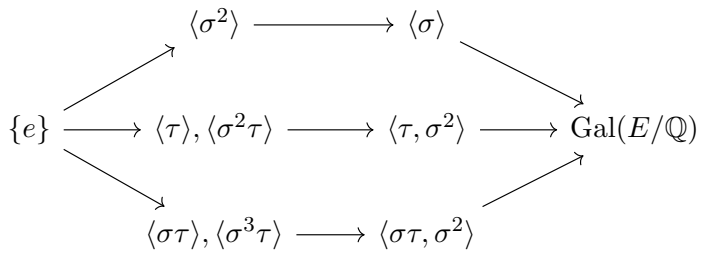
$$\alpha, \quad -\alpha, \quad i\alpha^{-1}, \quad -i\alpha^{-1}.$$

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 $\operatorname{Gal}(E/\mathbb{Q})$ 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 $\operatorname{Gal}(E/\mathbb{Q}) \cong D_8$.

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

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

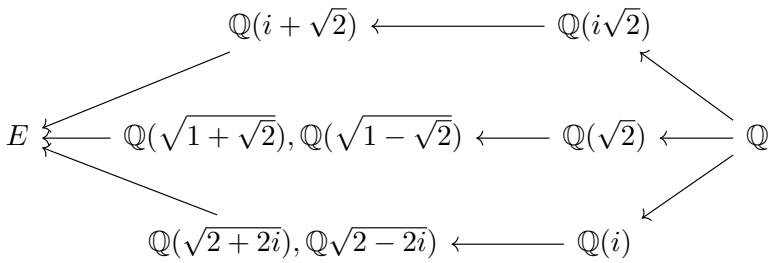
Also, note that squaring we deduce that,

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

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

Supposons tout d'abord que $a^2 - b^2 d$ 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 $(\alpha\beta)^2 = a^2 - b^2 d$, 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 $a^2 - b^2 d$ 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 5.
Soit $K \subseteq L$ une extension Q_8-galoisienne (où Q_8 est le groupe des quaternions), et soit $f \in K[x]$ un polynôme irréductible tel que L est un corps de décomposition de f. Démontrez que $\deg f = 8$.

Solution.

Supposons par l'absurde que $d := \deg(f) < 8$, et soit $\alpha \in L$ une racine de f. Alors $[K(\alpha) : K] = d < 8$, donc il suffit de montrer que $K(\alpha) = L$ pour obtenir une contradiction.

Comme tous les sous-groupes de Q_8 sont normaux (nous vous laissons le soin de faire ce calcul), l'extension $K(\alpha)/K$ est Galoisienne par le théorème fondamental de la théorie de Galois. On sait que dans une extension Galoisienne, tout les polynômes minimaux des éléments scindent, les racines de ces polynômes étant formant des orbites sous le groupe de Galois. O<n en déduit que $m_{\alpha,K} = f$ se scinde sur $K(\alpha)$. Comme L est le corps de décomposition de L, on a donc forcément que $L = K(\alpha)$, ce qui donne une contradiction.