

**Exercice 1.** (a) As  $\alpha \notin K^p$  it follows that for all  $\beta \in K$  we have  $\beta^p \neq \alpha$  and thus  $x^p - \alpha \in K[x]$  does not admit roots in  $K$ . Let  $F$  be a decomposition field of  $x^p - \alpha$  over  $K$  and let  $\beta \in F$  be a root of this polynomial. We have that:

$$x^p - \alpha = x^p - \beta^p = (x - \beta)^p \text{ in } F[x].$$

Let  $m_{\beta,K}(x) \in K[x]$  denote the minimal polynomial of  $\beta$  over  $K$ . As  $\beta$  is a root of  $x^p - \alpha$ , it follows that  $m_{\beta,K}(x) | x^p - \alpha = (x - \beta)^p$ . Therefore there exists some  $i$ ,  $1 \leq i \leq p$ , such that  $m_{\beta,K}(x) = (x - \beta)^i$ . Now, as  $m_{\beta,K}(x) \in K[x]$  we have that:

$$(x - \beta)^i = \sum_{j=0}^i (-1)^j \binom{i}{j} x^{i-j} \beta^j = x^i - i\beta x^{i-1} + \dots + (-1)^i \beta^i \in K[x].$$

It follows that  $-i\beta = 0$  and so  $i = p$ . Therefore  $m_{\beta,K}(x) = (x - \beta)^p = x^p - \alpha$  and we conclude that  $x^p - \alpha \in K[x]$  is irreducible.

- (b) To show that  $L$  is a field, we will show that the polynomial  $y^2 - x(x-1)(x+1) \in (\mathbb{F}_p(x))[y]$  is irreducible. As  $y^2 - x(x-1)(x+1)$  is a unitary polynomial, it is primitive and so, by Gauss III, it is irreducible in  $(\mathbb{F}_p(x))[y]$  if and only if it is irreducible in  $(\mathbb{F}_p[x])[y]$ . Now,  $x \in \mathbb{F}_p[x]$  is irreducible and we use Eisenstein with " $p = x$ " (here  $p$  denotes the irreducible in Eisenstein criterion) to deduce that  $y^2 - x(x-1)(x+1)$  is irreducible in  $(\mathbb{F}_p[x])[y]$ .
- (c) By Proposition 4.5.7, as  $\text{char}(L) = p$ , we have that  $L$  is perfect if and only if  $L^p = L$ . We will show that  $x \notin L^p$ .

Assume by contradiction that  $x \in L^p$ . Then, there exists  $f \in L$  such that  $x = f^p$ . It follows that  $f \in L$  is a root of the polynomial  $t^p - x \in \mathbb{F}_p(x)[t]$ . As  $x \in \mathbb{F}_p(x)$  is not a  $p^{\text{th}}$  power, we see this using from example the degree of polynomials, it follows that the polynomial  $t^p - x$  is irreducible in  $(\mathbb{F}_p(x))[t]$ , see item (a). This shows that  $m_{f,\mathbb{F}_p(x)}(t) \sim t^p - x \in (\mathbb{F}_p(x))[t]$ .

Consider the chain of extensions:

$$\mathbb{F}_p(x) \subseteq (\mathbb{F}_p(x))(f) \subseteq L$$

and we have  $[(\mathbb{F}_p(x))(f) : \mathbb{F}_p(x)] | [L : \mathbb{F}_p(x)]$ . But  $[L : \mathbb{F}_p(x)] = 2$  and  $[(\mathbb{F}_p(x))(f) : \mathbb{F}_p(x)] = p$ , where  $p \neq 2$ . We have arrived at a contradiction.

- (d) We have that  $L = (\mathbb{F}_2(x))[y]/(y^2 + x(x+1)^2)$ . Note that the polynomial  $y^2 + x(x+1)^2 \in (\mathbb{F}_2(x))[y]$  admits  $\sqrt{x}(x+1)$  as a double root and so it is irreducible in  $(\mathbb{F}_2(x))[y]$ . Now, by Proposition 4.2.25, it follows that  $L = (\mathbb{F}_2(x))(\sqrt{x}(x+1)) = (\mathbb{F}_2(x))(\sqrt{x}) = \mathbb{F}_2(\sqrt{x})$ . For the last equality, note that  $\mathbb{F}_2(\sqrt{x}) \subseteq (\mathbb{F}_2(x))(\sqrt{x})$  and, as  $\mathbb{F}_2(x) \subseteq \mathbb{F}_2(\sqrt{x})$ , we have  $(\mathbb{F}_2(x))(\sqrt{x}) \subseteq (\mathbb{F}_2(\sqrt{x}))(\sqrt{x}) = \mathbb{F}_2(\sqrt{x})$ .

As  $\text{char}(L) = 2$ , it follows that  $L$  is perfect if and only if  $L^2 = L$ , see Proposition 4.5.7. But

$$\begin{aligned} L^2 &= \{f(\sqrt{x})^2 \mid f(\sqrt{x}) \in L\} = \left\{ \left( \frac{f_1(\sqrt{x})}{f_2(\sqrt{x})} \right)^2 \mid f_1(\sqrt{x}), f_2(\sqrt{x}) \in \mathbb{F}_2[\sqrt{x}], f_2(\sqrt{x}) \neq 0 \right\} \\ &= \left\{ \frac{f_1(x)}{f_2(x)} \mid f_1(x), f_2(x) \in \mathbb{F}_2[x], f_2(x) \neq 0 \right\} = \mathbb{F}_2(x) \end{aligned}$$

and clearly  $\sqrt{x} \notin L^2$ .

**Exercise 2(a)(i)** Let  $\alpha \in L \setminus K$ . As  $\alpha^2 \in K$ , it follows that  $\alpha$  is a root of the polynomial  $x^2 + \alpha^2 \in K[x]$  and thus  $[K(\alpha) : K] \leq 2$ . On the other hand, we have that  $[K(\alpha) : K] \geq 2$ , as  $\alpha \notin K$ , and we conclude that  $[K(\alpha) : K] = 2$  and  $K(\alpha) = L$ .

(ii) The polynomial  $x^2 + \alpha^2 \in K[x]$ , where  $\alpha \in L \setminus K$ , admits  $\alpha$  as a double root, hence it is irreducible in  $K[x]$ . Now, as this is a unitary irreducible polynomial of degree 2 and as  $\alpha \notin K$ , it follows that  $m_{\alpha, K}(x) = x^2 + \alpha^2$  and so we conclude that  $\alpha \in L \setminus K$  is inseparable.

(b)(i) Let  $\alpha \in L \setminus K$  be such that  $\alpha^2 \notin K$ . First, we have that  $[K(\alpha) : K] \geq 2$  and, as  $K(\alpha) \subseteq L$ , it follows that  $[K(\alpha) : K] \leq [L : K] = 2$ , and so  $[K(\alpha) : K] = 2$ , hence  $K(\alpha) = L$ .

Secondly, as  $\alpha^2 \in K(\alpha)$  and  $\alpha^2 \notin K$ , there exist  $a, b \in K$ ,  $a \neq 0$ , such that  $\alpha^2 = a\alpha + b$ . Then:

$$\left(\frac{\alpha}{a}\right)^2 = \left(\frac{\alpha}{a}\right) + \frac{b}{a^2}.$$

Set  $\beta = \frac{\alpha}{a} \in K(\alpha)$  and  $c = \frac{b}{a^2} \in K$ . We have that  $K(\alpha) = K(\frac{\alpha}{a}) = K(\beta)$  and so  $L = K(\beta)$ . Moreover,  $\beta$  is a root of the unitary polynomial  $x^2 + x + c \in K[x]$  and, as  $[K(\beta) : K] = 2$ , we conclude that  $m_{\beta, K}(x) = x^2 + x + c$ .

(ii) Note that a polynomial of the form  $x^2 + x + c$  is always separable as the derivative is  $1 \neq 0$ . So,  $\beta$  is automatically separable. Now  $\beta + 1 \in K(\beta)$  is a root of  $m_{\beta, K}(x)$ , as  $(\beta + 1)^2 + (\beta + 1) + c = \beta^2 + \beta + c = 0$ , and we conclude that  $\tau : K(\beta) \rightarrow K(\beta)$  given by  $\tau(\beta) = \beta + 1$  is an automorphism of  $K(\beta)$ . Then, by Proposition 4.6.3.4 we have that  $|\text{Gal}(K(\beta)/K)| = 2$ .

(iii) Note that  $K(\beta)^{\langle \tau \rangle} = K$  by theorem 4.6.13. If  $\gamma \in L \setminus K$  then  $\tau(\gamma) \neq \gamma$  and by proposition 4.6.3.(3), we get that the minimal polynomial of  $\gamma$  is  $(t - \gamma)(t - \tau(\gamma))$ . Therefore  $K \subset L$  is separable.

### Exercise 3.

We use the same techniques as in Example 4.6.5, and denote  $G = \text{Gal}(K/\mathbb{Q}) = \text{Aut}_{\mathbb{Q}}(K)$ .

- Let  $K = \mathbb{Q}(i)$ . The irreducible polynomial  $x^2 + 1 \in \mathbb{Q}[x]$  has two distinct roots in  $\mathbb{Q}(i)$ , and they are  $i$  and  $-i$ . From Prop 4.6.3(1), it follows that every element in  $G$  sends  $i$  to  $i$  or to  $-i$ . By Prop 4.6.3(2), there is at most one element in  $G$  for each possibility. By Prop 4.6.3(4), it holds that  $|\text{Gal}(K/\mathbb{Q})| = [\mathbb{Q}(i) : \mathbb{Q}] = 2$ , hence  $\text{Gal}(K/\mathbb{Q}) = \{\text{id}_{\mathbb{Q}(i)}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ , where (the identity sends  $i$  to  $i$ , and)  $\sigma$  sends  $i$  to  $-i$ . As  $\sigma$  is  $\mathbb{Q}$ -linear, we have that  $\sigma(a + ib) = a - ib$ , the conjugation.
- Let  $K = \mathbb{Q}(\sqrt{7})$ . Using the same steps as above, considering the irreducible polynomial  $x^2 - 7 \in \mathbb{Q}[x]$ , we get that  $\text{Gal}(K/\mathbb{Q}) = \{\text{id}_{\mathbb{Q}(\sqrt{7})}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ , where (the identity sends  $\sqrt{7}$  to  $\sqrt{7}$ , and)  $\sigma$  sends  $\sqrt{7}$  to  $-\sqrt{7}$ . As  $\sigma$  is  $\mathbb{Q}$ -linear, we have that  $\sigma(a + \sqrt{7}b) = a - \sqrt{7}b$ .
- Let  $K = \mathbb{Q}(\sqrt[3]{2})$ . The irreducible polynomial  $x^3 - 2 \in \mathbb{Q}[x]$  has only one root in  $\mathbb{Q}(\sqrt[3]{2})$ . As by Prop 4.6.3(1), every root of this polynomial gets sent to a root of the same polynomial by an element in  $G$ , and for each such possibility there is at most one element in  $G$  by Prop 4.6.3(2), we conclude that  $G = \{\text{id}_{\mathbb{Q}(\sqrt[3]{2})}\}$  is trivial.
- Let  $K = \mathbb{Q}(\omega^2)$ , where  $\omega = e^{2i\pi/3}$ . The irreducible polynomial  $x^2 + x + 1 \in \mathbb{Q}[x]$  has two roots in  $\mathbb{Q}(\omega)$ , which are  $\omega$  and  $\omega^2$ . As for the first and second example, it follows that  $G$  is cyclic of order two, consisting of the identity and  $\sigma$ , which sends  $\omega$  to  $\omega^2$ . We have in fact  $K = \mathbb{Q}(i\sqrt{3})$ , and one could have argued as in the first two points.

### Exercise 4.

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 developing

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

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  $\pm\sqrt{1-\sqrt{2}} \notin \mathbb{Q}(\sqrt{1+\sqrt{2}})$ . Let  $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q})$ . Then  $\sigma(\sqrt{1+\sqrt{2}}) \in \mathbb{Q}(\sqrt{1+\sqrt{2}})$  is a root of  $m_{\sqrt{1+\sqrt{2}}, \mathbb{Q}}(x)$  and thus  $\sigma(\sqrt{1+\sqrt{2}}) = \pm\sqrt{1+\sqrt{2}}$ , see Proposition 4.6.3 (c). It follows that  $|\text{Gal}(\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q})| = 2$  and we conclude, using Corollary 4.6.13, that the extension  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$  is not Galois.

### Exercise 5.

In the following solutions, we use the same technique to find the minimal polynomials as in Example 4.6.11. With Proposition 4.6.10, 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  $z$ .

- As in Example 4.6.4 (3), we see that  $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . The elements in  $G$  are the identity,  $\sigma$ , with  $\sigma(\sqrt{3}) = \sqrt{3}$  and  $\sigma(\sqrt{7}) = -\sqrt{7}$ ,  $\tau$  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

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

- We note that since  $\beta = -1 \in \mathbb{Q}$ , it holds that  $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$ .  $\alpha$  is a root of the polynomial  $x^3 + 1$ . The other two roots are  $-1$ , and  $e^{-2i\pi/3} = \bar{\alpha}$ . Since one of the roots is contained in  $\mathbb{Q}$ , over which every element of the Galois group acts as the identity we get by Prop 4.6.3 (1) that every element of the Galois group  $G$  either sends  $\alpha$  to  $\alpha$ , or to  $\bar{\alpha}$ . By (b), there exists at most one element for each possibility. Hence  $|G| \leq 2$ . There are exactly two automorphisms, one being the identity, and the other acting on  $\alpha$  by sending  $\alpha$  to  $\bar{\alpha}$ . Therefore,  $G \cong \mathbb{Z}/2\mathbb{Z}$ .

Again, we calculate the minimal polynomial of an element  $z = (a + b\alpha) \in \mathbb{Q}(\alpha)$  as above. Its

minimal polynomial is  $m_{z,\mathbb{Q}} = (x - a - b\alpha)(x - a - b\bar{\alpha})$ , if the factors are different. We get

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

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 4.6.4 (c), we see that  $\text{Gal}(\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q})$  contains 4 elements, the identity,  $\sigma, \tau$  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  $\text{Gal}(\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . On the elements  $\alpha$  and  $\beta$ , 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

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

We note that the element  $\alpha$  is of the form  $\alpha = \frac{1}{2} + \frac{1}{2}(i\sqrt{3})$  in the basis  $\{1, i, \sqrt{3}, i\sqrt{3}\}$ . Then, the minimal polynomials are of the form

$$\begin{aligned} m_{\alpha,\mathbb{Q}} &= (x - (0.5 + 0.5i\sqrt{3}))(x - (0.5 - 0.5i\sqrt{3})) = (x - \alpha)(x - e^{-i\pi/3}) \\ m_{\alpha+\beta,\mathbb{Q}} &= (x - (0.5 + i + 0.5i\sqrt{3}))(x - (0.5 + i - 0.5\sqrt{3}i))(x - (0.5 - i - 0.5\sqrt{3}i))(x - (0.5 - i + 0.5\sqrt{3}i)) \\ m_{\alpha\beta,\mathbb{Q}} &= (x - (0.5i - 0.5\sqrt{3}))(x - (0.5i + 0.5\sqrt{3}))(x - (-0.5i - 0.5\sqrt{3}))(x - (-0.5i + 0.5\sqrt{3})) \\ m_{\alpha^{-1},\mathbb{Q}} &= m_{e^{-i\pi/3},\mathbb{Q}} = m_{0.5-0.5i\sqrt{3},\mathbb{Q}} = (x - (0.5 - 0.5i\sqrt{3}))(x - (0.5 + 0.5i\sqrt{3})) \end{aligned}$$

4. Let  $\alpha = e^{(i\pi/6)}$  and  $\beta = i$ . We first calculate  $G = \text{Gal}(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})$ . We remark that  $\beta = \alpha^3$ , and hence  $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$ . Furthermore,  $\alpha$  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  $\alpha$  is  $m_{\alpha,\mathbb{Q}} = x^4 - x^2 + 1$ . Since by adjoining  $\alpha$  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,  $\tau, \sigma, \eta$ , where the root  $\alpha$  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 ele-

ments  $id, \tau, \sigma, \eta$ . It follows that

$$\begin{aligned}
m_{\alpha, \mathbb{Q}} &= (x - \alpha)(x - \tau(\alpha))(x - \sigma(\alpha))(x - \eta(\alpha)) = (x - \alpha)(x - \alpha^5)(x - \alpha^7)(x - \alpha^{11}) = x^4 - x^2 + 1 \\
m_{\alpha+\beta, \mathbb{Q}} &= m_{\alpha+\alpha^3, \mathbb{Q}} = (x - (\alpha + \alpha^3))(x - \tau(\alpha + \alpha^3))(x - \sigma(\alpha + \alpha^3))(x - \eta(\alpha + \alpha^3)) \\
&= (x - (\alpha + \alpha^3))(x - (\alpha^5 + \alpha^3))(x - (\alpha^7 + \alpha^9))(x - (\alpha^{11} + \alpha^9)) = x^4 + 3x^2 + 9 \\
m_{\alpha\beta, \mathbb{Q}} &= m_{\alpha^4, \mathbb{Q}} = m_{-0.5+0.5i\sqrt{3}, \mathbb{Q}} = (x - \alpha^4)(x - \tau(\alpha^4))(x - \sigma(\alpha^4))(x - \eta(\alpha^4)) \\
&= (x - \alpha^4)(x - \alpha^8)(x - \alpha^4)(x - \alpha^8) = x^2 + x + 1 \\
m_{\alpha^{-1}, \mathbb{Q}} &= m_{\alpha^{11}, \mathbb{Q}} = (x - \alpha^{11})(x - \tau(\alpha^{11}))(x - \sigma(\alpha^{11}))(x - \eta(\alpha^{11})) \\
&= (x - \alpha^{11})(x - \alpha^7)(x - \alpha^7)(x - \alpha) = x^4 - x^2 + 1
\end{aligned}$$

**Exercise 6.** 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. Let  $\alpha, \beta$  and  $\gamma$  be the three roots of  $f$  in its splitting field. 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.

*One could also see that as the derivative of this polynomial has no real zeroes ( $a > 0$ ) and distinct zeroes would mean at least one zero for the derivative by Rolle so that the polynomial has at least one zero. But because it is a real polynomial of degree 3 it has one real zero by continuity because it tends to  $\pm\infty$  when the variable goes to  $\pm\infty$ .*

3. As  $\deg f = 3$ , and complex roots of a real polynomial come in complex conjugate pairs,  $f$  has to have a real root. Let this real root be  $\alpha$ . 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  $\beta$  and  $\gamma$ , cannot be contained in  $\mathbb{Q}(\alpha)$ . So, every element  $g \in \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$  can send  $\alpha$  only to  $\alpha$ . However, as  $\alpha$  generated  $\mathbb{Q}(\alpha)$  this means that  $g = \text{id}$ .

4. Let  $\alpha, \beta$  and  $\gamma$  be as in the previous point. Then both  $\beta$  and  $\gamma$  are roots of  $h = \frac{f}{x-\alpha} \in \mathbb{Q}(\alpha)[x]$ . As this polynomial has degree 2, and  $\beta$  and  $\gamma$  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  $\alpha, \beta$  and  $\gamma$ , which yields an embedding  $G \hookrightarrow S_3$ . As both have 6 elements, this is in fact an isomorphism.

**Exercise 7.** 1. Let  $\beta$  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  $\beta$  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  $\beta$  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  $\sigma_\gamma$ , 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  $\beta$  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  $f : u^p - u + t = 0 \Leftrightarrow u^p - u = -t$ , 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  $\mathbb{F}_p(u)$ .

**Exercise 8** (Galois correspondence). 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

4.6.3(d), it follows that  $|\text{Gal}(L/\mathbb{Q})| = 2$  and so  $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ . The only subgroups of  $\text{Gal}(L/\mathbb{Q})$  are  $\text{Gal}(L/\mathbb{Q})$  and  $\{\text{Id}_L\}$ , therefore the only sub-extensions of  $L$  are  $\mathbb{Q} = L^{\text{Gal}(L/\mathbb{Q})}$  and  $L = L^{\{\text{Id}_L\}}$ .

2. Let  $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . We have seen in Series 9, Exercise 5.2 that  $[L : \mathbb{Q}] = 4$ . Now,  $\mathbb{Q}$  is a perfect field and  $L$  is the decomposition field of  $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$  over  $\mathbb{Q}$ , hence the extension  $\mathbb{Q} \subseteq L$  is Galois. By Proposition 4.6.3(d), it follows that  $|\text{Gal}(L/\mathbb{Q})| = 4$ . Now, let  $\sigma, \tau \in \text{Gal}(L/\mathbb{Q})$  be such that  $\sigma(\sqrt{2}) = -\sqrt{2}$  and  $\sigma(\sqrt{3}) = \sqrt{3}$ , respectively  $\tau(\sqrt{2}) = \sqrt{2}$  and  $\tau(\sqrt{3}) = -\sqrt{3}$ . We see that  $\sigma^2 = \tau^2 = \text{Id}_L$  and that  $\sigma\tau = \tau\sigma$ . Therefore  $\text{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Now,  $\text{Gal}(L/\mathbb{Q})$  admits 3 non-trivial proper subgroups:  $\langle \sigma \rangle$ ,  $\langle \tau \rangle$  and  $\langle \sigma\tau \rangle$ , each isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ . Let  $H$  be one of these subgroups. By applying Theorem 4.6.18, we determine that  $L^H \subseteq L$  is Galois and  $[L : L^H] = |H| = 2$ . Therefore,  $[L^H : \mathbb{Q}] = 2$ . One checks that  $\mathbb{Q}(\sqrt{3}) \subseteq L^{\langle \sigma \rangle}$ , as  $\sigma(\sqrt{3}) = \sqrt{3}$ , and, similarly, that  $\mathbb{Q}(\sqrt{2}) \subseteq L^{\langle \tau \rangle}$  and  $\mathbb{Q}(\sqrt{6}) \subseteq L^{\langle \sigma\tau \rangle}$ , respectively. We conclude that

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

3. Let  $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  and consider the extension chain:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq L$$

We have that  $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 8$ , as  $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$  is a root of the polynomial  $x^2 - 5 \in \mathbb{Q}(\sqrt{2}, \sqrt{3})[x]$ . Now,  $\mathbb{Q}$  is a perfect field and  $L$  is the splitting field of  $(x^2 - 2)(x^2 - 3)(x^2 - 5) \in \mathbb{Q}[x]$  over  $\mathbb{Q}$ , hence the extension  $\mathbb{Q} \subseteq L$  is Galois. By Proposition 4.6.3(d), it follows that  $|\text{Gal}(L/\mathbb{Q})| = 8$ . Let  $\sigma_1, \sigma_2, \sigma_3 \in \text{Gal}(L/\mathbb{Q})$  be such that:

$$\begin{aligned} \sigma_1(\sqrt{2}) &= -\sqrt{2}, \quad \sigma_1(\sqrt{3}) = \sqrt{3} \quad \text{and} \quad \sigma_1(\sqrt{5}) = \sqrt{5} \\ \sigma_2(\sqrt{2}) &= \sqrt{2}, \quad \sigma_2(\sqrt{3}) = -\sqrt{3} \quad \text{and} \quad \sigma_2(\sqrt{5}) = \sqrt{5} \\ \sigma_3(\sqrt{2}) &= \sqrt{2}, \quad \sigma_3(\sqrt{3}) = \sqrt{3} \quad \text{and} \quad \sigma_3(\sqrt{5}) = -\sqrt{5} \end{aligned}$$

One shows that  $\sigma_i^2 = \text{Id}_L$  for all  $i = 1, 2, 3$  and that  $\sigma_i\sigma_j = \sigma_j\sigma_i$  for all  $i \neq j$ , therefore determining that  $\text{Gal}(L/\mathbb{Q}) = \langle \sigma_1, \sigma_2, \sigma_3 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . We first consider the subgroups of order 2 of  $\text{Gal}(L/\mathbb{Q})$ . There are 7 of them and each of these is cyclic and generated by an element of  $\text{Gal}(L/\mathbb{Q})$ . Let  $H$  be one of these subgroups. We apply Theorem 4.6.18 to determine that  $L^H \subseteq L$  is Galois with  $[L : L^H] = |H| = 2$ . Therefore we have  $[L^H : \mathbb{Q}] = 4$ .

Let  $H = \langle \sigma_1 \rangle$ . 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:

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

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

We now consider the subgroups of order 4 of  $\text{Gal}(L/\mathbb{Q})$ . Again, there are 7 of them and each of these is generated by two distinct elements of order 2 of  $\text{Gal}(L/\mathbb{Q})$  and is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Let  $H$  be one of these subgroups. We apply Theorem 4.6.18 to determine that  $L^H \subseteq L$  is Galois with  $[L : L^H] = |H| = 4$ . Therefore we have  $[L^H : \mathbb{Q}] = 2$ . One shows that:

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

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

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  $\mathbb{Q}$ . By Proposition 4.6.3(d), it follows that  $|\text{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$ . 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 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:

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

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

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

Let  $\sigma, \tau \in \text{Gal}(E/\mathbb{Q})$  be such that  $\sigma(\sqrt{1 + \sqrt{2}}) = \sqrt{1 - \sqrt{2}}$  and  $\sigma(i) = -i$ , respectively  $\tau(\sqrt{1 + \sqrt{2}}) = \sqrt{1 + \sqrt{2}}$  and  $\tau(i) = -i$ . One checks that:

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

$$\sigma^3(\sqrt{1 + \sqrt{2}}) = -\sqrt{1 - \sqrt{2}}, \quad \sigma^3(i) = -i$$

$$\sigma^4(\sqrt{1 + \sqrt{2}}) = \sqrt{1 + \sqrt{2}}, \quad \sigma^4(i) = i$$

and thus deduces that  $\sigma^4 = \tau^2 = \text{Id}_E$ . Now  $\langle \sigma \rangle$  is a subgroup of order 4 in  $\text{Gal}(E/\mathbb{Q})$  and  $\tau \notin \langle \sigma \rangle$ . We deduce that  $\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \tau \rangle$  and, moreover, as  $\sigma\tau \neq \tau\sigma$ ,  $\text{Gal}(E/\mathbb{Q})$  is non-commutative. Lastly,  $\text{Gal}(E/\mathbb{Q})$  admits two elements of order 2:  $\sigma^2$  and  $\tau$ , and we conclude that  $\text{Gal}(E/\mathbb{Q}) \cong D_8$ .

We now determine the subgroups of  $\text{Gal}(E/\mathbb{Q})$ . There are 5 elements of order 2 in  $\text{Gal}(E/\mathbb{Q})$ :  $\tau, \sigma^2, \tau\sigma^2, \tau\sigma$  and  $\sigma\tau$ , each generating a cyclic group of order 2. Let  $H$  be one of these subgroups. By applying Theorem 4.6.18, we determine that  $E^H \subseteq E$  is Galois and  $[E : E^H] = |H| = 2$ . Therefore,  $[E^H : \mathbb{Q}] = 4$ . One checks that:

$$\tau\sigma^2(\sqrt{1 + \sqrt{2}}) = \tau(-\sqrt{1 + \sqrt{2}}) = -\sqrt{1 + \sqrt{2}} \text{ and } \tau\sigma^2(i) = -i$$

$$\tau\sigma(\sqrt{1 + \sqrt{2}}) = \tau(\sqrt{1 - \sqrt{2}}) = \tau(i(\sqrt{1 + \sqrt{2}})^{-1}) = -\sqrt{1 - \sqrt{2}} \text{ and } \tau\sigma(i) = i$$



$$\sigma\tau(\sqrt{1+\sqrt{2}}) = \sigma(\sqrt{1+\sqrt{2}}) = \sqrt{1-\sqrt{2}} \text{ and } \sigma\tau(i) = i$$

and therefore

$$\tau\sigma^2(\sqrt{2}) = \tau\sigma^2((\sqrt{1+\sqrt{2}})^2 - 1) = (\tau\sigma^2((\sqrt{1+\sqrt{2}})^2) - 1) = (-\sqrt{1+\sqrt{2}})^2 - 1 = \sqrt{2}$$

$$\begin{aligned} \tau\sigma(\sqrt{1+\sqrt{2}} - \sqrt{1-\sqrt{2}}) &= \tau\sigma(\sqrt{1+\sqrt{2}}) - \tau\sigma(i(\sqrt{1+\sqrt{2}})^{-1}) = -\sqrt{1-\sqrt{2}} - \tau(-i(\sqrt{1-\sqrt{2}})^{-1}) \\ &= -\sqrt{1-\sqrt{2}} - \tau(-\sqrt{1+\sqrt{2}}) = \sqrt{1+\sqrt{2}} - \sqrt{1-\sqrt{2}} \end{aligned}$$

$$\begin{aligned} \sigma\tau(\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}}) &= \sqrt{1-\sqrt{2}} + \sigma\tau(i(\sqrt{1+\sqrt{2}})^{-1}) = \sqrt{1-\sqrt{2}} + \sigma(-i(\sqrt{1+\sqrt{2}})^{-1}) \\ &= \sqrt{1-\sqrt{2}} + i(\sqrt{1-\sqrt{2}})^{-1} = \sqrt{1-\sqrt{2}} + \sqrt{1+\sqrt{2}} \end{aligned}$$

The corresponding sub-extensions are

$$E^{\langle\tau\rangle} = \mathbb{Q}(\sqrt{1+\sqrt{2}}), \quad E^{\langle\sigma^2\rangle} = \mathbb{Q}(\sqrt{1-\sqrt{2}}), \quad E^{\langle\tau\sigma^2\rangle} = \mathbb{Q}(\sqrt{2}, i)$$

$$E^{\langle\tau\sigma\rangle} = \mathbb{Q}(\sqrt{1+\sqrt{2}} - \sqrt{1-\sqrt{2}}) \text{ and } E^{\langle\sigma\tau\rangle} = \mathbb{Q}(\sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}}).$$

Lastly,  $\text{Gal}(E/\mathbb{Q})$  admits 3 subgroups of order 4, one of which is cyclic,  $\langle\sigma\rangle$ , and the other two are isomorphic to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ,  $\langle\tau, \sigma^2\rangle$  and  $\langle\tau\sigma, \sigma^2\rangle$ . Let  $H$  be one of these subgroups. By applying Theorem 4.6.18, we determine that  $E^H \subseteq E$  is Galois and  $[E : E^H] = |H| = 4$ . Therefore,  $[E^H : \mathbb{Q}] = 2$ . One checks that:

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

$$\begin{cases} \tau(\sqrt{2}) = \tau(\sqrt{1+\sqrt{2}})^2 - 1 = (\sqrt{1+\sqrt{2}})^2 - 1 = \sqrt{2} \\ \sigma^2(\sqrt{2}) = \sigma^2((\sqrt{1+\sqrt{2}})^2 - 1) = (-\sqrt{1+\sqrt{2}})^2 - 1 = \sqrt{2} \end{cases}$$

$$\tau\sigma(i) = \tau(-i) = i \text{ and } \sigma^2(i) = i$$

The corresponding sub-extensions are:

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

### Exercise 9.

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  $F = \mathbb{Q}[x_1, \dots, x_n]$  and for each  $\sigma \in G$  define:

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

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

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

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

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

Let  $H = \{\phi_\sigma \mid \sigma \in G\}$  be a subset of  $\text{Aut}_{\mathbb{Q}}(E)$ . 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  $\text{Aut}_{\mathbb{Q}}(E)$ . 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  $[E : E^H] = |H| = |\text{Gal}(E/E^H)|$ , hence  $E^H \subseteq E$  is Galois, see Corollary 4.6.13. We conclude that  $\text{Gal}(E/E^H) = H \cong G$ .

**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  $X \rightarrow \mathbb{P}_{\mathbb{C}}^1$  tel que si on enlève un nombre fini de points à  $\mathbb{P}_{\mathbb{C}}^1$ , le morphisme devient un revêtement au sens topologique.
2.  $\mathbb{P}_{\mathbb{C}}^1$  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  $F_n \rightarrow G$  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  $X \rightarrow \mathbb{P}_{\mathbb{C}}^1$  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 10.

Remarquons que

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

Notons que  $\mathbb{C}(\sqrt{t}) \rightarrow \mathbb{C}(\sqrt{t})$  qui envoie  $\sqrt{t} \mapsto \frac{\sqrt{t+1}}{\sqrt{t-1}}$  et  $\sqrt{t} \mapsto \frac{\sqrt{t-1}}{\sqrt{t+1}}$  sont des automorphismes. Comme  $X^n - \sqrt{t}$  est irréductible par Eisenstein, il suit que les deux polynômes en facteur ci-dessus sont irréductibles. On voit alors que l'extension

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

est de degré  $2n$ . Notons  $x := \sqrt[n]{\frac{\sqrt{t+1}}{\sqrt{t-1}}}$ . Les racines de  $X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1$  sont

$$x, \xi_n x, \dots, \xi_n^{n-1} x, \frac{1}{x}, \xi_n \frac{1}{x}, \dots, \xi_n^{n-1} \frac{1}{x},$$

où  $\xi_n$  est une racine primitive  $n$ -ième de l'unité. Dès lors  $\mathbb{C}\left(\sqrt[n]{\frac{\sqrt{t+1}}{\sqrt{t-1}}}\right)$  est le corps de décomposition  $X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1$ .

Notons  $\sigma \in \text{Gal}(L_n/\mathbb{C}(t))$  l'automorphisme tel que  $\sigma(x) = \xi_n x$  pour  $\xi_n$ . Notons  $\tau$  pour l'automorphisme tel que  $\tau(x) = \frac{1}{x}$ . Comme les racines de  $X^{2n} - 2\left(\frac{t+1}{t-1}\right)X^n + 1$  sont de la forme  $x^\epsilon \xi_n^j$  pour  $\epsilon = 1, -1$  et  $j = 0, \dots, n-1$ , on voit que tout élément du groupe de Galois est de la forme  $\tau^\epsilon \sigma^j$ . Comme  $\sigma^n = \text{id}$ ,  $\tau^2 = \text{id}$  et  $\tau\sigma\tau\sigma = \text{id}$  on a dès lors un morphisme surjectif

$$D_{2n} \rightarrow \text{Gal}(L_n/\mathbb{C}(t))$$

qui est un isomorphisme par cardinalité.

**Exercice bonus.**

1. Soit  $K \subseteq L$  une extension finie de corps, et supposons que  $K$  est parfait alors que  $L$  ne l'est pas. Il existe alors un polynôme irréductible  $f(t) \in L[t]$  tel que  $f$  a des racines multiples dans son corps de décomposition  $E$ . Soit  $\alpha \in E$  une racine multiple de  $f(t)$ , et soit  $g(t)$  le polynôme minimal de  $\alpha$  dans  $K$ .

omme  $g(\alpha) = 0$ , on a par définition que  $f(t)$  divise  $g(t)$  dans  $L[t]$ . Ainsi,  $\alpha$  est une racine double de  $g(t)$ . Or, comme  $K$  est parfait,  $g$  n'a que des racines simples, ce qui donne donc une contradiction.

2. Notons  $K$  le corps de l'énoncé, et pour tout  $n > 0$ , soit

$$K_n := \mathbb{F}_p(t)[X_1, X_2, \dots, X_n]/(X_1^p - t, X_2^p - X_1, \dots, X_n^p - X_{n-1}).$$

Montrons tout d'abord que chaque  $K_n$  est un corps. Montrons tout d'abord que

$$\mathbb{F}_p(t)[X_1, X_2, \dots, X_n]/(X_1^p - t, X_2^p - X_1, \dots, X_n^p - X_{n-1}) \cong \mathbb{F}_p(t)[X_n]/(X_n^{p^n} - t).$$

On a un morphisme naturel

$$f: \mathbb{F}_p(t)[X_n] \rightarrow \mathbb{F}_p(t)[X_1, X_2, \dots, X_n]/(X_1^p - t, X_2^p - X_1, \dots, X_n^p - X_{n-1})$$

envoyant  $X_n$  sur  $X_n$ . Ce morphisme est surjective, vu que dans le quotient de droite, chaque  $X_i$  vaut une puissance de  $X_n$ . De plus, on vérifie que  $X_n^{p^n} - t \in \ker(f)$ , donc on obtient par passage un quotient un morphisme surjectif

$$\mathbb{F}_p(t)[X_n]/(X_n^{p^n} - t) \rightarrow \mathbb{F}_p(t)[X_1, X_2, \dots, X_n]/(X_1^p - t, X_2^p - X_1, \dots, X_n^p - X_{n-1}).$$

De plus, le polynôme  $X_n^{p^n} - t \in \mathbb{F}_p(t)[X_n]$  est irréductible. EN effet, par le lemme de Gauss, il suffit montrer que  $X_n^{p^n} - t \in \mathbb{F}_p[t, X_n]$  est irréductible. C'est bien le cas, par exemple par le critère d'Eisenstein appliqué a  $t \in \mathbb{F}_p[t, X_n]$ .

Comme  $\mathbb{F}_p(t)[X_n]$  est principal, l'idéal  $(X_n^{p^n} - t)$  est alors automatiquement maximal, et donc le quotient  $\mathbb{F}_p(t)[X_n]/(X_n^{p^n} - t)$  est un corps. Le morphisme  $f$  est alors automatiquement injectif, car un corps n'a pas d'idéal non-trivial.

Ainsi, la preuve ci-dessus montre que  $K_n$  est un corps. Notez que l'on a un morphisme

$$\mathbb{F}_p(t)[X_1, \dots, X_n] \rightarrow \mathbb{F}_p(t)[X_j]_{j \geq 1} \rightarrow K,$$

qui en passant au quotient donne un morphisme  $\phi_n: K_n \rightarrow K$ . Par le même argument que ci-dessus,  $\phi_n$  est injectif, et donc  $\phi_n(K_n)$  est un sous-corps de  $K$ .

Finalement, comme seulement un nombre fini de variable n'apparaît dans un élément de  $\mathbb{F}_p(t)[X_n]_{n \geq 1}$ , on en déduit automatiquement de

$$K = \bigcup_{n \geq 1} \phi_n(K_n).$$

On peut maintenant déduire que  $K$  est un corps. Soit  $0 \neq \alpha \in K$ . Alors  $\alpha \in \phi_n(K_n)$  pour un certain  $n$ , et donc vu que  $\phi_n(K_n)$  est un corps,  $\alpha$  admet bel et bien un inverse.

Montrons finalement que  $K$  est parfait, en montrant que  $K^p = K$ . Pour chaque  $n$ , notons par  $t^{1/p^n}$  l'image de  $X_n$  dans  $K$  (cette notation a du sens, car  $(t^{1/p^n})^{p^n} = t$ ). Alors un élément  $f \in K$  s'écrit

$$\sum_{i=1}^n a_i t^{1/p^i}$$

avec  $a_i \in \mathbb{F}_p$ . Alors

$$\left( \sum_{i=2}^{n+1} a_{i-1} t^{1/p^i} \right)^p = \sum_{i=2}^{n+1} a_{i-1}^p \left( t^{1/p^i} \right)^p = \sum_{i=2}^{n+1} a_{i-1} t^{1/p^{i-1}} = f,$$

et donc  $f \in K^p$ . Ainsi, on a montré que  $K$  était parfait.

3. Comme  $K^p = K$ , le morphisme de Frobenius  $(\cdot)^p: K \rightarrow K$  est surjectif. Il est aussi injectif car  $K$  est un corps, et donc c'est un isomorphisme. Soit alors  $\phi'$  le morphisme  $K[X] \rightarrow K[X]$  fixant  $X$  et valant l'inverse du Frobenius sur  $K$ . Par construction,  $\phi' = \phi^{-1}$  et donc  $\phi$  est un isomorphisme.
4. Fixons  $i \in \mathbb{Z}$ . Soient  $\alpha_j$  les racines de  $f$  dans  $L$  ( $L$  est alors généré par les  $\alpha_j$  par définition). Soit aussi  $L_i$  le corps de décomposition de  $\phi_i(f)$  sur  $L$ .

Montrons que les racines de  $\phi_i(f)$  sont les  $\alpha_j^{p^i}$ . Ecrivons  $f = \sum_s a_s X^s$ , et  $\beta \in L_i$ . Alors

$$\phi_i(f)(\beta) = \sum_s a_s^{p^i} \beta = \sum_s a_s^{p^i} (\beta^{p^{-i}})^{p^i} = \left( \sum_s a_s \beta \right)^{p^i},$$

et donc

$$\phi_i(f)(\beta) = 0 \iff \beta = \alpha_j^{p^i}$$

pour un certain  $i$ . Cela montre que  $L$  contient toutes les racines de  $\phi_i(f)$ , et donc que  $L = L_i$ . De plus,  $L$  est bien généré par les éléments  $\alpha_j^{p^i}$ . En effet, soit  $M_i$  le sous-corps de  $L$  généré par ces éléments. Vu que  $M_i$  est parfait par le point (1), on a alors que pour tout  $j$ ,

$$\alpha_j = (\alpha_j^{p^i})^{p^{-i}} \in M_i,$$

et donc on a bien et bien  $M_i = L$ . On a donc montré que  $L$  était le corps de décomposition de  $\phi_i(f)$ .