EPFL - Printemps 2022	Prof. Z. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 12	

Exercice 1(a)(i) Let $\alpha \in L\backslash K$. As $\alpha^2 \in K$, it follows that α 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 $\alpha \in L\backslash K$, admits α 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 $\alpha \in L\backslash K$ is inseparable.

(b)(i) Let $\alpha \in L\backslash K$ 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, β 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, β is automatically separable. Then, by Proposition 4.6.3 (d) we have that $|\operatorname{Gal}(K(\beta)/K)| \geq 2$. Let $\tau \in \operatorname{Gal}(K(\beta)/K)$, $\tau \neq \operatorname{Id}_{K(\beta)}$. Then $\tau(\beta)$ is a root of $m_{\beta,K}(x)$, see Proposition 4.6.3 (a), and $\tau(\beta) \neq \beta$, as $\tau \neq \operatorname{Id}_{K(\beta)}$. 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 $\tau : K(\beta) \to K(\beta)$ given by $\tau(\beta) = \beta+1$ is an automorphism of $K(\beta)$.

(iii) Assume there exists $\gamma \in L\backslash K$ such that $\gamma^2 \in K$. Now, as $L = K(\beta)$, we have that there exist $a, b \in K$ such that $\gamma = a\beta + b$. Keeping in mind that $\beta^2 = \beta + c$, it follows that:

$$\gamma^2 = a^2\beta + a^2c + b^2 \in K.$$

It follows that $a = 0$ and $\gamma = b \in K$, a contradiction. Thus, for all $\gamma \in L\backslash K$ we have that $\gamma^2 \notin K$ and we argue as in item (b)(i) to show that $m_{\gamma,K}(x) = x^2+x+c_\gamma$, where $c_\gamma \in K$.

Exercice 2. (a) Let $\alpha \in K^p$ and assume that there exist $\beta, \gamma \in K$, such that $\alpha = \beta^p$ and $\alpha = \gamma^p$. Let $x^p - \alpha \in K^p[x]$. We have that $x^p - \alpha = x^p - \beta^p = (x-\beta)^p$ and thus β is a root of $x^p - \alpha$ with multiplicity p. As $\deg(x^p-\alpha) = p$, it follows that β is the unique distinct root of $x^p - \alpha$. On the other hand, γ is a also a root of $x^p - \alpha$ and thus $\gamma = \beta$.

(b) As $\phi \in \operatorname{Aut}(K^p)$, for all $\alpha \in K$ there exists a unique $\beta_\alpha \in K$ such that $\phi(\alpha^p) = \beta_\alpha^p$. Let $\psi : K \to K$ be given by $\psi(\alpha) = \beta_\alpha$ for all $\alpha \in K$. We will show that $\psi \in \operatorname{Aut}(K)$ and that ψ is an extension of ϕ, i.e. $\psi(\alpha^p) = \phi(\alpha^p)$ for all $\alpha \in K$.

First, let $\alpha, \gamma \in K$. We know that there exist unique $\beta_\alpha \in K$, respectively $\beta_\gamma \in K$, such that $\phi(\alpha^p) = \beta_\alpha^p$, respectively $\phi(\gamma^p) = \beta_\gamma^p$. Then:

$$\phi((\alpha+\gamma)^p) = \phi(\alpha^p+\gamma^p) = \phi(\alpha^p)+\phi(\gamma^p) = \beta_\alpha^p + \beta_\gamma^p = (\beta_\alpha+\beta_\gamma)^p$$

and thus $\psi(\alpha+\gamma) = \beta_\alpha + \beta_\gamma = \psi(\alpha)+\psi(\gamma)$ for all α , $\gamma \in K$. Similarly,

$$\phi((\alpha\cdot\gamma)^p) = \phi(\alpha^p\cdot\gamma^p) = \phi(\alpha^p)\cdot\phi(\gamma^p) = \beta_\alpha^p\cdot\beta_\gamma^p = (\beta_\alpha\cdot\beta_\gamma)^p$$

and thus $\psi(\alpha \cdot \gamma) = \beta_\alpha \cdot \beta_\gamma = \psi(\alpha) \cdot \psi(\gamma)$ for all α , $\gamma \in K$. Lastly, we have that $\phi(1) = 1$ and so $\psi(1) = 1$.

We have shown that ψ is a homomorphism of fields and, being a homomorphism of fields, we have that ψ is injective. To show surjectivity, let $\beta \in K$. Then $\beta^p \in K^p$ and, as $\phi \in \mathrm{Aut}(K^p)$, there exists $\alpha \in K^p$ such that $\phi(\alpha) = \beta^p$. Now, by point (a), we have that there exists a unique $\gamma \in K$ such that $\gamma^p = \alpha$ and therefore $\phi(\gamma^p) = \beta^p$. Hence, we have that $\psi(\gamma) = \beta$ and thus ψ is surjective.

We now show that ψ extends ϕ. For this let $\alpha \in K$ and let β_α be the unique element of K such that $\phi(\alpha^p) = \beta_\alpha^p$. Then $\psi(\alpha) = \beta_\alpha$ and we have:

$$\phi(\alpha^p) = \beta_\alpha^p = \psi(\alpha)^p = \psi(\alpha^p).$$

Lastly, we show the unicity of ψ. For this let $\psi^{'} \in \mathrm{Aut}(K)$ be an extension of ϕ. Note that as both ψ and $\psi^{'}$ are extensions of ϕ, we have:

$$\psi^{'}(\alpha^p) = \psi(\alpha^p) \; (= \phi(\alpha^p))$$

for all $\alpha \in K$. Therefore $\psi^{'}(\alpha)^p = \psi(\alpha)^p$, giving $(\psi^{'}(\alpha) - \psi(\alpha))^p = 0$ and thus $\psi^{'}(\alpha) = \psi(\alpha)$ for all $\alpha \in K$.

Exercice 3. (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 β over K. As β 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:

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

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 $p = x$ 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 $\mathrm{char}(L) = p$, 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^{th} power, see Exercice 3, 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 $\mathrm{char}(L) = 2$, it follows that L is perfect if and only if $L^2 = L$, see Proposition 4.5.7. But

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

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

Exercice 4. 1. Let $\mathbb{Q} \subseteq K$. Let $\varphi \in \mathrm{Aut}(K)$ an automorphism $\varphi : K \to K$. As automorphisms of fields are in particular homomorphisms of rings, we use that $\varphi(1) = 1$, and get that $\forall n \in \mathbb{Z}$,

$$\varphi(n) = \varphi(n \cdot 1) = n \cdot \varphi(1) = n.$$

If we let $m, n \in \mathbb{Z}$, then

$$m = \varphi(m) = \varphi\left(\frac{m}{n} \cdot n\right) = \varphi\left(\frac{m}{n}\right) \cdot \varphi(n) = \varphi\left(\frac{m}{n}\right) \cdot n,$$

from which it follows that $\varphi\left(\frac{m}{n}\right) = \frac{m}{n}$. This proves that φ acts as the identity on $\mathbb{Q}$.

2. We use the same techniques as in Example 4.6.4, and denote $G = \mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(K)$.

- 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 $|\ \mathrm{Gal}(K/\mathbb{Q})\ | = [\mathbb{Q}(i) : \mathbb{Q}] = 2$, hence $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(i)}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$, where (the identity sends i to i, and) σ sends i to $-i$. As σ 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 $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\sqrt{7})}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$, where (the identity sends $\sqrt{7}$ to $\sqrt{7}$, and) σ sends $\sqrt{7}$ to $-\sqrt{7}$. As σ 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 $G = \{\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}\}$ 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 ω and ω^2. As for the first and second example, it follows that G is cyclic of order two, consisting of the identity and σ, which sends ω to ω^2.

Exercice 5. 1. The Frobenius morphism acts on the basis $\{1, \alpha\}$ as follows:

$$F(1) = 1, \quad F(\alpha) = \alpha^2 = 1 + \alpha,$$

and hence, the matrix in the base $\{1, \alpha\}$ is

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

We obtain the eigenvalues by finding the roots of the characteristic polynomial, $p(\lambda)$

$$p(\lambda) = \det(M - \lambda I) = \det \begin{pmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{pmatrix} = (1-\lambda)^2 = (1+\lambda)^2,$$

since we are working in characteristic 2. Its root is 1, with multiplicity 2. The eigenspace for this eigenvalue is $E := \{v \in \mathbb{F}_2^2 \mid (M+I)v = 0\}$, and consists of and all scalar multiples of the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. As its dimension is $1 < 2$, this matrix is not diagonalizable over $\mathbb{F}_2$.

2. The Frobenius morphism acts on the basis $\{1, \beta, \beta^2\}$ as follows:

$$F(1) = 1, \quad F(\beta) = \beta^2, \quad F(\beta^2) = \beta^4 = \beta\beta^3 = \beta(\beta+1) = \beta^2 + \beta$$

and hence, the matrix in the base $\{1, \beta, \beta^2\}$ is

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

We obtain the eigenvalues by finding the roots of the characteristic polynomial, $p(\lambda)$

$$p(\lambda) = \det(M - \lambda I) = \det \begin{pmatrix} 1-\lambda & 0 & 0 \\ 0 & -\lambda & 1 \\ 0 & 1 & 1-\lambda \end{pmatrix} = (1-\lambda)(\lambda^2-\lambda-1) = (1+\lambda)(\lambda^2+\lambda+1),$$

since we are working over characteristic 2. The roots of this polynomials are $1, \alpha$, and α^2, with α from the first part of the exercise. The only root contained in $\mathbb{F}_2$ is 1. Its eigenspace is $E_1 = \{v \in \mathbb{F}_2^3 \mid (M+I)v = 0\}$, which consists of all scalar multiples of the vector $(1,0,0)$. Since the dimension of this eigenspace is $1 < 3$, the matrix is not diagonalizable over $\mathbb{F}_2$. All roots are contained in $\mathbb{F}_2(\alpha) = \mathbb{F}_4$. The eigenspace of α is $E_\alpha = \{v \in \mathbb{F}_2^3 \mid (M+\alpha I)v = 0\}$, and consists of scalar multiples of the vector $(0,1,\alpha)$. The eigenspace of α^2 is $E_{\alpha^2} = \{v \in \mathbb{F}_2^3 \mid (M+\alpha^2 I)v = 0\}$, and consists of scalar multiples of the vector $(0,1,\alpha^2)$. As there are three distinct eigenvalues in $\mathbb{F}_4$, the matrix is diagonalizable over $\mathbb{F}_4$.

Exercice 6.

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.

1. 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, 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

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

2. We note that since $\beta = -1 \in \mathbb{Q}$, it holds that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$. α is a root of the polynomial $x^3 + 1$. The other two roots are -1, and $e^{-2i\pi/3} = \overline{\alpha}$. 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 α to α, or to $\overline{\alpha}$. 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 α by sending α to $\overline{\alpha}$. 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 $m_{z,\mathbb{Q}} = (x - a - b\alpha)(x - a - b\overline{\alpha})$, if the factors are different. 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 4.6.4 (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

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

   We note that the element α 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

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

4. Let $\alpha = e^{(i\pi/6)}$ and $\beta = i$. We first calculate $G = \mathrm{Gal}(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})$. 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

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

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

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

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