Exercice 1. (a) Let $\gamma = \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$. We have that $\gamma-\sqrt{2} = \sqrt{3}$ and so $(\gamma-\sqrt{2})^2 = 3$. This gives $\gamma^2 - 1 = 2\gamma\sqrt{2}$, therefore $(\gamma^2-1)^2 = 8\gamma^2$ and so $\gamma^4 - 10\gamma^2 + 1 = 0$. It follows that the polynomial $t^4 - 10t^2 + 1 \in \mathbb{Q}[t]$ admits γ as a root. We will now show that this polynomial is irreducible.

Assume that $\frac{p}{r} \in \mathbb{Q}$, where $p, r \in \mathbb{Z}$, $\gcd(p,r) = 1$ and $r \neq 0$, is a root of $t^4 - 10t^2 + 1$. Then $p \mid 1$, $r \mid 1$ and so $\frac{p}{r} = \pm 1$. One checks that neither 1 nor -1 is a root of $t^4 - 10t^2 + 1$. We now assume that there exist $a, b, c, d \in \mathbb{Q}$ such that

$$t^4 - 10t^2 + 1 = (t^2 + at + b)(t^2 + ct + d).$$

Then $\begin{cases} a+c=0 \\ b+ac+d=-10 \\ ad+bc=0 \\ bd=1 \end{cases}$ and we deduce that $c(b-d) = 0$.

(a) If $c = 0$, then $\begin{cases} b+d=-10 \\ bd=1 \end{cases}$ which gives $b^2 + 10b + 1 = 0$. This implies that $b \in \mathbb{Q}$ is a root of the polynomial $t^2 + 10t + 1 \in \mathbb{Q}[t]$. If we write $b = \frac{p}{r}$, where $p, r \in \mathbb{Z}$ with $\gcd(p,r) = 1$ and $r \neq 0$, then $p \mid 1$, $r \mid 1$ and so $b = \pm 1$. But neither 1 nor -1 is a root of $t^2 + 10t + 1$.

(b) If $b = d$, then $b^2 = 1$ and so $b = \pm 1$. Moreover, as $b + ac + d = -10$ we also get that $c^2 = 10 + 2b$ and so $c^2 \in \{8, 12\}$, contradicting the fact that $c \in \mathbb{Q}$.

We conclude that $t^4 - 10t^2 + 1 \in \mathbb{Q}[t]$ is irreducible and therefore, as it admits $\sqrt{2}+\sqrt{3}$ as a root, we have that $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}}(t) = t^4 - 10t^2 + 1$ and $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. Lastly, as $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$, see Exercise 5.2 of Series 9, we conclude that $\sqrt{2}+\sqrt{3}$ is a primitive element of $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

(b) As $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$, it follows that $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2},\sqrt{3})) = 4$ and so, to show that the set $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$, it suffices to show that it is linearly independent. For this, let $a, b, c, d \in \mathbb{Q}$ be such that

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0.$$

Then $a + d\sqrt{6} = -(b\sqrt{2} + c\sqrt{3})$ and so $(a + d\sqrt{6})^2 = (b\sqrt{2} + c\sqrt{3})^2$ which gives

$$a^2 + 6d^2 - 2b^2 - 3c^2 + 2(ad - bc)\sqrt{6} = 0.$$

As $\sqrt{6} \notin \mathbb{Q}$ it follows that $\begin{cases} a^2 + 6d^2 - 2b^2 - 3c^2 = 0 \\ ad = bc \end{cases}$.

Analogously, since $a + b\sqrt{2} = -(c\sqrt{3} + d\sqrt{6})$ and $a + c\sqrt{3} = -(b\sqrt{2} + d\sqrt{6})$, respectively, one shows that $\begin{cases} a^2 + 2b^2 - 3c^2 - 6d^2 = 0 \\ ab = 3cd \end{cases}$ and $\begin{cases} a^2 + 3c^2 - 2b^2 - 6d^2 = 0 \\ ac = 2bd \end{cases}$, respectively.

Now:

$$\begin{cases} a^2 + 6d^2 - 2b^2 - 3c^2 = 0 \\ a^2 + 2b^2 - 3c^2 - 6d^2 = 0 \\ a^2 + 3c^2 - 2b^2 - 6d^2 = 0 \end{cases} \implies a^2 = \frac{1}{3}(2b^2 + 3c^2 + 6d^2)$$

which gives

$$\begin{cases} a^2 = \frac{1}{3}(2b^2+3c^2+6d^2) \\ a^2+2b^2-3c^2-6d^2=0 \end{cases} \implies b^2 = \frac{1}{4}(3c^2+6d^2) \text{ and so } a^2 = \frac{1}{2}(3c^2+6d^2).$$

Then

$$\begin{cases} a^2 = \frac{1}{2}(3c^2+6d^2) \\ b^2 = \frac{1}{4}(3c^2+6d^2) \\ a^2+3c^2-2b^2-6d^2=0 \end{cases} \implies c^2 = 2d^2.$$

If $d \neq 0$, then $\sqrt{2} = \frac{c}{d} \in \mathbb{Q}$, which is a contradiction. It follows that $d = 0$ and, consequently, $c = b = a = 0$. We conclude that $a = b = c = d = 0$ and therefore $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is linearly independent.

(c) Assume that $\gamma = a\sqrt{3} + b\sqrt{6}$ is primitive in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. If $a = 0$ or $b = 0$, then $\gamma = b\sqrt{6}$, respectively $\gamma = a\sqrt{3}$, and, since $\mathbb{Q}(\sqrt{6}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$,respectively, it follows that γ is not primitive in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, a contradiction.

Assume that $a,\ b \neq 0$. Now, $a\sqrt{3} + b\sqrt{6}$ is primitive in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ if and only if $\sqrt{3} + c\sqrt{6}$, where $c = \frac{b}{a} \neq 0$, is primitive in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. As $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}+c\sqrt{6}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ we have $[\mathbb{Q}(\sqrt{3}+c\sqrt{6}) : \mathbb{Q}] \mid 4$ and so $[\mathbb{Q}(\sqrt{3}+c\sqrt{6}) : \mathbb{Q}] \in \{1, 2, 4\}$. Clearly, $[\mathbb{Q}(\sqrt{3}+c\sqrt{6}) : \mathbb{Q}] \neq 1$ as $\sqrt{3}+c\sqrt{6} \notin \mathbb{Q}$. Assume that $[\mathbb{Q}(\sqrt{3}+c\sqrt{6}) : \mathbb{Q}] = 2$. Then, there exists a polynomial $t^2 + \alpha t + \beta \in \mathbb{Q}[t]$ which admits $\sqrt{3}+c\sqrt{6}$ as a root. Thus:

$$(\sqrt{3}+c\sqrt{6})^2 + \alpha(\sqrt{3}+c\sqrt{6}) + \beta = 0$$

and so:

$$6c\sqrt{2} + \alpha\sqrt{3} + c\alpha\sqrt{6} + 3 + 6c^2 + \beta = 0.$$

By item (b), it follows that $c = 0$, contradicting the fact that $b \neq 0$. We conclude that $[\mathbb{Q}(\sqrt{3}+c\sqrt{6}) : \mathbb{Q}] = 4$ and therefore $\mathbb{Q}(\sqrt{3}+c\sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(d) Now, $a\sqrt{2} + b\sqrt{3} + c\sqrt{6}$, where $a, b, c \in \mathbb{Q}^*$, is primitive in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ if and only if $\sqrt{2} + d\sqrt{3} + e\sqrt{6}$, where $d = \frac{b}{a} \neq 0$ and $e = \frac{c}{a} \neq 0$, is primitive in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We argue as in item (c) to show that $[\mathbb{Q}(\sqrt{2}+d\sqrt{3}+e\sqrt{6}) : \mathbb{Q}] \in \{1, 2, 4\}$ and that $[\mathbb{Q}(\sqrt{2}+d\sqrt{3}+e\sqrt{6}) : \mathbb{Q}] \neq 1$. Assume $[\mathbb{Q}(\sqrt{2}+d\sqrt{3}+e\sqrt{6}) : \mathbb{Q}] = 2$. Then there exists a polynomial $t^2 + \alpha t + \beta \in \mathbb{Q}[t]$ that admits $\sqrt{2}+d\sqrt{3}+e\sqrt{6}$ as a root. We have that:

$$(\sqrt{2}+d\sqrt{3}+e\sqrt{6})^2 + \alpha(\sqrt{2}+d\sqrt{3}+e\sqrt{6}) + \beta = 0$$

and so $\begin{cases} 4e + \alpha d = 0 \\ 6de + \alpha = 0 \end{cases}$. Then $\alpha = -6de$ and we have $4e - 6d^2e = e(4 - 6d^2) = 0$. As $e \neq 0$ it follows that $6 = (\frac{2}{d})^2$ and so $\sqrt{6} \in \mathbb{Q}$, a contradiction.

We conclude that $[\mathbb{Q}(\sqrt{2}+d\sqrt{3}+e\sqrt{6}) : \mathbb{Q}] = 4$ and therefore $\mathbb{Q}(\sqrt{2}+d\sqrt{3}+e\sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Exercice 2. 1. Let β be a root of f. It holds that $\beta^p - \beta + \alpha = 0$. Let $\gamma \in \mathbb{F}_p \subseteq K$. Then, using Fermat's little theorem, which states that $\gamma^p = \gamma$ modulo p, it holds that over a field of characteristic p, we have

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

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

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

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

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

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

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

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

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

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

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

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

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

Exercice 3. 1. First we note that we may apply the third Gauss lemma, from which it follows that f is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$. We then argue as in Example 3.9.4 (b) that showing irreducibility of f in $\mathbb{Z}[x]$ can be done by showing irreducibility of $ev_{y+1}(f)$ in $\mathbb{Z}[y]$ since the evaluation $ev_{y+1} : \mathbb{Z}[x] \to \mathbb{Z}[y]$ is an isomorphism. But

$$ev_{y+1}(f) = (y+1)^6 + (y+1)^3 + 1 = y^6 + 6y^5 + 15y^4 + 21y^3 + 18y^2 + 9y + 3,$$

which is irreducible in $\mathbb{Z}[y]$ by applying Eisensteins criterion with $p = 3$.

2. Let α be a root of f. Then, with $\alpha^6 + \alpha^3 + 1 = 0$ it follows that $\alpha^6 = -\alpha^3 - 1$, and hence $\alpha^9 = \alpha^3 \cdot \alpha^6 = \alpha^3(-\alpha^3 - 1) = -\alpha^6 - \alpha^3 = -(-\alpha^3 - 1) - \alpha^3 = \alpha^3 + 1 - \alpha^3 = 1$, and so α is a root of $x^9 - 1$ as well.

It holds that

$$x^9 - 1 = (x^6 + x^3 + 1)(x^3 - 1).$$

Using Prop. 4.4.10 (c), it follows from $\gcd(x^9 - 1, \frac{\partial}{\partial x}(x^9 - 1)) = \gcd(x^9 - 1, 9x^8) = 1$ that the polynomial $x^9 - 1$ does not have any double roots. Its 9 roots are the 9-th roots of unity. Hence α is a 9-th root of unity as well. The 9-th roots of unity that are not primitive are those roots that are simultaneously 3-rd roots of unity as well. But α can not be one of those roots, since if α was a root simultaneously of f and of x^3-1, then α would be a double root of $f\cdot(x^3-1)=x^9-1$, which is not possible. We conclude that α is a primitive 9-th root of unity.

3. Let α be as above a root of f. Then, $\alpha \in \{e^{2\pi ik/9} \mid k=1,2,4,5,7,8\}$, and we may assume without loss of generality that $\alpha = e^{2\pi i/9}$. Then, the other roots of f are $\alpha^2,\alpha^4,\alpha^5,\alpha^7,\alpha^8$. By adjoining α to $\mathbb{Q}$, we therefore adjoin all roots of f, from which it follows that $L=\mathbb{Q}(\alpha)$.

   Now by Prop 4.6.3 (a), every element in $\mathrm{Gal}(L/\mathbb{Q})$ acts on the roots of f in L. These 6 roots are described above. By (b), as $L=\mathbb{Q}(\alpha)$, there is at most one element in the Galois group which sends α to one of other primitive roots α^k, where $k=1,2,4,5,7,8$. Hence there are at most 6 elements in the Galois group. But, using irreducibility of f, and part (c), there are exactly 6, with the automorphisms defined by $\sigma_k(\alpha)=\alpha^k$. The identification with $(\mathbb{Z}/9\mathbb{Z})^\times$ is the obvious one, identifying $\sigma_k \in \mathrm{Gal}(L/\mathbb{Q})$ with $k\in(\mathbb{Z}/9\mathbb{Z})^\times$. Lastly, this extension is Galois by Thm. 4.6.15, using $\mathbb{Q}$ is perfect, and hence the extension is separable.

4. We have the following fields extensions, $\mathbb{Q}\subseteq\mathbb{Q}(\alpha+\overline{\alpha})\subseteq\mathbb{Q}(\alpha)$, where $\overline{\alpha}$ denotes the complex conjugate of α. We remark that $\overline{\alpha}=\alpha^8\in\mathbb{Q}(\alpha)$.

   Since the extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is Galois, we have that $[\mathbb{Q}(\alpha):\mathbb{Q}]=|\,\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})|=6$. We note that the polynomial $g(x)=x^3-3x+1\in\mathbb{Q}[x]$ vanishes at $\alpha+\overline{\alpha}$. The other roots of this polynomial are $\alpha^2+\alpha^7$, and $\alpha^4+\alpha^5$. Since no root is contained in the field $\mathbb{Q}$, the polynomial g is irreducible over $\mathbb{Q}$, and it is the minimal polynomial of $\alpha+\overline{\alpha}$ over $\mathbb{Q}$. Therefore, $[\mathbb{Q}(\alpha+\overline{\alpha}):\mathbb{Q}]=3$, and furthermore, the field $\mathbb{Q}(\alpha+\overline{\alpha})$ is the splitting field of the polynomial g over $\mathbb{Q}$. (Since the other two roots can be expressed in terms of $\alpha+\overline{\alpha}$, and hence adjoining the roots $\alpha+\overline{\alpha}$ ensures that all roots are contained in the field extension.) Again using Thm 4.6.15, and using that $\mathbb{Q}$ is perfect, and hence the extension is separable, we conclude that the extension $\mathbb{Q}(\alpha+\overline{\alpha})$ over $\mathbb{Q}$ is Galois of degree 3.

Exercice 4 (Automorphism of $\mathbb{C}(x)$). 1. We note that all $\mathbb{C}$ - automorphisms of $\mathbb{C}(x)$ are determined by the image of x. We have that:

$$F^2(x)=i\frac{x+1}{x-1} \text{ and } F^3(x)=x,$$

therefore $F^3=\mathrm{Id}_{\mathbb{C}(x)}$. Similarly, we have:

$$G^2(x)=\frac{x(-i-1)+1-i}{x(i+1)+1-i} \text{ and } G^3(x)=x$$

therefore $G^3=\mathrm{Id}_{\mathbb{C}(x)}$. Lastly, as

$$FG(x)=-\frac{1}{x} \text{ and } GF(x)=-x,$$

it follows that $(FG)^2=(GF)^2=\mathrm{Id}_{\mathbb{C}(x)}$.

2. By item 1. we have $[(FG)\circ(GF)](x)=[(GF)\circ(FG)](x)=\frac{1}{x}$ and we see that FG and GF are commuting elements of order 2. It follows that the subgroup generated by them, $<FG,GF>$, is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and, moreover, it is normal in $\mathcal{A}$, since

$$F(FG)F^{-1}=FFGF^2=F(FGFG)G^2F=F(\mathrm{Id}_{\mathbb{C}(x)})G^2F=(FG)(GF)$$

and

$$G(FG)G^{-1}=GF$$

3. First, by items 1. and 2., we have that $3 \mid |\mathcal{A}|$ and $4 \mid |\mathcal{A}|$, therefore $|\mathcal{A}| \geq 12$. Since $FGFG = GFGF = \mathrm{Id}_{\mathbb{C}(x)}$, it follows that

$$FGF = G^2 \text{ and } GFG = F^2$$

and, keeping in mind the other relations established in items 1. and 2., one shows that $\mathrm{Id}_{\mathbb{C}(x)}$, F, F^2, G, G^2, FG, GF, F^2G, FG^2, G^2F, GF^2, FG^2F are distinct elements of $\mathcal{A}$.

Secondly, as $\mathcal{A} =< F, G >$, then if $H \in \mathcal{A}$, we have $H = F^{i_1}G^{j_1} \cdots F^{i_n}G^{j_m}$, where $n, m \geq 0$ and $i_1, \dots, i_n, j_1, \dots, j_m \in \mathbb{Z}$. Since $F^3 = G^3 = \mathrm{Id}_{\mathbb{C}(x)}$, we have $i_1, j_m \in \{0, 1, 2\}$ and $i_2, \dots, i_n, j_1, \dots, j_{m-1} \in \{1, 2\}$. Lastly, as FG and GF commute, $(FG)^2 = (GF)^2 = \mathrm{Id}_{\mathbb{C}(x)}$, $FGF = G^2$ and $GFG = F^2$, we deduce that $n + m \leq 3$ and conclude that $\mathcal{A} = \{\mathrm{Id}_{\mathbb{C}(x)} F, G, F^2, G^2, FG, GF, F^2G, FG^2, G^2F, GF^2, FG^2F\}$.

4. To show that this group is isomorphic to A_4, we establish the following isomorphism:

$$\sigma : \mathcal{A} \to A_4 \text{ with } \sigma(F) = (123) \text{ and } \sigma(G) = (234).$$

Knowing a presentation of A_4 by generators and relations, the calculations in items 1.,2. and 3. establish the isomorphism.

Another way to establish this isomorphism is to note that $\mathcal{A}$ is a non-commutative group with 12 elements which admits a normal subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Inspecting the classification of finite groups of order 12, we determine that $\mathcal{A} \cong A_4$.

Exercice 5 (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 $|\operatorname{Gal}(L/\mathbb{Q})| = 2$ 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 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 $|\operatorname{Gal}(L/\mathbb{Q})| = 4$. Now, let $\sigma, \tau \in \operatorname{Gal}(L/\mathbb{Q})$ 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 $\sigma^2 = \tau^2 = \mathrm{Id}_L$ and that $\sigma\tau = \tau\sigma$. Therefore $\operatorname{Gal}(L/\mathbb{Q}) =< \sigma, \tau > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 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. 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 $\mathbb{Q}(\sqrt{3}) \subseteq L^{<\sigma>}$, 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. 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 $|\operatorname{Gal}(L/\mathbb{Q})| = 8$. Let $\sigma_1, \sigma_2, \sigma_3 \in \operatorname{Gal}(L/\mathbb{Q})$ be such that:

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

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

One shows that $\sigma_i^2 = \mathrm{Id}_L$ for all $i = 1, 2, 3$ and that $\sigma_i\sigma_j = \sigma_j\sigma_i$ for all $i \neq j$, therefore determining that $\mathrm{Gal}(L/\mathbb{Q}) =< \sigma_1, \sigma_2, \sigma_3 >\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We first consider the subgroups of order 2 of $\mathrm{Gal}(L/\mathbb{Q})$. There are 7 of them and each of these is cyclic and generated by an element of $\mathrm{Gal}(L/\mathbb{Q})$. 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 $H =< \sigma_1 >$. One checks that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq L^H$, as $\sigma_1(\sqrt{3}) = \sqrt{3}$ and $\sigma_1(\sqrt{5}) = \sqrt{5}$. Therefore, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq L^H$, where $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$ and $[L^H : \mathbb{Q}] = 4$. We conclude that $L^H = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Similarly, one shows that:

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

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

We now consider the subgroups of order 4 of $\mathrm{Gal}(L/\mathbb{Q})$. Again, there are 7 of them and each of these is generated by two distinct elements of order 2 of $\mathrm{Gal}(L/\mathbb{Q})$ and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let H be one of these subgroups. 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:

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

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

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 $\mathbb{Q}$. By Proposition 4.6.3(d), it follows that $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$. We see that $t^4 - 2t^2 - 1 = (t^2 - 1 - \sqrt{2})(t^2 - 1 + \sqrt{2}) = (t - \sqrt{1 + \sqrt{2}})(t + \sqrt{1 + \sqrt{2}})(t - \sqrt{1 - \sqrt{2}})(t + \sqrt{1 - \sqrt{2}})$. Therefore $E = \mathbb{Q}(\sqrt{1 + \sqrt{2}}, \sqrt{1 - \sqrt{2}})$. Now, we 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 $|\operatorname{Gal}(E/\mathbb{Q})| = 8$.

Let $\sigma, \tau \in \operatorname{Gal}(E/\mathbb{Q})$ 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:

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

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

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

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

We now determine the subgroups of $\operatorname{Gal}(E/\mathbb{Q})$. There are 5 elements of order 2 in $\operatorname{Gal}(E/\mathbb{Q})$: τ,σ^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

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

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

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

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

Exercice 6.
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 know by Exercise 2. that $\sqrt{1+\sqrt{2}}$ is a root of the irreducible polynomial $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$, hence $m_{\sqrt{1+\sqrt{2}},\mathbb{Q}}(x) = x^4 - 2x^2 - 1$ and $[\mathbb{Q}(\sqrt{1+\sqrt{2}}) : \mathbb{Q}] = 4$. Moreover, we have already seen that 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 $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q})$. 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 $|\mathrm{Gal}(\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q})| = 2$ and we conclude, using Corollary 4.6.13, that the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is not Galois.

Exercice 7. 1. As $K \subseteq L$ is Galois, hence separable, and of finite degree, we have that $L = K(\alpha)$ for some $\alpha \in L \backslash K$, see Theorem 4.5.10. Similarly, one argues that $E = L(\beta)$ for some $\beta \in E \backslash L$.

For all $\sigma \in \mathrm{Gal}(L/K)$, let $\sigma^x : L[x] \to L[x]$ be the induced homomorphism, i.e.

$$\sigma^x(\sum_{i=1}^{n} a_i x^i) = \sum_{i=1}^{n} \sigma(a_i)x^i.$$

Note that, since σ is a K-automorphism of L, it follows that σ^x is an isomorphism of $L[x]$.

Consider the polynomial $m_1 = m_{\beta,L}$ and note that it is irreducible and separable over L. Let $\{m_1, m_2, \ldots, m_r\}$ be the $\mathrm{Gal}(L/K)$-orbit of m_1 in $L[x]$, where $m_i \nsim m_j$ for all $i \neq j$. Now, since m_1 is irreducible and, since for all m_i, $1 \leq i \leq r$, there exists $\sigma_i \in \mathrm{Gal}(L/K)$ such that $\sigma_i^x(m_1) = m_i$, it follows that m_i is irreducible for all $1 \leq i \leq r$. Therefore, $\gcd(m_i, m_j) = 1$ for all $i \neq j$.

We will now show that the polynomials m_i, $1 \leq i \leq r$, are separable. First, note that m_1 is separable as the extension $L \subseteq E$ is Galois, hence we have that $\gcd(m_1, \frac{d}{dx}m_1) = 1$, see

Corollary 4.4.10. Since for all $1 \leq i \leq r$ there exists $\sigma_i \in \mathrm{Gal}(L/K)$ such that $\sigma_i^x(m_1) = m_i$, we have that $\sigma_i^x(\frac{d}{dx}m_1) = \frac{d}{dx}m_i$ and thus $1 = \sigma_i^x(\gcd(m_1, \frac{d}{dx}m_1)) = \gcd(m_i, \frac{d}{dx}m_i)$. It follows that the polynomial $m_i(x) \in L[x]$ is separable for all $1 \leq i \leq r$.

Set $g(x) = \prod_{i=1}^{r} m_i(x) \in L[x]$. Now, we have shown that the m_i's, $1 \leq i \leq r$, are separable polynomials with $\gcd(m_i, m_j) = 1$, for all $i \neq j$. It follows that the polynomial $g(x)$ is also separable over L. We also remark that for all $\sigma \in \mathrm{Gal}(L/K)$ we have that

$$\sigma^x(g) = \sigma^x(\prod_{i=1}^{r} \sigma_i^x(m_1)) = \prod_{i=1}^{r}(\sigma^x \circ \sigma_i^x)(m_1) = \prod_{i=1}^{r} m_i,$$

as $\{m_1, m_2, \ldots, m_r\}$ is the $\mathrm{Gal}(L/K)$-orbit of m_1 and $\sigma \circ \sigma_i \in \mathrm{Gal}(L/K)$ for all $\sigma \in \mathrm{Gal}(L/K)$ and all $1 \leq i \leq r$. Therefore, we have that $g(x) \in L^{\mathrm{Gal}(L/K)}[x] = K[x]$, as $K \subseteq L$ is Galois.

Let F be the decomposition field of $m_{\alpha,K} \cdot g$ over K. Then F is generated by the roots of $m_{\alpha,K}$ and the roots of g. Note that $m_{\alpha,K}$ and g do not admit a common root $\gamma \in F$. If they would then $\gamma \in L$, as L is the decomposition field of $m_{\alpha,K}$, and therefore there would exist $1 \leq i \leq r$ such that $m_i(\gamma) = 0$, contradicting the fact that the m_i's are irreducible polynomials in $L[x]$. Now, as g and $m_{\alpha,K}$ are separable polynomials that do not admit common roots, it follows that F is generated by separable elements and thus the extension $K \subseteq F$ is Galois. Lastly, we have that $E \subseteq F$, as $E = L(\beta)$, $L = K(\alpha)$ and α, $\beta \in F$, since they are roots of $m_{\alpha,K}$ and g, respectively. We have shown that there exist a tower of extensions $K \subseteq E \subseteq F$ with $K \subseteq F$ Galois.

2. Let $\alpha \in E$. Then, we have $L \subseteq L(\alpha) \subseteq E$, where the extension $L \subseteq L(\alpha)$ is finite and separable. Now, let $m_{\alpha,L}(x) = \sum_{i=1}^{r} a_i x^i \in L[x]$. Then we have the tower of extensions $K \subseteq K(a_1, \ldots, a_r) \subseteq K(a_1, \ldots, a_r, \alpha) \subseteq L(\alpha)$ where $K \subseteq K(a_1, \ldots, a_r)$ and $K(a_1, \ldots, a_r) \subseteq K(a_1, \ldots, a_r, \alpha)$ are finite and separable. Moreover, we note that $m_{\alpha,L}(x) \in K(a_1, \ldots, a_r)[x]$.

   Set F to be the splitting field of $\prod_{i=1}^{r} m_{a_i,K}(x)$ over K. Then $F : K$ is finite and F is generated, over K, by the roots of $m_{a_i,K}$ for all $1 \leq i \leq r$, see Lemma 4.3.3. As a_i is separable over K for all $1 \leq i \leq r$, then so are all the other roots of $m_{a_i,K}$ and we deduce that the extension $K \subseteq F$ is separable. Hence, it is Galois. Moreover, we note that $K(a_1, \ldots, a_r) \subseteq F$.

   Set G be the splitting field of $m_{\alpha,L}(x)$ over F. Then $[G : F]$ is finite and G is generated, over F, by the roots of the polynomial $m_{\alpha,L}(x)$, see Lemma 4.3.3. As $\alpha \in K(a_1, \ldots, a_r, \alpha)$ is separable over $K(a_1, \ldots, a_r)$, we have that α is separable over F, since $m_{\alpha,F} | m_{\alpha,K(a_1,\ldots,a_r)}$. Therefore, the extension $F \subseteq G$ is Galois and finite. Moreover, we have that $K(a_1, \ldots, a_r, \alpha) \subseteq G$. We have built the following extension diagram:

$$\begin{array}{ccccccc} K & \hookrightarrow & K(a_1,\ldots,a_r) & \hookrightarrow & K(a_1,\ldots,a_r,\alpha) & & \\ & & \downarrow & & \downarrow & & \\ K & \hookrightarrow & F & \hookrightarrow & G & \hookrightarrow & H \end{array}$$

   where $K \subseteq H$ is a Galois extension, see item 1. Therefore, H is separable over K, hence, in particular, we have that $K(a_1, \ldots, a_r, \alpha)$ is separable over K. We have shown that all $\alpha \in E$ are separable over K and we conclude that E is separable over K.

Exercice 8.
Let K be a countable field and consider the polynomial ring $K[x]$. For all $i \geq 0$ define the subsets $K^i[x] \subseteq K[x]$ with $K^i[x] = \{f \in K[x] | \deg(f) = i\}$. We remark that $K[x] = \bigcup_{i \geq 0} K^i[x]$ and that

$K^i[x] \cong K^i$, hence $|K^i[x]| = i \cdot |K| = |K|$, for all $i \geq 0$. It follows that $|K[x]| = \aleph_0 \cdot |K| = \aleph_0$ and so $K[x]$ is also countable.

We define the map $\phi : \overline{K} \to K[x]$ by $\phi(\alpha) = m_{\alpha,K}$. Now the subset $\phi(\overline{K})$ of $K[x]$ contains all polynomials of the form $x - \alpha$, where $\alpha \in K$, hence $\phi(\overline{K})$ is also countable. Lastly, for any $m_{\alpha,K} \in \phi(\overline{K})$ we have that the preimage $\phi^{-1}(m_{\alpha,K})$ is non-empty and finite, as $\alpha \in \phi^{-1}(m_{\alpha,K})$ and $m_{\alpha,K}$ admits a finite number of roots. We conclude that $\overline{K}$ has the same cardinality as $\phi(\overline{K})$, hence it is countable.

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

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

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

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

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

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

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

Supplementary exercise

Exercice 10. 1. As $K \subseteq L$ is a purely inseparable extension, it follows that $\alpha \in L \backslash K$ is purely inseparable over K, thus there exists $n \geq 1$ such that $\alpha^{p^n} \in K$. We fix such an $\alpha \in L \backslash K$ and we let $\sigma \in \operatorname{Gal}(L/K)$. It suffices to show that $\sigma(\alpha) = \alpha$.

The element $\alpha \in L/K$ is the unique p^nth root of α^{p^n}, see Exercise 2.(a) of Series 11. Therefore, it suffices to show that $(\sigma(\alpha))^{p^n} = \alpha^{p^n}$. We have:

$$(\sigma(\alpha))^{p^n} = \sigma(\alpha^{p^n}) = \alpha^{p^n}.$$

We conclude that $\operatorname{Gal}(L/K) = \{\mathrm{Id}_L\}$.

2. First, we will show that $L_{insep,K} \subseteq L^{\operatorname{Gal}(L/K)}$. For this, let $\alpha \in L_{insep,K}$ and let $\sigma \in \operatorname{Gal}(L/K)$. As $\alpha \in L_{insep,K}$, there exists $n \in \mathbb{Z}_{\geq 0}$ such that $\alpha^{p^n} \in K$. Then:

$$\sigma(\alpha)^{p^n} = \sigma(\alpha^{p^n}) = \alpha^{p^n} \in K$$

and it follows that $\sigma(\alpha) \in L_{insep,K}$. Hence the restriction $\sigma|_{L_{insep,K}}$ is a K-automorphism of $L_{insep,K}$ and thus $\sigma|_{L_{insep,K}} = \mathrm{Id}_{L_{insep,K}}$, see item 1. Therefore $\sigma(\alpha) = \sigma|_{L_{insep,K}}(\alpha) = \alpha$ for all $\alpha \in L_{insep,K}$ and thus $L_{insep,K} \subseteq L^{\operatorname{Gal}(L/K)}$.

We now consider the extension tower:

$$K \subseteq L_{insep,K} \subseteq L^{\operatorname{Gal}(L/K)} \subseteq L.$$

We have that $[L : K] = [L : L_{insep,K}][L_{insep,K} : K]$, hence $[L : L_{insep,K}] = |\operatorname{Gal}(L/K)|$.On the other hand, we have $[L : L^{\operatorname{Gal}(L/K)}] = |\operatorname{Gal}(L/K)|$, see Theorem 4.6.12, and we deduce that $[L^{\operatorname{Gal}(L/K)} : L_{insep,K}] = 1$, hence $L^{\operatorname{Gal}(L/K)} = L_{insep,K}$. Lastly, the extension $L^{\operatorname{Gal}(L/K)} \subseteq L$ is separable, see Proposition 4.6.10, and we conclude that $L_{insep,K} \subseteq L$ is separable.