Exercise 10.1. Let $K, E, F \subseteq L$ be fields, $E : K, F : K$ be finite extensions. Prove

(a) if $E : K$ is separable, then $EF : F$ is separable;

(b) if $E : K$ and $F : K$ are both separable, then $EF : K$ and $E \cap F : K$ are both separable;

(c) if $E : K$ is Galois, then $EF : F$ is Galois;

(d) if $E : K$ and $F : K$ are both Galois, then $EF : K$ and $E \cap F : K$ are both Galois.

(a) *Solution.* Suppose $E : K$ is separable. We are given that $E : K$ and $F : K$ are finite, so we can write $E = K(\alpha_1, \ldots, \alpha_n)$ and $F = K(\beta_1, \ldots, \beta_m)$ for $\alpha_i \in E$ and $\beta_j \in F$. Then the composite field EF becomes

$$\begin{aligned} EF &= K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) \\ &= F(\alpha_1, \ldots, \alpha_n). \end{aligned}$$

Since $E : K$ is finite it is also algebraic, hence the minimum polynomial for each element of E is well defined over K, and similarly for $EF : F$. For any $b \in F$, the minimal polynomial over F is $x - b$, which has distinct roots, so b is separable over F. Hence it is enough to show that $\alpha_1, \ldots, \alpha_n$ is separable over F.

We have that μ_α^K is separable by hypothesis for all $\alpha \in \{\alpha_1, \ldots, \alpha_n\}$. Then $\mu_\alpha^K(x) \in K[x] \subseteq F[x]$ so μ_α^F divides μ_α^K and thus μ_α^F is thus also separable, whence $EF : F$ is separable. □

(b) *Solution.* Suppose $E : K$ and $F : K$ are both separable. Similarly to part (a), we can write

$$EF = K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m),$$

for $\alpha_i \in E$ and $\beta_j \in F$. By definition, a is separable over K for all $a \in E$, and similarly for $b \in F$. Then each $\alpha_1, \ldots, \alpha_n \in E,\ \beta_1, \ldots, \beta_m \in F$ is separable over K. By theorem an extension $K(\gamma_1, \ldots, \gamma_k) : K$ is separable iff each γ_i is separable over K. Thus $EF : K$ is separable. Furthermore, we know $E : K$ is separable and $E \cap F \subseteq E$, so $E \cap F : K$ is separable by definition. □

(c) *Solution.* Suppose $E : K$ is Galois. Then $E : K$ is normal and separable by definition. Since $E : K$ and $F : K$ are both finite and $E : K$ is normal, we have by lemma that $EF : F$ is normal and by part (a), $EF : F$ is separable. Thus $EF : F$ is Galois. □

(d) *Solution.* Suppose $E : K$ and $F : K$ are both Galois. Then $E : K$ and $F : K$ are both normal and separable by definition. Since $E : K$ and $F : K$ are both finite and normal, we have by lemma that $EF : K$ and $E \cap F : K$ are both normal and by part (b), $EF : K$ and $E \cap F : K$ are both separable. Thus $EF : K$ and $E \cap F : K$ are both Galois. □

Exercise 10.2. (a) Find the splitting field L of the polynomial $f(t) = t^4 - 4t^2 + 5$.

(b) Prove that $[L : \mathbb{Q}]$ is either 4 or 8.

(c) Find 10 intermediate fields of the extension $L : \mathbb{Q}$ and their degrees.

(d) (for enthusiasts) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(f)$.

(a) *Solution.* Notice that

$$t^4 - 4t^2 + 5 = 0 \quad \Longrightarrow \quad t^4 - 4t^2 + 4 = \left(t^2 - 2\right)^2 = -1.$$

Hence $t^2 - 2 = \pm i$ and we have roots $t \in \left\{\sqrt{2+i}, -\sqrt{2+i}, \sqrt{2-i}, -\sqrt{2-i}\right\}$. Thus

$$L = \mathbb{Q}\left(\sqrt{2+i}, \sqrt{2-i}\right)$$

□

(b) *Solution.* Clearly for $E := \mathbb{Q}\left(\sqrt{2+i}\right)$, we have that $E:\mathbb{Q}$ is a degree 4 extension. We note here that $i \in E$, which follows from the fact that $\left(\sqrt{2+i}\right)^2 - 2 = i$. So the minimum polynomial for $\sqrt{2-i}$ over E is $x^2 - (2-i)$. Hence if $\sqrt{2-i} \in E$, then $[L:\mathbb{Q}] = 4$ but if not, then $[L:E] = 2$ whence $[L:\mathbb{Q}] = 8$ by the tower law.

Notice that $F := \mathbb{Q}\left(\sqrt{2+i} + \sqrt{2-i}\right)$ is a proper subset of L. It is easy to see that $[F:\mathbb{Q}] = 4$, so we have $[L:\mathbb{Q}] > 4$. Thus $\sqrt{2-i} \notin E$ whence $L:E$ must have degree 2 and by the tower law, $[L:\mathbb{Q}] = 8$. □

(c) *Solution.* Notice

$$\left[\overline{\sqrt{2+i}}\right]^2 = \overline{\left[\left(\sqrt{2+i}\right)^2\right]} = \overline{2+i} = 2-i \qquad \Longrightarrow \qquad \overline{\sqrt{2+i}} = \sqrt{2-i}.$$

That is, the square roots of complex conjugates are themselves complex conjugates. Define σ such that $\sqrt{2+i} \mapsto \sqrt{2-i}$ and $\sqrt{2-i} \mapsto -\sqrt{2+i}$, and let τ be complex conjugation. Obviously $\tau^2 = \sigma^4 = \mathrm{Id.}$. Notice

$$\tau\sigma\tau\left(\sqrt{2+i}\right) = \tau\sigma\left(\sqrt{2-i}\right) = \tau\left(-\sqrt{2+i}\right) = -\sqrt{2-i} = \sigma^{-1}\left(\sqrt{2+i}\right).$$

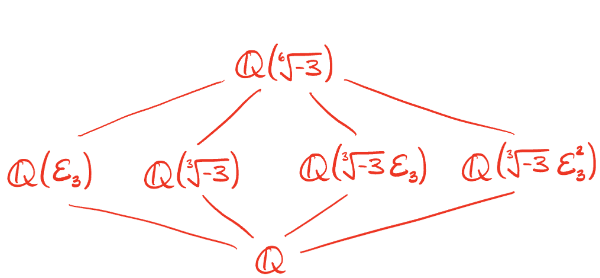
That is, $\tau\sigma\tau = \sigma^{-1}$ These are the defining features of D_4, the dihedral group of 4 points. Hence $\mathrm{Gal}_{\mathbb{Q}}\left(t^4 - 4t^2 + 5\right) \cong D_4$ has exactly ten subgroups, and by the Galois correspondence there are ten intermediate fields. We can idenitfy these subfields of L by finding the fixed field L^H for each subgroup H of D_4. Letting $\alpha = \sqrt{2+i}$ and $\beta = \sqrt{2-i}$, we have:

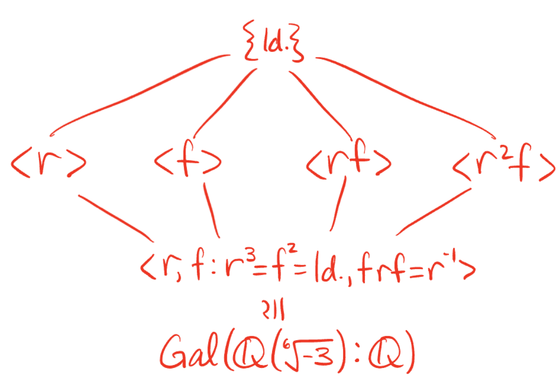
$$\begin{aligned}
1 &= [\mathbb{Q}:\mathbb{Q}], \\
2 &= [\mathbb{Q}(i):\mathbb{Q}] = \left[\mathbb{Q}\left(\sqrt{5}\right):\mathbb{Q}\right] = [\mathbb{Q}(\alpha/\beta):\mathbb{Q}], \\
4 &= [\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\beta):\mathbb{Q}] = \left[\mathbb{Q}\left(i,\sqrt{5}\right):\mathbb{Q}\right] = [\mathbb{Q}(\alpha+\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha-\beta):\mathbb{Q}], \\
8 &= [L:\mathbb{Q}]
\end{aligned}$$

□

Exercise 10.3. Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}\left(t^6+3\right)$. *Hint*: Use the calculations (and the notation, if you like) from Lecture 18.

Solution. From Lecture 18, we have that the splitting field is $L = \mathbb{Q}\left(\sqrt[6]{-3}\right)$ and $\mathrm{Gal}_{\mathbb{Q}}\left(t^6+3\right) \cong D_3 \cong S_3$. Cubing the generator yields $\sqrt[3]{-3}$, whence we have the subfield $\mathbb{Q}\left(\sqrt[3]{-3}\right) \subseteq L$. Moreover, we know $\varepsilon_6 \in L$ from lecture so we have $\varepsilon_3 = \varepsilon_6^2 \in L$ and we can generate subfields $\mathbb{Q}(\varepsilon_3)$, $\mathbb{Q}\left(\varepsilon_3\sqrt[3]{-3}\right)$, and $\mathbb{Q}\left(\varepsilon_3^2\sqrt[3]{-3}\right)$. We note here that $\sqrt[6]{-3}^3 = i\sqrt{3}$ and $\mathbb{Q}(\varepsilon_3) = \mathbb{Q}(\varepsilon_6) = \mathbb{Q}\left(i\sqrt{3}\right)$, which can easily be seen by decomposing ε_3 and ε_6 by Euler's formula. Thus we have identified all the unique subfields of $\mathbb{Q}\left(\sqrt[6]{-3}\right)$.





$\square$