**Exercise 7.1.** Let $K = \mathbb{Q}$, $M = \mathbb{Q}(2^{1/3})$ and $L = \mathbb{Q}(2^{1/3}, \sqrt{3}, i)$. Prove that $L : K$ and $L : M$ are normal but $M : K$ is not normal.

*Solution.* We know that a field extension $F_1 : F_2$ is normal iff it is a splitting field extension for some $f \in F_2[t]$. Consider the polynomial $f(t) = (t^2 - 3)(t^2 + 1)$. Then,

$$f(t) = (t + \sqrt{3})(t - \sqrt{3})(t + i)(t - i),$$

whence $L : M$ is a splitting field extension for $f$.

Next, consider $g(t) = (t^2 - 3)(t^2 + 1)(t^3 - 2)$. Then,

$$f(t) = (t + \sqrt{3})(t - \sqrt{3})(t + i)(t - i)(t - \sqrt[3]{2})(t - \varepsilon_3 \sqrt[3]{2})(t - \varepsilon_3^2 \sqrt[3]{2}),$$

where $\varepsilon_3 = \exp\left(\frac{2\pi}{3} i\right)$. Notice,

$$\begin{aligned}\varepsilon_3 &= \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) \\ &= -\frac{1}{2} + i\frac{\sqrt{3}}{2} \\ &= \frac{1}{2}\left(-1 + i\sqrt{3}\right) \in \mathbb{Q}(3^{1/3}, i, \sqrt{3})\end{aligned}$$

$$\begin{aligned}\varepsilon_3^2 &= \cos\left(\frac{4\pi}{3}\right) + i \sin\left(\frac{4\pi}{3}\right) \\ &= -\frac{1}{2} - i\frac{\sqrt{3}}{2} \in \mathbb{Q}(2^{1/3}, i, \sqrt{3}) \\ &= \frac{1}{2}\left(-1 - i\sqrt{3}\right) \in \mathbb{Q}(2^{1/3}, i, \sqrt{3}).\end{aligned}$$

Thus $L : K$ is a splitting field extension for $f$, hence it is normal.

By definition, an extension $M : K$ is normal if $\forall \alpha \in M$, the minimum polynomial of $\alpha$ over $K$, $\mu_\alpha^K(t)$, splits over $M[t]$. Obviously, $\sqrt[3]{2} \in \mathbb{Q}(2^{1/3})$ by construction. However, notice that for $\alpha = \sqrt[3]{2}$,

$$\begin{aligned}\mu_\alpha^K(t) &= t^3 - 2 \\ &= (t - \sqrt[3]{2})(t - \varepsilon_3 \sqrt[3]{2})(t - \varepsilon_3^2 \sqrt[3]{2}),\end{aligned}$$

where $\varepsilon_3 = \exp\left(\frac{2\pi}{3} i\right)$. However, we just showed that $\varepsilon_3$ and $\varepsilon_3^2$ are complex numbers and thus the linear factors $(t - \varepsilon_3 \sqrt[3]{2})$ and $(t - \varepsilon_3^2 \sqrt[3]{2})$ do not lie in $M[t]$. Thus $M : K$ is not a normal extension by definiton. ☐

**Exercise 7.2.1.** Let $K - L$ be algebraic, $\alpha \in L$ and $\sigma : K \to \overline{K}$ be a homomorphism. Prove that $\mu_\alpha^K$ is separable over $K$ iff $\sigma(\mu_\alpha^K)$ is separable over $\sigma(K)$.

*Solution.* Since we have a homomorphism from $K \to \overline{K}$, we know that the extension $\overline{K} : K$ exists. Moreover, it is obviously algebraic by definition of $\overline{K}$. Thus there exists some isomorphism $\overline{\sigma} : \overline{K} \to \overline{K}$ extending $\sigma$, and we note that $\overline{\sigma}|_K = \sigma$. Since $K - L$ is algebraic we know that $\mu_\alpha^K$ exists. Further, since all coefficients of $\mu_\alpha^K$ are in $K$ and $K \subseteq \overline{K}$, we can say $\mu_\alpha^K(t) \in \overline{K}[t]$. By definition of algebraic closure, observe that we can split $\mu_\alpha^K$ over $\overline{K}[t]$ in the following form:

$$\mu_\alpha^K(t) = \prod_{i=1}^{d} (t - \alpha_i)^{r_i}, \quad r \in \mathbb{N}$$

Since $\overline{\sigma}|_K = \sigma$, we have that $\overline{\sigma}(\mu_\alpha^K) = \sigma(\mu_\alpha^K)$ and $\overline{\sigma}(K) = \sigma(K)$. We know homomorphisms preserve operations, whence

$$\overline{\sigma}\left(\mu_\alpha^K(t)\right) = \prod_{i=1}^{d} (t - \overline{\sigma}(\alpha_i))^{r_i} = \prod_{i=1}^{d} (t - \sigma(\alpha_i))^{r_i}.$$

Furthermore, any field homomorphism must be injective, so each $\overline{\sigma}(\alpha_i)$ is necessarily distinct. Hence $\mu_\alpha^K$ has multiple roots $\iff \overline{\sigma}(\mu_\alpha^K) = \sigma(\mu_\alpha^K)$ has multiple roots. Moreover by irreducibility of $\mu_\alpha^K$ over $K$, we have that $\overline{\sigma}(\mu_\alpha^K) = \sigma(\mu_\alpha^K)$ is irreducible over the image of $K$. Thus $\mu_\alpha^K$ is separable over $K \iff \sigma(\mu_\alpha^K)$ is separable over $\sigma(K)$. $\square$

**Exercise 7.2.2.** Let $L : K$ be a splitting field for $f \in K[t]$. Prove that if $f$ is separable, then $L : K$ is separable.

*Solution.* We are given that $L : K$ is a splitting field extension for $f$, and by theorem we know $L = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_j \in L$ is a root of $f$ for $1 \leq j \leq n$. Then for each $j$ the minimum polynomial of $\alpha_j$ must divide $f$, and thus $\mu_{\alpha_j}^K$ is separable over $K$ by separability of $f$ and the definition of separable. Then $\alpha_j$ is separable over $K$ for each $j$ and hence $L : K$ is separable by theorem. $\square$

**Exercise 7.3.** Let $L : K$ be a splitting field extension for a polynomial $f \in K[t]$. Then $L : K$ is separable iff $f$ is separable over $K$.

*Solution.* We saw in 7.2.2 that separability of $f$ implies separability of $L : K$. Hence it is enough to show that the separability of $L : K$ implies the separability of $f$. Similarly to the previous problem, we have that $L = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_j \in L$ is a root of $f$ for $1 \leq j \leq n$. By theorem, the separability of $L : K$ implies that each $\alpha_j$ is separable over $K$. Thus by definition of separability of $\alpha_j$, we have that $\mu_{\alpha_j}^K$ is separable. Then since $\alpha_j$ is a root of $f$, we know $\mu_{\alpha_j}^K \,\big|\, f$ for all $j$. Assume ad absurdum that $f$ is not separable. Then upon splitting over $L$, there must be some linear factor $(t - \alpha_k)$ raised to the power of at least 2. By uniqueness of $\mu_{\alpha_k}^K$ this tells us that $\mu_{\alpha_k}^K$ must also have a repeated root, contradicting the separability of $\mu_{\alpha_k}^K$. Hence $f$ must be separable over $K$. $\square$

**Exercise 7.4.** Let $K - M - L$ be an algebraic extension. Prove that $K - L$ is separable iff $K - M$ and $M - L$ are separable.

*Solution.* ( $\Longrightarrow$ ) Suppose $K - L$ is separable. Then $\alpha$ is separable (i.e. algebraic and $\mu_\alpha^K$ separable) over $K$ for all $\alpha \in L$. Since $M \subseteq L$, we have that $\beta$ is separable over $K$ for all $\beta \in M$, whence $K - M$ is separable. It remains to show that $M - L$ is separable. Suppose $\gamma \in M$. Since $\gamma \in L$, we have that $\mu_\gamma^K$ is separable. Consider $\mu_\gamma^M$. We have by lemma that $\mu_\gamma^M \,\big|\, \mu_\gamma^K$ in $M[t]$. Since $\mu_\gamma^K$ splits into distinct linear factors, this means $\mu_\gamma^M$ must have distinct roots as well. So $\mu_\gamma^M$ is separable and thus $\gamma$ is separable for all $\gamma \in L$. Thus by definition $L : M$ is separable.

( $\Longleftarrow$ ) Assume that both $K - M$ and $M - L$ are separable. We wish to show that $L$ is separable over $K$. Let $\alpha \in L$. By separability of $L : M$, we have that $\mu_\alpha^M(t)$ is separable. Since $\alpha$ is algebraic over $K$, its minimal polynomial over $K$, $\mu_\alpha^K(t) \in K[t]$, exists. Moreover, because $K \subset M$, we can view $\mu_\alpha^K(t)$ as a polynomial in $M[t]$. Since $\mu_\alpha^K$ and $\mu_\alpha^M$ share a root, we have that $\mu_\alpha^M(t) \mid \mu_\alpha^K(t)$ in $M[t]$. That is, there exists some $h(t) \in M[t]$ such that $\mu_\alpha^K(t) = \mu_\alpha^M(t)h(t)$.

Now, assume ad absurdum that $\mu_\alpha^K(t)$ is not separable. Then in its factorization over an algebraic closure some linear factor appears with multiplicity $\geq 2$. That is, there exists some $\gamma$ such that $(t - \gamma)^n$ divides $\mu_\alpha^K(t)$ with $n \geq 2$. We know $\mu_\alpha^M(t)$ has distinct roots, so $(t - \gamma)$ must be a factor of $h(t)$ with multiplicity $\geq 1$. Notice that

$$D(\mu_\alpha^K(t)) = D(\mu_\alpha^M(t))h(t) + \mu_\alpha^M(t)D(h(t)), \tag{1}$$

and if we let $t = \gamma$,

$$D(\mu_\alpha^K(\gamma)) = D(\mu_\alpha^M(\gamma))h(\gamma) + \mu_\alpha^M(\gamma)D(h(\gamma)). \tag{2}$$

Since $\gamma$ is a repeated root of $\mu_\alpha^K$, we have that $D(\mu_\alpha^K(\gamma)) = 0$. Also since $\mu_\alpha^K(\gamma) = \mu_\alpha^M(\gamma)h(\gamma) = 0$, either $\mu_\alpha^M(\gamma) = 0$ or $h(\gamma) = 0$ must be true.

*Case 1 ($\mu_\alpha^M(\gamma) = 0$).* In this case, equation (2) simplifies to $0 = D(\mu_\alpha^M(\gamma))h(\gamma)$. If $h(\gamma) \neq 0$ then $\gamma$ must be a repeated root of $\mu_\alpha^M$, contradicting its separability. ■

*Case 2 ($h(\gamma) = 0$).* In this case, equation (2) simplifies to $0 = \mu_\alpha^M(\gamma)D(h(\gamma))$. We know $\mu_\alpha^M(\gamma) \neq 0$ otherwise we return to case 1 and reach a contradiction. Thus $D(h(\gamma)) = 0$ must be true, whence $\gamma$ is a repeated root of $h(t)$. ■

Thus a repeated root in $\mu_\alpha^K$ forces one of its factors with coefficients in $M$ to have a repeated root and thus be inseparable. But then $\gamma$ would become inseparable since the minimum polynomial of $\gamma$ over $M$ must divide $h$, which contradicts the fact that $L : M$ is separable. Thus $\mu_\alpha^K$ must be separable over $L$ for arbitrary $\alpha$, whence $L : K$ is separable. □