Q1 Show that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Proof. Consider $\mathbb{Q}$ as a subfield of $\mathbb{C}$. For each $n \in \mathbb{N}$, $\sqrt[n]{2} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, as it is a root of the polynomial $x^n - 2 \in \mathbb{Q}[x]$. In fact, $m_{\sqrt[n]{2},\mathbb{Q}}(x) = x^n - 2$, since it is monic and irreducible over $\mathbb{Q}$, by Eisenstein's criterion. Then

$$[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = \deg m_{\sqrt[n]{2},\mathbb{Q}}(x) = \deg(x^n - 2) = n.$$

So $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ is algebraic, therefore $\overline{\mathbb{Q}(\sqrt[n]{2})} = \overline{\mathbb{Q}}$. We may now deduce

$$[\overline{\mathbb{Q}} : \mathbb{Q}] = [\overline{\mathbb{Q}(\sqrt[n]{2})} : \mathbb{Q}(\sqrt[n]{2})][\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n.$$

Since $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$ for all $n \in \mathbb{N}$, then necessarily $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

$$a + (b \cdot c) = (a + b) \cdot (a + c)$$

$\square$

Q2 Let $F \subseteq K \subseteq L$ be fields. Show that if L/F is separable, then both K/F and L/K are separable.

Proof. We first show K/F is separable. For each $\alpha \in K$, we also have $\alpha \in L$. And since L/F is separable, then α is separable over F. Hence, K/F is separable.

Next, we show L/K is separable. First, note that L/F is algebraic, so K/F and L/K are both algebraic. Let $\alpha \in L$ and consider its minimal polynomials $m_{\alpha,K}(x) \in K[x]$ and $m_{\alpha,F}(x) \in F[x]$. Since the minimal polynomial of α over F is also a polynomial over K with α as a root, then $m_{\alpha,K}(x) \mid m_{\alpha,F}(x)$. Then any root $\beta \in \overline{K}$ of $m_{\alpha,K}(x)$ is also a root of $m_{\alpha,F}(x)$. Moreover, because K/F is algebraic, we have $\overline{K} = \overline{F}$, so $\beta \in \overline{F}$.

Since L/F is separable and $\alpha \in L$, then $m_{\alpha,F}(x)$ is separable over F. Then β is a simple root for $m_{\alpha,F}(x)$. In $\overline{K}[x] = \overline{F}[x]$, we must at least have $(x-\beta) \mid m_{\alpha,K}(x)$. However, $(x-\beta)^2$ must not divide $m_{\alpha,K}(x)$, as $m_{\alpha,K}(x) \mid m_{\alpha,F}(x)$ but $(x-\beta)^2$ does not divide $m_{\alpha,F}(x)$. Hence, β is a simple root for $m_{\alpha,K}(x)$, and we conclude that L/K is separable.

$\square$

Q3 Let F be a field and A be a subset of $F[x]$. An algebraic extension K of F is called a *splitting field* for A over F if

(i) every polynomial in A splits completely in $K[x]$,

(ii) if $F \subseteq E \subseteq K$ and every polynomial in A splits completely in $E[x]$, then $E = K$.

Lemma 1. Let K/F be a field extension and let $f(x), g(x) \in F[x]$ be nonzero polynomials such that their product $f(x)g(x)$ splits completely in $K[x]$. Then both $f(x)$ and $g(x)$ split completely in $K[x]$.

Proof. We will use induction on $n = \deg f(x)g(x)$. For the base case, $n = 1$, we have

$$f(x)g(x) = a(x - \alpha)$$

for some $a \in F^\times$ and $\alpha \in K$. Then $\deg f(x) + \deg g(x) = 1$, so one of the two polynomials has degree 1 and the other has degree 0. Assume $\deg g(x) = 0$, so $g(x) = g \in F^\times$ (and $g(x)$ splits completely in $K[x]$). Then

$$f(x) = g^{-1}a(x - \alpha)$$

is a factorization of $f(x)$ into linear factors in $K[x]$, so $f(x)$ splits completely in $K[x]$.

As the induction hypothesis, assume the result is true for any pair of polynomials in $K[x]$ whose product has degree at most $n - 1$. Now suppose $\deg f(x)g(x) = n$, so

$$f(x)g(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$$

for some $a \in F^\times$ and $\alpha_1, \ldots, \alpha_n \in K$. Since $x - \alpha_n$ is an irreducible polynomial in the UFD $K[x]$, then it is prime. Then the fact that $(x - \alpha_n) \bigm| f(x)g(x)$ implies $x - \alpha_n$ divides either $f(x)$ or $g(x)$. Without loss of generality, assume $(x - \alpha_n) \bigm| g(x)$, so

$$g(x) = (x - \alpha_n)h(x)$$

for some $h(x) \in K[x]$ with $\deg h(x) = \deg g(x) - 1$. Then we have

$$f(x)h(x) = a(x - \alpha_1) \cdots (x - \alpha_{n-1}).$$

Because $\deg f(x)h(x) = n - 1$, then we may apply the induction hypothesis to deduce that both $f(x)$ and $h(x)$ split completely in $K[x]$. As $h(x)$ splits completely in $K[x]$, we write

$$h(x) = b(x - \beta_1) \cdots (x - \beta_m)$$

for some $b \in F^\times$ and $\beta_1, \ldots, \beta_m \in K$. Then

$$g(x) = b(x - \beta_1) \cdots (x - \beta_m)(x - \alpha_n),$$

which is a factorization of $g(x)$ into linear factors in $K[x]$. Hence, $g(x)$ splits completely in $K[x]$, which completes the induction.

□

(a) Suppose that $A = \{f_1(x), f_2(x), \ldots, f_n(x)\} \subseteq F[x]$. Let $f(x) = \prod_{j=1}^n f_j(x)$ and K be a splitting field of $f(x) \in F[x]$. Show that that K is a splitting field of A over F.

Proof. We will use induction on n. For the base case, if $n = 1$, then $f(x) = f_1(x)$ and K is simply the splitting field of $f_1(x)$. This is the same as saying K is the splitting field for the singleton $A = \{f_1(x)\}$.

For the inductive hypotheses, assume that the result is true for any subset of $F[x]$ containing at most $n-1$ polynomials. For $j = 1, \ldots, n-2$ define $g_j(x) = f_j(x)$, and define $g_{n-1}(x) = f_{n-1}(x)f_n(x)$. Then we apply the induction hypothesis to the subset $B = \{g_1(x), \ldots, g_{n-1}(x)\} \subseteq F[x]$ containing $n-1$ polynomials. We see that

$$g_1(x) \cdots g_{n-1}(x) = f_1(x) \cdots f_{n-1}(x) f_n(x) = f(x),$$

so K is a splitting field of B over F. In particular, $g_{n-1}(x) = f_{n-1}(x)f_n(x)$ splits completely in $K[x]$, so Lemma 1 tells us that both $f_{n-1}(x)$ and $f_n(x)$ split completely in $K[x]$. And since $f_1(x), \ldots, f_{n-2}(x) \in B$ also split completely in $K[x]$, we conclude that every polynomial in A splits completely in $K[x]$.

Suppose E is a field such that $F \subseteq E \subseteq K$ and every polynomial in A splits completely in $E[x]$. Then, for $j = 1, \ldots, n-2$, each $g_j(x) = f_j(x)$ splits completely in $E[x]$. We write

$$f_{n-1}(x) = a(x-\alpha_1)\cdots(x-\alpha_m) \quad \text{and} \quad f_n(x) = b(x-\beta_1)\cdots(x-\beta_k),$$

for some $a, b \in F^\times$ and $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_k \in E$. Then

$$g_{n-1}(x) = ab(x-\alpha_1)\cdots(x-\alpha_m)(x-\beta_1)\cdots(x-\beta_k)$$

is a factorization of $g_{n-1}(x)$ into linear factors in $E[x]$. Hence, every polynomial in B splits completely in $E[x]$. Since K is a splitting field of B over F, then $E = K$. Thus, K is a splitting field of A over F.

□

(b) Let $S \subseteq \overline{F}$ be the subset consisting of roots of polynomials in A. Show that $F(S)$ is a splitting field of A over F.

Proof. Because $F(S) \subseteq \overline{F}$, we know that $F(S)/F$ is an algebraic field extension. For each $f(x) \in A$, we have

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$$

for some $a \in F$ and $\alpha_1, \ldots, \alpha_n \in \overline{F}$. Since $\alpha_1, \ldots, \alpha_n$ are precisely the roots of $f(x)$, they are contained in $S \subseteq F(S)$. Therefore, this is a factorization of $f(x)$ into linear factors in $(F(S))[x]$, i.e., every polynomial in A splits completely in $(F(S))[x]$.

Suppose E is a field such that $F \subseteq E \subseteq F(S)$ and every polynomial in A splits completely in $E[x]$. Given $\alpha \in S$, there is some $f(x) \in A$ such that α is a root of $f(x)$. Then we write

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n),$$

for some $a \in F$ and $\alpha_1, \ldots, \alpha_n \in E$. Since $f(\alpha) = 0$, then $\alpha = \alpha_j$ for some j. This implies $\alpha \in E$, and we conclude that $S \subseteq E$. Since the field E also contains F, then in fact $F(S) \subseteq E$. Therefore, as we have the opposite inclusion by assumption, we have equality $E = F(S)$. Hence, $F(S)$ is a splitting field of A over F.

□

(c) Suppose that K is a splitting field of A over F. Show that there exists a field isomorphism $\varphi : K \to F(S)$ such that $\varphi|_F = \mathrm{id}_F$.
(Hint: Prop 5 on Apr 13 can be useful.)

Proof. Both $F(S)/F$ and K/F are algebraic. Consider the algebraic closure $\overline{F}$ of F, which contains $F(S)$ as a subfield. Then Proposition 5 implies the existence of a field embedding $\varphi : K \to \overline{F}$ such that the following diagram commutes:

$$\begin{tikzcd}
F \arrow[r, hook] \arrow[d, hook] & F(S) \arrow[r, hook] & \overline{F} \\
K \arrow[urr, "\varphi"'] & &
\end{tikzcd}$$

In particular, $\varphi|_F = \mathrm{id}_F$. Since the inclusion map $F \hookrightarrow \overline{F}$ is injective, then φ is injective, therefore $K \cong \varphi(K)$. We claim that $\varphi(K) = F(S)$.

Given a polynomial $f(x) \in A$, we have

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$$

for some $a \in F^\times$ and $\alpha_1, \ldots, \alpha_n \in F(S)$. More specifically, we know that $\alpha_1, \ldots, \alpha_n \in S$. Additionally,

$$f(x) = b(x - \beta_1) \cdots (x - \beta_n)$$

for some $b \in F^\times$ and $\beta_1, \ldots, \beta_n \in K$. Extending φ to a ring homomorphism $\varphi' : K[x] \to \overline{F}[x]$, we know that $\varphi'|_{F[x]} = \mathrm{id}_{F[x]}$. Then in $\overline{F}[x]$, we find

$$f(x) = \varphi'(f(x)) = \varphi'(b(x - \beta_1) \cdots (x - \beta_n)) = b(x - \varphi(\beta_1)) \cdots (x - \varphi(\beta_n)).$$

Then we now have two factorizations of $f(x)$ into linear factors in $\overline{F}[x]$, given by

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n) = b(x - \varphi(\beta_1)) \cdots (x - \varphi(\beta_n)).$$

Since $\overline{F}[x]$ is a UFD then, up to reordering, $\alpha_j = \varphi(\beta_j)$ for $j = 1, \ldots, n$. That is, every root of $f(x)$ in $\overline{F}$ is an element of $\varphi(K)$. Since this is true for all polynomials in A, then we must have $S \subseteq \varphi(K)$. And since $F = \varphi(F) \subseteq \varphi(K)$, then we must have $F(S) \subseteq \varphi(K)$. Since K is a splitting field for A over F, then so is $\varphi(A)$. And since $F(S)$ is also a splitting field for A over F, then in fact $F(S) = \varphi(K)$. Hence, $\varphi : K \to F(S)$ is an isomorphism which is the identity on F.

$\square$

Q4 Let F be a field of characteristic p. Show that if K/F is a finite inseparable field extension, then $p \mid [K : F]$.

Proof. Since K/F inseparable, then there exists some element $\alpha \in K$ such that $m_{\alpha,F}(x)$ is inseparable, so $\deg m_{\alpha,F}(x) \geq 2$ and $\gcd(m_{\alpha,F}(x), m'_{\alpha,F}(x)) \neq 1$. Since $m_{\alpha,F}(x)$ is irreducible, this means that $m_{\alpha,F}(x)$ divides $m'_{\alpha,F}(x)$. But the degree of $m_{\alpha,F}(x)$ is strictly greater than the degree of its derivative, and the only polynomial multiple of $m_{\alpha,F}(x)$ with a lesser degree is 0. Therefore, $m'_{\alpha,F}(x) = 0$. Suppose

$$m_{\alpha,F}(x) = x^n + \sum_{j=0}^{n-1} a_j x^j$$

where $n = \deg m_{\alpha,F}(x)$, then

$$m'_{\alpha,F}(x) = nx^{n-1} + \sum_{j=1}^{n-1} j a_j x^{j-1}.$$

But $\deg m_{\alpha,F}(x) \geq 2$ and $\deg m'_{\alpha,F}(x) = 0$. so we must have $n = 0$ in F, which means that n is an integer multiple of p. Therefore,

$$[K : F] = [K : F(\alpha)][F(\alpha) : F] = [K : F(\alpha)] \cdot n$$

is an integer multiple of p, i.e., $p \mid [K : F]$.

$\square$