Q1 Let K/F be a field extension. Show that if $\alpha \in K$ is a root of $f(x) \in F[x]$ and $\deg f(x) = [F(\alpha) : F]$, then $f(x)$ is irreducible in $F[x]$.

Proof. By assumption $f(x) \in F[x]$ and $f(\alpha) = 0$, so α is algebraic over F. Then consider the minimal polynomial $m_{\alpha,F}(x) \in F[x]$. We know that $m_{\alpha,F}(x) \mid f(x)$ and

$$\deg f(x) = [F(\alpha) : F] = \deg m_{\alpha,F}(x).$$

Therefore, there is some $a \in F^\times$ such that $am_{\alpha,F}(x) = f(x)$. Since the minimal polynomial of α is irreducible and $f(x)$ is associate to that minimal polynomial, we conclude that $f(x)$ must be irreducible.

□

Lemma 1. If K/F is a field extension and $\alpha \in K, \alpha \notin F$ with $\alpha^2 \in F$, then $[F(\alpha) : F] = 2$.

Proof. Note that $x^2 - \alpha^2 \in F[x]$ and has α as a root, so α is algebraic over F. Then there is some minimal polynomial $m_{\alpha,F}(x) \in F[x]$, with $[F(\alpha) : F] = \deg m_{\alpha,F}(x) \leq 2$. If the degree of the minimal polynomial were 1, then we would have $m_{\alpha,F}(x) = x - \alpha$, but this is not a polynomial in $F[x]$. So in fact $[F(\alpha) : F] = \deg m_{\alpha,F}(x) = 2$.

□

Q2 Problem 13.2.13 Suppose $F = \mathbb{Q}(\alpha_1, \alpha_1, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $i = 1, 2, \ldots, n$. Prove that $\sqrt[3]{2} \notin F$.

Proof. Let $F_n = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. If $F_n = \mathbb{Q}$, then clearly $\sqrt[3]{2} \notin F_n$. We will first prove, by induction on n, that $[F_n : \mathbb{Q}]$ is a power of 2. Without loss of generality, assume $\alpha_1 \notin \mathbb{Q}$ (as, otherwise, $F_1 = \mathbb{Q}$), then Lemma 1 gives us the base case of $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 2$. Now assume $[F_{n-1} : \mathbb{Q}] = 2^k$ with $k \geq 0$. If $\alpha_n \in F_{n-1}$, then $F_n = F_{n-1}$ and the result holds, trivially. On the other hand, if $\alpha_n \notin F_{n-1}$ then by Lemma 1, $[F_n : F_{n-1}] = 2$, so

$$[F_n : \mathbb{Q}] = [F_n : F_{n-1}][F_{n-1} : \mathbb{Q}] = 2 \cdot 2^k = 2^{k+1}.$$

Returning to the notation $F = F_n$, we conclude that $[F : \mathbb{Q}]$ is a power of 2.

We now consider the polynomial $x^3 - 2 \in \mathbb{Q}[x]$. By Eisenstein's criterion for $\mathbb{Z}[x]$, this polynomial is irreducible in $\mathbb{Q}[x]$. Since it is also monic and has $\sqrt[3]{2}$ as a root, then it is the minimal polynomial for $\sqrt[3]{2}$ over $\mathbb{Q}$. Therefore,

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg m_{\sqrt[3]{2},\mathbb{Q}}(x) = 3.$$

Suppose for contradiction that $\sqrt[3]{2} \in F$. Then $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of F, giving us

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[3]{2})] \cdot 3.$$

However, this contradicts the fact that $[F : \mathbb{Q}]$ is a power of 2, therefore $\sqrt[3]{2} \notin F$.

□

Q3 Problem 13.2.16 Let K/F be an algebraic extension and let R be a ring contained in K and containing F. Show that R is a subfield of K containing F.

Proof. Since R is a subring of K, it suffices to show that R is closed under taking inverses. Let $r \in R \subseteq K$ be nonzero, so r is algebraic over F. Then r has a minimal polynomial $m_{r,F}(x) \in F[x] \subseteq R[x]$. In particular, take

$$m_{r,F}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, \ldots, a_{n-1} \in F \subseteq R$. Note that we must have $a_0 \neq 0$, otherwise

$$m_{r,F}(r) = r(r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_2 r + a_1) = -a_0 = 0.$$

But $r \neq 0$ and R is an integral domain, implying that the polynomial

$$x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_2 x + a_1 \in F[x]$$

would have r as a root, but not have $m_{r,F}(x)$ as a factor. Hence, $a_0 \neq 0$ so

$$r(r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_2 r + a_1)(-a_0^{-1}) = 1.$$

Since $a_0 \in F$, then $a_0^{-1} \in F \subseteq R$. Thus,

$$r^{-1} = (r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_2 r + a_1)(-a_0^{-1}) \in R,$$

so R is a subfield of K.

□

Q4 Problem 13.4.1 Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.

The roots of $x^4 - 2$ in $\mathbb{C}$ are $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. Both $\sqrt[4]{2}$ and $i\sqrt[4]{2}$ must be in the splitting field, implying that

$$(\sqrt[4]{2})^{-1} \cdot i\sqrt[4]{2} = i$$

is in the splitting field. Since $\sqrt[4]{2}$ and i generate all four roots, the splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$. Since $x^4 - 2$ is irreducible in $\mathbb{Q}[x]$ (by Eisenstein's criterion for $\mathbb{Z}[x]$) and has $\sqrt[4]{2}$ as a root, then it is the minimal polynomial for $\sqrt[4]{2}$ over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.

The minimal polynomial for i over $\mathbb{Q}$ is $x^2 + 1$, and we claim it to be the same over $\mathbb{Q}(\sqrt[4]{2})$. Note that $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, so for all $a \in \mathbb{Q}(\sqrt[4]{2})$, we have $a^2 \geq 0$. Thus, $x^1 + 1$ has no roots in $\mathbb{Q}(\sqrt[4]{2})$, so it is irreducible in $(\mathbb{Q}(\sqrt[4]{2}))[x]$. Hence,

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Q5 Show that $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ is a splitting field of $x^{12} - 1 \in \mathbb{Q}[x]$ and $[\mathbb{Q}(\sqrt{3}, \sqrt{-1}) : \mathbb{Q}] = 4$.

Factoring the polynomial in $\mathbb{C}$, we find

$$x^{12} - 1 = \prod_{k=0}^{11} (x - e^{\pi i k/6}).$$

The roots are evenly spaced on unit circle, separated by an angle of $\pi/6$. The real and imaginary components of the roots are $0, \pm 1/2, \pm\sqrt{3}, \pm 1$. In particular, the splitting field contains $\sqrt{3}$ and i and all the of roots. Moreover, all the roots can be obtained through field operations on $\mathbb{Q}$ with $\sqrt{3}$ and i. Hence, the splitting field is precisely $\mathbb{Q}(\sqrt{3}, i)$.

The minimal polynomial for $\sqrt{3}$ over $\mathbb{Q}$ is $x^2 - 3$, and the minimal polynomial for i over $\mathbb{Q}(\sqrt{3})$ is $x^2 + 1$ (by the same argument as in Q4). Therefore,

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$