Q1 Problem 13.1.1 Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.

Since $p(x) \in \mathbb{Z}[x]$ is monic with $3 \mid 9$ and $3 \mid 6$, but $3^2 = 9 \nmid 6$, Eisenstein's Criterion for $\mathbb{Z}[x]$ tells us that $p(x)$ is irreducible in $\mathbb{Q}[x]$. Applying the Euclidean algorithm to $p(x)$ and $x + 1$, we find

$$p(x) = x^3 + 9x + 6 = (x + 1)(x^2 - x + 10) - 4.$$

Then in $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(p(x))$, we have $p(\theta) = 0$, so

$$0 = (\theta + 1)(\theta^2 - \theta + 10) - 4.$$

Hence, $(1 + \theta)^{-1} = (\theta^2 - \theta + 10)/4$.

Q2 Problem 13.2.7 Prove that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ [one is obvious, for the other consider $(\sqrt{2} + \sqrt{3})^2$, etc.]. Conclude that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2} + \sqrt{3}$.

Clearly, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. To show the opposite inclusion, it suffices to show that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Let $a = \sqrt{2} + \sqrt{3}$, then

$$\begin{aligned}
\frac{1}{2}(a^2 - 5)a - 2a &= \frac{1}{2}(2 + 2\sqrt{2}\sqrt{3} + 3 - 5)a - 2a \\
&= \sqrt{2}\sqrt{3}(\sqrt{2} + \sqrt{3}) - 2a \\
&= 2\sqrt{3} + 3\sqrt{2} - 2\sqrt{2} - 2\sqrt{3} \\
&= \sqrt{2}.
\end{aligned}$$

Hence, $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, which also gives us $\sqrt{3} = a - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Therefore, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

We now have that

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3}),$$

so

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

The degree of $\sqrt{3}$ in the field $\mathbb{Q}(\sqrt{2})$ is the degree of a minimal polynomial of $\sqrt{3}$ in the same field. We will show that $x^2 - 3$ is a minimal polynomial for $\sqrt{3}$. Since $x^2 - 3$ is monic and has $\sqrt{3}$ as a root, then it remains to show that it is irreducible in $\mathbb{Q}(\sqrt{2})$. Since its degree is 2, then it is irreducible in $\mathbb{Q}(\sqrt{2})$ if and only if it has a root in $\mathbb{Q}(\sqrt{2})$. Suppose for contradiction that $a + b\sqrt{2}$ is such a root, i.e., $a, b \in \mathbb{Q}$. Then

$$3 = (a + b\sqrt{2})^2 = a^2 + 2ab\sqrt{2} + 2b^2.$$

If $a = 0$, then $\sqrt{3} = b\sqrt{2}$. In which case we would have $\sqrt{6} = 2b$, implying that $\sqrt{6}$ is rational, which is not the case. If $b = 0$, then $\sqrt{3} = a$ is a rational number, which is also not the case. So both a and b are nonzero, implying that

$$\frac{3 - a^2 - 2b^2}{2ab} = \sqrt{2}$$

is a rational number, which is not the case. Therefore, $x^2 - 3$ has no roots, and is therefore irreducible, in $\mathbb{Q}(\sqrt{2})$. Hence,

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

We know that such a polynomial in $\mathbb{Q}[x]$ must be of degree 4, so we consider

$$(\sqrt{2} + \sqrt{3})^4 = 49 + 20\sqrt{6}.$$

Also knowing that $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, then we see that

$$(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 = -1.$$

So the polynomial $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ is monic, irreducible, and has $\sqrt{2} + \sqrt{3}$ as a root.

Q3 Let K/F be a field extension and $\alpha_1, \dots, \alpha_n \in K$. Show that

$$F(\alpha_1, \dots, \alpha_n) = (F(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n).$$

(The LHS is the subfield generated by $\alpha_1, \dots, \alpha_n$ over F. The RHS is the subfield generated by α_n over the field $F(\alpha_1, \dots, \alpha_{n-1})$.

Proof. By definition, $F(S)$ is the intersection of all subfields of K containing $F \cup S$. So

$$F \cup \{\alpha_1, \dots, \alpha_{n-1}\} \subseteq F(\alpha_1, \dots, \alpha_{n-1}) \subseteq (F(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n).$$

And since $\alpha_n \in (F(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n)$, we conclude that

$$F \cup \{\alpha_1, \dots, \alpha_n\} \subseteq (F(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n).$$

And since $(F(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n)$ is a subfield of K, then this tells us that

$$F(\alpha_1, \dots, \alpha_n) \subseteq (F(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n).$$

Now since $F(\alpha_1, \dots, \alpha_n)$ is a subfield of K containing F and the elements $\alpha_1, \dots, \alpha_{n-1}$, then we have the inclusion

$$F(\alpha_1, \dots, \alpha_{n-1}) \subseteq F(\alpha_1, \dots, \alpha_n).$$

And since $F(\alpha_1, \dots, \alpha_n)$ also contains α_n, then in fact

$$(F(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n) \subseteq F(\alpha_1, \dots, \alpha_n),$$

giving us equality. $\square$

Q4 Let K/F be a field extension and $\alpha, \beta \in K$. Suppose that $[F(\alpha) : F]$ and $[F(\beta) : F]$ are both finite.

(a) Show that $[F(\alpha) : F] \geq [F(\alpha, \beta) : F(\beta)]$.

Proof. Since $[F(\alpha) : F] < \infty$, then α is algebraic over F and a minimal polynomial $m_{\alpha,F}(x) \in F[x]$. Since $F \subseteq F(\beta)$, then we also have $m_{\alpha,F}(x) \in (F(\beta))[x]$, so $m_{\alpha,F(\beta)}(x) \mid m_{\alpha,F}(x)$, giving us

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

□

(b) Show that $[F(\alpha, \beta) : F] \leq [F(\alpha) : F][F(\beta) : F]$, and the equality holds if $[F(\alpha) : F]$ and $[F(\beta) : F]$ are coprime.

Proof. Since the result of (a) holds for both α and β and the degree of a field extension is always at least 1, then we have

$$[F(\alpha, \beta) : F] \leq [F(\alpha) : F][F(\beta) : F].$$

Suppose $n = [F(\alpha) : F]$ and $m = [F(\beta) : F]$ are coprime. Then since $F(\alpha, \beta)/F$ is a finite extension and $F(\alpha)$ and $F(\beta)$ are subfields, then both n and m divide $k = [F(\alpha, \beta) : F]$. And since they are coprime, $nm \mid k$. And since $k \leq nm$, then we must have $k = nm$.

□

(c) Given $\alpha_1, \ldots, \alpha_n \in K$ with $[F(\alpha_j) : F]$, $1 \leq j \leq n$, all finite, show that

$$[F(\alpha_1, \ldots, \alpha_n) : F] \leq [F(\alpha_1) : F][F(\alpha_2) : F] \cdots [F(\alpha_n) : F].$$

Proof. For induction on n, (b) gives us the base case. Now suppose the inequality holds for $n - 1$. We first see that

$$[(F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})] \leq [F(\alpha_n) : F],$$

since the minimal polynomial of α_n in F is also a polynomial in $F(\alpha_1, \ldots, \alpha_{n-1})$ with α_n as a root. Hence, the minimal polynomial of α_n in the latter field must have degree at most $[F(\alpha_n) : F]$, which is to say that the above inequality holds. With this and the inductive hypothesis, we find

$$\begin{aligned}
[F(\alpha_1, \ldots, \alpha_n) : F] &= [(F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : F] \\
&= [F(\alpha_1, \ldots, \alpha_{n-1}) : F][(F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})] \\
&\leq [F(\alpha_1) : F] \cdots [F(\alpha_{n-1}) : F][F(\alpha_n) : F].
\end{aligned}$$

□