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

**Solution.** Irreducibility follows from Eisenstein’s criterion with \( p = 3 \). To evaluate \( 1/(1 + \theta) \), note that we must have \( 1/(1 + \theta) = a + b\theta + c\theta^2 \) for some \( a, b, c \in \mathbb{Q} \). Multiplying this out, we find that

\[
a + (a + b)\theta + (b + c)\theta^2 + c\theta^3 = 1,
\]

but we also have \( \theta^3 = -9\theta - 6 \), so this simplifies to

\[
(a - 6c) + (a + b - 9c)\theta + (b + c)\theta^2 = 1.
\]

Solving for \( a, b, c \) gives \( a = 5/2, b = -1/4, \) and \( c = 1/4 \). Thus

\[
\frac{1}{1 + \theta} = \frac{5}{2} - \frac{\theta}{4} + \frac{\theta^2}{4}.
\]

Problem (13.1.2). Show that \( x^3 - 2x - 2 \) is irreducible over \( \mathbb{Q} \) and let \( \theta \) be a root. Compute \( (1 + \theta)(1 + \theta + \theta^2) \) and \( \frac{1 + \theta}{1 + \theta + \theta^2} \) in \( \mathbb{Q}(\theta) \).

**Solution.** This polynomial is irreducible by Eisenstein with \( p = 2 \). We perform the multiplication and division just as in the previous problem to get

\[
(1 + \theta)(1 + \theta + \theta^2) = 3 + 4\theta + 2\theta^2
\]

and

\[
\frac{1 + \theta}{1 + \theta + \theta^2} = \frac{1}{3} + \frac{2\theta}{3} - \frac{\theta^2}{3}.
\]

Problem (13.1.3). Show that \( x^3 + x + 1 \) is irreducible over \( \mathbb{F}_2 \) and let \( \theta \) be a root. Compute the powers of \( \theta \) in \( \mathbb{F}_2(\theta) \).

**Solution.** If a cubic polynomial factors, then one of its factors must be linear. Hence, to check that \( x^3 + x + 1 \) is irreducible over \( \mathbb{F}_2 \), it suffices to show that it has no roots in \( \mathbb{F}_2 \). Since \( \mathbb{F}_2 = \{0, 1\} \) has only two elements, it is easy to check that this polynomial
has no roots. Hence it’s irreducible. For the powers, we have

\[
\begin{align*}
\theta^0 &= 1, \\
\theta^1 &= \theta, \\
\theta^2 &= \theta^2, \\
\theta^3 &= \theta + 1, \\
\theta^4 &= \theta^2 + \theta, \\
\theta^5 &= \theta^2 + \theta + 1, \\
\theta^6 &= \theta^2 + 1, \\
\theta^7 &= 1.
\end{align*}
\]

**Problem (13.1.7).** Prove that \(x^3 - nx + 2\) is irreducible for \(n \neq -1, 3, 5\).

**Solution.** If this polynomial is reducible, it must have a linear factor. By the rational root theorem, its linear factor must be of the form \((x - a)\), where \(a \in \{\pm 1, \pm 2\}\). So, we just check these four possibilities to find out which values of \(n\) give us linear factors. If \(a = -1\), then the polynomial has a root at \(a\) if and only if \(n = -1\). If \(a = 1\) or \(-2\), then the polynomial has a root at \(a\) if and only if \(n = 3\). If \(a = 2\), then the polynomial has a root at \(a\) if and only if \(n = 5\). Hence, \(x^3 - nx + 2\) is irreducible for all other values of \(n\).

**Problem (13.2.1).** Let \(\mathbb{F}\) be a finite field of characteristic \(p\). Prove that \(|\mathbb{F}| = p^n\) for some positive integer \(n\).

**Solution.** Suppose \(|\mathbb{F}|\) were divisible by some other prime \(q\). By Cauchy’s theorem, there would be a subgroup of the additive group of \(\mathbb{F}\) of order \(q\). In particular, there would be some element \(x\) of (exact) additive order \(q\), so \(qx = 0\). But \(px = (1 + \cdots + 1)x = 0x = 0\) (where there are \(p\) 1’s in the parentheses). So, \(px = qx = 0\), so \(0 = \gcd(p, q)x = x\), which contradicts the claim that \(x\) had order \(q\). Hence \(|\mathbb{F}|\) is a power of \(p\).

**Problem (13.2.2).** Let \(g(x) = x^2 + x - 1\) and let \(h(x) = x^3 - x + 1\). Obtain fields of 4, 8, 9, and 27 elements by adjoining a root of \(f(x)\) to the field \(F\) where \(f(x) = g(x)\) or \(h(x)\) and \(F = \mathbb{F}_2\) or \(\mathbb{F}_3\). Write down the multiplication tables for the fields with 4 and 9 elements and show that the nonzero elements form a cyclic group.

**Solution.** We note that \(g\) and \(h\) are both irreducible over \(\mathbb{F}_2\) and \(\mathbb{F}_3\). Hence \(\mathbb{F}_2[x]/(g(x))\) is a field with 4 elements, \(\mathbb{F}_2[x]/(h(x))\) is a field with 8 elements, \(\mathbb{F}_3[x]/(g(x))\) is a field with 9 elements, and \(\mathbb{F}_3[x]/(h(x))\) is a field with 27 elements. For the multiplication tables, we have
for $\mathbb{F}_4$ and

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>x</th>
<th>x + 1</th>
<th>x + 2</th>
<th>2x</th>
<th>2x + 1</th>
<th>2x + 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>x</td>
<td>x + 1</td>
<td>x + 2</td>
<td>2x</td>
<td>2x + 1</td>
<td>2x + 2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>x</td>
<td>2x</td>
<td>2x + 2</td>
<td>2x + 1</td>
<td>x</td>
<td>x + 2</td>
</tr>
<tr>
<td>x</td>
<td>0</td>
<td>2</td>
<td>x</td>
<td>x + 1</td>
<td>x + 1</td>
<td>x + 2</td>
<td>2x</td>
<td>2x + 1</td>
<td>2x + 2</td>
</tr>
<tr>
<td>x + 1</td>
<td>0</td>
<td>x + 1</td>
<td>2x + 2</td>
<td>1</td>
<td>x + 2</td>
<td>2x</td>
<td>2</td>
<td>x</td>
<td>2x + 1</td>
</tr>
<tr>
<td>x + 2</td>
<td>0</td>
<td>x + 2</td>
<td>2x + 1</td>
<td>x + 1</td>
<td>2x</td>
<td>2</td>
<td>2x + 2</td>
<td>1</td>
<td>x</td>
</tr>
<tr>
<td>2x</td>
<td>0</td>
<td>2x</td>
<td>x</td>
<td>x + 2</td>
<td>2</td>
<td>2x + 2</td>
<td>2x + 1</td>
<td>x + 1</td>
<td>1</td>
</tr>
<tr>
<td>2x + 1</td>
<td>0</td>
<td>2x + 1</td>
<td>x + 2</td>
<td>2x + 2</td>
<td>x</td>
<td>1</td>
<td>x + 1</td>
<td>2</td>
<td>2x</td>
</tr>
<tr>
<td>2x + 2</td>
<td>0</td>
<td>2x + 2</td>
<td>x + 1</td>
<td>2</td>
<td>2x + 1</td>
<td>x</td>
<td>1</td>
<td>2x</td>
<td>x + 2</td>
</tr>
</tbody>
</table>

for $\mathbb{F}_9$. These groups are cyclic, generated by $x$ in each case. (More generally, any finite subgroup of the multiplicative group of any field is always cyclic.)

**Problem (13.2.10).** Determine the degree of the extension $\sqrt{3 + 2\sqrt{2}}$ over $\mathbb{Q}$.

**Solution.** Since $(1 + \sqrt{2})^2 = 3 + 2\sqrt{2}$, we have

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

which has degree 2 over $\mathbb{Q}$.

**Problem (13.2.11).** (a) Let $\sqrt{3 + 4i}$ denote the square root of the complex number $3 + 4i$ that lies in the first quadrant and let $\sqrt{3 - 4i}$ denote the square root of $3 - 4i$ that lies in the fourth quadrant. Prove that $[\mathbb{Q}(\sqrt{3+4i} + \sqrt{3-4i}) : \mathbb{Q}] = 1$.

(b) Determine the degree of the extension $\mathbb{Q}(\sqrt{1 + \sqrt{-3} + \sqrt{1 - \sqrt{-3}}})$ over $\mathbb{Q}$.

**Solution.** (a) Since $\sqrt{3 + 4i} = 1 + 2i$ and $\sqrt{3 - 4i} = 1 - 2i$, we have

$$\sqrt{3 + 4i} + \sqrt{3 - 4i} = (1 + 2i) + (1 - 2i) = 2 \in \mathbb{Q}.$$

Hence the extension in question has degree 1.

(b) We have

$$\left(\sqrt{1 + \sqrt{-3} + \sqrt{1 - \sqrt{-3}}}\right)^2 = 6.$$

Hence, the extension in question is just $\mathbb{Q}(\sqrt{6})/\mathbb{Q}$, which has degree 2.

**Problem (13.2.14).** Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.
**Solution.** Since $\alpha$ is clearly a root of the quadratic equation $X^2 - \alpha^2$ in $F(\alpha^2)$, we must have $[F(\alpha) : F(\alpha^2)] = 1$ or $2$. But it can’t be 2, since if it were, we would have

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)] [F(\alpha^2) : F],$$

and the first degree on the right is even, so the degree on the left would also be even. This would contradict the hypothesis that $[F(\alpha) : F]$ is odd. Hence $[F(\alpha) : F(\alpha^2)] = 1$, meaning that $F(\alpha) = F(\alpha^2)$. (There’s another way to do this problem more explicitly, in terms of the minimal polynomial for $\alpha$.)

**Problem (13.2.17).** Let $f(x)$ be an irreducible polynomial of degree $n$ over a field $F$. Let $g(x)$ be any polynomial in $F[x]$. Prove that every irreducible factor of the composite polynomial $f(g(x))$ has degree divisible by $n$.

**Solution.** Let $\alpha$ be a root of $f(g(x))$, and let $L = F(\alpha)$. Then $g(\alpha)$ is a root of $F$. Let $K = F(g(\alpha))$. Hence $K$ is a root field of $f$ over $F$. We have

$$[L : F] = [L : K][K : F] = n[L : K],$$

so $n \mid [L : F]$. But $[L : F]$ is the degree of the minimal polynomial of $\alpha$. Since $\alpha$ was arbitrary, each factor of $f(g(x))$ has degree divisible by $n$. 