Exercise 1 (DF 9.2: 5)**.** *Exhibit all the ideals in the ring $F[x]/(p(x))$, where F is a field and $p(x) \in F[x]$ (describe them in terms of the factorization of $p(x)$).*

By the fourth isomorphism theorem for rings, a subring A of $F[x]$ containing $(p(x))$ is an ideal of $F[x]$ if and only if $A/(p(x))$ is an ideal of $F[x]/(p(x))$. Thus this problem reduces to describing the ideals of $F[x]$.

Since F is a field, $F[x]$ is a unique factorization domain and a principal ideal domain. Then we can write $p(x)$ as

$$p(x) = \prod_{i=1}^{m} p_i(x)$$

for some m, and we can generate any ideal of $F[x]$ with a single polynomial. Now $(p(x)) \subset (q(x))$ if and only if $q(x)$ divides $p(x)$, so all ideals of $F[x]$ containing $(p(x))$ can be generated the factors of $p(x)$. Thus the ideals of $F[x]$ are of the form $(p_{i_1} \cdots p_{i_k})$ for $k \leq m$, and the ideals of $F[x]/(p(x))$ are of the form

$$(p_{i_1} \cdots p_{i_k})/(p(x)).$$

Exercise 2 (DF 9.4: 1)**.** *Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles.*

a. $x^2 + x + 1$ *in* $\mathbb{F}_2[x]$.

b. $x^3 + x + 1$ *in* $\mathbb{F}_3[x]$.

c. $x^4 + 1$ *in* $\mathbb{F}_5[x]$.

d. $x^4 + 10x^2 + 1$ *in* $\mathbb{Z}[x]$.

a. Since this polynomial is degree 2, its reducibility coincides with the existence of roots in $\mathbb{F}_2$. Since the polynomial is nonzero when evaluated at both 0 and 1, it is irreducible.

b. This polynomial has the root $1 \in \mathbb{F}_3$, so we can write it as $x^3 + x + 1 = (x - 1)(x^2 + x + 2)$. Then since $x^2 + x + 2$ has no roots in $\mathbb{F}_3$, we have expressed the original polynomial in terms of irreducibles.

c. We can write this polynomial as $(2x^2 + 1)(3x^2 + 1)$. Neither of these quadratics have roots in $\mathbb{F}_5$, so they are both irreducible.

d. This polynomial is irreducible in $\mathbb{Q}[x]$ (and by extension in $\mathbb{Z}[x]$) by Eisenstein's criterion for $p = 2$.

Exercise 3 (DF 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 $\mathbb{Q}(\theta)$.*

The polynomial $p(x)$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion for the prime 3. We can use the fact that $\theta^3 + 9\theta + 6 = 0$ to calculate the inverse of $1+\theta$ in $\mathbb{Q}(\theta)$.

Any element in $\mathbb{Q}(\theta)$ can be written

$$a_0 + a_1\theta + a_2\theta^2,$$

for $a_i \in \mathbb{Q}$. We wish to find such an element of $\mathbb{Q}(\theta)$ such that it multiplies with $1+\theta$ to yield 1. We have

$$\begin{aligned} 1 &= (1+\theta)(a_0 + a_1\theta + a_2\theta^2) \\ 0 &= (a_0 - 1) + (a_0 + a_1)\theta + (a_1 + a_2)\theta^2 + a_2\theta^3. \end{aligned}$$

Since, as noted earlier, $\theta^3 = -9\theta - 6$, this becomes

$$0 = (a_0 - 6a_2 - 1) + (a_0 + a_1 - 9a_2)\theta + (a_1 + a_2)\theta^2.$$

This gives a system in $(a_0 - 6a_2 - 1)$, $(a_0 + a_1 - 9a_2)$, and $(a_1 + a_2)$ all equal 0. Solving the system yields

$$a_0 = \frac{5}{2}, \quad a_1 = -\frac{1}{4}, \quad \text{and } a_2 = \frac{1}{4}.$$

Thus the inverse of $1+\theta$ in $\mathbb{Q}(\theta)$ is

$$\frac{5}{2} - \frac{1}{4}\theta + \frac{1}{4}\theta^2.$$

Exercise 4 (DF 13.1: 3)**.** *Show that $x^3 + x + 1$ is ireducible over $\mathbb{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbb{F}_2(\theta)$.*

Let $p(x) = x^3 + x + 1$, then since $p(0)$ and $p(1)$ are both nonzero, $p(x)$ has no roots in $\mathbb{F}_2$, so it is irreducible in $\mathbb{F}_2[x]$. Since $p(x)$ has degree 3, the field $\mathbb{F}_2(\theta)$ has basis $\{1, \theta, \theta^2\}$. Thus we need only compute the powers of θ that are greater than 2.

- Since $p(\theta) = \theta^3 + \theta + 1 = 0$, we have $\theta^3 = -\theta - 1 = \theta + 1$.
- $\theta^4 = \theta^3\theta = \theta^2 + \theta$.
- $\theta^5 = \theta^4\theta = \theta^3 + \theta^2 = 1 + \theta + \theta^2$.
- $\theta^6 = \theta + \theta^2 + \theta^3 = 1 = \theta^2$.
- $\theta^7 = \theta + \theta^3 = 1$.

From here the pattern repeats.

Exercise 5 (DF 13.1: 7)**.** *Prove that $x^3 - nx + 2$ is irreducible for $n \neq -1, 3, 5$.*

Let $f_n(x) = x^3 - nx + 2$. If a rational root c/d of $f_n(x)$ exists, then it satisfies $c \mid a_0 = 2$ and $d \mid a_n = 1$. This means that the possible values of c and d are $c = \pm 1, \pm 2$ and $d = \pm 1$, so the possible rational roots are ± 1 and ± 2. Evaluating $f_n(x)$ at these points yields

$$\begin{aligned} f_n(1) &= 3 - n \\ f_n(-1) &= 1 + n \\ f_n(2) &= 2(5 - n) \\ f_n(-2) &= -2(3 - n). \end{aligned}$$

We are given that $n \neq -1, 3, 5$, however, so these quantities can never be 0. Thus $f_n(x)$ is irreducible over $\mathbb{Q}$.

Exercise 6 (DF 13.2: 1)**.** *Let $\mathbb{F}$ be a finite field of characteristic p. Prove that $|\mathbb{F}| = p^n$ for some positive integer n.*

We know that any field $\mathbb{F}$ is an extension of it prime subfield F, and since the character of $\mathbb{F}$ is p, F is isomorphic to $\mathbb{F}_p$. Since $\mathbb{F}$ is finite, there is some basis $\{\alpha_i\}_{i=1}^n$ for $\mathbb{F}$ as an $F-$ vector space. This means we can write all elements of $\mathbb{F}$ uniquely as

$$\sum_{i=1}^{n} f_i \alpha_i,$$

where $f_i \in F$. Since there are p different f_i, there are p^n different ways of assigning the f_i, so this means that $|\mathbb{F}| = p^n$.

Exercise 7 (DF 13.2: 3)**.** *Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$.*

The element $1 + i$ is a root of $x - 1 + i$, but this is not over $\mathbb{Q}$. We can remove the i by multiplying by the polynomial with the conjugate $1 - i$ as a root, which will give us a polynomial which is over $\mathbb{Q}$ instead of $\mathbb{C}$. We get

$$(x - (1 - i))(x - (1 + i)) = x^2 - 2x + 2,$$

which is over $\mathbb{Q}$ and contians $1 - i$ as a root. As it turns out, this is the exact polynomial we're looking for. By Eisenstein's criterion for $p = 2$, it is irreducible over $\mathbb{Q}$. Thus it is the minimal polynomial over $\mathbb{Q}$ for $1 + i$.

Exercise 8 (DF 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.*

Let $r \in R$ be nonzero, then r is necessarily in K, so it is algebraic over F. Then there exists a minimal polynomial $m_r(x) = \sum_{i=0}^{n} c_0 k^i$ over F with r as a root. Now c_0 must be nonzero, since otherwise we could factor out an x from it $m_r(x)$, meaning it wouldn't be irreducible. Since c_0 is nonzero and is an element of a field, it has an inverse c_0^{-1}. We can then use this inverse to calculate an inverse for r:

$$\begin{aligned} c_0 + c_1 r + \cdots + c_n r^n &= 0 \\ (-c_0^{-1})(c_0 + c_1 r + \cdots + c_n r^n) &= 0 \\ (-c_0^{-1})(c_1 r + \cdots + c_n r^n) &= 1 \\ r(-c_0^{-1})(c_1 + \cdots + c_n r^{n-1}) &= 1 \end{aligned}$$

Since we have found an inverse for an arbitrary nonzero element of R, it must be a field.

Exercise 9. *If $a_0, \ldots, a_n$ are distinct elements of a field F and $b_0, \ldots, b_n$ are any elements of F, then there is at most one polynomial $f \in F[x]$ with $\deg f \leq n$ such that $f(a_i) = b_i$ for $i = 0, 1, \ldots, n$.*

We will show this by contradiction. Suppose f and g are both polynomials of degree no greater than n satisfying $f(a_i) = g(a_i) = b_i$ for all i. Then $(f - g)(a_i) = 0$ for all i, meaning that it has $n+1$ roots; however, $f - g$ has degree no greater than n, so it can have no more than n roots if it is nonzero. Thus $f - g$ is actually the zero polynomial, so $f = g$, so we can have no more than 1 polynomial satisfying the given condition.

Exercise 10. *Construct a field of 27 elements.*

Let $p(x) = x^3+x^2+2$ be a polynomial over $\mathbb{F}_3$, then we claim that $F = \mathbb{F}_3/(p(x))$ is a field with 27 elements. The polynomial $p(x)$ is irreducible over $\mathbb{F}_3$ since it has no roots in $\mathbb{F}_3$, so the quotient F is a degree 3 field extension of $\mathbb{F}_3$. This means the elements of F can all be uniquely written in the form

$$f_1 + f_2\theta + f_3\theta^2,$$

where $f_i \in \mathbb{F}_3$ and θ is a root of $p(x)$. Since there are $3^3 = 27$ possible ways of assigning the f_i, there are 27 elements of F.