Chapter 5

Quotient Rings and Field Extensions

In this chapter we describe a method for producing field extension of a given field. If $F$ is a field, then a field extension is a field $K$ that contains $F$. For example, $\mathbb{C}$ is a field extension of $\mathbb{R}$ since $\mathbb{C}$ is a field containing $\mathbb{R}$. Similarly, $\mathbb{C}$ is a field extension of $\mathbb{Q}$. For coding theory we need field extensions of $\mathbb{Z}_2$. To produce a field extension of a field $F$ we will use a polynomial $f(x)$ with coefficients in $F$, and we will produce it by mimicing the idea of producing the integers modulo $n$ by starting with the integers and a fixed integer $n$. In order to do this we need to know that the arithmetic of polynomials is sufficiently similar to the arithmetic of integers. In the first section of this chapter we see that notions relating to divisibility work just as well for polynomials over a field as for the integers.

5.1 Arithmetic of Polynomial Rings

Let $F$ be a field, and let $F[x]$ be the ring of polynomials in the indeterminate $x$. High school students study the arithmetic of this ring without saying so in so many words, at least for the case $F = \mathbb{R}$. In this section we make a formal study of this arithmetic, seeing that much of what we did for integers above can be done in the ring $F[x]$. We start with the most basic definition.

Definition 5.1. Let $f$ and $g$ be polynomials in $F[x]$. Then we say that $f$ divides $g$, or $g$ is divisible by $f$, if there is a polynomial $h$ with $g = fh$.

The greatest common divisor of two integers $a$ and $b$ is the largest integer dividing both $a$ and $b$. This definition needs to be modified a little for polynomials. While we cannot talk about “largest” polynomial in the same manner as for integers, we can talk about the degree of a polynomial. Recall that the degree of a nonzero polynomial $f$ is the largest integer $m$ for which the coefficient of $x^m$ is nonzero. If $f(x) = a_nx^n + \cdots + a_1x + a_0$ with $a_n \neq 0$, then the degree of $f(x)$ is $n$. We write $\deg(f)$ for the degree of $f$. The degree function allows us to measure size of polynomials. However, there is one extra complication. For example, any polynomial of the form $ax^2$ with $a \neq 0$ divides $x^2$ and $x^3$. Thus, there isn’t a unique
polynomial of highest degree that divides a pair of polynomials. To pick one out, we consider monic polynomials, polynomials whose leading coefficient is 1. For example, $x^2$ is the monic polynomial of degree 2 that divides both $x^2$ and $x^3$, while $5x^2$ is not monic. As a piece of terminology, we will refer to an element $f \in F[x]$ as a polynomial over $F$.

**Definition 5.2.** Let $f$ and $g$ be polynomials over $F$, not both zero. Then a greatest common divisor of $f$ and $g$ is a monic polynomial of largest degree that divides both $f$ and $g$.

The problem with the definition above has to do with uniqueness. Could there be more than one greatest common divisor of a pair of polynomials? The answer is no, and we will prove this after we prove the analogue of the division algorithm.

The main reason for assuming that the coefficients of our polynomials lie in a field is to ensure that the division algorithm is valid. Before we prove it, we need a simple lemma to ensure that the division algorithm is valid. Before we prove it, we need a simple lemma about degrees. For convenience, we set $\deg(0) = -\infty$. We also make the convention that $-\infty + -\infty = -\infty$ and $-\infty + n = -\infty$ for any integer $n$. The point of these conventions is to make the statement in the following lemma and other results as simple as possible.

**Lemma 5.3.** Let $F$ be a field and let $f$ and $g$ be polynomials over $F$. Then $\deg(fg) = \deg(f) + \deg(g)$.

**Proof.** If either $f = 0$ or $g = 0$, then the equality $\deg(fg) = \deg(f) + \deg(g)$ is true by our convention above. So, suppose that $f \neq 0$ and $g \neq 0$. Write $f = a_nx^n + \cdots + a_0$ and $g = b_mx^m + \cdots + b_0$ with $a_n \neq 0$ and $b_m \neq 0$. Therefore, $\deg(f) = n$ and $\deg(g) = m$. The definition of polynomial multiplication yields

$$fg = (a_nb_m)x^{n+m} + (a_nb_{m-1} + a_{n-1}b_m)x^{n+m-1} + \cdots + a_0b_0.$$  

Now, since the coefficients come from a field, which has no zero divisors, we can conclude that $a_nb_m \neq 0$, and so $\deg(fg) = n + m = \deg(f) + \deg(g)$, as desired. $\square$

**Proposition 5.4 (Division Algorithm).** Let $F$ be a field and let $f$ and $g$ be polynomials over $F$ with $f$ nonzero. Then there are unique polynomials $q$ and $r$ with $g = qf + r$ with $\deg(r) < \deg(f)$.

**Proof.** Let

$$\mathcal{S} = \{ t \in F[x] : t = g - qf \text{ for some } q \in F[x]\}.$$  

Then $\mathcal{S}$ is a nonempty set of polynomials, since $g \in \mathcal{S}$. Thus, by the well ordering property of the integers, there is a polynomial $r$ of least degree in $\mathcal{S}$. By definition, there is a $q \in F[x]$ with $r = g - qf$, so $g = qf + r$. We need to see that $\deg(r) < \deg(f)$. If, on the other hand, $\deg(r) \geq \deg(f)$, say $n = \deg(f)$ and $m = \deg(r)$. If $f = a_nx^n + \cdots + a_0$ and $r = r_mx^m + \cdots + r_0$ with $a_n \neq 0$ and $r_m \neq 0$, then by thinking about the method of long division of polynomials, we realize that we may write $r = (r_m a_n^{-1})x^{m-n}f + r'$ with $\deg(r') < m = \deg(r)$. But then

$$g = qf + r = qf + (r_m a_n^{-1})x^{m-n}f + r' = (q + r_m a_n^{-1})x^{m-n}f + r',$$
which shows that $r' \in \mathcal{S}$. Since $\deg(r') < \deg(r)$, this would be a contradiction to the choice of $r$. Therefore, $\deg(r) \geq \deg(f)$ is false, so $\deg(r) < \deg(f)$, as we wanted to prove. This proves existence of $q$ and $r$. For uniqueness, suppose that $g = qf + r$ and $g = q'f + r'$ for some polynomials $q, q'$ and $r, r'$ in $F[x]$, and with $\deg(r), \deg(r') < \deg(f)$. Then $qf + r = q'f + r'$, so $(q - q')f = r' - r$. Taking degrees and using the lemma, we have

$$\deg(q' - q) + \deg(f) = \deg(r' - r).$$

Since $\deg(r) < \deg(f)$ and $\deg(r') < \deg(f)$, we have $\deg(r' - r) < \deg(f)$. However, if $\deg(q' - q) \geq 0$, this is a contradiction to the equation above. The only way for this to hold is for $\deg(q' - q) = \deg(r' - r) = -\infty$. Thus, $q' - q = 0 = r' - r$, so $q' = q$ and $r' = r$, proving uniqueness. 

We now prove the existence of greatest common divisors of polynomials, and also prove the representation theorem analogous to Proposition ??

**Proposition 5.5.** Let $F$ be a field and let $f$ and $g$ be polynomials over $F$, not both zero. Then $\gcd(f, g)$ exists and is unique. Furthermore, there are polynomials $h$ and $k$ with $\gcd(f, g) = hf + kg$.

**Proof.** We will prove this by proving the representation result. Let

$$\mathcal{S} = \{hf + kg : h, k \in F[x]\}.$$ 

Then $\mathcal{S}$ contains nonzero polynomials as $f = 1 \cdot f + 0 \cdot g$ and $g = 0 \cdot f + 1 \cdot g$ both lie in $\mathcal{S}$. Therefore, there is a nonzero polynomial $d \in \mathcal{S}$ of smallest degree by the well ordering principle. Write $d = hf + kg$ for some $h, k \in F[x]$. By dividing by the leading coefficient of $d$, we may assume that $d$ is monic without changing the condition $e \in \mathcal{S}$. We claim that $d = \gcd(f, g)$. To show that $e$ is a common divisor of $f$ and $g$, first consider $f$. By the division algorithm, we may write $f = qd + r$ for some polynomials $q$ and $r$, and with $\deg(r) < \deg(d)$. Then

$$r = f - qd = f - q(hf + kg) = (1 - qh)f + (-qk)g.$$ 

This shows $r \in \mathcal{S}$. If $r \neq 0$, this would be a contradiction to the choice of $d$ since $\deg(r) < \deg(d)$. Therefore, $r = 0$, which shows that $f = qd$, and so $d$ divides $f$. Similarly, $d$ divides $g$. Thus, $d$ is a common divisor of $f$ and $g$. If $e$ is any other common divisor of $f$ and $g$, then $e$ divides any combination of $f$ and $g$; in particular, $e$ divides $hf + kg = d$. This forces $\deg(e) \leq \deg(d)$ by Lemma 5.3. Thus, $d$ is the monic polynomial of largest degree that divides $f$ and $g$, so $d$ is a greatest common divisor of $f$ and $g$. This proves everything but uniqueness. For that, suppose that $d$ and $d'$ are both monic common divisors of $f$ and $g$ of largest degree. By the proof above, we may write both $d$ and $d'$ as combinations of $f$ and $g$. Also, from this, the argument above shows that $d$ divides $d'$ and vice-versa. If $d' = ad$
and \( \text{deg}(ab) = 0 \), which means that \( a \) and \( b \) are both constants. But, since \( d \) and \( d' \) are monic, for \( d' = ad \) to be monic, \( a = 1 \). Thus, \( d' = ad = d \).

### 5.2 Ideals and Quotient Rings

We will construct extension fields of a field \( F \) by starting with an ideal of the polynomial ring \( F[x] \) and constructing the associated quotient ring. We must therefore begin by defining ideals.

**Definition 5.6.** Let \( R \) be a ring. An ideal \( I \) is a nonempty subset of \( R \) such that (i) if \( a, b \in I \), then \( a + b \in I \), and (ii) if \( a \in I \) and \( r \in R \), then \( ar \in I \) and \( ra \in I \).

This definition says that an ideal is a subset of \( R \) closed under addition that satisfies a strengthened form of closure under multiplication. Not only is the product of two elements of \( I \) also in \( I \), but that the product of an element of \( I \) and any element of \( r \) is an element of \( I \).

**Example 5.7.** Let \( R = \mathbb{Z} \). If \( n \) is an integer, let \( n\mathbb{Z} \) be the set of all multiples of \( \mathbb{Z} \). That is,

\[ n\mathbb{Z} = \{na : a \in \mathbb{Z}\} \, . \]

To see that this set is an ideal, first consider addition. If \( x, y \in n\mathbb{Z} \), then there integers \( a \) and \( b \) with \( x = na \) and \( y = nb \). Then \( x + y = na + nb = n(a + b) \). Therefore, \( x + y \in n\mathbb{Z} \).

Second, for multiplication, let \( x = na \in n\mathbb{Z} \) and let \( r \in \mathbb{Z} \). Then \( rx = x(r) = r(na) = n(ra) \), a multiple of \( n \). Therefore, \( rx \in n\mathbb{Z} \). This proves that \( n\mathbb{Z} \) is an ideal. If \( n > 0 \), notice that

\[ n\mathbb{Z} = \{0, n, 2n, \ldots, -n, -2n, \ldots\} \]

is the same as the equivalence class of \( 0 \) under the relation congruence modulo \( n \). This is an important connection that we will revisit.

**Example 5.8.** Let \( R = F[x] \) be the ring of polynomials over a field, and let \( f \in F[x] \). Let

\[ I = \{gf : g \in F[x]\} \, , \]

the set of all multiples of \( f \). This set is an ideal of \( F[x] \) by the same calculation as in the previous example. However, we repeat this calculation. For closure under addition, let \( h, k \in I \). Then \( h = gf \) and \( k = g'f \) for some polynomials \( g \) and \( g' \). Then \( h + k = gf + g'f = (g + g')f \), a multiple of \( f \), so \( h + k \in I \). For multiplication, let \( h = gf \in I \), and let \( a \in F[x] \). Then \( ah = ha = agf = (ag)f \), a multiple of \( f \), so \( ah \in I \). Thus, \( I \) is an ideal of \( F[x] \). This ideal is typically denoted by \( (f) \).
Example 5.9. Let $R$ be any commutative ring, and let $a \in R$. Let
\[ aR = \{ ar : r \in R \}. \]

We can consider $aR$ to be the set of multiples of $a$. We show that $aR$ is an ideal of $R$. First, let $x, y \in aR$. Then $x = ar$ and $y = as$ for some $r, s \in R$. Then $x + y = ar + as = a(r + s)$, so $x + y \in aR$. Next, let $x = ar \in aR$ and let $z \in R$. Then $xz = arz = a(rz) \in aR$. Also, $zx = xz$ since $R$ is commutative, so $zx \in aR$. Therefore, $aR$ is an ideal of $R$. This construction generalizes the previous two examples. The ideal $aR$ is typically called the ideal generated by $a$. It is often written as $(a)$.

Example 5.10. Let $R$ be any commutative ring, and let $a, b \in R$. Set
\[ I = \{ ar + bs : r, s \in R \}. \]

To see that $I$ is an ideal of $R$, first let $x, y \in I$. Then $x = ar + bs$ and $y = ar' + bs'$ for some $r, s, r', s' \in R$. Then
\[
\begin{align*}
x + y &= (ar + bs) + (ar' + bs') \\
&= (ar + ar') + (bs + bs') \\
&= a(r + r') + b(s + s') \in I
\end{align*}
\]
by the associative and distributive properties. Next, let $x \in I$ and $z \in R$. Again, $x = ar + bs$ for some $r, s \in R$. Then
\[
\begin{align*}
xyz &= (ar + bs)z = (ar)z + (bs)z \\
&= a(rz) + b(sz).
\end{align*}
\]
This calculation shows that $xz \in I$. Again, since $R$ is commutative, $zx = xz$, so $zx \in I$. Thus, $I$ is an ideal of $R$. We can generalize this example to any finite number of elements of $R$: given $a_1, \ldots, a_n \in R$, if
\[ J = \{ a_1r_1 + \cdots + a_nr_n : r_i \in R \text{ for each } i \}, \]
then a similar argument will show that $J$ is an ideal of $R$. The ideal $J$ is typically referred to as the ideal generated by the elements $a_1, \ldots, a_n$, and it is often denoted by $(a_1, \ldots, a_n)$.

The division algorithm has a nice application to the structure of ideals of $\mathbb{Z}$ or of $F[x]$. We prove the result for polynomials, leaving the analogous result for $\mathbb{Z}$ to the reader.

Theorem 5.11. Let $F$ be a field. Then any ideal of $F[x]$ can be generated by a single polynomial. That is, if $I$ is an ideal of $F[x]$, then there is a polynomial $f$ with $I = (f) = \{ fg : g \in F[x] \}$. 


Proof. Let $I$ be an ideal of $F[x]$. If $I = \{0\}$, then $I = (0)$. So, suppose that $I$ is nonzero. Let $f \in I$ be a nonzero polynomial of least degree. We claim that $I = (f)$. To prove this, let $g \in I$. By the division algorithm, there are polynomials $q, r$ with $g = qf + r$ and $\deg(r) < \deg(f)$. Since $f \in I$, the product $qf \in I$, and thus $g - qf \in I$ as $g \in I$. We conclude that $r \in I$. However, the assumption on the degree of $f$ shows that the condition $\deg(r) < \deg(f)$ forces $r = 0$. Thus, $g = qf \in (f)$. This proves $I \subseteq (f)$. Since every multiple of $f$ is in $I$, the reverse inclusion $(f) \subseteq I$ is also true. Therefore, $I = (f)$. 

We can give an ideal theoretic description of greatest common divisors in $\mathbb{Z}$ and in $F[x]$. Suppose that $f$ and $g$ are polynomials over a field $F$. If $\gcd(f, g) = d$, then we have proved that $d = fh + gk$ for some polynomials $h, k$. Therefore, $d$ is an element of the ideal $I = \{fs + gt : s, t \in F[x]\}$. However, since $d$ divides $f$ and $g$, it follows that $d$ divides every element of $I$. Therefore, $I = (d)$ is simply the set of multiples of $d$. Therefore, one can identify the greatest common divisor of $f$ and $g$ by identifying a monic polynomial $d$ satisfying $I = (d)$.

We now use ideals to define quotient rings. In order to define them, we first need to specify what are their elements. These are cosets, which we now define. We have seen cosets when we discussed decoding with the Hamming code. These cosets arose from a subspace of a vector space. The idea here is essentially the same; the only difference is that we start with an ideal of a ring instead of a subspace of a vector space.

**Definition 5.12.** Let $R$ be a ring and let $I$ be an ideal of $R$. If $a \in R$, then the coset $a + I$ is defined as $a + I = \{a + x : x \in I\}$.

Recall the description of equivalence classes for the relation congruence modulo $n$. For example, if $n = 5$, then we have five equivalence classes, and they are

\[
\begin{align*}
\overline{0} & = \{0, 5, 10, \ldots, -5, -10, \ldots\}, \\
\overline{1} & = \{1, 6, 11, \ldots, -4, -9, -14, \ldots\}, \\
\overline{2} & = \{2, 7, 12, \ldots, -3, -8, -13, \ldots\}, \\
\overline{3} & = \{3, 8, 13, \ldots, -2, -7, -12, \ldots\}, \\
\overline{4} & = \{4, 9, 14, \ldots, -1, -6, -11, \ldots\}.
\end{align*}
\]

By the first example above, the set $5\mathbb{Z}$ of multiples of 5 forms an ideal of $\mathbb{Z}$. These five equivalence classes can be described as cosets, namely,

\[
\begin{align*}
\overline{0} & = 0 + 5\mathbb{Z}, \\
\overline{1} & = 1 + 5\mathbb{Z}, \\
\overline{2} & = 2 + 5\mathbb{Z}, \\
\overline{3} & = 3 + 5\mathbb{Z}, \\
\overline{4} & = 4 + 5\mathbb{Z}.
\end{align*}
\]
In general, for any integer \( a \), we have \( a + 5\mathbb{Z} = \overline{a} \). Thus, cosets for the ideal \( 5\mathbb{Z} \) are the same as equivalence classes modulo 5. In fact, more generally, if \( n \) is any positive integer, then the equivalence class \( \overline{a} \) of an integer \( a \) modulo \( n \) is the coset \( a + n\mathbb{Z} \) of the ideal \( n\mathbb{Z} \).

We have seen that an equivalence classes can have different names. Modulo 5, we have \( \overline{1} = \overline{6} \) and \( \overline{2} = \overline{-3} = \overline{22} \), for example. Similarly, cosets can be represented in different ways. If \( R = F[x] \) and \( I = x\mathbb{R} \), the ideal of multiples of the polynomial \( x \), then \( 0 + I = x + I = x^2 + I = 4x^{17} + I \). Also, \( 1 + I = (x + 1) + I \). For some terminology, we refer to \( a \) as a coset representative of \( a + I \). One important thing to remember is that the coset representative is not unique, as the examples above demonstrate.

When we defined operations on \( \mathbb{Z}_n \), we defined them with the formulas \( \overline{a} + \overline{b} = \overline{a+b} \) and \( \overline{a} \cdot \overline{b} = \overline{ab} \). Since these equivalence classes are the same thing as cosets for \( n\mathbb{Z} \), this leads us to consider a generalization. If we replace \( \mathbb{Z} \) by any ring and \( n\mathbb{Z} \) by any ideal, we can mimic these formulas to define operations on cosets. First, we give a name to the set of cosets.

**Definition 5.13.** If \( I \) is an ideal of a ring \( R \), let \( R/I \) denote the set of cosets of \( I \). In other words, \( R/I = \{a + I : a \in R\} \).

We now define operations on \( R/I \) in a manner like the operations on \( \mathbb{Z}_n \). We define

\[
(a + I) + (b + I) = (a + b) + I,
\]

\[
(a + I) \cdot (b + I) = (ab) + I.
\]

In other words, to add or multiply two cosets, first add or multiply their coset representatives, then take the corresponding coset. As with the operations on \( \mathbb{Z}_n \), we have to check that these formulas make sense. In other words, the name we give to a coset should not affect the value we get when adding or multiplying. We first need to know when two elements represent the same coset. To help with the proof, we point out two simple properties. If \( I \) is an ideal, then \( 0 \in I \). Furthermore, if \( r \in I \), then \( -r \in I \). The proofs of these facts are left as exercises.

**Lemma 5.14.** Let \( I \) be an ideal of a ring \( R \). If \( a, b \in R \), then \( a + I = b + I \) if and only if \( a - b \in I \).

**Proof.** Let \( a, b \in R \). First suppose that \( a + I = b + I \). From \( 0 \in I \) we get \( a = a + 0 \in a + I \), so \( a \in b + I \). Therefore, there is an \( x \in I \) with \( a = b + x \). Thus, \( a - b = x \in I \). Conversely, suppose that \( a - b \in I \). If we set \( x = a - b \), an element of \( I \), then \( a = b + x \). This shows \( a \in b + I \). So, for any \( y \in I \), we have \( a + y = b + (x + y) \in I \), as \( I \) is closed under addition. Therefore, \( a + I \subseteq b + I \). The reverse inclusion is similar; by using \( -x = b - a \), again an element of \( I \), we will get the inclusion \( b + I \subseteq a + I \), and so \( a + I = b + I \). \( \square \)

In fact, we can generalize the fact that equivalence classes modulo \( n \) are the same thing as cosets for \( n\mathbb{Z} \). Given an ideal, we can define an equivalence relation by mimicking congruence modulo \( n \). To phrase this relation in a new way, \( a \equiv b \mod n \) if and only if \( a - b \) is a multiple of \( n \), so \( a \equiv b \mod n \) if and only if \( a - b \in n\mathbb{Z} \). Thus, given an ideal \( I \) of a ring \( R \), we may
define a relation by \( x \equiv y \mod I \) if \( x - y \in I \). One can prove in the same manner as for congruence modulo \( n \) that this is an equivalence relation, and that, for any \( a \in R \), the coset \( a + I \) is the equivalence class of \( a \).

**Lemma 5.15.** Let \( I \) be an ideal of a ring \( R \). Let \( a, b, c, d \in R \).

1. If \( a + I = c + I \) and \( b + I = d + I \), then \( a + b + I = c + d + I \).
2. If \( a + I = c + I \) and \( b + I = d + I \), then \( ab + I = cd + I \).

**Proof.** Suppose that \( a, b, c, d \in R \) satisfy \( a + I = c + I \) and \( b + I = d + I \). To prove the first statement, by the lemma we have elements \( x, y \in I \) with \( a - c = x \) and \( b - d = y \). Then

\[
(a + b) - (c + d) = a + b - c - d \\
= (a - c) + (b - d) \\
= x + y \in I.
\]

Therefore, again by the lemma, \( (a + b) + I = (c + d) + I \). For the second statement, we rewrite the equations above as \( a = c + x \) and \( b = d + y \). Then

\[
ab = (c + x)(d + y) = c(d + y) + x(d + y) \\
= cd + (cx + xd + xy).
\]

Since \( x, y \in I \), the three elements \( cx, xd, xy \) are all elements of \( I \). Thus, the sum \( cx + xd + xy \in I \). This shows us that \( ab - cd \in I \), so the lemma yields \( ab + I = cd + I \).

The consequence of the lemma is exactly that our coset operations make sense. Thus, we can ask whether or not \( R/I \) is a ring. The answer is yes, and the proof is easy, and is exactly parallel to the proof for \( \mathbb{Z}_n \).

**Theorem 5.16.** Let \( I \) be an ideal of a ring \( R \). Then \( R/I \), together with the operations of coset addition and multiplication, forms a ring.

**Proof.** We have several properties to verify. Most follow immediately from the definition of the operations and from the ring properties of \( R \). For example, to prove that coset addition is commutative, we see that for any \( a, b \in R \), we have

\[
(a + I) + (b + I) = (a + b) + I \\
= (b + a) + I \\
= (b + I) + (a + I).
\]

This used exactly the definition of coset addition and commutativity of addition in \( R \). Most of the other ring properties hold for similar reasons, so we only verify those that are a little different. For existence of an additive identity, we have the additive identity 0 of \( R \), and it
is natural to guess that $0 + I$ is the identity for $R/I$. To see that this is indeed true, let $a + I \in R/I$. Then
\[(a + I) + (0 + I) = (a + 0) + I = a + I.\]
Thus, $0 + I$ is the additive identity for $R/I$. Similarly $1 + I$ is the multiplicative identity, since
\[(a + I) \cdot (1 + I) = (a \cdot 1) + I = a + I\]
and
\[(1 + I) \cdot (a + I) = (1 \cdot a) + I = a + I\]
for all $a + I \in R/I$. Finally, the additive inverse of $a + I$ is $-a + I$ since
\[(a + I) + (-a + I) = (a + (-a)) + I = 0 + I.\]
Therefore, $R/I$ is a ring.

The ring $R/I$ is called a quotient ring of $R$. This idea allows us to construct new rings from old rings. For example, the ring $\mathbb{Z}_n$ is really the same thing as the quotient ring $\mathbb{Z}/n\mathbb{Z}$, since we have identified the equivalence classes modulo $n$; that is, the elements of $\mathbb{Z}_n$, with the cosets of $n\mathbb{Z}$; i.e., the elements of $\mathbb{Z}/n\mathbb{Z}$. It is this construction applied to polynomial rings that we will use to build extension fields. We recall Proposition ?? above that says $\mathbb{Z}_n$ is a field if and only if $n$ is a prime. To generalize this result to polynomials, we first need to define the polynomial analogue of a prime number.

**Definition 5.17.** Let $F$ be a field. A nonconstant polynomial $f \in F[x]$ is said to be irreducible over $F$ if whenever $f$ can be factored as $f = gh$, then either $g$ or $h$ is a constant polynomial.

Before we give some examples, recall that a constant polynomial is simply a polynomial of degree 0; that is, it is a polynomial of the form $f(x) = a$ for some $a \in F$. Any such polynomial has degree 0 if it is not the zero polynomial.

**Example 5.18.** The terminology irreducible over $F$ in the definition above is used because irreducibility is a relative term. The polynomial $x^2 + 1$ factors over $\mathbb{C}$ as $x^2 + 1 = (x-i)(x+i)$. However, we show that $x^2 + 1$ is irreducible over $\mathbb{R}$. One way to do this would be to write $x^2 + 1 = (ax + b)(cx + d)$, and obtain a system of nonlinear equations in $a, b, c, d$, and show there is no solution to this system. However, we do it in an easier way, although one that uses a fact left as an exercise. Since $\deg(x^2 + 1) = 2$, if it factors over $\mathbb{R}$, then it must have a root in $\mathbb{R}$. However, $x^2 + 1$ clearly has no roots in $\mathbb{R}$. Thus, $x^2 + 1$ is irreducible over $\mathbb{R}$.

**Example 5.19.** The polynomial $x$ is irreducible. For, if we can factor $x = gh$, taking degrees of both sides gives $1 = \deg(g) + \deg(h)$. Thus, one of the degrees of $g$ and $h$ is 1 and the other is 0. The one with degree 0 is a constant polynomial. Thus, we cannot factor $x$ with both factors nonconstant. So, $x$ is irreducible. This argument shows that any polynomial of degree 1 is irreducible.
Example 5.20. Consider $x^2 + 1$ as a polynomial in $\mathbb{Z}_5[x]$. Unlike the case of $\mathbb{Q}[x]$, this polynomial does factor over $\mathbb{Z}_5$, since $x^2 + 1 = (x - 2)(x - 3)$ in $\mathbb{Z}_5[x]$. In particular, $x^2 + 1$ has two roots in $\mathbb{Z}_5$. However, for $F = \mathbb{Z}_3$, the polynomial $x^2 + 1$ is irreducible since $x^2 + 1$ has no roots in $\mathbb{Z}_3$; it is easy to see that none of the three elements 0, 1, and 2 are roots of $x^2 + 1$.

We now show that extension fields can be produced from irreducible polynomials.

**Proposition 5.21.** Let $F$ be a field, and let $f \in F[x]$ be a polynomial. If $I = (f)$ is the ideal generated by an irreducible polynomial $f$, then $F[x]/I$ is a field.

**Proof.** Let $F$ be a field, and let $f \in F[x]$ be irreducible. Set $I = (f)$. We wish to prove that $F[x]/I$ is a field. We know it is a commutative ring, so we only need to prove that every nonzero element has a multiplicative inverse. Let $g + I \in F[x]/I$ be nonzero. Then $g + I \neq 0 + I$, so $g \notin I$. This means $f$ does not divide $g$. Since $f$ is irreducible, we can conclude that $\gcd(f, g) = 1$. Thus, there are $h, k \in F[x]$ with $1 = hf + kg$. Because $hf \in I$, $kg - 1 \in I$, so $kg + I = 1 + I$. By the definition of coset multiplication, this yields $(k + I)(g + I) = 1 + I$. Therefore, $k + I$ is the multiplicative inverse of $g + I$. Because we have proved that an arbitrary nonzero element of $F[x]/I$ has a multiplicative inverse, this commutative ring is a field. \hfill $\square$

The converse of this result is also true; if $F[x]/(f)$ is a field, then $f$ is an irreducible polynomial. We leave the verification of this fact to an exercise.

To help work with these quotient rings, we see how the division algorithm can help us write elements of $F[x]/(f)$. Set $I = (f)$. Given $g \in F[x]$, by the division algorithm we may write $g = qf + r$ for some $g, r \in F[x]$ and with $\deg(r) < \deg(f)$. Then $g - r = qf \in I$, so $g + I = r + I$. This argument shows that any coset $g + I$ is equal to a coset $r + I$ for some polynomial $r$ with $\deg(r) < \deg(f)$. Thus, $F[x]/(f) = \{r + I : r \in F[x], \deg(r) < \deg(f)\}$. This result is the analogue of the description $\mathbb{Z}_n = \{\overline{a} : 0 \leq a < n\} = \{a + (n) : 0 \leq a < n\}$.

Example 5.22. Let $F = \mathbb{R}$, and consider the irreducible polynomial $f = x^2 + 1$. In this example we will relate the field $\mathbb{R}[x]/(x^2 + 1)$ to the field of complex numbers $\mathbb{C}$. As in the previous example, the division algorithm implies that every element of this quotient ring can be written in the form $a + bx + I$, where $I = (x^2 + 1)$. Addition in this ring is given by

$$(a + bx + I) + (c + dx + I) = (a + c) + (b + d)x + I.$$ 

For multiplication, we have

$$(a + bx + I)(c + dx + I) = (a + bx)(c + dx) + I$$

$$= ac + bdx^2 + (ad + bc)x + I$$

$$= (ac - bd) + (ad + bc)x + I;$$

the simplification in the last equation comes from the equation $bdx^2 + I = -bd + I$. Since $x^2 + 1 \in I$, we have $x^2 + I = -1 + I$, so multiplying both sides by $bd + I$ yields this equation.
If you look at these formulas for the operations in $\mathbb{R}[x]/(x^2 + 1)$, you may see a similarity between the operations on $\mathbb{C}$:

\[
(a + bi) + (c + di) = (a + c) + (b + d)i \\
(a + bi)(c + di) = (ac - bd) + (ad + bc)i.
\]

In fact, one can view this construction as a way of building the complex numbers from the real numbers and the polynomial $x^2 + 1$.

**Example 5.23.** Let $F = \mathbb{Z}_2$, and consider $f = x^2 + x + 1$. This is an irreducible over $\mathbb{Z}_2$ since it is quadratic and has no roots in $\mathbb{Z}_2$; the only elements of $\mathbb{Z}_2$ are 0 and 1, and neither is a root. Consider $K = \mathbb{Z}_2[x]/(x^2 + x + 1)$. This is a field by the previous proposition. We write out an addition and multiplication table for $K$ once we write down all elements of $K$.

First, by the comment above, any coset in $K$ can be represented by a polynomial of the form $ax + b$ with $a, b \in \mathbb{Z}_2$; this is because any remainder after division by $f$ must have degree less than $\deg(f) = 2$. So, $K = \{0 + I, 1 + I, x + I, 1 + x + I\}$.

Thus, $K$ is a field with 4 elements. The following tables then represent addition and multiplication in $K$.

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

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

If you look closely at these tables, you may see a resemblance between them and the tables of Example 5.22 above. In fact, if you label $x + I$ as $a$ and $1 + x + I$ as $b$, along with $0 = 0 + I$ and $1 = 1 + I$, the tables in both cases are identical. In fact, the tables of Example 5.22 were found by building $K$, and then labeling the elements as 0, 1, $a$, and $b$ in place of $0 + I$, $1 + I$, $x + I$, and $1 + x + I$.

**Example 5.24.** Let $f(x) = x^3 + x + 1$. Then this polynomial is irreducible over $\mathbb{Z}_2$. To see this, we first note that it has no roots in $\mathbb{Z}_2$ as $f(0) = f(1) = 1$. Since $\deg(f) = 3$, if it factored, then it would have a linear factor, and so a root in $\mathbb{Z}_2$. Since this does not happen, it is irreducible. We consider the field $K = \mathbb{Z}_2[x]/(x^3 + x + 1)$. We write $I = (x^3 + x + 1)$.
and set $\alpha = x + I$. We first note an interesting fact about this field; every nonzero element of $K$ is a power of $\alpha$. First of all, we have

$$K = \{0 + I, 1 + I, x + I, (x + 1) + I, x^2 + I, (x^2 + 1) + I, (x^2 + x) + I, (x^2 + x + 1) + I\}.$$  

We then see that

$$\alpha = x + I,$$
$$\alpha^2 = x^2 + I,$$
$$\alpha^3 = x^3 + I = (x + 1) + I = \alpha + 1$$
$$\alpha^4 = x^4 + I = x(x + 1) + I = (x^2 + x) + I = \alpha^2 + \alpha$$
$$\alpha^5 = x^5 + I = x^3 + x^2 + I = (x^2 + x + 1) + I = \alpha^2 + \alpha + 1$$
$$\alpha^6 = x^6 + I = (\alpha^3)^2 = (x^2 + 1) + I = \alpha^2 + 1$$
$$\alpha^7 = x^7 + I = x(x^2 + 1) + I = x^3 + x + I = 1 + I.$$  

To obtain these equations we used several calculational steps. For example, we used the definition of coset multiplication. For instance, $\alpha^2 = (x + I)^2 = x^2 + I$ from this definition.

Next, for $\alpha^3 = x^3 + I$, since $x^3 + x + 1 \in I$, we have $x^3 + I = (x + 1) + I$. For other equations, we used combinations of these ideas. For example, to simplify $\alpha^5 = x^5 + I$, first note that

$$\alpha^5 = \alpha^3 \cdot \alpha^2 = ((x + 1) + I)(x^2 + I)$$
$$= x^3 + x^2 + I$$
$$= (x^2 + x + 1) + I$$

since $x^3 + x + 1 \in I$.