We are interested in these rings thanks to their applications in error-correcting codes. Usually our field \( F \) of coefficients will be finite.

**Beware**

Don't confuse polynomials with functions.

For example, look at:

- \( f(x) = x^2 + x + 1 \in \mathbb{Z}_3[x] \)
- \( g(x) = x^4 + x + 1 \in \mathbb{Z}_3[x] \).

Note that these 2 polynomials represent the same function — even though the 2 polynomials are different. The function maps \( \mathbb{Z}_3 \to \mathbb{Z}_3 \).

Proof: Plug in the elements of \( \mathbb{Z}_3 \):

\[
\begin{align*}
f(0) &= 1, \\
f(1) &= 0, \\
f(-1) &= 1,
\end{align*}
\]
\[
\begin{align*}
g(0) &= 1, \\
g(1) &= 0, \\
g(-1) &= 1.
\end{align*}
\]

Note: There are \( 3 \cdot 3 \cdot 3 = 27 \) functions \( \mathbb{Z}_3 \to \mathbb{Z}_3 \) and \( \mathbb{Z}_3[x] \) is infinite (\( F = \text{field} \)).

We know that \( F[x] \) is a ring (in fact, an integral domain (see Gallian, p. 290)).

**Addition:** in \( \mathbb{Z}_3[x] \)

\[
(x^2 + 2x + 1) + (x^3 + 2) = x^3 + x^2 + 2x
\]

**Multiplication:** in \( \mathbb{Z}_3[x] \)

\[
\begin{align*}
\frac{x^2 + 2x + 1}{x^3 + 2} &= \frac{2x^2 + 4x + 2}{x^3 + 2x^4 + x^3 + 2x^2 + x + 2} \\
4 &\equiv 1 \pmod{3}
\end{align*}
\]
So, in $\mathbb{Z}_3[x]$

$$(x^3 + 2)(x^2 + 2x + 1) = x^5 + 2x^4 + x^3 + 2x^2 + x + 2$$

**Defn.** $F = \text{field}$

$f(x) \in F[x]$ of degree $> 0$ is **irreducible** if

- $f(x) \neq g(x) \cdot h(x)$ for $g(x), h(x) \in F[x]$ implies either $g(x)$ or $h(x)$ is of degree 0 (a constant polynomial).

**Note:** $F[x]$ is very much like $\mathbb{Z}$

The units are the non-0, constant polynomials.
The primes are the irreducible polynomials.

**Example** Finding irreducible polynomials in $\mathbb{Z}_2[x]$

**Degree 1**

- $x$, $x+1$  Both are irreducible.

**Degree 2**

The polynomials of degree 2 (reducible + irreducible) are

- $x^2$, $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$

Note that $x^2 = x \cdot x$ reducible

- $x^2 + 1 = (x+1)^2$ reducible

- $x^2 + x = x(x+1)$ reducible.

What about $x^2 + x + 1$? Is it irreducible?

Does $x$ or $x + 1$ divide it?

No!

$$x^2 + x + 1 = x(x+1) + 1$$

If $x$ (or $x+1$) were to divide $x^2 + x + 1$, then $x$ (or $x+1$) would divide 1, impossible as degree 1 = 0 $\Rightarrow$ no non-constant polynomial can divide it.

So $x^2 + x + 1$ is the only irreducible polynomial of degree 2 in $\mathbb{Z}_2[x]$. 
degree 3 The degree 3 reducible + irreducible polynomials in \( \mathbb{Z}_2[x] \) are
\[
\begin{align*}
&x^3, 
&x^3 + 1,
&x^3 + x,
&x^3 + x^2,
&x^3 + x^2 + x,
&x^3 + x^2 + x + 1.
\end{align*}
\]
Which of these are irreducible?
To answer this question it helps to know that for \( a \in \mathbb{Z}_2 \),
\[(x-a) \text{ divides } f(x) \in \mathbb{Z}_2[x] \iff f(a) = 0.\]
We prove this in a few pages.

\[\begin{align*}
&\{\text{So } f(x) \text{ of degree 3 reducible } \iff \text{ has a degree 1 factor } \iff f(a) = 0 \text{ for some } a \in \mathbb{Z}_2.\}
\end{align*}\]
Clearly 5 of our polynomials are reducible:
\[
\begin{align*}
x^3 &= x \cdot x \cdot x \\
x^3 + x &= x(x^2 + 1) \\
x^3 + x^2 &= x^2(x + 1) \\
x^3 + x^2 + x + 1 &= (x+1)(x^2 + 1) \\
x^3 + x^2 + x &= x(x^2 + x + 1)
\end{align*}
\]
What of the rest? Use \( \bigcirc \)
\[
\begin{align*}
&f(x) = x^3 + 1 \iff f(1) = 0 \iff f(x) \text{ reducible} \\
&f(x) = x^3 + x + 1 \iff f(1) = 1 = f(0) \iff f(x) \text{ irreducible} \\
&f(x) = x^3 + x^2 + 1 \iff f(1) = 1 = f(0) \iff f(x) \text{ irreducible}
\end{align*}
\]
So the only irreducible degree 3 polynomials in \( \mathbb{Z}_2[x] \) are
\[
\begin{align*}
&x^3 + x + 1, \\
&x^3 + x^2 + 1.
\end{align*}
\]
So \( \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle \cong \{a \theta^2 + b \theta + c \mid a,b,c \in \mathbb{Z}_2\} \)
where \( \theta^3 + \theta + 1 = 0 \).

This is the finite field with 8 elements.
It will turn out that replacing \( x^3 + x + 1 \)
by \( x^3 + x^2 + 1 \) yields an isomorphic field.
In order to understand polynomial rings \( F[x] \), where \( F = \text{field} \), we need the division algorithm. Then we will be able to prove polynomial versions of \( \mathbb{Z} \) - theorems; e.g. the fundamental theorem of arithmetic, Euclid's algorithm, lemma, ...

The division algorithm works just as it did in high school - more or less:

**Example** In \( \mathbb{Z}_2[x] \)

\[
\frac{x^2 + x + 1}{x^5 + x^4 + x^3 + x^2 + x + 1} = \frac{x^3 + 1}{x^5 + x^4 + x^3}
\]

\[
x^2 + x + 1
\]

\[
x^2 + x + 1
\]

\[
0
\]

So \( x^5 + x^4 + x^3 + x^2 + x + 1 = (x^2 + x + 1)(x^3 + 1) \).

**Example** In \( \mathbb{Z}_3[x] \)

\[
\frac{2x + 1}{2x + 1} = \frac{x^2 + x + 2}{4x^2 + 2x}
\]

\[
-x + 2
\]

\[
2x + 1
\]

\[
1
\]

\[
x^2 + x + 2 = (2x + 1)^2 + 1
\]

*Note:* We are definitely using the fact that \( \mathbb{Z}_3 \) is a field and

\[
2^{-1} = 2 \pmod{3}
\]

i.e.

\[
2 \cdot 2 = 1 \pmod{3}
\]
Division Algorithm for $F[x]$, $F = \text{field}$

Given $f(x)$ and $g(x) \in F[x]$, there are $r(x)$ and $q(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

and degree $r < \text{degree } g$

or $r(x)$ is the $0$-polynomial

For the proof, see Gallian, p. 296.

For $a_n \neq 0$, $m \geq n$

$$g(x) = (a_n x^n + \cdots) \bigg/ \left( b_m x^m + \cdots \right) = f(x)$$

or lower degree than $m$

If $m < n$, let $r = f$

Corollary 1. $F = \text{field}$, $a \in F$, $f(x) \in F[x]$

$$f(a) = 0 \iff \left( f(x) = (x-a)g(x), \text{ for some } g(x) \in F[x] \right)$$

Proof $\Rightarrow$ By the division algorithm

$$f(x) = (x-a)g(x) + r$$

degree $r = 0$ or $r = 0$

So $r \in F$ and plugging $x = a$ yields $0 = f(a) = r$

$\Rightarrow f(x) = (x-a)g(x)$.

$\Leftarrow$ clear.
Corollary 2. \( f(x) \in F[x], \) degree \( f = n \Rightarrow \)

\( f(x) \) has at most \( n \) roots counting multiplicity (This means \((x-1)^2\) has 2 roots counting 1 twice).

Proof

By Corollary 1, \( f(a) = 0 \Rightarrow f(x) = (x-a)g(x). \)
Here \( \deg f = \deg g + 1 \Rightarrow \deg g = \deg f - 1. \)
So we finish the proof by induction on the degree of \( f. \)

Corollary 3. Every ideal in \( F[x] \) is principal.

Let \( I \) be an ideal in \( F[x]. \) If \( I = \{0\}, \) we're done. So assume \( I \neq \{0\}. \) Let \( f(x) \) be an element of \( I \) with minimal degree.

Then

\[ \text{Claim: } I = \langle f(x) \rangle = \{ g(x) f(x) | g(x) \in F[x] \}. \]

Proof:

Let \( h(x) \in I. \) Use the division algorithm to see \( \exists q(x), r(x) \in F[x] \) such that

\[ h(x) = q(x)f(x) + r(x), \quad \{ \deg r < \deg f \text{ or } r = 0 \}. \]

Then

\[ r(x) = h(x) - q(x)f(x) \in I \]

\[ I \subseteq F[x]. \text{ } I \in I \]

By the minimality of degree \( f, \) then

\[ r = 0 \text{ and } h(x) \in \langle f(x) \rangle. \]
# Problems from Gallian

**# 33, p. 250**

Recall Gallian #58, p. 250

This problem \( \Rightarrow \) since \( \mathbb{Z}_p = \text{finite field} \)

if \( p = \text{prime} \), So \( \text{p/a} \Rightarrow a^{p-1} \equiv 1 \pmod{p} \)

**Proof**

\( \text{a} \in U(p) \), \( |U(p)| = p-1 \)

Use Lagrange's thm, Cor. 4, p. 143

This means every \( a \in \mathbb{Z}_p \) is a root of \( x^{p-1} - 1 \). Thus \( (x-a) \) divides \( (x^{p-1} - 1) \) for all \( a \in U(p) \) Moreover \( (x-a) \) and \( (x-b) \) are relatively prime polynomials if \( a \neq b \) in \( U(p) \)

So \( (x-a)(x-b) \) divides \( (x^{p-1} - 1) \), \( a \neq b \in U(p) \)

By induction \( g(x) = \prod_{a=1}^{p-1} (x-a) \) divides \( (x^{p-1} - 1) = f(x) \)

Since degree \( g = \text{degree} f = p-1 \)

the polynomials \( f \) and \( g \) must be equal up to a constant multiple.

But since the lead coefficients are both 1, the constant multiple must be 1 and \( f = g \).

**# 34, p. 302**

From #38, note that the constant term in \( x^{p-1} - 1 \) is \(-1\)

while that of \( \prod_{a=1}^{p-1} (x-a) \)

is \( (p-1)! \)

Thus \( (p-1)! \equiv -1 \pmod{p} \)

if \( p = \text{prime} \).

For the converse, note that when \( p = ab \), \( 1 < a, b < p \) we have \( a \) divides \( p \) and \( a \) divides \( (p-1)! \).

So if \( (p-1)! \equiv -1 \pmod{p} \) we'd have \( a \mid 1 \) impossible
Factoring Polynomials

\[ F = \text{field} \]

**Thm.** \( p(x) \in F[x] \)
\( p(x) \) irreducible \( \iff \langle p(x) \rangle = \text{maximal ideal in } F[x] \)

**Proof.** (same as for \( \mathbb{Z} \))

\( p(x) \) irreducible
\( I = \text{ideal in } F[x] \) such that
\( \langle p(x) \rangle \subset I \subset F[x] \).

We know \( I = \langle g(x) \rangle \) for some \( g(x) \in F[x] \)

\( \implies p(x) = g(x) \cdot h(x) \) for some \( h(x) \in F[x] \)

\( p(x) \) irreducible \( \implies \) either \( g \) or \( h \) is constant

If \( g \) is constant \( I = F[x] \)
If \( h \) is constant \( I = \langle p(x) \rangle \)

Thus \( \langle p(x) \rangle \) is maximal

\( \iff \) Suppose \( \langle p(x) \rangle \) maximal.

Then if \( p(x) = g(x) \cdot h(x) \) for some \( g(x), h(x) \in F[x] \)
with degree \( g \) + degree \( h \) both non-zero,

\( \langle p(x) \rangle \subsetneq \langle g(x) \rangle \subsetneq F[x] \)

Contradicts \( \langle p(x) \rangle \) maximal

**Cor.** \( p(x) \) irreducible in \( F[x] \)

\[ F[x]/\langle p(x) \rangle = \bigoplus \text{field} \]

Proof. Use Thm 14.4 on p. 254 of Gallian

(Ideal in \( \text{Ring with 1} \)) \( R/I = \text{field} \iff I \) maximal

**Examples Abound**

\[ F_8 = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle = \text{(field with 8 elements)} \]
\[ \mathbb{F}_8 = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle \]

The elements of \( \mathbb{F}_8 \) can be viewed as
\[
\alpha = a_0 + a_1 \theta + a_2 \theta^2, \quad a_j \in \mathbb{Z}_2
\]

\( \theta \) a root of \( x^3 + x + 1 = 0 \).

Some people call \( \mathbb{F}_8 = GF(8) \) "GF" stands for Galois field.

Note that \( a_0 + a_1 \theta + a_2 \theta^2 = r(\theta) \)
is a polynomial of degree \( \leq 3 = \deg(x^3 + x + 1) \).

Thus the elements \( r(x) \) represent the
remainders of polynomials in \( \mathbb{Z}_2[x] \)
upon division by \( x^3 + x + 1 \).

This is analogous to saying \( \mathbb{Z}/163\mathbb{Z} \)
consists of remainders of integers upon division by 163.

If you know what a vector space is, then note
\( \mathbb{F}_8 \) is a vector space over \( \mathbb{Z}_2 \). It is 3-dimensional
and \( \{1, \theta, \theta^2\} \) is a basis.

Writing elements of \( \mathbb{F}_8 \) in the form
\[
a_0 + a_1 \theta + a_2 \theta^2, \quad a_j \in \mathbb{Z}_2
\]

makes it easy to add but hard to multiply. So we seek a generator
of the multiplicative group \( \mathbb{F}_8^* = \mathbb{F}_8 \setminus \{0\} \).

It turns out that \( \langle \theta \rangle = \mathbb{F}_8^* \).
Table of Powers of \( \Theta \)

\[
\Theta^3 + \Theta + 1 = 0 \implies \Theta^3 = -\Theta - 1 = \Theta + 1
\]
as \( -1 = 1 \pmod{2} \)

\[
\Theta \left( a_0 + a_1 \Theta + a_2 \Theta^3 \right) = a_0 \Theta + a_1 \Theta^2 + a_2 \Theta^3
\]

\[
= a_0 \Theta + a_1 \Theta^2 + a_2 (\Theta + 1)
\]

\[
= a_2 + (a_0 + a_2) \Theta + a_1 \Theta^2
\]

So multiplication by \( \Theta \) sends the coefficients

\[
(a_0, a_1, a_2) \rightarrow (a_2, a_0 + a_2, a_1)
\]

This is a feedback shift register.

<table>
<thead>
<tr>
<th>Element of ( \mathbb{F}_8 )</th>
<th>( a_0 )</th>
<th>( a_1 )</th>
<th>( a_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Theta )</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \Theta^2 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \Theta^3 )</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \Theta^4 )</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( \Theta^5 )</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( \Theta^6 )</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( 1 = \Theta^7 )</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Thus we have a cyclic group

\[ \langle \Theta \rangle = \mathbb{F}_8^* = \mathbb{F}_8 - \{0\} \]

We call \( x^3 + x + 1 \) a primitive polynomial.

It is easy to multiply elements once you write them as powers of \( \Theta \).

Feedback Shift Register

\[ a_0 \xrightarrow{\oplus} a_1 \rightarrow a_2 \]

Here's the picture

You can use primitive polynomials to construct these. Cycles through \( 2^n - 1 \) states before repeat. Useful for codes.