Recall: Let F be a field.

Definition: $f(x) \in F[x]$ is said to be irreducible if $f(x)$ cannot be factored into polynomials $g(x), h(x) \in F[x]$, where $1 \leq \deg(g(x)), \deg(h(x)) \leq \deg(f(x)) - 1$.

Proposition: Let $p(x), q(x) \in D[x]$ where D is an integral domain. Then $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$.

Proposition: Let M be an ideal of a commutative ring R with identity. Then M is maximal if and only if R/M is a field.

Proposition: Every ideal of $F[x]$ has the form $\langle f(x) \rangle$ for some $f(x) \in F[x]$.

Theorem: Let F be a field and $f(x) \in F[x]$. Then $\langle f(x) \rangle$ is a maximal ideal if and only if $f(x)$ is irreducible.

Proof: ($\Rightarrow$) Suppose $f(x)$ is not irreducible over F, i.e $\exists\, g(x), h(x) \in F[x]$ s.t. $f(x) = g(x)h(x)$ and $1 \leq \deg(g(x)), \deg(h(x)) < \deg(f(x))$. We want to show that $\exists\, I \triangleleft F$ such that $\langle f(x) \rangle \subsetneq I \subsetneq F[x]$.

Let $I = \langle g(x) \rangle$. Since $f(x) = g(x)h(x) \in \langle g(x) \rangle$, then $\langle f(x) \rangle \subset \langle g(x) \rangle$. Then by the above proposition, every polynomial in $\langle f(x) \rangle$ has degree larger than $\deg(f(x))$ and larger than $\deg(g(x))$. Therefore, $g(x) \notin \langle f(x) \rangle$ and so $\langle f(x) \rangle \subsetneq \langle g(x) \rangle$. Therefore, every polynomial in $\langle g(x) \rangle$ has degree at least $\deg(g(x))$ and at least 1. So $\langle g(x) \rangle$ does not contain polynomials of degree 0, and so $\langle g(x) \rangle \subsetneq F[x]$. Therefore one direction of the proof is complete.

($\Leftarrow$) Suppose $f(x)$ is irreducible over F. Let $I \triangleleft F[x]$ such that

$\langle f(x)\rangle \subset I \subset F[x]$ We want to show that $I = \langle f(x)\rangle$ or $I = F[x]$. Then $I = \langle g(x)\rangle$ for some $g(x) \in F[x]$. Since $f(x) \in \langle g(x)\rangle$, then $f(x) = r(x)g(x)$ for some $r(x) \in F[x]$. Since $f(x)$ is irreducible, then either $\deg(r(x)) = 0$ or $\deg(g(x)) = 0$.

Case 1: If $\deg(r(x)) = 0$, then $r(x) = b$ for some $b \neq 0 \in F$ and so $g(x) = b^{-1}f(x) \in \langle f(x)\rangle$, thus $\langle f(x)\rangle = \langle g(x)\rangle = 1$.

Case 2: If $\deg(g(x)) = 0$, then $g(x) = c$ for some $c \neq 0 \in F$ and so $c^{-1}c \in \langle g(x)\rangle$ and so $\langle g(x)\rangle = F[x]$.

Therefore, $\langle f(x)\rangle$ is a maximal ideal of $F[x]$.

Corollary: Let F be a field and let $f(x) \in F[x]$. Then $F[x]/\langle f(x)\rangle$ is a field if and only if $f(x)$ is irreducible over F.

Corollary: Let F be a field and $p(x)$ is an irreducible polynomial on F. If $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

Proof: Suppose $a(x)b(x) = r(x)p(x)$ for some $r(x) \in F[x]$. Then in $F[x]/\langle p(x)\rangle$, $(a(x) + \langle p(x)\rangle)(b(x) + \langle p(x)\rangle) = a(x)b(x) + \langle p(x)\rangle = \langle p(x)\rangle$

Then $F[x]/\langle p(x)\rangle$ is a field so it has no zero divisors. Therefore $a(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle$ or $b(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle$, and so $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

Aside. If $F = \mathbb{Z}_3$, then $p(x)$ has degree 3, x^3+1 which is irreducible in $\mathbb{Z}_3$.

Example: Construct a finite field of order 9.

The tool that we use is $F[x]/\langle p(x)\rangle$ where $p(x)$ is a polynomial over F. We know that we will have elements of the form $a + \langle p(x)\rangle$ for all $a \in F$. We can take $\mathbb{Z}_3$ because $9 = 3^2$. Now we need a polynomial $p(x)$ that is irreducible in $F[x]$. We can have

$0 + \langle x^3+1 \rangle$, $1 + \langle x^3+1 \rangle$, $2 + \langle x^3+1 \rangle$, $x + \langle x^3+1 \rangle$, $x+1+\langle x^3+1 \rangle$

$x+2+\langle x^3+1 \rangle$, $x^2 + \langle x^3+1 \rangle$, $x^2+1+\langle x^3+1 \rangle$, $x^2+2+\langle x^3+1 \rangle$, ...

Any distinct in $\mathbb{Z}_3[x]/\langle x^3+1 \rangle$ has the form $ax^2+bx+c+\langle x^3+1 \rangle$,

where $a, b, c \in \mathbb{Z}_3$. This means we have 3^3 different choices.

So $\deg(p(x)) = 2$ is needed.