Recall for a field $F$, $F[x]$ is a PID.

**Theorem 8.6.6** Let $I = (p(x)) < F[x]$ be an ideal. $I$ is maximal $\iff$

$p(x)$ is irreducible.

Recall $I$ is maximal $\iff$ $F[x]/I$ is a field.

**Examples**

1) $\mathbb{R}[x]/(x^2 + 1) = \mathbb{C}$

2) $\mathbb{Q}[x]/(x^2 + x + 1) = \mathbb{Q}(-\sqrt{3})$
\[ \{ a + b \sqrt{-3} : a, b \in \mathbb{Q} \} \]

3) \[ \frac{\mathbb{Z}[x]}{(x^2 + x + 1)} = \mathbb{F}_4 = \text{the field with 4 elements} \]

\[ \{ 0, 1, x, x+1 \} \]

Proof \[ \Rightarrow \text{if } p(x) = f(x)g(x) \text{ with } \deg f > 0 \]
and \[ \deg g > 0 \], then \[ f \text{ and } g \text{ map to zero divisors in } \mathbb{F}[\mathbb{Z}[x]]/I \], so \[ \mathbb{R} \text{ is not a field}. \]

\[ \mathbb{F}[\mathbb{Z}[x]]/(p(x)) \]

\[ \Leftarrow \text{Suppose } p(x) \text{ is irreducible} \]
Suppose $I \neq J \neq (1)$, i.e. that $I$ is not maximal.

Since $F[x]$ is a PID,

$J = (\text{some element of } F[x])$. Since $f(x) \in J$

$p(x) = \text{some element of } F[x] \cdot q(x)$ for some $q(x)$

If $\deg q > 0$ and $\deg \text{some element of } F[x] > 0$

then $p(x)$ is reducible

If $\deg \text{some element of } F[x] = 0$ then $J = (1)$.

$\deg q = 0$ then $J = I$

Hence $I$ is maximal. QED
Recall an ideal $I \subset R$ is prime iff $R/I$ is a domain. 
$I$ is maximal iff $R/I$ is field. 
Hence every maximal ideal is prime.

Con 8.6.7 in $F[x]$, $(p(x))$ is prime.
$\Rightarrow$ it is maximal.
$\Rightarrow$ $p(x)$ is irreducible.

Proof
$p$ irreducible $\Rightarrow (p)$ is maximal
$\Rightarrow (p)$ prime

Suppose $(p)$ is prime and
\( p(x) = f(x)g(x) \) with \( \deg f, \deg g \geq 0 \)

This means \( fg = 0 \) in \( \mathbb{K}[x] / (\mathfrak{p}) \)

which cannot be since \( \mathbb{K}[x] / (\mathfrak{p}) \)

is a domain. \hfill \text{QED}

Con\( \mathfrak{o} \mathfrak{f} \) \( c_0, b, b + c_0 b, 0 \)

in \( \mathbb{F}[x] \)

I prime \( \iff \) I maximal \( \iff \mathbb{F}[x]/I \) is a field.
Linear algebra revisited

A vector space over $F$ is an abelian group in which we have scalar multiplication by elements in $F$.

A set $S = \{v_1, v_2, \ldots, v_n\} \subseteq V$ is linearly independent if $c_1 v_1 + c_2 v_2 + \cdots + c_n v_n = 0$ for $c_i \in F$ only if $c_1 = c_2 = \cdots = c_n = 0$.

A basis $B$ of $V$ is a maximal linearly independent set. Let $B = \{v_1, \ldots, v_n, \ldots, v_m\}$. 
so each \( v \in V \) has the form

\[
\sum c_i v_i \quad \text{for } c_i \in \mathbb{F} \quad \text{for unique } c_i
\]

(almost all \( c_i = 0 \)).

A subspace \( W \subset V \) is a subset closed under scalar multiplication.

**Examples**

1) \( \mathbb{F}[x] \) is a vector space \( \mathbb{F} \) with

basis \( \{ 1, x, x^2, x^3, \ldots \} \)

2) The set of polynomials of deg \( < n \)
in a subspace with basis

\( \{ 1, x, \ldots, x^{n-1} \} \)
Prop 10.1.8 Let $V$ be a vector space over a field $F$ with $v \in V$ and $c \in F$

1) $cv = 0 \iff c = 0 \text{ or } v = 0$

2) $(c)v = - (cv) = c(-v)$.

Then 10.1.17 A subset $U \subset V$ is a subspace iff $\forall c \in F$ and $u, w \in U$

1) $u - w \in U$ [U is a subgroup of $V$]

2) $cm \in V$ [closure under scalar multiplication]
Def: A vector space is finite dimensional if it has a finite basis.

Then in this case any 2 bases have the same size $n$, the dimension of $V$.

Examples

1) $C$ has dimension 2 as a vector space over $\mathbb{R}$.
2) \( \dim_\mathbb{Q} \mathbb{Q}(\sqrt{2}) = 2 \)

\[
\mathbb{Q}(\sqrt{2}) = \{ a + b \sqrt{2} : a, b \in \mathbb{Q} \}
\]

\[
= \mathbb{Q}[x] / (x^2 - 2)
\]

\( \dim_\mathbb{F} V \) = dimension of \( V \) as a vector space over \( \mathbb{F} \).

3) \( \dim_{\mathbb{F}_{41}} \mathbb{F}_{41} = 2 \)

where \( \mathbb{F}_{41} = \mathbb{Z}/2[\![x]\!] / (x^2 + x + 1) \)

\( \dim_{\mathbb{F}_{41}} \mathbb{F}_{41} = 3 \)
4) \( \mathbb{Q} \cap \mathbb{Q}(\sqrt[3]{3}) = \mathbb{Q}[x]/(x^3 - 3) \)

\( \mathbb{Q} \cap \mathbb{Q}[y]/(y^2 + y + 1) \)

\( L = K[x]/(x^3 - 2) \)

\( = \{ a + b \sqrt[3]{2} + c \sqrt[3]{4^2} : a, b, c \in \mathbb{K} \} \)

\( \dim_\mathbb{Q} L = 6 \quad \dim_\mathbb{K} L = 3 \quad \dim_\mathbb{Q} \mathbb{K} = 2 \)

In general, when we have
fields $K < K < L$ with $L$ finite dimensional over $K$,
$\dim_K L = \dim_K L \dim_K K$

$K \supset F$ descent for field.

Prop Let $V$ be a vector space of dimension $n$ over field $F$ and let
$\{v_1, v_2, \ldots, v_m\}$ with $m < n$ be
linearly independent. Then we can find $v_{n+1}, v_{n+2}, \ldots, v_m$ such
that \( \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m \) is a basis of \( V \).