Thm 8.6.6 Let \( p(x) \in \mathbb{F}[x] \) be a field and \( I = (p(x)) \subset \mathbb{F}[x] \).

\( I \) is maximal \( \iff \) \( p(x) \) is irreducible.

Cor 8.6.7 \( \text{In } R = \mathbb{F}[x] \)

\( (p(x)) \) is prime \( \iff \) \( (p(x)) \) is maximal \( \iff \) \( p(x) \) is irreducible.

This means \( R/I \) is a field.

Example \( \mathbb{F} = \mathbb{R} \) and \( p(x) = x^2 + 1 \).
\[ \mathbb{R}[x]/(x^2 + 1) = \mathbb{C} \]

where \( x = \sqrt{-1} \).

In general prime ideals need not be maximal.

Example: \( \mathbb{R} = \mathbb{Z}[x] \)

\((x) \) is prime but not maximal.

\((x, 2) \) is maximal.

Proof of 8.6.7: Suppose \( (p(x)) = \mathbb{R} \).

\( p(x) \) is prime. We know \( \mathbb{R} \) is a PID.
Suppose $I$ is not maximal but is contained in a bigger ideal $J = (f(x))$. Then $f(x) = g(x)q(x)$ so $\phi$ is not irreducible.

Let $\overline{R} = \frac{R}{I} = \overline{\{x\}}/(\overline{\phi(x)})$ and let $\overline{f}$ and $\overline{g}$ denote the images of $f$ and $g$ in $\overline{R}$.

Since $\overline{\phi(x)}$ is prime, $\overline{R}$ is a domain. Hence $\overline{f} \overline{g} = 0$ implies
either \( \overline{f} = 0 \) or \( \overline{g} = 0 \)
if \( \overline{f} = 0 \) then \( \overline{f} \) is a multiple of \( \overline{p} \)
if \( \overline{g} = 0 \) then \( \overline{g} \) is a multiple of \( \overline{p} \)

Hence \( (\overline{p}) = (\overline{f}) \) and \( f \) is maximal.

**Review of linear algebra**

Can define a vector space \( V \) over any field \( F \), not just \( \mathbb{R} \) or \( \mathbb{C} \).
Can define linear independence, basis and dimension over any $F$ and subspaces.

Examples:

1) $F[x]$ is a vector space over $F$.
   - It is infinite dimensional.

2) The set of polynomials of degree < $n$ is an $n$-dimensional vector space.
Prop 10.1.8: Let $V$ be a vector space over $F$ with $v \in V$ and $c \in F$.

1) $(cv = 0) \iff c = 0 \quad \forall v, v = 0$.
2) $(c)v = -(cv) = c(-v)$.

Thm 10.1.10: A subset $U$ of $V$ is a subspace if $\forall \, c \in F$ and $v, w \in U$,

1) $v - w \in U$
2) $c \cdot v \in U$
We can define the dimension of a vector space in the usual way. It may or may not be finite.

**Examples**

1) \(\mathbb{R}^2\) has dim 2 over \(\mathbb{R}\).

2) \(\mathbb{Q}(\sqrt{2})\) has dim 2 over \(\mathbb{Q}\).

\[\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2\]
3) \( \dim_{\mathbb{F}_2} \mathbb{F}_4 = 2 \)
\[
\mathbb{F}_4 = \mathbb{Z}/2[x]/(x^2 + x + 1)
\]
\[
\mathbb{F}_8 = \mathbb{Z}/2[x]/(x^3 + x + 1)
\]

\[
= \{ a + b \cdot x + c \cdot x^2 : a, b, c \in \mathbb{Z}/2 \}
\]

4) \( \mathbb{Q} \subset \mathbb{K} \subset \mathbb{L} \)
\[
\mathbb{Q}(\sqrt{3}) \quad \mathbb{K}[\sqrt{2}] \quad \mathbb{K}[\sqrt{1/(\sqrt{2} - 2)}]
\]
\[
\mathbb{Q}[x]/(x^2 + 3) \quad \mathbb{K}[\sqrt{7}/(\sqrt{2} - 2)]
\]
\[ \dim_k K = 2 \quad \dim_k L = 3 \]
and \[ \dim_k L = 6 \]

In general, when \[ k < K < L \] then
\[ \dim_k L = \dim_k K \dim_k L. \]

Prop: Let \( V \) be a vector space of \( \dim_m n > m \) with \( m \) linearly independent vectors.
\{ v_1, v_2, \ldots, v_m \}. \text{ Then we can add } n-m \text{ more vectors to get a basis of } U.\]

- Field extensions:
  If \( p(x) \in F[x] \) is irreducible, then \( F[x]/(p(x)) \) is a field extension of \( F \).
Problem 10.22. Let $F \subseteq E$ with $\alpha \in E$. Let $E$ be a splitting of $E$

$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : b \geq g \in F[\alpha] \right\}$

= subfield of $E$.

1) $F[\alpha]$ is a splitting of $E$ containing $F$. 

$F[\alpha] = \left\{ f(x) : f \in F[x] \right\}$
2) $F[x]$ is the smallest such subring

3) $F(x)$ is a subfield of $E$ containing $F$

4) $R$ is the smallest such subfield

Proof: 1) and 3) are obvious

For 2) let $F \subseteq R \subseteq E$
where \( R \) is a subring.

Then every polynomial of \( x \) over \( F \) is in \( R \), so \( R \supset F(\alpha) \).

Proof of 9) is similar.

QED

Def: We say \( E \) is an algebraic extension of \( F \) if it is
\( F(x) \) for some \( x \in E \).

We will see next time that

\[
F([x]) = F(x).
\]