Thm 1. Let $F$ be a field and suppose $p(x) \in F[x]$. 

$I = \langle p(x) \rangle$ is maximal if and only if $p(x)$ is irreducible.

Proof: Suppose $I = \langle p(x) \rangle$ is maximal, $\Rightarrow I$ is a prime ideal and a maximal ideal is proper and non-zero 

$\therefore p(x) \neq 0$

Suppose $p(x) = f(x)g(x)$ 

$\deg(f) < \deg(p), \deg(g) < \deg(p)$

$I = \langle p(x) \rangle$ is prime, $p(x) \in I \Rightarrow f(x)g(x) \in I$

$\therefore$ either $f(x) \in I$ or $g(x) \in I$ (since $I$ prime)

Say $f(x) \in I \Rightarrow f(x) = p(x)q(x)$ for some $q(x) \in F[x]$ 

but this is a contradiction since $\deg(f) \geq \deg(p)$ 

$\therefore p(x)$ is irreducible

Suppose $p(x)$ irr. over $F[x]$, $p(x) \in I \Rightarrow I = \langle p(x) \rangle$

$\therefore I \trianglelefteq \langle p(x) \rangle \trianglelefteq J \leq F[x]$

$J$ is a principal ideal, say $J = \langle s(x) \rangle$ for some $s(x) \in F[x]$

$p(x) \in J \Rightarrow p(x) = f(x)g(x)$ for some $g(x) \in F[x]$. 

(For some $g(x) \in F[x]$).
But $p(x)$ is irreducible $\Rightarrow$ $f(x) = c \in F$ or $g(x) = c \in F$.

$\Rightarrow$ $J = \langle c \rangle = \{ c \cdot r(x) \mid r(x) \in F[x] \}$.

- If $f(x) = c \Rightarrow J = \langle 1 \rangle = F[x]$
- If $g(x) = c \Rightarrow J = \langle f(x) \rangle = \langle p(x) \rangle = I$

$\therefore I = \langle p(x) \rangle$ is maximal.

**Corollary**
Let $I$ be a field, $p(x) \in F[x]$. A non-zero, proper ideal $I$ in $F[x]$ is prime iff $p(x)$ is irreducible.

Additionally, $I$ is maximal iff $I$ is a non-zero, proper, prime ideal.

**Proof:** Showed above (in proof) that if $I$ prime (non-zero) $\Rightarrow$ $p(x)$ is irreducible. By Thm above, $p(x)$ irreducible $\Rightarrow I = \langle p(x) \rangle$ is maximal $\Rightarrow I$ is prime.

**Field of Fractions**

- $D$ - integral domain
- $S = \{ (a, b) \mid a, b \in D, b \neq 0 \}$

Define an eq. relation $(a,b) \sim (c,d) \iff ad = bc \text{ in } D$ $(\text{Think } \frac{a}{b} = \frac{c}{d})$
Lemma: \( \sim \) is an equivalence relation.

Proof:

- \( \sim \) reflexive \( (a,b) \sim (a,b) \)
  
  \[ a \cdot b = ba \text{ which is true since } D \text{ is commutative} \]

- (Symmetric) if \( (a,b) \sim (c,d) \) \( \iff (c,d) \sim (a,b) \)

  \[ ad = bc \iff cb = da \]

  These are same since

  \( D \) is commutative

- (Transitive)

  \[ (a,b) \sim (c,d), (c,d) \sim (e,f) \]

  \[ \begin{align*}
  ad &= bc \\
  cf &= dg
  \end{align*} \]

  \[ af = be \iff (a,b) \sim (e,f) \]

\[ \therefore S \text{ is a set of eq. classes} \]

\[ F_D = S \]

\[ \text{Field of fractions of } D \]

Let \( a,b,c,d \in D \)
Add: $[a, b] + [c, d] = [ad + bc, bd]$

mult: $[a, b][c, d] = [ac, bd]$

Lemma: Operations in $F_D$ (above) are well defined.

Proof: (Addition) Suppose $[a_1, b_1] = [a_2, b_2]$, $[c_1, d_1] = [c_2, d_2]$

Show $[a_1, b_1] + [c_1, d_1] = [a_2, b_2] + [c_2, d_2]$

Show $[a_1 b_1 + b_1 c_1, b_1 d_1] = [a_2 d_2 + b_2 c_2, b_2 d_2]$

Show $(a_1 b_1 + b_1 c_1) b_2 d_2 = (a_2 d_2 + b_2 c_2) b_1 d_1 \in D$

$= a_1 b_1 b_2 d_2 + b_1 c_1 b_2 d_2 = a_1 b_2 d_1 d_2 + b_1 b_2 d_1 c_2$

$= (a_1 d_2 + b_2 c_2) b_1 d_1$

Lemma: $F_D$ with ops above is a field.

Proof:

Add identity: $[0, 1]$ since $[a, b] + [0, 1] = [a + 0, b + 1] = [a, b]$

Add inverse is: $[-a, b]$
Multinves is \([b,a]\), i.e. \([a,b] \cdot [b,a] = [ab,\overline{ab}] = [1,1]\)

\[\rightarrow ab = \overline{ab}\]

etc.

**Thm.** 1 Let \(D\) be an integral domain. \(D\) can be imbedded in a field of fractions \(\mathbb{F}_D\) where and \([a,b] \in \mathbb{F}_D\) can be expressed as a

\[ [a,b] = \frac{[a,1]}{[b,1]} \quad a, b \in D \]

Also \(\mathbb{F}_D\) is unique, i.e., if \(E\) is any field s.t. \(D \subseteq E\)

then \(\exists \psi : \mathbb{F}_D \rightarrow E\)

\[ [a,b] \mapsto ab^{-1} \]

giving an isomorphism \(\mathbb{F}_D \cong \text{Subfield of } E\)

**Aside** in practice write \(a/b \in \mathbb{F}_D\), subfield = subring which is a field

Think about \(D = \mathbb{Z}\), \(\mathbb{F}_D = \mathbb{Q}\)

and \(E = \mathbb{R}\) or \(E = \mathbb{C}\), etc.

**Proof:** 1 First show \(D\) can be embedded in \(\mathbb{F}_D\)

Define a map \(\phi : D \rightarrow \mathbb{F}_D\)

\[ a \mapsto \frac{[a,1]}{[b,1]} \]

let \(a, b \in D\)

\(\phi\) is a hom.

\[ \phi(ab) = [ab,1] = \frac{[a,1]}{[b,1]} \cdot \frac{[b,1]}{[c,1]} = \phi(a) \phi(b) \]
\[ \phi(a+b) = [a+b, 1] = [a, 1] + [b, 1] = \phi(a) + \phi(b) \]

\[ \therefore \phi \text{ is hcm.} \]

Show \( \phi \) is 1-1. Suppose \( \phi(a) = \phi(b) \)

\[ [a, 1] = [b, 1] \implies 1a = 1b \implies a = b. \]

\[ \therefore \text{D can be imbedded in } F_0 \text{ r.o.} \quad \begin{array}{c}
\mathbb{D} \cong \phi(D) \leq F_0 \\
\uparrow
\end{array} \\
\text{By 1st iso. thm.} \\
\text{Since } \ker(\phi) = \{0\} \\
\phi(0) \text{ is a subring of } F_0. \]

- Any \([a, b] \in F_0\) is a quotient (of two things in \(\phi(D)\))

Since \( \phi(a) [\phi(b)]^{-1} = [a, 1] [b, 1]^{-1} = [a, 1][1, b]^{-1} = [a, b]^{-1} \)

\[ \frac{\phi(a)}{\phi(b)} \]

Now let \( E \) be a field, \( D \subseteq E \) (as subring)

\[ \psi : F_0 \to E \]

\[ [a, b] \mapsto a b^{-1} \]

- Show \( \psi \) is well defined \( [a_1, b_1] = [a_2, b_2] \)

\[ \psi([a_1, b_1]) = a_1 b_1^{-1} = a_2 b_2^{-1} = \psi([a_2, b_2]) \]

\[ \iff a_1 b_2 = b_1 a_2 \]

\[ \text{By this, in } E \]

\[ \psi([a_1, b_1]) = a_1 b_1^{-1} = a_2 b_2^{-1} = \psi([a_2, b_2]) \]
\[ \psi \text{ is well defined} \]

Show \( \psi \) is a hom.

\[ \psi \left( [a, b] \cdot [c, d] \right) = \psi \left( [ac, bd] \right) = ac (bd)^{-1} \]
\[ = ab^{-1} cd^{-1} \]
\[ = \psi([a, b]) \psi([c, d]) \]

Check \( \psi([a, b] + [c, d]) = \psi([a, b]) + \psi([c, d]) \)

\( \psi \) is hom.

Consider \( \ker \psi \)

If \( \psi([a, b]) = ab^{-1} = 0 \Rightarrow a = b \cdot 0 \)
\[ [a, b] = [0, 1] \]

\( \therefore \ker \psi = [0, 1] \) in \( \mathbb{F}_p \), \( \therefore \psi \) is 1-1

By First Isomorphism Theorem
\[ \mathbb{F}_0 = \mathbb{F}_0 / \ker \psi \cong \psi(\mathbb{F}_0) \leq E \]

\[ \text{Ex} \quad \mathbb{Q}[x] - \text{is an integral domain} \]
\[ \mathbb{Q}(x) = \left\{ \frac{p(x)}{q(x)} \mid q(x) \neq 0, \ p(x), q(x) \in \mathbb{Q}[x] \right\} \]

\[ \text{Ex} \quad \mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \right\} \text{ contains } \mathbb{Q} \]
and \( \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \)
Corollary 1 Let $F$ be a field of characteristic zero. Then $F$ contains a subfield isomorphic to $\mathbb{Q}$.

Corollary 1 Let $F$ be a field of characteristic $P$. Then $F$ contains a subfield isomorphic to $\mathbb{Z}_p$.

Vector Spaces

Can define a vector space over any field $F$.

Definition A vector space $V$ over a field $F$ is:

- A group $(V, +)$ (with addition) with a scalar product $\alpha V$ for $\alpha \in F$, $v \in V$ s.t.:
  - $\lambda (\beta v) = (\lambda \beta) v$
  - $(\alpha + \beta)v = \alpha v + \beta v$
  - $\lambda (v + w) = \lambda v + \lambda w$
  - $1 \cdot v = v$

Example $\mathbb{R}^n$, $\mathbb{C}^n$

Example If $F$ is a field, $F[x]$ is a vector space over $F$:

- The vectors in $F[x]$ are polynomials
- Vector addition is poly. addition
- $\lambda f(x)$ scalar mult. by field element
Example \[ C[a, b] = \{ f : [a, b] \to \mathbb{R} \mid f \text{ continuous} \} \]

Example \[ V = \mathbb{Q}(\sqrt{2}) \text{ is a vector space over } \mathbb{Q} \]
\[ u, v \in \mathbb{Q}(\sqrt{2}) \]
\[ u + v = (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \]

Proposition Let \( V \) be a vector space over \( F \). The following holds:

- \( 0 \cdot v = 0 \in V \) \( \forall v \in V, 0 \in F \)
- \( a \cdot 0 = 0 \) \( \forall a \in F, 0 \in V \)
- if \( x \cdot v = 0 \Rightarrow x = 0 \in F \) or \( v = 0 \in V \)
- \((-1) \cdot v = -v \) \( -1 \in F \), \(-v \in V \)
- \((-a) \cdot v = (-a) \cdot v = a \cdot (-v) \)

Subspaces

\( W \) is a subspace of a vector space \( V \) if \( W \) is closed under vector addition (i.e., Abelian subgroup) and scalar multi. i.e.

- \( u + w \in W \) \( \forall u, w \in W \)
- \( a \cdot w \in W \) \( \forall a \in F, w \in W \)
\[ W = \sum_{i=0}^{\infty} a_i x^i \mid n \in \mathbb{Z}_{\geq 0}, a_i \in F \]

Is a subspace of \( U = F[x] \)

**Def.** \( v_1, \ldots, v_n \in U \), \( d_1, \ldots, d_n \in F \)

\[ w = \sum_{i=1}^{n} d_i v_i = d_1 v_1 + \cdots + d_n v_n \]

\( w \) is a \underline{linear combination} of \( v_1, \ldots, v_n \)

\[ W = \text{Span}_F(v_1, \ldots, v_n) = \left\{ \sum_{i=1}^{n} d_i v_i \mid d_i \in F \right\} \]

**Prop.** Let \( S = \left\{ v_1, \ldots, v_n \right\} \) be vectors in a vector space \( U \)

\( \text{Span}_F(S) \) is a subspace of \( U \).

**Def.** A set of vectors \( v_1, \ldots, v_n \) is \underline{linearly independent} if

\[ d_1 v_1 + d_2 v_2 + \cdots + d_n v_n = 0 \]

if and only if \( d_1 = d_2 = \cdots = d_n = 0 \).

**Def.** If there are \underline{non-zero} \( d_i \)'s \( s.t. \)

\[ d_1 v_1 + d_2 v_2 + \cdots + d_n v_n = 0 \], then \( \{v_1, \ldots, v_n\} \) is \underline{linearly dependent}.
Prop/ Let \( \{ v_1, \ldots, v_n \} \) be a linearly independent set in a vector space \( V \).

Suppose \( a_1 v_1 + \cdots + a_n v_n = b_1 v_1 + \cdots + b_n v_n \),

then \( a_1 = b_1, \ldots, a_n = b_n \).

Proof:
\[
\alpha_1 v_1 + \cdots + \alpha_n v_n = \beta_1 v_1 + \cdots + \beta_n v_n
\]

\[\left( \alpha_1 - \beta_1 \right) v_1 + \cdots + \left( \alpha_n - \beta_n \right) v_n = 0\]

Since \( \{ v_1, \ldots, v_n \} \) are linearly independent \( \Rightarrow \alpha_i - \beta_i = 0 \)

\( \Rightarrow \alpha_i = \beta_i \forall i \).

Prop/ \( \{ v_1, \ldots, v_n \} \) are linearly dependent

iff some \( v_i \) is a linear combination of the others.

Prop/ Suppose \( V = \text{Span}_F \{ v_1, \ldots, v_n \} \) where \( v_1, \ldots, v_n \) are linearly independent. If \( m > n \) then any set of \( m \) vectors in \( V \) must be linearly dependent.

Def/ \( \{ e_1, \ldots, e_n \} \) is a basis of \( V \) if \( \{ e_1, \ldots, e_n \} \) are linearly independent and \( V = \text{Span}_F \{ e_1, \ldots, e_n \} \).

Ex/ \( (1,0,0), (0,1,0), (0,0,1) \) is a basis of \( \mathbb{R}^3 \).
Ex. \[ \{ 1, \sqrt{2}, 3 \} \text{ or } \{ 1 + \sqrt{2}, 1 - \sqrt{2}, 3 \} \text{ are bases of } \mathbb{Q}(\sqrt{2}) \]

Prop. Let \( \{ e_1, \ldots, e_m \} \) and \( \{ f_1, \ldots, f_n \} \) be bases for a vector space \( V \) then \( m = n \).

Def. Let \( \{ e_1, \ldots, e_n \} \) is a basis for a vector space \( V \)
define the dimension of \( V \):

\[
dim(V) = n.
\]

Thm. Let \( V \) be a vector space of dimension \( n \).

1) If \( S = \{ v_1, \ldots, v_n \} \) is a set of linearly independent vectors in \( V \), then \( S \) is a basis for \( V \).

2) If \( S = \{ v_1, \ldots, v_n \} \) spans \( V \), then \( S \) is a basis for \( V \).

3) If \( S = \{ v_1, \ldots, v_k \} \) is a set of linearly independent vectors in \( V \), \( k < n \), then \( \exists v_{k+1}, \ldots, v_n \) s.t.

\[
\{ v_1, \ldots, v_k, v_{k+1}, \ldots, v_n \} \text{ is a basis for } V.
\]
Fields

- When is a field $F$ contained in a larger field $F_1$?
- What fields are between $\mathbb{Q}$ and $\mathbb{R}$?

Let $F$ be a field, $p(x) \in F[x]$:

Can we find a field $E$, $F \subseteq E$, s.t.

$p(x)$ factors into linear factors over $E[x]$.

---

Consider $p(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$.

\[ p(x) = (x^2 - 2)(x^2 - 3) \]

\[ \iff p \text{ has no zeros in } \mathbb{Q}, \text{ has 4 zeros in } \mathbb{R} \]

Can find smaller fields where $p(x)$ has zeros:

- $\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$
- $\mathbb{Q}(\sqrt{3}) = \{ a + b\sqrt{3} \mid a, b \in \mathbb{Q} \}$

- 2 roots in either field.
Extension Fields

A field $E$ is an extension field of a field $F$ if $F$ is a subfield of $E$. $F$ is called the base of $E$. Write $F \subseteq E$

Example 1

$F = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$E = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \{a + b(\sqrt{2} + \sqrt{3}) \mid a, b \in \mathbb{Q}\}$

$E$ is an extension field of $F$

$\sqrt{2} + \sqrt{3} \in E \quad \frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2} \in E$