Thm | 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 $\deg(f) < \deg(p)$

$\therefore p(x)$ is irreducible

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

$\therefore I = \langle p(x) \rangle \subseteq J \subseteq F[x]$

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

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

But $p(x)$ is irreducible $\Rightarrow$ $f(x) = c \in F$ or $g(x) = c \in F$

$J = \langle c \rangle = \{ c \cdot r(x) \mid r(x) \in F[x] \} = \langle 1 \rangle$

- 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 F 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 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

Think $\frac{a}{b}$

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

Define an eq. relation

$(a, b) \sim (c, d) \iff ad = bc$ in D

(Think $\frac{a}{b} = \frac{c}{d}$)

Lemma 1 $\sim$ is an equivilance relation.

Proof: • $\sim$ reflexive $(a,b) \sim (a,b)$

$ab = ba$ which is true since D is commutive

• (symetric) if $(a,b) \sim (c,d) \iff (c,d) \sim (a,b)$

$ad = bc \iff cb = da$

these are same since D is commutive

• (transitive)

$(a,b) \sim (c,d)$, $(c,d) \sim (e,f)$

$ad = bc$ $\quad$ $cf = de$

$afd = adf = bcf = bde = bed$

$af = be \iff (a,b) \sim (e,f)$.

∎

$\therefore$ S is a ~~SA~~ of eq. classes

$F_D = S$

↑ Field of fractions of D ← an integral domain

Let $a,b,c,d \in D$

Add: $[a,b]+[c,d] = [ad+bc,\ bd]$

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

Lemma 1 Operations in F_D (above) are well defined.

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

$a_1 b_2 = b_1 a_2$ $\quad$ $c_1 d_2 = d_1 c_2$

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

$\|$ $\quad$ $\|$

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

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

$= a_1 d_1 b_2 d_2 + b_1 c_1 b_2 d_2 = b_1 a_2 d_1 d_2 + b_1 b_2 d_1 c_2$

$= (a_2 d_2 + b_2 c_2) b_1 d_1$

∎

Lemma 1 F_D with ops. above is a field.

Proof:

Add identity: $[0,1] = \frac{0}{1}$ since $[a,b]+[0,1] = [a\cdot 1 + b\cdot 0,\ b\cdot 1] = [a,b]$

Add inverse is: $[-a,b]$

Mult inves is $[b,a]$, i.e. $[a,b]\cdot[b,a] = [ab, \cancel{ab}]$ $\rightsquigarrow ab=ab$

$= [1,1]$

etc. ∎

Thm. Let D be an integral domain. D can be imbedded in a field of fractions F_D where and $[a,b] \in F_D$ can be expressed as a

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

Also F_D is unique, ie, if E is any field s.t $D \leq E$ then $\exists$ $\psi : F_D \to E$

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

giving an isomorphism $F_D \cong$ subfield of E

Aside in practice write $\frac{a}{b} \in F_D$, subfield = subring which is a field

Think about $D = \mathbb{Z}$, $F_D = \mathbb{Q}$

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

Proof: First show D can be embedded in F_D

Define a map $\phi : D \to F_D$

$a \mapsto [a,1]$ $(= \frac{a}{1})$

Let $a,b \in D$

ϕ is a hom.

$$\phi(a\cdot b) = [ab,1] = [a,1]\,[b,1] = \phi(a)\phi(b)$$

$$\phi(a+b) = [a+b, 1] = [a,1] + [b,1] = \phi(a)+\phi(b)$$

$\therefore$ ϕ is hom.

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

$$[a,1] = [b,1] \Rightarrow 1\cdot a = 1\cdot b$$
$$\Rightarrow a = b.$$

$\therefore$ D can be imebedden in F_D i.e. $D \cong \phi(D) \leq F_D$

↑ By 1st iso. theorem

Since $\ker(\phi) = \{0\}$

$\phi(D)$ is a subring of F_D.

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

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

$= [a,b]$

$\phi(a)$ = $\dfrac{\phi(a)}{\phi(b)}$

Now Let E be a field, $D \leq E$ (as subring)

$$\psi : F_D \to E$$
$$[a,b] \mapsto ab^{-1}$$

- Show ψ is well defined $[a_1, b_1] = [a_2, b_2]$ $\Rightarrow a_1 b_2 = b_1 a_2$ (By this, in E)

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

$\therefore \psi$ is well defined

· Show ψ is a hom.

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

$$= ab^{-1}cd^{-1}$$

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

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

ψ 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 F_D $\therefore$ ψ is 1-1

$\therefore$ By First isomorphism theorem

$F_D = F_D / \ker \psi \simeq \psi(F_D) \subseteq E$ ← a subfield of E

■

Ex| $\mathbb{Q}[x]$ - is an integral domain

$$\mathbb{Q}(x) = \left\{ \frac{p(x)}{q(x)} \;\middle|\; q(x) \neq 0,\ p(x), q(x) \in \mathbb{Q}[x] \right\}$$

Ex| $\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a,b \in \mathbb{Q} \}$ contains $\mathbb{Z}$

and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$

Coro Let F be a field of characteristic zero. Then F contains a subfield isomorphic to $\mathbb{Q}$.

Coro 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.

Def: A vector space V over a field F is:

- A abelian group V (with addition) with a scalar product αV for $\alpha \in F$, $v \in V$ s.t.:

  $\alpha, \beta \in F$, $v, w \in V$

  - $\alpha(\beta v) = (\alpha\beta)v$
  - $(\alpha+\beta)v = \alpha v + \beta v$
  - $\alpha(v+w) = \alpha v + \alpha w$
  - $1 \cdot v = v$

Ex $\mathbb{R}^n$, $\mathbb{Q}^n$

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

- the vectors in $F[x]$ are polynomials
- vector add is poly. add
- $\alpha f(x)$ ← scalar mult. by field element

[Ex] $C[a,b] = \{ f : [a,b] \to \mathbb{R} \mid f \text{ continuous} \}$

[Ex] $V = \mathbb{Q}(\sqrt{2})$ is a vector space over $\mathbb{Q}$

$u, v \in \mathbb{Q}(\sqrt{2})$

$$u + v = \underbrace{(a + b\sqrt{2})}_{u} + \underbrace{(c + d\sqrt{2})}_{v} = (a+c) + (b+d)\sqrt{2}$$

Proposition Let V be a v. space over F. The following holds:

- $0 \cdot v = 0 \in V \quad \forall\, v \in V,\ 0 \in F$
- $\alpha \cdot 0 = 0 \quad \forall\, \alpha \in F,\ 0 \in V$
- if $\alpha v = 0 \Rightarrow \alpha = 0 \in F$ or $v = 0 \in V$
- $(-1)\, v = -v \quad -1 \in F,\ -v \in V$
- $-(\alpha v) = (-\alpha) v = \alpha (-v)$

Subspaces

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

- $v + w \in W \quad \forall\, v, w \in W$
- $\alpha w \in W \quad \forall\, \alpha \in F,\ w \in W$

Ex $W = \{$ poly in $F[x]$ with no odd powers $\}$

$$= \left\{ \sum_{i=0}^{n} a_i x^{2i} \;\middle|\; n \in \mathbb{Z}_{\geq 0},\ a_i \in F \right\}$$

is a subspace of $V = F[x]$

Def $v_1, \dots, v_n \in V$, $\alpha_1, \dots, \alpha_n \in F$

$$w = \sum_{i=1}^{n} \alpha_i v_i = \alpha_1 v_1 + \cdots + \alpha_n v_n$$

w is a linear combination of $v_1, \dots, v_n$

$$W = \mathrm{Span}_F(v_1, \dots, v_n) = \left\{ \sum_{i=1}^{n} \alpha_i v_i \;\middle|\; \alpha_i \in F \right\}$$

Prop Let $S = \{v_1, \dots, v_n\}$ be vectors in a v. space V

$\mathrm{Span}_F(S)$ is a subspace of V.

Def A set of vectors $v_1, \dots, v_n$ is linearly independent if

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

if and only if $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

Def if there are non-zero α_i's s.t

$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$, then $\{v_1, \dots, v_n\}$ is linearly dependent

Prop Let $\{v_1, \dots, v_n\}$ be a linearly independent set in a V. space V.

Suppose $$\alpha_1 v_1 + \cdots + \alpha_n v_n = \beta_1 v_1 + \cdots + \beta_n v_n,$$

then $\alpha_1 = \beta_1, \dots, \alpha_n = \beta_n$

Proof:

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = \beta_1 v_1 + \cdots + \beta_n v_n$$

$$(\alpha_1 - \beta_1) v_1 + \cdots + (\alpha_n - \beta_n) v_n = 0$$

Since $\{v_1, \dots, v_n\}$ are lin. independent $\Rightarrow \alpha_i - \beta_i = 0$

$\Rightarrow \alpha_i = \beta_i \quad \forall i$, □

Prop $\{v_1, \dots, v_n\}$ are lin. dependent iff some v_i is a lin. combo. of the others.

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

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

Ex $(1,0,0), (0,1,0), (0,0,1)$ is a basis of $\mathbb{R}^3$.

Ex) $\{1, \sqrt{2}\}$ or $\{1+\sqrt{2}, 1-\sqrt{2}\}$ are bases of $\mathbb{Q}(\sqrt{2})$

Prop) If $\{e_1, \dots, e_m\}$, $\{f_1, \dots, f_n\}$ are basis for a v. space V then $m = n$.

Def) If $\{e_1, \dots, e_n\}$ is a basis for a v. space V define the dimension of V:

$$\dim(V) = n.$$

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

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

2) If $S = \{v_1, \dots, v_n\}$ spans V, then S is a basis for V

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

$$\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\} \text{ is a basis for } V.$$

Fields

- when is a field F contained in a larger field?
- 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 $E[x]$.

i.e. all of the roots of $p(x)$ are in E.

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

$= (x^2-2)(x^2-3)$

$\therefore$ p has no zeros in $\mathbb{Q}$, 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 <u>extension field</u> of a field F if F is a subfield of E. F is called the base of E. Write $F \subset E$

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

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

E is an extension field of F

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