Section 21 - Field of quotients.

Let R be a ring.

R a field $\Longrightarrow$ R an integral domain.

$\Longleftarrow$

E.g. $\mathbb{Z}$ is an integral domain, not a field, & not all $a \in \mathbb{Z}^*$ have multiplicative inverses.

$\mathbb{Z}$ is subring of $\mathbb{Q}$, and $\mathbb{Q}$ is a field.

"Useful", e.g. can analyse equations

$f(x) = 0$ $\quad x \in \mathbb{Z}$

by first finding solutions in $\mathbb{Q}$, then checking if $x \in \mathbb{Z}$.

$2x - 3 = 0$

$\Updownarrow$

$x = \frac{3}{2} \notin \mathbb{Z}$.

Today: Any integral domain D is a subring of a field F, where elements of F are $\frac{a}{b}$ $a, b \in D$.

of the form

Let D be an integral domain, our mission to construct F

Keep example $D = \mathbb{Z}$, $F = \mathbb{Q}$ in mind.

Step 1: Define F as a set.

Attempt 1: $(F =) D \times D = \{(a,b) \mid a, b \in D\}$ $\quad \left((a,b) \longleftrightarrow \frac{a}{b}\right)$

Problem: Don't want $(a, 0)$, since "$\frac{a}{0}$" should not be defined.

Attempt 2: $(F=)\{(a,b) \mid a \in D,\ b \in D \setminus \{0\}\} = S$.

Problem: In $\mathbb{Q}$ have multiple ways of representing a number,

$$\frac{2}{3} = \frac{4}{6} = \frac{6}{9} \ \cdots$$
$$\updownarrow \qquad \updownarrow \qquad \updownarrow$$
$$(2,3) \quad (4,6) \quad (6,9), \ldots$$

Must consider $(2,3), (4,6), \ldots$ the same element.

Def $(a,b), (c,d) \in S$ are equivalent, write $(a,b) \sim (c,d)$, if $ad = bc$.

E.g. $D = \mathbb{Z}$, $(2,3) \sim (4,6)$ since $(2)(6) = (3)(4)$.

Lemma $\sim$ is an equivalence relation

Proof: Reflexive: $(a,b) \sim (a,b)$ $\quad ab = ba$ ✓

Symmetric: $(a,b) \sim (c,d)$: $\quad ad = bc$
$\Updownarrow \qquad\qquad\qquad \Updownarrow$
$(c,d) \sim (a,b)$: $\quad cb = da$

Transitive: Assume $(a,b) \sim (c,d)$ $\quad (c,d) \overset{*}{\sim} (r,s)$.

Want $(a,b) \sim (r,s)$.

$$(a,b) \sim (c,d) \Longrightarrow ad = bc$$
$$\Longrightarrow asd = bcs$$
$$\overset{(*)}{\Longrightarrow} asd = brd$$
$$\overset{d \neq 0 \ \&\ D \text{ is I.D.}}{\Longrightarrow} as = br.$$
$$\Longrightarrow (a,b) \sim (r,s).$$

(*) $(c,d) \sim (r,s)$ gives $cs = rd$

Get equivalence classes for $\sim$ in S.

Write $[(a,b)]$ for equivalence class of (a,b).

$F = \{$Equivalence classes of $\sim$ in $S\}$.

Step 2: Define addition & multiplication on F, by

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$$

$$[(a,b)][(c,d)] = [(ac, bd)].$$

Lemma: This is well-defined.

E.g. If $(a_1, b_1) \sim (a_2, b_2)$, $(c_1, d_1) \sim (c_2, d_2)$, then

$$(a_1 d_1 + b_1 c_1, b_1 d_1) \sim (a_2 d_2 + b_2 c_2, b_2 d_2)$$

and $(a_1 c_1, b_1 d_1) \sim (a_2 c_2, b_2 c_2)$.

Step 3: Check that F is a field.

E.g.
- $(F, +)$ is abelian group, $[(0,1)]$ is identity
  $-[(a,b)] = [(-a, b)]$
- Multiplication is associative & commutative
- Distributive laws hold
- F has unity $[(1,1)]$
- If $[(a,b)] \neq [(0,1)]$ then $a \neq 0$, and
  $[(a,b)]^{-1} = [(b,a)]$.

Step 4: F contains "a copy of" D.

Let $i : D \longrightarrow F$ be given by

$i(a) = [(a,1)]$.

Thm i is a ring homomorphism and gives an isomorphism of D with a subring of F.

Proof $a, b \in D$ $\quad i(a)+i(b) = [(a,1)]+[(b,1)] = [(a1+1b,(1)(1))] = [(a+b,1)]$

$$= i(a+b)$$

$$i(a)\,i(b) = [(a,1)][(b,1)] = [(ab,(1)(1))] = [(ab,1)] = i(ab).$$

i is one-to-one: $i(a) = i(b)$

$$\Downarrow$$

$$[(a,1)] = [(b,1)]$$

$$\Downarrow$$

$$a1 = 1b$$

$$\Downarrow$$

$$a = b.$$

Hence $i : D \longrightarrow i[D] \leq F$ is an isomorphism.

Note Every element $[(a,b)] \in F$ is ~~whatever~~ of the form

$$i(a)/i(b) = [(a,1)][(b,1)]^{-1} = [(a,1)][(1,b)] = [(a,b)].$$

Def ~~A field F containing~~ A field F is a field of quotients for an integral domain D if

(1) $\exists$ ring homomorphism $i : D \longrightarrow F$ ~~such~~ giving ~~a~~ isomorphism $D \simeq i[D]$

(2) Every ~~$x \in F$~~ $x \in F$ is of the form

$$x = i(a)/i(b)$$

for some $a, b \in D$.

Often say "F contains D".

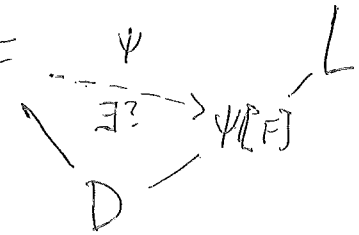
A Field of fractions is unique.

Let D be an integral domain, F a field of quotients and L a field containing D.

Example $D = \mathbb{Z}$, $F = \mathbb{Q}$, $L = \mathbb{R}$.

Thm There exists a one-to-one homomorphism $\psi : F \to L$ such that $\psi(a) = a$ for all $a \in D$.

Proof



Write $a/_F b$ & $a/_L b$ for $a, b \in D$ & their fractions in F (resp. L).

F is field of fractions $\Longrightarrow$ every $x \in F$ is of form $x = a/_F b$ $a, b \in D$.

Define $\psi : F \to L$ by

$$\psi(a/_F b) = a/_L b.$$

Check well-defined:

$$\begin{array}{c} a_1/_F b_1 = a_2/_F b_2 \\ \Downarrow \\ a_1 b_2 = a_2 b_1 \\ \Downarrow \\ a_1/_L b_1 = a_2/_L b_2 \\ \Downarrow \\ \psi(a_1/_F b_1) = \psi(a_2/_F b_2). \end{array}$$

Check also ring homomorphism + one-to-one.

Corollary Any field containing an integral domain D contains a field of fractions of D

Corollary Any two fields of fractions of an integral domain are isomorphic.

Examples • $D = \mathbb{Z}[\frac{1}{2}] = \left\{ \frac{k}{2^n} \mid k \in \mathbb{Z},\ n \geq 0,\ n \in \mathbb{Z} \right\}$

D is an integral domain.

$D < \mathbb{Q}$, and every $\frac{a}{b} \in \mathbb{Q}$ is a fraction of elements of $D \Longrightarrow \mathbb{Q}$ is a field of fractions for D.

• $D = \mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \} < \mathbb{C}$.

Field of fractions is

$$F = \left\{ \frac{a+bi}{c+di} \mid a, b, c, d \in \mathbb{Z} \quad c + di \neq 0 \right\} < \mathbb{C}.$$

Section 22 - Rings of polynomials

Let R be a ring.

Naively, "polynomial with coefficients in R" means some expression

$$a_0 + a_1 x + \cdots + a_n x^n,$$

where the $a_i \in R$.

Note: A polynomial is not "a special kind of function", really just formal expression. The symbol x does not represent an element of R.

Proper definition: A polynomial $f(x)$ with coefficients in R is an infinite formal sum

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots \qquad a_i \in R$$

such that only finitely many $a_i \neq 0$.

- The a_i are coefficients of $f(x)$
- Degree of $f(x) = \begin{cases} \text{undefined if all } a_i = 0 \\ \text{otherwise} = \text{biggest } i \text{ s.t. } a_i \neq 0. \end{cases}$
- If degree of $f(x)$ is n, have

  $$f(x) = a_0 + a_1 x + \cdots + a_n x^n + 0x^{n+1} + 0x^{n+2} + \cdots,$$

  write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$.
- Write x^i for $1x^i$, & leave out $0x^i$.
- E.g. $f(x) = 2 + 1x + 0x^2 + 1x^3 + 0x^4 + 0x^5 + \cdots$

  $= 2 + x + x^3$.

Define addition, $f(x) = \sum_{i=0}^{\infty} a_i x^i \quad g(x) = \sum_{i=0}^{\infty} b_i x^i$

$$f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i.$$

Define multiplication

$$f(x)g(x) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i$$

These are the same formulas which hold for "ordinary" real polynomials.

<u>Thm</u> The set $R[x]$ of all polynomials with coefficients in R is a ring with the above operations.

R commutative $\Longrightarrow R[x]$ commutative

R has unity $1 \Longrightarrow R[x]$ has unity

$$1 = (1 + 0x + 0x^2 + \cdots).$$

<u>Proof omitted.</u>

<u>Example</u>: • Consider $\mathbb{Z}_2[x]$. Here

$$(1 + x) + x = (1 + 0) + (1 + 1)x = 1$$

$$(1+x)(1+x) = (1)(1) + \big((1)(1) + (1)(1)\big)x + \big((1)(1)\big)x^2$$

$$= 1 + 0x + x^2 = 1 + x^2.$$

• In $\mathbb{Z}_4[x]$

$$(1 + 2x)(1 + 2x) = 1 + \big((2)(2) + (2)(2)\big)x + (2)(2)x^2$$

$$= 1 + 0x + 0x^2 = 1.$$

Polynomials in more than one indeterminate

Thm D is an integral domain $\Longrightarrow D[x]$ is an integral domain.

Special case: F a field $\Longrightarrow F[x]$ is an integral domain.

$F[x]$ **not** a field, x is not a unit.

Example: $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_p[x]$ are integral domains.

If F is a field, write $F(x)$ for the field of fractions of $F[x]$, called the **field of rational functions over F.**

E.g. $\dfrac{a_0 + \cdots + a_n x^n}{b_0 + \cdots + b_m x^m}$, with $a_i, b_i \in \mathbb{Q}$.

Elements of $\mathbb{Q}(x)$ are

Evaluation homomorphisms

Let $F \leq E$ be fields, $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$

"solve equation $f(x) = 0$" in E, i.e. find $\alpha \in E$ such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$.

E.g. $F = \mathbb{Q}$, $E = \mathbb{R}$ or $\mathbb{C}$, $f(x) = x^2 + 1$ no solutions if $E = \mathbb{R}$, solutions $\pm i$ if $E = \mathbb{C}$.

Thm Let $F \leq E$ be fields, let $\alpha \in E$. The map $\phi_\alpha : F[x] \longrightarrow E$ given by

$$\phi_\alpha(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

is a homomorphism.

Partial proof $\phi_\alpha(f(x))\phi_\alpha(g(x)) = \phi_\alpha(f(x)g(x))$

Let $f(x) = a_0 + \cdots + a_n x^n$, $g(x) = b_0 + \cdots + b_m x^m$.

$$LHS = (a_0 + a_1\alpha + \cdots + a_n\alpha^n)(b_0 + b_1\alpha + \cdots + b_m\alpha^m)$$

$$= a_0b_0 + (a_1b_0 + a_0b_1)\alpha + \cdots + a_nb_m\alpha^{m+n}$$

$$RHS = \phi_\alpha(f(x)g(x)) = \phi_\alpha(a_0b_0 + (a_1b_0 + a_0b_1)x + \cdots + a_nb_m x^{m+n})$$

$$= a_0b_0 + (a_1b_0 + a_0b_1)\alpha + \cdots + a_nb_m\alpha^{m+n}.$$

□

Example: For $0 \in E$, $f(x) = a_0 + \cdots + a_n x^n$, get

$$\phi_0(f(x)) = a_0 + a_1 0 + a_2 0^2 + \cdots + a_n 0^n$$

$$= a_0.$$

Example: For $f(x) = x^2 + 1 \in \mathbb{Q}[x]$, $i \in \mathbb{C}$, $\phi_i : \mathbb{Q}[x] \to \mathbb{C}$ gives

$$\phi_i(f(x)) = 1 + i^2 = 1 + (-1) = 0.$$

$\Longrightarrow x^2 + 1 \in \ker \phi_i$.

Example: $F = \mathbb{Q}$, $E = \mathbb{R}$, $e \in \mathbb{R}$. It's known that

$$a_0 + a_1 e + \cdots + a_n e^n = 0 \qquad a_i \in \mathbb{Q}$$

$$\Downarrow$$

all $a_i = 0$.

This means that for $\phi_e : \mathbb{Q}[x] \to \mathbb{R}$, $\phi_e(f(x)) = 0 \Rightarrow f(x) = 0$.

Hence $\ker \phi_e = \{0\}$, so ϕ_e is injective.

$$\phi_e[\mathbb{Q}[x]] < \mathbb{R}.$$

Definition Let $F \leq E$ be fields, $\alpha \in E$, $f(x) \in F[x]$.

Say Write $f(x) = \phi_\alpha(f(x)) \in E$, say α is **a zero of $f(x)$** if

$$f(\alpha) = 0.$$

Basic goal: Given field F, $f(x) \in F[x]$, find an extension $E \geq F$ s.t. $\exists\, \alpha \in E$, $f(\alpha) = 0$.

Basic strategy & example: $F = \mathbb{Q}$, $f(x) = x^2 - 2$ has no zeros in $\mathbb{Q}$. Construct new field

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

containing a zero of $f(x)$.