Abstract Algebra
Review

Rings

Def: Rings

$(R, \times, +)$ where R is a set, $+$ and $\times$ are binary operations s.t

(1) $(R, +)$ is an abelian group

(2) $\times$ is associative $\quad a(bc) = (ab)c$

(3) Distributivity:

$$(a+b)c = ac + bc$$
$$a(b+c) = ab + ac$$

Def: Commutative Rings

Rings s.t multiplication is commutative

ie $\quad ab = ba$

Examples

(1) Rings without identity:

→ $2\mathbb{Z}$ as 1 is not even

(2) Commutative rings:

→ $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

→ $\mathbb{Z}/n\mathbb{Z}$

(3) Any group can be turned into a ring by defining $xy = 0 \quad \forall x, y \in R$ } Trivial ring

(4) Ring of functions: for any $X \neq \emptyset$ and any ring A, the set of functions

$$f: X \longrightarrow A$$

is a ring with operations

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)\,g(x)$$

This ring is commutative iff A is

This ring has 1 iff A has.

Def : Division Ring

A ring R with identity 1 s.t

(1) $1 \neq 0$

(2) every $a \in R$ s.t $a \neq 0$ has an inverse a^{-1} s.t $aa^{-1} = a^{-1}a = 1$

Def : Field

A field is a commutative, division ring

Proposition (Immediate properties of rings)

For any ring R

(1) $0r = r0 = 0, \quad \forall r \in R$

(2) $(-r)s = r(-s) = -(rs), \quad \forall r, s \in R$

(3) $(-r)(-s) = rs, \quad \forall r, s \in R$

(4) if $1 \in R$, then 1 is unique and $-r = (-1)r, \quad \forall r \in R$

Proposition

A finite division ring is a field.

Def : Zero divisor

Let R be a ring. Let $r \neq 0$
Then r is a zero divisor if $\exists s \in R, s \neq 0$ s.t $rs = 0$ or $sr = 0$

Def : Unit

Let R be a ring with identity 1.
Then $r \in R$ is called a unit if $\exists s \in R$ s.t $rs = sr = 1$

Def : $R^\times$

$R^\times$ is the set of units in a ring R,
$(R^\times, \times)$ is a group under multiplication called the group of units.

Proposition

→ If $r \in R$ is a zero-divisor, then r is not a unit
If $r \in R$ is a unit, then r is not a zero divisor.

→ fields have no zero divisors.

Def: Integral Domain

An Integral Domain (ID) is a commutative ring with $1 \in R$ s.t it has no zero divisor.

Properties of ID

(1) Cancellation laws hold i.e
if $a, b, c \in R$ s.t a is not a zero divisor
→ if $ab = ac$, then either $a = 0$ or $b = c$

In an integral domain if $ab = ac$, then $a = 0$ or $b = c$.

Proposition

Any finite integral domain is a field.

Proof: we only need to show, $\forall x \neq 0. \exists x^{-1}$
Define for a fixed $a \neq 0$, $\varphi : R \longmapsto R$ s.t $\varphi(x) = ax$
Then, this is injective by cancellation law. Since R is finite & φ is injective, φ is surjective. $\therefore \exists r$ s.t $\varphi(r) = ar = 1$
$\therefore r = a^{-1}$.

Def: Subring

A subring of ring R is a subgroup $P \subset R$
s.t
(i) P is closed under multiplication

Def: Polynomial Rings

Let R be a commutative ring with identity 1.
Let x be an indeterminate.
Then, $R[x]$ is a ring of polynomials

$$R[x] = \left\{ \sum_{i=1}^{n} a_i x^i \;\middle|\; n \geq 0,\ a_i \in R \right\}$$

$R[x]$ is a commutative ring with identity 1.

→ If $a_n \neq 0$, then the degree of the polynomial is n

→ If $a_n = 1$, then this is called a monic polynomial

→ $R \subset R[x]$ is the set of constant polynomials

→ If S is a subring of R,
then $S[x]$ is a subring of $R[x]$.

Proposition: (Properties of polynomial rings)

If R is an I.D. and $p(x), q(x) \in R[x]$
s.t $p(x) \neq 0$, $q(x) \neq 0$.
then,

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$
(2) the units of $R[x]$ are the same as the units of R.
(3) $R[x]$ is an integral domain.

Ring homomorphism (or ring morphism)

Def : Ring morphism

Let R, S be rings.
A ring morphism $\varphi : R \longrightarrow S$
satisfies (1) $\varphi(a+b) = \varphi(a) + \varphi(b)$
(2) $\varphi(ab) = \varphi(a)\varphi(b)$

Def : Ring isomorphism

A ring morphism $\varphi : R \longrightarrow S$ s.t φ is bijective.

Idials

Def: Idials

Let R be a ring.
Let $r \in R$ and let $I \subset R$
Define $rI := \{ ri \mid i \in I \}$
$Ir := \{ ir \mid i \in I \}$

Then,

(1) A subset $I \subset R$ is a right ideal of R if (a) I is a subring of R and
(b) $Ir \subseteq I$ for any $r \in R$.

(2) A subset $I \subset R$ is a left ideal of R if (a) I is a subring of R and
(b) $rI \subseteq I$ for any $r \in R$

(3) If I is both a left ideal and right ideal, then I is called an ideal of R

→ $I \trianglelefteq R$ if $rI \subset I$, $Ir \subset I$ for any $r \in I$
and I is a subring

Def: Quotient Rings

Let $I \trianglelefteq R$
Then R/I is a quotient ring:

$$R/I = \{ r+I \mid r \in R \} \Big/ (r+I = s+I \text{ if } r-s \in I)$$

The operations are defined below

↓

→ If $I \subset R$ is a subgroup s.t

$$\begin{bmatrix} (r+s)+I = (r+I)+(s+I) \\ rs+I = (r+I)(s+I) \end{bmatrix} \leftarrow \text{these operations are well-defined,}$$

then I is an ideal of R

If I is an ideal of R, then under these binary operations, ~~properties are satisfied.~~ R/I is a ring

Proposition (Isomorphism Theorems for Rings)

(1) (First Isomorphism Theorem for Rings)
If $\varphi : R \to S$ is a ring morphism,
then $\ker \varphi$ is an ideal of R
$\operatorname{Im} \varphi$ is a subring of S
$R/\ker \varphi \cong \varphi(R)$

(2) If I is an ideal of R, then the map $R \longrightarrow R/I$
defined by $r \longrightarrow r+I$
is a surjective ring morphism with kernel I.
This is called the natural projection of R onto R/I.

(3) Every ideal is the kernel of a ring morphism
(and vice-versa)

(4) (Second Isomorphism Theorem for Rings)
Let $A \subset R$ be a subring
Let $B \lhd R$
Then, $A+B = \{a+b \mid a \in A, b \in B\} \subset R$
$A \cap B \lhd A$
$(A+B)/B \cong A/(A \cap B)$

(5) Third Isomorphism Theorem for Rings
Let I and J be ideals i.e. $I \lhd R, J \lhd R$
and let $I \subseteq J$
Then, $J/I \lhd R/I$
$(R/I)/(J/I) \cong R/J$

(6) Lattice Isomorphism Theorem for Rings

(a) Let $I \lhd R$
Then, the correspondence $A \longleftrightarrow A/I$ (where $I \subset A \subset R$)
is an inclusion-preserving bijection between the
set of subrings of R that contain I
and the set of subrings of R/I.
↳ Meaning: Let $A \subseteq B$, $I \subset A$, $I \subset B$
Then $A/I \subseteq B/I$
if $J \subseteq K$ s.t. $J \lhd R$, $K \lhd R$, $I \subset J$, $I \subset K$
Then $J/I \subseteq K/I$

(b) $I \subset A \subset R$, A subring is
Then, $A \lhd R$ iff $A/I \lhd R/I$.

Special Ideals

Proper Ideals

Def: Proper ideal

$I \lhd R$ is proper if $I \neq R$

Proposition

Let $I \lhd R$ where R is a ring with 1.

(1) $I = R$ if and only if $1 \in I$

(2) If R is commutative, then R is a field iff its only ideals are $\{0\}$ and R.

Proof:

(1) Suppose $I = R$, then we are done
Suppose $1 \in I$. Since it is an ideal $Ir \subset I$, $rI \subset I$, $\forall r$.
So, $R \subset I$

(2) Suppose R is a field.
Let $r \in R$. Then $\exists r^{-1}$. If $I \lhd R$, $rI \subset I$
So, if $x \in I$
then $x^{-1}x = 1 \in I$
So, $I = R$
If only $0 \in I$, then $I = \{0\}$.

Same proof for reverse direction.

Proposition: If R is a field, then any non-zero morphism $\varphi : R \to S$ is an injection

Ideals generated by a set

Let R be a ring with 1.
Let $A \subset R$ be a subset

(1) $(A) \lhd R$ is the smallest ideal of R containing A.
called the ideal generated by A

$$(A) = \bigcap_{(I \lhd R, A \subseteq I)} I$$

(2) $RA := \{\sum_i r_i a_i \mid r_i \in R, a_i \in I, n \in \mathbb{N}^+\}$
RA is the left ideal generated by A
AR is the right ideal generated by A
RAR is the ideal generated by A.
If R is commutative, $RA = AR = RAR. = (A)$

(3) A finitely generated ideal is an ideal generated by a finite set.

Principal ideals

Principal ideals are $I \triangleleft R$ s.t $I = (r)$ where $r \in R$ a fixed single element.

Maximal Ideals

Def: Maximal Ideal

Let R be a ring with $1 \in R$.
$M \triangleleft R$ is maximal if (1) $M \neq R$
(2) the only ideals containing M are M and R.

Proposition:

In a ring with $1 \in R$, every proper ideal I is contained in a maximal ideal M
$I \subset M$.

Proposition:

R commutative, with $1 \in R$
Then $M \triangleleft R$ is maximal if and only if R/M is a field.

Prime Ideal

Def: Prime Ideal

Suppose R is a commutative ring with $1 \in R$.
$P \triangleleft R$ is called prime if (1) $P \neq R$
(2) $xy \in P \Rightarrow x \in P$ or $y \in P$.

Proposition

R commutative, with $1 \in R$
$P \underset{\text{prime}}{\triangleleft} R \iff R/P$ is an integral domain

Proposition

R is commutative. Then $M \underset{\text{maximal}}{\triangleleft} R \Rightarrow M \underset{\text{prime}}{\triangleleft} R$

Rings of fractions
Fields of fractions

Def: Ring of fractions / Field of fractions

$R \longrightarrow$ commutative ring

$D \subset R$ s.t (1) $D \neq \phi$

(2) $0 \notin D$

D contains no zero divisors

(3) D is closed under multiplication

Then, $D^{-1}R$ is a commutative ring with $1 \in D^{-1}R$

s.t (1) $R \subset D^{-1}R$

(2) any $d \in D$ is a unit in $D^{-1}R$

(3) any $x \in D^{-1}R$ is of the form

$$x = \frac{r}{d}, \quad r \in R, d \in D$$

If $D = R - \{0\}$, then $D^{-1}R$ is called the a field of fractions or quotient field.

↓ better definition

Def: Multiplicative Subset

D is a multiplicative subset of a ring R if (1) $1 \in D$

(2) D is closed under multiplication

Def: Ring of fractions

$D^{-1}R = \left\{ \frac{r}{d} \mid r \in R, d \in D \right\}$ with the equivalence relation

$$\frac{r_1}{d_1} = \frac{r_2}{d_2} \quad \text{iff} \quad f(r_1 d_2 - r_2 d_1) = 0 \text{ for some } f \in D.$$

→ Canonical map: $R \longrightarrow D^{-1}R$ by $a \longrightarrow \frac{a}{1}$

→ If $0 \in D$, then $D^{-1}R = \{0\}$, the zero ring.

Examples of rings of fractions

(1) $A_f = S^{-1}A$ where $S = \{1, f, f^2, \dots\}$

Note:

$$\boxed{A_f \longleftrightarrow A[x]/(fx-1)}$$

Proof:

Suppose $\frac{a}{f^n} \in A_f$.

Let $u = \bar{x} \in A[x]/(fx-1)$

Then map $\frac{a}{f^n} \longrightarrow au^n$

This is well-defined: if $\frac{a}{f^n} = \frac{b}{f^m} \in A_f$

then $f^k(af^m - bf^n) = 0$

Then, using that $fu = 1$, can show $au^n = bu^m$.

Map $\varphi : A[x]/(xf-1) \longrightarrow A_f$

by $\varphi(x) = \frac{1}{f}$, $\varphi(a) = \frac{a}{1}$

Note $\varphi(xf-1) = \frac{1}{f}\cdot\left(\frac{f}{1}\right) - 1 = 0$

Easy to show they are inverses.

(2) $A_p = S^{-1}A$ where $S = A - p$ for some prime ideal $p \underset{\text{prime}}{\lhd} A$.

(3) $K(A) = S^{-1}A$ where $S = A - \{0\}$ and A is an I.D.,

↳ fraction field.

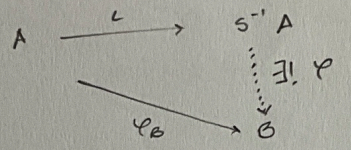
Proposition (Universal property of the ring of fractions)

Let B be an A-algebra s.t $\varphi_B : A \longrightarrow B$

satisfies $\varphi_B(A) \subset B^\times$

Let $\iota : A \longrightarrow S^{-1}A$ be the canonical map

Then, $\exists!$ $\varphi : S^{-1}A \longrightarrow B$ s.t $\varphi_B = \varphi \circ \iota$



Proof:

Let $\varphi : S^{-1}A \longrightarrow B$ by $\varphi\left(\frac{a}{s}\right) = \varphi_B(a)\,\varphi_B(s)^{-1}$

→ well-definedness

Suppose $\frac{a}{s} = \frac{a'}{s'} \Rightarrow t(as' - a's) = 0$ for some $t \in S$

Then $\varphi\left(\frac{a}{s}\right) = \varphi_B(a)\,\varphi_B(s)^{-1}$. $\varphi\left(\frac{a'}{s'}\right) = \varphi_B(a')\,\varphi_B(s')^{-1}$

Now $\varphi_B(t)\left(\varphi_B(a)\varphi_B(s')^{-1} - \varphi_B(a')\,\varphi_B(s)^{-1}\right) = 0$

since φ_B is a morphism & $t(as' - a's) = 0$

Since $\varphi_B(t)$ is a unit in B (by def.), we cancel it.

Then, $\varphi_B(a)\,\varphi_B(s') = \varphi_B(a')\,\varphi_B(s)$

$\varphi_B(a)\,\varphi_B(s)^{-1} = \varphi'_B(a')\,\varphi_B(s')^{-1}$

→ Check ring homomorphism

→ Uniqueness:

Let $\Psi : S^{-1}A \longrightarrow B$ be another A-algebra morphism satisfying this

Then, for $s \in S$,

$\varphi_B(s) = (\Psi \circ \iota)(s) = \Psi\left(\frac{s}{1}\right)$

Now, $\Psi\left(\frac{s}{1}\right)$ must be the inverse of $\Psi(s)$.

So, $\Psi\left(\frac{a}{s}\right) = \Psi\left(\frac{a}{1} \cdot \frac{1}{s}\right) = \Psi\left(\frac{a}{1}\right)\Psi\left(\frac{1}{s}\right)$

$= \varphi_B(a)\,\varphi_B(s)^{-1}$

$= \varphi\left(\frac{a}{s}\right)$

Euclidean Domains (ED)

Def: Norm

Any function $N: R \longrightarrow \mathbb{Z}^+ \cup \{0\}$

with $N(0) = 0$ is called a norm on the integral domain R.

— if $N(a) > 0 \quad \forall a \neq 0$, then N is called a positive norm.

Def: Euclidean Domains

An ID R is called a Euclidean domain if $\exists$ a norm N on R s.t $\forall a, b \in R$ with $b \neq 0$, $\exists q, r \in R$ s.t

(1) $a = bq + r$ (quotient, remainder)

(2) $r = 0$ or $N(r) < N(b)$

Examples of Euclidean Domain

(1) All fields

(2) $\mathbb{Z}$ with $N(a) = |a|$

(3) If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain with $N(p(x)) = \deg p(x)$

Proposition

Euclidean Domains are Principal Ideal Domains

Principal Ideal Domains (PIDs)

Def: PID

A PID is an ID in which every ideal is principal
(i.e. $I \lhd R \Rightarrow I = (x)$ for some $x \in R$)

Examples:

(1) $\mathbb{Z}$

Proposition:

Let R be a PID. Let $a, b \in R$ s.t $a \neq 0, b \neq 0$,
Let d be a generator for the ideal (a, b)
Then
(1) $d = \gcd(a, b)$
(2) $d = ax + by$ for some $x, y \in R$
(3) d is unique up to multiplication by a unit of R.

Proposition:

Every non-zero prime ideal in a PID is a maximal ideal.

Corollary:

If R is a commutative ring s.t $R[x]$ is a PID or ED,
then R is a field.

Irreducible elements, Prime Elements

Def: Irreducible, Prime, Associate

Let R be an I.D.

(1) Let $x \in R$ s.t. x is not a unit.
Then, x is irreducible $\iff$ $x = ab$ implies either a is a unit or b is a unit.

(2) Let $x \in R$, $x \neq 0$.
Then, x is called prime if the ideal (x) is prime.

$\Updownarrow$ equivalently

$x \neq 0$ is prime if it is not a unit and whenever x divides ab, either x divides a or x divides b.

(3) $x \in R$ and $y \in R$ are associate if $x = uy$ for some unit $u \in R$.

Proposition:
In an I.D., a prime element is always irreducible.

Proposition:
In a P.I.D., a non-zero $x \in R$ is a prime if and only if it is irreducible.

Unique Factorization Domain (UFD)

Def: Unique factorization Domain (UFD)

A UFD is an ID, R, s.t $\forall x \in R$, x not a unit:

(1) x is a finite product of irreducibles:

$$x = p_1 p_2 \cdots p_r$$

(2) This decomposition is unique up to associates i.e

if $x = p_1 p_2 \cdots p_r$

$x = q_1 q_2 \cdots q_m$

then $r = m$ and, after renumbering, p_i is associate to q_i, $\forall i$.

Examples

(1) All fields are UFDs.

(2) If F is a UFD, then $F[x]$ is a UFD.

Proposition

In a UFD, $x \neq 0$ is a prime iff x is an irreducible

Proposition:

Let $a \neq 0$, $b \neq 0$ in a UFD. Let $a = u p_1^{e_1} \cdots p_n^{e_n}$

and $b = v p_1^{f_1} \cdots p_n^{f_n}$

be the prime factorizations of a and b. (here u, v are units)

and $e_1, \ldots, e_n, f_1, \ldots, f_n \geq 0$

Then, $d = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)} = \gcd(a, b)$

Proposition:

Every P.I.D is a UFD

$\therefore$ Every E.D is a UFD.

Localisation

Let R be a commutative ring with $1 \in R$.

Def: Multiplicative Subset

$D \subset R$ is a multiplicative subset if

(1) $1 \in D$

(2) D is closed under multiplication

Note: we allow $0 \in D$.

Examples of multiplicative subsets

(1) $I \underset{\text{prime}}{\lhd} R$. Then $R - I$ is a multiplicative subset.

↳ prime ideals are proper so $R - I \ni 1$.

Also, ~~$ab \in R \setminus I$~~ $\Rightarrow a \notin I, b \notin I \Rightarrow ab \notin I$. as I is prime

(2) $\{1, d, d^2, d^3, \ldots\} \subset R$ for some $d \in R$

(3) $N = \{a \mid a \in R, a \text{ is not a zero divisor}\} \subset R$

↳ $1 \in N$ as 1 is not a zero-divisor

xy is also a non-zero divisor if x and y are.

Def: Localisation of R at D

Let R be a commutative ring with $1 \in R$.

Let $D \subset R$ be a multiplicative subset.

Define $D \times R$ with the equivalence relation:

$(d, a) \sim (d', a')$ if $f(da' - ad') = 0$ for some $f \in D$.

Then, $D^{-1}R$ is the localisation of R at D:

$$D^{-1}R = \left\{ \underbrace{[(d,a)]}_{\text{equivalence class of } (d,a)} =: \frac{d}{a} \;\middle|\; (d,a) \in D \times R/\sim \right\}$$

with $0 = \frac{0}{1}$, $1 = \frac{1}{1}$, $\frac{ab}{de} = \frac{a}{d} \cdot \frac{b}{e}$, $\frac{a}{d} + \frac{b}{e} = \frac{ae + bd}{de}$

→ $D^{-1}R$ is a ring

→ Canonical ring morphism: $\iota : R \longrightarrow D^{-1}R$

by $\iota(a) = \frac{a}{1}$

Note: $\iota(D) \subset (D^{-1}R)^\times$ as $\iota(d) = \frac{d}{1}$ has the inverse $\frac{1}{d}$

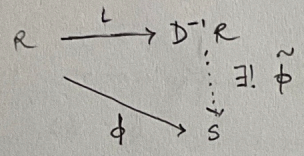
Proposition

Let $\phi : R \longrightarrow S$ be a ring morphism

Let $D \subset R$ be a multiplicative subset.

Suppose, $\phi(D) \subset S^\times$

Then, $\exists!\ \tilde{\phi} : D^{-1}R \longrightarrow S$ s.t $\phi = \tilde{\phi} \circ L$



Proof :

(check review notes)

Examples of localisations

(1) $\mathbb{Q} = (\mathbb{Z} - \{0\})^{-1}\mathbb{Z}$

(2) $(\mathbb{Z} - (p))^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}$ where p is a prime

(3) $\{1, d, d^2, d^3, \dots\}^{-1}\mathbb{Z} = \left\{ \frac{a}{d^n} \in \mathbb{Q} \mid a \in \mathbb{Z},\ n \in \mathbb{Z}_{\geq 0} \right\}$

(4) $\left(\mathbb{C}[x,y] - (x,y)\right)^{-1}\mathbb{C}[x,y] = \left\{ \frac{f}{g} \mid f, g \in \mathbb{C}[x,y],\ g(0,0) \neq 0 \right\}$

Proposition (Immediate properties)

(1) $0 \in D \iff D^{-1}R = \{0\}$

(2) $R \longrightarrow D^{-1}R$ is injective $\iff$ D contains no zero divisors

(3) If $D \subset R^\times$, then $D^{-1}R = R$

Proof:

(1) Suppose $0 \in D$,
Then, for any $\frac{a}{b} \in D^{-1}R$, $\frac{a}{b} = \frac{0}{f}$

as $0 \cdot (af - 0b) = 0$

Suppose $\{0\} = D^{-1}R$
Then, consider $\frac{a}{b}$ which must be equal to $\frac{0}{1}$
let $a \neq 0$.
So, $f(a - 0) = 0$ for some $f \in D$.
Then, either $a = 0$ or $0 \in D$.
But if $a = 0$, this same argument applies
↓ show all $a \in D$ and $a = 0$.

(2) Suppose $\iota : R \longrightarrow D^{-1}R$ is injective
Suppose D contains zero divisors x and y.
let $y = a - a'$ where $a \neq a'$ as $y \neq 0$.
Then, $x(a - a') = 0$
$x(a \cdot 1 - a' \cdot 1) = 0$
$\Rightarrow \frac{a}{1} = \frac{a'}{1}$ even though $a \neq a'$
which contradicts injectivity

(3) Suppose $D \subset R^\times$. Use the universal property

$$\begin{array}{ccc} R & \xrightarrow{\iota} & D^{-1}R \\ & \searrow^{id_R} & \downarrow \exists! \tilde{\phi} \\ & & R \end{array}$$

note that $id_R(D) = D \subset R^\times$

Then $\tilde{\phi} \circ \iota = id_R$ for some unique $\tilde{\phi}$.
Define $\tilde{\phi}\left(\frac{a}{d}\right) = ad^{-1}$.
→ Note that $\tilde{\phi}$ is surjective as for any $r \in R$,

$$\tilde{\phi}\left(\frac{r}{1}\right) = r$$

Now, note that $\tilde{\phi} \circ \iota = id_R$.
On the other hand $\iota \circ \tilde{\phi} = id_{D^{-1}R}$ because:

$$\begin{array}{ccc} R & \xrightarrow{\iota} & D^{-1}R \\ & \searrow^{\iota} & \downarrow \iota \circ \tilde{\phi} \\ & & D^{-1}R \end{array}$$

as $\iota \circ \tilde{\phi} \circ \iota = \iota \cdot id_R = \iota$
and $\iota(D) \subset D^{-1}R$
By uniqueness in the universal property

$$\iota \circ \tilde{\phi} = id_{D^{-1}R}.$$

So, $\tilde{\phi}$ is an isomorphism.

Proposition

(1) If R is an I.D., then $(R - \{0\})^{-1} R$ is a field.

(2) Ring R is an I.D. $\iff$ R embeds as a subring of a field.

Notation

(1) $\{1, d, d^2, \ldots\}^{-1} R = R_d \cong R[x] / (dx - 1)$

$\longrightarrow$ here $R_d \longrightarrow R[x] / (dx-1)$

by sending $\frac{1}{d}$ to x

and vice-versa.

(2) $I \triangleleft_{\text{prime}} R$, then $(R - I)^{-1} R = R_I$

Note

(1) $\{\text{Ideals in } R\} \longrightarrow \{\text{Ideals in } D^{-1}R\}$

This is by the extension morphism:

for any $I \lhd R$, map it to

$D^{-1}I \lhd D^{-1}R$ defined by

$I^e := D^{-1}I = \{\frac{a}{d} \mid a \in I, d \in D\}$

(2) $\{\text{Ideals in } D^{-1}R\} \longrightarrow \{\text{Ideals in } R \text{ saturated w.r.t } D\}$

This is by the contraction:

for any $J \lhd D^{-1}R$, map it to

$J^c := \{r \in R \mid \frac{r}{1} \in J\} \lhd R$

J^c is the saturation of J^c wrt D $\longrightarrow$ $J^c \subseteq (J^c)^{sat_D}$ as $\frac{r}{1} \in J \Rightarrow 1 \cdot r \in J^c$ and $1 \in D$

$(J^c)^{sat_D} \subseteq J^c$ as $sr \in J^c \Rightarrow \frac{sr}{1} \in J$

$\Rightarrow \frac{1}{s} \cdot \frac{sr}{1} = \frac{r}{1} \in J$

Def: D-saturated ideal

An ideal $X \lhd R$ is D-saturated if $X = \{r \in R \mid \exists d \in D \text{ s.t } dr \in X\} = X^{sat_D}$

(3) $\{\text{Ideals } J \lhd D^{-1}R\} \longleftrightarrow \{\text{Ideals } I \lhd R \text{ s.t } I \cap D = \phi \text{ and saturated wrt } D\}$

This is given by $I^e \longleftarrow I$

$J \longrightarrow J^c$

Note $(I^e)^c = \{r \in R \mid \exists d \in D, \text{ s.t } rd \in I\} = I^{sat_D}$

Note: if $I \cap D \neq \phi$, then $I^e = D^{-1}R$

Conversely, $J = (J^c)^e$

~~(4) { prime ideals I of R }~~

(4) $\left\{ \begin{array}{l} I \triangleleft_{\text{prime}} R \\ \text{with } I \cap D = \phi \end{array} \right\} \longleftrightarrow \{ \text{prime ideals of } D^{-1}R \}$

$I \longrightarrow D^{-1}I$

$J^c \longleftarrow J$

~~(⇐) Suppose, $I \triangleleft R$~~

~~what are the~~