Rings

Defⁿ: $(R, +, \cdot)$ is a ring if

① $(R, +)$ is abelian group [Closed, Ass, Id, Inv, Commute]

② $(R, \cdot)$ is semi-group [Closed, Ass.]

③ Distributive $a.(b+c) = a.b + a.c$, $(b+c).a = ba + c.a$

Ring with unity ≡ Ring ⊕ Mult. Identity (1)

Commutative ring ≡ Ring ⊕ $\cdot$ commutes

Division ring ≡ where non-zero elements form group (×)
(must have unity, non-zero have inverse, atleast 2 elements)

⊕ Commutative gives Field -?? (OR zero divisors ≠ already absent in DR, Not req)

- Zero divisor ≡ $a \neq 0, b \neq 0$ but $ab = 0 \Rightarrow a, b$ are zero divisors

* Integral Domain ≡ R ⊕ Commutative ⊕ Unity (1) ⊕ No zero divis

  └ Ex- $(I, +, \cdot)$ — Not a field.

  [Field − Inverse ≡ I.D]

  ~~Unity~~ Unity is present

* Field ≡ Commutative Ring with unity and every non-zero element is invertible w.r.t $\times_n$.

* Boolean Ring ≡ $\forall a \in R \Rightarrow a^2 = a$.

  └ Every boolean ring is abelian.

  $(a+a)^2 = a+a \Rightarrow a+a=0 \Rightarrow a = -a$, $ab+ab=0$

  $(a+b)^2 = a+b \Rightarrow ab+ba=0 \Rightarrow ab = b(-a) \Rightarrow ab = ba$

  └ Has characteristic 2. $[(a+a)^2 = a+a \Rightarrow a+a=0 \Rightarrow 2a=0$
  $a \neq 0 \Rightarrow 1.a = a \neq 0$. So 2 is least]

(1) R is w/o zero divisors iff cancellation laws hold.

$\Leftarrow$ Given cancellation laws hold

Assume $ab=0$ s.t $a\neq 0, b\neq 0$

$ab = a.0 \Rightarrow \boxed{b=0} \longrightarrow\!\leftarrow$

(2) Finite Integral Domain is a field. ← To prove field

F be F.ID $\equiv \{a_1, \ldots a_n\}$ be elements distinct.

TS: Every element in $F \neq\{0\}$ has an inverse:

Let $x\neq 0 \in F$,

$\therefore xa_1, \ldots xa_n \in F$.

All these are distinct $\Rightarrow xa_i = xa_j \Rightarrow x(a_i - a_j) = 0$

$\Rightarrow a_i = a_j \longrightarrow\!\leftarrow$

So, $xa_1, \ldots xa_n$ are all distinct elements of F.

As $1 \in F$, $xa_k = 1$ for some k

$\Rightarrow x^{-1} = a_k$ So, x has an inverse

$xa_k = x$

a_k is identity, As. $(xa_i)a_k = xa_ka_i = (xa_i)$

So a_k is identity.

3) p be prime. $I_p = \{0, 1, \dots p-1\}$ forms a field $+_p, \times_p$

- Closed $\equiv \forall a, b \in I_p \Rightarrow a +_p b = r \quad 0 \le r < p \Rightarrow a +_p b \in I_p$
- Ass. $\equiv a +_p (b +_p c) = a +_p (b + c) =$ remainder when $(a+b+c)$ divided by p

$=$ rem $(a+b)+c$ divided by $p = (a+b) +_p c = (a +_p b) +_p c$

- Id $\equiv 0 +_p a = a$.
- Inverse $\equiv 0 +_p 0 = 0$ [0 is inverse of itself]

$\equiv r \neq 0$ then $p - r \in I_p$

$\therefore (p-r) +_p r =$ remainder 0 when divided by p

$= r +_p (p-r)$

$\therefore p - r$ is inverse of r

So every element has inverse $+_p$.

- Comm $\equiv a +_p b = b +_p a$

- Closed $\equiv a \times_p b = r \quad 0 \le r < p \Rightarrow \times_p$ is closed
- Ass $\equiv a \times_p (b \times_p c) = a \times_p (bc) \quad [b \times_p c \equiv bc \bmod p]$

$=$ rem when $a(bc)$ divided by p

$= (ab) \times_p c = (a \times_p b) \times_p c$

- Id $\equiv \exists\, 1 \in I_p$ such that $a \times_p 1 = 1 \times_p a = a$
- Inv $\equiv$ Let $S \neq 0 \in I_p$ then $1 \le S \le p-1$

Consider $1 \times_p S, 2 \times_p S \dots p-1 \times_p S \in I_p$ (As closed)

All are distinct, or $\Rightarrow$ Let $1 \le i, j \le p-1$, $i > j$

$\therefore 0 < (i-j) < p-1$

If $i \times_p S = j \times_p S \Rightarrow$ is, js leave same remainder / p

$\Rightarrow (i-j)S$ is divided by $p \Rightarrow p \mid (i-j)$ or $p \mid S \rightarrow\leftarrow$ (as p is prime)

So, all are distinct.

One must be equal to 1 $\Rightarrow k \times_p S = 1 \Rightarrow k$ is (S^{-1})

So inverse exists.

Not needed. Use F.I.D is a field.

divisors $\rightarrow a \times_p b = 0 \Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b \Rightarrow a = 0$ or $b = 0$

So, No zero divisors exist.

(+) Commutative $\times_p$ (+) $a \times_p (b +_p c) = (a \times_p b) +_p (a \times_p c)$

If p composite, Zero divisors, not inverse

(2) Show ring $\mathbb{Z}_p$ is field iff p is a prime.

$\Rightarrow$ Let $\mathbb{Z}_p$ be a field.

If possible, let p be composite : $p = mn$ $1 < m < p$, $1 < n < p$

So, $mn = p = 0 \bmod p$

$m \neq 0, n \neq 0 \Rightarrow mn = 0$. So, $\mathbb{Z}_p$ is not integral domain $\rightarrow\leftarrow$
(zero divisors)

$\Leftarrow$ Let p be prime.

TS: $\mathbb{Z}_p$ field $\Rightarrow$ w.r.t $\mathbb{Z}_p$ is finite comm. ring with unity

(+) A F.ID is a field

└ TS: $\mathbb{Z}_p$ is Integral domain.

Let $m, n \in \mathbb{I}_p$ such that $mn = 0$ in $\mathbb{I}_p$.

Then $p \mid mn \Rightarrow p \mid m$ or $p \mid n \Rightarrow m = 0$ or $n = 0$

So, $\mathbb{Z}_p$ has no zero divisors. $\Rightarrow$ $\mathbb{Z}_p$ is FID.

(3) Nilpotent Element $\equiv$ $a \in R$, $\exists\, n \in \mathbb{N}$ s.t $a^n = 0$, then 'a' is nilpotent element of R

└ An ID has no non-zero nilpotent element.

└ Let R be ID, $a \neq 0 \in R$

$a^1 = a \neq 0$, $a^2 = a.a \neq 0$ (R is ID)

Let $a^n \neq 0$, $a^{n+1} = a.a^n \neq 0$ (R is ID) and $a \neq 0$, $a^n \neq 0$

So by induction, a is not nilpotent element

└ ab is nilpotent, then so is ba

$(ab)^n = 0$ $\quad (ba)^{n+1} = b(ab)^n a = 0$

Subring

(1). S is a subring of R iff $\forall a,b \in S \Rightarrow \overset{a-b\in S}{ab \in S}$.

└ For subfield → $a-b \in S$ ⊕ $ab^{-1} \in S$

Ex- Union of 2 sub-rings need not be subring

$IR = I$, $S_1 = \{2n\}$ $S_2 = \{3n / n \in I\}$

$S_1 \cup S_2 \equiv 2+3 = 5 \notin S_1 \cup S_2$.

Pv ⇒ Centre of a ring is a subring

⇓

Pv ⇒ Centre of a division ring is a field.

Characteristic of a ring ≡ Smallest +ve integer n s.t.

∃ +ve integer n, $na = 0$ $\forall a \in R$.

└ If no int exists ≡ Characteristic of Ring = 0 or ∞

(1). If R is a ring with unity element, then R has characteristic $p > 0$ iff p is least +ve int $p \cdot 1 = 0$.

⇒ Easy ⇐ $p1 = 0$.

For any $a \in R \Rightarrow pa = a + a + \ldots$ a p times

$= a(1+1+\ldots 1)$ p times

$= a(p1) = 0 \Rightarrow p$ is charac. of R

(2) Characteristic of Integral domain is 0 or prime.

⇒ Assume $n = ab$ $1 < a, b < n$

$nx = 0 \Rightarrow ab(x) = 0 \Rightarrow ab(x)y = 0.y \Rightarrow ab(xy) = 0$.

$\Rightarrow xy + xy + \ldots$ ab times $= 0 \Rightarrow (x+x+\ldots a \text{ times})(y+y+\ldots b \text{ times}) = 0$.

$(ax)(by) = 0 \Rightarrow ax = 0$ or $by = 0$

⇒ For 0, obvious.

Ideals

IMP TO SHOW

A (non-empty) subset S of a ring R is called an ideal if

$S \neq \phi$ (+) { (i) $(S,+)$ is a subgroup of $(R,+)$ $[a-b \in S]$
(ii) $s \in S, r \in R \Rightarrow sr, rs \in S$.

- Improper Ideals ≡ Unit Ideal (R), Null Ideal $\{0\}$
- TS: Ideal → Both sides must.

Ex → Subring but not Ideal [Integers over Rationals]

(*) A field has no proper ideals. — (IMP)

(1) R commutative with unit element has only 0 and R as ideals $\Rightarrow$ R is a field.

TS: $\forall a \neq 0 \in R$, $\exists a^{-1} \in R$.

Let $Ra = \{ra \mid r \in R\}$

Also non-empty show
$r_1a - r_2a = (r_1 - r_2)a \in Ra$.

└ TS: Ra is an ideal
- $(ra)x = (rx)a \in Ra$ as $(rx \in R)$
- $x(ra) = (xr)a \in Ra$ as $(xr \in R)$

Now $1 \in R \Rightarrow 1.a \in Ra \Rightarrow Ra \neq \{0\}$. So $Ra = R$

All elements of R can be written as $ra \Rightarrow 1 = r_i a \Rightarrow a^{-1} = r_i$

$\therefore R$ is a field

TIP:

(2) Show sum of two ideals is an ideal ≡ (both sides)

$S_1, S_2 \equiv S_1 + S_2 = \{x+y \mid (x \in S_1, y \in S_2)\}$

$0 \in R \Rightarrow 0 \in S_1$, $0 \in S_2 \Rightarrow 0+0 \in S_1 + S_2$

$\Rightarrow$ $S_1 + S_2 \neq \phi$ ⟸ ALWAYS Show THIS FIRST

③ If U is an ideal of R, P.T. $r(U) = \{x \in R \mid xu = 0 \ \forall u \in U\}$ is an ideal of R.

Since $0.u = 0 \Rightarrow 0 \in r(U) \Rightarrow r(U) \neq \phi$ and subset of R.
$(\forall u \in U)$.

Let $x, y \in r(U)$ $\quad xu = 0,\ yu = 0 \ \forall u \in U$

① $(x-y)u = xu - yu = 0 - 0 = 0$

② Let $r \in R \Rightarrow (rx)u = r(xu) = r0 = 0 \Rightarrow rx \in U$

$(xr)u = x(ru) = xy.$

where $y \in U$ as U is an ideal $\Rightarrow ru \in U$.

Since $x \in r(U)$, $y \in U \Rightarrow xy = 0 \Rightarrow (xr)u = 0$.

$\Rightarrow xr \in U$

$r(U)$ is an ideal of R.

Rw

④ A, B be two ideals of commutative ring R with unity s.t $R = A + B$. Show $AB = A \cap B$.

Given A, B are ideals $\rightarrow AB \subseteq A \cap B$

Let $x \in A \cap B \Rightarrow$ as $R = A + B \Rightarrow 1 = a + b \quad a \in A, b \in B$

$x = x.1 = x(a+b) = xa + xb$

($xa \in AB$, $xa = ax$) $\quad xb \in AB$

$\Rightarrow x \in AB \Rightarrow A \cap B \subseteq AB$

So, $A \cap B = AB$

5) A, B ideals ⇒ AB, A∩B, A+B are ideals
(If Right id, right inverse exists then done)

6). R be a ring with unity with only {0}, R as right ideals.
P.T R is a division ring.

Use aR → Show right ideal ⇒ aR = R ⇒ ab = 1 (right inverse of a)
TS: Left inverse ≡ b ≠ 0 or (1 = ab = 0) → ←. So b ≠ 0.
Then ∃ c, bc = 1 ⇒ ~~ab = ab. 1 = ab~~ ba = ba.1 ⇒ ba = b(a.b)c
So, b is left inverse as well ⇒ bc = ba = 1
— instead right id and right inverse exist → So, R is division ring.

Ideal generated by a subset of a ring.

U ideal generated by S ⇒ U = ⟨S⟩, if
(i) S ⊆ U (ii) for any ideal V of R, S ⊆ V ⇒ U ⊆ V.

(1) A+B is an ideal generated by A∪B
↳ A+B = ⟨A∪B⟩

Principal ideal ≡ If an ideal U is gen. by a single element.
↳ U = ⟨a⟩, U is the smallest ideal containing 'a'.

↳ 2 principal ideals ≡ Null ideal, Unit Ideal.
↳ Every ideal of a field ~~has~~ is a principal ideal

* Principal Ideal Ring if every ideal in ring R is principal ideal.

* Principal Ideal Domain (PID + Every ideal is principal)

- A commutative ring without zero divisors and with unity and every ideal S is a principal ideal.

Ring ⊕ Commutative ⊕ No Zero divisors ⊕ 1 ⊕ Princi. Ideal

(1) Every field is a PID. [Pf: Show only two ideals]

(2) Every ideal of ring of integers is a principal ideal.

If $S = \{0\}$ ✓

Let $S \neq \{0\}$ then S contains non-zero elements

- Let $a \neq 0 \in S$, then $-a \in S \Rightarrow S$ has +ve, -ve integers

Let s be least +ve int in S. and p be any element in S.

$$p = sq + r \Rightarrow \underset{\in S}{p} - \underset{\in S}{sq} \in S \Rightarrow r \in S. \quad 0 \leq r < s.$$

So, r must be 0 or else contradiction

$\Rightarrow p = sq \Rightarrow$ So S is generated by s. $\Rightarrow \boxed{S = (s)}$

Quotient Ring.

If S is an ideal, then set $R/S = \{S+a \mid a \in R\}$ of all residue classes of S in R. forms a ring:

$$(S+a)+(S+b) = (S+a+b)$$

$$(S+a)(S+b) = (S+ab)$$

(1) Show well defined.

$\Rightarrow$ $S+a = S+a'$ $\quad S+b = S+b' \Rightarrow [a' \in S+a,\ b' \in S+b.]$

~~$(S+a)+(S+b) = (S+a')+(S+b')$~~

So, $\exists\ \alpha, \beta \in S$ s.t $a' = a+\alpha$, $b' = b+\beta$.

$(a'+b') = (a+b)+(\alpha+\beta) \Rightarrow (a'+b')-(a+b) \in \alpha+\beta$

$\Rightarrow (a'+b')-(a+b) \in S \Rightarrow S+(a'+b') = S+(a+b)$

$\Rightarrow (S+a)+(S+b) = (S+a')+(S+b')$

$\Rightarrow a'b' = (\alpha+a)(\beta+b) = ab+\alpha\beta+\alpha b+\beta a.$

$\Rightarrow a'b'-ab \in S \Rightarrow S+ab = S+a'b'$

$\Rightarrow (S+a)(S+b) = (S+a')(S+b')$

(2). Ring Properties $\Rightarrow$ [Obvious]

* Prime Ideal

Ideal P is prime if for any $a, b \in R$; $ab \in P \Rightarrow a \in P$ or $b \in P$

(1) R be commutative ring, P is ideal.

P is prime iff R/P is integral domain.

$\Leftarrow$ TS: P is prime. $ab \in P \Rightarrow a \in P$ or $b \in P$.

Let $ab \in P \Rightarrow$ In $R/P \Rightarrow (P+ab) = 0+P$.

$\Rightarrow (P+a)(P+b) = (P+0)$

As R/P is integral domain $\Rightarrow P+a = 0+P$ or $P+b = 0+P$.

$\Rightarrow a \in P$ or $b \in P$. ✓

$\Rightarrow$ TS: R/P is integral domain

Let $P+a, P+b \in R/P$ s.t $(P+a)(P+b) = P+0$

$\Rightarrow P+ab = P+0 \Rightarrow ab \in P$.

As P is prime $\Rightarrow ab \in P \Rightarrow a \in P$ or $b \in P$.

$\Rightarrow a+P = 0$ or $b+P = 0$

$\Rightarrow R/P$ is integral domain

Maximal Ideal.

Here R is ring to integers
↳ So R is E.D ⇒ PID

M be an ideal, $M \neq R$, if for any ideal N, $M \subseteq N \subseteq R$, then $M = N$ or $R = N$.

Revise

① $M = (n_0)$ is maximal $\Leftrightarrow$ n_0 is prime $\Leftrightarrow$ n_0 is irreducible

$\Rightarrow$ n_0 is prime. $\Rightarrow n_0 = ab \Rightarrow a = 1$ or $a = n_0$; as n_0 is prime.

$\Leftarrow$ Let $(a) = U$, $M \subset U \subset \mathbb{Z}$

If $a = 1 \Rightarrow (1) = \mathbb{Z} = U$

$a = n_0 \Rightarrow (n_0) = M = U$.

As prime ≡ irreducible on PID
An ED is a PID

So, $M \subseteq U \subseteq \mathbb{Z} \Rightarrow U = \mathbb{Z}$ or $U = M$.

Hence, $M = (n_0)$ is a maximal ideal of $\mathbb{Z}$.

$\Rightarrow$ Let $M = (n_0)$ is maximal.

Assume $n_0 = ab$ $a, b \neq 1, a, b \neq -1$. — (1)

Let $U = (a)$, $x \in M$.

$x = n_0 r \Rightarrow x = (ab)r \Rightarrow x = a(br) \Rightarrow x \in U$.

$M \subseteq U \subseteq \mathbb{Z}$

But since M is a maximal ideal ⇒

$U = M$ or $U = \mathbb{Z} \Rightarrow a = 1$, but assume $a \neq 1$ →←

($a = n_0 l$)

$n_0 = ab$

$n_0 = (n_0 l) b \Rightarrow lb = 1 \Rightarrow b = 1$ →←

So, ① is wrong

For $\mathbb{Z}$ can use above, not always
In PID prime ≡ irreducible → Can use above for PIDs.
In PID prime ideal ≡ maximal ideal.

Possible to have multiple (maximal ideal) → Find → list out all ideals

$\mathbb{Z} \rightarrow \langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle$ all maximal ideals. (P7) (*)

(2) (*) R is commutative ring with unity, then an ideal M of R is maximal iff R/M is a field.

Revise

$\Rightarrow$ M is maximal

TS: R/M is a field

TS: Every non-zero elements of R/M has multi. inverse

Let $a+M \in R/M$ s.t $a \notin M$

Now create an ideal generated by a

If $\langle a \rangle = \{ar \mid r \in R\}$ is a principal ideal of R.

Then $\langle a \rangle + M$ is an ideal (Sum of 2 ideals).

$a = a \cdot 1 + 0 \in \langle a \rangle + M$ and $a \notin M$

$M \subset \langle a \rangle + M \subseteq R$.

So, $\langle a \rangle + M = R$. as M is maximal.

$\Rightarrow 1 = ar + M \Rightarrow 1 = (a+M)(r+M)$

$(r+M)$ is $(a+M)^{-1}$. So R/M is a field

Revise

$\Leftarrow$ R/M is a field

TS: M is maximal.

Let U be ideal s.t $M \subset U \subseteq R$

TS: $U = R$.

Since, $M \subset U \Rightarrow \exists p \in U$, $p \notin M$.

$\Rightarrow p+M$ is non-zero elem of R/M.

$\Rightarrow$ R/M field $\Rightarrow 1+M = (p+M)(q+M)$

$\Rightarrow 1+M = pq+M \Rightarrow 1-pq \in M$

$M \subset U \Rightarrow 1-pq \in U$, $p \in U$ + U is ideal $\Rightarrow pq \in U$.

$\Rightarrow 1-pq+pq \in U \Rightarrow 1 \in U \Rightarrow U = R$

1991

(3) A comm. ring with unity, maximal ideal is prime ideal.

R, M ≡ maximal → R/M is field → R/M is integral domain

R/M is I.D ⇔ M is prime ⇒ M is prime ideal.

Rmk

Ex → Comm ring w/o unity ⇒ Max Ideal ⇏ Prime Ideal

⟨2⟩ = R , ⟨4⟩ is max ideal (Show)

⟨4⟩ is not prime as $2.2 = 4$, $2 \notin \langle 4 \rangle$, $4 \in \langle 4 \rangle$

(4) Comm. ring with unity. M is maximal, $x \in R$,

P.T $\exists \alpha \in R$ s.t $x \notin M \Rightarrow 1 - x\alpha \in M$.

Let Principal ideal $\equiv \langle x \rangle$

$\langle x \rangle + M$ is ideal s.t $M \subset \langle x \rangle + M$,

As M is maximal ⇒ $\langle x \rangle + M = R \Rightarrow \langle x \rangle + M = 1$

$\exists a \in M, \alpha \in R \Rightarrow 1 = a + x\alpha \Rightarrow 1 - x\alpha = a$

$\Rightarrow 1 - x\alpha \in M$

For prime ideal P → Show R/P is integral domain.

- Integral Domain is Commutative & has identity
- $\phi(1) = 1'$ only if R' is an integral domain

$\phi: R \to R'$

- TS $\phi: R \to R'$ is an isomorphism, only show ϕ is 1-1.

$\phi(e) = \phi(e.e) = \phi(e).\phi(e) \Rightarrow \phi(e).e' = \phi(e).\phi(e)$

In ID cancellation holds $\Rightarrow$ $\underline{\phi(e) = e'}$

Homomorphism $\begin{cases} f(a+b) = f(a) \oplus f(b) \\ f(ab) = f(a) \otimes f(b) \end{cases}$

Homomorphic Image (R is of R') → **f: is homo, $R \xrightarrow{\text{onto}} R'$**

Isomorphism → **Homo + 1-1**

Isomorphic image → R is iso. image of R' if $f: R \to R'$
f is homo, onto, 1-1
$[R \cong R']$

Natural homomorphism ≡ $f: R \to \frac{R}{U}$ [where U is an ideal]

) Homo. Image of Comm. ring is commutative.

) f: homo → $\begin{cases} f(0) = 0' \\ f(1) = 1' \end{cases}$

An example ⇒

$f: \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \to a$

└ onto, homo

└ Counter-example → Image has unity, not the ring
Image is comm, not the ring

* Fundamental Thm of Homomorphism

$R, R' \Rightarrow f: R \to R'$ be **onto**, **homomorphism** with **Ker f.** ($\ker f$ an ideal) $R \simeq R' \Rightarrow \frac{R}{\ker f} \cong R'$

$\Rightarrow$ Let $f: R \to R'$ be a homomorphism and onto

$\ker f = \{x \in R / f(x) = 0', 0' \text{ is the identity of } R'\}$

$\ker f = U$ (U is an ideal of R)

So, R/U is well-defined $= \{x + U / x \in R\}$

T.S: $(R/U \simeq R')$

$\phi: \frac{R}{U} \longrightarrow R'$ s.t $\phi(a+U) = f(a) \ \forall a \in R$.

① ϕ is well-defined. $\left[\begin{matrix} a+U = b+U \Rightarrow a-b \in U \Rightarrow f(a-b) = 0 \\ f(a) = f(b) \Rightarrow \phi(a+u) = \phi(b+U) \end{matrix}\right]$

② ϕ is 1-1, onto, homomorphism.

Imbedding of rings

Ring R is imbedded in R' if $\exists$
$f: R \to R'$ s.t f is homomorphism, f is 1-1

Cor ⇒ ① f is isomorphism, so $f(R)$ is subring of R'
Also, R and $f(R)$ are isomorphic rings
② $f: R \to f(R)$ is onto isomorphism
$R \cong f(R)$

Field of Quotients

Every integral domain can be imbedded in a field.

∴ Let D be integral domain, atleast two elements.
$S = \{(a,b) \mid a,b \in D, b \neq 0\}$ then $S \neq \phi$ and $S \subset D \times D$

Define $(a,b) \sim (c,d) \iff ad = bc$.

① Prove $\sim$ is equivalence relation. [EASY].
$\sim$ partitions S into equivalence classes.

② Let F denote set of all equivalence classes on $S \Rightarrow F = \{\frac{a}{b} \mid (a,b) \in S\}$
Since $\frac{0}{a}, \frac{a}{a} \in F \Rightarrow$ Set F has (atleast two elements)

③ Define $+ \to \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\cdot \to \frac{a}{b} \cdot \frac{c}{d} = \frac{ca}{bd}$

[As D has no zero divisors $\to bd \neq 0 \Rightarrow \frac{ad+bc}{bd}, \frac{ac}{bd} \in D$, ✓]

Show well-defined ⇒ $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'} \Rightarrow ab' = ba'$, $cd' = c'd$.

→ $ab'dd = ba'dd'$ and $bb'cd' = bb'c'd$
→ $ab'dd' + bb'cd' = ba'dd' + bb'c'd \Rightarrow (ad+bc)b'd' = (a'd'+b'c')bd$
→ $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ ⊕ is well-defined

④ Show $(F, \oplus, \otimes)$ is a field

- $(F, \oplus)$ – abelian group
- $(F, \otimes)$ – Semi-group
- Distributive property
- Multi Identity ≡ For $U \neq 0 \in D$, $\frac{U}{U} \in F$ s.t.
  $\frac{a}{b} \cdot \frac{u}{u} = \frac{au}{bu} = \frac{a}{b} \; \forall \; \frac{a}{b} \in F$
  So, U/U is unity
- Inverse ≡ $\frac{a}{b} \in F$, $b \neq 0 \Rightarrow \frac{a}{b} \neq \frac{0}{U} \Rightarrow au \neq 0 \Rightarrow a \neq 0$ & $U \neq 0$
  So, $\frac{b}{a} \in F \Rightarrow \frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{u}{u}$

⑤ Define $\phi : D \to F \Rightarrow \phi(a) = (a, 1)$ ∴

- Show ϕ is homo, ϕ is 1-1

So, D is embedded in F.

3] Let R be the ring of all real valued continuous functions on closed unit interval. Show $M = \{f \in R \mid f(1/3) = 0\}$ is maximal ideal.

Given R as a ring with $\circ$

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

① M is an ideal. $\Rightarrow$ $O(x) = 0$ be zero function $\Rightarrow O(x) \in M$ as $O(1/2) = 0$

$f, g \in M$, $f(1/3) = g(1/3) = 0$

$\cdot (f-g)1/3 = f(1/3) - g(1/3) = 0$

$h \in R \Rightarrow \cdot (fg)1/3 = f(1/3)g(1/3) = h(1/3).0 = 0 \Rightarrow (hg \in M)$

$\cdot$ Ily $(gh \in M)$

So, M is an ideal of R.

② M is maximal ideal.

Let if possible, U be an ideal s.t $M \subset U \subset R$ s.t $M \neq U$.

TS: $U = R$.

Let $g \in U$ s.t $g \notin M \Rightarrow g(1/3) = \alpha$ where $\alpha \neq 0$

Let $p(x) = g(x) - \alpha$ s.t $p(1/3) = 0$ s.t $p(x) \in M \subset U$.

As $p(x) \in U$, $g(x) \in U \Rightarrow g(x) - p(x) = \alpha \in U$.

As α is a real value, α^{-1} exists, U is ideal $\Rightarrow \alpha\alpha^{-1} \in U$

$\Rightarrow 1 \in U$.

As $1 \in U$, so $U = R$.

Thus, M is maximal ideal

Euclidean Domain / Euclidean Ring

→ (Commutative)

- An integral Domain is a Euclidean domain if $\forall\ a(\neq 0) \in D$, there is a non-negative integer $d(a)$ s.t.

(i) $\forall a, b \in D, a \neq, b \neq 0$; $d(a) \leq d(ab)$

(ii) For any $a, b \in D$, $b \neq 0$ $\exists\ q, r \in D \Rightarrow a = bq + r$.
$r = 0$ or $d(r) < d(b)$

Ring of Integers in a Euclidean Domain.

Thm: Ring of Gaussian integers is a Euclidean Domain.

$\mathbb{Z}[i] = [a + ib \mid a, b \in \mathbb{Z}]$

Define mapping $d: \mathbb{Z}[i] - \{0\} \to \mathbb{Z}$ by.

$d(x+iy) = x^2 + y^2$ as $x \neq 0$ or $y \neq 0$, $x^2 + y^2 \geq 1$.

Let $z_1 = a+ib$ $z_2 = c+id$ where $z_1 \neq 0$ & $z_2 \neq 0$.

- $z_1 z_2 = (ac - bd) + i(ad + bc)$

So, $d(z_1 z_2) = (ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2) \geq a^2+b^2$
$\geq d(z_1)$
$\geq d(z_2)$

- $\frac{z_1}{z_2} = \frac{a+ib}{c+id} = \frac{ac+bd}{c^2+d^2} + i\frac{(bc-ad)}{c^2+d^2} = (p+iq)$

where p, q are rational numbers

corresponding to p, q we can find integers p', q' s.t $|p-p'| \leq 1/2$
$|q-q'| \leq 1/2$.

Let $t = p' + q'i$, then $t \in \mathbb{Z}[i]$

Let $\frac{z_1}{z_2} = \lambda \Rightarrow z_1 = \lambda z_2 - t z_2 + t z_2 \Rightarrow z_1 = (\lambda - t) z_2 + t z_2$.
$(\lambda = p + iq)$

Now, $\boxed{z_1 = t z_2 + r} \to (\lambda - t) z_2$.

$z_1, z_2, t \in \mathbb{Z}[i] \Rightarrow z_1 - t z_2 \in \mathbb{Z}[i] \Rightarrow r \in \mathbb{Z}[i]$

Instead use 2-step ⇒ First Divide y by n.
Then $y\bar{x}$ by $x\bar{x} \Rightarrow d(y\bar{x} - tx\bar{x}) < d(x\bar{x})$

$\therefore \exists\ t, r \in \mathbb{Z}[i]$ s.t

$z_1 = tz_2 + r$ where $r = 0$ or $d(r) = d[(1-t)z_2]$

$d(r) = d[(p-p') + (q-q')i] = [(p-p')^2 + (q-q')^2]\, dz_2$.

$\leq \left(\frac{1}{4} + \frac{1}{4}\right) dz_2 = \frac{1}{2} d(z_2) < d(z_2)$.

So, Bowed

(8) Show $\mathbb{Z}(\sqrt{2}) = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ is a ED

1. Define $d : \mathbb{Z}(\sqrt{2}) - \{0\} \to \mathbb{Z}$ by

$$d(m+n\sqrt{2}) = |m^2 - 2n^2| \quad \forall\ m+n\sqrt{2} \in \mathbb{Z}[\sqrt{2}] - \{0\}$$

We have $m \neq 0$ or $n \neq 0 \Rightarrow d(m+n\sqrt{2})$ is the int ≥ 0.

- Let $a = m+n\sqrt{2} \neq b = m_1 + n_1\sqrt{2} \neq 0$

$ab = (mm_1 + 2n_1n_2) + (mn_1 + nm_1)\sqrt{2}$

$d(ab) = |(mm_1 + 2n_1n_2)^2 - 2(mn_1 + nm_1)^2|$

$= |(m^2 - 2n^2)(m_1^2 - 2n_1^2)|$

$= |m^2 - 2n^2|\,|m_1^2 - 2n_1^2| \geq |m^2 - 2n^2|$

$d(ab) \geq d(a)$.

- $\frac{a}{b} = \frac{mm_1 - 2n_1n}{m_1^2 - 2n_1^2} + \frac{m_1n - mn_1}{m_1^2 - 2n_1^2}\sqrt{2}$. (After rationalise)

$= \underbrace{p + q\sqrt{2}}_{(\lambda)}$ $\quad p, q \in \mathbb{Q}$.

Corresponding to p, q we can find p', q' such that

$|p-p'| \leq 1/2$, $|q-q'| \leq 1/2$ $\quad$ $|p'-p| \leq 1/2$, $|q'-q| \leq 1/2$

Let $t = p' + q'\sqrt{2}$ $\quad$ $t \in Z(\sqrt{2})$

$\frac{a}{b} = \lambda \Rightarrow a = \underbrace{(\lambda - t)b}_{\gamma} + tb = tb + \gamma$

$a - tb \in Z(\sqrt{2}) \Rightarrow \gamma \in Z(\sqrt{2})$

So, we see $\exists\ t, \gamma$ s.t $t, \gamma \in Z[\sqrt{2}]$

$a = tb + \gamma$ where $\gamma = 0$ or

$d(\gamma) = d\{(\lambda - t)b\} = d\{(p-p') + (q-q')\sqrt{2}\}\, d(b)$

$= \frac{3}{4} d(b) < d(b)$

So $Z[2]$ is ED

* Every Euclidean Ring is Principal Ideal Ring

(Every ideal of E.R is Principal Ideal)

$\Rightarrow$ R be E.R, U be an ideal of R.

TS: U is a principal ideal

Let $U=\{0\} \Rightarrow U=\{0\}$ is princi. ideal

If $U \neq \{0\} \Rightarrow U$ has non-zero elems.

$\exists x \in U$ and $x \neq 0$ So that $\{d(x) / x \neq 0\}$ is non-emtty of ~~(+ve 0)~~ non-neg. integers

- By well-ordering principle, $\exists b \neq 0$ in U, with $d(b) \leq d(x) \quad \forall x \in U \ (\neq 0)$ $\rightarrow$ (1)

TS $\equiv$ $U = \langle b \rangle$

Let $a \in U$,

By div. algorithm

$a = bt + r$

Now $d(r) = 0$ or $0 < d(r) < d(b)$

$\Rightarrow$ If $d(r) < d(b)$ and $a \in U$, $b \in U \Rightarrow bt \in U$ as U is ideal.

$\Rightarrow r = a - bt \in U \Rightarrow d(r) < d(b) \rightarrow\leftarrow$ (1)

So, $r = 0 \Rightarrow \boxed{a = bq}$

$U = \{bq \mid q \in R\} = \langle d \rangle$

Hence, every ideal is a princi. ideal

Every Euclidean ring ⇒ Commutative ① possesses unity element.

R be E.R ⇒ R is principal ideal ② ⇒ $R = \langle r \rangle$.

$R = \{ rq / q \in R \}$

$r \in R \Rightarrow r = rq_1$ for some $q_1 \in R$.

TS: q_1 is unity

$a \in R \Rightarrow a = rp \Rightarrow aq_1 = rpq_1 \Rightarrow qq_1 = prq_1 \Rightarrow aq_1 = pr$

$\Rightarrow \boxed{aq_1 = rp} = a.$

So, q_1 is unity.

Counter

~~X Ring of Integers is PID, but not ED~~

• Units ≡

R be commutative ring with unity.

$a \in R$ is a unit if $\exists\ b \in R$ such that $ab = 1$

Ex → $\mathbb{Z} \Rightarrow \pm 1$, $\mathbb{Z}[i] \Rightarrow \pm 1, \pm i$

Q $\mathbb{Z}(\sqrt{2})$ has infinite units.

$(3+2\sqrt{2})(3-2\sqrt{2}) = 9-8 = 1.$

$(3+2\sqrt{2})$ is a unit in $\mathbb{Z}(\sqrt{2})$ – all powers of $(3+2\sqrt{2})$ are also units

Remark

Th ⇒ $a, b \neq 0 \in R$, where R is Euclidean ring.

• If b is a unit then $d(ab) = d(a)$

Pf

$d(ab) \geq d(a)$ – ①

$bc = 1 \Rightarrow$ $d(a(bc)) \geq d(ab)$

$\Rightarrow d(a.1) \geq d(ab)$ – ②

$\Rightarrow d(a) = d(ab)$

• If b is not a unit, $d(ab) > d(a)$

By division algo ⇒ $\exists\ q, r$ s.t ⇒ (Divide a by ab)

$a = q(ab) + r$ ↗ $r = 0$ or $d(r) < d(ab)$

If $r = 0 \Rightarrow a = q(ab) \Rightarrow a(1-qb) = 0 \Rightarrow qb = 1 \Rightarrow b$ is unit →←

So, $r \neq 0 \Rightarrow d(r) < d(ab) \Rightarrow d(a - q(ab)) < d(ab)$

$d(a) \leq d(a(1-qb)) < d(ab)$

But, $d(a(1-qb)) \geq d(a)$ by Defn

So, $d(a) < d(ab)$

A non-zero 'a' of E.R is unit $\Leftrightarrow d(a) = d(1)$.

s unit $\Rightarrow ax = 1 \rightarrow d(a) \le d(ax) = d(1)$ & $d(1) \le d(1.a) = d(a)$]

$= d(1) \Rightarrow$ If a not unit $\rightarrow d(1) < d(1.x) \rightarrow \leftarrow$

Associates

a is an associate of b $\Rightarrow$ if $a = bu$, where u is unit

Ex $\rightarrow$ $2+3i$, $2i-3$ are associates in $\mathbb{Z}[i]$

$i(2+3i) = 2i-3$ and i is unit in $\mathbb{Z}[i]$

R be comm-ring (+) $a, b \neq 0$

GCD $\equiv$ d is gcd $(a,b) \Rightarrow$ If (i) $d|a$ and $d|b$

(ii) whenever $c \neq 0 \in R$ $c|a$ and $c|b \Rightarrow c|d$.

LCM $\equiv$ $\boxed{c \neq 0}$ is l.c.m if (i) $a|c$, $b|c$.

(ii) $x \neq 0$, $a|x$, $b|x$ then $c|x$

NOTE: May or may not have l.c.m/hcf.
lcm/hcf may not be unique.

Ex $\rightarrow$ E of even integers $(4,6)$ < no hcf $2 \nmid 6$ as $3 \notin E$
No lcm 4×12 as $\cancel{3} \notin E$

$\mathbb{Z}_{12}$. Find l.cm, hcf $\Rightarrow \boxed{\bar{6}, \bar{8}}$ ⟸ (*) Revise

$\bar{6} = \bar{3}.\bar{2} = \bar{10}.\bar{3}$ $\quad$ $\bar{8} = \bar{4}.\bar{2} = \bar{10}.\bar{2}$

└ hcf ┘

└ $2|6$ and $2|8 \Rightarrow$ If $x|6$, $x|8 \Rightarrow x|8-6 \Rightarrow x|\bar{2}$

└ $\bar{10}|6$, $\bar{10}|8 \Rightarrow$ If $x|6$, $x|8 \Rightarrow x|6-8 \Rightarrow x|\bar{10}$

└ So, HCF $= \bar{2}, \bar{10}$

LCM $\Rightarrow 6|x$, $8|x \Rightarrow 6|x \Rightarrow x = 6y \Rightarrow \bar{x} = \bar{0}$ or $\bar{6}$

As $\bar{x} \neq \bar{0} \Rightarrow 6 = 8\bar{z}$ has no solution in $\mathbb{Z}_{12}$ | No LCM exists

IMPORTANT

* R be E.R. Then any 2 elems a, b in R have a gcd d. Also $d = \lambda a + \mu b$.

Let A be set of $(ra + sb)$ elements. $(r, s \in R)$

TS: A is an ideal. $\Rightarrow$ EASY.

As A is an ideal in R and R is E.R then A is a principal ideal.

$\exists d \in R \Rightarrow A = \langle d \rangle. \Rightarrow d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

R has a unit element $1 \Rightarrow a = 1.a + 0.b \in A.\ b = 0.a + 1.b \in A$

So, $a = dx_0$, $b = dy_0$.

Suppose $c|a, c|b \Rightarrow c|\lambda a, c|\mu b \Rightarrow c|\lambda a + \mu b \Rightarrow c|d$

Revise ~ !!

* In a PID, prime $\equiv$ irreducible (iff).

$\Rightarrow$ p be prime, $p = ab$ then $p|ab \Rightarrow p|a$ or $p|b$.

If $p|a \Rightarrow px = a \Rightarrow p = pxb \Rightarrow 1 = bx \Rightarrow b$ is a unit

(Same for $p|b$)

$\Leftarrow$ p irreducible, $p|ab$ — If $p|a$ ✓ else $p \nmid a$ then

$1 = \gcd(p, a) = d \Rightarrow dx = p,\ dy = a$.

TS: d is unit $\rightarrow$ If not, $-x$ is unit [as p irreducible]

$d = \lambda a + \mu p$. $\quad \times \leftarrow$ $\quad \because d = px^{-1} \Rightarrow a = px^{-1}y \Rightarrow p|a \rightarrow \leftarrow$

$dd^{-1} = d^{-1}\lambda a + d^{-1}\mu p \Rightarrow b = \lambda d^{-1}ab + \mu d^{-1}bp.$

As $p|ab$, $p|RHS \Rightarrow \boxed{p|b.}$ ✓

Remember

ALITER: p is irreducible $\Rightarrow$ Show (p) is maximal $\Rightarrow$ p is prime

Let $(p) \subsetneq I \subsetneq R$. As PID $\Rightarrow I = (i) \Rightarrow p = ix$

$\Rightarrow x$ is unit $\Rightarrow i = px^{-1} \Rightarrow (p) = (I) \rightarrow \leftarrow$

As p irreducible

i is not unit as $I \neq R$.

So (p) is maximal.

Prime vs

$p \neq 0$, $\sqrt{p}$

$p|ab \Rightarrow$

Show (i) in $\mathbb{Z}[\sqrt{-5}]$

$\rightarrow$ Not unit

$\sqrt{-5}(a + b\sqrt{-}$

$\Rightarrow \sqrt{-5}a = 1$ +

imag.

Prime (G

If $\sqrt{-5} \mid (a +$

$\sqrt{-5}(x + y\sqrt{-5}) =$

$-5y = ac - 5b$

$\Rightarrow 5|ac \Rightarrow$

5 is prim

If $5|a \Rightarrow \sqrt{-}$

$\Rightarrow \sqrt{5} \mid (a$

Ly if $5|c \Rightarrow$

Hence Pr

Prime vs Irreducible. —— $p \neq 0$, p is not unit
$p = ab \Rightarrow a$ or b is a unit

- $p \neq 0$, p is not unit ①
- $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ ②

In PID they coincide

Show (i) $\sqrt{-5}$ is prime in $\mathbb{Z}[\sqrt{-5}]$

(ii) 3 is irreducible, not prime

⇒ Learn as example.

① Not unit :

$\sqrt{-5}(a+b\sqrt{-5}) = 1$

$\Rightarrow \underbrace{\sqrt{-5}a}_{\text{imag.}} = \underbrace{1+5b}_{\text{int}}$ Not possible

$3(a+b\sqrt{-5}) = 1$

$\underbrace{3b\sqrt{-5}}_{\text{Imag.}} = \underbrace{1-3a}_{\text{int}}$ → Not possible

② Prime (Good - REVISE) ✍

If $\sqrt{-5} \mid (a+b\sqrt{-5})(c+d\sqrt{-5})$

$\sqrt{-5}(x+y\sqrt{-5}) = (a+b\sqrt{-5})(c+d\sqrt{-5})$

$-5y = ac - 5bd$, $5(bd-y) = ac$

$\Rightarrow 5 \mid ac \Rightarrow 5 \mid a$ or $5 \mid c$ as 5 is prime

If $5 \mid a \Rightarrow \sqrt{-5}\sqrt{-5} \mid a \Rightarrow \sqrt{-5} \mid a$.

$\Rightarrow \sqrt{-5} \mid (a+b\sqrt{-5})$

Ulty if $5 \mid c \Rightarrow \sqrt{-5} \mid (c+d\sqrt{-5})$

Hence Proved

Irreducible.

$3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$

$\bar{3} = (a-b\sqrt{-5})(c-d\sqrt{-5})$

$9 = (a^2+5b^2)(c^2+5d^2)$

$\downarrow$

1, 3, 9

unit ┘ └ Not possible

If $a^2+5b^2 = 9 \Rightarrow c^2+5d^2 = 1$ - unit

Hence irreducible

③ Not prime.

$(2+\sqrt{-5})(2-\sqrt{-5}) = 9$

$3 \mid 9 \Rightarrow$ TS $3 \mid$

$3(a+\sqrt{-5}b) = 2+\sqrt{-5}$

$\Rightarrow 3(a-\sqrt{-5}b) = 2-\sqrt{-5}$

$\Rightarrow 9(a^2+5b^2) = 9$

$\Rightarrow a = \pm 1, b = 0 \Rightarrow$

$\pm 3 = 2+\sqrt{-5}$ Not possible

Ulty ⇒

* Polynomial Rings. (F is a field)

Ans. A RESULT

① If F is a field, then F[x] is a Euclidean ring.

- F[x] is an integral domain with unity [Basic Proof]

Let $d(f(x)) = \deg f(x)$ which is non-ve integer.

If $\deg(f(x).g(x)) = \deg\{f(x)\} + \deg\{g(x)\}$;

So, $\deg(f(x).g(x)) \geq \deg f(x), \deg(g(x))$ As $\deg \geq 0$

- Let $f(x) = t(x)g(x) + r(x)$.

If $\deg f(x) < \deg g(x) \Rightarrow f(x) = 0.g(x) + r(x)$

② Let $f(x) = a_0 + a_1x + \dots a_mx^m \quad g(x) = b_0 + b_1x + \dots b_nx^n$

and $\deg f(x) \geq g(x) \Rightarrow f_1(x) = f(x) - \frac{a_m}{b_n} x^{m-n} g(x)$.

So, $f_1(x) = 0$ or $\deg f_1(x) < m := \deg(f(x))$

↓

$f(x) = \frac{a_m}{b_n} x^{m-n} g(x) + (0)$

$f(x) = t(x)g(x) + r(x)$

↳ Induction $\equiv f_1(x) = t_1(x)g(x) + r(x)$

$r(x) = 0$ or $\deg(r(x)) < \deg g(x)$

$f(x) = [a_m b_n^{-1} x^{m-n} + t_1(x)]\, g(x) + r(x)$

② F is a field, F[x] is a PID (Princi. Ideal Domain)

- Show F[x] is E.D (①)
- Let A be an ideal of F[x], $A \neq 0, \neq F[x]$

Consider $f(x) \in A$ s.t $\deg f(x)$ is least. (By Well ordering P.)

If $g(x) \in A \Rightarrow g(x) = p(x)f(x) + r(x) \Rightarrow r(x) = g(x) - p(x)f(x)$

$r(x) \in A$, $\deg(r(x)) < \deg(f(x))$ by E.D $\Rightarrow$ So $r(x) = 0$

③ AB is an ideal $\equiv AB = \sum_{i \in F} a_i b_i$ $\quad a_i \in A,\ b_i \in B$. F is finite

---

④ Polynomial $p(x) \in F[x]$ is irreducible over F if $p(x) = a(x)\,b(x)$ then either $a(x)$ or $b(x)$ has degree 0

⑤ Ideal $A = (p(x))$ is maximal iff $p(x)$ is irreducible over F.

⑥ If $\langle p(x) \rangle$ is irreducible $\Rightarrow$ A is maximal $\rightarrow$ $F[x]/p(x)$ is field

⑦ Primitive Polynomial $\equiv a_0 + a_1 x + \cdots a_n x^n$ if $\gcd(a_0, \ldots a_n) = 1$.

Content $\equiv \gcd(a_0, \ldots a_n)$

$f(x), g(x)$ are two non-zero elements of $F[x]$

$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

$f(x) = a_0 + a_1 x + \dots a_m x^m$ $\quad g(x) = b_0 + \dots b_n x^n$

$a_m \neq 0, b_n \neq 0$ $\quad$ L m $\quad$ L n (degree)

$f(x)g(x) = c_0 + \dots c_k x^k.$

$\boxed{c_t = a_t b_0 + a_{t-1} b_1 + \dots a_0 b_t}$

$\boxed{c_{m+n} = a_m b_n.} \neq 0.$

c_i for $i > m+n \Rightarrow a_i b_0 + \dots + a_0 b_i$ $\quad$ So either $a_i > m$ or $i > n$

Since $i > m+n$

So, $a_k = 0$ or $b_j = 0 \Rightarrow \boxed{c_i = 0 \quad i > m+n}$

$F[x]$ is ED $\Rightarrow$ PID $\Rightarrow$ Has gcd of 2 elements

$\Rightarrow f(x)$ can be uniquely factorized

$F[x]/\langle x^2+1 \rangle$ is field isomorphic to complex numbers

$F[x]/x^2+1 = \{(x^2+1) + ax + b \mid a, b \in F\}$

Define $\phi((x^2+1) + ax + b) = ai + b.$

L Welldefined clearly (no proof)

Also 1-1, onto

$\phi((x^2+1) + ax + b) + (x^2+1) + a_1 x + b_1) = \phi((x^2+1) + (a+a_1)x + b + b_1)$

$= ai + b + a_1 i + b_1$

$= \phi((x^2+1) + ax + b) + \phi((x^2+1) + a_1 x + b_1)$

ϕ for product (Basic).

• Gauss Lemma.

If primitive polynomial $f(x)$ can be factored as product of 2 polynomials having rational coefficients, it can be factored as product of two poly with integer coefficients

→ Suppose $f(x) = u(x)v(x)$. (u, v have rational coeff)

By clearing denominators and taking out factors.

$f(x) = \frac{a}{b}\lambda(x)\mu(x)$ (where $a, b \in \mathbb{Z}$), (λ, μ are primitive)

So, $b \cdot f(x) = a\lambda(x)\mu(x)$.

As f is primitive $\Rightarrow c(f(x)) = b$

(content)

Also, $\lambda\mu$ is primitive $\Rightarrow$ content RHS $= a$

So, $a = b \Rightarrow \boxed{f(x) = \lambda(x)\mu(x)}$

Revise

• Eisenstein Criterion. $f(x) = a_0 + \dots a_n x^n$ be poly with integer coefficients

Suppose for some prime p, $p \nmid a_n$, $p \mid a_1, \dots p \mid a_0$, $p^2 \nmid a_0$. Then $f(x)$ is irreducible over rationals.

→ Assume $f(x)$ is primitive (WLOG) [as $p \nmid a_n$].

If $f(x)$ factors as two rational polynomials

↳ By Gauss Lemma → $f(x) = (b_0 + b_1 x + \dots b_r x^r)(c_0 + \dots c_s x^s)$

where b_i, c_j are integers

So, $a_0 = b_0 c_0 \rightarrow p \mid a_0$, $p^2 \nmid a_0 \rightarrow p \mid b_0$ or $p \mid c_0$ (not both).

Suppose $p \mid b_0$ and $p \nmid c_0$ → Not all $b_0, \dots b_r$ can be divisible by p or all coefficients of $f(x)$ would be divisible by p ($\rightarrow\leftarrow$).

Let b_k be 1st b not divisible by p $\Rightarrow a_k = b_k c_0 + b_{k-1} c_1 + \dots b_0 c_k$.

(divisible by p)

So $p \mid b_k c_0$ / But $p \nmid (c_0, b_k)$ $\rightarrow\leftarrow$ So, $f(x)$ cannot be factored.

Prove $1 + x + \cdots x^{p-1}$ is irreducible over rationals

$f(x)$ is irreducible iff $f(x+1)$ is irreducible in $\mathbb{Z}[x]$.

$$f(x) = \frac{1-x^p}{1-x} = \frac{x^p-1}{x-1}$$

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + {}^pC_1 x^{p-2} + \cdots {}^pC_{p-1} x + 0.$$

So, Using eisenstein criterion $\Rightarrow p \mid a_i \quad p \nmid 1$

$\Rightarrow f(x)$ is irreducible

* UFD.

- An integral domain R with unit element is a UFD if
  - any non-zero element in R is either a unit or can be written as product of finite number of irreducibles
  - Such decomposition is unique upto order and associates of irreducible elements

$\Rightarrow R[x] \equiv f(x) \in R[x] \Rightarrow f(x) = a f_1(x)$.
where $a = c(f(x))$ and $f_1(x)$ is primitive

$\Rightarrow R$ be a UFD $\rightarrow$ ID $\rightarrow$ it has a field of quotients F
If $f(x) \in F[x]$ then $f(x) = \frac{f_0(x)}{a}$,
where $f_0(x) \in R[x]$, $a \in R$. (Proof-!)

- If $f(x)$ in $R[x]$ is both primitive and irreducible then it is irreducible in $F[x]$ and vice-versa.

$\Rightarrow f(x) \in R[x]$ be irreducible in $R[x]$ but not in $F[x]$
$f(x) = g(x)h(x)$ $g(x), h(x) \in F(x)$ and of the degree

$g(x) = \frac{g_0(x)}{a} = \frac{\alpha\, g_1(x)}{a}$
$h(x) = \frac{h_0(x)}{b} = \frac{\beta\, h_1(x)}{b}$

$g_0(x), h_0(x) \in R[x]$
$\alpha, \beta \equiv c(g_0), c(h_0)$
g_1, h_1 primitive in $R[x]$

$f(x) = \frac{\alpha\beta}{ab} g_1(x) h_1(x) \Rightarrow ab\, f(x) = \alpha\beta\, g_1(x) h_1(x)$

As $f(x)$ and $g_1 h_1$ are primitive, content (LHS = RHS) $\Rightarrow ab = \alpha\beta$
So, $f(x) = g_1(x) h_1(x) \Rightarrow f(x)$ factorizable in $R[x]$ $\rightarrow\leftarrow$

$\Leftarrow$ If $f(x) = g(x)h(x)$ in $R[x]$ ($g, h \neq$ zero, unit)
But $R[x] \subset F[x] \Rightarrow g(x), h(x) \in F[x]$
So, $f(x) = g(x)h(x)$ in $F[x]$ $\rightarrow\leftarrow$

$f(x) \in F[x] \Rightarrow f(x) = \frac{f_0(x)}{a}$ $\quad a \in R$, $f_0(x) \in R[x]$

F is field of quotients of R

$\Rightarrow f_0 = b f_1(x)$. where $f_1(x)$ is primitive in $R[x]$

$R[x] \subset F[x]$ $\Rightarrow f(x) = \frac{b}{a} f_1(x)$.

R is UFD $\Rightarrow$ R[x] is also a UFD

Let $f(x) \in R[x]$ be non-zero, non-unit

- $f(x) = c f_1(x)$ where c is content(f). $f_1(x)$ is primitive.
- $f_1(x)$ is primitive in $R[x]$, then it can be factored in unique ways as a product of irreducibles in $R[x]$
- $f_1(x) = f_1'(x) f_1''(x) \dots f_1^{(n)}(x)$. where $f_1^{(i)}$ are irreducibles and this representation is unique upto associates
- Also $c \in R \Rightarrow c = c_1 c_2 \dots c_m$ where c_i are irreducibles
- So, we have $f(x) = c_1 c_2 \dots c_m f_1'(x) f_1''(x) \dots f_1^{(n)}(x)$.

Proof

$f(x) = \sum \frac{a_i}{b_i} x^i = \frac{a}{a} \sum \frac{a_i}{b_i} x^i$ $\quad a = \text{l.c.m}(b_i)$

$= \frac{1}{a} \sum \frac{a a_i}{b_i} x^i = \frac{1}{a} \sum a a' x^i = \frac{1}{a} f_0(x)$.

Factorize a polynomial

↳ 1st express it as a primitive in $R[x]$ ← content

* Properties from R to $R[x]$

- From $R[x]$ to R → obvious as ..... R is isomorphic to a subring of $R[x]$

1) R has unity iff $R[x]$ has unity.

⇒ R has unity 1 then $e(x) = 1 + 0x + 0.x^2 + \cdots$ is unity in $R[x]$

⇐ Let $R[x]$ have unity.

$\theta : R[x] \to R$ such that, $\theta(f(x)) = a_0$.

Then θ is onto homomorphism.

So, R is homomorphic image of $R[x]$ and has unity.

If $e(x)$ is unity of $R[x]$, then $\theta(e(x))$ is unity of R.

2) R is integral domain iff $R[x]$ is integral domain

⇐ (isomorphic to subring of $R[x]$)

⇒ R be I.D. $\quad f(x), g(x) \neq 0, \in R[x]$

$f(x) = a_0 + a_1 x + \cdots a_m x^m$

$g(x) = b_0 + b_1 x + \cdots b_n x^n$.

$f(x)g(x) = 0$ $\quad f(x)$ & $g(x)$ both can't be constants (as R is I.D.)

Atleast one of f, g is non-constant → its degree ≥ 1.

$\deg\{fg\} \geq 1 \Rightarrow fg \neq 0$. $\forall$

Either $f = 0$ or $g = 0$.

(3) Show $\frac{Z_3[x]}{I}$ where $I = \langle x^2+x+1 \rangle$ is not an integral domain.

$(x+2) + I \in \frac{Z_3[x]}{I}$

$\left((x+2)+I\right)^2 = (x+2)^2 + I = x^2 + 1.x + 1 + I$
$(4 \equiv 1)$

$= I$ = zero of $\frac{Z_3[x]}{I}$.

But, $(x+2)+I \neq I$.

So, $\frac{Z_3[x]}{I}$ is not an integral domain

(4) Show that ideal $A = \{xf(x) + 2g(x) \mid f, g \in Z[x]\}$ is not a principal ideal.

Suppose $A = \langle k(x) \rangle$.

$x = x(1+0\cdots) + 2(0 + 0x^2 + \cdots) \in A = \langle k(x) \rangle$

$\boxed{x = k(x)g(x)}$, Similarly $\boxed{2 = k(x)t(x)}$

(Cross multiplying)

$x \cdot k(x)t(x) = 2k(x)g(x) \Rightarrow \boxed{2g(x) = xt(x)}$

Each coeff of $t(x)$ is even $\Rightarrow t(x) = 2r(x)$

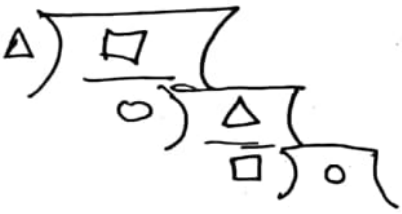
$2 = 2k(x)r(x) \Rightarrow r(x)k(x) = 1 \Rightarrow 1 \in \langle k(x) \rangle$

$\Rightarrow \langle k(x) \rangle = Z[x] = A$

But $1 \notin A$ or $1 = x(a_0 + a_1 x + \cdots) + 2(b_0 + b_1 x + \cdots)$

$1 = 2b_0 \Rightarrow b_0 = \frac{1}{2} \Rightarrow g(x) \notin Z[x]$ $\rightarrow\leftarrow$

⑤ Gcd →



• $11+7i$, $18-i$ in $\mathbb{Z}[i]$

$$\frac{18-i}{11+7i} \times \frac{11-7i}{11-7i} = \frac{191}{170} - \frac{137}{170}i$$

$$= \left(1 + \frac{21}{170}\right) - \left(1 - \frac{33}{170}\right)i$$

$$= (1-i) + \left(\frac{21}{170} + \frac{33i}{170}\right)$$

$$\boxed{(11+7i)(1-i) + 3i = 18-i}$$

$$\frac{11+7i}{3i} \times \frac{(-3i)}{(-3i)} = \frac{7}{3} - \frac{11}{3}i = (2-3i) + \left(\frac{1}{3} - \frac{2i}{3}\right)$$

$$\boxed{(3i)(2-3i) + (2+i) = 11+7i}$$

$$\frac{3i}{2+i} \times \frac{2-i}{2-i} = i + \left(\frac{3}{5} + \frac{1}{5}i\right)$$

$$3i = i(2+i) + (1+i)$$

$$\frac{2+i}{1+i} \cdot \frac{1-i}{1-i} = 1 + \left(\frac{1}{2} - \frac{1}{2}i\right)$$

$$(2+i) = (1+i) + 1$$

$$\frac{(1+i)}{1} = (1+i) + 0$$

$$\boxed{GD = 1}$$

(6) Prove $F[x]/\langle x^2+1\rangle$ is a field isomorphic to field of complex numbers. $F \equiv$ field of reals.

x^2+1 is irreducible over reals.
So, ideal $\langle x^2+1\rangle$ is maximal.
So, $F[x]/\langle x^2+1\rangle$ is a field
} Remember.

$F[x]/\langle x^2+1\rangle = \langle x^2+1\rangle + ax+b \mid a,b \in F$

TS: A one-one, onto homomorphism

φ: $\varphi(\langle x^2+1\rangle + ax+b) = b+ia$.

- φ is well-defined — Clearly
- Homomorphism.

$\varphi(\langle x^2+1\rangle + ax+b + (\langle x^2+1\rangle + a'x+b'))$

$= \varphi(\langle x^2+1\rangle + (a+a')x + (b+b'))$

$= (b+b') + i(a+a') = (b+ia)+(b'+ia')$

$= \varphi(\langle x^2+1\rangle + ax+b) + \varphi(\langle x^2+1\rangle + a'x+b')$

$\varphi((\langle x^2+1\rangle + ax+b).(\langle x^2+1\rangle + a'x+b'))$

$= \varphi(\langle x^2+1\rangle + (ax+b)(a'x+b'))$

$= \varphi(\langle x^2+1\rangle + (ab'+ba')x + (bb'-aa'))$

$= (a+ib)(a'+ib') = \varphi$ - - - -

- 1-1, onto — obvious

⑦ Show $Z_5[x]$ is a UFD.

$\Rightarrow$ $Z_5[x]$ is UFD if Z_5 is a UFD.

Here Z_5 is a field $\Rightarrow$ Z_5 is UFD

⑧ $\mathbb{Z}[i]/(1+3i) \cong \mathbb{Z}/10\mathbb{Z}$.

Let $\phi: \mathbb{Z} \to \mathbb{Z}[i]/(1+3i)$: $\phi(z) = z + (1+3i)\mathbb{Z}[i]$

- Then $\ker \phi = (1+3i)(a+bi)$ for some $a, b \in \mathbb{Z}$

$(1+3i)(a+bi) \in \mathbb{Z}$ iff $3a+b=0$.

$\ker \phi = \{(1+3i)(a-3ai) \mid a \in \mathbb{Z}\}$

$= \{a+9a+3ia-3ai \mid a \in \mathbb{Z}\} = \{10a \mid a \in \mathbb{Z}\}$

$= 10\mathbb{Z}$

- ϕ is onto

Let $(a+bi) + \langle (1+3i) \rangle \in \mathbb{Z}[i]/(1+3i)$

$a+bi = a - \frac{b}{3} + \frac{b}{3} + bi = a - \frac{b}{3} + \frac{b}{3}(1+3i)$

$\phi(a - \frac{b}{3}) = (a+bi) + \langle 1+3i \rangle$ So onto

Show $F[x]/(x^2+1) \cong F[x]/(x^2+x+4)$

$F \equiv \mathbb{Z}_{11}$

Trivial others

Let Map be:

$\theta: F[x]/\langle x^2+1\rangle \longrightarrow F[x]/\langle x^2+x+4\rangle$

$\theta\left[\alpha x+\beta+\langle x^2+1\rangle\right] = \alpha x + (\beta - 5\alpha)$.

2008

* n is +ve even integer s.t $a^n = a \ \forall a \in R$.
Show $a+a=0$ and $a+b=0 \Rightarrow a=b \ \forall a,b \in R$.

$a^n = a \rightarrow a = a^n$

$\rightarrow a = (-1)^n a^n$

$\rightarrow a = (-a)^n = -a$.

$a+b=0 \rightarrow a = -b$

$\rightarrow a^n = b^n \therefore a = b$.

* Find ideals of Z_{12}. Ideals of $Z_{12} \otimes Z_{12}$.

Describe maximal ideals of $\mathbb{Z}[i]$

. Show $\mathbb{Z}[i]$ is Euclidean Domain.

. Then $\mathbb{Z}[i]$ is PID.

. In PID maximal ideal $\equiv$ generated by prime p.

. So all primes p in $\mathbb{Z}[i]$ generate max. ideals

Find $([5]+[6])^{-1}$ and $(-[4])^{-1}$ in $\mathbb{Z}_7$.

$([11])^{-1} \equiv [4]^{-1}$ $\qquad [4][2] = [1]$

$\Rightarrow [4]^{-1} = \underline{[2]}$

$(-[4])^{-1} = [3]^{-1} = \underline{[5]}$

For polynomial rings ⇒

F is Integral Domain So is F[x]

UFD So is F[x]

direct from F to F[x]

Ring Examples

① Integral domain, not a field

- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$
- $\mathbb{J}[i] = \{a + bi \,/\, a, b \in I\}$ — Gaussian Integers

② Subring of non-commutative ring is commutative.

- $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

③ Subring has different identity than ring.

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv$ ring S.ring → $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ → $Id\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

④ ED ⇒ PID ⇒ UFD

⑤ Every element p, which is prime iff (p) is maximal.
holds true only for PID
(Show E.D, ⇒ PID, Then find maximal ideals)

⑥ $\mathbb{Z}$ is UFD ⇒ $\mathbb{Z}[x]$ is also UFD

$\mathbb{Z}$ is ED, PID, UFD

F is field ⟹ $F[x]$ is ED [Starting Point]

p is irreducible $\Rightarrow$ (p) is maximal

Only if F is PID $\quad (p \in F)$

R/M is field $\Leftrightarrow$ M is maximal ideal

R/M is I.D $\Leftrightarrow$ M is prime ideal

↑ For all prime ideal proofs – Very Useful.

In PID prime $\Leftrightarrow$ irreducible.

(To show not PID, Not ED)