14/11

Example

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

(Recall!)
R is an integral domain, and it is said to be Euclidean domain if $\exists\ \lambda$

$$\lambda : R \to \mathbb{N} \cup \{0\}$$

$a,b \in R$, $b \neq 0$ then $a = bq + r$ for some $q, r \in R$ and $r = 0$ (or) $\lambda(r) < \lambda(b)$

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

$$N(a+bi) = a^2 + b^2$$

Let $a+bi,\ c+di \in \mathbb{Z}[i]$, $c+id \neq 0$

If $c+di \mid a+bi$ in $\mathbb{Z}[i]$, then

$$r+si = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2}$$

$$= \frac{ac+bd + (bc-ad)i}{c^2+d^2} \in \mathbb{Q}[i]$$

If $r+si \in \mathbb{Q}$, we can pick $m,n \in \mathbb{Z}$ such that $|r-m| \leq 1/2$ and $|s-n| \leq 1/2$

$\alpha = a+bi$, $\beta = c+di$, $\delta = m+ni \in \mathbb{Z}[i]$

$$\Rightarrow (\alpha/\beta - \delta) = (r+si) - (m+ni)$$

$$N(\alpha/\beta - \delta) = N((r-m) + (s-n)i)$$

$$\leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$$

$$\Rightarrow N(\alpha - \beta\delta) < N(\beta)$$

$$\Rightarrow \alpha = \beta\delta + \alpha - \beta\delta$$

Exercise

- Verify if $\mathbb{Z}[\omega]$ is Euclidean $\omega = \frac{-1-\sqrt{-3}}{2}$ (??)

  $N(a+b\omega) =$

Definition

- Let $a, b \in R$. We say that $a \mid b$ if $\exists\, c \in R$ such that $b = ac$

- Two elements $a, b \in R$ are said to be associates if $a = bc$ for some unit $c \in R$

- A non-zero element (non-unit) $a \in R$ is said to be irreducible if $a = bc \Rightarrow b$ is a unit or c is a unit

- A non-zero element (non-unit) $p \in R$ is said to be prime if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

* For any integral domain, primes are irreducibles

(Proof)

Let $p \in R$ be a prime and $p = ab$

$\Rightarrow p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$

WLOG, assume $p \mid a$

$\Rightarrow \exists\, c \in R$ such that $a = pc$

$\Rightarrow p = pcb \Rightarrow p(1-cb) = 0$

$\Rightarrow 1 = cb$

$\Rightarrow b, c$ are units [Note that $p \nmid ab$ gave that b is unit if $p \mid a$]

$\Rightarrow p$ is irreducible

Converse need not be true!

Example

$$\mathbb{Z}[\sqrt{-5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$$

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$$

- 2 is irreducible

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

$\Rightarrow N(2) = (a^2 + 5b^2)(c^2 + 5d^2)$

$\downarrow$

$4 \qquad \{1, 2, 4\}$

$\Rightarrow a + bi\sqrt{5} = \pm 1$ or ± 2

- 2 is not prime

$2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$

But $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid 1 - \sqrt{-5}$

Definition

An element $d \in R$ is called a gcd of $a, b \in R$

if (a) $d \mid a$, $d \mid b$

(b) $d' \mid a$, $d' \mid b \Rightarrow d' \mid d$

Proof

Let $(d) = (a, b)$

$a \in (d) \Rightarrow d \mid a$

$b \in (d) \Rightarrow d \mid b$

Suppose $d' \mid a$, $d' \mid b$

$\Rightarrow (a) \subseteq (d')$ and $(b) \subseteq (d')$

$\Rightarrow (a, b) \subseteq d'$

$\Rightarrow (d) \subseteq d'$

$\Rightarrow d' \mid d$

$\Rightarrow (d)$ is gcd of a, b

Corollary

If $a, b \in R$ and $\gcd(a,b) = d$, then $\exists\, x, y \in R$ such that $ax + by = d$

In particular, if $\gcd(a,b) = 1$, then $(a,b) = R$

Corollary

If R is a PID, then irreducibles are primes

Proof

Suppose R is a PID and p is irreducible

Let $p \mid ab$ and $p \nmid a$

$\Rightarrow \quad ax + py = 1 \qquad (\exists\, x, y \in R)$

$\Rightarrow \quad abx + pby = b$

$\Rightarrow \quad p \mid b$

$\Rightarrow$ p is prime

Lemma

Let R be a PID and $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_k) \subseteq \cdots$ be a chain of ideals. Then $\exists\, k \in \mathbb{N}$ such that $(a_k) = (a_{k+l}) \quad \forall\, l > 0$

Proof

Let $I = \bigcup_{i=1}^{\infty} (a_i) \quad \Rightarrow \quad I \trianglelefteq R$

Then $I = (a)$

$\Rightarrow \quad a \in \bigcup_{i=1}^{\infty} (a_i)$

$\Rightarrow \quad a \in (a_k)$

$\Rightarrow \quad I = (a) = (a_k) = (a_{k+1})$

Proposition

In a PID, every non zero element can be written as product of irreducible elements

Proof

Let $a \in R$, $a \neq 0$

- First, we show that $\exists\, p \in R$ such that p is irreducible and $p \mid a$

If a is irreducible, we are done!

If not
$$a = b_1 c_1$$
$$\Rightarrow (b_1) \supseteq (a)$$

If b_1 is irreducible, we are done! Else
$$b_1 = b_2 c_2$$
$$\Rightarrow (a) \subseteq (b_1) \subseteq (b_2)$$

By the above Lemma, $\exists\, k \in \mathbb{N}$ such that $b_k \mid a$ for some prime $b_k \in R$.

- Let $a \in R \setminus \{0\}$

If a is prime, we are done

Otherwise $a = p_1 c$ for some prime $p_1 \in R$

If $c = p_2 c_1$, where p_2 is prime
if c_1 is unit, we are done!

If not, we continue
$$(c) \subseteq (c_1) \subseteq (c_2) \subseteq (c_3) \cdots$$
By the above Lemma, it stops at finite stage

Lemma

Let $p \in R$ be a prime and $a \in R \setminus \{0\}$

then $\exists\, n \geq 0$ such that $p^n \mid a$ but $p^{n+1} \nmid a$

Proof

Suppose contradiction of lemma is true

$\Rightarrow p^n \mid a \quad \forall n \in \mathbb{N} \cup \{0\}$

$$a \to p^n b_n$$
$$a \to p^{n+1} b_{n+1}$$
$$\vdots$$

$p^n b_n = p^{n+1} b_{n+1} \Rightarrow b_n = p\, b_{n+1}$

$\Rightarrow (b_n) \subseteq (b_{n+1})$

$(b_n) \subseteq (b_{n+1}) \subseteq \dots\dots$

By lemma, it stops at finite stage $(\rightarrow\leftarrow)$

$\Rightarrow$ Contradiction to lemma is not true

Definition

Let R be a PID, $a \in R \setminus \{0\}$ and p is prime

$\text{ord}_p\, a = \max\{n : p^n \mid a\}$

Lemma

$\text{ord}_p\, ab = \text{ord}_p\, a + \text{ord}_p\, b$

Let $\alpha = \text{ord}_p\, a$, $\beta = \text{ord}_p\, b$

$\Rightarrow a = p^\alpha c_1$ where $p \nmid c_1$

$b = p^\beta c_2$ where $p \nmid c_2$

$\Rightarrow ab = p^{\alpha+\beta} c_1 c_2$ $\qquad p \nmid c_1$ and $p \nmid c_2 \Rightarrow p \nmid c_1 c_2$

$\Rightarrow \text{ord}_p\, ab = \alpha + \beta$

$= \text{ord}_p\, a + \text{ord}_p\, b$

Let R be a PID and

$$S = \{ p \in R \mid \text{① } p \text{ is a prime; ② Any prime in } R \text{ is associate to some } \cancel{\text{}}\text{ prime in } S \text{; ③ No two distinct elements of } S \text{ are associates} \}$$

Theorem

Let R be a PID. Then any nonzero element $a \in R$ can be written as (uniquely!)

$$a = c \prod_{p \in S} p^{a(p)}$$

$$a(p) = \text{ord}_p a$$

(Proof)

Existence follows from proposition

$a = c \prod p^{(a(p))}$, For any $q \in S$

$$\text{ord}_q a = \sum a(p) \, \text{ord}_q p$$

$$= \sum_{p \neq q} a(p) \, \underbrace{\text{ord}_q p}_{\to 0} + a(p) \; (p = q)$$

$$= a(p) \; (p = q)$$

$$\Rightarrow \text{ord}_q a = a(q)$$

Definition

An integral domain is said to be a UFD (or) Unique Factorization Domain if any non-zero element can be written uniquely (upto an associate) as product of irreducible elements.

$$ED \Longrightarrow PID \Rightarrow UFD$$