Lecture 14: Unique factorization domain(UFD)

05 October 2020
11:30

Recall: 1) An int dom R is a ED if $\exists$ a norm $N: R^{\times} \to \mathbb{Z}_{\geq 0}$ s.t. $\forall a, b \in R^{\times}$ $\exists q, r \in R$ satisfying $a = bq + r$ with $r = 0$ or $N(r) < N(b)$.

2) An ID R is a PID if every R-ideal is principal (gen by 1 element)

- R ED $\Rightarrow$ R PID
- x irred if x nonzero nonunit & $x = yz \Rightarrow y$ is a unit or z is a unit
- x prime if " " " & $x | ab \Rightarrow x | a$ or $x | b$.
- R an int dom. x prime $\Rightarrow$ x irred.
- R PID. x irred $\iff$ x prime.
- R a PID then every nonzero prime ideal is maximal. $\mathbb{Z}[x]$ is not a PID.
- $R[x]$ is a PID iff R is a field.
- $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID but not a ED.
  - R is a PID iff R has Dedekind-Hasse norm. i.e. $N: R^{\times} \to \mathbb{Z}_{\geq 0}$ s.t. $\forall a, b$, $b | a$ or $\exists x, y \in R$ s.t. $N(ax + by) < N(b)$

    (Saw if part)
  - R is a ED but not a field. Then R has "universal side divisor" i.e. $u \in R$ nonzero nonunit s.t. $\forall x \in R$ either $u | x$ or $x - uq$ is a unit for some q in R.

Definition: Unique Factorization Domain (UFD).
Let R be an integral domain such that for any $x \in R$ nonzero nonunit, x can be uniquely written as product of irreducibles, where uniqueness means the following:

$x = p_1 \cdots p_n = q_1 \cdots q_m$ where $p_1, \ldots, p_n, q_1, \ldots, q_m$ are irreducible. Then

$n = m$ & after a reordering p_i & q_i are associates for all $1 \le i \le n$. "(i.e. $p_i = u_i q_i$ for some unit $u_i \in R$)"

Def^n: Let R be a comm ring with unity and $x, y \in R$ then x, y are said to be associates if $\exists\, u \in R$ unit s.t. $x = uy$.

It's denoted by $x \sim y$.

Note that $\sim$ is an equivalence relation

$\sim$ is reflexive & symmetric ✓

$x \sim y$ & $y \sim z \Rightarrow \exists\, u, v \in R$ units s.t. $x = uy$ & $y = vz$.

$\Rightarrow x = uvz$. But uv is a unit.

Hence $x \sim z$.

Ex: $\mathbb{Z}$ is a UFD.

x irred iff $y \mid x \Rightarrow [y] = [1]$ or $[y] = [x]$ (associate)

i.e. $y \sim 1$ or $y \sim x$

Prop: Let R be a PID then R is a UFD.

Pf: Let $x \in R$ be a nonzero nonunit

$\exists$ a maximal ideal $P_1 \subseteq R$ s.t. $x \in P_1$.

Then $P_1 = (p_1)$ & $x \in (p_1) \Rightarrow \exists\, x_2 \in R$

s.t. $x = x_1 = p_1 x_2$. Note p_1 is prime and hence irreducible

If x_2 is a unit then $x = x_1$ is irreducible. Stop.

Otherwise repeat to get

$x_2 = p_2 x_3$ where p_2 is irred & $x_3 \in R$.

$\Rightarrow x_1 = p_1 p_2 x_3$ if x_3 is a unit, then stop.

$= p_1 x_2$ is prod of irred. ($x_2 = p_2 x_3$ is irred. if x_3 is unit)

Otherwise continue ....

Suppose this never stops. Let $x_1, x_2, x_3, \ldots$ be obtained by this process.

$I = (x_1, x_2, x_3, \ldots)$ be the ideal

gen by $x_1, x_2, \ldots$

Since R is a PID $\exists\, y \in I$ s.t. $I = (y)$.

Note $(x_1) \subseteq (x_2) \subseteq (x_3) \subseteq \ldots$

$\boxed{\text{So } I = \bigcup_{i \geq 1} (x_i)}$. Hence $y \in (x_n)$ for some n.

Then $y = u x_n$ for some $u \in R$

Also $x_n = p_n x_{n+1}$, p_n irred.; $x_{n+1} \in (y) = I$

$\Rightarrow x_{n+1} = v y$ for some $v \in R$.

Hence $y = u x_n = u p_n x_{n+1} = u v p_n y$

$\Rightarrow u v p_n = 1$ is a unit. A contradiction!

(to p_n is irred. and hence nonunit)

Hence $\exists\, n$ s.t. x_n is a unit.

$\Rightarrow x = x_1 = p_1 x_2 = p_1 p_2 x_3 = \cdots = p_1 p_2 \cdots p_{n-1} x_n$

where $p_1, \ldots, p_{n-1}$ are irred.

So $x = p_1 \cdots p_{n-2} \cdot (p_{n-1} x_n)$

Uniqueness:

Let $x = p_1 \cdots p_n = q_1 \cdots q_m$ be product of irred. i.e. $p_1, \dots, p_n$ & $q_1, \dots, q_m$ are irred elements of R.

p_1 is irred & R is a PID $\Rightarrow p_1$ is a prime element. Since $p_1 \mid x = q_1 \cdots q_m$

$\overset{p_1 \text{ is a prime element}}{\Longrightarrow}$ $p_1 \mid q_{i_1}$ for some $i_1 \in \{1, \dots, m\}$

$\Rightarrow q_{i_1} = u_1 p_1$

But q_{i_1} is irred. so u_1 is a unit. $\Rightarrow p_1$ & q_{i_1} are associates

After reordering q_i's (i.e. interchanging q_1 & q_{i_1}) we obtain that p_1 & q_1 are associates. ($q_1 = \underset{\text{unit}}{u_1} p_1$)

$$x = \cancel{p_1} p_2 \cdots p_n = q_1 \cdots q_m = u_1 \cancel{p_1} q_2 \cdots q_m$$

$$\Rightarrow \quad p_2 \cdots p_n = u_1 q_2 \cdots q_m$$

$$\Rightarrow \quad p_2 \mid u_1^{-1} p_2 \cdots p_n = q_2 \cdots q_m$$

$\overset{p_2 \text{ is prime}}{\Longrightarrow}$ $p_2 \mid q_{i_2}$ for some $2 \le i_2 \le m$

So $q_{i_2} = u_2 p_2$ for some $u_2 \in R$

But q_{i_2} is irred., hence u_2 is a unit.

Again reorder q's to get $p_2 \sim q_2$

Continuing this way, we get a reordering of q's s.t. $p_i \sim q_i$ $1 \le i \le n$.

and $m \geq n$. But by symmetry $n \geq m$

Hence $n = m$. $\blacksquare$

Example: 1) $k[X]$ where k is a field.
2) $\mathbb{Z}[X]$ is a UFD.
3) $k[X_1, \dots, X_n]$ is a UFD for k a field or $k = \mathbb{Z}$.

Non examples: 1) $\mathbb{Z}[\sqrt{5}]$ or $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

2) $\bar{X}, \bar{Y}, \bar{Z}, \bar{W} \in \dfrac{\mathbb{Q}[X, Y, Z, W]}{(XY - ZW)} = R$

$\bar{X}\bar{Y} \in R$
$\overset{\shortparallel}{\bar{Z}\bar{W}}$

But $\bar{X}, \bar{Y}, \bar{Z}, \bar{W}$ are irred but none of them are assosiates to each other.

(*) Let R be a UFD & $x \in R$. Then x is irred $\Leftrightarrow$ x is prime.

Pf: Enough to show: $(\Rightarrow)$:
Suppose $x | ab$ for $a, b \in R$.
$\Rightarrow$ (*) $\boxed{ab = xy}$ for some $y \in R$
If a is unit or b is a unit then $x | b$ or $x | a$ and we are done.
Otherwise $\exists p_1, \dots, p_n \in R$ irred & $q_1, \dots, q_m \in R$ irred. s.t.
$a = p_1 \cdots p_n$ & $b = q_1 \cdots q_m$.
Also $y = r_1 \cdots r_k$ r_i irred. in R

$x r_1 \cdots r_k = p_1 \cdots p_n q_1 \cdots q_m$ from (*)
Uniqueness for irreducible factorization implies $x \sim p_i$ for some $1 \le i \le n$ or $\Rightarrow x | a$
$x \sim q_j$ " " $1 \le j \le m \Rightarrow x | b$