Lecture 15: UFD continued

07 October 2020

10:29

Recall: 1) R is a UFD if it is an int. domain and every nonzero nonunit can be written uniquely as product of irreducible elements of R.

2) A PID is a UFD. (Converse is not true)

3) R a UFD $\Rightarrow R[X]$ a UFD (Will be proved later)

4) In a UFD, irreducibles are primes.

5) $\mathbb{Z}[\sqrt{-3}]$ is not a UFD ; $\dfrac{\mathbb{Q}[X,Y,Z,W]}{(XY-ZW)}$ is not a UFD.

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

$a,b,c,d \in \mathbb{Z}$

Apply norm

$4 = (a^2+3b^2)(c^2+3d^2)$

May assume $b=0$

$(1+\sqrt{-3}) = a(c+d\sqrt{-3})$

$ac = 1$ & $ad = 1$

$\Rightarrow a = \pm 1 \Rightarrow 1+\sqrt{-3}$ is irred.

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 \Rightarrow 1+\sqrt{-3} \mid 4 = 2\cdot 2$

But $1+\sqrt{-3} \nmid 2$

$(1+\sqrt{-3})(a+b\sqrt{-3}) \neq 2 \quad \forall a,b \in \mathbb{Z}$

$\Rightarrow 1+\sqrt{-3}$ is not a prime.

$\overline{X}$ is irred. but not a prime.

Prop: Let R be a UFD and $a, b \in R$. Then

$a = u p_1^{e_1} \cdots p_r^{e_r}$ for some $r \geq 0$, $u, v \in R$ unit, $p_1, \ldots, p_r$ irred elements of R and

$b = v p_1^{b_1} \cdots p_r^{b_r}$ $\quad e_1, \ldots, e_r, b_1, \ldots, b_r \in \mathbb{Z}_{\geq 0}$.

and $\gcd(a, b) = p_1^{\min(e_1, b_1)} p_2^{\min(e_2, b_2)} \cdots p_r^{\min(e_r, b_r)}$

Pf: Since R is a UFD

$a = u p_1^{e_1} \cdots p_n^{e_n}$ for some $n \geq 0$, $p_1, \ldots, p_n, u \in R$ with u unit $p_1, \ldots, p_n$ irred & $e_1, \ldots, e_n \in \mathbb{Z}_{>0}$.

and $b = v p_1^{b_1} \cdots p_n^{b_n} p_{n+1}^{b_{n+1}} \cdots p_r^{b_r}$ for some $r \geq n$, $v \in R$ unit, $p_{n+1}, \ldots, p_r$ irred. & $b_1, \ldots, b_r \in \mathbb{Z}_{\geq 0}$

Set $e_{n+1} = e_{n+2} = \cdots = e_r = 0$

Let $d = p_1^{\min(e_1, b_1)} \cdots\cdots p_r^{\min(e_r, b_r)}$ then

$d \mid a$ & $d \mid b$. Let $d' \mid a$ & $d' \mid b$.

$(\because a = d u p_1^{e_1 - \min(e_1, b_1)} \cdots\cdots p_r^{e_r - \min(e_r, b_r)})$

Then $a = d' a_1$ & $b = d' b_1$. By uniqueness of factorization in UFD, factorizing d' we get, $d' = w p_1^{l_1} \cdots p_r^{l_r}$ with w unit & $l_i \leq e_i$ (as $d' \mid a$) and $l_i \leq b_i$ (as $d' \mid b$)

Hence $l_i \leq \min(e_i, b_i) \Rightarrow d' \mid d$. $\Rightarrow$

$d = \gcd(a, b)$. $\blacksquare$

Prop: Every PID admits a Dedekind-Hasse norm.

Pf: $N : R^{\times} \longrightarrow \mathbb{Z}_{>0}$

units $\longmapsto 1$

x non unit, $x = p_1 \cdots p_n \longmapsto 2^n$ where p_i irred.

$N(x) = 2^n$

WTS:
Let $a, b \in R$ either $b \mid a$ or $\exists\, x, y \in R$

s.t. $N(ax + by) < N(b)$.

Suppose $b \nmid a$. Let $(d) = (a, b)$

$d \mid b$ & $b \nmid d$ ($\because$ if $b \mid d$ $\Rightarrow b \mid a$)

Let $d = p_1 \cdots p_n$ then

& $b = p_1 \cdots p_n q_1 \cdots q_m$ & $m \geq 1$

$\Rightarrow N(d) = 2^n < N(b) = 2^{n+m}$

& $d = ax + by$ for some $x, y \in R$. ∎

"$N(x) = n+1$ should work"

Thm: Let R be an integral domain. R is a UFD iff

1) Every irred element in R is prime and
2) Every strictly increasing chain of principal ideals is of finite length.

Pf: $(\Rightarrow)$: (1) ✓

(2): Let

$(0) \subsetneq (x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \cdots$ be a strictly increasing chain of principal ideals.

Let $x_1 = p_1 \cdots p_n$ $\quad p_i \in R$ irred.

$$\left.\begin{array}{l} x_1 \in (x_2) \Rightarrow x_2 \mid x_1 \\ \& \ (x_2) \neq (x_1) \Rightarrow x_1 \nmid x_2 \end{array}\right\} \quad x_1 = x_2 y_1 \text{ for } y_1 \in R$$

where y_1 is nonzero non unit

No of irreducible factors in x_2 is strictly less than n. $\quad$ Let $x_2 = q_1 \cdots q_m$ as prod of irr
$y = r_1 \cdots r_k$

$$p_1 \cdots p_n = q_1 \cdots q_m r_1 \cdots r_k$$

Uniqueness $\Rightarrow$ $m+k=n \Rightarrow m<n$

$|||^{ly}$ No of irr factors of x_3 < No of irr factors of x_2 and so on. So the length of the chain of the principal ideals

$(x_1) \subsetneq (x_2) \subsetneq \cdots$ can be at most n.

$(\Leftarrow)$:

Let $x \in R$ nonzero nonunit.

Want to show x is a product of irreducibles.

Claim: $x = p_1 y$ where p_1 is irred. & $y \in R$.

If x is irred then done.

otherwise $\exists\, x_1, y_1 \in R$ s.t.

$x = x_1 y_1$ where x_1 & y_1 are nonunits.

$\Rightarrow (x) \subsetneq (x_1)$ ($\because y_1$ is nonunit)

Now if x_1 is irred then we have shown that $x = p_1 y_1$ where p_1 is irred in R & $y_1 \in R$ with $p_1 = x_1$

otherwise

$x_1 = x_2 y_2$ where x_2, y_2 are nonunit.

and $(x_1) \subsetneq (x_2)$

Continuing this way we obtain a strictly increasing seq of principal ideals

$(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$

So by (2) it must stop say at n^{th} spot. So x_n must be irred.

So $x = x_1 y_1 = x_2 y_2 y_1 = \cdots = x_n y_n y_{n-1} \cdots y_1$

$\Rightarrow x = p_1 y$ where p_1 is irred in R & $y \in R$.

with $p_1 = x_n$ & $y = y_1 \cdots y_n$

Claim: $x = p_1 \cdots p_n$ where $p_i \in R$ are irred.

Pf: By prev claim

$x = p_1 y_1$ for some $p_1 \in R$ irred & $y_1 \in R$.

If y_1 is a unit or irred then done

otherwise

$y_1 = p_2 y_2$ where p_2 irr & $y_2 \in R$

and continue this way if y_2 is not irred.

$(x) \subsetneq (y_1) \subsetneq (y_2) \subsetneq \cdots$

(strictness is true because p_1, p_2 are irred & hence not a unit)

Again by (2) this has to stop at ~~say~~ after n steps. Then

$x = p_1 \cdots p_n y_n$ as product of irred.

Exc: Show uniqueness of irred factorization using (1).

Hint: See PIDs are UFDs proof.