Lec 12/4

Tuesday, December 4, 2018 11:31

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is P.I.D. but not Euclidean

$$\text{Field} \Rightarrow \underset{\uparrow \text{ euclid}}{\text{Euclidean}} \Rightarrow \text{P.I.D} \underset{\uparrow \text{ primary decomp. thm}}{\Longrightarrow} \text{U.F.D}$$

(easy: Euclidean $\Rightarrow$ U.F.D) (all inclusions are proper).

1: $\mathbb{Z}[x]$ is not a p.i.d but it is a u.f.d. (by Gauss Lemma R: ufd $\Rightarrow$ $R[x]$: ufd)

↳ $(2,x)$ is not principal $\neq (a+bx)$ for any $a,b \in \mathbb{Z}$

2: $R = \mathbb{Z}[\sqrt{-3}] \neq \mathcal{O}(\sqrt{-3}) = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Prove R is not a U.F.D.

$(1-\sqrt{-3})(1+\sqrt{-3}) = 4 = 2\cdot 2$. Show $2, 1\pm\sqrt{-3}$ are irreducible.

a is irred. if $a = b\cdot c \Longrightarrow b \in R^{\times}$ or $c \in R^{\times}$.

Alternately: 2 is irreducible, $(2) \ni (1-\sqrt{-3})(1+\sqrt{-3})$ is not a prime ideal
$\Rightarrow R$ is not a U.F.D. (in a UFD, $\left(\begin{smallmatrix}\text{irred}\\ \text{elt}\end{smallmatrix}\right)$ is prime).

Aside: $N: \mathbb{Z}[\sqrt{-3}] \longrightarrow \mathbb{Z}_{\geq 0}$. If $N(a+b\sqrt{-3}) = a^2+3b^2$ then $N(\alpha\beta) = N(\alpha)N(\beta)$.

If $\alpha \neq 0$, $\beta \in R$, $\frac{\beta}{\alpha} \in \mathbb{Q}[\sqrt{-3}]$.

$$\exists\, m,n \text{ s.t. } \Big|\underbrace{\frac{\beta}{\alpha} - m - n\sqrt{-3}}_{r = p+q\sqrt{-3} \text{ where } p,q \in [-\frac{1}{2},\frac{1}{2}]}\Big|^2 \leqslant \frac{1}{4} + \frac{3}{4}$$

$$\Rightarrow \beta = (m+n\sqrt{-3})\alpha + \underbrace{r\alpha}$$

↳ remainder has norm $\leq$ norm(α)

(Not $<$)

3: $\underset{\text{field.}}{K}[x]$ (Eisenstein Criterion).

$f(x) = a_n x^n + a_{n-1} x_{n-1} + \cdots + a_0 \in R[x]$ is primitive, R is U.F.D.

If $\exists$ prime ideal $P \subsetneq R$ s.t. $a_n \notin P$, $a_{n-1}, \dots, a_0 \in P$, $a_0 \notin P^2$,

then $f(x)$ is irreducible.

(recall primitive if $c | a_i \ \forall i \Rightarrow c \in R^{\times}$ (i.e. gcd of coeffs is 1)).

Pedestrian's Criterion

$f(x) \in K[x]$, $\deg(f) = 2$ or 3 $\quad f(x)$ irred $\Leftrightarrow f(\alpha) \neq 0 \ \forall \alpha \in K$.

eg $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irred.

4: $x^p - x \in \mathbb{F}_p[x]$

$\quad \| $

$x(x^{p-1} - 1)$. $\quad x^{p-1} - 1 = \prod_{\alpha \in \mathbb{F}_p \setminus \{0\}} (x - \alpha)$. t.s. $\alpha^{p-1} = 1 \ \forall \alpha \neq 0$.

True b.c. $\mathbb{F}_p \setminus \{0\}$ is a mult group and $\operatorname{ord}(\alpha) \mid p-1$.

So RHS | LHS, but they have the same degree.

K: char K = p prime

$$\begin{array}{ccc} K & \xrightarrow{\sigma_p} & K \\ x & \longmapsto & x^p \end{array} \qquad \sigma_p(\alpha) = \alpha \quad \forall \alpha \in \mathbb{F}_p \subseteq K.$$

<u>Local Rings</u>:

$\mathbb{Q}[x]$ is local. F

PID - every ideal is cyclic

Local - only one max'l ideal

Local rings:

(1) $\mathbb{Q}[x] / (x^7)$ — still a P.I.R — not D!

- only one prime ideal

i.e. every elt is either a unit or nilpotent

any ring → R / M^ℓ ← any max'l ideal

(2) $R = \left\{ \dfrac{f(x,y)}{g(x,y)} \;\middle|\; g(0,0) \neq 0 \right\}$, $f(x,y), g(x,y) \in \mathbb{Q}[x,y]$.

$= S^{-1}\mathbb{Q}[x,y]$

$S = \mathbb{Q}[x,y] \setminus (x,y)$

$M = \left\{ \dfrac{f(x,y)}{g(x,y)} \;\middle|\; \begin{array}{l} f(0,0) = 0 \\ g(0,0) \neq 0 \end{array} \right\}$

- M is an ideal $(= (x,y))$
- $M \sqcup R^\times = R$

$\Rightarrow$ (R, M) is a local ring

(7) $\mathbb{Z}[x] / (x^2 - 5) \cong \mathbb{Z}[\sqrt{5}]$

$$\mathbb{Z}[x] \xrightarrow{\text{eval}} \mathbb{Z}[\sqrt{5}]$$

$$n \in \mathbb{Z} \longmapsto n$$

$$x \longmapsto \sqrt{5}$$

$$a + bx \longmapsto a + b\sqrt{5} \quad \Rightarrow \text{surj} \checkmark$$

$$x^2 - 5 \in \operatorname{Ker}(\text{eval}) \subsetneq \mathbb{Z}[x]$$

$$\operatorname{Ker}(\text{eval}) \supseteq (x^2 - 5)$$

Prove $(x^2 - 5) \supset \operatorname{Ker}(\text{eval})$.

$g(\sqrt{5}) = 0 \Rightarrow$ g is div by $x^2 - 5$

$$\left(\begin{array}{l} \text{Over } \mathbb{R},\ g(x) \text{ is div by } x - \sqrt{5},\ x + \sqrt{5} \\ g(x) = (x^2-5)\,\bar{g}(x) \text{ over } \mathbb{R}[x], \\ \text{T.S. coeff of } \bar{g} \text{ are in } \mathbb{Z}. \end{array} \right).$$

$\int$ilm burn