Lec 7

Last time: Unique Factorization Domain!

- If R is Noetherian $\Rightarrow$ every elt factors into irreds
- If R has factorization into irreds
  R is a UFD $\Leftrightarrow$ All irreds are prime!

Thm Every PID is a UFD

Pf Let R be a PID

- R is Noeth b/c every ideal gen'd by 1 elt (so certainly fin gen)

Let π be an irred. WTS π is prime.

Suppose $\pi \mid xy$

Consider (π, x) as R PID $\exists\, a \in R$ so $(\pi, x) = (a)$

$\Rightarrow \pi \in (a) \Rightarrow a \mid \pi$, since π irred 2 cases.

1) $a \nsim \pi$ since $x \in (a)$, $a \mid x$ so $\pi \mid x$

2) a is a unit $\Rightarrow (\pi, x) = (1)$

$\Rightarrow (a) = R$ $\quad \exists\, u, v \in R$ so $u\pi + vx = 1$ (multiply)

$\Rightarrow u\pi y + vxy = y$

$\pi \mid u\pi y + vxy \Rightarrow \pi \mid y$

(by hypothesis)

Rmk In any domain, can define gcd

i.e. d is gcd of x, y if $d \mid x$ & $d \mid y$ & $(e \mid x, e \mid y \Rightarrow e \mid d)$

Rmk 2 gcd's always exist in UFD

But don't always have Bezout. $\mathbb{C}[x, y]$ with x, y their gcd is 1 but can't get 1 from x, y.

3) in a PID get Bezout

$(x,y) = (d) \iff d = \gcd(x,y)$

Def) R is a domain. A **euclidean fnc** is a fnc

$\varphi : R \setminus \{0\} \longrightarrow \{0, 1, 2, \dots\}$

s.t the following div alg holds

given $x, y \in R$, $y \neq 0$ $\exists\, q, r \in R$

s.t $x = yq + r$ with $\varphi(r) < \varphi(y)$ or $r = 0$

A **euclidean domain** is a domain w/ Euc fnc

Prop) Every Euclidean domain R is a PID

Pf) let $I \subseteq R$ be a nonzero ideal

let $y \in I$ with $\varphi(y)$ minimal

Claim) $I = (y)$

let $x \in I$ be given. Write $x = yq + r$

$\Rightarrow r \in I$ as $r = x - yq$ ($x \in I$, $yq \in I$)

where $r = 0$ or $\varphi(r) < \varphi(y)$

↳ not possible by choice of y

$\Rightarrow x = qy \in (y)$

Ex) 1) $\mathbb{Z}$ is a euclidean domain.

let $\varphi(x) = |x|$

2) If F is a field then $F[x]$ is a euclidean ring where $\varphi(f) = \deg(f)$

3) $\mathbb{Z}[i]$ is a euclidean domain.

$\varphi(a+bi) = a^2 + b^2 = |a+bi|^2$

let $x, y \in \mathbb{Z}[i]$, $y \neq 0$

let $q \in \mathbb{Z}[i]$ be nearest Gaussian int to $\frac{x}{y} =: q + \varepsilon$

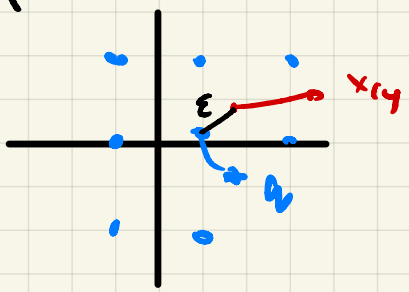
So, $x = yq + yε$ → r

$\varphi(r) = \varphi(yε) = |εy|^2 = |ε|^2 \varphi(y) < \varphi(y)$ (complex absolute)

as $|ε|^2 < 1$

Note $ε = α + iβ$ & $|α|, |β| \le \frac{1}{2}$

So, $|ε|^2 \le 1/4 + 1/4 = 1/2 < 1$



4) $ω = e^{\frac{2πi}{3}} = \frac{-1+\sqrt{-3}}{2}$ 3 root of unite

$\mathbb{Z}[ω] = \{a + ωb \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

euclidean w/

$\varphi(z) = |z|^2$ $\varphi(a+bω) = a^2 - ab + b^2$

The ring of integers in $\mathbb{Q}(\sqrt{d})$ a.s. $d \in \mathbb{Z}$ sqr free is $R_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod 4 \end{cases}$

$R_d = \{x \in \mathbb{Q}(\sqrt{d}) \mid \exists \text{ monic } f \in \mathbb{Z}[t] \text{ s.t. } f(x) = 0\}$

So, $\mathbb{Z}[ω] = R_{-3}$ & $\mathbb{Z}[i] = R_i$

Facts! 1) R_{-1} & R_{-3} are euclidean (PID ⇒ UFD)

2) R_{-5} is NOT UFD $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

3) R_{-19} is a PID, but not Euclidean

4) R_{69} is euclidean but not norm euclidean (N not eu)

5) For R_d UFD ⇔ PID

In R_d get norm $N(x + y\sqrt{d}) = x^2 - dy^2$

↳ consider this $d = -3$

Relf equ

6) $\exists$ exactly 9 $d<0$ s.t R_d is a PID (Sm no ex)

7) Unknown if $\exists \infty$ many $d>0$ s.t R_d is PID

8) If $d<0$ then $R_0^\times$ is finite

9) for $d>0$, $R_d^\times$ is $\mathbb{Z}$ or $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

<u>Soln</u> of Pell eqn $=1$ are units in R_d