Recall: Q: Is x^2+1 reducible in $R = (\mathbb{Z}/5)[x]$?

factors: $(x+2)(x+3) = x^2+5x+6 \equiv x^2+1 \pmod 5$.

whenever $\exists$ solution to $x^2+1=0$.

i.e. asking: $\exists x$ s.t. $x^2 \equiv -1 \ (5)$.

$x^2+y^2 \equiv 0 \pmod p$ $(\Leftrightarrow p \equiv 1 \ (4)$ or $p=2)$.

$x^2 \equiv -y^2 \Leftrightarrow (x\bar{y})^2 \equiv -1$. $(y \cdot \bar{y} \equiv 1)$.

Rings, Ideal, Euclidean Domain $\Rightarrow$ PID.

Thm: Ring is Euclidean $\Rightarrow$ PID.

pf: Let $I \subset R$ be an ideal. $(\& \ I \neq (0))$.

Look at $S = \{N(n) : n \in I \setminus \{0\}\} \subseteq \mathbb{N}$.

$N : R \setminus \{0\} \to \mathbb{N}$. Let $s \in S$ be least.

Let $d \in I$ be s.t. $N(d) = s$.

(If $I = (n_1, \dots, n_k)$, then $d = \gcd(n_1, \dots, n_k)$),

$\Rightarrow (d) \subset I$. Claim: $I = (d)$.

$\square$

Take any $m \in I$. By division algorithm,

$\exists q, r$ s.t. $m = dq + r$ & $\begin{cases} N(r) < N(d) \\ \text{OR} \\ r = 0 \end{cases}$

Can't happen, since d has least norm!

$\Rightarrow r = 0 \Rightarrow m = dq$.

$\Rightarrow m \in (d) \Rightarrow I \subset (d) \subset I$ ∎

Next claim: PID $\Rightarrow$ Noetherian.

Recall: R is Noetherian if: whenever $I_1 \subset I_2 \subset I_3 \subset \cdots$, then $\exists N$ s.t. $\forall n \geq N$, $I_n = I_N$.

$A \subsetneq B$

In $R = \mathbb{Z}$, $I_1 = (25, 75) = (25)$

$(25) \subseteq (25) \subseteq (25) \subseteq (5) \subseteq (5) \subseteq (1) = R$.
($25\mathbb{Z}$, $5\mathbb{Z}$.) $\subseteq (5) \subseteq \cdots$

Given $n_1, n_2, \ldots$ $I_1 = (n_1) \subseteq I_2 = (n_1, n_2)$

$R = \mathbb{Z}^{\mathbb{N}} = (n_1, n_2, n_3, \ldots) \ni [3, 1, 4, 1, 5, 9, \ldots]$.

($n_1 \in 2\mathbb{Z}$, $n_2 \in 2\mathbb{Z}$)

In this ring, $I_1 = ([1, 0, \ldots, 0]) \subset ([1, 0, \ldots, 0], [0, 1, 0, \ldots, 0]) = I_2$

Not Noetherian $\subset I_3 \subset \cdots$

Exercise: Demonstrate that $\mathbb{Z}[\sqrt{-5}]$ is not Noetherian (~~Prob.~~ Q: Is there an increasing sequence of ideals?).

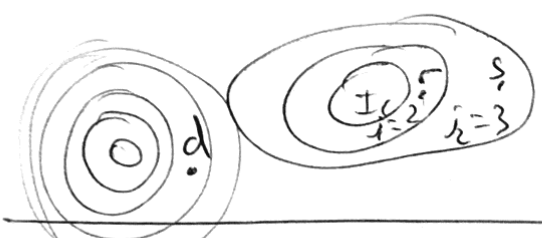
Recall pf that PID $\Rightarrow$ Noetherian:

Let R be a PID, Let

$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ increasing chain of ideals. Exercise 1: $I = \bigcup_{\text{nested}} I_j$ = ideal.

(Non-e.g.: $S = \underbrace{(2) \cup (3)}_{\not\ni 7} \begin{cases} \stackrel{?}{=} \mathbb{Z} = R & 2 \in S \\ \stackrel{?}{=} (6) & 3 \in S \\ & 2+3 = 5 \notin S. \end{cases}$)

Solution: Let $r, s \in I$, $r \in I \Rightarrow \exists j_1$ s.t. $r \in I_{j_1}$ & $\exists j_2$ s.t. $s \in I_{j_2}$ (Let $j = \max(j_1, j_2)$).



$r, s \in I_j \in$ ideal $\Rightarrow$ $r+s \in I_j \subset I$.

So $I = \cup I_j$ is an ideal. $\Rightarrow I = (d)$. Since R is a PID. But $d \in I = \cup I_j$ so $\exists N$ s.t. $d \in I_N \Rightarrow (d) \subset I_N$ (B) so $I \subset I_N$.

So: All ideals I_n after I_N $\subset I_n$, But they can't add any new elements to I.

Last step: Noetherian $\Rightarrow$ UFD. ($\Rightarrow \mathbb{Z}[\omega]$ UFD).

Lemma: If R is Noetherian, then any element $r \in R$ is a finite product of units & irreducibles. ($s|r \Rightarrow s \in R^\times$ or $(s)=(r)$).

Pf: If r is not irreducible $\Rightarrow \exists\, r_1 | r$, $r_1 \notin R^\times$ & $(r_1) \neq (r)$. If r_1 not irreducible, then $\exists\, r_2 | r_1$ & $r_2 \notin R^\times$ & $(r_2) \neq (r_1)$.

Claim: $\exists$ some $\ell | r$, ℓ irreducible

$$\vdots$$

$$(r) \subsetneq (r_1) \subsetneq (r_2) \subsetneq (r_3) \subsetneq \cdots$$

But R is Noetherian, so can't go on forever. Must stop, stops when r_j = irreducible.

$$r_j \mid r_{j-1} \mid r_{j-2} \cdots \mid r \Rightarrow \exists\, \ell \mid r,$$

ℓ = irreducible.

Why is $r = u \cdot \ell_1 \cdots \ell_n$ ← irreducibles? (unit).

Just showed that $\exists\, \ell_1 | r$, ℓ_1 irreducible.

So ∃ s_1 s.t. $r = \ell_1 \cdot s_1$. So if $s_1 \neq$ irred,
$\exists\, \ell_2 \mid s_2$, ℓ_2 = irred., $s_2 = \ell_2 \cdot s_3$.

$$(r) \subsetneq (s_1) \subsetneq (s_2) \subsetneq (s_3) \subsetneq \cdots$$

Claim must stabilize/stop. So some s_J = irred.
& $r = \ell_1 \cdots \ell_J \cdot s_J$ · all irreducibles.

~~Lemma: Given prime $p \in R$.~~

Exercise 2: In PID, prime ⟺ irreducible.

Recall p prime if $p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$.

→ If p is prime & $r \mid p$. Want: $r \in R^\times$ or $(r) = (p)$.

Assume R is Noetherian

Lemma: Given prime (≠ 0) $p \in R$, &
$a \in R$, $\exists\, n \in \mathbb{N}$ s.t. $p^n \| a$. i.e.
$p^n \mid a$ & $p^{n+1} \nmid a$. ($\Rightarrow \mathrm{ord}_p(a) = n$).

Pf: If $p \mid a$, $a = p \cdot a_1$ if $p \mid a_1$, $a_1 = p \cdot a_2$, ...
So: $(a) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots$ Must STOP.
$\Rightarrow p^n \mid a$ & $p^{n+1} \nmid a$. (5)

Lemma: If R Noetherian & p prime $\Rightarrow$

$$ord_p(a \cdot b) = ord_p(a) + ord_p(b) \quad (a,b \in R \setminus \{0\})$$

Pf = same as for $\mathbb{Z}$.

$\mathbb{Z}[\sqrt{5}]$ ← has primes & irred.
& some irreducibles (eg. $\underline{(1+\sqrt{5})}$) are not prime.
$1 \cdot 3$

Pf: If $p^n \| a$ & $p^m \| b$ $\Rightarrow$

$p^{n+m} \mid a \cdot b$ since $a = p^n \cdot a_1$ & $b = p^m \cdot b_1$

So $a \cdot b = p^{n+m} \cdot a_1 \cdot b_1$ & $(a_1, p) = R$, $(b_1, p) = R$.

So $p \nmid a_1 \cdot b_1$ since $p \nmid a_1$ & $p \nmid b_1$, $p^{n+m} \| a \cdot b$

Thm (Noetherian $\Rightarrow$ UFD): Any $r \in R^{\{0\}}$ is uniquely expresses as $r = u \cdot \prod p^{e_p}$ ← $e_p \in \mathbb{N}$

unit ← u ; p ← prime

& $e_p = ord_p(r)$.

Fix some list of (up to $\sim$) non-associate primes.

Pf: Fix prime q & take ord_q of both sides (6).