# Lecture 4: PIDs have unique factorization



**Last time:** $R$ int. domain, $r$ non-zero

**Irreducible:** $r = ab \Rightarrow$ one of $a, b$ is a unit

**Prime:** $r \mid ab \Rightarrow r \mid a$ or $r \mid b$ ($\Rightarrow$ irreducible)

**Associates:** $r = us$ for $u$ a unit.

**Unique Factorization Domain:** An int. domain $R$ where for each non-unit $r \neq 0$ in $R$

(a) $r = p_1 p_2 \cdots p_n$ with $p_i$ irreducible

(b) $r = \underbrace{q_1 \cdots q_m}_{\text{irreducible}} \Rightarrow n = m$ and, after reordering, $q_i$ is an assoc of $p_i$.

---

**Prop:** In a PID, an irreducible $r$ is prime.

**Pf:** Recall $r$ prime $\Leftrightarrow$ $(r)$ is prime. Will show $(r)$ is maximal. If $(r) \subseteq (m) \subseteq R$ then $r = s \cdot m$. By irred of $r$ either

(a) $s$ is a unit $\Rightarrow (r) = (m)$

(b) $m$ is a unit $\Rightarrow (m) = R$

So $(r)$ is maximal and hence prime.

# Basic props of UFDs.

① Prime elts are irreducible.

② gcd's work as expected:

$$\left.\begin{array}{l} a = u p_1^{e_1} \cdots p_n^{e_n} \\ b = \underset{\uparrow \atop \text{unit}}{u'} \underbrace{p_1^{e_1'} \cdots p_n^{e_n'}}_{\substack{\text{non-assoc.} \\ \text{irreducibles}}} \end{array}\right\} \Longrightarrow \gcd(a,b) = \underbrace{p_1^{\min(e_1,e_1')} \cdots p_n^{\min(e_n,e_n')}}_{g.}$$

$e_i$ and $e_i'$ poss 0

Pf's: See section 8.3 or next page of these notes.

Pf of 1: Suppose an irreducible $r$ divides $ab$, i.e. $ab = cr$. Expand $a, b, c$ as prod of irred $(a_1 \cdots a_j)(b_1 \cdots b_k) = (c_1 \cdots c_\ell) r$. By uniqueness, some $a_i$ or $b_i$ is an assoc of $r \Rightarrow r | a$ or $r | b$. ▨

Pf of 2: Clearly $g | a$ and $g | b$. If a common divisor $d = q^e r$ where $q$ is irred, then $a = q^e r s$ and $b = q^e r s'$; since $rs$ and $rs'$ have factorizations, uniqueness means $q$ is an assoc of some $p_i$ and $e \le \min(e_i, e_i')$. ▨

Thm: A PID has unique factorization.

Pf: Let $r \in R$.

A. $r = p_1 p_2 \cdots p_n$ with $p_i$ irreducible.

If $r$ is irreducible, then done. Otherwise $r = r_1 s_1$ for non-units $r_1$ and $s_1$. Continue by factoring $r_1$ and $s_1$, if possible. Either we eventually get a factorization, or we have sequences

$r_0 = r, r_1, r_2, \ldots$ and $s_1, s_2, \ldots$ of nonunits with $r_k = r_{k+1} s_{k+1}$ for $k \geq 0$.

Set $I_r = (r_k)$. Then $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ since $r_k \in I_{k+1}$ and $I_k = I_{k+1}$ would imply $r_{k+1} = q r_k = q r_{k+1} s_{k+1} \Rightarrow s_{k+1}$ is a unit.

Set $I = \bigcup_k I_k$ an ideal of $R$. As $R$ is a PID, have $I = (a)$. Must have a $k$ with $a \in I_k$, but then $I_k = I_j = I$ for $j \geq k$ a contradiction. So $r$ has a factor. into irreducibles.

B. Uniqueness. Suppose $r = q_1 q_2 \cdots q_m$ is some other factorization. As $R$ is a PID, each $p_i$ is prime. Hence $p_1$ divides some $q_i$, say $q_1 = u p_1$. As $q_1$ is irred, $u$ is a unit and so $p_1$ and $q_1$ are associates. So

$$p_2 p_3 \cdots p_n = (u^{-1} q_2) q_3 \cdots q_m$$

and now repeat. $\square$

<u>Thm</u> $p \in \mathbb{Z}$ an odd prime. Then $p = a^2 + b^2$ for $a, b \in \mathbb{Z} \iff p \equiv 1 \bmod 4$. [Will prove using that $\mathbb{Z}[i]$ is a UFD.

<u>Ex</u>: $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, etc.

<u>Note</u>: ($\Rightarrow$) is clear since $a^2, b^2 \equiv 0$ or $1 \bmod 4$ and $p \equiv 1$ or $3 \bmod 4$.

<u>Connection</u>: $p = a^2 + b^2 \iff p$ is reducible in $\mathbb{Z}[i]$

<u>Recall</u>: The norm $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ is $N(a+bi) = |a+bi|^2 = a^2 + b^2$.

<u>Pf</u>: ($\Rightarrow$) If $p = a^2 + b^2$ then $p = (a+bi)(a-bi)$ in $\mathbb{Z}[i]$. Neither factor is a unit since they have norm $p \neq 1$.

($\Leftarrow$) Suppose $p = \alpha \cdot \beta$ for nonunits $\alpha, \beta$. Then $p^2 = N(p) = N(\alpha \cdot \beta) = N(\alpha) N(\beta)$.

Since the only elts in $\mathbb{Z}[i]$ with norm $1$ are the units $\{1, -1, i, -i\}$, we must have $N(\alpha) = N(\beta) = p$. Thus if $\alpha = a + bi$ we have $p = a^2 + b^2$. ▨

Pf of Thm: ($\Leftarrow$) Suppose $p \equiv 1 \bmod 4$.

There is same $a \in \mathbb{Z}$ with $a^2 \equiv -1 \bmod p$, namely $a = \left(\frac{p-1}{2}\right)!$ ✪. Thus $p \mid a^2+1$ in $\mathbb{Z}$.

Suppose $p$ were irreducible in $\mathbb{Z}[i]$; as $\mathbb{Z}[i]$ is a PID, $p$ is prime as well. Thus as

$a^2+1 = (a+i)(a-i)$, we must have $p \mid a+i$ or $p \mid a-i$. Both are impossible since $p(c+di) = pc + pdi$. So $p$ is reducible $\Rightarrow p = a^2+b^2$. ▨

✪ $p = 4n+1$ so $a = (2n)!$ First

$-1 \equiv (p-1)! \bmod p$ by pairing each elt of $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ with its inverse, which is unique except for $-1$. So

$$-1 \equiv (p-1)! \equiv (1 \cdot 2 \cdots \cdot 2n)((2n+1) \cdot \cdots \cdot (4n))$$
$$\equiv (2n!)((-2n) \cdot \cdots \cdot (-2)(-1))$$
$$\equiv (2n!)^2(-1)^{2n} \equiv a^2 \bmod p.$$