Lecture 20: PIDs are UFDs; factorization in $\mathbb{Z}[i]$

§31-34 of [R2]
§8.3 of [DF]

Last time: R int. domain, $r \neq 0$ a nonunit.

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

Prime: $r \mid ab \Rightarrow r \mid a$ or $r \mid b$. **Associates:** $r = us$ for u a unit.

Unique Factorization Domain: An int. domain R where for each $r \neq 0$ nonunit have:

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

(b) $r = q_1 q_2 \cdots q_m \Rightarrow n = m$ and can reorder so q_i is an assoc of p_i
(q_i irred)

Thm: A PID has unique factorization.

Pf: Let $r \neq 0$ a nonunit in R

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

If r is irredicible, then done. Otherwise $r = r_1 s_1$ for nonunits r_1 and s_1. Continue by factoring r_1 and s_1, if possible. Either we eventually get a factorization, or we find sequences

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 $r \Rightarrow r \mid a$ or $r \mid b$. ▨

Pf of ②: Clearly $g \mid a$ and $g \mid b$. If a common divisor $d = g^e r$ where g is irred, then $a = g^e r s$ and $b = g^e r s'$; since rs and rs' have factorizations, uniqueness means g 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 ineducibles.

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 ined, u is a unit and so p_1 and q_1 are associates. So

$$p_2 p_3 \cdots p_n = (u q_2) q_3 \cdots q_m$$

and now repeat. ▨

Thm $p \in \mathbb{Z}$ 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.]

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

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

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

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

Pf: ($\Rightarrow$) 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 α, β.

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 some $a \in \mathbb{Z}$ 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 distinct except for -1. So

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