Lecture 4: PIDs have unique factorization

Last time: R int domain, r nonzero

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)

associate: $s = ur$ for u a unit.

Unique Factorization Domain: An int domain R where each $r \in R$

① $r = p_1 \cdots p_n$ with p_i irreducible.

② $r = q_1 \cdots q_m \Rightarrow m = n$ and, after reordering, q_i is an associate of p_i.

Basic props of U.F.Ds:

① irreducible elts are prime.

② gcds work the way you expect:

$$a = u\, p_1^{e_1} \cdots p_k^{e_k}$$

$$b = u'\, p_1^{e_1'} \cdots p_k^{e_k'} \longrightarrow \gcd(a,b) = p_1^{\min(e_1, e_1')} \cdots p_k^{\min(e_k, e_k')}$$

units → $p_1, \ldots, p_k$ irreducibles, with e_k, e_k' possibly 0.

Pf of ①: Let r be irred, and suppose $r \mid ab$, i.e. $ab = cr$

Expand a, b, c as prod. of irred: $(a_1 \cdots a_k)(b_1 \cdots b_j) = (c_1 \cdots c_e)\, r$

By uniqueness, some a_i or b_i is an assoc. of $r \Rightarrow r \mid a$ or $r \mid b$. ∎

Thm: A P.I.D. has unique factorization.

In particular, every Euclidean domain is a U.F.D.

Proof: Let $r \in R$.

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

If r is irred, then done. If instead $r = r_1 s_1$ for non units r_1, s_1 continue by factoring r_1 and s_1 possible. Either we eventually get a factorization into irreds, or construct a seq $r_0 = r, r_1, r_2, \ldots$ of nonunits where $r_k = r_{k+1} s_{k+1}$ for a nonunit s_{k+1}.

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

Set $I = \bigcup_k I_k$, an ideal of R. As R is a P.I.D. have $I = (a)$. Must have $a \in I_k$ for some k. But then $I_j = I_k = I$ for all $j \geq k$

a contradiction. So r has a factorization into ineducibles.

B. Uniqueness. Suppose $r = q_1 q_2 \cdots q_m$ is some other factorization. As R is a P.I.D., 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 $p_2 p_3 \cdots p_n = (u^{-1} q_2) q_3 \cdots q_m$, and so repeat. ▨

Thm: $p \in \mathbb{Z}$ an odd prime. Then $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$ iff $p \equiv 1 \bmod 4$.

Ex: $1^2 + 2^2 = 5$, $2^2 + 3^2 = 13$, $2^2 + 5^2 = 29$

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

Will prove using that $\mathbb{Z}[i]$ is a U.F.D.

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

Recall: $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ sending $\alpha = a+bi$ to
$|\alpha|^2 = \alpha\bar{\alpha} = a^2+b^2$.

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 $p^2 = N(p) = N(\alpha)N(\beta)$ and as $N(\alpha) = 1$
$\Rightarrow \alpha \in \underbrace{\{\pm 1, \pm i\}}_{\text{units}}$, must have $p = N(\alpha) = N(a+bi)$
$= a^2+b^2$. ▨

Proof of Thm: ($\Leftarrow$) Suppose $p \equiv 1 \bmod 4$.
There is an $a \in \mathbb{Z}$ with $a^2 \equiv -1 \bmod p$,
namely $a = \left(\frac{p-1}{2}\right)!$ (★) Thus $p \mid a^2+1$. If
p is irreducible in $\mathbb{Z}[i]$, then it's prime
since $\mathbb{Z}[i]$ is a U.F.D. Then as $a^2+1 = (a+i)(a-i)$,
must have $p \mid a+i$ or $p \mid a-i$, both which
are impossible since $p(c+di) = pc+pdi$.
So p must be reducible $\Rightarrow p = a^2+b^2$. ▨

(★) Details: $p = 4n+1$, so $a = (2n)!$.

First

$$-1 \equiv (p-1)! \bmod p$$

by pairing up each elt of $(\mathbb{Z}/p\mathbb{Z})^\times$ with its inverse, which is distinct except for -1.

So

$$-1 \equiv (p-1)! \equiv (1 \cdot 2 \cdot \cdots \cdot 2n) \cdot ((2n+1) \cdot \cdots \cdot (4n-1))$$

$$\equiv (1 \cdot 2 \cdot \cdots \cdot 2n)((p-2n) \cdot \cdots \cdot (p-2)(p-1))$$

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

as needed.