Lecture 3: Principal Ideal Domains

Last time:

Euclidean Domain: An int domain R w/ $N: R \to \mathbb{Z}_{\geq 0}$ sat $N(0)=0$ and $\forall a,b \in R$ with $b \neq 0$ then $a = qb + r$ with $r=0$ or $N(r) < N(b)$.

Thm: In a Euclidean Domain every ideal is principal, i.e. $I = (a) = \{ra \mid r \in R\}$.

Principal Ideal Domain: An integral domain where every ideal is principal.

Ex: $\mathbb{Z}$, Euclidean domains, $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ ← Not Euclidean, see text.

Non ex: $\mathbb{Z}[\sqrt{-5}]$, e.g. $(2, 1+\sqrt{-5})$ is a non-princ. ideal [On HW #2].

[Goal (Next lecture) P.I.D. have unique factorization.]

Thm: R a PID. For $a, b \in R$, suppose $(a,b) = (g)$.
Then ① g is a gcd for a, b.
② $g = sa + tb$ for some $s, t \in R$.

Pf: ② is immediate from $(a,b) = (g)$. Since $a, b \in (g)$, must have $g | a$ and $g | b$. If $d | a$ and $d | b$, then $d | g$ by ②. So g is a gcd. ▨

Note: Some rings have gcd's but not ②, e.g. $\mathbb{Q}[x,y]$ then $\gcd(x,y) = 1$ by can't have $1 = px + qy$.

R an integral domain, $r \in R$ non-zero.

Unit: $\exists s \in R$ with $rs = 1$.

Reducible: $r = ab$ with a, b nonunits.

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

Prime: $r | ab \Rightarrow r | a$ or $r | b$.

Prop: A prime $r \in R$ is irreducible.

Pf: If $r = ab$ then can assume $r | a$, i.e. $a = cr$.
Then $r = ab = crb \Rightarrow (1 - cb) r = 0 \Rightarrow cb = 1 \Rightarrow$ b is a unit. ▨

However, 3 is irred. in $\mathbb{Z}[\sqrt{-5}]$ (on HW), but not prime since $3^2 = 9 = (2+\sqrt{-5})(2-\sqrt{-5})$ and 3 divides neither $2+\sqrt{5}$ or $2-\sqrt{-5}$.

Aside: In a PID, any irred. elt. is prime [Only if asked.]

$I \subseteq R$ a proper ideal ($I \subsetneq R$).

Prime: $a \cdot b \in I \Rightarrow a \in I$ or $b \in I$.

$\Leftrightarrow R/I$ is also an integral domain

Maximal: $\nexists$ an ideal $I \subsetneq J \subsetneq R$. $\Leftrightarrow R/I$ is a field.

Note: (r) is a prime ideal $\Leftrightarrow$ r is a prime elt.

Pf: $s \in (r) \Leftrightarrow s = ar \Leftrightarrow r \mid s$. So the two statements are really the same. $\square$

Thm In a PID, every prime ideal is maximal.

Pf: Let $(p) \subseteq R$ be prime. Suppose $(p) \subseteq (m)$. Then $p = rm$. As p is prime it is irreducible

So either:

ⓐ r is a unit $\Rightarrow (p) = (m)$

ⓑ m is a unit $\Rightarrow (m) = R$

Hence (p) is maximal. $\square$

Note: $\mathbb{Z}[x]$ is not a PID, since (x) is prime but not maximal. [This dispite the fact that $F[x]$ is Euclidean when F is a field.]

R int. domain. Elements r and s are associates if $r = us$ for some unit $u \in R$.

Unique Factorization Domain: An int. domain where for every non-zero non-unit r:

(a) $r = p_1 p_2 \cdots p_n$ where the p_i are irreducible.

(b) This is unique in that any other factorization $r = q_1 \cdots q_m$ can be reordered so that p_i is an associate of q_i. [in particular $n = m$.]

Ex: PID's [Next time]

Non Ex: $\mathbb{Z}[\sqrt{-5}]$ has (a) but not (b)

$\mathbb{Z}[\sqrt[n]{2} \,;\, n \in \mathbb{Z}_{>0}]$ doesn't have (a) as

$$2 = \sqrt{2} \cdot \sqrt{2} = (\sqrt[4]{2})^4 = (\sqrt[8]{2})^8 = \cdots$$