Lecture 3: Principal Ideal Domains

Office hours this week: M 10-11 Tu 2-4 in 378 AH.

Last time:

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

$\Rightarrow$ Every ideal is principal, $I = (a) = \{ra \mid r \in R\}$

A ring w/ gcds but $\gcd(a,b) \neq sa + tb$: $R = \mathbb{Q}[x, y]$

$a = x$, $b = y$

$\gcd = 1$

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

Ex: $\mathbb{Z}$, any Euclidean domain

Non Ex: $\mathbb{Z}[\sqrt{-5}]$, e.g. $(2, 1+\sqrt{-5})$ is not prime.

P.I.D. but not Euclidean: $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ (see text)

[Goal: PIDs have unique factorization.]

Thm: R a P.I.D. 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 $a, b \in (g)$ have $g|a$ and $g|b$. If $d|a$ and $d|b$ then $d|g$ by ②. So g is a gcd. ▨

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

unit: $\exists\, s \in R$ with $rs = 1$,

reducible: $r = ab$ with a, b non units.

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

prime: $r \mid ab \Rightarrow r \mid a$ or $r \mid b$.

Note: prime $\Rightarrow$ irreducible, but not always the other way.

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

In $\mathbb{Z}[\sqrt{-5}]$, 3 is irreducible (HW) but not prime since $3^2 = (2+\sqrt{-5})(2-\sqrt{-5})$ but 3 divides neither $(2+\sqrt{-5})$ or $(2-\sqrt{-5})$.

$I \subsetneq R$ a *proper* ideal

prime: $a \cdot b \in I \Rightarrow a \in I$ or $b \in I$

$\Leftrightarrow R/I$ is also an int. 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 prime.

Pf: Let $I = (r)$. Then $s \in I \Leftrightarrow s = ar \Leftrightarrow r \mid s$, and so the statements are the same. ▨

Thm: In a P.I.D. every nonzero prime ideal is maximal.

Pf: Let (p) be a prime ideal of R. Suppose $(p) \subseteq (m)$.

Then $p = rm$. As p is prime, it is irreducible.

So either ⓐ r is a unit $\Rightarrow (p) = (m)$ or

ⓑ m is a unit $\Rightarrow (m) = R$.

So (p) is maximal. ▨

Ex: $\mathbb{Z}[x]$ is not a P.I.D., since (x) is prime but not maximal.

Note: $R[x]$ is only Euclidean when R is a field.
(ess. $N(a)=0 \Rightarrow a$ is a unit)

R integral domain.

r and s are <u>associates</u> if $r = us$ for a unit $u \in R$.

R is a <u>Unique Factorization Domain</u> (U.F.D.) if for every nonzero nonunit r then

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

(b) This decomp is <u>unique</u> 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 $n = m$.

<u>Next time</u>: P.I.D. $\Rightarrow$ U.F.D.

<u>Non U.F.Ds</u>: $\mathbb{Z}[\sqrt{-5}]$ has (a) but not (b).

$\mathbb{Z}[\sqrt[n]{2}; n \in \mathbb{N}]$ doesn't have (a):

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