Lecture 3: Principal Ideal Domains

Last time:

**Euclidean Domain:** An integral domain $R$ with $N: R \to \mathbb{Z}_{\geq 0}$ 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. $I = (a) = \{ ra | r \in R \}$.  

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

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

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

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

**Thm:** If $R$ is a PID, then 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:** (1) is immediate from $(a, b) = (g)$. Since $a, b \in (g)$, we must have $g | a$ and $g | b$. If $d | a$ and $d | b$, then $d | g$ by (1). 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 irreducible in \( \mathbb{Z}[\sqrt{-5}] \) (on HW), but not prime as \( 3^2 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5}) \) and 3 divides neither \( 2 + \sqrt{-5} \) nor \( 2 - \sqrt{-5} \).

I \in R \text{ a proper ideal } (I \neq R).

**Prime**: \( a, b \in I \Rightarrow a \in I \text{ or } b \in I \Leftrightarrow R/I \text{ is also an integral domain}. \)

**Maximal**: \( \forall \text{ an ideal } I \neq J \neq R \Rightarrow R/I \text{ is a field}. \)

**Note**: \( (r) \) is a prime ideal \( \Leftrightarrow r \text{ is a prime elt.} \)

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

**Thm**: In a PID, every prime ideal is maximal.

**Pf**: Let \( (p) \leq R \) be prime \( \Rightarrow p \text{ is prime hence irreducible}. \)

Suppose \( (p) \leq (m). \) Then \( p = rm. \) As \( p \) is irreducible, either:

- \( a \) \( r \text{ is a unit } \Rightarrow (p) = (m) \)
- \( b \) \( m \text{ is a unit } \Rightarrow (m) = R. \)

Hence \( (p) \) is maximal.

**Cor**: In a PID, \( r \text{ is prime } \Leftrightarrow r \text{ is irreducible}. \)

**Pf**: Same as the thm, since max ideals are prime.
Note: \( \mathbb{Z}[x] \) is not a PID, since \((x)\) is prime but not maximal. [This despite the fact that \( F[x] \) is Euclidean when \( F \) is a field.]

\[ \text{R int. domain. Elements} \ r \ \text{and} \ s \ \text{are associate if} \ r = us \ \text{for some unit} \ u \in R. \]

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

\( a) \ r = p_1 \cdot p_2 \cdots p_n \) 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 \( n = m. \)]

\underline{Ex}: PID's [Next time]

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

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

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