Dillan Marroquin
MATH 331.1001
Scribing Week 14
Due. 29 November 2021

Lecture 35

An ideal $I \trianglelefteq R$ is **principal** iff $\exists a \in I$such that $I = (a) = \{ra | r \in R\}$.

Example. 1. Let $R = \mathbb{Z}$, $I = n\mathbb{Z} = (n)$.

2. For every ring, the zero ideal is principal and R is a principal ideal (i.e. $\{0_R\} = (0)$), $R = (1)$.)

Definition (35.1)**.** A ring R is a **principal ideal ring (PIR)** iff every ideal of R is principal.
R is a **principal ideal domain (PID)** iff R is an integral domain and R is a PIR.

Recall Theorem 34.4 which stated that $\mathbb{Z}$ is a PID (wasn't worded like this).

Proposition (35.2)**.** $\forall n > 1$, $\mathbb{Z}/n/Z$ is a PIR.

Proposition (35.3)**.** A field $\mathbb{K}$ has exactly 2 ideals: the zero ideal and $\mathbb{K}$.

Corollary (35.4)**.** 1. A field is a PID.

2. If $\mathbb{K}$ is a field and $\varphi : \mathbb{K} \to S$ is a ring homomorphism, then φ is injective OR S is the zero ring.

3. $\mathbb{Z}/n\mathbb{Z}$ is a PID if n is prime.

Remark (35.5)**.** 1. Nice Theorem in Paulin: "If R is a finite integral domain, then R is a field." So, $\mathbb{Z}/n\mathbb{Z}$ being an integral domain implies $(\mathbb{Z}/n\mathbb{Z})^\times = \{[k] | \gcd(k,n) = 1\} = \{[1],[2],\ldots,[n-1]\}$ since this is a field. Therefore if $d|n$ and $d < n$, then $d = 1$. Thus n is prime and we conclude $\mathbb{Z}/n\mathbb{Z}$ is a PID iff $\mathbb{Z}/n\mathbb{Z}$ is a field iff $n = p$ prime.

2. $\mathbb{Z}[x]$ is an integral domain by Theorem 33.4, but is not a PID.

How to Get More Examples of PIDs?

Recall in Theorem 13.3 (wayyyy back then), we showed that every subgroup of a cyclic group is cyclic. Crucial in our proof was the division algorithm in $\mathbb{Z}$.

Definition (35.6)**.** Let R be a commutative ring such that $0 \neq 1$.

1. A **Euclidean function** on R is a set-theoretic function $N : R - \{0_R\} \to \mathbb{N} \cup \{0\}$ such that
   (a) $\forall a \in R$, $\forall b \in R - \{0_R\}$, $N(a) \leq N(ab)$.
   (b) $\forall a \in R$ and $\forall b \neq 0 \in R$, $\exists q, r \in R$ such that $a = bq + r$ with either $r = 0$ OR $N(r) < N(b)$.
2. An integral domain is the **Euclidean domain** iff R admits a Euclidean function.

Theorem (35.7)**.** The following are Euclidean domains:

1. $\mathbb{Z}$ with $N(m) := |m|$ $\forall m \neq 0$ (absolute value).
2. Any field $\mathbb{K}$ with $N(a) := 1$ $\forall a \neq 0 \in \mathbb{K}$.
3. $\mathbb{Z}[i]$ with $N(k + ib) := a^2 + b^2$ $\forall a + ib \neq 0$.
4. Polynomial Ring $\mathbb{K}[x]$ with coefficients in a field $\mathbb{K}$, $N(f) := \deg(f)$ $\forall f \neq 0$.