1.15 Lecture 13: Euclidean Domains, PIDs and UFDs

1.15.1 R is a Euclidean domain $\Longrightarrow$ R is a PID

Definition. Let $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$ be the set of nonnegative integers.

- A **Euclidean domain** is an integral domain R with a function

$$\sigma\colon R - \{0\} \to \mathbb{Z}_{\geq 0}, \qquad \text{a } \textbf{size function}$$

  such that if $a, b \in R$ and $a \neq 0$ then there exist $q, r \in R$ such that

$$b = aq + r, \qquad \text{where either } r = 0 \text{ or } \sigma(r) < \sigma(a).$$

- Let R be a commutative ring. A **principal ideal** is an ideal generated by a single element.

- A **principal ideal domain** (or **PID**) is an integral domain for which every ideal is principal.

Theorem 1.64. *If R is a Euclidean domain then R is a principal ideal domain.*

HW: Show that $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{-19}]$ is a PID that is not a Euclidean domain.

Proposition 1.65. *Let $\mathbb{A}$ be a PID. Then $\mathbb{A}$ satisfies ACC.*

1.15.2 R is a PID $\Longrightarrow$ R is a UFD

Definition. Let R be an integral domain.

- A **unit** is an element $a \in R$ such that $aR = R$.
- An element $p \in R$ is **irreducible** if pR if $p \neq 0$, $pR \neq R$ and R/pR is a simple R-module.
- A **unique factorization domain** (or **UFD**) is an integral domain R such that
  (a) If $x \in R$ then there exist irreducible $p_1, \ldots, p_n \in R$ such that $x = p_1 \cdots p_n$.
  (b) If $x \in R$ and $x = p_1 \cdots p_n = uq_1 \cdots q_m$ where $u \in R$ is a unit and $p_1, \ldots, p_n,\ \ q_1, \ldots, q_m \in R$ are irreducible then $m = n$ and there exists a permutation $\sigma\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ and units $u_1, \ldots, u_n \in R$ such that

$$\text{if } i \in \{1, \ldots, n\} \text{ then } q_i = u_i p_{\sigma(i)}.$$

The following theorem is a consequence of the Jordan-Hölder Theorem.

Theorem 1.66. *If R is a principal ideal domain then R is a unique factorization domain.*

HW: Show that $\mathbb{C}[x, y]$ and $\mathbb{Z}[x]$ are UFDs that are not PIDs.

HW: Show that if R is a PID and $p \in R$ then p is irreducible if and only if pR is a maximal ideal.

HW: Show that if R is a UFD and $p \in R$ is irreducible then pR is a prime ideal.

1.15.3 Some Proofs

Theorem 1.67. *A Euclidean domain is a principal ideal domain.*

Proof. Assume R is a Euclidean domain with size function $\sigma\colon (R-\{0\}) \to \mathbb{Z}_{\ge 0}$.
Let I be an ideal of R.
To show: There exists $a \in R$ such that $I = aR$.

Case 1: $I = \{0\}$. Then $I = 0R$.
Case 2: $I \neq \{0\}$.
Let $a \in I$, $a \neq 0$, such that $\sigma(a)$ is as small as possible.
To show: $I = aR$.
To show: (a) $I \subseteq aR$.
(b) $aR \subseteq I$.

(a) Let $b \in I$.
To show: $b \in (a)$.
Then there exist $q, r \in R$ such that $b = aq + r$ where either $r = 0$ or $\sigma(r) < \sigma(a)$.
Since $r = b - aq$ and $b \in I$ and $a \in I$ then $r \in I$.
Since $a \in I$ is such that $\sigma(a)$ is as small as possible we cannot have $\sigma(r) < \sigma(a)$.
So $r = 0$.
So $b = aq$.
So $b \in aR$.
So $I \subseteq aR$.
(b) To show: $aR \subseteq I$.
Since $a \in I$ then $aR \subseteq I$.

So $I = aR$.
So every ideal I of R is a principal ideal.

So R is a principal ideal domain. □

Proposition 1.68. *Let $\mathbb{A}$ be a PID. Then $\mathbb{A}$ satisfies ACC.*

Proof. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals in $\mathbb{A}$.
To show: There exists $k \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}_{>k}$ then $J_n = J_k$.
Let

$$I_{\mathrm{un}} = \bigcup_{j \in \mathbb{Z}_{>0}} I_j.$$

Then I_{un} is an ideal of $\mathbb{A}$.
Since $\mathbb{A}$ is a PID then there exists $d \in \mathbb{A}$ such that $I_{\mathrm{un}} = d\mathbb{A}$.
To show: There exists $k \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}_{>k}$ then $I_n = I_k$.
Let $k \in \mathbb{Z}_{>0}$ such that $d \in I_k$.
To show: If $n \in \mathbb{Z}_{>k}$ then $I_n = I_k$.
Assume $n \in \mathbb{Z}_{>k}$. Then

$$I_k \subseteq I_n \subseteq I_{\mathrm{un}} = d\mathbb{A} \subseteq I_k.$$

So $I_n = I_k$.
So $\mathbb{A}$ satisfies ACC. □