Lecture 12: Euclidean Domains

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Euclidean Domains

- In group theory, the division algorithm in $\mathbb{Z}$ is used to show that $\mathbb{Z}$ is a PID.
- The division algorithm in $F[x]$ is used to show that $F[x]$ is a PID.
- Motivated by the division (Euclidean) algorithm in the rings $\mathbb{Z}$ and $F[x]$, now we investigate the integral domains which have this property.

Euclidean Domains

Definition

Let D be an integral domain and let $\upsilon : D^* \to \mathbb{Z}^+ \cup \{0\}$ be a function from nonzero elements of D to nonnegative integers such that the followings are satisfied:

1. For all $a, b \in D$ with $0_D \neq b$, $\exists\ q, r \in D$ such that $a = bq + r$, where either $r = 0$ or $\upsilon(r) < \upsilon(b)$.
2. For all $a, b \in D^*$, $\upsilon(a) \leq \upsilon(ab)$.

The function υ is called a **Euclidean norm (**Euclidean valuation**)** on D. An integral domain D is called an **Euclidean domain (ED)** if there exists a Euclidean norm on D.

Examples:

1. $\mathbb{Z}$ is a ED with the Euclidean norm

$$\begin{array}{cccc} v: \mathbb{Z}^* & \longrightarrow & \mathbb{Z}^+ \cup \{0\}. \\ n & \longrightarrow & v(n) = |n| \end{array}$$

- The first conditon holds by the division algorithm for $\mathbb{Z}$.
- The second condition follows from $|ab| = |a|\,|b|$ and $|a| \geq 1$ for $a \in \mathbb{Z}^*$.

2. $F[x]$ is a ED with the Euclidean norm

$$\begin{array}{cccc} v: F^*[x] & \longrightarrow & \mathbb{Z}^+ \cup \{0\} \\ f(x) & \longrightarrow & v(f(x)) = \deg f(x) \end{array}.$$

- The first conditon holds by the division algorithm for $F[x]$.
- The second condition follows from $\deg(f(x)\,g(x)) = \deg f(x) + \deg g(x)$.

3. The set of Gaussian integers

$$\mathbb{Z}[i] = \{\alpha = a + ib \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

is an integral domain. The norm function on $\mathbb{Z}[i]$ is defined by

$$N(\alpha) := \alpha\overline{\alpha} = (a + ib)(a - ib) = a^2 + b^2,$$

where $\overline{\alpha}$ is conjugate of α.

$\mathbb{Z}[i]$ is a ED with the Euclidean norm

$$\begin{array}{rcl} \upsilon : \mathbb{Z}[i] \setminus \{0\} & \longrightarrow & \mathbb{Z}^+ \cup \{0\}. \\ \alpha & \longrightarrow & \upsilon(\alpha) = N(\alpha) \end{array}$$

Euclidean Domains

Theorem

Every ED is a PID.

Corollaries:

1. Every ED is a UFD.
2. In a ED, irreducible and prime elements are the same.
3. In a ED, there exists a gcd of two elements not both zero.

Euclidean Domains

Euclidean Algorithm: Let D be a ED with Euclidean norm υ, and let a, b be nonzero elements of D. Then $\exists q_1, r_1 \in D$ such that

$$a = bq_1 + r_1, \text{ either } r_1 = 0 \text{ or } \upsilon(r_1) < \upsilon(b).$$

If $r_1 = 0$, then $\gcd(a, b) = b$. If $r_1 \neq 0$, then $\exists q_2, r_2 \in D$ such that

$$b = r_1 q_2 + r_2, \text{ either } r_2 = 0 \text{ or } \upsilon(r_2) < \upsilon(r_1).$$

Continuing this process,

$$r_{i-1} = r_i q_{i+1} + r_{i+1}, \text{ either } r_{i+1} = 0 \text{ or } \upsilon(r_{i+1}) < \upsilon(r_i).$$

Then the sequence $r_1, r_2, \cdots$ must terminate with some $r_k = 0$.
If r_k is the first $r_i = 0$, then $\gcd(a, b) = r_{k-1}$.
Moreover if $\gcd(a, b) = d$, then $\exists x, y \in D$ such that $ax + by = d$.

Euclidean Domains

Definition

Let D be an integral domain. A **multiplicative norm** N on D, is a function $N : D \longrightarrow \mathbb{Z}$ such that

1. $N(\alpha) = 0 \Leftrightarrow \alpha = 0$
2. $N(\alpha\beta) = N(\alpha)\,N(\beta)$ for all $\alpha, \beta \in D$.

Theorem

$|N(\alpha)| = 1 \Leftrightarrow \alpha$ is a unit.
If every $\alpha \in D$ such that $|N(\alpha)| = 1$ is a unit in D, then an element $\pi \in D$ with $|N(\pi)| = p$ is an irreducible in D.

Multiplicative norm is a fundamental tool in algebraic number theory.

Example: Let $\mathbb{Z}[i\sqrt{5}] = \left\{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$. Consider the multiplicative norm $N : \mathbb{Z}[i\sqrt{5}] \longrightarrow \mathbb{Z}$ by $N\left(a + ib\sqrt{5}\right) = a^2 + 5b^2$.

- $3 = 3 + 0i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ is irreducible.
  Consider
  $$3 = \left(a + bi\sqrt{5}\right)\left(c + di\sqrt{5}\right).$$
  By the help of the norm, either $a + bi\sqrt{5}$ is a unit or $c + di\sqrt{5}$ is a unit, then 3 is irreducible.
- $$9 = 3.3 = \left(2 + \sqrt{-5}\right)\left(2 - \sqrt{-5}\right).$$
  Since $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ are irreducible, then $\mathbb{Z}[i\sqrt{5}]$ is not a UFD.