Lecture 10

Euclidean Domains

Definition 10.1

Let R be an integral domain.
Any function
$$N\colon R \to \mathbb{Z}^+ \cup \{0\}$$
such that $N(0) = 0$ is called a **norm**.

Example 10.1 The zero norm
$$\begin{aligned} N\colon R &\to \mathbb{Z}^+ \cup \{0\} \\ r &\mapsto 0 \end{aligned}$$

Example 10.2 The absolute value on the integers
$$\begin{aligned} N\colon \mathbb{Z} &\to \mathbb{Z}^+ \cup \{0\} \\ n &\mapsto |n| \end{aligned}$$

Definition 10.2

An integral domain R is a **Euclidean domain** if it admits a norm N such that $\forall a, b \in R$ and $b \neq 0$, there exists $q, r \in R$ such that
$$a = qb + r$$
where $r = 0$ or $N(b) > N(r)$.
We call q the **quotient** of a by b and r the **remainder** of a with respect to b.

Recall the Euclidean Division Algorithm
$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_{n+2} r_n \end{aligned}$$
which must terminated because
$$N(b) > N(r_0) > N(r_1) \cdots > N(r_n) > N(r_{n+1}) = N(0) = 0$$

Example 10.3 Fields F are Euclidean domains with any norm N.
If $a, b \in F$, $b \neq 0$, then
$$a = \underbrace{(a \cdot b^{-1})}_{\text{quotient}} \cdot b + 0$$
which means in a field, you can always divide evenly.

Example 10.4 The integers $\mathbb{Z}$ are a Euclidean domain with $N(a) = |a|$.

Example 10.5 If F is a field, the polynomial ring $F[x]$ is a Euclidean domain with norm $N(p) \coloneqq \deg(p)$

Proof. Let $a(x), b(x) \in F[x]$ and $b(x) \neq 0$.
We proceed by induction on $\deg(a) = N(a)$.
If $a(x) = 0$, then $0 = 0 \bullet b(x) + 0$.
So we may assume $a(x) \neq 0$. If $\deg(a) < \deg(b)$, then

$$N(a) < N(b) \implies a(x) = 0 \bullet b(x) + a(x)$$

So we may assume $\deg(a) \geq \deg(b)$, i.e

$$\begin{aligned} a(x) &= a_m x^m + a_{n-1} x^{m-1} + \cdots + a_0 \\ b(x) &= b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0 \end{aligned}$$

and since $b(x) \neq 0$ then $b_n \neq 0$ and so $b_n^{-1} \in F$.
Let

$$a'(x) = a(x) - \frac{a_m}{b_n} x^{m-n} \bullet b(x)$$

then $\deg(a') < \deg(a)$.
By induction on $\deg(a)$ there exist $q'(x), r'(x)$ such that $N(r') < N(b)$ or $r'(x) = 0$ and

$$a' = q' \bullet b + r'$$

Hence we can write

$$\begin{aligned} a =& a' + \frac{a_m}{b_n} x^{m-n} \bullet b(x) \\ a(x) =& [q'(x) \bullet b(x) + r'(x)] + \left[\frac{a_m}{b_n} x^{m-n} b(x)\right] \\ =& \left[q'(x) + \frac{a_m}{b_n} x^{m-n}\right] b(x) + r'(x) \end{aligned}$$

■

Proposition 10.1

Every ideal in a Euclidean domain is principal.

Proof. If $I \subset R$ is a non-zero ideal, consider

$$\mathcal{N} = \{N(a) | a \in I\} \subset \mathbb{Z}^+ \cup \{0\}$$

By the well-ordering principle, there exists $d \in I$ such that $N(d) = \min \mathcal{N}$. Clearly

$$d \in I \implies (d) \subset I$$

Conversely, suppose $a \in I$, then

$$a = q \bullet d + r$$

where $r = 0$ or $N(r) < N(d)$.

If $r = 0$, then

$$a = q \cdot d \implies a \in (d) \implies I = (d)$$

If $r \neq 0$, then $a - qd = r$. However

$$a, d \in I \implies a - qd \in I \implies r \in I$$

and because we let $N(r) < N(d)$ then $r = 0$. ■

Corollary 10.1

Every ideal in $\mathbb{Z}$ is principal.

Definition 10.3

Let R be a commutative ring with $1 \neq 0$ and $a, b \in R$ such that $b \neq 0$.

(1) We say $a \in R$ is a **multiple** of b if there exists an $r \in R$ such that

$$a = r \cdot b$$

We call b a divisor of a, in this case, (i.e $b \mid a$).

(2) A **greatest common divisor** of $a, b \in R$ is $d \neq 0$ such that
   - (i) $d \mid a$, $d \mid b$
   - (ii) If $d' \mid a, d' \mid b$, then $d' \mid d$.

We write $d = \gcd(a, b)$ or sometimes just $d = (a, b)$.

Recall $b \mid a$ if and only if $(a) \subset (b)$

Definition 10.4

Let $I = (a, b) \subset R$, then $d \in R$ is a **greatest common divisor** $d = \gcd(a, b)$ if

(i) $I \subset (d)$

(ii) If $I \subset (d')$, then $(d) \subset (d')$.

In other words, $d \in R$ is a greatest common divisor $a, b \in R$ if (d) is the smallest principal ideal containing (a, b).

Proposition 10.2

If $a, b \in R$ are nonzero, and $(a, b) = d$ then $d = \gcd(a, b)$

Theorem 10.1

If R is a Euclidean domain, then greatest common divisors **always** exist

Proof.

$$\left.\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_{n+2} r_n \end{aligned}\right\} \implies r_n = \gcd(a, b)$$

■

Definition 10.5

A **principal ideal domain** (PID) is an integral domain in which every ideal is principal

Theorem 10.2

Every Euclidean domain is a PID, i.e

$$\text{Integral domain} \supsetneq \text{ PID } \supsetneq \text{ Euclidean domain}$$

Theorem 10.3

Let R be a PID and $a, b \in R$ nonzero. If $(a, b) = (d)$, then

(1) d is a greatest common divisor of a, b.
(2) There exist $x, y \in R$ such that $d = ax + by$.
(3) d is a unique to multiplication by a unit.

Claim: $\mathbb{Z}[x]$ is an integral domain BUT $(2, x)$ is not principal therefore $\mathbb{Z}[x]$ is not a PID.

Proof. Suppose $(2, x) = (p(x))$, then

$$2 = q(x)p(x) \implies \deg p(x) = 0$$

i.e $p(x) \equiv a \in \mathbb{Z}$.
Moreover $a \mid 2$ implies $a = \pm 1, \pm 2$. Also, $(2, x) \neq \mathbb{Z}[x]$ e.g

$$3 \neq 2p(x) + x \bullet q(x)$$

Then $p(x) \neq \pm$ otherwise $(2, x) = (1) = \mathbb{Z}[x]$. Therefore $p(x)$ must be ± 2.
But $(2, x) \neq (2)$ because $x \neq 2 \bullet q(x)$.
Essentially, the issue is that 2 has no multiplicative inverse in $\mathbb{Z}$ but the coefficient of x is 1. ■

Theorem 10.4

Every non-zero prime in a PID is maximal, e.g. in $\mathbb{Z}$, every prime is maximal.

Proof. Let $(p) \subset R$ be a nonzero prime in a PID.
There exists a maximal ideal $M \subset$ such that $(p) \subset M$.
Since R is a PID, then every ideal is principal, hence

$$M = (m) \implies m \mid p \implies \exists r \in R,\, p = r \bullet m$$

Because (p) is prime either $r \in (p)$ or $m \in (p)$.
If $m \in (p)$ then $(m) = (p)$.
Suppose $r \in (p)$, say $r = s \bullet p$, $s \in R$. Then

$$p = r \bullet m = (s \bullet p) \bullet m \implies p \bullet (1 - s \bullet m) = 0$$

Since R is an integral domain and $p \neq 0$, then

$$1 - sm = 0 \implies sm = 1 \implies m \in R^{\times}$$

But then $(m) = R$, which means (m) is not maximal, by definition. This is a contradiction and hence

$$(p) = (m)$$

is maximal. $\blacksquare$

Theorem 10.5

If R is a commutative ring such that $R[x]$ is a PID, then R is a field.

Proof. Suppose $R[x]$ is a PID (in particular, an integral domain), then $R \subset R[x]$ is an integral domain. We use a clever trick

$$R[x]/(x) \cong R \implies (x) \text{ is prime} \implies (x) \text{ is maximal} \implies R \text{ is a field}$$

$\blacksquare$