L10: Euclidean Domains and PIDs

Definition 10.1: Norm

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 norm on the integers

$$\begin{aligned} N\colon \mathbb{Z} &\to \mathbb{Z}^+ \cup \{0\} \\ n &\mapsto |n| \end{aligned}$$

Definition 10.2: Euclidean Domain, Quotient, Remainder

An integral domain R is a **Euclidean domain** if it admits a norm N such that for all $a, b \in R$ and $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r$$

where $r = 0$ or $N(b) > N(r)$ (i.e Euclidean domains have the *familiar* division property known as the Euclidean condition).
We call q the **quotient** of a by b and r the **remainder** of a with respect to b.

What is nice about Euclidean domains is that you have the Euclidean Division Algorithm

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

which must terminate because by the well ordering on the non-negative integers, you are constantly reducing the size of the remainder, so you must eventually reach 0.

$$N(b) > N(r_0) > N(r_1) \cdots > N(r_n) > N(r_{n+1}) = N(0) = 0$$

Example 10.3. Fields F are Euclidean domains with any norm N.
If $a, b \in F$, $b \neq 0$, then

$$a = \underbrace{(a \bullet b^{-1})}_{\text{quotient}} \bullet b + 0$$

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 $N(p) \coloneqq \deg(p)$. It's important to note that non-zero elements can have zero norm, as in this case, the constant polynomials have degree 0.

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

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

which verifies the Euclidean condition.
Now 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 since the coefficient ring is a field, we know $b_n^{-1} \in F$.
Let

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

then $\deg(a') < \deg(a)$ because we got rid of the term $a_m X^m$
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

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

and this also satisfies the Euclidean condition. ■

Proposition 10.3: Euclidean domains are principal

Every ideal in a Euclidean domain is principal.

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

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

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

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

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 by construction $N(r) < N(d)$ this is impossible as d is the element with minimum norm. Hence, $r = 0$ and we go back to the previous situation.
Therefore, $(d) = I$. ■

Corollary 10.4: Ideals in $\mathbb{Z}$ are principal

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

Think about it like this: in the integers, if you consider the ideal generated by 2 and 3 and you know $3 = 2 \cdot 1 + 1$, that means if 3 is in the ideal with 2, 1 must also be in the ideal. So the $(2, 3) = (1)$, so you have the whole ring. With similar logic, you can see that $(4, 6) = (2)$. This extends to the general Euclidean domain as seen in Prop 10.1, as the ideal (d) is the greatest common divisor.

Definition 10.5: Multiple, Divisor, GCD

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 that $b \,|\, a$ if and only if $(a) \subset (b)$.

Definition 10.6: Ideal GCD

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 of $a, b \in R$ if (d) is the smallest principal ideal containing (a, b).

Proposition 10.7

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

Theorem 10.8: GCDs exist in Euclidean domains

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

Proof.

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

■

Definition 10.9: Principal Ideal Domain

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

Theorem 10.10: Euclidean domain is PID is Integral domain

Every Euclidean domain is a PID, i.e

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

Theorem 10.11

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

(1) d is a greatest common divisor of a and 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 in particular $(2, X)$ is not principal therefore $\mathbb{Z}[X]$ is not a PID.

Proof.
Suppose it is principal, i.e $(2, X) = (p(X))$, then

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

i.e $p(X) \equiv a \in \mathbb{Z}$.
Moreover $a \,|\, 2$ implies $a = \pm 1, \pm 2$. Also, $(2, X) \neq \mathbb{Z}[X]$ as for example

$$3 \neq \underbrace{2p(X)}_{\text{3 is not even}} + \underbrace{X \bullet q(X)}_{\text{would need to be 0}}$$

Then, $p(X) \neq \pm 1$ 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. So, nothing makes sense when $p(X) = \pm 1, \pm 2$ which means the initial assumption was false and $(2, X)$ is not principal. ■

Theorem 10.12: Nonzero primes ideals are maximal in PID

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 $M \subset R$ such that $(p) \subset M$.
Since R is a PID, then every ideal is principal, hence

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

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. ■

Theorem 10.13: If $R[X]$ is PID then R is field

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

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