Euclidean Domains

Defn: Let R be an integral domain.

Any function

$$N : R \longrightarrow \mathbb{Z}^+ \cup \{0\}$$

s.t. $N(0) = 0$ is called a <u>norm</u>

e.g. ⓪ $N : R \longrightarrow \mathbb{Z}^+ \cup \{0\}$

$$r \longmapsto 0$$

① $N : \mathbb{Z} \longrightarrow \mathbb{Z}^+ \cup \{0\}$

$$n \longmapsto |n|$$

An integral domain R is a <u>Euclidean domain</u>

if it admits a norm N

s.t. $\forall a, b \in R$, $b \neq 0$

$\exists q, r \in R$ s.t. $a = qb + r$, $r = 0$ or $N(b) > N(r)$

We call q the <u>quotient</u> of a by b

r the <u>remainder</u> of a with respect to b.

Division Algorithm:

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

Must terminate b/c

$N(b) > N(r_0) > N(r_1)$

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

Examples:

① Fields F are ED w/ any norm N.

If $a, b \in F$, $b \neq 0$

Then $a = \underbrace{(a \cdot b^{-1})}_{\text{quotient}} \cdot b + 0$ — in a field, you can always divide evenly

② The integers $\mathbb{Z}$ are ED with $N(a) = |a|$

③ If F is a field,

The polynomial ring $F[x]$ is a ED w/ $N(p) := \deg(p)$

PF: Let $a(x), b(x) \in F[x]$, $b(x) \neq 0$

we proceed by induction on $\deg(a) = N(a)$

If $a(x) = 0$, then $0 = 0 \cdot b(x) + 0$ ✓

So we may assume $a(x) \neq 0$

If $\deg(a) < \deg(b)$, then $N(a) < N(b)$

$\implies a(x) = 0 \cdot b(x) + a(x)$ ✓

So we may assume $\deg(a) \geq \deg(b)$

$$a(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_0$$

$$b(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_0$$

$b(x) \neq 0 \implies b_n \neq 0 \implies b_n^{-1} \in F$

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

- $\deg(a') < \deg(a)$

By induction on $\deg(a)$

$\exists\, q'(x), r'(x)$ s.t. $N(r') < N(b)$ or $r' = 0$

s.t. $a' = q' \cdot b + r'$

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

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

$$= \left[q'(x) + \frac{a_m}{b_n} x^{m-n}\right] b(x) + r'(x) \quad \checkmark$$

$\square$

<u>Prop:</u> Every ideal in a Euclidean domain is principal

<u>Pf:</u> 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, $\exists\, d \in I$ s.t. $N(d) = \min \mathcal{N}$

Clearly, $d \in I \Longrightarrow (d) \subset I$

Conversely, suppose $a \in I$

$\Longrightarrow a = q \cdot d + r$, where $r = 0$ or $N(r) < N(d)$.

If $r = 0$, then $a = q \cdot d \Longrightarrow a \in (d) \Longrightarrow I = (d)$

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

However, $a, d \in I \Longrightarrow a - qd \in I \Longrightarrow r \in I$

Because $N(r) < N(d) \longrightarrow \swarrow$

$\Longrightarrow r = 0$

$\square$

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

Defn: Let R be a comm. ring w/ $1 \neq 0$

$a, b \in R$, $b \neq 0$

(1) we say $a \in R$ is a multiple of b if

$\exists\, r \in R$ s.t. $a = r \cdot b$

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 $d \neq 0$

s.t. (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: $b \mid a$ iff $(a) \subset (b)$

Redefinition/Thm: 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)

Prop: If $a, b \in R$ are nonzero, and $(a,b) = (d)$

Then $d = \gcd(a,b)$

Thm: If R is a Euclidean domain

Then greatest common divisors always exist.

Pf:/Alg.

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

$\square$

Defn: A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Thm: Every Euclidean domain is PID.

$$\text{Int. dom.} \supsetneq \text{PID} \supsetneq \text{Euclidean domains.}$$

Thm: Let R be a PID, $a, b \in R$ nonzero

Then if $(a,b) = (d)$

1. d is a greatest common divisor of a, b
2. $\exists\ x, y \in R$ s.t. $d = ax + by$
3. d is unique to multiplication by a unit

Ex: $\mathbb{Z}[x]$ is an int. dom.

BUT: $(2, x)$ is not principal. $\Rightarrow \mathbb{Z}[x]$ is not a PID.

Suppose $(2, x) = (p(x))$

Then $2 = q(x)\,p(x) \Longrightarrow \deg p(x) = 0$

i.e. $p(x) \equiv a \in \mathbb{Z}$

Moreover $a \mid 2 \Longrightarrow a = \pm 1, \pm 2$

$(2, x) \neq \mathbb{Z}[x]$

e.g. $3 \neq \underbrace{2p(x)}_{3 \text{ is not even.}} + \underbrace{x \cdot q(x)}_{\text{would necessarily be } 0}$

$\Longrightarrow p(x) \neq \pm 1$ (otherwise $(2, x) = (1) = \mathbb{Z}[x]$)

$\Longrightarrow p(x) = \pm 2.$

But $(2, x) \neq (2)$, b/c $x \neq 2 \cdot q(x)$

Essentially: The issue is that 2 has no multiplicative inverse in $\mathbb{Z}$ but the coefficient of x is 1!

$\square$

<u>Thm</u>: Every non-zero prime in a PID is maximal

e.g. In $\mathbb{Z}$, every prime is maximal

<u>Pf</u>: Let $(p) \subset R$ a nonzero prime in a PID

$\exists$ maximal ideal $M \subset R$ s.t. $M \supset (p)$

R is a PID $\Longrightarrow M = (m) \Longrightarrow m \mid p.$

i.e. $\exists r \in R$ s.t. $p = r \cdot m$

Because (p) is prime,

$r \in (p)$

or $m \in (p)$.

If $m \in (p)$ then $(m) = (p)$.

So suppose $r \in (p)$, say $r = s \cdot p$, $s \in R$.

Then $p = r \cdot m = (s \cdot p) \cdot m$

$\Longrightarrow$ $p \cdot (1 - s \cdot m) = 0$

Since R is an int. dom., $p \neq 0$ $\Longrightarrow$ $1 - s \cdot m = 0$

$\Longrightarrow$ $m \in R^\times$

But then $(m) = R$ $\longrightarrow$ $\Leftarrow$ i.e. (m) not maximal

$\Longrightarrow$ $(p) = (m)$ is maximal. $\square$

<u>Thm:</u> If R is a comm ring s.t.

$R[x]$ is a PID

Then R is a field.

<u>Pf:</u> Suppose $R[x]$ is a PID (in part. an int. dom.)

$\Longrightarrow$ $R \subset R[x]$ is an int. dom.

<u>Trick:</u> $R[x]/(x) \cong R$

$\Longrightarrow$ (x) is prime $\Longrightarrow$ (x) is maximal

$\Longrightarrow$ R is a field $\square$