1 Divisibility in Integral Domains

We continue again with our discussion on this.

1.1 Euclidian Domain

Definition 1.1

An integral domain is called a **Euclidian domain** (ED) if there exists a function

$$d : D \setminus \{0\} \mapsto \mathbb{Z}_{\geq 0}$$

such that

1. $d(a) \leq d(ab)$ for all $a, b \in D \setminus \{0\}$.
2. If $a, b \in D$ with $b \neq 0$, then there exist $q, r \in D$ such that

$$a = bq + r$$

and either $r = 0$ or $d(r) < d(b)$.

Remark: This is basically just long division. In other words, this is an "abstraction" of when long division exists.

1.1.1 Example 1: The Integers

The integers, $\mathbb{Z}$, are an Euclidian domain with $d(a) = |a|$.

1. If $a, b \in \mathbb{Z} \setminus \{0\}$, then $|ab| = |a||b| \geq 1$. This implies that

$$d(ab) \geq d(a)$$

2. Long division, specifically if $a, b \in \mathbb{Z}$ with $b \neq 0$, then

$$a = bq + r$$

and

$$r = 0 \text{ or } 0 < r < |b|$$

i.e. $d(r) < d(b)$.

1.1.2 Example 2: A Field

Consider $\mathbb{F}[x]$, where $\mathbb{F}$ is a field. Then, this is an Euclidian domain with $d(f(x)) = \deg f(x)$.

1. $\deg(g(x)f(x)) = \deg g(x) + \deg f(x) \geq \deg g(x)$. This implies that

$$d(f(x)g(x)) \geq d(g(x))$$

2. This is just long division. If $f(x), g(x) \in \mathbb{F}[x]$, then there exists $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

and

$$r(x) = 0 \text{ or } \deg r(x) < \deg g(x) \implies d(r(x)) < d(g(x))$$

1.1.3 Example 3: Gaussian Integers

Consider $\mathbb{Z}[i]$ with $d(a+bi) = a^2 + b^2$.

1. $d(xy) = d(x)d(y) \geq d(x)$ by $a^2 + b^2 \geq 1$ if $a + bi \neq 0 + 0i$.
2. Let $x, y \in \mathbb{Z}[i]$ and $y \neq 0$. Then
$$xy^{-1} \in \mathbb{Q}[i] \supseteq \mathbb{Z}[i]$$
We can then write $xy^{-1} = s + ti$ for $s, t \in \mathbb{Q}$. In other words, an integer part plus a small fractional part. Let m be the closest integer to s and let n be the closest integer to t such that
$$|s - m| \leq \frac{1}{2}$$
$$|t - n| \leq \frac{1}{2}$$
So now we have
$$xy^{-1} = m + ni + (s - m) + (t - n)i$$
so that
$$x = \underbrace{(m + ni)y}_{\in \mathbb{Z}[i]} + ((s - m) + (t - n)i)y$$
But we know that
$$((s - m) + (t - n)i)y = x - (m + ni)y \in \mathbb{Z}[i]$$
Either
$$((s - m) + (t - n)i)y = 0$$
or
$$\begin{aligned} d(((s - m) + (t - n)i)y) &= d((s - m) + (t - n)i)d(y) \\ &= ((s - m)^2 + (t - n)^2)d(y) \\ &\leq \left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right) d(y) \\ &= \frac{1}{2}d(y) < d(y) \end{aligned}$$

1.2 Euclidian Domain

Theorem 1.1

Every Euclidian domain is a PID.

Proof. Let D be an ED and $I \subseteq D$ a non-zero ideal. Choose $a \in I \setminus \{0\}$ with $d(a)$ minimal. If $b \in I$ then $b = aq + r$ with $r = 0$ or $d(r) < d(a)$. But, $r = b - aq \in I$ so by minimality, $r = 0$ or $d(r) \geq d(a)$, implying that $r = 0$ and thus $I = \langle a \rangle$. □

Remarks:

- $\mathbb{Z}[i]$ is a PID and so a UFD.
- $\mathbb{Z}[\sqrt{-3}]$ is not a PID and so not a ED. In particular, $\mathbb{Z}[\sqrt{-3}]$ with $N(a + b\sqrt{-3}) = a^2 + 3b^2$ fails the properties of ED.

- From this theorem, we now know that an integral domain being an ED implies that it is also a PID which implies that it is also a UFD; that is:

$$\text{ED} \implies \text{PID} \implies \text{UFD}$$

  The converse is *not* true.

- There exists a UFD which is not a PID.

Theorem 1.2

If D is a UFD, then so is $D[x]$.

Remark: In particular, $\mathbb{Z}[x]$ is a UFD and *not* a PID.