1 Divisibility in Integral Domains

We will continue our discussion on divisibility in integral domains.

1.1 Unique Factorization Domain

Definition 1.1

An integral domain D is a **unique factorization domain** (UFD) if it satisfies two properties:

1. Every non-zero, non-unit element of D can be written as a product of irreducibles.
2. Up to reordering and up to associates, this factorization is unique.

1.1.1 Example 1: The Integers

Show that $\mathbb{Z}$ is a UFD.

Proof. (Sketch.) We show existence and uniqueness.

- **Existence:** We induct on the integer $N > 1$.
  - Base Case: $N = 2$ is irreducible since it is prime.
  - Inductive Step: If N is prime, it's already irreducible. Otherwise, $N = ab$ for $a, b < N$. But, by the inductive hypothesis, a, b are products of irreducible, so N is irreducible.
- **Uniqueness:** Suppose $p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$. WLOG $n \leq m$, $p_1 | q_1 q_2 \ldots q_m$. By Euclid's lemma, we know that
$$p_1 | q_i$$
for some i. WLOG, $i = 1$. But, $q_i = \pm p_1$. We repeat this process until
$$\pm 1 = q_{n+1} \ldots q_m$$
but this isn't possible unless $n = m$, in which case you get $\pm 1 = 1$.

This concludes this proof. □

1.1.2 Example 2: Another Ring

Show that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

Proof. This is not a UFD because

- There are non-unique factorizations
$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$
- And 2, $1 \pm \sqrt{-3}$ are irreducibles but not primes.

Which means we are done. □

1.2 PIDs and UFDs

Theorem 1.1

Every PID is a UFD.

Lemma 1.1

In a PID, any strictly ascending chain of ideals

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

must have finite length.

Proof. We prove existence and uniqueness.

- **Existence:** Let $a_0 \in D$ be non-zero, non-unit. If a_0 is irreducible, we're done. Otherwise, write $a_0 = b_1 a_1$ for $b_1, a_1 \in D$ non-units. This implies that $\langle a_0 \rangle \subset \langle a_1 \rangle$. We can repeat this process over and over again (this part omitted), but note that this chain is finite, so it terminates at some $\langle a_n \rangle$ for an irreducible number, or that
$$a_0 = (b_1 b_2 \dots b_r) a_r$$
i.e. a_r is irreducible and $a_r | a_0$. Write $a_0 = c_1 p_1$ for p_1 irreducible. We can recursively define this process like so

  if c_i is irreducible, stop. Otherwise, $c_i = c_{i+1} p_{i+1}$, where p_{i+1} is irreducible with c_{i+1} being a non-unit. This gives us
  $$\langle c_i \rangle \subset \langle c_{i+1} \rangle$$
  Thus, $\langle c_1 \rangle \subset \langle c_2 \rangle \subset \langle c_3 \rangle \subset \dots$. This chain has finite length, so it terminates at $\langle c_s \rangle$ for some integer s. This implies that c_s is irreducible. Therefore,
  $$a_0 = \underbrace{p_1 p_2 p_3 p_4 \dots p_s}_{\text{Irreducible by construction}} \quad c_s$$
  and c_s is irreducible. So, we wrote a product of irreducibles.

- **Uniqueness:** Same idea as above.

So, we are done. □

Proof. Let $I_1 \subset I_2 \subset \dots$ be a strictly ascending chain of ideals. Let

$$I = \bigcup_k I_k \subseteq D$$

where I is itself an ideal. Since D is a PID, there exists a $d \in D$ such that

$$I = \langle d \rangle$$

but $d \in I = \bigcup_k I_k$. Thus, $d \in I_j$ for some j. This implies that $\langle d \rangle \subseteq I_j \subseteq I = \langle d \rangle$, so these are all equalities. But, I_j must be the last element; otherwise, $I_j \subseteq I_{j+1}$ since it is a strictly ascending chain, but this would imply that $I_j \subset I$. □

1.2.1 Example 1: Polynomial Rings

If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a PID. This implies that $\mathbb{F}[x]$ is a UFD.

1.2.2 Example 2: Chains

In $\mathbb{Z}$, consider the following ideals in our chain:

$$\{0\} \subset \langle 2 \rangle \subset \mathbb{Z}$$

since $\langle 2 \rangle$ is maximal. If we wanted a longer chain, we could have

$$\{0\} \subset \langle 100 \rangle \subset \langle 50 \rangle \subset \ldots \subset \mathbb{Z}$$

Here, there are only a finite number of choices we can pick.