Ring Theory, Part II: Classification of Integral Domains

Jay Havaldar

In this chapter, we talk about Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains.

0.1 Euclidean Domains

We define a **norm** on an integral domain R. It is analogous to the idea of a norm on a vector space.

Definition: A function $f : R \to \mathbb{Z}$ so that $N(0) = 0$ is called a norm. If $N(a) > 0$ for $a \neq 0$, then it is called a positive norm.

Now, we can define the Euclidean algorithm (which finds a common divisor for two elements).

Definition: An integral domain R is a **Euclidean domain** if there exists a norm N so that for all nonzero $a, b \in R$, we can write:

$$a = qb + r$$

For some element q with $N(r) < N(b)$ or $r = 0$.

Proposition

> Every Euclidean domain is a principal ideal domain, i.e. each ideal can be generated by a single element. In particular, if we have a nonzero ideal I, then I is generated by d, any nonzero element of I with minimum norm.

This proof is fairly straightforward. Dividing any element by d leaves a remainder with a norm smaller than that of d. But this is impossible, so indeed d divides every element in the ring.

Definition: Let R be a commutative ring and let $a, b \neq 0$. A greatest common divisor d of a, b is an element such that $d \mid a, d \mid b$, and if any other element d' is a common divisor, then $d' \mid d$.

Indeed, the greatest common divisor (if it exists) is a generator for the unique principal ideal containing a, b. It is clear to see then, that if this divisor is a unit, then a, b generate a maximal ideal.

Proposition

> If a, b nonzero elements in a commutative ring R, and $(a, b) = (d)$ for some element d, then d is a greatest common divisor of a, b.

Furthermore, it is clear that greatest common divisors are unique up to units.

0.2 Principal Ideal Domains

Definition: A principal ideal domain is an integral domain in which every ideal is principal.

Note that by an earlier proposition, every Euclidean domain is a principal ideal domain. However, the converse is not true. The ideal $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a principal ideal domain but not a Euclidean domain.

Proposition

> Every nonzero prime ideal in a principal ideal domain is maximal.

This follows straightforwardly from the definitions.

Corollary

> If R is a commutative ring and $R[x]$ is a principal ideal domain, then R is a field.

Assume R is a PID. Then in particular, R is an integral domain. Therefore, since (x) is a nonzero prime ideal, (x) must be maximal. Therefore, R is a field. The converse is also true and is very important for field theory.

> If k is a field, the $k[x]$ is a PID.

This follows from the fact that $k[x]$ is a UFD, with the norm given by the degree of a given polynomial. The Euclidean algorithm works in $k[x]$.

0.3 Unique Factorization Domains

Definition: Let R be an integral domain. Suppose $r \in R$ and r is nonzero and not a unit. Then r is **irreducible** if whenever it is written as a product $r = ab$, then at least one of a or b must be a unit.

Definition: Suppose $p \in R$ is nonzero. Then p is **prime** if (p) is a prime ideal.

Definition: Two elements a, b are said to be associate in R if $a = ub$ for some unit u.

Proposition

> In an integral domain, a prime element is irreducible.

Suppose we have a prime element $p = ab$. Then either $p \mid a$ or $p \mid b$. WLOG, let $p \mid a$. Then $a = px$ for some $x \in R$ and therefore $p = pxb$. But then we have $xb = 1$ and therefore b is a unit. Therefore p is irreducible.

However, the converse is not necessarily true! Look at the element 3 in $\mathbb{Z}[\sqrt{-5}]$, since 9 can be factored in the complex plane into terms not dividing 3.

Proposition

> In a principal ideal domain, irreducible elements are prime.

Check that any ideal generated by an irreducible element is maximal. By an earlier theorem, a prime ideal is maximal in a PID (in general, a maximal ideal is always prime).

Definition: A unique factorization domain is an integral domain in which every nonzero element which is not a unit can be written as a finite product of irreducibles, and this decomposition is unique up to associates.

We also have the following useful fact:

Proposition

> An element is irreducible iff the ideal it generates is maximal amongst the principal ideals.

So there is some correspondence between irreducible elements and maximal ideals, and between prime elements and prime ideals (far more obvious). It makes sense, then, that if all ideals are principal, then the two notions coincide.

Proposition

> In a UFD, irreducible elements are prime.

So indeed, UFDs are also domains in which these two notions collapse. Finally, we get the following classification:

Proposition:

> Every principal ideal domain is a unique factorization domain.

So finally, we have:

$$\text{Fields} \subset \text{Euclidean Domains} \subset \text{Principal Ideal Domains} \subset \text{UFDs} \subset \text{Integral Domains}$$

Each inclusion is proper.

- $\mathbb{Z}$ is a Euclidean domain but not a field.
- $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID but not a Euclidean domain.
- $\mathbb{Z}[x]$ is a UFD but not a PID.
- $\mathbb{Z}[\sqrt{-5}]$ is an integral domain but not a UFD.