L11: Unique Factorization Domains

Definition 11.1: Irreducible/Reducible, Prime, Associate Elements

Let R be an integral domain

(i) Suppose $r \in R \setminus \{0\}$, $r \notin R^\times$.
We say r is **irreducible** if whenever $r = a \cdot b$, either $a \in R^\times$ or $b \in R^\times$.
We say r is **reducible** if it is not irreducible.

(ii) Suppose $r \in R \setminus \{0\}$, $r \notin R^\times$
We say r is **prime** if (r) is a prime ideal.
In other words, if $r \mid a \cdot b$, then either $r \mid a$ or $r \mid b$.

(iii) We say $a, b \in R$ are **associates** if there exists $u \in R^\times$ such that $a = u \cdot b$.
(If a and b generate the same principal ideal, then they are associates. Check HW3 P1)

Proposition 11.2: Prime elements in integral domain are irreducible

Any prime element in an integral domain is irreducible.

Proof. Suppose $p = a \cdot b \in R$ and (p) is a prime ideal.
Then $p \in (p)$ implies $a \in (p)$ or $b \in (p)$. W.l.o.g let $a \in (p)$.
So $\exists r \in R$ such that $a = p \cdot r$ and hence

$$p = (p \cdot r) \cdot b = p \cdot (r \cdot b)$$

Since R is an integral domain, we can cancel p, then, $1 = r \cdot b$, so $b \in R^\times$. ■

Example 11.1. It turns out to be that the converse is not true, i.e irreducible but not prime elements.
Consider the ring

$$\mathbb{Z}[\sqrt{-5}] :- \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

There exists a norm on this (not exactly the same as the norm for Euclidean domains), with properties

- $N(a + b\sqrt{-5}) \coloneqq a^2 + 5b^2$
- $N(x \cdot y) = N(x) \cdot N(y)$
- $N(x) = \pm 1$ if an only if $x \in \mathbb{Z}[\sqrt{-5}]^\times$

Claim: $2 + \sqrt{-5}$ is irreducible

Proof. Suppose

$$2 + \sqrt{-5} = (a + b\sqrt{-5}) \cdot (c + d\sqrt{-5})$$

Then

$$N(2 + \sqrt{-5}) = 4 + 5 = 9 \implies N(a + b\sqrt{-5}) \mid 9 \implies N(a + b\sqrt{-5}) = \pm 1 \text{ or } \pm 3$$

Observe that if $b \neq 0$, then

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 \geq 5$$

Therefore we have to assume $b = 0$ if we want the norm to be $\pm 1, \pm 3$ and so

$$b = 0 \implies N(a + b\sqrt{-5}) = N(a) = a^2$$

So the norm is a perfect square, and since the only candidates are ± 1 and ± 3, the only perfect square between them is 1 and hence

$$N(a + b\sqrt{-5}) = 1 \implies a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]^\times$$

which means that $2 + \sqrt{-5}$ is irreducible. ■

Claim: $2 + \sqrt{-5}$ is **not** prime.

Proof. We know

$$3^2 = 9 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5}) \in (2 + \sqrt{-5})$$

It remains to show that 3 is not in the ideal $(2 + \sqrt{-5})$, i.e $3 \notin (2 + \sqrt{-5})$. If $3 = (a + b\sqrt{-5}) \cdot (2 + \sqrt{-5})$, then

$$9 = N(3) = N(a + b\sqrt{-5}) \cdot N(2 + \sqrt{-5}) = N(a + b\sqrt{-5}) \cdot 9 \implies N(a + b\sqrt{-5}) = 1$$

which immediately tells us $b = 0$ and $a = \pm 1$.
But $3 \neq \pm(2 + \sqrt{-5})$ hence $2 + \sqrt{-5}$ is not prime. ■

We see that in an arbitrary integral domain, the notion of primality and irreduciblity are not the same. However, there are circumstances where they are the same thing.

Proposition 11.3: Element in PID is prime iff it is irreducible

In a PID an element is prime *iff* it is irreducible.

Proof. Prop 11.2 shows prime $\implies$ irred.; it remains to show irred. $\implies$ prime.
Suppose $r \in R$ is irreducible and recall that maximal ideals are prime. Hence we will show that (r) is maximal.
Suppose $(r) \subset (m) \subsetneq R$, then

$$r \in (m) \implies \exists s \in R,\ r = s \cdot m \underbrace{\implies}_{r \text{ irreducible}} s = R^\times \text{ or } m \in R^\times$$

By assumption $(m) \subsetneq R$ and this implies

$$m \notin R^\times \implies s \in R^\times \implies r \text{ and } m \text{ associates} \implies (r) = (m)$$ ■

Example 11.2. In $\mathbb{Z}$, the irreducibles are the primes (and their negatives)

Observe that the factorization of any integer into primes is unique!
We see that irreducibility, in the natural sense, is about not being able to be split up into smaller pieces (up to a unit). Primality, while similar, is more about divisibility. We saw that 9 could be represented by fundamentally two different ideals, namely (3) and $(2 + \sqrt{-5})$.

Definition 11.4: Unique Factorization Domain

A **unique factorization domain** (UFD) is an integral domain R such that for all $r \in r \setminus \{0\}$, $r \notin R^\times$

(i) $r = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ for p_i irreducible.

(ii) This decomposition is unique up to associates and reordering, i.e if

$$r = q_1 \cdot \ldots \cdot q_m, \quad q_j \text{ irreducible}$$

Then after reordering, $q_i = u_i p_i, u_i \in R^\times$ and $n = m$.

Example 11.3. Fields are vacuously UFDs, because the definition of a UFD constrains non-units to certain conditions however in a field you only have units, so these constraints don't apply.

Example 11.4. $\mathbb{Z}$ is a UFD.

Example 11.5. $\mathbb{Z}[\sqrt{-5}]$ is **not** a UFD as

$$3^2 = 9 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$$

and $3, 2 \pm \sqrt{-5}$ are irreducibles which are not associate.

Proposition 11.5: Element in UFD is prime iff it is irreducible

In a UFD, an element is prime *iff* it is irreducible.

Proof. It suffices to show once more that irreducible $\implies$ prime.
Suppose $r \in R$ is irreducible and $a \cdot b \in (r)$ i.e there exists $c \in R$ such that $a \cdot b = r \cdot c$
By unique factorization in a UFD, a, b, c have unique factorizations, i.e

$$\begin{aligned} a &= p_1 \cdot p_2 \cdot \ldots \cdot p_n, \quad p_i \text{ irreducible, unique} \\ b &= q_1 \cdot q_2 \cdot \ldots \cdot q_m, \quad q_j \text{ irreducible, unique} \\ c &= r_1 \cdot r_2 \cdot \ldots \cdot r_l, \quad r_k \text{ irreducible, unique} \end{aligned}$$

Since $a \cdot b = r \cdot c$ we have

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_m = r \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_l$$

since r is irreducible, both sides are factorizations into irreducibles. By unique factorization and w.l.o.g.

$$r = u \cdot p_1, \, u \in R^\times \implies r | a$$ ■

and so $a \in (r)$ which means (r) is a prime ideal (with q you get $b \in (r)$).

Proposition 11.6: Nonzero elements in UFD have GCD

Let $a, b \in R \setminus \{0\}$ in a UFD. Then there is a greatest common divisor of a, b in R.

Proof. We write for $u, v \in R^\times$ and p_i's irreducible

$$a = u \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$$
$$b = v \cdot p_1^{f_1} \cdot p_2^{f_2} \cdot \ldots \cdot p_n^{f_n}$$

We allow some exponents to be 0 ($p_i^0 = 1$) and we require $p_i \neq p_j$ if $i \neq j$ for example

$$\begin{pmatrix} 12 = 2^2 \cdot 3 \to 12 = 2^2 \cdot 3^1 \cdot 5^0 \\ 20 = 2^2 \cdot 5 \to 20 = 2^2 \cdot 3^0 \cdot 5^1 \end{pmatrix}$$

So the elements a, b can be written in terms of the same irreducibles to certain powers.
Claim:

$$d = p_1^{\min\{e_1, d_1\}} \cdot p_2^{\min\{e_2, d_2\}} \cdot \ldots \cdot p_n^{\min\{e_n, d_n\}}$$

is the gcd of a and b.

> ***Proof.*** Clearly $d \mid a$, $d \mid b$, by construction, since it's factors come from the same set of factors of a, b, namely p_i. Since d is a common divisor, it remains to show it is a greatest common divisor.
> If $c \mid a$, $c \mid b$, then we want to see that $c \mid d$. Unique factorization tells us
>
> $$c = q_1^{g_1} \cdot \ldots \cdot q_m^{g_m}, \quad q_i \text{ irreducible}, \quad q_i \neq q_j, \text{ and } g_i > 0$$
>
> Since $c \mid a$, $c \mid b$, then after (possibly) changing associates we see that the set of factors of c have to be factors of a and b, i.e
>
> $$\{q_1, \ldots, q_n\} \subset \{p_1, \ldots, p_n\}$$
>
> and since c divides both a and b then $g_i \leq \min\{e_i, f_i\}$ and thus $c \mid d$. ■

Therefore there exists a greatest common divisor of a, b in R, namely, the d we have shown. ■