

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 $a = u \cdot b$.

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 then, $1 = r \cdot b$, so $b \in R^\times$. ■

Example 11.1. Irreducible but not prime.

Consider the ring

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

Then

- $N(a + b\sqrt{-5}) := a^2 + 5b^2$
- $N(x \cdot y) = N(x) \cdot N(y)$
- $N(x) = \pm 1$ if and 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

$$b = 0 \implies N(a+b\sqrt{-5}) = N(a) = a^2 \implies N(a+b\sqrt{-5}) = 1 \implies a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]^\times$$

■

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

Proof. We know

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

However, $3 \notin (2 + \sqrt{-5})$.

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 $3 \notin \pm(N(a + b\sqrt{-5}) \cdot N(2 + \sqrt{-5}))$

■

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

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

Proof. It suffices to show that irreducible \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

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

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

$$m \notin R^\times \implies s \in R^\times \implies (r) = (m)$$

■

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!

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) $r = p_1 \cdot p_2 \cdot \dots \cdot p_k$ for p_i irreducible.

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

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

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

Example 11.3. Fields are vacuously UFDs

Example 11.4. \mathbb{Z} are a UFD

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

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

and $3, 2 \pm \sqrt{-5}$ are irreducibles.

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

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_n, \quad p_i \text{ irreducible, unique}$$

$$b = q_1 \cdot q_2 \cdot \dots \cdot q_m, \quad q_j \text{ irreducible, unique}$$

$$c = r_1 \cdot r_2 \cdot \dots \cdot r_l, \quad r_k \text{ irreducible, unique}$$

Hence

$$p_1 \cdot p_2 \cdot \dots \cdot p_n \cdot q_1 \cdot q_2 \cdot \dots \cdot q_m = r \cdot r_1 \cdot r_2 \cdot \dots \cdot r_l$$

so by unique factorization, w.l.o.g

$$r = u \cdot p_1, \quad u \in R^\times \implies r \mid a$$

■

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

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

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

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

Claim: $d = p_1^{\min\{e_1, f_1\}} \cdot p_2^{\min\{e_2, f_2\}} \cdot \dots \cdot p_n^{\min\{e_n, f_n\}}$ is the $\gcd(a, b)$.

Proof. Clearly $d \mid a, d \mid b$.

If $c \mid a, c \mid b$, then we want to see that $c \mid d$.

Unique factorization says for q_i irreducible, $q_i \neq q_j$ and $g_i > 0$, we have

$$c = q_1^{g_1} \cdot \dots \cdot q_m^{g_m}$$

Since $c \mid a, c \mid b$, then after changing associates

$$\{q_1, \dots, q_m\} \subset \{p_1, \dots, p_n\}, \quad g_i \leq \min\{e_i, f_i\} \implies c \mid d$$

■

And so there exists a greatest common divisor of a, b in R .

■