Unique Factorization Domains

Defn: Let R be an integral domain.

① Suppose $r \in R \setminus \{0\}$, $r \notin R^\times$

we say r is <u>irreducible</u> if

whenever $r = a \cdot b$, either $a \in R^\times$ or $b \in R^\times$

we say r is <u>reducible</u> if it is not irreducible

② Suppose $r \in R \setminus \{0\}$, $r \notin R^\times$

we say r is <u>prime</u> if

(r) is a prime ideal

In other words, if $r \mid a \cdot b$, then either $r \mid a$ or $r \mid b$.

③ We say $a, b \in R$ are <u>associates</u> if

$\exists\, u \in R^\times$ s.t. $a = u \cdot b$

Prop: Any prime element in an integral domain is irreducible.

Pf: Suppose $p = a \cdot b \in R$ and (p) is a prime ideal

Then $p \in (p) \implies a \in (p)$ or $b \in (p)$

wlog $a \in (p)$. So $\exists\, r \in R$ s.t. $a = p \cdot r$

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

R int. dom. $\implies 1 = r \cdot b \implies b \in R^\times$ $\square$

Example: Irreducible but not prime.

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

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

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

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

$$N(2+\sqrt{-5}) = 4+5 = 9.$$

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

Obs: If $b \neq 0$, then $N(a+b\sqrt{-5}) = a^2 + 5b^2 \geq 5$

$\implies b = 0$

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

$\implies a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]^\times$

$\square$

<u>Claim</u>: $2+\sqrt{-5}$ is <u>not</u> prime.

<u>Pf</u>: $3^2 = 9 = (2+\sqrt{-5})\cdot(2-\sqrt{-5}) \in (2+\sqrt{-5})$

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

If $3 = (a+b\sqrt{-5})\cdot(2+\sqrt{-5})$

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

$$\begin{array}{ll} \parallel & \\ 9 & = N(a+b\sqrt{-5})\cdot 9 \end{array}$$

$\Longrightarrow N(a+b\sqrt{-5}) = 1$

$\Longrightarrow b=0$ and $a = \pm 1$

But $3 \neq \pm(2+\sqrt{-5})$ $\square$

<u>Prop</u>: In a PID an element is prime iff it is irreducible.

<u>Pf</u>: Suffices to show irred. $\Longrightarrow$ prime.

Suppose $r \in R$ is irreducible

Recall: maximal ideals are prime.

we will show (r) is maximal

Suppose $(r) \subset (m) \subsetneq R$

$\implies r \in (m)$, $\exists\, s \in R$ s.t. $r = s \cdot m$.

r is irreducible $\implies s \in R^\times$ or $m \in R^\times$

By assumption $(m) \subsetneq R \implies m \notin R^\times$

$\implies s \in R^\times$

$\implies (r) = (m)$ $\square$

<u>Examples:</u> In $\mathbb{Z}$, the irreducibles are the primes (and their negatives)

<u>Obs:</u> The factorization of any integer into primes is <u>unique</u>!

<u>Defn:</u> A <u>unique factorization domain</u> (or <u>UFD</u>)

is an integral domain R

s.t. $\forall\, r \in R \setminus \{0\}$, $r \notin R^\times$

① $r = p_1 \cdot p_2 \cdot \text{—} \, p_k$, p_i irreducible

② This decomposition is unique up to associates + reordering.

i.e. if $r = q_1 \cdot \cdots q_m$, q_j irreducible

Then after reordering, $q_i = u_i p_i$, $u_i \in R^\times$

and $n = m$

Examples

① Fields are vacuously UFD's

② $\mathbb{Z}$ are a UFD

③ $\mathbb{Z}[\sqrt{-5}]$ is <u>not</u> a UFD.

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

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

<u>Prop</u>: In a UFD an element is prime iff it is irreducible

<u>Pf</u>: Suffices to show irred. $\Rightarrow$ prime.

Suppose $r \in R$ is irred.

and $a \cdot b \in (r)$

$\Rightarrow \exists\, c \in R$ s.t. $a \cdot b = r \cdot c$

By unique factorization

$$a = p_1 \cdot p_2 \cdot \cdots \cdot p_n \qquad p_i \text{ irred., unique}$$

$$b = q_1 \cdot q_2 \cdot \cdots \cdot q_m \qquad q_j \text{ irred. unique}$$

$$c = r_1 \cdot r_2 \cdot \cdots \cdot r_e \qquad r_k \text{ irred., unique}$$

$$p_1 \cdot p_2 \cdots p_n \cdot q_1 \cdots q_m = r \cdot r_1 \cdot r_2 \cdots r_e$$

$\Rightarrow$ by unique factorization, wlog. $r = u \cdot p_1$, $u \in R^\times \Rightarrow r \mid a$

$\square$

Prop: Let $a, b \in R \setminus \{0\}$ in a UFD

Then there is a greatest common divisor of a, b. in R.

Pf: we write

$$a = u \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n} \qquad u, v \in R^\times$$

$$b = v \cdot p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n} \qquad p_i\text{'s irreducible}$$

we allow some exponents to be zero $(p_i^0 = 1)$

and we require $p_i \neq p_j$ if $i \neq j$

$$\left(\text{e.g. } \begin{array}{l} 12 = 2^2 \cdot 3 \\ 20 = 2^2 \cdot 5 \end{array} \rightsquigarrow \begin{array}{l} 12 = 2^2 \cdot 3^1 \cdot 5^0 \\ 20 = 2^2 \cdot 3^0 \cdot 5^1 \end{array} \right).$$

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

is the $\gcd(a, b)$

Pf: Clearly $d \mid a$, $d \mid b$

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

unique factorization says

$$c = q_1^{g_1} \cdots q_m^{g_m} \qquad \begin{array}{l} q_i\text{'s irreducible} \\ q_i \neq q_j \\ g_i > 0 \end{array} \quad \left(\begin{array}{c} \text{This is the} \\ \text{unique factorization} \\ \text{of } c \end{array} \right)$$

Since $c \mid a$, $c \mid b$ $\implies$ After changing associates

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