Factorization in Integral Domains

R - integral domain (Non-trivial, commutative, $ab = 0_R \Rightarrow \begin{matrix} a = 0_R \\ \text{or} \\ b = 0_R \end{matrix}$)

Definition

Given $a, b \in R$, we say a and b are <u>associated</u> if $a = rb$ where $r \in R^*$.

Examples 1/ $\mathbb{Z}^* = \{\pm 1\} \Rightarrow a, b$ associated $\Leftrightarrow a = \pm b$

2/ F a field $\Rightarrow F^* = F \setminus \{0_F\}$

$\Rightarrow a, b$ associated $\Rightarrow$ Either $a = b = 0_F$ <u>or</u>
$a \neq 0_F$ and $b \neq 0_F$

Exercise $a, b \in R$ (I.D.) associated $\Leftrightarrow (a) = (b)$

Definition $a \in R$ is <u>irreducible</u> if

1/ $a \neq 0_R$

2/ $a \notin R^*$

3/ $a = bc \Rightarrow b \in R^*$ <u>or</u> $c \in R^*$

Example

1/ $R = \mathbb{Z}$, a irreducible $\Leftrightarrow a = \pm p$ (prime)

2/ A field has no irreducible elements.

Remark Assume $a, b \in R$ are associated, then

a irreducible $\Leftrightarrow$ b irreducible

Definition

A ring R is said to be a **unique factorization domain** (UFD) if

1. R is an integral domain
2. Given $x \in R$, if $x \neq 0_R$ and $x \notin R^*$ then $\exists\, a_1, \ldots, a_n \in R$ **irreducible** such that

$$a = a_1 \cdots a_n$$

Called an irreducible factorization

3. If $a = b_1 \cdots b_m$ is another such irreducible factorization, $n = m$ and, perhaps after reordering a_i is associated to b_i $\forall i \in \{1, \ldots, n\}$.

Remark

Fundamental Theorem of Arithmetic $\Rightarrow$ $\mathbb{Z}$ is a UFD

Example

associated

$$6 = 2 \times 3 = (-2) \times (-3)$$

associated

A UFD has many properties in common with $\mathbb{Z}$

Remark If R is a UFD then every $a \in R \setminus \{0_R\}$ can be written in the form

$$a = u p_1^{\alpha_1} \cdots p_n^{\alpha_n} \quad \text{where}$$

1/ $u \in R^*$

2/ p_i are pairwise non-associate irreducible

unique up to association and reordering

3/ $\alpha_i \in \mathbb{N} \cup \{0\}$ $\forall i \in \{1, \dots, n\}$

Definition Let R be an integral domain. Given $a, b \in R$, we say $m \in R$ is a highest common factor (HCF) of a and b if

m a common factor of a and b

1/ $m \mid a$ and $m \mid b$ and 2/ $d \mid a$ and $d \mid b \Rightarrow d \mid m$

Definition Let R be an integral domain. Given $a, b \in R$, we say $m \in R$ is a lowest common multiple (LCM) of a and b if

m a common multiple of a and b

1/ $a \mid m$ and $b \mid m$ and 2/ $a \mid d$ and $b \mid d \Rightarrow m \mid d$

Theorem Let R be a UFD. Let $a, b \in R \setminus \{0_R\}$ have irreducible factorizations:

$$a = u p_1^{\alpha_1} \cdots p_n^{\alpha_n}, \quad b = v p_1^{\beta_1} \cdots p_n^{\beta_n}$$

Then $p_1^{\min(\alpha_1, \beta_1)} \cdots p_n^{\min(\alpha_n, \beta_n)} = \text{HCF of } a, b$

$p_1^{\max(\alpha_1, \beta_1)} \cdots p_n^{\max(\alpha_n, \beta_n)} = \text{LCM of } a, b$

Proof Follows from the uniqueness of irreducible factorizations. See notes for more details. $\square$