Unique Factorization Domains

Kevin James

Definition

Let R be an integral domain.

1. Suppose $r \in R$ is a nonzero non-unit. The r is said to be irreducible in R if whenever $r = ab$ with $a, b \in R$, at least one of a and b must be a unit in R. Otherwise, r is said to be reducible.
2. A nonzero element $p \in R$ is called prime in R if the ideal (p) is a prime ideal.
3. Two elements $a, b \in R$ are said to be associates in R if there is $u \in R^\times$ with $a = bu$.

Definition

Let R be an integral domain.

1. Suppose $r \in R$ is a nonzero non-unit. The r is said to be irreducible in R if whenever $r = ab$ with $a, b \in R$, at least one of a and b must be a unit in R. Otherwise, r is said to be reducible.
2. A nonzero element $p \in R$ is called prime in R if the ideal (p) is a prime ideal.
3. Two elements $a, b \in R$ are said to be associates in R if there is $u \in R^{\times}$ with $a = bu$.

Proposition

In an integral domain a prime element is irreducible.

Definition

Let R be an integral domain.

1. Suppose $r \in R$ is a nonzero non-unit. The r is said to be irreducible in R if whenever $r = ab$ with $a, b \in R$, at least one of a and b must be a unit in R. Otherwise, r is said to be reducible.
2. A nonzero element $p \in R$ is called prime in R if the ideal (p) is a prime ideal.
3. Two elements $a, b \in R$ are said to be associates in R if there is $u \in R^\times$ with $a = bu$.

Proposition

In an integral domain a prime element is irreducible.

Proposition

In a PID, a nonzero element is prime if and only if it is irreducible.

Definition

A Unique Factorization Domain (UFD) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following properties.

1. r can be written as a finite product of irreducibles $p_i \in R$, that is $r = p_1 p_2 \cdots p_n$ and
2. the decomposition above is unique up to associates and rearrangement, that is if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles $q_i \in R$, then $m = n$ and for each $1 \leq i \leq n$, $\exists! 1 \leq j \leq n; u \in R^\times$ such that $q_i = up_j$.

Definition

A Unique Factorization Domain (UFD) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following properties.

1. r can be written as a finite product of irreducibles $p_i \in R$, that is $r = p_1 p_2 \cdots p_n$ and
2. the decomposition above is unique up to associates and rearrangement, that is if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles $q_i \in R$, then $m = n$ and for each $1 \leq i \leq n$, $\exists! 1 \leq j \leq n; u \in R^\times$ such that $q_i = u p_j$.

Proposition

In a UFD a nonzero element is prime if and only if it is irreducible.

Proposition

Let R be a UFD and let $a, b \in R$ be non-zero elements. Suppose that

$$a = up_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}, \text{ and } b = vp_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

are prime factorizations for a and b, where $u, v \in R^\times$, the primes $p_1, \ldots, p_n$ are distinct and the exponents $e_i, f_i \geq 0$. Then the element

$$d = p_1^{\min(e_1,f_1)} p_2^{min(e_2,f_2)} \ldots p_n^{min(e_n,f_n)}$$

is a greatest common divisor of a and b.

Proposition

Let R be a UFD and let $a, b \in R$ be non-zero elements. Suppose that

$$a = up_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}, \text{ and } b = vp_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

are prime factorizations for a and b, where $u, v \in R^\times$, the primes $p_1, \ldots, p_n$ are distinct and the exponents $e_i, f_i \geq 0$. Then the element

$$d = p_1^{\min(e_1,f_1)} p_2^{min(e_2,f_2)} \cdots p_n^{min(e_n,f_n)}$$

is a greatest common divisor of a and b.

Theorem

Every PID is a UFD. In particular, every Euclidean Domain is a PID and a UFD.

Corollary (Fundamental Theorem of Arithmetic)

$\mathbb{Z}$ is a UFD.

Corollary (Fundamental Theorem of Arithmetic)

$\mathbb{Z}$ is a UFD.

Corollary

Let R be a PID. Then there exists a multiplicative Dedekind-Hasse norm on R.