Euclidean Domains

Kevin James

Definition

Suppose that R is an integral domain. Any function $N : R \to \mathbb{N} \cup \{0\}$ with $N(0) = 0$ is a norm. If $N(a) > 0$, $\forall a \in R \setminus \{0_R\}$, then N is called a positive norm.

Definition

An integral domain R is called a Euclidean Domain if R has a division algorithm. That is, if there is a norm N of R such that for any $a, b \in R$ with $b \neq 0_R$ there exists $q, r \in R$ satisfying:

1. $a = bq + r$, and
2. $r = 0_R$ or $N(r) < N(b)$.

For such $q, r \in R$, q is called a quotient and r is called a remainder upon divison of a by b.

Note

The existence of a division algorithm for a ring R allows employment of the Euclidean Algorithm in R for computation of greatest common divisors.

Proposition

If R is a Euclidean Domain, then every ideal is principal. More precisely, if $I \trianglelefteq R$, then $I = (d)$ where d is any element of I of minimum norm.

Example

- $\mathbb{Z}$ is a Euclidean domain and thus all ideals of $\mathbb{Z}$ are principal.
- $\mathbb{Q}[x]$ is a Euclidean domain.
- $\mathbb{Z}[x]$ is not a Euclidean domain since one can check that $(3, x)$ is not principal.

Definition

Let R be a commutative ring and let $a, b \in R$ with $b \neq 0_R$.

1. We say that a is a multiple of b if there is $c \in R$ such that $a = bc$. We also say that b divides a and write $b|a$.
2. A greatest common divisor of a and b (if it exists) is an element $d \in R$ satisfying
   1. $d|a$ and $d|b$, and
   2. if $d' \in R$, $d'|a$ and $d'|b$ then $d'|d$ also.

Proposition

If $a, b \in R$ and $(a, b) = (d)$ then d is a greatest common divisor of a and b.

Proposition

Suppose that R is an integral domain and that $d, d' \in R$. If $(d) = (d')$, then there is a unit $u \in R^\times$ such that $d = ud'$. In particular, if d and d' are greatest common divisors of a and b then $d = ud'$ for some $u \in R^\times$.

Theorem

Let R be a Euclidean domain and let $a, b \in R$ be non-zero. Let $d = r_n$ be the final non-zero remainder in the Euclidean Algorithm.

1. *d is a greatest common divisor of a and b, and*
2. *$(a, b) = (d)$. In particular, d is an R-linear combination of a and b. That is there are $x, y \in R$ such that $d = ax + by$.*

Definition

Suppose that R is an integral domain. Denote by $\tilde{R} = R^{\times} \cup \{0_R\}$. We say that $u \in R \setminus \tilde{R}$ is a universal side divisor if $\forall x \in R$, $\exists z \in \tilde{R}$ such that u divides $x - z$. That is, there is $q \in R$ and $z \in \tilde{R}$ such that $x = qu + z$.

Proposition

Let R be an integral domain that is not a field. If R is a Euclidean domain then R has universal side divisors.

Example

$R = \mathbb{Z}\left[\frac{(1+\sqrt{-19})}{2}\right]$ is an integral domain which has no universal side divisors and is therefore not a Euclidean domain.