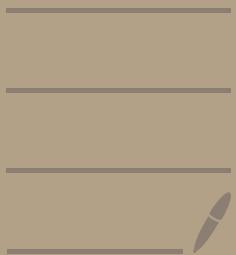


Euclidean domain



Def. $(R, +, \cdot)$ domain R is an Euclidean domain if $\exists f: R \setminus \{0\} \rightarrow \mathbb{N}_0$ s.t. $\forall a, b \in R \setminus \{0\}$ $\exists q, r \in R$ s.t. $a = qb + r$ where $r = 0$ or $f(r) < f(b)$.
 f is called Euclidean function

example: $(\mathbb{Z}, +, \cdot)$ is an Euclidean domain

Prop. If F is a field F is an Euclidean domain.

Prop. $(R, +, \cdot)$ Euclidean domain $\Rightarrow R$ is principle ideal domain

Def. $(R, +, \cdot)$ domain $N: R \rightarrow \mathbb{R}^{>0}$ is a norm if
 $N(x) = 0 \Leftrightarrow x = 0$
 $N(x) = 1 \Leftrightarrow x$ is an unit
 $\forall a, b \in R, N(ab) = N(a)N(b)$

example. Gauss integral ring $\mathbb{Z}[i] = \mathbb{Z}[i\sqrt{-1}] = \{a+bi : a, b \in \mathbb{Z}\}$
 $N(a+bi) = \sqrt{a^2+b^2}$

Prop. $\mathbb{Z}[i]$ is an Euclidean domain.

Proof. suppose $a = x+iy, b = z+iw \in \mathbb{Z}[i]$
 $\exists a, b$ s.t. $\frac{a}{b} = \frac{x+iy}{z+iw} = \frac{xz-yw}{z^2+w^2} + i \frac{xw+yz}{z^2+w^2} \in \mathbb{Q}[i]$

$$\exists m, n \in \mathbb{Z} \text{ s.t. } \begin{cases} \left| m - \frac{xz-yw}{z^2+w^2} \right| \leq \frac{1}{2} \\ \left| n - \frac{xw+yz}{z^2+w^2} \right| \leq \frac{1}{2} \end{cases} \quad (\text{m, n are the closest integer})$$

Suppose $q = mt$ in , $r = a - qb$

To prove $r=0$ or $N(r) < N(b)$

$$r = a - qb = b \left(\frac{a}{b} - q \right) = \left(m - \frac{xz-yw}{z^2+w^2} \right) + t \left(n - \frac{xw+yz}{z^2+w^2} \right)$$

($r \neq 0$)

$$\text{thus } N(r) \leq \left(\frac{1}{2}\right)^t + \left(\frac{1}{2}\right)^s = \frac{1}{2}$$

$$b \neq 0 \quad N(b) \geq 1 \geq N(r)$$

Prop. $(R, +, \cdot)$ domain $N: R \rightarrow \mathbb{N}_0$ norm $x \in R$
 $N(x)$ is a prime $\Rightarrow x$ irreducible