Integral Domains

September 12, 2023 11:34 AM

A commutative ring D with a multiplicative identity 1_D is an <u>integral domain</u> if $\forall a, b \in D$

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0.$$

E.g. $\mathbb{Z}$ ✓ $\quad \mathbb{Z}_6$ ✗ $\quad 2 \cdot 3 = 6 = 0.$

Def. Let D be an int. dom. and $a, b \in D$ with $b \neq 0$. If $\exists q \in D$ s.t. $a = bq$ then we say b divides a written $b | a$ and q is the <u>quotient</u>.

Def. Let $a, b \in D$, $a \neq 0$, $b \neq 0$. An element $g \in D$ is called <u>a</u> greatest common divisor of a and b if
(i) $g | a$ and $g | b$ (g is a common divisor)
(ii) if $h | a$ and $h | b$ then $h | g$.

E.g. in $\mathbb{Z}$ $\gcd(6,4) = \pm 2$ ← the common divisors <u>$\pm 1, \pm 2$</u>.

E.g. in $\mathbb{Q}[x]$ $\gcd(x^2-1, x^3-1) = c(x-1)$. for $c \neq 0$, $c \in \mathbb{Q}$.
$x^2-1 = (x-1)(x+1)$, $\quad x^3-1 = (x-1)(x^2+x+1)$

E.g. in $\mathbb{Z}[x,y]$ $\gcd(x^2-y^2, x^3-y^3) = (x-y)$ or $(y-x)$

How can we compute gcds in $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{Z}[x,y]$.
$\mathbb{Z}$, $\mathbb{Q}[x]$ ↑ Euc. Alg. $\quad \mathbb{Z}[x,y]$ ✗

<u>Euclidean Domains</u>

An integral domain E is a <u>Euclidean domain</u> if $\exists\ v : E \setminus \{0\} \to \mathbb{N} \cup \{0\}$ (Euclidean norm) that satisfies

(i) $\forall a, b \in E \setminus \{0\}$ $\quad v(ab) \geq v(a)$

(ii) ... (Euclidean ÷).

(i) $\forall a,b \in E \setminus \{0\}$ $\quad v(ab) \geq v(a)$

(ii) $\forall a,b \in E$, $b \neq 0$, $\exists q,r \in E$ s.t. (Euclidean $\div$).

$a = bq + r$ where $r = 0$ or $v(r) < v(b)$.

Example. $\mathbb{Z}$ $\quad v(a) = |a|$ $\quad |ab| = |a| \cdot |b| \geq |a|$ ✓

$a \div b$. $\quad a = \underline{b}q + \underline{r}$ s.t. $0 \leq r < \underline{b}$. ✓ $b > 0$.

$13 \div 5$: $\quad 13 = 5 \cdot 2 + 3$ $\quad |3| < |5|$

$13 \div -5$: $\quad 13 = (-5)(-2) + 3$ $\quad |3| < |-5|$

$13 = (-5)(-3) - 2$ $\quad |-2| < |-5|$.

Example $F[x]$ where F is any field e.g. $F = \mathbb{Q}$.

$v(a) = \deg(a)$. $\quad \deg(a \cdot b) = \underset{\geq 0}{\deg(a)} + \underset{\geq 0}{\deg(b)} \geq \deg(a)$.

$v(ab) \geq v(a)$.

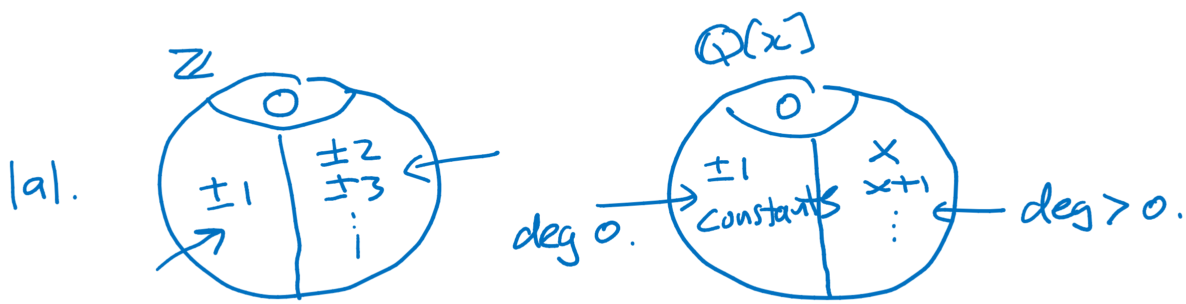
$a = bq + r$ $\quad r = 0$ or $\deg(r) < \deg(b)$.

Lemma. Let E be a Euclidean domain, u be a unit in E and $c \neq 0$ and not a unit in E. Then

(i) $v(u) = v(1)$.

(ii) $v(u) < v(c)$. [units are the smallest elements in E]

(iii) $v(u \cdot c) = v(c)$.



Example 3. Gaussian integers

$\mathbb{Z}[i] = \{ a + bi : i^2 = -1,\ a, b \in \mathbb{Z} \}$

units ± 1, $\pm i$.