Lecture 4 Division in Integral Domains

January 21, 2021 12:01 PM

Assignment #1 due Monday @ 11pm

Office hours	Me	Tian
Friday	9am–10am	10am–11am.
Monday	9am–10am	10am–11am.

In $\mathbb{Z}$ $ab=0 \Rightarrow a=0$ or $b=0$

In $\mathbb{Z}_6$ $\underline{2}\cdot\underline{3}=0$

In $\mathbb{Z}$ $\cancel{a}x=\cancel{a}y$ and $a\neq 0 \Rightarrow x=y$.

In $\mathbb{Z}_6$ $\underline{2\cdot 1}=\underline{2\cdot 4}=2$

Def Let R be a ring and $a,b,c \in R$.

If $a\neq 0$ and $b\neq 0$ and $ab=0$ we say a and b are <u>zero divisors</u>.

If $a\neq 0$ and $ab=ac \Rightarrow b=c$ we say the <u>cacellation law holds</u>

Lemma. A ring has no zero divisors $\Leftrightarrow$ the cancellation law holds.

Proof ($\Rightarrow$). Given R has no z.d.s. Let $a,b,c \in R$.

$$\underset{a\neq 0}{ab=ac} \Rightarrow ab-ac=0 \Rightarrow \underset{\neq 0}{a}(\underline{b-c})=0 \underset{R \text{ has no z.d.s}}{\Rightarrow} b-c=0 \Rightarrow b=c.$$

($\Leftarrow$) Exercise: $ab=0 \Rightarrow a\cdot b=a\cdot 0$.

Def A commutative ring (with 1_R) D is an <u>integral domain</u> if D has no zero divisors. (if the CAN. LAW holds).

Theorem. If $\overset{\mathbb{Z}}{D}$ is an int. dom. then $\overset{\mathbb{Z}[x]}{\underline{D}[x]}$ is an int. dom.

Proof. Let a,b be non-zero polynomials in $D[x]$.

So $a=\underline{a_n x}^{n \leftarrow \deg a}+\cdots+a_1 x+a_0$ where $a_n\neq 0$ and $n\geq 0$.

and $b=b_m x^{m\leftarrow \deg b.}+\cdots+b_1 x+b_0$ where $b_m\neq 0$ and $m\geq 0$.

$a \cdot b = a_n \cdot b_m x^{n+m} + \cdots + a_0 b_0 \neq 0$. so $D[x]$ has no z.d.s.
$\cdot \overset{\#}{0}$ (D has no z.d.s.)

In $D[x]$ $\deg(a \cdot b) = n+m = \deg a + \deg b$.

Divisision and Factorization in Int. Doms. 2.3

Let D be an int. dom. A non-zero element $b \in D$ is a divisor of $a \in D$ if $\exists q \in D$ s.t. $a = bq$ (b divides a).
If b divides a we write $b|a$.
E.g. In $\mathbb{Q}[x]$ $x+1 \mid x^2-1$ because $\underset{a}{x^2-1} = \underset{b}{(x+1)}\underset{q}{(x-1)}$.

Def. Let $a, b, g, d \in D$. g is a greatest common divisor of a and b if

(i) $g|a$ and $g|b$ (g is a common divisor)
(ii) $d|a$ and $d|b \Rightarrow d|g$. (common divisors | g).

Do gcds exist in D? No $\mathbb{Q}[\sin, \cos]/(\sin^2 + \cos^2 - 1)$.

In $\mathbb{Z}$ $\gcd(4, 6) = 2, -2$. $\Rightarrow$ gcds are not unique

In $\mathbb{Q}[x]$ $\gcd(x^3, x^2+x) = x, -x, \frac{1}{2}x, 2x$

Observe: if $g = \gcd(a,b)$ and $h = \gcd(a,b)$ $g|h$ and $h|g$.

Def. Two elements $a, b \in D$ are <u>associates</u> if $a|b$ and $b|a$.
We write $a \sim b$.
E.g. In $\mathbb{Z}$ $2|-2$ and $-2|2$ so $2 \sim -2$.

Lemma. Let $a, b \in D$ with $a \neq 0, b \neq 0$. Then
$a \sim b \Leftrightarrow a = bu$ for some unit $u \in D$.

In $\mathbb{Z}$ $2 = (-2) \cdot (-1)$ and $-1 \in \mathbb{Z}^*$

In $\mathbb{Z}$ $\quad 2 = (-2)\cdot(-1)$ and $-1 \in \mathbb{Z}^*$

Proof. ($\Rightarrow$) $\quad a \sim b \Rightarrow a|b \Rightarrow b = a\cdot c$ for some $c \in D$
$\qquad\qquad\qquad\qquad\quad b|a \Rightarrow a = b\cdot u$ for some $u \in D$

$$a\cdot b = \underline{(bu)\cdot(a\cdot c)} \Rightarrow \cancel{(a\cdot b)}\cdot 1 = \cancel{(a\cdot b)}(u\cdot c)$$
$\times$ is comm.

$\Rightarrow 1 = u\cdot c \Rightarrow u$ is a unit.

($\Leftarrow$). $\quad a = bu$ for u a unit $\Rightarrow b|a$

$$a = bu \Rightarrow a\cdot u^{-1} = (bu)u^{-1} \Rightarrow a\cdot u^{-1} = b. \Rightarrow a|b.$$

Therefore $a \sim b$.

Theorem. In an int. dom. D the relation $a \sim b$ is an equivalence relation. Therefore $\sim$ partitions the non-zero elements of D into into equivalence classes called associate classes.

E.g. $\mathbb{Z}\setminus\{0\} = \{1,-1\} \cup \{2,-2\} \cup \{3,-3\} \cup \cdots$
these are sets of integers which divide each other.

Let $c \in \mathbb{Q}^*$.

E.g. $\underline{\mathbb{Q}[x]\setminus\{0\}} = \mathbb{Q}\setminus\{0\} \cup \{c\,x\} \cup \{c(x+1)\} \cup \cdots$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \{c(2x+3)\}$

$$\gcd(2x+3, \underline{4x+6}) = 2x+3$$
$$= 2(2x+3) = 1\cdot x + \tfrac{3}{2}$$

Def Let $n : D\setminus\{0\} \to D$ be a function s.t. $n(a)$ returns the "canonical" or "standard" representative from the associate class with a. Let $u : D\setminus\{0\} \to D$ return the unit in D s.t. $a = n(a)\cdot u(a) \Rightarrow \underline{n(a)} = a/u(a)$.

$\gcd(4,6) = \pm 2$.

Ex: 1. $\mathbb{Z}$ $\quad n(a) = |a|$ and $u(a) = \text{sign}(a)$.

2. $\mathbb{Q}$ $\quad n(a) = 1 \quad u(a) = a. \qquad \gcd(\tfrac{2}{3}, \tfrac{4}{5}) = 1.$

3. $D[x]$ $\quad u(a) = u(\text{lcoeff}(a)) \quad n(a) = a/u(a).$

E.g. Let $a = -4x+6$

in $\mathbb{Q}[x]$ $\quad u(a) = -4 \quad n(a) = 1\cdot x - \frac{6}{4} = x - \frac{3}{2}$

in $\mathbb{Z}[x]$ $\quad u(a) = u(-4) = -1. \quad n(a) = +4x - 6.$