Integral Domains

Definition: A **zero-divisor** is a nonzero element of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition: An **integral domain** is a commutative ring with unity and no zero-divisors.

Note: In an integral domain, a product is 0 only if one of the factors is zero.

Examples:

- $\mathbb{Z}[x]$, the ring of polynomials with integer coefficients is an integral domain.
- $\mathbb{Z}_p$ of integers modulo a prime p is an integral domain.

- The ring $\mathbb{Z}_n$ of integers modulo n is not an integral domain when n is not prime.

(e.g. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ $\quad 2 \cdot 2 = 0 \bmod 4$)

- The ring $M_2(\mathbb{Z})$ of 2×2 matrices over integers is not an integral domain

(e.g. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$)

Remark: Note that, in general, the nonzero elements do not form a group under multiplication (e.g. elements might not have inverses). But integral domains allow cancellation:

Theorem: Let $a, b,$ and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Proof: $ab = ac \Rightarrow ab - ac = 0 \Rightarrow$

$a(b-c) = 0 \Rightarrow a = 0$ or $b = c$

since $a \neq 0$ we have $b = c$

□

MTH 339

Definition: A field is a commutative ring with unity in which every nonzero element is a unit.

Clearly, every field is an integral domain. To see this, assume $a \neq 0$ and $ab = 0$. Then $a^{-1}ab = a^{-1}0 = 0$ so $b = 0$. In a field, we often write $ab^{-1} = \frac{a}{b}$ ("a divided by b").

Theorem: A finite integral domain is a field.

Proof: Let D be a finite integral domain with unity 1. Let $a \in D$, $a \neq 0$. We need to show that a is a unit. If $a = 1$, there is nothing to prove. Assume $a \neq 1$. Consider the sequence $a, a^2, a^3, \ldots$
Since D is finite, there are positive integers i, j with $i > j$ and $a^i = a^j$.

From $a^i = a^j$, we use cancellation to show $a^{i-j} = 1$. Since $a \neq 1$, we know that $i-j > 1$ and a^{i-j-1} is the inverse of a.

□

Corollary: $\mathbb{Z}_p$ is a Field

For every prime p, $\mathbb{Z}_p$, the ring of integers modulo p is a field.

Proof: We only need to prove that $\mathbb{Z}_p$ has no zero-divisors. So, suppose that $a, b \in \mathbb{Z}_p$ and $ab = 0$. Since $ab \in \mathbb{Z}_p$, there is a k such that $ab = pk$. By Euclid's Lemma, $p \mid a$ or $p \mid b$. Thus, in $\mathbb{Z}_p$, $a = 0$ or $b = 0$

□

Example: • $\mathbb{Z}_5[i] = \{a+bi \mid a,b \in \mathbb{Z}_5,\ i^2=-1\}$ is not an integral domain as

$(1+2i)(1-2i) = 1 - 4i^2 = 0 \mod 5.$

• $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ is a Field. We need to show the existence of inverse elements;

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

Definition: Characteristic of a Ring

The characteristic of a ring R is the least positive integer n such that $n \cdot x = 0$ for all $x \in R$. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\operatorname{char} R$.

Examples:
- $\mathbb{Z}$ has the characteristic 0 and
- $\mathbb{Z}_n$ has the characteristic n.
- $\mathbb{Z}_2[x]$ has characteristic 2 (do now!)

Theorem: Let R be a ring with unity 1. If 1 has infinite order under addition, then $\text{char } R = 0$. If 1 has order n under addition, then $\text{char } R = n$.

Proof: If 1 has infinite order, there is no n such that $n \cdot 1 = 0$, so $\text{char } R = 0$.

Now suppose that 1 has additive order n. Then $n \cdot 1 = 0$ and n is the least positive integer with this property. For any $x \in R$ we have

$$n \cdot x = x + x + \cdots + x \quad (n \text{ summands})$$
$$= 1x + 1x + \cdots + 1x$$
$$= (1 + 1 + 1 \cdots 1)x$$
$$= (n \cdot 1)x = 0x = 0 \Rightarrow \text{char } R = n$$

□

MTH 339

7/8

Theorem: Characteristic of an Integral Domain

The characteristic of an integral domain is 0 or prime.

Proof: We show that if the additive order of 1 is finite, it must be prime.

Suppose 1 has order n and $n = st$, where $1 \leq s, t \leq n$, so

$$0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1)$$

(refers to ex 15, → do now)

Therefore, we have $s \cdot 1 = 0$ or $t \cdot 1 = 0$.

Since n is the least positive integer with the property that $n \cdot 1 = 0$, we have $s = n$ or $t = n$. Thus, n is prime

□

Remark: We are often interested in polynomials with coefficients from a ring. This gets difficult if we have zero-divisors.

Consider $x^2 - 4x + 3 = 0$ in $\mathbb{Z}[x]$.

Then, we can find all solutions by factoring

$$x^2 - 4x + 3 = 0, \quad (x-3)(x-1) = 0$$

$$\Rightarrow \quad x = 3 \quad \text{or} \quad x = 1$$

In $\mathbb{Z}_{12}$, however, we have pairs of nonzero elements whose products are zero:

$2 \cdot 6 = 0 \mod 12$, $3 \cdot 4 = 0 \mod 12$, etc.

To solve $x^2 - 4x + 3 = 0$ in $\mathbb{Z}_{12}$, we can try each element and find $1, 3, 7, 9$ are solutions.

In $\mathbb{Z}_{11}$ or $\mathbb{Z}_{13}$ we only have 1 and 3 as $\mathbb{Z}_{11}$ and $\mathbb{Z}_{13}$ are integral domains

MTH 339 - Do now

1./ Show that $\mathbb{Z}_2[x]$ has characteristic 2.

($p \in \mathbb{Z}_2[x] = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

$2 \cdot p = 2a_n x^n + 2a_{n-1} x^{n-1} + \cdots + 2a_1 x + 2a_0$

$= 0 \pmod 2$)

2./ Consider $M_2(2\mathbb{Z})$. What are the elements, does it have a unity? What is its characteristic?

($\begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix}$, does not have unity, characteristic 0)

3./ (Ex 15, ch 12, p. 262)

If $a, b \in R$ (ring R) and let m be an integer

Prove that $m \cdot (ab) = (m \cdot a) b = a (m \cdot b)$.

MTH 339 - HW

1./ Show that every nonzero element of $\mathbb{Z}_n$ is a unit or a zero-divisor.

2./ In $\mathbb{Z}_7$, give a reasonable interpretation for the expressions $1/2$, $-2/3$, $\sqrt{-3}$, and $1/6$.

3./ Let a belong to a R with unity and suppose that $a^n = 0$ for some n. (Such an element is called nilpotent). Prove that $1-a$ has a multiplicative inverse in R.) Hint: Consider $(1-a)(1+a+a^2+\cdots+a^{n-1})$.

4./ Show that the nilpotent elements of a commutative ring form a subring.

5./ Show that $\mathbb{Z}_n$ has a nonzero nilpotent element if and only if n is divisible by the square of some prime

6./ Let $R = \{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10. Prove that R is a field.

MTH 339 - HW

7./ Let F be a field of order 2^n.
Prove that $\text{char } F = 2$. Is this statement true if 2 is replaced by any prime p?

8./ Show that any finite field has order p^n, where p is a prime.
(Hint: use facts about finite Abelian groups)