Section 19 – Integral domains

Instructor: Yifan Yang

Spring 2007

Observation and motivation

- There are rings in which $ab = 0$ implies $a = 0$ or $b = 0$. For examples, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}[x]$ are all such rings.
- There are also ring in which there exist some a, b such that $a, b \neq 0$, but $ab = 0$. For example, in $\mathbb{Z}_6$ we have $2 \cdot 3 = 0$. Also, in $M_2(\mathbb{R})$ we have $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- In the first cases, an equation of the form $(x - a)(x - b) = 0$ has exactly two solutions a and b since $(x - a)(x - b) = 0$ implies $x - a = 0$ or $x - b = 0$.
- In the second cases, an equation $(x - a)(x - b) = 0$ may have more than two solutions. For example, $2, 3, 6, 11$ are all solutions of $(x - 2)(x - 3) = 0$ in $\mathbb{Z}_{12}$.
- This shows that the these two classes of rings are fundamentally different.

Divisors of zero

Definition
If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are divisors of zero (or zero divisors).

Example
1. 2, 3, 4, are all zero divisors in $\mathbb{Z}_6$.
2. The matrices $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are zero divisors in $M_2(\mathbb{R})$.

Zero divisors of $\mathbb{Z}_n$

Theorem (19.3)

The zero divisors of $\mathbb{Z}_n$ are precisely the nonzero elements that are not relatively prime to n.

Corollary (19.4)

If p is a prime, then $\mathbb{Z}_p$ has no zero divisors.

Proof of Theorem 19.3

- Case $\gcd(m, n) = d > 1$. We have

$$m\left(\frac{n}{d}\right) = n\left(\frac{m}{d}\right) = 0,$$

  and m is a zero divisor.
- Case $\gcd(m, n) = 1$. Assume that $mk = 0$ in $\mathbb{Z}_n$, i.e., $n|mk$. Since m is relatively prime to n, we have $n|k$, i.e., $k = 0$ in $\mathbb{Z}_n$. We see that m is not a zero divisor. □

Cancellation law

Theorem (19.5)

The cancellation law (i.e., $ab = ac, a \neq 0 \Rightarrow b = c$) holds for a ring R if and only if R has no zero divisors.

Proof.

- $\Rightarrow$. Assume that the cancellation law holds, but $ab = 0$ for some $a, b \neq 0$. Then we have $ab = 0 = a0$, but $b \neq 0$, which is a contradiction.
- $\Leftarrow$. Assume that R has no zero divisors. If $ab = ac$ and $a \neq 0$, then $ab - ac = 0$, which, by the distributive law, gives $a(b - c) = 0$. Since R has no zero divisors and a is assumed to be nonzero, we have $b - c = 0$ and thus $b = c$.

□

Remarks

- Let R be a ring with zero divisors. Even if $ab = ac$ and $a \neq 0$ do not imply $b = c$ for general $a, b, c \in R$, the cancellation law still holds for the cases when a has a multiplicative inverse.

  For example, in $\mathbb{Z}_{15}$, $2a = 2b$ still implies $a = b$ since 2 is relatively prime to 15.

  Also, if A is an invertible matrix in $M_2(\mathbb{R})$, then $AB = AC$ still implies $B = C$.

- If R is a ring with no zero divisors, then the equation $ax = b$ has at most one solution in R.

Notation b/a

Suppose that R is a commutative ring with no zero divisors, and that a is a unit in R. Then the equation $ax = b$ has exactly one solution $a^{-1}b$. For convenience, we let b/a denote this element $a^{-1}b$. The notation $1/a$ will denote a^{-1} in this case.

However, when R is not commutative, we do not use this notation because we do not know whether b/a means $a^{-1}b$ or ba^{-1}.

Integral domains

Definition

A commutative ring R with unity $1 \neq 0$ that has no zero divisors is an integral domain.

Example

1. The ring of integers $\mathbb{Z}$ is an integral domain. In fact, this is why we call such rings “integral” domains.
2. If p is a prime, then $\mathbb{Z}_p$ is an integral domain. On the other hand, if n is composite, then $\mathbb{Z}_n$ is not an integral domain.
3. The direct product $R \times S$ of two nonzero rings R and S is never an integral domain since $(r, 0)(0, s) = (0, 0)$ for all $r \in R$ and $s \in S$.

Fields are integral domains

Theorem (19.9)

Every field F is an integral domain.

Proof.

Suppose that $a, b \in F$ is such that $ab = 0$. We need to show that if $a \neq 0$, then $b = 0$. By the associativity of multiplication, we have

$$0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b.$$

This proves the theorem. $\square$

Finite integral domains are fields

Theorem (19.11)

Every finite integral domain D is a field.

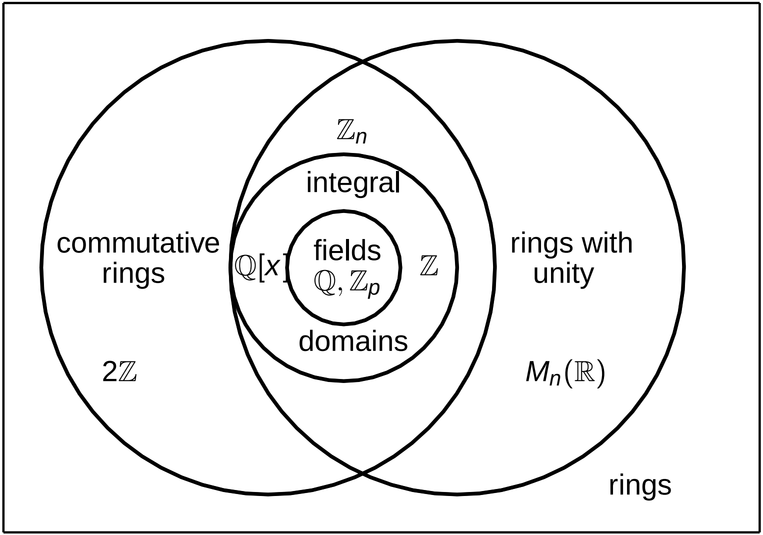
Corollary (19.12)

If p is a prime, then $\mathbb{Z}_p$ is a field.

Proof of Theorem 19.11

- We need to show that every nonzero element a of D has a multiplicative inverse.
- Let $0, 1, a_1, \ldots, a_n$ be all the elements of the finite integral domain D.
- Consider the products $0 = a0, a = a1, aa_1, \ldots, aa_n$.
- These products are all distinct since $ab = ac$ implies $b = c$ by Theorem 19.5.
- Thus, $0, a, aa_1, \ldots, aa_n$ must be all the elements of D.
- One of these must be 1, i.e., $aa_i = 1$ for some a_i. This proves the theorem. $\square$

Relations between various rings



In-class exercises

1. Find all solutions of $x^3 - 2x^2 - 3x = 0$ in $\mathbb{Z}_{12}$.
2. Characterize all the zero divisors of $M_2(\mathbb{R})$.
3. Let F be the set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ with addition and multiplication given by

$$f + g : x \mapsto f(x) + g(x), \qquad f \cdot g : x \mapsto f(x)g(x).$$

   Find the proper place for F in the diagram on the last page.

The characteristic of a ring

Definition

Let R be a ring. Suppose that there is a positive integer n such that $n \cdot a = 0$ for all $a \in R$. The least such positive integer is the characteristic of the ring R. If no such positive integer exists, then R is of characteristic 0.

Example

1. The rings $\mathbb{Z}_n$ are of characteristic n.
2. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all of characteristic 0.

The characteristic of a ring

Theorem (19.15)

Let R be a ring with unity. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$, then R has characteristic 0. If $n \cdot 1 = 0$ for some $n \in \mathbb{Z}^+$, then the smallest such integer n is the characteristic of R.

Proof.

If $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$, then R is clearly of characteristic 0, by definition.
If $n \cdot 1 = 0$ for some $n \in \mathbb{Z}^+$, then for all $a \in R$, we have

$$n \cdot a = (a + \cdots + a) = a(1 + \cdots + 1) = a(n \cdot 1) = a0 = 0.$$

Then the theorem follows. □

Homework

Problems 2, 10, 12, 23, 27, 28, 29, 30 of Section 19.